eForensics Magazine

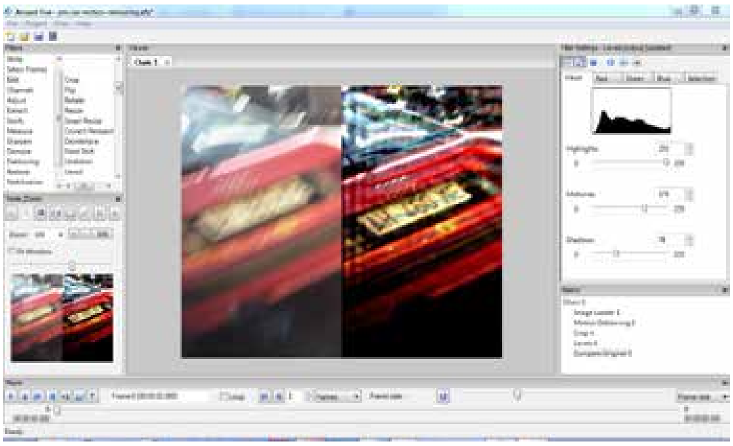
Network

VOL. 1 NO. 1

CAPTURING REAL-TIME INSTANT MESSAGES WITH PACKET CAPTURE TECHNOLOGIES

- WHATS SO DIFFERENT ABOUT CYBERCRIME
- A WINDOW INTO THE WORLD OF SUPERVISING DETECTIVE INVESTIGATOR SHAUN WINTER
- PACKET CAPTURING FOR FORENSICS INVESTIGATIONS

Issue 22/2012 (1) August



AMPED
FIVE
THE FORENSIC IMAGE PROCESSING SOFTWARE
ANALYZE RESTORE ENHANCE CERTIFY
AMPED
FIVE

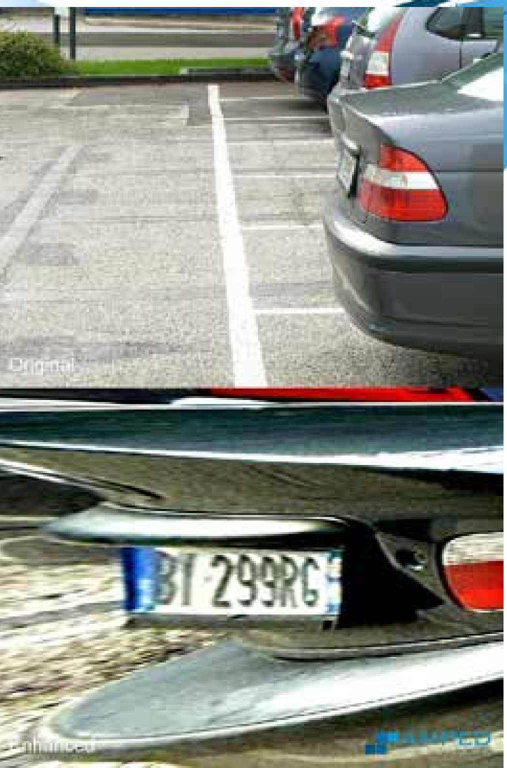
- Designed from top to bottom as a purpose built self-contained tool for forensic needs

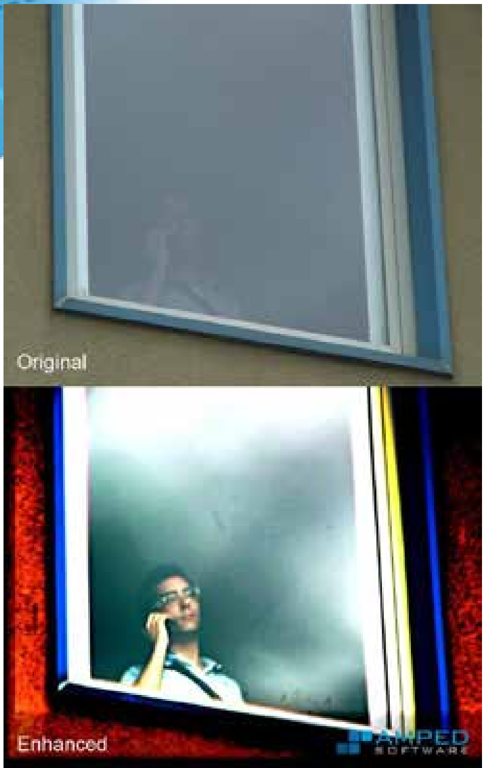
- Support for images, videos and live streams
  Integrated lossless DVR capture tool
  Native support for Milestone XProtect® surveillance live feeds and archived files

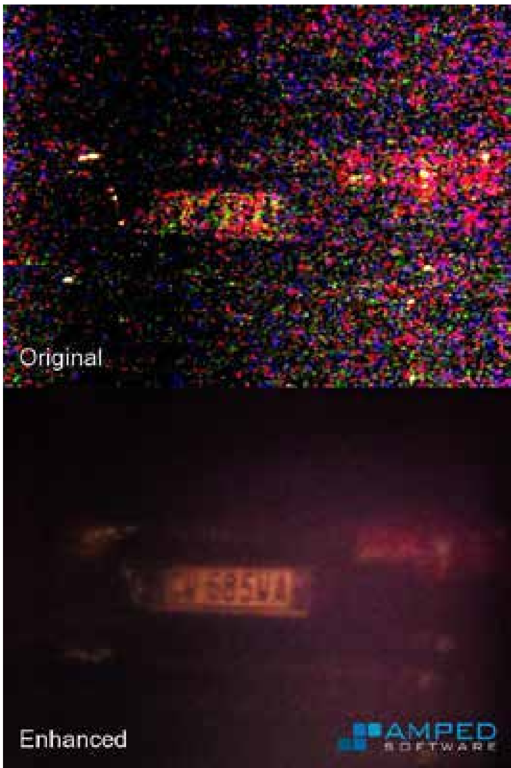
- More than 70 filters for sharpening, denoising, integration, format conversion, distortion correction, image stabilization, Fourier transform, image resizing, intensity adjustments, super resolution, perspective correction...

- Optimized workflow for quick and scientific processing

- Unique concept of filters: Drop, add, delete, modify, move, copy, paste, any filter in any position. Modify any parameter of any operation in any order; the results can be applied and seen immediately, even while playing a video
- One solution with tools for all types of work. From CCTV to intelligence operations video or latent fingerprints and document comparisons, Amped Five can do it all







eForensics Magazine

TEAM

Editor: Kamil Kaczorowski
kamil.kaczorowski@software.com.pl

Betatesters/Proofreaders: Olivier Caleff, Akash Rosen, Sheri Lee, Derek Thomas, Cindy Brodie, Dan Dieterle, Matthew Harvey,Mada R. Perdhana, Danilo Massa, Jan-Tilo Kirchhoff, Roshan Harneker, Nick Miter, Sailaja Aduri, Andy Gibison, Nicolas Villatte, Marcelo Zúñiga Torres, Joshua Williams, Pardhasaradhi,

Senior Consultant/Publisher: Paweł Marciniak

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

Art Director: *Mateusz Jagielski*
mateuszjagielski@gmail.com
DTP: Mateusz Jagielski

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

Marketing Director: Ewa Dudzic

Publisher: Software Media Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.eforensicsmag.com

DISCLAIMER!

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

Dear Readers!

My name is Kamil and I am responsible for eForensics Magazine – Network. Finally, the work is done and I have to say that I am very proud to present first issue of our magazine to you, dear readers. It was a big effort for me to coordinate the work on the magazine but with help of people involved in this project we have succeeded. Our Magazine is in an initial phase but I can assure you that we are going to work on development of the magazine even harder to provide you with latest news from digital forensics world. I would like to thank everybody involved in this project, it is a real pleasure to work with specialists such as eForensic Team and I hope we will work together long time.

The magazine is created by professionals from around the world and thanks to their shared effort we can present to you cutting-edge technologies and solutions. Although this part of eForensics magazine is focused on network forensics, we included an article that may not be necessary involved in the subject. In our very fast paced world, people need information about high technologies and for that reason we created eForensics. We also want to create a community of people interested in digital forensics and I am sure that will happen. Every day I am receiving more and more emails from people who would like to contribute to the magazine by publishing articles. I would like to thank all of you for that effort which I really appreciate and I will try my best in giving you such opportunity.

Our main goal is to publish practical articles about latest news from digital forensics field and for that reason we are constantly looking for forensic experts who would like to be part of our community. Internet has been dynamically developing over last decade and does not seem to be slowing down in any near future. Most of the globe population have access to the Internet including various kind of criminals that are out there to steal our personal details, identity and money. Network Forensics is a forensic science which goal is to investigate cases of Internet misuse and making it better place.

Enjoy reading!

Kamil Kaczorowski
& eForensics Team

INTERVIEW OF THE ISSUE:

NETWORK

MEDIA:

A WINDOW INTO THE WORLD OF SUPERVISING DETECTIVE INVESTIGATOR SHAUN WINTER

by Liora Farkovitz

Supervising Detective Investigator, Shaun Winter, has been working with the Brooklyn District Attorney's office in New York as head of the Special Investigations Unit Computer Forensics Lab for more than eighteen years. A position many people would consider the Crème de le Crème in the digital forensics field, S. I. Winters has come to take it all in stride. His emergence in this role as a senior technology professional was built upon a foundation of traditional investigatory skills. As is the case with any municipal agency, Winter is challenged by limited resources, an exponential demand on his department's expertise, and the inevitable technophobia that most forensic investigators are forced to overcome.

While initially forensic investigation demands were more isolated to crimes where the computer was a central tool used in the commission of a crime, like enticement crimes on the part of pedophiles, as the gulf between the different types of devices we use every day have begun to overlap, so have the sources of available evidence. Yet how we treat the differences in these devices in order to maintain forensic integrity is vital. Supervising Inspector Winter generously shared a window into his every day world with eForensics Magazine for this debut article in August of 2012.

For students and professionals that are interested in pursuing a career in digital forensics, this interview should provide enlightening and interesting perspectives about the public service provided by S. I. Shaun Winter.

LF: Did you go into your police work with the intention of protecting children in particular or is that just something that evolved?

SW: It evolved. When I got promoted to Supervisor of the Computer Crimes Unit, and the unit consisted of one investigator and one supervisor, me being both roles, it was a natural function for me to investigate enticement cases and things of that nature. I became involved early on at the outset of my appointment to this position and put a good amount of time, effort, energy and focus on doing online chats as an undercover agent, identifying individuals who would be willing to meet or exchange pornography, with whom they clearly thought was a minor. Not only did it go from pornography, I've done several child pornography cases and was able to utilize outside state sources and resources to actually prosecute these cases. So I've done a couple of federal cases involving child pornography. It just became a natural progression.

LF: We both graduated [from High School], around 1980 and probably watched as technology came along. I graduated from school [University] with a degree in Social Work with the intention of working with this population and helping kids that were drug-addicted or sexually abused overcome those kinds of problems. But when I got out of school, Reagan had just been re-elected and there were no jobs available in that field. So I ended up going into technology, because I am just good at it. I have a natural sort of knack for it.

SW: I share that. I was not looking forward to doing this. It was basically, 'You're going to be the supervisor for the Computer Crimes Unit because you know how to turn a computer on and turn it off.' That was my starting point. I now supervise the Computer Forensics Unit and I also supervise our Technical Surveillance Unit, which covers our wiretaps and all the equipment used for undercover purposes.

LF: I would love your job. I would really love it, doing that.

SW: I tell you, I am well-rounded, well-versed, but the way Computer Forensics is required much more frequently, our whole team is challenged to meet the demand. As soon as we get more resources, we are suddenly short again because the demand has increased. It's just the way it works out in this field - that really is where this is all at now.

LF: Exactly.

SW: And it's hard to explain that, you know, what you used to understand – I've been in this office for almost 18 years. I've spent a lot of years following people in the car and doing it the old-fashioned way, so I do understand how that functions. But times have changed.

LF: But don't you think there's sort of a similarity between the way that you follow someone in a car and the way that you look at say their – if you want to use more of a technical term - their "footprint"?

SW: Oh yes. You can track and see, and even from a forensics perspective. I also teach at a two-year college, and I explain to my students from a forensics perspective we are all creatures of habit. Human beings are that way by nature, and our behavior is very easy to see on a computer. I always look for what's the anomaly? I always look for what's different, only because it's very simple to see that if someone's into child pornography, you're going to see those folders with those names setup with the various folders or images or videos. That's the nature of the mind, because we are structured in our minds and we structure how we want to find things later. So I always look for the opposite, because we are. The footprint is there. It's very easy to see if you understand what you're looking for.

LF: So, is most of the work that you do isolated to the storage compartment of a device? Or are you correlating what's on the device with what you see as their Internet activity? When you're like… I'm supposed to isolate this to smart phones, but I mean…

SW: Well I mean, smart phones have become a computer. Androids are a computer. iPhones are computers now. Nobody walks around with the old-fashioned, 'I can only make a phone call with this thing' cell phone.

So you actually can look, and in a limited context. I mean, you're not looking at a desktop which is expansive in what it retains. But you are looking at the iPhone or you are looking at the Android and you're going, 'Okay, fine, I'm looking for certain files. I'm looking for where they're stored.'

The key is these phones retain GPS.

In analyzing the contents of the phone, the first time through I may have missed something. When I looked at it again, I said, 'Ah!', because I realized I was able to utilize the GPS functions in this phone to correlate location with other evidence found in the overall case, because there it was on the phone.

And that's your footprint in a cleaner sense, and in a more modern, technological sense as far as identifying where somebody was without physically being there to see this.

LF: On the GPS information, just because I'm not the technician here, could you tell just the fact that they [the suspect] were there, or could you tell how long they were there? Did you have a series of pings on the GPS system that would tell you they were at a certain location from say, 2:38 to 3:15?

SW: It won't give you lengths or periods of time. It's going to associate – in this particular example, it may associate a filename. It could be a photo. You take a photo and the phone is saying, 'This photo was taken here'. So you can focalize and localize where a particular activity or event occurred.

So, it's kind of like the acquisition aspect of it, because you want to make sure you acquire your evidence cleanly, which is forensically sound. You're not changing the phone; you're not adding to the phone; you're acquiring it just as you had received it and then it's the progression of, 'Okay, fine, what is on this device? Let me look at this…'

Are we dealing with a case where somebody's got [Village Voice] Back Page ads? Or you can see a web history for Back Page ads? You can actually see where there's a screenshot, and some phones actually do these automatic screenshots and you actually see that particular evidence sitting on the device still - when you now have it to review as your evidence be it six months, or a year later.

LF: So this automatic picture , this is taken by the smart phone itself?

SW: Yeah, I'm seeing some phones, you can actually take your screenshot as if you were at your desktop or the phone does a temporary save. So there are times you'll see messages on the phone in the context of an exchange.

LF: And it's a temporary screenshot?

SW: Right, it's a screenshot. So there's a multitude of things that phones now give you that they didn't give us say four years ago, five years ago. I mean our generation – and you're speaking about our generation [50ish] – we have been the most fortunate generation to see this tremendous advance in technology.

LF: Amazing.

SW: When we were in college, I don't know if you had an electric typewriter. I had an old Royal typewriter. I still have that Royal typewriter, alright.

LF: No, I didn't have a computer. I wrote everything by hand. But when I did go to work in the work force, I went to work for this attorney named David Kaplan and he had the only IBM PC XT in our home town, and so I learned everything from no hard drive, no nothing.

SW: Right. I had my professor; I bought his old Royal – manual – from him, for $40 dollars. And I still have that typewriter, and I tell my children to stay away from that typewriter. Don't touch it; don't break it. That's your father's prized possession. It got him through college. And here we are, when I progressed into the work force, my first exposure to computers, aside from a computer class that I took in undergraduate school, which I hated , (I've always hated computers and I still hate computers), but it was MSDOS. You had to know DOS prompts just to work your way through the system.

LF: I know, I know. I still remember the commands.

SW: Right, so you know, you think about it and that's just in the desktop realm of the world. Windows revolutionized how we get to our data. But now think of phones and phones are that next progression of revolution in communications and digital storage.

LF: I don't get rid of my phones because I have too much data that I need to extract from them before I get rid of them.

SW: Right, it's a walking computer.

LF: It's a record of my life, the last four phones that I have. So on the technical side, I love the technology and I enjoy it and I like the problem solving. I used to always say that social work and technology were similar in that it was the same kind of problem solving. You were still putting the pieces of the puzzle together; just the computers didn't talk back in the same way. They weren't as difficult to get along with as some people!

SW: Sometimes. Sometimes.

LF: Sometimes. Sometimes. So is there a particular type of software that you prefer to use?

SW: For telephones? For phones? We use Cellebrite. Cellebrite is the primary market tool for digital forensic acquisitions of cellular devices.

LF: Do you use any other product to compare against what they provide? Or you're so confident in what Cellebrite provides that you don't look at anything else at all?

SW: We had some other tools but they weren't as dynamic as Cellebrite was. I mean there was Paraben, EnCase which was at the forefront of desktop forensic tools also came out with their own phone acquisition tool. In this field, because these tools are so unique, they're also very costly. So Cellebrite was a good investment tool. We use some software tools to compliment what we get from Cellebrite so that it enhances or provides the second viewer … not me. I review the evidence before I put it on my disk. We have a very good procedure as far as how evidence comes in and how evidence goes out. I review it before I put it on disk before I turn it over to the prosecutor. There are some software tools that enable us to make it more readable, more understandable for the less knowledgeable mind or less knowledgeable eye.

LF: The less sophisticated technology…

SW: Yeah. You try to, in a sense, dummy it down so that you say, 'Okay, fine, this is what you want. You see it here and you see it here and you see it here.' And they go, 'Oh, now I understand!"

LF: Right. I find myself having to do the same kind of thing. I try to use somebody's real-world work in life to give them something to compare, 'This is like filing in a filing cabinet or this is like long-distance was…' or something along those lines to help them have a point of reference.

One of the things I was going to ask you, because kids that are – and when I say kids, I'm going to say anyone under 21 roughly – have grown up with cell phones. Most of the kids that I know have had cell phones of their own since they were in elementary school. And now that the phones are so sophisticated, they're really not thinking about them in terms of what the capability of the software or the hardware is, they're just thinking of what's "cool" in their pocket.

SW: What I can get to while I have my phone, yes, Facebook and things of that nature.

LF: Right. How are the phones being used by kids that are under 21 or so today in crimes or in other capacities that surprise you? What are the most surprising things that you see them doing with phones today?

SW: Taking pictures of themselves and the communications via text messages.

LF: The sexting you mean?

SW: Sexting, the storage of photographs of themselves that might be compromising in a sense. That seems to be one of the big things. And you know, then also the sites they go into, Facebook being in particular the one… I see the range as far as what these are capable of doing, and what I see in evidence purposes, is a lot of young individuals where they do that, the sexting and things of that nature. We've had quite a few human trafficking cases involving young individuals and that's where the appointments are being setup and things of that nature via text messages.

LF: Right. I mean the text message is almost replacing the phone call.

SW: Yes, yes.

LF: I use it quite a lot, mostly because it gives that person an opportunity to answer at their convenience instead of having to give me their full attention when they may have other things they need to do.

SW: The other side also, if you think about it, initially email replaced conversations.

LF: True.

SW: Instant messaging replaced conversations. Text messaging is that next progression, because some phones do have instant messaging capabilities be it AOL, Yahoo, whichever version of instant messaging you use(d) but now text messages are okay, 'Fine, it's just me and you. I have your number, you have my contact [information], we've saved, so we go back and forth'.

LF: So what percentage of the cases that are prosecuted – I mean, I guess out of your area would be 100%, but in general out of the DA's office would you say have this kind of data from smart phones or computers?

SW: Oh, quite a bit. I mean in the beginning of the year, we did an analysis of the additional work we've taken on from when I first started the unit. I now have one person that works with me, and we kind of took a look at how much work has come in. And the impact of phones has almost tripled our workload, and now we're seeing more and more smart phones which are sometimes easy to acquire but more problematic because you have to treat them like a computer.

LF: Right, so it's much more time-consuming isn't it?

SW: It is. It's more time-consuming, and you know, when I first started working in this office I serviced just a small component of the office. I now service the entire office, and we're seeing a lot of the trial zones, which traditionally in the past weren't necessarily proactive, they were just, 'Here's an arrest and we'll go to grand jury and we'll go to trial.' But now they're becoming a big component of our forensics because officers are seizing cell phones in the field, vouchering them, bringing them here for analysis and it substantiates the cases.

We had an attempted murder, and the woman used her phone to search for chemicals that could be put into the target, the complaining witness, to poison her. It was a dispute involving a husband having children with two different women. And that phone was it. That phone had everything. That phone essentially resolved the case, where she then took a plea to attempted manslaughter. She's like, 'You're not going to get me. You're not going to get me!' Then all of a sudden with the phone it's like, 'We've got you!!!' and that was from a trial zone case. It wasn't even a proactive investigatory unit in this office; it was basic trial zone work. So it runs the gambit now. It's hard to give a number because it seems to be across the board.

LF: Would you have been able to check the records of this suspect's cell phone carrier and see the same activities on her smartphone?

SW: This was all web browser information, and one of the difficulties especially with cell phones and their usage for Internet purposes is [compared to a desktop unit]– if I was to send an IP request to Sprint for a particular date and time and if I look at your history, you use a particular Yahoo email account. And I ask Outlook to give me all your IPs, and I see you use some Cable Vision which is local and Time Warner which is local and that's pretty much going to tie you to a residence. IPs with cell carriers, you're going to be out of luck because their response to you will be, 'We don't retain that information'.

LF: Carriers don't retain that information? Even for the police department?

SW: No, they don't retain it. You can understand why, because with the millions of phones that are out there it would be a huge undertaking to have servers that can say okay, on this date and time our IP for a cellular device was assigned to that phone which then became this phone maybe hours later. With the advent of Static IP, you have an IP into your house [assigned to the router]. It may stay that way for months; two months, or three months. That's easy for them to retain that.

LF: Because it stays until you reboot your router.

SW: It's static so it's not changing, whereas with a phone, it's perpetually changing.

LF: It's dynamic. It always changes every time you boot it, every time…

SW: Right.

LF: In terms of tips or tools, what would you be willing to share with our readers? Something that would be an interesting technique that you use that helps you, or particular training or organizations that helped you? What would you share with someone that wants to do what you do?

SW: To be in the forensics field – the first thing I would tell everybody, before they got into the forensics field, is that if you do come across any kind of digital media, be it a desktop or a phone, if it's off don't turn it on! If it's on, try to identify what's on and then turn it off and remove the battery, because there are wiping tools now.

You know, iPhone connects 'in the cloud' so if you have a Mac at home and you have an iPhone and you have an iPad, you could actually access the information from one device to the other which provides you the opportunity to wipe the contents of a phone. The other thing also is if you get a phone and you're curious and you don't know the password, a lot of phones if you do one try, two tries, three tries and it's the incorrect password, at a certain point that phone will go, 'You're not the owner of this phone'. Guess what we're doing to the data on the phone?

LF: Oh my gosh, really?

SW: We're wiping it away. So that's the one thing we've seen. We're told 'Well, they turned it on...' And I said 'Don't tell me!!!' That's the key, especially if you're a first responder and you come across digital media. Try to interact with that device as little as possible, because from a forensics perspective, if a device was off and you took it today, when we do the analysis and the imaging and the analysis, we should see from the BIOS the last time it was on wasn't today. Not in-between the two dates, because then we have to explain why it's been altered.

So that's the key to keeping it forensically sound, understanding that these are devices – they are fragile devices, and the minimal contact with them gives us a better opportunity to testify later as to how forensically we obtained the evidence, point one and point two, this is everything that was on the phone before we got it. I think it's ultimately the one point I always try to make is don't turn it on, don't touch it, don't try to figure out the password if you don't know it because those are various aspects of a forensics analysis that will kill it.

LF: That's very interesting. Really, really interesting. Thank you so much for your time today Supervising Inspector Shaun Winter!

SW: You're welcome, my pleasure.

Author bio

Liora Farkovitz is the Founding Partner of Legacy Strategic Development, LLC the developer of TechnologicalEvidence.com. She is the author of "Understanding Technological Evidence for the Legal Professional: 101 the Basics", and co-developer of "The Electronic Advantage" a four hour online training course for attorneys, the judiciary, paralegals and legal parties. This is her debut article with eForensics Magazine. If you have any questions or comments, or suggestions for future articles please contact the author at liora@technologicalevidence.com.

AMPED
FIVE
THE FORENSIC IMAGE PROCESSING SOFTWARE
ANALYZE RESTORE ENHANCE CERTIFY
AMPED
FIVE

Virscent
TECHNOLOGIES
An IIT Kharagpur Alumni Venture

Virscent Technologies Pvt. Ltd., a Brainchild of a team of **IIT Kharagpur Graduates**, has been **Incubated in E-Cell IIT Kharagpur**. It is an IT Solutions & Training Company, Offering Web, Security and Network Solutions, IT Consulting and Support Services to numerous clients across the Globe.

We provide the following services:

a. Penetration Testing
b. Multimedia Services
c. Web Development
d. Training:
  a. Corporate Training
  b. Classroom Training
  c. Training programs for Educational Institutions.

Our Partners:

1. E-Cell IIT Kharagpur
2. Education Project Council of India

Website: www.virscent.com

Blog : www.virscent.com/blog

WHAT'S SO DIFFERENT ABOUT CYBERCRIME?

BOB BIRD

1. THE NATURE, REALITY AND THREATS POSED BY CYBERCRIME & THE DIGITAL ENVIRONMENT.

A personal perspective on the development of eCrime, the problems faced by Law Enforcement in addressing it and what it is telling us about the potential for future success in combating it. The main difference is that the average global police force still needs to be trained and developed into a force to try to combat cyber-criminals. Even today, the police force can't take direct action against some international cyber-criminals without getting their country of origin involved or even acknowledgement that there is a crime and that is where the real crux of the issue lies. Not one country is immune or maybe even knows how to recognize or combat cyber-related crimes. A historical perspective – "And you may ask yourself, Well how I get here?"

The Talking Heads song "Once in a Lifetime" featured the line: "And you may ask yourself, how did I get here?" which has a certain resonance to my mind with the issue of Cybercrime or eCrime as it appears to be morphing into as we speak. As a classification of offending, it has been in existence only as long as the commercialization of the Internet. Given the all-pervasive nature of the Internet, Cybercrime has been assessed as representing a "Clear and Present danger" (Deloitte 2012). In that context I will seek to present a perspective upon its origins, nature, answer and question if it is different, why and UK Law Enforcement response to it.

There is no universal definition of Cyber Crime, although there tends to be an acceptance of the types of crimes it refers to.

Definitions of cybercrime include:

– the use of any computer network for crime (ACPO UK Police)

– any criminal offence committed against or with the help of a computer network (Council of Europe).

The Association of Chief Police Officer's (ACPO) definition in the UK has recently been modified to refer to e-Crime and states that it is: "The use of networked computers or internet technology to commit or facilitate the commission of crime." This would appear to be as loose and broad as one could possibly seek to define (or not as the case may be) It would then follow that as a proportion of total crime it is: 1) identified as a priority 2) known in terms of numbers of offences and 3) has large numbers of police officers and staff dedicated to its investigation and detection.

I will seek to contextualize this relatively new phenomenon and identify why in respect of the UK its complexity is compounded by the politics of crime and how this has confused the issue.

2. CRIME IN THE UK THE LAST 40 YEARS

The issue of crime is as old as the laws that have been drawn up to combat it. However there is little debate concerning the question as to how crime as an issue dominated political debate during the later decades of the 20th Century. After the Second World War the pace of societal change within Britain was initially tentative with the austerity of the 1950's but as the reign of Queen Elizabeth advanced into the 60's, an era of freedom, growth and relative prosperity began. There was a blip in the 1970's where industrial disputes and economic uncertainty hindered growth but Margaret Thatcher's Conservative government effectively battledwith the unions and won, heralding an era of growth and increased consumer wealth. The arrival of colour televisions, video recorders and availability of motor vehicles signaled the consumer era and this also coincided with an expansion of crime. The criminal opportunities these new consumer goods offered lead to large increases in house burglaries, vehicle related crime and other thefts, collectively known as "volume crime" due to their large numbers. The Labour Party of Tony Blair, after many years in opposition to the conservative government sought to identify how they could be both electable and retain power to implement their political philosophy. Central to this was to remove from the conservatives, their self-appointed status as the "Party of Law and Order." Tony Blair summed it up in his sound bite, "Tough on crime, tough on the causes of crime" identifying the social inequalities that were largely thought as responsible for creating an expansion in crime and criminality. The new Labour government in the late 1990'2 set targets for the police to reduce crime in the key areas of highest crime and bought about a revolution in policing where its effectiveness was measured in detections (how many were caught and convicted) as well as the overall reductions in crime that it was effective in achieving.) Inevitably this success in halting the inexorable rises in crime and perceived effectiveness changed the nature of the political debate. It then became a matter of questioning the statistics provided by the police and whether the reductions claimed where actual; reductions in crime or achieved through “creative accounting.” The UK has 43 independent Police Forces and whilst these operate under the same judicial system, there was a surprising lack of consistency in the way in which they executed their basic functions. This was visually reflected in different uniforms, but less obviously in the ways in which they recorded crime and characterized incidents. The Labour government was keen to standardize and centralize its control of policing and as a result, the National Crime Recording Standard (NCRS) was codified as were the Home Office Counting Rules. In effect these documents and the regime of central scrutiny standardized crime recording and arguably validated crime statistics for the first time. This has resulted from the disparity between the official statistics and the British Crime Survey (BCS). The BCS had initially shown a growing gap between what the Police stated had been reported to them and the estimates gained from interviewing a range of respondents. Incrementally the gap between the BCS and official statistics has narrowed as crime recording remained under close scrutiny.The quarterly and annual publishing of Home Office statistics remained the subject of political debate, but the arguments tended to be on the minutiae of specific crimes and related to what political capital could be made over increases in crimes of public concern e.g. knife and gun crime. So what the hell has this to do with Cybercrime, you might say? Well the reductions in crime and recording procedures were politically effective as an argument regarding their veracity, essentially that they could be believed. However around 2005 when the prospect of increased internet activity and growth was translating itself into criminal opportunity presented as real problem and dilemma for the government and policing. The potential explosion in crime figures in what was an ill-defined, fast moving and poorly understood area meant that no government was likely to welcome new categories of crime that were likely to inflate the numbers and undermine the reductions achieved over a number of years.

3. SECONDARY REPORTING

The key change that has impacted upon Cybercrime in this context is 2 fold. Firstly the Police lost their role as the primary receiver of crime complaints relating to significant areas of crime, which involve Cyber or eCrime. In particular, the credit card companies and banks became primary receivers of this crime recording. In 2007 I was the victim of a fraud where £4000 was transferred from my accounts via a telephone banking scam. I reported it to the bank who recompensed me and their “investigations” branch took the relevant details of a crime that never appeared on any “police” statistics. It is my belief that apart from “locking the stable door after the horse has bolted” i.e. changed their procedures regarding telephone banking which had been the root cause of me becoming a victim, their active investigation was minimal and cursory. Whilst the Victim’s Charter places upon the Police certain responsibilities regarding what a victim of crime should expect in relation to service and information, commercial enterprises are less encumbered. As a commercial entity, banks and credit card companies are sensitive to the publication of the levels of fraud that they fall subject to and are not in the habit of publishing ”crime statistics.” This secondary reporting has meant that official crime statistics have not been skewed to reflect this changed nature of crime but then are arguably particularly unrepresentative of the exact nature of crime in the UK.

4. “SO WHAT IS THE STATE OF ECRIME IN THE UK?”

The vexatious question as to the extent of eCrime is mired in the issue of a lack of counting standard and the fact that buy its nature, victims may not have as yet realised that they have been victimised. The phenomena of “identity theft” and the value of that personal data has changed the nature of criminality in this respect and provided new opportunities for criminals.

PCeU
Police Central e-crime Unit

Deloitte's 2010 White paper Clear and Present Danger, characterised eCrime as being a particular issue in that "Data is more Valuable than Money, Once Spent, money is gone, but data can be used and reused to produce more money. The ability to reuse data to access on-line banking applications, authorize and activate credit cards, or access organization networks has enabled cyber criminals to create an extensive archive of data for ongoing illicit activities." So the creation of a new "commodity" in criminal opportunity terms has been made all the more pertinent by the growth of internet access and broadband communication. In 1996, 3.4 million UK adults were online; by 2006 this had expanded to 28.5 million and as of 2012it is estimated at 41.6 million. Crime in the virtual world was characterised by a triangle of three factors: Victim, Location and offender. The key element in many crimes has been the physical proximity of an offender to the victim. It has been this element that for the "solvability" of crime, that has been for many years key to any police success. The element of the virtual world that by its very nature is the Internet means that these key elements are more intangible in the virtual as against physical world. Whilst Locard's Principle, key to physical forensics that "Every contact leaves a trace" has a good deal of resonance for digital forensics, the "digital dust" that evidences this can be harder to determine. There are various estimates as to the extent of eCrime that dependent upon your point of view either represent an educated "guestimate" or a potentially vast under-estimate. For that reason I choose to quote none, save that a rationale in problem solving is that in order to understand a problem, you first need to quantify it. In the absence of any framework to accurately assess the extent of the problem that is the priority rather than quoting arbitrary estimates of what may be happening.

5. "WHAT GETS MEASURED IS WHAT GETS DONE"

There is a truism that is particularly prevalent within Policing circles and that is "What gets measured is what gets done." That is to say that if you have a target to reduce house burglary by 5% it is likely that you will put effort in terms of personal and investigation into achieving that reduction. Within the UK the focus upon achieving crime reductions and associated targets within the criminal justice system upon convicting offenders, gave the rationale for budgetary priorities and decisions upon core activity. In this respect Cybercrime has always been the "Cinderella" of Policing i.e. the under-funded, under resourced and over looked element that received scant recognition for its importance and relevance. In order to understand why this has occurred, I must briefly give a potted history of the development of "Cyber Policing" or Hi-Tech Crime Units (HTCU) in the UK. Prior to "Operation Ore," Hi-Tech Crime had been the subject of debate, which was generally lost upon senior police management who saw computers as a new and menacing phenomena that they often totally misunderstood. In 2002 Operation Ore was the first nationwide investigation into on line Pedophiles that resulted in UK Police forces receiving significant funding to set up HTCU's.In 2001 the National Hi-Tech Crime Unit (NHTCU) was formed at New Scotland Yard and almost inevitably its Metropolitan Police focus did not encourage other forces to emulate its functions. This had resulted from an initiative from ACPO who identified that this new and burgeoning form of crime had been inadequately addressed by the then responsible agency, the National Crime Squad (NCS). The development of HTCUs had few guidelines with local Forces required to establish and equip them. As a result the small number of officers posted to these duties had varying levels of expertise and ability, but generally battled on heroically as prototype CyberCops. Nationally, the continuing debate amongst politician and senior police officers lead to the NHTCU being subsumed into the renamed and rebadged Serious and Organized Crime Agency (SOCA). It is arguable that this was a particular nadir for CyberPolicing as any focus and direction that the NHCTU possessed was all but lost as SOCA's attempt to validate its existence inevitably focused on more spectacular crime targets such as organized drug smuggling and money laundering. At a local level HTCU's found that their workload was increasing as eBay frauds became more prevalent and the development of mobile communications and GPRS became pervasive. In major investigations, traditional forensic methods of recovery had long been the mainstay for major investigation. However increasing forensic awareness of criminals and the focus upon "volume" crime had a negative impact upon their successes. The huge growth in the general use of mobile telephones was reflected in their use by criminals and as a result HTCU's were inundated with requests for examination of these devices. (As well as the related material from CCTV cameras.) There is virtually no major investigation (and a huge number of lesser offences) where the potential evidence that these devices can possess, is not a major feature. The murders in Soham of Holly Wells and Jessica Chapman in 2002 highlighted the evidential importance of GPRS not least in that the last recorded signals transmitted from the girls was in the immediate vicinity of the perpetrator, Ian Huntley house. Over time, the growth of mobile devices, their complexity and capability has led to an increasing burden uponHTCU in processing them expeditiously. Inevitably the backlog of work has grown with estimates of between 3-15 months UK wide. I will conclude this rush through Hi Tech Police history by referring to the latest development of national Hi-Tech Crime. In 2013 SOCA is to cease to exist (though reports of its death have in some quarters been pronounced as premature) and the as yet non-existent National Crime Agency (NCA) will undertake its remit, fulfilling the Conservative political ambition of establishing a British Federal Bureau of investigation (FBI). In case you though that I had overdone the acronyms, this was preceded by the establishment of the PCeU - Police Central e-crime Uni in the Met in 2008. This was supported in 2012 by the establishment of regional eCrime "Hubs" funded for 4 years. It is fair to conclude that the development of ePolicing in the UK has been a patchwork of some concrete gains, missed opportunities and lack of direction. Will these new structures be more effective? The answer is probably yes given the questionable performance of the structures that preceded them. One unanswered element within this is the numbers of officers and staff dedicated to this function, either in total or as a proportion of policing resources. There are no readily accessible numbers of officers who staff HTCUs but I would estimate that between 250 and 500 is probably the right "ball park" estimate with me believing it would be at the lower end of those figures. The UK police establishment as of 31st March 2012 was 134,101which at a time of falling police budgets (20% over 4 years from 2011) is a reducing figure. The proportion of officer dedicated to Internet related crime is pitifully small and is unlikely to be significantly increased in the foreseeable future. You see what gets measured is what gets done and there are no targets for CyberCrime.

6. AND WHAT ABOUT THE CYBERCRIMINAL

Finally, I have to say a little about the profile of the Cybercriminal and what that means for this area of crime. Various commentators have sought to characterize eCrime as “New wine in old bottles” or “Old crimes with new tools.” Essentially, the Internet has provided a new medium with which to perpetrate crimes that were otherwise achieved by more conventional methods. The initial legislative approach in the UK would appear to support this supposition in that the 1990 Computer Misuse Act 1990 (as amended by the 2006 Police and Justice Act) is the substantive legislation relating to eCrime. There has been debate as to the effectiveness of the Act, not least because the penalties under the Act are viewed as particularly lenient and as a result no deterrent to this activity. As a result investigators and prosecutors have sought to use existing legislation, with greater penalties, to prosecute offenders. The media representation of “identified” (notice the emphasis) offenders has been broadly to characterise offenders, in a different manner to other offenders. It is outside the remit of this article to effectively establish this argument, but I would cite a high profile case to illustrate the point. The protracted issue of extradition to the US of Gary McKInnon is one case in point, not least because it highlights the different jurisdictional elements between to “ally” countries. As one reformed UK hacker put it to me, “Scared of the Cops no, scared of extradition to the US, Yes! It scared the shit out of me!” The characterisation of McKInnon is indicative: “McKinnon, aged 46 from north London, has Asperger’s syndrome, and could face up to 60 years in jail if he is convicted in a US court. He has admitted hacking into US military computers but says he was looking for evidence of UFOs.” (Guardian 2012) First of all his Asperger’s is quoted almost as a qualification as for his nerd hacker status, whilst his alleged UFO quest marks him down as an X Files aficionado whose “Trust No one” mantra has proved inexorably true. The portrayal of the alleged Cybercriminal has the kind of qualification added to any alleged offending, that the acquisitive rioting looter in last years’Summer riots in the UK was singularly bereft of. The cybercriminal like the hacker, has been represented in the media and cinema in a stylised format. “The Girl with the Dragon Tattoo” has a female hacker heroine, whose illegal activities are given a pseudo-moral makeover, seeks to justify activities on Machiavellian grounds.

I would bring up that there are other relatively newer forms of eCrime that are not classified as purely criminal: hacktivismas in basically a thin line between protesting and using cyber-based tools to steal or deface or further protest against the target and APT (advanced persist threat) which in classical terms are either government sponsored or well funded infrastructure of people that normally wouldn’t be cyber criminals but use their training to infiltrate, deploy and collect data as business goals. Hacktivism attracts the cyber-criminal element or their methods and it’s not clear that the intent is seen as criminal by the participants.   Whereas the APT people or groups are more structured as a business like entity that apparently see patriotism as their goal and not the stealing of data from other businesses or organizations that are used by their overseers to ultimately make the decisions.   So are these people merely misguided are in a way victims of the people with the cyber criminal skills or the politically means to achieve the goal.

Conclusion

I have sought to explain how cybercrime, cybercriminals and cyberpolicing have elements that fundamentally appear to set them apart from the Criminal landscape prior to its appearance. There is an element to the speed and expansive growth with the Internet as a phenomena has overtaken our preparedness for it, not least in respect of understanding and quantifying it. I have purposely not included Terrorist related cyber activity and state sponsored cyber warfare as I believe it would require another expansive appreciation and would potentially cloud the issues under discussion. So what is so different about Cyber or eCrime? – well it’s a debate that has not had sufficient public airing to define whether it should be viewed and treated as different. Is that something to make the cognoscente think?

I don’t think mentioning that there are other forms of non-criminal intent that used tools and methods that once were a part of the cyber-crime modus operandi clouds the discussion (as the author brings this up in the first section). In my opinion it instills that it’s not as clear cut as being criminal in the physical world or the cyber one as the due to the sense of anonymity of the Internet, more and more people try things that they may not do in the “real world’.

References

Aas, KF (2011) Globalization & Crime. Sage

Casey, E (2011) Digital Evidence and Computer Crime 3e Academic Press

Clough, J (2010) Principles of Cybercrime Cambridge University Press

Fafinski, S (2009) Computer Misuse Response Regulation and the Law. Willan

Gollman, D (2011) Computer Security. Wiley

Gragido, W &Pirc, J (2011) Cybercrime and Espionage.Syngress

Jewkes, Y &Yar, M (2010) Handbook of Internet Crime Willan

Marras, M-H (2012) Computer Forensics Jones & Bartlett Learning

Minkes, J &Minkes, L (2008) Corporate and White Collar Crime. Sage

Morrisey, S (2011) iOSForesnic Analysis Apress

Schneier, B (2000) Secrets & Lies. Wiley

http://www.official-documents.gov.uk/document/cm78/7842/7842.pdf UK Cyber Security Strategy

http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime Cybercrime figures

http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf Full Report

http://securitywatch.pcmag.com/adobe/283622-mcafee-s-decade-of-cybercrime#fbid=l_sBeVNV9qH McAfee’s decade of Cybercrime

http://www.yourrights.org.uk/yourrights/rights-of-victims-and-witnesses/your-rights-if-you-report-a-crime-to-the-police/index.html Victims Charter

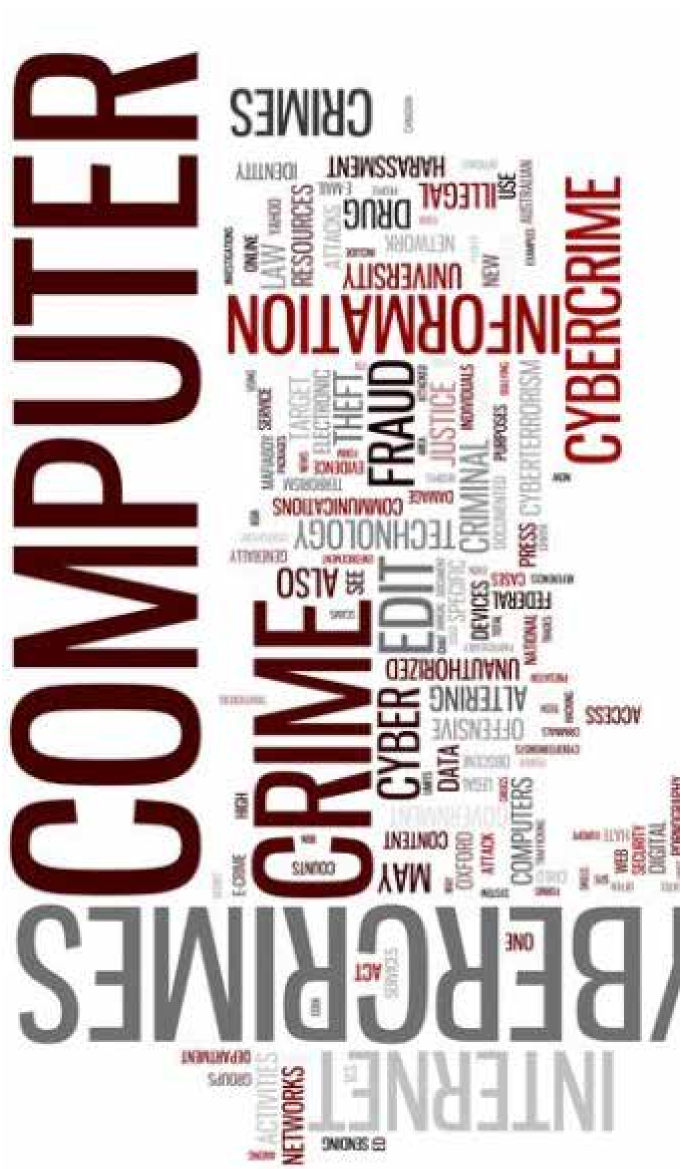
http://en.wikipedia.org/wiki/Operation_Ore Operation Ore

http://www.guardian.co.uk/government-computing-network/2012/feb/08/police-launch-e-crime-units-cyber-crimee Crime hubs

Author bio

Bob Bird is aLecturer in Forensic Computing and Ethical Hacking in the Engineering and Computing Faculty at Coventry University, UK. He was for 30 years a police officer rising to the rank of Superintendent before retiring in 2007 and starting his academic career. He was responsible for a number of major murder investigations as Senior Investigating Officer and developed the first police Intranet for West Midlands Police in 1999. He was the operational Commander for Operation Javari, an outbreak of major civil disorder in Birmingham, UK in 2006.Robert.bird@coventry.ac.ukTwitter @CovUni4n6

obe/283622-mcafee-s-decade-of-cybercrime#fbid=l_sBeVNV9qH McAfee's decade of Cybercrime
http://www.yourrights.org.uk/yourrights/rights-of-victims-and-witnesses/your-rights-if-you-report-a-crime-to-the-police/index.html Victims Charter
http://en.wikipedia.org/wiki/Operation_Ore Operation Ore
http://www.guardian.co.uk/government-computing-network/2012/feb/08/police-launch-e-crime-units-cyber-crimeeCrime hubs



PACKET CAPTURING FOR FORENSICS INVESTIGATIONS – TOOLS & TECHNIQUES

LUKASZ KACZOROWSKI

Network forensic is a sub-branch of digital forensic which deals with monitoring and capturing network traffics in order to discover source of security breach. There are many reasons behind necessity of that sub-brunch being a part of a digital investigation and many tools to choose from.

Computer Forensics methods may not always be enough to solve investigation. For example, if there was unauthorized access and some data have been stolen. Since the hacker had access to the system he could clean up after himself i.e. delete logs. In that case there is no evidence of identity of the thief. Here comes packet sniffer which monitors and logs all the traffic from and to server.

Network traffic is extremely volatile data therefore difficult to store because it changes all the time and the number of sent packets may amounts to few thousands on a single host within few minutes. There are tools which purpose is to collect packets on a network. In this article I have described interface and features of a two most popular capturing tools.

OSI MODEL

To take full advantage of packet capturing tools one have to have full understanding of OSI Reference Model. The model is composed of seven layers and has been devised to facilitate building, troubleshooting and understanding network protocols. Each layer describes stage data have to go through before it is send onto the wire to another host. Layers are separated from each other, however they have input and output interfaces. Output of one layer feeds input of another one (lower or higher depends whether data is send or received). This way programmer can be flexible in build new protocols, as long as they stick with common interfaces. Also it is much easier to understand the way protocols works because you can focus on one separated layer which have dedicated function. I have briefly described each layer and its function below. Every packet sniffer divides network traffic into categories which are as the network layers. Each has different attributes such as addresses, ports and much more which uniquely identify connections.

THE LAYERS OF OSI MODEL

The seven layers can be divided into two parts. First, Application Set (including Application, Presentation, and Session) which is concern with actual application data and its preparation before sending out, Application Set is usually contained within one single application such as Web browser. Transport Set (including Transport, Network Data-Link and Physical) which makes sure data is send as reliably and as fast as possible to correct recipient.

Application - this layer is concern with actual application data. It's the only layer which has direct contact with OS. Protocols such as HTTP, FTP or DNS works at this layer.
Data unit: data

Presentation – it's usually part of applications that communicate over the network. At this layer data is changed to common format so that it is readable to application on the other side. Html or PDF are good example.

Data unit: data.

Session – Similarly to Presentation, it is part of communicating applications. Deal with different sessions that are open by application. Good example of session in action is a web browser which has few tabs open, each to different server. Session make sure that received data is send to correct tab.

Data unit: data.

Transport – provide end-to-end communication for application. Together with Network layer create so-called sockets which uniquely identify connection. There are two of protocols at this layer, UDP which is best effort protocol. This means it does not maintain connection or retransmit lost packets (used in voice or video communication. Second, TCP protocol is reliable, perform three-way hand-shake to assure reliable communication, error-checking and retransmission in case packet loose

Data unit: segment

Network – uses IP addressing scheme and routers to chose best path to given destination and forward those packets along that path. Routing protocols used at this layer could be BGP, EIGRP, OSPF or RIP.

Data unit: packets

Data-Link – this layer is local, uses MAC addresses and switches to switch frames within local network. MAC address is valid only locally and changes at each segment it is forwarded. If destination of a host is remote, frame is forwarded to default gateway. Example of Data-Link protocols: Ethernet, PPP, HDLC, Frame-Relay.

Physical – it is the lower layer of OSI Model and therefore totally physical. The only thing we can see here is raw bits send onto transmission medium (wire, fibre-optic or air).
On this I will conclude writing about OSI Model, it is not comprehensive description and if you need more please review articles widely available on the internet.

CONNECTION TECHNIQUES

There are many packet capturing tools available on the market. They all differ in some way, be this capabilities or ease of use. I have written about a few of many I have experience with and found them the most useful.

So, How to tap into the network…

Packet sniffers set network adapter to promiscuous mode which means it capture all packets even ones not destined to that host. However, even the best tool will not capture all network traffic if it is not connect to the right place. If hubs were still in use it would be much easier. As you know hubs forward packets to all of its interfaces apart of the one it came from, this means that connecting host with sniffer running to just any hub's port will capture every single packet that travel through that hub. However, most of internetworks use switches which create separate circuit for each connection. This means that host connected to a switch receives only packet destined to it. There are methods to make switch send all traffic through sniffing device by using specially crafted ARP packets and more. I did not write about them because they are considered illegal and are highly disruptive to the network. What I have focused in this article is two ways to tap into a network. SPAN Port (port mirroring) and Network Tap device both enable network administrator to intercept and store network traffic for investigation in case it is needed.

SPAN Port

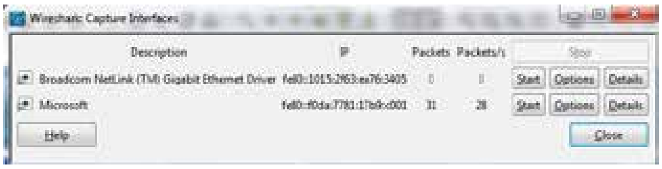
SPAN Port is a feature of a switch's software. All traffic going through the switch is aggregated and sends to port on which sniffer or IDS is connected. SPAN Port works at Layer 2 (Data-Link) thus all data from Layer 1 and most data from Layer 2 inc. corrupt packets are discarded by switches. Plus, since it is feature implemented in software it consumes extra system resources. Anyway, SPAN Port is the best choice when we want to see what is going on inside a switch.

Network Tap

Second option to tap into network infrastructure is "Network Tap" which is placed between point A and B in network and copies bit by bit all the traffic going along those two points. Taping point may be intercepting traffic going from switch to router or firewall. Since it works at Layer 1 (physical), exact copy of the traffic is gathered.

Network Forensic Tools and Technics. Wireshark

The most popular free, open source packet sniffer on the market. Available on Linux as well as Windows. It has endless number of features and a lot of filters enables user to search required data among ocean of packets. These undoubtedly grate aspects makes Wireshark quite difficult to use even for more advances users. That is why I have decided to write a short tutorial showing the most important filters, its syntax and operators.
Once Wireshark is up and running on a host you will have to choose a network adapter to set into promiscuous mode and capture packet from. List of available adapters will look similarly to that on Figure 1.



Wireshark Capture Interfaces

	Description	IP	Packets	Packets/s	Stop		
	Broadcom NetLink (TM) Gigabit Ethernet Driver	fe80::1015:2f63:ea76:3405	0	0	Start	Options	Details
	Microsoft	fe80::f0da:7781:17b9:c001	31	28	Start	Options	Details

Figure 1. List of available adapters

The interface of Wireshark is constructed of three panes (Figure 2):

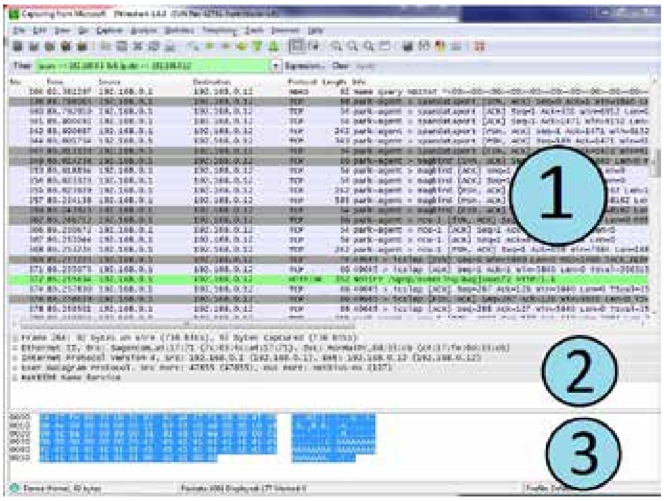


Figure 2. Construction of Wireshark

1. Packet List - contain list of all packet captured in current session. It has few columns with detail about packet number, time of capture, source and destination address and protocol used.
2. Packet Details – the middle pane contain hierarchical list of information carried in a packet at all layers beginning from Layer 2 (Data-Link) to Layer 7 (Application). The list can be expanded and collapsed.
3. Packet Bytes – the lower pane shows not processed packets in their raw form, just the way they travel through the wire.

Wireshark uses filters to display only filters that are relevant to undertaken investigation. They are built similarly to upside down DNS structure. By this I mean that filter start with general type of sought element such as protocol (eth, ip, tcp) on the left and follows that with dot and more specific element on the right, such as flag within that protocol (MAC or IP address or one of TCP flag).

For example, eth.addr == 00:11:22:33:44:55:66:77 means, display all Ethernet frames which contain given MAC address. Filters applied together with arithmetical and logical operators upon captured data enable an investigator to find and display only sought packets. There is literally thousands of possibilities, it would take a small book to write about them all. However, a few of examples I have included should show you capabilities of Wireshark.

All of the filters can be joined together using one or more arithmetical and/or logical operators.

ARITHMETICAL OPERATORS:

eq or ==	- equals to
ne or !=	- not equals to
gt or >	- greater than
lt or <	- less than
ge or >=	- grater or equal
le or <=	- less or equal

LOGIC OPERATORS:

And	or	&&	- logic AND
Or	or	||	- logic OR
xor	or	^^	- logic XOR
not	or	!	- logic NOT
[n] […]			- substring operator

For example to find direct conversation between to hosts an investigator can use two filters with one operator. The filter below would show one way conversation between a host and a default gateway on local network.

```
IP.src == 192.168.0.10  &&  IP.dst == 192.168.0.1
```

That is just simple example; Wireshark is capable of much more complex filtering which reveal just any type of data that may be useful in digital investigation. Although Wireshark is excellent software for some it require patience and knowledge at high level. Wireshark can be used in network forensic investigation however is not the most handy sniffer out there. Definitively, Wireshark is much better choice for network administrator or networking student who wants to learn how internet protocols works then for Digital Investigator who only wants to collect evidence. There are sniffers are much easier to use because they filter and group packets for a user. One of such is another graphic interface sniffer Network Miner.

A complementary tool with packet capture software is Chaos Reader. It helps break down the packet capture saved files (pcap) into discrete parts. Each of these parts can help analysis the whole pcap then strictly reading the packets within the Wireshark or other packet capture tool. It is also good for those not yet familiar with the packet capture format.

Network Miner

Network Miner is a Network Forensic Analysis Tool (NFAT), available only for Windows. First version was release in 2007 and since then became popular among incident response team and law enforcement. Two version of that packet sniffer are available, free one which have a few function less than commercial version. Commercial version cost €500 and possesses extra features such as Port Independent Protocol Identification (PIPI), Exporting results to CSV / Excel, Host colouring support and few more. It has GUI based interface similarly to Wireshark. It is much better choice for Digital Investigator because of its ease of use as compering to Wireshark. Network Miner is host-centric, oppose to Wireshark which is packet-centric. It groups and displays a collection of data regarding actual hosts communicating over the network. It does not use filters. Instead, it is composed out of twelve panes which group captured data.

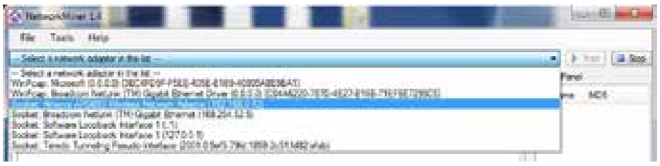


Figure 3. Network adapter
To start capturing you have to select network adapter which is then set to promiscuous mode. (Figure 3)

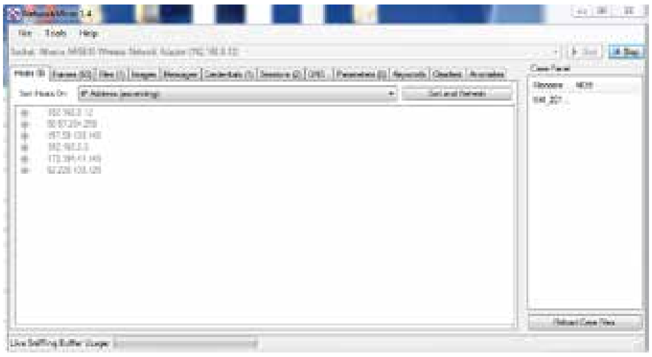


Figure 4. The final result
Once network adapter have been chosen packets are collected and grouped in real time. (Figure 4)

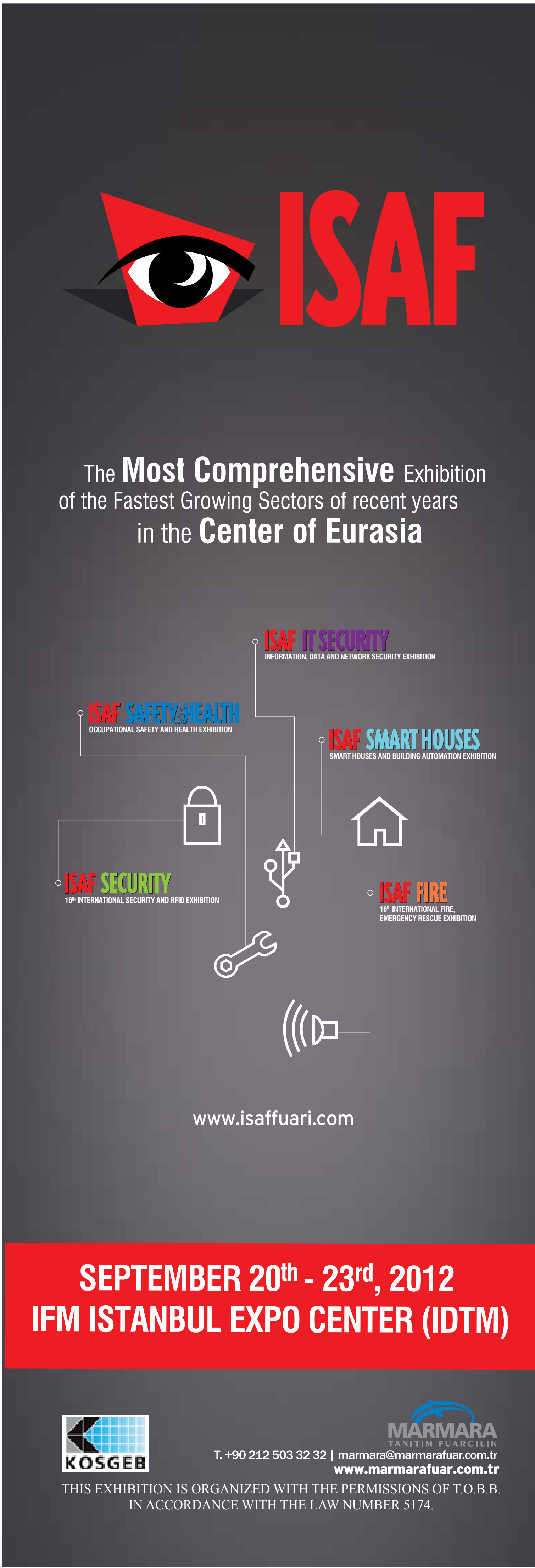
Each pane has its unique data which is clear and easy to browse. Below I have given short description of every pane.
Hosts – contains info about hosts participating in the communication. You can find their MAC and IP addresses here. Also, Network Miner performs fingerprinting to find out host OS.

- Frames – Display captured frames, so-called sockets, source and destination IPs together with accompanied port numbers.
- Files – Network Miner reconstruct TCP stream to obtain files which then can be accessed from this pane.
- Images – Similarly to previous function, images are retrieved from TCP streams and can be viewed in real time from this pane.
- Messages – Any emails or other types of messages if not encrypted will show up in here.
- Credentials – Usernames and passwords sent in clear text may be accessed from this pane. FTP servers or any other server that sends credentials in clear text.
- Sessions – information interchange (dialogs) which have been established between two or more devices (HTTP or TCP sessions). May be used to check if there was a connection between two host.
- DNS – All queries that have been resolved are stored here That include server and client IP as well as queries and an answers to them.
- Parameters – displays parameters exchanged between two applications, it could be HTTP cookie or HTTP header.
- Keywords – Stored data may be searched for keyword presence. It can be "username" or "password".
- Clear text – Any clear text passing through the network is displayed in this pane in real time.
- Anomalies – feature which monitors passing traffic and compares it to database of signatures looking for anything suspicious (intrusion, virus attack).

To Conclude:
In this article I have written about issues that have to be taken into consideration before we start capturing data and two most popular packet capturing tools. This article does not exhaust the topic in any way and there is much more to learn in **Network Forensic** field. The article does not say about every feature of **Wireshark** or **Network Miner** which are definitely one of the top-notch on the market but there much more tools to choose and each have its pros and cons. Network forensics is relatively new field in digital forensics therefore quickly developing one so we have much more to look forward in the future. If you have any feedback or would like to discuss issues raised in this article I can be reached at l.kaczorowski1@googlemail.com.

Author bio

Lukasz Kaczorowski is network and network security enthusiast currently studying 4th year at Caledonian University Bsc Network and System Support. Author holds professional certificates such as CompTia Network+ and Cisco CCNA.



RECOVERING IE HISTORY USING PASCO IN LINUX UBUNTU 12.04

CARLOS CAJIGAS MSc, EnCE, CFCE, CDFE

Reconstructing and examining web browsing history is a task that is required during most forensic examinations. Luckily, popular commercial tools have done a good job of simplifying the reconstruction process for us. While commercial tools simplify the process, the software often comes with a hefty price tag.

Although not as user friendly as the commercial tools, Pasco can parse the browsing history contained in the Internet Explorer's index.dat file and output the results in a field delimited manner that can be imported into the spreadsheet program of your choice. The spreadsheet can then be sorted by date to shed light on the browsing patterns of the subject in your investigation. Pasco is an open source tool that you can use for free.

THE GOAL:

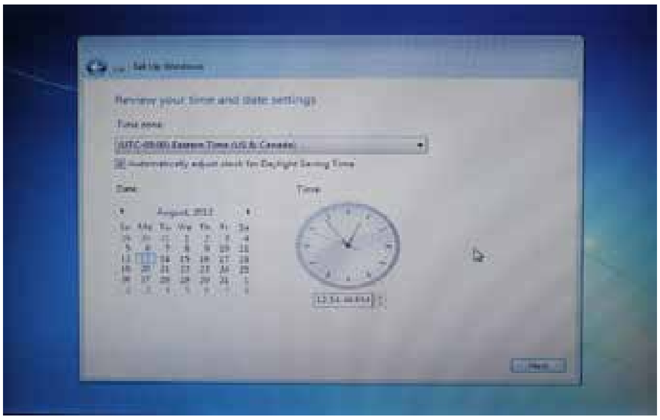
The plan is to recreate the steps that will lead to data being added to an index.dat file. We will accomplish this by conducting some Internet Explorer web browsing in our own controlled environment. We will then use Pasco to examine our own browsing history.

The Backtrack live DVD comes bundled with Pasco, but for the purposes of this article, I used an examination computer with Ubuntu 12.04 installed on it.

CONTROLLED ENVIRONMENT:

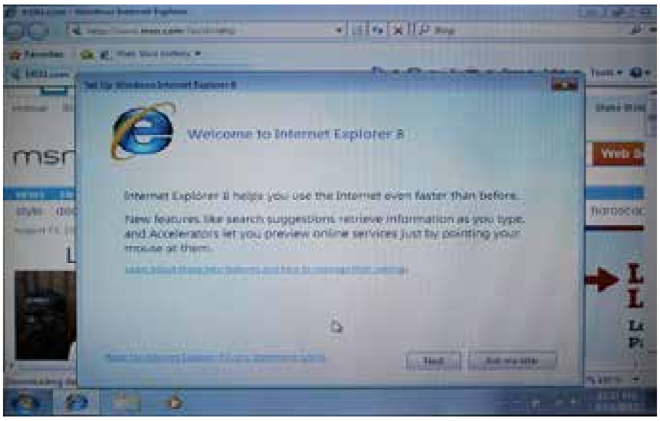
In order to create our own Internet Explorer index.dat file, I began by installing a new Windows 7 Home Premium Operating System on my Laptop.

When it came time to set the time clock, I selected Eastern Standard Time, as I am currently living in the East Coast of the US.



Set Up Windows
Review your time and date settings
Time zone:
(UTC-05:00) Eastern Time (US & Canada)
Date:
August, 2012
Time:

The installation completed and I logged in as user "Carlos". I gave the laptop an internet connection and opened the Internet Explorer (IE) Browser.



Welcome to Internet Explorer 8

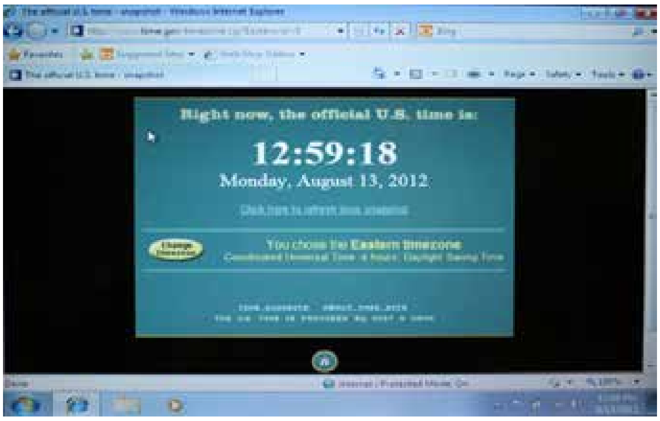
Internet Explorer 8 helps you use the Internet even faster than before.

New features like search suggestions retrieve information as you type, and Accelerators let you preview online services just by pointing your mouse at them.

The first time that IE is launched, a Microsoft owned website opens in the background and you are welcomed with the "Welcome to IE 8" screen asking you to set it up. I clicked on the "Ask me Later" button to avoid the set up process. A second Tab immediately opened, redirecting me to another Microsoft owned website.

I waited for the second tab to load, and I then closed the IE window. I closed the window, because I wanted to start our own browsing session on a separate IE window.

At 12:58 pm, I launched a new IE window. The browsing window opened and the default Microsoft owned website loaded up. I then went to the address bar and typed *www.time.gov/timezone.cgi?Eastern/d/-5* and pressed enter. I navigated to this website to confirm that the local time of the computer matched the current local time from time.gov.



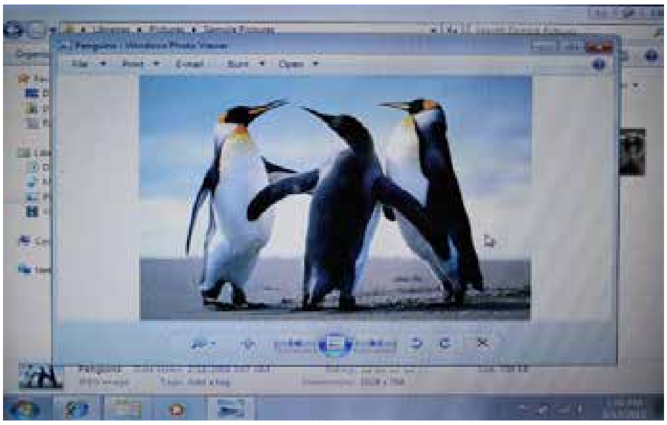
Right now, the official U.S. time is:

12:59:18

Monday, August 13, 2012

You chose the Eastern timezone

After navigating to time.gov, I launched Windows Explorer and opened the Penguins.jpg picture located in the "C:\Users\Public\Pictures\Sample Pictures" folder.

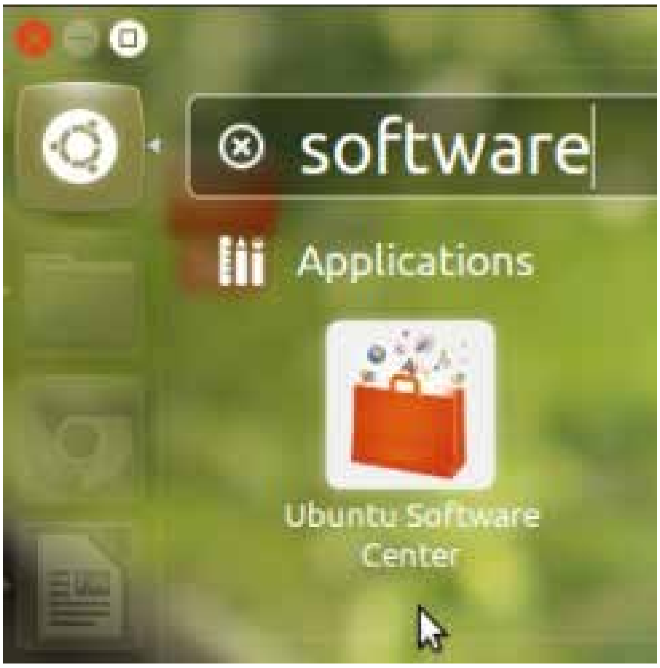


Navigating to time.gov and opening the Penguins.jpg picture are two actions that should be recorded by the index.dat file. I then closed all windows and shut down the computer. This concludes the controlled environment part of our test. Let's move on to the next part.

INSTALLING THE TOOLS:

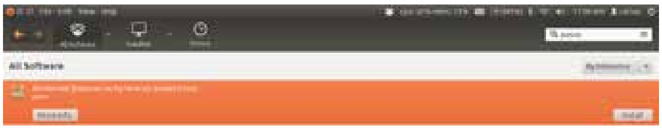
The tool that we will use for the examination is not included in Ubuntu by default. It can be downloaded from the Ubuntu Software Center. The tool that we will need to accomplish the task is Pasco. Let's head over to the Ubuntu Software Center for the tool.

Click on the Dash Home circle, located on the top left of your screen, type in "software" and click on the Ubuntu Software Center icon that will appear.

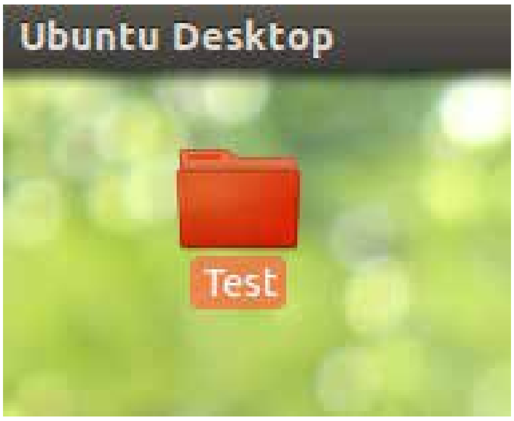


software

After the Ubuntu Software Center opens, you will see a search box on the top-right corner of your screen. Type "pasco" and click on the install button. You will be prompted for your root password. Enter your root password and wait for the program to install.



Now that we have the program that we need, close the Ubuntu Software Center. The next step is to prepare a working folder to receive the results from our analysis. Go to your desktop, right click on your desktop and select “create new folder”, name it “Test”.

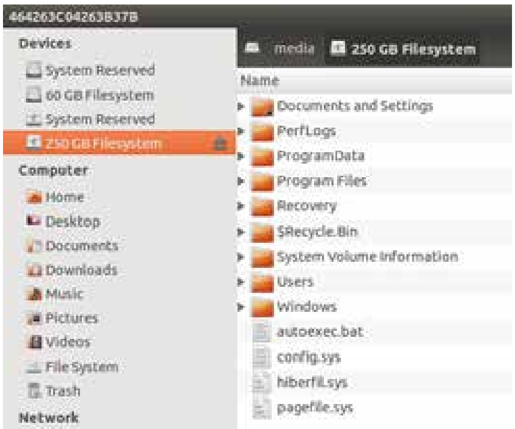


THE EXAMINATION:

For the examination part of the test I chose to examine our Windows 7 installation by removing the hard drive from the Laptop and connecting it directly to my examination computer with Ubuntu installed on it. I placed the hard drive into a USB enclosure and connected the USB cord to a previously validated USB hardware write-blocker. I then connected the write blocker to a USB port on my examination computer.

If you do not have a write-blocker handy, you do not have to use one, just remember to never connect evidence media to a computer without the use of a previously validated write-blocking procedure. From now on, we will refer to the hard drive containing the Windows 7 installation as our “Test Media.”

Make sure your test media is connected to the computer and open Nautilus. Nautilus is the file manager for the GNOME desktop environment. You can launch Nautilus by left clicking on the “folder” looking icon in your taskbar. Nautilus is going to display your connected devices on the top left side of the window. My test media is the one that says “250GB Filesystem”. Click on the name of your test media to mount it (if it isn’t mounted already). By default, Ubuntu mounts its connected devices inside of the “media” folder.


464263C04263B37B

Devices
- System Reserved
- 60 GB Filesystem
- System Reserved
- 250 GB Filesystem

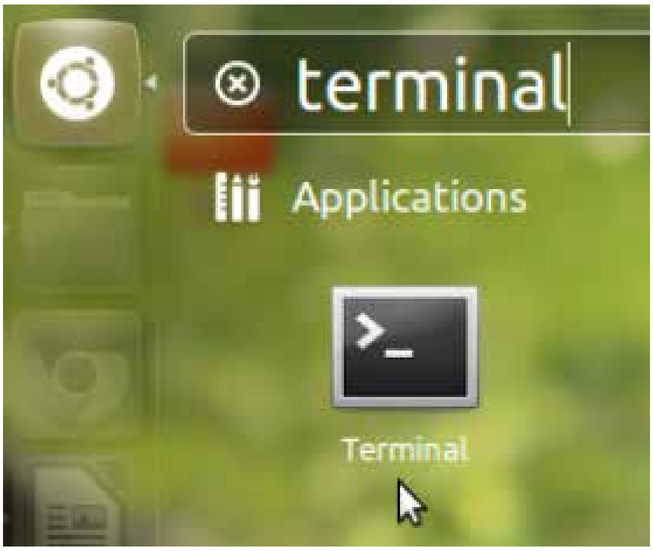
Computer
- Home
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- File System
- Trash

Network

media | 250 GB Filesystem

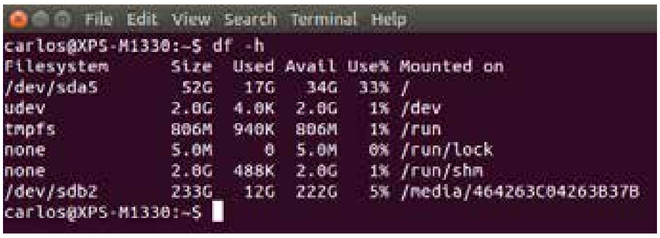
Name
- Documents and Settings
- PerfLogs
- ProgramData
- Program Files
- Recovery
- $Recycle.Bin
- System Volume Information
- Users
- Windows
- autoexec.bat
- config.sys
- hiberfil.sys
- pagefile.sys

Now open a Terminal Window. In Ubuntu you can accomplish this by pressing Ctrl-Alt-T at the same time or by going to the Dash Home and typing in “terminal.”



Once the terminal window is open, Type the following into the terminal to determine which devices are currently mounted in your system.

df -h

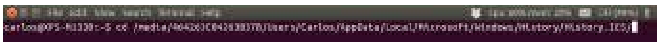


```
carlos@XPS-M1330:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda5        52G   17G   34G  33% /
udev            2.0G  4.0K  2.0G   1% /dev
tmpfs           806M  940K  806M   1% /run
none            5.0M     0  5.0M   0% /run/lock
none            2.0G  488K  2.0G   1% /run/shm
/dev/sdb2       233G   12G  222G   5% /media/464263C04263B37B
carlos@XPS-M1330:~$
```

Notice that my test media was mounted under the “media” folder as 464263C04263B37B.

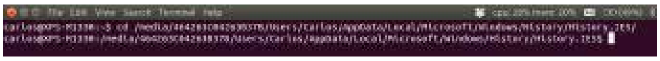
We are almost ready to use Pasco. Pasco is a very simple program to use. Pasco is used by pointing it to the index.dat and then redirecting its output to the location of your choice. An example of its usage is “$ pasco index.dat > pascoresults.csv”. Before we use Pasco, we need to navigate to the location where the index.dat is located on the test media. On a Windows 7 operating system the index.dat containing the browsing history is located at:
/Users/<User>/AppData/Local/Microsoft/Windows/History/History.IE5/index.dat.

We will use the CD command to change directory into the desktop. Type the following into the terminal.



```
carlos@XPS-M1330:~$ cd /media/464263C04263B37B/Users/Carlos/AppData/Local/Microsoft/Windows/History/History.IE5/
```

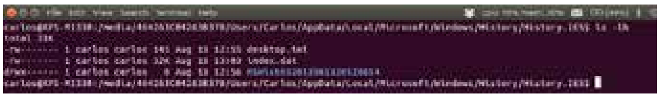
Replace “464263C04263B37B” with the directory assigned to your test media and replace “Carlos” with the name of the user account that you are targeting. After doing so, press enter.



```
carlos@XPS-M1330:~$ cd /media/464263C04263B37B/Users/Carlos/AppData/Local/Microsoft/Windows/History/History.IE5/
carlos@XPS-M1330:/media/464263C04263B37B/Users/Carlos/AppData/Local/Microsoft/Windows/History/History.IE5$
```

The dollar sign after History.IE5 indicates that "History.IE5" is your current directory, exactly what we wanted.

Now type "ls -lh" into the terminal and press enter, to see if we have an index.dat file in our current directory. LS is the list files command. The flag -l uses a long listing format, and the flag -h prints the file's size in human readable format.



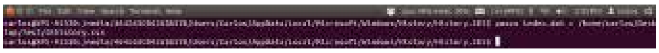
```
carlos@XPS-M1330:/media/4E4263C842638378/Users/Carlos/AppData/Local/Microsoft/Windows/History/History.IE5$ ls -lh
total 33K
-rw------- 1 carlos carlos 141 Aug 13 12:55 desktop.ini
-rw------- 1 carlos carlos 32K Aug 13 13:02 index.dat
drwx------ 1 carlos carlos   0 Aug 13 12:56 MSHist012012081320120814
carlos@XPS-M1330:/media/4E4263C842638378/Users/Carlos/AppData/Local/Microsoft/Windows/History/History.IE5$
```

Notice that yes, we do have an index.dat file in our current directory.

Now it's time to call Pasco. Type the command below into the terminal and press enter.

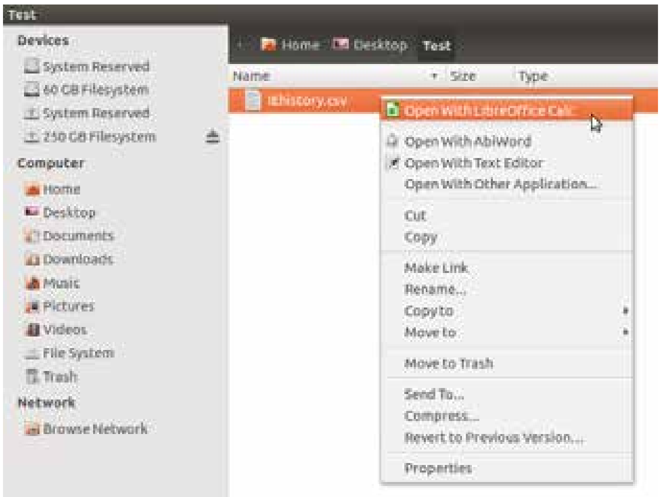
pasco index.dat > /home/carlos/Desktop/Test/IEhistory.csv This command will point Pasco to the index.dat file and redirect its output into a file appropriately named IEhistory.csv, into our previously created Test folder on the Desktop (replace "carlos" with the user you are currently logged in as).

If you get your cursor back without displaying any errors, then you know that the command worked according to your input.

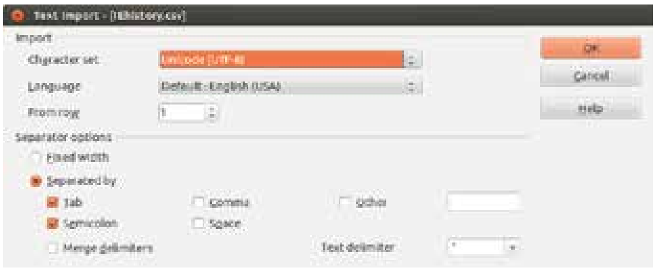


```
carlos@XPS-M1330:/media/4E4263C842638378/Users/Carlos/AppData/Local/Microsoft/Windows/History/History.IE5$ pasco index.dat > /home/carlos/Desktop/Test/IEhistory.csv
carlos@XPS-M1330:/media/4E4263C842638378/Users/Carlos/AppData/Local/Microsoft/Windows/History/History.IE5$
```

Now open Nautilus, navigate to the IEhistory.csv file inside of the Test folder and open it with LibreOffice Calc.LibreOfficeCalc is Ubuntu's default spreadsheet viewer.



When it opens, you will be asked to select how you want LibreOfficeCalc to interpret the fields in your file. The options will be under the Separator Options area. I chose to have the data separated by "Tab" and "Semicolon", by adding a checkmark next to them. After doing so I pressed "Ok".



Text Import - [IEhistory.csv]

Import

Character set: Unicode (UTF-8)

Language: Default - English (USA)

From row: 1

Separator options

○ Fixed width

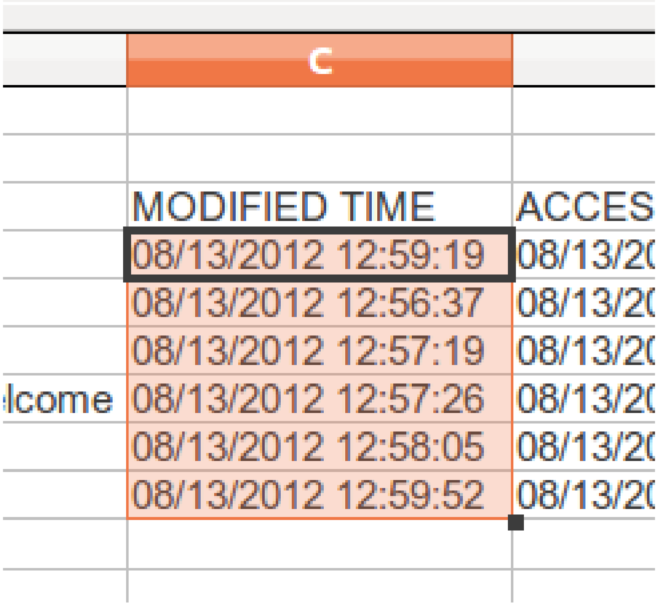
● Separated by

☑ Tab ☐ Comma ☐ Other

☑ Semicolon ☐ Space

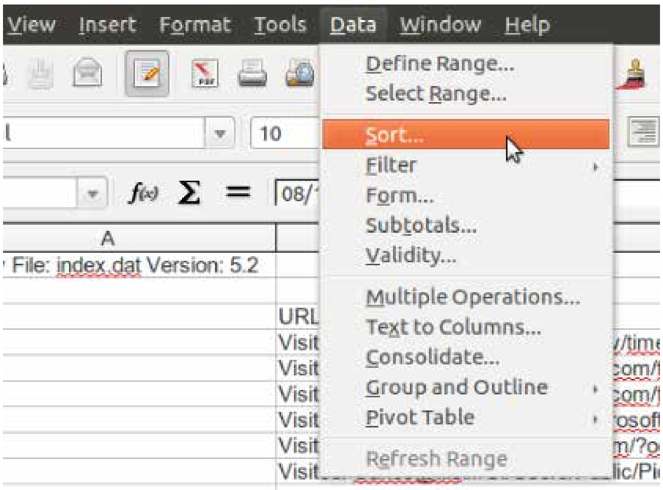
☐ Merge delimiters Text delimiter: "

The file will then open and it will display the data that was parsed from the index.dat file. The final step is to sort it by date and time. Head over to the "MODIFIED TIME" row and highlight the items in it.

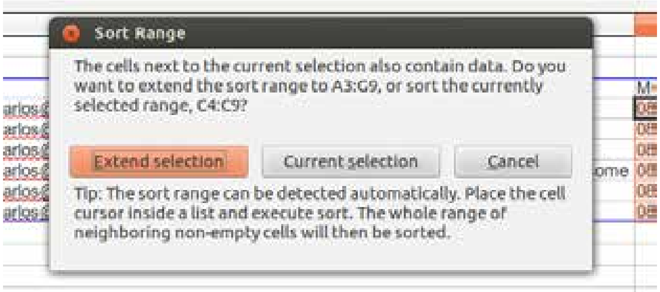


	C	
	MODIFIED TIME	ACCES
	08/13/2012 12:59:19	08/13/2(
	08/13/2012 12:56:37	08/13/2(
	08/13/2012 12:57:19	08/13/2(
lcome	08/13/2012 12:57:26	08/13/2(
	08/13/2012 12:58:05	08/13/2(
	08/13/2012 12:59:52	08/13/2(

Mouse over to the "Data" tab and click on "Sort".



Select "Extend Selection" so that all of the fields get sorted at the same time.

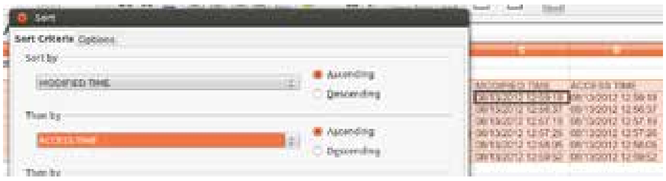


Sort Range

The cells next to the current selection also contain data. Do you want to extend the sort range to A3:G9, or sort the currently selected range, C4:C9?

Tip: The sort range can be detected automatically. Place the cell cursor inside a list and execute sort. The whole range of neighboring non-empty cells will then be sorted.

Then tell it to sort by "MODIFIED TIME" followed by "ACCESS TIME" and press "Ok".



Sort

Sort Criteria | Options

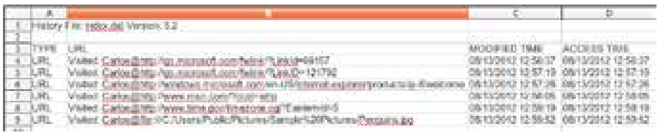
Sort by: MODIFIED TIME — ● Ascending ○ Descending

Then by: ACCESS TIME — ● Ascending ○ Descending

Then by

MODIFIED TIME	ACCESS TIME
08/13/2012 12:56:37	08/13/2012 12:56:37
08/13/2012 12:56:37	08/13/2012 12:56:37
08/13/2012 12:57:19	08/13/2012 12:57:19
08/13/2012 12:57:26	08/13/2012 12:57:26
08/13/2012 12:58:05	08/13/2012 12:58:05
08/13/2012 12:59:52	08/13/2012 12:59:52

And that's it. Below are the results of the data parsed by Pasco in the order that the browsing occurred, sorted by the local time of the computer.



History File: index.dat Version: 5.2

TYPE	URL	MODIFIED TIME	ACCESS TIME
URL	Visited: Carlos@http://go.microsoft.com/fwlink/?LinkId=69157	08/13/2012 12:56:37	08/13/2012 12:56:37
URL	Visited: Carlos@http://go.microsoft.com/fwlink/?LinkID=121792	08/13/2012 12:57:19	08/13/2012 12:57:19
URL	Visited: Carlos@http://windows.microsoft.com/en-US/internet-explorer/products/ie-9/welcome	08/13/2012 12:57:26	08/13/2012 12:57:26
URL	Visited: Carlos@http://www.msn.com/?ocid=iehp	08/13/2012 12:58:05	08/13/2012 12:58:05
URL	Visited: Carlos@http://www.time.gov/timezone.cgi?Eastern/d/-5	08/13/2012 12:58:19	08/13/2012 12:58:19
URL	Visited: Carlos@file:///C:/Users/Public/Pictures/Sample%20Pictures/Penguins.jpg	08/13/2012 12:59:52	08/13/2012 12:59:52

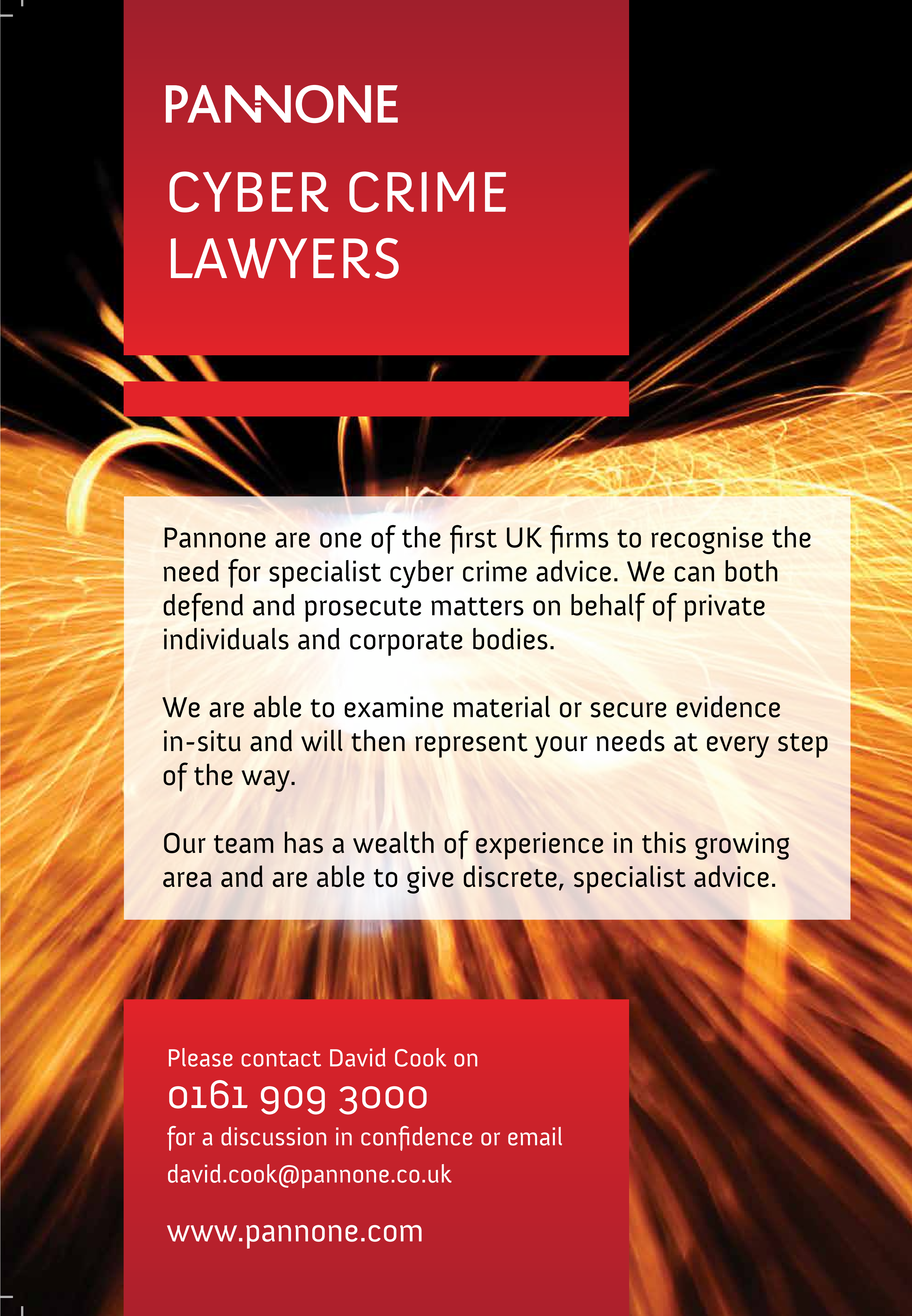
At 12:58PM, when we opened the new IE Window the default Microsoft owned website opened up (msn.com). A minute later we navigated to time.gov, and then opened the Penguins.jpg image. All of our actions were recorded by the index.dat file and parsed by Pasco in an easy to read spreadsheet.

CONCLUSION:

Pasco is an easy to use tool that can help you parse the IE browsing History of a specific user in your investigation.

If this procedure worked for your case, and you are able to use it in the course of your investigation, we would like to hear from you. E-mail the author of this article at carlos@epyxforensics.com.

CARLOS CAJIGAS MSc, EnCE, CFCE, CDFE



CAPTURING INSTANT MESSAGES WITH PACKET CAPTURE TECHNOLOGIES

NICHOLAS MITER

INTRODUCTION

Most commercial forensic software packages focus on indexing and intelligently searching data archived in hard drives, networks, and e-mail servers. These tools work well when archived information accurately reports employee communication. However, deleted or real-time traffic is not fully recoverable with traditional search utilities. A comprehensive discovery package must capture, filter, and store real-time data to tell a more complete, and interesting story. Real-time forensic technologies, however, implicate several legal principals such as wire-tapping laws, waiver of privacy restrictions, and evidentiary rules not common with archived information. This article discusses some of these principals and provides a simple example of a forensic tool that captures instant messaging traffic and stores it in a Microsoft SQL Database Server. Many forensic toolkits support importing data from commercial database systems.

EVIDENTIARY VALUE

The probative value of instant messages and other forms of real-time communication is enormous because case participants do not anticipate that their messages and phone calls could be used against them. They will be more likely to share key insights during these conversations. Courts usually consider the probative value of relevant evidence against its prejudicial effect. Recorded communications are more reliable and truthful when the declarant doesn't know or even suspect he is being monitored. The "surprise" effect results in judicial efficiency because case participants will have an even greater incentive to tell the truth and settle a case because the court will be more objective. Furthermore, real-time messages are often composed of short, simple concepts that can be easily separated from irrelevant messages. An irrelevant or privileged message can be redacted from a transcript, leaving information that is understood without the unredacted portions. This is important for a couple reasons. First, when traditional documents are redacted, the remaining portions are hard to read because context is missing. A jury can be confused or worse mislead. An instant message, in contrast, is understood on its own without including every other instant message. Also, increasingly popular electronic discovery software that intelligently categorizes information by mood or concept must distinguish between concepts embedded in documents, paragraphs, and sentences. For instance, an entire document may have a positive, optimistic tone but one paragraph could be pessimistic. Categorizing the entire document as neutral because the pessimistic and optimistic paragraphs cancel each other out would be inaccurate. Instant messages are composed of short, discrete sentences that can easily be coded and analyzed with intelligent software without the need to distinguish between sentences and paragraphs because each message usually includes only one concept. Also, real-time communications more easily fit evidentiary rules known as hearsay exceptions because they tend to include statements of intent, present sense impressions, and admissions against interest. Hearsay is an out of court statement used to prove the truth of the matter asserted. A statement like, "I just wired $1,000,000 to a company in Europe" is hearsay if it was made out of court and is being used to prove that I really wired a sum of money to Europe. The court would need direct evidence of the transaction because hearsay isn't admissible. Hearsay tends to be inadmissible because there are problems memorizing and recalling exactly what the declarant said. There are also concerns over truthfulness because the declarant can't be cross examined about the statement. Unless a hearsay exception applies, hearsay is generally inadmissible.

Records of real-time communication are more reliable than traditional forms of hearsay because it is a perfect record of exactly what was said. There are no problems with remembering and recalling the exact statement. Recalling the exact statement is critical to understanding the context behind the statement because a statement could have more than one meaning. Recalling the precise statement helps decode what, exactly, was meant. Also, hearsay exceptions like statements of intent can easily be found in real-time communication. For example, if an employee tells someone he intends to wire funds to complete a transaction, these statements may be admissible to prove the declarant actually wired funds.

CRIMINAL PENALTIES FOR WIRETAPPING

The criminal penalties for illegally eavesdropping or recording a conversation are severe and warrant consulting with a licensed attorney. Federal laws criminalize the capture of any communication transmitted electronically without the consent of one of the participants. They also criminalize attempted eavesdropping, conspiracy to eavesdrop, and disclosing illegally obtained information. Thus, planning to install an illegal wiretap or working on a project to install an illegal wiretap could subject all participants to a criminal liability. Also, disclosing information obtained from an illegal wiretap is also criminal. There are exceptions for law enforcement purposes. The scope of the act is criminal, however, and the exceptions pertain to law enforcement agents obtaining emergency warrants. Likewise, state governments and territories also criminalize wiretapping. Nearly all states and territories in the United States criminalize illegal wiretaps. According to the National Conference of State Legislatures, forty states require one party to consent, while twelve require all parties to consent. Some states even criminalize the failure to report illegal wiretapping. There are also several laws applicable to eavesdropping on government employees, as well as wiretapping private companies that do business with the government. A review by a qualified attorney should be performed prior to recording any real-time data.

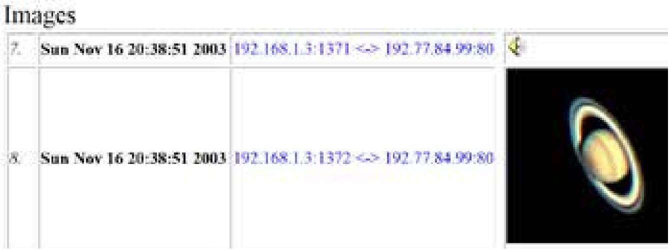
WAIVERS FOR WORK RELATED PURPOSES

A legal waiver may provide a company with permission to record employee communication. However, it may be sufficient to waive consent from other parties privy to the communication. Also, an employee located in a single-consent state may communicate with employees in dual-consent states. While legal in the employee's home state, the wiretap is criminal in the other and subjects the company to litigation risk and possible criminal liability. A wiretap pursuant to a judicial warrant, or discovery order, in contrast mitigates criminal liability. However, the wiretap should be narrow to prevent inadvertent discovery of private information and an attorney should be consulted in all cases.

EXAMPLE SETUP

There are many tools available to record network traffic and extract real-time communication like instant messages as well VOIP traffic. These tools should be placed in a location where network traffic routinely crosses. The data collected is then exported to a commercial database and analyzed with commercial forensic and electronic discovery software. The software can generate printouts of real-time communication to be reviewed and then used in trial.

ColaSoft's CapseFree was chosen because it is free, intuitive, and automatically assembles instant messages. ColaSoft also offers a WiFi version that captures messages in a WiFi environment, automatically decrypting traffic with a predefined key. The software extracts and reassembled packets in real-time, composes instant messages, and exports data to an Excel file. There are other tools like Chaos Reader that capture and log network traffic. Chaos Reader is an extendable utility written in Perl compatible with Windows and Linux platforms. Chaos Reader offers preset filters recognizing certain types of network traffic. The utility recognizes web, internet relay chat, e-mail, and file transfers. It does not currently recognize instant messages or voice over IP traffic but can be programmed to do so. The toolkit also captures images and keeps a detailed record of logged network traffic. Chaos Reader isn't as intuitive as ColaSoft's CapsaFree, because it runs in Perl and does not utilize a graphical user interface. However, Chaos Reader does support many types of network traffic including IP Version 6. ColaSoft, in contrast, is easier to use, features an intuitive user interface, and automatically reassembles instant messages.



Images

7.	Sun Nov 16 20:38:51 2003	192.168.1.3:1371 <-> 192.77.84.99:80	
8.	Sun Nov 16 20:38:51 2003	192.168.1.3:1372 <-> 192.77.84.99:80	

Figure 1. Log displaying pictures captured with ChaosReader

(Taken from: http://chaosreader.sourceforge.net/Chaos01/image.html)

The logs from both software packages can be imported to a commercial database like SQL Server and accessed with forensic and electronic discovery toolkits. The logs must get exported to a commonly used data file format, like flat files or a CSV file, and then imported with a commercial database software package. In this example, logs are imported with Microsoft Access into a Microsoft SQL 2012 database.

The software in this example does not access data archived on employee hard drives. Instead, it records network traffic in real time. The location of the wiretap must be able to intercept all network traffic coming from and going to the employees in question. The wiretap must be capable of recording all data going to and from that employee's systems. If the employee uses a smart phone or personal internet connection while at work, these devices may interfere with the wiretap because network traffic could bypass the wiretap. A network policy preventing employees from accessing the internet through personal devices prevents bypassing the wiretap and results in a more thorough collection of evidence.

The tap should be installed in a physically secured location to preserve evidence and prevent inadvertent damage to the equipment. Inadvertent damage could cause the courts to mistakenly believe the evidence was intentionally deleted and give the court reason sanction counsel and the company. The tap should also be hidden to prevent alerting employees subject to the order that their communications are subject to a wiretap and to prevent them from accessing evidence. Ideally, the tap should be installed in a secure, hidden and remote location capable of accessing all of the employee's network traffic.

A network location capable of intercepting the employee's traffic should be identified from network diagrams. A small office can easily be tapped by intercepting all incoming and outgoing communications through a router and modem. A large network, in contrast, may require identifying the locations of bridges, switches, as well as logging data to ensure accuracy, and possibly routing all traffic through custom routes.

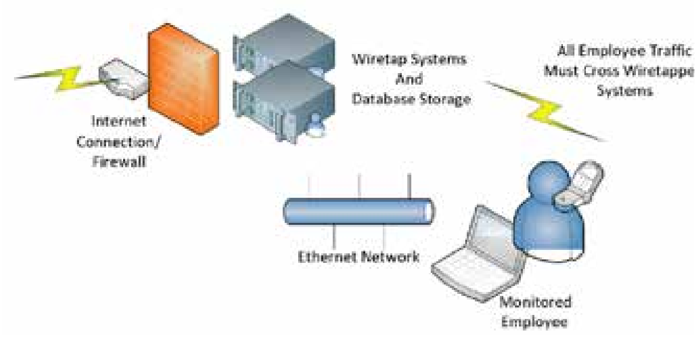


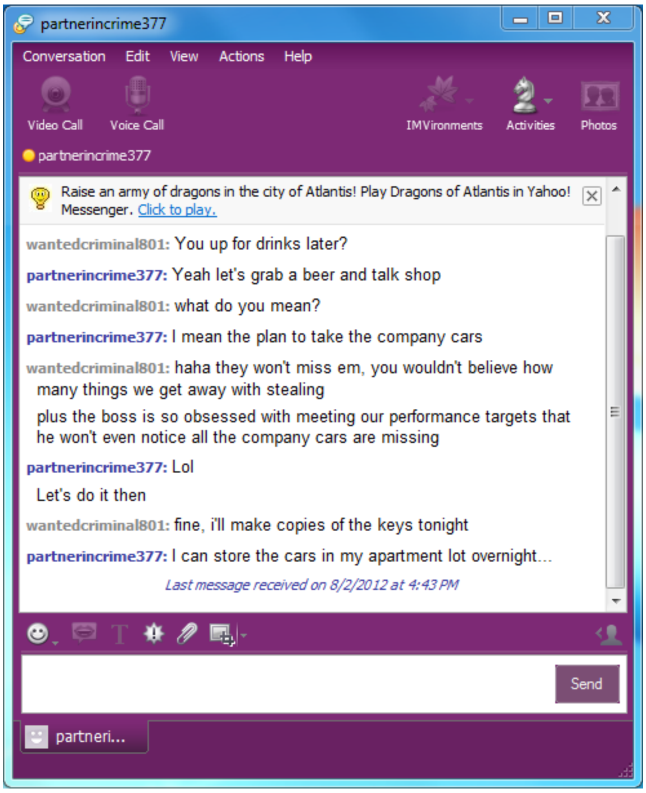
Figure 2. Where to place wiretap systems in an Ethernet Network

Once a location is chosen and a wiretapping system is installed, the system should monitor, filter, and log data. Courts generally require scientific and technical evidence to be reliable. The software chosen must meet reliability guidelines as Federal Courts, in particular, may require the collection process to be proven with statistical precision. There is little margin for error, and the software and hardware platforms must be capable of performing their intended tasks and reporting expected and actual error rates.

Extracted data should be stored in a secure location using mathematical checksums to verify data integrity and prevent breaking the chain of custody. Passwords should restrict unauthorized access, and logs should record the transfer of evidence from one system to another.

STEP 1: CAPTURE THE PACKETS WITH AN EASY TO USE NETWORK MONITORING TOOL

In this example, two users are planning to steal company cars. An example system will be used to capture and store statements relating to the conspiracy to be used in trial.



Raise an army of dragons in the city of Atlantis! Play Dragons of Atlantis in Yahoo! Messenger. Click to play.

wantedcriminal801: You up for drinks later?

partnerincrime377: Yeah let's grab a beer and talk shop

wantedcriminal801: what do you mean?

partnerincrime377: I mean the plan to take the company cars

wantedcriminal801: haha they won't miss em, you wouldn't believe how many things we get away with stealing

plus the boss is so obsessed with meeting our performance targets that he won't even notice all the company cars are missing

partnerincrime377: Lol

Let's do it then

wantedcriminal801: fine, i'll make copies of the keys tonight

partnerincrime377: I can store the cars in my apartment lot overnight...

Last message received on 8/2/2012 at 4:43 PM

Figure 2. Employees Planning a Crime with Instant Messages

ColaSoft created Capsa Free, a simple packet capturing tool that can parse instant messages and web traffic. They include a free version located which can be downloaded from their website.

Download and install Capsa Free on a system and place the system in a location capable of accessing network traffic. The system's network card will surreptitiously record and filtering network traffic. Start the application and begin capturing instant messages.

Start Capsa Free and begin capturing instant messages.

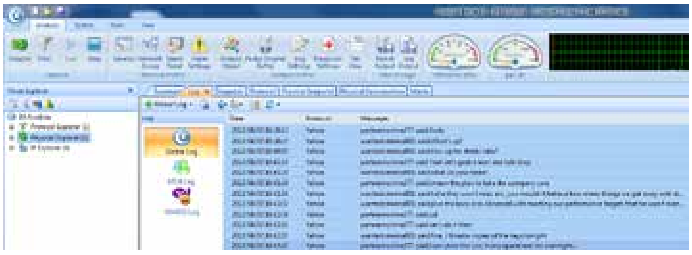


Figure 3. CapsaFree's Intuitive Interface Recognizes and Captures Yahoo and MSN Messages

STEP 2: EXPORT THE CAPTURED DATA TO EXCEL

Next, export the instant messages to an Excel file. Capsa Free does not support exporting files attached to instant messages like pictures, but other applications may. Chaos Reader does support exporting attachments like graphics but the messages must be manually reassembled. If Capsa Free captures instant messages and Chaos Reader stores corresponding attachments, the attachments from Chaos Reader must be manually matched with the corresponding messages from Capsa Free.

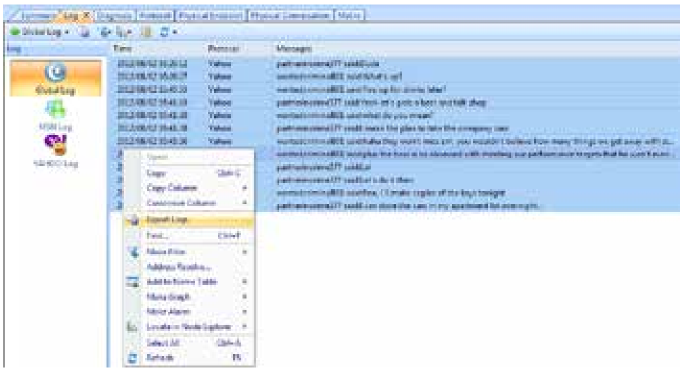


Figure 4. Exporting Instant Messages Captured with CapsaFree

Select a location to save the exported messages. Capsa Free will export the instant messages. A database application like Microsoft SQL Server can then import the messages for use with most forensic and electronic discovery applications. Protect the database's integrity by limiting access, logging all changes, making frequent backing ups, and creating checksums of raw database files before migrating raw database files. The checksums verify evidence was not added or removed when the database was transferred from one system to another. In addition, modify only one database at one time. Do not allow users to add data to several databases because data could be lost. Also, do not lose database files, store them in unsecure locations for long periods of time, or give them to adverse, interested parties.

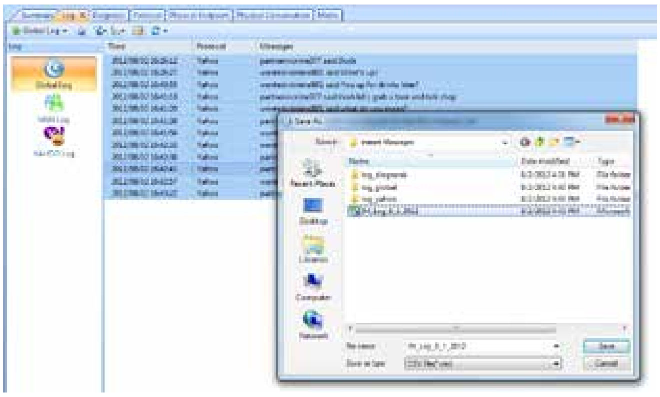


Figure 5. Carefully Select a Secure Location to Transfer Log Files

STEP 3: IMPORT THE DATA INTO A COMMERCIAL DATABASE PACKAGE LIKE SQL SERVER

Start Microsoft Access and create a new Table. Import the Instant Messages from Excel.

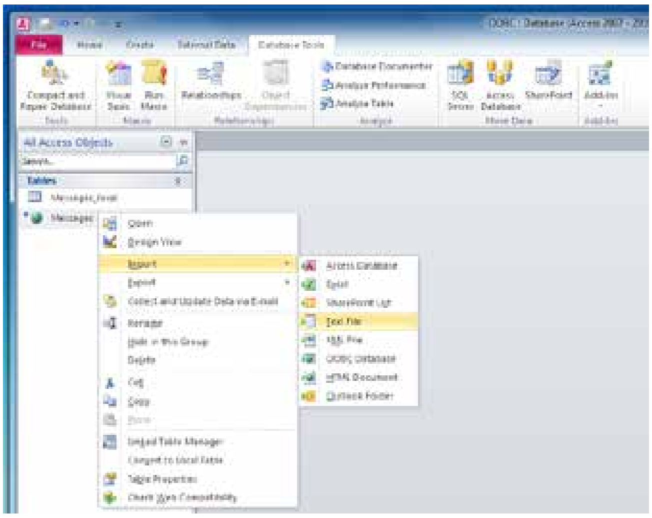


Figure 6. Importing a Log File with Microsoft Access

Select the Excel file containing the instant messages. Also select the destination table in Access.

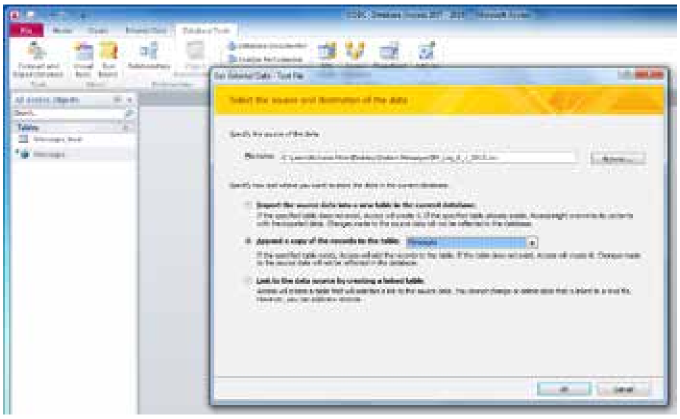

Get External Data - Text File
Select the source and destination of the data
OK
Cancel

Figure 7. Add the Log File to a Table Linked to a SQL Database

Specify the location of table field names in the Excel Spreadsheet, as well as formatting characteristics like field delimiters, and text qualifiers.

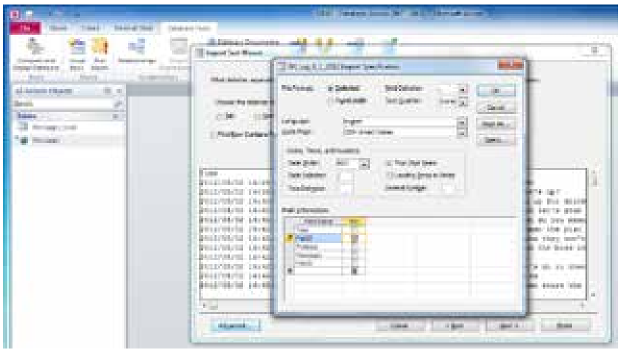
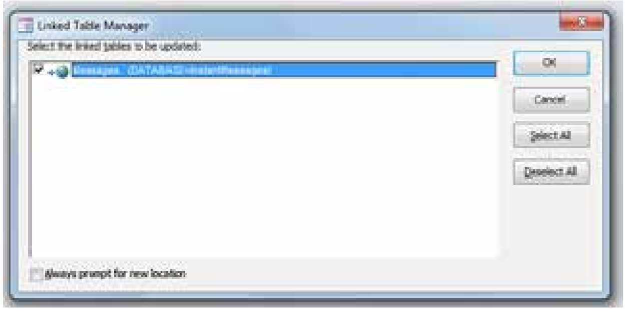


Figure 8. Specify which parts of the log file contain database fields

Link the Table to a SQL Server Database.


Linked Table Manager

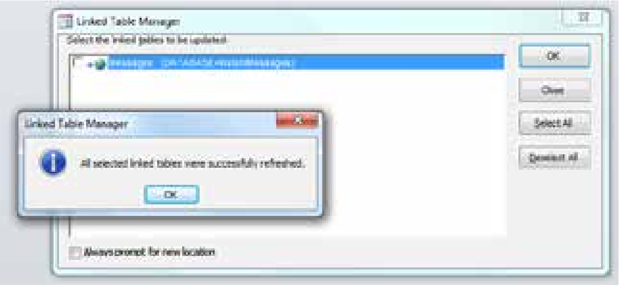
Select the linked tables to be updated:

☑ Messages (DATABASE=InstantMessages)

☐ Always prompt for new location

Figure 9. Specify a Table Linked to an ODBC connection

Refresh the SQL Database with the imported data.


Linked Table Manager

Select the linked tables to be updated:

Messages (DATABASE=InstantMessages)

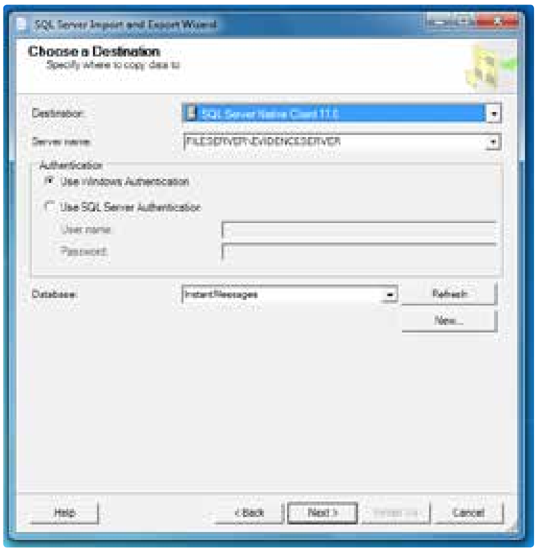
Linked Table Manager

All selected linked tables were successfully refreshed.

☐ Always prompt for new location

Figure 10. ODBC refreshes the table

Synch the Access Table with SQL Server. Choose the correct database.


SQL Server Import and Export Wizard

Choose a Destination

Specify where to copy data to

Destination: SQL Server Native Client 11.0

Server name: FILESERVER\EVIDENCESERVER

Authentication

● Use Windows Authentication

○ Use SQL Server Authentication

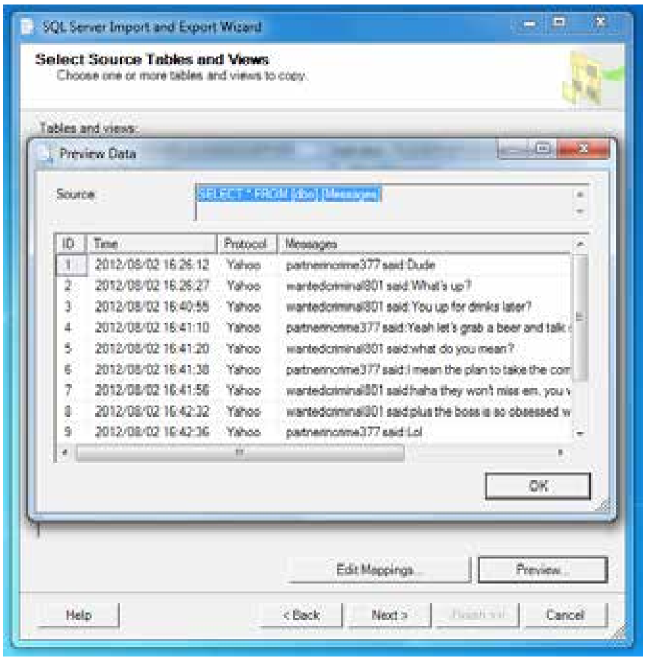
User name:

Password:

Database: InstantMessages

Figure 11. Connect to the SQL Database with the ODBC connection and update

Verify the instant messages were successfully added to the SQL Database.


SQL Server Import and Export Wizard
Select Source Tables and Views
Choose one or more tables and views to copy.
Tables and views:
Preview Data
Source
SELECT * FROM [dbo].[Messages]
OK
Edit Mappings...
Preview...
Help
< Back
Next >
Finish >>|
Cancel

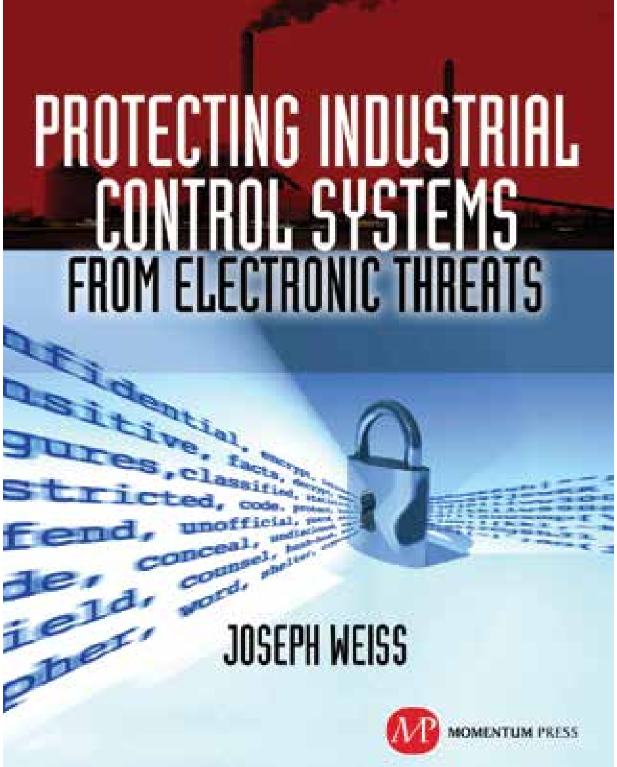
ID	Time	Protocol	Messages
1	2012/08/02 16:26:12	Yahoo	partnerincrime377 said:Dude
2	2012/08/02 16:26:27	Yahoo	wantedcriminal801 said:What's up?
3	2012/08/02 16:40:55	Yahoo	wantedcriminal801 said:You up for drinks later?
4	2012/08/02 16:41:10	Yahoo	partnerincrime377 said:Yeah let's grab a beer and talk
5	2012/08/02 16:41:20	Yahoo	wantedcriminal801 said:what do you mean?
6	2012/08/02 16:41:38	Yahoo	partnerincrime377 said:I mean the plan to take the cor
7	2012/08/02 16:41:56	Yahoo	wantedcriminal801 said:haha they won't miss em. you v
8	2012/08/02 16:42:32	Yahoo	wantedcriminal801 said:plus the boss is so obsessed w
9	2012/08/02 16:42:36	Yahoo	partnerincrime377 said:Lol

Figure 12. Verify data was successfully appended in SQL

In summary, installing a wiretap can easily record real-time communication and provide valuable insights at trial. A party who thought they successfully deleted archived evidence can be impeached with evidence collected real-time. In addition, the threat of recording real-time communication improves judicial accuracy and efficiency by giving all parties an incentive to tell the truth and settle because they will know at the outset the courts will be more objective. These technologies also subject users to potential criminal and civil liability for illegal wiretaps, and wiretaps without a proper warrant.

Author bio

Nicholas Miter has a Juris Doctor from the University of Pennsylvania Law School, a Bachelor of Science in Computer Science from the University of Illinois at Champaign-Urbana, and has worked for innovative companies like Microsoft, Intel, AT&T, Factset Research Systems, and most recently Nuix. He has completed several Finance classes at the Wharton School of Business and served as an editor for the Journal of Labor and Employment Law.


PROTECTING INDUSTRIAL CONTROL SYSTEMS FROM ELECTRONIC THREATS
JOSEPH WEISS
MOMENTUM PRESS

ACUMIN

Global **Information Risk Management** Recruitment

Information Security & Risk Management | Governance & Compliance
Penetration Testing, Forensics & Intrusion Analysis | Technical Security | Business Continuity Management
Sales Engineering | Sales & Marketing | Public Sector Security | Executive Management

Network and/or Application Penetration Tester

Ref: 14951 **Location:** UK wide **Salary:** £25k-£75k base + bonus + package
Job Type: Permanent

Multiple opportunities for Penetration Testers. Varying levels of experience will be considered. You will be offered first rate project exposure as well as on-going training, culminating in superb earning potential.

Key competencies and experience required:

- Use of a variety of network security testing tools and exploits to identify vulnerabilities and recommend corrective action
- Manual penetration testing and a deep understanding of IP networking in a security context
- Deep knowledge of IP networking protocols
- Experience with security testing of Web-based applications
- Intimate knowledge of at least one enterprise development framework
- Proven ability to explain verbally the output of a penetration test to a non-technical client
- Strong inter-personal and communication skills
- Report-writing and presentation skills
- Must be prepared to travel

Desirables:

- Code review skills
- CHECK, CREST or TIGER qualification
- Current UK driving licence

Please email your CV to careers@acumin.co.uk quoting the reference above

Web Application Penetration Tester and Security Specialist

Ref: RF14803 **Location:** South East **Salary package:** £400-£600 per day
Job Type: Contract

This blue chip finance organisation is currently developing its internal information security function, and as such has identified a need for a lead security specialist with a particular focus on web application security.

Responsibilities

- Conduct technical security assessments against strategic initiatives prior to final release in to an operating environment.
- Carry out such tests and assessments against internal standards as well as industry standards such as SAS70 and PCI-DSS.
- Define and execute penetration tests as part of the review lifecycle for infrastructure, applications, and web applications.
- Perform regular vulnerability assessments using scanning tools to ensure the on going security of systems to emerging and known threats.
- Provide expertise in to forensics investigations and incident management as required.
- Identify and manage required resources, creating reusable documentation, processes, and toolsets.

Requirements:

- Strong understanding of technical security principles around penetration testing, vulnerability management, and forensics.
- Knowledge of current assessment techniques and toolsets such as OWASP guidelines, WebInspect and Fortify.
- Prior working experience of industry standards and processes - PCI, ITIL, Prince, COBIT, COSO.
- Demonstrable track record of security design, review, and implementation.

Please email your CV to careers@acumin.co.uk quoting the reference above

Acumin Consulting Ltd
Suite 22, Beautfort Court,
Admirals Way,
London E14 9XL

Telephone	+44 (0)20 7997 3838
Fax	+44 (0)20 7987 8243
Email	info@acumin.co.uk

www.acumin.co.uk
www.acuminconsulting.com

AN INTRODUCTION ON IMAGE AND VIDEO FORENSICS - DRAFT

MARTINO JERIAN - AMPED SOFTWARE - MARTINO.JERIAN@AMPEDSOFTWARE.COM

Abstract

Surveillance cameras, photo enabled cell phones and fully featured digital cameras are present almost everywhere in our lives. Very often they constitute a very important element in forensic cases, being used as investigation elements, as evidence, or maybe as alibi. Yet, due to CSI-style fictions and lack of training, many times this material is used in a way that can invalidate the case, important aspects are overlooked or lead to unrealistic expectations. The purpose of this article is to give some foundation on forensic image and video analysis to those who are more likely to have to deal with this kind of material.

INTRODUCTION

There aren't any uniquely accepted terms describing what we are calling image (and video) forensics. Some call it forensic imaging, others forensic video analysis, or forensic photography, or with many other combinations of similar terms.

All these names represent pretty similar concepts or slightly different aspects of the same branch. If we limit our analysis to the most technical aspect, probably the most correct term to call it is forensic image processing, which is the application of image processing techniques to forensic sciences.

Forensic image processing is the intersection of two different fields:

Forensic science (from Wikipedia): "forensic science (often shortened to forensics) is the application of a broad spectrum of sciences to answer questions of interest to a legal system."

Image processing (from Wikipedia): "In electrical engineering and computer science, image processing is any form of signal processing for which the input is an image, such as a photograph or video frame; the output of image processing may be either an image or, a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it. Image processing usually refers to digital image processing, but optical and analog image processing also are possible. This article is about general techniques that apply to all of them. The acquisition of images (producing the input image in the first place) is referred to as imaging."

Nowadays image processing is done almost entirely working in the digital domain, so basically we use forensic image processing to try to find the needed answers in a legal proceeding thanks to the processing and analysis of images and videos in digital form, that are finally just a sequence of encoded numbers that represent some informative content.

Generally speaking, image processing is used both to process actual image files (jpeg, bmp....) and video files, that can be either in a standard format, like avi, or in closed formats generally used by proprietary surveillance systems.

One of the fundamental documents formally describing the different terms is the IAI-LEVA Forensic Imaging and Multimedia Glossary (http://www.theiai.org/guidelines/iai-leva/

forensic_imaging_multi-media_glossary_v7.pdf). It basically divides media forensics in three different branches: forensic audio, forensic video, and forensic photography.

In this article we'll focus on forensic video, with particular regards to the enhancement and analysis of videos coming from surveillance devices. Very similar considerations can be done for the enhancement of pictures and videos coming from a more generic context.

The analyst's job doesn't start and end with viewing and enhancing a video, as it's more complex: the data of interest must be identified, decoded properly, and the process must be documented clearly and sometimes presented to the court for testifying about it.

In the following of the article we'll outline all the steps that characterize a complete and comprehensive analysis. Not all the steps are done in all the cases, depending on the specific situation and the court requests. Many times the analyst is not the one that recovers the data and may not be needed to present the result. But it's important to keep in mind the overall workflow.

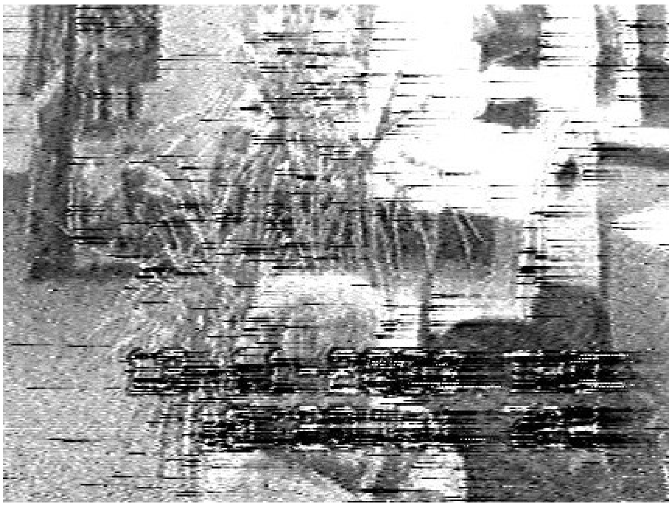
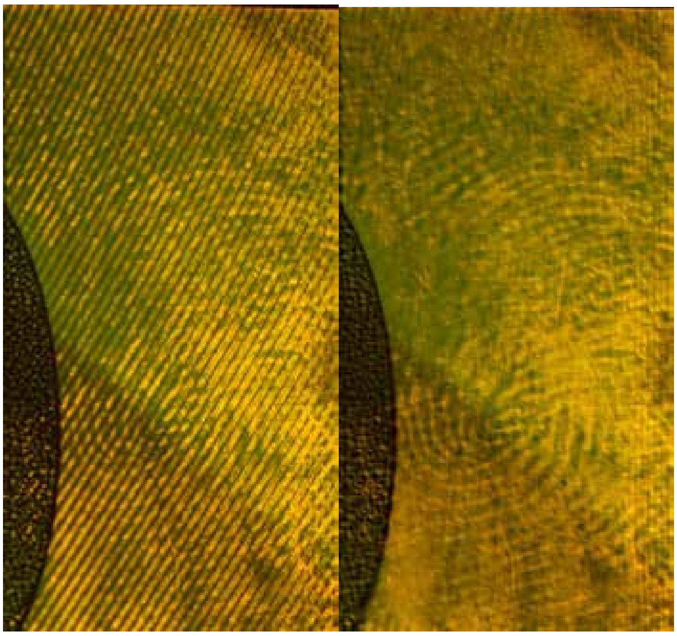


Figure 1: CCTV video is one of the primary source of data for image and video forensics



GATHERING THE DATA

This step may be the most important and can be very complex and critical for evidence integrity. Unfortunately, this is generally not done by the experts, or by those who know how to take care to document the steps. Worst case, the original evidence is gathered by a patrol officer who is the first on the scene. A low-res copy of an original is output to a disk or thumb-drive, and the original DVR is left to be copied over by the next day's footage. This happens far too frequently, and gets everyone off to a pretty bad start.

The ideal situation would be if the acquisition is taken with procedures typical of digital forensics, but very often the analyst has to work on images received by mail or on videos burned onto a DVD without any care.

These are some of the situations that may be faced in this step:

- Analyze a disk image for complete and deleted files.
- Export a video from a DVR.
- Copy a file from an hard disk.
- Capture a video from an analog device (e.g. VHS).

Even a simple operation like a copy should be done in the most scientifically relevant way by verifying hash codes and so on.

For police investigators working in the real world case of evidence gathered by a non-scientific responder, with a little better communication, training, and diplomacy, the situation can be improved.

VIEWING AND CONVERTING THE FILES

Once the data has been retrieved, it's necessary to view it. For plain video files, it is not a big problem, having the proper codecs. To determine which approach we take, we need to know what we are looking at. This step generally defines the challenges that we may be facing:

- We have a disk image and we need to reconstruct images and videos, even the ones that may have been deleted (this is common in child pornography cases, for example).
- We have a dump of a DVR drive and don't know how the data is encoded.
- We have an export of surveillance footage, but the video is in a proprietary format (a very common situation).

With this step, we may need to do some research to really define what we need to complete the job. Do we need to focus first on data recovery? Do we need to find a better decoder? Do we need to find a better player for the video or means to export it properly?

Sometimes, this is an easy step, other times it is far more difficult and time consuming. Remember, this is a scientific pursuit and science sometimes can't be rushed.

Viewing and exporting the video can seem like a trivial task, but it is not. There are literally hundreds of different proprietary video formats, all bound exclusively to the producer software, which is often buggy, not updated for newer versions of Windows, and many times without enough or good enough exporting options. The first and most important rule is too always keep the original format along with its player.

As said, too often the analyst will receive just some snapshots of the video file as jpeg, or maybe one converted avi with a quality much lower than the original.
It is, in fact, of extreme importance to always keep the original, for the following reasons:

1. If you need to go to court and start the processing on data which is not the original and which is not generable again with a scientific and repeatable process, this may invalidate the case.

2. You must always start from the original to be sure to keep the highest possible quality.

Once you have the player, how do you export data from it?

- if your player allows you to save frames and you can identify a short number of frames that are of interest, you can manually save them as single pictures, preferably in an uncompressed format such as Bitmap or TIFF. Avoid using JPEG, which will compress the images again, removing details and adding artifacts. Please also note that TIFF images can be compressed with a JPEG algorithm, but that this is not the most common case.

- if you need a longer part of the video, saving single frames is not practical. In this case you need to export the video (if your software allows it). If you have the possibility to select the codec for exporting, choose Raw Video or another lossless codec. Be careful because the produced file (especially in the case of Raw Video)will become huge.

- if you are in the worst situation, where your player does not have the possibility to export data in any way, you must capture snapshots of the screen. For a few frames you can just capture the screen content in the clipboard and then paste it in any imaging program. If you have many frames you will need some software that allows the creation of screencasts. Also in this case you need to save the video with the highest possible quality, preferably without compression, and avoiding duplicate and lost frames. This is quite a complex subject on its own.

Please note that some players allow basic image processing functions, such as the adjustment of contrast and brightness or JPEG deblocking. If you are going to export the file to use it in another software, try to disable this feature, since you will need to start from the most original data.
Also please note that the exporting function of some software actually captures nothing but the content of the screen, so be careful to play the video at its original size in order to avoid the introduction of interpolated frames.

FINDING EVENTS AND IMAGES OF INTEREST FOR THE CASE

At this step we should be able to view the videos or the images, but we need to find the right ones! Two examples of what we may face may be:

- Finding images of interest in a large database.

- Looking for an event of interest in several hours of video.

This step can be helped with communication from other team member working on this case. For most cases, the basic thing we need to understand is: what happened, and when did it happen?
It's really unbelievable how often the analyst is given some video, without telling them what to look for. Details like the time of the day, the involved car, or the event to look for may be obvious for those who are spending days on a case, but not for someone who is just looking at the video for the first time.
And of course, software tools may help too, with technologies such as video content analysis and face recognition. Even simple procedures like motion detection, can save hours of viewing time. Since very often CCTV cameras are static, looking for events of interest based on the motion which is found on some part of the footage is very useful, at least for the first analysis.

IDENTIFYING THE SOURCE OF THE IMAGES

Depending on the situation we may need to understand how the original files have been generated. With some generalization this may be called image ballistics. Understanding the type of file and the source can help to put in a different light several aspects of a case. Some analysis that may be done could be:

- Identify the type of source (digital camera, scanned image, computer generated, etc.).

- Identify the camera model used for taking the picture.

- Identify the specific device that has taken the picture.

We need to document the source so that we can maintain the integrity of our evidence. This will help us if we have to go to court later.
Going back to what we have mentioned in the previous sections, it's very important at least to understand if we are working on an original file or not. For example, if the object of the analysis is an avi file, but the surveillance system that the file was generated from uses a proprietary format we will need to request the proper file and player. Even if the original file has been lost or overwritten, at least we are aware that we are not working on the primary source.

VERIFY THE INTEGRITY

At this point we may be interested in understanding if we can trust the data we have gathered. Is there a probability that someone altered it? This can be done on various levels.

- Verify if the file the file has been manipulated, for example altering the metadata.

- Verify if the image has been manipulated, for example converting the format, resizing, or cropping it.

- Verify if the content has been manipulated, for example removing or adding a subject.

Tampering is becoming more commonplace. It can be done innocently (like converting formats from the original to a low -res media file) or purposeful "photoshopping" to manipulate facts. In this digital age, it is something that we need to address.
Even though it's much more difficult to tamper with video files, it happens. It's very important to evaluate with some practical induction if the tampering was worth the case, but so many actual cases happened where images and videos have been modified that it's worth at least asking if the original data is as such.

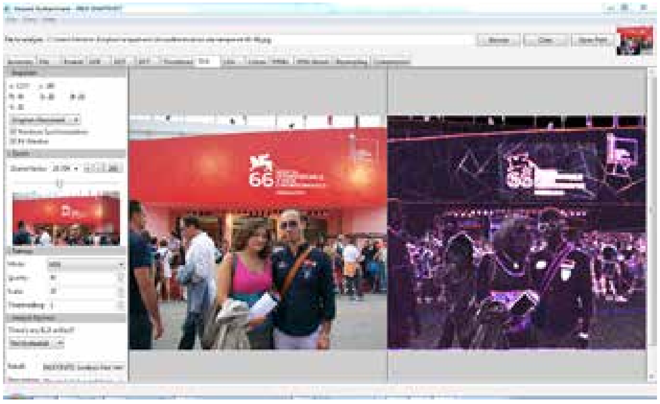


Figure 2: identifying tampered images; the area around the festival logo and number (66) has been modified.

UNDERSTANDING THE QUALITY OF THE IMAGES AND ITS ISSUES

The next step is to understand if the quality of the image is good enough to get the information we need. Typical questions that the analyst should ask himself are:

- If we see a car, are we able to read the license plate? Or if we have a face, do we have enough pixels for a reliable identification?
- Does the image effectively contains the information we need (e.g. the license plate has enough pixels)?
- If not, can the information be recovered or viewed better with image enhancement or image restoration techniques?
- What are the specific defects in the image? Can they be recovered?

Technical knowledge and experience is very important to estimate quickly if we have enough quality or not. It is not always easy to estimate the minimum quality to get useful results. A shortcut with things like faces and license plates is zooming in and counting pixels. If you only have six or eight pixels to draw all the characters in a license plate, the probability of success is pretty close to zero, no matter the techniques you use.

VIDEO ENHANCEMENT AND CLARIFICATION

Once we have identified the problems affecting the images or videos it's possible to enhance and restore the images. This step is actually pretty vast, and can involve processes like:

- Image enhancement techniques: emphasize (or reduce) some features of interest of the image (contrast enhancement, histogram equalization, sharpening…).
- Image restoration techniques: understand the mathematical model of a known disturb and try to invert the model to recover the image without the defect (deblurring, Fourier filtering, frame integration…).

There are several tools available on the market, such as Amped Five, by the writer's company - Amped Software (http://ampedsoftware.com), that provide image processing tools specifically cut for forensic applications. Since the different defects are usually present together, quite often it is necessary to apply even more than ten different algorithms to properly enhance the image.

Very often the analyst is asked for impossible results: it is very important, as forensic scientists, to be aware of what is possible and was is not possible to recover. In general, if there is no useful information in our picture, we cannot - and absolutely must not - recreate it. We are able to recover the information only if it is already in the image, hidden by defect or poor image features.

No one can guarantee the great results found with Hollywood magic on the CSI shows, but sometimes it is possible to get amazing results.

One thing that is really important to remember in this step is documenting the enhancement process. Some of the specialized forensic software does this automatically, so you have documentation to take to court. General purpose software does not usually provide enough tools for this issue.

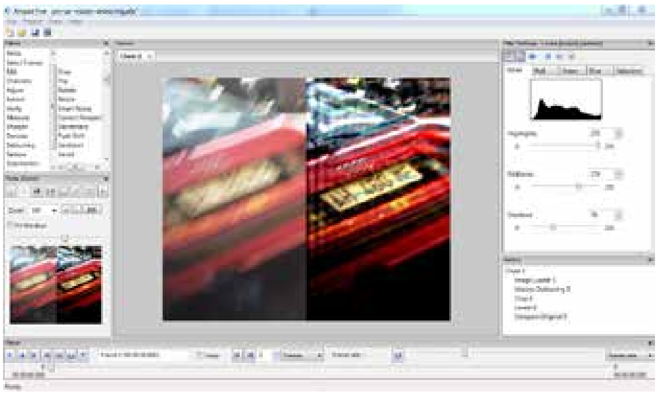


Figure 3: an example of license plate deblurring

ANALYZE THE RESULTS

This step consists in drawing some conclusions on the enhanced images, thus converting the visual information in some more precise informative content related to the case. The enhancement step would be useless if there's no improvement to the content of the image so we can understand and classify it. An example of what can be done, in this phase, depending on the context, is:

- Compare a face in two different images.
- Compare a face with a known subject.
- Read the license of a vehicle.
- Identify the place where a picture is taken.
- Measure the height of a subject.
- Find the corresponding fingerprints in a database.

If it's not possible to get the needed results it's possible to go back and repeat the previous steps, or determine that from the provided data it's not possible to get any useful information. Again, this is a scientific process and should be left without emotion. Sometimes it is too easy to get bent out of shape over a ton of work without results; but those are sometimes the cards that we are dealt.

A very important aspect is that of objectivity: very often, especially with low quality images, different people see different things, and usually it's what they wanted to see. For this reason, in some cases it would be better to work on the data with very little understanding on the overall case.

It's very common that people see what they want to believe: a random reflection in a glass becomes a face, a JPEG artifact becomes a letter of a license plate and so on. Many times there are simple explanations for what they see, many doubts on the non-expert interpretation, and being purely objective with customers is often hard in itself.

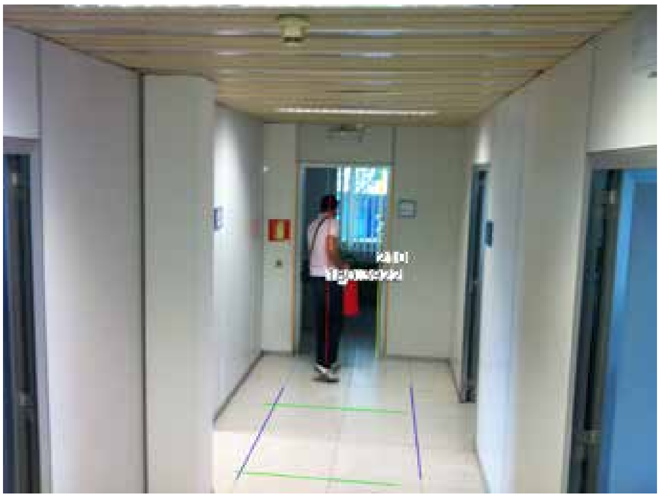


Figure 4: measurement of a subject with single view metrology

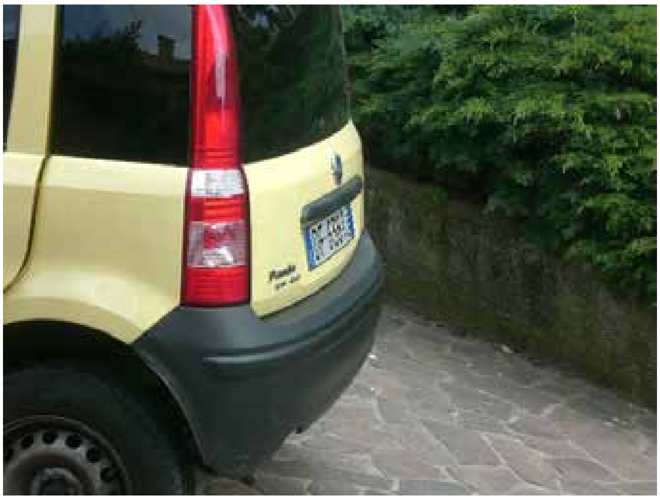


Figure 5: perspective correction (original)

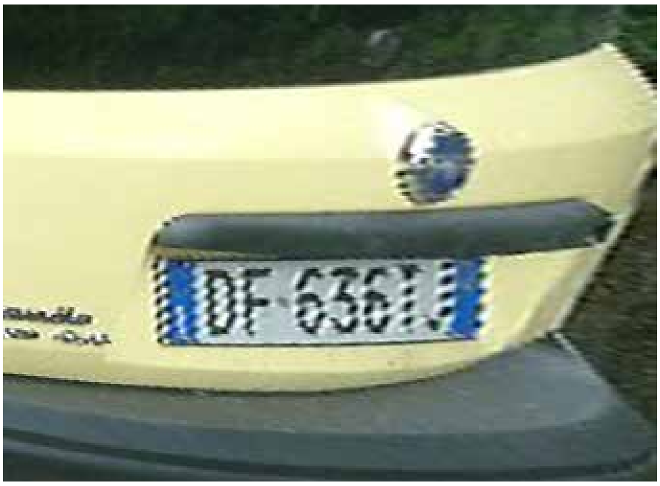


Figure 6: perspective correction (processed)

VALIDATION OF THE PROCEDURE

Validation isn't just focused on the quality of the result. It is also about the quality of the process used to gain the result. It must be always maintained that the techniques used must be valid both from the scientific point of view and follow a procedural set of standards accepted by the courts that have jurisdiction on the current job. This is extremely important for the verification of image integrity and for documenting the enhancement workflow.

A few things to consider are:

- State of the art techniques must be validated by peer review and accepted by the scientific communities.
- The results must be scientific and repeatable.
- A detailed audit trail must be kept to explain how we go from the original image to the enhanced one.
- This may be seen (and actually is) as manipulation of evidence, and thus we must be able to justify it properly from the scientific point of view. In this case, documentation is key.

PRESENTATION OF THE RESULTS

Getting the results is not enough. Often the expert is called to explain them to the court and the jury: you must be able to make them understand and accept the techniques you used. Scientists, engineers, attorneys, and normal people speak different languages. It is really important to organize any fact in a clear and open manner, with technical rigor, but in a manner that is understandable by normal people.

A good defense attorney/prosecutor will try to trip the expert up with the "has this image been photoshopped?" question and questions about certainty, possibility, etc. Often their questioning tends to be less focused on science, and more focused on emotion. In court, emotions are often charged and an attack on the expert process can be presented as a personal attack with the idea to get him/her to deviate from facts. That is the game-plan for attorneys when they can't debate the facts.

The key to overcoming this type of questioning is to document the workflow and stick to the science. This is scientific, but it has to be explained to non-scientific people. The expert needs to present the facts of the case and explain the science in plain language in an organized, clear, and concise manner. At the very minimum, it's needed to show:

- The original.
- Where it came from and how it has been retrieved.
- What steps were taken to get the result.
- How that result relates to the case.
- What scientific methods were used to validate the result.

It's not an easy task, as very often complex matters are oversimplified to be understood by laymen and at the end of the day the work of the expert witness can amount to nothing.

THE BOTTOM LINE

We have seen an outline of the principal tasks to face when dealing with image and video forensics cases.

Often, the expert may work in a team and only concentrate on a couple of them. Again, the point to drag away from this whole outline of workflow is organization and methodology of overall processes.

Depending on the subject of the work, it may be not formally necessary to define these steps so clearly, but critical and systematic thinking are really the foundation of this job.

Author bio

Martino Jerian is an electronic engineer specialized in image and video processing for forensic applications.

In 2008 he founded Amped Software (http://ampedsoftware.com), with the single mission to develop the one-stop software for any need related to image and video processing for forensic and security applications. Its flagship product, Amped Five (http://ampedsoftware.com/five), is used worldwide by forensic labs and law enforcement agencies.

He also worked as forensic image / video analyst and expert witness on several well-known cases.

PC Fix
PCFix
Fix Windows Registry
& Repair PC Errors!
Before you continue:
Free scan your Computer now!
Improve PC Stability and performances
Clean you registry from Windows errors
Instant Scan

FORENSIC 3D IMAGERY UNLOCKS HIDDEN EVIDENCE

HERBERT RAWLINSON

I never knew I had an interest in forensics or law enforcment, it just sort of happened one day. It was the spring of 2006, and I was waiting to watch my daughter perform with her dance company at a local school. As usual the fathers of the dancers would find each other and pass the time waiting for their girls to go on stage. This day was no different than any of the others and pretty soon one of the dads and I were deep into a conversation. I have been in the television and movie industry for a number of years and was explaining to this dad about this new technology we were using to digitally visualize complex scenes using the latest 3D software in a process called pre-visualization (PreViz). Soon he started asking a lot of detailed questions way beyond any normal interest in my work. I knew something was up but I could not figure out the angle...and then he told me what he did for a living he was a Deputy District Attorney for the County of Los Angeles.

By the end of the conversation this dad had surmised that by developing a three dimensional visual aid during the investigation process county law enforcement and DA's offices alike could benefit greatly from this technology. A 3D recreation could complete the process and achieve a successful prosecution if these powerful visual aids were used in court. It provides a visual reference to complex scientific evidence making it easier to understand. He explained that most juries find it hard to grasp complex scientific evidence especially when it comes to trajectory, spatter and physical evidence related to human movement. That coupled with days and days of „expert testimony" most on the jury become numb to the facts and can easily accept any alternative theory provided by a defense attorney or expert witness. „Forensic evidence when present at a crime scene points to the most logical scenario, then if we use a 3D crime recreation to help explain the scenario ..." Deputy DA Robert Villa had an idea. And I became an accidental forensic expert.

People V. Seymour

He explained to me the problem he was having with an upcoming murder trial. The defense was that the victim was shot by the defendant accidentally when he dropped his gun. The forensic evidence indicated that the wound track of the bullet could not have been fired from a gun on the ground, unless the 300+ pound 70 year old preacher was doing a ballet move my daughter would be envious of. I built a 3D recreation using the same software used to create a PreViz and took the information given to me by DA Villa. We knew the height of the victim and estimated the height of the accused and built the environment to scale. We changed a few parameters and behaviors and were able to see the results instantly. After some tweaking, we finally had a good working animation of his version of what happened, the defendant's version of what happened and how the preacher would have to have his leg behind him at a 90 degree angle to match the coroners findings.

Finding the best way to present a „to scale" version of the crime had its challenges. After visiting the actually crime scene I was able to use a simple trick to give my recreation a realistic sense of space and scale. I took a 1 foot by 1 foot foam cube and placed it on the street where the crime took place. Then I took several picture and videos from severel different angles. I took these images and compared them to my animation and made the appropriate scale changes. The next challenge was how I can make this cost effective so, the county could afford it. Living in the Los Angeles are where Hollywood rates for 3D artist are huge and visual effects and animation studios open and close on a weekly basis. I had to come up with a way to streamline the process and make it as cheap as possible. With a small group of talented people with the same vision and building an asset library of people and buying the vehicles already pre-built and then rigging these asset to perform the function I needed, drastically reduced production costs.

The problem now was could DA Villa use the recreation in court. If he presented the video as evidence in court, during his case-in-chief, he would have to put me on the stand and subject me to cross-examination. I had no formal training and knew very little of forensics. DA Villa asked me several questions that he would expect a defense attorney to ask. My answer to most of his questions were either „I don't Know" or „Because he, DA Villa, wanted me to do it that way". We both agreed that my testifying would be a mistake. After a few minutes he came up with another idea, „I'll just use it in my closing argument". He told me how the recreation would just be an extension of his view of the evidence of the case. He asked me if I could manipulate the environment as he argued to the jury. I told him that I would be comfortable doing that, so that is what we did. He got his conviction and I got my introduction to criminal forensics...I was hooked.

People v. Kamara

About a year later, DA Villa came to me with another case. Again, he had a defendant who claimed that he wasn't at the murder scene. A single drop of the defendant's blood in the alley behind the victim's apartment along with a blood trail of the victim's blood was the only physical evidence connecting the defendant to the murder. The defendant and the victim did not get along and the victim had been looking for the defendant to fight him. Through animations, we were able to illustrate how a fight in the alley led to the defendant stabbing the victim.

On the second go around in court obvious problems arose with showing the animation in real time. Moving around the environment as he was giving his closing arguments was problematic and very cumbersome. I was using a program that was not built to run complex animations in real time. To view a finished PreViz you would normally render out the scene at several different angles and cut the pictures together using editing software. I started to think of other options at this point.

People v. Moore

We teamed up again a few months later on a DNA cold hit case. Once again, DA Villa had to explain how the defendant's blood got into the victim's car. Eighteen years had passed since the murder and there were no identification witnesses. The forensic evidence consisted of a lot of the defendant's blood on the drivers' side of the car, several bullet holes in the vehicle and a scar on the defendant's left arm. The victim was carjacked in the parking lot of a store. During the carjacking, the victim was shot several times. A friend of the victim shot at the person taking the car, as he drove off. We were able to establish the angle of the shots based on the positions of the principals involved and the photos of the vehicle and the trajectory of the bullet strikes. There was one particular sharp entry bullet track that was identical to a scar on the defendant's arm. We had now perfected the presentation, of the recreations during the closing argument, to coincide with the prosecutor's argument for maximum impact on a jury.

This was by far the most animation in on scene I have ever attempted and tried to run in real time in court. With all the cars and all the people it was just too large of a file to run smoothly. I struggled with it and again became frustrated and knew then I had to come up with a better idea for presentation. The animations look great and were very effective but some of the impact was lost due to the presentation problems.

People v. Spector

About this time other DAs in LA County noticed what I was doing for DA Villa. I was contacted by DA Alan Jackson to work on the Phil Spector murder. Even though this was the most high profile case I had worked on to date, it was rather simple. Two people minimal movement and only a few seconds long. But it ran smooth in court and had and interesting impact on the jury.

DA Jackson was concerned that if it "looked to slick" the jury might think he was trying to "put one over on them". Since I try to make the characters look like the people they represent, well let's just say my Phil Spector came out looking a little scary. In the end, we were able to present a compelling visual argument that aided in his conviction.

People v. Winzer

In 2009, DA Villa came to me once again with a real complicated project to see if I could put together a crime scene recreation. This case involved a „provocative act murder" which is basically a case where a defendant shoots at someone and that person shoots back and kills a third person. The person who shoots first can be charged with the killing. This factual scenario involved three moving vehicles, a person running and bullet traces at the same time. The goal of the recreation was to show how police officers believed the shots were coming from one vehicle, when in reality the shots were coming from the defendant standing on the opposite side of the vehicle shooting at the same car.

Knowing that this animation would not run smooth or run at all in court using the 3D software, I decided to tackle the problem. With the help of my team of animation experts, we loaded the animation into a video game engine and produced a video game of the crime. When it came time to view the animation, as we have done many times in the past, I showed up to DA Villa's office without my computer. He looked at me with great concern because he knew the laptop that I was using in court is a high powered machine. I handed him a CD with the game on it, he loaded it onto his laptop, I gave him a quick tutorial on how to run it and his eyes grew wide with excitement. Once he took it home and his 10 year old daughter showed him how to play a video game DA Villa was able to walk through the crime scene and run the animation from any angle he wanted.

By utilizing 3D modeling during the forensic process, and eventually using a custom video game to show the visuals during the prosecution,   I have been able to provide juries with pictures that are worth a thousand words.

Herbert Rawlinson
Owner, Forensic 3D Imagery

herbrawlinson@cs.com

http://www.youtube.com/watch?v=voyI0etCwbY

IN THE UPCOMING ISSUE OF EFORENSICS NETWORK...

WIRELESS FORENSICS

& MORE...

Available to download on September 22th

If you would like to contact eForensics team, just send an email to en@eforensicsmag.com.
We will reply a.s.a.p.

eForensics Magazine has a rights to change the content of the next Magazine Edition.

Now Hiring

Teamwork

Innovation

Quality

Integrity

Passion

Sense of Security

Compliance, Protection
and Business Confidence

Sense of Security is an Australian based information security and risk management consulting practice. From our offices in Sydney and Melbourne we deliver industry leading services and research to our clients locally, nationally and internationally.

Since our inception in 2002, our company has performed tremendously well. We thrive on team work, service excellence and leadership through research and innovation. We are seeking talented people to join our team. If you are an experienced security consultant with a thorough understanding of Networking, Operation Systems and Application Security, please apply with a resume to careers@senseofsecurity.com.au and quote reference PTM-TS-12.

info@senseofsecurity.com.au
www.senseofsecurity.com.au