eForensics Magazine

Vol.04 NO.02

OPEN

EXPLORING, DECRYPTING, DISSECTING AND DECIPHERING

STEGANALYSIS

DATA RECOVERY: BEST PRACTICES FOR SERVICE PROVIDERS

DISSECTING AND DECIPHERING THE COMMUNICATIONS OF CYBER ESPIONAGE MALWARE

CYBER BLACK BOX DECRYPT

P2 COMMANDER

Issue 02/2015 (41) March ISSN 2300-6986

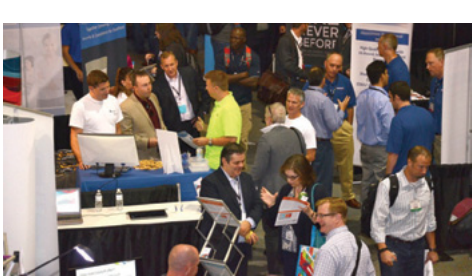
Big Data Gets Real in Boston!

People are talking about BigData TechCon!

"Big Data TechCon is a great learning experience and very intensive."
—Huaxia Rui, Assistant Professor, University of Rochester

"Get some sleep beforehand, and divide and conquer the packed schedule with colleagues."
—Paul Reed, Technology Strategy & Innovation, FIS

"Worthwhile, technical, and a breath of fresh air."
—Julian Gottesman, CIO, DRA Imaging



"Big Data TechCon is definitely worth the investment."
—Sunil Epari, Solutions Architect, Epari Inc.

BigData TECHCON

April 26-28, 2015

Seaport World Trade Center Hotel

Big Data TechCon is the HOW-TO technical conference for professionals implementing Big Data solutions at their company

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

- Process and analyze the real-time data pouring into your organization
- Learn how to extract better data analytics and predictive analysis to produce the kind of actionable information and reports your organization needs.
- Come up to speed on the latest Big Data technologies like Yarn, Hadoop, Apache Spark and Cascading
- Understand HOW to leverage Big Data to help your organization today

www.BigDataTechCon.com

A BZ Media Event

eForensics Magazine
TEAM

Editor:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Betatesters/Proofreaders:
Olivier Caleff, Kishore P.V., JohanScholtz, Mark Dearlove, Massa Danilo, Andrew J. Levandoski, Robert E. Vanaman, Tom Urquhart, M1ndl3ss, Henrik Becker, JAMES FLEIT, Richard C Leitz Jr

Senior Consultant/Publisher:
Paweł Marciniak

CEO: Joanna Kretowicz
jaonna.kretowicz@eforensicsmag.com

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

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

DTP: Ireneusz Pogroszewski

Publisher: Software Press Sp. z o.o.
02-676 Warszawa, ul. Postępu 17D
Phone: 1 917 338 3631
www.eforensicsmag.com

Dear Readers,

We are pleased to present you our new issue of eForensics Magazine – "EXPLORING, DECRYPTING, DISSECTING AND DECIPHERING". We hope that you will enjoy reading our Magazine and subjects covered in this issue will help you stay updated and aware of all possible pitfalls! It's an Open issue and subjects are the mash-up what we found interesting together with our team of authors.

As we publish "Workshop's eBooks" regularly as sum-up of materials from our workshops, such form of the magazine gives us a chance to present you various topics. Some of them can be extended in the future - we count on your feedback!

We know that the new convention is still something new for you but we believe that it will give you more benefits.

The schedule of our online courses you can find under this link http://eforensicsmag.com/all-courses/ After each online course you will get dedicated eBook.

It's very special time of the year... Easter brings family and friends together. May the true meaning of the holiday season and Spring that is coming fills your heart and home with many blessings. Thank you for all the support.

Happy Easter!

Joanna Kretowicz
CEO at SW Press
EIC of eForensics Magazine

Techno Security & Forensics Investigations Conference

Mobile Forensics World

May 31 - June 3, 2015

Marriott Resort at Grande Dunes

Myrtle Beach, SC · USA

The international meeting place for IT security professionals in the USA

Since 1998

Register Now at

www.TechnoSecurity.us

with promo code **EFOR15** for a

20% discount on conference rates!

Comexposium IT & Digital Security and Mobility Trade Shows & Events:

lesassises de la sécurité et des systèmes d'information · rooms · lecercle européen de la sécurité et des systèmes d'information · Techno Security & Forensics Investigations Conference · Mobile Forensics World · CARTES SECURE CONNEXIONS · CARTES SECURE CONNEXIONS AMERICA · an event by comexposium The place to be

DISSECTING AND DECIPHERING THE COMMUNICATIONS OF CYBER ESPIONAGE MALWARE

by Monnappa KA

The number of cyber espionage attacks(APT) is undoubtedly on the rise targeting government, military, corporate, educational, and civil society networks today. These advanced and sophisticated attacks focus on individual organizations in an effort to extract valuable information. Sometimes, these advanced attacks are allegedly linked to state-sponsored activities but may also be carried out by individual groups with their own goals. The cyber espionage actors (APT attackers) use malicious software (malware) to infect their targets. reverse engineering is an effective method which helps in thoroughly dissecting and understanding the capabilities of such malicious software.

What you will learn...

- Performing reverse engineering
- Techniques used by the cyber espionage actors
- Understanding the encrypted communication of malware
- Decrypting the communication of malware

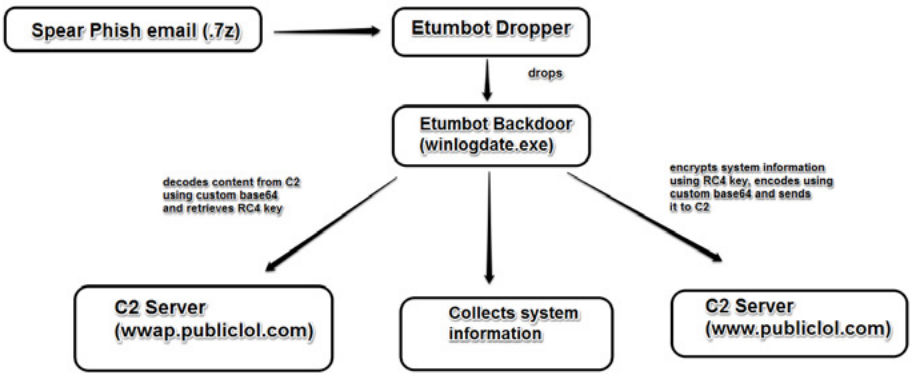
What you should know...

- Basic understanding of malware
- Knowledge of operating system processes
- Understanding of Windows Internals
- Understanding of Windows API

In this article, we will look at a cyber espionage campaign where a malware called “Etumbot” was used to target the victims and we will see how reverse engineering this malware can help in understanding the techniques used by the espionage actors, its encrypted communication and finally we will also see how to decrypt the communication of malware using a python script.

ETUMBOT CYBER ESPIONAGE CAMPAIGN

Etumbot backdoor was used in targeted attacks against technology, media and government organizations. This backdoor was delivered to targets via spear phishing emails as an archive file (.7z or .rar), extracting the archive contains a malware file which posed as an office document file (.doc or .xls). Upon execution this backdoor retrieves the encryption key from the C2 (command and control) server and then encrypts and sends the collected system information using the retrieved encryption key to the C2 server.



Fifure 1.

SANDBOX ANALYSIS OF ETUMBOT DROPPER(5340.EXE)

A) FILE SYSTEM AND PROCESS ACTIVITY

To understand the capabilities of the malware, the malware was run in the sandbox. Upon execution the malware drops a file “winlogdate.exe” (which is Etumbot backdoor). After creating these files, malware creates a process from the created file “winlogdate.exe”. The file and process activities are shown below:

```
=====================[DYNAMIC ANALYSIS RESULTS]=====================

FILE, REGISTRY AND PROCESS ACTIVITIES
==================================
"9/6/2014 15:33:5.281","registry","SetValueKey","C:\WINDOWS\system32\lsass.exe","HKLM\SAM\SAM\Domains\Account\Users\000001F4\F"
"9/6/2014 15:33:5.484","process","created","C:\Program Files\VMware\VMware Tools\VMwareUser.exe","C:\malware_analysis\5340.exe"
"9/6/2014 15:33:15.94","process","created","C:\malware_analysis\5340.exe","C:\Documents and Settings\Administrator\Application Data\Microsoft\winlogdate.exe"
"9/6/2014 15:33:15.78","file","Write","C:\malware_analysis\5340.exe","C:\Documents and Settings\Administrator\Application Data\Microsoft\winlogdate.exe"
"9/6/2014 15:33:15.78","file","Delete","C:\malware_analysis\5340.exe","C:\Documents and Settings\Administrator\ka4a8213.log"
"9/6/2014 15:33:15.94","file","Write","C:\malware_analysis\5340.exe","C:\Documents and Settings\Administrator\Local Settings\Temp\kb71271.log"
"9/6/2014 15:33:15.172","process","created","C:\malware_analysis\5340.exe","C:\WINDOWS\regedit.exe"
"9/6/2014 15:33:15.250","registry","SetValueKey","C:\Documents and Settings\Administrator\Application Data\Microsoft\winlogdate.exe","HKCU\Software\Microsoft\Wind
"9/6/2014 15:33:15.250","registry","SetValueKey","C:\Documents and Settings\Administrator\Application Data\Microsoft\winlogdate.exe","HKCU\Software\Microsoft\Wind
"9/6/2014 15:33:15.250","registry","SetValueKey","C:\Documents and Settings\Administrator\Application Data\Microsoft\winlogdate.exe","HKCU\Software\Microsoft\Wind
"9/6/2014 15:33:15.344","registry","SetValueKey","C:\WINDOWS\regedit.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Update"
```

Figure 2.

B) REGISTRY ACTIVITY

The malware persists (survives reboot) by creating a run registry key and adding the dropped file (winlogdate.exe) as the value (as shown below)

```
REGISTRY ACTIVITY
==============================

"registry","SetValueKey","C:\WINDOWS\regedit.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Update"   <- Creates a registry key

Registry: \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
Key name: Run (S)
Last updated: 2014-06-09 07:26:10 UTC+0000

Subkeys:

Values:
REG_SZ        ZoomIt          : (S) C:\softwares\ZoomIt\ZoomIt.exe
REG_SZ        ctfmon.exe      : (S) C:\WINDOWS\system32\ctfmon.exe
REG_SZ        Update          : (S) C:\Documents and Settings\Administrator\Application Data\Microsoft\winlogdate.exe

Creates a registry value to survive the reboot
```

Figure 3.

C) NETWORK ACTIVITY

Upon executing the malware makes a dns query to the C2 domain (wwap.publiclol.com) as shown below

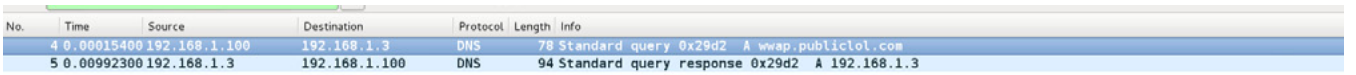


Figure 4.

after resolving the domain name, the malware makes two C2 communications In the first communication pattern the malware receives response from the C2 server. The response looks like an encoded string as shown below.

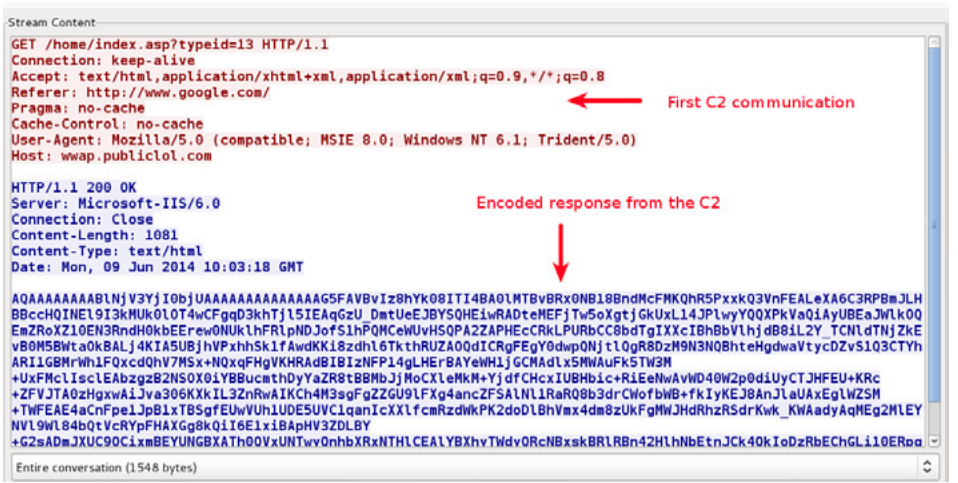


Figure 5.

In the second communication pattern the malware sends a request, which looks like a request to download an image file (.jpg), but the string before .jpg looks like an encrypted string. In order understand these communication patterns, lets reverse engineer the Etumbot backdoor. Below screenshot shows the second encrypted C2 callback.

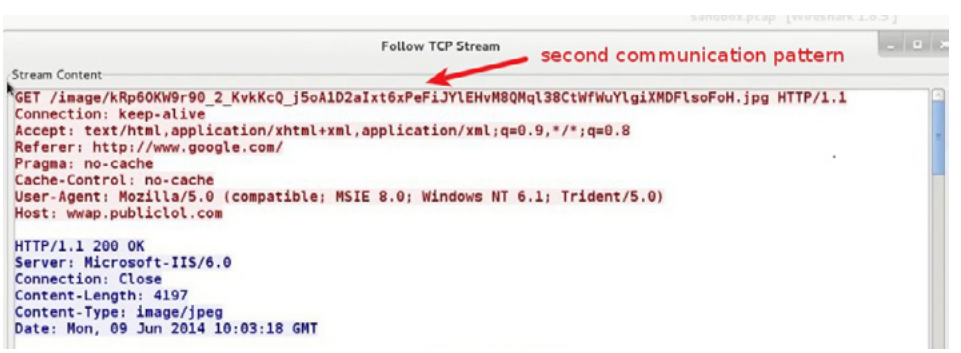


Figure 6.

REVERSE ENGINEERING THE COMMUNICATIONS OF ETUMBOT BACKDOOR (WINLOGDATE.EXE)

Sandbox analysis helped in determining the file system, process, registry and network activity but it does not answer questions like how the malware is using the encoded response from the first C2 communication and what is that encrypted string before the .jpg in the second C2 communication. Reverse Engineering the etumbot backdoor can help us answer the above question.

A) REVERSING THE FIRST C2 COMMUNICATION

Etumbot Backdoor calls the below function. This function implements the First Communication pattern, this function is interesting because this function in turn calls multiple http related API's (HttpOpenRequest, HttpSendRequest, InternetConnect, InternetOpen) as shown in the call graph below. Inspecting this function will help us understand the malware communication.

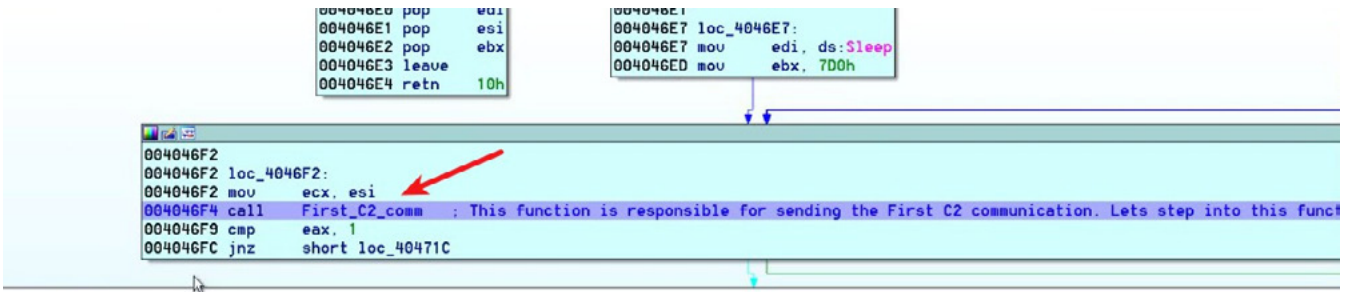


Figure 7.

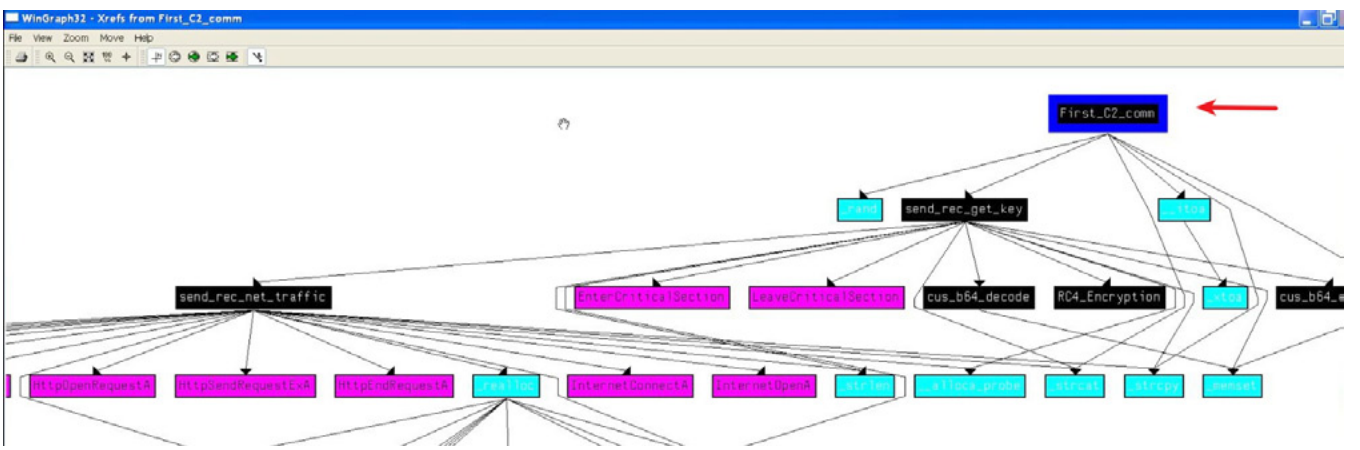


Figure 8.

After stepping into the function(Fist_C2_comm), malware calls an API "InternetConnectA" and passes the string " wwap.publiclol.com" as one of its parameter . This shows that malware uses the below API call to open an http session with the C2 Server (wwap.publiclol.com) as shown in the below screenshot.

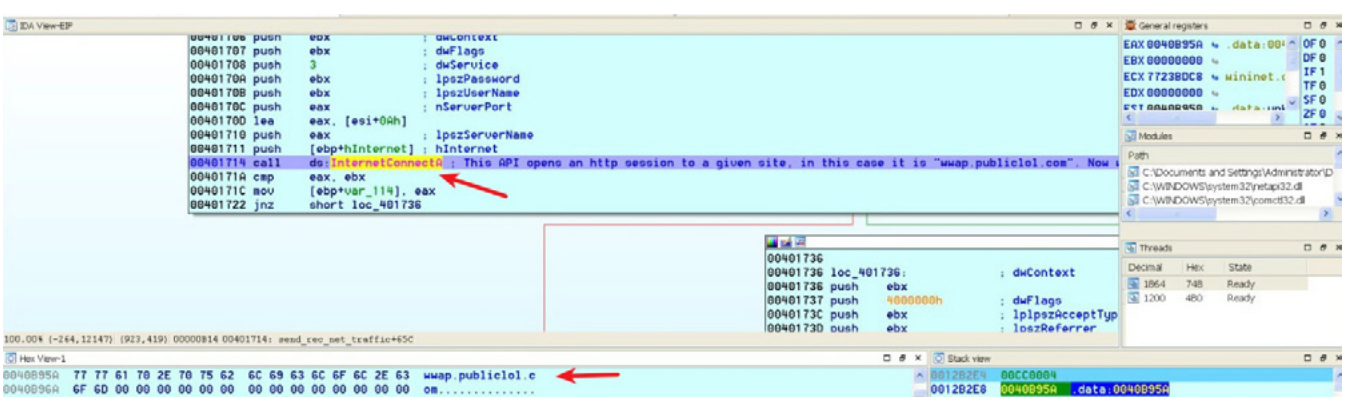


Figure 9.

Etumbot backdoor then calls the API HttpOpenRequestA as shown in the below screenshot with one of the parameter as /home/index.asp?typid=13. This shows that malware is going to establish an http connection requesting for the that object.

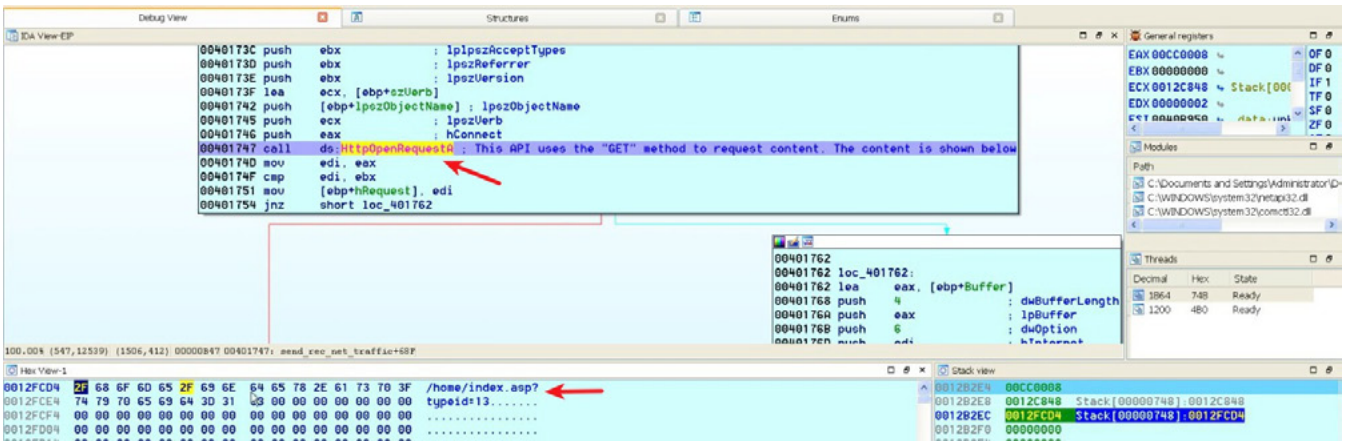


Figure 10.

Etumbot Backdoor uses the API HttpSendRequest to send the request to the C2 server and then receives an encoded response from the C2 server as shown in the below screenshots.

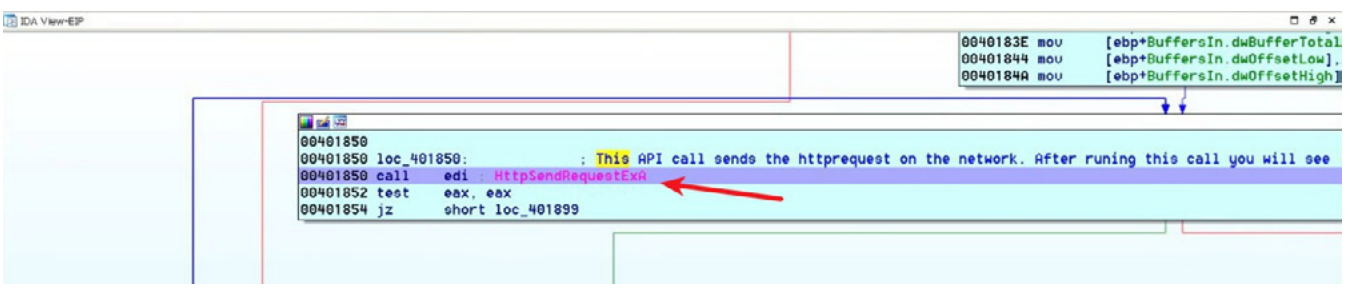


Figure 11.

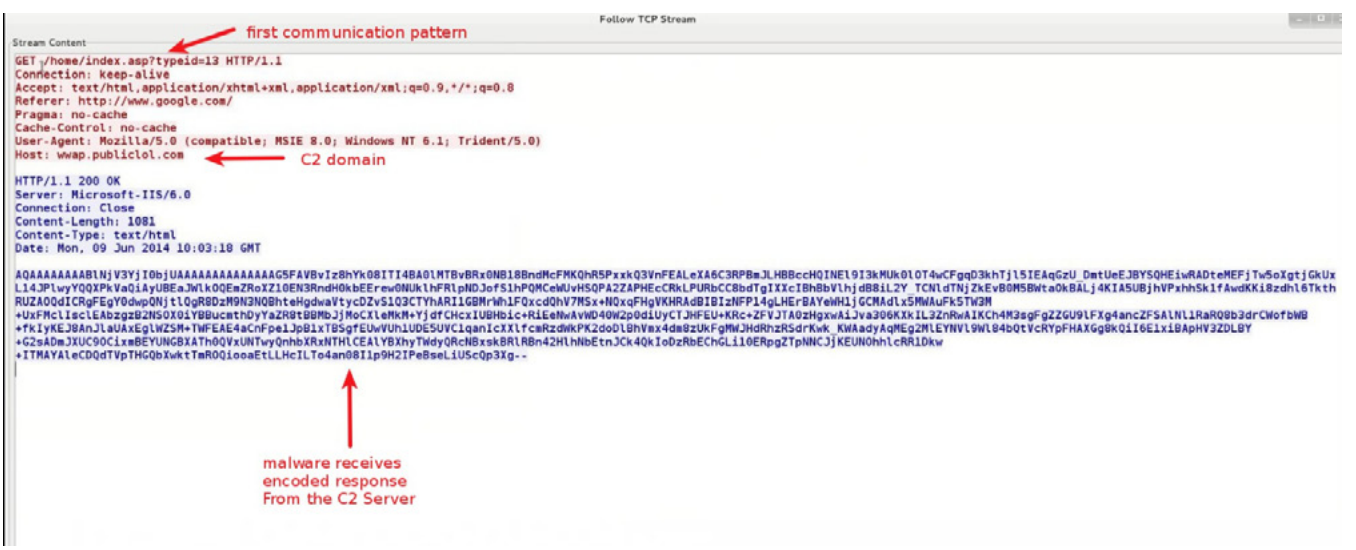


Figure 12.

Etumbot backdoor receives the encoded response from the C2 using the API InternetReadFile as shown in the below screenshot.

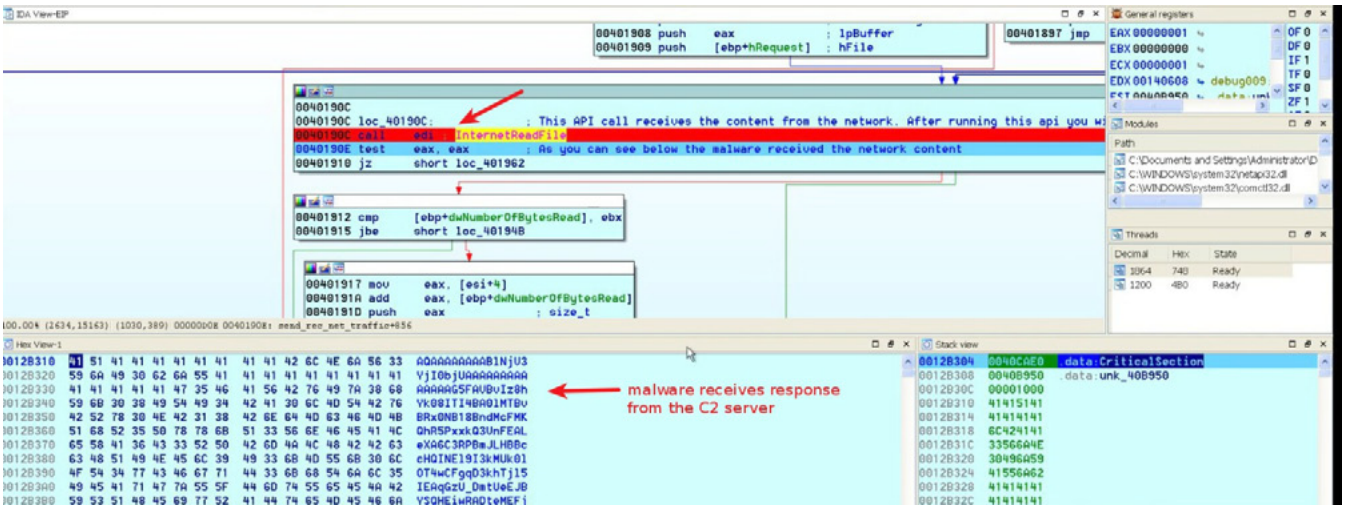


Figure 13.

Etumbot backdoor passes the received content from the C2 to the custom base64 algorithm which decodes the received content and extracts the RC4 key starting at offset 8 as shown in the below screenshot. This RC4 key is used to encrypt subsequent communications. From this it can be deduced that the first C2 communication pattern is used by the malware to receive the RC4 key from the attackers

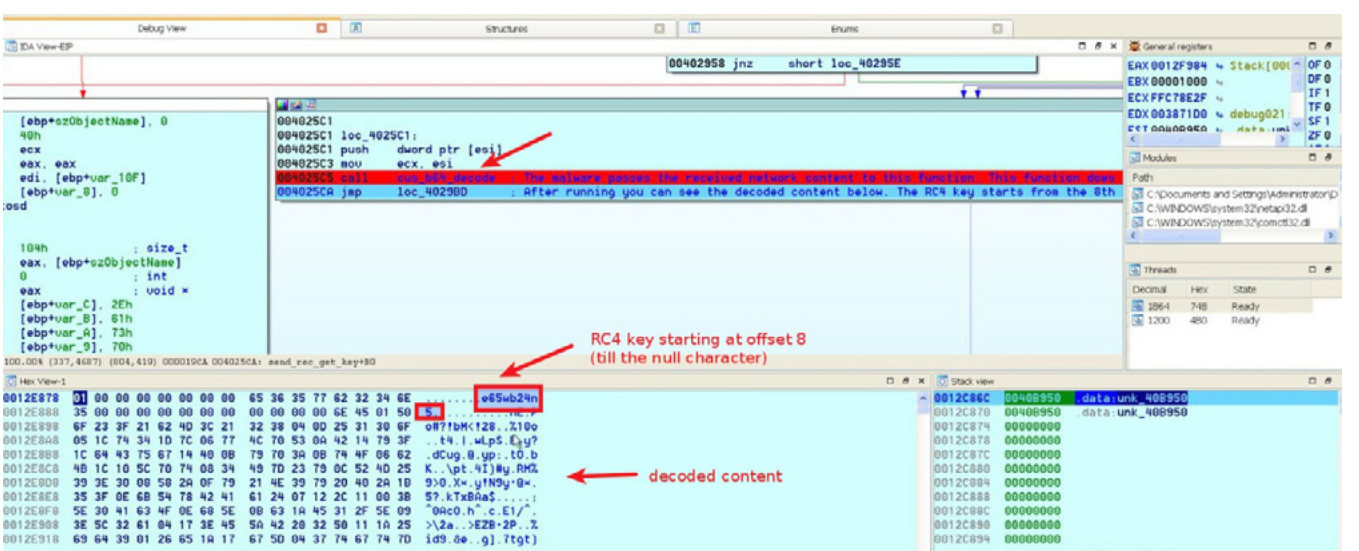


Figure 14.

Now we know that malware uses the first c2 communication to receive the content from the C2 server, decode it and extracts the RC4 key.

B) REVERSING THE SECOND C2 COMMUNICATION

Once the malware decodes the RC4 key from the first C2 communication, it then calls the below function (renamed as Second_c2_comm). This function implements the Second Communication pattern, this function calls multiple http functions as shown in the call graph below

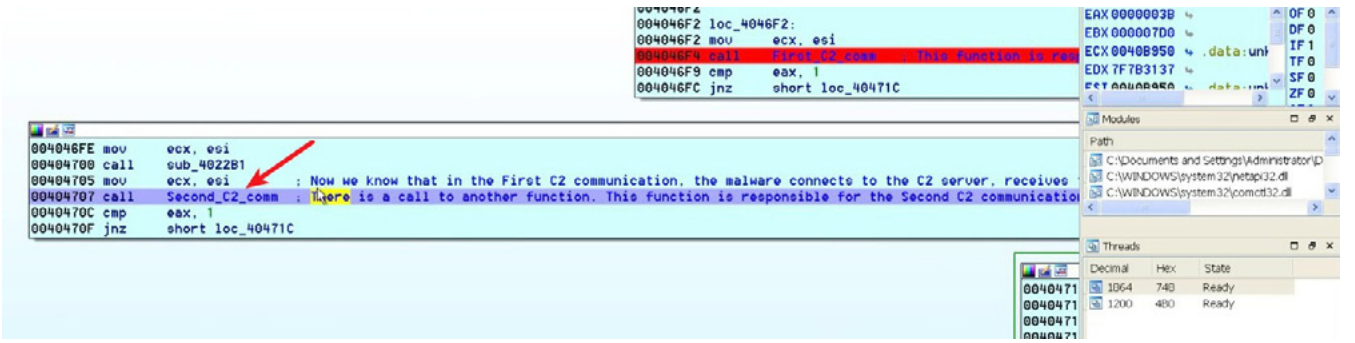


Figure 15.

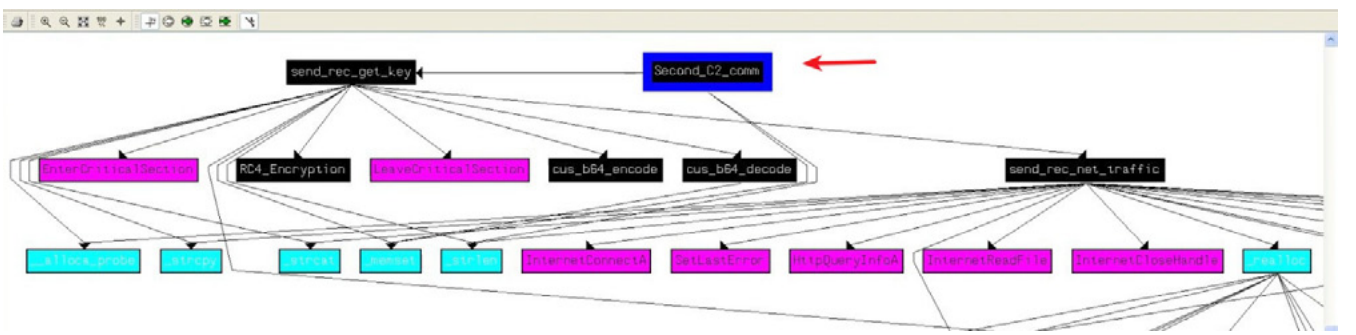


Figure 16.

Etumbot Backdoor collects the system information (hostname, username, ip and proxy details) and passes it to the RC4 function (with the RC4 key retrieved from the first communication).

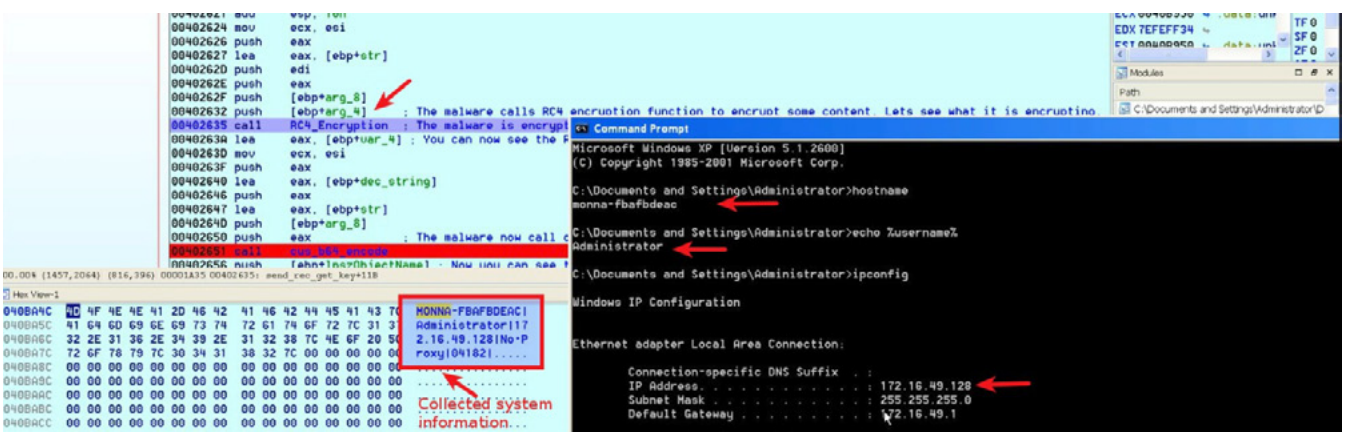


Figure 17.

The collected system information is then encrypted with RC4 key which was retrieved from the first communication. Below screenshot shows the RC4 encrypted system information. This shows that malware uses the RC4 key retrieved from the first communication to encrypt the collected system information

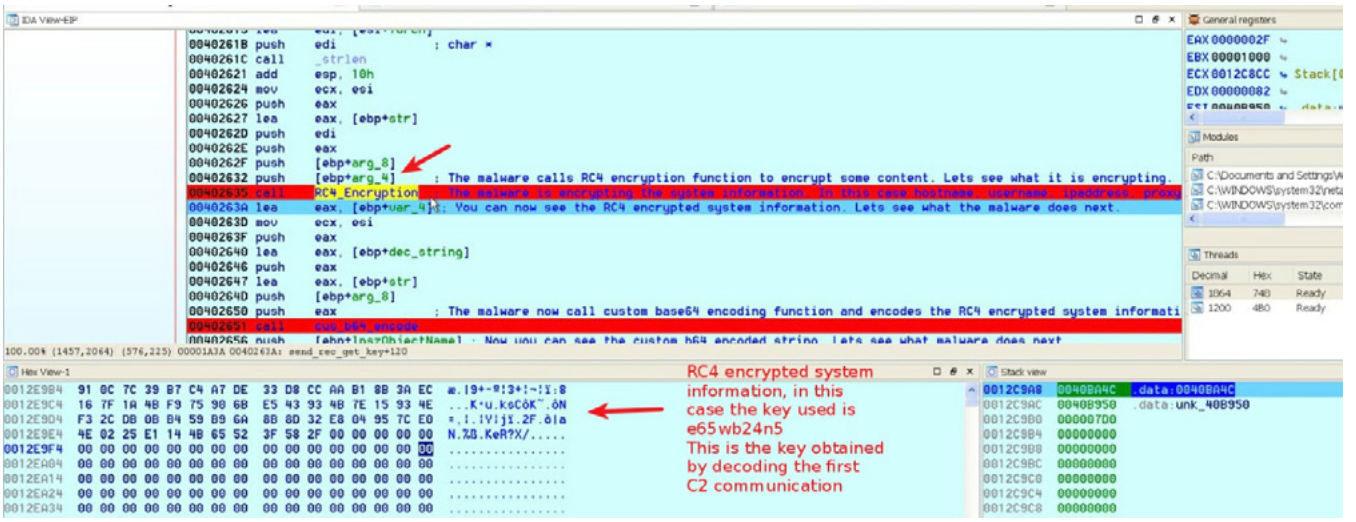


Figure 18.

The RC4 encrypted system information is then passed to the custom base64 encoding function as shown below

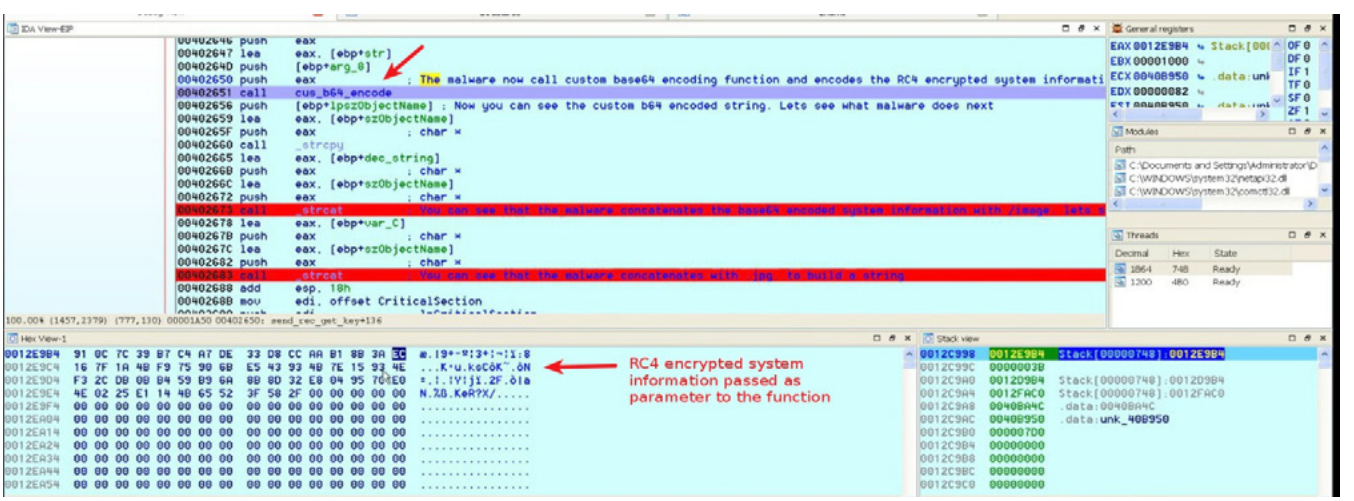


Figure 19.

The RC4 encrypted system information is then encoded with custom base64 encoding algorithm as shown below.

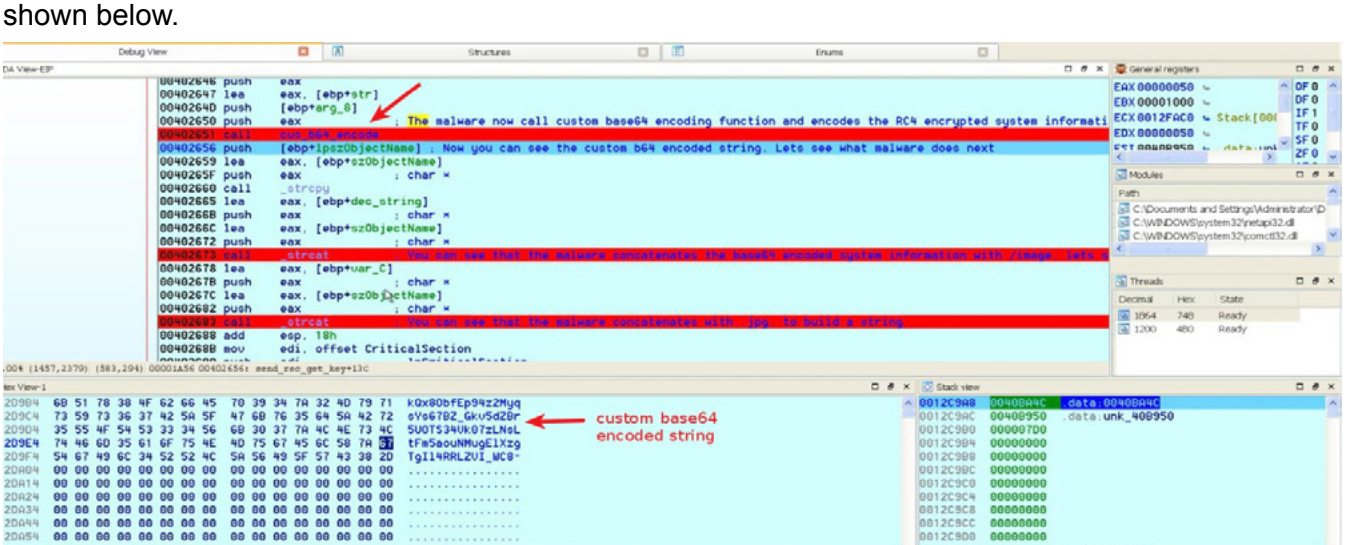


Figure 20.

The base64 encoded string is then passed to strcat function which concatenates it with /image/ and .jpg to form a final string as shown in the below screenshots.

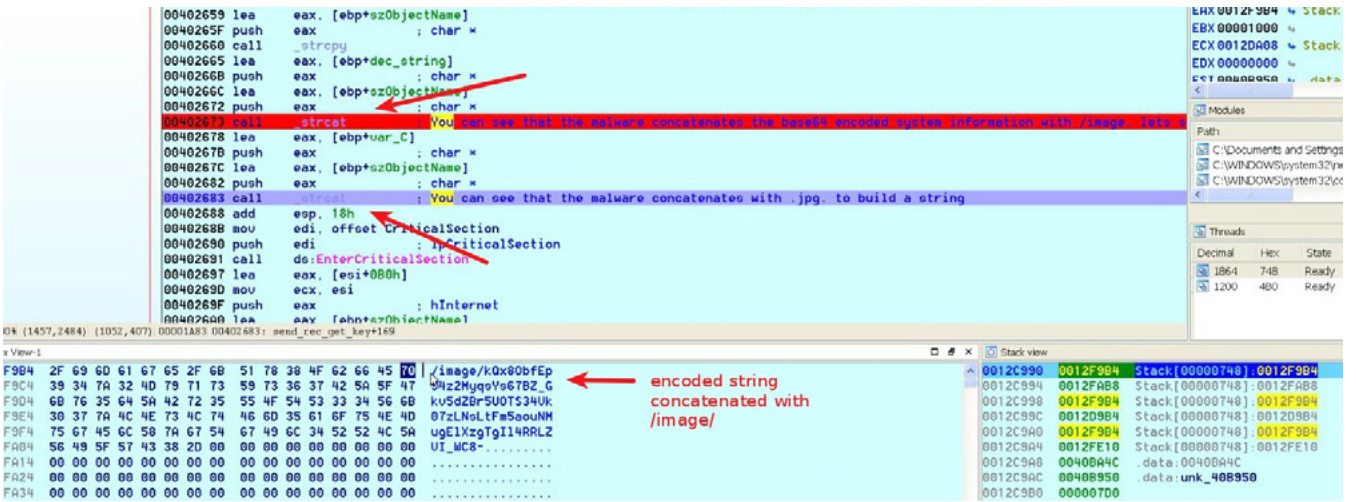


Figure 21.

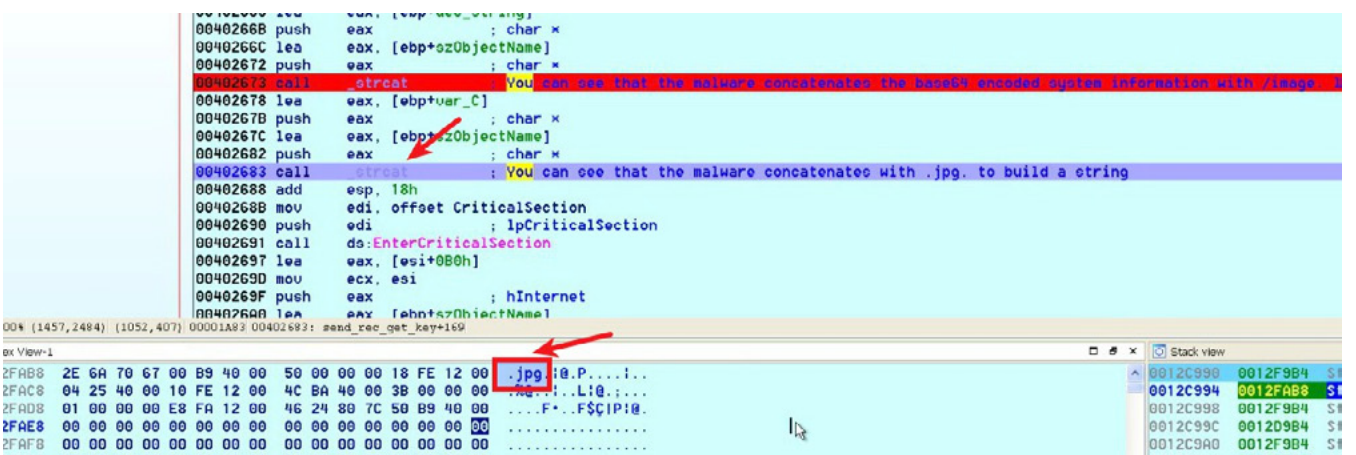


Figure 22.

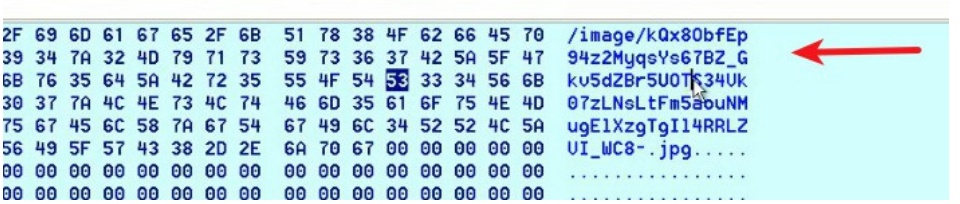


Figure 23.

The malware then connects to the C2 server (*wwap.publiclol.com*) using the concatenated string as the http request pattern as shown in the below screenshots.

Figure 24.

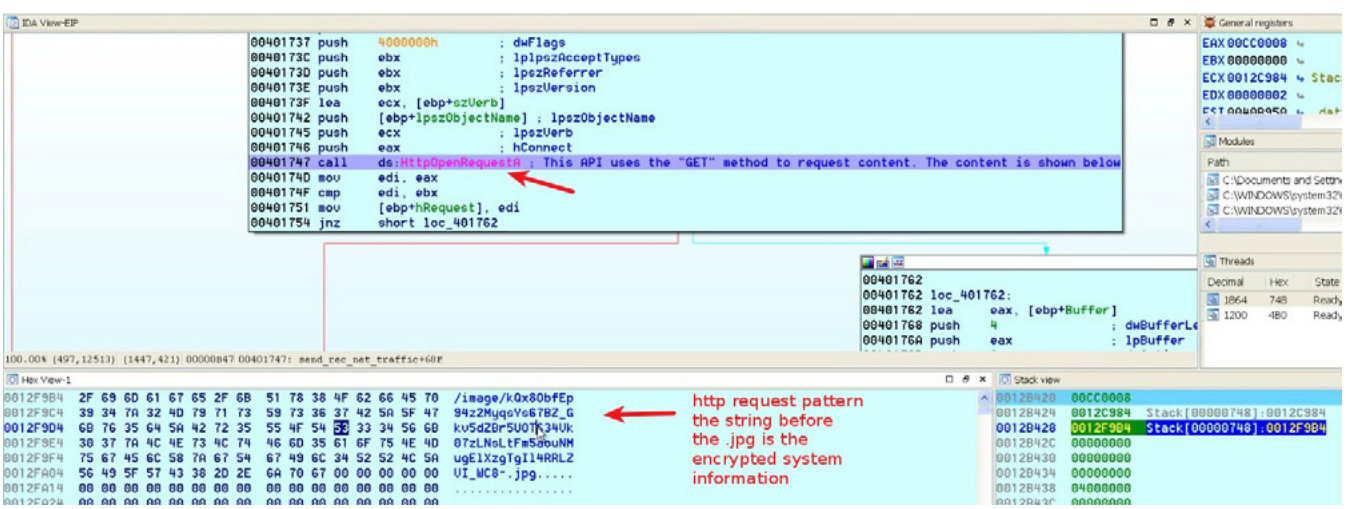


Figure 25.

Malware sends the http request as shown in the below screenshots. As you can see from packet capture the encrypted system information (content after /image and before .jpg is the encrypted system information) is sent to the attackers this way. Now we know how malware decodes the RC4 key from first communication and uses this RC4 key to encrypt subsequent communications. Now We can write decryptors to extract the RC4 key and to decrypt the communications.

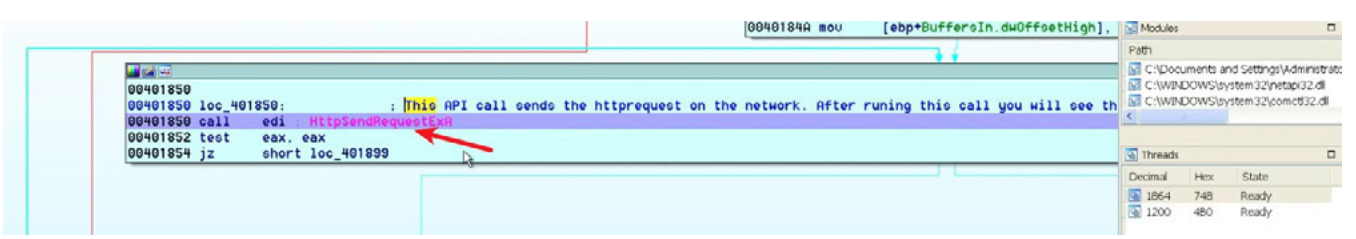


Figure 26.

Figure 27.

DECRYPTING THE COMMUNICATIONS OF ETUMBOT BACKDOOR (WINLOGDATE.EXE)

A) EXTRACTING THE RC4 KEY FROM FIRST C2 COMMUNICATION

In order to decrypt the malware communication, we need to know the key that was used to encrypt the traffic. The malware obtains the key by decoding the C2 response from the First C2 communication. This is an interesting trick which makes sure that the encryption key is retrieved only when the malware is allowed to connect to the C2, this is probably an attempt by the attackers to make sure the key is not obtained when run in an isolated (sandbox) environment. Below screenshot shows the C2 response from the First C2 communication.

Figure 28.

After reverse engineering the malware sample, we know that malware decodes this content and obtains the RC4 key. The RC4 key is located after the first 8 bytes of the decoded traffic and terminated by the null byte ("\x00"). In order to decode and extract the RC4 key, a simple script (get_key.py) was written, which takes the C2 response as input, decodes it and extracts the RC4 key. The script is shown below.

```
'''
Created on Jun 09, 2014
@author: Monnappa

This script takes the response from the C2, decodes and extracts the RC4 key, which is later used by the malware to send encrypted system
information to the attackers.
'''
import sys
import base64

class Malware():

    def get_decoded_content(self, c2_resp):
        c2_resp = c2_resp.replace('_','/').replace('-','=')
        decoded = base64.b64decode(c2_resp)
        return decoded

    def get_key_from_c2_response(self, c2_resp):
        dec_c2_resp = self.get_decoded_content(c2_resp)
        content = dec_c2_resp[8:]
        index = content.find("\x00")
        rc4_key = content[:index]
        return rc4_key

if __name__ == "__main__":

    c2_response = sys.argv[1]
    mal = Malware()
    rc4_key = mal.get_key_from_c2_response(c2_response)
    print "\n"
    print "OUTPUT:"
    print "=============================="
    print "Extracted RC4 Key from C2 response: %s" % rc4_key
```

Figure 29.

after running the script, the RC4 key was extracted as shown below. As you can see the RC4 key extracted matches with the RC4 key determined using reverse engineering.

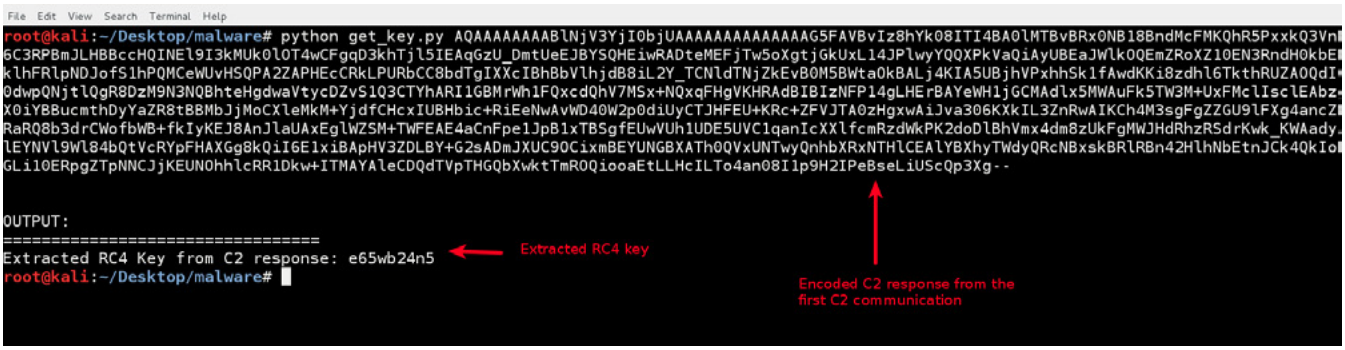


Figure 30.

B) DECRYPTING THE SECOND C2 COMMUNICATION

Now that we have obtained the RC4 key. we can decrypt the second C2 communication. Even though the second C2 communication looks like a request to download a image file but the content before the (.jpg) is the encrypted system information sent to the attacker. The second C2 communication is shown below.

Figure 31.

In order to decrypt the encrypted traffic, a script was written (decrypt_communication.py) which take the encrypted string as input and decrypts using the RC4 key. The script is shown below

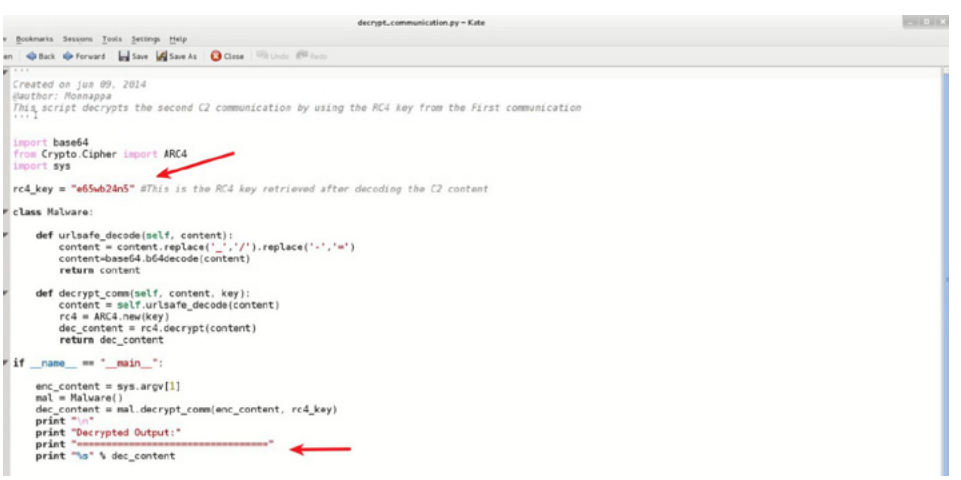


Figure 32.

After running the script you can see the encrypted string was decrypted, this is the system information that was sent to the attacker (as shown in the below screenshot).

In this case hostname, username, ip address and proxy details were sent to the attacker.

MYHOTSNAME --> is the hostname of the infected machine (in this case hostname of my sandbox)

Administrator --> is the username

192.168.1.100 ---> ip address of the infected machine (In this case ip address of sandbox)

No Proxy --> proxy settings.

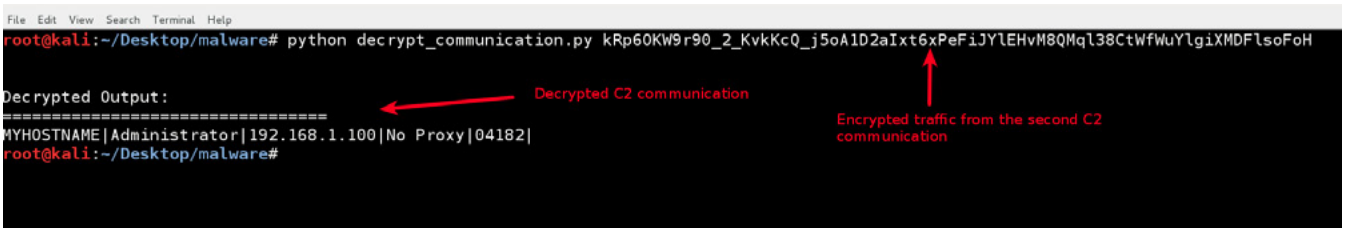


Figure 33.

The below screenshot shows the hostname, username and ip address of the sandbox machine where the sample was execute. This confirms the information that was sent to the attacker.

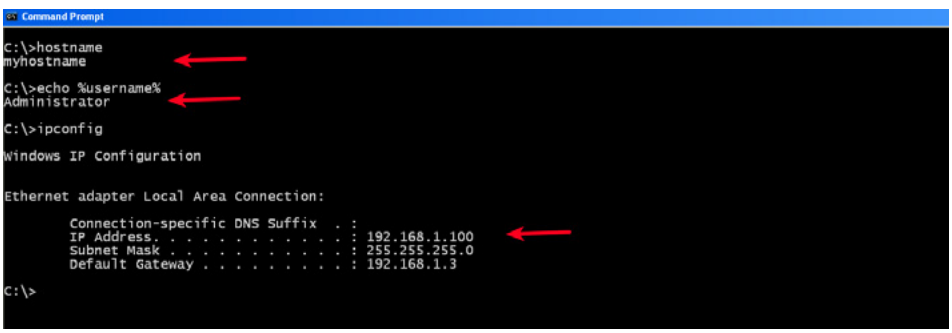


Figure 34.

CONCLUSION

Reverse Engineering is a powerful and effective technique which helps in dissecting and understanding the capabilities of the malware. In this using reverse engineering we were able to understand encrypted communication patterns of etumbot backdoor, we were able to extract RC4 key and decrypt the subsequent communications of the etumbot malware.

REFERENCES

a) Video links of this article:

- *https://www.youtube.com/watch?v=Bwgl0xOqEjk*
- *https://www.youtube.com/watch?v=x8ViLZ3eBj8*
- *https://www.youtube.com/watch?v=XL8G-XBCBG0*

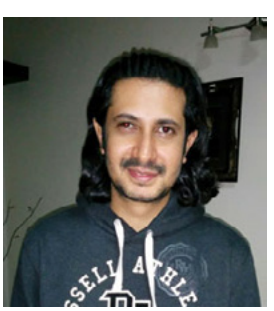
b) ARBOR Networks Report on Etumbot

- *http://www.arbornetworks.com/asert/2014/06/illuminating-the-etumbot-apt-backdoor/*

c) FireEye's Blog post

- *http://www.fireeye.com/blog/technical/botnet-activities-research/2014/09/darwins-favorite-apt-group-2.html*

MONNAPPA KA



Monnappa KA is based out of Bangalore, India. He works with Cisco Systems focusing on threat intelligence and investigation of advanced cyber attacks. His fields of interest include malware analysis, reverse engineering, memory forensics and threat intelligence.As an active speaker in security conferences like Nullcon and at SecurityXploded (cyber security) meetings, he has presented on various topics which include memory forensics, malware analysis, rootkit analysis and reverse engineering. He has also authored various articles on these topics in Hakin9, eForensics and Hack Insight magazines.

STEGANALYSIS: EXPLORING THE VIRTUAL STEGANOGRAPHIC LABORATORY

PART 1: THE LSB-STEGANALYSIS

by Cordny Nederkoorn

Steganography is the art of obfuscation, hiding information in plain sight, while Steganalysis is the art of finding this hidden information. For computer forensics professionals, steganalysis is becoming a daily job. Different tools are available for steganalysis, with The Virtual Steganographic Laboratory being one of these tools. This article is the first of a series where different functions of VSL will be tested and discussed.

What you will learn...

- Basic understanding of steganalysis
- Differences between steganalysis and steganography
- Use of the Virtual Steganographic Laboratory for steganology
- Least Significant Bit (LSB) method

What you should know...

- Basic understanding steganography
- Basic use of GUI based tools
- Basic understanding of dragging and dropping files in a Windows-environment

Steganography [1] is the art of obfuscation, hiding information in plain sight. When steganography is used for criminal activities forensic analysts are called in to find the hidden information, which then can be used as evidence in a criminal court.

Steganalysis [2] is the process of finding this hidden information.

Steganography and steganalysis together is called steganology.

Eforensics Magazine has discussed different steganography and steganalysis techniques in the past. [3]

The tools discussed were very technical in nature and some difficult to use.

The Virtual Steganographic Laboratory (VSL) [4] is an application for steganology, which can be used as a GUI, without having to do manual statistical calculations yourself.

It is a graphical block diagramming tool that allows complex using, testing and adjusting of methods both for image steganography and steganalysis.

This can be done by built-in modules which enable different steganology techniques and visualizations.

This article is the start of a series which will describe the VSL and its different functions.

We will start with how the VSL can be useful for LSB (Least Significant Bit) steganalysis.

OBJECT TO TEST

As stated earlier, VSL is a graphical block diagramming tool.

It was developed in 2008 by Michal Wegrzyn and Pawel Forczmanski from the West Pomeranian University of Technology in Szczecin, Poland. The current version is 1.1.

It can be freely downloaded via sourceforge.net [5].

The goal of the application is hiding data in digital applications, detecting its presence and testing its robustness using a number of steganalysis techniques.

Processing can be done in parallel or by batch.

The VSL modules can be used for different goals:

1. Data can be hidden with basic Least Significant Bit (LSB) method, with more advanced Karhunen-Loeve Transform (KLT) technique or by F5 algorithm, which uses DCT transformation in JPEG files.
2. For steganalysis two advanced techniques can be used. First, RS-Analysis: efficient steganalysis for LSB methods – and the second one – Binary Similarity Measures (BSM) method with Support Vector Machines (SVMs) classifier: blind steganalysis (universal) technique, which can be used to detect any kind of steganography.
3. VSL contains also many other modules like several distortion techniques, which can be used to test resistance of steganographic techniques. The VSL has build-in modules, which helps with research, reports, file handling, image analysis etc.

In this article it will be shown through an experiment VSL can be used to hide information in an image using the Least Significant Bit (LSB) Insertion Method [6] (steganography) and also can be used to expose the hidden information (steganalysis).

THE EXPERIMENT

Prerequisites:

- VSL tool (downloaded from *sourceforge.net*)
- An image-file, large enough to hide information, unseen by the human eye
- A text document

Steps:

- Open VSL.
- A VSL Desktop appears showing a pane with a modules list, a menu bar and a Status bar.

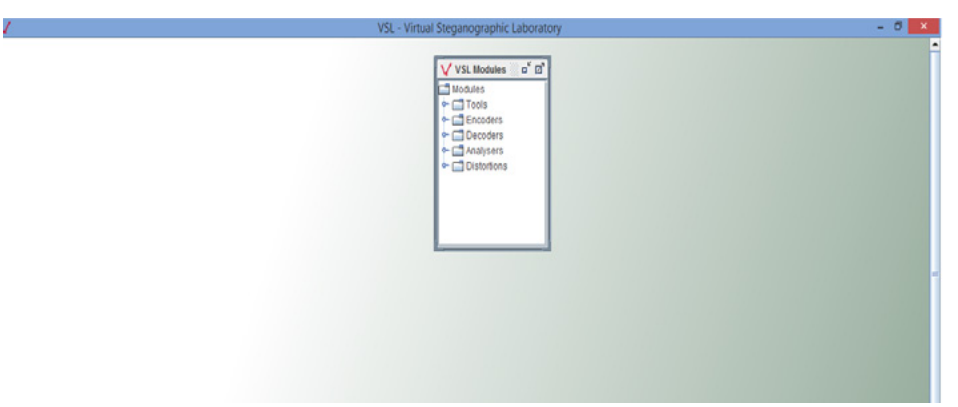


Figure 1. The VSL Desktop

First we have to give VSL the input for steganography.

Open Tools from the open modules list on the screen.

From the module Tools drag and drop the following 2 submodules on the VSL Desktop: Input, Output. The VSL Desktop will show 2 extra blocks now: Input, Output

Open in the module List the Module Encoders.

From the module Encoders drag and drop the following submodule on the VSL Desktop: LSB.E The VSL Desktop will show 1 extra block now: LSB.E.

The blocks can be connected by arrows: Right-click on a block and choose Connect;

Drag the arrow to the block to be connected.

Now we have the flow visible for steganography.

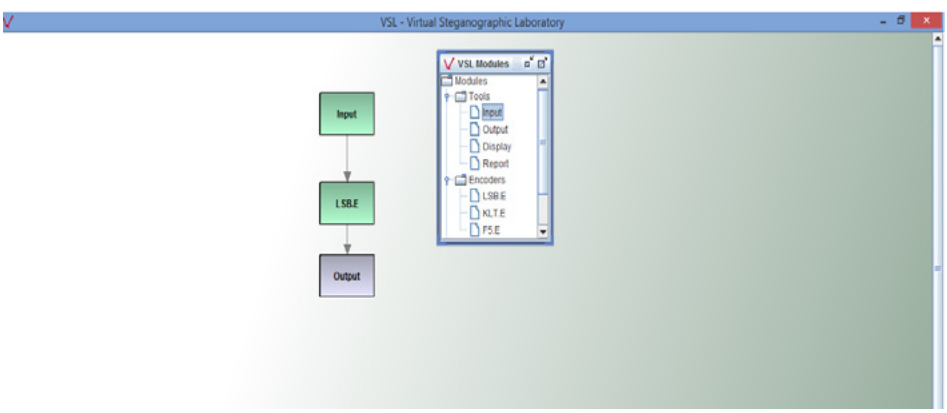


Figure 2. The steganography flow in the VSL

The Input block has to contain the image to be steganographed:

Right-click the Input Block and choose Select Input.

A popup appears. By using the + and – Button an image can be added or removed.

For this experiment an image of a crow is used as seen in Figure 3.

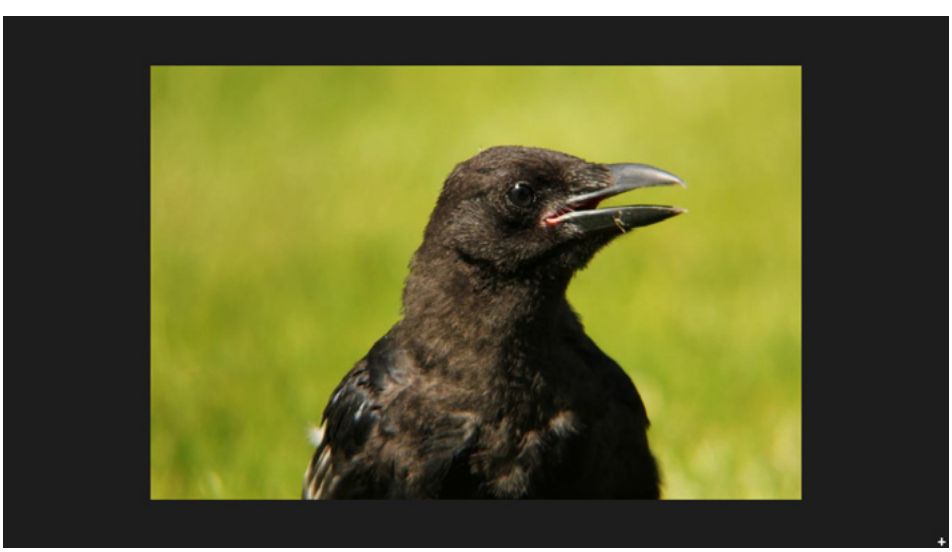


Figure 3. The image of a crow as used in this experiment

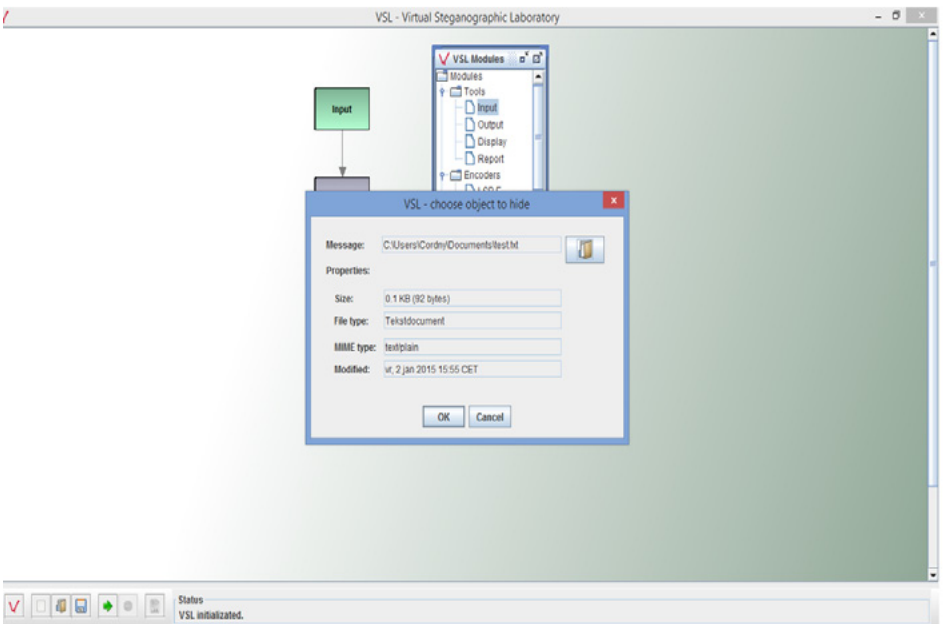


Figure 4. Popup VSL – choose object to hide

Now we have to add a hidden file to the Crow image file

Right-click the LSB.E block and choose Message …

The popup VSL – Choose object to hide appears.

Insert an object via the Ins.-button.

For this experiment a text-file was used, which was uploaded to the program as seen in Figure 4 and 5.

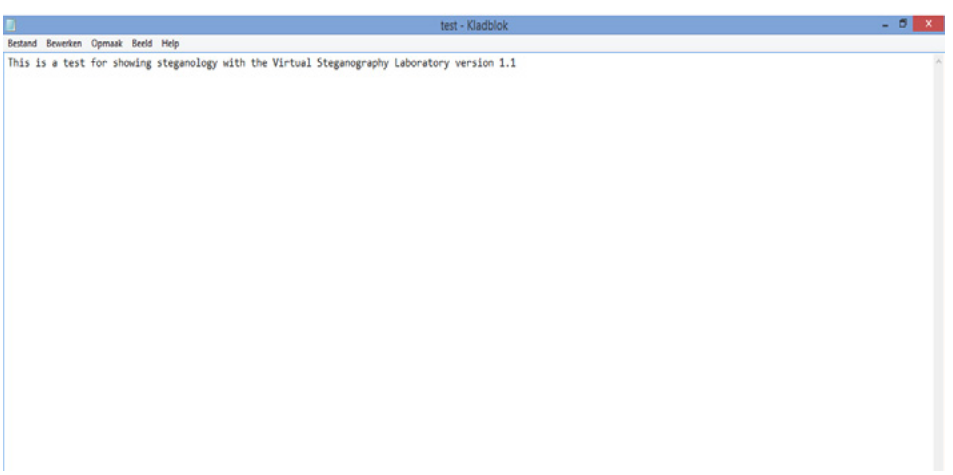


Figure 5. The test-file used

We are not ready yet. As with every experiment the results have to be shown.

Right-click the block Output and choose Select output.

The popup VSL – Choose output folder appears where an output folder and its format (!!) can be selected. For this we use the png-format.

Now the experiment can start.

Click the arrow-button or CTRL-ENTER.

The status will change from *VSL initializated* to *Starting experiment*.

When the experiment is finished the status will say so.

The results of the experiment can be found in the Results folder we selected.

Here we find the image of the crow we selected as input for this experiment,but is it the same file?

Let's find out.

To do this we have to change some Blocks.

For the block Input:

Substitute the image of the crow for the file resulting for this experiment as found in the Results folder

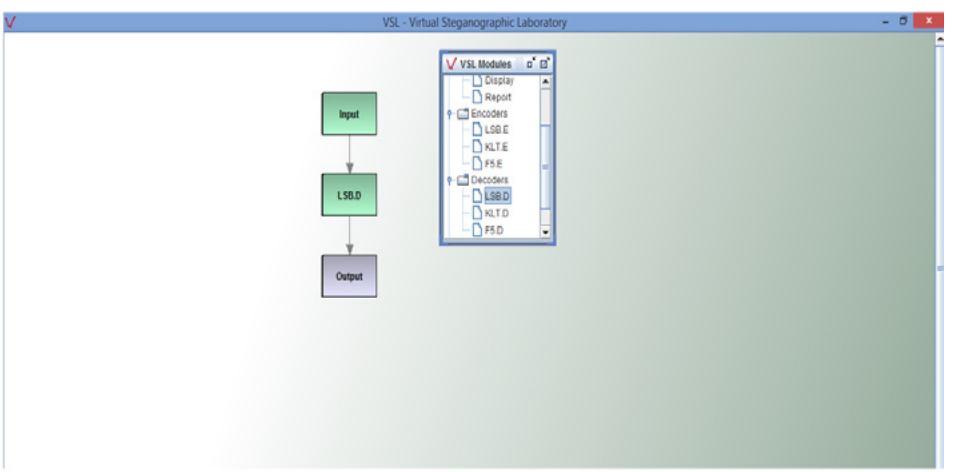


Figure 6. The VSL-flow for steganalysis

For the block LSB.E:

Substitute this block with the submodule LSB.D found in the VSL Module Decoders

You will have to reconnect the blocks again as you did in the previous experiment.

Now run the experiment again by clicking the arrow button or CTRL-ENTER.

Go to the Results folder and open the results of this experiment.

The file shows the text document which you had hidden in the image-file of the crow.

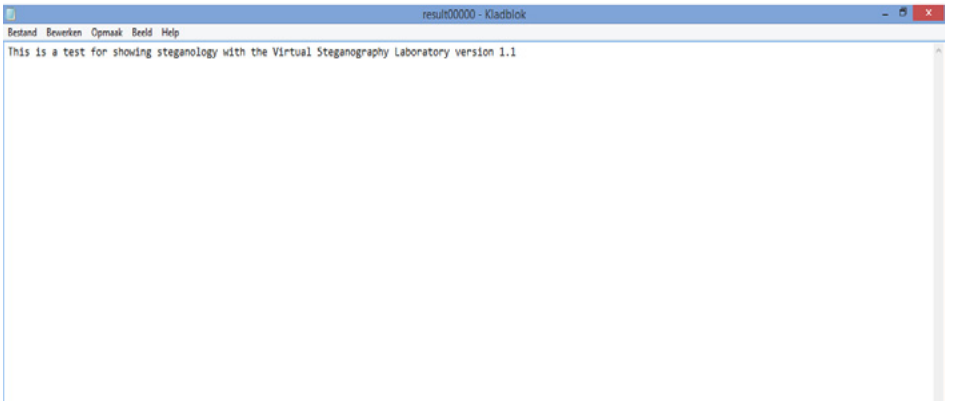


Figure 7. The hidden file as found by steganalysis via the VSL

This ends our LSB-experiment with VSL where both steganography and steganalysis are showed via an easy to use GUI.

CONCLUSION

As we saw in the above experiments, VSL is a steganology application that can both be used for steganography and steganalysis. We also saw that VSL is easy to use: by just dragging and dropping you can easily make steganology flows, without having to know the technical details behind the steganology.

For this experiment the Least Significant Bit insertion method was used, which is used frequently in steganology.

Steganology is an exciting, dynamic forensics field, where forensics, statistics and knowledge of image files is required to get the correct results

As already stated, this article is the first in a series. The future articles will cover more steganology techniques.

NOTES

As with every tool, a fool with a tool is just a fool.

Before using the VSL application you should know the basics of steganology and in particular the techniques you are going to use.

If not, experiments can go wrong by noncorrect experimental steps or may result in misinterpretations. Steganology methods are mostly build on statistics and this requires lots of practice. Also, when possible; always run an experiment twice, the software being used can have a bug that may result in wrong or misinterpretions by the forensic analysis.

BIBLIOGRAPHY

- http://en.wikipedia.org/wiki/steganography
- http://en.wikipedia.org/steganalysis
- Eforensics Magazine: Investigating Steganography in Social Networks: a "How-To for the Average Joe (Tanner AL, 2014); Steganography: the Art of hidden Data in plain Sight (Lopez P., 2014); The Interview with James E. Wingate Vice President of Backbone Security (Biondo G.; Kishore P.V., 2014).
- Information Systems Architecture and Technology: Information Systems and Computer Communication Networks Virtual Steganographic Laboratory for Digital Images (Forczmański, P., Węgrzyn M. Wrocław, Polska, 2008), pp. 163–174.
- http://sourceforge.net/projects/vsl/files/vsl/vsl-1.1/vsl-1.1.zip/download
- http://www.garykessler.net/library/steganography.html (good description on the LSB Insertion method)

CORDNY NEDERKOORN

Cordny Nederkoorn is an experienced software tester with a special interest in computer forensics and security. He founded the social network TestingSaaS where he discusses his thoughts on computer forensics, SaaS, security, electronic payments and online identity and privacy. http//testingsaas.blogspot.com | http://twitter.com/testingsaas | http://facebook.com/testingsaas.

NEW STRATEGIES FOR SECURE, COMPLIANT PAYMENT SYSTEMS IN THE CLOUD

by Randal Asay, Chief Technology Officer, Catbird

Gartner research shows that virtualization has surpassed 50 percent of all server workloads and predicts it will reach 86 percent in 2016. Virtualization offers flexibility, scalability and cost savings to organizations across all industries, so it's only logical that financial institutions would want to capitalize on these business benefits as well. In increasing numbers, these institutions are migrating their payment systems to private clouds.

As with the adoption of all new technologies, migration to the cloud poses its challenges. One of them is the realization that the perimeter security employed by traditional networks cannot, on its own, secure cardholder data. Another challenge is enforcing and documenting compliance for the many security regulations that the financial industry requires. A multifaceted approach to security is required for the cloud.

VIRTUALIZATION'S EFFICIENCY AND COST SAVINGS

Virtualization is the process of creating virtual versions of servers, personal computers, network adapters, switches and routers and more with the use of software. This results in virtual machines (VMs) that each run on a single high-powered server and have their own distinct operating system and application. A hypervisor is another software component, acting like a traffic cop to oversee the computing resources for each VM.

VMs have all of the respective functional benefits of physical hardware needed for IT operations but don't require the same infrastructure. It's common in a physical data center to allocate one or more servers to a single application. This procedure isolates applications, protecting them, but rendering them underused. These servers, of course, cost the same amount to maintain

and manage as their fully used counterparts. Therefore, organizations can typically save 40 percent or more on overall IT costs when they virtualize these physical assets. Likewise, companies can lower operational costs by using a private cloud that either resides within the organization's firewall or with a service provider like Rackspace or Amazon Web Services. As financial institutions search for ways to more efficiently process payments, data center consolidation projects will continue to rise.

THE CHALLENGE OF COMPLIANCE

By law, sensitive information such as cardholder data, personally identifiable information (PII), and other financial account data, must be protected by their respective financial institutions. Additionally, documentation is critical to provide evidence of control as prescribed by regulatory compliance frameworks, such as the Gramm-Leach-Billey Act (GBLA), the Sarbanes-Oxley (SOX) Act and Payment Card Industry Data Security Standard (PCI DSS).

The governing body of all merchants that accept credit cards, the PCI Security Standards Council, has put together PCI DSS Virtualization Guidelines and PCI DSS Cloud Computing Guidelines to help organizations understand the requirements for virtualized payment systems.

As mentioned above, the standard perimeter security used to protect the network simply cannot easily and comprehensively protect cardholder data, PII and other sensitive information inside the cloud. Asset management, policy enforcement, and data segmentation require tools that reside inside virtualized infrastructure. Software-defined solutions, especially those deployed at the hypervisor level, can provide effective zone-based security and contextual awareness when properly configured.

PCI DSS REQUIREMENTS FOR VIRTUALIZATION

To create a virtualized cardholder data environment (CDE) that is both secure and compliant, financial institutions must adhere to four significant requirements in PCI DSS Version 3.0:

- A new PCI DSS requirement reads: "Maintain an inventory of system components that are in scope for PCI DSS." Using an automated inventory discovery and management system will assist financial institutions in complying with this requirement due to the dynamic nature of virtual components.
- A PCI DSS sub-requirement and its test procedures were modified: "Current network diagram that identifies all connections between the cardholder data environment and other networks, including wireless networks." Using an automated network diagramming solutions will help provide complete, 24/7 visibility into security and compliance.
- For virtualized CDEs, a new PCI DSS sub-requirement was added: "Current diagram that shows all cardholder data flows in a dynamic virtual CDE will be nearly impossible without automation."
- All virtualization technology in the CDE is susceptible to a PCI DSS assessment. The following was added to PCI DSS under Network Segmentation for the purposes of an audit: "To be considered out of scope for PCI DSS, a system component must be properly isolated (segmented) from the CDE, such that even if the out-of-scope system component was compromised it could not impact the security of the CDE."

A MULTI-FACETED APPROACH

As cloud environments expand and VMs move, adapting physical tools becomes cumbersome and risky. Many organizations have attempted to adapt traditional physical security tools to protect their private clouds, with inadequate results. Financial institutions are already a prime target for breach attacks. In fact, a comprehensive assessment by Verizon suggests that 2013 was a transitional year from geopolitical attacks to large-scale attacks on payment card systems.

Compliance is only one component of the comprehensive security strategy critical to protecting customer data. Securing data based on classification needs to be sophisticated enough that assets have layers of security, ultimately protecting and securing the asset based on the attributes of that asset's workloads. Sensitive data needs to be encapsulated by its own unique security policy.

Technical tools that provide full visibility into the virtual environment need to be implemented. A properly configured asset discovery solution with network visualization can enable full analysis of traffic and ensure proper workload segmentation.

Internal network activity must be hidden from external attackers, and segmentation (or zoning) is the answer. Using this strategy, any breach that occurs will be confined to IT assets and data that lie within that segment. By automatically applying security and compliance policies to virtual assets and data in the cloud, segments can also improve manageability.

Also fundamental to the foundation of a sound security strategy is continuous monitoring of activity. With proper visibility at the right levels of the network, breaches can be detected, prevented, logged and reported in real time. Active enforcement of policies is also necessary to mitigate the severity of breaches.

As these security layers are established, remaining compliant becomes easier.

Including a tool within this architecture that maps security controls to compliance frameworks can significantly reduce audit scope by offering an automated method to provide evidence of control. The entire layered solution positions IT to attain an optimized level of security and compliance.

AUTOMATING FOR A MORE SECURE FUTURE

Organizations across the board are adopting virtualization as a way to streamline operational efficiencies and save money. Financial institutions are joining this wave and moving their payment processing into private clouds. In order to meet the strict requirements of the financial industry, they need to maintain granular control of sensitive data within the cloud. Automated tools have been developed to meet the specific challenges found within virtual environments. In partnership with perimeter controls, these tools not only help safeguard data in the cloud but also provide evidence that auditors need as proof of compliance. Financial institutions that want to future-proof their data centers via virtualization can now implement leading-edge security measures that can lead to greater customer trust, a stronger brand and greater profits.

RANDAL ASAY

Randal Asay joined Catbird in 2013 with over 15 years of experience in network security, architecture, implementation, and security best practices in commercial and government environments. Prior to Catbird, Randal served as Director of Engineering at Walmart Stores Inc., developing industry-leading code analysis practices to support security and compliance initiatives as well as addressing enhancements to perimeter and network security and overall policy enforcement. He led the E-commerce Infrastructure teams through extensive growth, delivering capacity management and technology refresh methods impacting network design, storage capacity and database tuning. Prior to Walmart, he applied his security expertise to the Information Assurance division of the United States Air Force. Randal holds Masters degrees in Information Technology Management and Business Administration from Webster University as well as a Bachelor of Science degree from Weber State University.

THE FREEWAY TO CISSP

by Patric J.M. Versteeg, CISSP CISM CISA CRISC CEH ECSA LPT SCF

The freeway (road) to CISSP. A long tedious drive along Route 44 of all ten domains of information security or is there a detour that will get you certified in a drag-race sprint?

What you will learn...

- how to pass the exam in the least amount of time,
- what resources you can utilize to pass the exam,
- Passing the exam vs getting certified,
- what to expect after certification,
- is it worth time and money?

What you should know...

- there are no prerequisites to learn from this article.

Experience. That is the key element to pass the exam and get certified in the least amount of time. Sorry. But there is no other short cut route. The covered topics cover a lot of ground within the specified domain and you need to be comfortable with at least one or two topics with every domain. I do not want to discourage you but with no experience you are looking towards 6 months of hard core study. With enough experience you should be able to finish within 3.

In even considering studying for the exam you should have at least sound knowledge and understanding (experience) in at least 6 of the 10 domains as outlined below. Remember that you need at least 5 years of experience in at least two of the 10 domains to get certified.

The CISSP exam consists of 250 questions that have a scoring mark of 70% and are draw from various information security topics within the (ISC)² CBK.

The CISSP CBK consists of the following ten domains:

- **Access Control** – a collection of mechanisms that work together to create security architecture to protect the assets of the information system.
  Concepts/methodologies/techniques
  Effectiveness
  Attacks
- **Telecommunications and Network Security** – discusses network structures,transmission methods, transport formats and security measures used toprovide availability, integrity and confidentiality.
  Network architecture and design
  Communication channels
  Network components
  Network attacks
- **Information Security Governance and Risk Management** – the identificationof an organization's information assets and the development, documentation and implementation of policies, standards, procedures and guidelines.
  Security governance and policy
  Information classification/ownership
  Contractual agreements and procurement processes

Risk management concepts
Personnel security
Security education, training and awareness
Certification and accreditation

- **Software Development Security** – refers to the controls that are included within systems and applications software and the steps used in their development.
  Systems development life cycle (SDLC)
  Application environment and security controls
  Effectiveness of application security
- **Cryptography** – the principles, means and methods of disguising information to ensure its integrity, confidentiality andauthenticity.
  Encryption concepts
  Digital signatures
  Cryptanalytic attacks
  Public Key Infrastructure (PKI)
  Information hiding alternatives
- **Security Architecture and Design** – contains the concepts, principles, structures and standards used to design,implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used toenforce various levels of confidentiality, integrity and availability.
  Fundamental concepts of security models
  Capabilities of information systems (e.g. memory protection, virtualization)
  Countermeasure principles
  Vulnerabilities and threats (e.g. cloud computing, aggregation, data flow control)
- **Operations Security** – used to identify the controls over hardware, media and the operators with access privileges to any of these resources.
  Resource protection
  Incident response
  Attack prevention and response
  Patch and vulnerability management
- **Business Continuity and Disaster Recovery Planning** – addresses the preservation of the business in the face of major disruptions to normal business operations.
  Business impact analysis
  Recovery strategy
  Disaster recovery process
  Provide training
- **Legal, Regulations, Investigations and Compliance** – addresses computer crime laws and regulations; the investigative measures and techniques which can be used to determine if a crime has been committed and methods to gather evidence.
  Legal issues
  Investigations
  Forensic procedures
  Compliance requirements/procedures
- **Physical (Environmental) Security** – addresses the threats, vulnerabilities and countermeasures that can be utilized tophysically protect an enterprise's resources and sensitive information.
  Site/facility design considerations
  Perimeter security
  Internal security
  Facilities security

[taken from *https://www.isc2.org/cissp-domains/default.aspx*]

WHAT RESOURCES YOU CAN UTILIZE TO PASS THE EXAM

The are no short cuts or cram documents towards passing the exam.

Still you are able to effectively utilize your time and minimize your efforts to pass the exam.

The first step to take is to gather the right set of resources to utilize.

STEP 1: INFORMATION GATHERING
Browse the (ISC)² (*https://www.isc2.org/cissp-training.aspx*) website and gather all information on the CISSP exam. Register for the exam outline and other free resources that are offered by (ISC)². Make yourself acquainted with the exam and certification procedures and find yourself certification sponsors.

On LinkedIn there are several CISSP prep study groups you can join so you can exchange experiences and read-up on the latest study and exam info.

Keep your information within scope. Having four books on the shelf that you did not read cover to cover is useless. I would advise reading two books cover to cover (see step 2 and 4)

Several different companies offer an official (ISC)² prep course. As I have taken this course as well and ending up performing step 2 through step 4 as well I would not recommend attending an official (ISC)² prep course unless you have the money to spend. An official ISC² prep course will teach you only so much that you will be performing the following steps as well, just to make sure.

STEP 1: FIRST DRIVER LESSONS
Browse over to CBT – Nuggets (*http://www.cbtnuggets.com/it-training-videos/course/isc2_cissp_2012*) get yourself a subscription. Watch and listen to all Keith Barker (funny and enthusiastic trainer!) has to say to get a first real gasp on what the exam is all about.

STEP 2: DRIVING ON A B-ROAD
Anybody who has ever taken the CISSP exam will reference “the gold bible” from Shon Haris.

A must have read for anybody who want to get certified. (*http://logicalsecurity.com/certified-information-systems-security-professional-cissp-solution-set/*) By obtaining this kit you not only get the book, on demand course, exam questions but also a set of mp3 files.

As you work through the material from Shon, listen to the mp3 files as you commute to and from work. Play it on a portable device in your car, on the bus, tram or while riding a bicycle. Even when you are not constantly listing (when your mind wanders off) you still get fed the information you need to pass the exam on a regular and in a consistent way.

STEP 3: PUT THE PEDAL TO THE METAL.
Browse over to test king (*http://www.test-king.com/exams/CISSP.htm*) , buy and use the test engine as a learning tool. If you can elaborate why you choose an answer you are on the right track. If you can’t, write the question down (mark it) and do your research.

Make sure you read and study up on all 2000+ questions at least two times.

This will not only enhance your knowledge on the ten CBK domains but it will also train you in reading exam questions. Remember: The exam is 250 questions in a boxed (and it seem short!) time frame. You need training in this field (exam taking)as well.

Do not expect the same questions on the exam! Remembering the answers to the questions will not help you. Reasoning will.

STEP 4: FINISH!
As you are about to finish, you can see the checkered flag (exam is just around the corner) , around two weeks before the exam, put all material you read and studied to the side. Keep listing to the mp3 files and get yourself the CISSP for Dummies book (ISBN-13: 978-1118362396). No, this is not a joke! I found that this book is an excellent tool for the recap of the CISSP curriculum. All topics are well covered and it feeds you just that extra piece of information that you need to pass.

PASSING THE EXAM VS GETTING CERTIFIED

In theory everyone can pass the exam, but only the few chosen, the elite become certified.

ISC² has set the ground rules towards certification as follows:

Once you are notified that you have successfully passed the examination, you will be required to subscribe to the (ISC)² Code of Ethics and have your application endorsed before the credential can be awarded. An endorsement form for this purpose must be completed and signed by an (ISC)² certified professional who is an active member, and who is able to attest to your professional experience.

With the Endorsement Time limit, you are required to become certified within nine (9) months of the date of your exam OR become an Associate of (ISC)². If you do not become certified or an Associate of (ISC)² within nine (9) months of the date of your exam you will be required to retake the exam in order to become certified. [taken from: *https://www.isc2.org/cissp-how-to-certify.aspx*]

Please read all information on the (ISC)² carefully and familiarize yourself with all the requirements set by (ISC)². It is imperative that you complete your endorsement within the time limit and that you have proof of all of your professional experience! It is experience that digging 5 years into the past to prove you have the required experience is tough. Even if you can remember what you did when, how are you going to prove it? Start thinking about it now! Before the exam, so you have everything lined up when your passing grade comes in.

WHAT TO EXPECT AFTER CERTIFICATION

(ISC)² requires you to acquire a minimal of 20 CPEs (Continuing Professional Education credits) per year and a total of 120 CPEs in a three year –roll over. You also need to pay an AMF (Annual Maintenance Fees) upon receipt of annual invoices.

Maintaining those 20 / 120 CPEs is not so much of hard labor as you might think and if you are working as an information security specialist it is even “easy” to maintain those. Go to some vendor presentations, enlist and attend chapter meetings, read a security book or write an security article ;-) ..

It all helps you advance in the information security field and provides you the CPEs you need.

But this is not the only thing to expect after certification, remaining in good standing as a member of (ISC)². If you really want to advance in your career you will use the CISSP certification as a springboard.

You need to dive deep in one or more domains of your choosing and specialize in one or more areas.

IS IT WORTH TIME AND MONEY?

A hard question to be answered. It depends. What is your goal? What do you want to achieve? For an independent contractor the CISSP certification is a must have. Period. You will not be considered for a contract (with a reasonable hour rate) without the CISSP designation.

If you are in a permanent position and you want to advance towards another position or another company, CISSP certification is a smart move.

Passing the CISSP exam will not make you an information security specialist or make you an IT security guru. It will give you the reasoning and means after choices that you are going to take down the road as you advance in your career. For every role, every company, in every country specific information security rules apply. You will not learn this in CISSP course. This is something you have to do on your own.

From my perspective, CISSP is a certification that will help you advance more in information security (management) than for IT security.

Is it worth the money? For me, personally, a big YES! The cost estimate is less than $2500.

With this investment you can shift your career in the highest gear.

Is it worth the time? For me, personally, a big YES! again. But are you up for the challenge?

SUMMARY

The CISSP exam is no joke! You have to study hard and put everything aside to become certified. And in the end it is all worth it. Internationally recognition of your knowledge and expertise. Becoming part of the elite cyber security professionals. And in time there will be more work than we all can handle together ;-)

If you fail the exam first time around? …. Go Harder or Go Home!

PATRIC J.M. VERSTEEG

The author has been working as an (security) consultant for large international companies for the past fifteen years and has also been involved in developing security exams and courses. He is certified for all major domains of information security and holds all major information security certifications. You can contact him under Info@S3cur1ty-Solutions.nl.

COMPUTER FORENSICS WITH P2 COMMANDER

by Pranshu Bajpai

Computer Forensics is the methodical series of procedures and techniques used for procuring evidence from computer systems and storage media. This evidence can then be analyzed for relevant information that is to be presented in a court of law. Computer Forensics has frequently been listed as one of the most intriguing computer professions, however beginners may find themselves overwhelmed quickly, as practical step-by-step procedures on this subject may be hard to come by.

This paper seeks to address IT professionals who are interested in Computer Forensics Investigations. However, registry hives explored in this case study hold a plethora of information that would be of use to everyone. To keep things interesting and practical, we will be simulating a 'real-life' scenario where you will assume the role of a forensics investigator and attempt to locate incriminating digital evidence in the disk. While doing so, here is what you will learn:

- How to obtain and replicate evidence disks (*Acquire*)
- How to verify the integrity of the evidence media (*Authenticate*)
- How to search for relevant information in the evidence disk (*Analyze*)
- How to explore the Windows registry hive structure and why it holds relevance to Computer Forensics Investigations

Scenario: A complaint was made to the authorities describing alleged Wi-Fi hacking activity. When the authorities arrived on the spot, they found a Dell laptop and an Alfa Card (wireless USB adapter) abandoned in the vicinity. Witnesses recall seeing a person with such equipment lingering in the vicinity of Wi-Fi access point. This abandoned equipment is seized as possible evidence.

Role: Computer Forensics Investigator

Purpose: Locate inculpatory or exculpatory evidence in the disk so that it may be presented in a court of law.

Evidence Disk: The seized Dell laptop disk can be downloaded here: part1 and part2. A 'dd' copy can be downloaded here: 1, 2, 3, 4, 5, 6, 7, 8.

Tools used: The tool we have chosen for the purposes of this investigation is Paraben's 'P2 Commander', however you are free to use other tools of your choosing ('EnCase', 'FTK', 'Prodiscover', etc).

Get a demonstration copy of Paraben's P2 Commander here.

Tasks performed: During the course of investigation, analysis of the evidence would require performing the 12 basic tasks of computer forensics:

1. Generating an image hash and confirming the integrity of the image
2. Determining the Operating System used on the disk
3. Determining the date of OS installation
4. Determining the registered owner, account name in use and the last recorded shut down date and time
5. Determining the account name of the user who mostly used the computer and the user who last logged into it
6. Determining the hacker handle of the user and tying the actual name of the user to his hacker handle
7. Determining the MAC and last allocated IP address of this computer
8. Locating the programs installed in this computer that could have been used for hacking purposes
9. Collecting information regarding the IRC service that was used by the owner
10. Searching the Recycle Bin for relevant information
11. Listing the Newsgroups that the owner of the computer has registered to
12. Determining the SMTP email address in use

OBTAINING AND REPLICATING EVIDENCE DISKS

As a forensics investigator, when you arrive at the crime scene, it is your foremost responsibility to acquire evidence without contamination. In the case of digital media, you need to ensure that the evidence disk is not corrupted in any manner. If the computer in question is turned off, seize it (and any other peripherals in the vicinity). However if the computer is turned on:

- Take pictures of the computer screen using a high resolution camera; if any windows are minimized, it is OK to maximize them and take pictures.
- For precautions, write down the contents of these windows.
- Often proper shutdown procedure should be used to turn off the computer but volatile (RAM) data may be lost after shutdown; if in doubt, take a senior's advice on what procedure would be best.

Before starting any kind of analysis, *make sure you have made at least two bit-by-bit copies of the evidence media.* It is suggested that the two copies be made using different tools. If one copy fails, having another copy will be worth the effort. Hardware write-protectors may be used to ensure that the integrity of the original evidence disk is preserved at all times.

ACQUIRING AN IMAGE OF THE EVIDENCE DISK (ACQUIRE)

To acquire an image of the disk in we will use the 'dd' command, in the following manner:

In Linux:

```
dd if=/dev/hda of=/home/user/Wireless_Hacking_Case.dd bs=512 conv=noerror,sync
```

In Windows:

```
dd.exe if=\.PhysicalDrive0 of=C:Pranshu_Case_ImagesPhysicalDrive0.img -md5sum -verifymd5 -
   md5out=C:Pranshu_Case_ImagesPhysicalDrive0.img.md5
```

Note: Here, 'if' refers to input file; 'of' refers to output file; '/dev/hda' is the physical drive. Read more about the 'dd' command here.

INVESTIGATING 'NEW CASE' AND 'ADDING EVIDENCE' IN P2 COMMANDER

Click 'New Case' [Figure 1]

Figure 1. New Case

(Enter Details of the Case) [Figure 2]

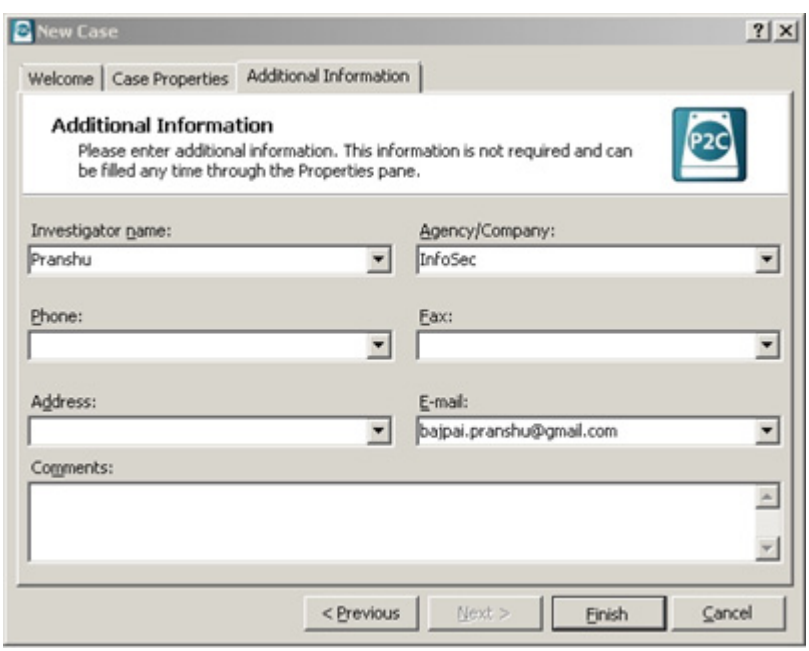


Figure 2. Details of the Case

Click ‘Add Evidence’->Choose ‘Image File’->’Auto-detect Image’ [Figure 3]

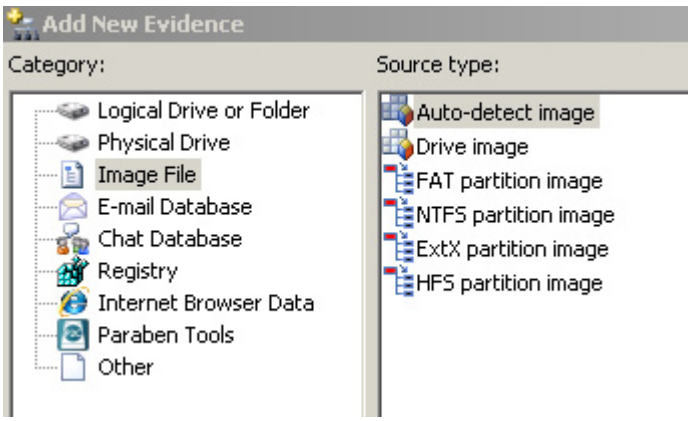


Figure 3. Adding Evidence

Now load the Evidence Disk Image that you have downloaded earlier.

Note: Paraben’s P2 Commander has a lot of windows where it displays relevant information about the case evidence. (Figure 4)

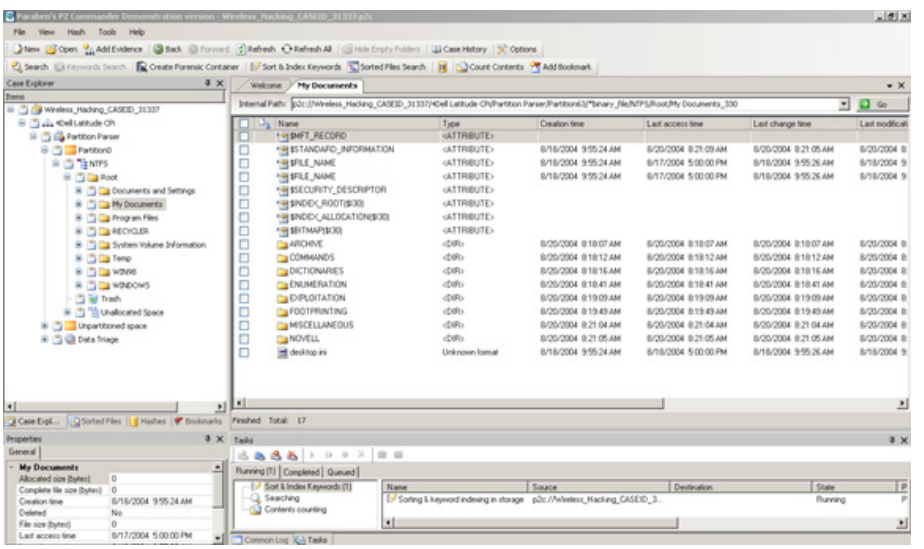


Figure 4. Information about the case evidence

GENERATING A HASH VALUE OF THE EVIDENCE MEDIA

Before commencing *Analysis* of the evidence media, it is mandatory to ensure that integrity of evidence is preserved. So for *Authentication* purposes, we generate a *hash value* of the media. As you probably know, this hash is a one-way function that serves to detect any modifications in the data. Therefore, if even a single bit is flipped in the evidence media (corruption), the hash value would differ and the corruption would be detected.

To generate a hash value using P2 Commander, follow these steps:

Right click a file and click ‘Add MD5 to hash database’. [Figure 5]

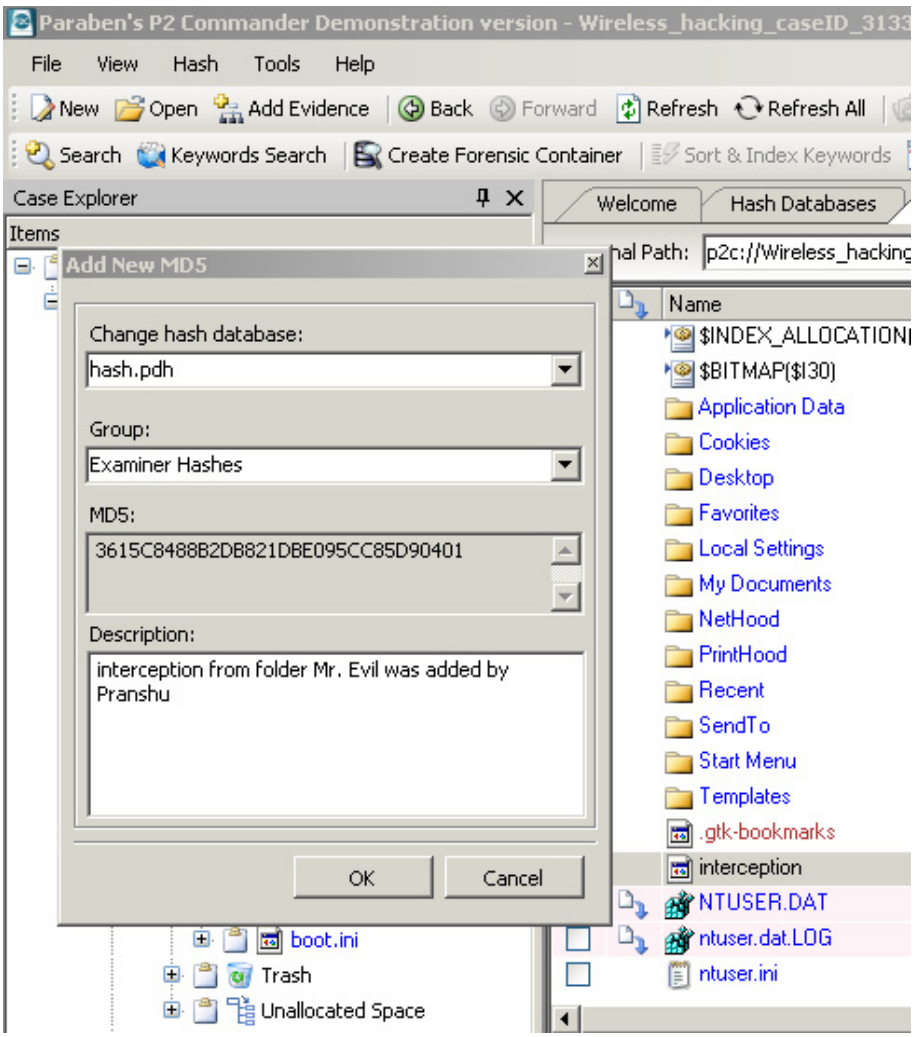


Figure 5. Adding MD5

You will notice that these hashes get added to the hash database of your choosing (in this case, ‘hash.pdh’). (Figure 6)

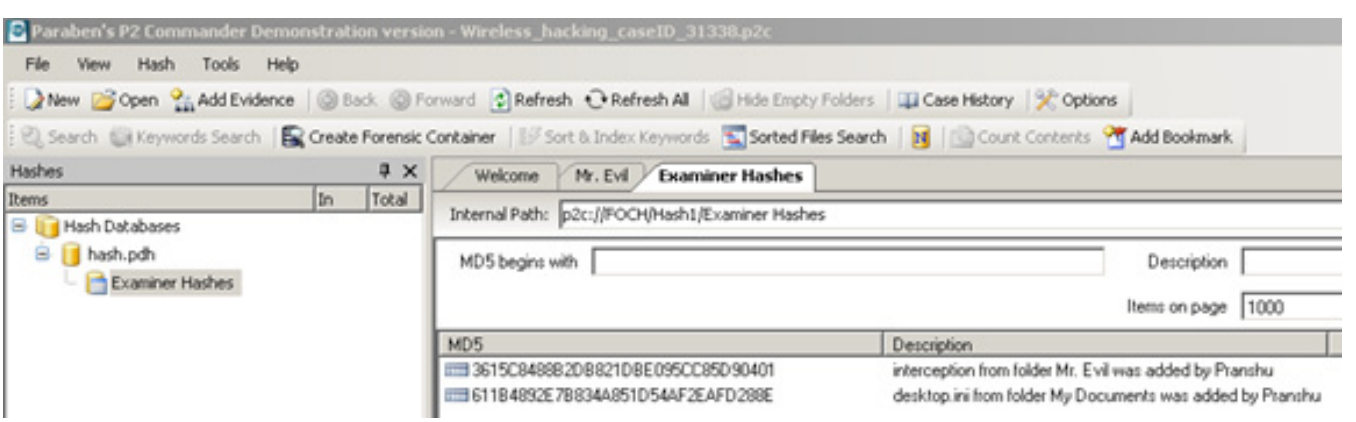


Figure 6. hash.pdh

MATCHING THE ACQUISITION HASH TO THE VERIFICATION HASH (AUTHENTICATE)

Before commencing any future investigations or analysis, *hash value should be verified.* The investigator would generate a hash of the evidence media (called the *Verification Hash*) and match it with the Acquisition Hash.

BEGINNING ANALYSIS OF THE EVIDENCE MEDIA (ANALYZE)

Now the investigator begins the process of locating inculpatory or exculpatory evidence in the disk.

Note: *Inculpatory* evidence proves that the suspect is guilty of the crime while *Exculpatory* evidence proves that he/she is innocent of it.

Note: At this point it is important to discuss: What are 'hives'? Hives are hierarchical structures where Windows stores a wealth of information. You have probably used 'regedit' in Windows to do some minor Registry tweaking and have seen the 5 root keys (hives). These are:

- HKEY_LOCAL_MACHINE (HKLM)
- HKEY_CURRENT_CONFIG (HKCC)
- HKEY_CLASSES_ROOT (HKCR)
- HKEY_USERS (HKU)
- HKEY_CURRENT_USER (HKCU)

The locations of keys and sub-keys within these hives may differ depending on the version of the Operating System in use. As we move with the 'Analysis' part of the investigation, the importance of these hives will become clear to you.

DETERMINING THE OPERATING SYSTEM USED ON THE COMPUTER

Although as soon as we view the files and folders on the evidence disk it becomes clear that a Windows OS was in use, we can know the exact version [Figure 7] at the following path:

```
WINDOWS/SYSTEM32/CONFIG/SOFTWARE/MICROSOFT/WINDOWS NT/CURRENT VERSION/PRODUCT NAME
```

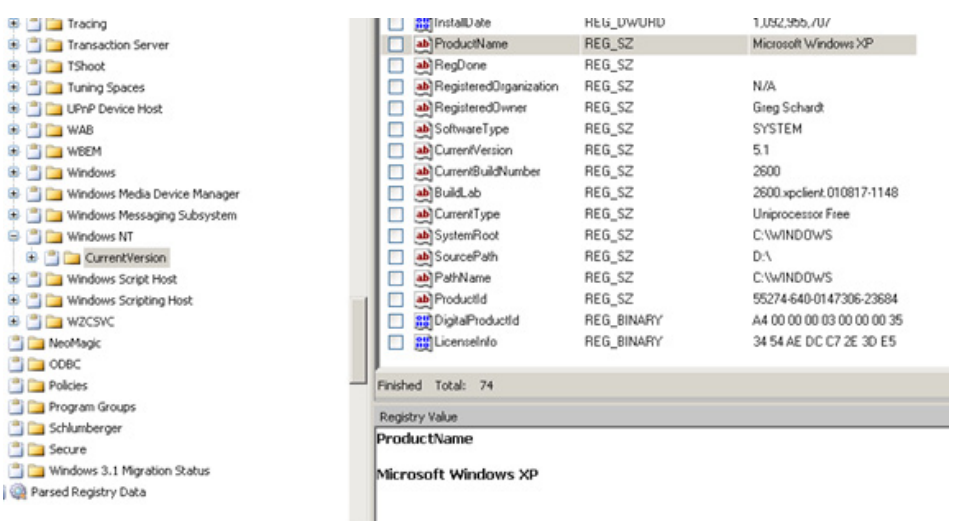


Figure 7. Determining the operating system used on the computer

OR

```
C:/boot.ini
```

Note: In P2 Commander, you would have to expand 'config->software' and then expand '$DATA' and then 'Registry File'. This would take you to '…/MICROSOFT/WINDOWS

```
NT/CURRENT VERSION/' [Figure 8]
```

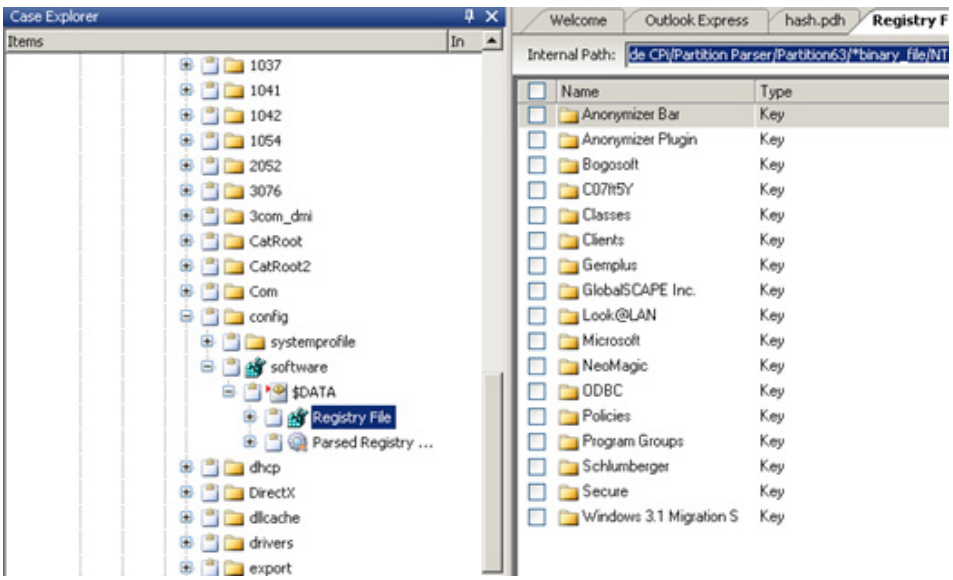


Figure 8. NT/CURRENT VERSION

DETERMINING THE DATE OF INSTALLATION

This information can be uncovered from the following path [Figure 9]:

```
WINDOWS/SYSTEM32/CONFIG/SOFTWARE/MICROSOFT/WINDOWS NT/CURRENT VERSION/INSTALL DATE
```

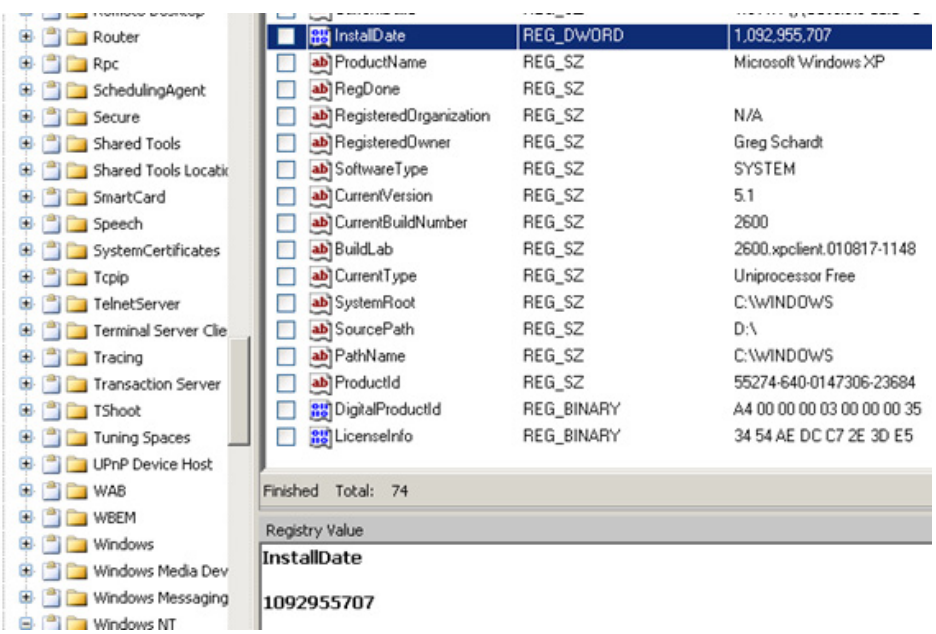


Figure 9. Uncovered information from the path

DETERMINING THE REGISTERED OWNER OF THIS COMPUTER

This information will help us determine the actual name of the criminal (if the crime is proven). [Figure 10] It can be uncovered at the following path:

```
WINDOWS/SYSTEM32/CONFIG/SOFTWARE/MICROSOFT/WINDOWS NT/CURRENT VERSION/REGISTERED OWNER
```

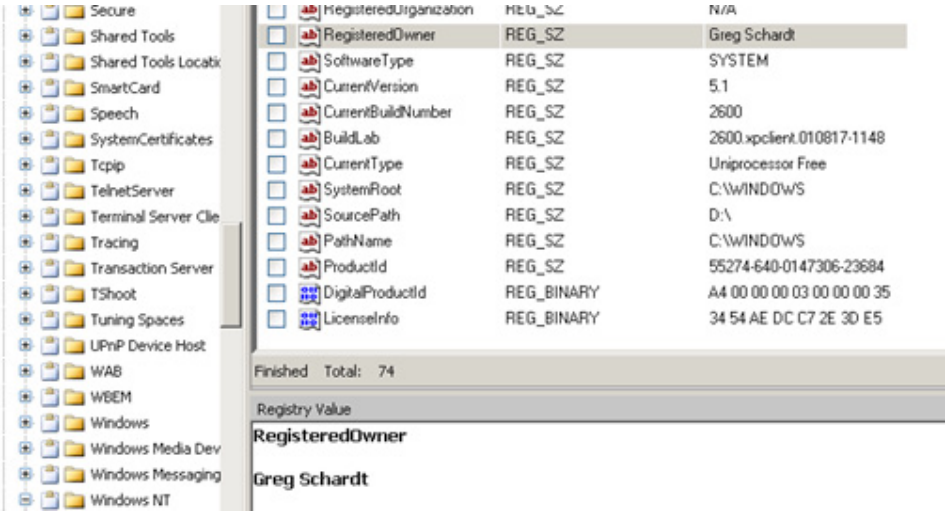


Figure 10. Determining actual name of the criminal

DETERMINING THE DEFAULT DOMAIN NAME

This information can be uncovered at the following path [Figure 11]:

```
WINDOWS/SYSREM32/CONFIG/SOFTWARE/MICROSOFT/WINDOWS NT/CURRENT VERSION/WINLOGON/DEFAULT DOMAIN NAME
```

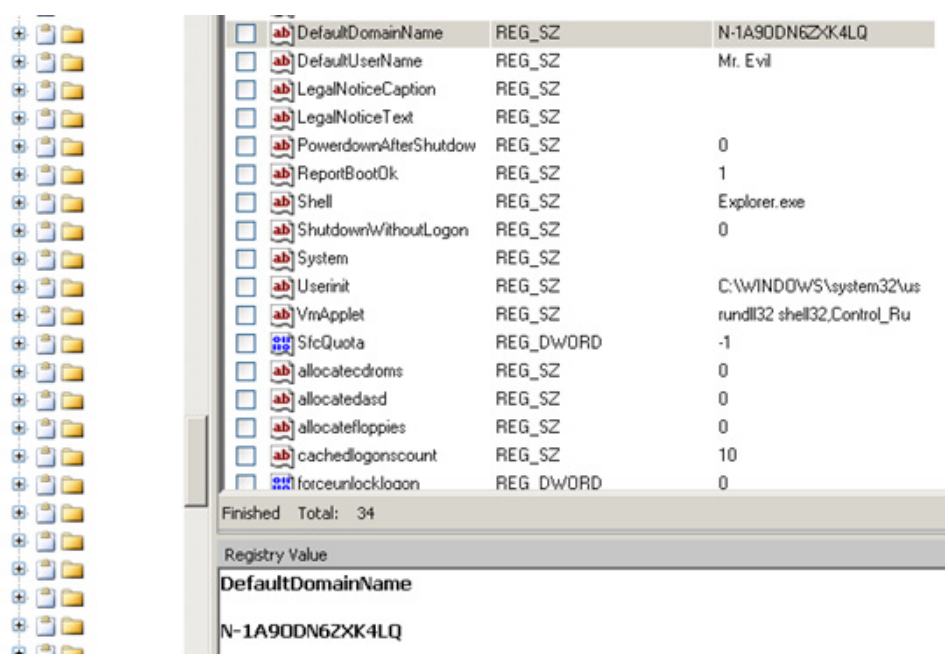


Figure 11. Determining default domain name

DETERMINING THE DEFAULT USER NAME

This information would help us determine the username that is used to log into this computer. It can be located at the following path [Figure 12]:

```
WINDOWS/SYSTEM32/CONFIG/SOFTWARE/MICROSOFT/WINDOWS NT/CURRENT VERSION/WINLOGON/DEFAULT USER NAME
```

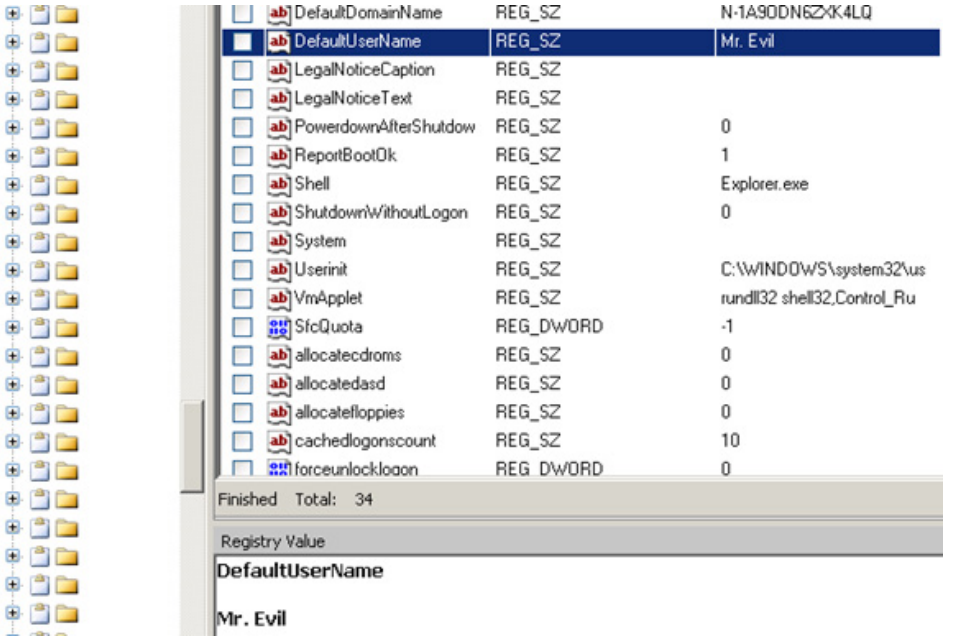


Figure 12. Determining the default username

DETERMINING THE TIME AND DATE OF WHEN THE COMPUTER WAS LAST SHUTDOWN

This information can be uncovered at the following path [Figure 13]:

```
WINDOWS/SYSTEM32/CONFIG/SOFTWARE/MICROSOFT/WINDOWS NT/CURRENT VERSION/PREFETCHER/EXIT TIME
```

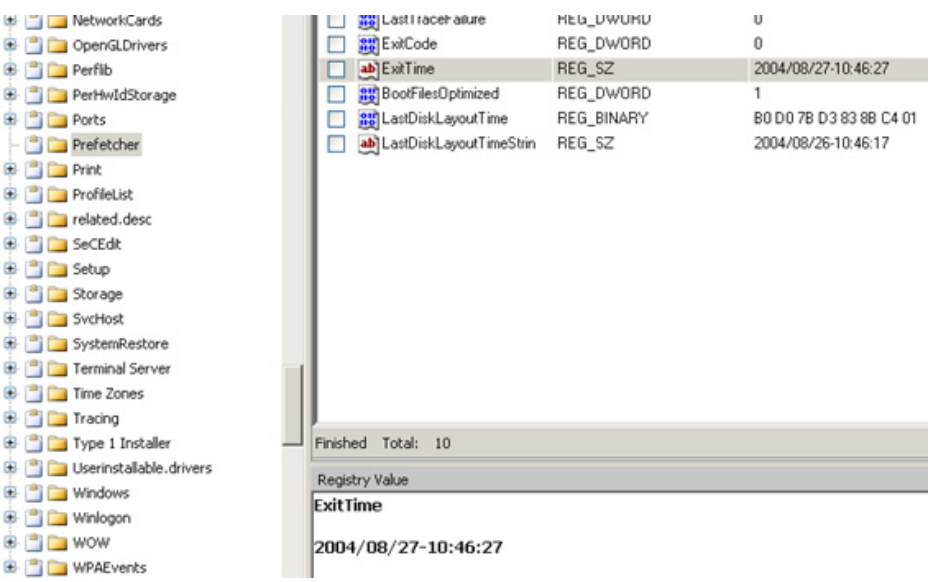


Figure 13. Determining the time and date when the computer was last shutdown

DETERMINING THE TOTAL NUMBER OF ACCOUNTS PRESENT ON THIS COMPUTER

A total of 5 accounts were found [Figure 14]. This information can be found in the SAM file:

```
SAMSAMDomainsAccountUsersNames
```

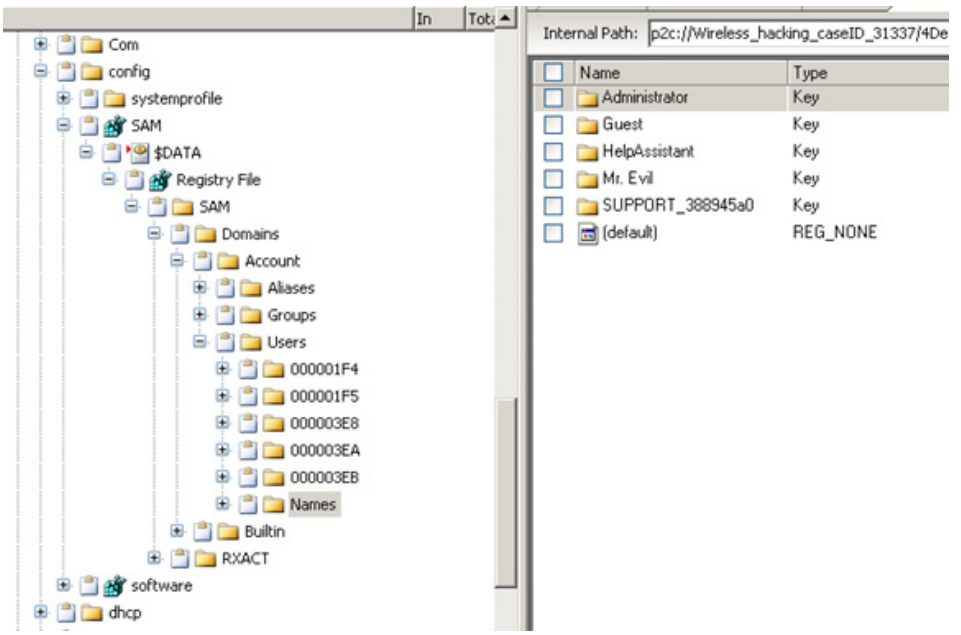


Figure 14. Total number of accounts

However, 4 of them are default Windows accounts and were never used. The one account mainly used, was that of 'Mr. Evil'. This information is suggested by the sub-keys found under 'Users' at the following path:

```
SAMSAMDomainsAccountUsers
```

DETERMINING THE LAST USER WHO LOGGED ONTO THIS COMPUTER

The system will obtain the last user who logged on from the key 'DefaultUserName'. This information can be uncovered from the following path [Figure 12]:

```
WINDOWS/SYSTEM32/CONFIG/SOFTWARE/MICROSOFT/WINDOWS NT/CURRENT VERSION/WINLOGON/DEFAULT USER NAME
```

TYING THE HACKER'S 'HANDLE' TO HIS REAL NAME

We have seen above that the owner of this computer is 'Greg Schardt' and his username is 'Mr. Evil'. Now to prove that Greg Schardt is Mr. Evil, we need to perform extensive searches for files that may provide the needed evidence. In this case, we found the following file to be of aid:

```
C:Program FilesLook@LANirunin.ini
```

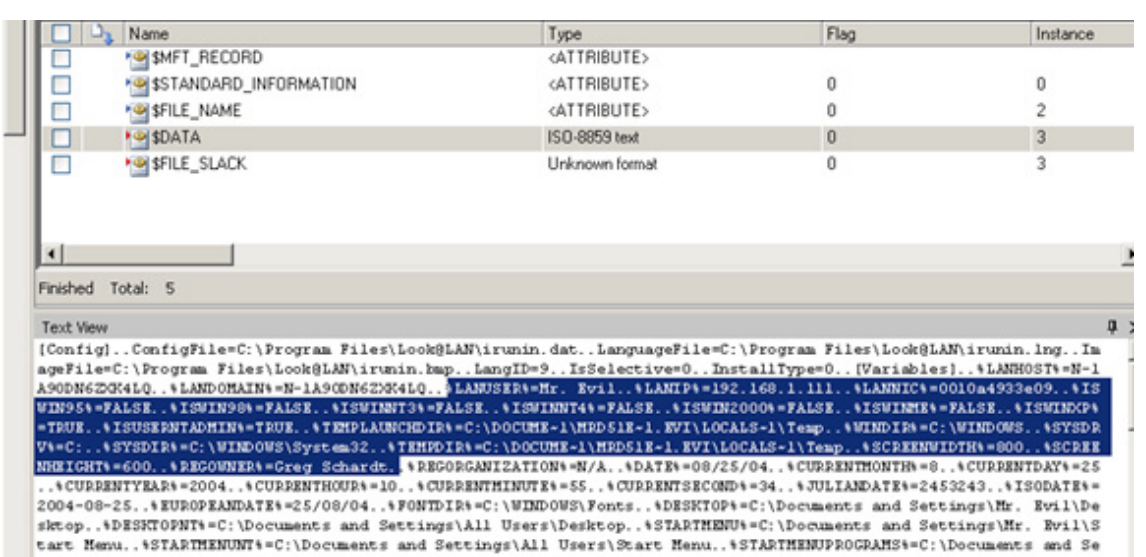


Figure 15. Tying the hacker's „handle" to his real name

This file would help tie Greg Schardt to his hacker handle of 'Mr. Evil'. [Figure 15]

DETERMINING THE NETWORK CARD THAT WAS USED ON THIS COMPUTER

This information can be uncovered from the following path:

```
WINDOWS/SYSTEM32/CONFIG/SOFTWARE/NTREGISTRY/MICROSOFT/ WINDOWS NT/CURRENT VERSION/NETWORKCARDS/11/
   DESCRIPTION
```

And

```
WINDOWS/SYSTEM32/CONFIG/SOFTWARE/NTREGISTRY/MICROSOFT/ WINDOWS NT/CURRENT VERSION /NETWORKCARDS/2/
   DESCRIPTION
```

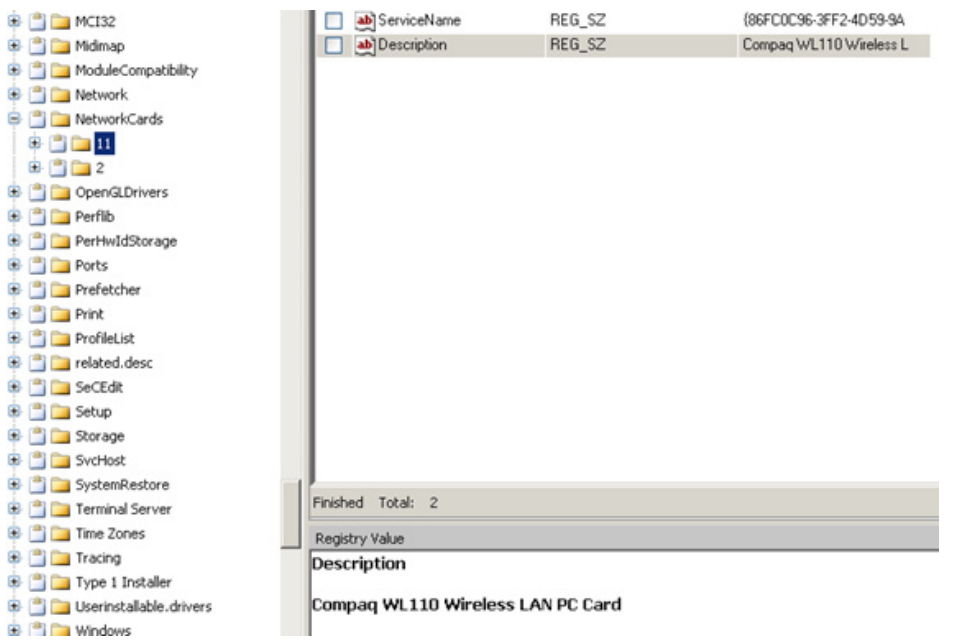


Figure 16. Determining the network card

Hence the network card used was 'Compaq WL110 Wireless LAN PC Card' (Xircom CardBus Ethernet 100 +Modem56 (Ethernet Interface)). [Figure 16]

DETERMINING THE PHYSICAL AND LOGICAL ADDRESSES USED BY THE COMPUTER (MAC ADDRESS AND IP ADDRESS)

Figure 17. Programs and tools

This file tells us that IP address was 192.168.1.111 and the MAC address is `0010a4933e09` [Figure 17]

SEARCHING FOR PROGRAMS/TOOLS THAT AIDED IN THE CRIME (WIRELESS HACKING)

This evidence can be uncovered from many locations. For example, the registry path:

```
WINDOWS/SYSTEM32/CONFIG/SOFTWARE/MICROSOFT/WINDOWS/CURRENT VERSION/UNINSTALL [Figure 18]
```

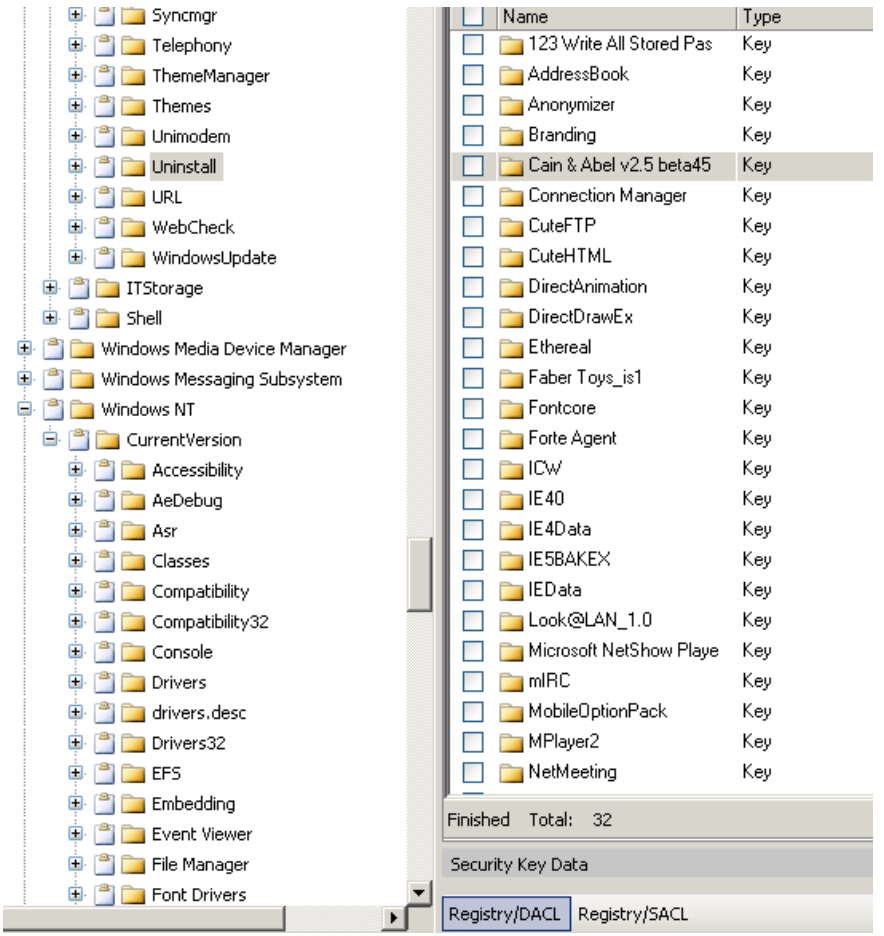


Figure 18. Programs and tools

This path shows a variety of hacking tools installed on the computer.

Also see the 'My Documents' folder and notice the presence of several hacking tools and password cracking dictionaries. [Figure 19]

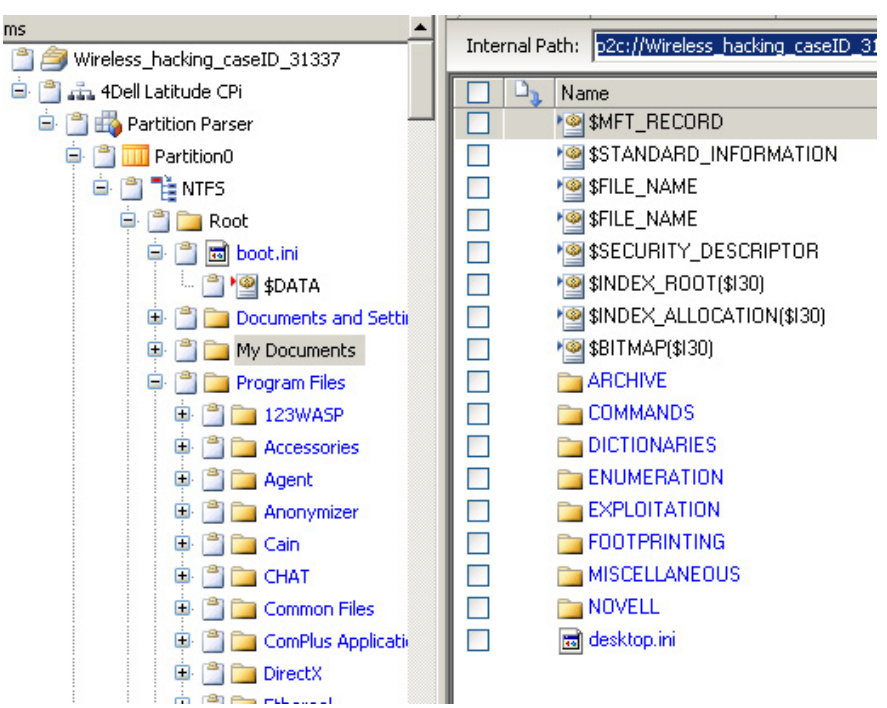


Figure 19. Used tools

Also note that the 'Desktop' folder has links to several hacking tools.

Following are some of hacking tools that were found on the computer:

- Cain & Abel v2.5 beta45 (password sniffer & cracker)
- Ethereal (packet sniffer)
- 123 Write All Stored Passwords (finds passwords in registry)
- Anonymizer (hides IP tracks when browsing)
- Look&LAN_1.0 (network discovery tool)
- NetStumbler (wireless access point discovery tool)

DETERMINING THE SMTP EMAIL ADDRESS THAT WAS USED ON THIS COMPUTER

The email address used was *whoknowsme@sbcglobal.net* [Figure 20] and this information can be located at:

```
C:/PROGRAM FILES/AGENT/DATA/AGENT.INI
```

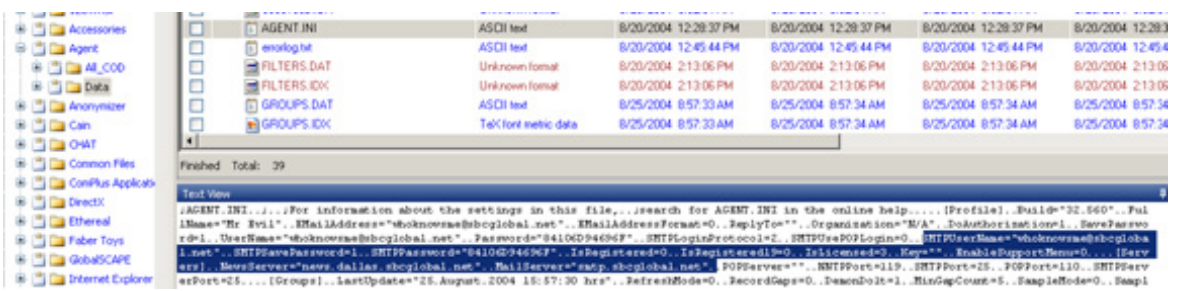


Figure 20. SMTP email address

Note that the saved SMTP password is also recovered, this can be used for further investigation of the SMTP email account.

DETERMINING THE NEWSGROUPS THAT THE COMPUTER'S USER HAS SUBSCRIBED TO

This information can be uncovered from the following path:

```
DOCUMENT AND SETTINGS/MR EVIL/LOCAL SETTINGS/APPLICATION DATA/IDENTITIES/MICROSOFT/OUTLOOK EXPRESS
```

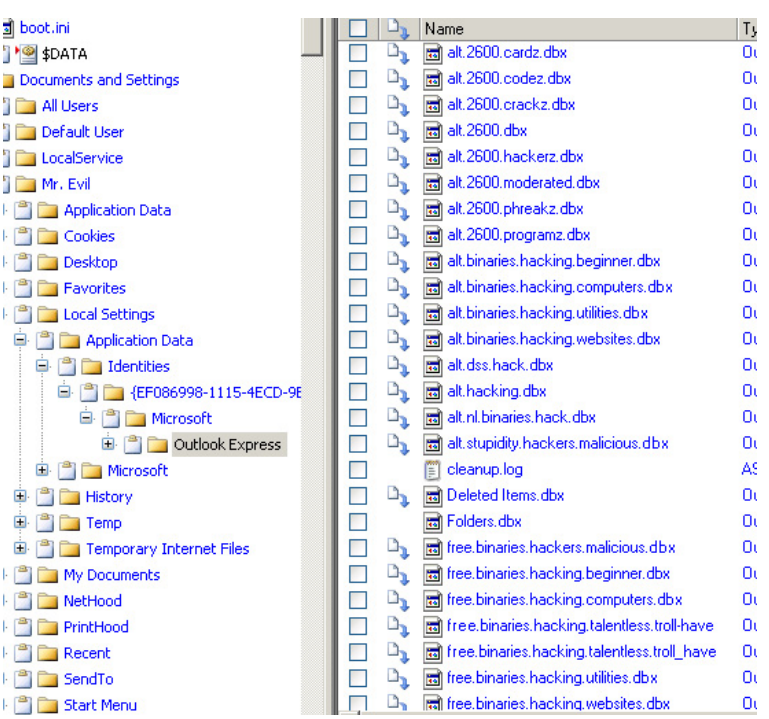


Figure 21. Newsgroups

The user has subscribed to several 'hacking' newsgroups as can be seen from the evidence. [Figure 21].

RECOVERING CHAT RELATED INFORMATION FROM THE IRC PROGRAM (MIRC)

The following path would reveal IRC related information like the username, nickname, email, host etc [Figure 22]:

```
C:/PROGRAM FILES/MIRC/MIRC.INI
```

Figure 22. Recovering Chat

Furthermore, MIRC logs chat sessions at the following location:

```
C:/PROGRAM FILES/mIRC/LOGS
```

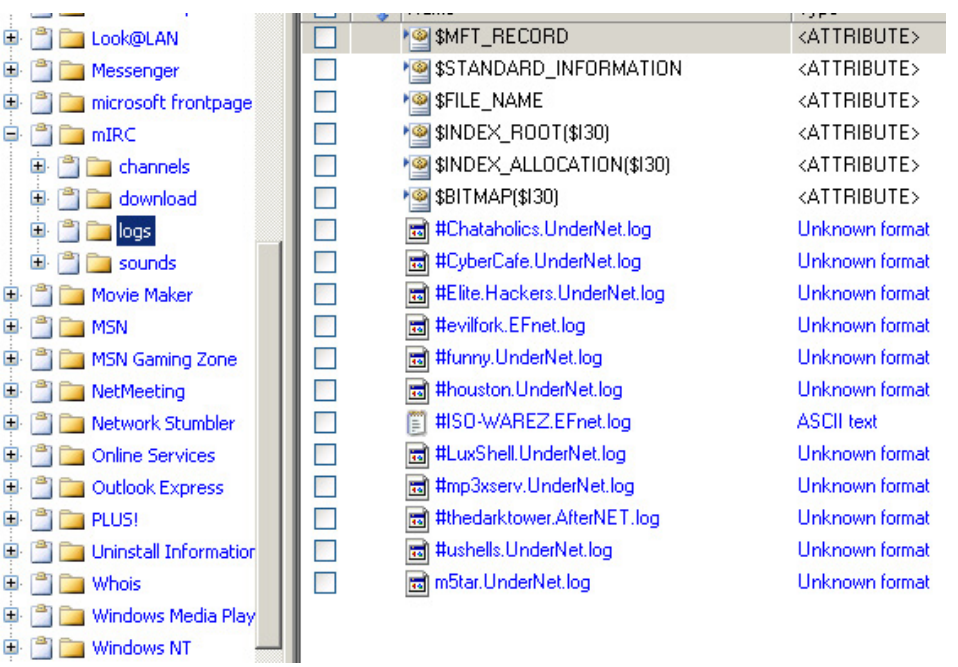


Figure 23. Chat sessions

Again we observe a lot of hacking-related chat channels in the logs. [Figure 23]

SEARCHING FOR THE 'ETHEREAL' PACKET CAPTURE FILE

Earlier we have noticed the presence of the sniffing tool 'Ethereal' on this computer. Now the challenge is to locate the packet capture file. I say it is a 'challenge', because in this particular case, the saved packet capture file has *no extension*and hence proved to be incredibly hard to locate. It was eventually located at the following path [Figure 24]:

```
C:/DOCUMENTS AND SETTINGS/MR EVIL/INTERCEPTION
```

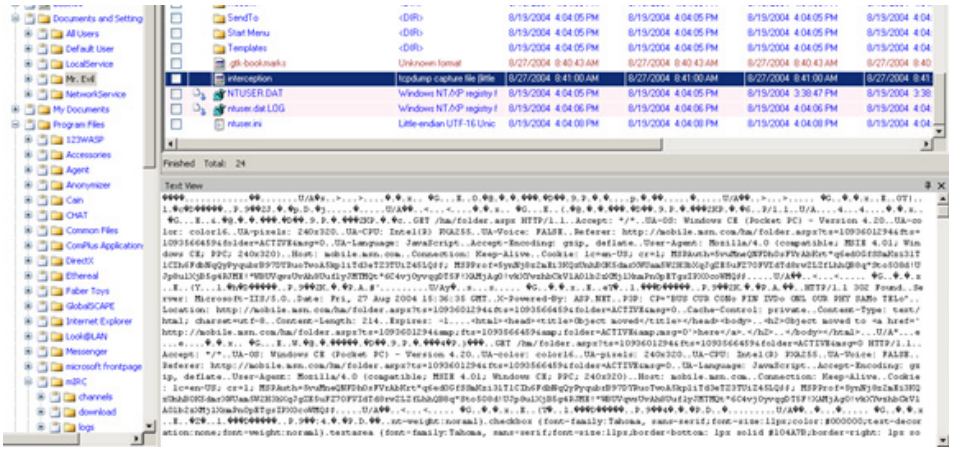


Figure 24. Ethereal Packet Capture File

Even though this file has no extension, our first clue is the name of the file 'interception'. Further analysis of the file revealed that it is in fact the file used to save the packets captured.

Note: Remember that this file is where the captured packets were saved. Packets captured from whom? Packets captured from the victim's machine. Therefore, it reveals the websites that the victim was visiting at the time of sniffing.

RECOVERING INFORMATION FROM THE RECYCLE BIN

The Recycle Bin can be a useful location for the purpose of forensics investigations, since the evidence the hacker would want to get rid of would probably end up here (though experienced hackers would 'shred' the evidence rather than simply deleting).

```
C:/RECYCLER
```

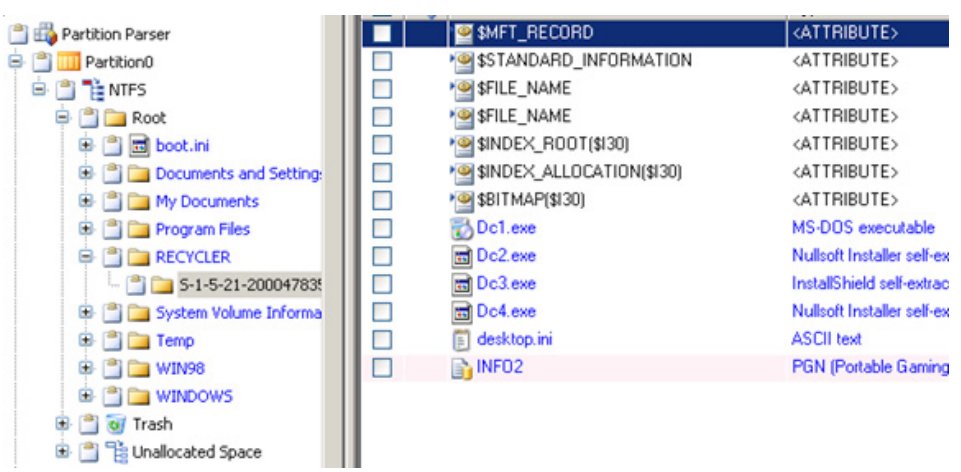


Figure 25. Recovering information from the recycle bin

Six deleted files were found in the Recycle Bin, some of these are hacking tools. [Figure 25]

DETERMINING THE FILES THAT WERE ACTUALLY REPORTED AS LOST (DELETED) BY THE FILE SYSTEM

The files that were found in the Recycle Bin were not actually deleted. They were just moved there. To determine the files that are actually deleted, go to the following location:

```
C:/WINDOWS/SYSTEM32/WBEM/REPOSITORY/FS/
```

In P2 Commander, you can notice a 'crossed out' icon in front of the file name, and the name itself is gray.

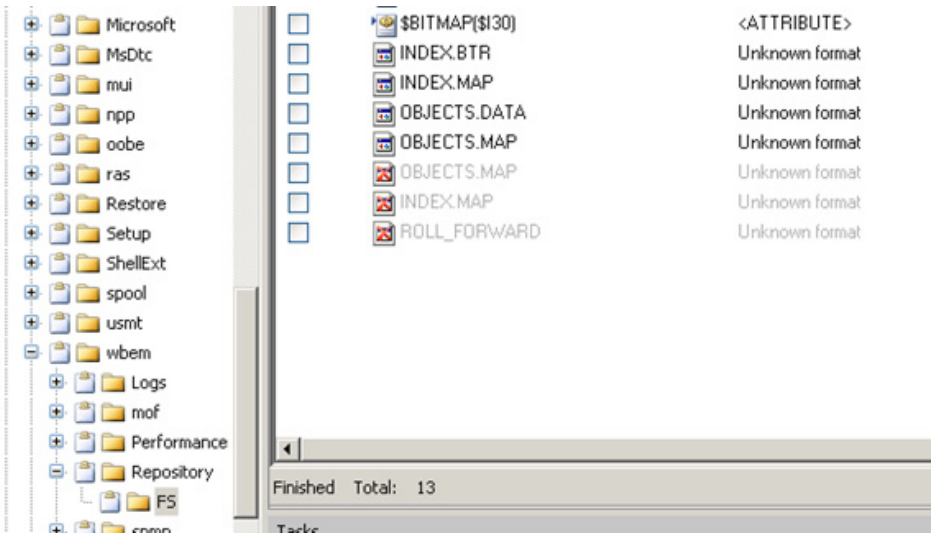


Figure 26. Determining the file reported as lost

This would tell you that 3 files are actually deleted [Figure 26].

CONCLUSION

All inculpatory or exculpatory evidence must be properly marked and collected by the examiner to be presented in a court of law. The *Chain of Evidence* must be properly maintained if the evidence is to stand in court. In simple words this means that information about who handled the evidence, at what time, for what purpose, for what duration, etc should be maintained. When not under examination, the evidence should be kept in the *Evidence locker* at all times. Access to the evidence is only granted to personnel who are authorized. The reason for all of this is pretty obvious: *Maintaining the integrity of the evidence at all times.*

This paper focused on a particular case to give you a 'feel' of what computer forensics investigations are like. However, it is in no way comprehensive enough to cover the variety of problems and complications faced by the investigator. The investigator may run into problems like:

- Limited knowledge: Forensics investigations require extensive knowledge of Operating Systems and their structure (for example, the Registry hives used to mine relevant information in this case require knowledgeable investigators who know where to look), programs, files, recovery of deleted files, etc. At certain points, an investigator may come across an unfamiliar Operating System and as a solution, may have to seek help from community experts who can tell where to look for certain information.
- Break in the Chain of Evidence or Evidence Corruption: This is a serious issue. If the Chain of Evidence cannot be established, the evidence becomes inadmissible. Also, without a proof of integrity, evidence is deemed corrupted.

Computers Forensics is a vast field of study and includes topics like *Processing Crime Scenes, Operating Systems and File Structures, Recovering Graphic Files and Defeating Steganography, Email Investigations, Mobile Device Investigations, Report Writing, Expert Testimony,* etc. However, it is definitely captivating (you get to solve crimes!!) and challenging – your knowledge will be tested to the max, as each case is unique.

PRANSHU BAJPAI

Pranshu Bajpai (MBA, MS) is an Information Security Researcher with a wide range of interests, namely penetration testing, computer forensics, privacy, wireless security, malware analysis and cryptography.

THE HIDDEN INFORMATION INTO CDRS (CALL DETAIL RECORD) CDRS ANALYSIS OPPORTUNITIES WITH SECURCUBE®PHONE LOG

by Nicola Chemello, Securcube

Nowadays the outlook is clear, everyone has at least one mobile device. Starting from the first mobile introduction, carriers and operators have realized the need to establish a clear system of logs to track users' activity and so create a reliable billing system. The CDR (Call Detail Record) is the document that summarizes all the mobile operations of a user.

What you will learn...

- To focus on CDR files (structure, contents)
- The purpose of CDR files within investigation and how to link them to other evidence sources
- How to find the right correlations between CDR files and investigation tips (with SECURCUBE®Phone Log)
- To take advantage of users' mobile activity, habits, movements to define a suspect's profile
- The chance of cell coverage track (BTS Tracker) within the investigation

What you should know...

- Basic knowledge about CDR files contents
- How CDR files can be obtained and utilized by investigators
- An idea of investigation work in progress
- The benefits of CDRs analysis and reports during the trial

Some of the available data are: date and hour of inbound and outbound calls, SMS, chats, connections, cell coverage coordinates and much more. Shown below an example of CDR structure (Figure 1). Data are collected with a row timeline logic. Each record of the row provides just one specific result, for example the date of a call. Results of the same typology are gathered together in columns. The theory is simple, but in practice the structure of a CDR file is not so easy to analyse. Data are compacted without spaces. The fast reading is an utopia. Just one file, maybe two to check can be laborious but workable. If the group of files is wide, an efficient search is no more possible. Despite that, why could be interesting to have a look and gain information from a CDR? The billing purpose is the carrier's activity, that's truth, but on the other hand a correct and authorized use of CDRs can be a great opportunity in the field of investigations too.

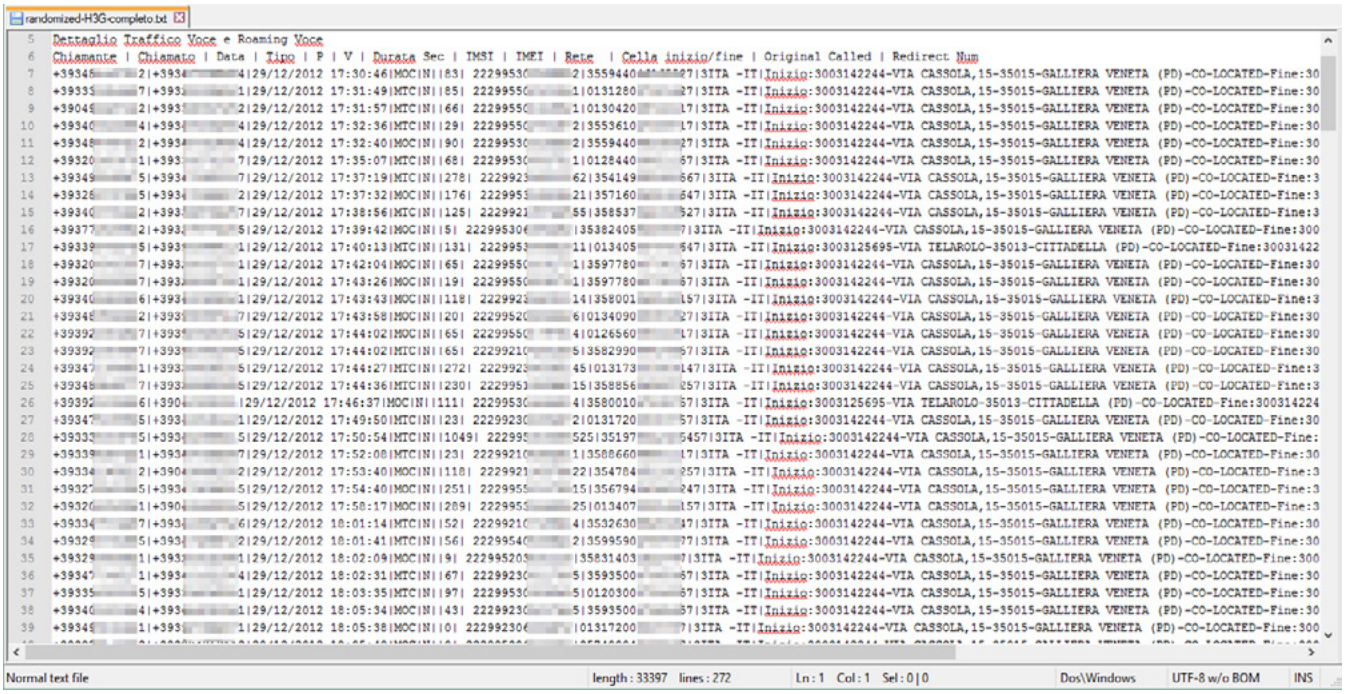


Figure 1. CDR example

Sometimes CDRs analysis is underrated but it can provide useful starting points and confirm or refuse hypotheses that come from other forensics tools and searches. In the past this operation was manual, long and complex. The huge amount of data couldn't receive a clear evaluation and the procedure was too much hard. Today, with the mobile globalization, there are millions and billions of records (just think of cell tower traffic of entire areas) and it is unrealistic to proceed with the CDR investigation without a support tool. The procedure automation increases the performance of the human activity and creates fundamental correlations starting from the simplest and most common cases.

It is necessary an intuitive graphical approach to manage millions of records simultaneously. Fast searches need to slim down the lists and underline the suspicious activity. All these investigator's wants become the key points functionalities to reach important results. With SECURCUBE®Phone Log, CDRs analysis includes the possibility of crossing mobile extraction, GPS coordinates and much more. How can the investigator obtain useful information hidden into CDRs?

As shown (Figure 2) the analysis of phone records can retrace lots of information. When the investigation starts, usually the range of hypotheses is wide. In general the suspect or the members of the gang are unknown or few details are available. The functionality Search on records of SECURCUBE®Phone Log offers basic and advanced filters of search to cross data and find the first correlations. Starting from the CDRs, that can show a user's activity, the cell area and its activities (it always depends on the file) it is possible to analyse and reduce gradually the amount of date till the right investigation idea. Higher is the quality of the filter search, better will be the result. The association of a cell area to a suspicious number or IMEI (identification mobile code), for example, can retrace common movements and provides an idea or a profile. An interesting feature is shown on the right side of the screen. After the search, the results appear and for each row it is displayed a summary of the activity (call, SMS etc.) with date and hour, geolocation and mobile phone details (brand, IMEI) that are information generally not included in CDRs but crucial. Save and export it to collect useful information for the next step of the investigation. This peculiarity is important most of all when the investigator, who is going to define the suspect's profile, doesn't have physically the device. In case of sequester the Police will exactly know what kind of device the suspect has to provide (to prevent mistakes).

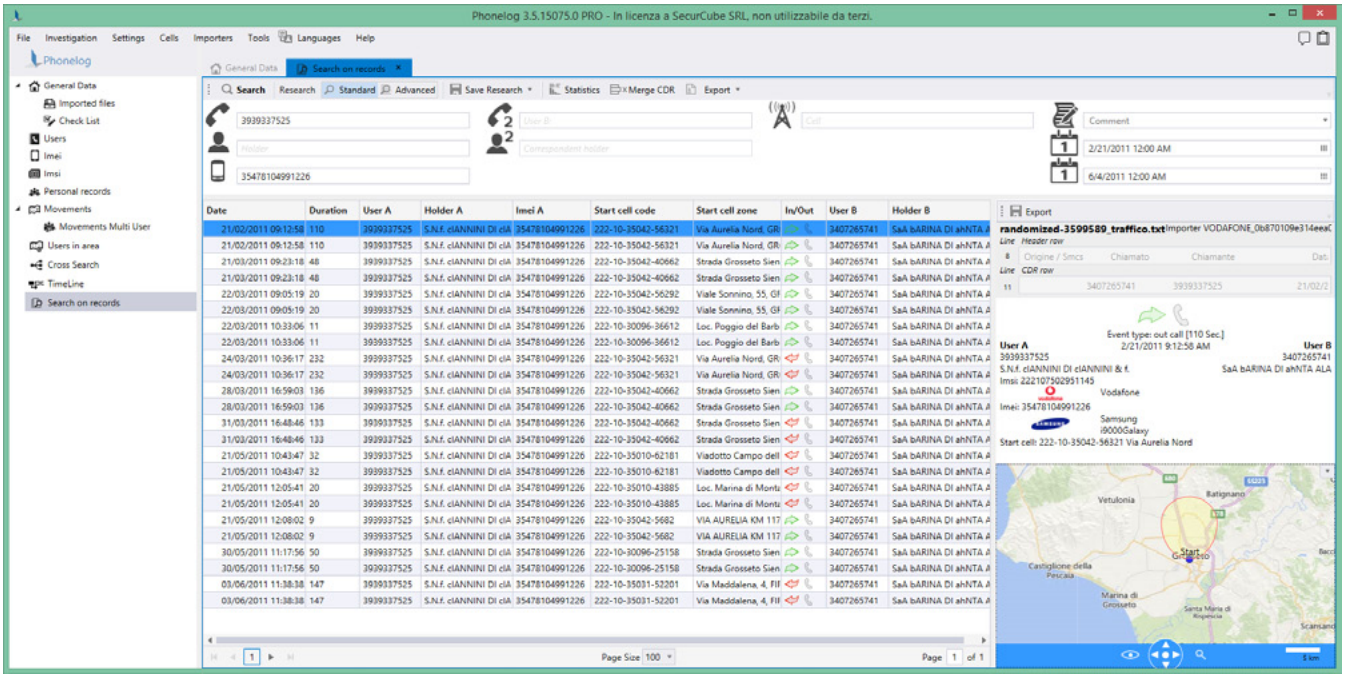


Figure 2. Search on records functionality

Let's think about a robbery case. The investigator has the CDRs of the misdeed place. He wants to know the suspects and the movements before and after the event. Firstly it is necessary to reduce the amount of data and separate people who live, work there (they obviously appear many times into cell CDRs). Anyway it must pay attention because it is probably that the suspects have observed the place for a long time before to act. These starting points can be easily supported by *Search on records* functionality. Gradually the number of rows will be reduced and by adding other data the scenario will be quite clear. In a second phase of the investigation, when the investigator obtains mobile phones and devices, it is useful to integrate the analysis with the extractions (photos, videos, chats etc.) to check exactly the suspect's profile and its probable guilt. Easy, fast and reliable. The time needed for the research is widely reduced and the tool can show exactly what the investigator is looking for.

During the investigation a hidden CDR information to consider carefully is the cell coverage measurement. The data can define the exact position of a subject, everywhere. Regarding the robbery mentioned before, it is possible to track and underline the potential way of escape of the suspect or the gang. Great and useful tool to obtain this information is the solution called Securcube BTS Tracker. The system can track, measure and verify cell coverage. These results can be imported and crossed with the work in progress CDRs analysis within SECURCUBE®Phone Log. BTS Tracker is able to identify proximity cells but also faraway cells detected but not hanged directly by the mobile device. Many times a suspect's profile is quite clear but the phone movements can question the hypothesis. As shown (Figure 3) on the map, cells coverage highlights the movements, escape route of the suspect. This result comes from log files provided by BTS Tracker solution to which can be easily added a second level of analysis regarding CDR activity. This track reduces the time needed for the investigation and assures to show important results to compare.

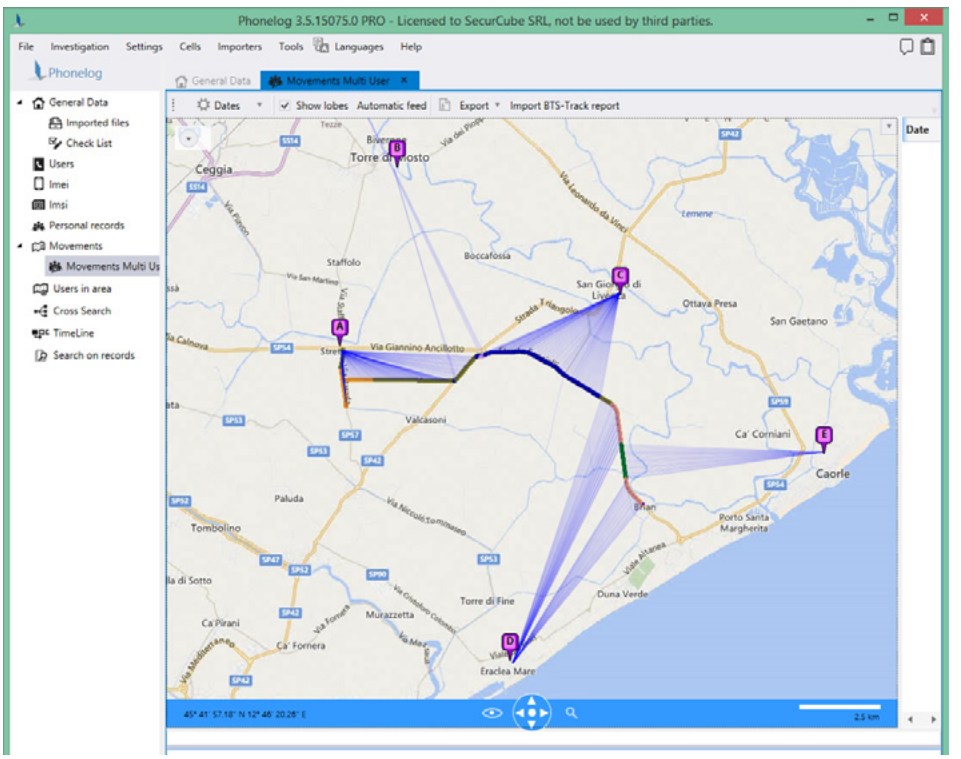


Figure 3. BTS Tracker measurements

Usually the investigator doesn't know exactly who made a crime. He has lots of data to manage and starting points. Similarities, suspicious or continued movements can represent the first step of a research in depth. With CDRs the investigation can change the way of doing analysis and find clear results to bring to trial. Nowadays a common situation is the stalker crime. The victim is constantly followed by a person who, most of all through the mobile phone, persecutes the victim's daily routine. This case is a great example of how a CDR can provide essential information to catch the suspect. The victim phone activity and movements have lots of similarities to those of the stalker. Anyway the stalker sometimes is unknown and to identify the right profile, it could be useful to cross the victim's CDR and cell CDR of the potential area of movement. There are lots of way to reach the stalker's profile and catch him. It depends on the case but basically a good way to proceed is, in fact, to find correlations with a CDRs analysis.

In support of patrols or stakeout, the CDRs analysis is the reliable way of doing investigation. Most of all, the data mentioned are out of any manipulation (files come directly from the carrier to the law enforcement agencies) and the result can be considered more affordable than other traditional and long procedure or suspect's tricks (fake chat, SMS cancellation and much more).

CDRs information has very important correlations with other sources of data. Just to mention the most important: reports from mobile forensics tools with detailed data regarding social network and chat activities like Facebook and Whatsapp; the highway traffic coordinates or data car movements and much more. The investigation can receive big improvement from the combined activity of these tools with obvious reliable results in the court of law.

SOURCE OF THE ARTICLE

- *www.securcube.net*
- *www.phonelog.it*

SECURCUBE

Securcube srl mission is to develop and continuously improve effective forensics software solutions for the law enforcement agencies. The purpose of SECURCUBE®Phone Log is to help the Italian and International investigators in the analysis of data phone arising from the telephone operators and to correlate them with other sources like phones features, tablets and GPS. Securcube srl has been founded in order to help law enforcement agencies to reduce the time needed for crime investigations. Securcube BTS tracker is the analyzer for cell phone coverage, useful to verify user presence everywhere. These innovative tools increase the performance and support the daily activity of all the law enforcement agencies.

DATA RECOVERY: BEST PRACTICES FOR SERVICE PROVIDERS

by Jonathan Yaeger

Computer service centers encounter failed hard drives. Data recovery can be a revenue source, but it must be wisely and carefully done. Well-intentioned but ill-informed efforts and practices can reduce or even ruin the prospects for successful recovery, and they can even expose the provider to legal liability.

As in medicine, the main precept of data recovery is "first, do no harm." The purpose of this article is to share basic data recovery practices intended to minimize the chances of harming a drive during the initial diagnostic and imaging (or copying) phases of the data recovery process.

The article will present general principles as well as specific examples.

THE LEARNING CURVE

Gaining expertise in data recovery is neither a quick nor easy process. There are many different drive makes and models; what works for one brand may not apply to another. Models from the same manufacturer can be markedly different in construction and operation. A huge amount of technical information and details must be absorbed and mastered to become even modestly adept.

Hard drive manufacturers are frugal about releasing technical details of their products because they want to safeguard their intellectual property and trade secrets.

Good drive diagnostic and firmware tools are expensive. Comprehensive training on how to use them is also generally expensive, when available. Most third-party data recovery training classes provide only a cursory introduction; there is no substitute for hours of hands-on experience.

Although much of what data recovery technicians learn and use comes from trial and error, *it is important not to get one's education at the client's expense*.

We receive a lot of drives that have been worked on by other technicians. A fair number of those have been damaged or ruined – along with the chances of recovery – by mistake. Incorporating a set of best practices for hard drive data recovery can improve the outcomes and be beneficial to all concerned.

GENERAL PRINCIPLES

- *Recognize your own limitations. A customer's best interests should be top priority.* Resist the temptation to experiment or gamble with a client's data – you can make things much worse! If you don't have the knowledge, equipment, experience and confidence to tackle a particular recovery job, then simply *stop*. It is better to pass on a service opportunity than to ruin forever a client's chances of getting back data.
  - Note that recovery pros sometimes sub out difficult jobs to others with specialized expertise, if it will ultimately benefit the client.
- *Proper diagnosis is essential.* You can't fix the problem unless you are sure what it is. However, you can make things worse by randomly trying things without understanding the nature of the failure.

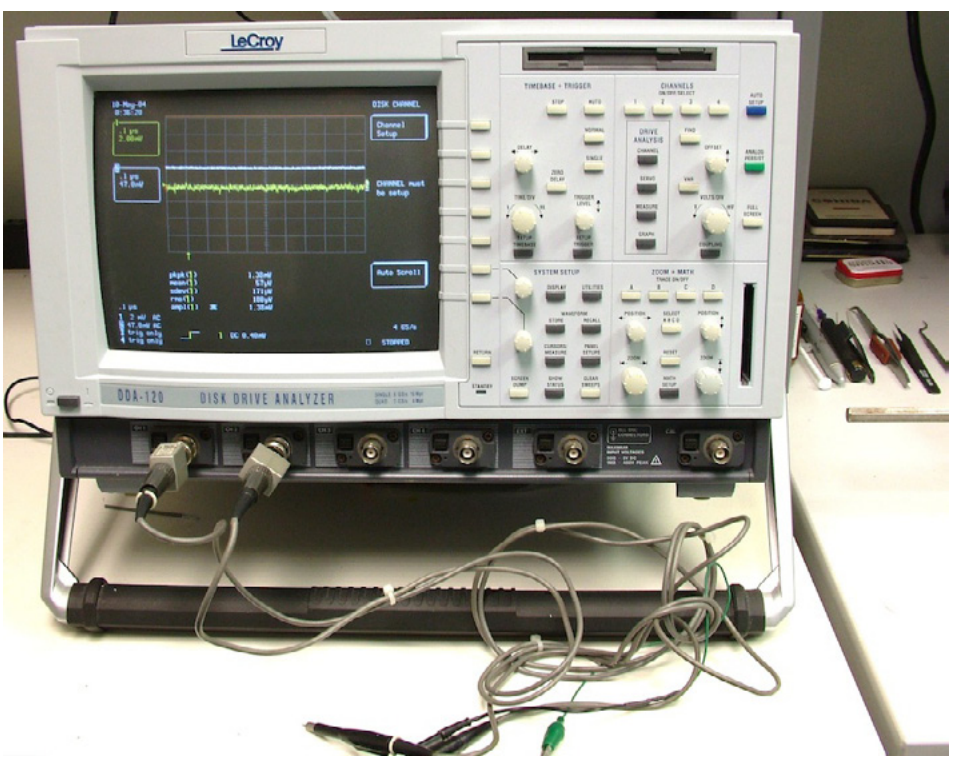


Figure 1. Data recovery requires the proper tools

- *If you don't have the proper tools, don't try to improvise*. If you must open the sealed chamber of a hard drive, do it only in a certified clean environment, which isn't a kitchen, bathroom, or garage.
- *Don't do something that can't be undone later on*. Keep a path open to the previous step so you can restore the drive to the same condition as you received it, if possible.
- *Document and label everything*. Record every step that you take in a recovery effort. It will help you or the next technician later. If you take good notes, you can build a library of "how to" steps for the next drive with similar issues.
- Put a label on each item of clients' property, including cables, to make sure that they receive all of their property back and that it is not commingled with someone else's. Label the drive's PCB to be sure that the original is restored if swapped.

Figure 2. Label everything

- *Try a new procedure on a test drive first*. Sometimes a new process or procedure will ruin a drive. Don't let it be a client's drive.
- *You can't use a software tool to compensate for a hardware problem*. If a drive is failing, trying to copy the data without fixing the underlying hardware issue is a recipe for disaster; the drive may fail and become unrecoverable. Learn to recognize hardware failure patterns, and when to stop what you are doing.
- *Look under the streetlight*. Use your five senses to examine a drive prior to working on it. A problem might be obvious if you take the time to look. A misdiagnosis not only wastes time, but also can put data at risk.
- *Treat all data as confidential data*. The client's data is valuable.
- Do not expose it to security risk or loss. After a recovery is complete, securely wipe any media used in the process and confirm the erasure.
- *Be honest and ethical*. Of all the "best practices," this is by far the most important. The "Golden Rule" certainly applies.
    - Doctors have learned that the best policy with patients is to be candid and forthright, and so it is with data recovery.

INITIAL EVALUATION: EXTERNAL APPEARANCES

The first step in the recovery process is to try to get a history from the client, i.e., what happened when the drive failed? Was it dropped? Was there a power outage? Clients may not have additional information, but when they do, it can be invaluable.

What do your senses tell you? Is the lid bent at a corner? Are there other signs of physical damage that suggest the drive had been dropped or abused?

The practice of "looking under the streetlight" means that you should take time to study a drive before doing anything. You may find obvious as well as hidden problems that will affect the diagnosis and dictate the course of the recovery. Overlooking a problem can result in wasted time and, sometimes, in loss of data.

EXAMINING THE PC BOARD

Examine the PC board area, especially with laptop hard drives. Is there any sign of fluid contamination or corrosion on the board? Does the drive smell like coffee or wine? Is it sticky? If so, there is contamination and likely PCB damage.

A drive that has been under water should be opened in a clean room as well, to check for fluid contamination on the inside. All contamination must be removed before the recovery process can commence.

Are there burned areas on the circuit board?

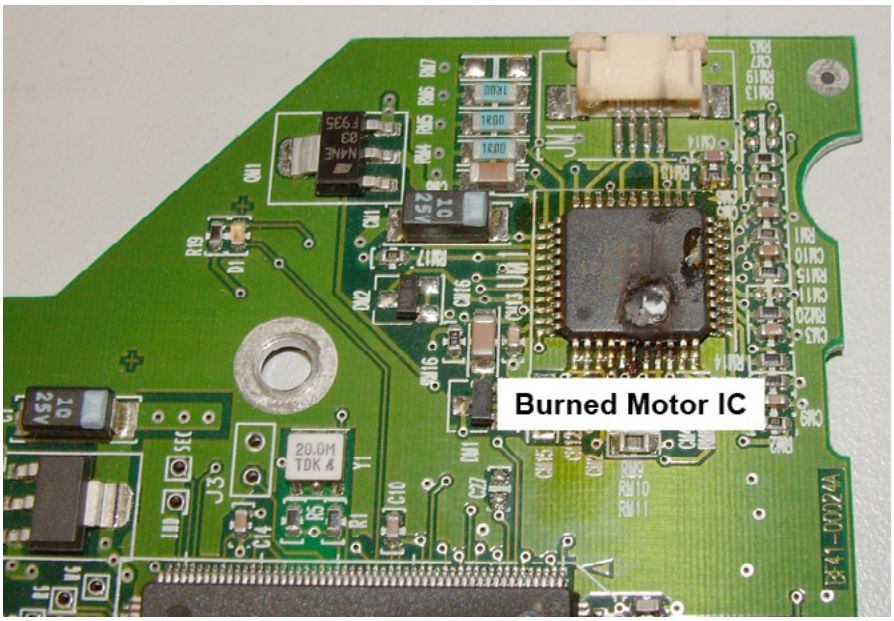


Figure 3. A burned motor integrated circuit

Figure 3 shows a burned motor chip on a PCB of a drive that – no surprise – did not spin up. Other PCB-related problems besides corrosion and contamination include damaged or defective parts.

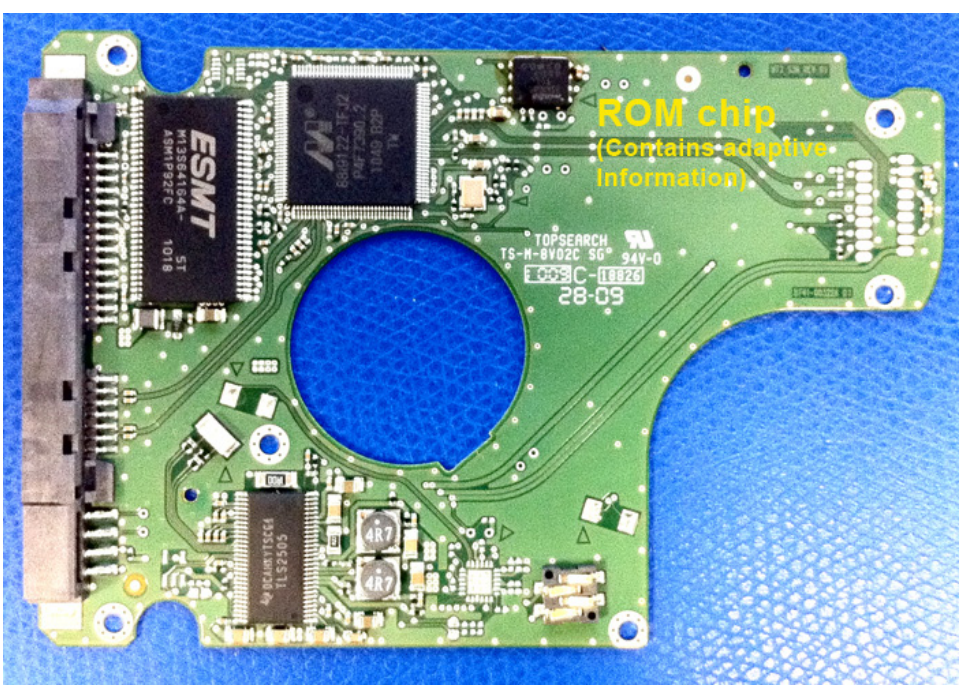


Figure 4. A PCB showing a ROM chip.

Most hard drive circuit boards contain unique information about the particular drive, either as part of a *ROM* (usually an *EEPROM*, or Electrically Erasable and Programmable Read-Only Memory circuit or "chip"), or embedded into the main processor. This unique information is called adaptive information or firmware.

Figure 4 shows a laptop PCB and the placement of the ROM on the board.

RULE: *You can't just replace a damaged PCB without transferring the adaptive information to the replacement PCB, a process that requires special equipment. The days of simply swapping PCBs are largely over.*

Sometimes service centers will swap a PCB and not tell the customer, or sometimes they discard the bad PCB. This makes future recovery efforts much more difficult – and sometimes even impossible.

Please note that recovery of Toshiba laptop drives and the newer Seagate drives in the F3 series may not be possible without their original PCB adaptive information.

RULE: Best practices dictate returning the bad drive with the original PCB attached, even if damaged, if the data cannot be fully recovered.

BEFORE APPLYING POWER TO A DRIVE

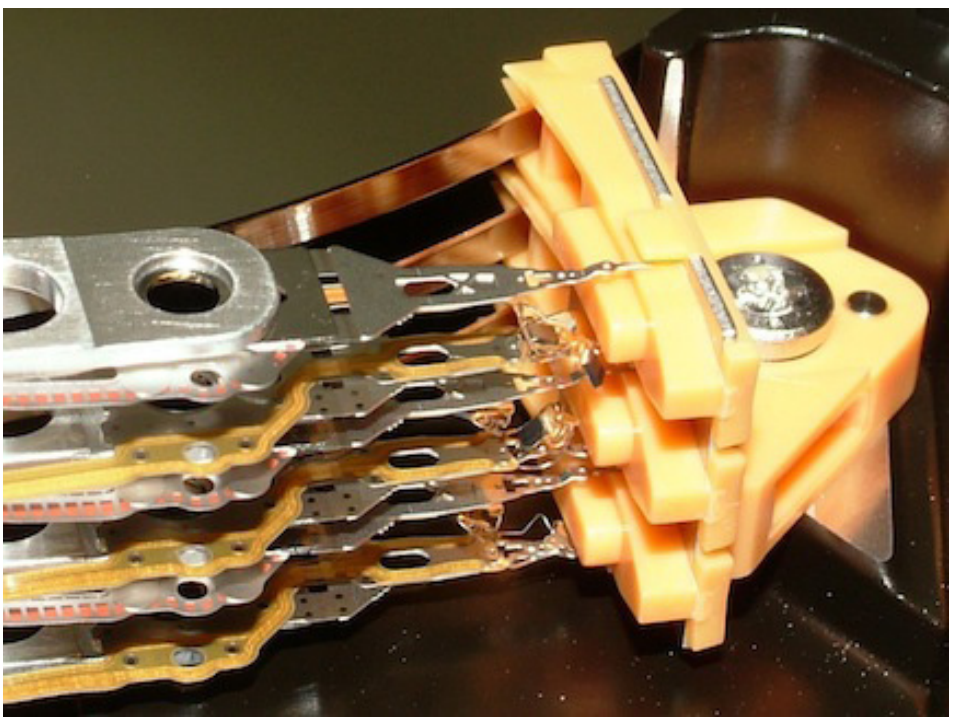


Figure 5. Damaged heads in a parking ramp

RULE: Do not apply power to a drive that you know or suspect has been dropped or subjected to shock! A drive that has been immersed in liquids or otherwise contaminated also shouldn't be powered. Read on to learn why.

Hard drives are amazing collections of high-tech mechanics, electronics, and internal software programs (also called *firmware*), but they are also very delicate machines.

During operation, tiny read-write heads fly over the data platters. There is a very tiny gap between the heads and the platters. If a drive receives a physical shock, the heads may crash into the platters, resulting in damage to both the heads and the platters. Sometimes damage may occur to the delicate heads if the drive is dropped when powered off. Figure 5 shows a set of mangled heads sitting in the parking ramp.

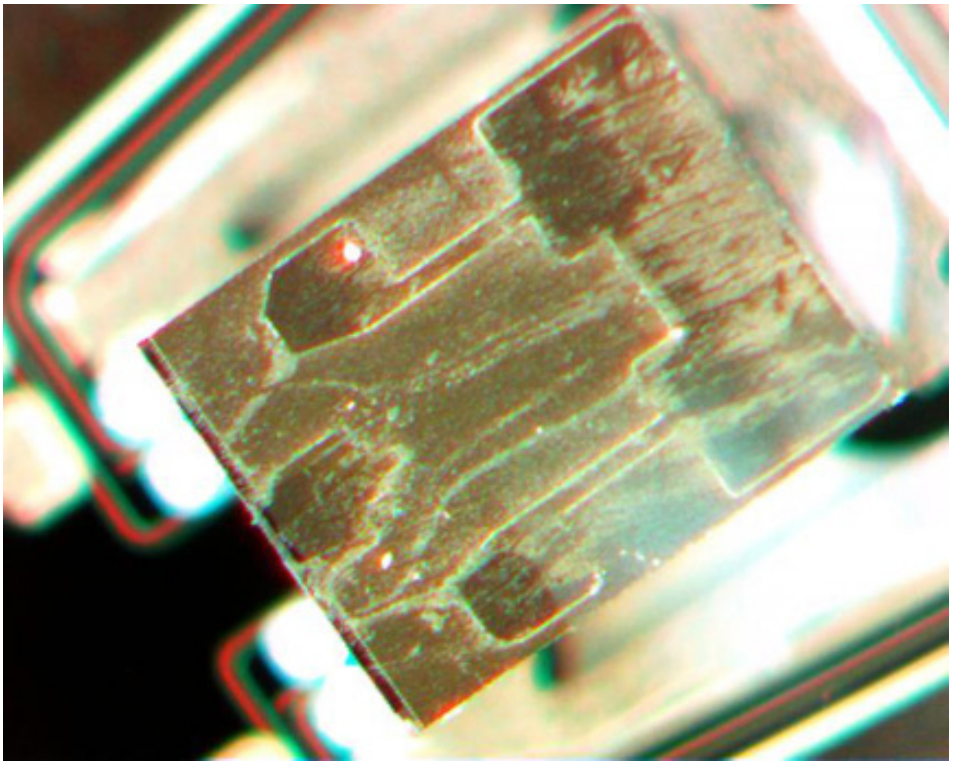


Figure 6. A scratched and contaminated head (magnified)

Figure 6 shows a close-up of a head damaged by a head crash. The head has scratched the media, and some of the drive's magnetic media is now tiny particles of metallic dust. Damaged platter areas are unrecoverable.

As soon as the drive is turned on, the deformed heads will move onto the platter and act like sandpaper or tiny knives, scraping data away along with the chance of recovery.

The debris kicked up by the process acts like large boulders randomly dropped onto a highway, meaning more crashes will follow. Particles larger than 0.25 microns cannot pass through the air cushion gap between the head and the platter.

For perspective, the diameter of a human hair is on average about 80 microns, which is 320 times larger.

Figure 7 shows what the drive will look like if it is operated with crashed heads. In this particular case, the data is gone for good; the client's data is "in the filter."

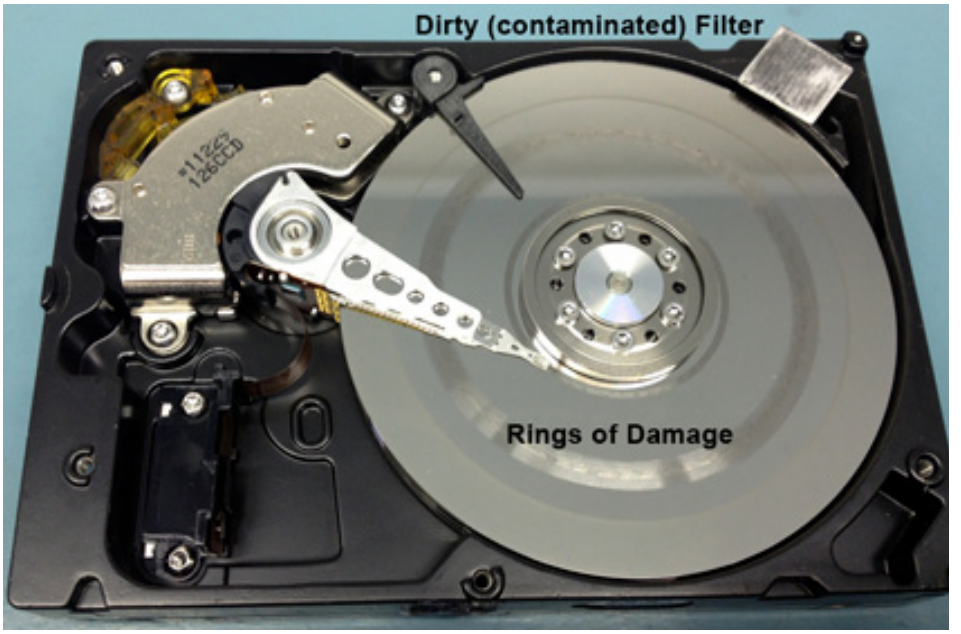


Figure 7. A hard drive with a head crash and media damage

Drives with slight media damage often can be recovered, though sometimes only partial recovery is possible; it depends on the extent of the damage. Working with media-damaged drives is a specialty, and some data recovery companies produce better results than others.

At this point, it should be clear that platter and head inspection are an important diagnostic part of the data recovery process, *but only in a true clean room environment*.

OPENING THE SEALED CHAMBER OF A HARD DRIVE

It is never a good idea to open up a hard drive outside of a clean room environment. Why? Because, as previously noted, it only takes a small particle to cause a head crash, and if you open a drive outside of a clean room environment, you *will* contaminate the drive and increase the chances of *premature failure* or *no recovery.*

Opening a crashed drive in a clean room can contaminate the work area, too.

Sometimes removing the lid of a perfectly good drive can also contaminate the sealed chamber; debris often accumulates around the lid's seal.

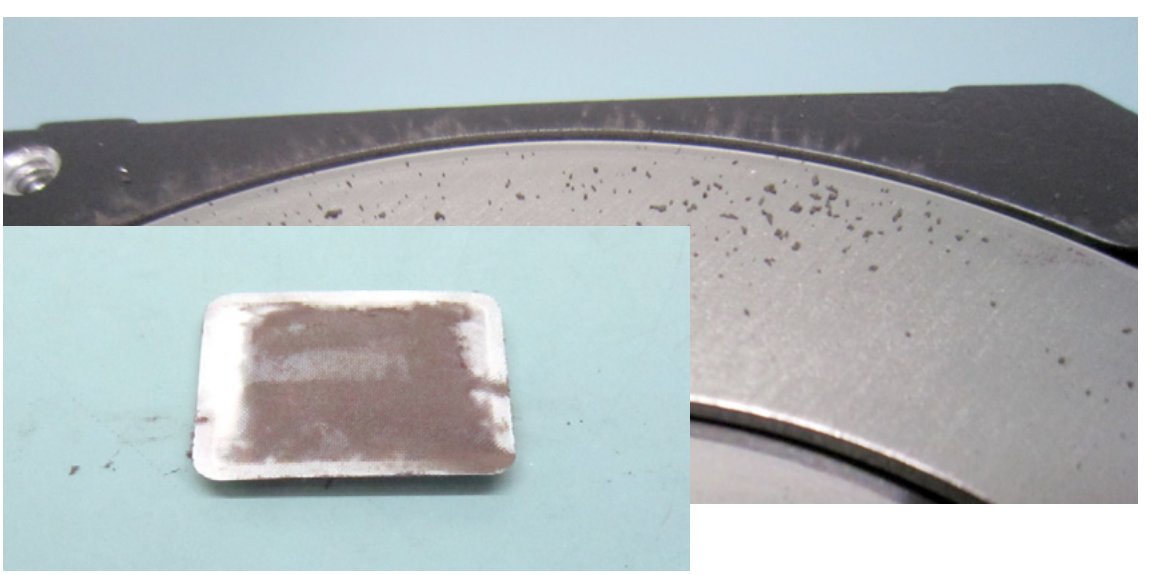


Figure 8. Close-up views of drive contamination

Another reason to not break the seal of a hard drive? If you are not authorized by the manufacturer to do so, you will *void the warranty*.

Resist the urge to "peek." Send the drive to a professional if clean room service is indicated. Many professional data recovery firms charge little or nothing for inspecting a drive prior to recovery.

APPLYING POWER TO A DRIVE

The temptation is usually unavoidable, but a dropped drive should not be powered up without a clean room inspection of the heads and media.

Ask your client if the drive was dropped. Unless you have a clean room and the experience and expertise, it's a good idea to refer dropped drives to qualified data recovery labs.

You may safely assume that the client has attempted to access the drive until a point of defeat was acknowledged. *Sometimes it is just a matter of a few seconds* of operation of a mechanically failed drive that later results in a difficult or impossible recovery job.

Once that you are satisfied that a drive is safe to power up, listen carefully to it. Drives that make unusual noises, especially scraping and high-pitched sounds, should be shut off immediately. Unusual drive noises often indicate damage in progress. *Whenever there is uncertainty, always err on the side of caution.*

IMAGING A DRIVE

A fundamental best practice of data recovery is to make a copy, or *image,* of the defective drive, then do the file recovery from the image. There are good reasons for this practice:

1. A failing hard drive may have a limited number of hours of operation left before it fails completely. It's best to try to get the data off a drive as quickly as possible, and with minimal damage to the original drive.
2. Sometimes more than one file recovery algorithm is required for optimal results. An image allows multiple recovery passes, whereas sometimes you get one shot with a failing drive.
3. The drive image is an archive of the original data and is often the only useful one.

It is important to understand how hard drives process read errors and perform other background tasks during normal operation.

Hard drives incorporate *housekeeping routines* into their firmware. These run in the background and are invisible to the end user. One standard routine is *defect management*, in which data in weak or failing sectors are moved to another region of the drive. The bad sectors are "marked out" and added to the *grown defect list*, also called the *G-List*.

Another housekeeping function is regularly updating the drive's *S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology)* logs.

These logs keep track of *attributes* of a drive's performance; examples include the number of times the drive is started up, the inability to read sectors, and updates to error logs. These attributes are expressed in terms of "threshold exceeded" and "threshold not exceeded" values, which can provide an early warning of a drive's impending failure (Figure 9).

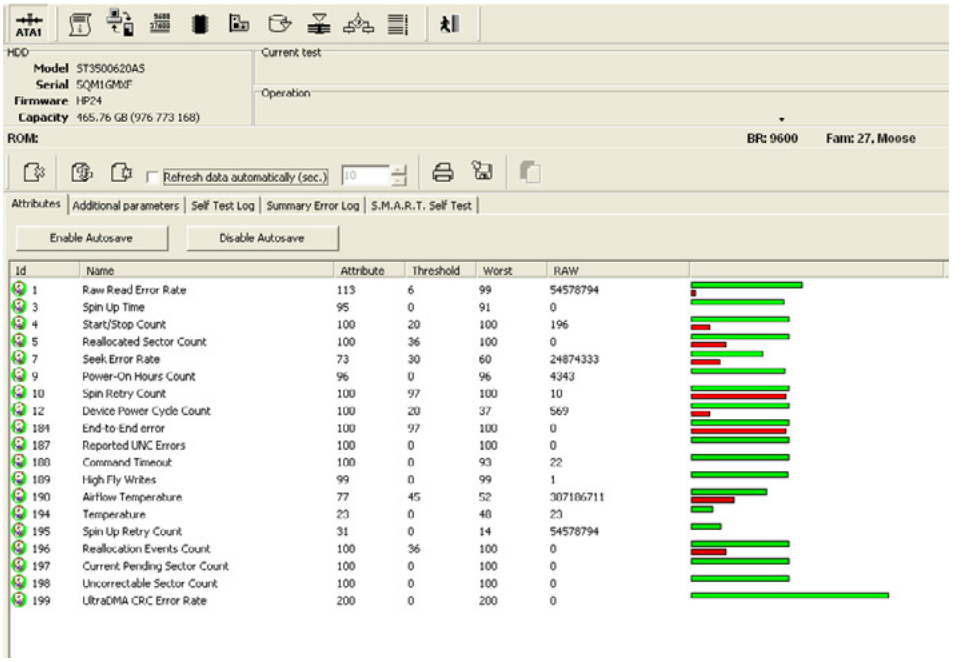


Figure 9. S.M.A.R.T. attributes display

Hard drives often fail in a cascading mode. For example, a drive's head might become dirty and fail to read or write data. Good sectors will be reported as bad, and the drive will try to move the data to another sector (i.e., through reallocation). If it cannot successfully write to the new location and verify the written data, it will report the new sector as bad, too. Each time it moves an allegedly bad sector, it will update both the G-List and S.M.A.R.T. logs. *The drive suffers a vicious cycle that interferes with imaging and eventually can lead to complete drive failure. Therefore, if the bad sector and S.M.A.R.T. management processes can be turned off during imaging, the chances of a successful and more complete image are greater.*

SOFTWARE VERSUS "HARDWARE" IMAGING

Hard drives may be duplicated (or imaged) by computers using software programs for that purpose. Drives can also be copied by *hardware imaging*, using specially designed circuit boards or dedicated machines.

Some hardware imagers have features that greatly surpass software-only capabilities. They can:

- Disable defect management and S.M.A.R.T. attribute processing;
- Permit multiple recovery passes on a failing hard drive;
- Adjust the speed and "depth" of the reading process by adjusting the types of resets, number of attempts to read each bad sector, etc.;
- Build a heads map and image by head;
- Turn off imaging or power, jump to a different head, skip a pre-assigned number of sectors, etc. upon programmed conditions;
- Have dedicated imagers that make faster imaging (versus PCs running software);
- Support file imaging by MFT or other directory structures.

According to Serge Shirobokov of DeepSpar, Inc., *"Regarding the software vs hardware imaging section, the biggest difference between the two is probably the fact that hardware can automatically reset drives on timeout and software just has to wait . . . If a read command falls on a bad area, hardware tools can limit the damage from that by cutting the processing time down to a few hundred milliseconds (then resetting the drive), while software must wait the full few seconds for a drive to come back with an error. This alone makes hardware imaging multiple times less damaging."*

Because most drives presented for data recovery are unhealthy by definition, using a hardware-based imaging solution is generally considered a best practice.

When software imaging, it is a good idea to use a write blocker with software imaging tools, because a PC may try to initialize a drive and can overwrite important boot or partition information. Write blockers permit reading from a drive, but block attempts to write or change data. Most are hardware devices, but some use software. Note that a write blocker usually does not prevent a drive from updating the S.M.A.R.T. or the G-List.

Unix's "dd" command-line instruction is sometimes suitable for making a drive image because it can copy sectors that are not part of the active directory, including "erased" files.

On the other hand, DOS command-line instructions such as XCOPY are only good for copying files that are listed in a directory. If the directory is corrupted, or files have been erased, XCOPY will skip those files.

There are a number of "off the shelf" utility programs for disk imaging. Software imaging solutions work well with *healthy* hard drives. However, they are limited, and possibly harmful, when working with problem drives such as those with many bad sectors, firmware issues, or failing heads.

As noted, the best way to work with a defective drive is to turn off the drive's defect processing (called *sector reallocation*) and to disable the S.M.A.R.T. logging function. This reduces the chances that the drive will self-destruct during the imaging process.

However, turning off sector reallocation requires a vendor command, i.e., code specifically written for a particular drive, model, or series. Some of these commands are proprietary and are not generally published. A viable software solution would have to incorporate the vendor commands and have a means of matching the commands to the drive to be imaged.

For the tech-savvy: The BIOS of most PCs offers a menu choice to turn off S.M.A.R.T. notifications of impending drive failure, but that feature does not affect the internal S.M.A.R.T. operations of the hard drive.

A standard ATA command to disable a drive's S.M.A.R.T. operations is described in section 7.52 of the T13 ATA standard, which states: "This command disables all S.M.A.R.T. capabilities within the device including any and all timer and event count functions related exclusively to this feature."[6]

The command is *B0h with a Feature register value of D9h*

WHEN TO STOP IMAGING

Remembering that a main precept of data recovery is "first, do no harm," it's critical to recognize when to stop, or when continuing is likely to do more harm than good.

Stop imaging when:

1. The drive makes clicking or other "unhealthy" noises;
2. The drive fails to come ready, or aborts;
3. The drive exhibits signs of cascading failure, i.e., one or more heads that were working when the process was started begin to fail.

A "gray" area is when there is a high unread or bad sector count. Sometimes it is hard to tell if this is due to media degradation (bad sectors), logic board failure, or another cause.

A head may spontaneously fail during the image process. The drive may be able to finish imaging the data on the remaining heads, or it may "crater" and cause a ring of damage and widespread contamination. At this point, having a clean room and the appropriate tools might save the recovery and a client's data.

RAIDS

A RAID originally stood for a "redundant array of inexpensive disks," which later became "an independent array of independent disks." Nonetheless, a RAID is a storage system that has more than one drive. RAIDs have level classifications, such as RAID 0, RAID 1, RAID 5 or RAID 10. The Wikipedia entry for RAID gives a good overview: *http://en.wikipedia.org/wiki/RAID*.

Figure 10. Configurable four-drive RAID array with front panel removed

ARAID 0 consisting of two drives isn't redundant at all and, as such, is mis-named. Both hard drives have to be recovered to get useful data from a RAID 0.

The redundancy feature of true RAIDs permits one or more drives of the array to fail and still retain functionality. The RAID senses the failure and adjusts the reading and writing of data accordingly.

For example, a single drive from a three-drive RAID 5 can fail. If a technician replaces the defective drive with another, the RAID "knows" – or prompts – the user to rebuild the RAID using the new drive. However, if two drives fail in the RAID 5 configuration, data recovery is required; the RAID can't rebuild from only one good drive.

The capability of automatic or semi-automatic RAID recovery after a drive failure is a great feature for the client, but if it's not completely understood by the technician, "experimenting" with a failed RAID array can compromise or even defeat subsequent data recovery attempts. It's easy to get into trouble if you don't know what you are doing.

BEST PRACTICE RULES FOR RAIDS

- If you don't know precisely what you are doing, *stop* what you are doing.
- Drives should *never* be swapped around and placed in different positions in a RAID.

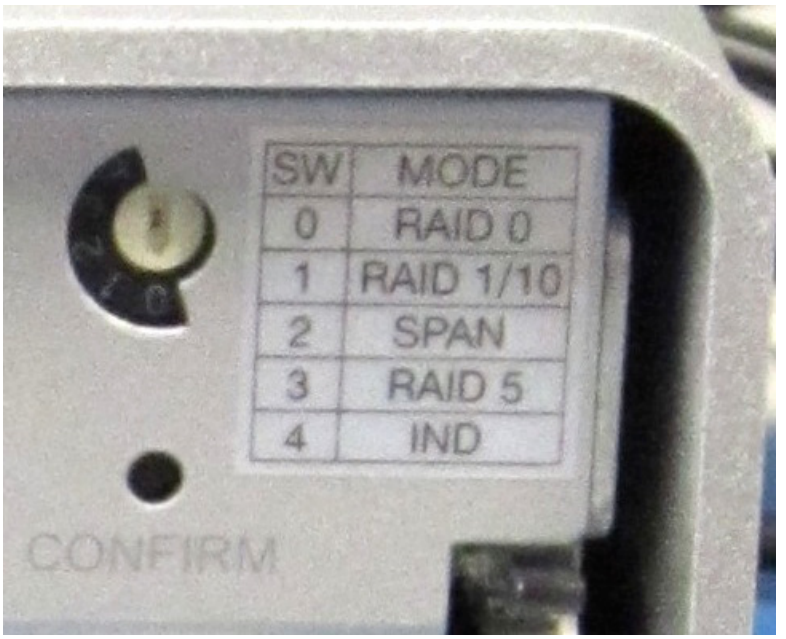


Figure 11. A RAID configurable switch

1. Figure 11 shows the configuration selector for the above RAID, which allows it to be set up in different RAID levels or modes. *Never change the mode on the fly*. This will cause severe data corruption.
2. *The best practice* when working with a problematic RAID is to make or clone copy of every drive, then *work on the copy only*. This will preserve the original RAID in "as received" condition, using the general principles of "do no harm" and "don't do anything you can't undo later."

POST-IMAGE PROCESSING

Generally, data recovery software (to rebuild files and folders) is run on the image to try to recover lost files, rebuild directories, etc. Another reason for running recovery software, versus simply copying data, is that most programs fix permissions issues with the recovered data set. There are several data recovery programs, and each seems to have a particular set of strengths and weaknesses. There is not a single program that is consistently the "best."

GOING FORWARD

Try to incorporate the General Principles (listed at the beginning) underlying best practices of data recovery. Strive to always do what is in the best interest of the customer, whenever there is a choice, and know your limits. Data recovery is an art as well as a science, but there is no substitute for knowledge acquired through experience.

JONATHAN YAEGER

Jonathan Yaeger is the owner of Data Savers, LLC, a leading data recovery firm in Atlanta, Georgia, since 2005. Data Savers, LLC offers high customer service and affordable recovery rates (www.datasaversllc.com). After working for E-Tech in 1980 as a technical sales manager for energy conservation products, Yaeger started Atlanta Technical Specialists, Inc. (ATS) in 1987. ATS, which was sold in 1999, offered PC sales, manufacturing, and component-level service. He has also been involved in a number of high tech ventures including AppForge, Inc., PhysicianAssist, and Atlanta Mac Service. Yaeger holds a Bachelors Degree from Emory University. He is an ative member of the North Atlanta Rotary Club, and resides in Atlanta, GA.

Contribution:

1. "Forensics and Hard Drive Data Imaging & Recovery. The Perils and Pitfalls of Working with Defective Hard Drives" –> Find it in Special Data Recovery Issue which was published in May 2013.

Data Savers, LLC

(770) 939-9363

jon@datasaversllc.com

DIY: CYBER BLACK BOX DECRYPT & MODIFY TRAFFIC ON-THE-FLY

by Dennis Chow, MBA, Senior Information Security Engineer

This article demonstrates how users can still be susceptible to their secure connections being monitored or modified without their knowledge on-the-fly with a device that a malicious person can put into the network. Legitimate use cases can be for troubleshooting or basic traffic monitoring for security purposes.

Other purposes can easily lead to compromised credentials or even unauthorized actions on behalf of the user. Read on to find out how you can build a DIY (Do It Yourself) Cyber Black Box that will decrypt SSL sessions and modify traffic at your will.

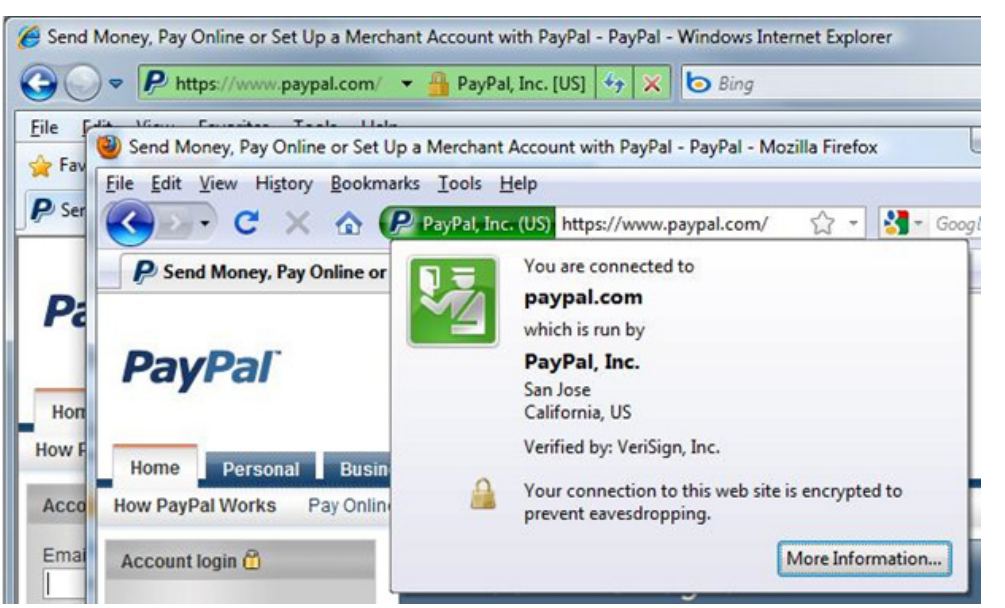


Figure 1.

PART 1
Summarizes good practices and how to detect and defend a potential black box on the network for any user.

PART 2
Shows you how to setup your own “Cyber Black Box” using common and readily available tools.

PART 3
[Screenshots] Decrypted SSL session passwords and on-the-fly modification of a chat session without the user knowing.

Trolls beware: This article is also meant to be short and concise without going into a huge amount advanced technical detail with the assumption that you know some of these concepts for the second piece of this article.

Disclaimer: The tutorial and technical information you see here is designed for educational and awareness only. Do not use this knowledge for unauthorized or illegal activity. Testing was conducted in a closed lab environment.

PART 1: WHO DO YOU TRUST?

As an consumer, pretty much everyone has some form of a login and password online: banking, email, school, work VPN, etc. Remember when they always say look for the padlock icon and or ensure your browser is pointed to “https” because it’s secure?

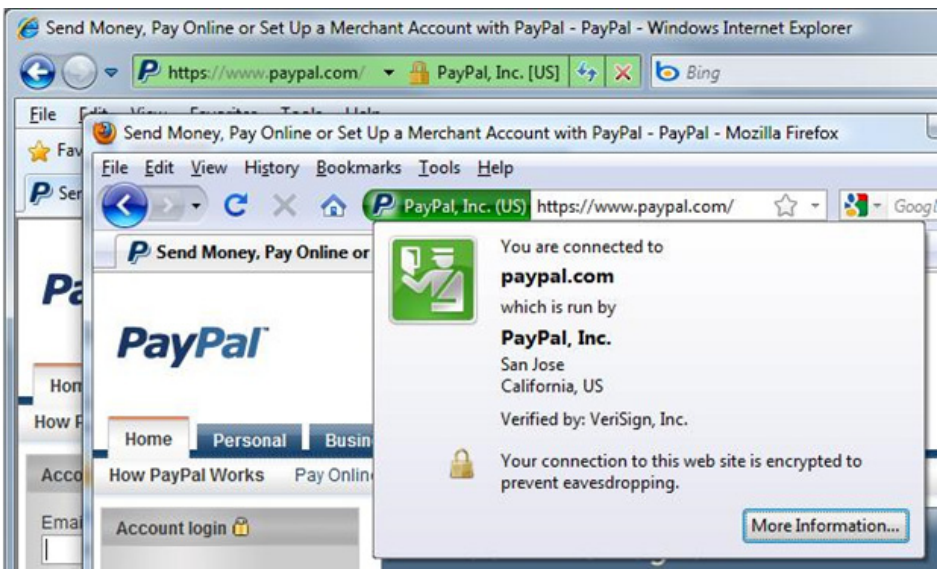


Figure 2.

And of course… someone should have also taught you to mind your browser’s warnings, right?

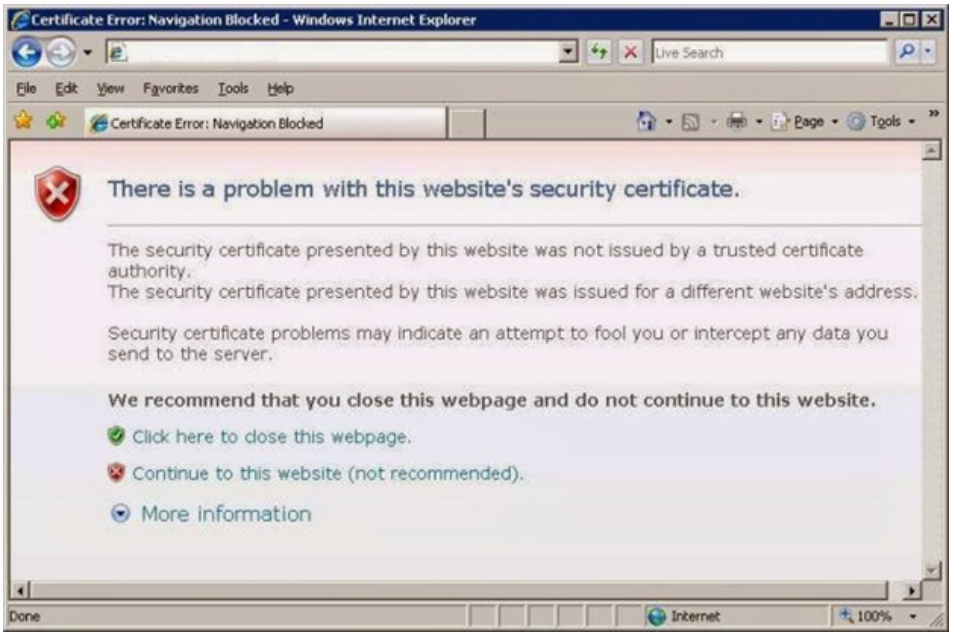


Figure 3.

Some people just click on the continue button anyways, and some people have just learn to ignore it. Have you ever read through it? It's basically saying that the identity of your website cannot be validated because the trust chain is broken. Huh? The SSL certificate trust is a hierarchy system designed to both encrypt and verify the identities of entities online so that your browser and other applications can know whether or not to proceed with connecting to it. When you see problems with a website's certificate of a website, it's almost always in your best interest not to continue to the website.

This is because someone could have place themselves electronically between you and the website or service that you're trying to access. Security professionals refer to this at MiTM (man-in-the-middle) based attacks. They essentially act as a proxy for you, and not in a good way. Think about how an interpreter service works, you want to communicate with another person; and that person relays your message to the end receiver. How they relay your message and what they tell the receiver could be changed or modified. The same goes in reverse.

WHAT CAN SOMEONE DO IN MITM?

They can retrieve your passwords, logins, cookie (session token), and many other items that was intended to remain private. In addition, in real time, they can modify any message that you send to how they want the other side of your connection to send or receive messages.

DEFENDING YOURSELF

Here are some useful tips to consider when you're surfing or connecting to anything in any environment, including your workplace: If you start seeing certificate warnings from your browser: Do not continue through SSL/TLS Certificate warnings. Call your local IT or Information Security team to investigateVisually check areas around your desk or around general "network gear" for any newly added or modified configurations and ensure you know what changed prior to powering anything on

If in a public connection, consider using an IPSEC based VPN such as VPN Gate to add an extra layer of protection to your connection or if using an existing SSL VPN, ensure the client performs certificate validation.

For IT Professionals: Always keep inventory and control on what changes in your environment physically and logically. Look for signs of interface flapping, followed by changes in ARP traffic, user complaints of connectivity behavior changes, and others.

For IT Security Professionals: Investigate net flows, observe TTL changes, monitor network traffic on multiple segments whenever possible, and other logging information from your SIEM with IT as your partner.

PART 2 CREATING AND USING THE CYBER BLACKBOX

In this tutorial and tech brief, we'll create a transparent "brouter" which forwarding is across a L2 bridge and then L3 and L4 traffic is routed internally to various applications as a pipe, parallel, or in multiple pipes to manipulate, decrypt, record, and generally spy on traffic. Let's get started.

Setup: My test box began with an Ubuntu 14.x Desktop edition install, the box I chose was a small form factor case on a spare computer I had laying around. Make sure it has 2 or more NIC's in it so you can have traffic flow 'in and out' of the box. If your NIC's do not have Auto MDIX or are not Gigabit NIC's you will need a crossover cable so you can put it "inline" something like your firewall and switch. Creating the bridge: Create the bridge by pairing 2 NIC's. Either use the built in network manager via your GUI or do it the command line way, it doesn't matter, example configuration provided below. Easy and lazy way: Open up Network Manager at the top right and add a new connection type, use the menu to select "Bridge" type of connection.

Edit the bridge connection you made and add in the 2 NIC's you wish to utilize to put your box inline somewhere, name it whatever you want. *Note: I turned off STP in this environment because you could trigger a switching loop if your bridge suddenly becomes the "root" bridge in the STP tree. I also set my forward delay to 3 seconds vs the default because I just don't feel like waiting on connections to converge on a lab network. Next, set either a manual IP or DHCP address to your bridge. Note, your bridge interface does NOT need an IP address if you have a separate management interface with an IP address to access the box. However, in walk through we're only using 2 NIC's "in and out" and I didn't feel like adding a default route.

Edit your connection under the general tab and ensure that both boxes are checked so your link stays up on reboot. Do the same and ensure the boxes are checked on all slave interfaces. In our case, the in and out only has eth0 and eth1.

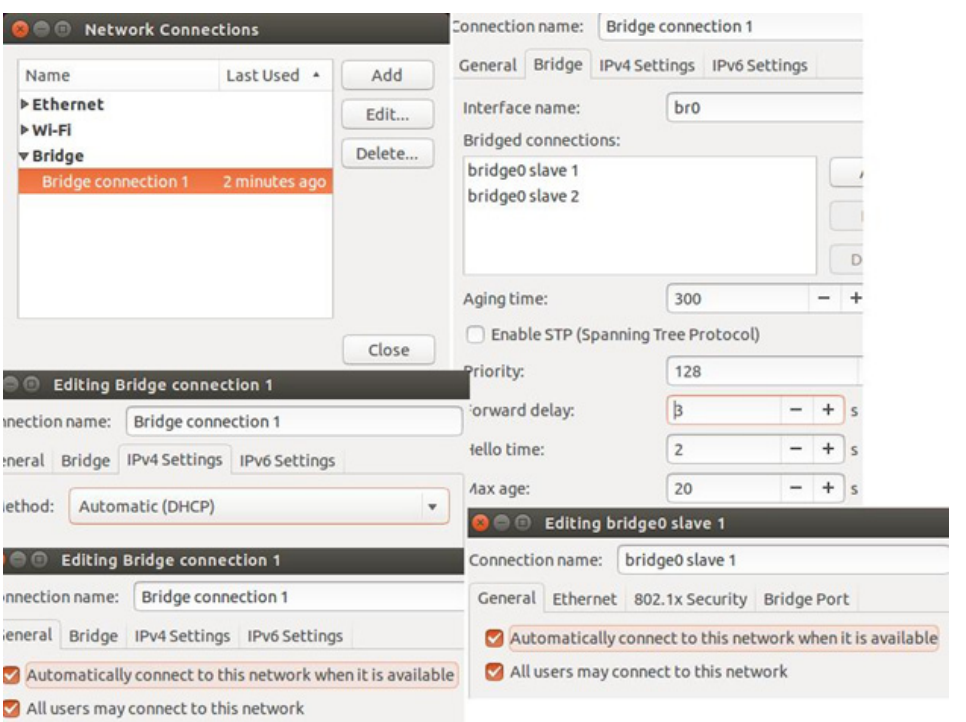


Figure 4.

And of course if you're wanting to do it the old fashion way, here's some sample commands you can run in bash if you do not use networkmanager or have disabled network manager:

```
aptget
install bridgeutils
y
brctl add br0
```

```
brctl addif br0 eth0
brctl addif br0 eth1
brctl stp br0 off
ifconfig eth0 0.0.0.0 down
ifconfig eth1 0.0.0.0 down
ifconfig eth0 up
ifconifg eth1 up
ifconfig br0 192.168.1.250 netmask 255.255.255.0 up
ip route add default gateway via 192.168.1.1
echo "nameserver 192.168.1.1" >> /etc/resolv.conf
```

*Note: You will now need to reboot the box using something like “shutdown r now” or “reboot” so the changes can take effect. If you didn’t configure your IP settings or defaultgateways, you WILL lose internet connectivity for those of you doing this remotely. We’ll be using primarily the following two tools for decryption and packet injection/modification: mitmproxy and netsed You can type these yourself or grab the copy of the bash script at my Github [install and launcher]

Once the box comes back up, log in and run the following commands in order, for any interaction, follow the instructions requested. You can click on the image if you want to expand it. These commands will switch you to root access, update your packages, create a folder in your directory, install all the dependencies automatically and enable IP forwarding in your kernel andto save it upon reboot. You’ll also notice that ICMP redirects are turned off. If you decide to put this as a gateway on the same physical network vs. inline this is turned off to prevent possible route change errors and inconsistencies. Also note that IP forwarding is enabled onall interfaces.

In our example, we only had 2 interfaces that became a bridge with an IP. If you have management interfaces, refer to this guide about setting IP forwarding per interface rather than across the entire system. We also disable the system firewall.

```
#Enter password and get root
sudo bash

#Get the packages and install them
apt-get update && apt-get upgrade -y
cd ~/
#Make the mitmproxy directory just in case
mkdir ~/.mitmproxy
apt-get install python-pip build-essential python-dev libffi-dev libssl-dev libxml2-dev libxslt1-dev netsed -y
pip install mitmproxy
pip install urwid

#Enable IP forwarding
sysctl -w net.ipv4.ip_forward=1
#Make it perm for IP Forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward
#Disable ICMP redirects since likely on same physical network
echo 0 | tee /proc/sys/net/ipv4/conf/*send_redirects

#Ensure firewall is off
ufw disable
```

Figure 5.

Now we can route traffic through iptables. If the image appears weird on the first line, it’s because I changed the numbers for the purposes of demonstration. This basically says configure the NAT table to add rules to prerouting chain on our bridge anything to tcp port 6969, 80, 443, redirect to local listening ports on the black box (in our case mitmproxy is listening on 8080, and netsed is listening on 1337). The end of it saves iptables so it stays enabled on reboot.

```
#Route     traffic to netsed
iptables -t nat -A PREROUTING -i br0 -p tcp  --dport  6969 j REDIRECT  --to-port  1337

#Straight route web traffic to mitmproxy no pipe
iptables -t nat -A PREROUTING -i br0 -p tcp --dport 80 -j REDIRECT --to-port 8080
iptables -t nat -A PREROUTING -i br0 -p tcp --dport 443 -j REDIRECT --to-port 8080
#Part of the iptables-persistent dpkg default on Ubuntu 14
iptables-save > /etc/iptables/rules.4
```

Figure 6.

You can specify any/all ports as your destination to be truly transparent and non port dependent; you can also pipe/chain funneling traffic between applications such as [netsed > mitmproxy] by doing dport

80,443 redirect to 1337 and then specify netsed on the output to redirect to the mitmproxy listening on 8080 as one example. In our example, we're just keeping them separate.

*Note: mitmproxy will generate it's own certificates. You will need to install the certificate on any end host that you want to mitm if you don't want them to receive the error(s), or use your own instead. Instructions found on the author's website. Also note, if the apps or embedded victim devices do SSL certificate validation checks and you can't install the cert, your connection will fail out.

PART 3 WHAT CAN YOU SEE OR DO?

Now either use the launcher script, or run the follow commands and you should now be able to start sniffing traffic, decrypting, and injecting packets upon sending. Voilà: We have passwords from a user trying to login into Yahoo mail that unfortunately either had the certificate installed, or pressed the continue page for the SSL certificate error in their browser. Mitmproxy is intercepting all tcp port 80 and 443 traffic and redirecting it to it's listener on 8080 then forwarding it back out to the website.

*If you can't see it, you can find the full size image here: *http://s27.postimg.org/5s481uv2b/mitmproxy_sslsnag.png.*

Not enough? Let's say we have a chat program that's trying to send a message. to another computer and you're tying message A and you expect your recipient to get that same message.

Not anymore, our Cyber Blackbox will modify what you said; and you wouldn't know what they received until it was too late. Now think about any emails that you may write in a day.

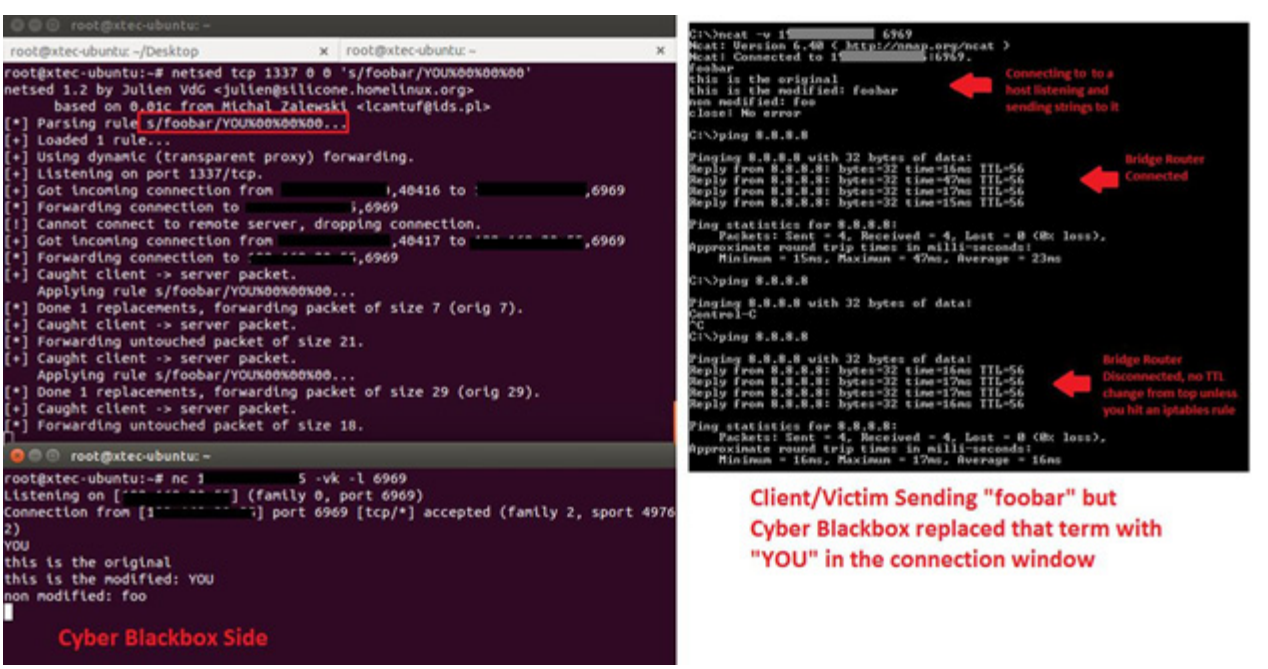


Figure 7.

*If you can't see it, you can find the full size image here: *http://s3.postimg.org/ephjw5yvn/netsed_injection.png.*

The picture on the right shows the client with a simple chat program. Cyber Blackbox is now replacing and injecting any word that says "foobar" with "YOU" in all caps. Notice the use of "%00" where it adds null characters to pad the transmission so the size of the TCP packet doesn't change and is less likely to crash the connection or for it to get rejected. We setup a simple listener on the blackbox to mimic a receiving user and what do you know; our sender said "foobar" in the first message, but all of a sudden the first message received was really "YOU" .

Other use cases for the Cyber Blackbox involve general packet captures to analyze, troubleshoot, or recompile traffic over time. Note, the use of the mitmproxy private key within something like tshark

or wireshark cannot be used on most modern sites as entities like Google, and Yahoo have enabled Perfect Forward Secrecy that prevents recorded session traffic to be decrypted correctly.

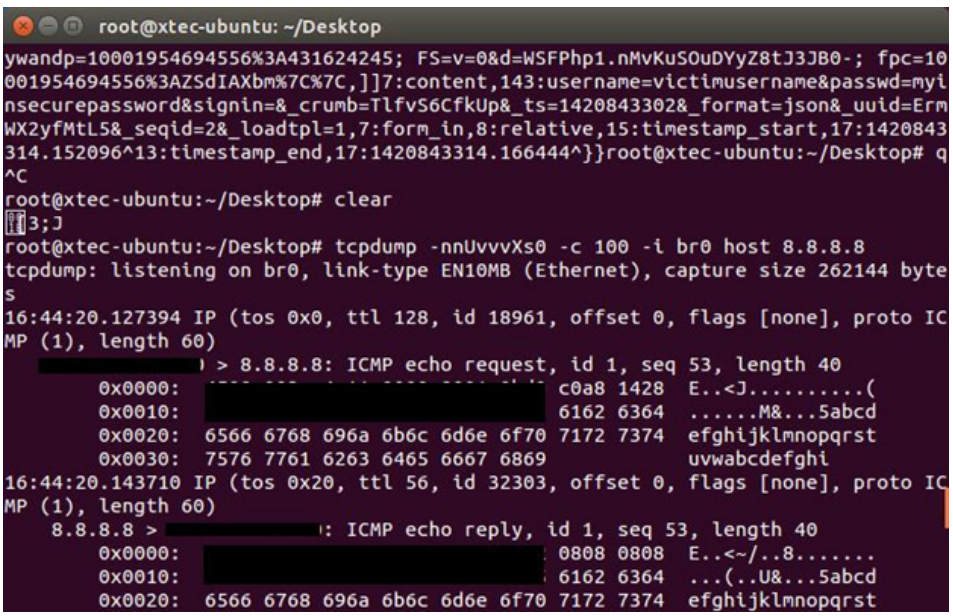


Figure 8.

This concludes this weekend's mini series on practical uses of cyber security tools and practices.

If you enjoyed this article you may also want to check out my other mini tutorials:

https://www.linkedin.com/pulse/fake-out-analytics-tracking-instead-blocking-dennis-chow-mba?trk=prof-post

https://www.linkedin.com/pulse/20140601182601-22590999-using-ntfs-alternate-data-streams-in-network-based-dlp?trk=prof-post

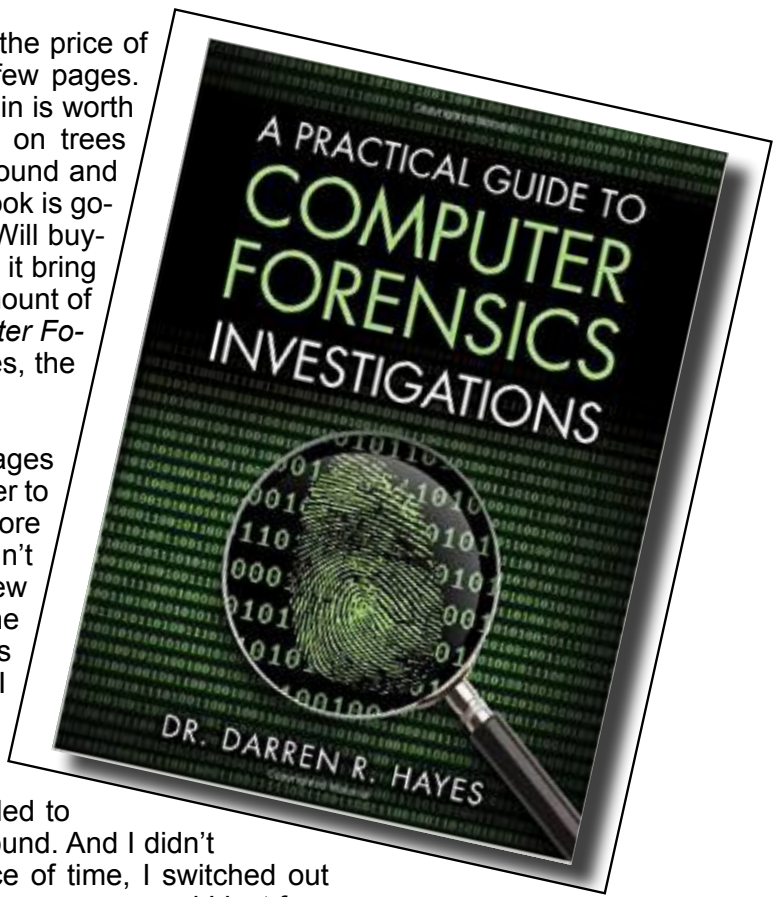
DENNIS CHOW

Dennis Chow is an IT Security Practitioner that has over 10 years in various positions in the Information Technology with 6 years in IT Security specific roles. He is currently a Senior Security Engineer at the world's largest medical center. Dennis also performs part-time consulting and trains new security analysts in the field. Currently, Dennis focuses much of his time performing penetration testing and other security operations. Dennis currently holds several industry recognized certifications including: GCFA, GCIH, GCIA, GPPA, C|EH, E|CSA, L|PT, and the CISSP.

A PRACTICAL GUIDE TO COMPUTER FORENSIC INVESTIGATIONS

BY DR. DARREN R. HAYES

Reviewed by Bob Monroe



Whenever I look at buying a book I look at the price of the book after I have flipped through a few pages. I want to know if the object I'm interested in is worth the cost associated with it. Money doesn't grow on trees but books are made of trees so the riddle goes around and around in my head. I need to know if that $65.00 book is going to bring a me return on investment somehow. Will buying that book make me a better professional or will it bring me enough enjoyment to warrant spending that amount of money? In the case of *A practical Guide to Computer Forensic Investigations* written by Dr. Darren R. Hayes, the answer is at the end of the review.

When I get a technical book I usually read a few pages throughout, bouncing around from chapter to chapter to get a feel for the book and how it was designed before I settle in to read the entire manual. Dr. Hayes didn't give me that opportunity because the first pages drew me in almost like a mystery novel. I couldn't put the darn thing down. The only reason I noticed this was because I coughed and saw the time on the clock. I was on page 139 and my highlighter was worn out.

Somehow the author managed to entice me with page after page of incredible information that I failed to adhere to my normal reading ritual of bouncing around. And I didn't even notice until I was on page 139. In that space of time, I switched out highlighters because my orange one dried up with over usage and I lost four hours of sleep. For example, during the Enron Oil scandal of 2001 the employees there shredded thousands of pages of documents but FBI forensic investigators were able to retrieve the equivalent to 10 times the size of the U.S. Library of Congress from hard drives. That's a whole lot of data recovery.

Here's another tidbit: Microsoft's COFEE program only works properly if the system is captured live and hasn't been powered down. This book goes into a large segment of live resident memory data recovery, all written in vivid detail by Dr. Hayes. Did you know that Bitlocker only activates when the device is shut down or the Bitlocker USB drive is removed? That's how the FBI was able to capture all that data from the recent Silk Road operator. The suspect was at a restaurant with his back to the door when federal agents swept in from behind and grabbed him and his laptop before he knew what happened. His computer was fully logged on and his encryption unlocked.

A Practical Guide to Computer Forensic Investigations goes into some of the basics of forensic investigation, as you might expect, but then dives into registry analysis, hard drive composition, file indexing, email event archives and pages after page of incredible information. Dr. Hayes writes long and in-depth about the differences between each version of Windows. He covers how each File Allocation Table (FAT) is different and what the examiner needs to consider based on the OS and update. While this topic alone could easily take up an entire book, Dr. Hayes manages to blanket Linux, and iOS too.

This is just the tip of the iceberg. *Practical Guide to Computer Forensic Investigations* also discusses the differences between media formats and how you need to consider your connections for evidence gathering. Many other forensic books cover this same topic but none do as good of a job as this author does. Wait until you see Dr. Hayes idea of a computer tool kit, besides including a soldering iron and wrenches, I could almost swear I saw a blow torch and a surgical knife. He doesn't mess around. What kind of doctor is this guy?

Some of the software tools mentioned in the book are your typical commercial tools for deep-lined pockets. For those of us without fat wallets, the good doctor adds plenty of free or open source tools that do the same thing as the expensive ones. In fact, many of the free tools work better. Dr. Hayes is very serious when he points out that you need to have you own set of tools and know those tools well. You need to know how your tools work before you have to use them in real cases. This may sound like common sense but you don't want to be called out by a legal team as a sworn expert witness only to have them make you look like an idiot because you didn't add the –d switch when you ran your acquisition tool. Be aware that some of the information is a bit disturbing because the author made sure to include plenty of real life examples of crimes. Child exploitation, murder and physical harm are cases that have the reader reminded that this isn't a hobby. The guilt or innocence of someone may rest on your shoulders as an investigator. Dr. Hayes brings up the team concept of working alongside other professionals who are building that case with you. It is your responsibility to conduct your portion of the investigation with as much knowledge as you can offer. This book is a huge part of your knowledge base.

Many new devices are part of the evidence collection process. This guide doesn't linger on just desktop or laptop machines. There are 501 pages of content that ranges from cellular signal interception, SIM card reading, different tablet operating systems, Android forensics, iPhone data analysis, RIM data acquisition, photo researching, Bluetooth data storage locations and everything in-between. These aren't merely mentioned as part of a paragraph, they are written about with extensive background information.

One example of smart thinking is a section on using grep to locate passwords, usernames, session dates, hidden text and other nefarious evidence inside innocent looking files. People looking to hide things have been tempted to put them in files and rename them. Dr. Hayes points out that the reader needs to look at dll files and other executables for images or contraband. This can be painful if performed without the aid of software filters. Greb can run through all these files for you as long as you supply the key word you are looking for. Each chapter has plenty of clear pictures and diagrams to help explain or show information. These information-filled chapters conclude with a summary of entire text, a list of key terms (almost like a glossary but better because the book has one of those too), classroom discussion questions to ponder and multiple choice questions. This is in line with most new technical books that can easily become classroom teaching textbooks. The classroom discussions posed some interesting questions that challenge the reader to fully understand the presented material in real-life situations. The chapters don't just end with some multiple choice questions though. The chapters continue with fill in the blank questions that reinforce your knowledge of the material. The last part of each chapter is a segment called *Projects*, where the reader is given assignments to research or investigate on their own.

This guide meets my criteria for a desk top reference book. I don't have much space on my desk so space is at a premium. I don't even have room for speakers so I manage (if you want to call it that) my little space based on how often I use a particular object. For books, I only have three books that have made it to a permanent spot on my desk. The other hundreds of books I have are stashed in the book cases above my desk, daring to collapse at any moment. *A Practical Guide to Computer Forensic Investigations* has earned a coveted spot on my desk. This means I have to get rid of my computer or move another hard drive to the attic. Some people give awards for great books, I give up space for great books.

So to answer the question of whether the book is worth the price, my answer is no, it is worth twice that amount.

BOB MONROE

Bob Monroe grew up in Southern California before he joined the U.S. Army in 1985. One of Bob's first military assignments introduced him to the world of hacking. His prankster ways ended abruptly in 1996 when he was almost caught hacking by an eighty-two year old librarian. This incident led to a renewed interest in cyber security, as a good guy. Since then, he has written several articles for publication and maintains a passion for digital security. Bob holds a Master of Science in Information Assurance from Norwich University.

Bob's specialty is cyber teaching and security awareness training. Along with work for the U.S. Army, he has taught security classes for the Veterans Administration, Military District of Washington, Commandant of the Marine Corp and staff, as well as countless others across the world. He holds a U.S. Patent for airport security automation technology that combines radar and thermal imaging to protect aircraft movement areas and the surrounding airspace. This patent does not impress the TSA folks at all and usually gives them a reason to strip search him instead.

Bob works with the Institute for Security and Open Methodologies (ISECOM.org) and Hacker High School as an editor and writer. Both organizations are non-profit, with the mission of teaching computer security methods across a global audience. In his spare time, Bob makes children's toys in his small woodshop. He still has all nine fingers, too. Oops, make that seven fingers

INTERVIEW WITH DR. DARREN HAYES,

AUTHOR OF A PRACTICAL GUIDE TO COMPUTER FORENSIC INVESTIGATION

by Bob Monroe

Dr. Darren Hayes of Pace University in New York City has had his fair share of digital forensic investigations since entering this field in 2006. He has worked on numerous civil investigations each year and has also been on over a dozen undercover operations, working alongside law enforcement to discover and extract evidence. Even some of his civil investigations have turned into criminal cases according to Dr. Hayes, “Finding the evidence is just one part of the investigation – I need to also prove that a suspect

DARREN HAYES

Dr. Darren Hayes is a leading expert in the field of digital forensics and cyber security. Hayes has been involved in computer forensics since 2006. Hayes is the Director of Cybersecurity and an Assistant Professor at Pace University, New York. In 2013, he was listed as one of the Top 10 Computer Forensics Professors, by Forensics Colleges. He has developed a computer forensics program at Pace and has created a computer forensics research laboratory at the Seidenberg School of Computer Science and Information Systems. Hayes continually conducts research, with his students at Pace, in support of law enforcement agencies both domestically and internationally. He has successfully been awarded grants, in the field of computer forensics, by the Department of Defense, National Science Foundation and other notable foundations. Hayes•s expertise not only includes traditional computer forensics but also extends to mobile forensics. He has developed four distinct courses in digital forensics, at Pace University, at the undergraduate and graduate levels. Hayes is also a professional consultant in computer forensics and cyber law for the Department of Education, New York.

As a forensics examiner, he has worked on numerous cases involving digital evidence in both civil and criminal investigations. For a number of years, Hayes has served on the Board of the High Technology Crime Investigation Association (HTCIA) Northeast Chapter and was the President of the HTCIA Northeast, 2013. He is back on the board and now serves as Second Vice President of the HTCIA Northeast in 2015.

He is an accomplished author with numerous peer-reviewed articles on computer forensics. Hayes has been both an author and reviewer for Pearson Prentice Hall for a number of years. He has co-authored two textbooks in the Skills for Success series and is now looking forward to publishing his book, with Pearson, in 2014 entitled, A Practical Guide to Computer Forensics Investigations. Hayes has appeared on Bloomberg Television, The Street and Fox 5 News and been quoted by CNN, The Guardian (UK), The Times (UK), Wall Street Journal, Financial Times, Forbes, Investor•s Business Daily, MarketWatch, CNBC, ABC News, Forensic Magazine, SC Magazine, PC Magazine, USA Today, Washington Post, New York Post, Daily News and Wired News to name but a few. He has also been invited to lecture for the Harvard Business Review, University College Dublin and, more recently, was Visiting Professor at Sapienza University, Rome, Italy.

was in control of that computer or device at the time". In December 2014, Pearson Publishing printed the first edition of Dr. Hayes new book *A Practical Guide to Computer Forensics Investigations.*

This book took four years to research and write. Time well spent for a man known as a leading expert in digital security and cyber forensics. After years of working with New York City's finest police officers and U.S. Department of Defense, Dr. Hayes put all of his efforts into turning that knowledge into an incredible 500 page guide. Even though he has a dual background in security and forensics, he hates when people think these are the same topic, "One mistake that people make that bother me the most are those who assume that computer forensics and security are the same." Most experts in either field would agree with him.

In security, you are being proactive and trying to provide confidentiality, availability and integrity of data to all authorized users. In cyber forensics, Dr. Hayes warns, "Attorneys generally want very specific evidence relating to a specific type of crime". These are two very different objectives. In security, if you are working with law enforcement it's because something went wrong with the security plan, such as a data breech or an attack. In forensics, you might be working with law enforcement from the beginning of a project but are reacting to an event - often criminal in nature.

Much like the discovery of personalized skin bacteria left on individual keyboards that can be used to determine who used that device last, Dr. Hayes work lays on the front lines of digital evidence discovery. His newest projects look at increasing a forensic examiner's portability by building inexpensive computer forensics imagers, cloners and smartphone imagers. He adds, "You can build a basic computer for about $100 and then the rest is just adding an open source distribution and adding some Linux commands."

This idea plays into the increasing use of microcomputers like the Raspberry Pi and the Beagle Bone Board. Dr. Phil Postra recently published his own book on this same topic of *Penetration Testing Using Low Power Devices*, which is predominately focused on the Beagle Bone Board to create a drone. Either low cost device can easily run Kali Forensic as the operating system and tool box. Kali offers metapackages of their tools based on Intel-Gathering, WiFi Pen Testing, Network Pen Testing, Documenting and other groups of tools. Dr. Hayes is working on this same research theme.

This doc's favorite tools include a laptop, Cellebrite UFED Touch, Disk Jockey cloning device, multihead screwdriver, USB write-blocker, FTK, BlackLight, X-Ways, Oxygen Forensic Suite and Wireshark. All of which are discussed quite well in his book *A Practical Guide to Computer Forensic Investigation.* When asked about why he liked using dd over other imaging tools, he responded with, "dd is a wonderful, robust tool for disk acquisitions. dd is a free Linux command-line tool that enables you to obtain a forensically-sound Raw image of a file, directory or hard drive. The command is very dynamic so that you can control exactly how the output should look. Additionally, dd can be used with the netcat (nc) command so that you can remotely image a hard drive over a network, which adds to its versatility." dd comes with most flavors of Linux. Kali includes a few new acquisition programs for those looking at ultra-portable platforms like the Raspberry Pi or the Beagle Bone Board. Running a USB hub powered hard drive on the RPi is a snap using an ample power supply like the Anker. All that hardware would fit into a small Tupperware container.

Of course that won't help when you are handed a bag of drives to examine like his recent case, "We recently worked on a case where we were provided a bag of hard drives from a RAID server. Therefore, we did not know the order that the drives were in. To further complicate matters, a number of critical system files on the hard drives were corrupted. Ultimately, we managed to extract the necessary evidence but it took a couple of weeks of frustrating work and numerous software tools. We were so excited to solve the issue in the end though."

Luckily, Dr. Hayes enjoys a nice cold glass of milk and cookies to relax after a long day of scanning drives. Living in New York City, he also has plenty of opportunities to grab an Italian hero sandwich from a local deli. He says, “Teaching is my passion but I enjoy working in the field and the lab.” As a professor at Pace University in the city that never sleeps, he is the Director of the Pace Cybersecurity Institute, where “I manage our computer forensics laboratory, lead faculty-student research, organize internship opportunities and host meetings and training throughout the year.” Besides those full time jobs he consults for attorneys in both civil and criminal investigations. Plus he plays the trumpet not the violin at the criminals sentencing trial.

BOB MONROE

Bob Monroe grew up in Southern California before he joined the U.S. Army in 1985. One of Bob’s first military assignments introduced him to the world of hacking. His prankster ways ended abruptly in 1996 when he was almost caught hacking by an eighty-two year old librarian. This incident led to a renewed interest in cyber security, as a good guy. Since then, he has written several articles for publication and maintains a passion for digital security. Bob holds a Master of Science in Information Assurance from Norwich University.

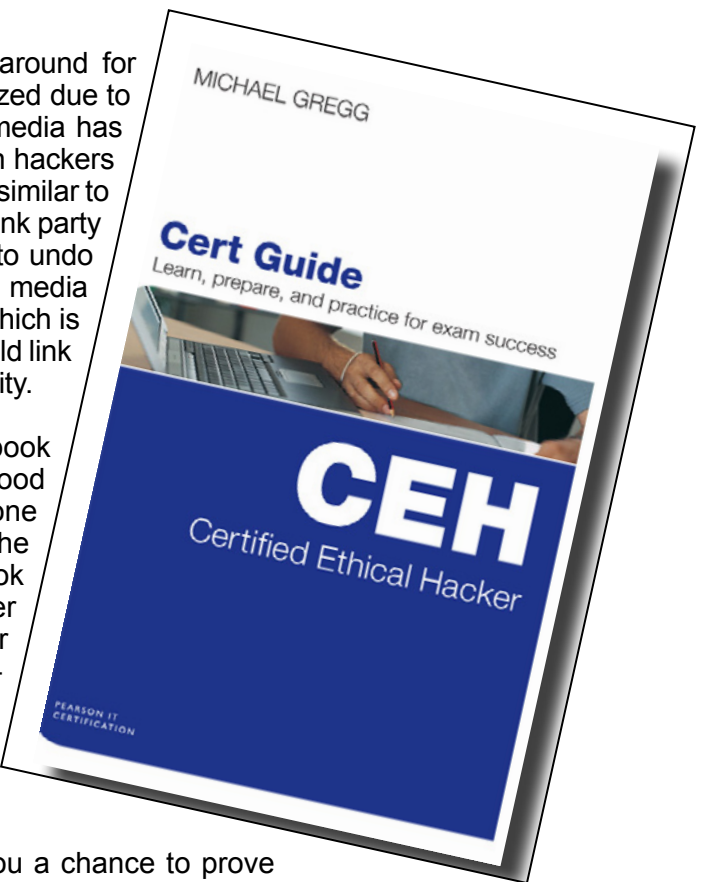
Bob’s specialty is cyber teaching and security awareness training. Along with work for the U.S. Army, he has taught security classes for the Veterans Administration, Military District of Washington, Commandant of the Marine Corp and staff, as well as countless others across the world. He holds a U.S. Patent for airport security automation technology that combines radar and thermal imaging to protect aircraft movement areas and the surrounding airspace. This patent does not impress the TSA folks at all and usually gives them a reason to strip search him instead.

Bob works with the Institute for Security and Open Methodologies (ISECOM.org) and Hacker High School as an editor and writer. Both organizations are non-profit, with the mission of teaching computer security methods across a global audience. In his spare time, Bob makes children’s toys in his small woodshop. He still has all nine fingers, too. Oops, make that seven fingers

CEH CERTIFIED ETHICAL HACKER CERT GUIDE

BY MICHAEL GREGG

Reviewed by Bob Monroe



Certified Ethical Hacking (CEH) has been around for many years but hasn't been widely recognized due to the use of the evil H-word (Hacker). The media has done a great job of blaming all technology woes on hackers so obtaining a certification with that name on it was similar to getting a bad tattoo on your forehead or posting drunk party pictures on a social media site. It has taken time to undo some of that poor naming damage but at least the media hasn't gotten a hold of the other name for CEHs, which is penetration testers. You can be sure the media would link that title to the porn industry instead of cyber security.

This is the second printing of Michael Gregg's book on CEH, which must mean he's popular and a good writer. Reading his book shows that he has done his research and drops plenty of names along the way. The overall purpose of this 640 plus page book (and practice exam DVD) is to prepare the reader for taking the EC-Council Certified Ethical Hacker 312-50 exam. This book is not a guide to hacking nor it is a license break into your neighbors WiFi router for free bandwidth. This is a license to learn and to show you how much you need to learn before you attempt the exam.

Like many exam prep books, this one offers you a chance to prove yourself early on by asking you a couple of basic questions. I guess "basic" is the wrong word because the difficultly of the question depends on how much you already know about each topic ahead of time. To make these questions a bit more slippery, the author left out portions of answers to see if you really know your stuff or if you are flapping like a fish inside a boat. An example of this is in question 2 of the first chapter.

What are two major laws in the United States that deal with computer crimes?

1. 1029 and 1030
2. 1026 and 1027
3. 1028 and 1029
4. 1027 and 1029

If you look at the question closely you will see that it asks about *major* laws. The answers you are given are actually sections or segments of U.S. laws. It's a legal technicality but it also throws off anyone who hasn't paid attention to Cyber Crime Law. If you breezed through this question you might want to go back and read Orin Kerr a bit deeper. The author does this on purpose in several areas in the book, where he gives you part of the answer but recommends you research yourself for the rest of the answer or the reason why things are done this way.

I wrote many notes of disagreement and encouragement as I read through the book. Little things like the Robert Morris Worm was created by Robert Morris Jr., not Robert Morris. Robert Morris Sr. was actually working in the ARPNET Incident Center (NSA's Situation Room before there was such as thing) when he found out his son lost control of a piece of code, known as the Morris Worm. Old history but a funny story anyways when told over cold beverages. Geeks do enjoy a good story too.

For those of you who already know about OSSTMM, you can skip the next couple of sentences. If you don't know what OSSTMM is, pay attention cause I was dancing around my computer when I saw it come up several times in the book. This is a testing methodology (free) created by hundreds of volunteer experts from around the world under the direction on Pete Herzog. The basic premise of this testing process is trust. You shouldn't take a computer, test it, harden it, retest it and call it secure because as soon as you add on another piece of hardware or software, your testing and trust goes out the window. OSSTMM was created to allow you a dynamic process to test and trust your network as you work. It is a continuous process that ensures you can trust that your data is not being siphoned off to your competitor or a hacker. You can find out more by either reading this book or going to *www.ISECOM.org*. Sorry for that plug but I work for ISECOM and Pete Herzog so I was thrilled to see it mentioned in the CEH guide.

There is a vital portion in the CEH book for required skills. It is way too often that we come across a security professional with all kinds of cool sounding certification but they don't know much about the fundamental tools we use. Believe it or not but good guys use the same tools bad guys do, each just uses different syntax. It is critical that anyone looking at the CEH know how Nmap, Wireshark, Kali (not Backtrack), putty, traceroute and a dozen other tools work from the command line (CLI). Forget GUI. Know CLI first because there are numerous undocumented commands available only to CLI. Mr. Gregg does a good job of lifting this mighty rock for his readers to look under but it is up to the reader to dig into each tool on their own. The same goes with the OSI model, ports and services. Learn them.

Some of the tools the author mentions are outdated which tells me that he must be trying to market towards defense contractors. Those poor souls were using Retina when I left back in 2006. BTW- Core Impact is written by four programmers in Argentina yet it is on the GSA schedule. It's also mentioned in this book as an exploit tool.

I was a bit disappointed that the author didn't bring up the need to document everything when conducting an ethical hack. Armitage is a framework for Metasploit that makes a pen testers life so much easier by documenting the results of every test on every node. Document everything in case things go sour during or after the test. It's not uncommon to find another hacker already inside a system you are contracted to test. Things can get very ugly and documentation is the only thing that will save your bacon if the other hacker decided he wants to make your life difficult.

Michael Gregg has a massive subject area to cover and he does a good job of touching on all the key points. Don't expect to read this book and then go pass the CEH exam. Even if you do, there is still so much more you will need to know as a CEH in the real world. Some of the stories about walking up to the receptionist and obtaining access to a conference room with network access are old wives tales. The receptionist is the gatekeeper, the holder of the keys and they aren't going to let anyone past their area without a pound of flesh or a permission slip. Those stories go back to Kevin Mitnick days.

The Certificated Ethical Hacker Cert Guide by Michael Gregg is well written and full of useful content. There are plenty of practice exam questions in the book and in the attached DVD. You may want to ask yourself why some of these questions are written they way they are. Think of cyber security as a massive puzzle. Each book you read, every blog you note and every tip you are given will slowly fill in that massive puzzle and allow you to see the big picture. It is a three dimensional puzzle where many things link together and you have to think about action and reaction as you work.

It is not a cat and mouse game: that is too linear. Michael Gregg provides some nice research spots to camp out and hunt your prey. Good luck.

BOB MONROE

Bob Monroe grew up in Southern California before he joined the U.S. Army in 1985. One of Bob's first military assignments introduced him to the world of hacking. His prankster ways ended abruptly in 1996 when he was almost caught hacking by an eighty-two year old librarian. This incident led to a renewed interest in cyber security, as a good guy. Since then, he has written several articles for publication and maintains a passion for digital security. Bob holds a Master of Science in Information Assurance from Norwich University.

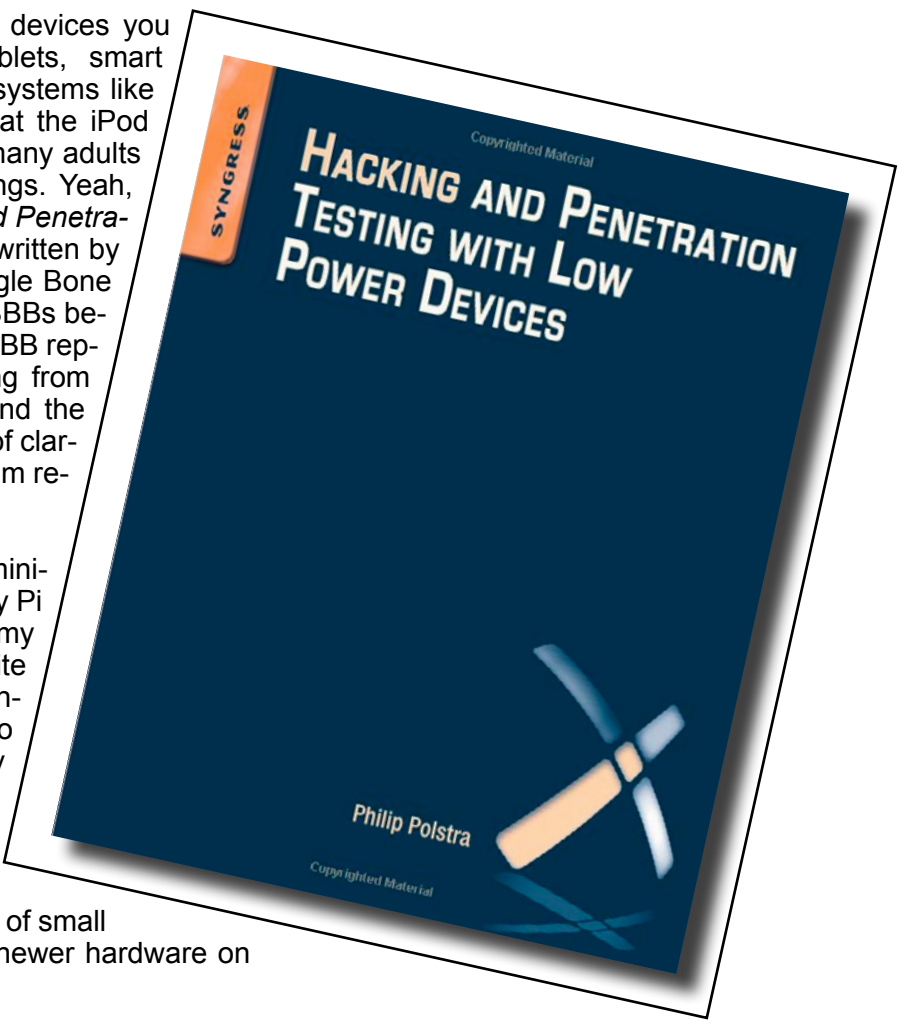
Bob's specialty is cyber teaching and security awareness training. Along with work for the U.S. Army, he has taught security classes for the Veterans Administration, Military District of Washington, Commandant of the Marine Corp and staff, as well as countless others across the world. He holds a U.S. Patent for airport security automation technology that combines radar and thermal imaging to protect aircraft movement areas and the surrounding airspace. This patent does not impress the TSA folks at all and usually gives them a reason to strip search him instead.

Bob works with the Institute for Security and Open Methodologies (ISECOM.org) and Hacker High School as an editor and writer. Both organizations are non-profit, with the mission of teaching computer security methods across a global audience. In his spare time, Bob makes children's toys in his small woodshop. He still has all nine fingers, too. Oops, make that seven fingers

HACKING AND PENETRATION TESTING WITH LOW POWER DEVICES

BY PHILIP POLSTRA

Reviewed by Bob Monroe



When you think of low power devices you may tend to focus on tablets, smart phones or portable gaming systems like the iPod Touch. Before you shout that the iPod isn't a gaming platform, tell me how many adults versus kids you see using those things. Yeah, its a toy alright. The book *Hacking and Penetration Testing with Low Power Devices* written by Dr. Philip Polstra is all about the Beagle Bone Board (BBB). I hope you've heard of BBBs because they are a cool minicomputer. BBB represents a collection of boards ranging from the BeagleBoard, BeagleBoard-xM and the BeagleBone Black. For the purposes of clarity, when you see BBB in this review, I'm referring to the BeagleBone Black.

Because I've been working with minicomputers like the BBB, the Raspberry Pi B+ and old Android phones, I've got my favorites just like you have your favorite socks. The author, Dr. Phil, makes plenty of evidence-based arguments as to why the BBB is his favorite. The only problem with his logic is that with any technology, it is outdated the moment he typed it out. One day the Beagle might be the top dog and the next day it's the Pi. These particular brands of small computers are being beefed up with newer hardware on a regular basis.

You should know though, that this book is aimed at teaching you how to use the BBB as a pen testing tool. The first chapter introduces you to the author's pride and joy, a compilation of devices that make up "the Deck." The Deck has been showcased at several hacking conventions over the years. The Deck is a system of tools that can be used as portable drones, air deployable remote control aircraft sensor and even an awesome looking Guitar-Hero platform. The information about building my own Deck was peppered throughout the book. There wasn't one section that tells you how to build a Deck but rather bits and pieces are discussed throughout the 237 page book. No cheat sheet was provided.

As with any professional hacker/pen tester, the author has to walk an ethical tightrope to ensure they don't teach everyone how to be criminal hackers yet still give the readers enough details to quench their desire for knowledge. Hacking is not about criminal activities, it is about learning new ways to do things beyond what the manufacture intended the product to do. You must learn and think on your own.

This book is filled with plenty of incredible knowledge that you may not find anywhere else. For example, chapter five Powering The Deck, covers the critical information needed to determine how to power your low power device. Anyone who has picked up a soldering iron, a voltmeter and some electronic component that requires a magnifying glass to lay down a perfect bead knows how easy it is to fry that device. Pay close attention to Dr. Phil's research and advice when it comes to providing juice to your low power project.

I like to be mobile so I use an Anker 5V 13000mA small charger, which has enough juice to jump start a car and power my devices. The Dr. Polstra provides the reader with plenty of options and plenty of cautions about under powering your device. Most of the newer mini computers have built-in power management hardware to keep the current regulated. The Anker has built-in technology to ensure your device gets exactly what it asks for even as the device environment changes due to the addition of a WiFi adapter, WiFi keyboard, Bluetooth dongle, touch screen, or refrigerator to keep your snacks cold. Dr. Phil warns the user about plugging in any old power adapter you have laying around. Most smart phone power adapters will gladly give the device 5V but it won't push past 1.5 A. Any drop in amps means your device shuts down or reboots or just allocates power to where it thinks it is important. Your pen tool could become worthless just because you went cheap on the power supply.

Don't do it. Respect the power! Ipad and tablet adapters should be used if you are going to rely on a wall outlet. The BBB can be powered by your computer or laptop via USB but you run the risk of lower amps. Again, respect the power and use the properly rated power adapter or supply if you are going to add on goodies to your board. When you do buy your computer, you are going to want to add on all kinds of neat capes or stuff to fill up the USB ports. The Pi B+ has four while the BBB has one USB port. The Pi B+ wasn't available when the book was sent to the printers so this is not covered.

Another nice aspect of the book that I was surprised to see was a really good overview of different Linux, Unix, Android and Windows CE operating systems. This was a wonderful learning opportunity simple because I use Ubuntu, Debian, Windows CE and Android for portable systems. Dr. Phil provides great advice on why you would want to follow his footsteps in using Ubuntu (unless you like Kali (Debian) which I prefer)). He covers each distro fork as well as which ones have the best repositories or support community.

This is essential when using low power devices because you don't want useless fluff (bloatware) taking up precious space or resources on your credit card sized project. Yes, these devices are credit card sized just a bit thicker and much cooler to work with. Each basic device runs about $35-$45 U.S., whether you buy a Pi or a BBB. These devices have more computing potential than many laptops and desktops yet use a fraction of the space. Many people ask me "what do you do with this little thing." I tell them that I can run them as a home media, web, email or FTP server. I can swap out operating systems just by changing out microSD cards. If you want to use the boards to be the brains of a robotics project, easy. Don't expect to plug and play, though. Maybe you want to replace your desktop with an ultra portable machine. I know the Pi will run Libre Office so I would imagine the BBB could too. Just buy a larger screen or plug in the HDMI to your TV to ease your eye strain.

Hacking and Penetration Testing with Low Power Devices is not entirely light reading. There are areas where the author drops a 100 meter anchor in the ocean of technology and then guides the reader on how far you need to go to retrieve this information. You will be thrown into a Linux terminal of piped commands to install the Deck OS and configure the basics for your BBB. Right from the start, the commands are very clean coding and well documented. I would have never thought to use || (dual piping) in a script. Luckily, Dr. Phil explains his process and shows the reader some basic python language (a must for any security professional to learn). He also explains why some conditions will work in certain shells but not others. If you ever wanted to know what a digital security professor reads, there are plenty of reference books cited along the way.

You need to consider that working with low power devices is a mis-mash of hardware building, software coding, scripting languages, learning by breaking (as it should be to separate the dedicated from the joyriders) and doing a hell of a lot more research on your own. Dr. Phil is not going to spoon fed you. He provides a path and the choices but it is up to the reader to dive into that ocean and learn the inner workings of low power hacking. This is cutting edge technology so don't expect easy answers to your questions. Dr Phil is a teacher who knows that the reader must invest time and effort on their own to make any hacking project.

I'm not sure if it was deliberate but some of the hacking tools he suggest are outdated. Backtrack is mentioned and discussed. Kali is another story since it was built to completely replace Backtrack from scratch. Kali is ported into anything including your kitchen toaster. I was interested to read his use of Xbee communication hardware. There are several new communication protocols going through the RFC stage, including 802.11p for vehicle communications. The Deck uses the Xbee chips for data transfers that, guess what, use very low power. RFC's aren't exciting to read but the last chapters of this book is focused on sensors, capturing traffic, as well as sending that information back to the mothership. This chapter will make you swallow your gum once you realize the potential and implications of this technology. Imagine a remote control plane flying over your house collecting (war driving) all your WiFi, cellular, Bluetooth, NFC data from people not working for the NSA.

Overall, I found some information caused me to sit up straight in my chair when I started to see the puzzle pieces forming into a picture of our privacy future. In full disclosure, I had worked with Dr. Phil on a project for the Institute for Security and Open Methodologies (ISECOM). No bodily fluids or money changed hands during that project. There are several nods to important pioneers of technology where Dr. Phil either gives you the persons name or sneaks in that acknowledgment. As I found out, if a sentence doesn't exactly make sense, there is a reason because the author is throwing a tongue and cheek remark at you to see if you're paying attention.

Hacking and Penetration Testing with Low Power Devices is aimed at teaching the reader how to work with the Beagle Bone Board to create the Deck or project of your choice. Low power computers are built for multiple uses. Once you have one in your hands, you can do numerous custom configurations to suite your interests. If you take the Deck project out of the book you still have a ton of great information on how to build and play with the inexpensive device. Due to the release of many other similar devices (Intel, Texas Instruments, AMD, Arm Cortex and more), the author provides you with ample details you will need to get the most out of whatever you purchase.

Respect the power!

BOB MONROE

Bob Monroe grew up in Southern California before he joined the U.S. Army in 1985. One of Bob's first military assignments introduced him to the world of hacking. His prankster ways ended abruptly in 1996 when he was almost caught hacking by an eighty-two year old librarian. This incident led to a renewed interest in cyber security, as a good guy. Since then, he has written several articles for publication and maintains a passion for digital security. Bob holds a Master of Science in Information Assurance from Norwich University.

Bob's specialty is cyber teaching and security awareness training. Along with work for the U.S. Army, he has taught security classes for the Veterans Administration, Military District of Washington, Commandant of the Marine Corp and staff, as well as countless others across the world. He holds a U.S. Patent for airport security automation technology that combines radar and thermal imaging to protect aircraft movement areas and the surrounding airspace. This patent does not impress the TSA folks at all and usually gives them a reason to strip search him instead.

Bob works with the Institute for Security and Open Methodologies (ISECOM.org) and Hacker High School as an editor and writer. Both organizations are non-profit, with the mission of teaching computer security methods across a global audience. In his spare time, Bob makes children's toys in his small woodshop. He still has all nine fingers, too. Oops, make that seven fingers

Improve your Firewall Auditing

As a penetration tester you have to be an expert in multiple technologies. Typically you are auditing systems installed and maintained by experienced people, often protective of their own methods and technologies. On any particular assessment testers may have to perform an analysis of Windows systems, UNIX systems, web applications, databases, wireless networking and a variety of network protocols and firewall devices. Any security issues identified within those technologies will then have to be explained in a way that both management and system maintainers can understand.

The network scanning phase of a penetration assessment will quickly identify a number of security weaknesses and services running on the scanned systems. This enables a tester to quickly focus on potentially vulnerable systems and services using a variety of tools that are designed to probe and examine them in more detail e.g. web service query tools. However this is only part of the picture and a more thorough analysis of most systems will involve having administrative access in order to examine in detail how they have been configured. In the case of firewalls, switches, routers and other infrastructure devices this could mean manually reviewing the configuration files saved from a wide variety of devices.

Although various tools exist that can examine some elements of a configuration, the assessment would typically end up being a largely manual process. Nipper Studio is a tool that enables penetration testers, and non-security professionals, to quickly perform a detailed analysis of network infrastructure devices. Nipper Studio does this by examining the actual configuration of the device, enabling a much more comprehensive and precise audit than a scanner could ever achieve.

Device Auditing	Scanners	Nipper Studio
Audit without Network Traffic	✗	✓
Authentication Configuration	✗	✓
Authorization Configuration	✗	✓
Accounting/Logging Configuration	✗	✓
Intrusion Detection/Prevention Configuration	✗	✓
Password Encryption Settings	✗	✓
Timeout Configuration	✗	✓
Physical Port Audit	✗	✓
Routing Configuration	✗	✓
VLAN Configuration	✗	✓
Network Address Translation	✗	✓
Network Protocols	✗	✓
Device Specific Options	✗	✓
Time Synchronization	✗	✓
Warning Messages (Banners)	✓*	✓
Network Administration Services	✓*	✓
Network Service Analysis	✓*	✓
Password Strength Assessment	✓*	✓
Software Vulnerability Analysis	✓*	✓
Network Filtering (ACL) Audit	✓*	✓
Wireless Networking	✓*	✓
VPN Configuration	✓*	✓

* Limitations and constraints will prevent a detailed audit