

# eForensics

## Magazine

**COMPUTER**

VOL.2NO.3

**50+**  
PAGES

# Memory Analysis using DumpIt and Volatility

A PRACTICAL APPROACH TO MALWARE MEMORY FORENSICS |

COLD BOOT MEMORY FORENSICS |

MALWARE FORENSICS & ZEUS |

SECURITY & ONLINE IDENTITY PROTOCOLS: A TESTER'S VIEW |

ESTABLISHING A CENTER FOR DIGITAL FORENSICS |

INVESTIGATIVE SERVICES ON THE CLOUD |

DIGITAL CONTINUITY OF GOVERNMENT RECORDS |



# AnDevCon

The Android Developer Conference

**BOSTON** • May 28-31, 2013

The Westin Boston Waterfront

Get the best real-world Android developer training anywhere!

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

Register Now  
and SAVE!

"AnDevCon is one of the best networking and information hubs available to Android developers."

—Nate Vogt, Android Developer, Willow Tree Apps



Register NOW at [www.AnDevCon.com](http://www.AnDevCon.com)

A BZ Media Event

Follow us: [twitter.com/AnDevCon](https://twitter.com/AnDevCon)

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



**Make them hang on your every word...  
Put them on the edge of their seats  
when you speak...**

**Leave them wanting more...  
It can happen, but ONLY IF YOU GET THIS:**

## **THE ELECTRONIC ADVANTAGE: 101 the Basics**

**This fast-paced, 4-hour, online tutorial is for any  
Skill level and even includes 10 case examples!  
All this for just \$360**



**BONUS GIFT:**  
**The first 50 orders get our incredible  
92 Page Tech Guide, eBook, and Audiobook  
a \$100 value**

**Go here now and order:  
[www.technologicalevidence.com](http://www.technologicalevidence.com)**

**Editors:** Joanna Kretowicz

[jaonna.kretowicz@eforensicsmag.com](mailto:jaonna.kretowicz@eforensicsmag.com)

**Betatesters/Proofreaders:** Roxana Grubbs,  
Kishore P.V, Vaman Amarjeet, Mada R Perdhana,  
Olivier Caleff, Jeff Weaver, Massa Danilo, Craig Mayer,  
Andrew J Levandoski, Richard Leitz, Lee Vigue,  
Elba Stevenson, Shirish Deshpande,  
Jan-Tilo Kirchhoff

**Senior Consultant/Publisher:** Paweł Marciniak

**CEO:** Ewa Dudzic

[ewa.dudzic@software.com.pl](mailto:ewa.dudzic@software.com.pl)

**Art Director:** Ireneusz Pogroszewski

[ireneusz.pogroszewski@software.com.pl](mailto:ireneusz.pogroszewski@software.com.pl)

**DTP:** Ireneusz Pogroszewski

**Production Director:** Andrzej Kuca

[andrzej.kuca@software.com.pl](mailto:andrzej.kuca@software.com.pl)

**Marketing Director:** Joanna Kretowicz

[jaonna.kretowicz@eforensicsmag.com](mailto:jaonna.kretowicz@eforensicsmag.com)

**Publisher:** Hakin9 Media Sp. z o.o. SK

02-682 Warszawa, ul. Bokszerska 1

Phone: 1 917 338 3631

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

## DISCLAIMER!

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

## Dear Readers!

Welcome to new issue of eForensics Magazine, just before Spring Holiday so we hope you'll find some free time to grab the magazine and delve into the topic. This time we shed light on Memory Forensics topic.

Analyzing system memory for artifacts is a technique used by forensic analysts, security specialists and those that analyze malware. Memory forensics plays an important role in investigations and incident response. It can help in extracting forensics artifacts from a computer's memory like running process, network connections, loaded modules, etc. In opening article our dear friend and contributor Dan Dieterle talks about how to obtain a complete copy of system memory from a computer using the easy to use program "DumpIt". We will then take this memory dump and analyze it with the popular memory analysis tool Volatility. In the next article Monnappa K covers the subject of Malware Memory Forensics showing how to use Memory Forensic Toolkits to analyze the memory artifacts with practical real life forensics scenarios whereas Alexander Sverdlov shows us that Cold Boot Memory dumping doesn't have to be so difficult to work with or way too expensive for experimenting.

In the next article Mikel Gastesi, Jozef Zsolnai and Nahim Faza give you an insight into the background of the development of Citadel in order to understand how the Trojan has developed in the manner it has. They take you through the process of examining forensically a sample of Citadel. Though it is important to understand the practical steps one has to take to decode and decrypt a piece of malware, it is also important to understand the why and how of the malware works the way it does.

Furthermore our expert Cordny Nederkoorn discusses possible threats associated with the use of online identity protocols, like OpenID and OAuth, which are used widely in social-media software for social sign on and data sharing. Whereas Rocky Termanini talks about the concept of building a Center for Digital Forensics Investigative Services on the cloud. Offering Digital Forensics as a Service (DFaaS) is an attractive venture which will prove to be profitable and highly successful.

Today there are data-mining techniques that allow the turnaround time on data requests to be measured in minutes. The procedures that are in place though, and the complexity of the operations that a civil servant has to follow, raises the turnaround time to days. The returned data must be the most appropriate, based on the search criteria, which creates the need of identifying and deleting duplicates. In the last article Dr. Stilianos Vidalis and Dr. Olga Angelopoulou present you the issue.

Taking advantage from this publication we would like to ask you for cooperation. Our aim is to be "your" magazine. To be helping hand when you need one and entertainment when you want to forget about your job and follow your passion. What are the topics you'd like us to cover? Tools you'd like to learn? Please share your needs and expectations towards our publications! We would like to ask you for a feedback concerning our work. Please, follow us on Twitter and Facebook, where you can find the latest news about our magazine and great contests. Do you like our magazine? Like it! Share it! We appreciate your every comment!

Enjoy your Spring Break with eForensics!

Joanna Kretowicz  
eForensics Magazine Product Manager  
and eForensics Team



## MEMORY ANALYSIS USING DUMPIT AND VOLATILITY

by Daniel Dieterle

Want an easy way to grab a memory dump from a live system and search it for forensic artifacts? Look no further than DumpIt and Volatility. In this article we will see how to pull pertinent information from a memory dump and cover some basic analysis with Volatility. We will also look at a memory image infected with Stuxnet.

06

12

## A PRACTICAL APPROACH TO MALWARE MEMORY FORENSICS

by Monnappa K

Memory Forensics is the analysis of the memory image taken from the running computer. It plays an important role in investigations and incident response. In this article, we will learn how to use Memory Forensic Toolkits such as Volatility to analyze the memory artifacts with practical real life forensics scenarios.

## COLD BOOT MEMORY FORENSICS

by Alexander Sverdlov

Cyber forensics professionals have long been familiar with memory forensics and its benefits – extracting encryption keys for Full Disk Encryption software, extracting data which was in the memory but not stored on disk after a fast shutdown – passwords, URLs, documents, photos, process names – however, the Cold Boot Memory dumping tools were either too difficult to work with or way too expensive for experimenting.

16

20

## MALWARE FORENSICS & ZEUS

by Mikel Gastesi, Jozef Zsolnai & Nahim Fazal

Citadel appeared early in 2012 and the immediate question that was asked was, is this new malware family or something that the cyber crime community had seen before. Upon examining the malware it quickly became apparent that the malware sample was very closely related to banking Trojan called Zeus that had been existence in one form or another for a few years. It was a variant of Zeus all be it with some new shiny features.

## SECURITY & ONLINE IDENTITY PROTOCOLS: A TESTER'S VIEW

by Cordny Nederkoorn

This article will discuss possible threats associated with the use of online identity protocols, like OpenID and OAuth, which are used widely in social-media software for social sign on and data sharing. OAuth will be used as an example to show how OAuth can be susceptible to malicious attacks, resulting in damage on users or applications that have implemented this protocol. The main attacks and countermeasures will be discussed.

28

34

## ESTABLISHING A CENTER FOR DIGITAL FORENSICS INVESTIGATIVE SERVICES ON THE CLOUD

by Rocky Termanini, PhD, CISSP

The concept of building a Center for Digital Forensics Investigative Services on the cloud is a compelling and totally innovative. Everything is becoming cost effective and cloud-centric, including selling Platform as a Service (PaaS), Software as a Service (SaaS). Now offering Digital Forensics as a Service (DFaaS) is an attractive venture which will prove to be profitable and highly successful.

## DIGITAL CONTINUITY OF GOVERNMENT RECORDS

by Dr. Stilianos Vidalis and Dr. Olga Angelopoulou

The first person to properly report and document the principles of information operations was Sun Tzu, thousands of years ago in his ancient Chinese military treatise. The same principles apply today across all of the different public and private sector organisations. It has become excessively important for public organisations to have the right information on the right time in order to be able to satisfy and service public needs in an appropriate manner, as specified by UK and EU legislation. It is equally important to apply innovation in extracting knowledge from existing data sets in order to proactively satisfy future needs of the public.

46



# MEMORY ANALYSIS USING DUMPLT AND VOLATILITY

by Daniel Dieterle

Want an easy way to grab a memory dump from a live system and search it for forensic artifacts? Look no further than DumpIt and Volatility. In this article we will see how to pull pertinent information from a memory dump and cover some basic analysis with Volatility. We will also look at a memory image infected with Stuxnet.

## What you will learn:

- How to grab a quick and easy dump of active memory
- How to recover forensics artifacts from the memory dump
- How to recover password hashes
- How to recover a process list and network connections
- How to analyze a machine infected with Stuxnet

## What you should know:

- Prior use of Volatility would be recommended but not required
- A Basic understanding of computer forensics
- A Basic understanding of registry use, processes and network connections.

Analyzing system memory for artifacts is a technique used by forensic analysts, security specialists and those that analyze malware.

In this article we will cover how to obtain a complete copy of system memory from a computer using the easy to use program “DumpIt”. We will then take this memory dump and analyze it with the popular memory analysis tool Volatility.

With Volatility, you can pull a list of what software was installed on a system, what processes were running, what network connections were active, and a whole lot more.

We will look at all of this and even see how to pull password hashes from a memory dump. Lastly we will try our hand at analyzing a memory image infected with a sample of Stuxnet.

Sound exciting? Well it is! Let's get started!

## OBTAINING A MEMORY DUMP

MoonSols, the creator of the ever popular “win32dd” and “win64dd” memory dump programs have combined both into a single executable that when executed creates a copy of physical memory and saves it into the current directory.

Simply download DumpIt [1], put it onto a USB drive or save it on your hard drive, double click it, select yes twice and before you know it you have a complete copy of your machine's memory sitting on disk (See Figure 1).

(If you are running it on Windows 7 you will need administrator's rights.)

The only thing you need to make sure of, especially if using a USB drive is that it is large enough to hold



the file that is created. The memory dump will be a little larger than the size of your installed RAM. So, for instance, a machine with 4GB RAM will produce a file almost 5 GBs in size. A system with 8GB of RAM will be about 9.5GB, and so on.

Once we have the memory dump saved, we can now analyze it with Volatility.

Just a note, forensically DumpIt may not be the best solution if you cannot make any changes to the contents of the target system. As you will see later, running DumpIt does add some lines to the command history (Figure 7) on the target system. But if making minor changes to the drive is not that big of a deal, DumpIt is probably one of the best choices for obtaining an easy memory image.

## ANALYZING A MEMORY IMAGE WITH VOLATILITY

Several programs exist for memory analysis; we will be using one of my favorites – “Volatility” [2]. If you are performing your analysis on a Windows system I recommend downloading the stand alone .exe version. You can also choose a version written in Python.

Once Volatility is installed, we need to get some information from the memory dump. Open up a command prompt and run the following command (Figure 2):

```
volatility imageinfo -f memorydumpfilename.raw
```

(Note: This can take a while to run if you have a large dump file.)

The “Imageinfo” command gives you several pieces of information. For now, we just need to know the profile type of the memory dump, in this case Win7SP1x86. We will use this in the next few steps.

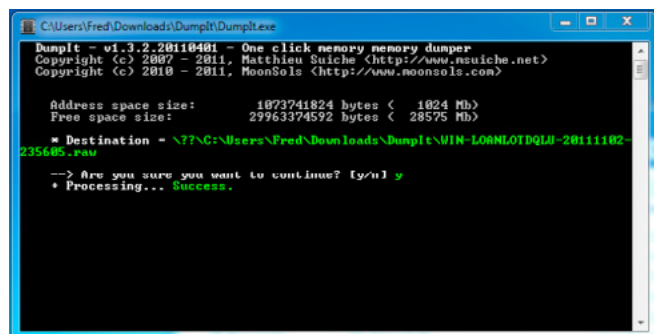


Figure 1. Creating a memory dump file with DumpIt

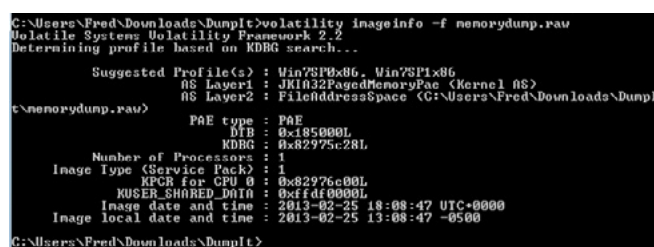


Figure 2. Recovering image information

## ANALYZING REGISTRY KEYS AND OBTAINING PASSWORD HASHES

Now, we need the hive list so we can get the starting location of where the registry information resides (Figure 3):

```
volatility hivelist -f memorydumpfilename.raw  
--profile=Win7SP1x86
```

We now have a list of where several key items are located in the memory dump. We can use this information to find individual artifacts or we can just dump the whole hive list.

To do so, you simply need to use the “hive-dump” command and the virtual memory address to the hive you want to view from the list recovered above. We will take a look at the Software hive, so we will use the virtual offset address of 0x8ccfc9c8 (Figure 4).

```
volatility -f memorydumpfilename.raw --profile=Win7SP1x86  
hivedump -o 0x8ccfc9c8
```

If you noticed from the highlighted areas, this user had 7 Zip installed, was using ATI Technologies software for his video card. He was also running the AVG Anti-Virus program as well as the Intrusion Detection System (IDS).

Using hivedump will return a ton of registry settings, which might be a little more than we need. You can also search the registry keys for specific data.

For example to find the name of the last logged in user you can check the WinLogon registry key as shown in Figure 5:

```
volatility -f memorydump.raw --profile=Win7SP1x86  
printkey -K "Software\Microsoft\Windows NT\  
CurrentVersion\Winlogon"
```

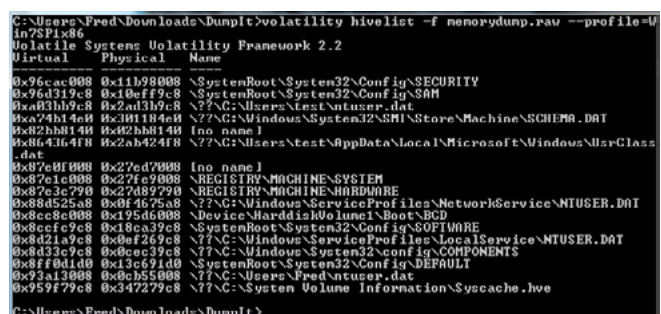


Figure 3. Recovering Hive list with memory location information

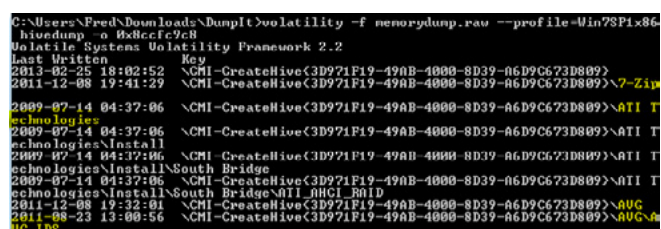


Figure 4. Recovering a complete Hive listing

Recovering registry information is good, but what many don't know is that a copy of the password hashes are stored in active memory. If you can obtain a memory image, you can get the password hashes. This is of importance to security penetration testers because if you have the hashes, you can then proceed to crack them or use them in pass the hash types of attacks to access other systems on the network.

To do this we need to know the starting memory locations for the System and SAM keys. We look in the hivelist above (Figure 3) and copy down the numbers in the first column that correspond to the SAM and SYSTEM locations. Place the virtual address for System in the -y switch and the address for the SAM into -s.

The following command pulls the password hashes out of memory and stores them in a text file called hashes.txt:

```
volatility hashdump -f memorydumpfilename.raw
--profile=Win7SP1x86 -y 0x87e1c008 -s 0x96d319c8 >
hashes.txt
```

Simply check the hash.txt file and you will see the admin hash and the password hashes for any users. Though beyond the scope of this article, these hashes could then be taken and cracked in an on-line hash cracking site or any one of the password cracking programs like John the Ripper or Hashcat.

## PROCESS LIST AND COMMAND HISTORY

Now let's take a look at recovering a list of the running processes and active network connections

```
C:\Users\Fred\Downloads\DumpIt\volatility -f memorydump.raw --profile=Win7SP1x86
printkey -R "Software\Microsoft\Windows NT\CurrentVersion\Winlogon"
Volatility Systems Volatility Framework 2.2
Legend: (S) = Stable (U) = Unstable

Registry: \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
Key name: Winlogon (S)
Last updated: 2007-07-14 04:34:14
Subkeys:

Values:
REG_SZ ExcludeProfileDirs : (S) AppData\Local;AppData\LocalLow;5Recycle.Bin

Registry: \??\C:\Users\Fred\NTUSER.DAT
Key name: Winlogon (S)
Last updated: 2011-09-16 15:58:24
```

Figure 5. Recovering last logged on user information

```
C:\Users\Fred\Downloads\DumpIt\volatility pslist -f memorydump.raw --profile=Win7SP1x86
Volatility Systems Volatility Framework 2.2
Offset(U) Name PID PPID Thds Hnds Sess Woud4 Star
-----
0x84338a20 System 4 0 89 1578 ----- 0 2012
0x84c3bba0 smss.exe 256 4 2 29 ----- 0 2012
0x84c39c48 csrss.exe 568 560 9 609 0 0 2012
0x8521453110 wininit.exe 624 616 11 386 1 0 2012
0x843a8500 wininit.exe 632 560 3 78 0 0 2012
0x84343420 winlogon.exe 668 616 3 114 1 0 2012
0x85306660 services.exe 736 632 7 219 0 0 2012
0x85306670 services.exe 744 632 6 625 0 0 2012
0x85306670 lsass.exe 756 632 10 145 0 0 2012
0x85306670 lsass.exe 768 736 11 367 0 0 2012
0x85809860 svchost.exe 988 736 7 299 0 0 2012
0x857ab770 svchost.exe 1080 736 20 495 0 0 2012
0x857ad030 svchost.exe 1120 736 18 462 0 0 2012
0x857f7b18 svchost.exe 1144 736 32 1328 0 0 2012
```

Figure 6. Displaying a Process list and associated PID numbers

from the captured memory file. Using Volatility's "pslist" command can be used to view the processes that were running on the Windows system (Figure 6):

```
volatility pslist -f memorydumpfilename.raw
--profile=Win7SP1x86
```

From the output of the command, we see the physical memory location, process name and the PID number of all process that were running. You can also use volatility to view the exact programs that may be running under the process. This helps malware analysts track down malicious processes and their associated programs. We will talk more on that later.

Another interesting command we can run is "cmdscan". This plug-in allows us to see what commands, if any, were run from the command prompt (Figure 7).

```
volatility cmdscan -f memorydump.raw
--profile=Win7SP1x86
```

As you can see it captured the steps I used to capture the memory image. I went to the e: drive, changed into the DumpIt directory and ran the command "Dumpit".

```
C:\Users\Fred\Downloads\DumpIt\volatility cmdscan -f memorydump.raw --profile=Win7SP1x86
Volatility Systems Volatility Framework 2.2
CommandProcess: conhost.exe Pid: 2568
CommandHistory: 0x1705d0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 6 LastAdded: 5 LastDisplayed: 5
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 @ 0x16e1a8: e:
Cmd #1 @ 0x16e1d8: dir
Cmd #2 @ 0x16db98: cd dumpit
Cmd #3 @ 0x16f7d8: cd volatility
Cmd #4 @ 0x16e1f8: dir
Cmd #5 @ 0x1662c0: Dumpit
Cmd #10 @ 0x100010: ?
Cmd #16 @ 0x1400c4: ?1777777
Cmd #17 @ 0x16cdd0: ?1777777
CommandProcess: conhost.exe Pid: 2568
CommandHistory: 0x1705d0 Application: Dumpit.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
```

Figure 7. Listing what commands were entered at the command prompt

```
C:\Users\Fred\Downloads\DumpIt\volatility netscan -f memorydump.raw --profile=Win7SP1x86
Volatility Systems Volatility Framework 2.2
Offset(P) Proto Local Address Created Foreign Address State
-----
0x3e770dc0 TCPv4 192.168.52.130:139 0.0.0.0:0 LISTENIN
G 4 System
0x3e7867f0 TCPv4 0.0.0.0:5357 0.0.0.0:0 LISTENIN
G 4 System
0x3e7867f0 TCPv6 :::5357 :::0 LISTENIN
G 4 System
0x3e78e2a8 TCPv4 0.0.0.0:49156 0.0.0.0:0 LISTENIN
G 736 services.exe
0x3e78e2a8 TCPv6 :::49156 :::0 LISTENIN
G 736 services.exe
0x3e7e9358 TCPv4 0.0.0.0:49157 0.0.0.0:0 LISTENIN
G 2092 svchost.exe
0x3e7e9358 TCPv6 :::49157 :::0 LISTENIN
G 2092 svchost.exe
0x3e814728 TCPv4 0.0.0.0:49152 0.0.0.0:0 LISTENIN
G 632 wininit.exe
0x3e840540 TCPv4 0.0.0.0:445 0.0.0.0:0 LISTENIN
G 4 System
0x3e840540 TCPv6 :::445 :::0 LISTENIN
G 4 System
0x3eb75bd0 TCPv4 0.0.0.0:135 0.0.0.0:0 LISTENIN
G 988 svchost.exe
0x3eb75bd0 TCPv6 :::135 :::0 LISTENIN
G 988 svchost.exe
0x3eb99990 TCPv4 0.0.0.0:49152 0.0.0.0:0 LISTENIN
G 632 wininit.exe
0x3eb99990 TCPv6 :::49152 :::0 LISTENIN
G 632 wininit.exe
0x3ebcfe60 TCPv4 0.0.0.0:49153 0.0.0.0:0 LISTENIN
G 1080 svchost.exe
0x3ebcfe60 TCPv6 0.0.0.0:49153 0.0.0.0:0 LISTENIN
G 1080 svchost.exe
0x3ec2ee48 TCPv4 0.0.0.0:135 0.0.0.0:0 LISTENIN
G 988 svchost.exe
0x3ec7d2d0 TCPv4 0.0.0.0:49155 0.0.0.0:0 LISTENIN
G 1144 svchost.exe
```

Figure 8. Using the "netscan" plugin to view active network connections



Not very helpful to us in this case, but a lot of hacker tools are run from the command line. If the user ran any command line programs or utilities, or used the command line to copy data, it would show up here for us to view.

## NETSCAN AND THE BIOS CACHE BUFFER

We can view network connections that were active from the memory dump by using the “netscan” command as shown in Figure 8:

```
volatility netscan -f memorydumpfilename.raw
--profile=Win7SP1x86
```

The data returned shows all network connections, including the process name, source and destination IP addresses – including ports. This is just a short snip of what was actually returned, the actual list is easily three times as long, because the user had several webpages open when the snapshot was taken.

This information helps the analyst see what network connections were active. But it can also help the penetration tester gain valuable information about the network.

The last command that we will look at is “bioskbd” shown in Figure 9.

```
volatility bioskbd -f memorydumpfilename.raw
--profile=Win7SP1x86
```

As you can see there is no data returned from this memory dump. But what does “bioskbd” actually do? This interesting command has the ability to pull passwords that are resident from the bios cache buffer. Though most newer systems (like the system that this memory dump was taken from) purge the bios keyboard buffer, many older ones did not. On an old system you might be able to retrieve BIOS boot passwords, or even the passwords for disk encryption systems.

## MALFIND – VOLATILITY IN ACTION

So far we have learned some interesting things that you can do with Volatility. But how would it be used in the real world?

It been kind of fun playing around with a memory dump from one of our own systems, but wouldn’t it be cool to take a look at some memory dumps that are from infected machines?

Well, you can!

The authors of the Malware Analyst’s Cookbook (exceptional book by the way) have been kind enough to post several memory dumps that you can play with.

So why don’t we take a look at a memory dump from a system infected with Stuxnet?

The memory images are posted on the Volatility project page. Simply download the Stuxnet sample

memory image file [3] and we will see what Volatility can do with an infected image.

First, let’s grab the *imageinfo* information for the Stuxnet memory dump (Figure 10):

```
volatility imageinfo -f stuxnet.vmem
```

Okay, it is a Windows XP SP3 image, so we will use that information with the profile switch.

Next, let’s take a look at what processes were running on the Stuxnet infected machine:

```
volatility pslist --profile=WinXPSP3x86 -f stuxnet.vmem
```

0x81e70020	lsass.exe	680	624
0x81c498c8	lsass.exe	868	668
0x81c47c00	lsass.exe	1928	668

Looking at this list you can see one of the signs of a Stuxnet, there are three copies of lsass.exe running, when there should only be one. The lsass process authenticates users for the Winlogon service.

Let’s do a process tree list and see if all three instances of lsass correspond to Winlogon:

```
volatility pstree --profile=WinXPSP3x86 -f stuxnet.vmem
```

From the process list we see that two of the processes connect to Pid 668 and one connects to 624. Looking at the Pid column from the Process Tree list in Figure 11, you can see that the third instance does in fact tie to Winlogon (624). But the two other instances connect to Services.exe (668).

```
C:\Users\Fred\Downloads\DumpIt>volatility bioskbd -f memorydump.raw --profile=Win7SP1x86
Volatility Systems Volatility Framework 2.2
Racii Scancode
C:\Users\Fred\Downloads\DumpIt>
```

Figure 9. Viewing data from the Bios Cache Buffer

```
C:\Users\Fred\Downloads\DumpIt>volatility imageinfo -f stuxnet.vmem
Volatility Systems Volatility Framework 2.2
Determining profile based on KDBG search...
Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
AS Layer1 : jKi632PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (C:\Users\Fred\Downloads\DumpIt\stuxnet.vmem)
PDE type : PDE
DIB : 0x319000L
KDBG : 0x80545ac0L
Number of Processors : 1
Image Type (Service Pack) : 3
KPCR for CPU 0 : 0xfffff000L
ROSER_SHARED_DATA : 0xfffff000L
Image date and time : 2011-06-03 04:31:36 UTC+0000
Image local date and time : 2011-06-03 00:31:36 -0400
C:\Users\Fred\Downloads\DumpIt>
```

Figure 10. Imageinfo for Stuxnet Image

```
C:\Users\Fred\Downloads\DumpIt>volatility pstree --profile=WinXPSP3x86 -f stuxnet.vmem
Volatility Systems Volatility Framework 2.2
Name Pid PPid Thda Hnda I
-----
0x822c8830: System 4 0 59 403 1
970-01-01 00:00:00
.. 0x820df020: smss.exe 376 4 3 19 2
010-10-29 17:08:53
.. 0x821a2da0: csrss.exe 600 376 11 375 2
010-10-29 17:08:54
.. 0x81da5650: winlogon.exe 624 376 19 570 2
010-10-29 17:08:54
.. 0x82073220: services.exe 668 624 21 431 2
010-10-29 17:08:54
```

Figure 11. Process Tree list for system infected with Stuxnet

Something is not right.

Let's run the "malfind" command and see what it detects. Malfind searches for hidden or injected code or DLLs in user mode memory. We will run malfind against the whole memory dump and see if it can find any suspicious code.

Let's use the `“-D outputfolder”` switch to specify a place for malfind to place any code segments that it finds.

```
volatility malfind --profile=WinXPSP3x86 -f stuxnet.  
vmem -D OutputFolder
```

As you can see from Figure 12 it found numerous samples of malicious code. All of the malicious code segments found were stored in our designated output directory.

But were any of them truly malicious?

If you go to the output directory, you see all the suspicious files stored as .dmp files. You can take these files and upload them to VirusTotal.com to see if it detects anything suspicious. Or if you are running Bitdefender like I was on my analysis machine, just wait a few seconds, and Bitdefender will remove the contents of the directory for you!

Figure 13 is a list of some of the alerts.

Looks like it detected Generic Backdoor, Generic Torjan and Gen:Variant.Graftor.Elzob. A quick internet search and you will find that Graftor.Elzob is also called Trojan.Stuxnet.16 by another AV engine.

We could go on and find Stuxnet registry key settings, hidden Dll's, file objects and numerous other

```

0x01000000 4d 5a 20 00 03 00 00 00 04 00 00 00 ff ff 00 00  NZ.....e
0x01000001 76 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  .....e
0x01000002 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0x01000003 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00  .....
0x10000004 4d                      DEC EBP
0x10000005 5a                      POP EDI
0x10000006 70                      NOP
0x10000007 00001                ADD EBX, AL
0x10000008 00000                ADD [EBX], AL
0x10000009 0000f00            ADD [EAX+EBX], AL
0x1000000a 00000                ADD [EBX], AL
0x1000000b ffffffff             DB 0xffffffff
0x1000000c 0000ff00           INC DWORD [EAX]
0x1000000d 0000S00000000       ADD [EAX+0xb], BH
0x1000000e 00000                ADD [EBX], AL
0x1000000f 0004000        ADD [EAX+0xb], AL
0x10000010 00000                ADD [EAX], AL
0x10000011 00000                ADD [EBX], AL
0x10000012 00000                ADD [EBX], AL
0x10000013 00000                ADD [EAX], AL
0x10000014 00000                ADD [EAX], AL
0x10000015 00000                ADD [EAX], AL
0x10000016 00000                ADD [EAX], AL
0x10000017 00000                ADD [EAX], AL
0x10000018 00000                ADD [EAX], AL
0x10000019 00000                ADD [EAX], AL
0x1000001a 00000                ADD [EAX], AL
0x1000001b 00000                ADD [EAX], AL
0x1000001c 00000                ADD [EAX], AL
0x1000001d 00000                ADD [EAX], AL
0x1000001e 00000                ADD [EAX], AL
0x1000001f 00000                ADD [EAX], AL
0x10000020 00000                ADD [EAX], AL
0x10000021 00000                ADD [EAX], AL
0x10000022 00000                ADD [EAX], AL
0x10000023 00000                ADD [EAX], AL
0x10000024 00000                ADD [EAX], AL
0x10000025 00000                ADD [EAX], AL
0x10000026 00000                ADD [EAX], AL
0x10000027 00000                ADD [EAX], AL
0x10000028 00000                ADD [EAX], AL
0x10000029 00000                ADD [EAX], AL
0x1000002a 00000                ADD [EAX], AL
0x1000002b 00000                ADD [EAX], AL
0x1000002c 00000                ADD [EAX], AL
0x1000002d 00000                ADD [EAX], AL
0x1000002e 00000                ADD [EAX], AL
0x1000002f 00000                ADD [EAX], AL
0x10000030 00000                ADD [EAX], AL
0x10000031 00000                ADD [EAX], AL
0x10000032 00000                ADD [EAX], AL
0x10000033 00000                ADD [EAX], AL
0x10000034 00000                ADD [EAX], AL
0x10000035 00000                ADD [EAX], AL
0x10000036 00000                ADD [EAX], AL
0x10000037 00000                ADD [EAX], AL
0x10000038 00000                ADD [EAX], AL
0x10000039 00000                ADD [EAX], AL
0x1000003a 00000                ADD [EAX], AL
0x1000003b 00000                ADD [EAX], AL
0x1000003c 00000                ADD [EAX], AL
0x1000003d 00000                ADD [EAX], AL
0x1000003e 00000                ADD [EAX], AL
0x1000003f 00000                ADD [EAX], AL
Process: lsass.exe Pid: 1928 Address: 0x000000
Vad Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Flags: Protection: 6
0x00000000 4d 5a 20 00 03 00 00 00 04 00 00 00 ff ff 00 00  0Z.....e
0x00000001 76 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  .....e
0x00000002 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0x00000003 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0x00000004 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....

```

**Figure 12.** *Snippets of Malicious code found by Malfind*

BitDefender has detected an infected item in c:\users\Fred\downloads\dlumpit\malware\process.061c1498c.0600000.dmp. Virus name: Backdoor.Genetic.577628. The file was disinfectd for your protection. If you want to recover the original file, click the Recover button.

Date: Monday, February 25, 2013 5:59:10 PM

BitDefender has detected an infected item in c:\users\Fred\downloads\dlumpit\malware\process.061c1498c.0x1000000.dmp. Virus name: Trojan.Genetic.9217115. The file was disinfectd for your protection. If you want to recover the original file, click the Recover button.

Date: Monday, February 25, 2013 5:59:05 PM

BitDefender has detected an infected item in C:\Users\Fred\Downloads\Dumpit\malware\process.061c147c00.06070000.dmp. Virus name: Trojan.Genetic.Graffo.Etzo.17846. The file was disinfectd for your protection. If you want to recover the original file, click the Recover button.

Date: Monday, February 25, 2013 5:59:01 PM

**Figure 13.** Recovered malicious code deleted by AV engine

## References

- [1] Download Moonsols DumpIt at <http://www.moonsols.com/2011/07/18/moonsols-dumpit-goes-mainstream/>
- [2] Volatility is available at <http://code.google.com/p/volatility/>
- [3] <http://code.google.com/p/volatility/wiki/FAQ>
- [4] <http://mnin.blogspot.com/2011/06/examining-stuxnets-footprint-in-memory.html>

artifacts in this memory sample all with using Volatility. But I will end this simple overview of analyzing Stuxnet here.

If you want to see a complete dismantling of Stuxnet with Volatility by an expert analyst (and creator of Volatility), check out Michael Hale Ligh's post "Stuxnet's Footprint in Memory with Volatility 2.0" [4].

## CONCLUSION

In this article we learned how to obtain a memory image from a system and several techniques to analyze it using Volatility. We also took a quick look at analyzing a system infected with malware.

Honestly, I have actually only covered the tip of the ice berg in using Volatility. It is capable of doing so much more.

Volatility is still evolving and new features are being added to it. The next version of Volatility (2.3) is slated to be out in April of this year. Several new plugins will be available for it (including an IE History Cache plugin!) and I also thought that Windows 8 support would be added, though I did not see it listed on the Volatility project page.

Dumplt and Volatility, two excellent tools for any Analyst's toolbox!

## Author bio



*Daniel Dieterle has 20 years of IT experience and has provided various levels of IT support to numerous companies from small businesses to large corporations. He enjoys computer security topics, is an internationally published security author and is the creator of the CyberArms Com-  
og (cyberarms.wordpress.com). He can be  
arms@live.com.*



# F.S.S.C.

## Forensic Security Solutions Co.

### A Computer Forensics and Network Security Consulting Co.

- Forensic Imaging & Preservation of Digital Data
- Forensic Analysis & Investigations
- E-Discovery Collections
- Targeted & Multi-User Collections
- Risk & Threat Analysis
- Vulnerability Assessment
- Penetration Testing
- Forensic Wiping of Digital Data Sources (Hard Drives, Thumb Drives, etc.)

Forensic Security Solutions Company is geared toward providing their customers with extraordinary project management and client interfacing that can be utilized for any size matter. Feel free to check us out at [www.ForensicSSC.com](http://www.ForensicSSC.com)

# F.S.S.C.



Tel: (908) 917-1482

Email: [Contact@ForensicSSC.com](mailto:Contact@ForensicSSC.com)

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

# A PRACTICAL APPROACH TO MALWARE MEMORY FORENSICS

by Monnappa K

Memory Forensics is the analysis of the memory image taken from the running computer. In this article, we will learn how to use Memory Forensic Toolkits such as Volatility to analyze the memory artifacts with practical real life forensics scenarios. Memory forensics plays an important role in investigations and incident response.

## What you will learn:

- Performing memory forensics
- Tools and techniques to Perform Memory forensics
- Volatility usage

## What you should know:

- Basic understanding of malware
- Knowledge of operating system process

It can help in extracting forensics artifacts from a computer's memory like running process, network connections, loaded modules etc. It can also help in unpacking, rootkit detection and reverse engineering.

## STEPS IN MEMORY FORENSICS

Below is the list of steps involved in memory forensics

- **Memory Acquisition** – This step involves dumping the memory of the target machine. On the physical machine you can use tools like *Win32dd/Win64dd*, *Memoryze*, *Dumplt*, *FastDump*. Whereas on the virtual machine, acquiring the memory image is easy, you can do it by suspending the VM and grabbing the “.vmem” file.
- **Memory Analysis** – once a memory image is acquired, the next step is

analyze the grabbed memory dump for forensic artifacts, tools like *Volatility* and others like *Memoryze* can be used to analyze the memory

## VOLATILITY QUICK OVERVIEW

Volatility is an advanced memory forensic framework written in python. Once the memory image has been acquired Volatility framework can be used to perform memory forensics on the acquired memory image. Volatility can be installed on multiple operating systems (Windows, Linux, Mac OS X). Installation details of volatility can be found at <http://code.google.com/p/volatility/wiki/FullInstallation>.

## VOLATILITY SYNTAX

- Using `-h` or `-help` option will display help options and list of available plugins



**Example:** python vol.py -h

- Use -f <filename> and -profile to indicate the memory dump you are analyzing

**Example:** python vol.py -f mem.dmp -profile=WinXPSP3x86

- To know the -profile info use below command:

**Example:** python vol.py -f mem.dmp imageinfo

## DEMO

In order to understand memory forensics and the steps involved. Let's look at a scenario, our analysis and flow will be based on the below scenario.

## DEMO SCENARIO

Your security device alerts on a malicious http connection to ip address 208.91.197.54 from a source

ip 192.168.1.100 on 8<sup>th</sup> June 2012 at around 13:30hrs. you are asked to investigate and do memory forensics on that machine 192.168.1.100

## MEMORY ACQUISITION

To start with, acquire the memory image from 192.168.1.100, using memory acquisition tools. For the sake of demo, the memory dump file is named as "infected.dmp".

## ANALYSIS

Now that we have acquired "infected.dmp", let's start our analysis

## STEP 1: START WITH WHAT WE KNOW

```
root@bt: ~/Volatility
root@bt:~/Volatility# python vol.py -f infected.dmp connections
Volatile Systems Volatility Framework 2.0
Offset(V) Local Address Remote Address Pid
-----
0x8943a558 192.168.1.100:1032 208.91.197.54:80 1748
```

We know from the security device alert that the host was making an http connection to 208.91.197.54. So let's look at the network connections.

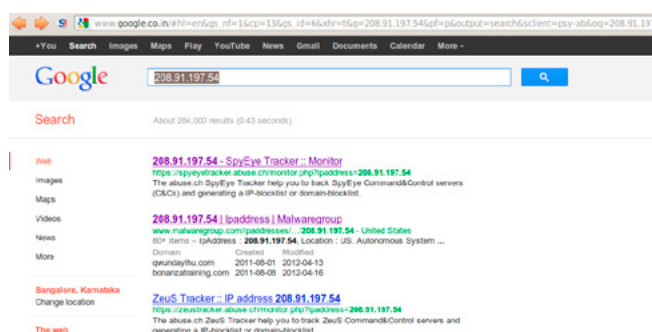
Volatility's connections module, shows connection to the malicious ip made by pid 1748

## STEP 3: WHO IS PID 1748?

```
root@bt:~/Volatility# python vol.py -f infected.dmp psscan
Volatile Systems Volatility Framework 2.0
Offset Name Pid PPID PDB Time created Time exited
-----
0x8932b020 B6232F3A9F9.exe 1672 1748 0x0f9c02a0 2012-06-08 13:27:55 2012-06-08 13:27:56
0x89339020 vmpryse.exe 584 880 0x0f9c0260 2012-02-26 12:07:19
0x8934c4a8 WdggradeHelper 428 780 0x0f9c0240 2012-02-26 12:07:19
0x89350740 vmtoolsd.exe 216 780 0x0f9c0220 2012-02-26 12:07:19
0x8935a360 explorer.exe 1748 1712 0x0f9c01c0 2012-02-26 12:07:17
0x893662b8 svchost.exe 964 780 0x0f9c0100 2012-02-26 12:07:11
0x894c6da0 svchost.exe 880 780 0x0f9c00e0 2012-02-26 12:07:11
0x895f1a58 cfmon.exe 1092 780 0x0f9c0200 2012-02-26 12:07:18
0x8964c020 cmd.exe 1648 1888 0x0f9c0280 2012-06-08 13:27:53
0x89656020 VMwareUser.exe 1888 1748 0x0f9c01e0 2012-02-26 12:07:18
0x89665630 winlogon.exe 636 376 0x0f9c0060 2012-02-26 12:07:11
0x897166a8 VMwareTray.exe 1880 1748 0x0f9c0180 2012-02-26 12:07:18
0x8971ca38 svchost.exe 1092 780 0x0f9c0140 2012-02-26 12:07:11
0x89732da0 csrss.exe 632 376 0x0f9c0040 2012-02-26 12:07:10
0x897aebf0 services.exe 780 656 0x0f9c0080 2012-02-26 12:07:11
0x89811020 lsass.exe 712 656 0x0f9c00a0 2012-02-26 12:07:11
0x89821020 smss.exe 376 4 0x0f9c0020 2012-02-26 12:07:10
0x8984c8e0 svchost.exe 1124 780 0x0f9c0160 2012-02-26 12:07:11
0x8984e170 svchost.exe 1048 780 0x0f9c0120 2012-02-26 12:07:11
0x89852300 vmacthlp.exe 868 780 0x0f9c00c0 2012-02-26 12:07:11
0x8992b830 System 4 0 0x03190000
```

Since the network connection to the ip 208.91.197.54 was made by pid 1748, we need to determine which process is associated with pid 1748. "psscan" shows pid 1748 belongs to explorer.exe, also two processes created during same time reported by security device (i.e. June 8<sup>th</sup> 2012)

## STEP2: INFO ABOUT 208.91.197.54



Google search shows this ip 208.91.197.54 to be associated with malware, probably "SpyEye", we need to confirm that with further analysis.

## STEP 4: PROCESS HANDLES OF EXPLORER. EXE

```
root@bt:~/Volatility# python vol.py -f infected.dmp handles -p 1748 -t Process
Volatile Systems Volatility Framework 2.0
Offset(V) Pid Type Details
-----
0x8915a348 1748 Process explorer.exe(1748)
0x8912b008 1748 Process B6232F3A9F9.exe(1672)
0x8912b008 1748 Process B6232F3A9F9.exe(1672)
```

Now that we know explorer.exe (which is an operating system process) was making connections to the malicious ip, there is a possibility that explorer.exe is infected. Let's look at the process handles of explorer.exe. The below screenshot shows Explorer.exe opens a handle to the B6232F3A9F9.exe, indicating explorer.exe might have created that process, which might also be malicious...let's focus on explorer.exe for now





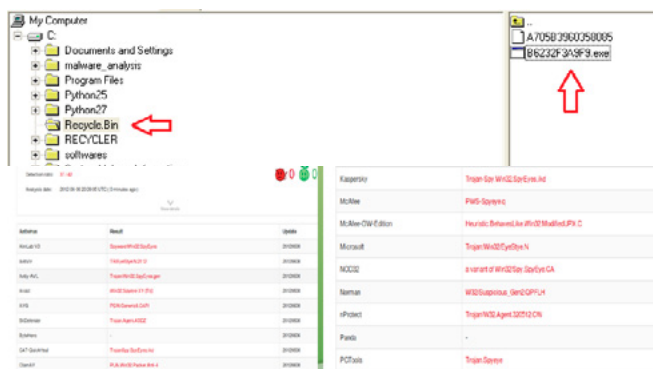
## STEP 11 – PRINTING THE REGISTRY KEY

```
root@kali:~/Volatility# python vol.py -f infected.dmp printkey -K "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
Volatility System Volatility Framework 2.0
Legend: (S) = Stable (V) = Volatile

Registry: \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
Key name: Run (S)
Last updated: 2013-10-31 15:07:20
Subkeys:
Values:
Registry: \Device\HarddiskVolume1\Windows\system32\config\default
Key name: Run (S)
Last updated: 2013-10-31 20:20:57
Subkeys:
Values:
Registry: \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
Key name: Run (S)
Last updated: 2012-06-08 13:27:56
Subkeys:
Values:
REG_SZ ctfmon.exe (S) C:\WINDOWS\system32\ctfmon.exe
REG_SZ 4239C3A1F7X2WKCQCUD (S) C:\Recycle.Bin\B6232F3A0F9.exe
```

Printing the registry key determined from the above step (step 10) shows that, malware creates registry key to survive the reboot

## STEP 12 – FINDING THE MALICIOUS EXE ON INFECTED MACHINE

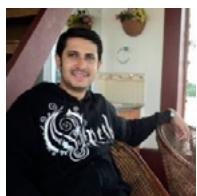


Now that we know the path to the suspicious exactable, let's find it on the infected machine. Finding malicious sample from infected host and virustotal submission confirms SpyEye infection.

## CONCLUSION

Memory forensics is a powerful technique and with a tool like Volatility it is possible to find and extract the forensic artifacts from the memory which helps in incident response, malware analysis and reverse engineering.

### Author bio



Monnappa K A is based out of Bangalore, India. He has an experience of 7 years in the security domain. He works with Cisco Systems as Information Security Investigator. He is also the member of a security research community SecurityXploded (SX). Besides his job routine he does reasearch on malware analysis and reverse engineering, he has presented on multiple topics like "Memory Forensics", "Advanced Malware Analysis", "Rootkit Analysis" and "Detection and Removal of Malwares" in the Bangalore security meetings. You can view the video demos of all this presentations by subscribing to this YouTube channel: <http://www.youtube.com/user/hackycracky22>.

## Cost of CCTV



1,8m CCTV Cameras in the UK



64%  
of cases  
involve CCTV



74%  
of CCTV footage  
comes from  
private sources



£30 per hour  
**£5040**  
surveillance  
cost per week  
per camera



5  
Officers



4  
Weeks of  
viewing  
Footage



40  
hours  
work



£30  
per hour

**£24,000 cost  
per criminal  
investigation**



39m man - hours  
per year across  
all 43 UK police forces



£30 per hour  
**£1,170m**  
Cost per year

### Solution



1  
Week  
footage



5 1/2  
hours  
work



**Save 95%  
of time**

Kinesense Limited  
79 Merrion Square  
Dublin 2, Ireland

e info@kinesense-vca.com  
t +353 (0) 16624546  
t UK +44 (0) 207 0961 550

# COLD BOOT MEMORY FORENSICS JUST GOT EASIER

by Alexander Sverdlov

Cyber forensics professionals have long been familiar with memory forensics and its benefits – extracting encryption keys for Full Disk Encryption software, extracting data which was in the memory but not stored on disk after a fast shutdown – passwords, URLs, documents, photos, process names – however, the Cold Boot Memory dumping tools were either too difficult to work with or way too expensive for experimenting.

## What you will learn:

- why memory forensics is important and how it can aid in obtaining evidence on an otherwise locked down and encrypted machine.
- how to use the tools mentioned in the article.
- the various caveats when dealing with memory forensics

## What you should know:

- Basic digital forensics background is desirable as the article does not discuss forensics in general, rather going directly to the technical issues.

One way to extract the encryption keys of an encrypted drive is to use a memory dump tool such as *Dumplt* (<http://www.moonsols.com/2011/07/18/moonsols-dumpit-goes-mainstream/>) while the machine is still running – which is the optimal variant, if you have access to the OS while it is still running and the desktop has not been locked with an unknown password.

There are tools to bypass the lock screen and tools to dump memory via FireWire – but this article will not get into them as they are far from the topic of Cold Boot memory dumping.

In order to obtain an image of the RAM contents after the computer has been shut down or rebooted (for example, by a criminal who has encrypted their drive and shuts the computer down once they know the police is at the door) – you need to

boot the computer with a live CD or a USB drive, which would then allow you to ‘dump’ the memory image on a drive for later analysis.

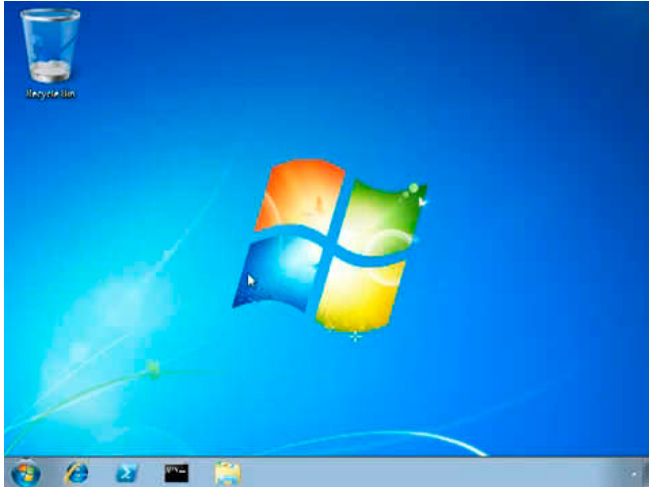
The two options which were freely available were for Linux (*msramdmp*) and BSD (*bios\_memimage*) – with the latter needing specialized build environment just to compile.

This all has changed since NoPaaSara developed and offered for free to the forensics community 2 small programs – both of them deal with the issue of performing a Cold Boot Memory Dump – and then extracting it to a file for later analysis.

## WHAT IS A COLD BOOT MEMORY DUMP?

It is the process of extracting the contents of memory after a reboot. Some of you might already be aware, that information is not wiped out of RAM





on reboot or shutdown – it is slowly decaying (especially if/when cooled down with liquid nitrogen) – which is useful, if the suspect computer drive is fully encrypted and you have no other means of extracting evidence but to hope for information being left in RAM.

Princeton University published an academic research on this topic in 2008 – since then, mostly due to the technical requirements to test their research, little to no further work has been done with the exception of the tool called *msramp* – which is, again, command-line based and can only be used by advanced Linux users.

According to the research published by Princeton University, data is retained in RAM chips for seconds to minutes after a reboot – even if the chips are physically removed from the motherboard.

The challenge here is quickly extracting the data from the chips – which is impossible with *msramp* as it's incredibly slow and this tool can only be used as a proof-of-concept.

## SOME CAVEATS

You must remember that information in RAM decays at a relatively rapid pace – especially with DDR3. Also, if you are working at a server – ECC ram cannot store information after a reboot, as all information is wiped on boot.

If the computer you are working with is a laptop, you will have a greater success in extracting some information from RAM after a reboot due to the power provided by its battery – whereas desktop computers need really rapid intervention in the form of liquid nitrogen memory cool-down in order to preserve the information stored in ram long enough for you to have time to extract it.

The data will continue decaying even after you power on the machine again, boot from a specialized USB drive and start dumping the memory to the USB drive – you can help the process by cooling down the chips using liquid nitrogen, for example – and continue cooling them down until the

process is finished. For 2GB or RAM it takes hours with *msramp* and about 30 minutes with the Princeton University bootable version.

You must remember, that if you decide to test the original tools developed by Princeton, you will most likely need a BSD system (the code does not compile well in Linux) – and even then it requires a decent amount of time to get the code to compile.

By struggling many hours with it, we decided to build our own tool using the code by Princeton and release it free to the public – after all, the code we used was freely available as well.

## USING RAM EXTRACTOR

NoPasara has developed 2 versions of their RAM Extractor program (both are completely free with no obligations) – both aim at doing the same thing, just one of them – the *msramp* version – is more of a proof-of-concept and should only be used for testing, as its speed is extremely slow (due to the original slow code of *msramp* – <http://www.mc-grewsecurity.com/tools/msramp/>)

The second version, the one which is based on the open source code released by Princeton University, is much faster and much more efficient, allowing for more data being captured before it decays completely (Figure 1).

You can download it from <http://nopasara.com/products/ram-extractor-princeton-version/> – once you extract the zip file, you will end up with 1 executable file, named *PrincetonExtractor-x86.exe*.

Right-click on that file, choose Properties, then click on Unblock.

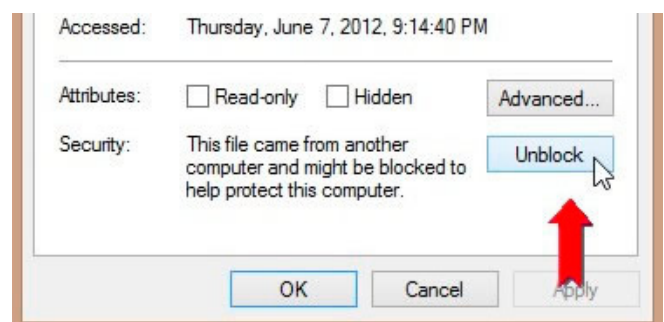


Figure 1. How to install the application

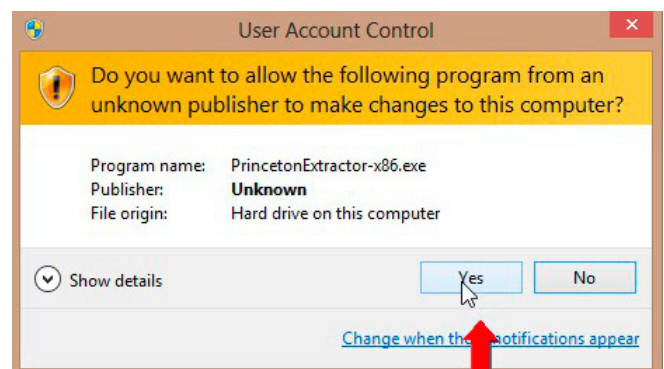


Figure 2. Next step

Click OK.

Insert a USB drive large enough to hold the entire RAM size (4GB or larger, up to 16GB on newer laptops) + a few extra Megs just in case (Figure 2).

Run the program – it will ask you for administrative rights (in order to be able to create partitions on the USB drive and convert it to a bootable drive): Figure 3.

Give the program permissions by clicking Yes and you will be greeted by the simple user interface.

To prepare your USB drive for use, click “Sanitize & Arm USB”. Be patient, the RAM Extractor now wipes your USB drive completely to prevent any data leftovers – it may take hours, depending on your drive size.

Once done, you are ready to boot your computer from the USB drive – please be patient as dumping a few gigabytes of data can take a while, especially with USB 2.0 speeds (Figure 4).

When completed, feel free to shut down the suspect / target computer – no modifications have been made to the hard drive so it is technically forensically intact.

Remove the USB drive and plug it in into your computer again – run the Princeton RAM Extractor and choose “Save RAM dump to file”:

You can then use your favorite forensics toolkit (FTK, EnCase, OSForensics or just Foremost / strings in Linux) to extract useful data from the RAM image.

Please remember, that you must cool down the RAM chips immediately after shutdown / restart and if possible act swiftly – as data in DDR3 chips decays with a really fast pace, even if powered on by a battery in a laptop. This is especially true for desktops where there is no battery to support the RAM after shutdown.

## NOTE

*You will not be able to use that USB drive in Windows anymore! It will only be useful for dumping RAM memory to file, unless you use your favorite partitioning software (I prefer GParted – <http://gparted.sourceforge.net/download.php> ) to create new partitions on the USB drive.*



Figure 3. Running the program

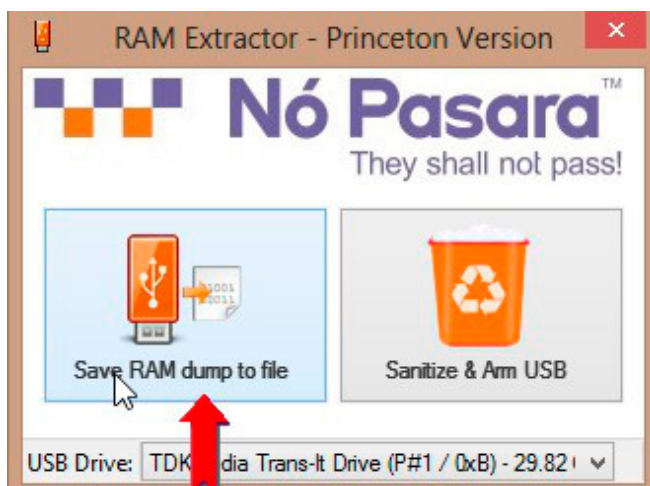


Figure 4. Booting from usb drive

## Author bio



Alexander Sverdlov is the founder of No-Pasara – an information security services & training startup. He has worked for large companies such as Hewlett-Packard and Axway, to name a few. Has no academic background but possesses extensive knowledge in INFOSEC and is often contacted for projects related to digital forensics and incident response from clients across the globe.



# Need help with compliance?



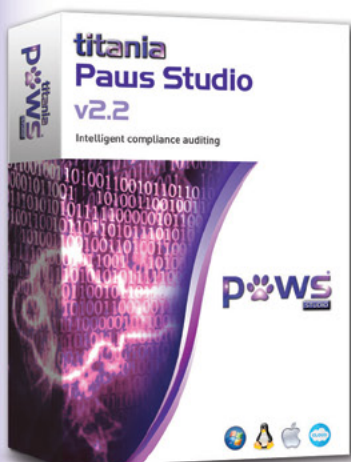
## Use Paws Studio to audit your workstations and servers

Paws Studio is efficient, easy to use and cost effective. The software provides comprehensive reporting and management summaries to appeal to all levels of your organization.

With Paws Studio you can:

1. Produce remote compliance audits using remote connectivity or audit offline with our unique Data Collector
2. Use the Remedy Table to quickly solve potential compliance issues
3. Create and modify your own policies using the Paws definition editor

**evaluate for free at**  
**[www.titania.com](http://www.titania.com)**



...from the creators of award winning Nipper Studio software

Compliance Checklist	Paws Studio
Antivirus	✓
Spyware	✓
Audit Policy	✓
Files & Directories	✓
Windows Firewalls	✓
Password Policies	✓
Password Warnings	✓
Permissions	✓
Registry Settings	✓
Software Updates	✓
Installed Software	✓
Illegal Software	✓
Software Versions	✓
User Policies	✓
User Rights	✓



**[enquiries@titania.com](mailto:enquiries@titania.com)**  
**T: +44 (0) 1905 888785**

# MALWARE FORENSICS & ZEUS

by **Mikel Gastesi, Jozef Zsolnai & Nahim Fazal**

During the course of this article you will learn all about the banking Trojan that goes by the name of Citadel. It is important to point out that the sample we are using in this article is an older version of the malware; the current version is V1.3.5.1 we will provide you with high level overview for this piece of code from its inception to its latest incarnation.



## What you will learn:

- Basic malware analysis techniques
- An understanding of the Zeus Trojan and infection artifacts
- How some easily available tools can be leveraged for malware analysis
- Malware lab overview using a VM environment

## What you should know:

- Basic understanding of the Windows environment
- Familiarity with the Windows command line
- Familiarity with hex editors

**Y**ou will gain an insight into the background of the development of Citadel in order to understand how the Trojan has developed in the manner it has. We will then take you through the process of examining forensically a sample of Citadel. Though it is important to understand the practical steps one has to take to decode and decrypt a piece of malware it is also important to understand the why and how of the malware works the way it does. By the end of the article you should have a very good understanding generally about banking Trojans and in particular about Citadel. The objective here is not to lead you through a step by step guide on how we analysed a single piece of malware. What we want to cover is the methodology used and this approach can be used irrespective of the malware sample you are working with.

## BACKGROUND TO THE MALWARE

Citadel appeared early in 2012 and the immediate question that was asked was, is this new malware family or something that the cyber crime community had seen before. Upon examining the malware it quickly became apparent that the malware sample was very closely related to banking Trojan called Zeus that had been existence in one form or another for a few years. It was a variant of Zeus all be it with some new shiny features.

It was advertised in various underground forums laying claim to new characteristics, but also admitting to being a variation on Zeus. Below you will see directly a snap shot of the actual language used by the cyber criminals to promote this malware to the underground buying fraternity.



Competition is strong for banking Trojans and just like the real world the marketing campaign pushes hard to have the new product noticed.

“We’re offering a great solution for creating and updating your botnet. We’re not trying to re-invent the wheel or come up with a revolutionary product. We have simply perfected the good old Zeus, making significant functionality improvements...”

The key objective of the malware in this instance is to grab banking credentials from innocent users by injecting the malicious code into a legitimate banking session. Once the banking credentials have been captured the malware will then attempt to take money from the users’ online account and transfer it before the user or the bank have an opportunity to spot what has happened. It is important to note that banks have developed a number of counter measures to combat the threat from banking Trojans. Below you can see what the user is presented with once the malware runs and injects into a session.

To give you an insight to how much development work has gone into producing this code here is what it costs to buy in the underground market, \$2400 for the builder and an administration panel, plus a monthly fee of \$125, and add on for additional services.

## METHODOLOGY – THE ENVIRONMENT

The first step once you have your sample of Citadel is to build a controlled environment in which it can be examined quickly and efficiently. The most common approach currently to creating this controlled environment is to use virtual software. You can choose any flavour out there currently and a quick Google search will provide you with a number of suitable candidates. I want to avoid mentioning a specific vendor in case it is viewed either an explicit or implicit endorsement. Using a virtual environment will allow you to emulate both servers and workstations on a single machine.

Each virtual PC or server that you create runs as if it was an independent machine and it is also possible to run different OS on your different machines. So you could for example have a virtual machine running Windows or Mac OS. Each virtual machine has its own unique IP and hardware resources.

What do you need in terms of hardware to run a virtual environment? With the hardware specs that are currently available today you could comfortably set up your virtual environment on a laptop and that would suffice. Of course if you choose to run this on a powerful desktop machine this would leave at your disposal a greater range of processing power and hooking your machines up to large displays may be much more convenient than working on a cramped laptop machine. We would suggest running virtual environments on your host machine that encompass both Windows 7 X86 X64 and also Windows XP. The host machine simply refers to the machine on which your virtual machines are essentially running on.

It is important to note that once you have your virtual machines up and running you will have at your disposal a virtual network too. Your virtualisation software will allow you to connect your virtual installations together thereby giving you a virtual network. All traffic generated by your machines will stay within your virtual network allowing for a few assumptions which I will cover later. What I would strongly recommend is that you take practical steps to ensure that your controlled environment is isolated from your physical network to ensure that if you do make any mistakes or overlook something you are not running the risk of infecting your production network. You can if you chose to run a DHCP service which will manage IP address allocation.

The biggest advantage that a virtual environment offers is the ability to infect and trash each virtual installation. All you have to make sure is that you make a back up of the files which “contain” each virtual machines configuration files. This will also allow you test machines with slight variations in configuration to gain a better understanding of how the malware functions. For example is the malware only able to infect a windows machine running a certain patch level? Does the malware have the ability to infect machines running different OS? It could be that the malware will have a run only once on a machine feature, built it into it meaning that you will have to trash your virtual machine and infect yourself on new VM if you want to capture the install process. Lastly an important point to draw to your attention is that some of the latest variants of banking Trojans are now actively looking to see if they are being run in a virtual environment. If they detect that they are they will not execute.

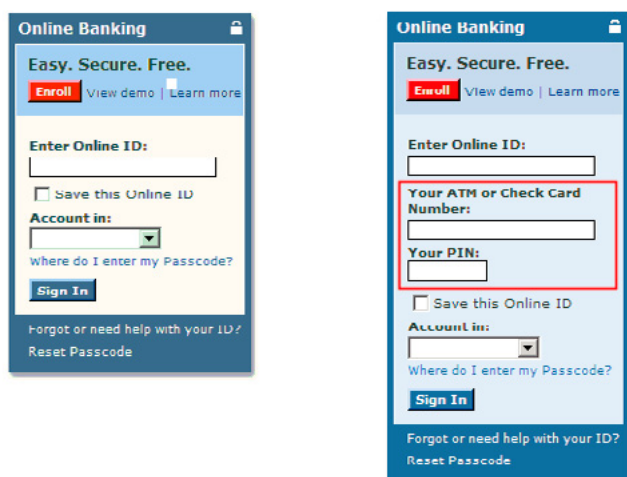


Figure 1.

## WHAT TO LOOK OUT FOR

Once your virtual environment is up and running what you need to focus on once the malware is running is what key changes it is making to your system. There will be files created, deleted, registry keys modified and network traffic generated. These footprints that most samples malware leave behind give you a good starting point to begin your forensic examination of what the malware is doing. There are a range of free tools that will enable you to understand what is happening on the infected system. One of the most useful software suites is Sysinternals. We are not going to cover in exhaustive detail what is contained within the software bundle but we will highlight some really useful tools. In particular, you would want to make use of Autoruns and Filemon. There is also a useful tool that an experienced investigator can use to examine the presence of rootkits on an infected machine. What you will need to do before you attempt to capture what changes are being made to your system is to make sure you have based lined your system before you introduced the malware into your environment.

In order to capture network traffic generated by your malware you can use something like Snort or WireShark. This will allow you to capture and browse network traffic as it is being generated. Figure 2 shows the out from Snort.

It is worth while noting that although some VM software may have built-in tools to capture network traffic it may not be sufficient for the purposes of malware forensics. We feel that you really need a

```
Running in packet dump mode
---- Initializing Snort ----
[Initializing Output Plugins]
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Decoding Ethernet

---- Initialization Complete ----

--> Snort! <--
Version 2.9.0.4 IPv6 (Build 110)
By Martin Roesch & The Snort Team: http://www.snort.org/snort-snort-t
eam
Copyright (C) 1998-2011 Sourcefire, Inc., et al.
Using libpcap version 1.1.1
Using PCRE version: 8.12 2011-01-15
Using ZLIB version: 1.2.5

Commencing packet processing (pid=16768)
```

Figure 2. Network traffic - the out from Snort

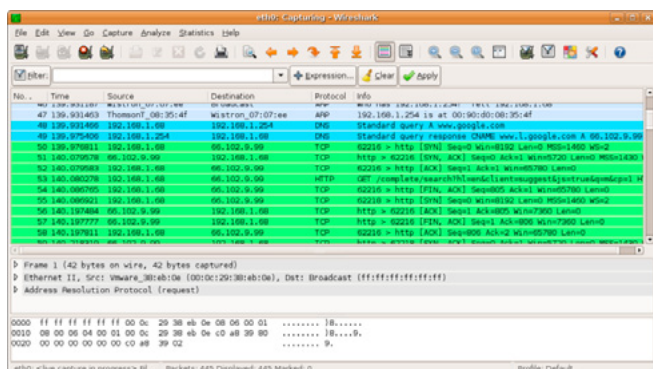


Figure 3. Output from WireShark

tool that is much more agile and capable of producing more targeted results and hence it is much better to opt for something more specialised such as WireShark or Snort. The next step will be to focus on gaining an understanding of how the malware actually works. What the previous steps allow you to do is to capture the footprints that the malware is going to leave behind on the infected machine. This evidence is useful in two ways. Firstly it allows you to understand how the malware behaves once it is running and secondly it will provide you an insight into what the core functions are of the malware. But we are going to need to delve deeper into the malware itself to understand what its key functions are in other words what is the purpose of the malware. In order to reverse engineer the executable associated with your malware you will need two key tools and these are a debugger and a disassembler. The process of debugging and disassembling the software will tell you what is it the malware looking to do. In this instance this process will tell us what files are being injected who or what is the target of the attack. How is the attack being played out? This is all vital evidence that can be used to produce a high level report to report on key questions. The first and the most fundamental question to be answered is what is the malware attempting to do. In this instance it is looking to inject into the users banking session and attempt to take money from the victims account. The second question is how it is attempting to do this.

To complete our analysis it is worth mentioning two additional tools that can be used when you are carrying out your investigation. In most versions of UNIX you will find something call a string programme. This can be useful to use in some instances because it has the ability to allow you to extract strings from executables and finally good old Perl as it can be used to automate some of the more common tasks associated with malware analysis.

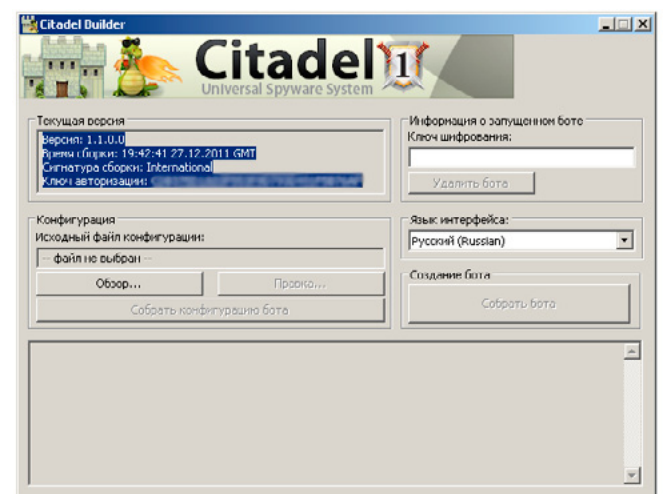


Figure 4. Builder for version 1.1.0.0 (Source: cyb3rsleuth.blogspot.com)



## INFECTION AND STARTUP

In this section we will analyse the Trojan's infection and start-up processes, to review its functional behaviour and at the same time compare it to already known versions of Zeus. Below you can see a Figure 4 of the builder, which is exactly the same as that of Zeus, but slightly customised with the name of Citadel.

The dropper weighs in at 175 Kb, similar in size to versions of Zeus (understandably so, bearing in mind its origin). The file comes packaged in a customised packer with numerous sections (10 sections plus the final data), amongst which, one can observe how the compression algorithms have been applied.

Curiously, they attempt to deceive the user by using the file properties by using the name of the Polish antivirus Arcavir, from the company Arcabit (Figure 6).

Once the file executes, the installation is similar to a Zeus installation, with a few changes. The file is created with a pseudo-random name, inside

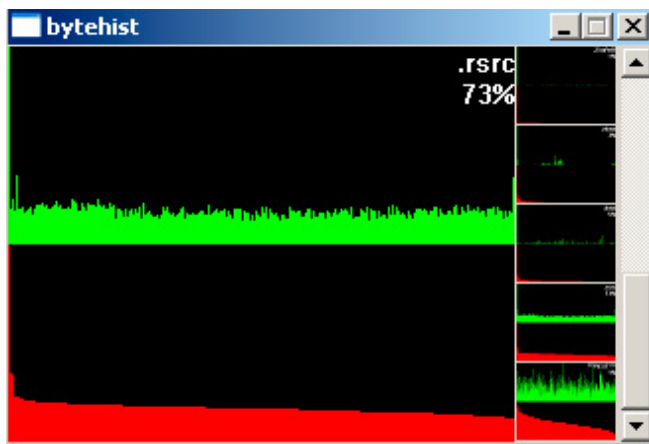


Figure 5. Histogram of bytes

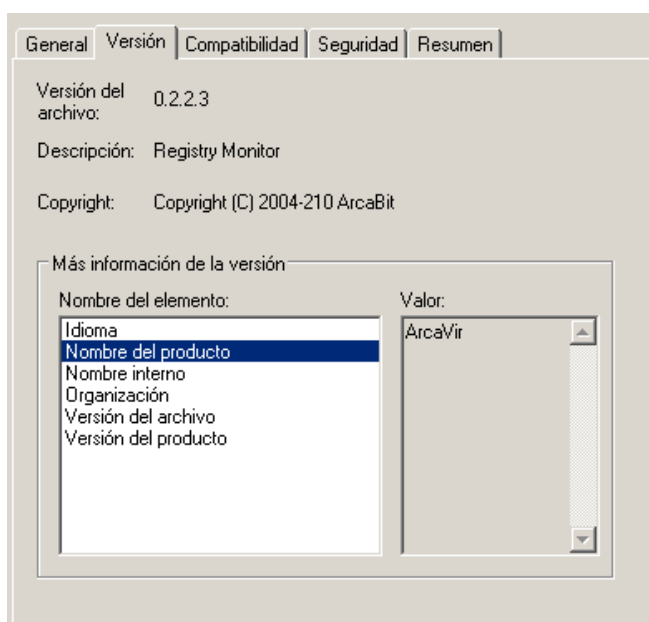


Figure 6. File properties

a folder with another pseudo-random name. The folder is stored in %appdata%, and the survival path inserted in the usual registry. The registry entry and the file are perfectly visible to the user, as no concealment techniques are used (Figure 7).

The use of these paths means the Trojan runs with limited user accounts, without even showing UAC warnings. The Trojan only accesses resources to which it has permission, not like the early versions of Zeus that needed administrator permissions.

The file that runs each time the machine starts up is different from the original, since it incorporates some encrypted bytes at the end, that store information about the machine. The most important information held is:

- Machine Name (Green)
- Unique machine identifier (Black)
- 16 byte key to decrypt the configuration through AES (Red)
- Relative paths to the files and the registry entries (Final names; Figure 8)

The bytes marked in black are the identifier of the infected machine, and are used to check that the machine that runs the malware is the same machine infected by the dropper. These same values are created in each Trojan run and compared to those stored in the file, so that if they do not agree it signifies a different runtime environment and will terminate the binary. It is also worth pointing out that the key stored in this chunk is not the same as the one used to decrypt the configuration file (downloaded from the Web). The configuration is stored once encrypted with a new key.

During start up, a peculiar characteristic of Zeus versions 2 is to search a certain part of the source code using a decryption of 4 bytes with RC4 to find the string "DAVE", something Citadel continues to do (Figure 9).

Once all the checks have taken place, the Trojan injects code into the explorer.exe process, and

Figure 7. Registry entry for system restart survival

Address	Hex dump	ASCII
0012FB58	F4 00 00 00 54 00 45 00 53 00 54 00 31 00 32 00	6...T.E.S.T.I.2
0012FB69	33 00 2D 00	2..
0012FB78	38 00 5F 00	8..
0012FB88	31 00 31 00	1.1.
0012FD00	00 00 32 00 00 00 00 00 00 00 00 00 00 00 00 00	0.2
0012FBA8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0012FBB8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0012FDC0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
0012FDB8	E8 32 DD 11 B7 41 80 6D 61 72 69 6F 45 24 4D F6	6210.AE8aric88Mo
0012FBB8	86 3F 2A 89 C4 1F EE B6 5A 61 85 D8 49 67 69 73	77.A0192a.0rgis
0012FDF0	C2 5C 6E 62 79 70 2E C5 70 C5 00 00 00 00 00 00	Unnyp.exe.....
0012FC08	55 71 74 65 5C 6F 76 65 72 2E 65 71 79 00 00 00	UqteOver.equ...
0012FC18	00 00 00 00 41 72 76 61 7A 6F 00 00 00 5A 69	...Arvazo...Zi
0012FC20	66 75 75 00 00 00 00 00 42 C2 00 75 C3 00 00 00	fwu....Ibhuc...
0012FC38	00 00 45 6E 69 74 6F 67 00 00 00 00 EC 70 38 0F	..Enitog....i88D

Figure 8. Final chunk

```

8D85 F4FEFFFF lea eax, [local_67]
E8 479CFFFF call fniyp_RC4
817D FC 4441 cmp [local_1], 45564144
75 1D jnz short n1yp_00429908
cmp bytes, 'DAVE'

```

Figure 9. Search for "DAVE"

from here continues to run and tries to download the configuration file. As can be seen, the request also sends some data. This data corresponds with the anti-tracker authentication advertised by the creators of Citadel (Figure 10).

Despite the configuration file being encrypted in AES, as shown in the sample, the request is made with a POST command with the data RC4 and XOR encrypted. The data is sent in this way: Figure 11.

Once the configuration has been downloaded, it is decrypted using AES (one of the biggest enhancements of this trojan) and stored in the registry but with a different key (mentioned earlier and stored in the last part of the binary).

The chosen path for this information is the same as ZeuS uses, that is, `HKEY_CURRENT_USER\Software\Microsoft`. Here, a pseudo random key name that contains values within the binary data is created, as can be seen in the following Figure 12.

Turning back to the injections, Citadel does not attempt to inject code in all processes, but has a list of certain processes that it tries to avoid. These just happen to be processes belonging to the antivirus companies (Figure 13).

Within the section on injections and dangers, this version hooks into functions used by the Google Chrome browser, some of which can be seen with

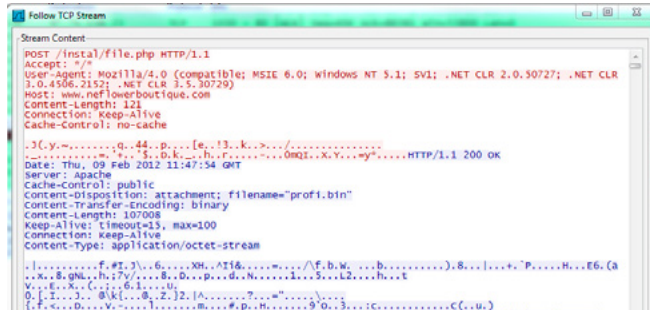


Figure 10. Request for the configuration file

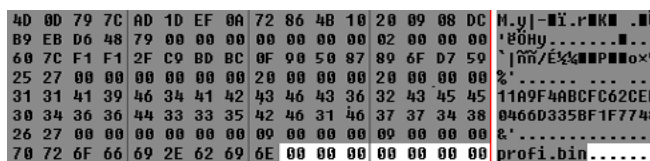


Figure 11. Unencrypted data

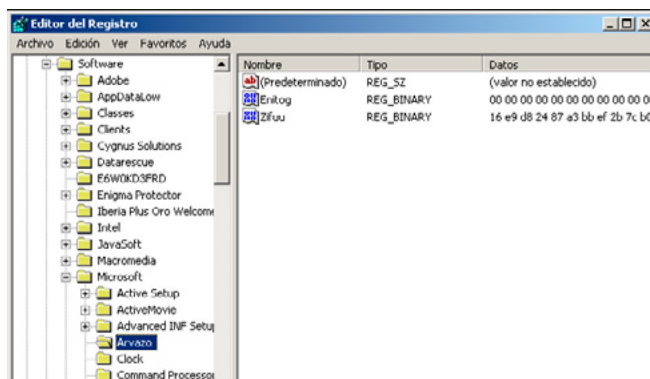


Figure 12. Configuration file stored in the registry

the usual hook detectors, while others cannot as they are not exported functions. These functions are: Figure 14.

We will now present two images showing a normal Connect function and also a hook set in the form of a jump instruction (JMP).

The redirection of blocked domains (generally used to avoid antivirus software updates) is not done in the system's hosts file, but in the same way as a redirection from a phishing page. In the latest analysed samples, the traffic has been seen to be redirected from all these pages to a Google IP, specifically 209.85.229.104 (Figure 17).

Another interesting function is the execution of certain instructions straight after infection has taken place. In the samples we analysed, this functionality is always used to examine the configura-

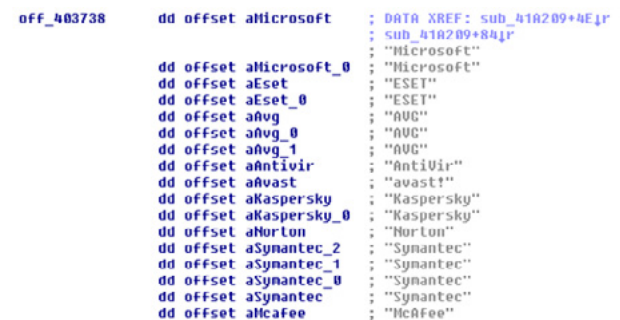


Figure 13. List of monitored antivirus

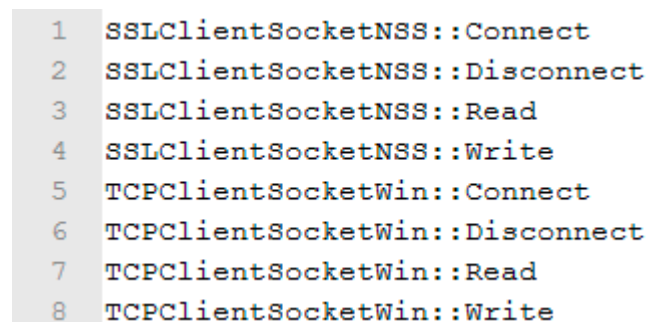


Figure 14. Hooks into the chrome.dll



Figure 15. Normal code

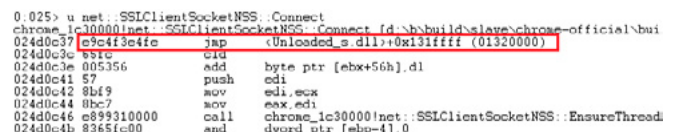


Figure 16. "Hooked" code

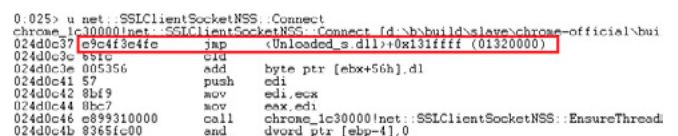


Figure 17. Some of the redirected domains



Video recording is another interesting option, as it means the results of the injections on real victims can be monitored. These are recorded in mkv format, using the following file naming convention at storage time:

As this is a new variant, the numbering has started at version 1 and, so far, we have seen versions 1.1.0.0, 1.1.3.0, 1.1.5.1, 1.2.0.0 and 1.2.4.0.

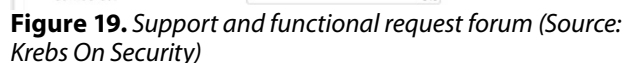
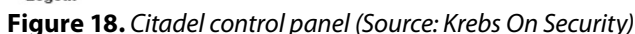
- os\_shutdown
- os\_reboot
- url\_open
- bot\_uninstall
- bot\_update
- dns\_filter\_add
- dns\_filter\_remove
- bot\_bc\_add
- bot\_bc\_remove
- bot\_httpinject\_disable
- bot\_httpinject\_enable
- fs\_path\_get
- fs\_search\_add
- fs\_search\_remove
- user\_destroy
- user\_logoff

- user\_execute
- user\_cookies\_get
- user\_cookies\_remove
- user\_certs\_get
- user\_certs\_remove
- user\_url\_block
- user\_url\_unblock
- user\_homepage\_set
- user\_ftpclients\_get
- user\_emailclients\_get
- user\_flashplayer\_get
- user\_flashplayer\_remove

Looking at this list of commands (above) we can see that this new family can steal credentials from installed applications. This and other less important Zeus functions can be found in Citadel. As an example, FTP credentials are stolen from different installed FTP clients, among which you can find Flashfxp, Total commander, Filezilla, Wsftp and SmartFTP.

In addition to technical enhancements, there are improvements in the control panel, the management of the botnet and the “service” offering. This product is not marketed in the usual way of selling the product and having no further relationship with the customer. The control panel interface shows a more careful look, but with few improvements (Figure 18).

The most interesting thing about this malware is its social aspect, as it offers the possibility to request fault correction and even request new functionality. Citadel's development is tailored to the



2012	Internet Explorer	Firefox	Chrome	Safari	Opera
January	20.1 %	37.1 %	35.3 %	4.3 %	2.4 %
2011	Internet Explorer	Firefox	Chrome	Safari	Opera
December	20.2 %	37.7 %	34.6 %	4.2 %	2.5 %
November	21.2 %	38.1 %	33.4 %	4.2 %	2.4 %

**Figure 20.** Browser usage (Source: w3schools.com)

demands of the user community, something that will undoubtedly help it win converts from other malware families which offer a product with closed features and no support beyond the user manual (Figure 19).

## CONCLUSION

During the course of our analysis, what has become abundantly clear is that this is a very interesting malware family, not only from a technical point of view, but also in that the group behind this new family, have known what steps to take to offer added extras. These extras are not offered by the best-known banking Trojan families, mainly Zeus etc.

Starting from the source code, one can catalogue Citadel, along with Ice-IX, as the most serious attempt to profit from last year's code filtering. Amongst the new features a highlight is the targeting of Google Chrome, something that surely the vast majority of builder buyers were awaiting anxiously. The reason is clear; Chrome is nowadays the second most widely used browser, beyond even Internet Explorer, as shown in the following Figure 20.

The use of AES encryption also deserves our attention. We cannot assume that this sample is related to Zeus samples, seen last September, with AES encryption. It may just be functionality implemented at the users' request. In the short term, Citadel's use will probably grow at a faster pace than its peers, with the added benefit of growing towards the users' needs and the user's, after all, are the best judges of their own requirements.

It is important to note that the process does not just stop there. Here at Lookwise what we do is to feed all of this forensic information into our SIEM tool called Lookwise. This process produces what we term Cyber intelligence that can be used to protect the critical assets of a network. Undertaking the forensic analysis will provide you with a rich seam of information which if used with the correct tool will provide you with much more than over view of how a piece of malware is attacking or stealing information. If used with an intelligent SIEM tool like Lookwise it can help you identify strains of malware even before they have breached your network.

We hope that by understanding the approach we took to creating the right environment with the right tools you now have a better understanding of how to go about tackling the problem of reversing a piece of malware.

## Nahim LLb Hons



*Across global markets the threat of e-Crime is hindering the ability of organisations to dynamically exploit new opportunities. While it was once a tactical and operational issue solely dealt with by IT departments, today e-Crime is a management imperative that can make or break your company's relationships, reputation and results.*

*Over the course of his professional career, Nahim has developed an expertise in the field of Cyber Threat Management. Nahim has defined major security strategies in order to help protect critical information assets (he has delivered and managed extensive projects for global banking entities) for major multinational organisations and provided bespoke workshops to the public sector.*

*Nahim has an extensive range of knowledge on areas including e-Crime consultancy fraud defensive strategies, research into latest e-Crime trends, bespoke training and development, disaster recovery planning and auditing and countermeasure consultancy. In the 21st century protecting your on-line presence is not just about processes and tools, it's about your company's ability to respond to customer needs, generate financial results, pursue new markets, and comply with legislation and regulation. Nahim's expertise can help an organisation overcome its most challenging hurdles, and realise new business opportunities. Nahim is currently employed in Barcelona by Lookwise Solutions – a leading provider of SIEM technology and Cyber Threat Management services. His role is to develop new services for combating cyber threats and to develop the company's presence throughout Europe, Middle East and Africa.*

<http://www.lookwisesolutions.com>

<http://www.lookwisesolutions.com/index.php/en/>





## IT Security Courses and Trainings

**IMF Academy is specialised in providing business information by means of distance learning courses and trainings. Below you find an overview of our IT security courses and trainings.**

### **Certified ISO27005 Risk Manager**

Learn the Best Practices in Information Security Risk Management with ISO 27005 and become Certified ISO 27005 Risk Manager with this 3-day training!

### **CompTIA Cloud Essentials Professional**

This 2-day Cloud Computing in-company training will qualify you for the vendor-neutral international CompTIA Cloud Essentials Professional (CEP) certificate.

### **Cloud Security (CCSK)**

2-day training preparing you for the Certificate of Cloud Security Knowledge (CCSK), the industry's first vendor-independent cloud security certification from the Cloud Security Alliance (CSA).

### **e-Security**

Learn in 9 lessons how to create and implement a best-practice e-security policy!



### **Information Security Management**

Improve every aspect of your information security!

### **SABSA Foundation**

The 5-day SABSA Foundation training provides a thorough coverage of the knowledge required for the SABSA Foundation level certificate.

### **SABSA Advanced**

The SABSA Advanced trainings will qualify you for the SABSA Practitioner certificate in Risk Assurance & Governance, Service Excellence and/or Architectural Design. You will be awarded with the title SABSA Chartered Practitioner (SCP).

### **TOGAF 9 and ArchiMate Foundation**

After completing this absolutely unique distance learning course and passing the necessary exams, you will receive the TOGAF 9 Foundation (Level 1) and ArchiMate Foundation certificate.



**For more information or to request the brochure please visit our website:**

<http://www.imfacademy.com/partner/hakin9>



IMF Academy

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

Tel: +31 (0)40 246 02 20

Fax: +31 (0)40 246 00 17

# SECURITY & ONLINE IDENTITY PROTOCOLS: A TESTER'S VIEW

by Cordny Nederkoorn

Consider the following example: Alice (resource owner) can grant a printing service, PrintMe (client) access to her protected photos stored at a photo sharing service, OnlinePhoto (resource server), without sharing her username and password with the printing service PrintMe. Instead, she authenticates directly with a server trusted by the photo sharing service, AuthServer (authorization server), which issues the printing service PrintMe delegationspecific credentials (access token).

## What you will learn:

- possible threats associated with the use of online identity protocols
- What are double redirection protocols?
- examples of double redirection protocols
- Introduction of OAuth
- susceptibilities OAuth to malicious attacks
- countermeasures OAuth to malicious attacks

## What you should know:

Basic understanding

- online identity and data sharing
- internet protocol
- online malicious attacks

**T**his process can be achieved by using a *double-redirection protocol*.

A double-redirection protocol is a security protocol where an application redirects the user's browser to a third-party that interacts with the user before redirecting the user back to the application. The third-party identifies the application to the user, authenticates the user, and asks for permission to identify the user to the application and grant the application access to resources and services on behalf of the user.

Double-redirection takes place for user and third-party; If Alice is sharing with PrintMe, she has a double-redirect, to AuthServer and then back to OnlinePhoto, when introducing OnlinePhoto to AuthServer.

Third-party PrintMe has also a double-redirect to AuthServer and then

back to OnlinePhoto for obtaining Alice's photos there.

Typical double redirection-examples are OpenID and OAuth. For this article OAuth will be discussed further.

OAuth is an emerging authorization standard being adopted by a growing number of sites like Twitter, Facebook, Google etc.

It is an open-web specification for organizations to access protected resources on each other's web sites. This is achieved, as we already saw, by allowing users to grant a third-party application access to their protected content without having to provide that application with their credentials.

Unlike OpenID, which is a federated authentication protocol, OAuth (Open Authorization), is intended for delegated authorization only and it



does not attempt to address user authentication concerns.

The OAuth-protocol has 2 versions: 1.0 and 2.0. The textbox 'differences OAuth1.0 & 2.0 will discuss the main differences.

OAuth has 2 distinct versions. The OAuth 1.0 protocol ([RFC5849]), was the result of a small ad-hoc community effort. OAuth 2.0 was designed to simplify the protocol. The OAuth 2.0 protocol is not backward compatible with OAuth 1.0. It's very distinctive. The two versions may co-exist on the network and implementations may choose to support both (Table 1).

Initiatives have been taken to expand the functionality of OAuth2.0.

An example of this expansion initiative (aka OAuth2.0 profile) is User Managed Access (UMA).

UMA defines how Alice as a resource owner can control access to her protected resource (photos) made by clients operated by requesting parties (like PrintMe), where the resources reside on a resource server, and where a centralized authorization server governs access based on resource owner policy.

UMA seems a lot like OAuth, but has some distinct features like that no redirect is necessary between Alice and PrintMe (both don't have to be online simultaneously). Next to this there is the addition of a distinct centralized authorization Server/Manager (which governs the resource owners access policy).

Finally, due to its extended functionality UMA introduces new terms to the OAuth terminology. For instance it is now designing a OAuth 2.0 Resource Set Registration draft where Alice as a Resource Owner can register its protected resources to the Authorization Server.

For now we will focus on the specifications of OAuth 2.0.

OAuth was mainly developed to cope with the client server password-problem.

Going back to the example, before OAuth Alice had to share her credentials with PrintMe, resulting in PrintMe knowing Alice's password and this way PrintMe has unlimited access to Alice's complete resources at OnlinePhoto.

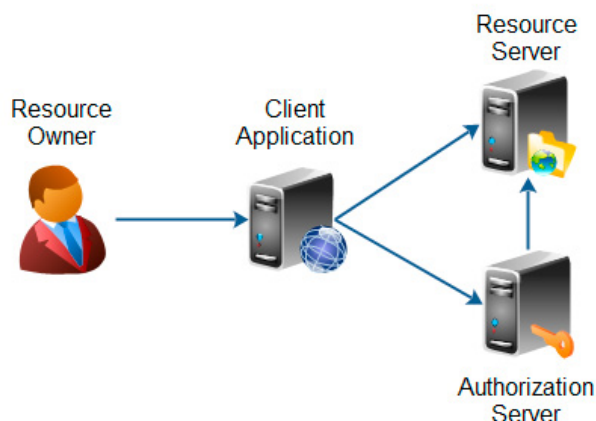
OAuth deals with this problem by introducing an authorization layer and separating the role of the

client from that of the resource owner. In OAuth, the client PrintMe requests access to resources (photos) controlled by the resource owner Alice and hosted by the resource server OnlinePhoto, and is issued a different set of credentials than those of the resource owner Alice. Instead of using Alices credentials to access her photos, the client PrintMe obtains an access token. Access tokens are issued to third-party clients by an authorization server with the approval of the resource owner. The client uses the access token to access the protected resources hosted by the resource server.

Access tokens can be in different forms: bearer tokens and proof tokens.

For clarity, these tokens will in this article be discussed as 1 token, although there are differences and bearer tokens must always be protected using transportlayer mechanisms such as SSL.

The key roles in OAuth2.0 are the resource owner, the client, the resource server and the authorization server as is illustrated in the Figure 1.



**Figure 1.** Key roles in OAuth2.0

The OAuth 2.0 roles (<http://tutorials.jenkov.com/oauth2/roles.html>).

**Resource owner :** An entity capable of granting access to a protected resource. When the resource owner is a person, it is referred to as an enduser.

**Resource server:** The server hosting the protected resources, capable of accepting and responding to protected resource requests using access tokens.

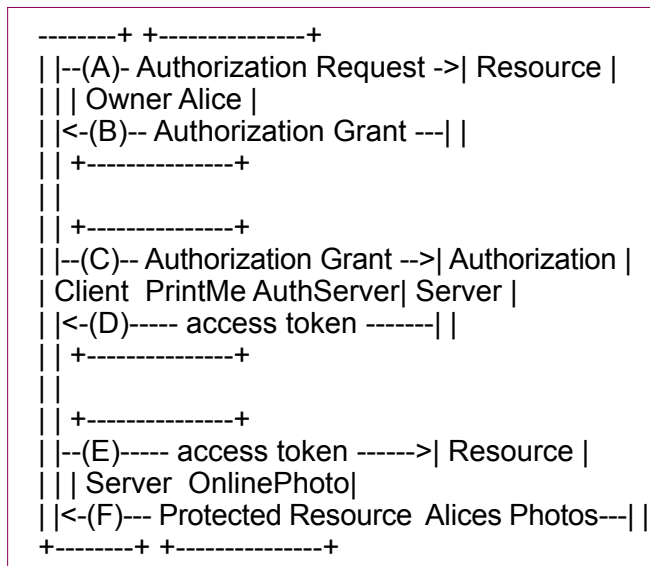
**Table 1.** Differences OAuth 1.0 and OAuth 2.0

OAuth 1.0	OAuth 2.0
Use of signature matching with every API call between client and server	Replaced signature for SSL,necessary for token generation; but SSL still has to be added by the OAuth roles to the OAuth2.0 implementation
No clear distinction of resource and authorization server	Specification clearly distinguishes implementation by resource server and authorization server
IETF Information document RFC 5849(not a Internet Standards Track Specification or Draft)	Not stable IETF draft (intended for Internet Standards Track Specification

**Client:** An application making protected resource requests on behalf of the resource owner and with its authorization. The term client does not imply any particular implementation characteristics (e.g. whether the application executes on a server, a desktop, or other devices).

**Authorization server:** The server issuing access tokens to the client after successfully authenticating the resource owner and obtaining authorization.

The following diagram shows the abstract protocol flow with a description of the flowsteps.



**Figure 2.** Abstract Protocol Flow

- (A) The client PrintMe requests authorization from the resource owner Alice. The authorization request can be made directly to the resource owner Alice(as shown), or preferably indirectly via the authorization server as an intermediary.
- (B) The client PrintMe receives an authorization grant, which is a credential representing the resource owner's authorization, expressed using one of four grant types defined in OAuth 2.0 or using an extension grant type. The authorization grant type depends on the method used by the client PrintMe to request authorization and the types supported by the authorization server.
- (C) The client PrintMe requests an access token by authenticating with the authorization server and presenting the authorization grant.
- (D) The authorization server authenticates the client PrintMe and validates the authorization grant, and if valid issues an access token.
- (E) The client PrintMe requests the protected resource (Alice's photo) from the resource server and authenticates by presenting the access token.
- (F) The resource server validates the access token, and if valid, serves the request

The OAuth 2.0 abstract flow shows six subflows involving the four OAuth 2.0 roles.

Next to the OAuth 2.0 abstract flow, there are 3 other known flows as described in the OAuth 2.0 protocol, the implicit grant flow, the resource owner password credentials flow and the client credentials flow . The implicit grant flow will be discussed further on. The latter flows are not double redirection flows and are out of scope for this article.

Each OAuth 2.0 role has its distinct weaknesses and examples of these will be addressed now.

The OAuth 2.0 threat model addresses also other weak spots in the OAuth abstract flow, but for clarity only two threats associated with each OAuth 2.0 role will be highlighted. Other threats can be found in the OAuth 2.0 threat model. When possible, the threats will be illustrated by using the OnlinePhoto example above.

## THREATS OAUTH 2.0

Resource owner

### THREAT: RESOURCE OWNER IMPERSONATION

The client PrintMe requests access to the protected resources of Alice available on the resource server OnlinePhoto. The resource owner Alice will respond to this access request by either granting or denying the client PrintMe access to Alice's photos.

Tony, a malicious client, can tap in to this authorization flow by transmitting the necessary requests programatically without the resource owner's consent. This may result in Tony gaining access to the protected resource.

The authorization server is most vulnerable when non-interactive authentication mechanisms (eg. certificates) are built in, allowing Tony to inject malicious code during a session, without alarming the resource server OnlinePhoto because it doesn't expect interaction from Alice as a user.

The authorization is also vulnerable when the authorization flow is split across multiple pages. This complexifies the code, enhancing the risks of bugs and therefore more chance of vulnerabilities to malicious code injections like malicious HTML user agents in eg. HTTP request headers.

The main countermeasure is to enforce user-interaction by asking the user Alice consent using CAPTCHAs, One-Time Passwords (eg. Texting).

### THREAT: OBTAIN USER PASSWORDS ON TRANSPORT

The authorization server for OnlinePhoto has a database containing username/password combinations.

Tony, our malicious attacker, can gain access to this database by launching an SQL injection attack.



To prevent such an attack a authorization server database can protect itself by not accepting input from the outside to be executed in its own queries. Better to do a regular peer code review than buy expensive SQL injection detection tools, which also can produce false positive/negative results.

Client

### THREAT: OBTAIN CLIENT SECRETS

Tony, the malicious attacker, could try to access the client's (PrintMe) obtained secrets from Alice by replay its refresh tokens and authorization codes, or obtain tokens on behalf of the attacked client (PrintMe's OnlinePhoto) with the privileges of that client.

The attack could be achieved during an insecure client installation (PrintMe's OnlinePhoto) or if the client as an application is an open source project, exposing its source code in its public repository.

A countermeasure is *Client secret revocation* where an authorization server may revoke a client's secret in order to prevent abuse of a revealed secret. This countermeasure should then be incorporated during the implementation of the OAuth application.

When your project is open source, it is advised to ask consent (through CAPTCHAs, texting etc.) to a user to access the code.

### THREAT: OPEN REDIRECTORS ON CLIENT

Here an important part of OAuth2.0-code plays a role: the *redirection URI*.

A URI is part of the URL (part after hostname) and is used as a path to guide the webserver's document root to the desired file or directory.

A redirect URI specifies exceptions to this and tells the browser 'to use this URL instead'.

During an authorization flow the redirection URI's value has to be presented and verified when exchanging tokens and authorization codes. But also *open redirectors* can be used during an authorization flow.

An open redirector is an endpoint using a parameter to automatically redirect a user-agent to the location specified by the parameter value without any validation. If the authorization server allows the client to register only part of the redirection URI, an attacker can use an open redirector operated by the client to construct a redirection URI that will pass the authorization server validation, but will send the authorization code or access token to an attacker controlled endpoint.

To minimize this risk it MUST be required for clients to register a full redirection URI as explained in the OAuth 2.0 core protocol.

Redirection URI's also play an important role during the Implicit Grant Flow.

The implicit grant flow is a simplified authorization code flow optimized for clients implemented in a browser using a scripting language such as JavaScript (Rich application). In the implicit flow, instead of issuing the client an authorization code, the client is issued an access token directly.

When issuing an access token during the implicit grant flow, the authorization server does not authenticate the client, but the identity could also be verified via the redirection URI used to deliver the access token to the client. This implies a threat, because the access token may be exposed to, not only the resource owner, but also to other applications with access to the resource owner's user-agent (the web-browser).

Such an application could be malicious and embed this access token into a constructed redirection URI, which he could show the client, tempting it to follow the mimicked redirection URI, leading to the attacker's access token authorized within the user's client.

This kind of forgery is known as CSRF: Cross-Site Request Forgery.

Countermeasures could be not to follow untrusted sites or use the State parameter (as given by the client in the client authorization request) for linking the authorization request initiated by the client with the redirection URI.

resource server

### THREAT: REPLAY AUTHORIZED RESOURCE SERVER REQUESTS

Tony, the malicious attacker, could attempt to replay valid requests in order to obtain/tamper user data on the resource server.

Countermeasures are establishing unique identification by resource server (signed requests, incorporating nouns and timestamps) and detect and refuse every request not qualifying for a signed request.

Integrity can be ensured (minimize phishing) by using transport layer mechanisms (TLS, SSL)

### THREAT: TOKEN LEAKAGE VIA LOGFILES AND HTTP REFERRERS

Access tokens can be sent via URI query parameters, which could lead to leakage to log files and HTTP referrers, which could be accessed by malicious attackers like Tony, enabling them to use the access tokens to access the secret.

Countermeasures could be to replace URI request parameters for POST parameters, setup a logging configuration, but also use authenticated requests and give token limits in scope and duration.

Authorization server

### THREAT: OBTAINING REFRESH TOKEN FROM AUTHORIZATION SERVER DATABASE

To explain this threat the *refresh token* should first be introduced.

## Literature

- Corella, F., Lewison, K.P., "Security Analysis of Double Redirection Protocols", Pomcor, February 2011
- Hammer-Lahav, E., "The OAuth 1.0 Protocol", RFC 5849, April 2010.
- Hardjono, T. Ed., "User-Managed Access (UMA) Core Protocol", draft-hardjono-OAuth-umacore-06B, december 2012
- Hardt, D. Ed., "The OAuth 2.0 Protocol", draft-ietf-OAuth-v2-31, July 2012.
- Lodderstedt, T., McGloin, M., and P. Hunt, "OAuth 2.0 Threat Model and Security Considerations", draft-ietf-OAuth-v2-threatmodel-06 (work in progress), June 2012.
- Sakimura, N. Ed., OpenID Connect Standard 1.0 – draft 14, December 2012

A refresh token could be seen as a long-lasting authorization of a client (PrintMe) to access resources (Alice's photos) on behalf of Alice. Refresh tokens are *only* exchanged between PrintMe and authorization server.

Clients use this kind of token to obtain ("refresh") new access tokens used for resource server invocations.

A threat can occur when an attacker may obtain refresh tokens from the authorization server's database by gaining access to the database or launching a SQL injection attack.

OAuth 2.0 implementers can countermeasure this by code reviewing for SQL injection detection and bind the token to the client id, so the attacker cannot obtain the required id and secret.

## THREAT: OBTAIN REFRESH TOKEN PHISHING BY COUNTERFEIT AUTHORIZATION SERVER

Another technique malicious clients use to capture refresh tokens is by redirecting the refresh tokens from the valid authorization server to a counterfeit one.

To arm against this threat a authorization server MUST use transport-layer mechanisms (TLS, SSL, VPN) to ensure integrity and avoid phishing.

## CONCLUSION

Double redirection protocols, as open standards, play an important role in online data sharing on so-

cial networks. OAuth 2.0 is an excellent example for this.

As an open standard it is interoperable over different social networks, but it also implies security risks because no cryptographic or security countermeasures are built in.

For secure OAuth 2.0-implementation it is therefore important to know the security weaknesses of the OAuth 2.0 -protocol. Depending on the kind of implementation, OAuth 2.0 -implementers can then add countermeasures, as described in this article per OAuth 2.0 role, to minimize the risk of successful malicious attacks against the implementation.



### Kantara Initiative

Kantara Initiative (<http://kantarainitiative.org/about/>) is a robust and open focal point for collaboration to address the issues we each share across the identity community. Kantara activities focus on requirement gathering for the development and operation of Trust Frameworks as well verification of actors within Trust Framework ecosystems. Kantara Initiative Accredits Assessors, Approves Credential Service Providers Services and Recognizes Service Components (Identity Proofing and Credential Management).

### Autho Bio



*Nederkoorn is a software testengineer, employed by Immune-IT, a Dutch software testconsultancy firm with customers in The Netherlands and Belgium. On a personal level Cordero helps Kantara Initiative improving the quality of the specification and implementation of UMA (User-Managed Access), a web authorization protocol building on OAuth 2.0. He discusses his work on different social media.*

*email: [cnederkoorn@immune.it](mailto:cnederkoorn@immune.it)*

*blog: <http://testingsaas.blogspot.com>*

*twitter: <http://www.twitter.com/testingsaas>*

*facebook: <http://www.facebook.com/TestingSaaS>*





**Allow  
us to  
guide  
your  
CAREER**



SENIOR  
PRACTITIONER



### 2013 PUBLIC COURSE SCHEDULE

#### CISMP

Mar 18-22, Apr 22-26, May 13-17, Jun 10-14,  
Jul 8-12, Sep 30 - Oct 4, Oct 14-18, Nov 18-22

#### PCiBCM

Mar 18-22, Apr 8-12, Apr 22-26, Jun 10-14, Jul 8-12,  
Aug 5-9, Sep 16 -20, Oct 14-18, Nov 11-15, Dec 9-13

#### PCiIRM

Apr 22-26, May 6-10, May 20-24, Jun 3-7, Jun 17-21,  
Jul 8-12, Jul 22-26, Aug 5-9, Oct 7-11, Oct 21-25, Nov 4-8,  
Nov 18-22, Dec 2-6, Dec 16-20

If you are interested in learning more, get in touch:  
[contact@infosecskills.com](mailto:contact@infosecskills.com).



PRACTITIONER

# ESTABLISHING A CENTER FOR DIGITAL FORENSICS

## INVESTIGATIVE SERVICES ON THE CLOUD

by Rocky Termanini, PhD, CISSP

The concept of building a Center for Digital Forensics Investigative Services on the cloud is a compelling and totally innovative. Everything is becoming cost effective and cloud-centric, including selling Platform as a Service (PaaS), Software as a Service (SaaS). Now offering Digital Forensics as a Service (DFaaS) is an attractive venture which will prove to be profitable and highly successful.

### What you will learn:

- Learn about the process of conducting Digital Forensics (DF) analyses.
- Create awareness that Digital Forensics is an essential course in computer science and MIS.
- Learn how to develop a business case to promote the establishment of a Digital Forensics Investigative Center.
- Learn more about how to use Bayesian Networks to help in the detection and deterrence of cybercrimes.

### What you should know:

- You need to have the skills of system analysis
- You need to have good skills in operating systems and how to read memory dumps.
- Have the training to use Digital Forensics software such as EnCase.
- Familiarity with cyber laws of the land.
- How to preserve the evidence of the crime while doing the analysis.

Given its innovative nature, I was able to promote the initiative of (DFaaS) in Academia to train Computer Science and Law students, and to offer forensic services to Law Enforcement agencies in the area (who badly needed it). Also, offer on-demand services to private companies who were victimized by a flurry of cyber-attacks from trade secrets theft, to credit card and bank account fraud.

This paper discusses my original concept of as a business proposal for the establishment of a Center for Digital Forensics Investigative Services on the cloud, as profit center, in other words, fee for service.

In order for the center of Digital Forensics Investigative Services (DFIS) to be successful, it should have solid sponsorship the public and private sectors, as well as the qualified resources

to perform the services, as above all, business-minded people who will focus on profitability and expansion of business with strategic customers.

### INTERNET AND CYBERCRIME

Cyberspace is a new world where the masters are datalords, and baudrate barbarians. They can steal legitimately whatever they want around the world. Anonymity allows them to indulge in extravagant role-playing whereby they form a dangerous underground movement to rob any information highway. As we migrate into higher cyberspace, citizens, businesses, the government, educational institutions, and other organizations have become an easy target of a new type of terrorism. Cybercrime has become multidimensional, totally virtual and globalized, and can be triggered from

anywhere. The battlefield has become the data center where “cybernauts” fight with their computers, laptops, notebooks and I pads. The Pentagon has moved to the cloud where the generals are tattooed geeks.

The following chart gives a partial list of the two-flavor malware inflicted on our societal fabric: Figure 1.

## INTRODUCTION TO DIGITAL FORENSICS

*Digital Forensics* (DF) simply is the reverse-engineering process of cyber-crime. The main goal of (DF) is to solve cybercrime, collect evidence and bring perpetrator to justice, in other words it is considered as *IT autopsy*. *Artificial Intelligence* (AI) and *Bayesian Network Modeling* (BNM) have been added to (DF) to extend the realm of forensics into forecasting and prediction posterior crimes. Now, we can extract knowledge from historical forensic and crime episodes and offer solid “reasoning” prediction on upcoming crimes (Figure 2).

## CYBERCRIME PREDICTION AND FORECASTING

One of the high-profile activities of the DFIS center is using Bayesian inference and probabilistic reasoning to forecast and predict cybercrime ahead of time, as shown in the diagram below. Artificial

Intelligence techniques will be used to develop a reasoning engine that will provide unbiased and realistic predictions. All crime episodes will be converted into Bayesian graphical patterns and stored in a central database. The reasoning engine will evaluate the different pattern and determine the likelihood of cyber-attacks with great accuracy (Figure 3).

The first step in Forensics is to reconstruct the crime and determine how it was committed. The second step in Forensics is to determine the motives and why it was committed. And the third step is to find out who did it.

Without referencing historical data, Forensics is practically impossible. Forensics needs to study pattern of similarly solved and unsolved crimes. Artificially intelligent and cognitive engineering have been very instrumental in building reasoning systems are built to help analyzing patterns of historical crimes (Figure 4).

## OVERWHELMING STATISTICS

Internet has offered a compelling opportunity to hackers to practice cybercrime. Good hackers can become good computer forensicians and vice versa. The fascinating part of the science is that the computer evidence often is transparently created by the computer’s operating system without the knowledge of the computer operator. The informa-

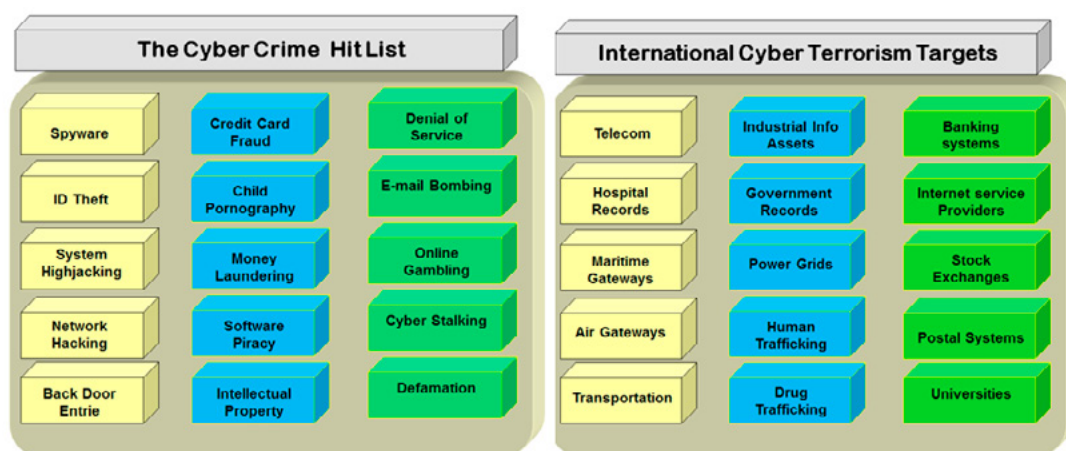


Figure 1. The Cyber Malware Continuum

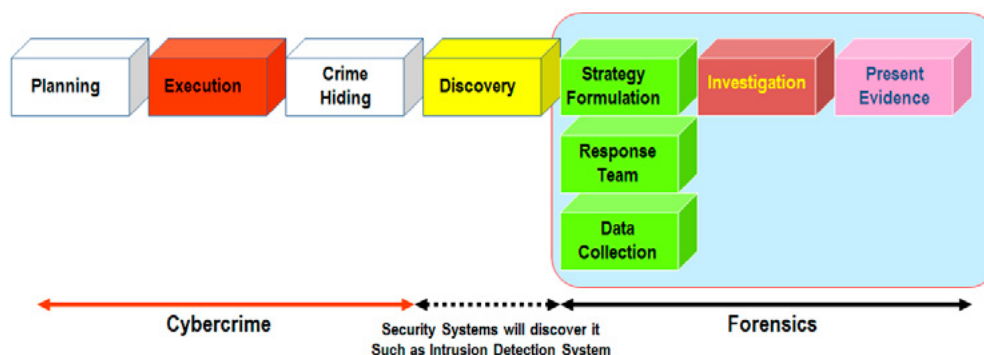


Figure 2. The Cyber of Digital Forensic



tion may actually be hidden from view. To find it, special forensic software tools and techniques are required.

That shows up in the statistics. According to FBI's Internet Crime Complaint Center (IC3), the statistics for 2011 is on the increase. Here's an excerpt from the banking industry: Figure 5.

Worse yet, the cost of hacker attacks appear to be rising. According to the 2011 "Computer Crime & Security Study," released by the FBI and the Computer Security Institute in San Francisco, some 90% of the 503 respondents from large corporations and government agencies said they had suffered over 25 cyber-attacks or security breaches in the past 12 months. The average financial toll (from the banking industry only) has from these has risen to \$38.3 million, from \$500,000 in 1997.

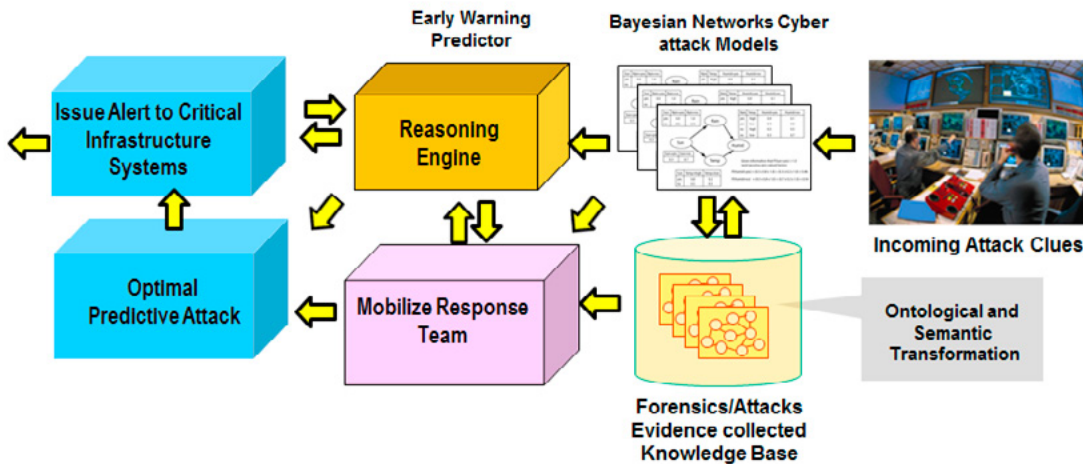
Formal digital Forensics started in early 2000, and initially, Academia did not give any attention to this marvelous profession. But most universities have adopted, or will start Digital Forensics courses in their Computer Science program.

The link [http://education-portal.com/articles/List\\_of\\_the\\_Best\\_Computer\\_Forensics\\_Schools\\_in\\_the\\_US.html](http://education-portal.com/articles/List_of_the_Best_Computer_Forensics_Schools_in_the_US.html), gives a partial list of the universities that offer an advance program in Digital Forensics.

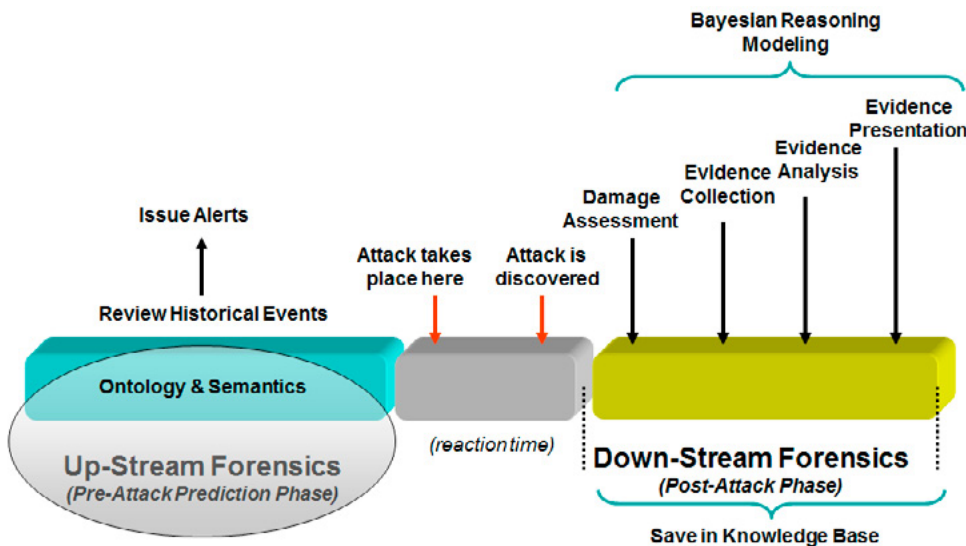
## PROPOSED ARCHITECTURE OF DFIS CENTER

The following chart shows the architecture of the (DFIS) center: The "trusted" cloud is in the center which represents the knowledge Farm as well as the client accounts and the APIs to their systems. The knowledge databases will also be on the cloud under the management of a trusted agency. The center will be on campus of a reputable school, and will have the tools and the necessary software to conduct the forensic analyses.

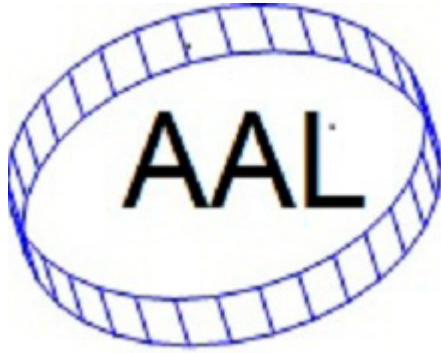
The Center will also have honeypot grids and stealth traps, to capture random attacks from global hackers. The Clients (on the left in yellow) will be able to review the results of the forensic analyses and submit forensic service requests called (eforensic-as-service) to the center (Figure 6).



**Figure 3.** The Cognitive Reasoning Process of Modern Digital Forensics at DFIS Center



**Figure 4.** The Process of Cognitive Digital Forensics





**Audit Associates Ltd**  
**AUDIT, ANTI-MONEY LAUNDERING, FRAUD & INFORMATION**  
**SECURITY SYSTEMS**  
**(Consultancy and Training)**

**Email: [auditassociateslimited@gmail.com](mailto:auditassociateslimited@gmail.com)**  
**Website: [www.fincrimines-auditassociates.com](http://www.fincrimines-auditassociates.com)**

Students from Academia will attend courses and training at the center. Clients from the private and public sectors will subscribe to the DFIS center on yearly basis.

## DFIS CLIENT BASE

There are four categories of clients who can use the center to help in their forensic investigations: Figure 7.

**Bank Crime Statistics (BCS)**  
Federally Insured Financial Institutions  
January 1, 2011 – December 31, 2011

Violations by Type of Institution

	Robberies	Burglaries	Larcenies
Commercial Banks	4,495	44	10
Mutual Savings Banks	15	0	0
Savings and Loan Associations	105	3	0
Credit Unions	398	13	1
Armored Carrier Companies	0	0	1
Totals	5,014	60	12

**Loot Taken and Recovered**  
Loot was taken in 4,534 (89 percent) of the 5,086 incidents. Loot taken is itemized as follows:

Cash	\$38,331,491.85
Securities—Face Value	\$100.00
Checks (Including Traveler's Checks)	\$2,310.11
Food Stamps	\$0.00
Other Property	\$9,600.00
Total	\$38,343,501.96

Figure 5. Excerpt from the banking industry

## DFIS TECHNICAL AND FORENSIC SERVICES

There will be a wide variety of services that the center can do to clients: Cloud and onsite services, cognitive products for early warning and forecasting and formal training seminars on ethical hacking (Figure 8).

## THE PIVOTAL ROLE OF THE DFIS CENTER

DFIS Center is an incredible knowledge and research hub that reaches out to all the sectors of business and industry. It is a crime fighter and provides a regimented book campy for training in Digital Forensics, ethical hacking and cyber security. DFIS empowers any academic institution with the latest in security technologies (Figure 9).

## THE FOUR BUSINESS DRIVERS OF DFISC

There are four major drivers that contribute to the importance of DFIS center, as shown in the figure below. The first driver is Technology which is the building blocks that shape up Digital Forensics. As technology moves along, it allows cyber criminals to pick up the latest advance and use them as weapons. The second driver is Academia which offers the stage for learning and knowledge acquisition. The third driver is Law Enforcement which relies on Digital Forensics to collect evidence and bring hackers to justice. The fourth driver is the business world which is offers a fertile ground for cybercrime. Business has always been plagued with enormous damages from cybercrime. It doesn't have the proper expertise or the time to respond to early warnings.

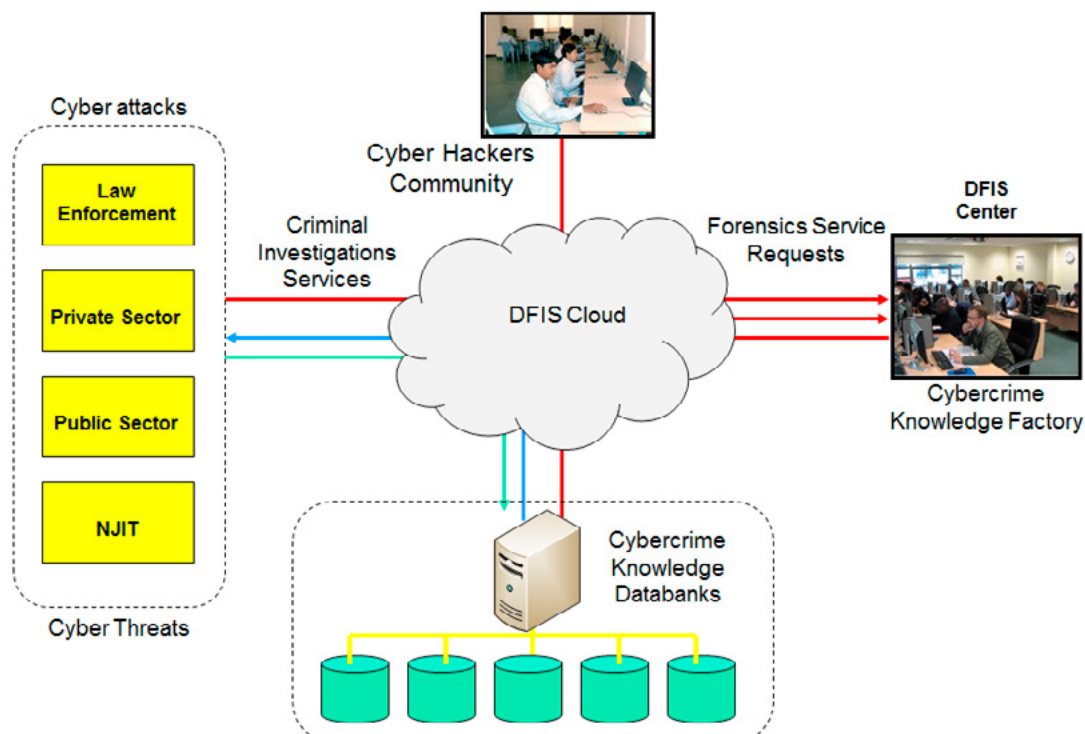


Figure 6. DFIS Center Architecture and Cloud Services



## ACADEMIC ALLIANCE

Internet is the cornerstone of a new paradigm in the process of changing our social order. In Academia, Internet has permeated into every department and program. In fact, Internet has become the most important topic in schools. It has drastically influenced every program from liberal arts to Anthropology. Internet courses have become mandatory regardless of student major. Lab work has become an integral part of the education continuum. Almost all Law schools have incorporated digital forensics into their formal program. The new Cyber Law has become a high-profile topic and gained universal popularity. Most schools expanded the computer labs to accommodate the increasing workload.

DFIS center would be the logical place to learn about cybercrime. The center will offer basic and advanced courses in Computer Forensics. The courseware will cover the whole cybercrime spectrum: psychology of the cybercriminal, the anat-

omy of crime, how to reverse engineer it, and reconstruct the crime. Students can major in Cybercrime and digital forensics and even get an advanced degree. Cyber law is in its infancy and cyber criminals know this and will take advantage of this grey area. Lawyers need to know how to deal with cybercrime and how apply cyber law to it. Most importantly, train the elite of the young generation how to be accountable, ethical and focused on professionalism.

## COLLABORATION WITH LAW ENFORCEMENT AGENCIES

It is evident that all the Law Enforcement agencies can only handle 30% of all the crimes. 70 % of the crimes remain unsolved and poorly handled. Since crime is on the rise in volume and sophistication, Law Enforcement agencies are running behind and welcome any help coming from center such as DFIS center. Some of the complex crimes such as international credit card fraud, Human traffick-

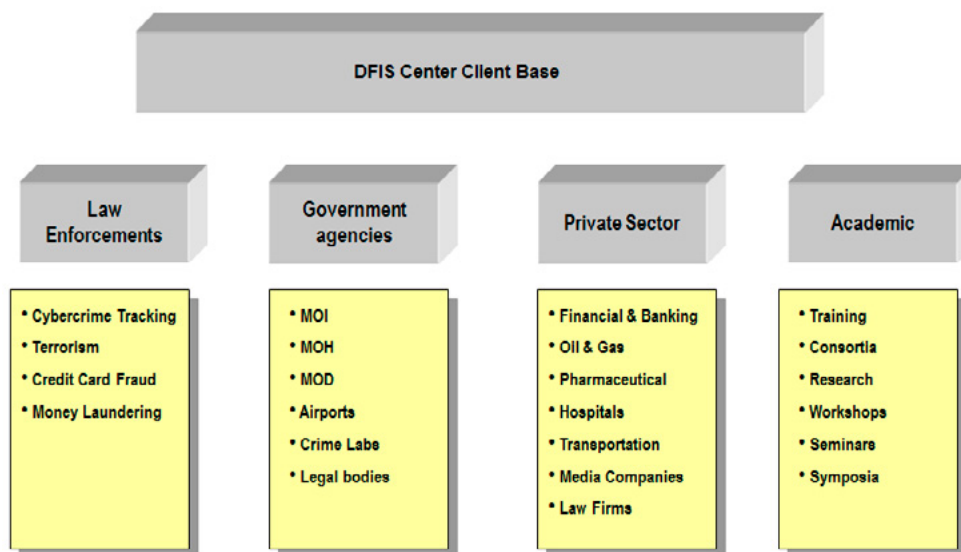


Figure 7. The Client Base for the Center

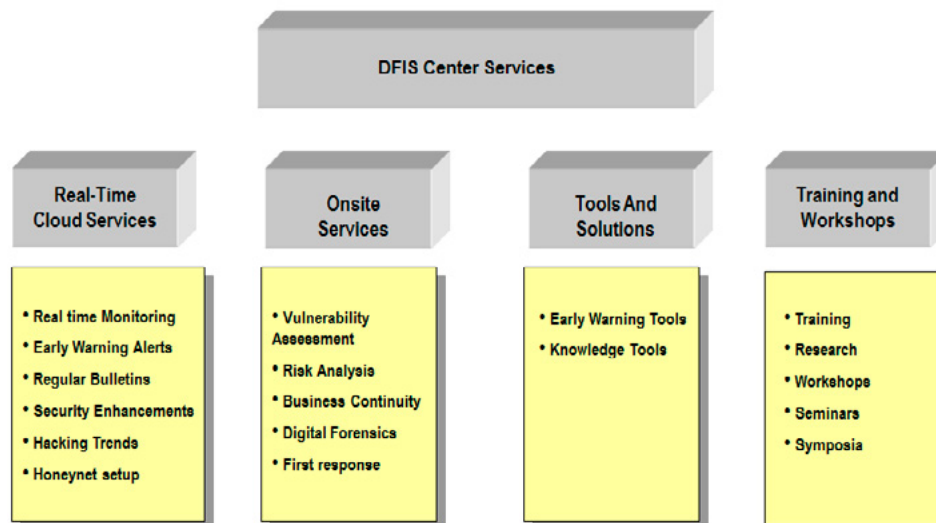


Figure 8. Portfolio of Services and Products

ing networks, drug trafficking, require high level of sophistication and patience.

The number of professional hackers (black hats) has been astronomically growing from a handful in 1993, 30,000 in 2009, and in 2011, the number reached 1 million. Plus the fact they have been at the leading edge of technology. Underground organizations have been hiring them to manage their business around the world. There are 200 international schools that teach advanced cybercrime. The Hacker Quarterly magazine publishes the most sophisticated malware and how to circumvent the attacks. Serious hackers are computer science graduates and develop innovative tools to crack almost any system. There are over 1500 Black Hat clubs organizations in the world that convene yearly to share crime technologies.

## STRATEGIC OPPORTUNITIES WITH THE US GOVERNMENT

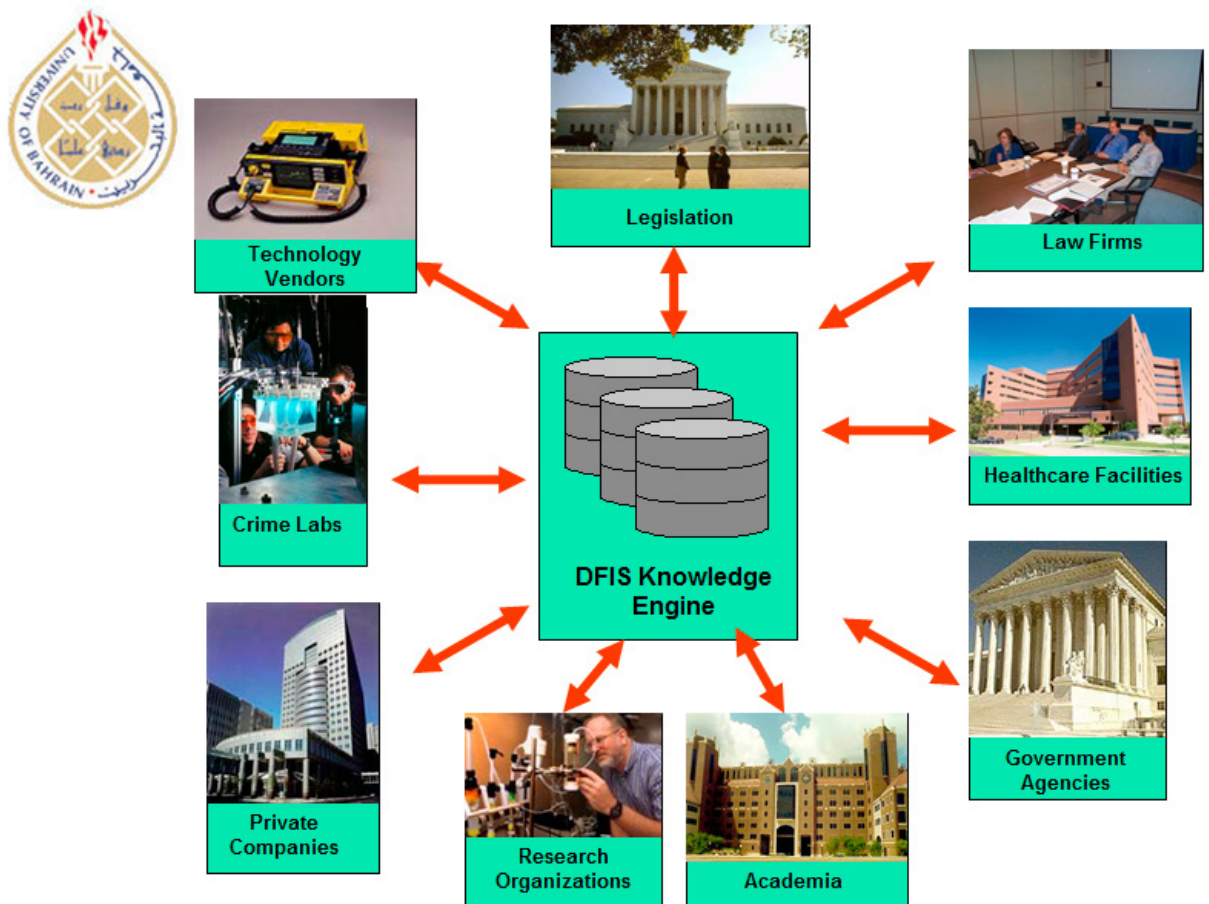
Since cybercrime has risen 29% in 2009 and 31 % in 2010, the demand for rapid forensic investigation is reaching the critical mass. The government is encouraging universities to take on part of the responsibility to launch new academic programs in cyber forensics and form consortia to develop new strategies and technologies.

Every year the US Government solicits research institutes and non-profit organizations on funding opportunities for specific projects such as Computer Forensics. The following is a partial list of the organizations that have great interest in fighting cybercrime and are willing to partner or going after special grants:

- The National Institute of Justice
- National Institute of Health (NIH)
- National Institute of Standards and Technology (NIST)
- Information Technology Association of America (ITAA) Computer Emergency Response Team (CERT)
- National Infrastructure Protection Center (NIPC)
- FBI National Cybercrime Division

## BUSINESS ALLIANCE

The success in today's business is achieved through strategic alliance and banding. The economic state-of-the-Health in 2011 has brought gloom and doom to every business sector. Crime also has risen at the workplace. Employees resorted to hacking to express their dissatisfaction with management and layoffs. Major banking institutions and manufacturing companies experience



**Figure 9.** Rhe DFISC as Central Cybercrime Fighter (Dr. Rocky Termanini Univeriity Of Bahrain 2006)

**Technology is a double sided sword.  
Internet makes you naked online!  
Get Secured & Get Certified!**

Welcome to the world of Certified Ethical Cracker  
with Hands-on practical sessions.



**CERTIFIED  
ETHICAL  
CRACKER**

An Advance **Information Security** Course

For more details, visit:

<http://www.infysec.com/training/courses/certified-ethical-cracker>

**infySEC UK :**

145-157, St.John Street,  
London, EC1V 4PW  
England, UK

Phone: +44-7405190001

**infySEC India :**

#37/45, P.H Road,  
Arumbakkam,  
Chennai- 600106  
TamilNadu, INDIA

Phone: +91-44-42611142,43



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

[enquiry@infysec.com](mailto:enquiry@infysec.com)



loss of data, theft of intellectual property, employee data breaching, Distributed Denial of Service, SQL poison and massive spam.

DFIS center will be able to render services to recover corrupt data, or to recover data that was deleted accidentally or on purpose, to track employee hacking and external bandits, to set up stealth software traps, key loggers, and honeypots for backdoor perpetrators.

Moving to the cloud has also opened a Pandora box of challenges across the board. The transport of information across the virtual U-bans of Internet, has given the black-hat communities a golden opportunity to commit fraud, steal people identities and bank account information, steal military and trade secrets, off-shore gambling, music and movie piracy and industrial espionage age. DFIS center will help companies set up the proper security and contingency standards before the migration to the cloud.

Many criminal organizations are also jumping on the cloud bandwagon to market their “Attacks-as-a-service” such as offering botnets for lease and sale.

## VALUE PROPOSITION OF DFIS CENTER

The Computer Forensics Investigative Services (DFIS) center seems a logical component of the University’s academic infrastructure. It is just like chemistry labs, media studios or computer labs. It is a vital component of Academia. Although unlike the other labs on campus, (DFIS) can be a profit center. The *Computer Emergency Response Team* (CERT) located in Carnegie Mellon University in Pittsburg Pa, is a center to track and monitor cybercrime at national level. At the same time, it is a viable training center for the students to learn more about cyber space malware.

There are over 120 reputable universities in the US that have similar cybercrime and Forensics in-

stitute like (DFIS). These campus-based institutes contribute more than 40% to the fight against cyber-crime in the country. The US Government in fact, relies heavily on such institutes for technical resources and support, in exchange for yearly grants.

Schools like the University of Massachusetts, UCLA, and Dartmouth have already launched CF classes and seminars, and their faculties speak about the topic at national conferences. Other universities, such as MIT, UCLA, and the University of Texas at Dallas, boast good computer science departments that conduct research in computer forensics. Most of these institutes have done great job in bringing national attention to their schools. Professor Susan Brenner of the University of Dayton <http://cybercrimes.net/> is an excellent testimony in supporting the Law school of the University.

As an intersection between Law and technology, (DFIS) will offer the following unique services:

- To help graduating school lawyers understand the process of Computer Forensics, Digital Evidence, preparing litigation and investigative cases, and monetary damages of hacking.
- To draw on a large pool of Computer Science, Law, or IS students for manpower to support research or to work on grants or help on special assignments such as Ethical Hacking.
- To help outside clients, lawyers, and Law Enforcement, identify, acquire, restore, and analyze electronic data in litigation, as well as testifying experts in IT autopsy and crime reconstruction.
- To provide formal workshops and certification courses in Computer Forensics, cybercrime prevention, and in Business Continuity.
- To explore all available funding opportunities from all agencies such as NIST, The Institute of Justice, DHS, DOD and others. (DFIS) will be a potential qualifier for several grants.

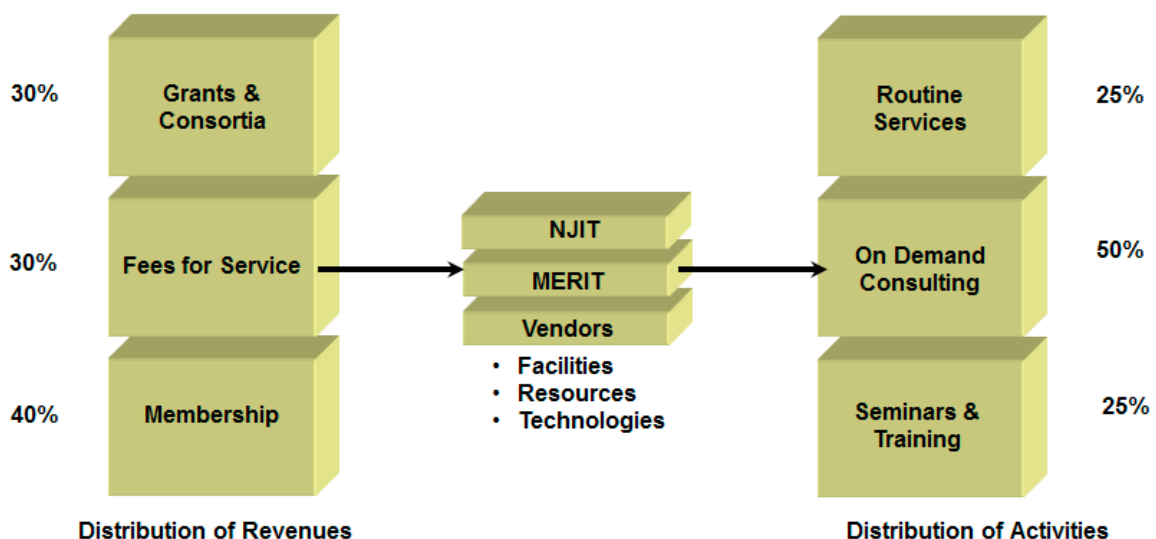


Figure 10. The DFIS Center Business Model

- To conduct research of computer crime and cyber terrorism and publish demographic surveys.
- To work and support of law enforcement, experts, and partner missions related to fighting computer crime and foreign counterintelligence missions related to cybercrimes and counter cyber terrorism.
- To link criminological and legal research to problems of criminality in the fields of computer technologies, with the purpose of rendering assistance to legislators, scientific, law enforcement and IT security administrators.
- To conduct seminars, conferences and international symposia on cybercrime and cyber terrorism.
- To create a library, a website, and publish articles and research results. (DFIS) will contribute to the international information exchange related with the struggle against criminality in the use of information technology.
- To prepare of students and analysts in the field of cybercrime prevention and investigation of illegal activities perpetrated through the use of information technology.

Table 1. Financial Case (Estimated Revenues for year 2012)

Item	Yearly Revenues	
Membership \$500/year for initially 50 members	\$25,000	Members will benefit from website bulletins and new about Forensics
Government Grants/Consortia	\$1,500,000	Funding will come from DHS/DOD/DOJ/
Disaster Recovery and Backup services	\$800,000	On demand requests from the private sector
On Demand State Government Investigation	\$3,000,000	On demand state Forensic investigations
Retaining Fees from private business 100 users	\$1,500,000	Banks, Pharma, and Hospitals contract to investigate cybercrime
Yearly Workshops (3 days)	\$120,000	Customer training
Yearly Seminars (1 day)	\$20,000	Management seminars
Total	\$6,945,000	

Table 2. Financial Case (Estimated Operating Costs)

Item	Yearly Expenses	Explanation
Director	\$120,000	The director will be responsible for the management of the center.
Forensic Technician2 (3)	\$240,000	Technicians will conduct the technical work
Hardware /Cloud	\$20,000	Special computer needs to be acquired for forensic work. Also connectivity with the cloud
Software/DB/Cloud deployment	\$10,000	EN CASE forensic software (1) will be provided by Guidance Software.
Travel/Training	\$4,000	Training for the technician
Supplies	\$6,000	Special material and accessories for forensic work
Facilities Leases	\$5,000	NJIT will offer space for the lab
Marketing	\$30,000	Reaching out to prospective clients
Courseware	\$20,000	Training material
Total Yearly Cost	\$435,000	

## FINANCIAL CASE



The cash flow of DFIS center will generated from three different sources: Consortia with academia, fee for service and yearly membership. The center will spend half

of its operating time working on forensic cases. Training and routine services (such as backup and recovery) will take 25% of the center's operation (Figure 10, Table 1 and Table 2).

Software Guidance is the company that markets En Case Forensic. <http://www.guidancesoftware.com/>.

## PART-6 DEPLOYMENT SCHEDULE OF THE DFIS CENTER



The DFIS center will require four months before it is fully operational. The Gantt chart implemented in 2006 (Figure 11).

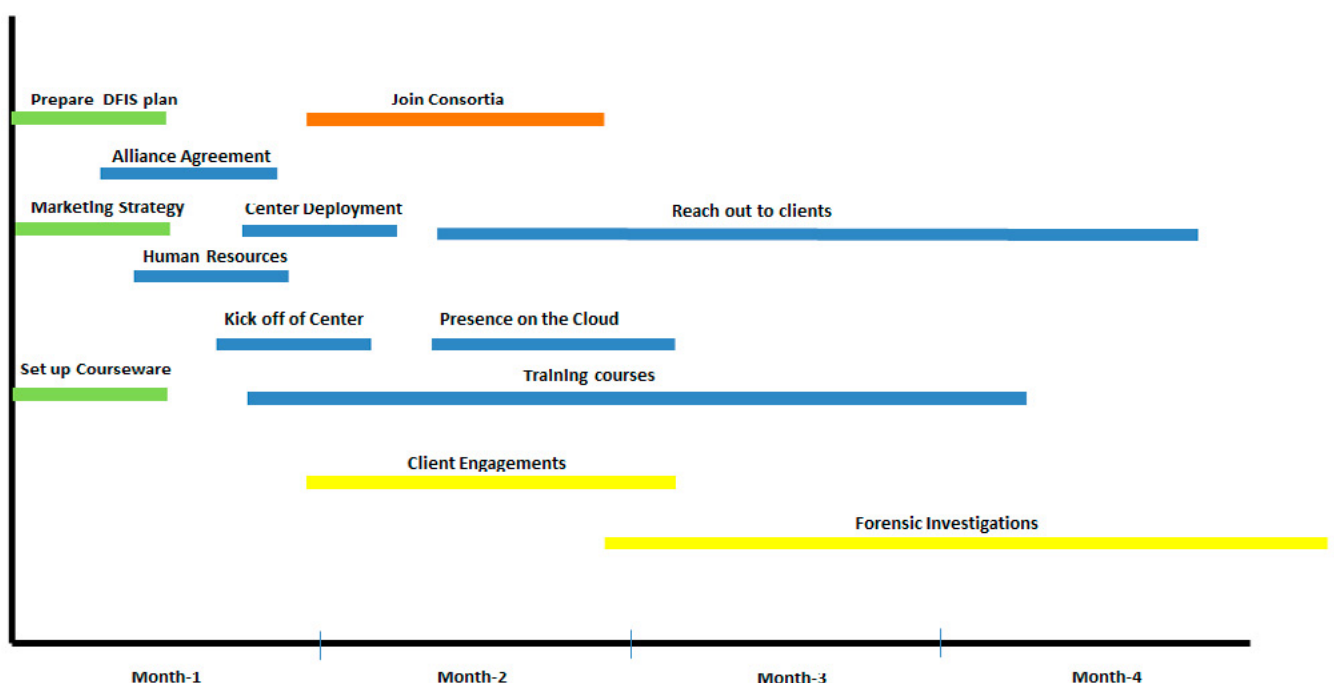
## Author bio



*Dr. Rocky Termanini is a cyber-security domain expert. He brings 45 years of multi-industry real-world experience to his clients and classes. He is a Professional Electrical Engineer and member of IEEE. He is a certified IT security professional, and member of the American College of Forensic Examiners.*

*Dr. Termanini is a senior advisor to Law Enforcement on Cyber-terrorism. He was an expert witness in court on cases related to Identity Theft and Credit Card Fraud. He advises companies on Information espionage and Business Intelligence. As a certified Forensics expert, he helps companies resolve internet crimes. He is the designer of the Smart Vaccine® and the Digital Immune Grid. He has lectured in several international conferences and taught the practical aspects of technology at several universities. He worked on several forensics projects in the US, and presented evidence in court.*

*Professor Termanini taught Information Systems classes at Connecticut State University, New York University, Quinnipiac University in Connecticut, and Connecticut State University. Also abroad, he taught at The University of Bahrain, and University College of Bahrain, and presently he is an adjunct professor at Abu Dhabi University. Dr. Termanini holds a PhD in Computer Science (Artificial Intelligence) from Yale University. He can be reached at [rocky@termanini.com](mailto:rocky@termanini.com).*



**Figure 11.** Deployment of the DFIS Center





# FORENSICS EUROPE EXPO

24 – 25 April 2013

Olympia, London

[ForensicsEuropeExpo.com](http://ForensicsEuropeExpo.com)

The Premier International Forensics Event for Police, Military, Intelligence Agencies, Lawyers, Corporate Forensic Analysts, Laboratories, Government Bodies and Agencies together with leading suppliers, services, equipment and practitioners from across the world.

Conferences – Workshops – Training – Networking – Exhibition

**REGISTER FOR FREE ENTRY TODAY**

[www.ForensicsEuropeExpo.com/digital](http://www.ForensicsEuropeExpo.com/digital)

Co-located with

  
**COUNTER  
TERROR EXPO**

Sponsored by



In Collaboration with



Organised in  
Partnership with



# DIGITAL CONTINUITY OF GOVERNMENT RECORDS

by **Dr. Stilianos Vidalis**, Lecturer at Staffordshire University and  
**Dr. Olga Angelopoulou** Lecturer at Derby University

The Digital Continuity project was conducted collaboratively by the University of Wales, Newport, Guidance Software and the Welsh Government in 2011. The centre of gravity of the project was to mine, categorise and classify (based on a pan-governmental vocabulary) information from a heterogeneous large scale computer infrastructure and store/fuse the search results in a forensically sound manner while destroying the duplicates and without disrupting daily staff operations.

**B**ack in 2007 the UK's government has identified a number of needs for public sector information. Those that related to this project were the following:

- Improve responsiveness to demand for public sector information,
- Ensure the most appropriate supply of information for re-use,
- Improve the supply of information for re-use,
- Promote innovative use of public sector information.

Those needs were re-iterated by Oliver Morley, Chief Executive of the National Archives in the UK in his speech about building a culture that shares knowledge more efficiently, and builds capability in the information of all kinds. The project brought together diverse knowledge from dif-

ferent business sectors in order to satisfy the aforementioned needs.

## INTRODUCTION

The first person to properly report and document the principles of information operations was Sun Tzu, thousands of years ago in his ancient Chinese military treatise. The same principles apply today across all of the different public and private sector organisations. It has become excessively important for public organisations to have the right information on the right time in order to be able to satisfy and service public needs in an appropriate manner, as specified by UK and EU legislation. It is equally important to apply innovation in extracting knowledge from existing data sets in order to proactively satisfy future needs of the public.

Today there are data-mining techniques that allow the turnaround time



on data requests to be measured in minutes. The procedures that are in place though, and the complexity of the operations that a civil servant has to follow, raises the turnaround time to days. The returned data must be the most appropriate, based on the search criteria, which creates the need of identifying and deleting duplicates. Furthermore, the data have to be stored in such a way that will allow for future farming and be able to address 'change' in the needs of the government and of the public.

In today's global interconnected world, information is considered to be the most important asset category under the context of risk management. Information can be knowledge, but cannot be defined as that. For defining information we will go back to 1995 when Michel Menou wrote that "...information encapsulates a wide range of concepts and phenomena...". "They relate to both processes and material states which are closely inter-related..." According to the same author, information can be:

- "A product, which encompasses information as thing, as object, as resource, as commodity,
- What is carried in a channel, including the channel itself,
- The contents."

Information is widely considered to have three abstractions: data, information and knowledge. We will add a fourth layer, that of the expertise. Data can be individual observations and low level primitive messages. Once we sort, classify or index them into organised sets, then we can refer to them as information. Our goal of course is to put the data elements in relational context for further analysis, which will result in understanding the information. Quoting Edward Waltz, the author of *Information Warfare Principles and Operations*: "Understanding of information provides a degree of comprehension of both the static and dynamic relationships of the objects of data and the ability to model structure and past (and future) behaviour of those objects. Knowledge includes both static content and dynamic processes."

Having enough knowledge regarding an issue will allow decision makers to develop expertise regarding that issue which in turn will allow for a shorter turnaround time for the decision to be implemented and for a greater trust to the correctness and appropriateness of that decision. We all thrive and aspire in doing things right, but are we doing the right things? Are we indeed making informed decisions to resolve our daily issues or are we simply compromising into doing what everyone else in our environment/community/virtual community is doing?

## THE PROBLEM

In 2011 the *Knowledge and Information Management Division* (KIMD) of the *Welsh Government*

(WG) had a diverse and heterogeneous network of approximately 6500 nodes that contained information stored in different data types: MS Office products, HTML, PDFs, files inherited from the merger of the many organisations that formed KIMD, statistics, engineering drawings and GIS data.

The KIMD IT Department had the constraint of not being able to introduce new servers in their server rooms, and actually the directive coming down from the British Government was on reducing the amount of servers, limiting the carbon footprint of the data centres, but also reducing their maintenance and running costs.

Against those constraints was the challenge of collecting data from their large scale heterogeneous computing infrastructure. Normally the process of collecting data that relate to specific criteria has the following steps:

- Identify, in collaboration with IT, all the locations where relevant data are kept, probably including servers as well as the employees' personal laptops/workstations;
- Collect the data (which normally cause disruption to normal user operations);
- Filter out the duplicates and the non-important data from the larger bulk that was collected; and
- Process the resulting filtered set of data so that they can be loaded into a document management system.

It is an expensive, resource-intensive process that depending on the scale of the environment can be very disruptive. We had to consider the different types of hardware and software that contained the data, as well as the diversity and age of the data. Furthermore, referring to the previous quote, data constitute only a part of the picture. In order to be able to develop knowledge and expertise we had to understand the processes that the data were used for in the past. The WG also had a need for automating the above process, limiting the turnaround time, and making it auditable, hence consistent and repeatable. Generalising, there are different methods for collecting data:

- Very basic, non-forensic copying of electronic files from employees' computers by the IT department using unsophisticated tools such as Windows Explorer;
- Manual collection by an expert performing either forensic or non-forensic machine-by-machine collections (i.e. not over the company network)
- In-house automated enterprise-wide forensic collection using a software application which can reach all the network nodes from a central location according to search criteria determined in a dynamic manner (and performed by a dedicated team according to a repeatable set



of processes and procedures), and can perform free in-house secondary culling and processing into a document management system.

The five factors that are affecting the forensically sound collection of data and in the same time constituted part of our requirements were: Scale, Cost, Responsibility, Context, Irretrievability, and Admissibility. There was also a requirement for a software application that could be implemented internally by the “KIMD” to search, identify, collect, and process electronically stored information from their heterogeneous large scale computer infrastructure from a central location without interfering with the employees’ use of their computers. The software had to provide the option of automated over-the-network collection of:

- Data responsive to search criteria:
  - keywords,
  - time-frames,
  - file types,
  - file metadata
- All user-created files based on user profile information.

The software had to use a methodology for extracting just the right data, cost effectively and in a manner which could not be challenged. User participation to the discovery, collection and storage of the data had to be kept at a minimum. Finally, KIMD’s infrastructure has been developing for the last two decades and data and processes dated back to the 80s. We had to fuse and analyse the data without the participation of the original data owners.

## THE RESULTS

The aim of the Digital Continuity project was to mine, categorise and classify information from a heterogeneous large-scale computer infrastructure and then store the search results in a forensically sound manner. Duplicate information was to be identified for destruction and the process was to be designed so that it could be implemented without disrupting staff operations.

The test data was a 217Gb (810,000 files) sample taken from the Welsh Government (WG) shared drives and email vault. The records concerned largely related to the work of the Department of Education and Skills though 25% of the sample were taken from the wider organisation in order to ensure that the classification system used were useful over a broad range of subjects. The test data were stored in a purpose build isolated virtualised test environment. All the project development work occurred within that test environment.

De-duplication of the test data was achieved. Some 35.88% of the files were identified as duplicates. Removing these files resulted in a saving of

29.49% of physical space. After one ‘pass’ of the data, it was possible to generate usable metadata for 75.7% of the de-duplicated data set. We will refer to this as the rich data set. The retention policies of the WG were used to design queries and rules for analysing the rich data set. It was possible to extract 65% of the files in the rich data set for long-term retention together with their metadata in a format that would allow transfer to the WG Electronic Document and Record Management System (ERDMS Known as iShare within the WG). This translates to 55% of the de-duplicated data set. Further analysis of the rich data set would have resulted in a better extraction rate.

The data acquisition took *24 hours and 3 minutes* for 211.9GB. That is 150.371MB/min, which is within the lower range of the network performance based on our performance tests. Projecting that to the whole infrastructure of the WG, it was estimated that a data acquisition through the eDiscovery Suite would take *290.5 days*. If we could get maximum performance from the network, then this estimate would fall to *60.6 days*. Of course, even this is not practical, hence it was recommended to *fragment the data set and parallelise the collection operation*.

The de-duplication process took *5 hours* for 211.9GB. Projecting that figure to the whole of the WG infrastructure it is estimated that a full de-duplication would take approximately *60.4 days*.

As this is not practical, it is recommended that the process should be done on the fragmented datasets, which will result in further parallelising the operation.

The indexing process took 5 days for 149.4GB. Using the 35.88% duplication figure, some 39395GB would need to be indexed. This would take an estimated 1318.451 days. With the suggested fragmentation of the data set and the parallelisation of the operation this time would be reduced.

There have been some technical (and non-technical) issues that affected our operations.

- The virtualisation of the e-Discovery components was problematic, as virtualising within a virtual environment caused instabilities to the majority of the eDiscovery components.
- Legacy data types created in FAT32 systems do not hold rich metadata. This meant that the e-discovery process did not produce metadata to the existing National Archives standards. The retrieved metadata were not sufficient to satisfy all the classification queries. Interviews with WG personnel had to be performed in order to collect additional primary data about the current practice of classifying documents in WG.
- The lack of dedicated hardware resources greatly affected the performance of the eDiscovery Suite components. The acquisition, hashing and indexing operations were most affected.

- Towards the end of the project, there was insufficient memory to load the case and initiate the keyword searches for further analysing the residual data.

Despite the above problems the test data set was preserved in a forensically sound manner for the duration of the project. The hashing and indexing operations were conducted automatically and transparently by the eDiscovery Suite with minimal human intervention and an audit trail for all of the data manipulation activities was maintained.

## CONCLUSIONS

Traditionally e-Discovery techniques are being used during litigation activities for identifying valuable assets and minimising costs. We managed to successfully apply digital forensic disciplines to the information management and governance field for providing the Welsh Government with an innovative solution to their complex problem of improving responsiveness to demand for public sector information, and ensuring the most appropriate supply of information for re-use. In the near future we will be further exploiting the developed method and the project artefacts in order to finely tune and streamline the operations. There are plans for setting up a private cloud infrastructure and using cloud resources in order to optimise the collection and indexing turnaround time.

### Author bio

*Dr. Stilianos Vidalis received his PhD in Threat Assessment under the context of Information Security in July 2004. He joined the University of Staffordshire in November 2012 where he is currently employed as a Lecturer. He is a panel member for the International Conference of Information Warfare, the Emerging Intelligent Data & Web Technologies Conference, the International Conference on Cybercrime and Computer Forensic 2013: One Digital World, many Digital Crimes, the International Conference on Cloud Security Management and for the European Conference of Information Warfare and Security. He is lecturing in the subjects of information security and digital forensics. His research interests are in the areas of Information Security, Information Operations, Digital Forensics, Threat Assessment, Profiling and effective computer defence mechanisms. [stilianos.vidalis@staffs.ac.uk](mailto:stilianos.vidalis@staffs.ac.uk)*

### Author bio

*Dr. Olga Angelopoulou is a lecturer in Digital Forensics at the University of Derby. She obtained a doctorate in Computing with the title: 'Analysis of Digital Evidence in Identity Theft Investigations'. Her research interests include Digital Forensics, Identity Theft, Online Fraud, Digital Investigation Methodologies and Online Social Networking. [o.angelopoulou@derby.ac.uk](mailto:o.angelopoulou@derby.ac.uk)*



**Staffordshire University** is offering undergraduate degrees in Forensic Computing and Cyber-Security.

Both the BSc in Cyber-Security and the BSc in Forensic Computing at Staffordshire University are highly practical multidisciplinary programmes designed to enable the scholars/students to proactively secure large scale heterogeneous computing infrastructures and identify and investigate cybercrimes, such as fraud, identity theft, phishing and pharming, software piracy and corporate espionage taking place in a variety of environments: standalone computers, intranets and the Internet, and virtualised infrastructures including Cloud environments. The programmes will equip the scholars with the appropriate skillset for securing and preserving digital crime scenes as well as forensically collecting and analysing digital artefacts.

Under the guidance of a highly experienced team, including experts from the Police and other Law Enforcement Agencies, scholars participate in full scale penetration tests and digital forensic investigations and analyse digital crime scenes that are set-up in our dedicated, self-contained digital forensic laboratories. They have access to the latest digital forensic software and hardware, including biometric kit and mobile phone forensic kit. The environment is designed to emulate the conditions found in the industry.

**Security  
News**

**Vulnerability  
Management**



**Secure Connexion**  
Security News. Investigations. Vulnerability Assessment.

*Currently developing hardware  
and software solutions for the  
home and business world.*

**Cybercrime  
Investigations**

**Beginner  
Concepts**





TrustSphere



# Global Reputation



TrustCloud

Industry's Most Comprehensive Real Time  
Dynamic Reputation List

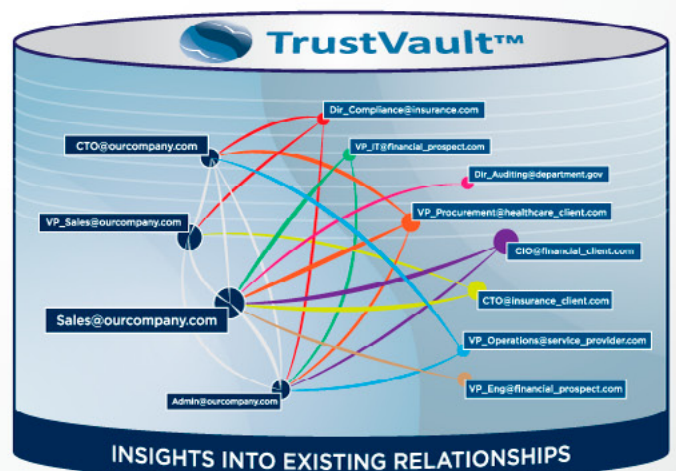


# Local Relationships



TrustVault™

Restoring Security, Integrity &  
Reliability to Messaging Systems



TrustSphere  
Tel: +65 6536 5203  
Fax: +65 6536 5463  
[www.TrustSphere.com](http://www.TrustSphere.com)

3 Phillip Street  
#13- 03 Commerce Point  
Singapore 048693



# Dr.Web SplDer is 8-legged!

New Package  
Installer

Improved Technology  
for Protection against  
yet-unknown Threats

Improved  
Parental Control

New Anti-Rootkit  
Module

Online Service  
Dr.Web Cloud

Free Upgrade  
to New Version

Unified User  
Interface

Better than ever: Dr.Web  
Security Space version 8.0!  
30-day trial available from  
<https://download.drweb.com/?lng=en>



**New Version**  
Dr.Web Security Space  
and Dr.Web Antivirus for Windows

# 8.0

Get your free 60-day license under  
<https://www.drweb.com/press/>



© Doctor Web  
2003 — 2013

Doctor Web is a Russian anti-virus vendor with a software development record dating back to 1992.  
[www.drweb.com](http://www.drweb.com)