Digital Forensic Investigations: Issues of Intangibility, Complications and Inconsistencies in Cyber-Crimes

Ezer Osei Yeboah-Boateng[1] and Elvis Akwa-Bonsu[2]

[1]*Ghana Technology University College (GTUC)*
[2]*Detectware Limited, Ghana*
Email: eyeboah-boateng@gtuc.edu.gh; elvis@detect-ware.net

Received 31 August 2015; Accepted 20 November 2015;
Publication 22 January 2016

Abstract

The use of the Internet and computing resources as vital business tools continue to gain prominence day-by-day. Computing resources are utilized to create innovative and value-added products and services. Associated with this trend is the extent of cyber-crimes committed against or using computers. Experts anticipate that the extent and severity of cyber-attacks have increased in recent times and are likely to explode, unless some mitigation measures are instituted to curb the menace. As a response to the growth of cyber-crimes, the field of digital forensics has emerged.

Digital forensic investigations have evolved with the passage of time and it's impacted by many externalities. A number of key challenges ought to be addressed, such as the intangibility, complications and inconsistencies associated with the investigations and presentation of prosecutorial artefacts. The digital evidence is usually intangible in nature, such as an electronic pulse or magnetic charge. The question is how can the intangibility of computer crime complicate the digital forensic investigations? To what extent can inconsistencies during the investigation mar the permissibility or admissibility of the evidence?

Journal of Cyber Security, Vol. 4, 87–104.
doi: 10.13052/jcsm2245-1439.425

This study is an experimentally exploratory set-up with virtual systems subjected to some malware exploits. Using live response tools, we collected data and analyzed the payloads and the infected systems. Utilizing triage information, memory and disk images were collected for analysis. We also carried out reverse engineering to decompose the payload.

The study unearthed the digital truth about malwares and cyber-criminal activities, whilst benchmarking with standard procedures for presenting court admissible digital evidence. The timelines of activities on infected systems were reconstructed. The study demonstrated that externalities of intangibility, complications and inconsistencies can easily mar digital forensic investigations or even bring the entire process to an abrupt end. Further studies would be carried out to demonstrate other ways perpetrators use in concealing valuable digital evidence in a cyber-crime.

Keywords: Digital Forensic Investigation, Cyber-crime, Digital evidence, Artefacts, Malwares, Payload.

1 Introduction

The use of the Internet and computing resources as vital business tools continue to gain prominence day-by-day. Computing resources are utilized to create innovative and value-added products and services [1]. Associated with this trend is the extent of cyber-crimes committed against or using computers. Experts anticipate that the extent and severity of cyber-attacks have increased in recent times and are likely to explode, unless some mitigation measures are instituted to curb the menace [2]. As a response to the growth of cyber-crimes, the field of digital forensics has emerged.

Typically, digital forensics involves carefully collecting and examining electronic evidence or artefacts, as well as accurate analysis and interpretation of collected evidence. This investigative process assesses the extent of damage to a compromised or an attacked system, as well as recovers lost information from such compromised system and ultimately, to present the digital evidence to prosecute the cyber-crime perpetrators. It has become imperative that law enforcement officers and digital forensics examiners adhere to high standards of the profession, if digital evidences were to be permissible in a competent court of jurisdiction.

Digital forensic investigations have evolved with the passage of time and its impacted by many externalities [3]. A number of key challenges ought to be addressed, such as the intangibility, complications and inconsistencies associated with the investigations and presentation of prosecutorial artefacts. The digital evidence is usually intangible in nature, such as an electronic pulse or magnetic charge. The question is, how can the intangibility of computer crime complicate the digital forensic investigations? To what extent can inconsistencies during the investigation mar the permissibility or admissibility of the evidence?

Cases abound whereby suspects were either incriminated or set free due to misinterpretation of digital evidence and/or inaccurate methods employed in collecting and analyzing the data.

The objectives of the study are:

- To collect and examine electronic evidence or artefacts – to assess the extent of damage and to recover lost information or data;
- To present digital evidence that would be admissible in court for the prosecution of cyber-crime perpetrators;
- To examine the externalities (network effects) that are likely to affect the admissibility of digital evidence in court, as well as to render the forensic investigations null and void.

Typically, in conducting forensic investigations, or incident response, a number of factors could hamper the admissibility of the results or evidence. In this paper, we have categorized the issues into three (3) externalities, which are:

- Intangibility – issues involving the RAM and memory analysis;
- Complications – issues involving anti-forensics, which can divert the focus of the investigations, or hide key evidential artefacts using such techniques as Steganography, Attention-Deficit-Disorder (ADD), Dementia, etc.;
- Inconsistencies – issues involving procedures, usage of tools and techniques, imaging of drives, chain-of-custody, the Locard Exchange Principles, etc.

The Locard Exchange Principle stipulates that the perpetrator is likely to leave traces and/or carry some evidentiary artefacts at the crime scene [4]. In expantiating the Locard's digital forensic cyber exchange principle, [5] posited that the traceable artefacts upon the cyber-incident, requires delving deeper into the compromised computing resource to adduce the evidence. This activity is challenging and by itself could introduce further complications and/or inconsistencies, if strict best practices are not adhered to.

2 Problem Formulation

Cyber-crime issues have assumed global dimension, with the perpetrators' profile ever becoming sophisticated [6], whilst forensic examiners and law enforcers are saddled with challenges in jurisdiction and prosecutorial difficulties [7]. Whereas emerging technologies are providing new opportunities for cyber criminals, new challenges and concerns for forensic examiners and law enforcement officers are emerging [8, 9]. The extent of cyber-crime has increased in recent times, and experts believe if nothing done to curb the menace, its impact is likely to be catastrophic in future [2].

Reported and/or documented cases of cyber-crimes and incidents are overwhelming and the quantum of dollar losses is gargantuan and mind-boggling. Interestingly, the reported cases during the period, 1991–1995, to the US CERT increased by almost 500% and the world-wide incidences had increased by over 700% [8]. Recently, the Malaysian CERT reported of 40.9% in fraud, 7.9% in malware, 5.3% in harassment, respective increases from 2013 to 2014 [10].

In a simulated penetration testing of US government computers, it was reported that about 65% successfully attacks occurred, with only 4% detected by the administrators [8]. It must be noted that lots of cyber incidents are not reported, and that unreported cases could also impede cyber-crime investigations.

In carrying out the incident response, the Forensic Examiner needs to answer a number of pertinent but daunting questions. For instance, "where did he obtain his/her tools from?"; "what standards and control measures or precautions are adhered to?"; "are the processes and procedures in conformity with laid down principles?"; "are there conformity or uniformity with his definitions, chain-of-custody and analysis – in respect of the admissibility of the digital evidence?"

The object of this study is to among others, carry out malware analysis, in order to determine the malware activities or operations, to comprehend the malware behavior, and analyze the workings of the malware codes. This study employs dynamic malware analysis, which can analyze activities in respect of threats attacking information assets in various states. For instance, attacks in transit or during transmission in networks and hosts, in storage or in file systems, in usage or in memory are all analyzed [11].

The paper is organized as follows: this introductory section deals with the background and problem formulation; the succeeding section deals with the literature review on digital forensic investigations and the externalities;

the following section deals with experiment and its approach; the following section presents the results and analysis. The implications of the findings are discussed and concluded.

3 Literature Review

This section reviews literature on digital forensic investigations and its challenges encountered, especially those that are likely to affect adversely the admissibility of the adduced evidence in court. Various concerns are at play here: from procedural through perceptions and technicalities.

Some of the issues raised to discredit digital forensic investigations include the lack of trained forensic analyst, proficiency testing, certifications, best practices, policies and procedures, laboratory standards, and accreditation, etc. [12].

3.1 Digital Forensics Investigation

Digital Forensic Investigation is basically incident response assessment to present digital evidence, which must be admissible in court, which may be used for either criminal or corporate and civil proceedings. The digital evidence artefacts often examined include, but not limited to, personal computers (PCs), laptops, notebooks, smartphones, cellphones, tablets, servers, GPS devices, Gaming Consoles, storage media, network devices and infrastructure, etc.

Some of the issues or cases usually being investigated include [13]:

- Use of smartphones to snap a picture or record a video, that was subsequently uploaded or shared unto a social network platform, e.g. Facebook, or sent via an email as an attachment;
- Use of computing resources to download an illicit image or file, e.g. child pornography, confidential corporate documents, etc.;
- Use of computing resources to commit financial crimes, fraud, money laundering, employee misconduct, copyright violations, distribution of inappropriate materials, etc. [14].

Another challenge with digital forensics is the perception of some law enforcement officers that digital forensics is merely an investigative tool, rather than a scientific evaluation [13]. This is more evident when due to organizational structural issues in the security agencies, officers are re-deployed periodically, without recourse to continuous experience leveraging in digital forensic investigations.

3.2 Intangibilities

Typically, intangibility is used to describe the ability to assess the value gained from engaging in an activity using any tangible evidence, e.g. software intangibility [15]. To what extent can the intangibility of cyber-crime complicate investigations and subsequently prosecution? Some difficulties encountered during investigations, especially in collecting evidence, can be associated with characteristic service attributes, which are either "intangibility, inseparability, perishability or heterogeneity" [16, p. 2].

In this study, we reckon malware activities as a computing service, albeit with negative network effects. Intangible nature of service(s) is such that it is performed and not easily measured. In describing the intangibility of services in computing, [16] related with the customer's change in his/her experiences, be it visible or not with change in computing resource state of operations. This introduces the potential for digital alteration in the evidence.

Evidentiary items are typically in both analog and digital formats [17], tangible and intangible forms, etc.

3.3 Complications

Generally, complications are difficulties or challenges emanating as a result of a certain circumstance or occurrence. In the context of digital forensic investigations, complications may arise from a cyber incident and the associated incident response. It may be legal, technical or ethical in nature. These complications can also emanate from the examiner or investigator, as well as the perpetrator, as he uses state-of-the-art techniques to circumvent the investigation.

The investigation becomes complicated even when one or a part of the compromised systems are geo-located in another jurisdiction [18]. Complications like this could sometimes end the investigations abruptly, though recent cases have seen the collaboration and cooperation of international law enforcement agencies, particularly the INTERPOL [19].

Another complication may arise with regards to the requirement of the forensic examiner to possess a state-accredited license in order to have the evidence admissible [20].

Some complications in investigating incident response or cyber-crimes arise out of objects or artefacts hiding using anti-forensic toolkits. Especially, in Windows based systems, since the Memory Analyzer tool has to run on the compromised machine, there's a potential for perpetrators to hide in memory dumps.

The use of anti-forensics are meant to thwart the investigations and to pollute the memory with fake artefacts. This study utilizes tools such as the Dementia (a DOS based tool for hiding "target artefacts in memory dumps – hides processes, process threads and [associated] connections" [21, p. 30]; Steganography – tools that facilitate hidden data in a carrier file or data; Attention Deficit Disorder (ADD) [22].

Microsoft Computer Online Forensic Evidence Extractor (COFEE) includes tools for password decryption, Internet history recovery and other data extraction. It also recovers data stored in volatile memory which could be lost if the computer were shut down.

3.4 Inconsistencies

Inconsistencies are anomalies, omissions, exaggerations or other loopholes found in forensic investigations contradictory to the evidence and which may compromise the value of the evidence or renders it inadmissible [20, 23].

These inconsistencies come in different forms. There are those associated with the compromised systems possibly due in part to the normal operations of the system (even in an uncompromised state) and that resulting from the compromises. These types of inconsistencies are described by [24] as temporal inconsistencies. They proposed a technique for detecting inconsistencies in digital forensics investigation.

Another type, jurisprudential inconsistencies may be due mainly to the lack of experiences of the judges on computer related crimes, cyber-crimes, or crimes committed with high-tech devices and/or against them, etc.

4 Methodology

In this section, we define the experimental set-up, its configurations, and the procedures and tools adopted for the exercise. Malware exploits utilized are clearly defined with its sources.

4.1 Experimental Set-up Laboratory

We installed a virtual environment using VirtualBox 5.0.4 for Windows hosts, from Oracle. This was for convenience and ease of use. Then, we installed Windows XP, both SP2 and SP3 packs. This was followed by a Linux operating system based toolkit, REMnux, for its robustness in respect of tools used for the analysis. In configuring the REMnux and the Windows servers, the default network setting is NAT (network address translation), but we configured it for "Host Only Adapter" and enabled promiscuous mode to "allow ALL".

It must be noted that, the set-up was carried out with a virtual-ware, so that the experiment does not interfere with the normal nor escalate malware to production environment.

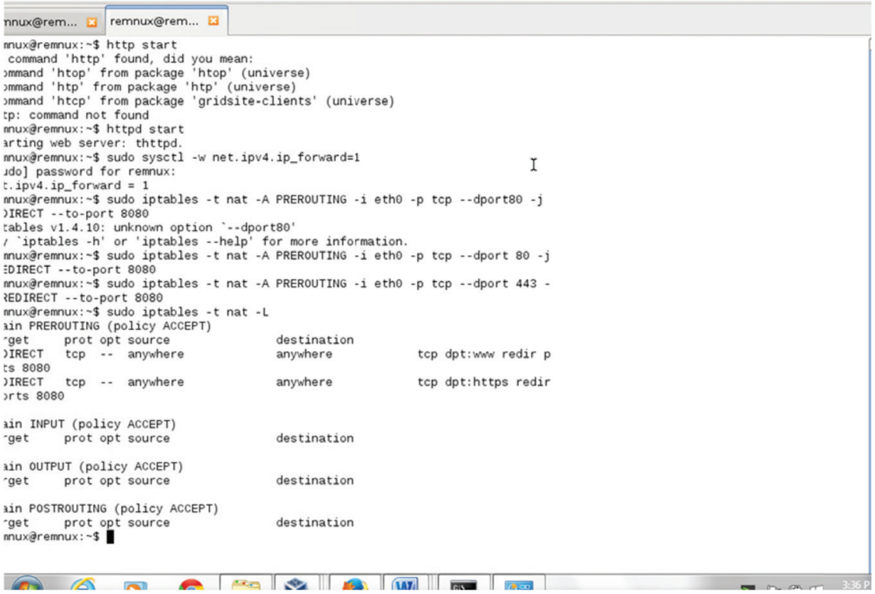
The captured images and data were also analyzed using other tools, such as TriageIR (for incident response), LiveResponse, Volatility, etc. For the host analysis, we used tools such as the Magnet Forensics RAMCapture, FTKImager, MFT Dumper (for the Master File Table), AnalyzeMFT (to create the timelines), etc. For the network analysis, we used tools such as the WireShark, NetworkMiner, TCPDump, etc. For the memory analysis, we used mainly the Volatility toolkit.

REMnux is a toolkit, developed by Lenny Zeltser [11], to help researchers and computer forensic investigators to extract artefacts for analysis, with the view to produce credible (court admissible) digital evidence. REMnux contains a number of tools and commands for analyzing malicious softwares or malwares. REMnux is pre-configured to facilitate the investigation by prompting the examiner to select the data to be exported, and it is usually saved and stored in the same drive space from which the tool was launched.

We configured the REMnux to run a pseudo DNS service called Fakedns, a proxy (a NAT server) with SSL protocol and as a gateway for the Windows machines. We reconfigured the IPTables by writing a script that points DNS requests to the REMnux gateway. The Fakedns (or pseudo DNS server) runs on the REMnux and uses "whereis fakedns" Linux command.

```
−sudo fakedns 192.168.56.103 - running
*// started a web server using Apache; to as certain, we opened a web browser for confirmation;
*// in setting up the IPTables
- sudo sysctl  − w net.ipv4.ip _ forward
−sudo iptables  − t nat  − A prerouting -1 eth0 -p tcp - - rdport
```

With this setup, any DNS requests from the victim machine are re-directed to the fakedns server. The IPTables have also been re-configured as follows: TCP #80 and/or TCP #443 meant for HTTP and HTTPs services are re-directed to the pre-configured port TCP #8080.



```
nnux@remnux:~$ http start
 command 'http' found, did you mean:
ommand 'htop' from package 'htop' (universe)
ommand 'htp' from package 'htp' (universe)
ommand 'htcp' from package 'gridsite-clients' (universe)
tp: command not found
nnux@remnux:~$ httpd start
arting web server: thttpd.
nnux@remnux:~$ sudo sysctl -w net.ipv4.ip_forward=1
udo] password for remnux:
t.ipv4.ip_forward = 1
nnux@remnux:~$ sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport80 -j
DIRECT --to-port 8080
tables v1.4.10: unknown option `--dport80'
/ `iptables -h' or 'iptables --help' for more information.
nnux@remnux:~$ sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j
EDIRECT --to-port 8080
nnux@remnux:~$ sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -
REDIRECT --to-port 8080
nnux@remnux:~$ sudo iptables -t nat -L
ain PREROUTING (policy ACCEPT)
rget     prot opt source               destination
DIRECT   tcp  --  anywhere             anywhere            tcp dpt:www redir p
ts 8080
DIRECT   tcp  --  anywhere             anywhere            tcp dpt:https redir
orts 8080

ain INPUT (policy ACCEPT)
rget     prot opt source               destination

ain OUTPUT (policy ACCEPT)
rget     prot opt source               destination

ain POSTROUTING (policy ACCEPT)
rget     prot opt source               destination
nnux@remnux:~$ █
```

Figure 1 Configuration of the REMnux.

4.2 Malware Samples & Tools Used

Malware exploits or samples used were mainly taken from [11]; the Trojan .Stabuniq was specifically used in the experiment. The Trojan.Stabuniq was discovered by Symantec on December 17, 2012 [25]. It is a Trojan horse that steals confidential information from compromised systems. It is usually found in proxy and gateway servers. Upon infection, the Trojan masquerades amongst the existing files. It could affect a banking machines as well as home PCs. The typical attack vector used by the Trojan.Stabuniq is through emails and malicious websites, using phishing attacks [26].

FTKImager was used to capture disk image for analysis; RAMCapture tool was used to capture a memory image for analysis; and WireShark and TCPDump, running on the REMnux, were used to capture network packets.

Amongst the tools utilized in the REMnux suite is a process explorer and monitor. These are advanced monitoring tools for Windows, which monitors in real-time system activities, including Registry and process threads and activities [27].

The monitoring capabilities include filtering and furnishing of a comprehensive list of event parameters, such as "session IDs, full thread stacks"

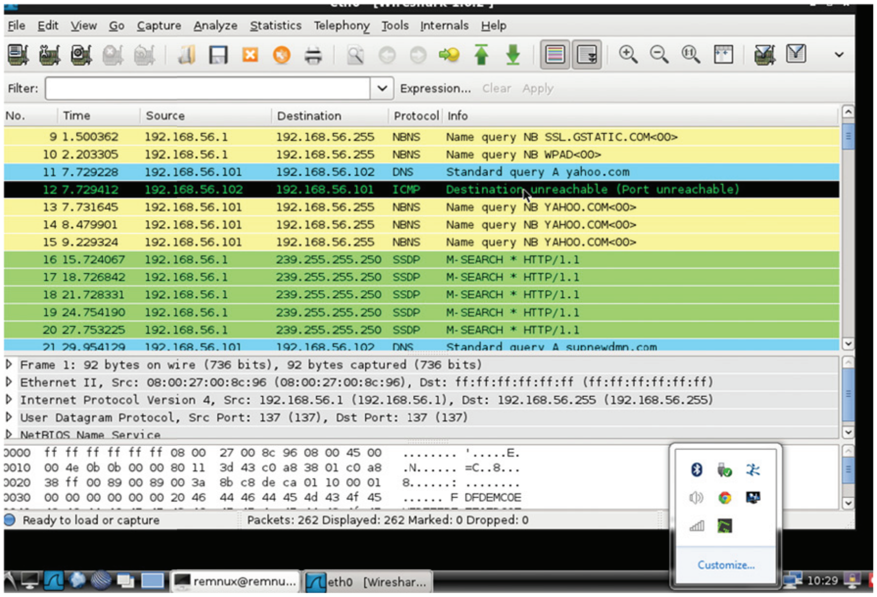
[27, p. 1] as well as logs and associated timestamps for boots and processes. We also used SysInternals utilities such as Regshot to facilitate the snap shots of processes running before and after the malware is launched. This helps in the comparison and analysis of the differences that have occurred.

5 Results & Analysis

This section presents the results of the experiment and some analytics of the malware behavior. First, we used the Magnet Foresnic RAMCapture tool to capture the memory image for analysis with the Volatility toolkit. The RAM image profile of the WIN SP2x86, image date and time created as 2015–10–11 13:47:40 UTC.

By inputting the Linux command: *remnux@remnux*: –$ ifconfig depicted the IP address of the REMnux: *eth0*: *link encap*: *Ethernet Hwaddr inet addr*: 192.168.56.102, which serves as a gateway, an internal DNS, running fakeDNS and WireShark.

Figure 2 depicts the system status before the launching of the malware exploits, whereas Figure 3 shows the system upon infection. Figure 3 also shows the network connections for the malware. The malware first contacted



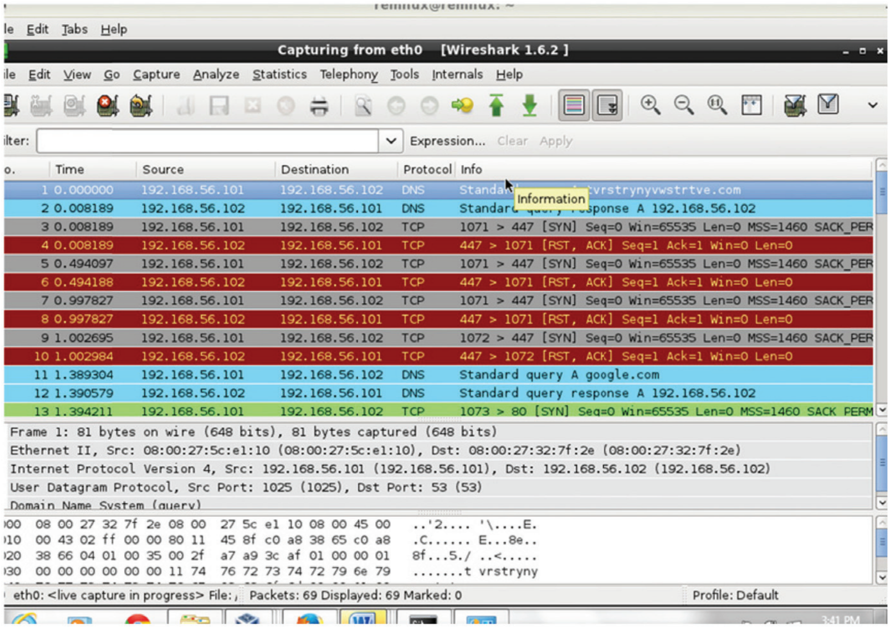
```
No.   Time         Source           Destination      Protocol Info
    9 1.500362     192.168.56.1     192.168.56.255   NBNS     Name query NB SSL.GSTATIC.COM<00>
   10 2.203305     192.168.56.1     192.168.56.255   NBNS     Name query NB WPAD<00>
   11 7.729228     192.168.56.101   192.168.56.102   DNS      Standard query A yahoo.com
   12 7.729412     192.168.56.102   192.168.56.101   ICMP     Destination unreachable (Port unreachable)
   13 7.731645     192.168.56.101   192.168.56.255   NBNS     Name query NB YAHOO.COM<00>
   14 8.479901     192.168.56.101   192.168.56.255   NBNS     Name query NB YAHOO.COM<00>
   15 9.229324     192.168.56.101   192.168.56.255   NBNS     Name query NB YAHOO.COM<00>
   16 15.724067    192.168.56.1     239.255.255.250  SSDP     M-SEARCH * HTTP/1.1
   17 18.726842    192.168.56.1     239.255.255.250  SSDP     M-SEARCH * HTTP/1.1
   18 21.728331    192.168.56.1     239.255.255.250  SSDP     M-SEARCH * HTTP/1.1
   19 24.754190    192.168.56.1     239.255.255.250  SSDP     M-SEARCH * HTTP/1.1
   20 27.753225    192.168.56.1     239.255.255.250  SSDP     M-SEARCH * HTTP/1.1
   21 29.954129    192.168.56.101   192.168.56.102   DNS      Standard query A supnewdmn.com

▷ Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
▷ Ethernet II, Src: 08:00:27:00:8c:96 (08:00:27:00:8c:96), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
▷ Internet Protocol Version 4, Src: 192.168.56.1 (192.168.56.1), Dst: 192.168.56.255 (192.168.56.255)
▷ User Datagram Protocol, Src Port: 137 (137), Dst Port: 137 (137)
▷ NetBIOS Name Service

0000  ff ff ff ff ff ff 08 00  27 00 8c 96 08 00 45 00   ........ '.....E.
0010  00 4e 0b 0b 00 00 80 11  3d 43 c0 a8 38 01 c0 a8   .N...... =C..8...
0020  38 ff 00 89 00 89 00 3a  8b c8 de ca 01 10 00 01   8......: ........
0030  00 00 00 00 00 00 20 46  44 46 44 45 4d 43 4f 45   ...... F DFDEMCOE

Ready to load or capture        Packets: 262 Displayed: 262 Marked: 0 Dropped: 0
```

Figure 2 WireShark Report before Malware Infection.


remnux@remnux: ~
le Edit Tabs Help
Capturing from eth0 [Wireshark 1.6.2]
ile Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
ilter:
Expression... Clear Apply
Information
Profile: Default

```
o.    Time        Source           Destination      Protocol  Info
    1 0.000000    192.168.56.101   192.168.56.102   DNS       Standa          tvrstrynyvwstrtve.com
    2 0.008189    192.168.56.102   192.168.56.101   DNS       Standard          sponse A 192.168.56.102
    3 0.008189    192.168.56.101   192.168.56.102   TCP       1071 > 447 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PER
    4 0.008189    192.168.56.102   192.168.56.101   TCP       447 > 1071 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    5 0.494097    192.168.56.101   192.168.56.102   TCP       1071 > 447 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PER
    6 0.494188    192.168.56.102   192.168.56.101   TCP       447 > 1071 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    7 0.997827    192.168.56.101   192.168.56.102   TCP       1071 > 447 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PER
    8 0.997827    192.168.56.102   192.168.56.101   TCP       447 > 1071 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
    9 1.002695    192.168.56.101   192.168.56.102   TCP       1072 > 447 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PER
   10 1.002984    192.168.56.102   192.168.56.101   TCP       447 > 1072 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   11 1.389304    192.168.56.101   192.168.56.102   DNS       Standard query A google.com
   12 1.390579    192.168.56.102   192.168.56.101   DNS       Standard query response A 192.168.56.102
   13 1.394211    192.168.56.101   192.168.56.102   TCP       1073 > 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM

Frame 1: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
Ethernet II, Src: 08:00:27:5c:e1:10 (08:00:27:5c:e1:10), Dst: 08:00:27:32:7f:2e (08:00:27:32:7f:2e)
Internet Protocol Version 4, Src: 192.168.56.101 (192.168.56.101), Dst: 192.168.56.102 (192.168.56.102)
User Datagram Protocol, Src Port: 1025 (1025), Dst Port: 53 (53)
Domain Name System (query)

)00  08 00 27 32 7f 2e 08 00  27 5c e1 10 08 00 45 00   ..'2.... '\....E.
)10  00 43 02 ff 00 00 80 11  45 8f c0 a8 38 65 c0 a8   .C...... E...8e..
)20  38 66 04 01 00 35 00 2f  a7 a9 3c af 01 00 00 01   8f...5./ ..<.....
)30  00 00 00 00 00 00 11 74  76 72 73 74 72 79 6e 79   .......t vrstryny

eth0: <live capture in progress> File: ,  Packets: 69 Displayed: 69 Marked: 0
```

Figure 3 WireShark Report after Malware Infection.

the DNS server after an infection to a site www.tvrstrynyvwstrtve.com which is a suspected domain.Carrying out further malware analysis reveals that, the Trojan.Stabuniq commonly affect x86 or 32-bit machines and compatibles, and Windows GUI based systems, with file type WIN32.exe.

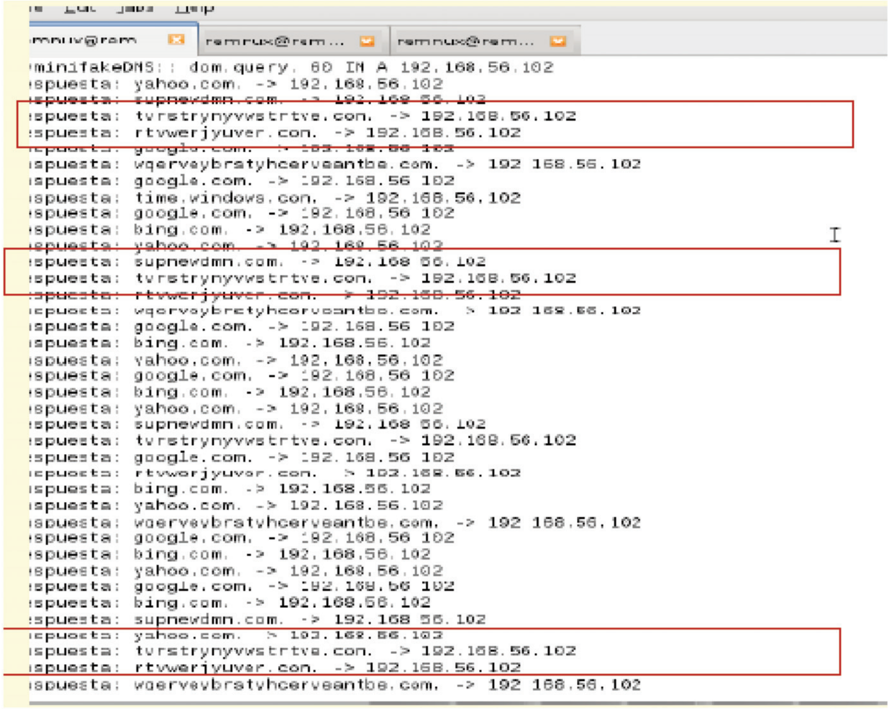
This malware uses the iEXPLORE.EXE, a legitimate file, to launch the viruses with its associated destructive payload.

With clean RAM image we found iEXPLORER with PIDs 164 and 152 and WSCNTFY 1054.

Using the Volatility toolkit, we executed "malfind" command and we found iEXPLORER with PIDs 1356, 1676 and 1684 as infected.

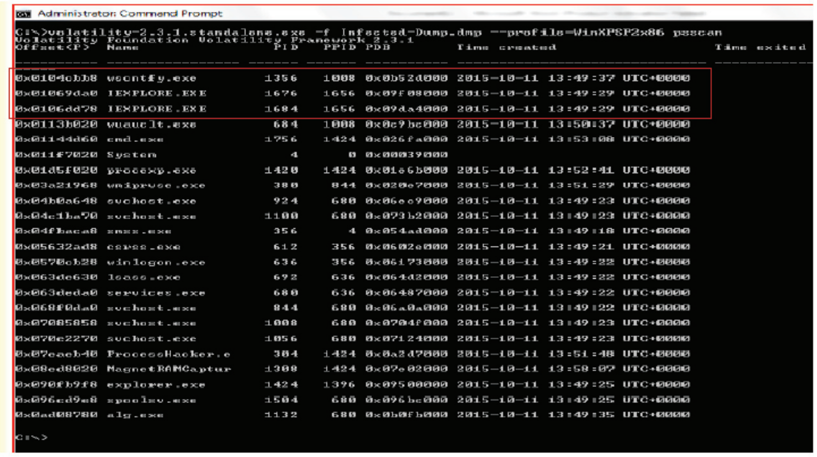
As indicated, the experiment was carried out in a controlled environment. This allows us to observe the creation of new files in the victim system, as it copies itself under different names and paths (c.f. Figures 4 & 5). The malware interacts with specific registry keys and injects the code into the iEXPLORE.EXE process, in order to ensure its persistence in the infected system, even after reboots.

We also observe some network activity in some domains as the malware interacts with the compromised system.



```
minifakeDNS:: dom.query. 60 IN A 192.168.56.102
spuesta: yahoo.com. -> 192.168.56.102
spuesta: supnewdmn.com. -> 192.168.56.102
spuesta: tvrstrynyvwstrtve.con. -> 192.168.56.102
spuesta: rtvwerjyuver.con. -> 192.168.56.102
spuesta: google.com. -> 192.168.56.102
spuesta: wqerveybrstyhcerveantbe.com. -> 192 168.56.102
spuesta: google.com. -> 192.168.56 102
spuesta: time.windows.con. -> 192.168.56.102
spuesta: google.com. -> 192.168.56 102
spuesta: bing.com. -> 192.168.56.102
spuesta: yahoo.com. -> 192.168.56.102
spuesta: supnewdmn.com. -> 192.168 56.102
spuesta: tvrstrynyvwstrtve.con. -> 192.168.56.102
spuesta: rtvwerjyuver.com. -> 192.168.56.102
spuesta: wqerveybrstyhcerveantbe.com. -> 192 168.56.102
spuesta: google.com. -> 192.168.56 102
spuesta: bing.com. -> 192.168.56.102
spuesta: yahoo.com. -> 192.168.56.102
spuesta: google.com. -> 192.168.56 102
spuesta: bing.com. -> 192.168.56.102
spuesta: yahoo.com. -> 192.168.56.102
spuesta: supnewdmn.com. -> 192.168 56.102
spuesta: tvrstrynyvwstrtve.con. -> 192.168.56.102
spuesta: google.com. -> 192.168.56 102
spuesta: rtvwerjyuver.con. -> 192.168.56.102
spuesta: bing.com. -> 192.168.56.102
spuesta: yahoo.com. -> 192.168.56.102
spuesta: wqerveybrstyhcerveantbe.com. -> 192 168.56.102
spuesta: google.com. -> 192.168.56 102
spuesta: bing.com. -> 192.168.56.102
spuesta: yahoo.com. -> 192.168.56.102
spuesta: google.com. -> 192.168.56 102
spuesta: bing.com. -> 192.168.56.102
spuesta: supnewdmn.com. -> 192.168 56.102
spuesta: yahoo.com. -> 192.168.56.102
spuesta: tvrstrynyvwstrtve.con. -> 192.168.56.102
spuesta: rtvwerjyuver.con. -> 192.168.56.102
spuesta: wqerveybrstyhcerveantbe.com. -> 192 168.56.102
```

Figure 4 FakeDNS in action with Command & Control.



```
C:\>volatility-2.3.1.standalone.exe -f Infected-Dump.dmp --profile=WinXPSP2x86 psscan
Volatility Foundation Volatility Framework 2.3.1
Offset(P)  Name                PID   PPID PDB        Time created                   Time exited
---------- ---------------- ------ ------ ---------- ------------------------------ ----------
0x0104cbb8 wscntfy.exe        1356   1008 0x0b52d000 2015-10-11 13:49:37 UTC+0000
0x01069da0 IEXPLORE.EXE       1676   1656 0x09f08000 2015-10-11 13:49:29 UTC+0000
0x0106dd78 IEXPLORE.EXE       1684   1656 0x09da4000 2015-10-11 13:49:29 UTC+0000
0x0113b020 wuauclt.exe         684   1008 0x0c9bc000 2015-10-11 13:50:37 UTC+0000
0x01144d60 cmd.exe            1756   1424 0x026fa000 2015-10-11 13:53:08 UTC+0000
0x011f7020 System                4      0 0x00039000
0x01d5f020 procexp.exe        1420   1424 0x01a6b000 2015-10-11 13:52:41 UTC+0000
0x03a21968 wmiprvse.exe        380    844 0x020e7000 2015-10-11 13:51:29 UTC+0000
0x04b0a648 svchost.exe         924    680 0x06ec9000 2015-10-11 13:49:23 UTC+0000
0x04c1ba70 svchost.exe        1100    680 0x073b2000 2015-10-11 13:49:23 UTC+0000
0x04fbaca8 smss.exe            356      4 0x054ad000 2015-10-11 13:49:18 UTC+0000
0x05632ad8 csrss.exe           612    356 0x0602e000 2015-10-11 13:49:21 UTC+0000
0x0570cb28 winlogon.exe        636    356 0x06173000 2015-10-11 13:49:22 UTC+0000
0x063de630 lsass.exe           692    636 0x064d2000 2015-10-11 13:49:22 UTC+0000
0x063deda0 services.exe        680    636 0x06487000 2015-10-11 13:49:22 UTC+0000
0x068f0da0 svchost.exe         844    680 0x06a0a000 2015-10-11 13:49:22 UTC+0000
0x07085858 svchost.exe        1008    680 0x0704f000 2015-10-11 13:49:23 UTC+0000
0x070e2270 svchost.exe        1056    680 0x07124000 2015-10-11 13:49:23 UTC+0000
0x07eacb40 ProcessHacker.e     384   1424 0x0a2d7000 2015-10-11 13:51:48 UTC+0000
0x08ed8020 MagnetRAMCaptur    1308   1424 0x07e02000 2015-10-11 13:58:07 UTC+0000
0x090fb9f8 explorer.exe       1424   1376 0x09500000 2015-10-11 13:49:25 UTC+0000
0x096cd9e8 spoolsv.exe        1504    680 0x096bc000 2015-10-11 13:49:25 UTC+0000
0x0ad08780 alg.exe            1132    680 0x0b0fb000 2015-10-11 13:49:35 UTC+0000

C:\>
```

Figure 5 Volatility Plugin (PSSCAN).

Figure 4 depicts the fakeDNS in action to facilitate the malware operations with command and control privileges. Figure 5 on the other hand, depicts the results of a Volatility plugin called PSSCAN on the infected image that revealed the PIDs for iEXPLORER 1676 and 1684 with PPID 1656, WSCNTFY 1356 with a PPID 10008, which is SVCHOST.

The iEXPLORE.EXE is part of the Windows OS, for the Internet Explorer browser. Again, we herewith note that the browser was not active. However, the analysis shows the iEXPLORE.EXE running at the background with multiple iEXPLORE.EXE processes [28]. This was an indication of the possible presence of a malware; in this case the Trojan.Stabuniq. Typical symptoms of an infected system include slow computer, slow Internet connection, multiple browser crashes, re-directing pop-ups, etc. [29, 30].

6 Conclusion

Basically, in digital forensic analysis the best practice is to make an image (and hash it) before embarking of the analysis. The original copy is kept safe, whilst the duplicated "exact" copy is analyzed or worked on. This way in the event of any mis-analysis, another copy can be obtained.

In using the analytical tools, we endeavored to recover the remnants of the infected files or deleted files. It must be noted that, we began the examination by first copying the compromised disk, bit-by-bit so that bad sectors, unallocated spaces and deleted files could be examined. Since the compromised system under this experiment is a Windows OS, we then examined the image using Master File Table (MFT) attributes. These include the filename, time stamps (especially, the last modified, or accessed times), as well as the index entries for folders [18].

It was observed that some viruses don't work on the virtual environment, i.e. they recognize that possibly malware analysis will be carried out and so blocks the vmware. Some viruses upon launching appear and after a couple of seconds disappear.

We set off in this study to explore the extent of externalities, such as intangibility, complications and inconsistencies, impacting on cyber-crime investigations. We simulated an experimental cyber-crime in which a system had been adversely impacted with malicious codes. Carefully, best practices were adhered to ensure that the investigation and analysis did not complicate the delicate "intangible" evidence of imputing that a malware attack has taken place. We have also demonstrated that the perpetrator could hide or conceal his tracks with some techniques, often referred to as anti-forensics. In essence, any of these externalities could either hamper investigations or even render the entire investigations null and void, and the evidence inadmissible in court.

Obviously, more work ought to be demonstrated in showcasing other ways anti-forensics are used to hide and evade apprehension in many cyber-crime cases.

References

[1] E. O. Yeboah-Boateng, Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA), 1 ed., Copenhagen: Institut for Elektroniske Systemer, Aalborg University, 2013.

[2] B. Cashell, W. D. Jackson, M. Jickling and B. Webel, "The Economic Impact of Cyber Attacks," US Congressional Reserach Service, 2004.

[3] A. Karran, J. Haggerty, D. Lamb, M. Taylor and D. Llewellyn-Jones, "A Social Network Discovery Model for Digital Forensics Investigations," in *6th International Workshop on Digital Forensics & Incident Analysis (WDFIA 2011),* 2011.

[4] Forensic Handbook, "Forensic Handbook," 12 August 2012. [Online]. Available: www.forensichandbook.com/locards-exchange-priniciple/. [Accessed 7 October 2015].

[5] K. Zatyko and J. Bay, "The Digital Forensic Cyber Exchange Principle," *Digital Forensic Investigator (DFI),* 14 December 2011.

[6] E. O. Yeboah-Boateng and P. M. Amanor, "Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices," *Journal of Emerging Trends in Computing and Information Sciences,* vol. 5, no. 4, pp. 297–307, April 2014.

[7] FBI IC3, "2014 Internet Crime Report," Federal Bureau of Investigations, Internet Crime Complaint Cneter (IC3), 2015.

[8] S. Charney and K. Alexander, "Computer Crime," Computer Crime Research Center (CCRC), 2002.

[9] PITAC, "Cyber-Security: A Crisis of Prioritization," National Coordination Office for Information Technology Research & Development, 2005.

[10] MyCERT, "MyCERT Quarterly Incident Statistics Summary Report," 2014.

[11] L. Zeltser, "Malware Sample Sources for Researchers," 2013. [Online]. Available: www.zeltser.com/malware-sample-sources/. [Accessed 24 September 2015].

[12] J. Moulin, “Digital Forensic: The Impact of Inconsistent Standards, Certifications and Accreditation,” 29015.

[13] SWGDE, Scientifc Working Group on Digital Forensics (SWGDE), 2014.

[14] E. O. Yeboah-Boateng and E. B. Boadi, “An Assessment of Corporate Security Policy Violations Using Live Forensics Analysis,” *International Journal of Cyber-Security & Digital Forensics (IJCSDF),* vol. 4, no. 11, pp. 1–10, 2013.

[15] Essays-Lab, “Buy Custom Computer Forensic Essay,” May 2015. [Online]. Available: www.essays-lab.com/free-samples/Research/computer-forensic.html. [Accessed 5 October 2015].

[16] A. Okunoye, “Increase in Computing Capacity and its Influence on Service Provision,” in 37th *Hawaii International Conference on System Sciences – 2004,* 2004.

[17] D. J. Price, “The Analog and Digtal World,” in *Handbook of Digital & Multimedia Forensic Evidence,* J. Barbara, Ed., Humana Press, 2008, pp. 1–10.

[18] S. Bui, M. Enyeart and J. Luong, “Issues in Computer Forensics,” 2003.

[19] INTERPOL, “INTERPOL and Trend Micro to Collaborate Against Cybercrime,” International Police, 24 June 2013. [Online]. Available: www.interpol.int/News-and-media/News/2013/PR076. [Accessed 7 October 2015].

[20] D. Shoemaker and W. A. Conklin, Cybersecurity: The Essential Body of Knowledge, Cengage Learning, Thomson Course Technology, 2011.

[21] L. Milkovic, “Defeating Windows Memory Forensics (29c3),” INFIGO, 2012.

[22] J. Stuttgen and M. Cohen, “Anti-Forensic Resilient Memory Acquisition,” *Digital Investigation,* vol. 10, pp. 105–115, 2013.

[23] B. Nelson, A. Phillips, F. Enfinger and C. Steuart, Guide to Computer Forensics and Investigations, Cengage Learning, Thomson Course Technology, 2004.

[24] A. Marrington, G. Mohay, A. Clark and H. Morarji, “Dealing with Temporal Inconsitency in Automated Computer Forensic Profiling,” Information Security Institute, Queensland University of Technology, 2009.

[25] E. D. Lucia, “Stabuniq in Depth,” 24 December 2012. [Online]. Available: www.contagiodump.blogspot.com/2012/12/dec/dec-2012-trojanst abuniq-samples.html. [Accessed 2 October 2015].

[26] C. Robertson, “Indicators of Compromise in Memory Forensics,” SANS Institute InfoSec Reading Room, 2013.

[27] M. Russinovich, “Process Monitor v3.2.,” TechNet, 26 May 2015. [Online]. Available: www.technet.microsoft.com/en-us/library/bb896645.aspx. [Accessed 11 October 2015].

[28] M. Sirorski and A. Honig, Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software, No Starch Press, 2012.

[29] Microsoft, “Malware Removal Guides: How to Remove Malware from Your Windows PC,” Microsoft Corporation, 2014. [Online]. Available: www.malwareremovalguides.info/iexplorer-exe-is-running-in-background/. [Accessed 2 October 2015].

[30] Y.-M. Wang, R. Roussev, C. Verbowski, A. Johnson and D. Ladd, “AskStrider: What has Changed in My Machine Lately?,” Microsoft Research, Microsoft Corporation, 2004.

[31] E. Casey, Handbook of Computer Crime Investigations: Forensic Tools and Technology, Academic Press, 2003.

[32] S. Chandra and R. K. Yadav, “Network Monitoring and Forensics,” *International Journal of Computer Science and Mobile Computing,* vol. 2, no. 8, pp. 181–185, 2013.

[33] L. Volonino and I. Redpath, e-Discovery for Dummies, Wiley Publishing, Inc., 2010.

Biographies

E. O. Yeboah-Boateng is a senior lecturer and the Head (acting Dean), Faculty of Informatics, at the Ghana Technology University College (GTUC), in Accra. Ezer is an ICT Specialist and a Telecoms Engineer, an executive with over 25 years of corporate experience and about 9 years in academia. He has over 10 peer-reviewed international journal papers to his credit, and well cited in Google Scholar. His research focuses on cyber-security vulnerabilities, digital forensics investigations (DFI), cyber-crime and crimeware, cloud computing, Big data and fuzzy systems.

E. Akwa-Bonsu is a Cyber Security Expert and Researcher. Elvis is the Head of Intelligence at Detectware, a private cyber-security firm in Accra, Ghana. With 18 years of corporate experience, Elvis focuses on offensive, destructive, and defensive technology that affect and protect enterprises. He frequently speaks on the subject of security standards, penetration testing/auditing, digital investigations, attack techniques, wireless security, covert channel communications, network security monitoring, Packet Analysis, Malware Analysis, steganography, incident response, malware analysis, Honeypots, vulnerability analysis, virtualization, cloud computing security, business continuity and security awareness.