

Computer Forensics Investigation - A Case Study

M.Sc. Computer Science (Specialization: Cyber Security)

by

A Rajesh , Dhruvi Ranjan Mohanty, Kamala Kannan .P,
Mahija.M.S, Naveen Kumar S, Nihala M N, Santhosh P,
Thanigai Vel.R

Enrollment no.: MSCS21R002, MSCS21R004,
MSCS21R006, MSCS21R007, MSCS21R008, MSCS21R009,
MSCS21R010, MSCS21R012

Under the guidance of

Dr.P.Thiyagarajan
Associate Professor
HOD of Dept. of Computer Science (Cyber Security)



DEPARTMENT OF COMPUTER SCIENCE
RAJIV GANDHI NATIONAL INSTITUTE OF YOUTH DEVELOPMENT,
SRIPERUMBUDUR - 602105

COPYRIGHT ©RGNIYD , SRIPERUMBUDUR
ALL RIGHTS RESERVED



Department of Computer Science
Rajiv Gandhi National Institute of
Youth Development
Sriperumbudur, Tamil Nadu
India - 602105

CERTIFICATE

This is to certify that I have examined the project entitled “Computer Forensics Investigation – A Case Study”, submitted by **A. Rajesh, Dhruti Ranjan Mohanty, Kamala Kannan .P, Mahija.M.S, Naveen Kumar S, Nihala M N, Santhosh P, Thanigai Vel.R** (Roll Number: *MSCS21R002, MSCS21R004, MSCS21R006, MSCS21R007, MSCS21R008, MSCS21R009, MSCS21R010, MSCS21R012*), the post-graduate students of **Department of Computer Science** in partial fulfillment for the award of degree of **Master of Computer Science** with specialization of **Cyber-Security**. I hereby accord my approval of it as a study carried out and presented in a manner required for its acceptance in fulfillment for **CSNS202 – Cyber and Digital Forensics** course for which it has been submitted. The project has fulfilled all the requirements as per the regulations of the institute as well as course instructor and has reached the standard needed for submission.

Place: Sriperumbudur

Date: 24/09/2022

Supervisor

Dr.P.Thiyagarajan

Department of Computer Science

Cyber Security

RGNIYD, Sriperumbudur

ACKNOWLEDGEMENT

We would like to express our sincere and deep gratitude to our supervisor and guide **Dr.P.Thiyagarajan**, Associate Professor, HOD of Computer Science (Cyber Security), for his kind and constant support during our post-graduation study. It has been an absolute privilege to work with Dr.P.Thiyagarajan for our project. His valuable advice, critical criticism and active supervision encouraged us to sharpen our research methodology and was instrumental in shaping our professional outlook.

ABSTRACT

The core goals of computer forensics are fairly straightforward: the preservation, identification, extraction, documentation, and interpretation of computer data. There are several policies and procedures that need to be out-lined and defined with regard to computer forensics are analysed in this paper. Data must be able to be retrieved and analysed without it is damaged. The authenticity of the data is also ensured. The widespread usage of computer forensics has resulted from the convergence of two factors: the increasing dependence of law enforcement on computing and the ubiquity of computers that followed from the microcomputer revolution. There is a plethora of hardware and software tools available to assist with the interpretation of forensic data. The Access Data Forensic Toolkit can be used by both law enforcement and the private sector to run complete forensic examinations of a computer.

Keywords: *Computer forensics, Malware analysis, Forensic case study, Digital evidence*

Computer Forensics Investigation - A Case Study

Author: Dept. of Cyber Security students (2021-23)

1 Introduction

Computer forensics is the implementation of the scientific method to digital media to reconstruct the factual information for judicial review. Another term for computer forensics is the collection and analysis of data from various computer resources including computer systems, computer networks, communication lines, and appropriate storage media for trial. The existence of computer science of forensics is much needed nowadays especially in the future because the number of computer based crimes can not be proven in real terms. To counteract those computer-related crimes, Computer Forensics plays a very important role. "Computer Forensics involves obtaining and analysing digital information for use as evidence in civil, criminal or administrative cases. A computer forensic investigation is an investigation where it checks the devices whether it is compromised by unauthorized access or not. Computer forensics investigators work as a team to investigate the case and conduct the forensic analysis by using different methodologies, software and tools. Computer forensic investigator must be aware of various laws and regulations and policies related to cyber crimes in their country. Computer forensic investigation divided into two categories. One is Public investigation which is conducted by government agencies. Another one is Private investigation which is conducted by private computer forensic team. This case study will cover only private investigation, since an incident happened at a new start-up SME. This case study includes computer forensic investigation model, data collections, acquisitions, forensics tools, malware analysis, legal characteristics of computer forensics. It also provides necessary recommendations, countermeasures and policies to ensure the SME will be placed in a secure network environment.

2 Case Study

A new start-up SME (small-medium enterprise) based in India with an E-government model has recently begun to notice anomalies in its accounting and product records. It has undertaken an initial check of system log files, and there are a number of suspicious entries and IP addresses with a large amount of data being sent outside the company firewall. They have also recently received a number of customer complaints saying that there is often a strange message displayed during order processing, and they are often re-directed to

a payment page that does not look legitimate. The company makes use of a general purpose e-Business package (OSCommerce) and has a small team of six IT support professionals, but they do not feel that they have the expertise to carry out a full scale malware/forensic investigation. As there is increased competition in the hi-tech domain, the company is anxious to ensure that their systems are not being compromised, and they have employed a digital forensic investigator to determine whether any malicious activity has taken place, and to ensure that there is no malware within their systems. Your task is to investigate the team's suspicions and to suggest to the team how they may be able to disinfect any machines affected with malware, and to ensure that no other machines in their premises or across the network have been infected. The team also wants you to carry out a digital forensics investigation to see whether you can trace the cause of the problems, and if necessary, to prepare a case against the perpetrators. The company uses Windows Server NT for its servers. Patches are applied by the IT support team on a monthly basis, but the team has noticed that a number of machines do not seem to have been patched.

3 Relevant Findings

According to the case study we can observe some valuable data are available which is very crucial for this case. Such as -

- Company is using Windows Server NT for its server.
- Patches are not applied in some machines.
- Number of suspicious entries and IP addresses with large amount of data being sent outside the company firewall.
- Customer complaints that some strange message displaying during order processing.
- The site is redirecting to a payment page that is not legitimate

4 What to do in this case?

- Follow the Digital forensic investigation process.
- What methodology should applied and Why.
- Collect digital evidence and what methods should taken for that.
- Malware investigation.
- Select forensic tools for evidence collection and malware analysis.
- Prepare a report for case.
- Countermeasures.

5 Computer Forensic Investigation Model

In 2001, the first Digital Forensics Research Workshop (DFRWS) proposed a general purpose digital forensics investigation process. It comprises of six(6) phases. Identification, Preservation, Collection, Examination, Analysis, Presentation. This is done in order to present evidence in a court of law when required.

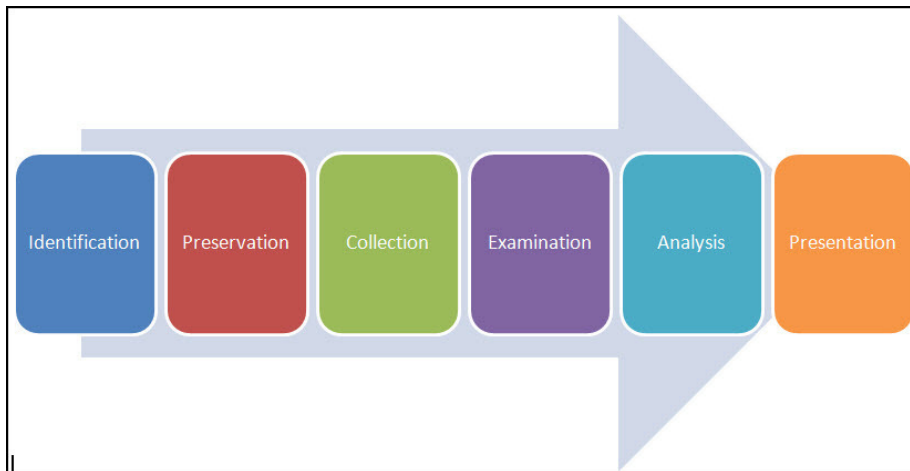


Figure 1: DFRWS model of investigation

6 Legal challenges of investigation

Legal challenges before we start our forensic investigation are as follows:

- We have to take the written permission from organisation to conduct the forensic investigation.
- Check whether law enforcement assistance is needed, and if needed they may be available for assistance during the investigation, or else we have to submit the investigation report to them at the end of the investigation.
- We have to take advice of legal professional if any potential things happen during investigation.
- Ensure the clients' confidential and privacy issues

7 Identification

This is the first step of computer forensic model. In this process identify the purpose of investigation, resources required during investigation, limit of inves-

tigation and objective of investigation need to prepare in order to conduct the investigation efficiently. This is considered as a proactive measure of investigation.

- Identify the incident with respect to 5W (why, when, where, what, who)
- Identify the impact of the investigation on the SME, such as loss of revenue and loss of confidential information.
- Identify the impact if the network system was compromised.
- Identify the security error in their network.
- Identify the forensic tools which can be used in this investigation.
- Identify the network device involve in the case such as router, switches, hub, computers, firewall, servers etc..
- Identify the external storage devices such as pen drive, flash drive, external hard disk, CD, DVD and memory cards.
- Gathering all shreds of relevant documents and information from the case.

8 Preservation

There are 3 methods to preserve a digital evidence.

8.1 Drive Imaging

Before forensic investigators begin analyzing evidence from a source, they need to create an image of the evidence. Imaging a drive is a forensic process in which an investigator will create a bit-by-bit duplicate of the drive. When analyzing an image forensic experts need to keep in mind the following points:

- Even wiped drives can keep important and recoverable data to identify.
- Forensic experts can recover all deleted files using forensic tools.
- Never perform forensic analysis on the original media. Always Operate on the duplicate or copy image.

”Write Blocker” is a tool designed to prevent any write access to the hard disk, thus permitting read-only access to the data storage devices without compromising the integrity of the data.

8.2 Hash Values

When a forensic investigator creates an image of the evidence for analysis, the process generates cryptographic hash values like MD5, SHA1, etc. Hash Values are critical as:

- If the hash values for the original and copy are different, then the copy is not identical to the original.
- It can't be predicted, no two files can have the same hash value, and if the file changes, the hash value changes.

If the hash values of the image and the original evidence do not match, it may raise concerns in court that the evidence has been tampered with.

8.3 Chain of Custody

Chain of custody is a legal term, which refers to the chronological sequence in which the items of evidence are to be handled for the successful investigation of a case. It must be proved in the court that the evidence is handled through the correct chain of custody, and only then will the evidence be acceptable in the court of law. The chain of custody tells who has collected the evidence from the crime scene (or anywhere else), who has handled it, who analysed and transferred the evidence, and where the evidence was stored. All the physical or electronic evidence is included here. Some common types of evidence includes:

- Blood

- DNA samples (fingerprints, footprints)
- Photographs
- Videos
- E-mails, text messages
- Internet history

9 Collection

Collecting evidence is the crucial knowledge that may help incident responders in understanding the process of attack and tracing the attacker. There are two different types of data that can be collected in a computer forensics investigation. They are volatile data and non-volatile data. Volatile data is the data on a live system that is lost after a computer is powered down, e.g. Random Access Memory (RAM), registry and caches. The 'live' examination of the device is required in order to include volatile data within any digital forensic investigation. Nonvolatile data is a type of digital information that is persistently stored within a file system on some form of electronic medium that is preserved in a specific state when power is removed, e.g. documents in HD. Since volatile data is short-lived, a computer forensic investigator must know the best way to capture it. Evidence can be collected locally or remotely.

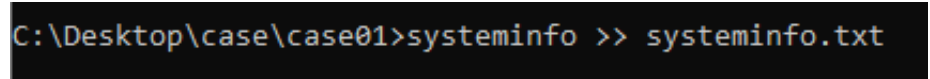
9.1 Volatile Data collection

In this paper, we will run a couple of CLI commands that help a forensic investigator to gather volatile data from the system as much as possible. The commands which we use in this post are not the whole list of commands, but these are most commonly used once.

As per forensic investigator, create a folder on the desktop name "case" and inside create another subfolder named as "case01" and then use an empty document to save the output which you will extract.

9.1.1 System Information

It is a system profiler including information related to the operating system, hardware, and software. We can collect this volatile data with the help of commands. All we need is to type this command.



```
C:\Desktop\case\case01>systeminfo >> systeminfo.txt
```

Figure 2: system information command

Now, go to the file location to see the results of this command. Where it will show all the system information about our system software and hardware.

```
systeminfo - Notepad
File Edit Format View Help
Host Name: DHRUTI
OS Name: Microsoft Windows 10 Pro
OS Version: 10.0.19044 N/A Build 19044
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: HP
Registered Organization: 00330-80000-00000-AA309
Product ID: 19-12-2021, 09:04:30
Original Install Date: 22-09-2022, 21:24:19
System Boot Time: Hewlett-Packard
System Manufacturer: HP Pavilion 15 Notebook PC
System Model: x64-based PC
System Type: 1 Processor(s) Installed.
Processor(s): [01]: Intel64 Family 6 Model 69 Stepping 1 GenuineIntel ~2601 Mhz
BIOS Version: Insyde F.09, 04-08-2014
Windows Directory: C:\Windows
System Directory: C:\Windows\system32
Boot Device: \Device\HarddiskVolume2
System Locale: en-us;English (United States)
Input Locale: 00004009
Time Zone: (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi
Total Physical Memory: 16,314 MB
Available Physical Memory: 13,078 MB
Virtual Memory: Max Size: 18,746 MB
Virtual Memory: Available: 15,328 MB
Virtual Memory: In Use: 3,418 MB
Page File Location(s): C:\pagefile.sys
Domain: WORKGROUP
Logon Server: \\DHRUTI
Hotfix(s): 18 Hotfix(s) Installed.
[01]: KB5017022
[02]: KB4562830
[03]: KB4570334
[04]: KB4577266
[05]: KB4577586
[06]: KB4580325
[07]: KB4586864
[08]: KB5003791
[09]: KB5012170
[10]: KB5017308
[11]: KB5007273
```

Figure 3: system information

9.1.2 Currently Available Network Connections

Network connectivity describes the extensive process of connecting various parts of a network. With the help of routers, switches, and gateways. We can check all the currently available network connections through the command line.

```
C:\Desktop\case\case01>netstat -nao >> networkinfo.txt
```

Figure 4: Network connection command

Now, open that text file to see all active connections in the system right now. It will also provide us with some extra details like state, PID, address, protocol.

networkinfo - Notepad

File Edit Format View Help

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	732
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	6160
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING	2220
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	1016
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	932
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1416
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	1384
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	3332
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	1008
TCP	127.0.0.1:7335	0.0.0.0:0	LISTENING	9932
TCP	127.0.0.1:18412	0.0.0.0:0	LISTENING	9932
TCP	127.0.0.1:44950	0.0.0.0:0	LISTENING	9932
TCP	127.0.0.1:44960	0.0.0.0:0	LISTENING	9932
TCP	170.0.14.56:139	0.0.0.0:0	LISTENING	4
TCP	170.0.14.56:49678	20.198.118.190:443	ESTABLISHED	4028
TCP	170.0.14.56:49753	157.90.91.75:443	ESTABLISHED	8348
TCP	170.0.14.56:49795	34.120.52.64:443	ESTABLISHED	8348
TCP	170.0.14.56:49802	74.125.24.188:5228	ESTABLISHED	8348
TCP	170.0.14.56:49838	34.193.113.164:443	ESTABLISHED	8348
TCP	170.0.14.56:49839	54.147.21.139:443	ESTABLISHED	8348
TCP	170.0.14.56:49841	18.205.229.213:443	ESTABLISHED	8348
TCP	170.0.14.56:49842	54.85.240.191:443	ESTABLISHED	8348
TCP	170.0.14.56:50011	20.44.229.112:443	TIME_WAIT	0
TCP	170.0.14.56:50012	199.232.20.159:443	ESTABLISHED	8348
TCP	192.168.56.1:139	0.0.0.0:0	LISTENING	4
TCP	[::]:135	[::]:0	LISTENING	732
TCP	[::]:445	[::]:0	LISTENING	4
TCP	[::]:5357	[::]:0	LISTENING	4
TCP	[::]:7680	[::]:0	LISTENING	2220
TCP	[::]:49664	[::]:0	LISTENING	1016
TCP	[::]:49665	[::]:0	LISTENING	932
TCP	[::]:49666	[::]:0	LISTENING	1416
TCP	[::]:49667	[::]:0	LISTENING	1384
TCP	[::]:49668	[::]:0	LISTENING	3332
TCP	[::]:49669	[::]:0	LISTENING	1008
UDP	0.0.0.0:500	*:*		3768
UDP	0.0.0.0:3702	*:*		7044

Figure 5: Network connection

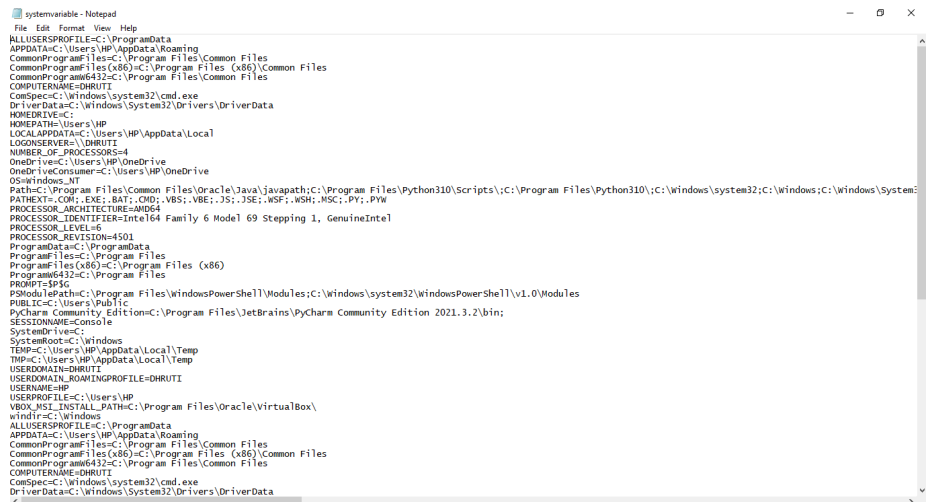
9.1.3 System Variables

A System variable is a dynamic named value that can affect the way running processes will behave on the computer. They are part of the system in which processes are running. For Example, a running process can query the value of the TEMP environment variable to discover a suitable location to store temporary files. We can check all system variable set in a system with a single command.

```
C:\Desktop\case\case01>set >> systemvariable.txt
```

Figure 6: System Variables command

Now, open the text file to see set system variables in the system.

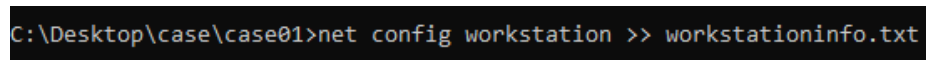


```
File Edit Format View Help
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\HP\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgram6432=C:\Program Files\Common Files
COMPUTERNAME=DHRUTI
ComSpec=C:\Windows\system32\cmd.exe
DriverData=C:\Windows\System32\Drivers\DriverData
HOMEDRIVE=C:
HOMEPATH=Users\HP
LOCALAPPDATA=C:\Users\HP\AppData\Local
LOGONSERVER=\\DHRUTI
NUMBER_OF_PROCESSORS=4
OneDrive=C:\Users\HP\OneDrive
OS=Windows_NT
Path=C:\Program Files\Oracle\Java\javapath;C:\Program Files\Python310\Scripts\;C:\Program Files\Python310\;C:\Windows\system32\;C:\Windows;C:\Windows\System32\
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC;.PY;.PMW
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 69 Stepping 1, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=4501
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
ProgramFiles(x86)=C:\Program Files (x86)
Program6432=C:\Program Files
PROXIES=
PSModulePath=C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules
PUBLIC=C:\Users\Public
PyCharm Community Edition=C:\Program Files\JetBrains\PyCharm Community Edition 2021.3.2\bin;
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\HP\AppData\Local\Temp
TMP=C:\Users\HP\AppData\Local\Temp
USERDOMAIN=DHRUTI
USERDOMAIN_ROAMINGPROFILE=DHRUTI
USERNAME=HP
USERPROFILE=C:\Users\HP
VBOX__INST__INSTALL_PATH=C:\Program Files\Oracle\VirtualBox\
windir=C:\Windows
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\HP\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgram6432=C:\Program Files\Common Files
COMPUTERNAME=DHRUTI
ComSpec=C:\Windows\system32\cmd.exe
DriverData=C:\Windows\System32\Drivers\DriverData
```

Figure 7: System Variables

9.1.4 Workstation Information

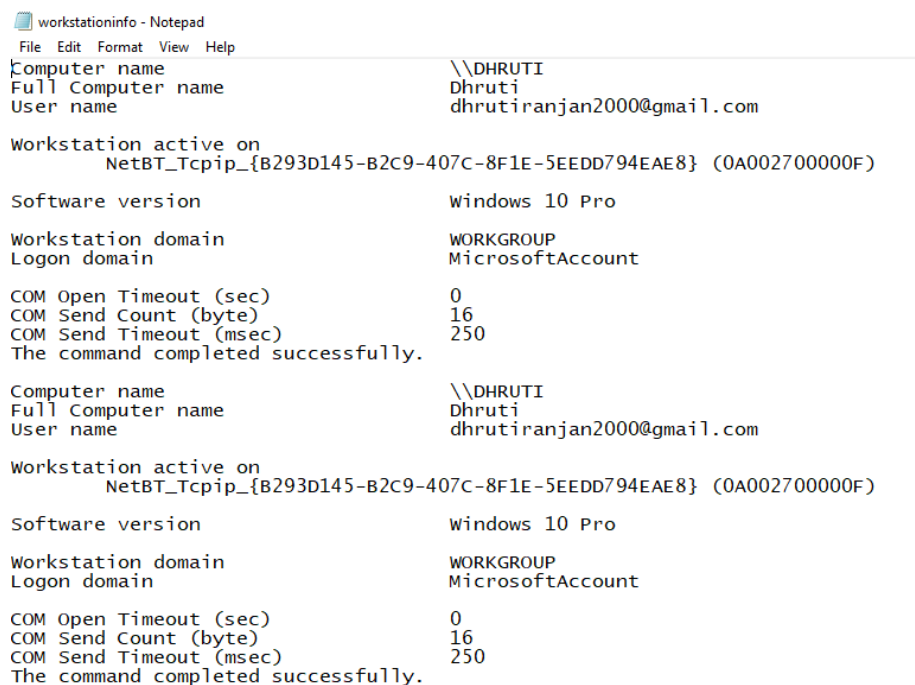
A workstation is known as a special computer designed for technical or scientific applications intended primarily to be used by one person at a time. They are commonly connected to a LAN and run multi-user operating systems. Follow these commands to get our workstation details.



```
C:\Desktop\case\case01>net config workstation >> workstationinfo.txt
```

Figure 8: Workstation details command

Now, open the text file to see the investigation results.



```

workstationinfo - Notepad
File Edit Format View Help
Computer name                \\DHRUTI
Full Computer name           Dhruti
User name                     dhrutiranjana2000@gmail.com

Workstation active on
NetBT_Tcpip_{B293D145-B2C9-407C-8F1E-5EEDD794EAE8} (0A002700000F)

Software version              Windows 10 Pro

Workstation domain            WORKGROUP
Logon domain                   MicrosoftAccount

COM Open Timeout (sec)        0
COM Send Count (byte)         16
COM Send Timeout (msec)       250
The command completed successfully.

Computer name                \\DHRUTI
Full Computer name           Dhruti
User name                     dhrutiranjana2000@gmail.com

Workstation active on
NetBT_Tcpip_{B293D145-B2C9-407C-8F1E-5EEDD794EAE8} (0A002700000F)

Software version              Windows 10 Pro

Workstation domain            WORKGROUP
Logon domain                   MicrosoftAccount

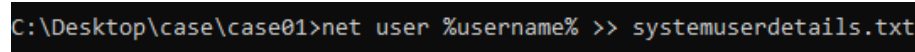
COM Open Timeout (sec)        0
COM Send Count (byte)         16
COM Send Timeout (msec)       250
The command completed successfully.

```

Figure 9: Workstation details

9.1.5 System User Details

A user is a person who is utilizing a computer or network service. Users of computer systems and software products generally lack the technical expertise required to fully understand how they work. To get that user details to follow this command.



```

C:\Desktop\case\case01>net user %username% >> systemuserdetails.txt

```

Figure 10: System User Details command

Now, open a text file to see the investigation report.

```
systemuserdetails - Notepad
File Edit Format View Help
User name HP
Full Name Hello Dhruti
Comment
User's comment
Country/region code 000 (System Default)
Account active Yes
Account expires Never

Password last set 27-12-2021 07:05:04
Password expires Never
Password changeable 27-12-2021 07:05:04
Password required No
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon 27-12-2021 07:05:01

Logon hours allowed All

Local Group Memberships *Administrators
Global Group memberships *None
The command completed successfully.

User name HP
Full Name Hello Dhruti
Comment
User's comment
Country/region code 000 (System Default)
Account active Yes
Account expires Never

Password last set 27-12-2021 07:05:04
Password expires Never
Password changeable 27-12-2021 07:05:04
Password required No
User may change password Yes
```

Figure 11: System User Details

9.1.6 DNS Configuration

DNS is the internet system for converting alphabetic names into the numeric IP address. When a web address is typed into the browser, DNS servers return the IP address of the web server associated with that name. To know the system DNS configuration follow this command.

```
C:\Desktop\case\case01>ipconfig /displaydns >> dnsconfiguration.txt
```

Figure 12: DNS Configuration command

Now open the text file to see the text report.

```
dnsconfiguration - Notepad
File Edit Format View Help
Windows IP Configuration

array616.prod.do.dsp.mp.microsoft.com
-----
Record Name . . . . . : array616.prod.do.dsp.mp.microsoft.com
Record Type . . . . . : 1
Time To Live . . . . . : 438
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 20.54.25.4

ctldl.windowsupdate.com
-----
Record Name . . . . . : ctldl.windowsupdate.com
Record Type . . . . . : 1
Time To Live . . . . . : 1129
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 117.18.232.240

array601.prod.do.dsp.mp.microsoft.com
-----
Record Name . . . . . : array601.prod.do.dsp.mp.microsoft.com
Record Type . . . . . : 1
Time To Live . . . . . : 2366
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 20.191.46.109

update.virtualbox.org
-----
Record Name . . . . . : update.virtualbox.org
Record Type . . . . . : 1
Time To Live . . . . . : 5900
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 137.254.60.34
```

Figure 13: DNS Configuration

We can also use various Windows-based tools to capture the volatile data like:

- ipconfig – Collecting subject system details.
- netusers and qusers – Identifying logged-in users
- netfile – Identifying the services and drivers
- doskey/history – Collecting command history
- FTK Imager - Data preview and imaging tool

There is a lot of evidence when the machine is in the volatile state, and so it must be ensured that the affected computers are not shut down in order to collect such evidences.

9.2 Non-volatile Data Collection

The first step in non-volatile data collection is to copy the content of entire target system. A "forensic image" (forensic copy) is a bit-by-bit, sector-by-sector direct copy of a physical storage device, including all files, folders and located or unallocated, free and slack space. Forensic images include not only all the files visible to the operating system but also deleted files and pieces of files left in the slack and free space. Imaging helps to preserve the original data as evidence without any changes in data which occurs during the forensic investigation. A forensic investigator uses a write blocker to connect to the target system and copy the entire contents of the target drive to another storage device by using any forensic tools. The only difference between forensic imaging and hard drive cloning is that forensic imaging can't be accessed without forensic tools, but hard drive cloning can easily be accessed with a mount drive. Forensic imaging will hash with MD5 or SHA-2 to ensure the integrity of digital evidence. We have to collect all the digital evidences like firewall logs, antivirus logs, domain controller logs, web server logs, windows event logs, database logs, IDS logs, and application logs. Target system Hard drives, External Storage devices and Windows NT Server Hard drive must be acquired for the digital forensic investigation in this case.

Autopsy and The Sleuth Kit (TSK) are likely the most well-known forensics tool kits in existence. The Sleuth Kit is a command-line tool that performs forensic analysis of forensic images of hard drives and smartphones. Autopsy is a GUI-based system that uses The Sleuth Kit behind the scenes.

10 Examination

Once we have gathered all the available evidences, we need to conduct the examination by the help of various computer forensic investigation tools. We also examine the file system, Windows registry, Network and Database forensic examination, as follows:

10.1 Files system examination

A file system is a storage structure on a computer that organizes data. It allows users to access data quickly and easily. Windows offers three file systems: NTFS, FAT32 and FAT16. For example, disks must be formatted with an appropriate file system before backup.

- **The FAT file system** - FAT stands for File Allocation Table and was developed by Microsoft in 1977. The family of FAT file systems includes FAT12, FAT16, FAT32 and exFAT. FAT is still a common format for USB sticks and external hard drives today.
- **The NTFS file system** - NTFS stands for New Technology File System and was designed in 1993 by Microsoft for Windows NT. The following

versions of NTFS exist so far: NTFS 1.0, NTFS 1.1, NTFS 2, NTFS 3.0 and NTFS 3.1., whereby a downward compatibility of the versions is given.

A key advantage of the NTFS file system is the file size. But also in terms of data security NTFS has more to offer. Users and user groups can be given permissions to read, write or execute drives, folders or files. When using FAT, data can be lost after a crash, while NTFS has better backup mechanisms by logging file changes. Other advantages of NTFS are file encryption, data compression, fast defragmentation and setting security attributes. MFT is the Master File Table which contains information about all files and disks, and it is also the first file in NTFS. When a file is deleted in Windows NT, the file will be renamed by OS and moved it to Recycle bin with a unique identity. OS stores information about the original path and original file name in info2 file. But if a file is deleted from the Recycle bin, then associated clusters are marked as available for new data. As an investigator, we must be aware of the Windows file systems FAT and NTFS in depth.

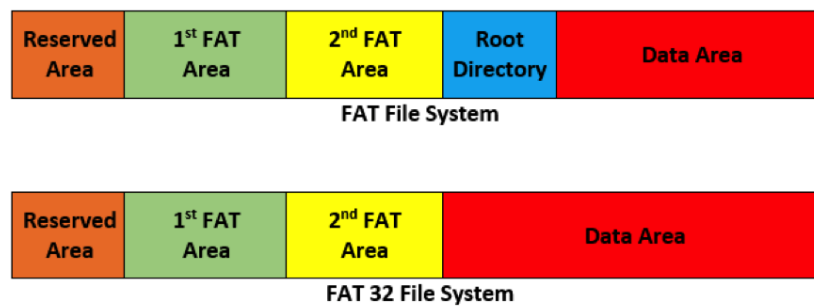


Figure 14: FAT and FAT32 file system

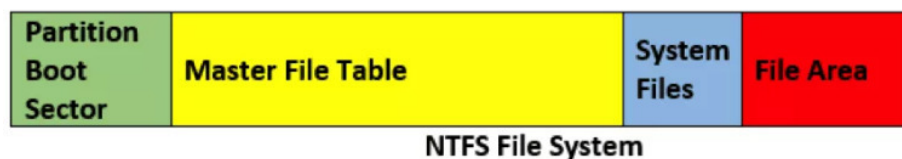


Figure 15: NTFS file system

10.2 Windows Registry Examination

Windows registry is an order of databases in a computer used by Microsoft in Windows 98, Windows CE, Windows NT and Windows 2000. The Registry or Windows Registry is the database that stores the low-level settings of the operating system and its applications that support registries. It contains commands for the installed applications. Whenever you install a registry-supported Windows application on your system, it automatically adds a new registry entry and stores all the essential information required for running the new application in it. For example, where the files are located, which other applications can use the new program, and more. The common structure of the windows registry is divided into "Hives" which are:

- **HKEY_CLASSES_ROOT** - It describes the file type, its extension, and Object Linking and Embedding (OLE) information.
- **HKEY_CURRENT_USER** - Contains the information and the settings of the currently logged-in user.
- **HKEY_LOCAL_MACHINE** - This is where most registries are present and are being edited. It contains device-specific information. Every user who can log in to the computer can access HKLM.
- **HKEY_USERS** - It contains data of all the user's accounts of the system.
- **HKEY_CURRENT_CONFIG** - This root key contains the details of the configuration of the hardware currently attached to the device.

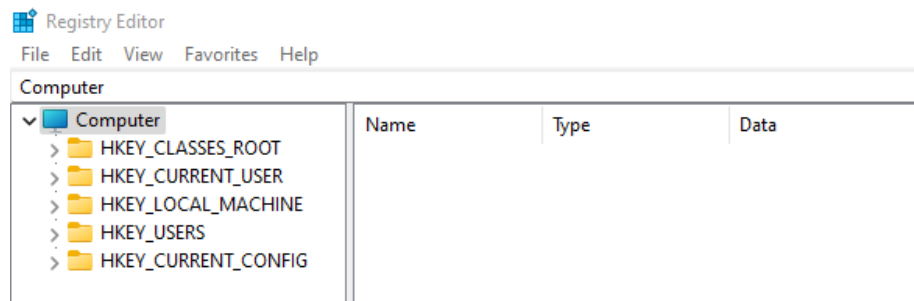


Figure 16: Windows Registry

10.2.1 Auto-start Location

Autostart Location is a location in the registry where the applications are set to be launched without a user initiation. With this functionality a malware can persistently run when the machine is turned on without a direct user interaction because it was already programmed to autostart itself or when a user runs some specific commands or processes.

A forensics investigator can examine the autostart location to determine if the attack has been performed by a user, a malware or by an attacker on the organization.

10.2.2 HKEY_CURRENT_USER

Hive which is created from HKEY_USERSID hive. User information is mapped to the HKEY_CURRENT_USER. The NTUSER.DAT holds information about registry specification settings of a user action and activities. Software maintains an executed list of commands run by a user. From this the investigator will be able to analyze from the registry if it was user activity, a malware action or an attack that is affecting the organization.

UserAssist consists of two keys that commonly look like globally unique identifiers that keep encrypted records of each object, application, etc. a user has accessed on the system. If an investigator has accessed the encrypted record, which is no longer definitive, it might indicate some action the user did to trigger the Malware through an application or any activity he might have done.

10.2.3 HKEY_LOCAL_MACHINE

All devices connected to the system are being maintained in a computer registry under the following key. Using the hives of the mounted drive, an investigator will have a clue when he/she analyzes the device ID content maintained in the registry to know which device was being mounted. When navigating to key values, they contain subkeys which look like globally unique identifiers, which when opened, an investigator can navigate to the ActiveSettings which reveals each wireless SSID in the form of a binary data type. When right-clicked to modify, it reveals the SSIDs in plain written format.

Though IP address and other network information can be found under HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\TCPIP\Interfaces\GUID, an investigator can use this information to tie a user in the organization to a particular time frame if the person's IP address appears to be discovered under the above Window registry.

Windows registry can also be a vital source of proof in a forensic investigation. By analyzing it we get user activity and all necessary programs a user had executed, devices used on the server or any of the organization's computers, and also revealed the IP address of users.

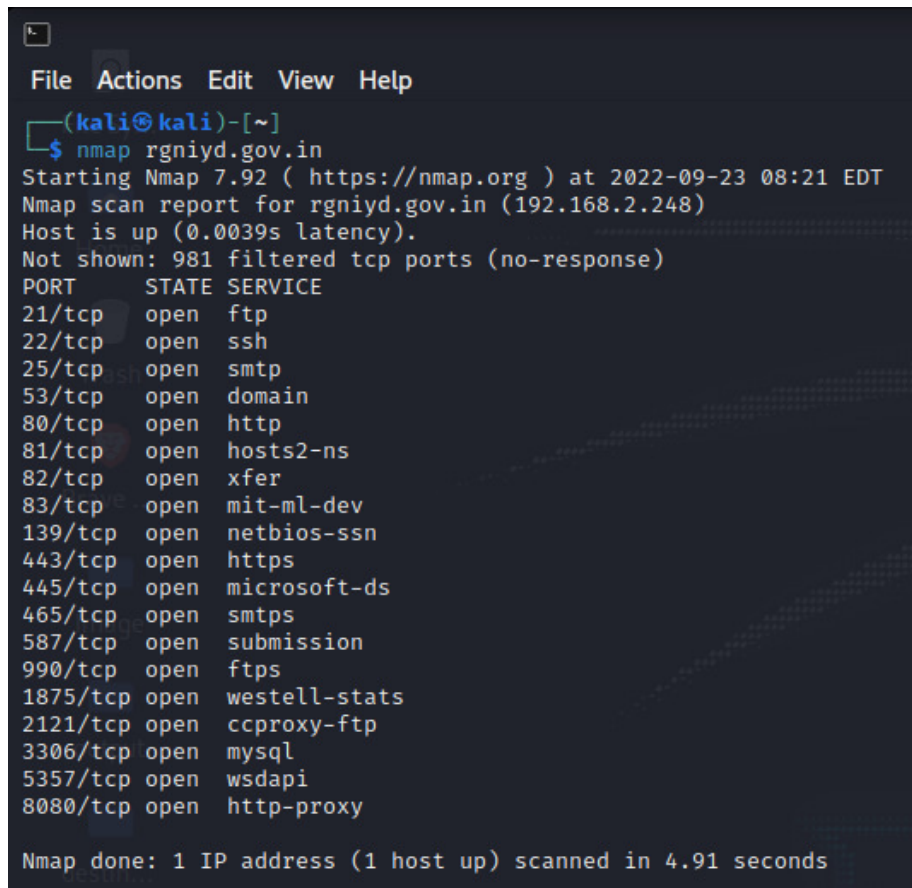
10.3 Network Forensic Examination

As, the types of the attacks increased in network security, the importance of network forensic is also increased. Network forensic is the sub category of digital forensics, that deals with the examination of network and its traffics going across a network for the purposes of information gathering, legal evidence, or intrusion detection. In other words, we can say that network forensics is the recording, analysing and capturing of network packets that are going across a

network to determine the exact source of security attacks. For network forensics, there are lots of open-source tools available like Wireshark, Snort, Nmap and Network Miner etc.

For this case we are using some powerful network forensics tool that are: Wireshark, Network Miner and N-map.

- **N-map** - N-map is an open source kali linux tool. Nmap allows you to scan your network and discover not only everything connected to it, but also a wide variety of information about what's connected, what services each host is operating, and so on. It allows a large number of scanning techniques, such as UDP, TCP connect, TCP SYN (half-open), and FTP.



```
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap rgniyd.gov.in
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-23 08:21 EDT
Nmap scan report for rgniyd.gov.in (192.168.2.248)
Host is up (0.0039s latency).
Not shown: 981 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
81/tcp    open  hosts2-ns
82/tcp    open  xfer
83/tcp    open  mit-ml-dev
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
465/tcp   open  smtps
587/tcp   open  submission
990/tcp   open  ftps
1875/tcp  open  westell-stats
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5357/tcp  open  wsddapi
8080/tcp  open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 4.91 seconds
```

Figure 17: Using N-map to see open ports

- **Wireshark** - Wireshark is an open source kali linux tool. Network administrators use it to troubleshoot network problems. Network security engineers use it to examine security problems. QA engineers use it to verify network applications. Wireshark is a great network protocol analyser that captures packets from a network connection in real time. With the help of Wireshark tool, we can filter the packets that will accomplish the main purpose i.e. to capture the packets selectively from the network and display and find the packets as our interest.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	192.168.2.248	DNS	72	Standard query 0xaaa0 A rgnid.gov.in
2	0.000019269	192.168.2.248	10.0.2.15	DNS	73	Standard query response 0xaaa0 AAAA rgnid.gov.in
3	0.000041640	192.168.2.248	10.0.2.15	DNS	89	Standard query response 0xd907 A rgnid.gov.in A 192.168.2.248
4	0.000099805	192.168.2.248	10.0.2.15	DNS	128	Standard query response 0xaaa0 AAAA rgnid.gov.in SOA ns2.nic.in
5	0.00021108	10.0.2.15	192.168.2.248	TCP	74	34312 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2454331244 TSecr=0 WS=128
6	0.00050626	10.0.2.15	192.168.2.248	TCP	74	42074 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2454331244 TSecr=0 WS=128
7	0.00064240	192.168.2.248	10.0.2.15	TCP	60	443 → 42074 [SYN, ACK] Seq=0 Ack=1 Win=65533 Len=0 MSS=1460
8	0.00058291	10.0.2.15	192.168.2.248	TCP	54	42074 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
9	0.00080574	10.0.2.15	192.168.2.248	TCP	54	42074 → 443 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
10	0.00045353	192.168.2.248	10.0.2.15	TCP	60	80 → 34312 [SYN, ACK] Seq=0 Ack=1 Win=65533 Len=0 MSS=1460
11	0.00050192	10.0.2.15	192.168.2.248	TCP	54	34312 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
12	0.00058980	10.0.2.15	192.168.2.248	TCP	54	34312 → 80 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
13	0.00000000	10.0.2.15	192.168.2.248	DNS	96	Standard query 0x0074 PTR 248.2.168.192.in-addr.arpa PTR rgnid.gov.in
14	0.001549418	192.168.2.248	10.0.2.15	DNS	113	Standard query response 0x0074 PTR 248.2.168.192.in-addr.arpa PTR rgnid.gov.in

Figure 18: Capturing packets using Wireshark

So, with the help of these two tools we can identify how the intruder penetrate in the existing security system and also what damages has been done by intruder.

10.4 Database Forensic Examination

Database forensics is a subfield of digital forensic science concerned with the forensic examination of databases and their metadata. A database is an organized collection of structured information, or data, typically stored electronically in a computer system. It is the use of electronic data stored in the database to reconstruct the clues, detect crimes, and accomplish case cracking. Database forensics examines who gets database access and what actions are taken. Large-scale data security breaches are a significant issue, and criminal investigators look for pertinent information. Database forensic experts are like detectives that investigate digital crimes. They hunt down cyberstalkers and cyberbullies by identifying malevolent hackers, identity thieves, and online fraudsters.

Database forensics investigator need to follow some following step while processing database forensic:

- Investigating computer systems and other digital storage devices for evidence.
- Investigating with the use of forensic tools for disks and databases as well as file readers and network forensic software

- Using software to examine email, computer registries, and files as well as mobile devices
- Recovering vital documents and images that have been destroyed or encrypted.
- Writing and speaking about discoveries.
- Providing digital evidence to corporate authorities, law enforcement, and the courts
- Detecting and remediating security breaches.

In the case study it is mentioned that a large amount of data is being sent out of the database. So we need to investigate the database using the database forensic tools. Database Forensic Investigation (DBFI) involves the identification, collection, preservation, reconstruction, analysis, and reporting of database incidents. To access the database of system investigator needs to get authorization from database server, then investigator start first process of DBFI. The investigator find any identity that store in database like log, registry etc. Investigator will check the audit logs used for last few months. The investigator will check the IP address whether its been changed or not because if its changed it can be access by remote controlled system, it leads to alter, steal or delete the database. By the help of DDL (Data Definition Language) command in SQL investigator can create the database or its objects (like table, index, function, views, store procedure, and triggers). DML (Data Manipulation Language) command is used to managing the data inside the database for identifying pre and post data are delete in a row or column in database by an attacker. Investigator can able to recover them, and it also helps us to prove or disprove that a data security breach has occurred within the database or not. CAINE (Computer Aided Investigative Environment) tools is used for check database forensic analysis. The DB browser for SQLite is a free, open-source tool for end users and developers who wants to use a familiar spreadsheet-like interface to manage database files without having to learn complicated SQL commands.

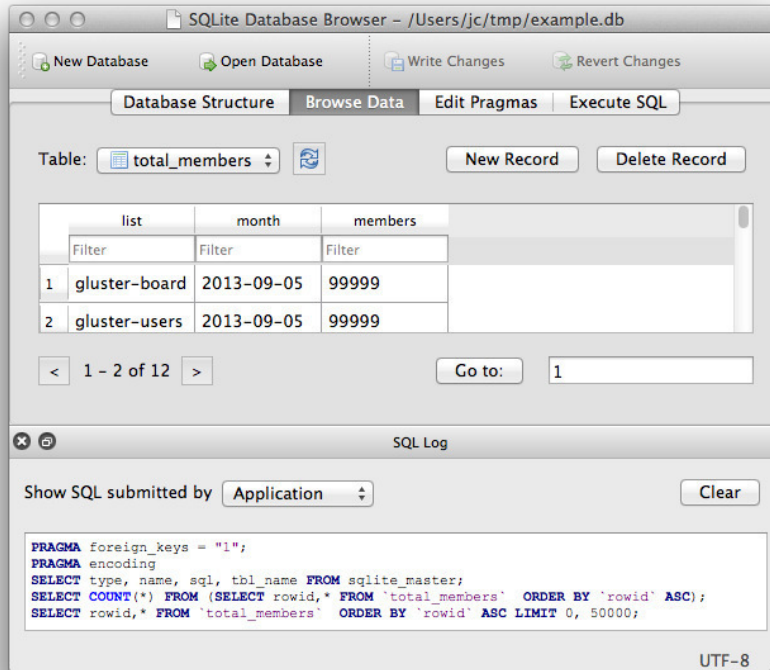


Figure 19: SQLite Database Browser

11 Analysis

Initially we have to analyze the collected evidences and examined that. We will look into the data to see whether any hidden files or unusual files are presented or not. Then if there is any unusual process running and if there are any ports and sockets opened unusually. We will also look if any application requests occurred unusually. Then we will check the account, whether any unusual account is presented or not. We will also find the patching level system, whether it is been updated or not. By the outcome of those analyses, we will come to know whether any malicious activities are presented or not.

By the outcome of those analyses, we will come to know whether any malicious activities are presented or not. In this case, there are malicious activities present in their network system. In order to find the malicious code capabilities and its aim, we have to do the malware executable analysis.

11.1 Malware Analysis

Malware analysis is the process of understanding the behavior and purpose of a suspicious file or URL. The output of the analysis aids in the detection and mitigation of the potential threat. The malware analysis can be divided into two parts, one is Static analysis and another one is Dynamic analysis.

11.1.1 Static analysis

Static analysis examines a malware file without actually running the program. This is the safest way to analyze malware, as executing the code could infect your system. In its most basic form, static analysis gleans information from malware without even viewing the code. Metadata such as file name, type, and size can yield clues about the nature of the malware. MD5 checksums or hashes can be compared with a database to determine if the malware has been previously recognized. And scanning with antivirus software can reveal what malware you're dealing with.

Advanced static analysis—also known as code analysis—dissects the binary file to study each component, still without executing it. One method is to reverse engineer the code using a dis assembler. Machine code is translated into assembly code, which is readable and understandable. By looking at the assembly instructions, an analyst can tell what the program is meant to do. A file's headers, functions, and strings can provide important details. Unfortunately, modern hackers are adept at evading this technique. By embedding certain syntax errors into their code, they can misdirect dis assemblers and ensure the malicious code still runs. Because static malware analysis can be more easily foiled, dynamic malware analysis is also necessary.

11.1.2 Dynamic analysis

Dynamic analysis executes suspected malicious code in a safe environment called a Sandbox. Or it is the running of malware sample for observing their behaviour in a system, before it infects their system or escape into the enterprise network. For the examination of malware, the system should be setup in a closed, isolated virtual environment, then only we can able to study thoroughly without any risk. There are different tools are available for doing dynamic analysis, such as Wireshark, Netcat, Process explorer, Regshot etc..

Therefore, by using this both analysis most of the answers which is required for investigations are able to find.

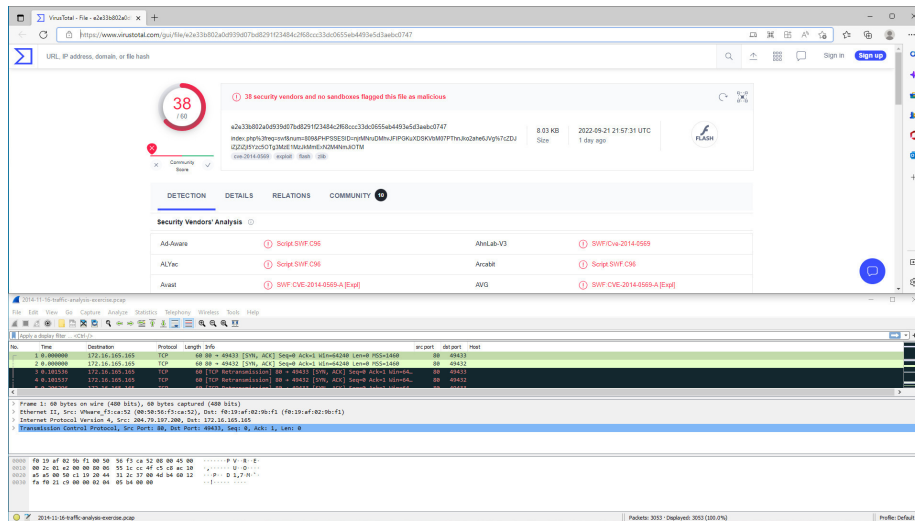


Figure 20: Malware analysis using Wireshark

12 Findings

After our investigation, we summarize our findings as follows:

- The forensic analysis identified that the systems had been compromised.
- OS patches were not installed in some systems.
- Malware was detected in SME systems.
- By seeing the functionality and aim of malware led us conclude that it is ‘spamming’ malware.
- Determined the attackers had access to the client’s systems using the malware by supplying in appropriate website link for payment gateway.

13 Remedial actions

By seeing the case, it is possible to take two important steps:

- **Train employees to identify and react to threats** - Cyber awareness training provides a basic understanding of cyber security best practice. Great training teaches employees to how to - identify and respond to the incident, practice safe internet habits and familiarize themselves with their organization’s cyber security related policies and abide by them.
- **Maintain asset lists, patches and updates** - Cyber crime prevention involves keeping your company’s hardware, software and digital assets up

to date through proper IT security asset management. A very easy and common way for hackers to get through a company's defenses is to simply take advantage of security gaps that exist due to outdated or unpatched IT infrastructure and software.

There are some countermeasures to protect against malware:

- Password protection
- Antivirus software
- Firewalls (hardware or software)
- IDS (Intrusion Detection System)
- Routers and Switches
- VPN (Virtual Private Networks)
- Logging and Audit

In our case, the most useful are the following:

- Firewall
- Logging and Audit

Firewalls provide protection against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic. Firewalls can also prevent malicious software from accessing a computer or network via the internet. Firewalls can be configured to block data from certain locations (i.e. computer network addresses), applications, or ports while allowing relevant and necessary data through. It displays a notification that the requested page is infected. If the Web page does not contain malicious code, it immediately becomes available to the user.

Logging will help you to identify patterns of activity on your networks, which in turn provide indicators of compromise. In the event of incidents, logging data can help to more effectively identify the source and the extent of compromise. For example, who and when tried to log on to the system and how this attempt ended, who and what information resources were used, what and who modified information resources.

Audit protects the critical data resources of an organization. Keeps the organization compliant to various security certifications. Identifies security loopholes before the hackers. Keeps the organization updated with security measures.

13.1 Security Policies

By definition, security policy refers to clear, comprehensive, and well-defined plans, rules, and practices that regulate access to an organization's system and the information included in it. Good policy protects not only information and

systems, but also individual employees and the organization as a whole. It also serves as a prominent statement to the outside world about the organization's commitment to security.

Specific actions that increase the likelihood of your policies actually being realized in the work environment include:

- **Specifically assign an empowered and committed administrator to be accountable for security:** Someone must make security a day-to-day priority. This designated staff member must be authorized to both reward and reprimand employees, as necessary, at all levels of organizational hierarchy.
- **Institute staff training that is specifically tailored to meet the requirements of security policy and the needs of your staff:** Recognize that most computer users have never been trained to properly use technology and what little training they do have was probably aimed at overcoming their fears and teaching them how to turn on their machines. At most, they may have learned how to use a particular piece of software for a specific application. Thus, the majority of your staff have little understanding of security issues, and there is no reason to expect that to change unless the organization does its part to correct the situation. Reluctance on the part of the organization to adequately prepare staff for making security policy a part of the work environment makes the rest of the effort an exercise in the theoretical and theory won't protect a system from threats that are all too real.
- **Enforce security regulations equally at all levels of the organization:** Each individual in the system must understand that he or she is personally accountable for security. Bosses have to say "get with the system," mean it, and prove it by doing so themselves. If the rules don't apply to everyone, then they apply to no one. This is not simply an egalitarian moral if the system is not secure from top to bottom, then, by definition, it is not secure!
- **Communicate organizational needs and expectations to staff in both initial and ongoing ways:** Make a serious attempt at getting the word out to staff, but don't be overly serious in its presentation. Just like in any marketing campaign, creativity and consistency will be rewarded by audience responsiveness.

13.1.1 Organizational security policy

An organizational security policy is a set of rules or procedures that is imposed by an organization on its operations to protect its sensitive data. The organizational security policies that are required by the evaluated configuration are as follows:

- Only those users who have been authorized to access the information within the system can access the system

- The system must limit the access to viewing of, modification of, and destruction of the information in protected resources to those authorized users who have a “need to know” that particular information.
- The users of the system are held accountable for their actions within the system.

14 Reporting

Reporting is the last step of the investigation model where you have to document everything like from collecting evidence to findings. The main goal of Computer forensics is to perform a structured investigation on a computing device to find out what happened or who was responsible for what happened, while maintaining a proper documented chain of evidence in a formal report. As a computer forensic investigator you should have knowledge about various types of computer forensic report such as formal report, written report, verbal report and examination plan. A formal report contains the facts from the investigation findings. A written report is like a declaration or an affidavit which can be sworn to under oath so that it must be clear, precise and detailed. A verbal report is less structured and is a preliminary report that addresses the areas of investigation not covered yet. An examination plan is a structured document that helps the investigator to understand the questions to be expected when he/she is justifying the evidences. An examination plan also helps the legal authorities to understand the terms and functions which were used in computer forensic investigation. Syntax or template of a Computer Forensic Report is as follows:

- Executive Summary
- Objectives
- Computer evidence analyzed
- Relevant findings
- Supporting details
- Investigation leads
- Additional subsection

15 Conclusion

This report contains how to conduct the Computer Forensic Investigation and Malware Investigation in different methods and using various tools. This report also contains the computer forensic investigation model and security policy procedures which must be implemented in every organization to improve the security network architecture. This report contain six step forensic investigation

model, it has an important part called analysis where we analysed the data which we gathered by various methods. This report also has the recommendations to avoid the security flaws in future.

Digital forensic investigation is a challenging process, because every incident differs from other incidents. A computer forensic investigator must be competent enough in Technical and Legal to conduct the investigation. Since the evidence which is provided by a computer forensic investigator can be an important part the case, the investigation report must be precise and in detail.

16 Team-Work

The entire project work was divided equally and judiciously among all the eight(8) team members. Each members of the team worked on digital forensic investigation process.

- **A Rajesh** worked on the topic network examination using free and open source tool Zenmap which primarily focused on visuals network mappings. In addition he worked on static malware analysis.
- **Dhruti Ranjan Mohanty** worked on the topics volatile data collection, non-volatile data collection using forensic tool The sleuth kit (TSK) and file system examination. In addition with he worked on dynamic malware analysis and report writing.
- **Kamala Kannan P** worked on the topics windows registry examination using forensic tool windows registry and file system examination, in addition with he worked on static malware analysis.
- **Mahija M.S** worked on the topics network examination using wireshark which primarily focused on capturing network packets. In addition with she worked on dynamic malware analysis using existing malware detection website.
- **Naveen Kumar S** worked on the topics non-volatile data collection using forensic tool Autopsy which primarily focused on forensic images of computer hard drives. In addition with he worked on static malware analysis.
- **Nihala M N** worked on the topics file system examination using open source kali linux tool called The bulk extractor which is a computer forensics tool that scans a disk image, a file, or a directory of files and extracts useful information without parsing the file system or file system structures. Bulk extractor is distinguished from other forensic tools by its speed and thoroughness. In addition with she worked on static analysis and remedial actions.
- **Santhosh P** worked on the topics network analysis using Network Forensic Analysis Tool (NFAT) for Windows called Network miner which can be used as a passive network sniffer/packet capturing tool in order to detect

operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network.

- **Thanigai Vel.R** worked on the topics database and network examination using CAINE OS which is a professional open source forensic platform that integrates software tools as modules along with powerful scripts in a graphical interface environment. In addition with he worked on dynamic malware analysis and security policies.

17 Reference

- <https://www.techtarget.com/searchsecurity/definition/computer-forensics>
- <https://www.hackingarticles.in/forensic-investigation-extract-volatile-data-manually/>
- <https://www.ufsexplorer.com/articles/file-systems-basics/>
- <https://support.microsoft.com/en-us/windows/how-to-open-registry-editor-in-windows-10-deab38e6-91d6-e0aa-4b7c-8878d9e07b11>
- <https://ieeexplore.ieee.org/document/6557293>
- https://www.researchgate.net/publication/261074415_Tools_for_collecting_volatile_data_A_survey_study
- <https://www.geeksforgeeks.org/computer-forensic-report-format/>
- <https://www.wireshark.org/docs/>
- <https://nmap.org/docs.html>
- https://wiki.sleuthkit.org/index.php?title=Main_Page
- <https://www.caine-live.net/page11/page11.html>
- <https://www.sleuthkit.org/index.php>
- <https://networkminer.en.softonic.com/>
- <https://www.kali.org/docs/introduction/download-official-kali-linux-images/>
- <https://www.kali.org/docs/introduction/download-official-kali-linux-images/>
- <https://www.kali.org/tools/bulk-extractor/>
- <https://recuva.en.softonic.com/>