Digital Forensics Analysis for Network Related Data

Mr. Abhishek Doshi[1], Dr. Priyanka Sharma[2]

[1]*Student, School of Information Technology & Cyber Security, Raksha Shakti University, Gujarat, India*
[2]*Director, Research & Development, Raksha Shakti University, Gujarat, India*

---***---

Abstract: *With the increase in the field of digital crime and data theft; the law enforcement agencies and investigators needs to have efficient tools scripts & methodologies to collect the required evidences and reproduce the data in understandable form. Network plays a vital role in communication process amongst the digital devices; where the data packets and requests are transferred. The main goal of the research is to extract and analyse digital evidences for network artefacts like IP addresses (Version 4 & 6), event & network log files of system, open source and proprietary tools/software/scripts, to help the law enforcement agencies and investigators with their investigation process in efficient manner and extract desired data. Here various open source tools and software are used to analyse and extract various evidences; moreover EnScript has been modified and redesigned to fetch relevant data. The results conclude with network related data set obtained from various networks.*

Keywords: Digital forensics, EnCase, FTK, Networking, Investigation.

1. INTRODUCTION

The word forensics is derived from a combination of Latin words *forensic* "on the forum" & *Scientia* "knowledge". Forensic science is referred to the process of applying scientific standard methods & techniques to criminal and civil proceedings. A forensic scientist or investigator collects, preserves, and analyses evidences during an investigation. Over time, the technical aspects of forensic investigations have evolved into sub-fields relating to the special conditions of the evidence involved, like digital forensics, hardware analysis, etc. with computer forensics being the branch of forensic science encompassing the examination and investigation of data & information found in digital Network forensics is sub-domain of digital forensics associated with tracking and analysing of computer devices and network traffic for the purpose of data and information collection, required files or intrusion detection within a network. Till date, it was enough to look at individual systems as objects containing digital evidences and files. Computing was centred based where collecting a computer and several disks and peripherals would assure collection of all relevant digital evidence and data. Today, however, computing and communication has become network-centred and distributed as more people rely on email, clouds and other network based platforms. It is no longer adequate to think about computers as an isolated object as many of them are connected together using various network technologies and topologies.

1.1. CHAIN OF CUSTODY

The Chain of Custody is the process of validating the collection, storage, movement and protection of evidence. The investigator must document the characteristics of the evidence to distinguish comparable devices and to identify the evidence. For digital evidence a hash value (MD5 and SHA) should be taken, if hardware devices are there, then proper sealed packing in faradays bag should be done.

The location, date and time of the seizure of the evidence should be noted. Every minute detail and process from acquisition to final result as evidence; should be well noted and followed properly.

1.2. DIGITAL EVIDENCES

The following are the categorized devices and files analysed during the research to obtain artefacts and relevant network based data.

Table-I: Types of Evidences

Category	Digital Evidence
Live systems	C.P.U (Windows based), Live Network, Broadband Router.
Image files of Hard disks and Memory devices	Image file of a Hard-disk.
Log files	Log files of remote desktop connections, web servers.
Mobile Phones	Android based Cellular mobile phone.
Captured network data	Network packets and data.

2. ACQUISITION & ANALYSIS OF THE EVIDENCE AND DATA

The evidences may be acquired from the crime location or may be captured with various tools and processes as discussed below. The integrity and nature of the evidence collected should be maintained as mentioned in chain of custody; for that various hash calculations, preservation process during data/hardware transfer and transport should be strictly followed. The analysis of the acquired evidence and data plays a key role in the investigation process; as the case mainly depends on the produced on the basis of the analysis. Thus, the analysis process should be fast, efficient, easy-to-use and standard; which should comply with the international standards and parameters as set by the court of law. The tools and processes used to analyse should be able to provide optimum and valid results which can be produced conclusively. Following processes describes the types of evidences which are examined majorly during investigation to obtain the artefacts and data relevant to the case.

2.1. LIVE SYSTEMS

The basic systems and devices seized during a raid are the hardware components which are live and contain volatile data. Now, for a network forensic analyst; devices like manageable switches, router, broadband routers, CPU, Network Interface Cards, Hard Disks, Digital Video Recorders and other devices connected in network as hardware evidences are seized and examined to get evidence data using various tools and methods.

The following table describes the data that can be fetched from the listed hardware systems:

Table-II: Data obtained from live systems

Hardware Device	Data obtained
Manageable switches	Logs, Network Paths, Rules, Filters, VLANs, NAT tables etc.
Routers	IP addresses, MAC addresses, Routes, static/dynamic IP logs, connection status, ports assigned etc.
CPU	IP addresses, MAC addresses, Routes, static/dynamic IP logs, ports assigned etc.
Digital Video Recorders	Static IP addresses, MAC addresses, Ports etc.

Here, windows based system and broadband router as evidence are examined primarily to obtain the basic network artefacts:

2.1.1. WINDOWS BASED SYSTEM

Windows operating system based evidences can be easy to examine if the log files are accessible during primary investigation. Event viewer of windows based systems can help investigators a lot to examine the network connections, profiles, sessions, system logon-logoff, wireless and bluetooth connections and almost every event occuring in front and back end of the system by assigning specific code(numeric) of that event. The events can be used to find evidences of the connections and event occuring or occured in the system; which can also be helpfull for auditing or troubleshooting the network or device. These events can also be exported as logs and viewd later with tools.Event Viewer can be found at: *C: \ ProgramData \Microsoft \ Windows \ Start Menu \ Programs \ Administrative Tools.* Here are few images of those artefacts and logs which can be helpful in the investigation of a windows based system which can show Service Set Identifier names and connection time and details:

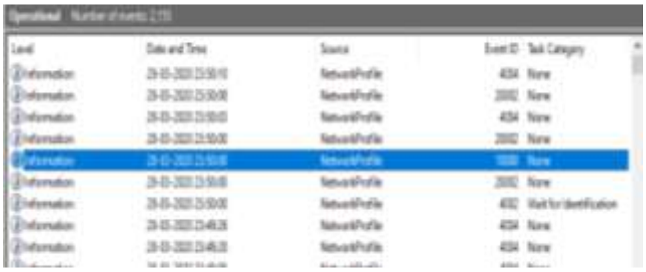


Fig 1: Log of Network Profile generated in the system

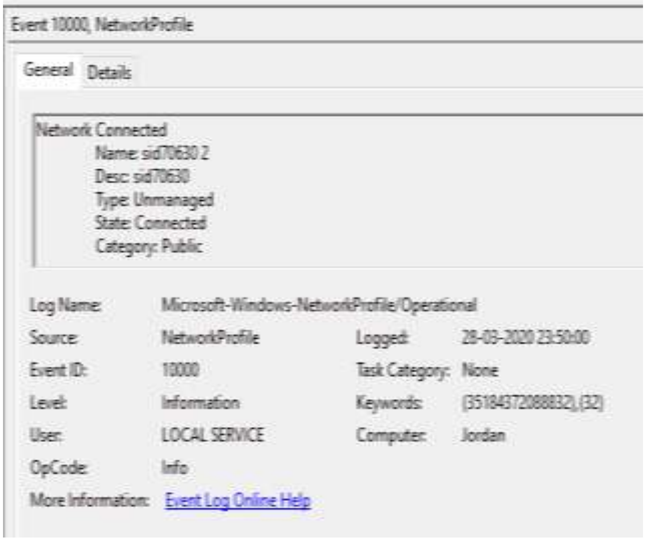


Fig 2: Network Profile generated in the system

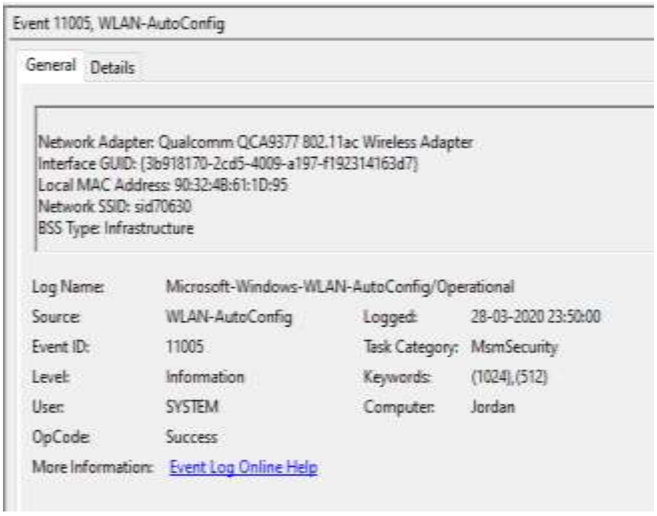


Fig 3: WLAN configuration event

2.1.2. COMMAND LINE UTILITY

ifconfig (interface configuration) windows based command is used to setup and analyse network interfaces. It can also be used at boot time to configure network as per requirement. It is majorly used for network debugging or listing out all the connected network active connections on the systems. Thus being a good command for primary investigation of local systems. Here an image is showed containing a sample demo output of Wi-Fi adapter and their physical and logical addresses.

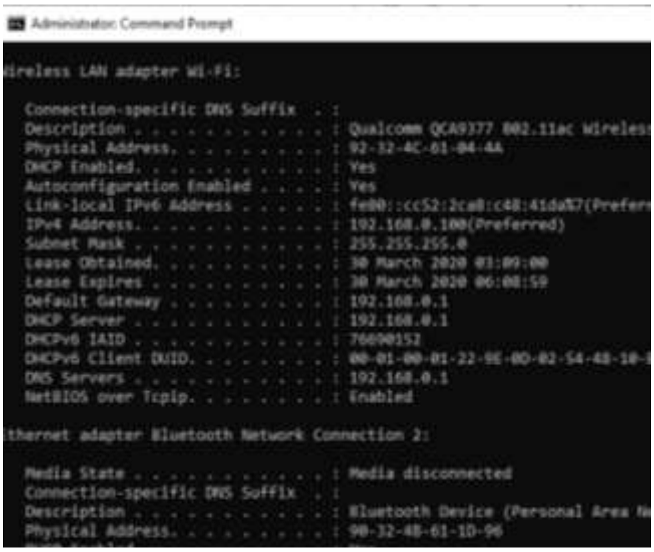


Fig 4: output of ifconfig /all command

Netstat (Network Statistics) is a command line based tool for displaying network connection on a particular system used to find live network associated interfaces, IP addresses, ports which are being utilized, routing tables etc. Here, a snapshot of the same is taken from an evidence which can detect if any backdoor is enabled leaking any data.

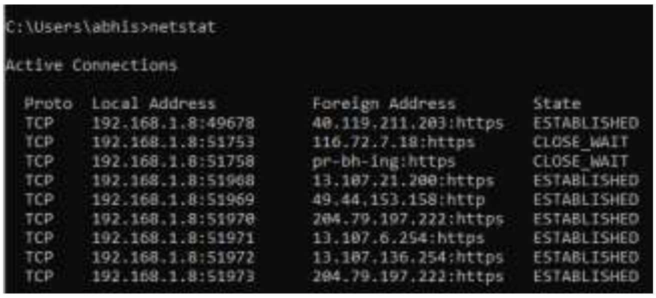


Fig 5: output of netstat command

2.1.3. ADVANCED IP SCANNER

Advanced IP Scanner is a free tool for windows system that scans your network connection over LAN, W-LAN, or Wi-Fi and listing down the computers and devices connected in the network. It work with Radmin; an administration software which works remotely, enhancing its results and capabilities. This software is war far easy capable and easy-to-use as a network scanner for all network domain people and agencies.

It has many features which makes it a great tool to use for network scanning other than forensics. If a system supports Wake-On-Lan; IP scanner can remotely shutdown computers and can wake them as per admin request. Lists can be made for your selected systems on your network. It can scan for open ports which helps the investigation team to find out the possible mode of intrusion or attack carried out on the network. A sample scan based on IP pool provided by the user is shown here.

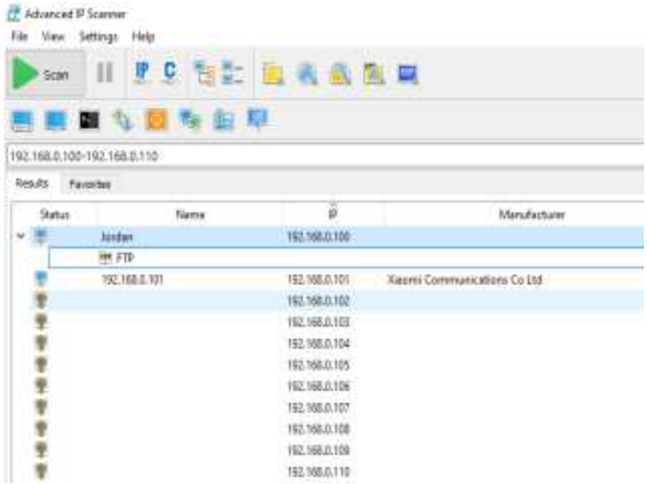


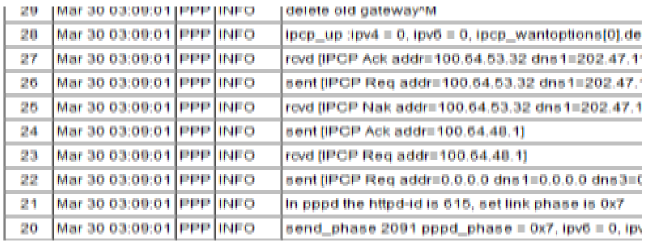
Fig 6: Live scan of the network using Advance IP Scanner

2.1.4. BROADBAND ROUTER

Most common and usefull evidence can be obtained from the network broadband router which acts as a gateway between WAN and LAN to access the world wide web or internet. Data such as WAN IP, ON/OFF time, DHCP connections, IP allotments, Errors, Forwarding ports and other such data can be found from the admin panel of the broadband routers. Here, DHCP allotment and PPP data information of IP address and DNS are obtained from a TP-Link Broadband router form the path** : *192.168.0.1/system tools/logs/* [**The path may change depending on router manucfacture]

Index	Time	Type	Level	Log Content
5	Mar 30 03:09:00	DHCP	INFO	DHCPS:Send ACK to 192.168.0.100
4	Mar 30 03:09:00	DHCP	INFO	DHCPS:Recv REQUEST from 92:32:4C:61:04:4A
3	Mar 30 03:09:00	DHCP	INFO	DHCPS:Send OFFER with ip 192.168.0.100
2	Mar 30 03:08:59	DHCP	INFO	DHCPS:Recv DISCOVER from 92:32:4C:61:04:4A
1	Mar 30 03:08:34	DHCP	NOTICE	DHCP server started

Fig 7: DHCP information obtained



29	Mar 30 03:09:01	PPP	INFO	delete old gateway^M
28	Mar 30 03:09:01	PPP	INFO	ipcp_up :ipv4 = 0, ipv6 = 0, ipcp_wantoptions[0].de
27	Mar 30 03:09:01	PPP	INFO	rcvd [IPCP Ack addr=100.64.53.32 dns1=202.47.1
26	Mar 30 03:09:01	PPP	INFO	sent [IPCP Req addr=100.64.53.32 dns1=202.47.
25	Mar 30 03:09:01	PPP	INFO	rcvd [IPCP Nak addr=100.64.53.32 dns1=202.47.1
24	Mar 30 03:09:01	PPP	INFO	sent [IPCP Ack addr=100.64.48.1]
23	Mar 30 03:09:01	PPP	INFO	rcvd [IPCP Req addr=100.64.48.1]
22	Mar 30 03:09:01	PPP	INFO	sent [IPCP Req addr=0.0.0.0 dns1=0.0.0.0 dns3=(
21	Mar 30 03:09:01	PPP	INFO	In pppd the httpd-id is 615, set link phase is 0x7
20	Mar 30 03:09:01	PPP	INFO	send_phase 2091 pppd_phase = 0x7, ipv6 = 0, ipv

Fig 8: PPP information obtained

Fig 9: Options of log type available to fetch and examine

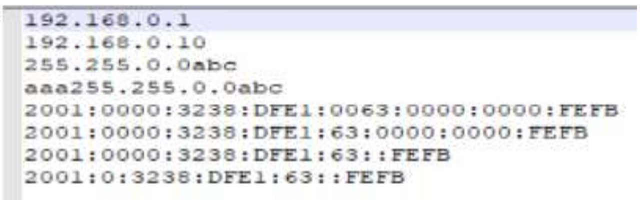
2.2. FORENSIC IMAGE FILES OF HARD DISK AND MEMORY DEVICES

Image files are bit-by-bit copy of the memory storage devices. These image files can be analysed for the artefacts extraction using various open source and proprietary softwares and scripts.

Here two such softwares are used namely EnCase (Version 6.19.7) and FTK (Version 6.4) licensed version. This search helps to find footprints and data related to the network.

2.2.1. ENCASE

EnCase is a forensic analyser tool used by law enforcement agencies and investigators. Encase contains various features and scripts for ease of search. EnScript; a script developed by EnCase is here developed and modified to search the evidence image of a physical drive containing the suspicious data. The scripts developed here are specifically finding IPv4 addresses (included in version 6), IPv6 addresses and MAC addresses stored within the image file acquired. The below IP addresses stored in a file which are the evidences to be found from the suspected device:



```
192.168.0.1
192.168.0.10
255.255.0.0abc
aaa255.255.0.0abc
2001:0000:3238:DFE1:0063:0000:0000:FEFB
2001:0000:3238:DFE1:63:0000:0000:FEFB
2001:0000:3238:DFE1:63::FEFB
2001:0:3238:DFE1:63::FEFB
```

Fig 10: Suspected file containing IP addresses to be found from evidence

The above file with IP is found using following method:

Fig 11: Evidence examination in EnCase

The EnScript snippet code used in EnCase to filter out and find the evidences:

```
include "GSI_Basic"
class MainClass
{
        LogRecordClass LogRecords; // will track the number of hits per specific IP address
        String StatusBarName;
        MainClass():
        LogRecords(),
        StatusBarName = "Searching - Find Valid IPs"
{
 bool InitSearch(SearchClass search)
{
        bool ret = false;
        KeywordClass keyword(null, StatusBarName + ": IP Address", KeywordClass::ANSI | KeywordClass::GREP, "##?#?\\.##?#?\\.##?#?\\.##?#?");
        if (search.AddKeyword(keyword))
{
        //make sure the keyword argument is NOT a list!
        ret = search.Create();
        if (!ret)
        SystemClass::Message(SystemClass::OK, "Error", "Fatal Error: SearchClass Creation Failure");
 }
 else
        SystemClass::Message(SystemClass::OK, "Error", "Fatal Error: Bad Keyword");
        return ret;
 }
```

Here the GREP section of EnScript are modified as per convenience to obtain results as required:

For IPv4	##?#?\\.##?#?\\.##?#?\\.##?#
For IPv6	##?#?#?#?:##?#?#?#?:##?#?#?#?:
For MAC	??-??-??-?? or ??:??:??:??

On searching the evidence using these scripts, the footprints of all IPv6 addresses are traced out which can be analysed in their associated file list.
The output can be obtained as follows for IPv6 addresses:

Fig 12: Desired Output in EnCase

Installation files, backup files, cache, cookies and bookmarks generated by the software and browsers in the system contains the footprints or traces of the IP addresses, network used, device information etc. which can be used as evidences to fetch remote connection logs or network used for a specific task which can be used as evidences by searching out through EnScripts.

2.2.2. FTK

FTK (Forensic ToolKit) by Access Data is commercial a forensics imager and analyser toolkit majorly used by law enforcement and investigators. It is majorly used to analyse evidence images and files to extract data and index them as per required for the case. Images, Files, Documents, Graphics, Bookmarks, cookies etc. based on extensions and file signature types are indexed and listed. Moreover, the file's integrity is maintained and hash calculation is also done. Here, in following images network artefacts can be found from the system files and FTK has a great feature which lists down all the network details, Wi-Fi details, MAC and gateway addresses connected to the system, which can be a great data as evidence during investigation.

First Connect Time	Last Connect Time	Network Name	Network Category	Gateway MAC Address
8/12/2017 12:18:33 AM	8/16/2017 1:01:09 AM	NET GEAR 123	Public	A4-2B-8C-C2-F5-20
12/22/2017 4:30:59 PM	1/12/2018 3:39:16 PM	TP-LINK_9CE6	Public	98-DE-D0-AB-9C-E6
8/11/2017 5:52:30 PM	1/30/2018 10:19:28 PM	Network	Public	30-B5-C2-2E-72-CE
9/13/2017 4:24:35 PM	9/13/2017 4:32:10 PM	JAYA	Public	00-17-7C-70-78-98
9/24/2017 5:08:02 AM	10/23/2017 1:20:08 PM	Sharma	Public	2C-30-33-2E-38-DA
12/7/2017 1:28:28 AM	1/20/2018 11:02:44 PM	Mafat	Public	B4-EF-FA-14-C2-C3
1/19/2018 1:31:10 AM	1/31/2018 1:57:34 AM	Administratorâ€™s iPhone	Public	2E-33-61-A6-0B-64
8/17/2017 10:50:05 PM	10/21/2017 4:00:27 PM	iPhone	Public	2E-33-61-F5-59-64
8/12/2017 12:01:33 AM	8/16/2017 1:01:04 AM	Network	Public	00-EB-D5-C6-E4-C0
9/29/2017 9:31:08 PM	12/28/2017 9:53:59 PM	Dev	Public	A0-AB-1B-D6-72-41
8/16/2017 4:41:13 PM	12/28/2017 9:56:13 PM	0000000000000	Public	1C-5F-2B-52-C4-0F
12/3/2017 2:28:08 AM	1/16/2018 1:17:06 AM	Administratorâ€™s iPhone	Public	2E-33-61-F5-59-64
8/12/2017 12:25:34 AM	8/12/2017 12:27:00 AM	Network	Public	98-DE-D0-4A-88-3E
8/11/2017 6:08:41 PM	8/16/2017 3:50:01 PM	Viratco	Public	1C-5F-2B-52-C4-0F
9/13/2017 6:42:33 PM	11/25/2017 1:30:13 AM	D-Link_DIR-615	Public	A0-AB-1B-D6-72-41

Fig 13: Network connections

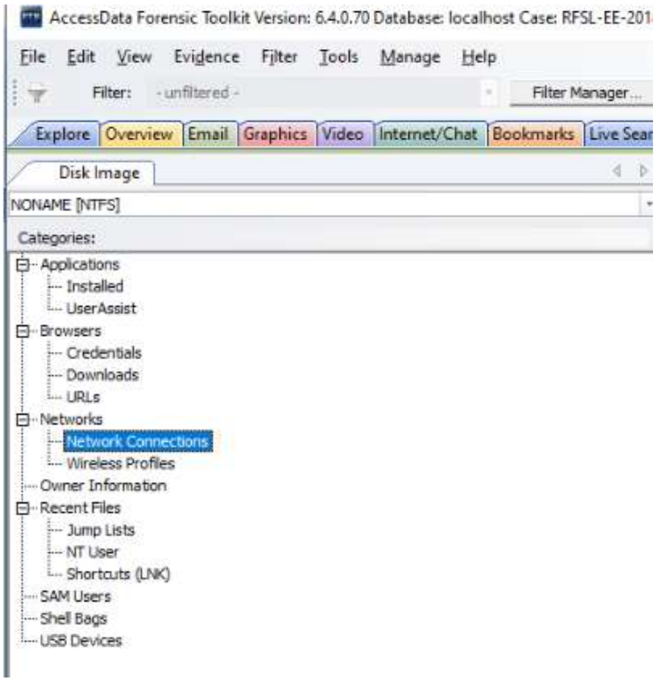


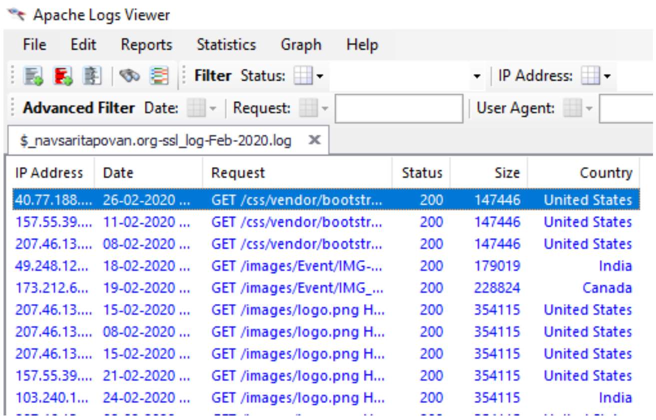
Fig 14: FTK categories

SSID	Wireless Authentication	Wireless Encryption	Profile Name
VirtualRouter.codeplex.com	WPA2PSK	AES	HOSTED_NETWORK_PROFILE
iPhone	WPA2PSK	AES	iPhone
Administratorâ€™s iPhone	WPA2PSK	AES	Administratorâ€™s iPhone
D-Link_DIR-615	WPA2PSK	AES	D-Link_DIR-615
Mafat	WPA2PSK	AES	Mafat
Dev	WPA2PSK	AES	Dev
0000000000000	WPA2PSK	AES	0000000000000
TP-LINK_9CE6	WPA2PSK	AES	TP-LINK_9CE6
ADYYUmVkbWkzUw	WPA2PSK	AES	ADYYUmVkbWkzUw
JAYA	WPAPSK	TKIP	JAYA
Ravi	WPA2PSK	AES	Ravi
Sharma	WPA2PSK	AES	Sharma
Orion Infotech	WPA2PSK	AES	Orion Infotech

Fig 15: Wireless connections

2.3. LOG FILES

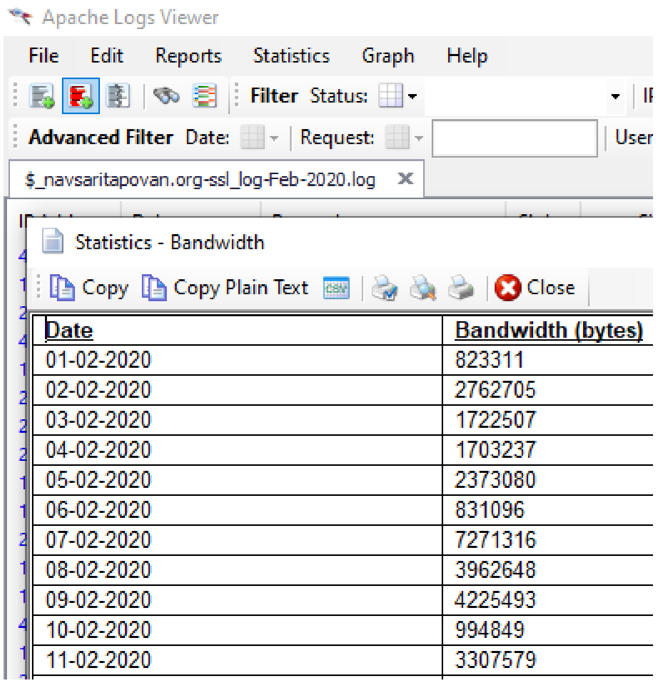
Log files are the registry or entries which are generated within the system or monitoring tool which records all events, errors, processes with proper timestamp and the users, IP or a unique identifier with it. These logs can be very much helpful and important for a digital crime evidence. A tool named Apache Log Viewer is used which helps to examine various logs from web servers, FTP servers, mail and other systems. Here the tool is used to examine a webserver log file, which helps in analysis of requests sent on webserver of webpage for accessing data. The log contains IP Address, Date, and Request for a Page with the method, country based on IP. Here the logs can be analysed for a DoS attack, webpage request, suspicious IP analysis and the timestamp of request where a crime regarding webserver was carried out.



IP Address	Date	Request	Status	Size	Country
40.77.188....	26-02-2020 ...	GET /css/vendor/bootstr...	200	147446	United States
157.55.39....	11-02-2020 ...	GET /css/vendor/bootstr...	200	147446	United States
207.46.13....	08-02-2020 ...	GET /css/vendor/bootstr...	200	147446	United States
49.248.12...	18-02-2020 ...	GET /images/Event/IMG-...	200	179019	India
173.212.6...	19-02-2020 ...	GET /images/Event/IMG_...	200	228824	Canada
207.46.13....	15-02-2020 ...	GET /images/logo.png H...	200	354115	United States
207.46.13....	08-02-2020 ...	GET /images/logo.png H...	200	354115	United States
207.46.13....	15-02-2020 ...	GET /images/logo.png H...	200	354115	United States
157.55.39....	21-02-2020 ...	GET /images/logo.png H...	200	354115	United States
103.240.1...	24-02-2020 ...	GET /images/logo.png H...	200	354115	India

Fig 16: Analysis log of webserver

Moreover, to examine and get evidences for DoS attack; bandwidth consumption statistics can be generated based on the requests on the website.



Date	Bandwidth (bytes)
01-02-2020	823311
02-02-2020	2762705
03-02-2020	1722507
04-02-2020	1703237
05-02-2020	2373080
06-02-2020	831096
07-02-2020	7271316
08-02-2020	3962648
09-02-2020	4225493
10-02-2020	994849
11-02-2020	3307579

Fig 17: Bandwidth analysis

2.4. MOBILE PHONES

The investigation for a digital crime does not limit till computer devices and logs; in this era mobile phones and cellular devices are also being used for crime; which can be examined for their artefacts and data. Mobile forensics is a whole different domain and research scope, but here only network artefacts are fetched from the device. Network artefacts here includes previous connected Wi-Fi, past Bluetooth connections, network based data or bookmarks, SIM based data. For the investigation, two commercial mobile forensic software namely XRY and Magnet AXIOM are used to find the artefacts from a cellular mobile phone model VIVO1812.

2.4.1 XRY & Magnet AXIOM

XRY & Magnet AXIOM are commercial software based tool specially designed for law enforcement agencies. They help to gain data and access of mobile phones involved in criminal investigation. These software helps to decode, Analyze, retrieve data such as files, media, graphics, system files and data, call logs, chats etc.

Here, a mobile device as evidence; on examination and analysis reveals Wi-Fi address, Wi-Fi name, Bluetooth address, logs etc. which can be used as an evidence to check whether the device trace as mac address is found on logs of the crime related devices.

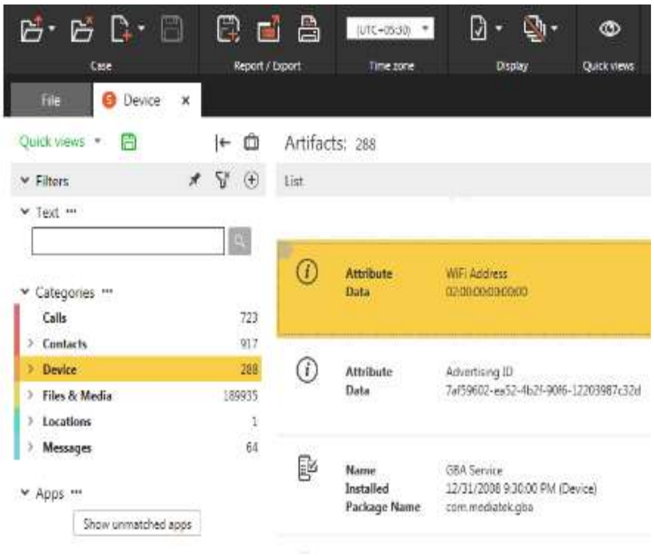
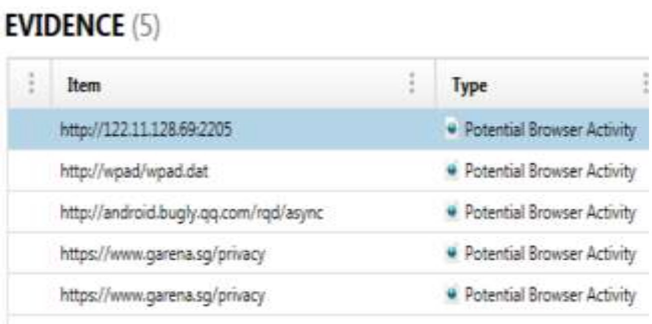
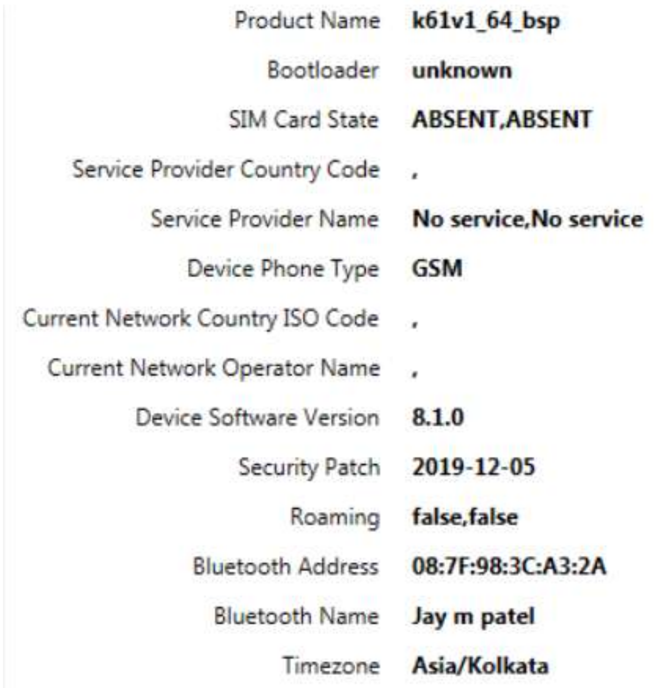


Fig 18: Device information section having network evidences



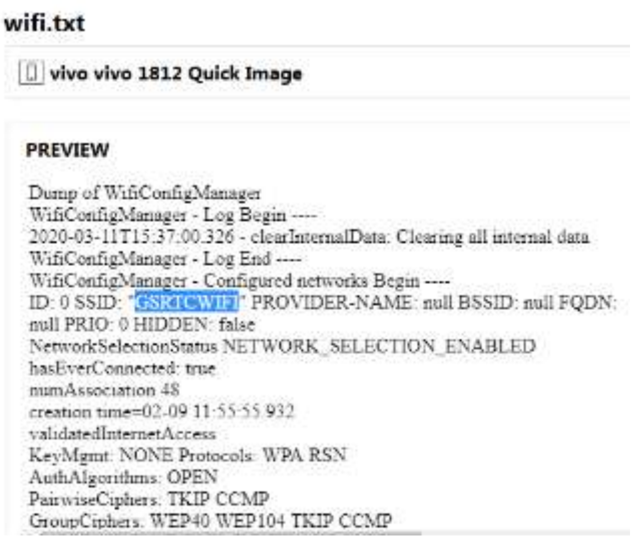
Item	Type
http://122.11.128.69:2205	Potential Browser Activity
http://wpad/wpad.dat	Potential Browser Activity
http://android.bugly.qq.com/rqd/async	Potential Browser Activity
https://www.garena.sg/privacy	Potential Browser Activity
https://www.garena.sg/privacy	Potential Browser Activity

Fig 19: IP and URL based evidences extracted from the device



Product Name	k61v1_64_bsp
Bootloader	unknown
SIM Card State	ABSENT,ABSENT
Service Provider Country Code	,
Service Provider Name	No service,No service
Device Phone Type	GSM
Current Network Country ISO Code	,
Current Network Operator Name	,
Device Software Version	8.1.0
Security Patch	2019-12-05
Roaming	false,false
Bluetooth Address	08:7F:98:3C:A3:2A
Bluetooth Name	Jay m patel
Timezone	Asia/Kolkata

Fig 20: Network based artefacts analysed by the software.



wifi.txt

vivo vivo 1812 Quick Image

PREVIEW

```
Dump of WifiConfigManager
WifiConfigManager - Log Begin ----
2020-03-11T15:37:00.326 - clearInternalData: Clearing all internal data
WifiConfigManager - Log End ----
WifiConfigManager - Configured networks Begin ----
ID: 0 SSID: "GSRTCWIFI" PROVIDER-NAME: null BSSID: null FQDN:
null PRIO: 0 HIDDEN: false
NetworkSelectionStatus NETWORK_SELECTION_ENABLED
hasEverConnected: true
numAssociation 48
creation time=02-09 11:55:55.932
validatedInternetAccess
KeyMgmt: NONE Protocols: WPA RSN
AuthAlgorithms: OPEN
PairwiseCiphers: TKIP CCMP
GroupCiphers: WEP40 WEP104 TKIP CCMP
```

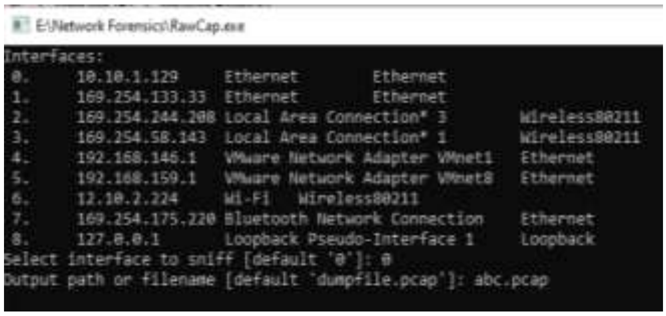
Fig 21: Wi-Fi connections with SSID and sessions fetched from device

2.5. CAPTURED NETWORK DATA

The data transmission in the network is in the form of packets. For instance, every request or messages sent are series of packets and every data/file transfer done leaves a series of packet. Based on type of packets, they may be classified as frames, cells, blocks or segments. The data and the captured packets during the network analysis are saved using the .pcap file extension. They are analysed to fetch certain network information such as connection / disconnection status, protocols, data, IP addresses etc. Few applications that can open and capture .pcap files are Wireshark, Network Miner, tcpdump, Packet Square - Cap edit etc.

2.5.1. RAWCAP

RawCap is a free command line network sniffer for Windows that uses raw sockets which captures data and generates pcap files. Here packets were captured from the local system so as to examine the nature or packets transmitting from the system. This can be used to capture packets and later check if any malicious key-logger or backdoor is enabled on the system, which might leak data.

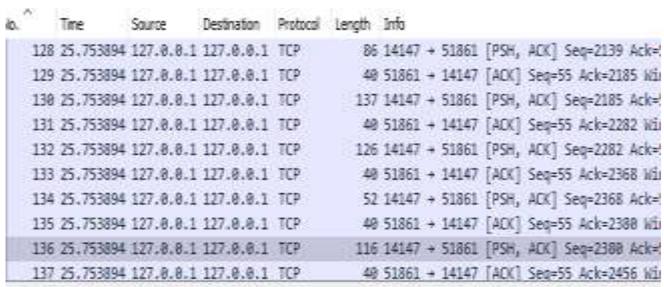


```
E:\Network Forensics\RawCap.exe
Interfaces:
 0.     10.10.1.129     Ethernet        Ethernet
 1.     169.254.133.33  Ethernet        Ethernet
 2.     169.254.244.208 Local Area Connection* 3        Wireless80211
 3.     169.254.58.143  Local Area Connection* 1        Wireless80211
 4.     192.168.146.1   VMware Network Adapter VMnet1   Ethernet
 5.     192.168.159.1   VMware Network Adapter VMnet8   Ethernet
 6.     12.10.2.224     Wi-Fi   Wireless80211
 7.     169.254.175.220 Bluetooth Network Connection    Ethernet
 8.     127.0.0.1       Loopback Pseudo-Interface 1     Loopback
Select interface to sniff [default '0']: 0
Output path or filename [default 'dumpfile.pcap']: abc.pcap
```

Fig 22: Capturing packets abc.pcap from interfaces

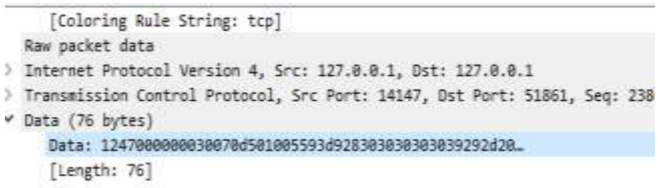
2.5.2. WIRESHARK

Wireshark is a packet sniffer and analyser tool to capture packets in live network environment and analyse packets in depth with a lot of analysing modules and techniques. It runs on Unix-like operating systems and Microsoft windows. It is one of the most important used tool in network analysis. It can sniff packets from various interfaces on a system and network. It can capture active (live network) as well as passive data (captured in packets). Below are the packets and data captured for a particular sever session where IP and requests are captured, which can be analysed for suspicious events.



No.	Time	Source	Destination	Protocol	Length	Info
128	25.753894	127.0.0.1	127.0.0.1	TCP	86	14147 → 51861 [PSH, ACK] Seq=2139 Ack=
129	25.753894	127.0.0.1	127.0.0.1	TCP	40	51861 → 14147 [ACK] Seq=55 Ack=2185 Wi
130	25.753894	127.0.0.1	127.0.0.1	TCP	137	14147 → 51861 [PSH, ACK] Seq=2185 Ack=
131	25.753894	127.0.0.1	127.0.0.1	TCP	40	51861 → 14147 [ACK] Seq=55 Ack=2282 Wi
132	25.753894	127.0.0.1	127.0.0.1	TCP	126	14147 → 51861 [PSH, ACK] Seq=2282 Ack=
133	25.753894	127.0.0.1	127.0.0.1	TCP	40	51861 → 14147 [ACK] Seq=55 Ack=2368 Wi
134	25.753894	127.0.0.1	127.0.0.1	TCP	52	14147 → 51861 [PSH, ACK] Seq=2368 Ack=
135	25.753894	127.0.0.1	127.0.0.1	TCP	40	51861 → 14147 [ACK] Seq=55 Ack=2380 Wi
136	25.753894	127.0.0.1	127.0.0.1	TCP	116	14147 → 51861 [PSH, ACK] Seq=2380 Ack=
137	25.753894	127.0.0.1	127.0.0.1	TCP	40	51861 → 14147 [ACK] Seq=55 Ack=2456 Wi

Fig 23: Captured packets analysis



```
    [Coloring Rule String: tcp]
  Raw packet data
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 14147, Dst Port: 51861, Seq: 238
v Data (76 bytes)
    Data: 124700000000030070d501005593d928303030303039292d20…
    [Length: 76]
```

Fig 24: Captured packets analysis in depth

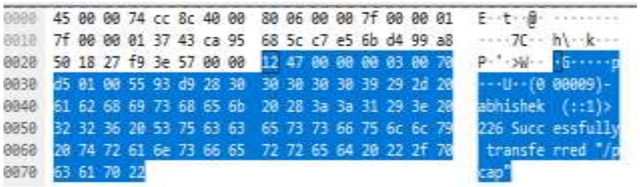


Fig 25: Captured packets analysis for the data transmitted

2.5.3. NETWORKMINER

NetworkMiner is a freely available and open-source forensic analysis tool for networks. It works on windows platform, Linus & MAC OS X based systems. It also can be used as passive sniffer or packet capturing tool to detect OS, hosts, sessions, ports, files, images, messages, credentials, DNS and other packet contents without interfering or putting load in the connected network. It can also parse certificate files and other essential data from the offline PCAP analysing. Here, as a part of investigation captured packets from a network are examined to find out credentials and hosts from a PCAP file which are involved in suspicious activities.

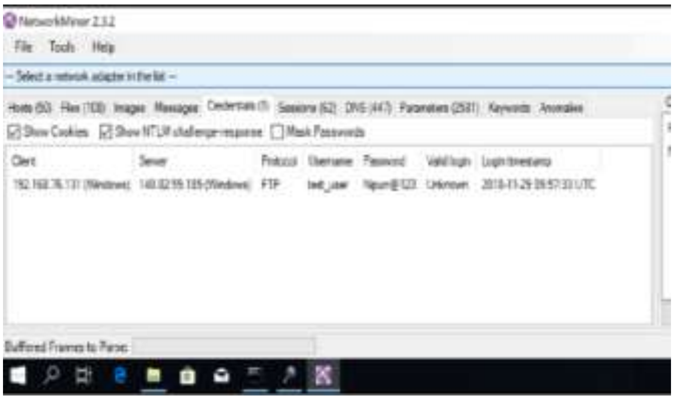


Fig 26: Network Miner capturing credentials transferred over network

Fig 27: Network Miner GUI sorting hosts

3. RESULTS

The following table consists of the results obtained from various examination processes and tools.

Table-III: Results obtained from each examination

Evidence \ Device	Method \ Tool used	Results
Live Systems	Event Viewer, Commands, IP Scanner	Network connections, Interface details, IP addresses and open ports of network.
Forensic Images of memory devices	EnCase, FTK	IP addresses, Network connections.
Log Files	Apache Log Viewer	Log analysis.
Mobile Phones	XRY, Magnet AXIOM	SSID, Network connection details, Bluetooth addresses, SIM details.
Captured network data	RawCap, Wireshark, Network Miner	All network data and network based requests captured in PCAP, Credentials, files and session data.

4. CONCLUSION

Using various tools & scripts like network miner, wireshark, Advance IP Scanner, Apache Log Viewer, XRY, Magnet Axiom, EnCase etc.; network artefacts and data which can be useful for investigation as evidence can be obtained. More tools like Nessus, nmap, angry IP Scanners can also be helpful in the investigation process. The end result and evidence should maintain the integrity and should be produced and derived with standard methods and tools. These tools and investigations can be used by the investigators to obtain their desired results in domain of network forensics.

REFERENCES:

[1.] Y. Kim and K. J. Kim, "A Forensic Model on DeletedFile Verification for Securing Digital Evidence". 978—14244-5493-8710 IEEE, 2010.

[2.] D. Chang, S. K. Sanadhya, M. Singh. "Security Analysis of MVHASH-B Similarity Hashing". Journal of Digital Forensics, Security and Law, JDFSL, Vol. 11, No. 2, pp. 21-34, 2015.

[3.] Montasari, Reza & Hill, Richard. (2019). Next-Generation Digital Forensics: Challenges and Future Paradigms. 205-212. 10.1109/ICGS3.2019.8688020.

[4.] "Crime scene and physical evidence awareness for non-forensic personnel," United Nations Office on

Drugs and Crime, 2009. Accessedon: Sep.3, 2019. [Online].
[5.] T. F. Kiely. ”Forensic evidence: science and the criminal law,” CRC Press, 2005.
[6.] J. Sachowski, “Understanding Digital Forensic Readiness,” Implementing Digital Forensic Readiness, pp. 80–86, 2019.
[7.] Shrivastava, Gulshan & Sharma, Kavita & Kumari, Reema. (2016). Network Forensics: Today and Tomorrow.