Digital Forensics Lab file

Submitted by

Student Name: OJASVI SINGH CHAUHAN
Roll No: R134218111
SAP ID: 500068394

SCHOOL OF COMPUTER SCIENCE

UNIVERSITY OF PETROLEUM & ENERGY STUDIES

Bidholi Campus, Energy Acres, Dehradun – 248007.

April - 2020

INDEX

Experiment No.	Experiment Name	Description
1	***Creating a Forensic Image using FTK Imager/Encase Imager***	• Creating Forensic Image • Check Integrity of Data • Analyze Forensic Image
2	***Creating RAM Dump using FTK Imager and Volatility***	• Create RAM Dump of Windows XP/7 • Analyze using Volatility
3	***Forensics Case Study***	• Solve the Case study (image file) provide in lab using Volatility tool • Use of Virus Total
4	***Capturing and analyzing network packets using Wireshark (Fundamentals)***	• Identification the live network • Capture Packets • Analyze the captured packets • Nmap using Wireshark
5	***Analyze the packets provided in lab and solve the questions using Wireshark***	• Analysis of various pcap files provided in lab using Wireshark
6	***Using Sysinternals tools for Network Tracking and Process Monitoring***	• Check Sysinternals tools • Monitor Live Processes • Capture RAM • Capture TCP/UDP packets • Monitor Hard Disk • Monitor Virtual Memory • Monitor Cache Memory
7	***Recovering and Inspecting deleted files***	• Check for Deleted Files • Recover the Deleted Files • Analyzing and Inspecting the recovered files • Use $Iparse to see the metadata • See metadata through command-line • Perform this using recovery option in ENCASE
8	***Email Forensics***	• Mail Service Providers • Email protocols • Recovering emails • Analyzing email header
9	***Web Browser Forensics***	• Web Browser working • Forensics activities on browser • Cache / Cookies analysis • Last Internet activity

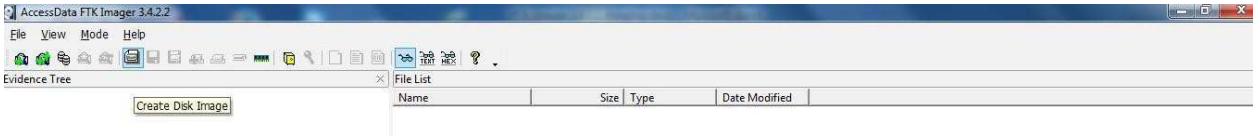
EXPERIMENT 1

Creating a Forensic Image using FTK Imager/Encase Imager

Use FTK Imager to create the image of files in pen drive and verify the hash values.

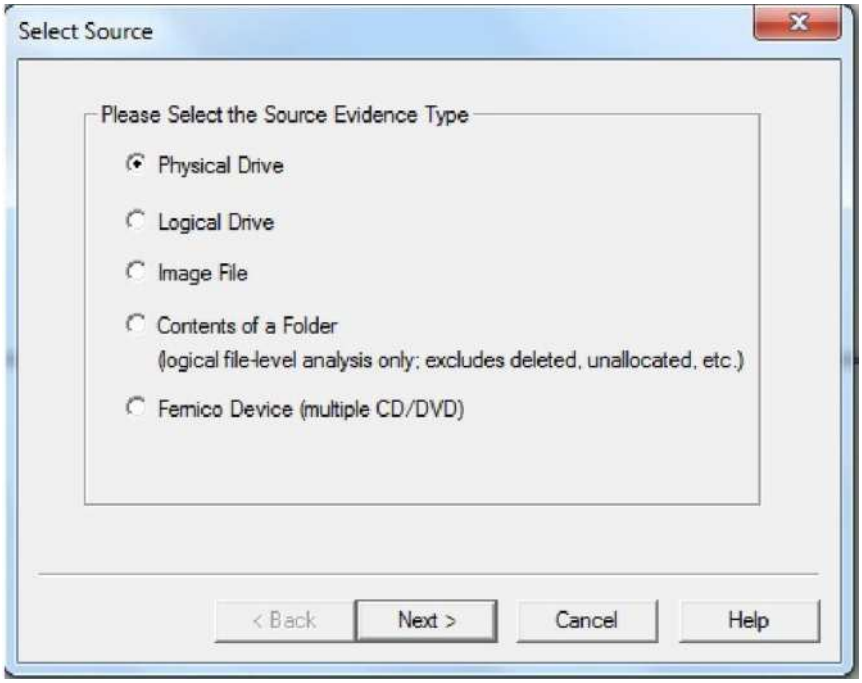
TASK I: Imaging

1. To run the application, select the application, right click on it and run as an "Administrator".
2. The application will be opened as shown below.

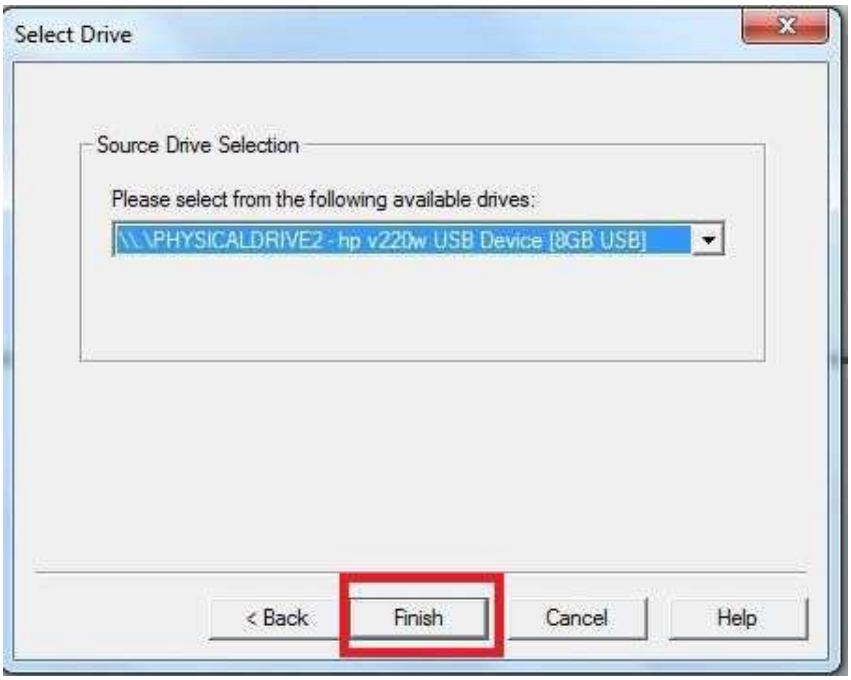


Now to create an Image, we need to select the icon as shown in the above image.
Note: In this experiment we have use Sandisk 15 GB pendrive to create an Image.

3. After clicking on the icon, the page will be opened as shown below:



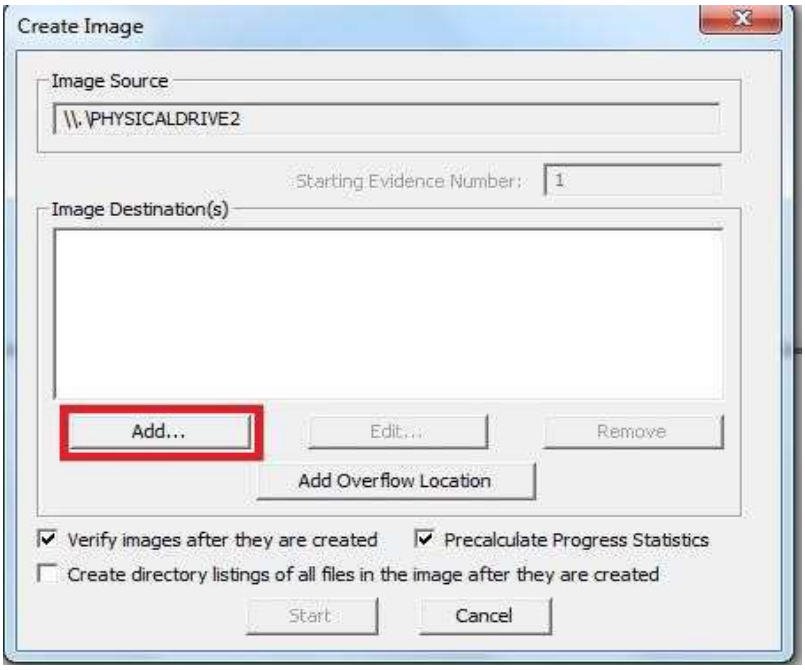
4. After selecting the device type, click on "Next" button to proceed, the page will be opened as shown below:



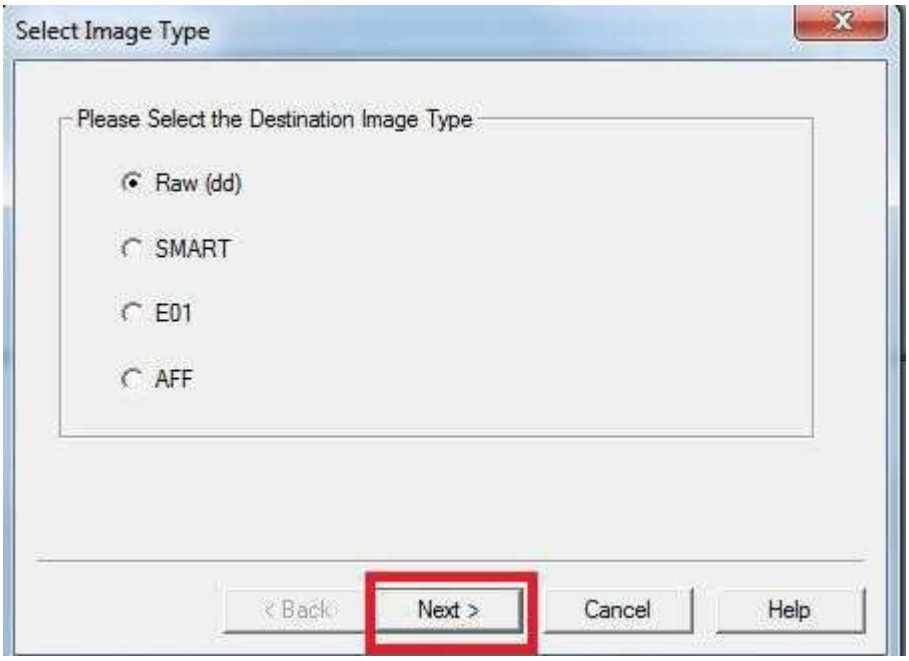
Select the drive to which you want to create an Image as shown above:

After selecting the drive, click on "Finish" button, the page will be opened as shown.

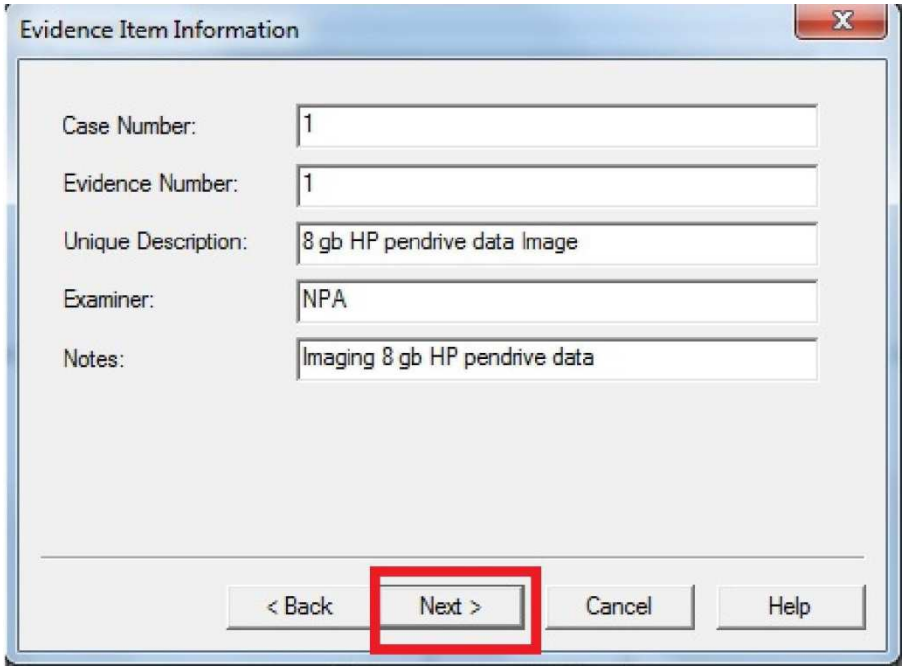
5. Click on "Add" button as shown above to add the destination location to save the image:-



6. After clicking on Add button, the page will be opened as shown above. Select the image type you want to create and click on "Next" button as shown below:-



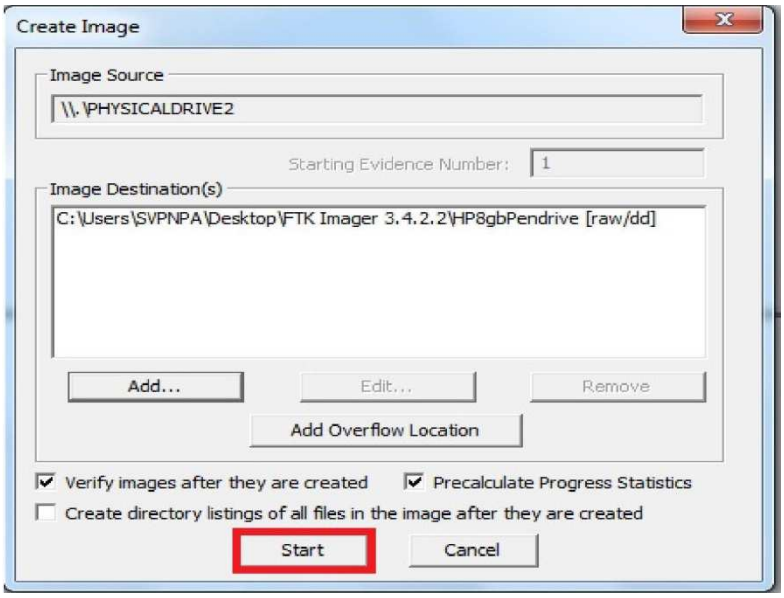
7. After clicking on "Next" button, the page will be displayed as shown below
8.



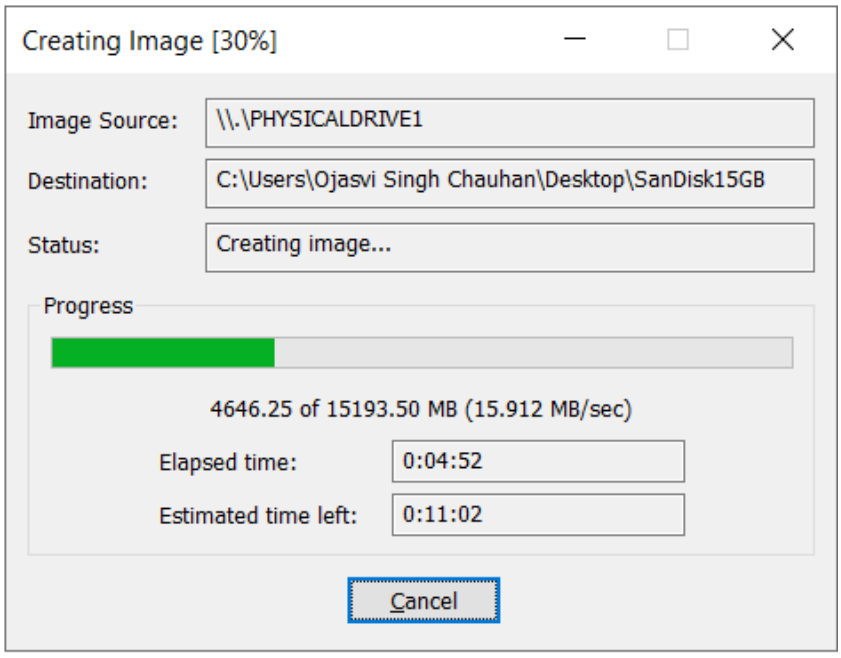
Fill the evidence item information and click on "Next" button as shown above.

9. Fill the image destination folder location details and Image File name details and Click on "Finish" button.

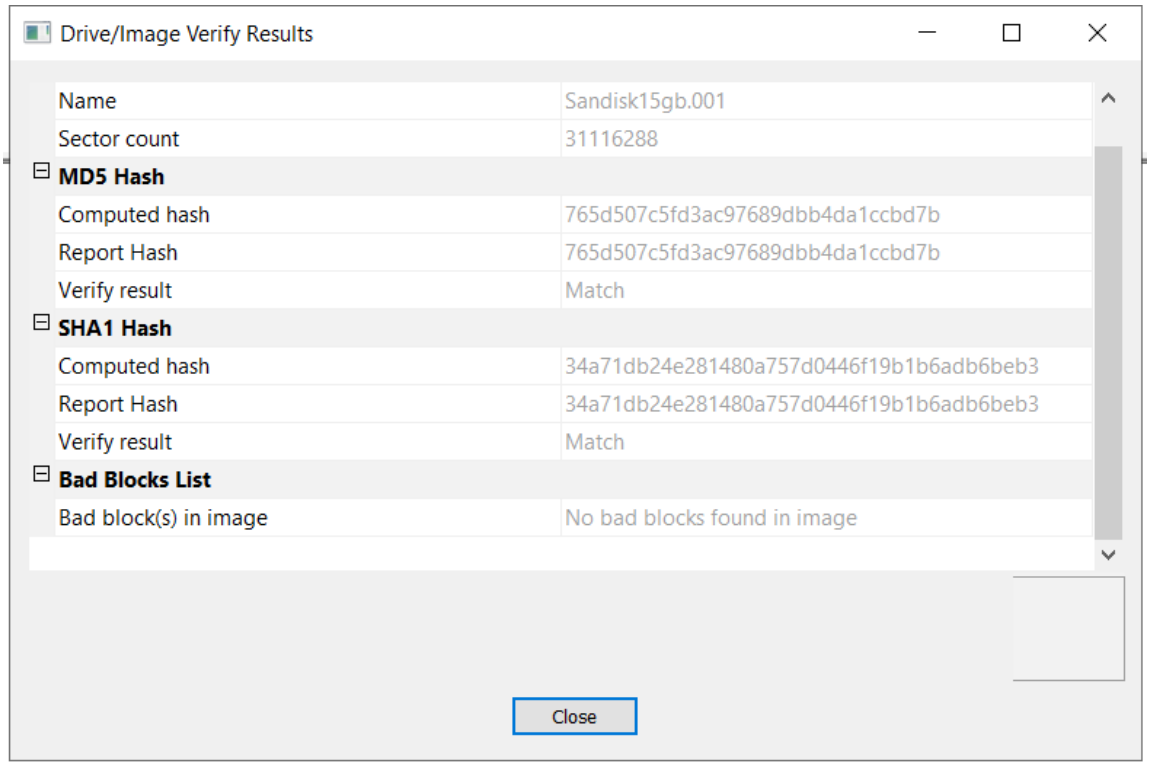
10. After clicking on Finish button, all the details will be added as shown below



Click on "Start" button as shown above to start imaging process. This can be observed from the below image.



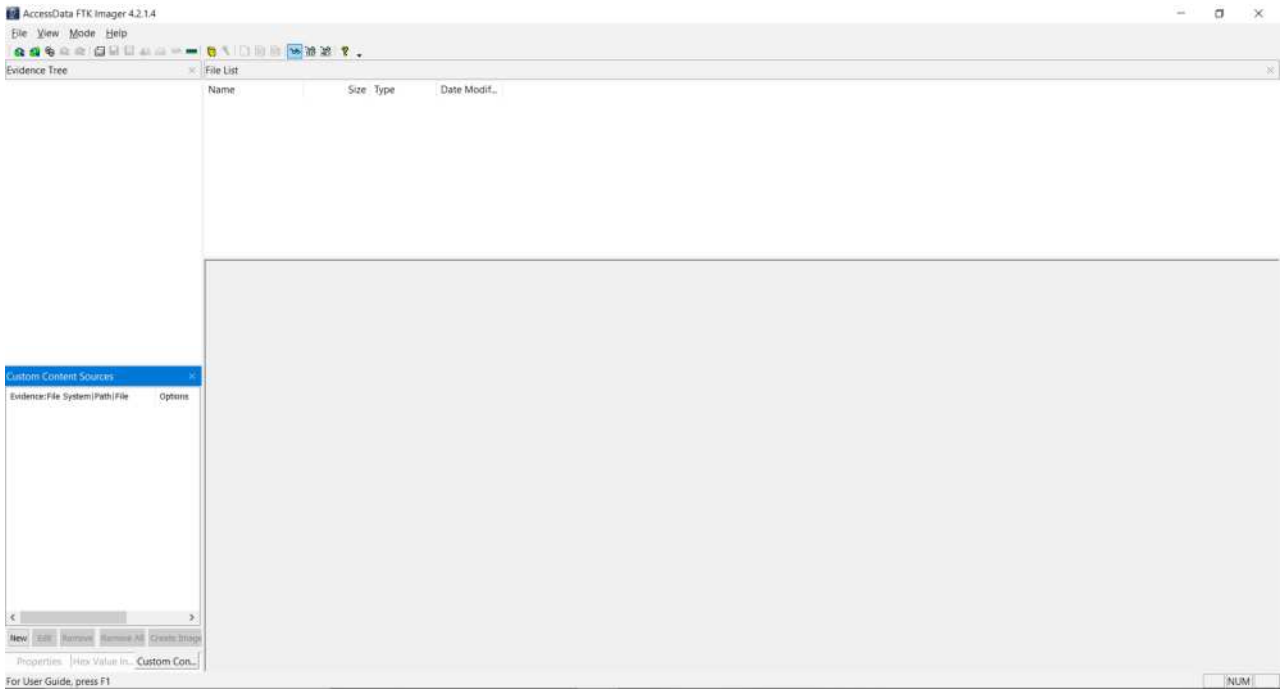
11. After completion of imaging, the hash value of the image will be calculated using MD5 and SHA1 algorithm and will be displayed as shown below.



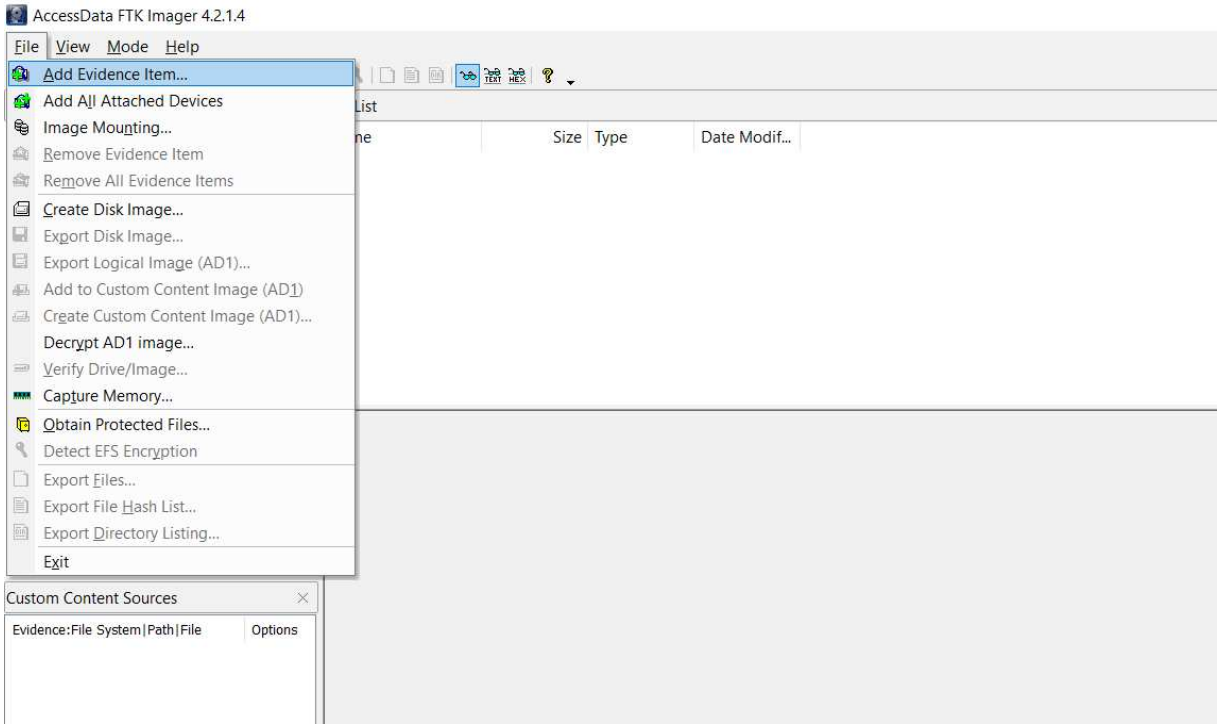
TASK II: Hashing

Verify the MD5 SHA1 hash value of an image Using FTK Imager version 4.2

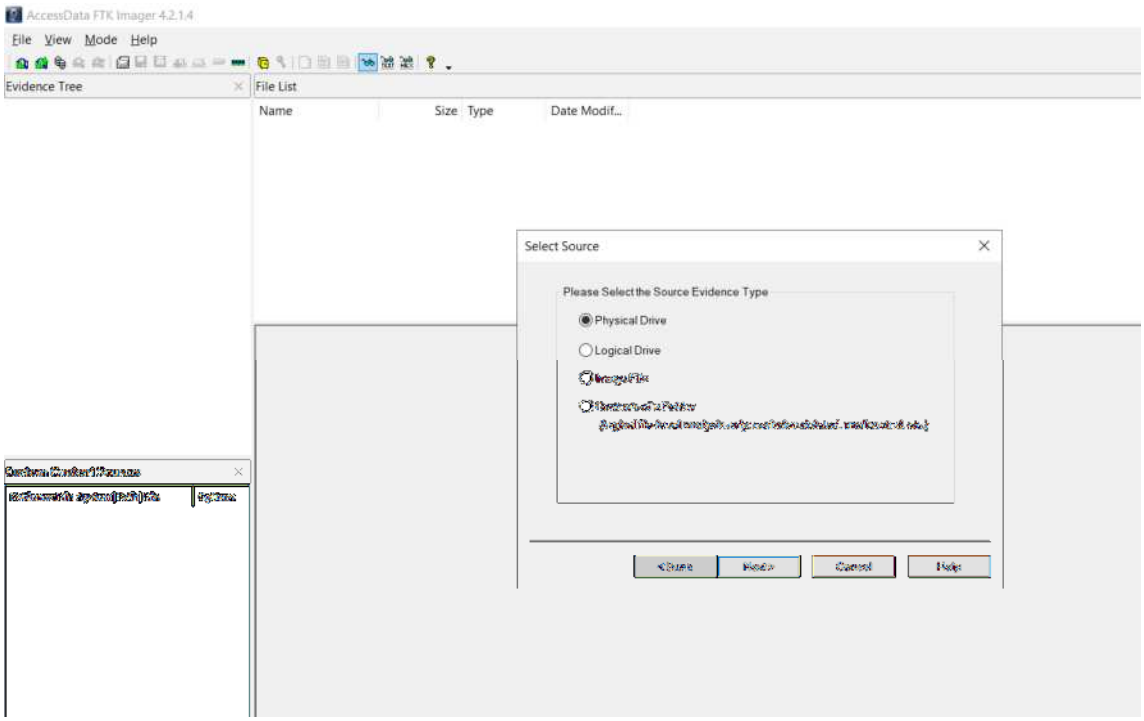
1. Launch FTK Imager

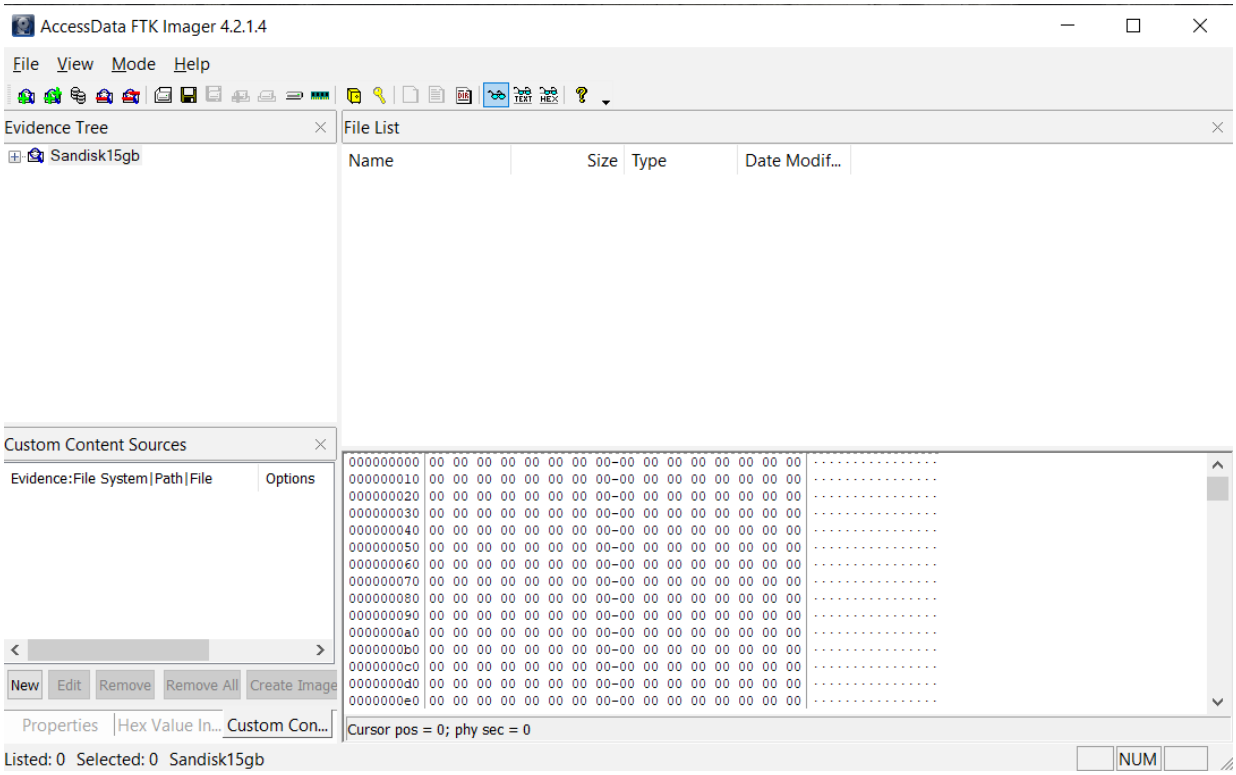


2. Select File > Add Evidence Item

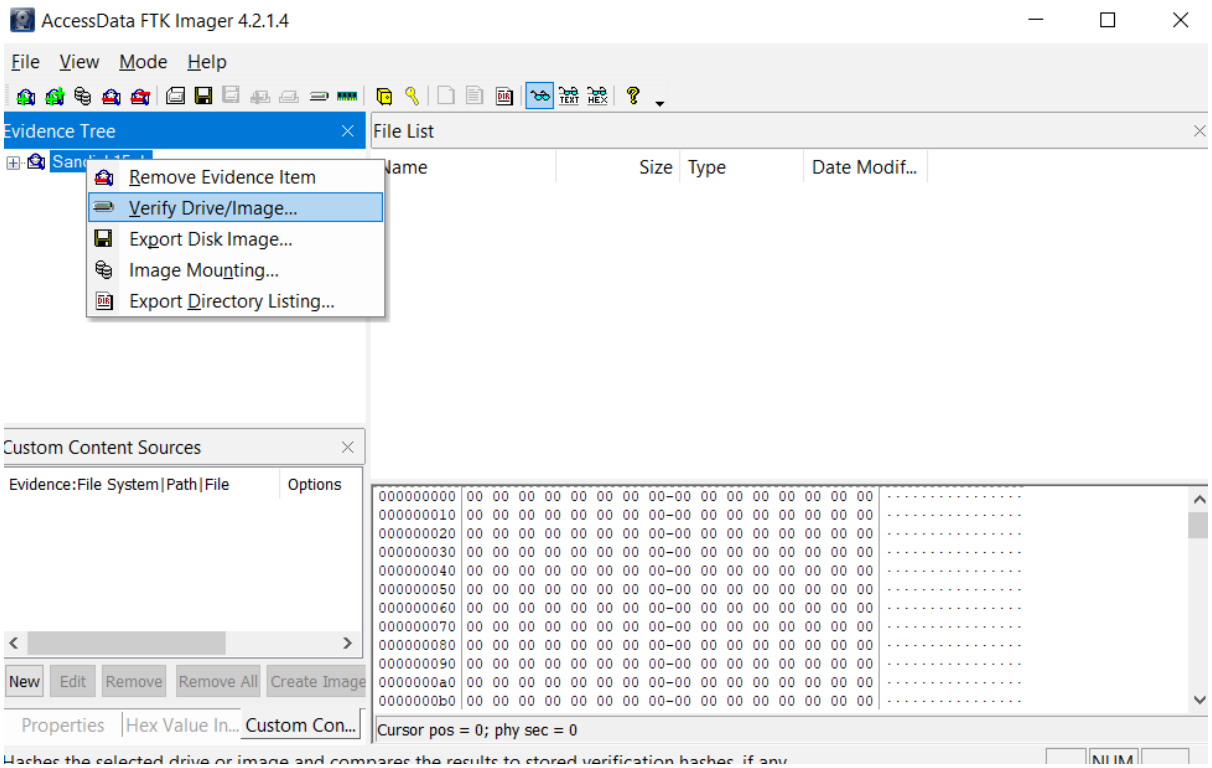


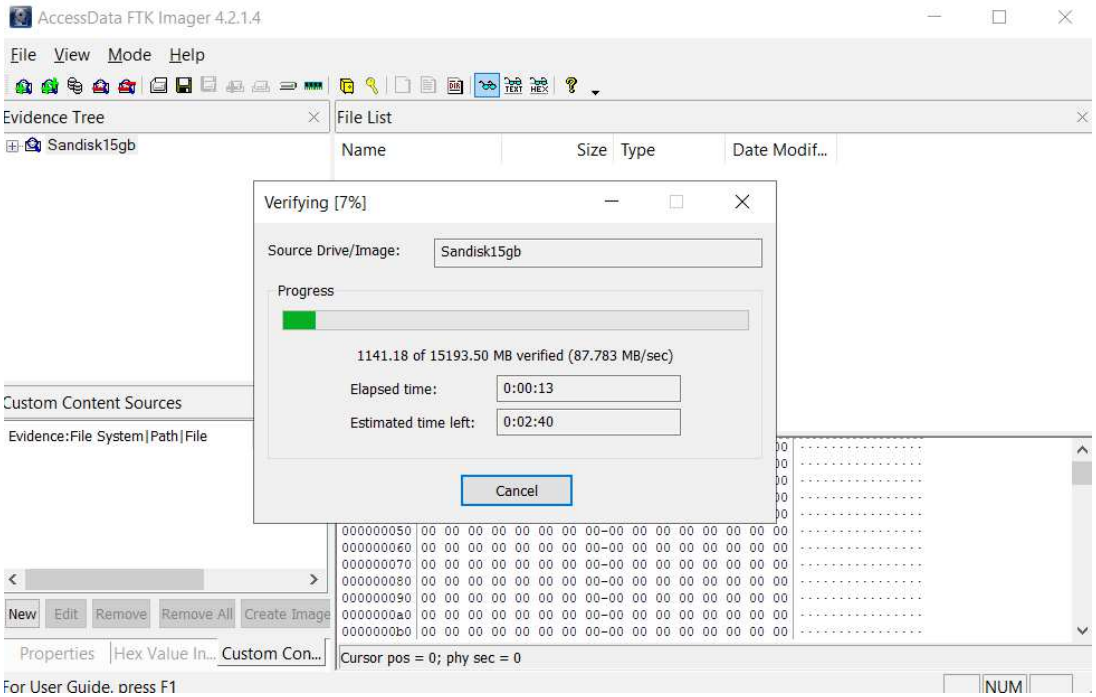
3. Select "Image File" and proceed to add the image



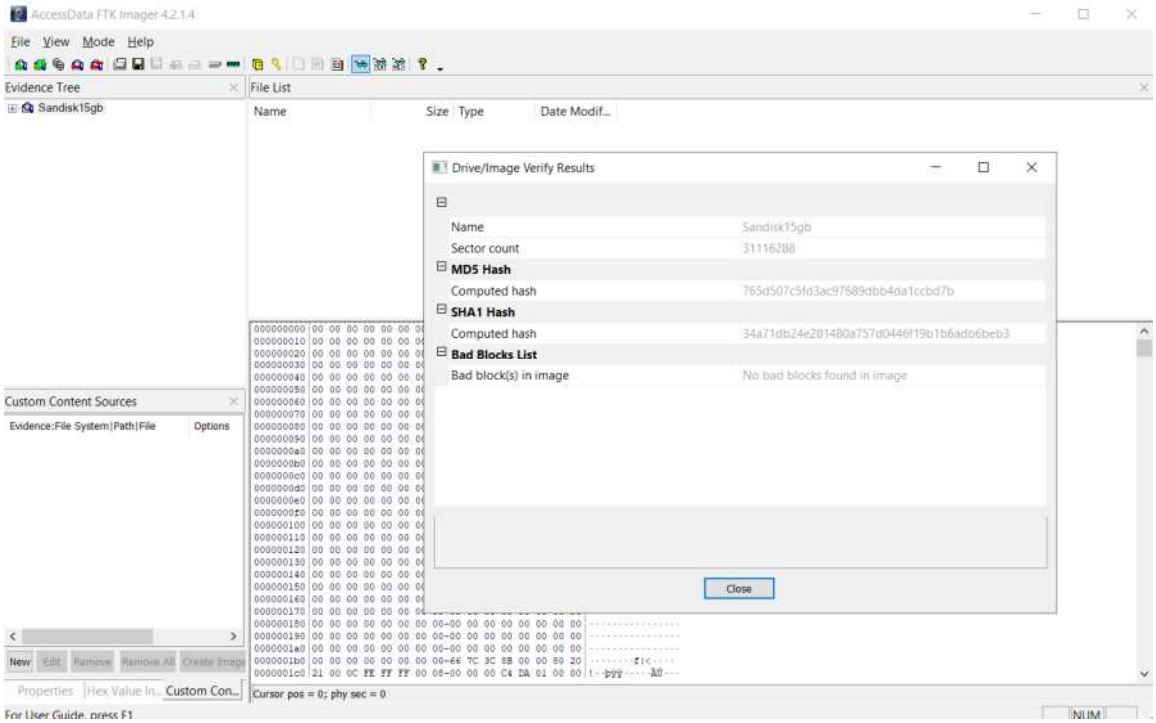


4. Under the "Evidence Tree", right click your image and select Verify Drive/Image.





5. Compare the hash value calculated to the known hash value.



EXPERIMENT – 2

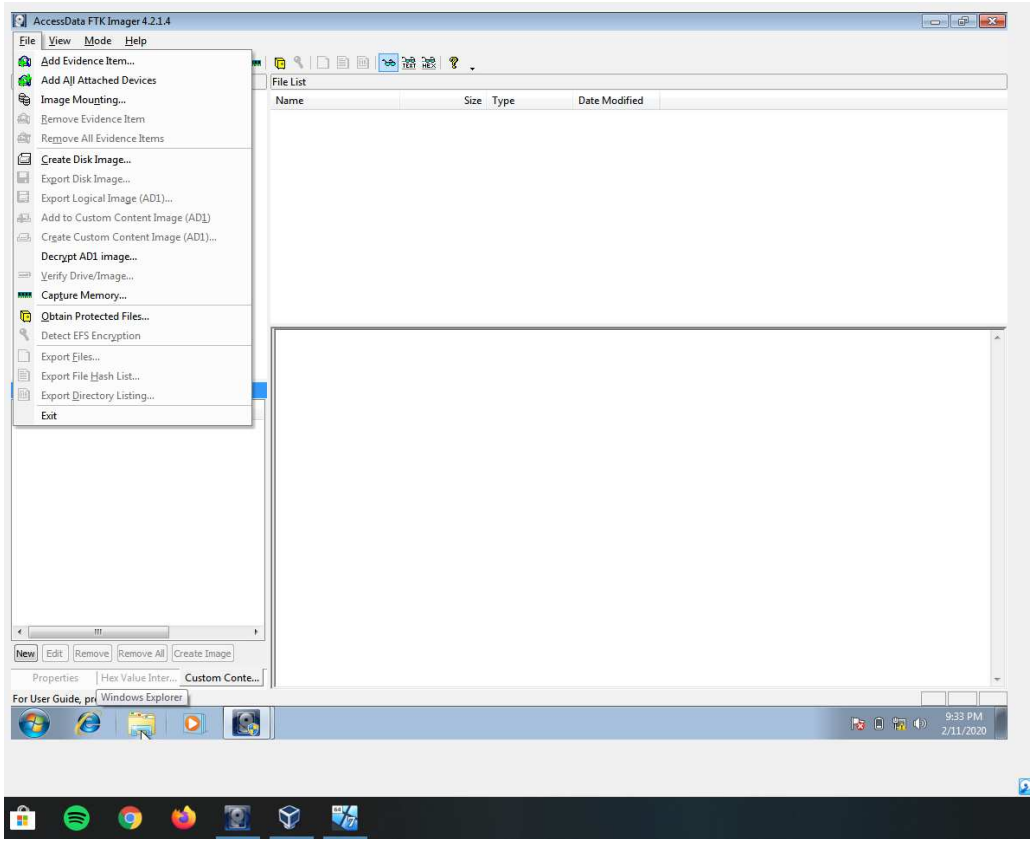
Creating RAM Dump using FTK Imager and Volatility

VOLATILITY: RAM DUMP

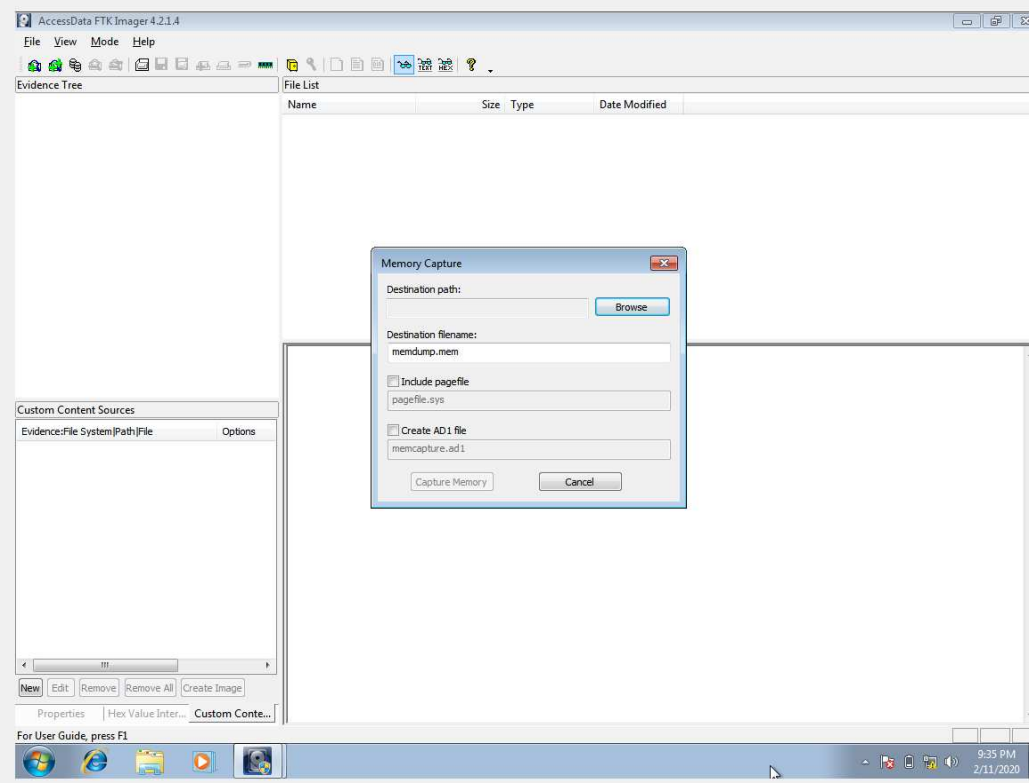
Aim: Creating a Ram dump using FTK Imager & analysing it using volatility.

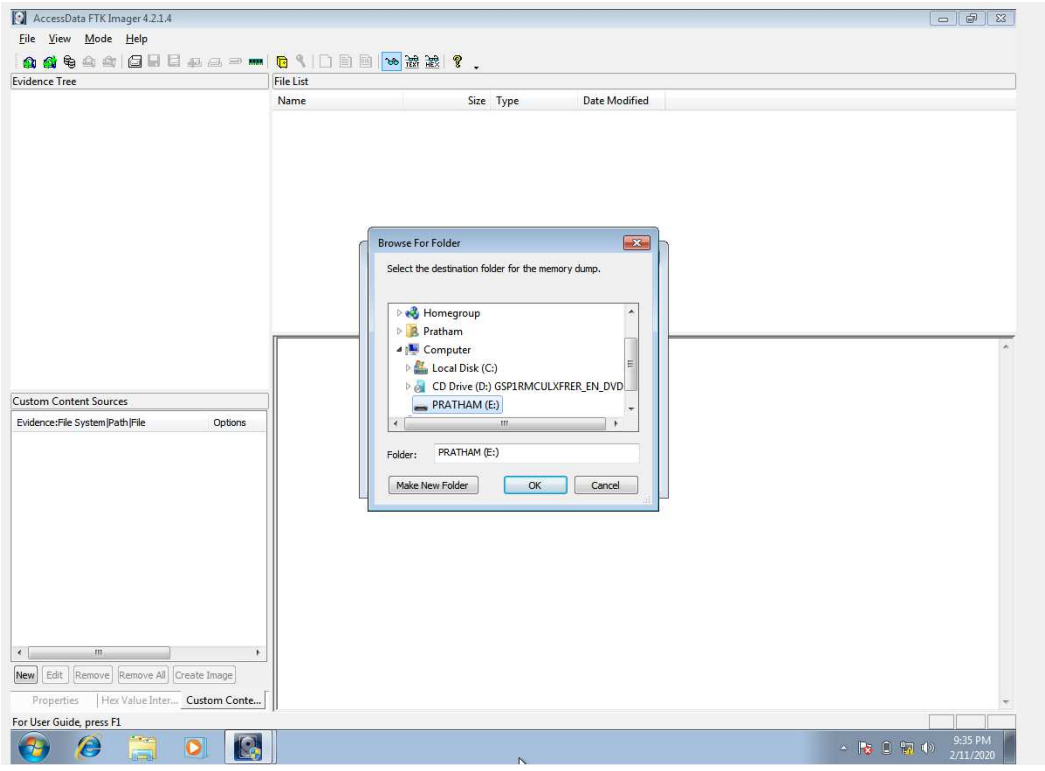
Procedure:

- Open FTK Imager and click on file.

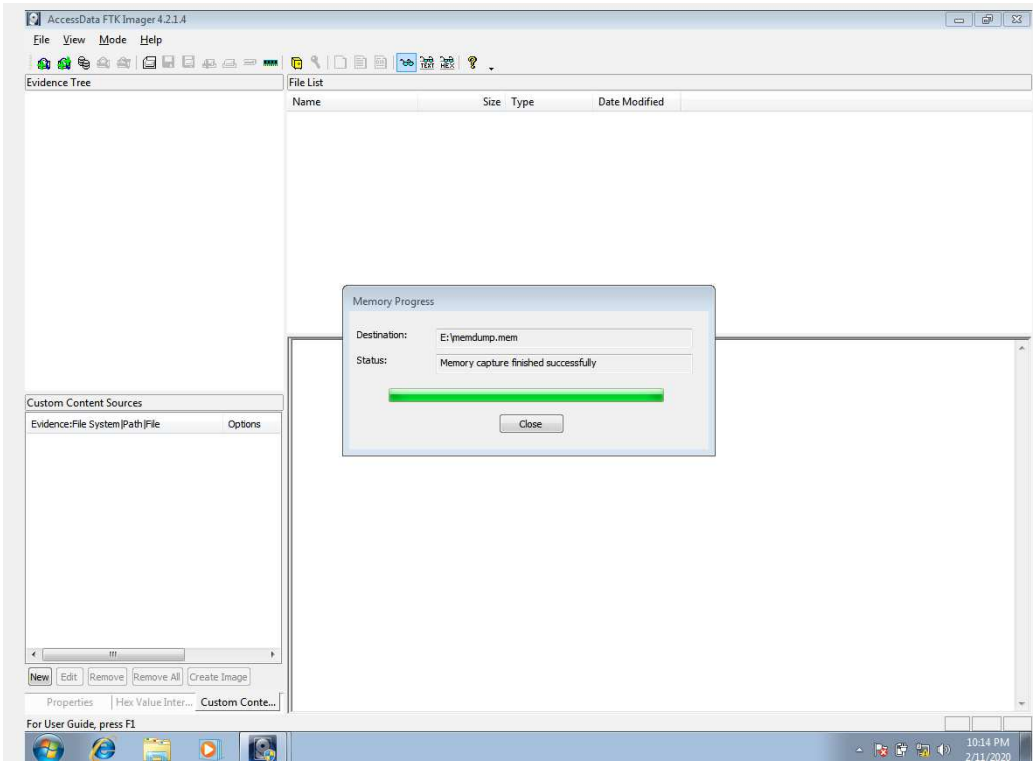


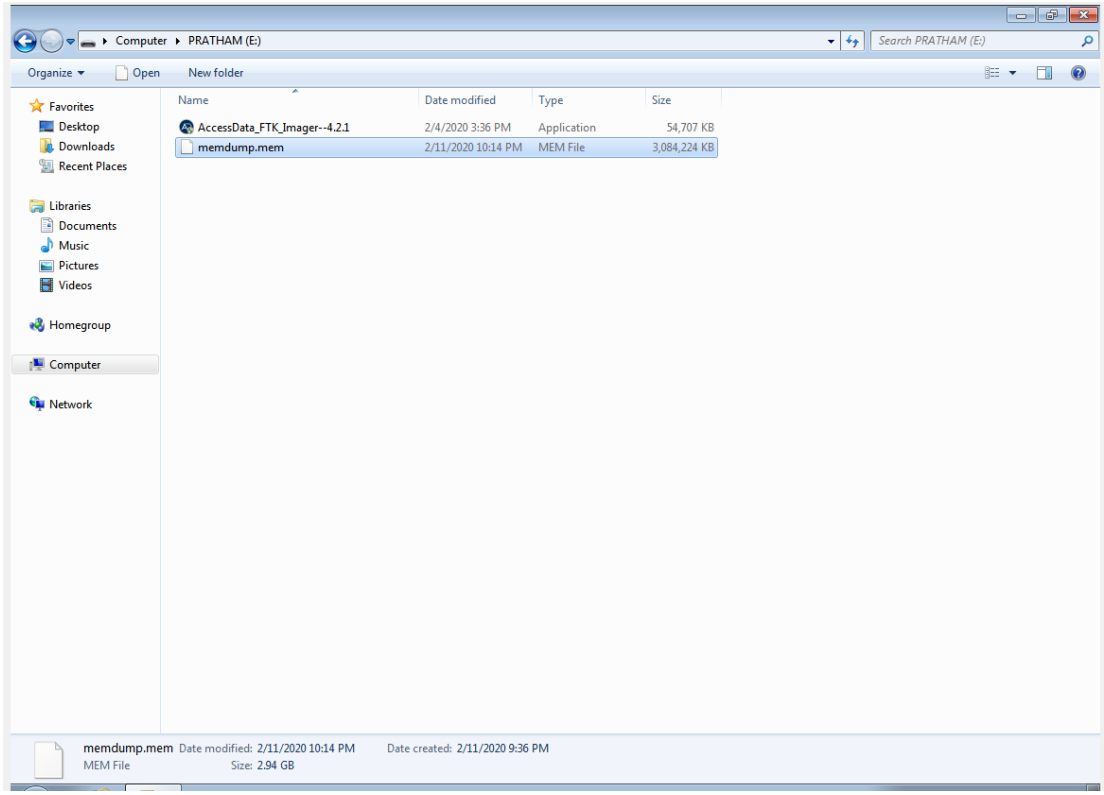
- Select capture memory and select the location where it is to be saved.





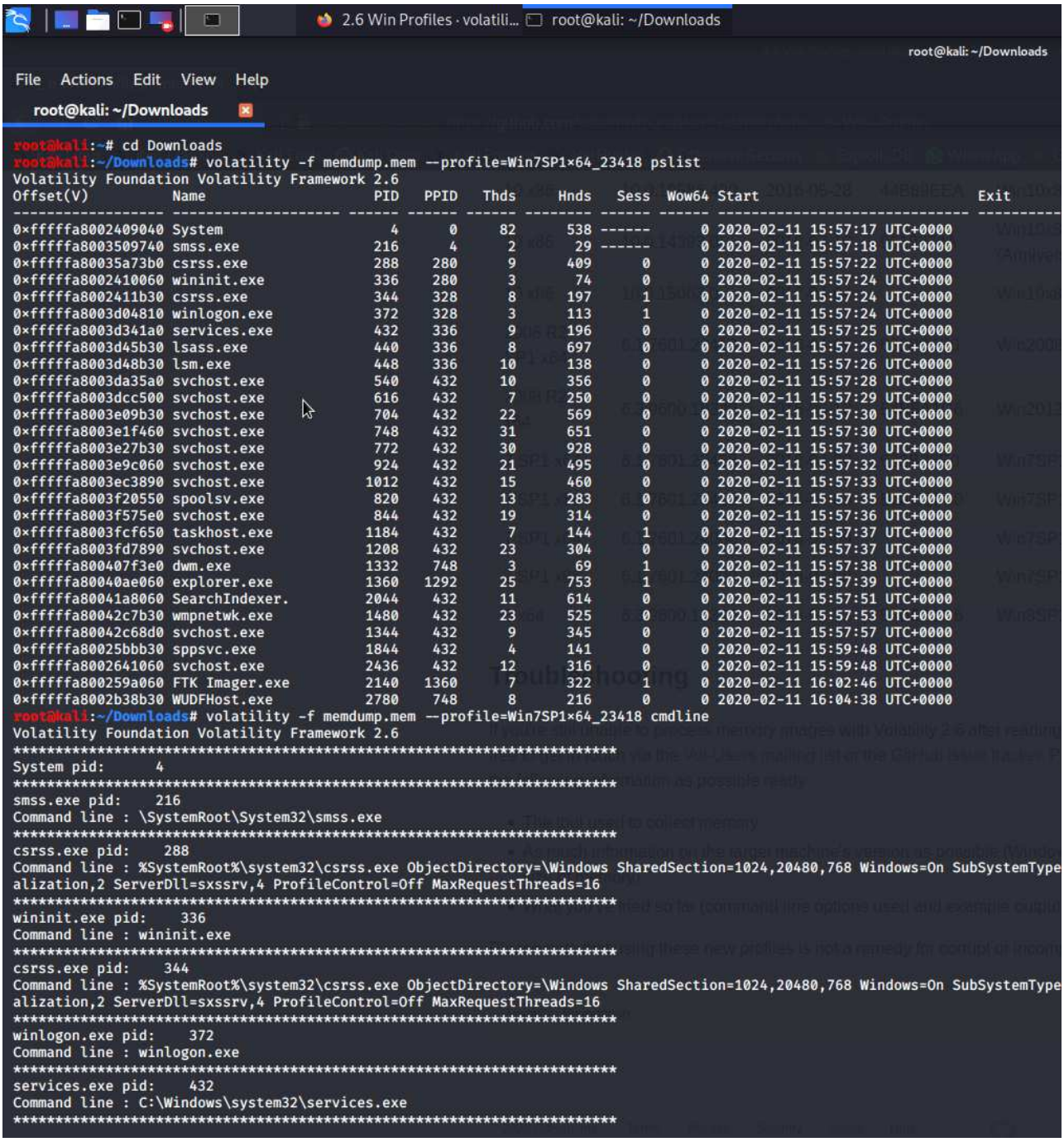
- A .mem file will be saved in the target folder.





- Copy the file to Kali partition.

- Run the file on volatility by setting the profile to Windows 7 and listing the processes by pslist.

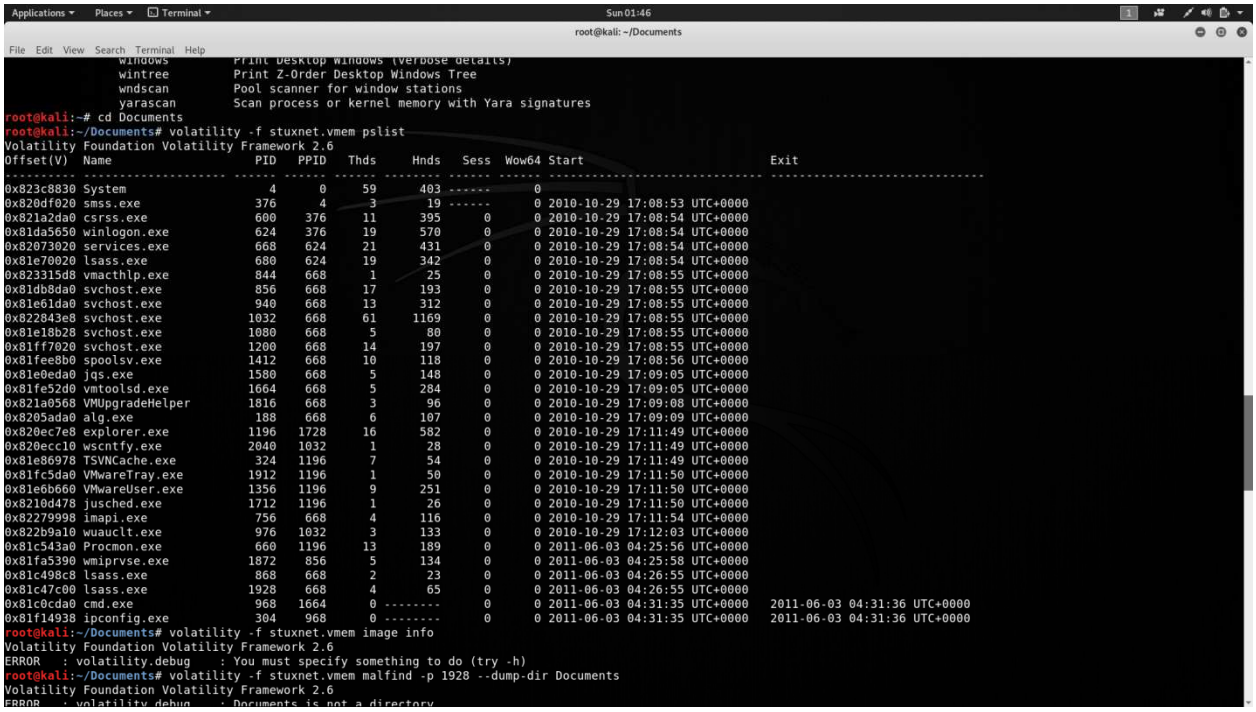


EXPERIMENT – 3

Forensics Case Study

Analysis of the Memory dump using Volatility Forensics tool

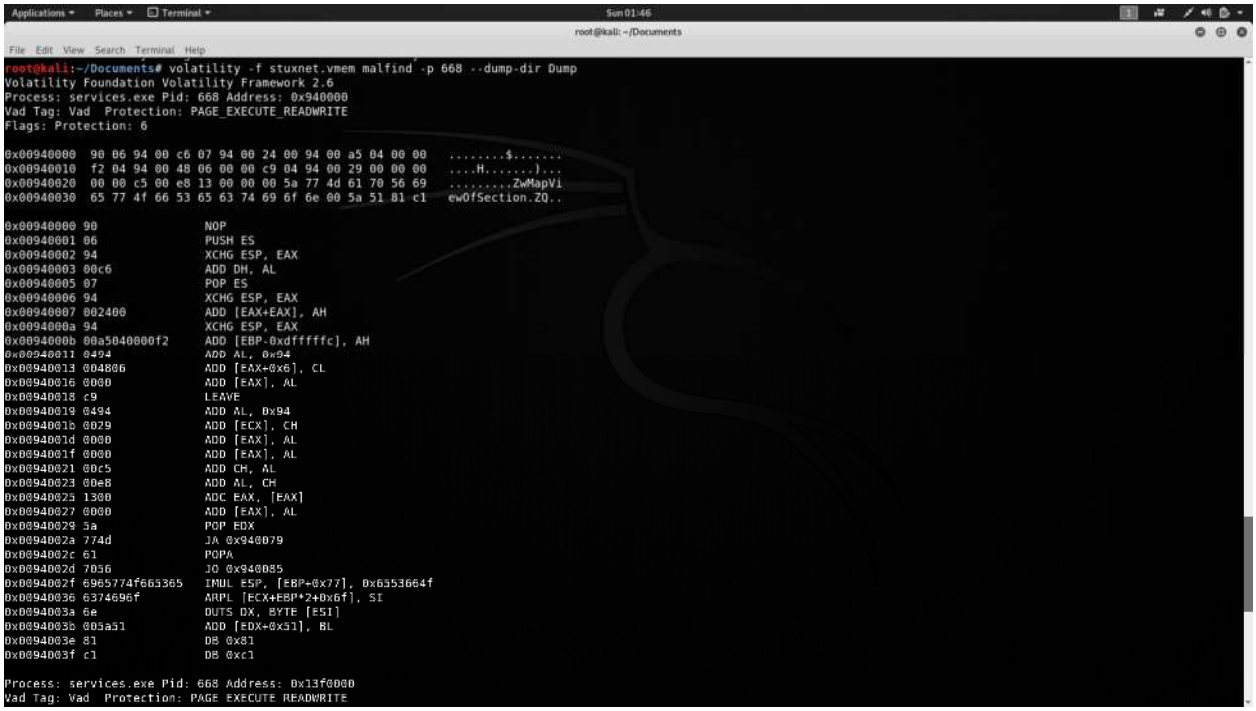
Command 1: Volatility -f stuxnet.vmem pslist



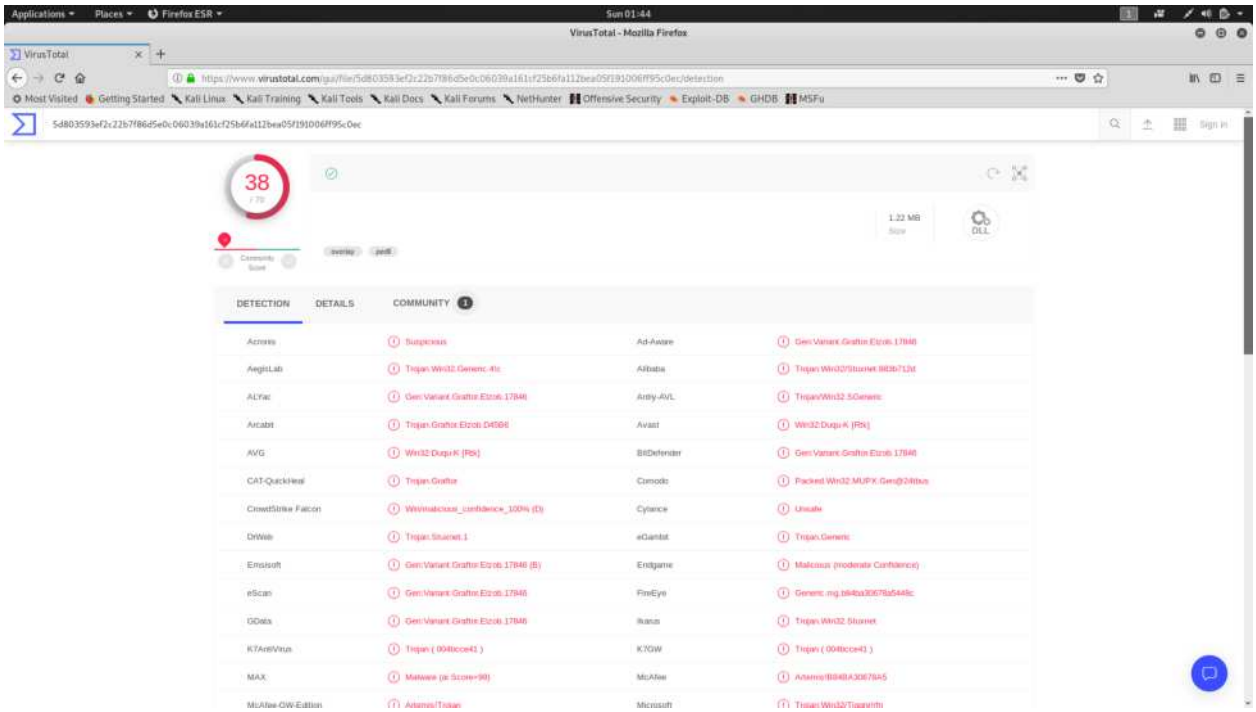
Then, we find connections and then we find any process in which we can find any malware.

"**lsass.exe**" is the Local Security Authentication Server. It verifies the validity of user logons to your PC or server. **Lsass** generates the **process** responsible for authenticating users for the Winlogon service. This is performed by using authentication packages such as the default, Msgina.

Command 2: volatility -f stuxnet.vmem malfind -p 668 –dump-dir dump



Then upload dump file on virustotal.com to check.



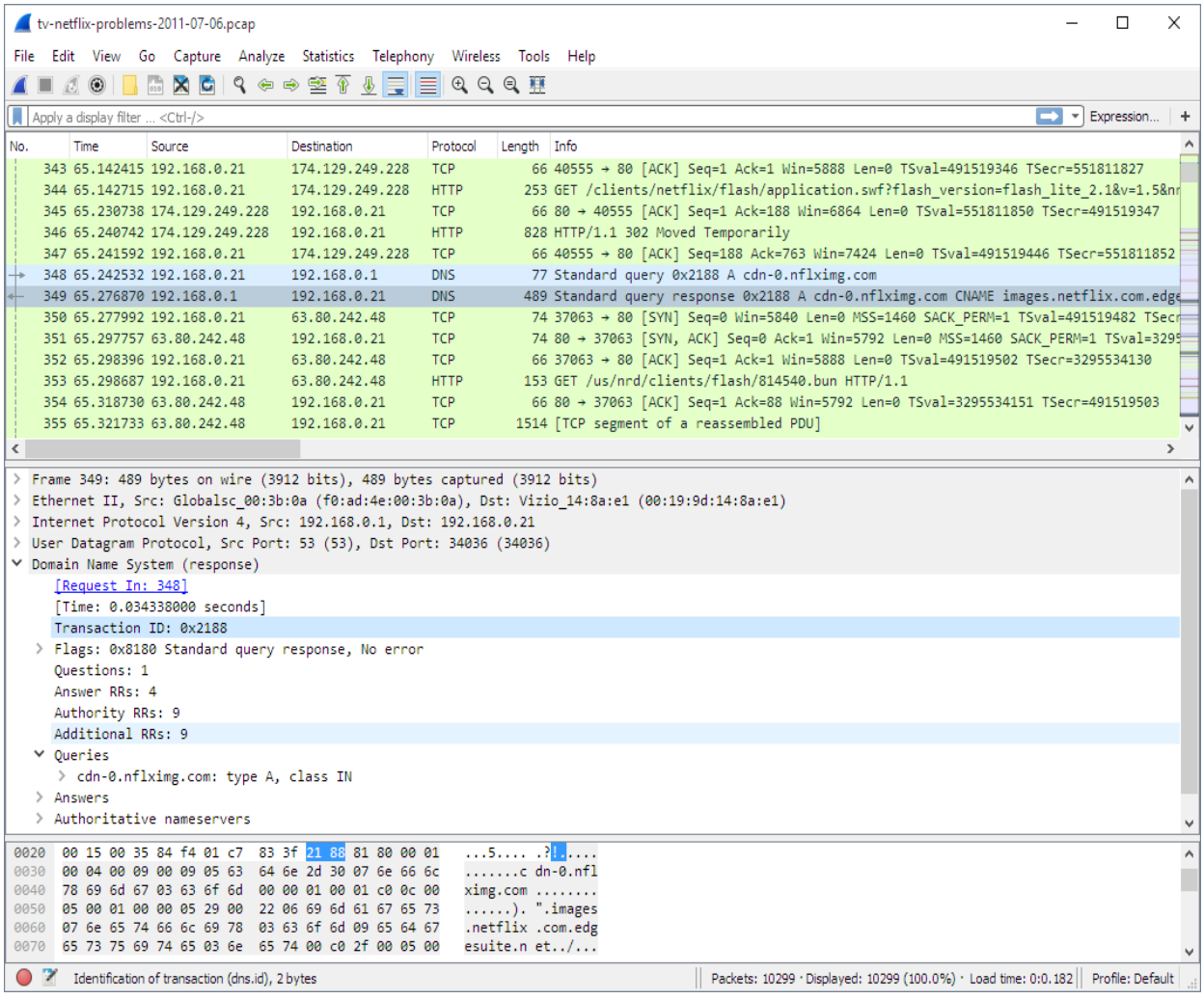
EXPERIMENT 4: WIRESHARK FUNDAMENTALS

1. What is Wireshark?

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. We could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

2. User Interface

a) The Main Window: Let's look at Wireshark's user interface. The Main window shows Wireshark as you would usually see it after some packets are captured or loaded.



Wireshark's main window consists of parts that are commonly known from many other GUI Programs.

1. The ***menu*** is used to start actions.

2. The ***main toolbar*** provides quick access to frequently used items from the menu.

3. The ***filter toolbar*** allows users to set *display filters* to filter which packets are displayed.

4. The ***packet list pane*** displays a summary of each packet captured. By clicking on packets in this pane you control what is displayed in the other two panes.

5. The ***packet details pane*** displays the packet selected in the packet list pane in more detail.

6. The ***packet bytes pane*** displays the data from the packet selected in the packet list pane, and highlights the field selected in the packet details pane.

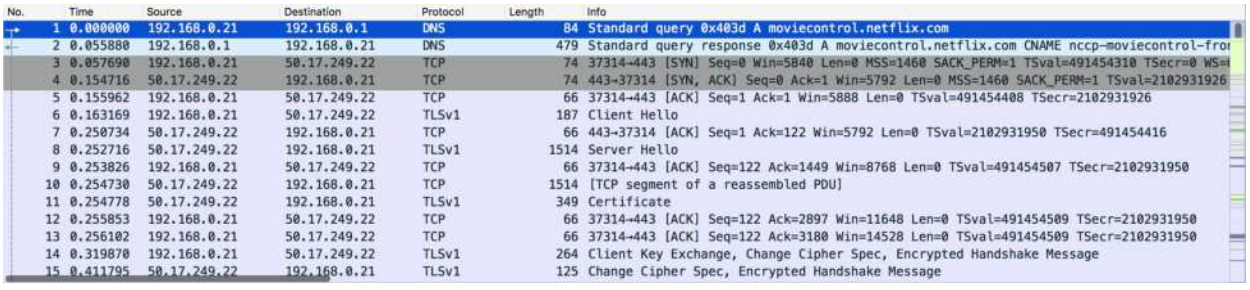
7. The ***statusbar*** shows some detailed information about the current program state and the captured data.

b) The "Main" Toolbar: The main toolbar provides quick access to frequently used items from the menu. This toolbar cannot be customized by the user, but it can be hidden using the View menu if the space on the screen is needed to show more packet data.

Main tool bar items:

Toolbar Icon	Toolbar Item	Menu Item	Description
	[Start]	Capture › Start	Starts capturing packets with the same options as the last capture or the default options if none were set (Start Capturing).
	[Stop]	Capture › Stop	Stops the currently running capture (Start Capturing).
	[Restart]	Capture › Restart	Restarts the current capture session.
	[Options...]	Capture › Options...	Opens the "Capture Options" dialog box. See Start Capturing for details.

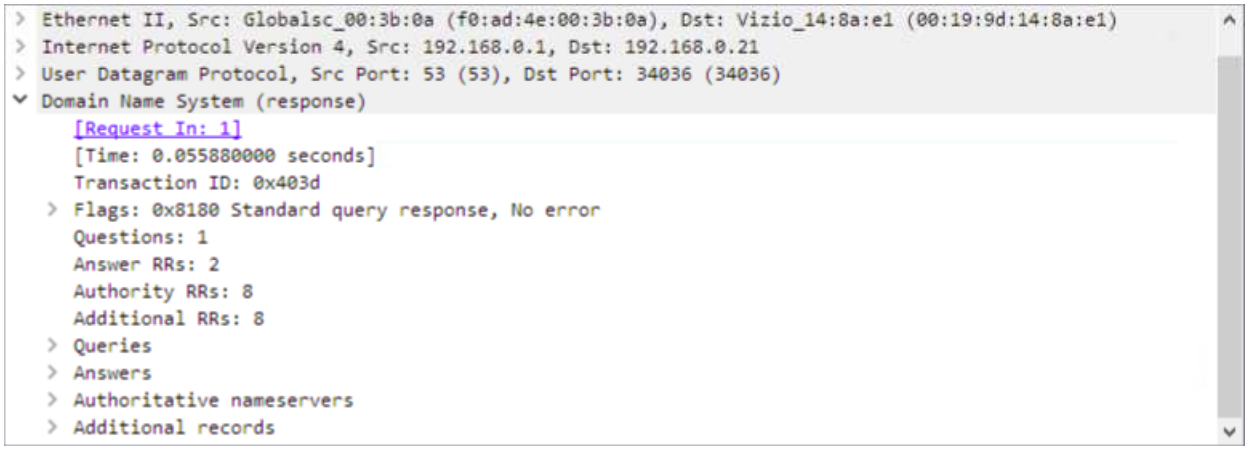
c) Packet List pane: The packet list pane displays all the packets in the current capture file. Each line in the packet list corresponds to one packet in the capture file. If you



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.21	192.168.0.1	DNS	84	Standard query 0x403d A moviecontrol.netflix.com
2	0.055880	192.168.0.1	192.168.0.21	DNS	479	Standard query response 0x403d A moviecontrol.netflix.com CNAME nccp-moviecontrol-fro
3	0.057690	192.168.0.21	50.17.249.22	TCP	74	37314→443 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491454310 TSecr=0 WS=
4	0.154716	50.17.249.22	192.168.0.21	TCP	74	443→37314 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=2102931926
5	0.155962	192.168.0.21	50.17.249.22	TCP	66	37314→443 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491454408 TSecr=2102931926
6	0.163169	192.168.0.21	50.17.249.22	TLSv1	187	Client Hello
7	0.250734	50.17.249.22	192.168.0.21	TCP	66	443→37314 [ACK] Seq=1 Ack=122 Win=5792 Len=0 TSval=2102931950 TSecr=491454416
8	0.252716	50.17.249.22	192.168.0.21	TLSv1	1514	Server Hello
9	0.253826	192.168.0.21	50.17.249.22	TCP	66	37314→443 [ACK] Seq=122 Ack=1449 Win=8768 Len=0 TSval=491454507 TSecr=2102931950
10	0.254730	50.17.249.22	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]
11	0.254778	50.17.249.22	192.168.0.21	TLSv1	349	Certificate
12	0.255853	192.168.0.21	50.17.249.22	TCP	66	37314→443 [ACK] Seq=122 Ack=2897 Win=11648 Len=0 TSval=491454509 TSecr=2102931950
13	0.256102	192.168.0.21	50.17.249.22	TCP	66	37314→443 [ACK] Seq=122 Ack=3180 Win=14528 Len=0 TSval=491454509 TSecr=2102931950
14	0.319870	192.168.0.21	50.17.249.22	TLSv1	264	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
15	0.411795	50.17.249.22	192.168.0.21	TLSv1	125	Change Cipher Spec, Encrypted Handshake Message

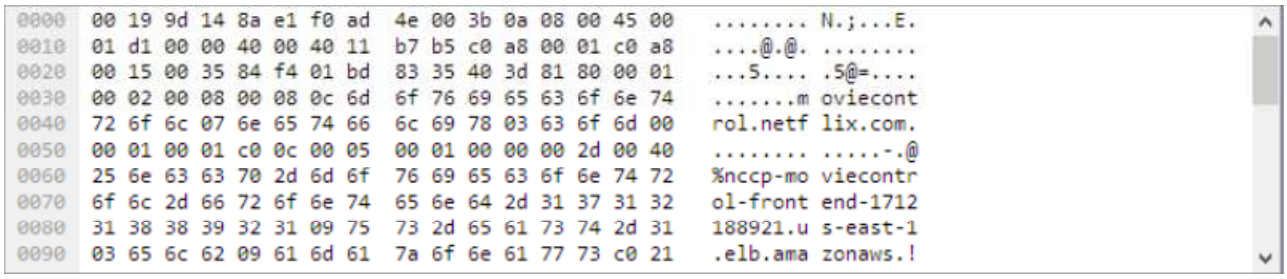
select a line in this pane, more details will be displayed in the “Packet Details” and “Packet Bytes” panes.

d) **Packet Details Pane:** The packet details pane shows the current packet (selected in the “Packet List” pane) in a more detailed form.



This pane shows the protocols and protocol fields of the packet selected in the “Packet List” pane. The protocols and fields of the packet are shown in a tree which can be expanded and collapsed.

e) **Packet Bytes Pane:** The packet bytes pane shows the data of the current packet (selected in the “Packet List” pane) in a hexdump style.



The “Packet Bytes” pane shows a canonical hex dump of the packet data. Each line contains the data offset, sixteen hexadecimal bytes, and sixteen ASCII bytes. Non-printalbe bytes are replaced with a period (“.”).

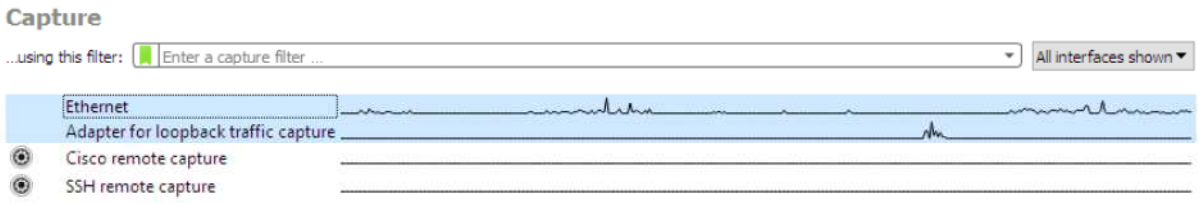
3. Capturing Live network Data

a. Introduction: Capturing live network data is one of the major features of Wireshark. The Wireshark capture engine provides the following features:

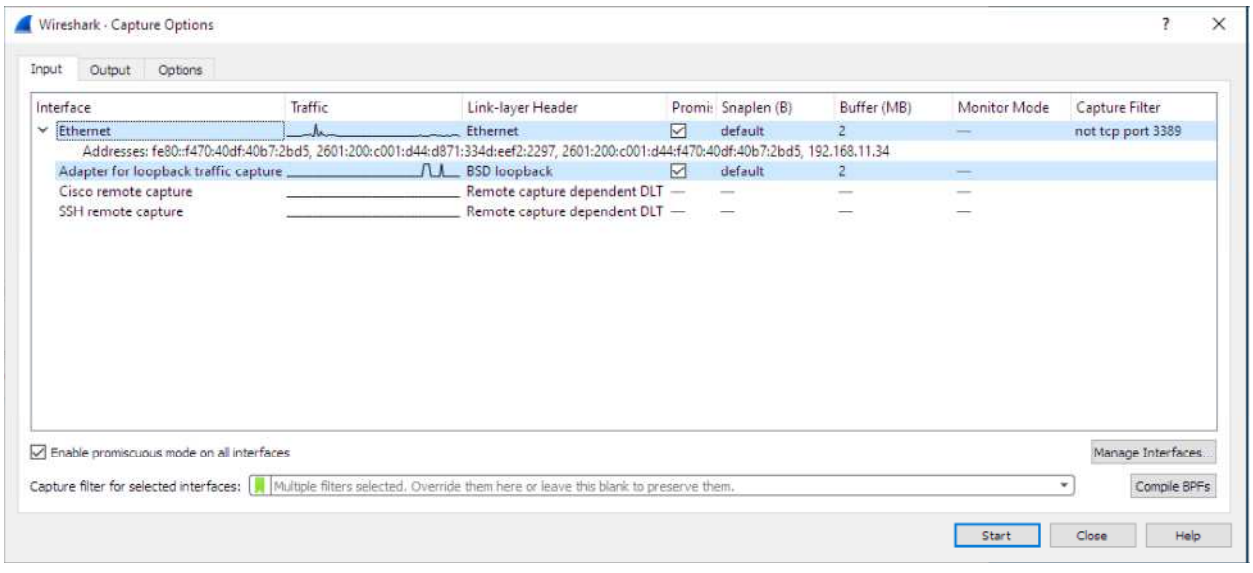
- Capture from different kinds of network hardware such as Ethernet or 802.11.
- Simultaneously capture from multiple network interfaces.
- Stop the capture on different triggers such as the amount of captured data, elapsed time, or the number of packets.
- Simultaneously show decoded packets while Wireshark is capturing.
- Filter packets, reducing the amount of data to be captured.
- Save packets in multiple files while doing a long term capture, optionally rotating through a fixed number of files (a "ringbuffer").

b. Capture types: Capture can be performed by two ways:

i. **The "Capture" Section Of The Welcome Screen:** When you open Wireshark without starting a capture or opening a capture file it will display the "Welcome Screen," which lists any recently opened capture files and available capture interfaces. Network activity for each interface will be shown in a sparkline next to the interface name. It is possible to select more than one interface and capture from them simultaneously.

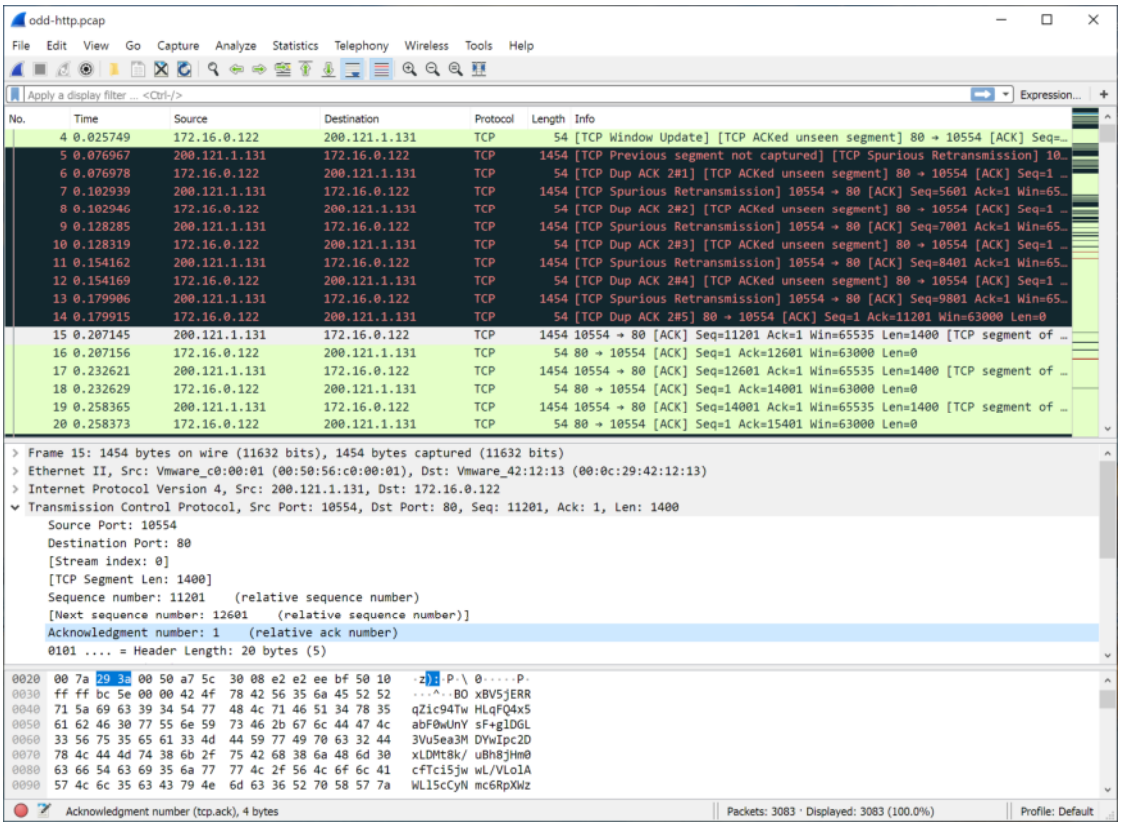


ii. **The "Capture Options" Dialog Box:** When you select **Capture › Options…** (or use the corresponding item in the main toolbar),Wireshark pops up the "Capture Options" dialog box as shown in The "Capture Options" input tab.

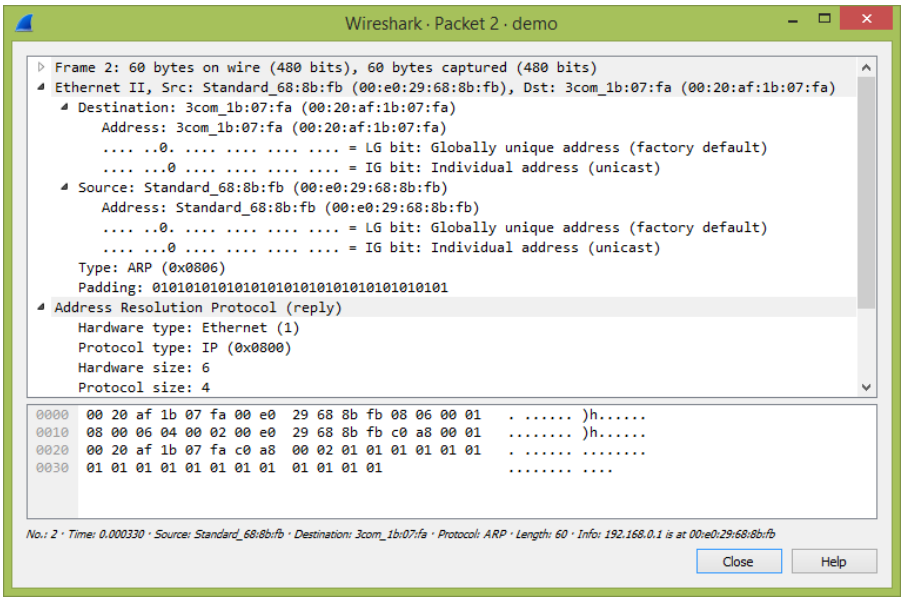


4. Working with Captured Packets

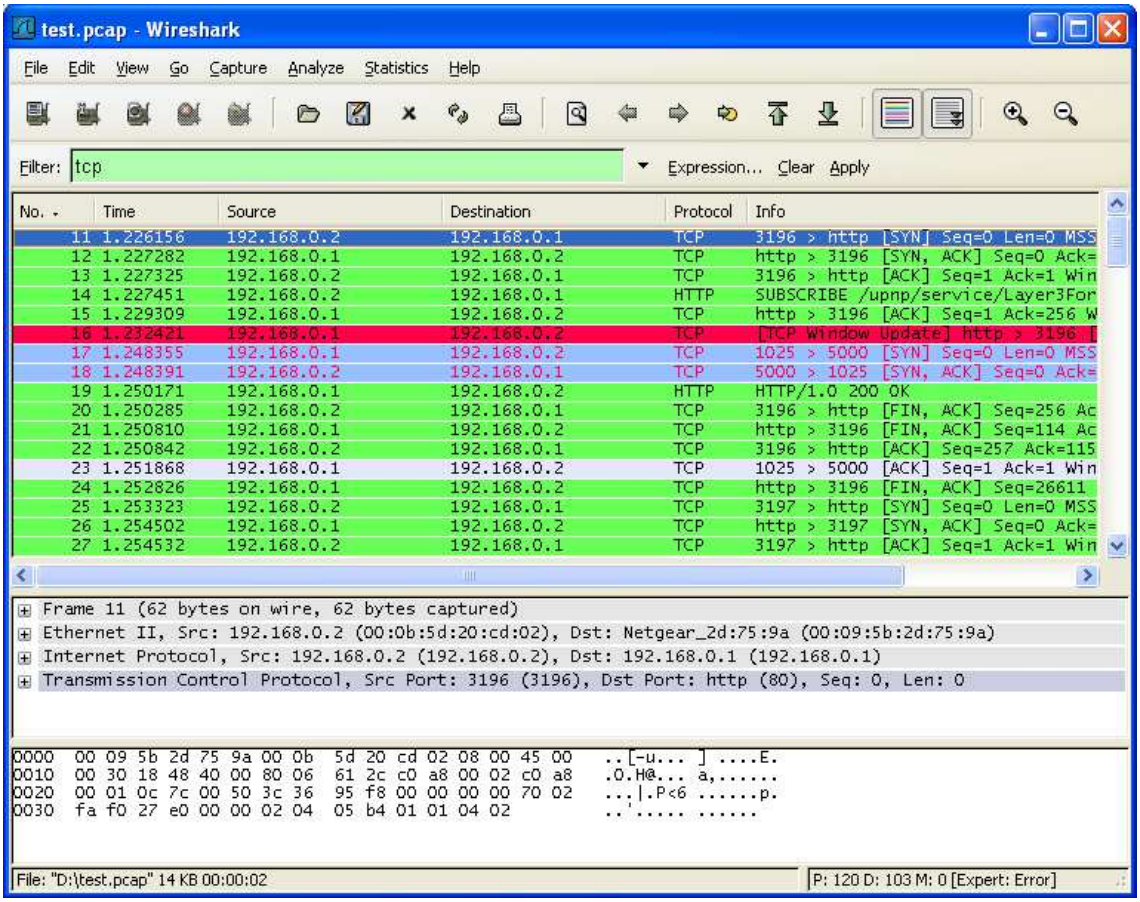
a. **Viewing Packets we've captured:** Once you have captured some packets or you have opened a previously saved capture file, you can view the packets that are displayed in the packet list pane by simply clicking on a packet in the packet list pane, which will bring up the selected packet in the tree view and byte view panes.



In addition we can view individual packets in a separate window as shown in viewing a packet in a separate window by selecting the packet in which you are interested in the packet list pane and selecting **View › Show Packet in New Window**. This allows us to easily compare two or more packets, even across multiple files.

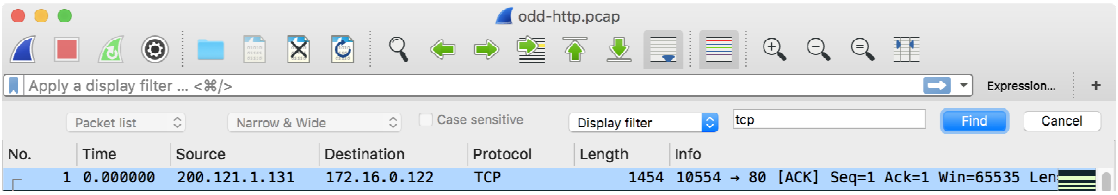


b. Filtering Packets while viewing: Wireshark has two filtering languages: *capture filters* and *display filters*. *Capture filters* are used for filtering when capturing packets and are discussed in Filtering while capturing.



c. Finding Packets: We can easily find packets once we have captured some packets or have read in a previously saved capture file. Simply select **Edit › Find Packet**… in the main menu. Wireshark will open a toolbar between the main toolbar and the packet list shown in The "Find Packet" toolbar.

The "Find Packet" Toolbar



We can search using the following criteria:

Display filter

Enter a display filter string into the text entry field and click the **[Find]** button. + For example, to find the three way handshake for a connection from host 192.168.0.1, use the following filter string:

```
ip.src==192.168.0.1 and tcp.flags.syn==1
```

The value to be found will be syntax checked while you type it in. If the syntax check of your value succeeds, the background of the entry field will turn green, if it fails, it will turn red. For more details see Filtering Packets While Viewing

Hexadecimal Value

Search for a specific byte sequence in the packet data. For example, use “ef:bb:bf” to find the next packet that contains the UTF-8 byte order mark.

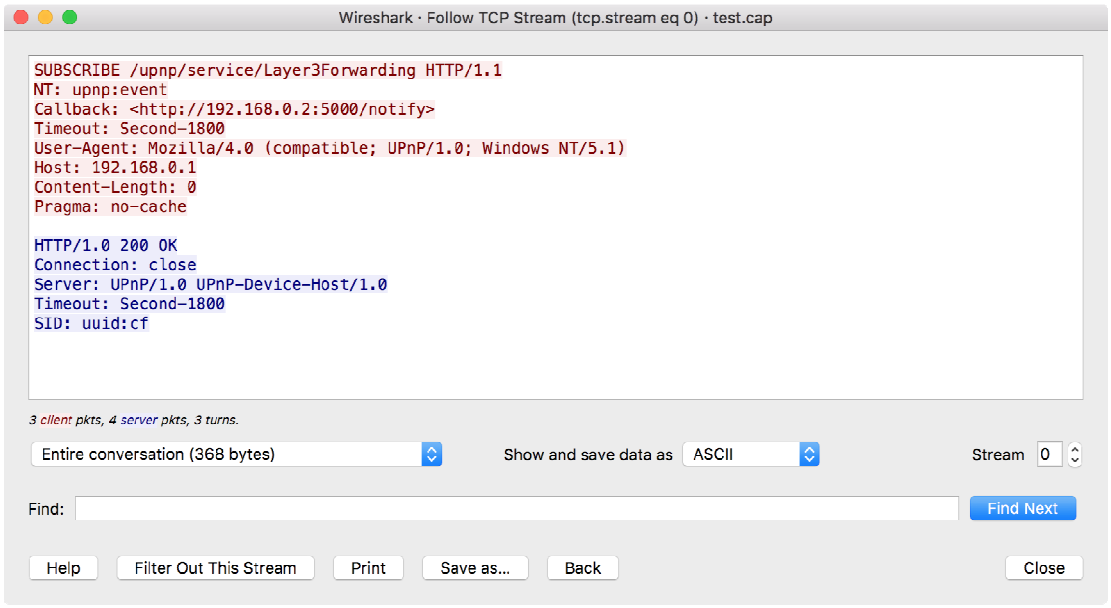
String

Find a string in the packet data, with various options.

5. Following Protocol Streams

It can be very helpful to see a protocol in the way that the application layer sees it. Perhaps we are looking for passwords in a Telnet stream, or we are trying to make sense of a data stream. Maybe we just need a display filter to show only the packets in a TLS or SSL stream. If so, Wireshark’s ability to follow protocol streams will be useful to us.

To filter to a particular stream, select a TCP, UDP, TLS, or HTTP packet in the packet list of the stream/connection we are interested in and then select the menu item **Analyze › Follow TCP Stream** (or use the context menu in the packet list). Wireshark will set an appropriate display filter and display a dialog box with the data from the stream laid out, as shown in The “Follow TCP Stream” dialog box.



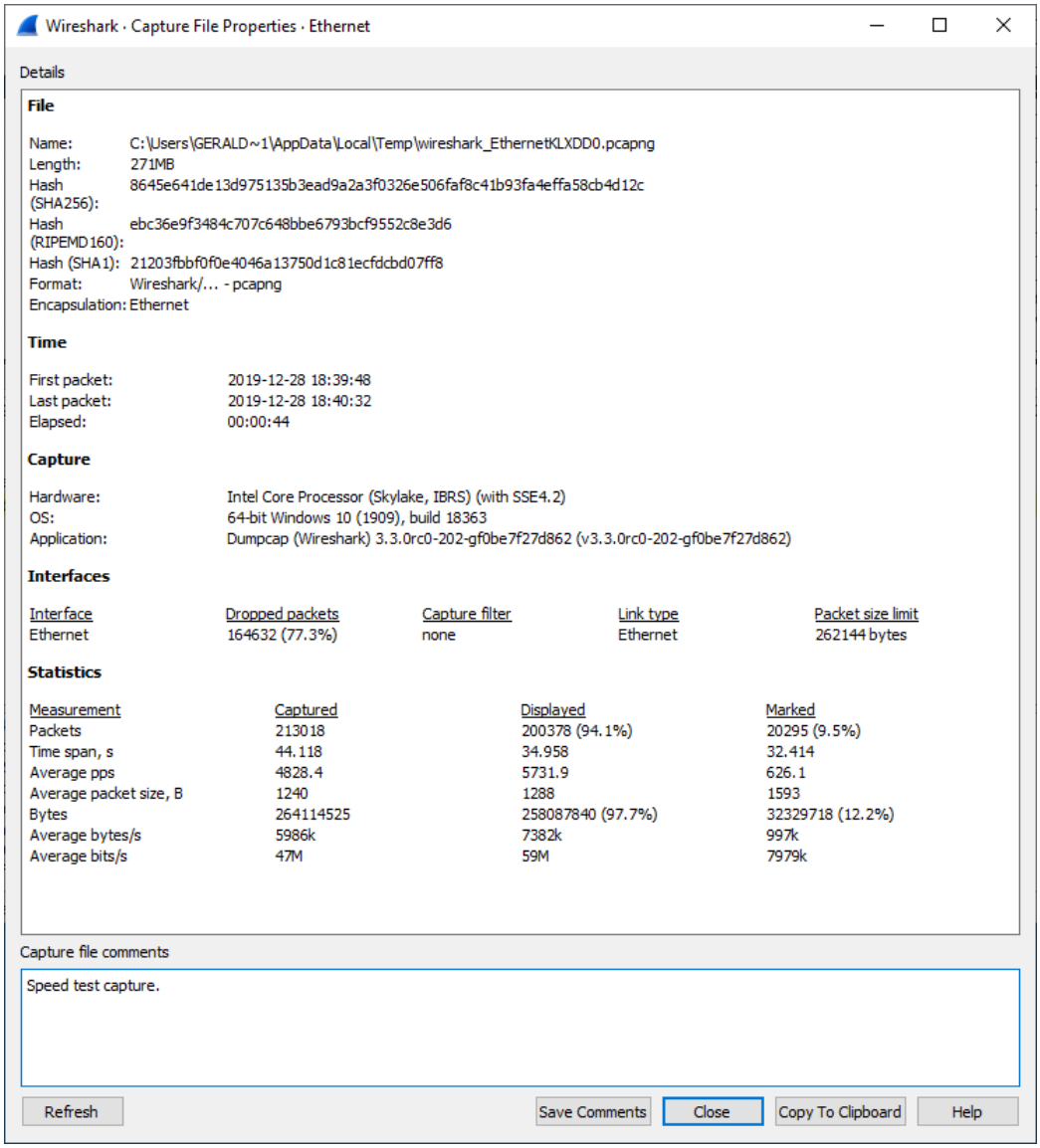
6. Statistics

a. **Introduction:** Wireshark provides a wide range of network statistics which can be accessed via the Statistics menu. These statistics range from general information about the loaded capture file (like the number of captured packets), to statistics about specific protocols (e.g. statistics about the number of HTTP requests and responses captured).

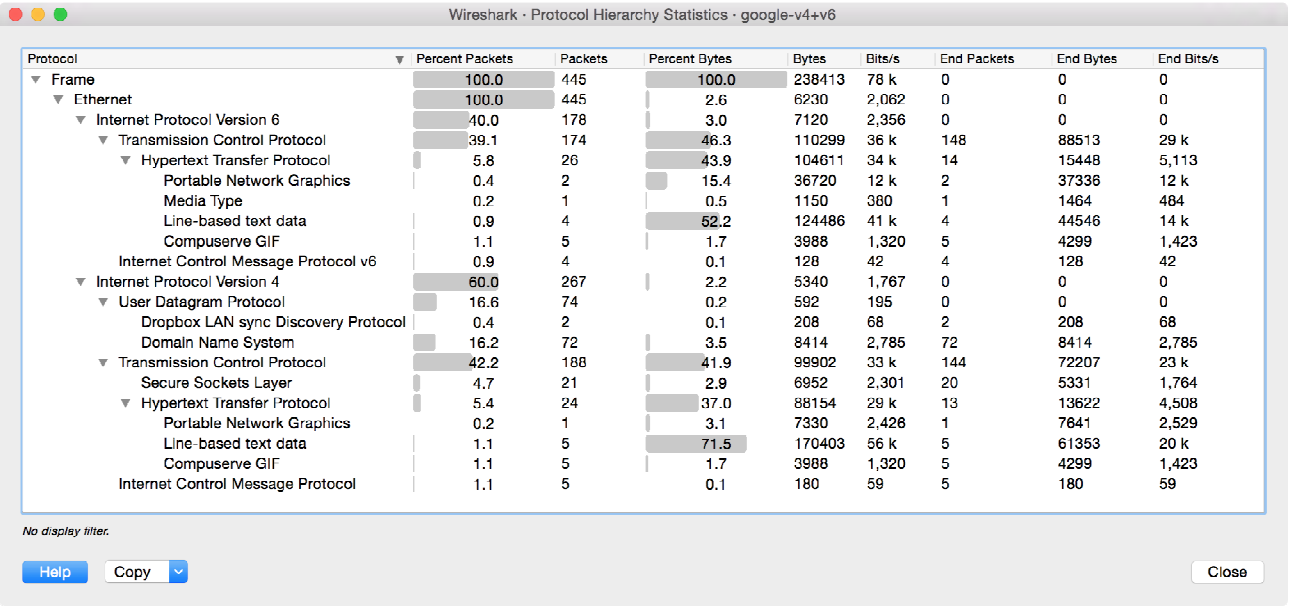
General statistics

- **Capture File Properties** about the capturefile.
- **Protocol Hierarchy** of the captured packets.
- **Conversations** e.g. traffic between specific IP addresses.
- **Endpoints** e.g. traffic to and from an IP addresses.
- **I/O Graphs** visualizing the number of packets (or similar) in time.

b. **The "Capture File Properties" Dialog**: General information about the current capture file.



c. **The "Protocol Hierarchy" Window:** The protocol hierarchy of the captured packets.



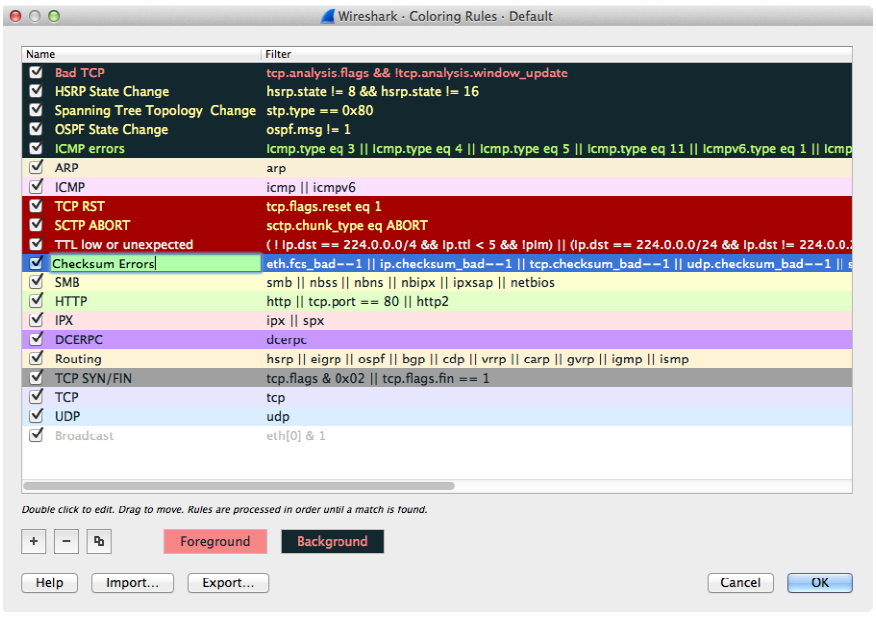
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	445	100.0	238413	78 k	0	0	0
Ethernet	100.0	445	2.6	6230	2,062	0	0	0
Internet Protocol Version 6	40.0	178	3.0	7120	2,356	0	0	0
Transmission Control Protocol	39.1	174	46.3	110299	36 k	148	88513	29 k
Hypertext Transfer Protocol	5.8	26	43.9	104611	34 k	14	15448	5,113
Portable Network Graphics	0.4	2	15.4	36720	12 k	2	37336	12 k
Media Type	0.2	1	0.5	1150	380	1	1464	484
Line-based text data	0.9	4	52.2	124486	41 k	4	44546	14 k
Compuserve GIF	1.1	5	1.7	3988	1,320	5	4299	1,423
Internet Control Message Protocol v6	0.9	4	0.1	128	42	4	128	42
Internet Protocol Version 4	60.0	267	2.2	5340	1,767	0	0	0
User Datagram Protocol	16.6	74	0.2	592	195	0	0	0
Dropbox LAN sync Discovery Protocol	0.4	2	0.1	208	68	2	208	68
Domain Name System	16.2	72	3.5	8414	2,785	72	8414	2,785
Transmission Control Protocol	42.2	188	41.9	99902	33 k	144	72207	23 k
Secure Sockets Layer	4.7	21	2.9	6952	2,301	20	5331	1,764
Hypertext Transfer Protocol	5.4	24	37.0	88154	29 k	13	13622	4,508
Portable Network Graphics	0.2	1	3.1	7330	2,426	1	7841	2,529
Line-based text data	1.1	5	71.5	170403	56 k	5	61353	20 k
Compuserve GIF	1.1	5	1.7	3988	1,320	5	4299	1,423
Internet Control Message Protocol	1.1	5	0.1	180	59	5	180	59

This is a tree of all the protocols in the capture. Each row contains the statistical values of one protocol. Two of the columns (*Percent Packets* and *Percent Bytes*) serve double duty as bar graphs. If a display filter is set, it will be shown at the bottom.

7. Customizing Wireshark

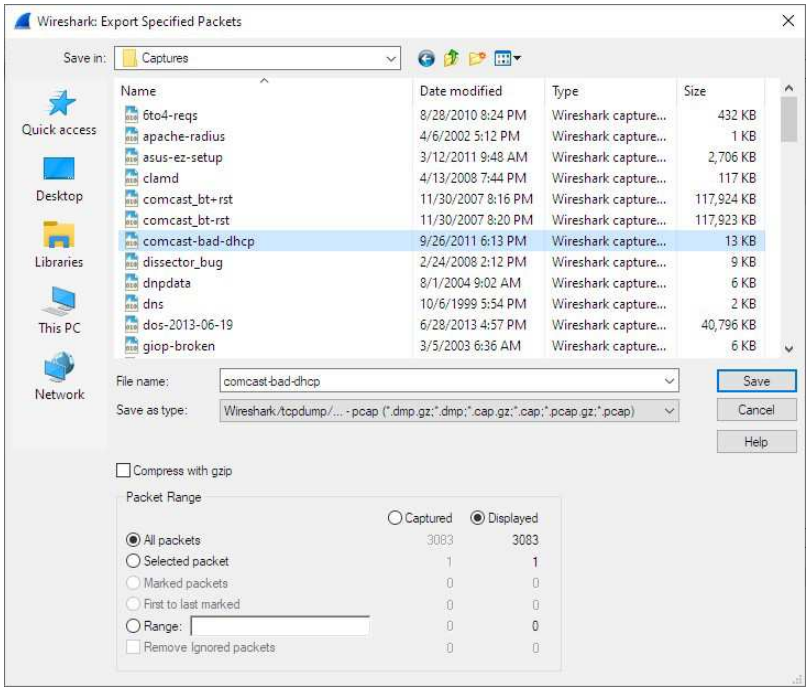
a. **Packet Colorization:** A very useful mechanism available in Wireshark is packet colorization. You can set up Wireshark so that it will colorize packets according to a display filter. This allows you to emphasize the packets you might be interested in.

To permanently colorize packets, select **View › Coloring Rules…**. Wireshark will display the "Coloring Rules" dialog box as shown in the "Coloring Rules" dialog box.



b. Exporting Data: Wireshark provides a variety of options for exporting packet data.

The “Export Specified Packets” Dialog Box



This is similar to the “Save” dialog box, but it lets you save specific packets. This can be useful for trimming irrelevant or unwanted packets from a capture file.

EXPERIMENT 5

WIRESHARK CASE STUDIES

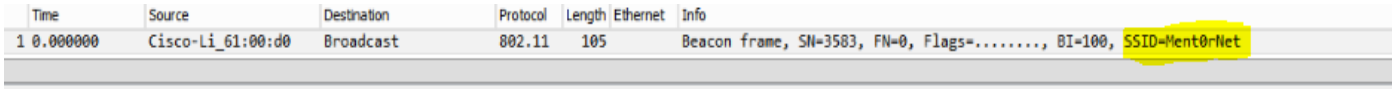
ACCESS POINT FORENSICS

1) Joe's WAP is beaconing. Based on the contents of the packet capture, What is:

a. The SSID of his access point?

- SSID = **Ment0rNet**

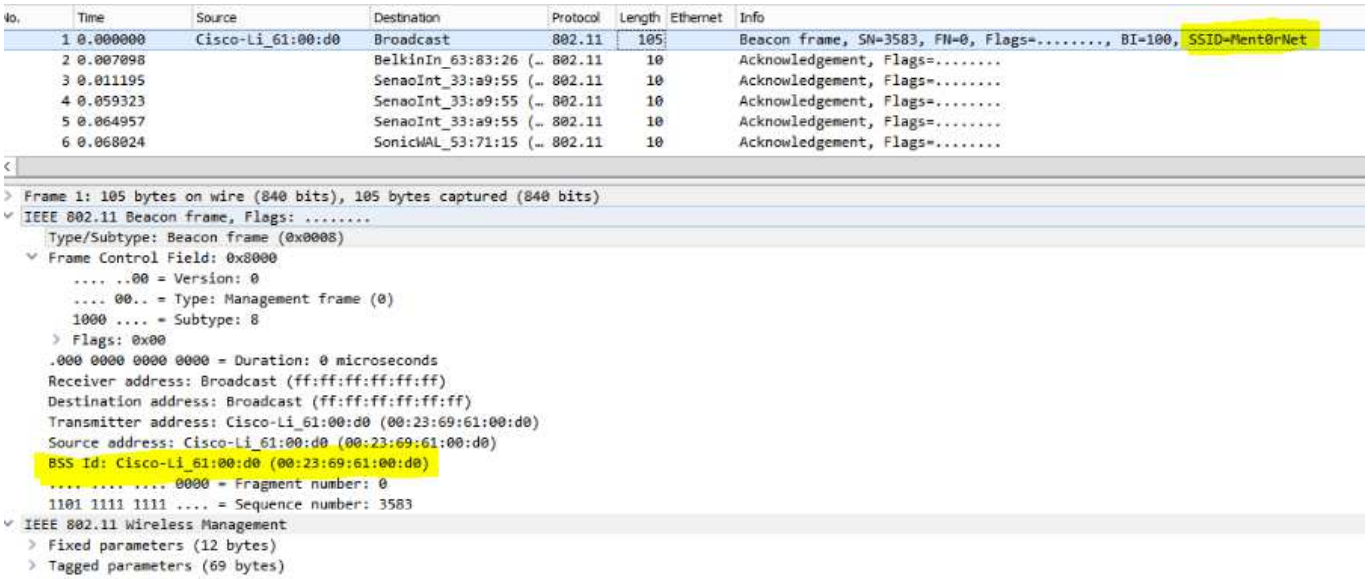
Steps: Open the access point forensics.pcap in the Wireshark and capture the packets and find for string ***Beacon*** in packet details and then analyze the Cisco packet.



b. The BSSID of his access point?

- BSSID = **Cisco-Li_61:00:d0 (00:23:69:61:00:d0)**

Steps: in the captured packets, inside the Frame section:-
Go to IEEE 802.11, by traversing down, we will get the BSSID:



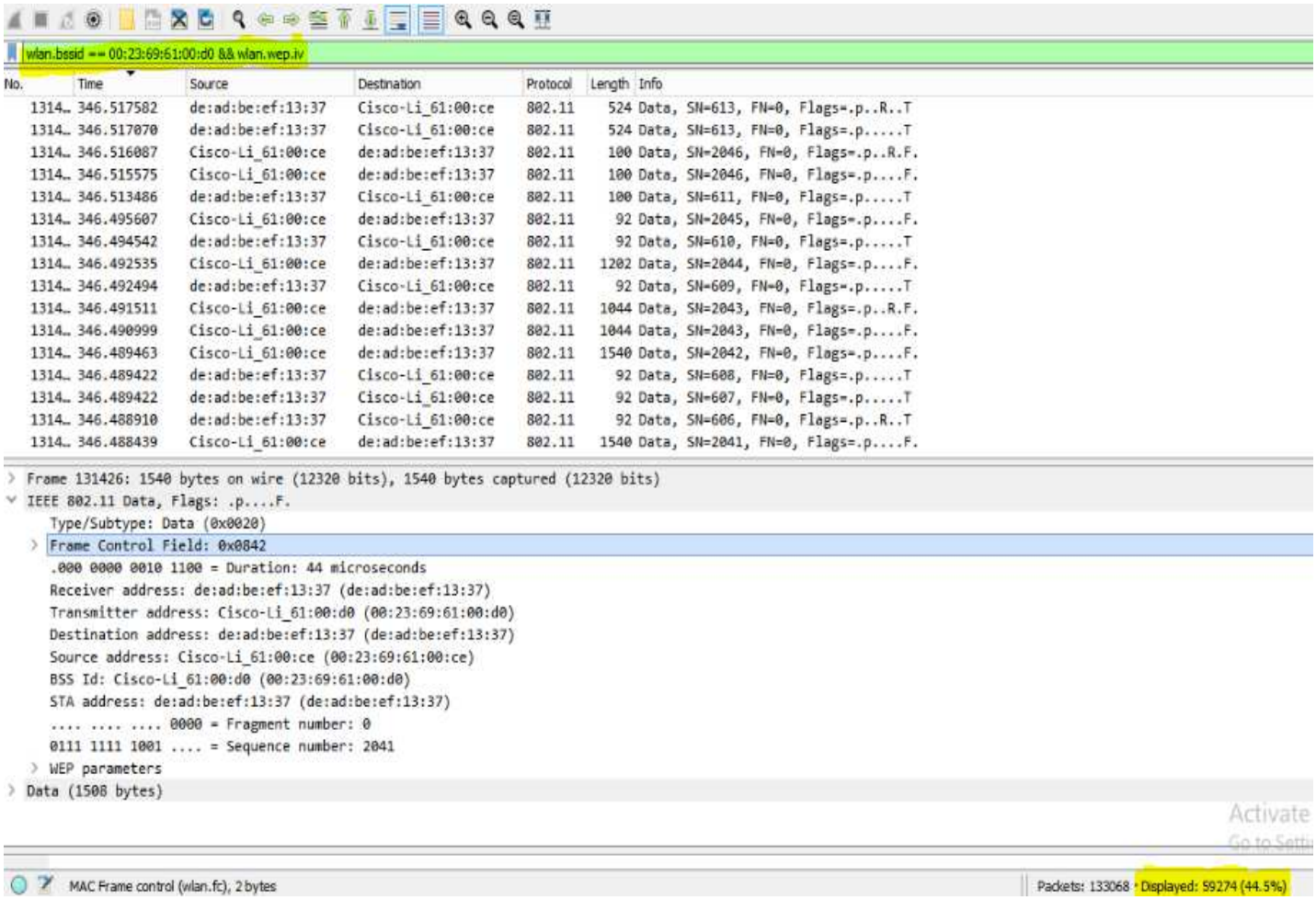
2) How long is the packet capture, from beginning to end (in SECONDS – please round to the nearest full second)?

The length of package captured was 133,068 with a maximum capture time in the last packet showing 413,576954. If rounded, the capture time is **414 seconds**

3) How many WEP-encrypted data frames are there total in the packet capture?

- Total WEP - encrypted data frames is **59274**

Steps: In the Wireshark, in the apply capture filter box, write the command: **wlan.bssid == 00:23:69:61:00:d0 && wlan.wep.iv** and in the bar present at the bottom of the Wireshark, it will be displayed:



4) How many *unique* WEP initialization vectors (IVs) are there TOTAL in the packet capture relating to Joe's access point?

- **29719**

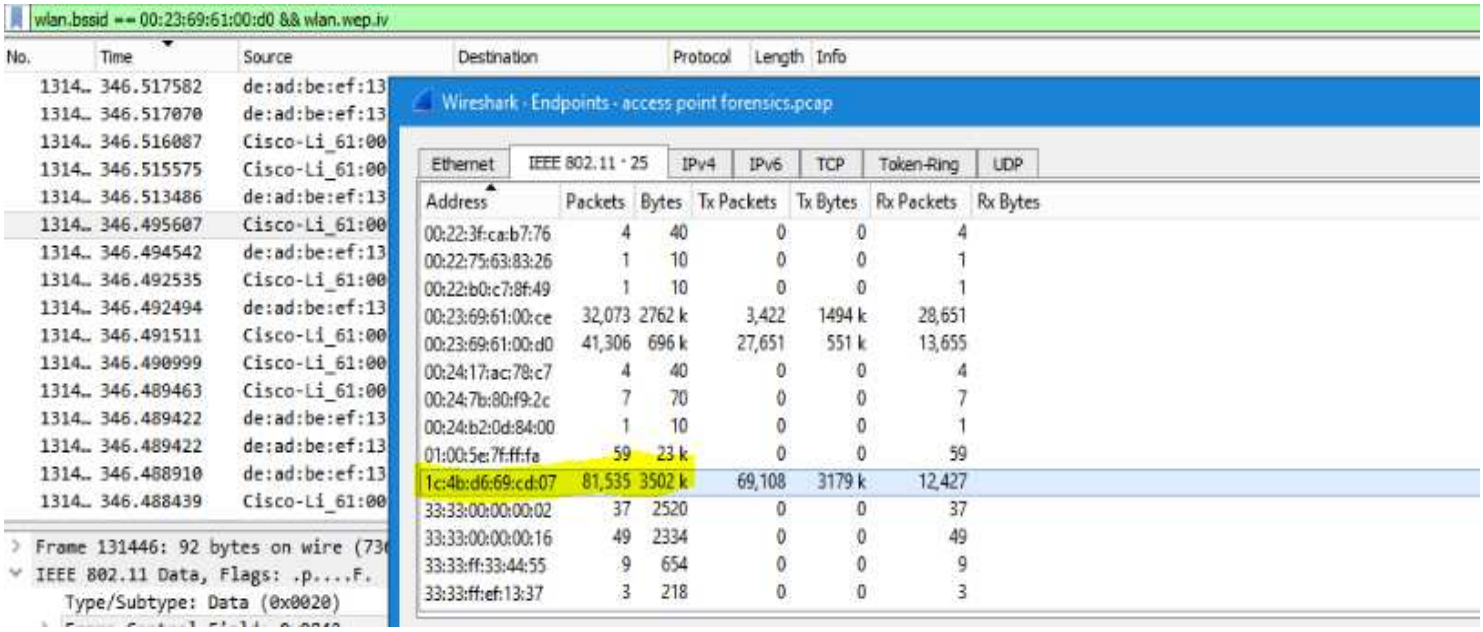
Steps: using terminal in the kali, write the commands:
tshark -r accesspointforensics.pcap -Y ' wlan.bssid == 00:23:69:61:00:d0 and wlan.wep.iv' -T fields -e wlan.wep.iv |sort -u| wc -l

5) What was the MAC address of the station executing the Layer 2 attacks?

- **1c:4b:d6:69:cd:07**

The one with the biggest value and as it is mentioned in the passage that Joey' s connection is dropping consistently.

Steps: In the statistics option, go to endpoint and select the Ethernet type to get the Mac address of the station executing the Layer 2 attacks.



6) How many *unique* IVs were generated (relating to Joe's access point):

a) By the attacker station?

14133

Steps: in the terminal, write the following commands:

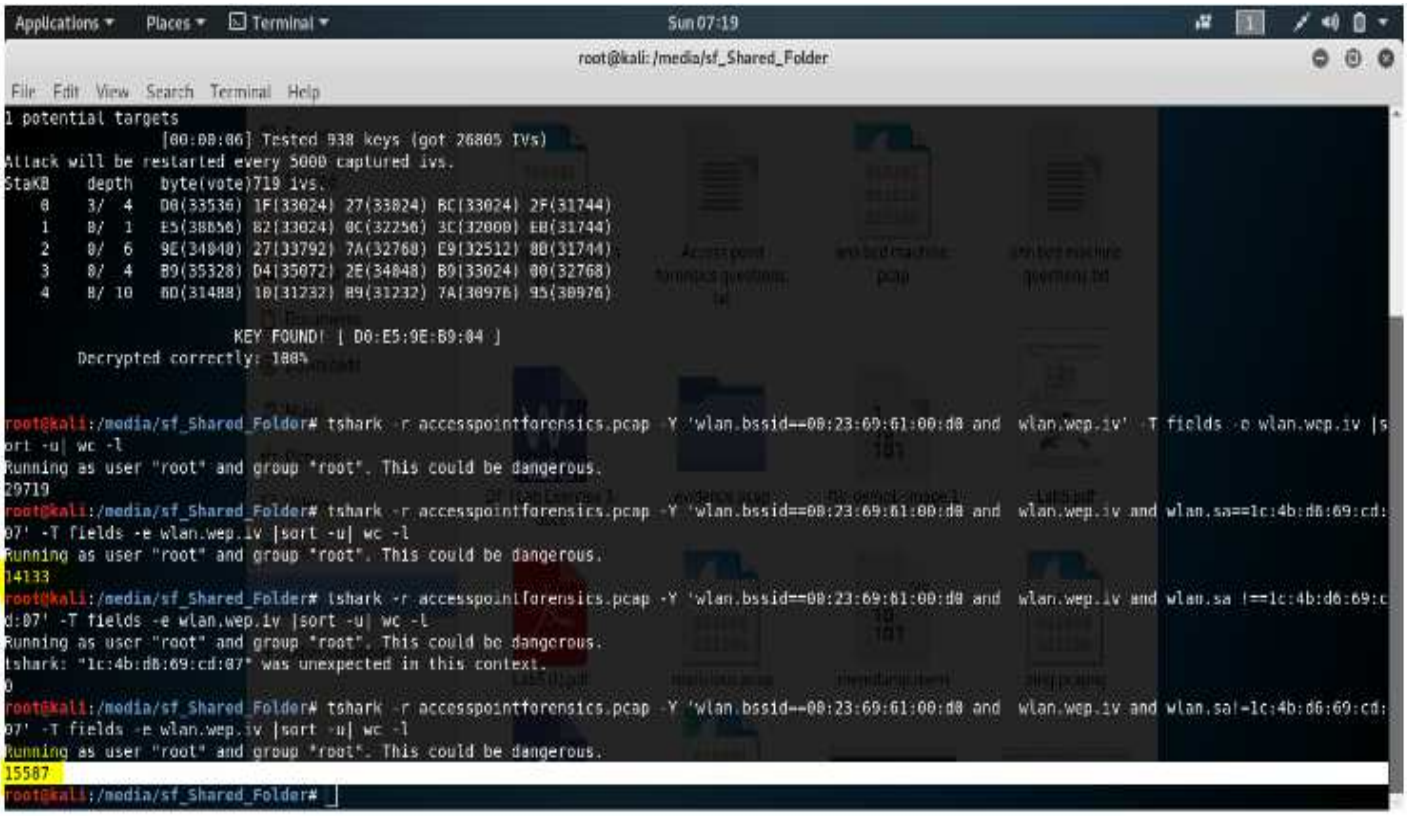
tshark -r wireshark.1.pcapng -Y 'wlan.bssid == 00:23:69:61:00:d0 and wlan.wep.iv and wlan.sa== 1c:4b:d6:69:cd:07' -T fields -e wlan.wep.iv |sort -u| wc-l

b) By all *other* stations combined? :

15587

Steps: In the terminal write the commands as:

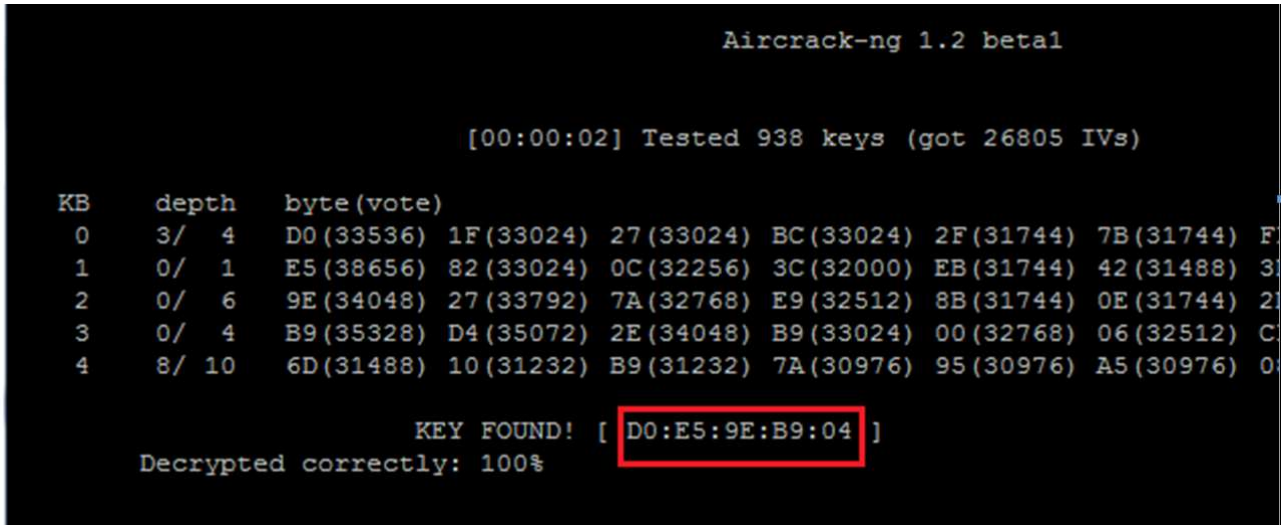
tshark -r wireshark.1.pcapng -Y 'wlan.bssid == 00:23:69:61:00:d0 and wlan.wep.iv and wlan.sa!= 1c:4b:d6:69:cd:07' -T fields -e wlan.wep.iv |sort -u| wc-l



7) What was the WEP key of Joe's WAP?

- D0:E5:9E:B9:04

Steps: write the command :
aircrack-ng accesspointforensics.pcap



ANN'S BED MACHINE

1. What is the name of Ann's IM buddy?

Buddy: **Sec558user1**

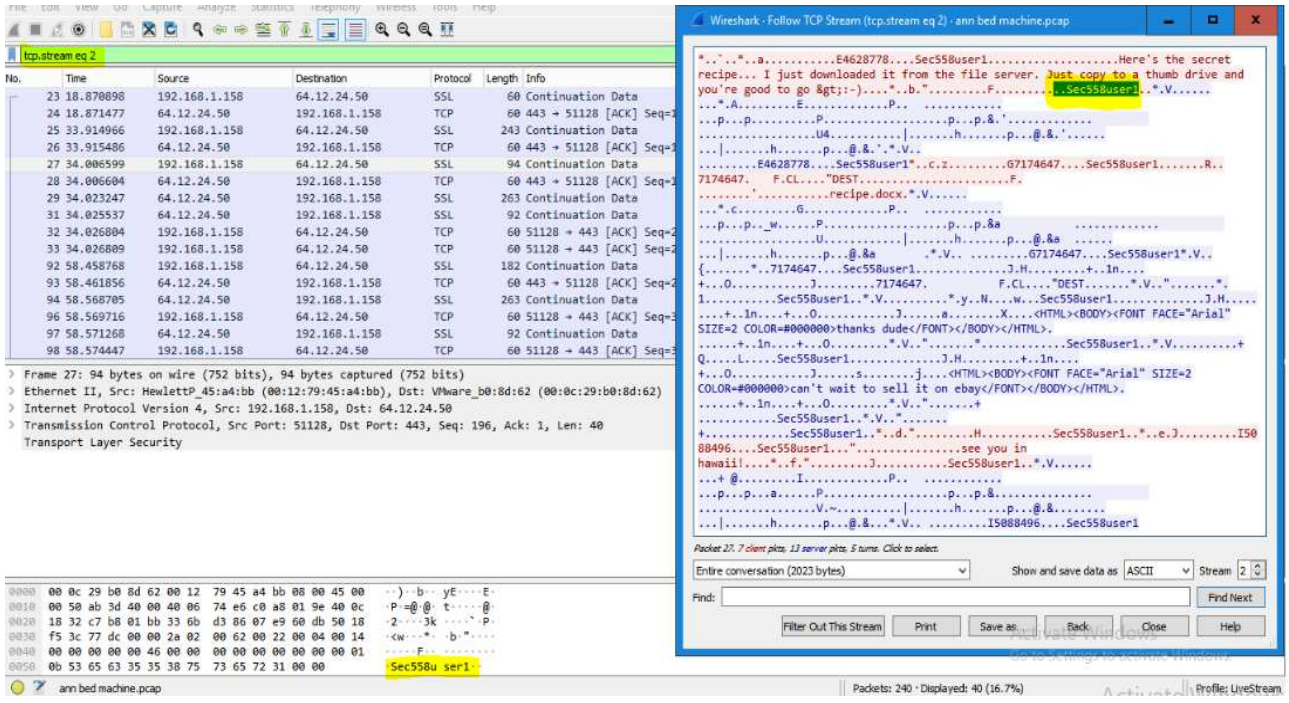
STEPS:

- In the apply filter option, apply filter *p-cap file with tcp.stream* eq 2.

It shows the packets in a session, and then we can sequentially analyze them as we increase the numbers.

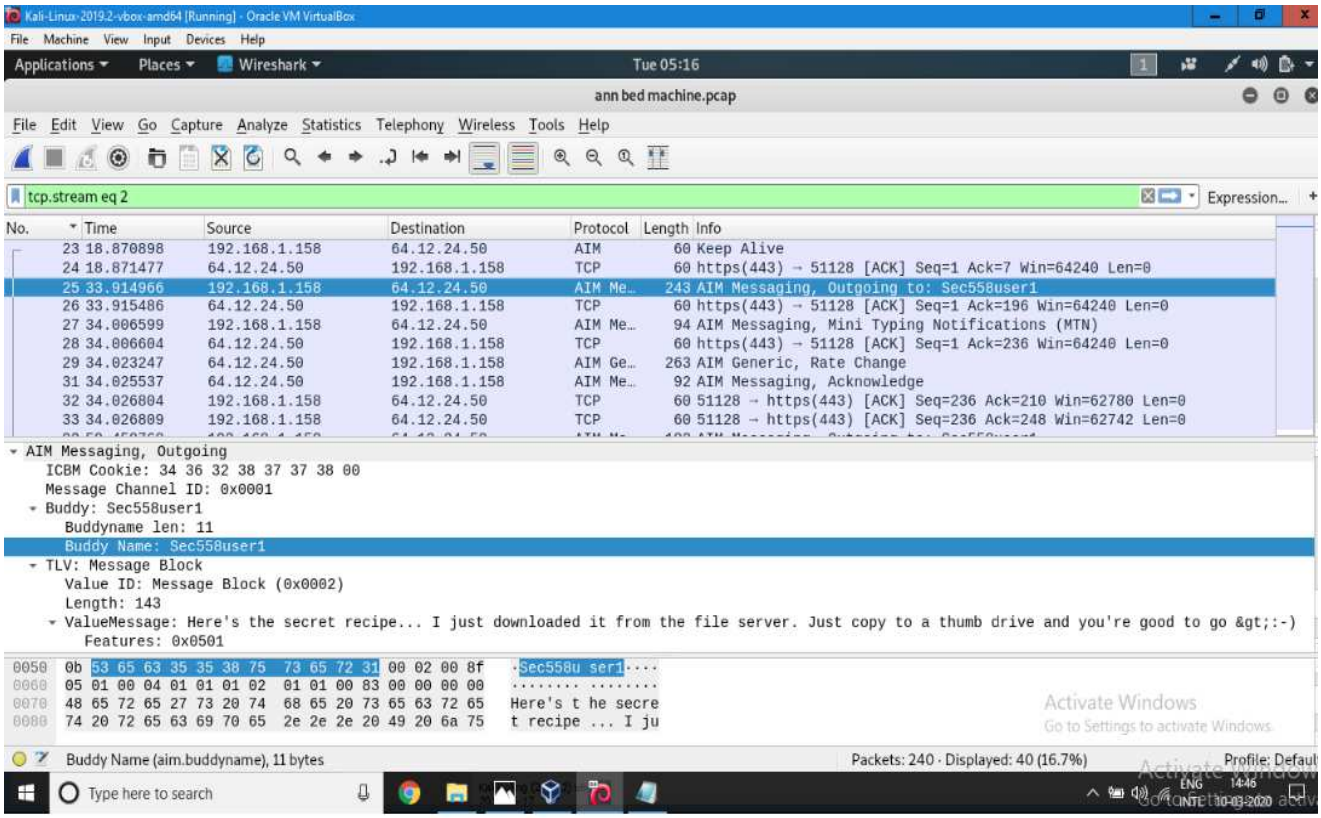
- Then we will see in the packet no. 21, 23, 27, 92 and few more showing the continuation of data.
- Now we will analyze any of them by clicking on follow stream and selecting the tcp stream.

The tcp stream will show the text as shown in screenshot:



- Now we will download and save the message of tcp stream in the kali.

- Then in the packet detail section, after selecting a particular packet,we will find the message in the **AIM MESSAGING** section and then we will be able to get the name of buddy name as Sec558user1.

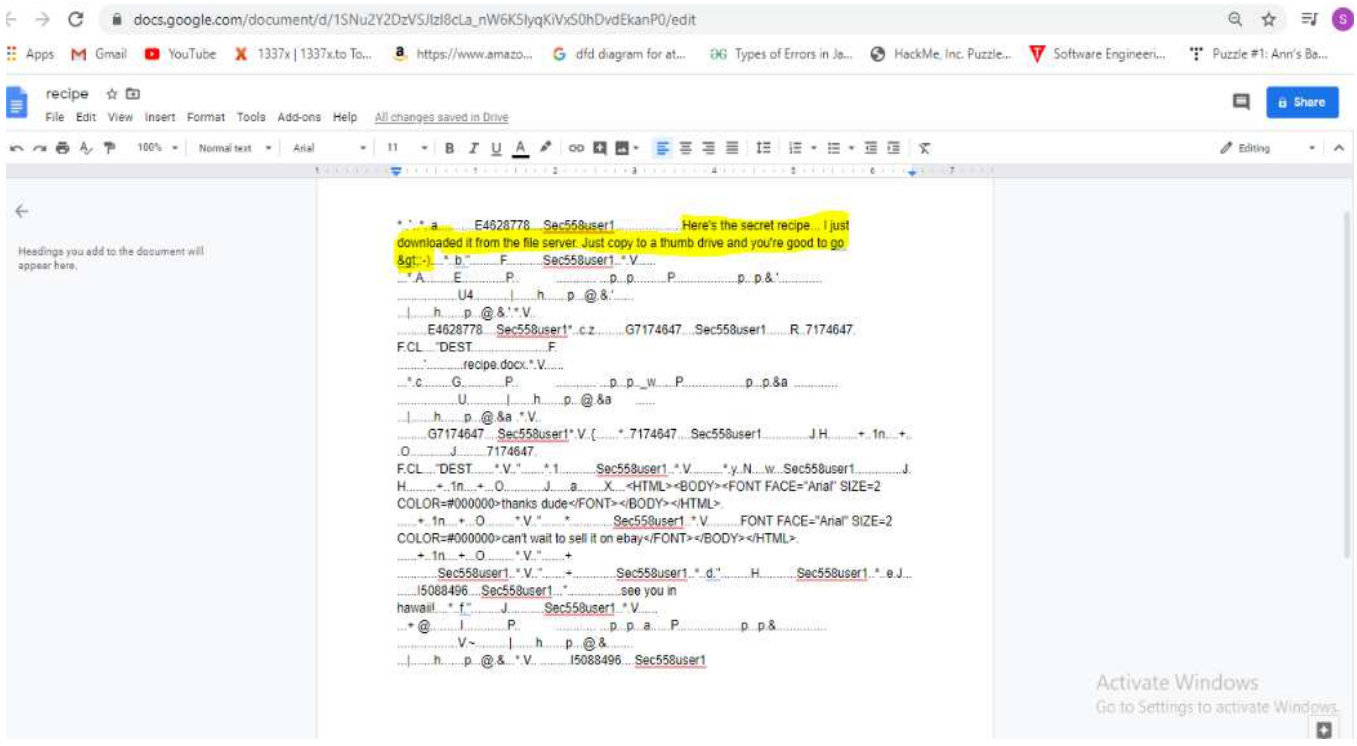


2. What was the first comment in the captured IM conversation?

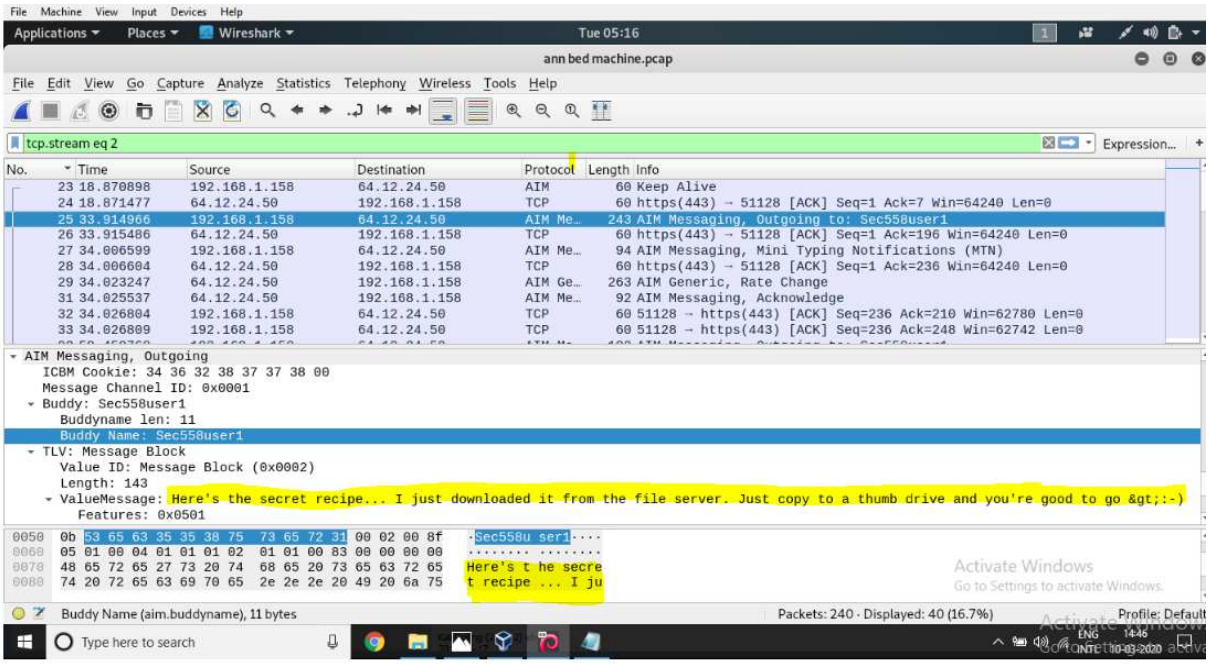
Value Message: **Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you're good to go >:-**

STEPS:

1. When we analyzed the packet 21 and opened the tcp stream, we were able to see the message as shown in the screenshot .Now we will download the message and again open the message in the wireshark.



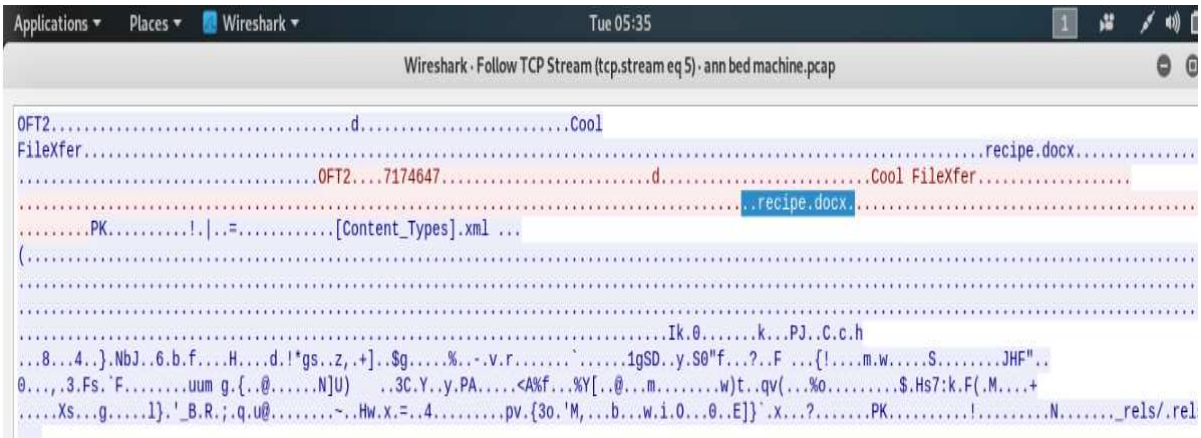
2. Opening the p-cap in the Wireshark. Here in the screenshot I have analyzed the packet 25, in the packet detail section, the highlighted part shows the value message which is the captured in conversation.



3. What is the name of the file Ann transferred?

- **RECEIPE.DOC**

Steps: To know the file name transferred, we will go in the statistics option and then in the conversation option we will select the TCP and various tcp packets transferred and port received and delivered. Information is present then we will analyse each packet by clicking on the follow stream and then we will get the name of file transferred. Then by knowing the port no and bytes option in the apply filter option we will apply tcp.port==5190 and then by searching in the string bytes, we will find the name as recipe.docx.



In the packet bytes panel section,we can see the name of the file trasferred as shown in the screenshot.

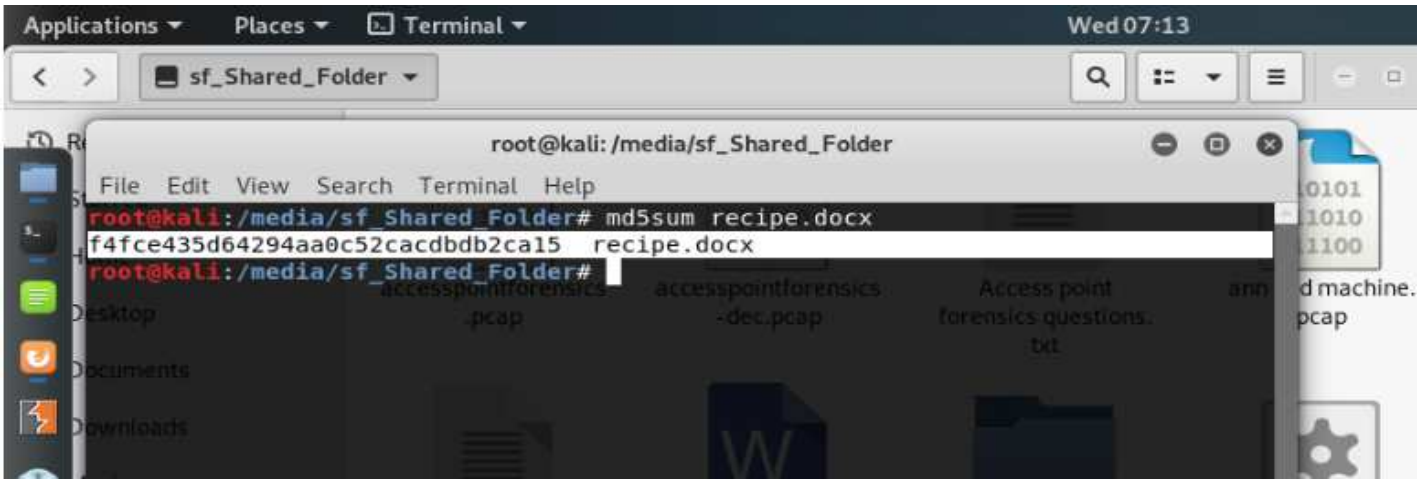
4. What was the MD5sum of the file?

```
   TCP payload (256 bytes)
   TCP segment data (256 bytes)
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00f0  00 00 00 00 00 00 72 65  63 69 70 65 2e 64 6f 63   ......re cipe.doc
0100  78 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   x....... ........
0110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0130  00 00 00 00 00 00                                 ......
```

The MD5sum of the file is shown:
Steps: We will download and save the recipe.docx and then in the terminal,write the commands :

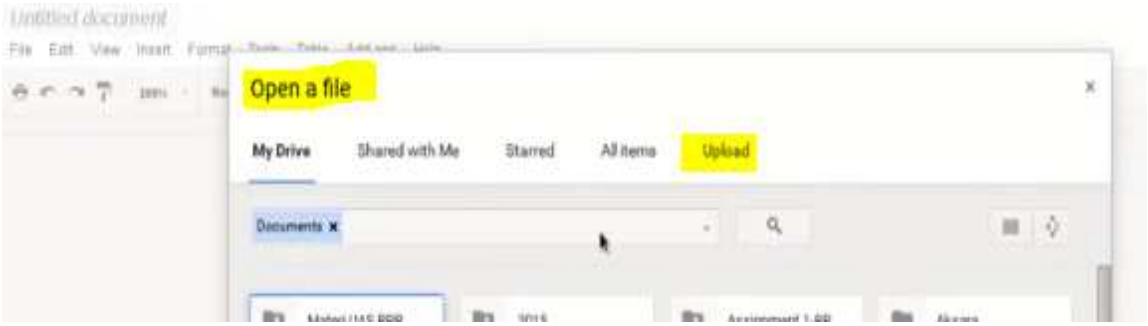
Md5sum recipe.docx

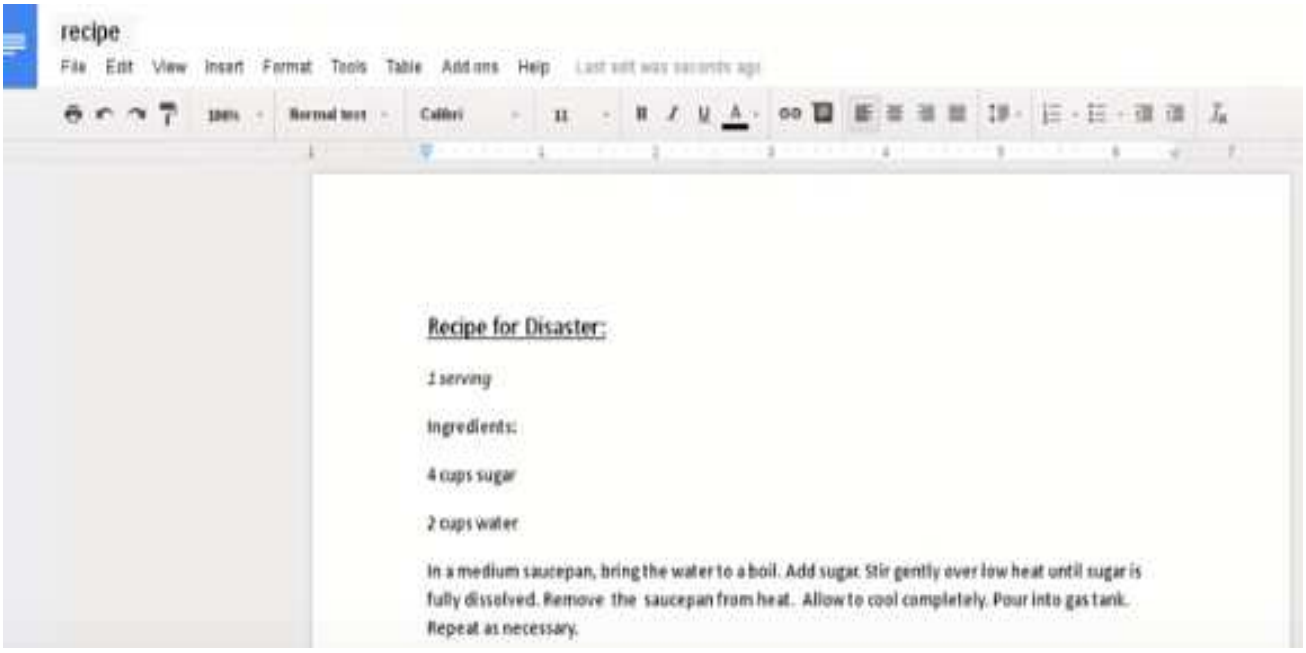
"f4fce435d64294aa0c52cacdbdb2ca15"



5. What is the secret recipe?

To get the secret recipe, open the recipe.docx in the untitiled document and upload it:
The result will be as shown in the figure:

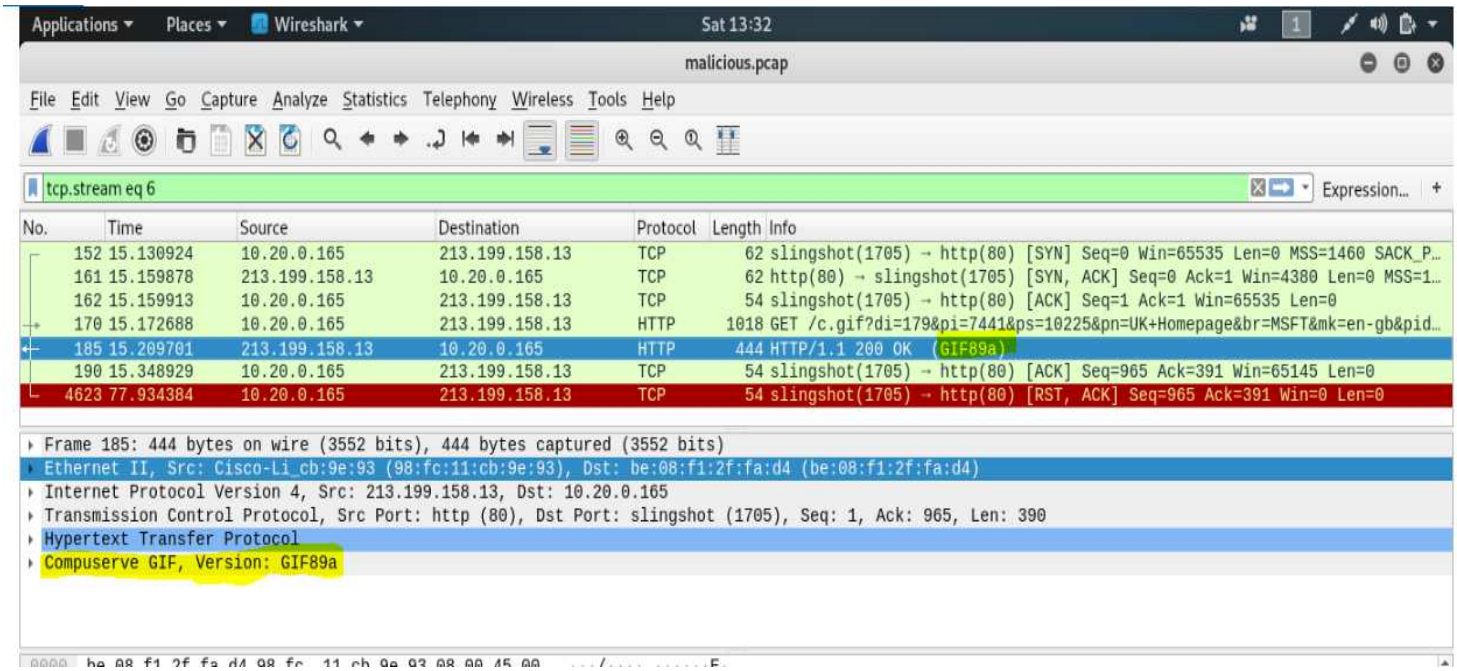

Untitled document
File Edit View Insert Format
Open a file
My Drive
Shared with Me
Starred
All items
Upload
Documents

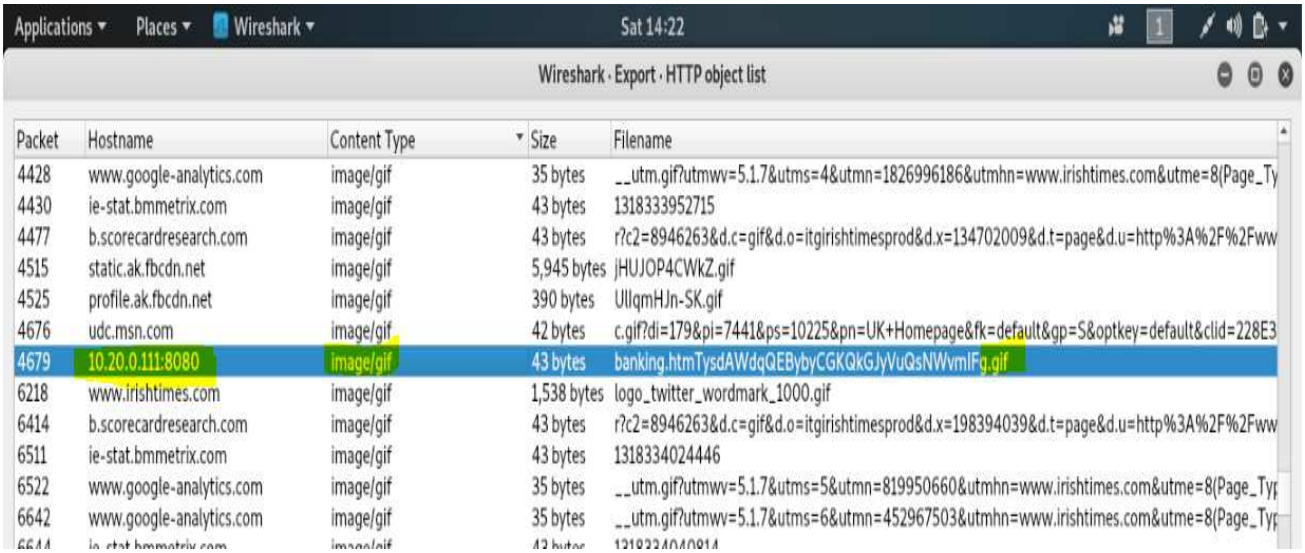

recipe
File Edit View Insert Format Tools Table Add-ons Help
Recipe for Disaster:
1 serving
Ingredients:
4 cups sugar
2 cups water
In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.

Malicious.pcap

1. **What was the complete URI of the original web request that led to the client being compromised?**
   - **http://10.20.0.111:8080/banking.htm**

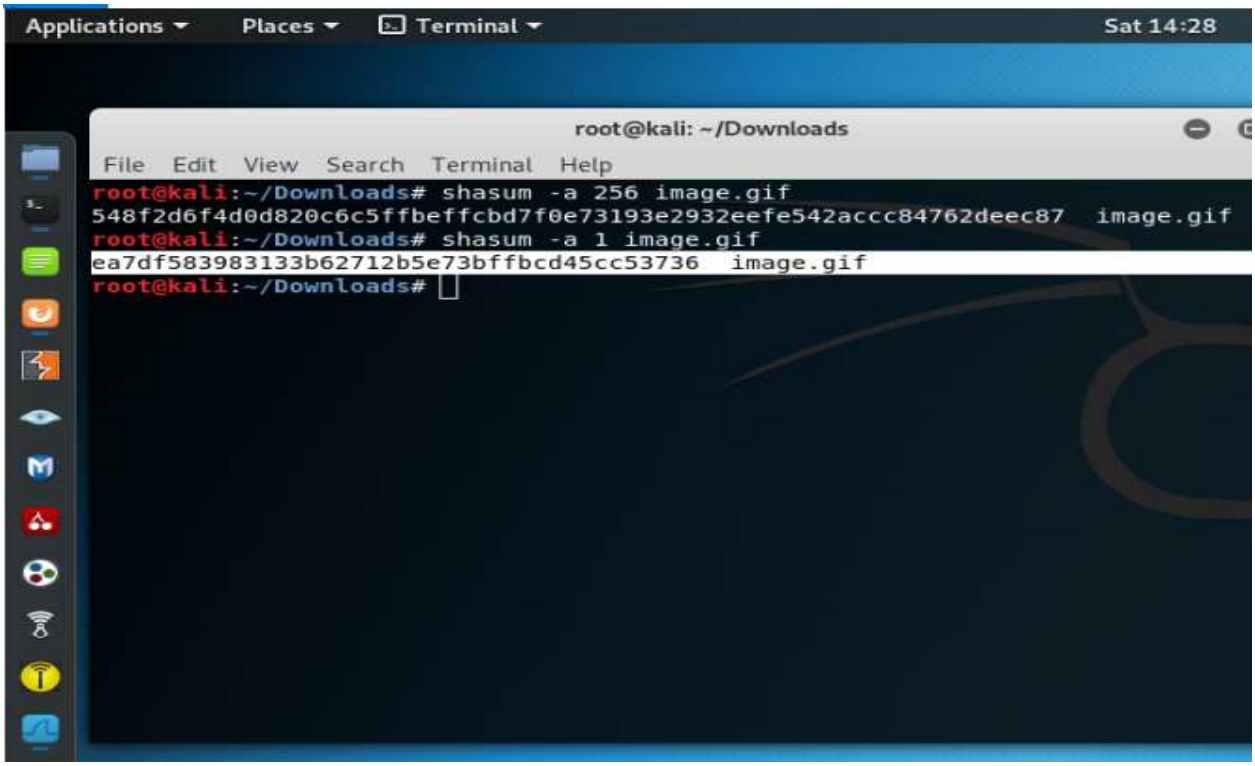
2. **What file type was requested in the final web request to the malicious server?**
   - **GIF**





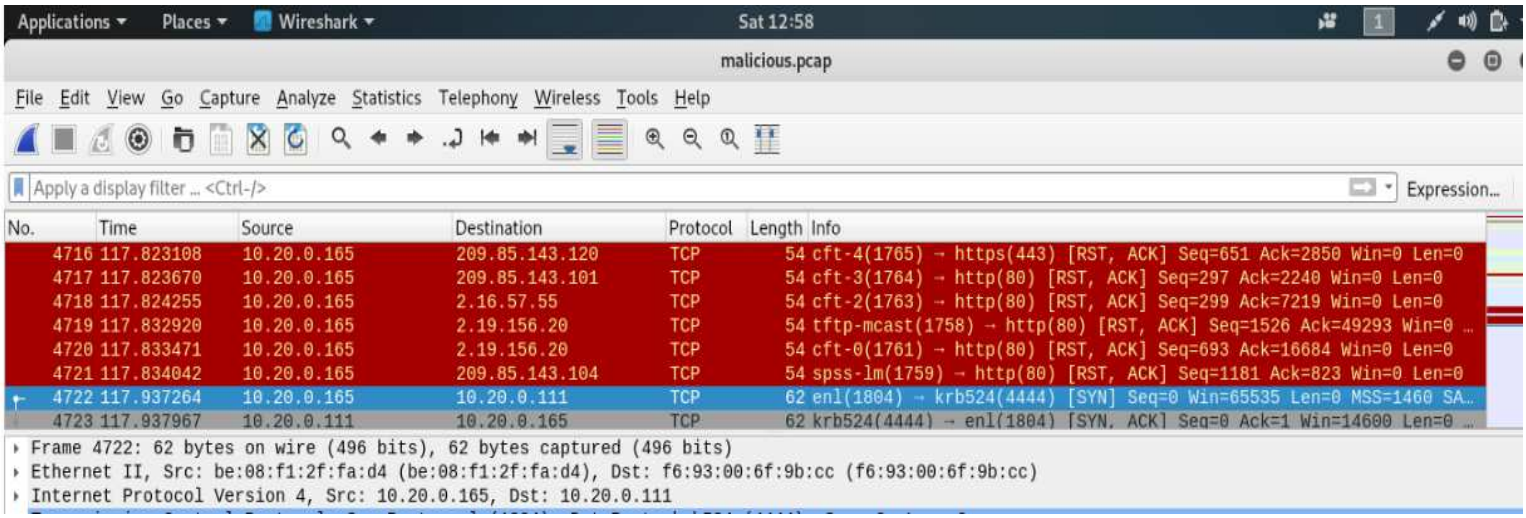
3. **What is the sha1 hash of the afore-mentioned file?**

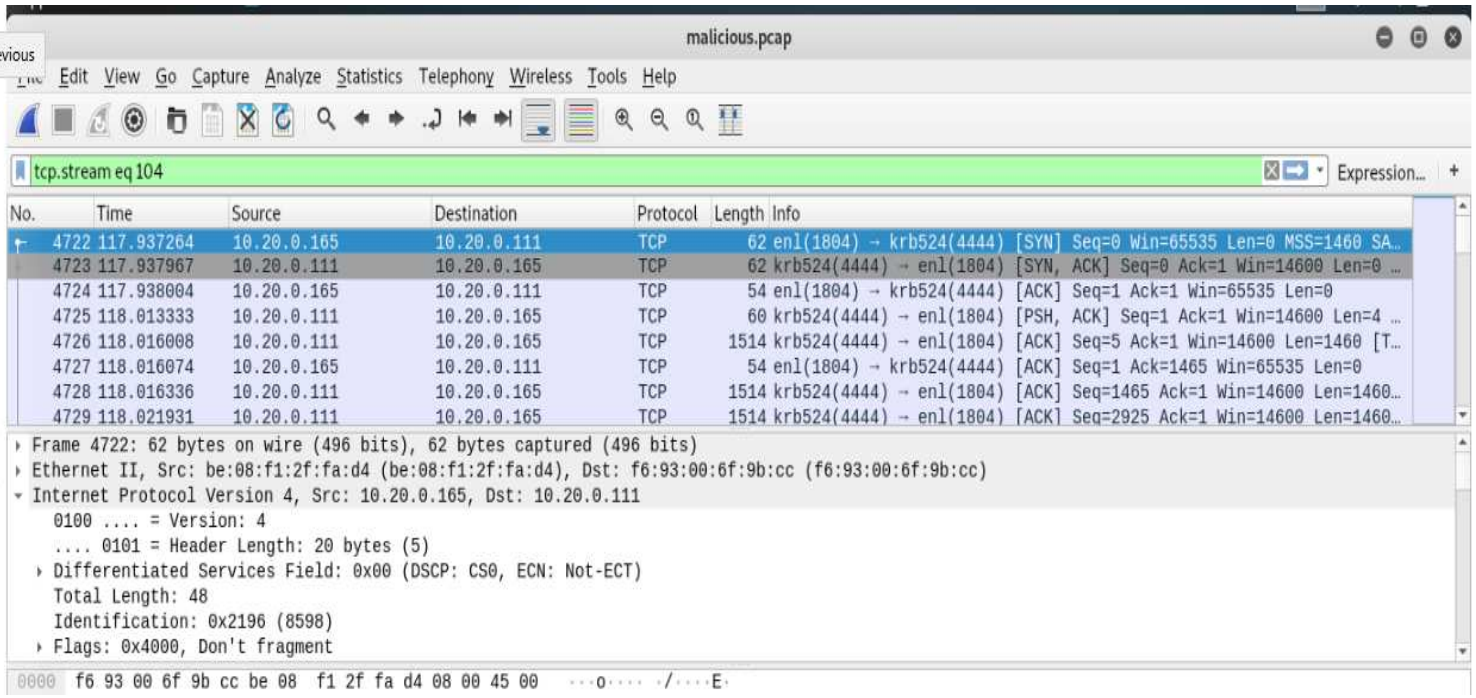
➢ ea7df583983133b62712b5e73bffbcd45cc53736



4. **What is the number of the first frame that indicates that the client has been compromised?**

➢ **4722**





PORT 4444 – Information

- Port Number: 4444
- TCP / UDP: TCP
- Delivery: Yes
- Protocol / Name: [Malware known as CrackDown] krb524,nv-video,eggdrop
- Port Description: [malware info: CrackDown] Common for eggdrop bot

Kbr524 (KNet Web Server) is vulnerable to a buffer overflow. By sending a specially-crafted request to **TCP port 4444**, containing an overly long string argument, a remote attacker could overflow a buffer and execute arbitrary code on the system or cause the server to crash. And in the screenshot we can see it very clearly that the packet above that packet i.e. 4721 is http port (80), thus this packet no 4722 is the first frame that indicates that the client has been compromised.

5. **At one point, the malicious server sends a malicious file to the client. What type of file is it?**

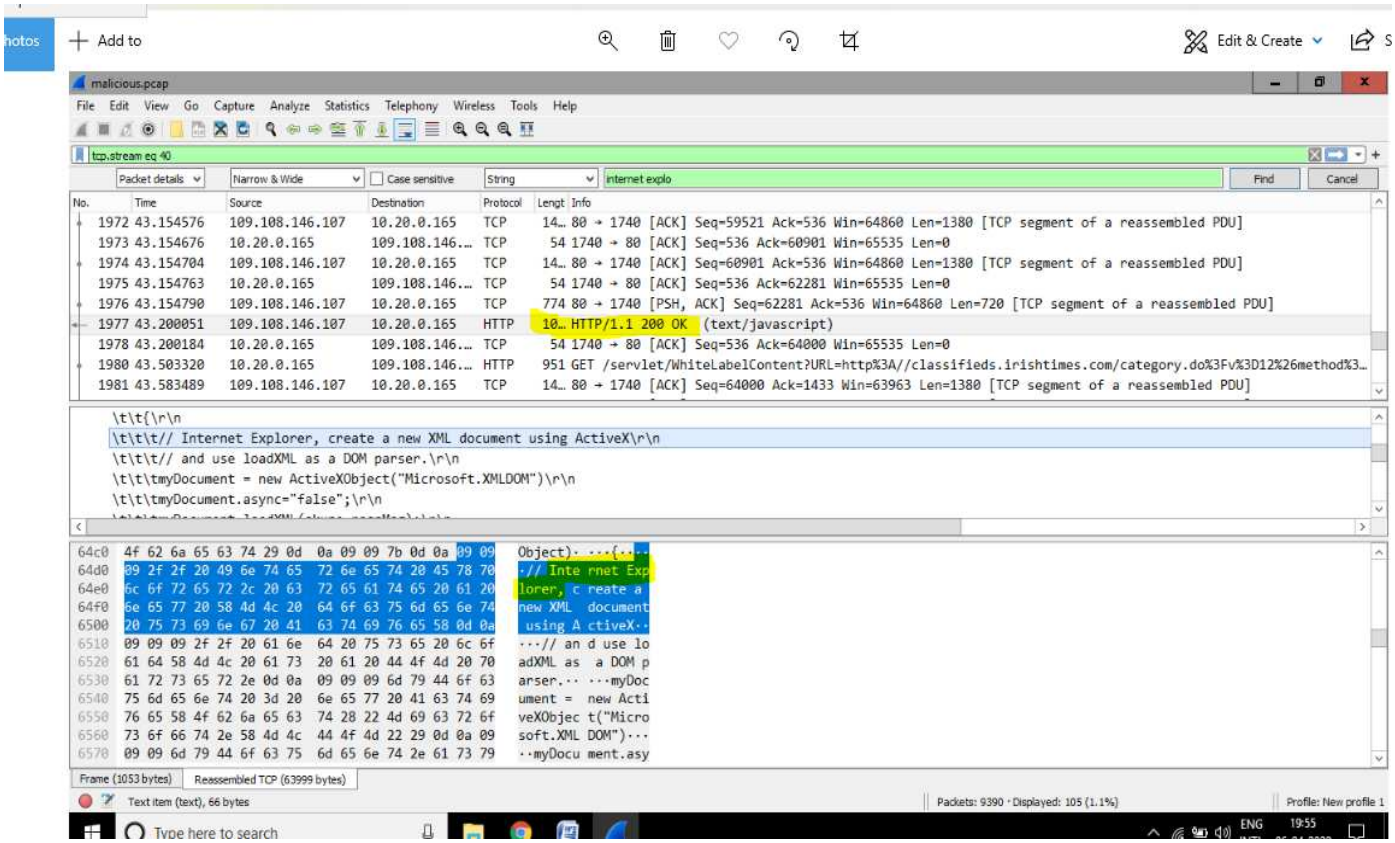
   - **Window exe file with written as MZ**

6. **What is the sha1 hash of the malicious file?**

➢ **94adf100411a80076192766a214e0ff92da13ab7**

7. What vulnerable software is exploited?

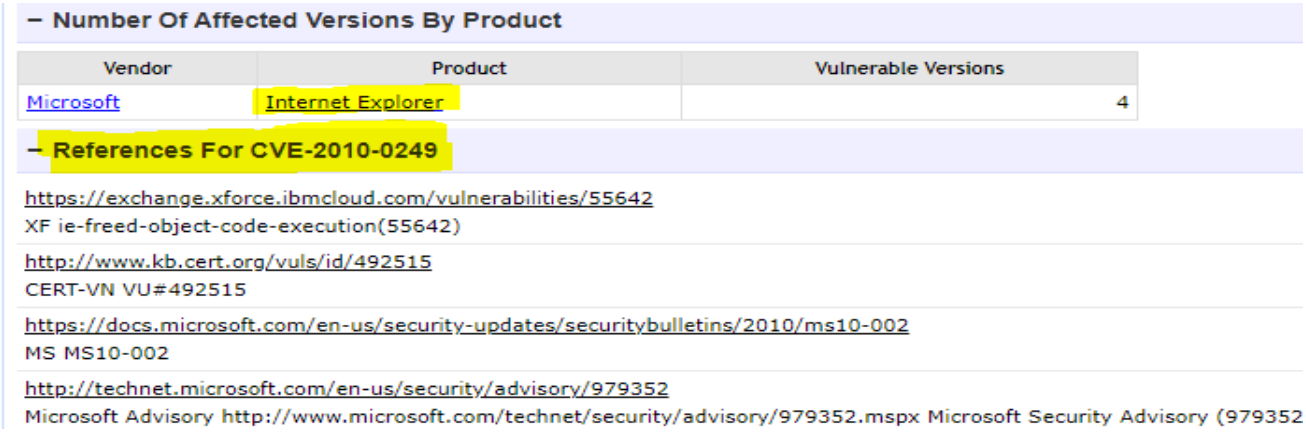
➢ **Internet explorer(ie6)**



8. Can you give the corresponding CVE security bulletin that covers the vulnerability here that was exploited (answer in form of CVE-$year-$number).

➢ **CVE-2010-0249**

CVE-2010-0249 : Use-after-free vulnerability in Microsoft **Internet Explorer 6, 6 SP1, 7, and 8 on Windows 2000 SP4; Windows XP SP2.**



– Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Microsoft	Internet Explorer	4

– References For CVE-2010-0249

https://exchange.xforce.ibmcloud.com/vulnerabilities/55642
XF ie-freed-object-code-execution(55642)

http://www.kb.cert.org/vuls/id/492515
CERT-VN VU#492515

https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-002
MS MS10-002

http://technet.microsoft.com/en-us/security/advisory/979352
Microsoft Advisory http://www.microsoft.com/technet/security/advisory/979352.mspx Microsoft Security Advisory (979352

9. From the capture, it is clear that the attacker gets a certain form of access (i.e. the interface), what (type of) access does the attacker "get" on the client?

- **Shell**

An *attacker* can use a web *shell* to issue commands, perform privilege escalation on the web server, and the ability to upload, delete, download and execute files.

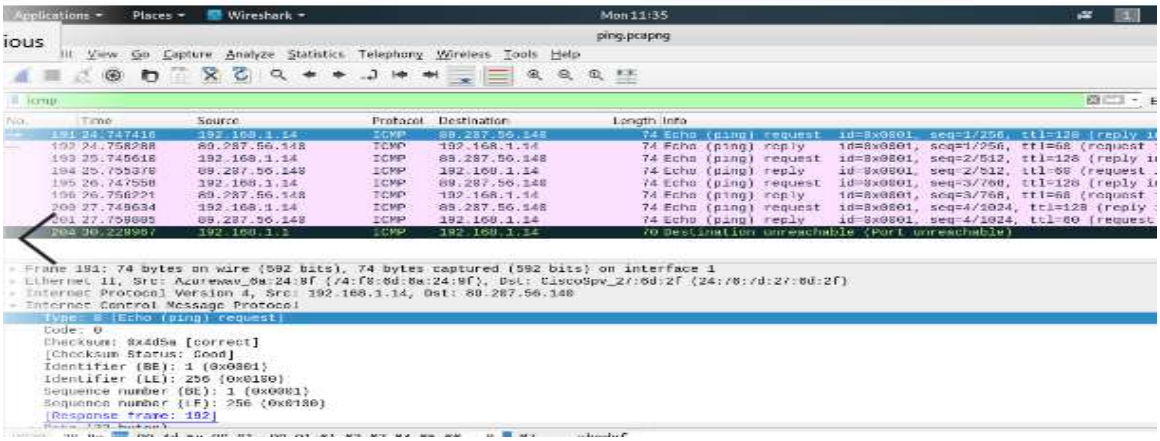
The screenshots shows the list of interfaces which the attacker get access and uses them to attack the client using shell**.**

Ping.pcap

1. What type of ICMP traffic is shown in this capture?

➢ **Echo Request/Reply**

The packet capture displays the type of packet (echo request/reply) in the 'info' column. I looked at the header information and determined the type of ICMP message from the first field 'Type'.

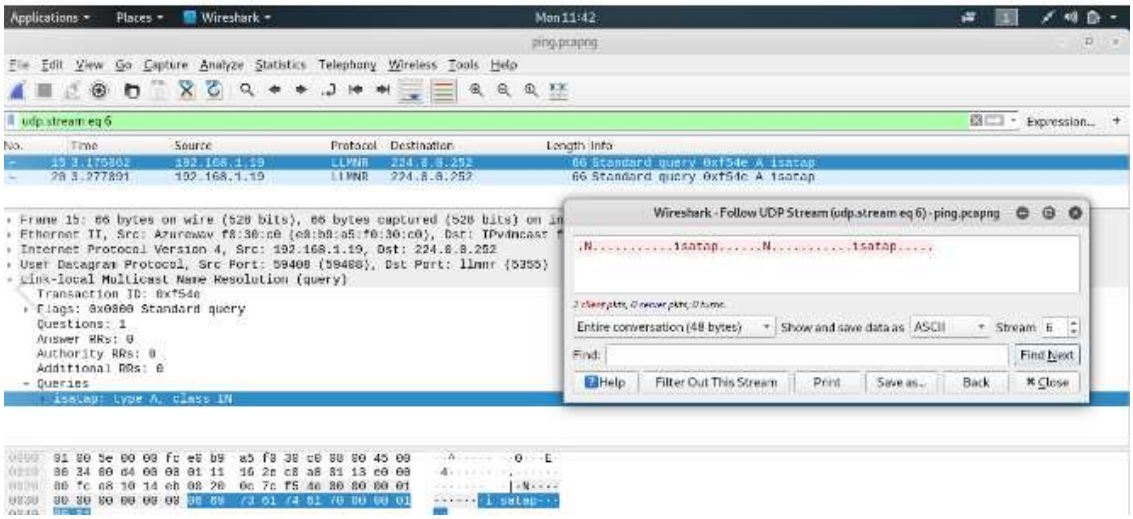


2. What is the number of the first frame that indicates that something funny might be going on?

➢ **15 NO FRAME**

Frame no. 15 is the first frame that suggests something funny might be going on.

Explanation: As I was looking for the hidden protocol, I noticed from the hex view that frame no. 15 was the first frame that indicated the beginning of an SSH connection. The host 192.168.5.217 kept sending ICMP reply packets every 1 or 2 seconds till frame 26 without waiting for a request which seemed strange.



15 (Unprompted reply with suspicious content - SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu6...)

3. What is the application layer protocol that is hidden within the ICMP traffic?

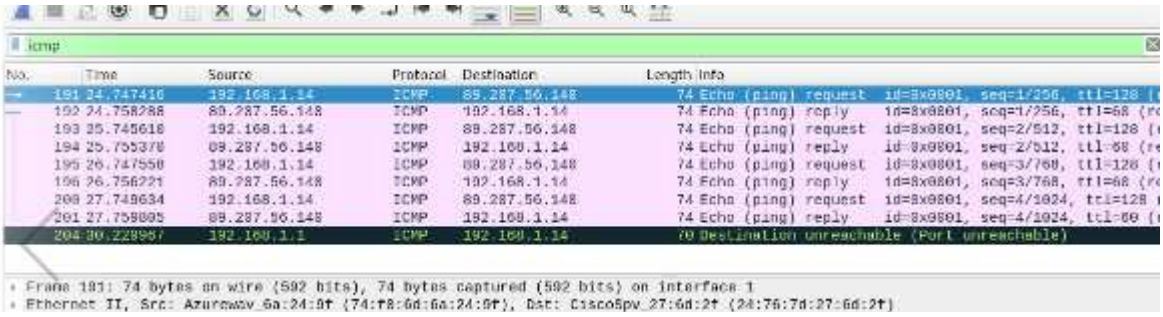
- The *SSH protocol* (also referred to as Secure Shell) is a method for secure remote login from one computer to another. It provides several alternative options for strong authentication, and it protects the communications security and integrity with strong encryption.

4. What tool most likely generated this 'malicious' traffic?

- **ICMP Tunnel**

  The tool that most likely generated this traffic could be Shell over ICMP or Ping Tunnel.

  Explanation: The tool that generated this traffic must support SSH traffic hidden within ICMP traffic also known as ICMP tunneling. I searched ‘ssh within icmp’ on Google. It allows a user to connect to a remote shell daemon, by using ICMP protocol instead of classical TCP. Another tool I came across is **Ping Tunnel** that holds a BSD license. It is used for sending TCP traffic over ICMP using the echo request/reply pings.



5. **What is the 'true' destination of the ICMP traffic generated from 192.168.5.208?**

- **172.16.15.138**

6. **What is the session identifier for each packet? (answer in hex, 2 bytes**

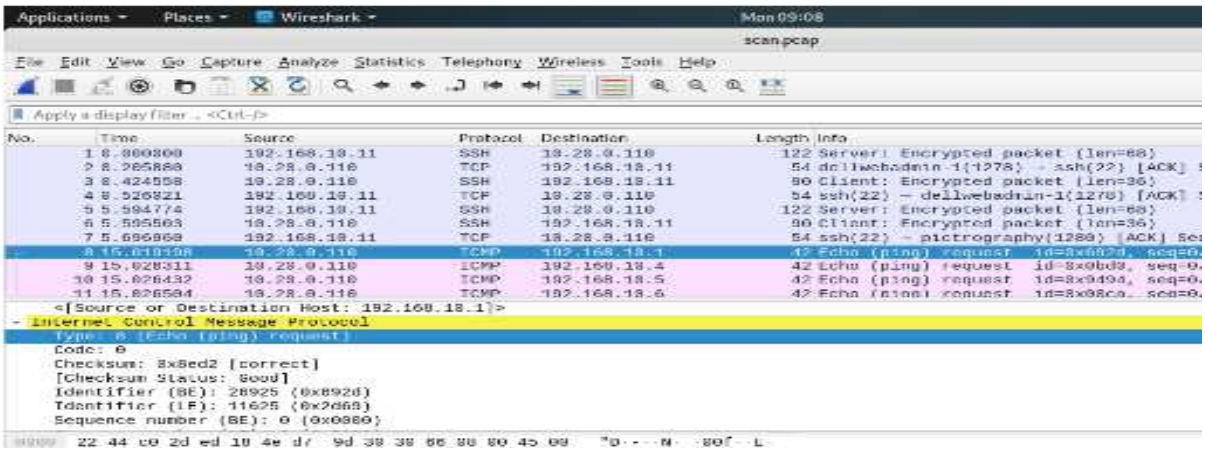
- **e59c**

The session identifiers could be easily determined by looking at the 'info' field. These identifiers are displayed in ICMP header information as both big endian and little endian formats.

Frame Range	Session Identifier (big endian representation)
1 - 12	0x0754
13 - 34	0xe59c
35 - 78	0xc7cc
79 - 306	0x8f5b

Scan.pcap

1. **What tool is generating this traffic?**

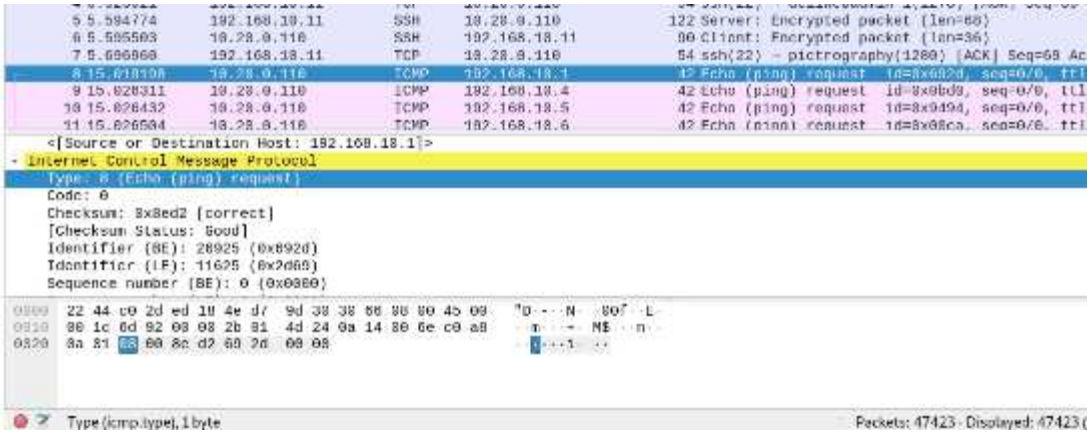


- **Icmp tool**

2. **What is the frame that indicates something strange might be going on?**
   - **Frame 8**

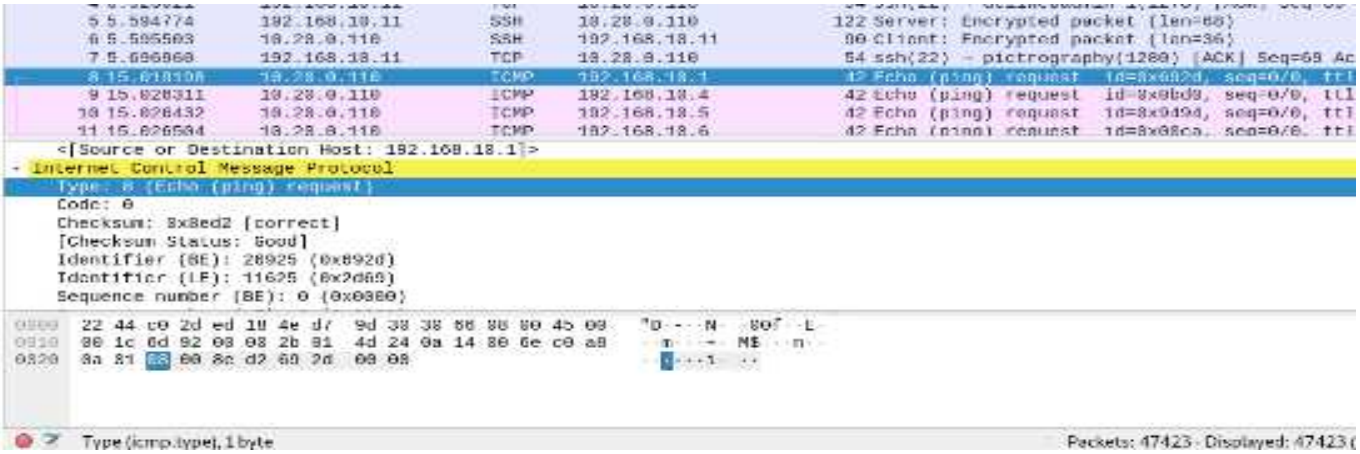
Frame no. 8 indicates something strange might be going on.

Explanation: I identified the malicious host as 10.20.0.110 from NetworkMiner. The first few frames were TCP and SSH request and replies. The 8th frame however was an ICMP ping request from the host 10.20.0.110 to host 198.168.10.1. The subsequent frames showed that the malicious host had sent ICMP ping requests to multiple ip addresses on the same network without receiving replies from every address.



3. **What does this frame constitute the beginning of? (What type of Scan?)**
   - **Ping Scan**

Explanation: According to nmap.org, this is one of the methods for Host Discovery to identify active or interesting hosts on the network. Therefore, the attacking host 10.20.0.110 was clearly trying to identify the active hosts by sending ICMP ping requests or doing the ping scan.



4. **The 'miscreant' then runs two scans beginning just after six minutes and 24 minutes into the trace, however, these traces weren't to his/her liking as they were too slow. On the following scans, a switch was removed from the command, what was this switch (just the letters, case-sensitive)?**

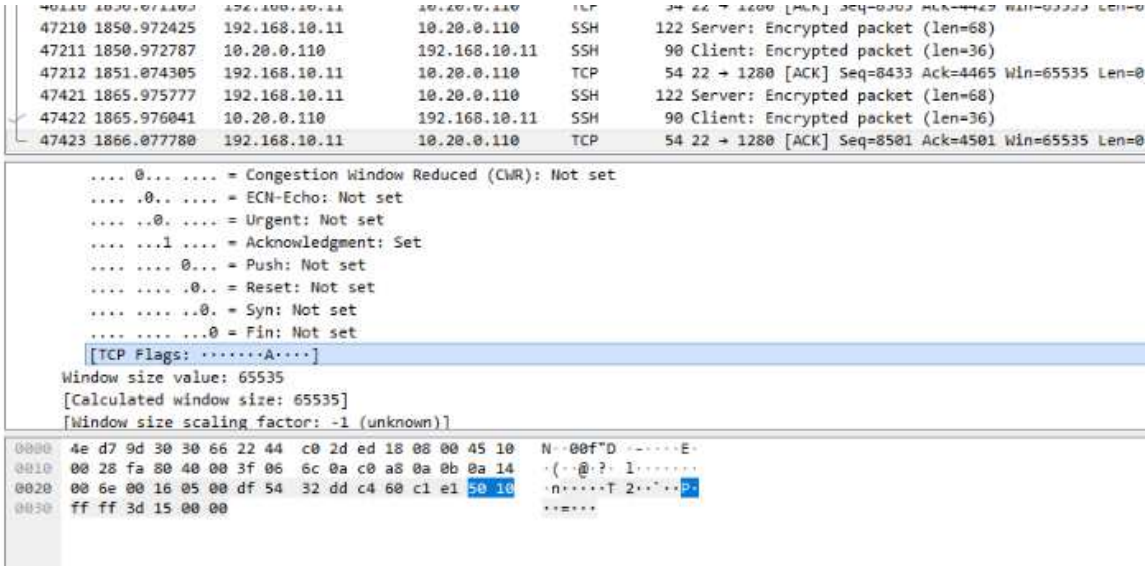
   - **Su is the name of the switch**

I applied the filter 'ip.addr == 10.20.0.110' and examined the pcap file in Wireshark. The two scans began after frame no. 16719 (time = 360 secs approx.) and frame no. 25519 (time = 1440 secs approx.). The packets captured after 360 secs showed that the miscreant had sent UDP packets and therefore it was performing a UDP scan this time. I was not clear what a command switch were so I searched 'namp command switches' on google. I found out that they were parameters used to perform specific type of scans [2]. The option listed for UDP scan was –sU. In order to find out more about the option, I visited the nmap.org and looked for UDP scan.

5. **What switch was added to the final scan (case-sensitive)?**

- **sS**

Explanation: I applied the filter 'ip.addr == 10.20.0.110' and examined the pcap file in Wireshark. On examining the packets after 1440 secs, I noticed that the protocol used was TCP. The first two steps of the TCP handshake were performed between the miscreant 10.20.0.110 and many other hosts. For instance, Frame no. 34051 shows a SYN packet sent from host 10.20.0.110 to 192.168.10.10. The victim machine replies with a SYN/ACK packet according to frame no. 34062. But, instead of sending an ACK packet, the miscreant sends a RST packet to terminate the connection before it is fully established, as it now knows that the port is open. This process is followed in the SYN Stealth scan by nmap according to the same document that I looked up for the previous question. Therefore, the miscreant performs the final scan as the SYN stealth scan .This confirmed that the switch added was –sS.



2018 – 02 – 13 Traffic Analysis

"OFFICE WORK"

Review the pcap, and document the following:

- Date and time of the malicious activity in UTC (GMT).
- IP address of the affected Windows host.
- Mac address of the affected Windows host.
- Host name of the affected Windows host.
- User account name on the affected Windows host.
- What malware might be involved.

ANSWERS:

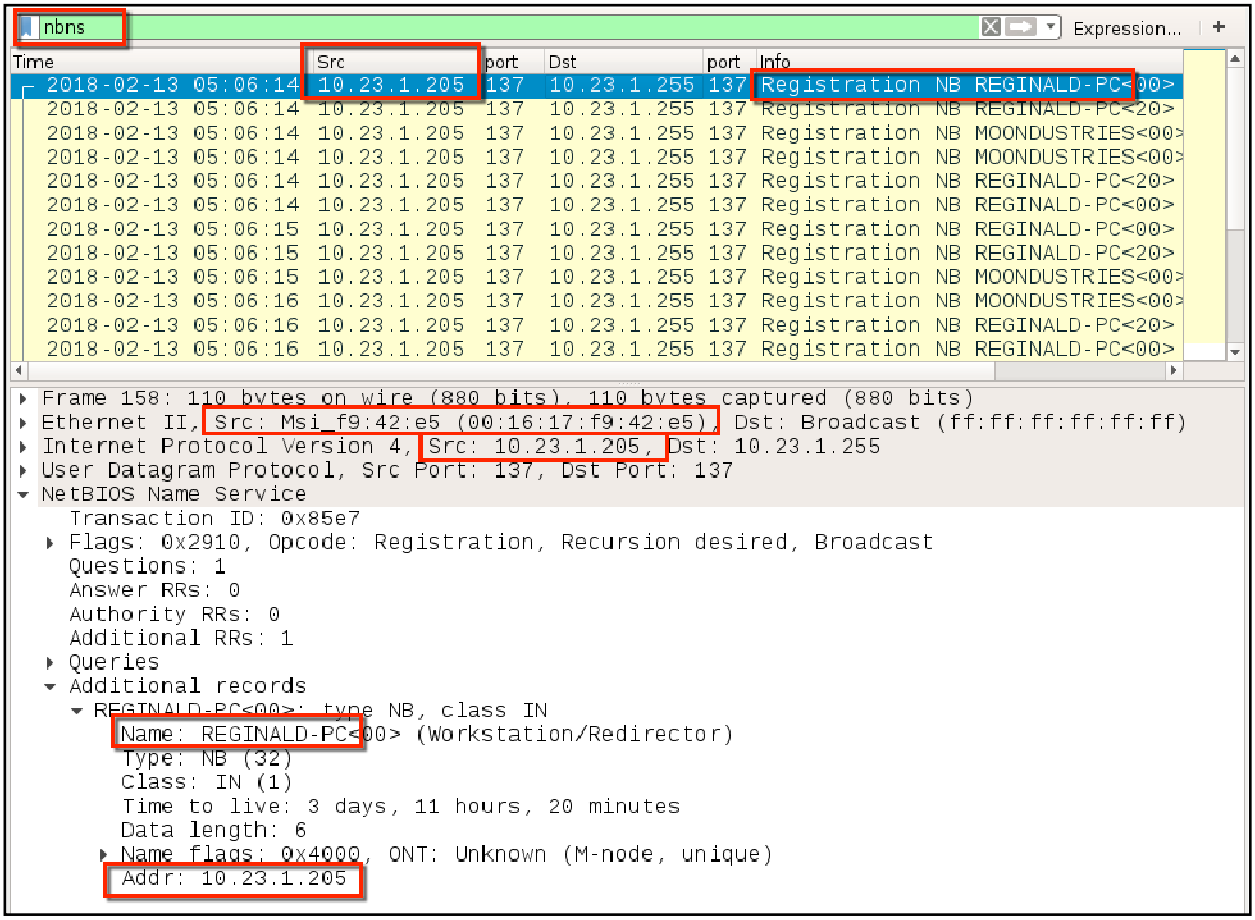
- Date/Time: **2018-02-13 at approximately 05:06 UTC**
- IP address: **10.23.1.205**
- Mac address: **00:16:17:f9:42:e5 (Msi_f9:42:e5)**
- Host name: **REGINALD-PC**
- User account name: **reginald.farnsworth**
- What malware might be involved: **DarkComet RAT**

DETAILS

User account ***reginald.farnsworth*** logged into his Windows client ***REGINALD-PC*** through a domain controller for ***moondustries.com***. The associated IP addresses are:

- Windows client (REGINALD-PC): 10.23.1.205
- Domain controller for moondustries.com: 10.23.1.7
- Broadcast address for this LAN segment: 10.23.1.255
- Gateway for this LAN segment: 10.23.1.1

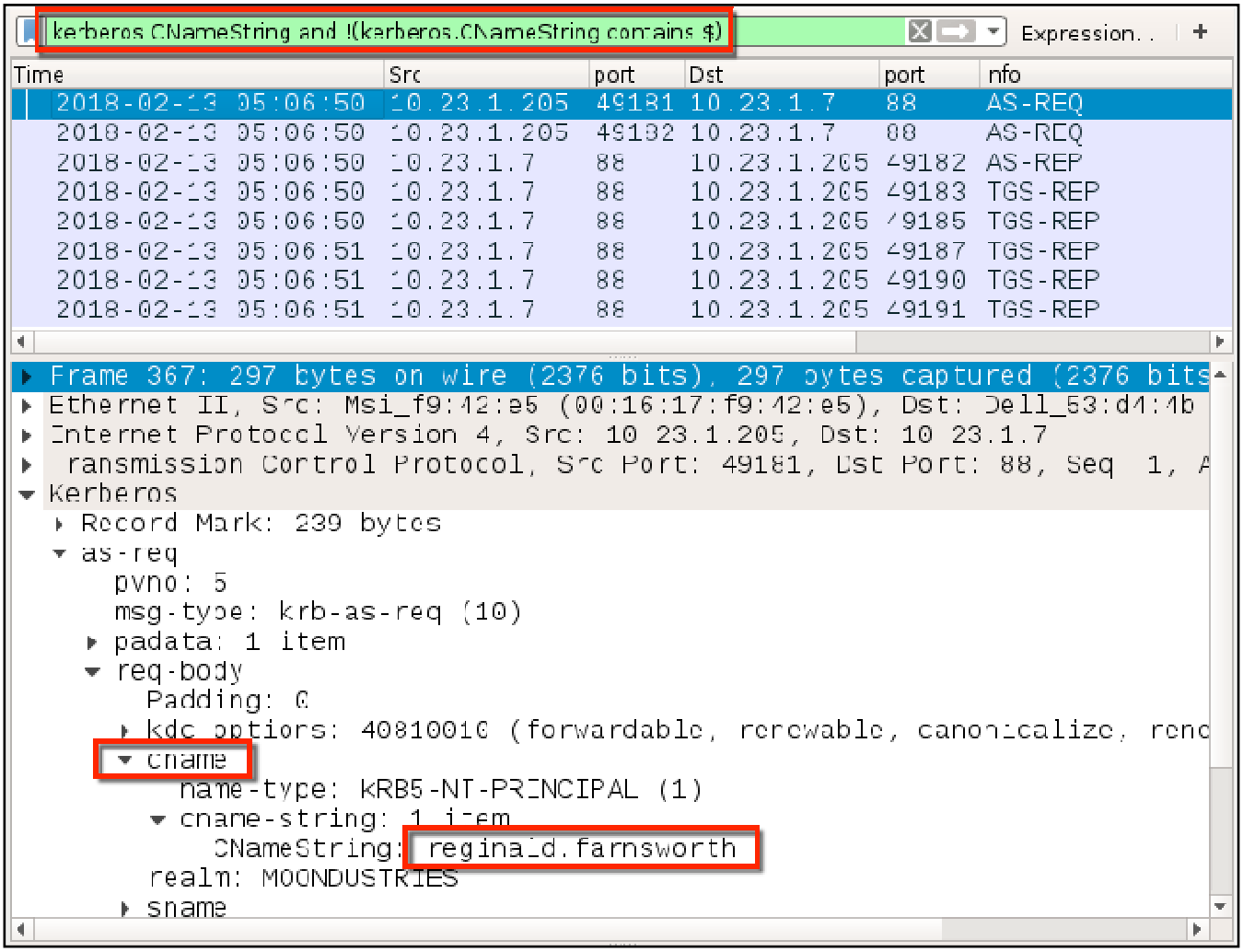
For Reginald's IP address, Mac address, and host name, filter on ***nbns*** and we'll find our answers as shown in the image below:



The user account name can be found through Kerberos traffic generated when Reginald logged into his Windows client. To find the user account name, we use the following Wireshark filter:

kerberos.CNameString and !(kerberos.CNameString contains $)

In the results, work our way down to the ***cname*** field and find the user account name as shown below:



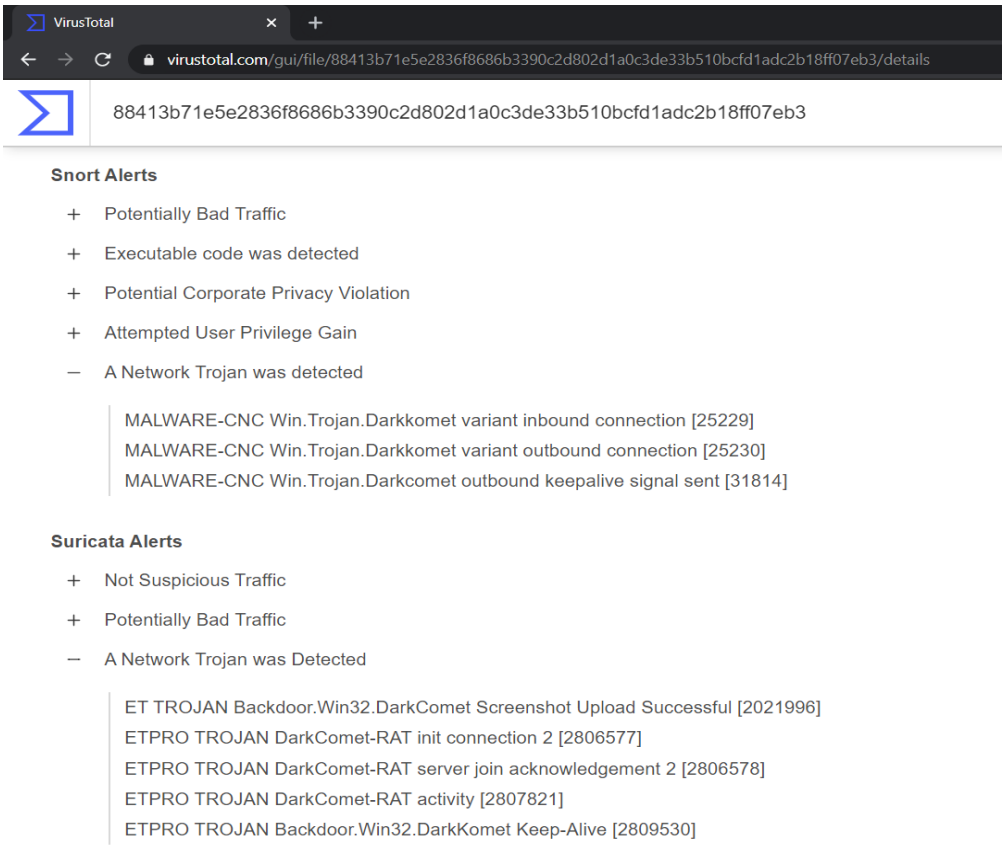
How can we find out the alerts? We can check the pcap on VirusTotal and PacketTotal. Both show alerts for the DarkComet RAT.

In the VirusTotal analysis of the pcap, we'll find alerts for DarkComet RAT under both the Snort and the Suricata alerts in the "File detail" section.

- https://www.virustotal.com/en/file/88413b71e5e2836f8686b3390c2d802d1a0c3de33b510 bcfd1adc2b18ff07eb3/analysis/

PacketTotal analysis of the pcap also shows several alerts for DarkComet on traffic to 185.86.151.37 over TCP port 2200:

- https://packettotal.com/app/analysis?id=6f4a5f6d7b3c4af88577fa79f8aa105d

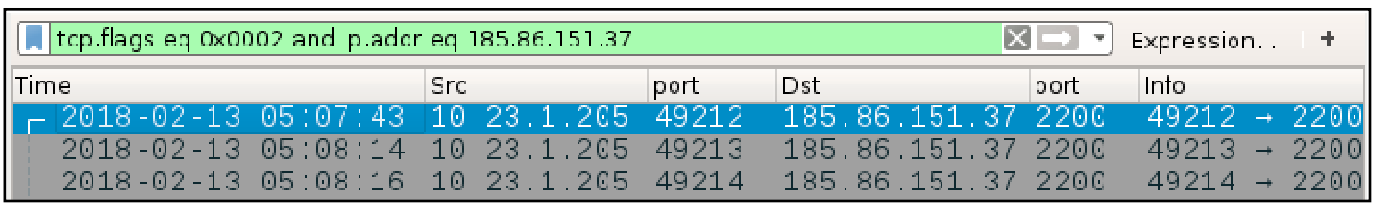


Snort Alert

- **MALWARE-CNC Win.Trojan.Darkkomet variant inbound connection [25229]**
- **MALWARE-CNC Win.Trojan.Darkkomet variant outbound connection [25230]**
- **MALWARE-CNC Win.Trojan.Darkcomet outbound keepalive signal sent [31814]**

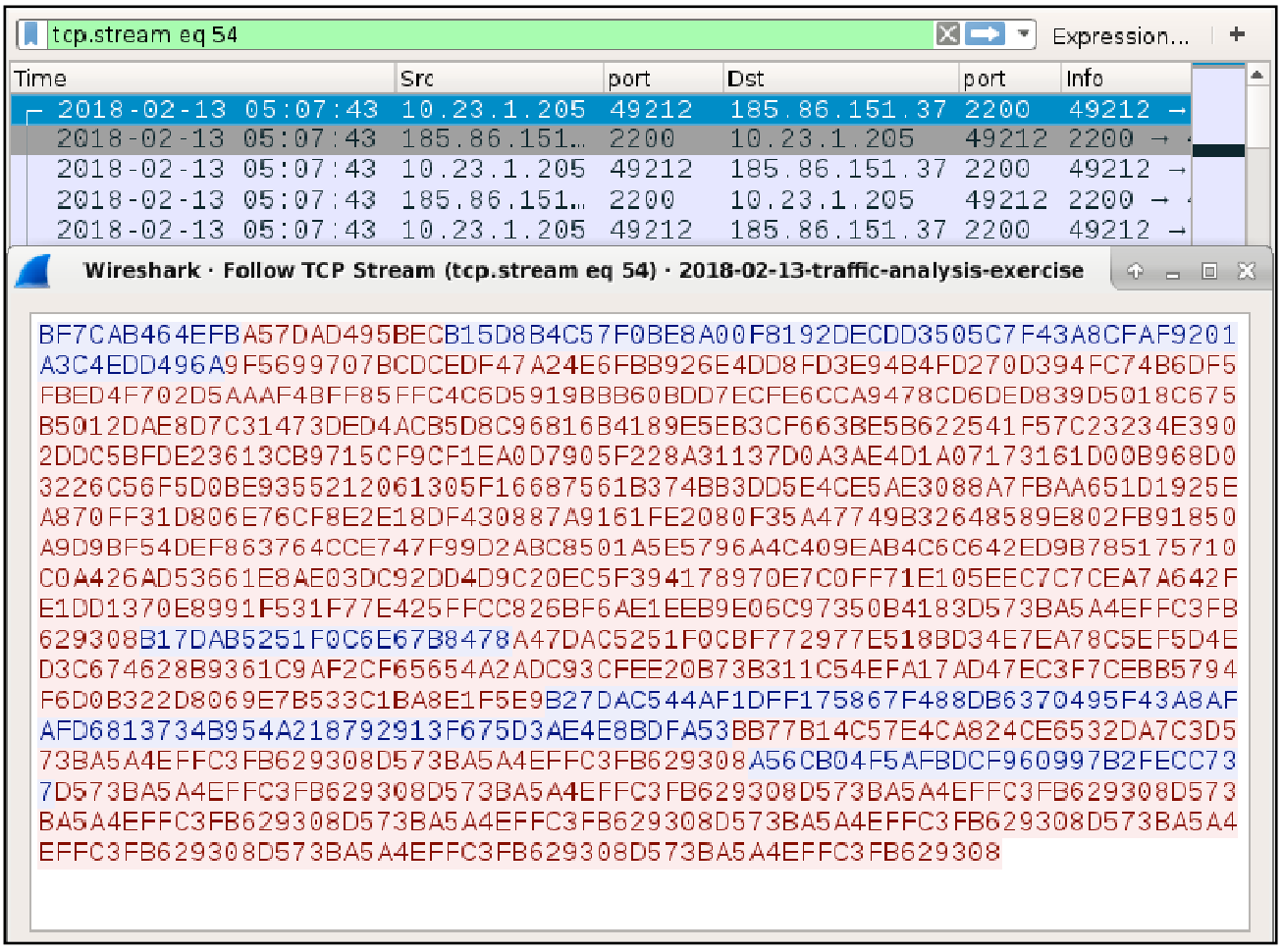
Suricata Alert

- **ET TROJAN Backdoor.Win32.DarkComet Screenshot Upload Successful [2021996]**
- **ETPRO TROJAN DarkComet-RAT init connection 2 [2806577]**
- **ETPRO TROJAN DarkComet-RAT server join acknowledgement 2 [2806578]**
- **ETPRO TROJAN DarkComet-RAT activity [2807821]**
- **ETPRO TROJAN Backdoor.Win32.DarkKomet Keep-Alive [2809530]**



Shown above: You'll find three TCP streams using the Wireshark filter ***tcp.flags eq 0x0002 and ip.addr eq 185.86.151.37***

Follow any one of the TCP streams shown in the above image, and we'll see what DarkComet traffic looks like.



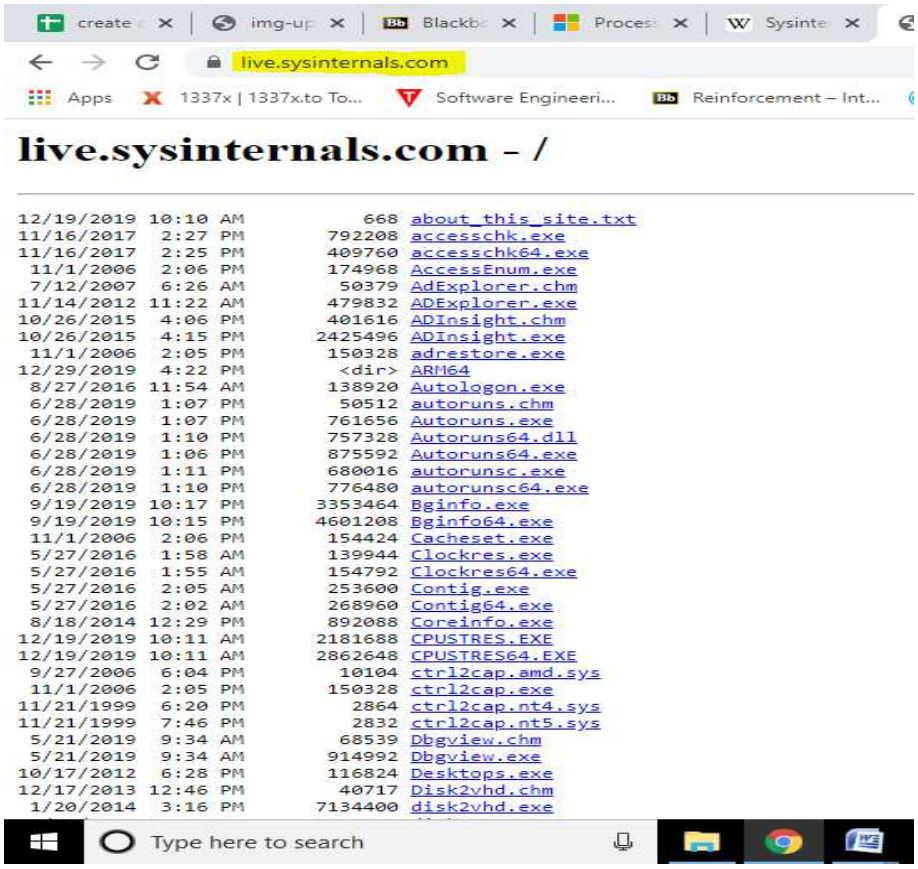
Shown above: A TCP stream of DarkComent RAT traffic from this infection.

EXPERIMENT 6

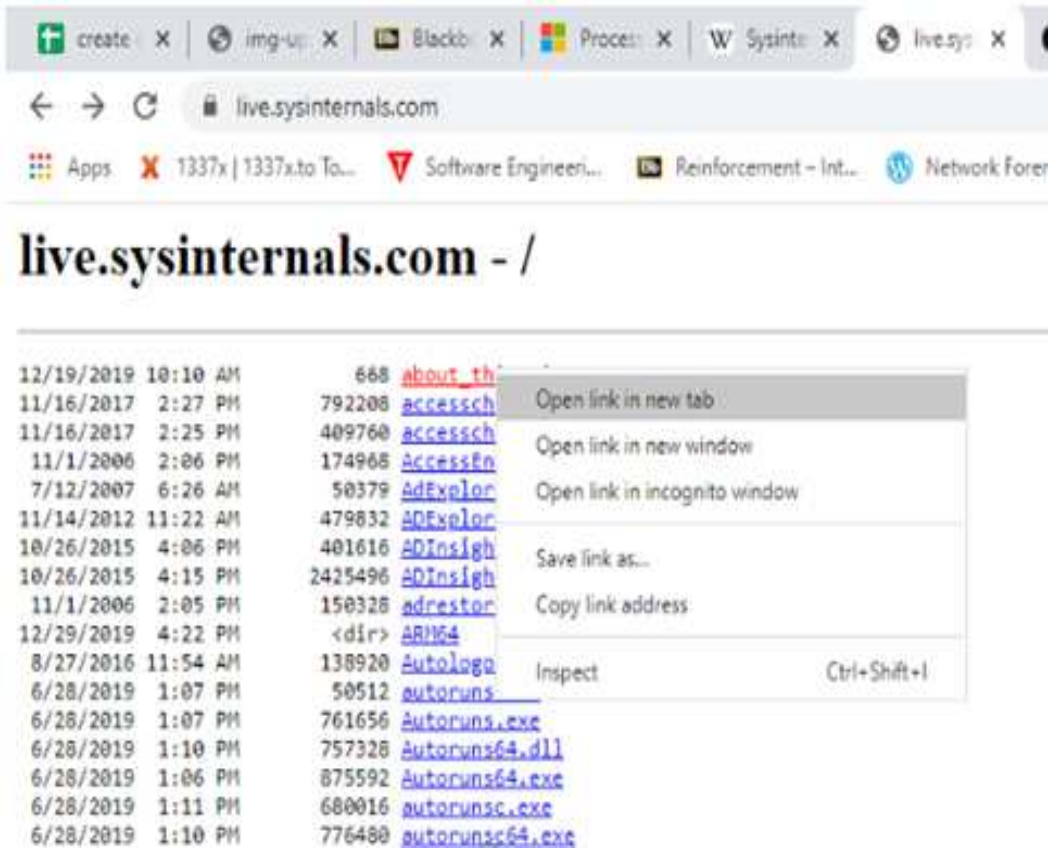
Using Sys-internals tools for Network Tracking and Process Monitoring

Windows Sysinternals is a website which offers technical resources and utilities to manage, diagnose, troubleshoot, and monitor a Microsoft Windows environment. The tools include utilities such as Process Explorer, which is a lot like Task Manager with a plethora of extra features, or Process Monitor, which monitors your PC for file-system, registry, or even network activity from almost any process on your system. Most of these tools are going to require administrator access on your computer, so you'd be wise to test them out in a virtual machine or a test computer if you aren't sure what you are doing — these are some heavy duty tools.

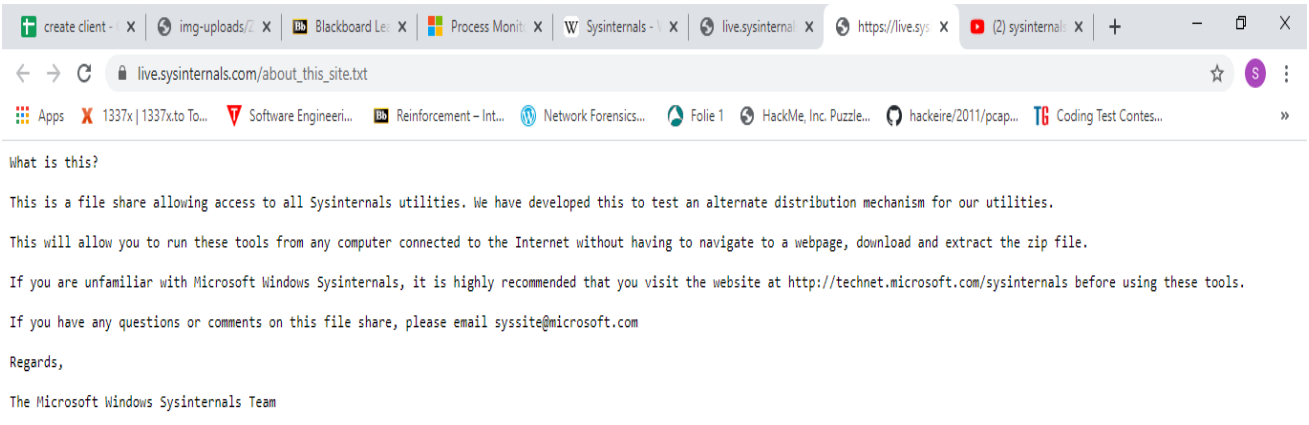
- **Check Sysinternals tools :** To check sysinternals tool, browse on the google and go to the website: **https://live.sysinternals.com/ ,** there we can see all the tools:



Now we can check the details about the tools by right click on the link as **: -:**



The details about the about this site is shown below :



Here is the list of all the sysinternal tools with their description of their job:

Process Explorer
v16.21 (May 16, 2017)
Find out what files, registry keys and other objects processes have open, which DLLs they have loaded, and more. This uniquely powerful utility will even show you who owns each process.

Process Monitor
v3.50 (February 13, 2018)
Monitor file system, Registry, process, thread and DLL activity in real-time.

PsExec
v2.2 (June 29, 2016)
Execute processes on remote systems.

PsFile
v1.03 (June 29, 2016)
See what files are opened remotely.

AccessChk
v6.20 (November 19, 2017)
AccessChk is a command-line tool for viewing the effective permissions on files, registry keys, services, processes, kernel objects, and more.

AccessEnum
v1.32 (November 1, 2006)
This simple yet powerful security tool shows you who has what access to directories, files and Registry keys on your systems. Use it to find holes in your permissions.

AdRestore
v1.1 (November 1, 2006)
Undelete Server 2003 Active Directory objects.

Autologon
v3.10 (August 29, 2016)
Bypass password screen during logon.

Autoruns
v13.95 (June 11, 2019)
See what programs are configured to startup automatically when your system boots and you login. Autoruns also shows you the full list of Registry and file locations where applications can configure auto-start settings.

CacheSet
v1.0 (November 1, 2006)
CacheSet is a program that allows you to control the Cache Manager's working set size using functions provided by NT. It's compatible with all versions of NT.

ClockRes
v2.1 (July 4, 2016)
View the resolution of the system clock, which is also the maximum timer resolution.

Hex2dec
v1.1 (July 4, 2016)
Convert hex numbers to decimal and vice versa.

Junction
v1.07 (July 4, 2016)
Create Win2K NTFS symbolic links.

LDMDump
v1.02 (November 1, 2006)
Dump the contents of the Logical Disk Manager's on-disk database, which describes the partitioning of Windows 2000 Dynamic disks.

ListDLLs
v3.2 (July 4, 2016)
List all the DLLs that are currently loaded, including where they are loaded and their version numbers.

ProcDump
v9.0 (May 16, 2017)
This command-line utility is aimed at capturing process dumps of otherwise difficult to isolate and reproduce CPU spikes.

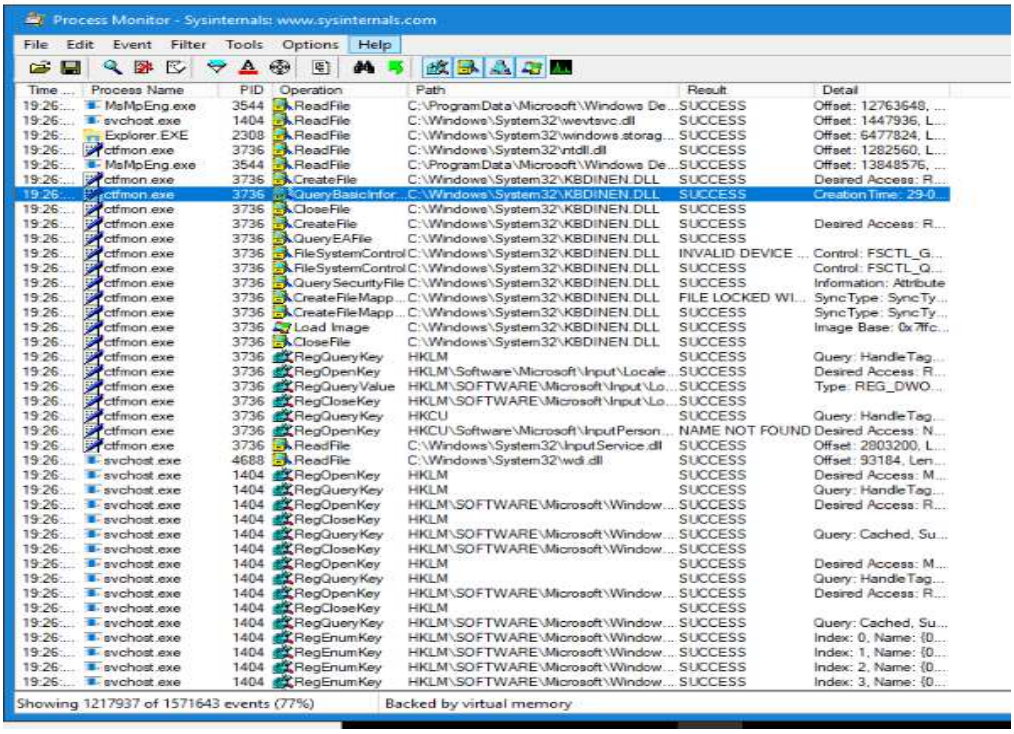
- **Monitor Live Processes:** *Process Monitor* is an advanced monitoring tool for Windows that shows real-time file system, Registry and process/thread activity. It combines the features of two legacy Sysinternals utilities, *Filemon* and *Regmon*, and adds an extensive list of enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

Process Monitor includes powerful monitoring and filtering capabilities, including:

- More data captured for operation input and output parameters
- Non-destructive filters allow you to set filters without losing data

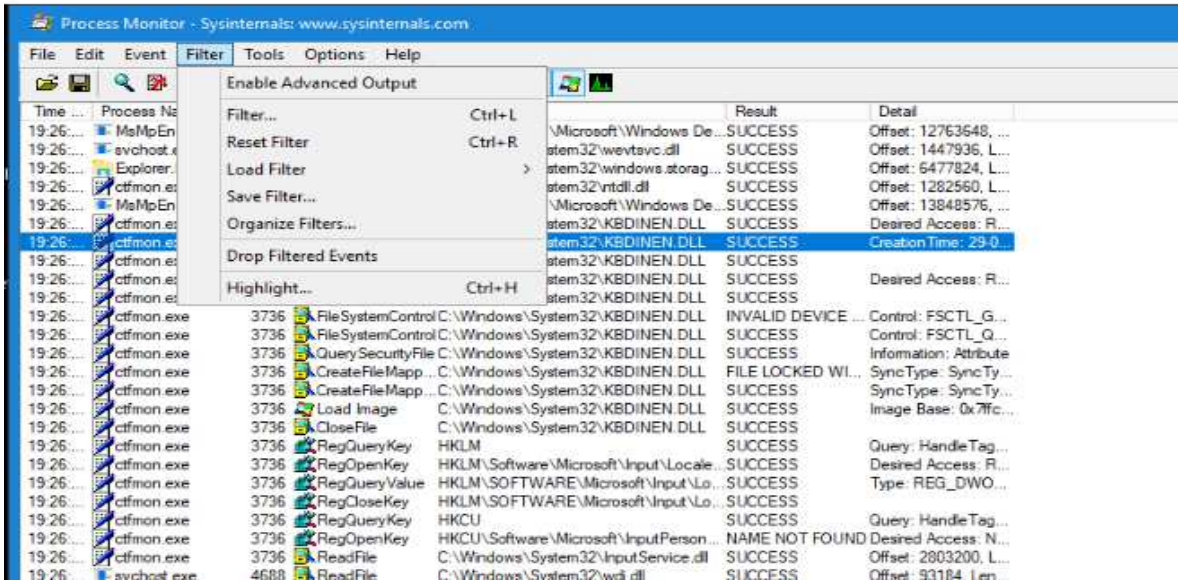
- Capture of thread stacks for each operation make it possible in many cases to identify the root cause of an operation
- Reliable capture of process details, including image path, command line, user and session ID
- Configurable and moveable columns for any event property
- Filters can be set for any data field, including fields not configured as columns
- Advanced logging architecture scales to tens of millions of captured events and gigabytes of log data.
  I installed the process monitor sysinternal tool, and then opened it on my system, the process monitor working is shown:

The Process Monitor Interface:

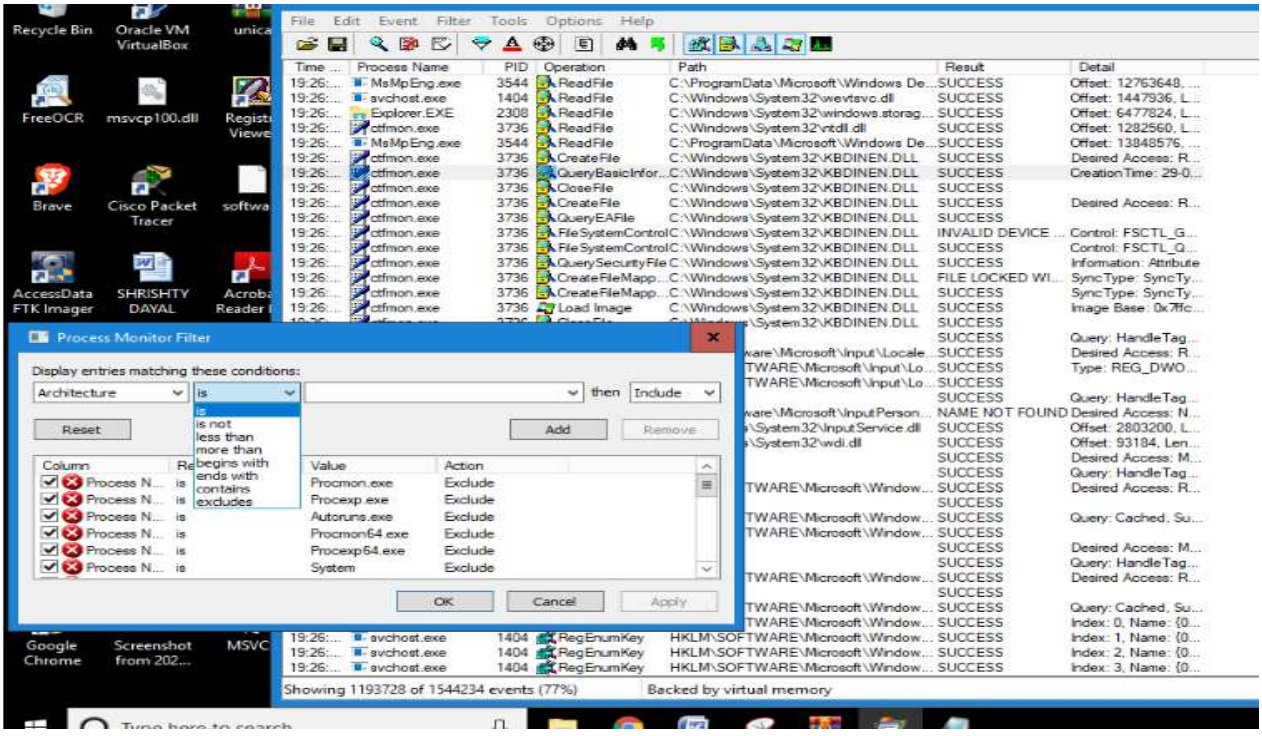


Description about the process monitor interface: When I first load up the Process Monitor interface, it was presented with an enormous number of rows of data, with more data flying in quickly. The first thing that I noticed was that to try filter those rows down to the much smaller subset of data.

- **Similar to wireshark, in this tool also we can apply filters as well:**

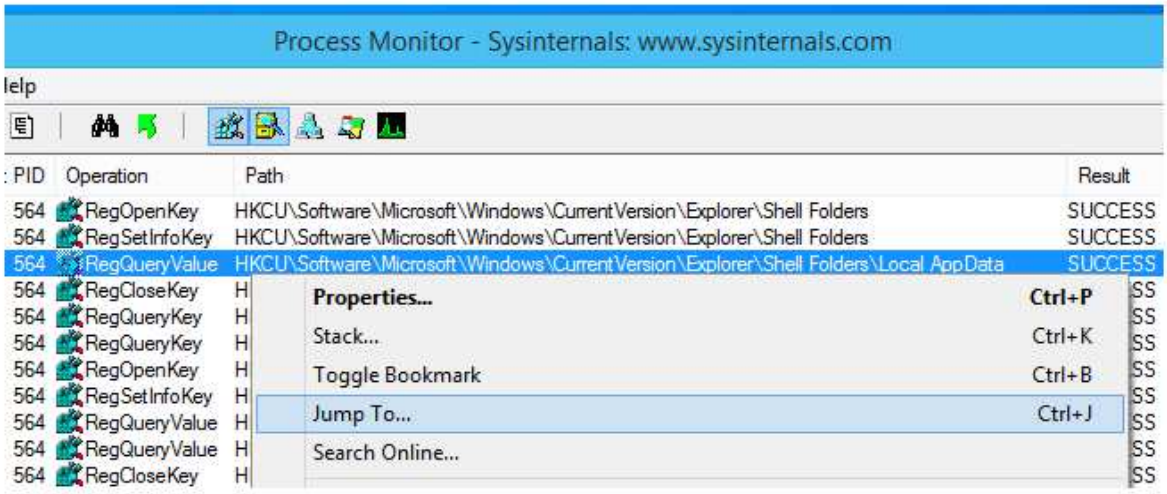


- **We can also remove or edit filters by selecting them in the list and then modifying or removing them :**



○ Jumping to an Event Data Path

All of this information is really great. We can right-click on the Path field for an item and use the Jump To option to quickly access that data to see what it contains and try to figure out why the application is requesting that data in the first place. We can also use the Search Online feature to quickly search for the name of the process, the registry path, or any other field, which can be really useful when you don't understand what something is used for



We can also add some additional columns to the default display:

Go to Options -> Select Columns.

One of the reasons for adding additional columns to the display is so we can very quickly filter by those events without being overwhelmed with data. Here are a few of the extra columns that we use:

Command Line

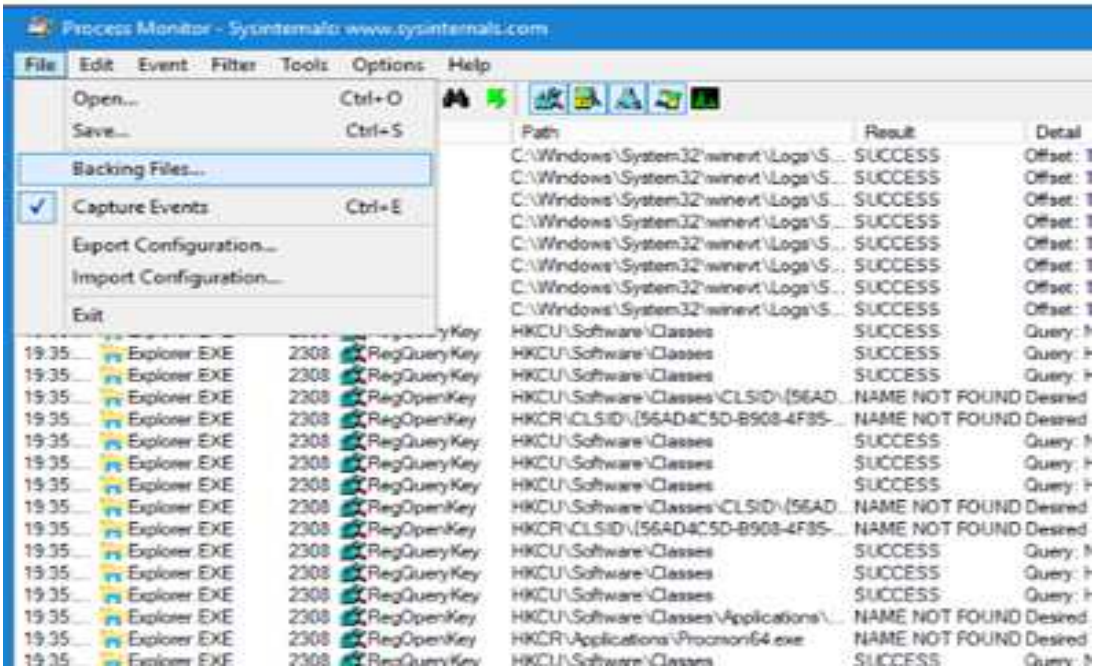
Company Name

Parent PID

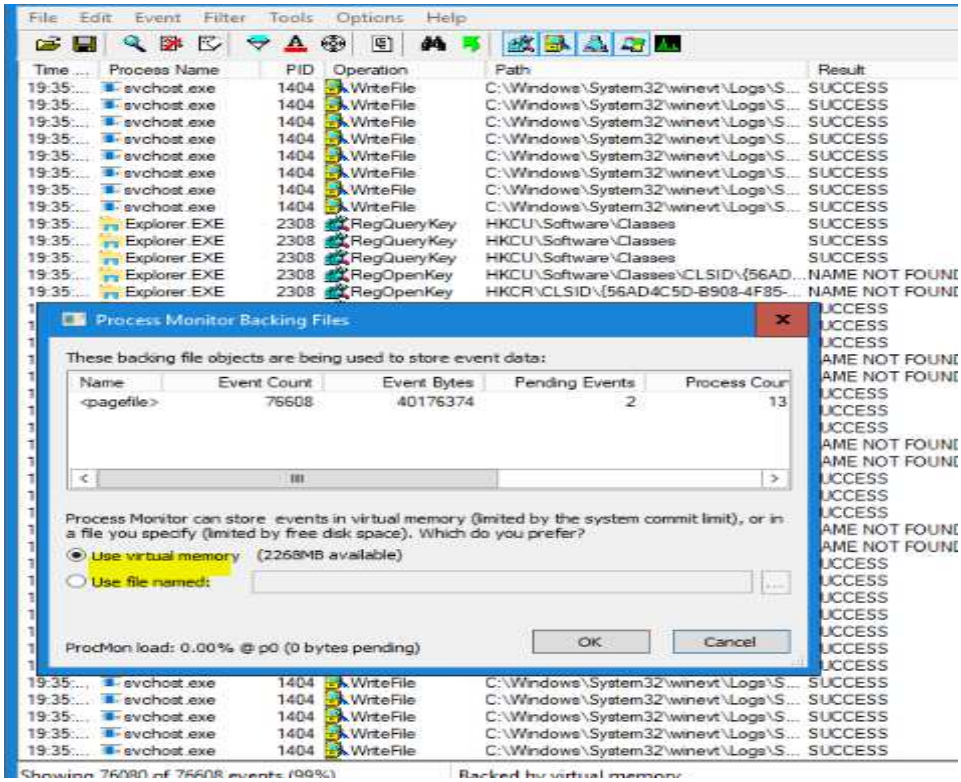
- ## Capture RAM

We can choose to store Process Monitor data in a file on disk instead of virtual memory

1. **Go to** File -> Backing files:



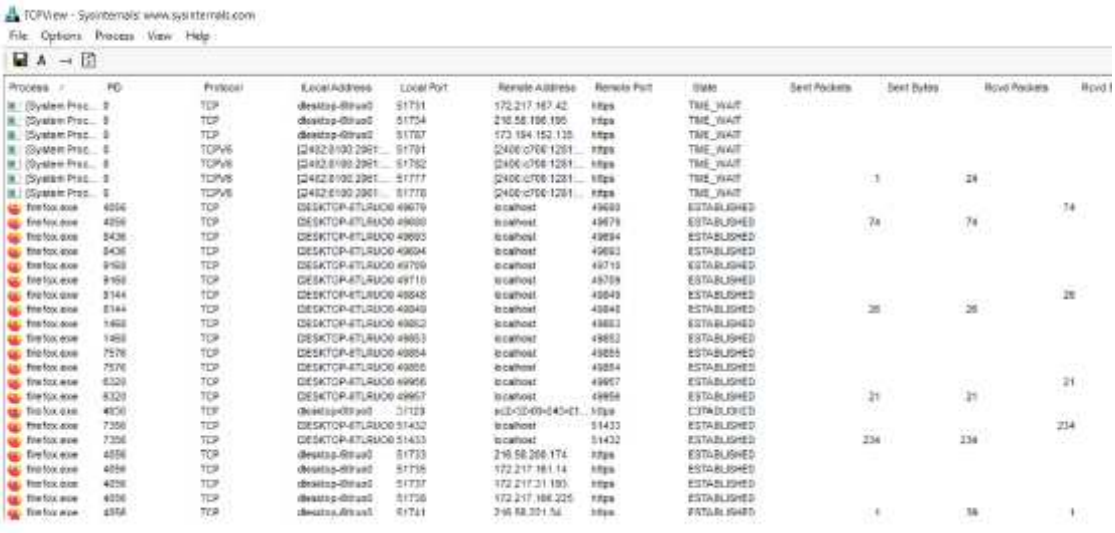
2. Specify the file where you want event data to be stored



- **MONITOR TCP/UDP PACKETS**

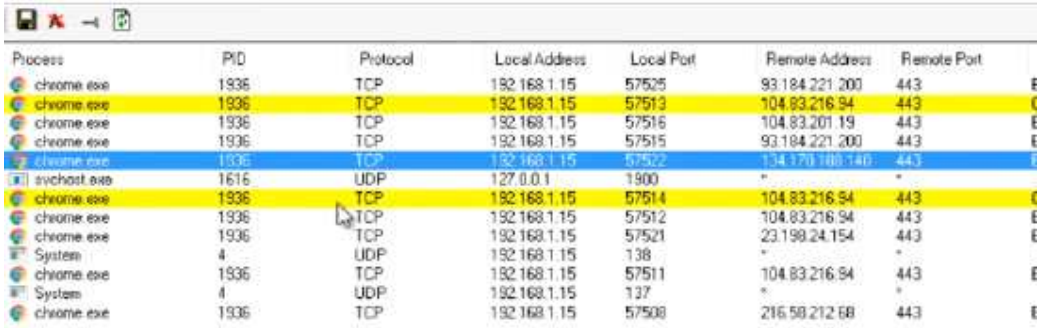
Open TCPView from the suite tools. TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections.

When you start TCPView it will enumerate all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions. You can use a toolbar button or menu item to toggle the display of resolved names. You can also



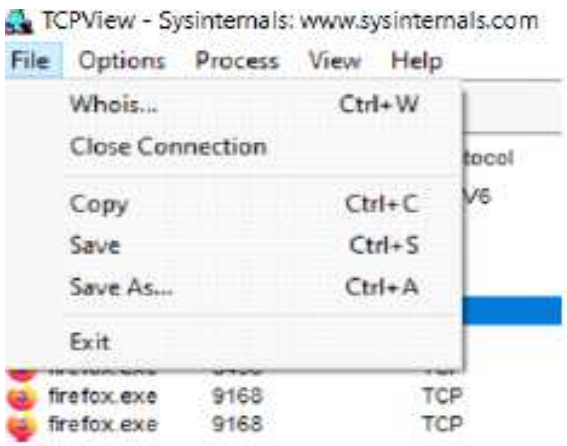
filter data in any column.

By default, TCPView updates every second, but you can use the Options>Refresh Rate menu item to change the rate. Endpoints that change state from one update to the next are highlighted in yellow; those that are deleted are shown in red, and new endpoints are shown in green.



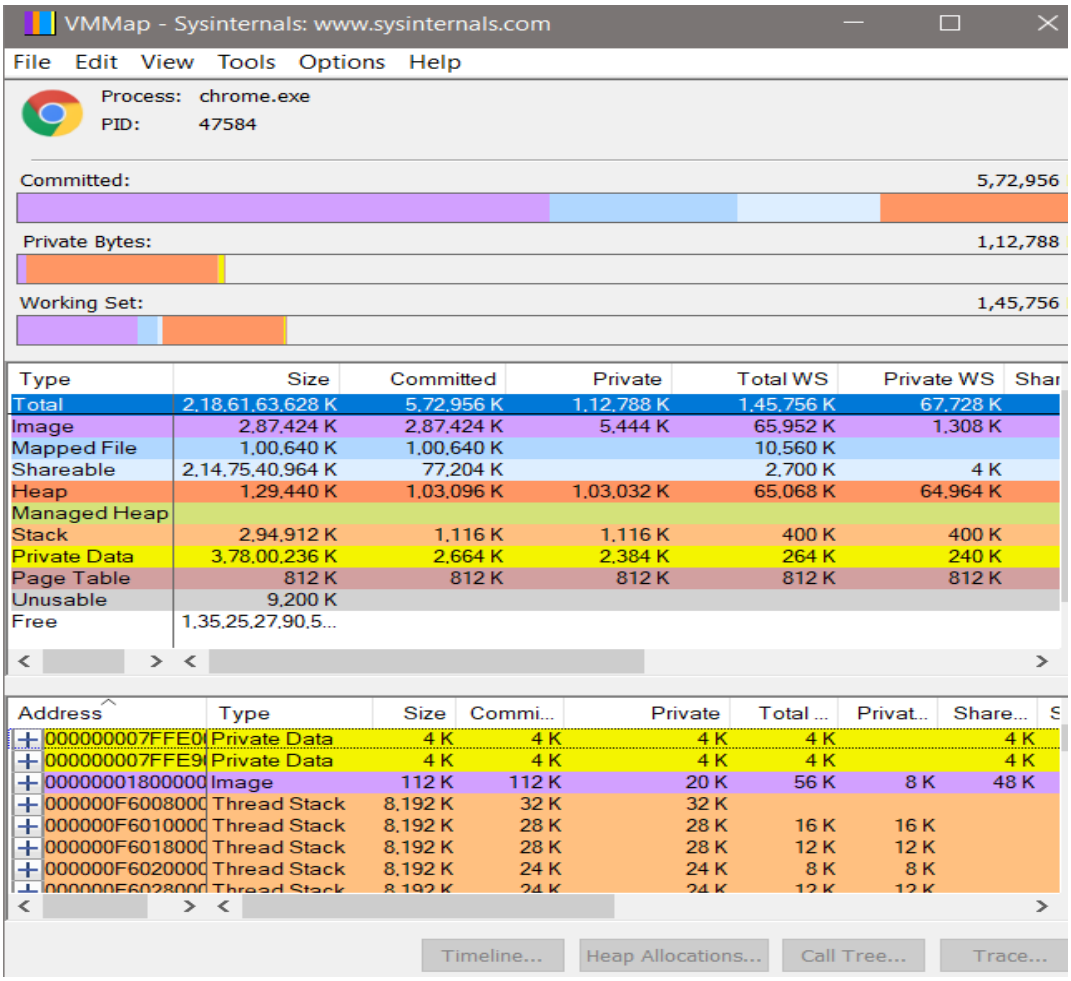
Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port
chrome.exe	1936	TCP	192.168.1.15	57525	93.184.221.200	443
chrome.exe	1936	TCP	192.168.1.15	57513	104.83.216.94	443
chrome.exe	1936	TCP	192.168.1.15	57516	104.83.201.19	443
chrome.exe	1936	TCP	192.168.1.15	57515	93.184.221.200	443
chrome.exe	1936	TCP	192.168.1.15	57522	134.170.188.140	443
svchost.exe	1616	UDP	127.0.0.1	1900	*	*
chrome.exe	1936	TCP	192.168.1.15	57514	104.83.216.94	443
chrome.exe	1936	TCP	192.168.1.15	57512	104.83.216.94	443
chrome.exe	1936	TCP	192.168.1.15	57521	23.198.24.154	443
System	4	UDP	192.168.1.15	138	*	*
chrome.exe	1936	TCP	192.168.1.15	57511	104.83.216.94	443
System	4	UDP	192.168.1.15	137	*	*
chrome.exe	1936	TCP	192.168.1.15	57508	216.58.212.68	443

We can close established TCP/IP connections (those labeled with a state of ESTABLISHED) by selecting File>Close Connections, or by right-clicking on a connection and choosing Close Connections from the resulting context menu.



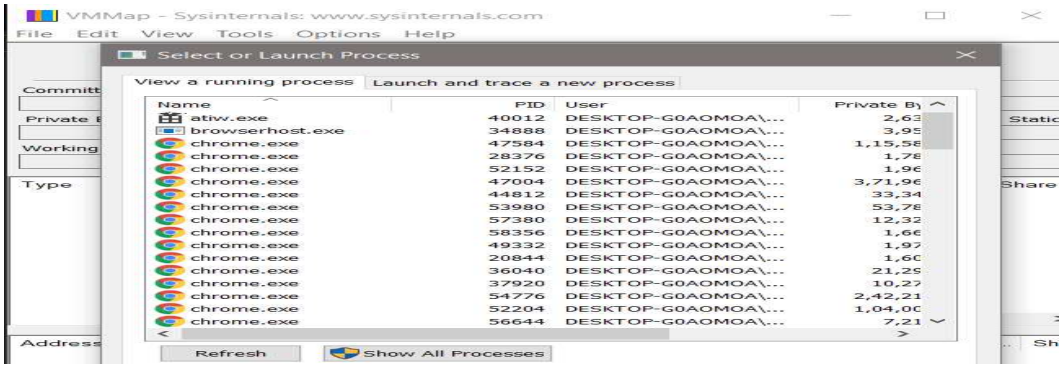
-
- **Monitor Virtual Memory**

To Monitor Virtual Memory using a Sys-Internals tool, we have to use VM-Map. We can find this in the SysInternals Suite package.Once we double click on the application we will be greeted by the major live processes of the system as we can see in the picture above and to take a look about their memory, we need to



select a process and click *'Okay'*.

Click the Start menu on your VPS' desktop, then using the 'Search programs and files' box simply type in resmon. Hit enter to start Resource **Monitor**. When the

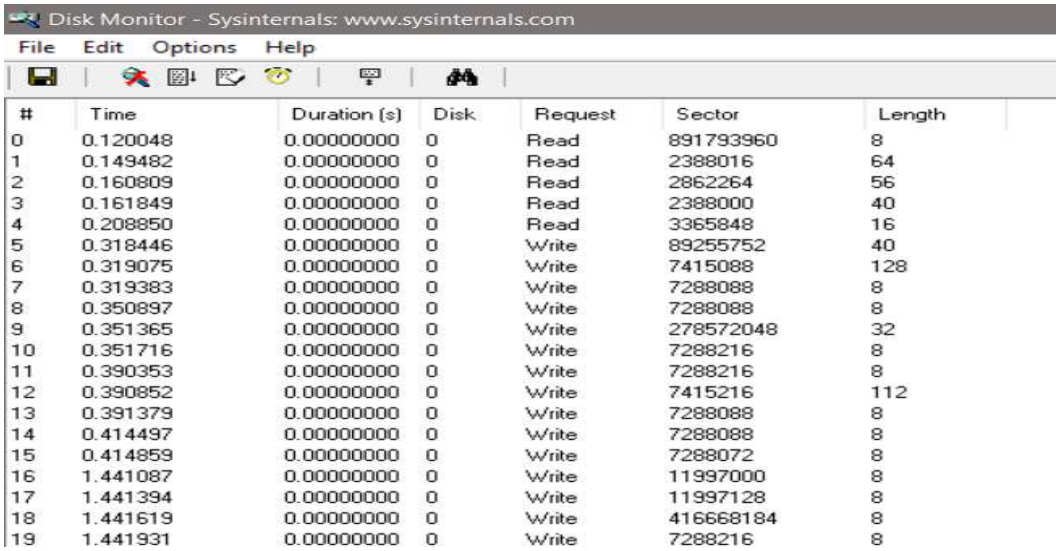


Resource **Monitor** window opens, click the **Memory** tab. In the upper section here we will see a list of running processes and how much **memory** they are using.

- **Monitor Hard Disk**

To monitor the activity inside the Hard Disk we need to use an application in SysInternals Suite package known as Disk Monitor. We can find it as Diskmon in the package. We need to open this application as an Administrator because a guest cannot access such sensitive information.

DiskMon is an application that logs and displays all hard disk activity on a Windows system. We can also minimize DiskMon to your system tray where it acts as a disk light, presenting a green icon when there is disk-read activity and a red icon when there is disk-write activity.

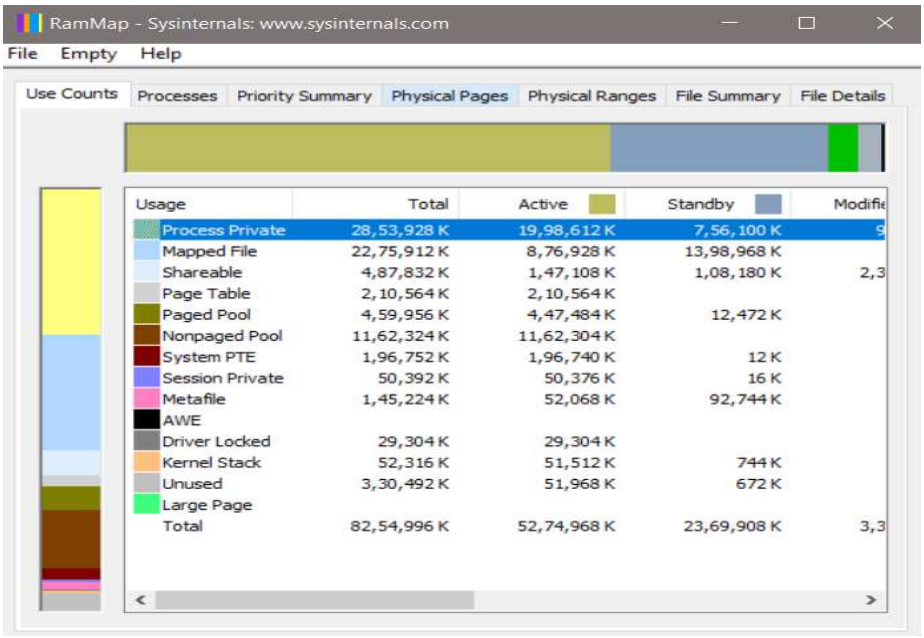


#	Time	Duration (s)	Disk	Request	Sector	Length
0	0.120048	0.00000000	0	Read	891793960	8
1	0.149482	0.00000000	0	Read	2388016	64
2	0.160809	0.00000000	0	Read	2862264	56
3	0.161849	0.00000000	0	Read	2388000	40
4	0.208850	0.00000000	0	Read	3365848	16
5	0.318446	0.00000000	0	Write	89255752	40
6	0.319075	0.00000000	0	Write	7415088	128
7	0.319383	0.00000000	0	Write	7288088	8
8	0.350897	0.00000000	0	Write	7288088	8
9	0.351365	0.00000000	0	Write	278572048	32
10	0.351716	0.00000000	0	Write	7288216	8
11	0.390353	0.00000000	0	Write	7288216	8
12	0.390852	0.00000000	0	Write	7415216	112
13	0.391379	0.00000000	0	Write	7288088	8
14	0.414497	0.00000000	0	Write	7288088	8
15	0.414859	0.00000000	0	Write	7288072	8
16	1.441087	0.00000000	0	Write	11997000	8
17	1.441394	0.00000000	0	Write	11997128	8
18	1.441619	0.00000000	0	Write	416668184	8
19	1.441931	0.00000000	0	Write	7288216	8

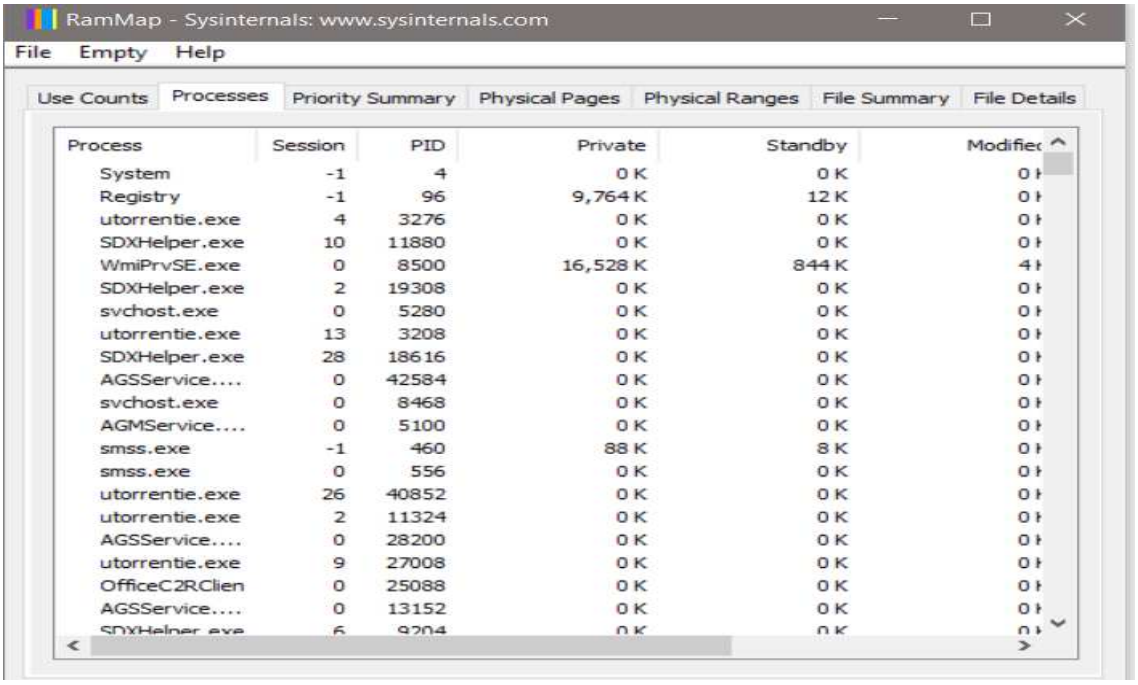
Therefore, as we can see in the image above these are some of the process that are running in the Hard Disk.

- **Monitor Cache Memory**

We know that cache memory is stored in RAM. Therefore, we need to use RAM-Map to monitor Cache Memory. We can find this in the Sys-Internals Suite package.



The above image shows the different portions of the RAM. To access the Cache processes we need to select the ‘Processes’ tab.



The picture above shows the processes stored in the RAM.

EXPERIMENT – 7.A

Recovering deleted files on Windows

In this experiment, what we do is we recover deleted files from pendrive.

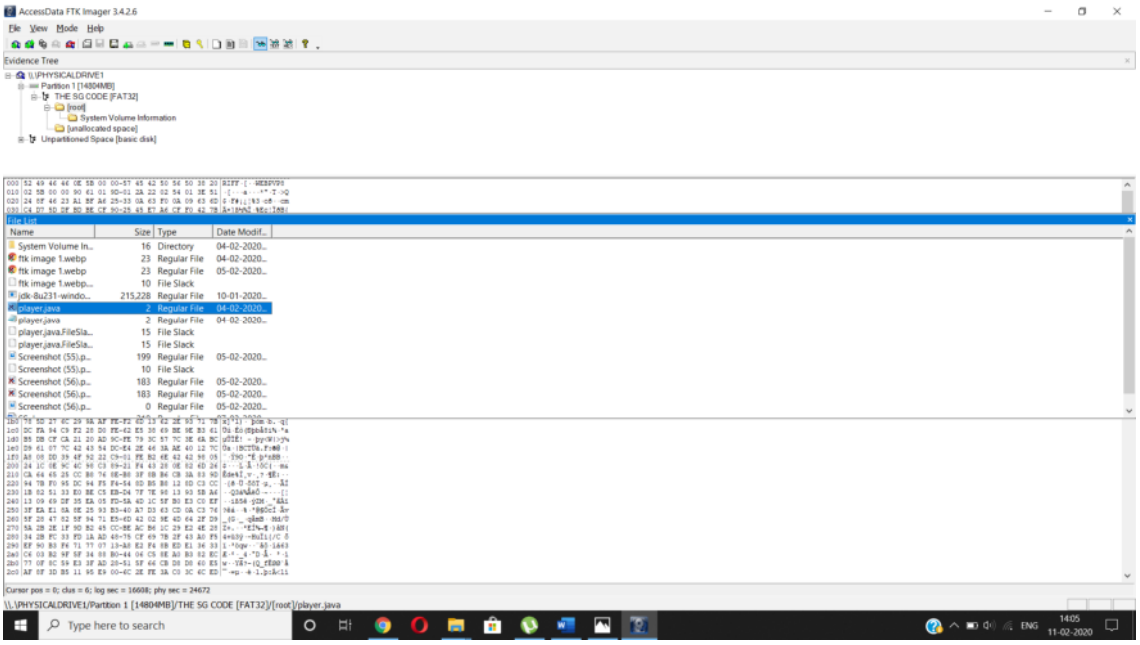
We achieve this by using FTK imager tool by deleting some files from the pen drive and then finding the deleted items on it.

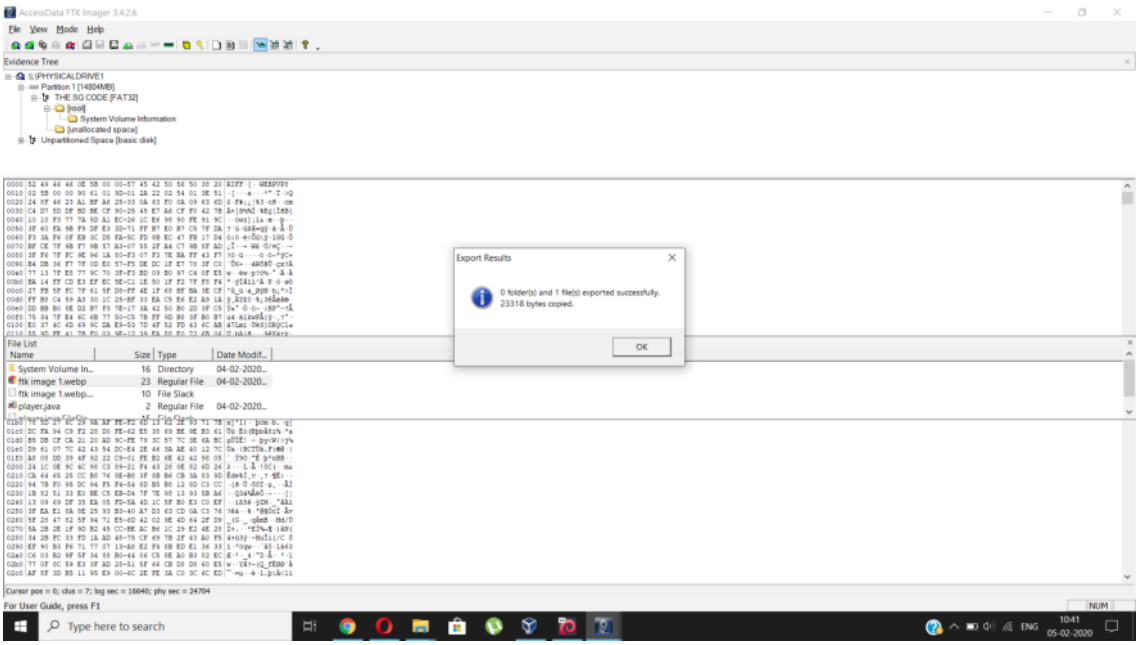
We do this for both linux and Windows.

In this we first add evidence item on the tool ADD EVIDENCE ITEM.

1. Launch FTK Imager
2. Select File > Add Evidence Item
3. Select "physical drive" which is pen drive here and proceed to add the file
4. Under the "Evidence Tree", right click your file and select Verify Drive.
5. Then here we right click and click on root option.
6. Then we find for the folder from we have deleted some files.
7. Here in front of the files where we have a cross mark it means it has been deleted from the pen drive very previously and we have to recover it.
8. For recovering it, we can right click on that picture of text file and can select the option of exporting it.
9. After this we can choose destination as of where to recover those deleted files or pic.

Snapshot:


AccessData FTK Imager 3.4.2.6
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE1
Partition 1 [14804MB]
THE SG CODE [FAT32]
[root]
System Volume Information
[unallocated space]
Unpartitioned Space [basic disk]
File List
Name Size Type Date Modif...
System Volume In... 16 Directory 04-02-2020...
ftk image 1.webp 23 Regular File 04-02-2020...
ftk image 1.webp 23 Regular File 05-02-2020...
ftk image 1.webp... 10 File Slack
jdk-8u231-windo... 215,228 Regular File 10-01-2020...
player.java 2 Regular File 04-02-2020...
player.java 2 Regular File 04-02-2020...
player.java.FileSla... 15 File Slack
player.java.FileSla... 15 File Slack
Screenshot (55).p... 199 Regular File 05-02-2020...
Screenshot (55).p... 10 File Slack
Screenshot (56).p... 183 Regular File 05-02-2020...
Screenshot (56).p... 183 Regular File 05-02-2020...
Screenshot (56).p... 0 Regular File 05-02-2020...
Cursor pos = 0; clus = 6; log sec = 16608; phy sec = 24672
\\.\PHYSICALDRIVE1/Partition 1 [14804MB]/THE SG CODE [FAT32]/[root]/player.java
Type here to search
ENG
1405
11-02-2020

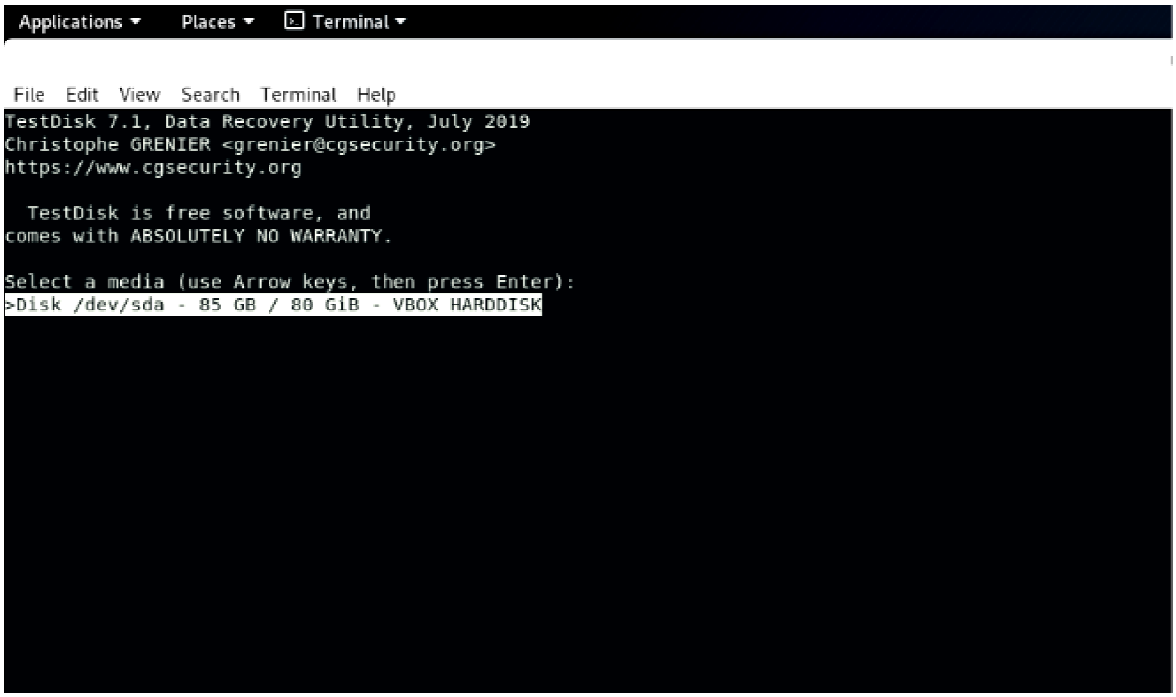

AccessData FTK Imager 3.4.2.6
File View Mode Help
Evidence Tree
\\.\PHYSICALDRIVE1
Partition 1 [14804MB]
THE SG CODE [FAT32]
[root]
System Volume Information
[unallocated space]
Unpartitioned Space [basic disk]
Export Results
0 folder(s) and 1 file(s) exported successfully.
23318 bytes copied.
OK
File List
Name Size Type Date Modif...
System Volume In... 16 Directory 04-02-2020...
ftk image 1.webp 23 Regular File 04-02-2020...
ftk image 1.webp... 10 File Slack
player.java 2 Regular File 04-02-2020...
Cursor pos = 0; clus = 7; log sec = 16640; phy sec = 24704
For User Guide, press F1
NUM
Type here to search
ENG
1041
05-02-2020

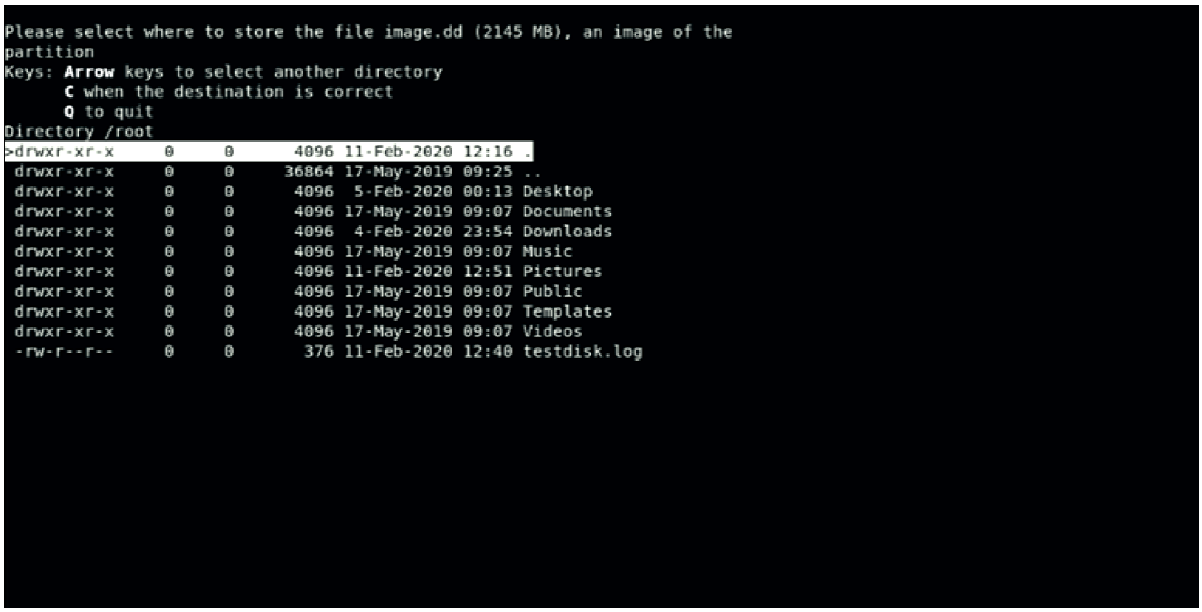
RECOVERING DELETED FILES ON LINUX SYSTEM

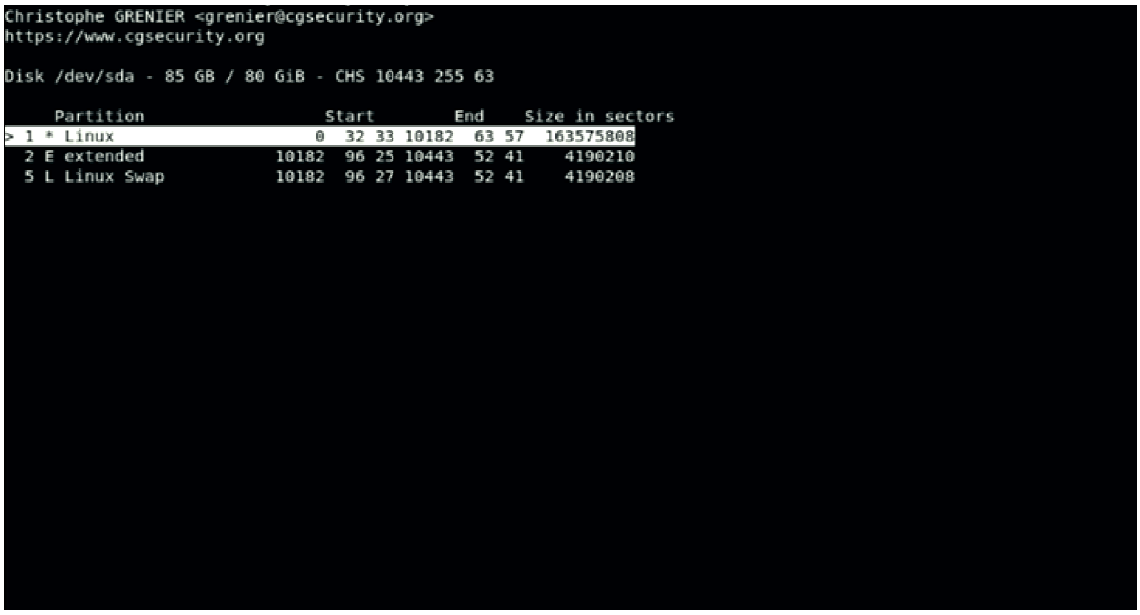
In this, we use tools such as TESTDISK which we downloaded from browser.

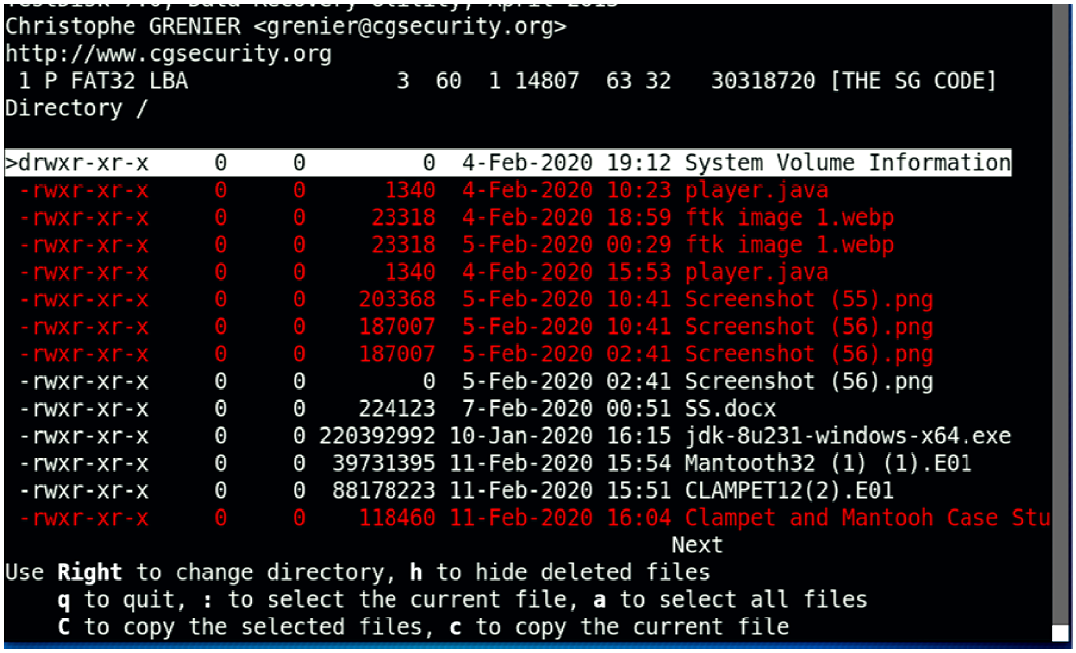
Test Disk is a free and open-source data recovery utility. It is primarily designed to help recover lost data storage partitions and/or make non-booting disks bootable again when these symptoms are caused by faulty software, certain types of viruses or human error.

Then we perform following commands to recover files on linux.


Applications
Places
Terminal
File Edit View Search Terminal Help
TestDisk 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
TestDisk is free software, and
comes with ABSOLUTELY NO WARRANTY.
Select a media (use Arrow keys, then press Enter):
>Disk /dev/sda - 85 GB / 80 GiB - VBOX HARDDISK


Please select where to store the file image.dd (2145 MB), an image of the
partition
Keys: Arrow keys to select another directory
C when the destination is correct
Q to quit
Directory /root
>drwxr-xr-x 0 0 4096 11-Feb-2020 12:16 .
drwxr-xr-x 0 0 36864 17-May-2019 09:25 ..
drwxr-xr-x 0 0 4096 5-Feb-2020 00:13 Desktop
drwxr-xr-x 0 0 4096 17-May-2019 09:07 Documents
drwxr-xr-x 0 0 4096 4-Feb-2020 23:54 Downloads
drwxr-xr-x 0 0 4096 17-May-2019 09:07 Music
drwxr-xr-x 0 0 4096 11-Feb-2020 12:51 Pictures
drwxr-xr-x 0 0 4096 17-May-2019 09:07 Public
drwxr-xr-x 0 0 4096 17-May-2019 09:07 Templates
drwxr-xr-x 0 0 4096 17-May-2019 09:07 Videos
-rw-r--r-- 0 0 376 11-Feb-2020 12:40 testdisk.log


Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org
Disk /dev/sda - 85 GB / 80 GiB - CHS 10443 255 63
Partition Start End Size in sectors
> 1 * Linux 0 32 33 10182 63 57 163575808
2 E extended 10182 96 25 10443 52 41 4190210
5 L Linux Swap 10182 96 27 10443 52 41 4190208


Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
1 P FAT32 LBA 3 60 1 14807 63 32 30318720 [THE SG CODE]
Directory /
>drwxr-xr-x 0 0 0 4-Feb-2020 19:12 System Volume Information
-rwxr-xr-x 0 0 1340 4-Feb-2020 10:23 player.java
-rwxr-xr-x 0 0 23318 4-Feb-2020 18:59 ftk image 1.webp
-rwxr-xr-x 0 0 23318 5-Feb-2020 00:29 ftk image 1.webp
-rwxr-xr-x 0 0 1340 4-Feb-2020 15:53 player.java
-rwxr-xr-x 0 0 203368 5-Feb-2020 10:41 Screenshot (55).png
-rwxr-xr-x 0 0 187007 5-Feb-2020 10:41 Screenshot (56).png
-rwxr-xr-x 0 0 187007 5-Feb-2020 02:41 Screenshot (56).png
-rwxr-xr-x 0 0 0 5-Feb-2020 02:41 Screenshot (56).png
-rwxr-xr-x 0 0 224123 7-Feb-2020 00:51 SS.docx
-rwxr-xr-x 0 0 220392992 10-Jan-2020 16:15 jdk-8u231-windows-x64.exe
-rwxr-xr-x 0 0 39731395 11-Feb-2020 15:54 Mantooth32 (1) (1).E01
-rwxr-xr-x 0 0 88178223 11-Feb-2020 15:51 CLAMPET12(2).E01
-rwxr-xr-x 0 0 118460 11-Feb-2020 16:04 Clampet and Mantooh Case Stu
Next
Use Right to change directory, h to hide deleted files
q to quit, : to select the current file, a to select all files
C to copy the selected files, c to copy the current file

EXPERIMENT – 7.B

GEORGE AND MARTHA CASE

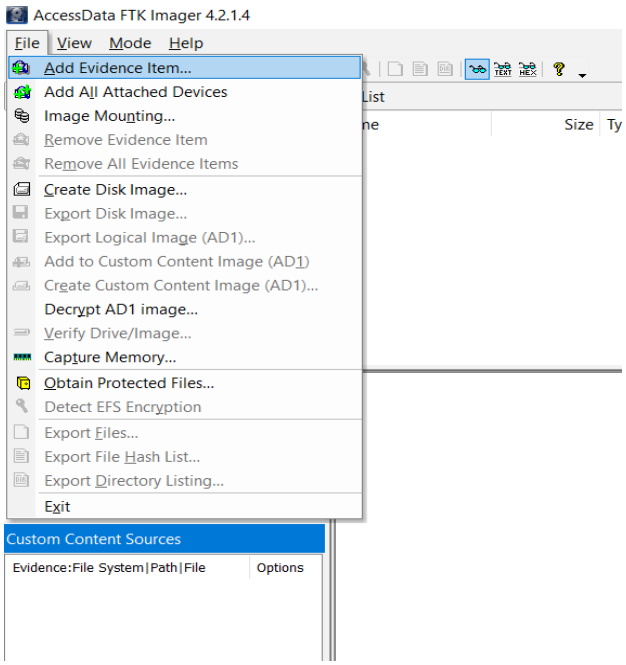
We have given a case of 2 people working in a company George and Martha.

George Montgomery has worked at a firm for several years and is now missing. Another employee, Martha, is also missing. No one knows where they are or has seen them in over a week, so Steve (George's supervisor) asks the IT Department to confiscate George's harddrive and all storage media in his work area.

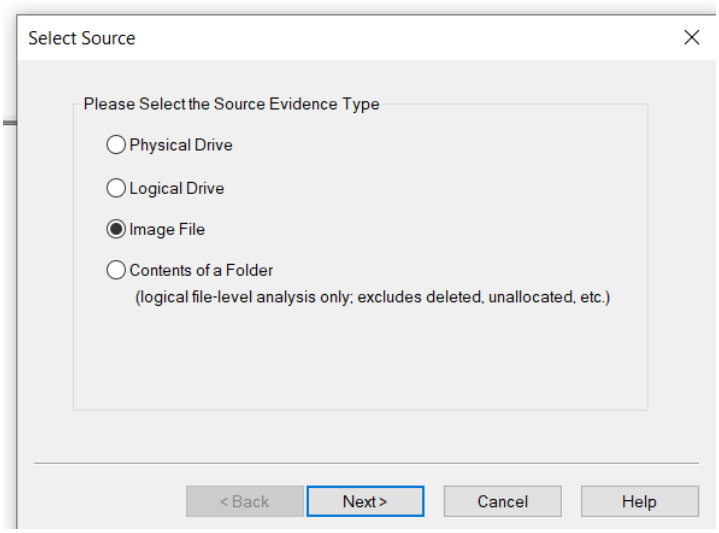
Investigate their scenario of what policies they broke and how they performed a theft of large amount of money.

Procedure:

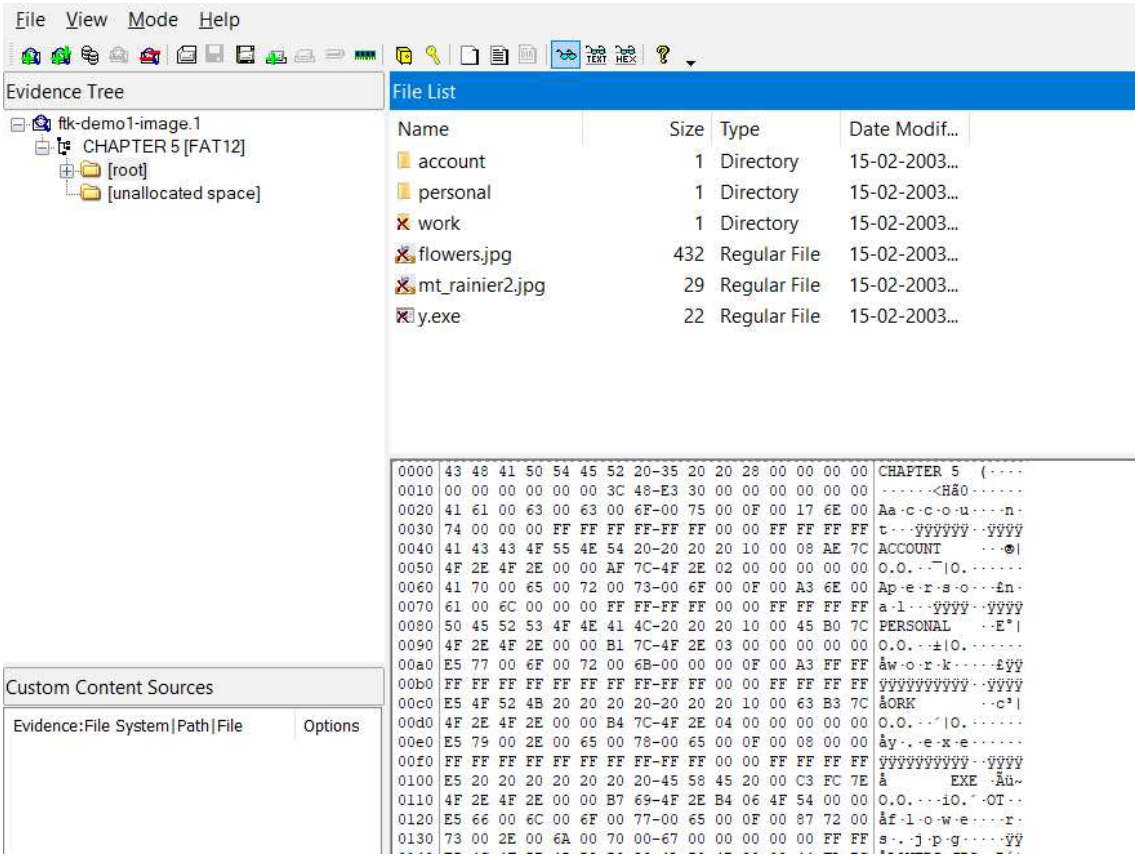
- Open the evidence file on FTK Imager using add evidence.



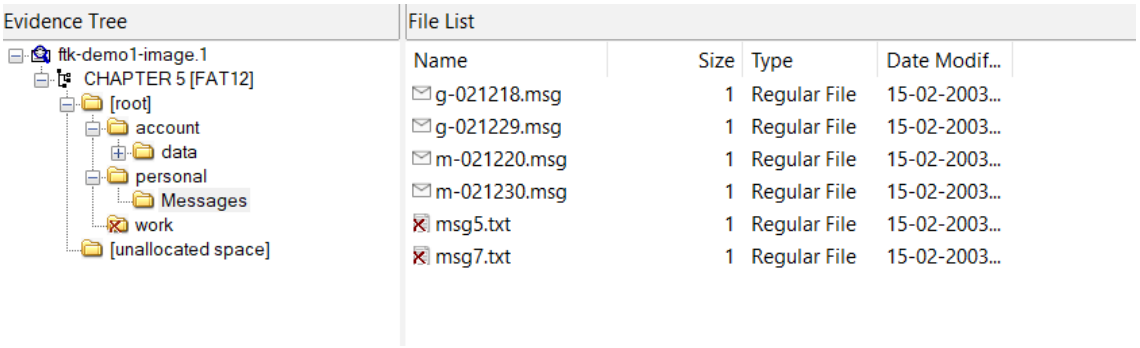
- Select image file.



- File's content will be loaded in the evidence tree. Click on the image to reveal folders.



- Check the personal>messages folder



- Upon reading the messages it was found that George was planning something illegal to get a lot of money.

```
From: Jones, George [mailto:georgej@widgets_intl.com]
Sent: 18 December 2001 18:37
To: James, Martha [marthaj@widgets_intl.com]
Subject: A plan


Martha,

I have a plan to pay for our vaction next Spring. I'll tell you about it later.

George
```

```
From: Jones, George [mailto:georgej@widgets_intl.com]
Sent: 29 December 2001 10:52
To: James, Martha [marthaj@widgets_intl.com]
Subject: Re: A plan

I can't talk about it now, it will have to wait until we can talk in private. Maybe Year's Eve.

George

------Original Message------
From: Jones, George [mailto:georgej@widgets_intl.com]
Sent: 26 December 2001 08:02
To: James, Martha [marthaj@widgets_intl.com]
Subject: A plan


Martha,

I have a plan to pay for our vaction next Spring. I'll tell you about it later.

George
```

George,

What are you talking about, what's the big deal?

Martha

------Original Message------
From: Jones, George [mailto:georgej@widgets_intl.com]
Sent: 29 December 2001 10:52
To: James, Martha [marthaj@widgets_intl.com]
Subject: Re: A plan

I can't talk about it now, it will have to wait until we can talk in private. Maybe Year's Eve.

George

- Some deleted texts were revealed too.

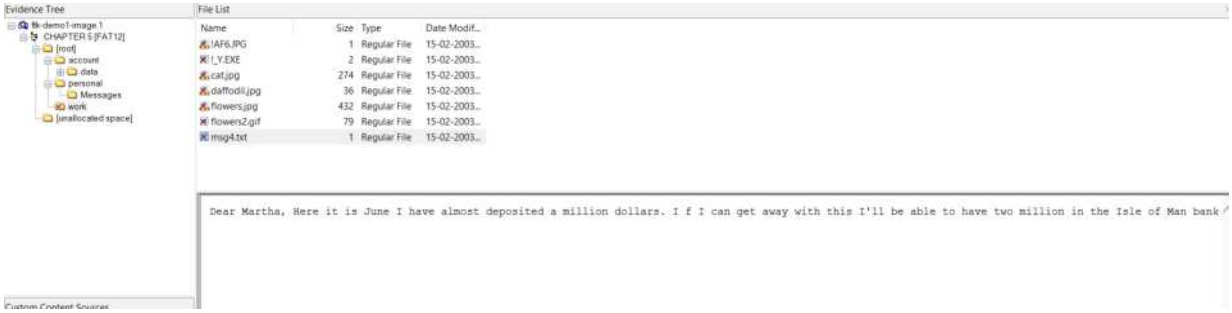
ear Mart ,

I've got a plan to get more cash. It involves rerouting invoices here at work to the field offices. It will take six months to get back here and we can be in Brazil enjoying the fruits of our labo

Mrge
Dr.

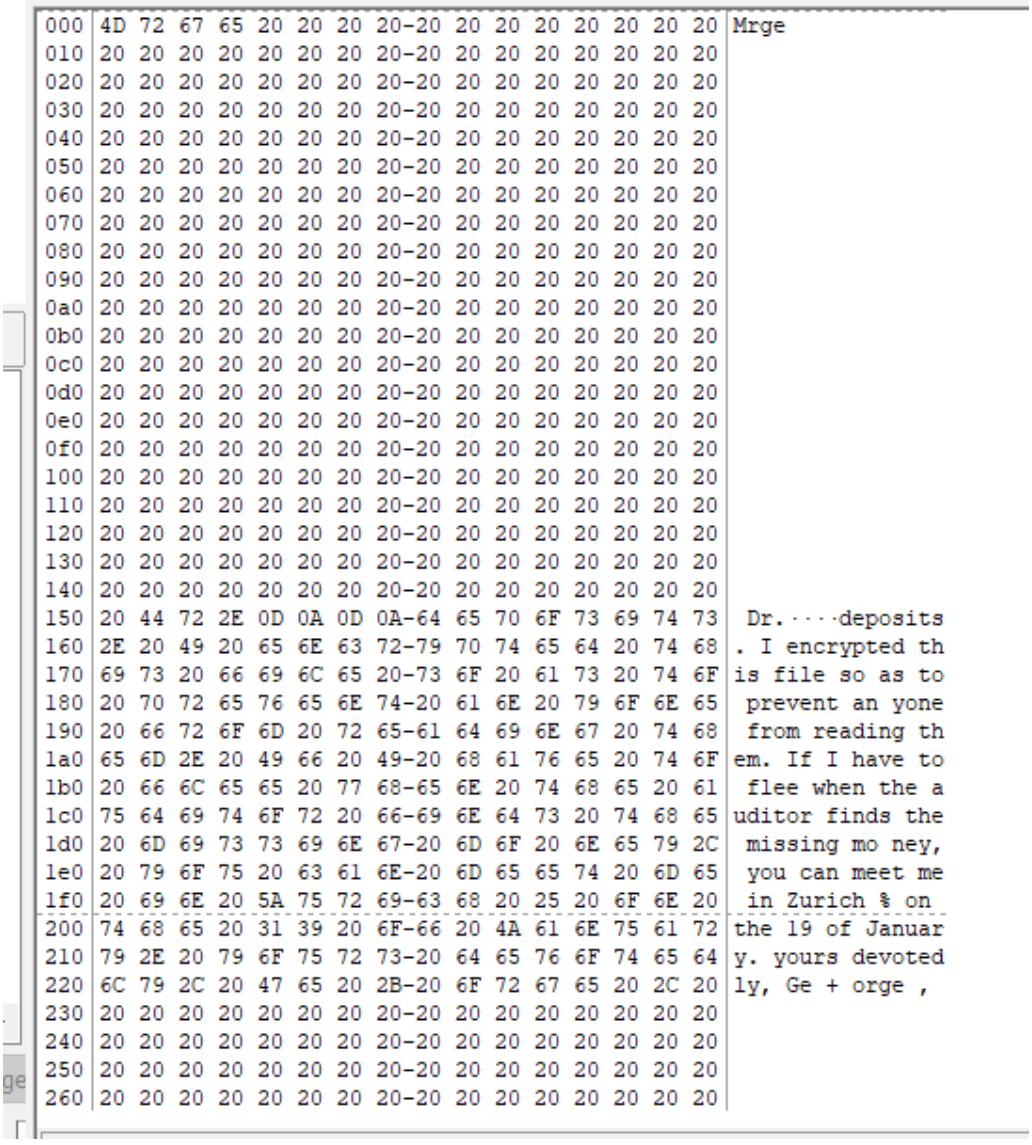
deposits. I encrypted this file so as to prevent an yone from reading them. If I have to flee when the auditor finds the missing mo ney, you can meet me in Zurich % on the 19 of January. yours devotedly, Ge + orge ,

- Check the work folder which was deleted.



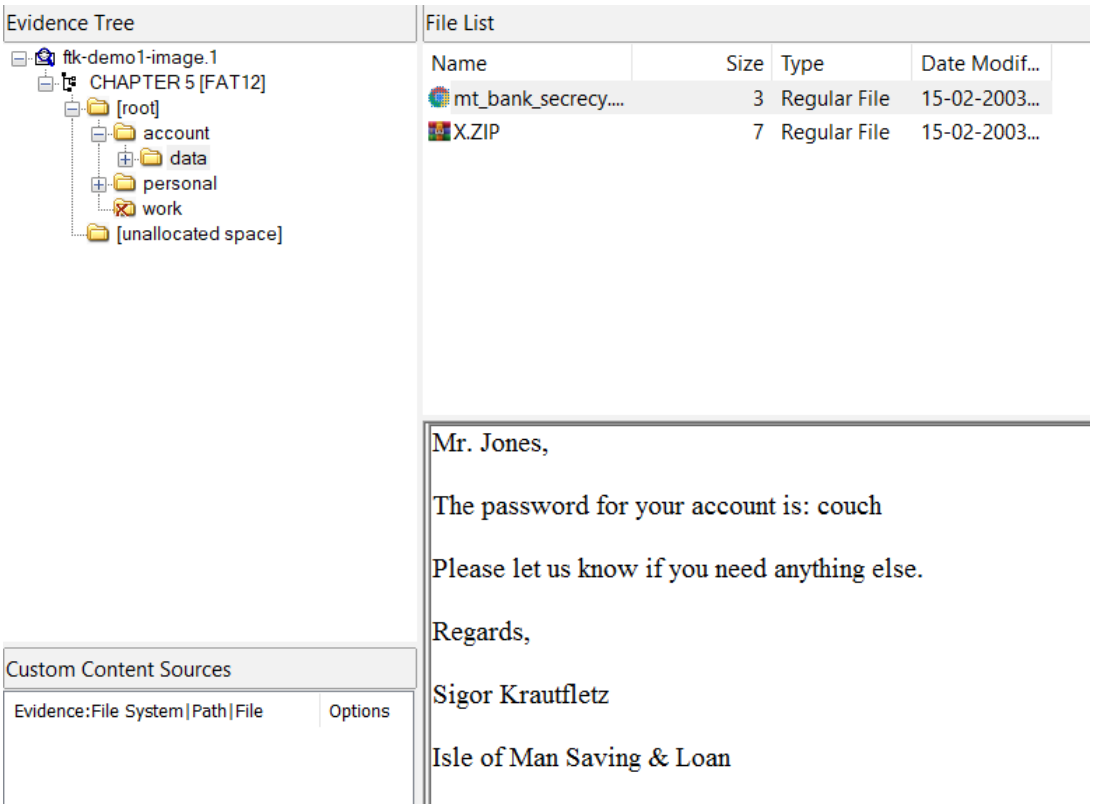
Dear Martha, Here it is June I have almost deposited a million dollars. I f I can get away with this I'll be able to have two million in the Isle of Man bank account by xmas time. more later, devo tedly yours, George

Name	Size	Type	Date Modif...
!AF6.JPG	1	Regular File	15-02-2003...
!_Y.EXE	2	Regular File	15-02-2003...
cat.jpg	274	Regular File	15-02-2003...
daffodil.jpg	36	Regular File	15-02-2003...
flowers.jpg	432	Regular File	15-02-2003...
flowers2.gif	79	Regular File	15-02-2003...
msg4.txt	1	Regular File	15-02-2003...

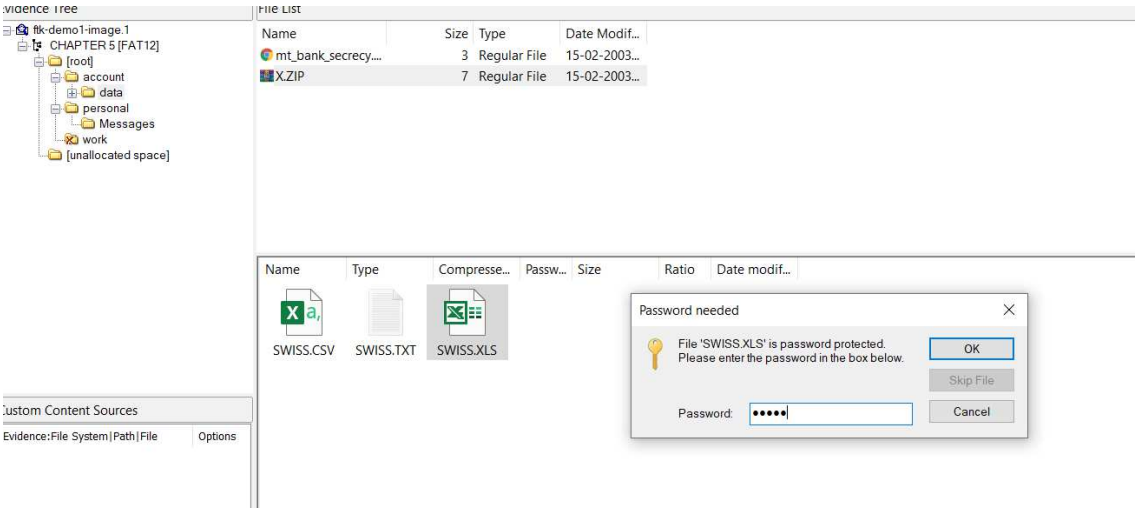


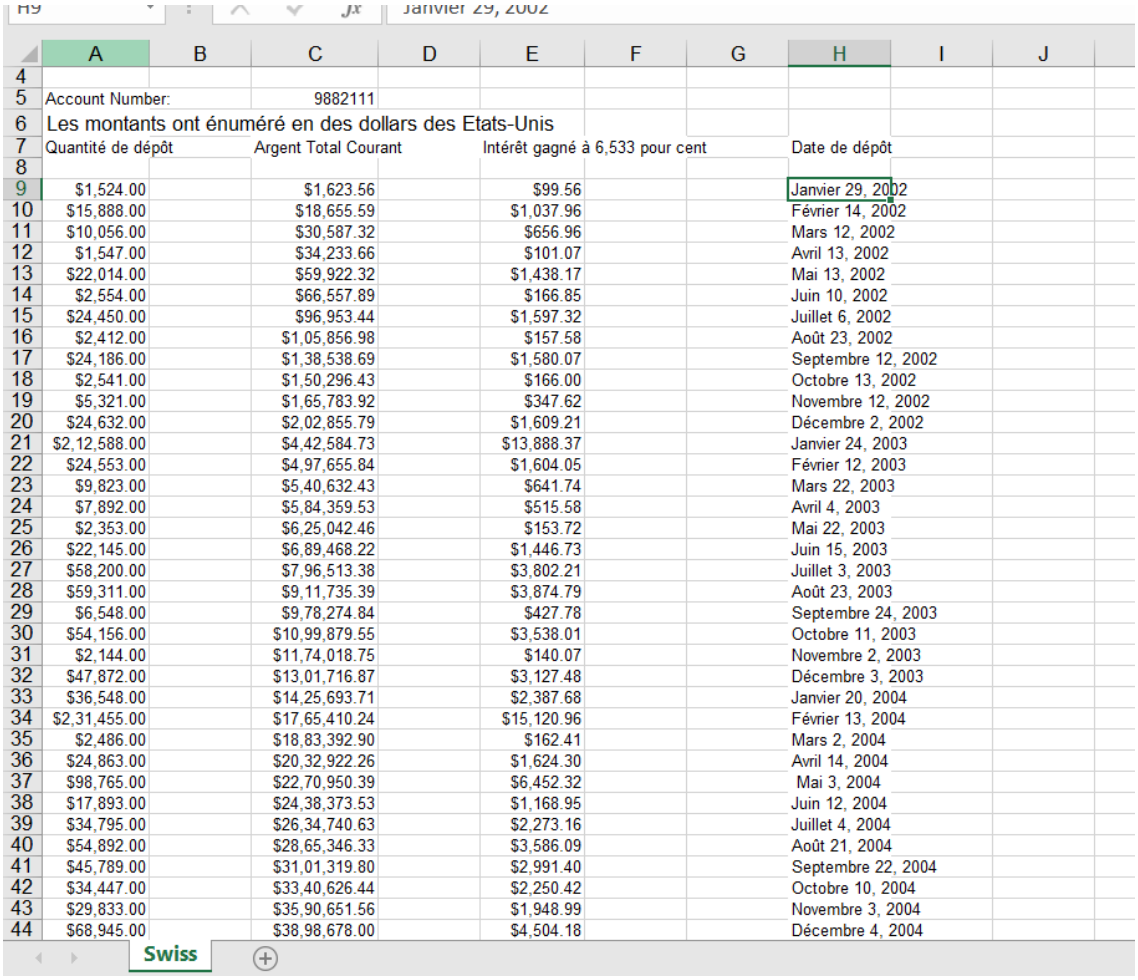
```
000 4D 72 67 65 20 20 20 20-20 20 20 20 20 20 20 20 Mrge
010 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
020 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
030 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
040 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
050 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
060 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
070 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
080 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
090 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
0a0 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
0b0 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
0c0 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
0d0 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
0e0 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
0f0 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
100 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
110 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
120 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
130 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
140 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
150 20 44 72 2E 0D 0A 0D 0A-64 65 70 6F 73 69 74 73  Dr.····deposits
160 2E 20 49 20 65 6E 63 72-79 70 74 65 64 20 74 68 . I encrypted th
170 69 73 20 66 69 6C 65 20-73 6F 20 61 73 20 74 6F is file so as to
180 20 70 72 65 76 65 6E 74-20 61 6E 20 79 6F 6E 65  prevent an yone
190 20 66 72 6F 6D 20 72 65-61 64 69 6E 67 20 74 68  from reading th
1a0 65 6D 2E 20 49 66 20 49-20 68 61 76 65 20 74 6F em. If I have to
1b0 20 66 6C 65 65 20 77 68-65 6E 20 74 68 65 20 61  flee when the a
1c0 75 64 69 74 6F 72 20 66-69 6E 64 73 20 74 68 65 uditor finds the
1d0 20 6D 69 73 73 69 6E 67-20 6D 6F 20 6E 65 79 2C  missing mo ney,
1e0 20 79 6F 75 20 63 61 6E-20 6D 65 65 74 20 6D 65  you can meet me
1f0 20 69 6E 20 5A 75 72 69-63 68 20 25 20 6F 6E 20  in Zurich % on
200 74 68 65 20 31 39 20 6F-66 20 4A 61 6E 75 61 72 the 19 of Januar
210 79 2E 20 79 6F 75 72 73-20 64 65 76 6F 74 65 64 y. yours devoted
220 6C 79 2C 20 47 65 20 2B-20 6F 72 67 65 20 2C 20 ly, Ge + orge ,
230 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
240 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
250 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
260 20 20 20 20 20 20 20 20-20 20 20 20 20 20 20 20
```

- Check the account>data folder. A web link reveals the password of a file to be “couch”.



- A zip file revealed some excel sheet which was opened using the password couch. It was a transaction sheet which showed illegal transactions made by George.





	A	B	C	D	E	F	G	H	I	J
4										
5	Account Number:		9882111							
6	Les montants ont énuméré en des dollars des Etats-Unis									
7	Quantité de dépôt		Argent Total Courant		Intérêt gagné à 6,533 pour cent			Date de dépôt		
8										
9	$1,524.00		$1,623.56		$99.56			Janvier 29, 2002		
10	$15,888.00		$18,655.59		$1,037.96			Février 14, 2002		
11	$10,056.00		$30,587.32		$656.96			Mars 12, 2002		
12	$1,547.00		$34,233.66		$101.07			Avril 13, 2002		
13	$22,014.00		$59,922.32		$1,438.17			Mai 13, 2002		
14	$2,554.00		$66,557.89		$166.85			Juin 10, 2002		
15	$24,450.00		$96,953.44		$1,597.32			Juillet 6, 2002		
16	$2,412.00		$1,05,856.98		$157.58			Août 23, 2002		
17	$24,186.00		$1,38,538.69		$1,580.07			Septembre 12, 2002		
18	$2,541.00		$1,50,296.43		$166.00			Octobre 13, 2002		
19	$5,321.00		$1,65,783.92		$347.62			Novembre 12, 2002		
20	$24,632.00		$2,02,855.79		$1,609.21			Décembre 2, 2002		
21	$2,12,588.00		$4,42,584.73		$13,888.37			Janvier 24, 2003		
22	$24,553.00		$4,97,655.84		$1,604.05			Février 12, 2003		
23	$9,823.00		$5,40,632.43		$641.74			Mars 22, 2003		
24	$7,892.00		$5,84,359.53		$515.58			Avril 4, 2003		
25	$2,353.00		$6,25,042.46		$153.72			Mai 22, 2003		
26	$22,145.00		$6,89,468.22		$1,446.73			Juin 15, 2003		
27	$58,200.00		$7,96,513.38		$3,802.21			Juillet 3, 2003		
28	$59,311.00		$9,11,735.39		$3,874.79			Août 23, 2003		
29	$6,548.00		$9,78,274.84		$427.78			Septembre 24, 2003		
30	$54,156.00		$10,99,879.55		$3,538.01			Octobre 11, 2003		
31	$2,144.00		$11,74,018.75		$140.07			Novembre 2, 2003		
32	$47,872.00		$13,01,716.87		$3,127.48			Décembre 3, 2003		
33	$36,548.00		$14,25,693.71		$2,387.68			Janvier 20, 2004		
34	$2,31,455.00		$17,65,410.24		$15,120.96			Février 13, 2004		
35	$2,486.00		$18,83,392.90		$162.41			Mars 2, 2004		
36	$24,863.00		$20,32,922.26		$1,624.30			Avril 14, 2004		
37	$98,765.00		$22,70,950.39		$6,452.32			Mai 3, 2004		
38	$17,893.00		$24,38,373.53		$1,168.95			Juin 12, 2004		
39	$34,795.00		$26,34,740.63		$2,273.16			Juillet 4, 2004		
40	$54,892.00		$28,65,346.33		$3,586.09			Août 21, 2004		
41	$45,789.00		$31,01,319.80		$2,991.40			Septembre 22, 2004		
42	$34,447.00		$33,40,626.44		$2,250.42			Octobre 10, 2004		
43	$29,833.00		$35,90,651.56		$1,948.99			Novembre 3, 2004		
44	$68,945.00		$38,98,678.00		$4,504.18			Décembre 4, 2004		

Swiss

- The unallocated folder revealed some further deleted files which upon recovery showed following:

Dear Mart ,

I've got a plan to get more cash. It involves rerouting invoices here at work to the field offices. It will take six months to get back here and we can be in Brazil enjoying the fruits of our labo
I'll tell you more about it when I get it started.

Yours always, George

Conclusion: George did some rerouting with his company's money to transfer it to his own account while sharing details of the same with Martha through emails and messages. Files for the same were found in the personal folder of George. An excel sheet of transactions of his account further proved that such transactions were made.

This proved that George and Martha were involved in the forgery.

EXPERIMENT 8.a

EMAIL FORENSICS

Email forensics refers to analyzing the source and content of emails as evidence. Investigation of email related crimes and incident involves various approaches.

Analyzing Email Header

- **View the Message Header in Google Mail (GMail) Webmail:**

  Login to your account on the webpage and open the message (click on it). Click on the "down-arrow" on the top-right of the message and select "Show Original". Now you will see the complete message source.

- **View the Message Header in Yahoo! Mail Webmail:**

  Login to your account on the webpage and open the message (click on it).
  Click on "Actions" and select "View Full Header".

- **View the Message Header in Hotmail Webmail:**

  Login to your account on the webpage and go to the message list.
  Right-click on the message and select "View Message Source".

- **View the Message Header in MS Outlook:**

  Open the message in MS Outlook. Now go to "View" and select "Message Options" - or "File" -> "Info" -> "Properties".

Look at "Internet Headers”

- **View the Message Header in Thunderbird:**

  Open the message, then click on "View" and select "Message Source".

- **View the Message Header in MS Windows Mail (and MS Outlook Express):**

  Select the message in the list, right-click on it and select "Properties" and go to "Details.

- **Standard Email Header Fields**

- Return Path: The email address which should be used for bounces.
  The mail server will send a message to the specified email address if the message cannot be delivered.
- Delivery-date: The data the message was delivered.
- Date: The date the message was sent.
- Message-ID: The ID of the message.
- X-Mailer: The mail client (mail program) used to send the message
- From: The message sender in the format: "Friendly Name" <email@address.tld>

- To: The message recipient in the format: "Friendly Name" <email@address.tld>

- Subject: The message subject

Recovering Emails:

1. Open Outlook.
2. Select the "Deleted Items" folder.
3. Go to the "Tools >> Recover Deleted Items from server"
4. Select the email(s) that you would like to recover.
5. Click the "Recover Selected Items" button (the icon is an email message with an arrow).
6. The email will go back to the "Deleted Items" folder it was in. (You may need to select another folder and then reselect this folder for it to appear.)

Similar methods can be used for all mailboxes.

Email Protocols

Email protocol is a standard method for exchanging information between email clients like Thunderbird, Apple Mail, or Mailbird and email provider's servers like Gmail, Outlook, Yahoo, and vice versa.

Following are some common Email Protocols:

SMTP: As the name suggests, Simple Message Transfer Protocol is responsible for email transfers between email clients (Windows Mail, Thunderbird, etc.) and email providers' servers (Gmail, Outlook, Yahoo). Companies use their SMTP server for email marketing and for sending automated transactional emails.

POP3: Email clients use Post Office Protocol 3 for retrieving messages from email servers. Email clients that use POP3 store messages on the user's computer, deleting them from the email server. People using email clients with POP3 also have the option of keeping their emails on the server after download.

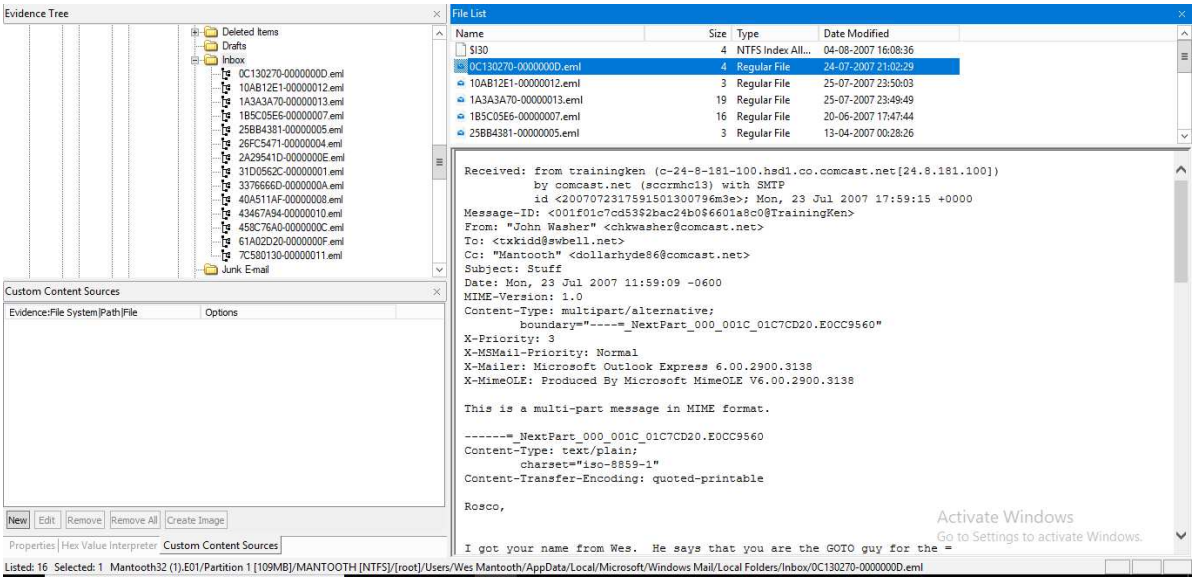
IMAP: Internet Message Access Protocol is similar to POP3, but unlike it, IMAP allows multiple users to send emails at a time. This is a helpful feature for business owners, who assign communication with customers to different team members — especially when they need to have access to one email address at one time.

EXPERIMENT 8.b

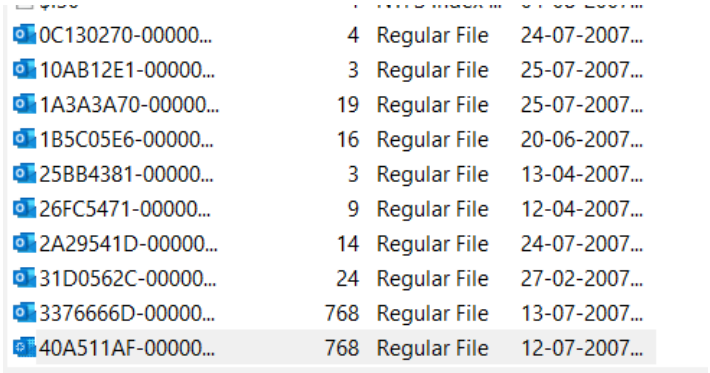
Case Study: Wes Mantooth

1. **Under the email category find the following details:**

a. Appointments: 11
b. Contacts: 8
c. Mails: 22
d. Notes: 4
e. Tasks: 5



2. **Look and bookmark 10 email messages?**



3. **An email was received by Wes Mantooth regarding a contact in Bujumbura, Africa. Locate the email and answer following:**

   a. **When was the email sent**

   08/01/2007

   b. **List all the parties associated with the email and note down their email.**

   RascoBadguy, chkwasher@comcast.com, dollarhyde86@comcast.com, skimmerman27@hotmail.com, molarman420@gmail.com

   c. **Are there any attachment to the email? If so, what are the file names?**

   Yes, there are attachments to the mail:
   Confidential Business Letter.doc

   d. **What is the originating email server ip address?**

   66.196.96.95

   e. **In which email box is this email located?**

   In Outlook.pst file, inside Inbox.

4. **Use an Index search, attempt to identify the real names associated with discovered email addresses?**

nail Address	**ame**
kwasher@comcast.com	hn Washer
llarhyde86@comcast.com	es Mantooth
olarman420@hotmail.com	es Mantooth
immerman27@hotmail.com	vid Thomas
kidd@swbell.net	scoBadguy

5. **Wes Mantooth sent an email to his mom. What is his mom's email?**

toothfairy@mentaldental.com

```
From: "Wes Mantooth" <dollarhyde86@comcast.net>
To: <toothfairy@mentaldental.com>
Subject: Hey Mom
Date: Thu, 12 Jul 2007 17:36:36 -0600
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_NextPart_000_0011_01C7C4AB.32251050"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Windows Mail 6.0.6000.16480
X-MimeOLE: Produced By Microsoft MimeOLE V6.0.6000.16480

This is a multi-part message in MIME format.
```

6. **What event was he discussed with his mother?**

He discussed about a Wedding Event with his mother. He mentioned that her mother needed his wedding pic which he got to know by his dad.

```
Hey there mom.  How is it going?

Dad said that you needed a pic of me for the weding announcment?

Here is a good one.

Thanks for all your help with that.  I am so busy with school, I don't =
know how I would have planned it!

Love ya!
```

7. **Wes Mantooth has a friend by name Joan Acetone. Where does he work?**

Yes, He had a friend by name Joan Acetone. He worked at ''Arbys, Inc.''

8. **Wes Mantooth dad had been away for a while. Wes mentioned him in a letter to someone called "sweetie". Where was his dad?**

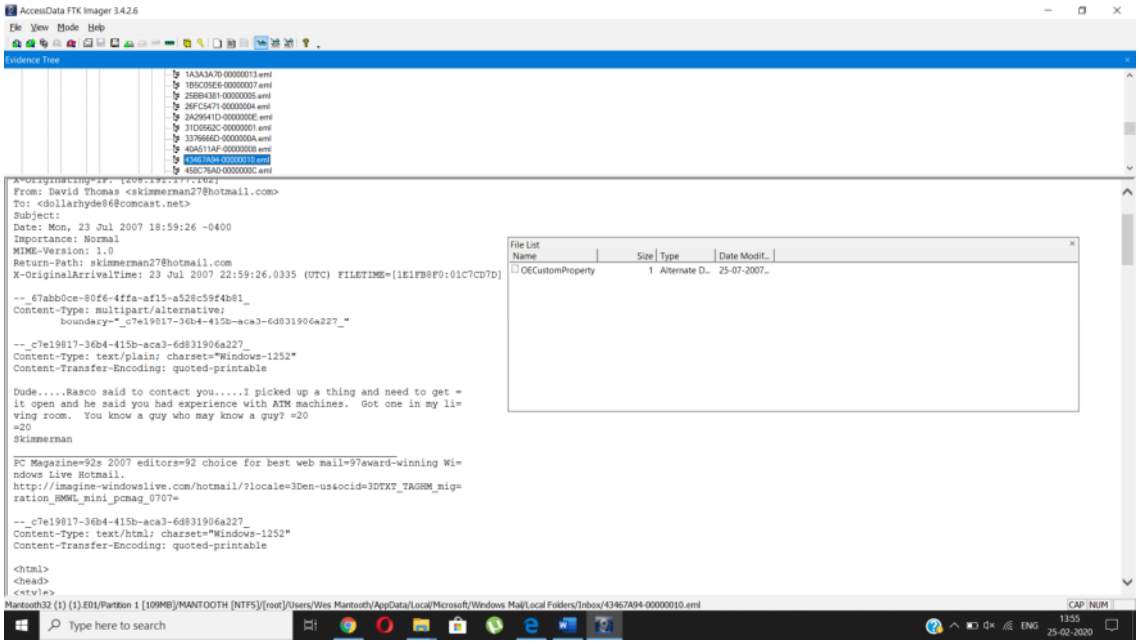
Mantooth's dad was just released from jail. (Dear Sweetie.doc)

9. **Wes Mantooth has a list of names of possible associates, two of which are john washer and Simple Simon. What is the name of the file where this information is located?**

~arl730.xar

10. **The word is that Wes is talking to Rasco about ragging ATM Machine card readers. Use the case evidence to verify this rumor and identify who else was involved. What is the accomplice real name?**

David Thomas – skimmerman27@hotmail.com



11. **What is the washer's AIM username?**

Washergonebad

Conclusion:

1. After a thorough investigation into Wes Mantooth's flash drive, I believe there is sufficient evidence to support illegal activity in many areas. Wes Mantooth has supported this evidence with emails between John Washer, Rasco Badguy, and David Thomas.

2. In these emails, Wes Mantooth discusses check, ATM, credit card, and prescription fraud. Also David Thomas produced evidence that showed he stole an ATM machine and was trying to break into it. There are plenty of pictures sent in these emails to show specific activities in these fraudulent areas.

3. He also found on the flash drive are illegal drug activities which include the production and sales of methamphetamines and marijuana. On this flash drive, there were two partitions set up that include both an EXT2 and NTFS files system. The NTFS files system included the bulk of the space used on the flash drive, and almost all of the evidence. Typically Windows is unable to see a second partition on a flash drive and it is a great way to hide things, since most people tend to use windows based machines and not Linux.

4. There were also 22 encrypted files stored on this flash drive. Three of these files are included in the report but the third file was only a picture of the front and back on a 1 million dollar bill.

EXPERIMENT 9.a

WEB BROWSER FORENSICS

Browser forensic is mainly used for analyzing things like browsing history and general web activity of a PC to check for suspicious usage or content that has been accessed. This also refers to monitoring traffic on a webpage and analysis of LOG files from server to get actual information about targeted machine.

Working of Web Browser

A Web browser is actually a software application that runs on your Internet-connected computer. It allows you to view Web pages, as well as use other content and technologies such as video, graphics files, and digital certificates, to name a few.

Browsers are able to display Web pages largely in part to an underlying Web protocol called HyperText Transfer Protocol (HTTP). HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. It is what allows Web clients and Web servers to communicate with each other. When you enter a Web address (URL) in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page and display the information in your browser. All Web servers serving Web sites and pages support the HTTP protocol.

Web browser forensic artifacts

Of course, each web browser leaves its own individual artifacts in the operating system. Types of artifacts from the web browser can vary depending on the version of the web browser. Typically, when researching artifacts of web browsers, you can extract the following types of artifacts:

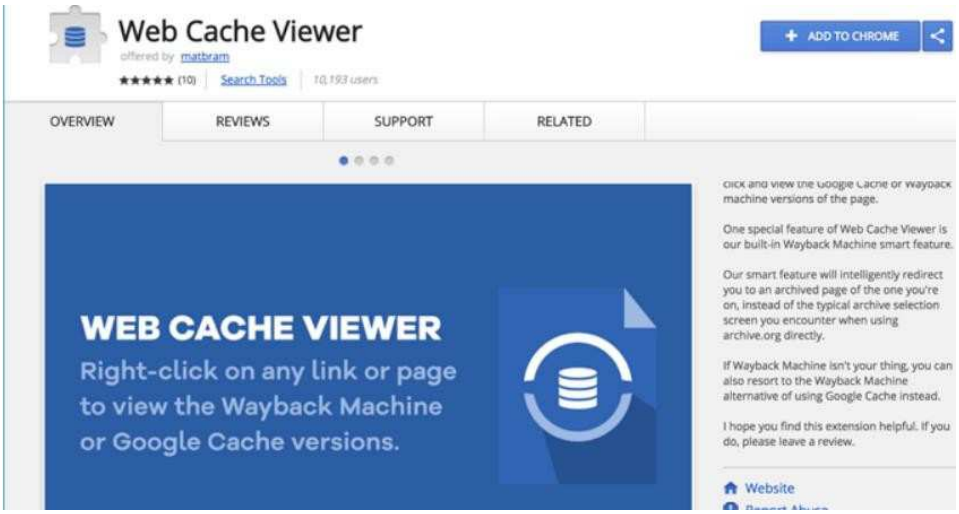
- History
- Cache
- Cookies
- Typed URLs

- Sessions
- Most visited sites

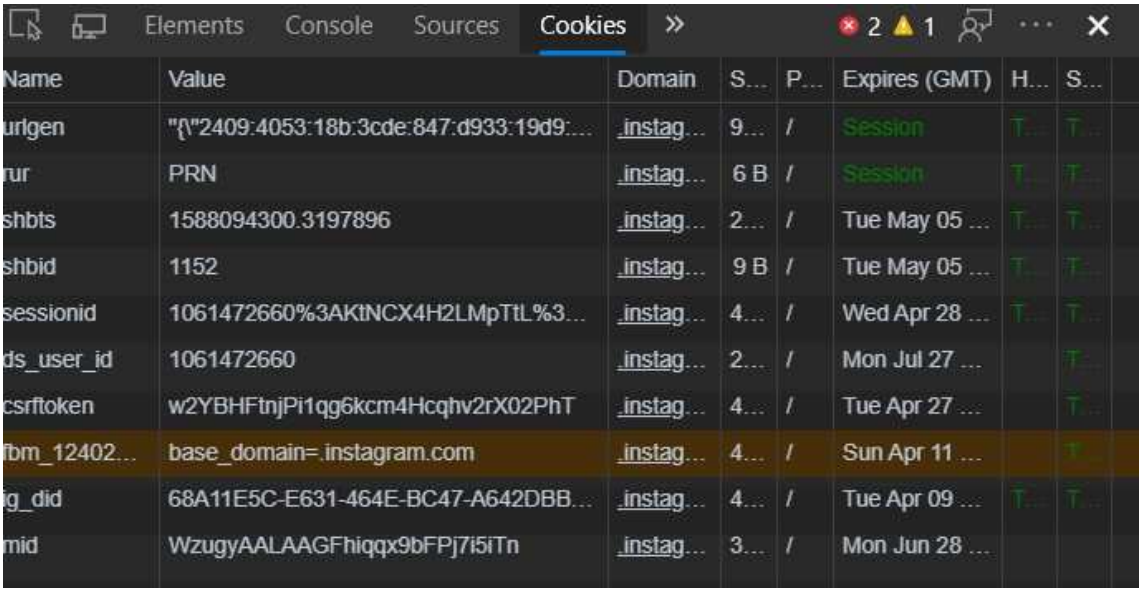
History and Favourites

View Cache Files Using Chrome Extension

1. Open your Chrome browser and go to the Chrome Web Store.
2. Search for "Web Cache Viewer" and add it on your browser. After installation, you can right-click on any web link in Chrome and choose "Web Cache Viewer". You can choose to view the cached page from either Wayback Machine or Google archive.



Cookie Analysis

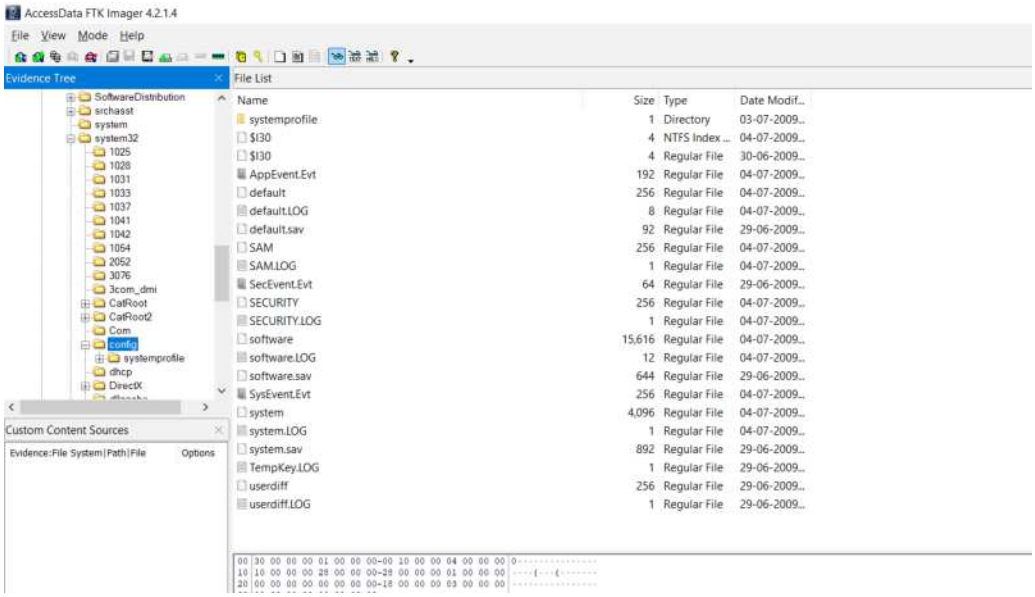


EXPERIMENT 9.b

Case Study: Granny Clampet

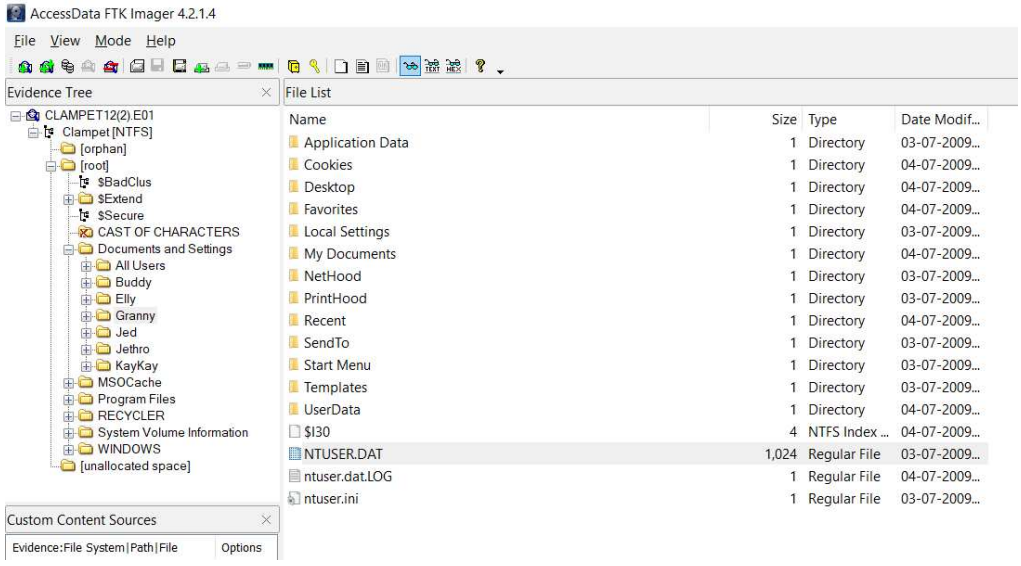
1. **Export all the registry files from the evidence?**

   For exporting config registry files go to following path :
   [root]\WINDOWS\system32\config\software



   For exporting NTUSER.DAT file go to following path:

   [root]\Documents and Settings\Granny\NTUSER.DAT



2. **Police suspect that Internet activity played a role, what internet sites did the suspect last visit?**

url1	REG_SZ	http://www.google.com/
url2	REG_SZ	http://www.live.com/
url3	REG_SZ	http://www.yahoo.com/
url4	REG_SZ	http://www.dogpile.com/
url5	REG_SZ	http://www.microsoft.com/isapi/redir.dll?prd=ie&p...

NTUSER.DAT[3548].tmp\Software\Microsoft\Internet Explorer\TypedURLs

3. **What was Granny's Internet Explorer home page?**

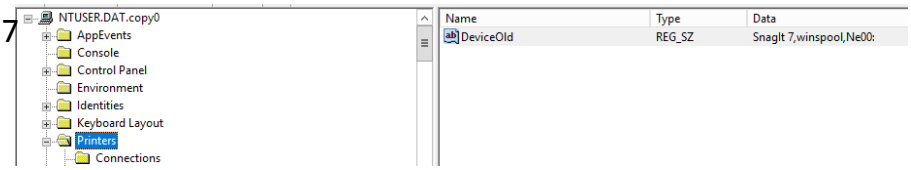
http://www.dogpile.com/

Start Page	REG_SZ	http://www.dogpile.com/

NTUSER.DAT[3548].tmp\Software\Microsoft\Internet Explorer\Main

4. **A. What printer was Granny using?**

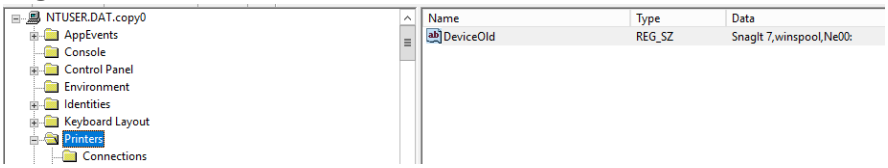
SnagIt 7



NTUSER.DAT[3548].tmp\Printers

B. What was Buddy's default printer?

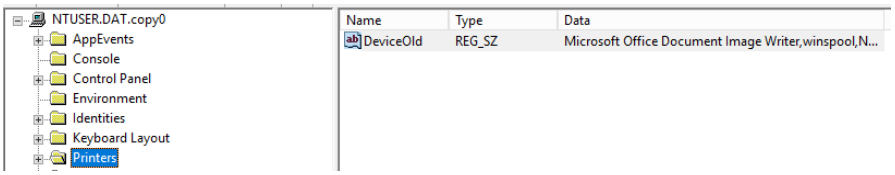
SnagIt 7



NTUSER.DAT[2269].tmp\Printers

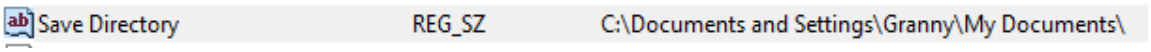
C. What was Jethro's default printer?

Microsoft Office Document Image Writer



NTUSER.DAT[2242].tmp\Printers

5. **What was the last location that Granny downloaded something from using Internet Explorer?**



NTUSER.DAT[3548].tmp\Software\Microsoft\Internet Explorer\Main

6. **Generate a report based on Granny's NTUSER.DAT file**

Registry Information

Registry Viewer Report

Granny's NTUSER.DAT file

Software\Microsoft\Internet Explorer\TypedURLs

Last Written Time 7/3/2009 22:34:22 UTC

Name	Type	Data
url1	REG_SZ	http://www.google.com/
url2	REG_SZ	http://www.live.com/
url3	REG_SZ	http://www.yahoo.com/
url4	REG_SZ	http://www.dogpile.com/
url5	REG_SZ	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome

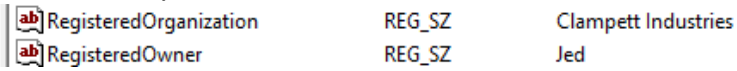
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

7. **Jethro maintained an email account. See if you can provide evidence of this account from the Inetcomm server Passwords area of protected storage system provider?**

Jethro email account
smurferator@gmail.com
NTUSER.DAT[2242].tmp\Software\Microsoft\Protected Storage System Provider\S-1-5-21-1409082233-2049760794-839522115-1003\Internet Explorer\Internet Explorer\email:StringData

8. **A. Who is the registered owner and what is the registered organization?**

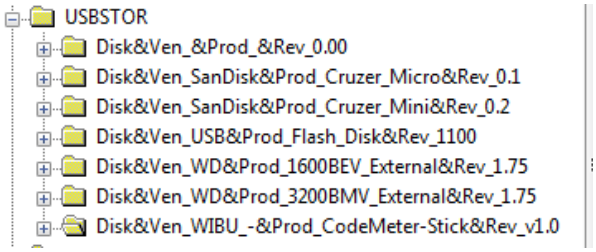
Jed, Clampett Industries



software[2314].tmp\Microsoft\Windows NT\CurrentVersion

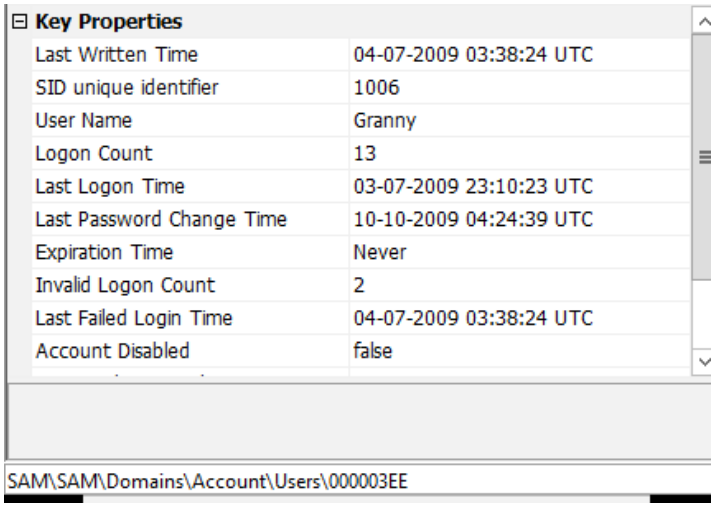
B. Investigators found some portable devices in the parlor? Can you give them any that can help them determine if any external or portable devices have been connected to the computer?

Yes, Investigators found some portable devices. They are listed as follows :



system[2310].tmp\ControlSet001\Enum\USBSTOR

C. Document when Granny last logged on to this machine
7/3/2009 23:10:23 UTC
SAM[2320].tmp\SAM\Domains\Account\Users\000003EE



D. Generate a Report based on the System File.

Registry Viewer Report

Registry Information

Granny's NTUSER.DAT file

Software\Microsoft\Internet Explorer\TypedURLs

Last Written Time	7/3/2009 22:34:22 UTC

Name	Type	Data
url1	REG_SZ	http://www.google.com/
url2	REG_SZ	http://www.live.com/
url3	REG_SZ	http://www.yahoo.com/
url4	REG_SZ	http://www.dogpile.com/
url5	REG_SZ	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Last Written Time	7/3/2009 23:31:27 UTC

Name	Type	Data
MRUListEx	REG_BINARY	MRU ordered list : 27, 26, 25, 24, 0, 23, 22, 16, 17, 21, 20, 1, 2, 19, 18, 15, 10, 14, 13, 12, 11, 9, 8, 7, 6, 5, 4, 3
27	REG_BINARY	Shortcut Target Name : Customers.xls Shortcut Name (ASCII) : Customers.lnk Shortcut Name (Unicode) : Customers.lnk
26	REG_BINARY	Shortcut Target Name : New Microsoft Excel Worksheet.xls Shortcut Name (ASCII) : New Microsoft Excel Worksheet.lnk Shortcut Name (Unicode) : New Microsoft Excel Worksheet.lnk
25	REG_BINARY	Shortcut Target Name : Apology number 2.doc Shortcut Name (ASCII) : Apology number 2.lnk Shortcut Name (Unicode) : Apology number 2.lnk
24	REG_BINARY	Shortcut Target Name : Apology.doc Shortcut Name (ASCII) : Apology.lnk Shortcut Name (Unicode) : Apology.lnk
0	REG_BINARY	Shortcut Target Name : Thank You Letter.doc Shortcut Name (ASCII) : Thank You Letter.lnk Shortcut Name (Unicode) : Thank You Letter.lnk