

DIGITAL FORENSICS LAB

Submitted to - Mr. Prateek Gupta

Submitted by - Kashish Srivastava

500067405

R134218079

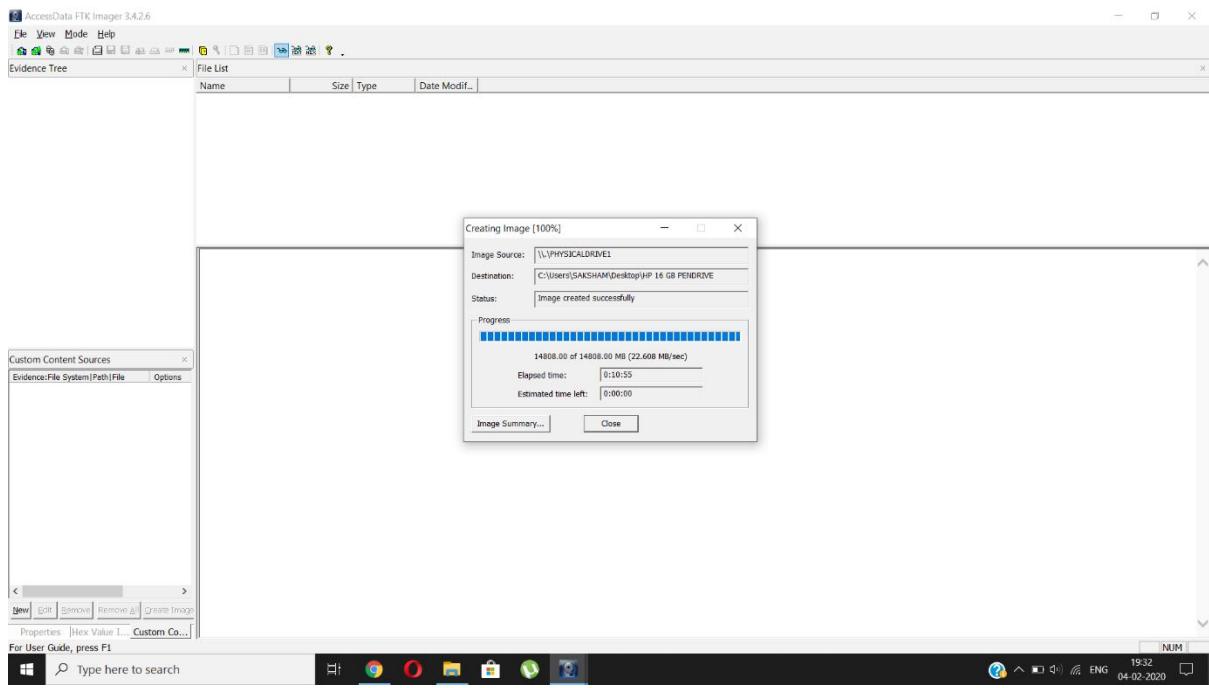
EXPERIMENT – 1

Creating a Forensics Image using FTK IMAGER

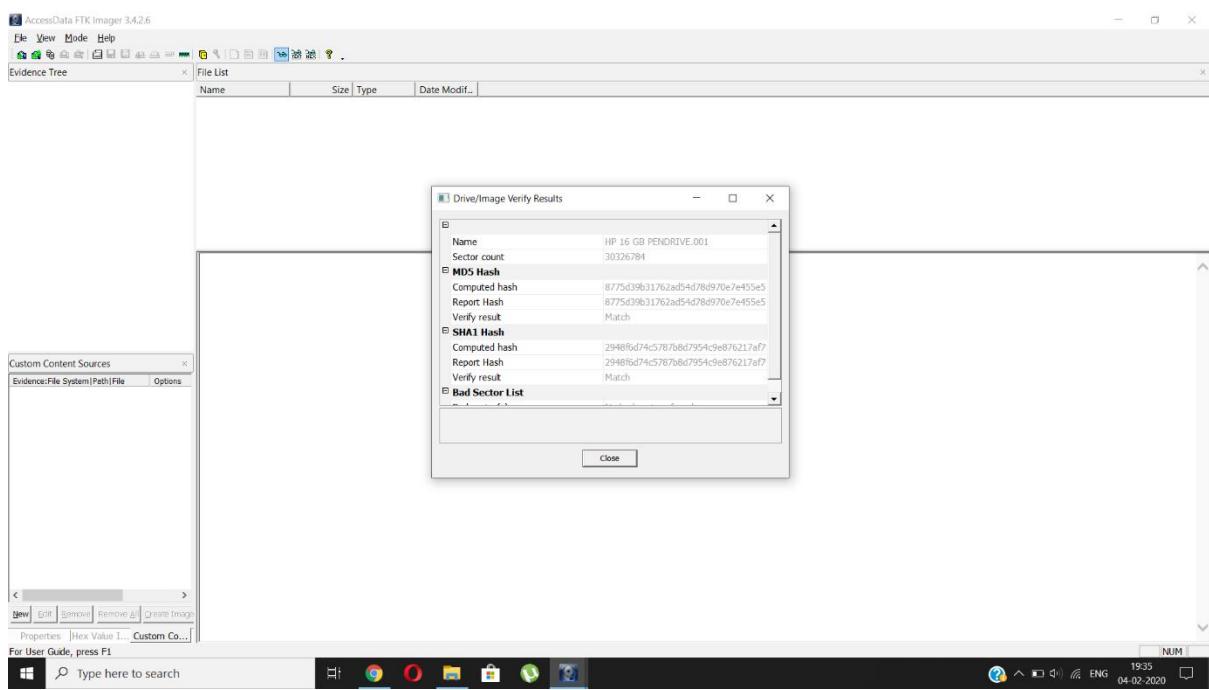
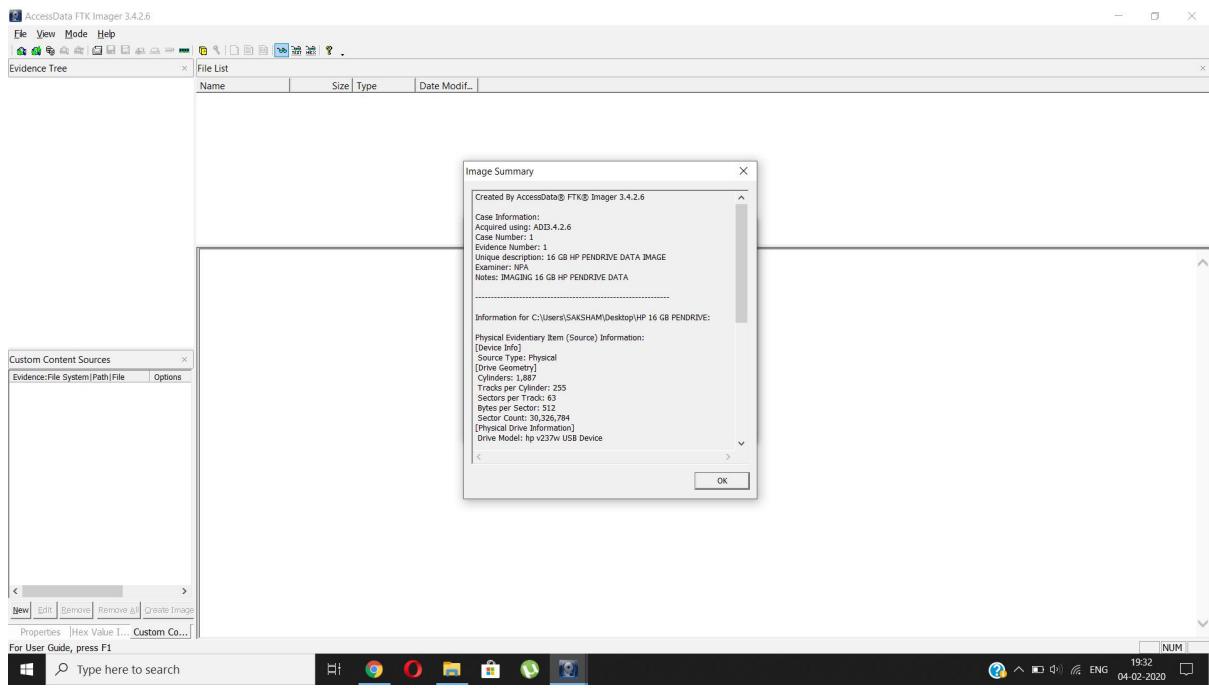
FTK Imager is a Windows acquisition tool and it can be download directly from Access Data website (<http://accessdata.com/>) for free of cost. FTK Imager is available in two types “FTK Imager” and “FTK Imager Lite”. Both the softwares have same features and functions. Only difference is lite version can be run from a Pendrive or External Source, so Setup is not required for this version. The version used for Second task is FTK Imager liteversion 3.4.2.2. Note: The hash values(in both tasks) have to be saved or noted down some where for further analysis to check the integrity of the image before Forensic analysis and after Forensics analysis.

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.



3. After clicking on the icon, the page will be opened
4. After selecting the device type, click on "Next" button to proceed, the page will be opened
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
7. After clicking on "Next" button, the page will be displayed
8. 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.

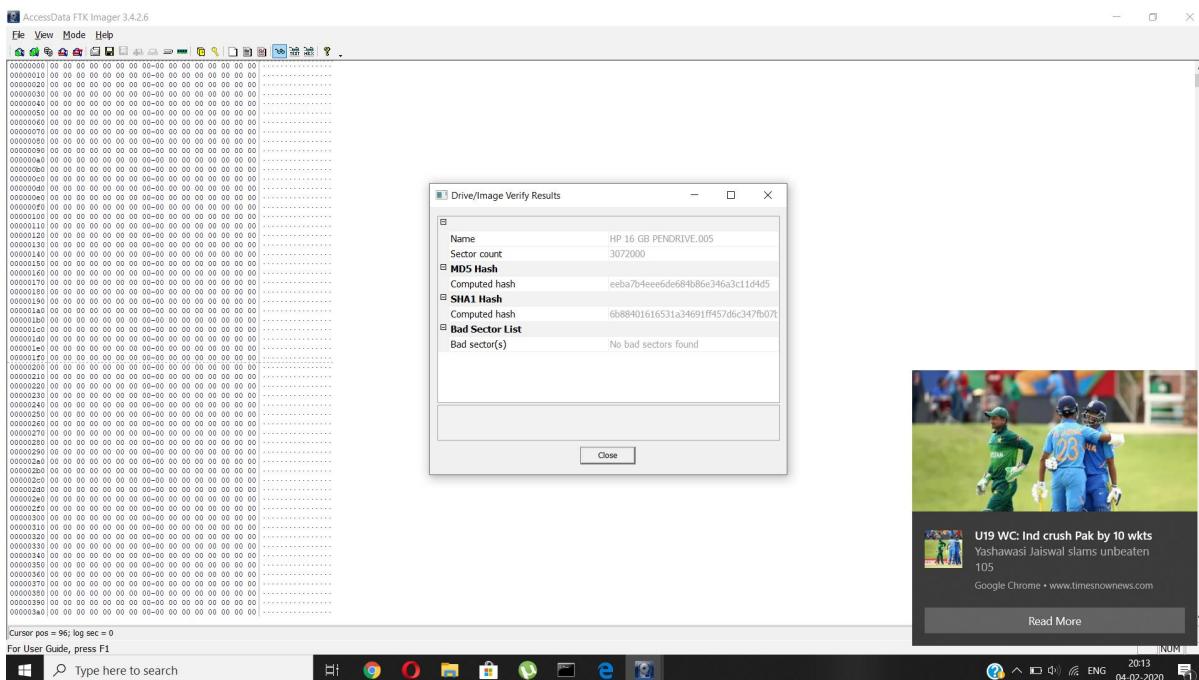
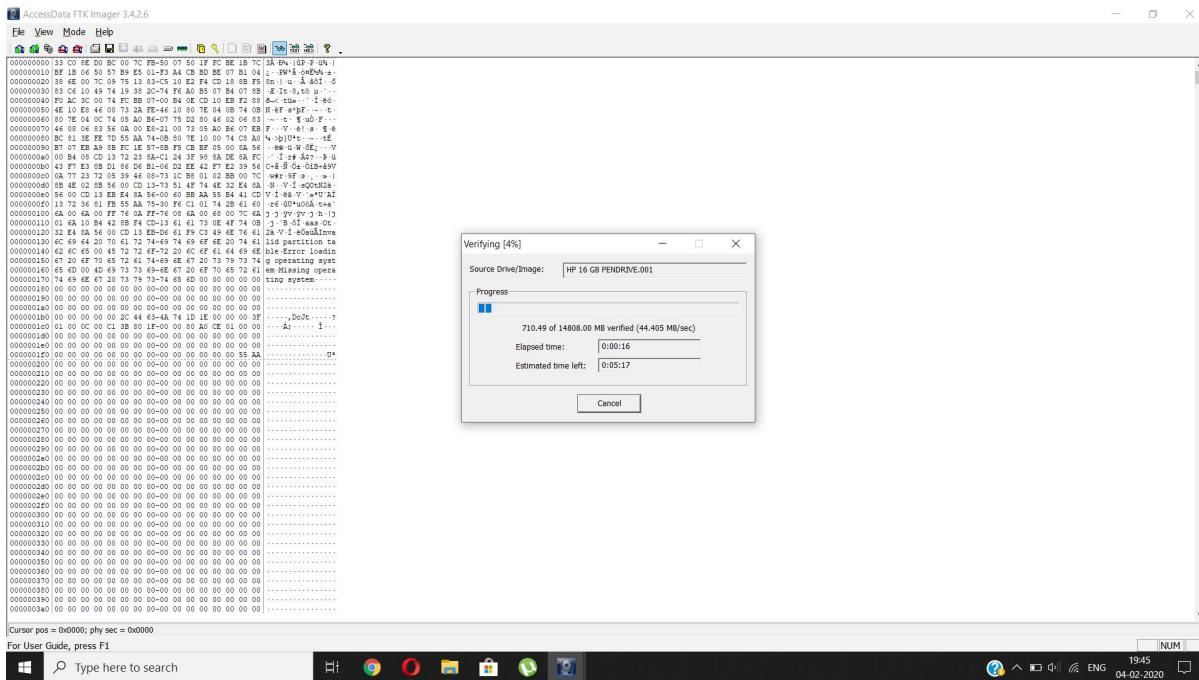


TASK II: Hashing

Download and Install FTK Imager 3.4.2 for this task

Verify the MD5 SHA1 hash value of an image Using FTK Imager version 3.4

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

VOLATILITY

Forensics case study-Stuxnet

Volatility is one of the best open source software programs for analyzing RAM in 32 bit/64 bit systems. It supports analysis for Linux, Windows, Mac, and Android systems. It is based on Python and can be run on Windows, Linux, and Mac systems. It can analyze raw dumps, crash dumps, VMware dumps.

In this experiment, we analyse a image of a file called stuxnet.vmem.

In this , we first find all the process in that file and their ID'S.

Stuxnet is a malicious computer worm, first uncovered in 2010, thought to have been in development since at least 2005. Stuxnet targets supervisory control and data acquisition systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran.

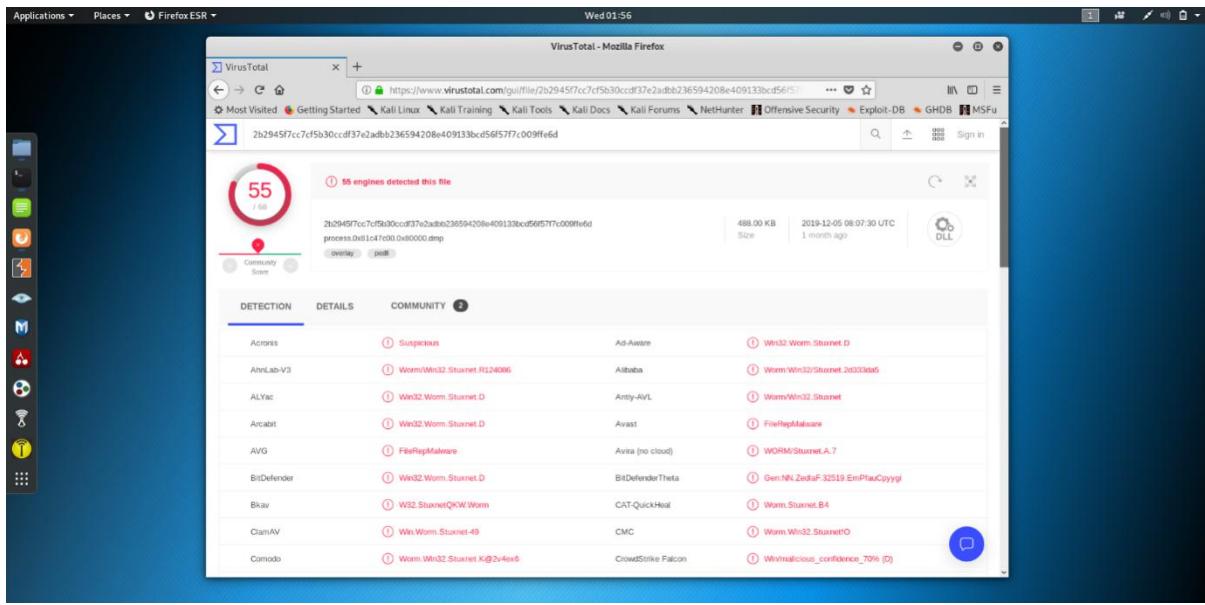
COMMAND USED : volatility -f stuxnet.vmem pslist

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

COMMAND USED : volatility -f Stuxnet.vmem malfind -p 1928 –dump-dir Stuxnet

"**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**.

The screenshot shows the Volatility Framework interface running on Kali Linux. The main window displays a memory dump of the lsass.exe process (PID 1928). The memory dump is shown as a hex dump with columns for Address, Value, and Type. A search bar at the top right allows for filtering the dump. Below the dump, various memory structures are identified, such as 'MZ', 'PE', and 'DLL'. On the left, a navigation pane shows the current file path: /Downloads/volatility - t stuxnet.vmem malfind - p 1928 --dump-dir stuxnet. The bottom status bar indicates the date and time (Wed 01:57) and the user (root:kali: ~/Downloads).



Then we upload files created on virustotal.com where we can find some malwares.

EXPERIMENT – 3

Creating Ram Dump using FTK and VOLATILITY

HERE WE CREATE IMAGE OF OUR RAM DUMP AND CREATE A RAM DUMP.

THEN IN IT WE APPLY SAME PROCESS WHICH WE DID FOR STUXNET.VMEM.

AND WE WILL FIND MALWARES IN IT.

root@kali:~# cd Desktop
root@kali:~/Desktop# volatility -f memdump.mem imageinfo
bash: volatility: command not found
root@kali:~/Desktop# volatility -f memdump.mem imageinfo
Volatility Framework Version 2.5.0-dev
INFO : volatility.debug : Determining profile based on KDBG search...
... Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
AS Layer1 : FileAddressSpace (/root/Desktop/memdump.mem)
PAE type : No PAE
DTB : 0x319000L
KDB : 0x27c94b6L
Number of Processors : 32
Image Type (Service Pack) : -
KPCR for CPU 0 : 0xffff5b495L
KPCR for CPU 1 : 0xffff5b495L
KPCR for CPU 2 : 0xffff5b495L
KPCR for CPU 3 : 0xffff5b495L
KPCR for CPU 4 : 0xffffd6d5b6L
KPCR for CPU 5 : 0xffffd6d5b6L
KPCR for CPU 6 : 0xffffd6d5b6L
KPCR for CPU 7 : 0xffffd6d5b6L
KPCR for CPU 8 : 0xffffd6d5b6L
KPCR for CPU 9 : 0xffffd6d5b6L
KPCR for CPU 10 : 0xffffd6d5b6L
KPCR for CPU 11 : 0xffffd6d5b6L
KPCR for CPU 12 : 0xffffd6d5b6L
KPCR for CPU 13 : 0xffffd6d5b6L
KPCR for CPU 14 : 0xffffd6d5b6L
KPCR for CPU 15 : 0xffffd6d5b6L
KPCR for CPU 16 : 0xffffd6d5b6L
KPCR for CPU 17 : 0xffffd6d5b6L
KPCR for CPU 18 : 0xffffd6d5b6L
KPCR for CPU 19 : 0xffffd6d5b6L
KPCR for CPU 20 : 0xffffd6d5b6L
KPCR for CPU 21 : 0xffffd6d5b6L
KPCR for CPU 22 : 0xffffd6d5b6L
KPCR for CPU 23 : 0xffffd6d5b6L
KPCR for CPU 24 : 0xffffd6d5b6L
KPCR for CPU 25 : 0xffffd6d5b6L
KPCR for CPU 26 : 0xffffd6d5b6L
KPCR for CPU 27 : 0xffffd6d5b6L
KPCR for CPU 28 : 0xffffd6d5b6L
KPCR for CPU 29 : 0xffffd6d5b6L
KPCR for CPU 30 : 0xffffd6d5b6L
KPCR for CPU 31 : 0xffffd6d5b6L
Image date and time : 1970-01-01 00:00:00 UTC+0000
Image local date and time : 1970-01-01 00:00:00 +0000

25 engines detected this file

	SHA-256	5b136147911b041f0126ce82dfd24c4e2c79553b65d3240ecea2dcab4452dc5	
25 / 63	File name	AcroSpeedLaunch.exe	
	File size	28.5 KB	
	Last analysis	2018-03-21 06:29:58 UTC	
Detection	Details	Behavior	Community
Ad-Aware	Trojan.GenericKD.30403828	AegisLab	Uds.Dangerousobject.Multi:c
ALYac	Trojan.GenericKD.30403828	Arcabit	Trojan.Generic.D1CFECF4
Avira	TR/Drop.Decay.izv	AVware	Trojan.Win32.Generic!BT
BitDefender	Trojan.GenericKD.30403828	CAT-QuickHeal	Trojan.Multi
Comodo	UnclassifiedMalware	Cylance	Unsafe
Emsisoft	Trojan.GenericKD.30403828 (B)	eScan	Trojan.GenericKD.30403828
F-Secure	Trojan.GenericKD.30403828	Fortinet	PossibleThreat
GData	Trojan.GenericKD.30403828	Ikarus	Trojan.Dropper.Decay
Kaspersky	UDS:DangerousObject.Multi.Generic	MAX	malware (ai score=99)
McAfee	Artemis!12CF6583F5A9	McAfee-GW-Edition	Artemis
Qihoo-360	Win32/Trojan.Multi.daf	Sophos AV	Mal/Generic-S
Symantec	Trojan.Gen.2	VIPRE	Trojan.Win32.Generic!BT
ZoneAlarm	UDS:DangerousObject.Multi.Generic	AhnLab-V3	Clean
AntiLy-AVL	Clean	Avast	Clean
Avast Mobile Security	Clean	AVG	Clean

EXPERIMENT – 4

Recovering abd Inspecting deleted files

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

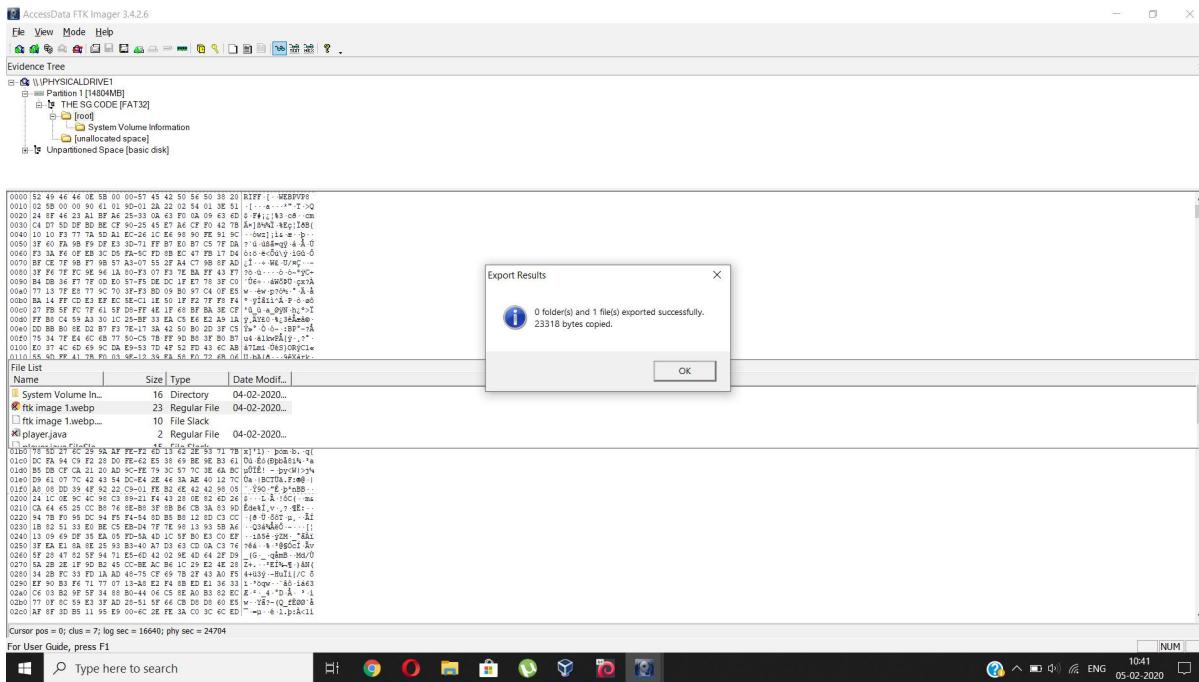
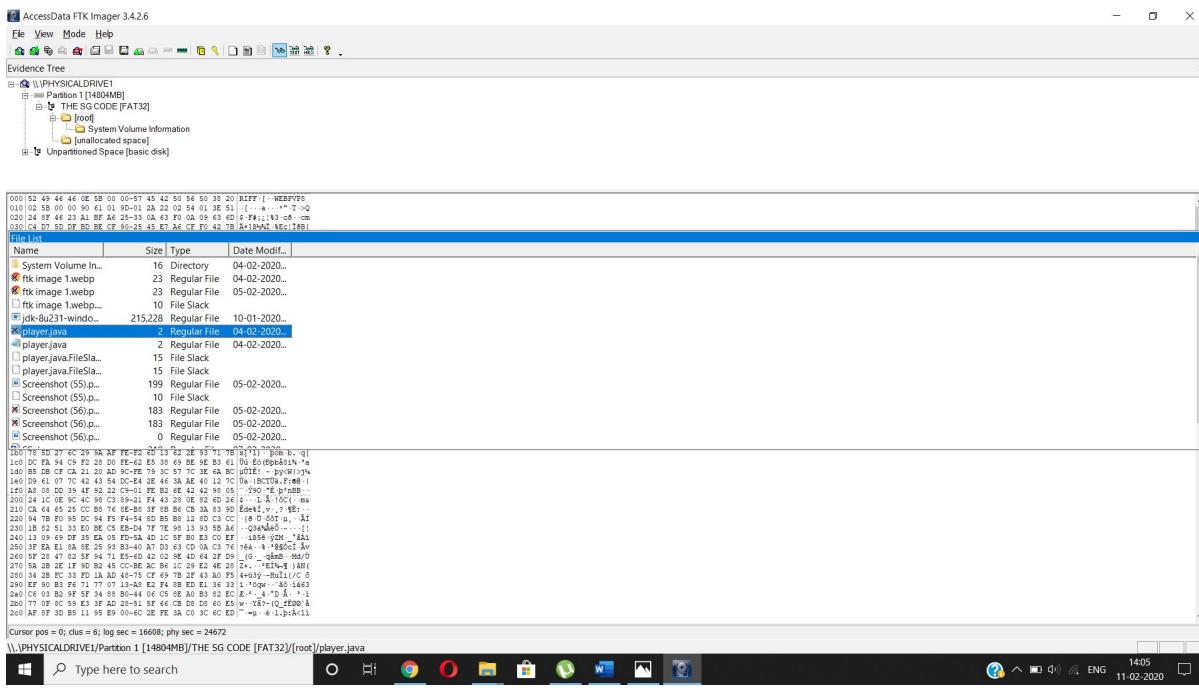
We achieve this by using FTK imager tool by deleting some files from the pen drive and then finding the deleted items on it.

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 :



EXPERIMENT – 5

GEORGE AND MARTHA CASE

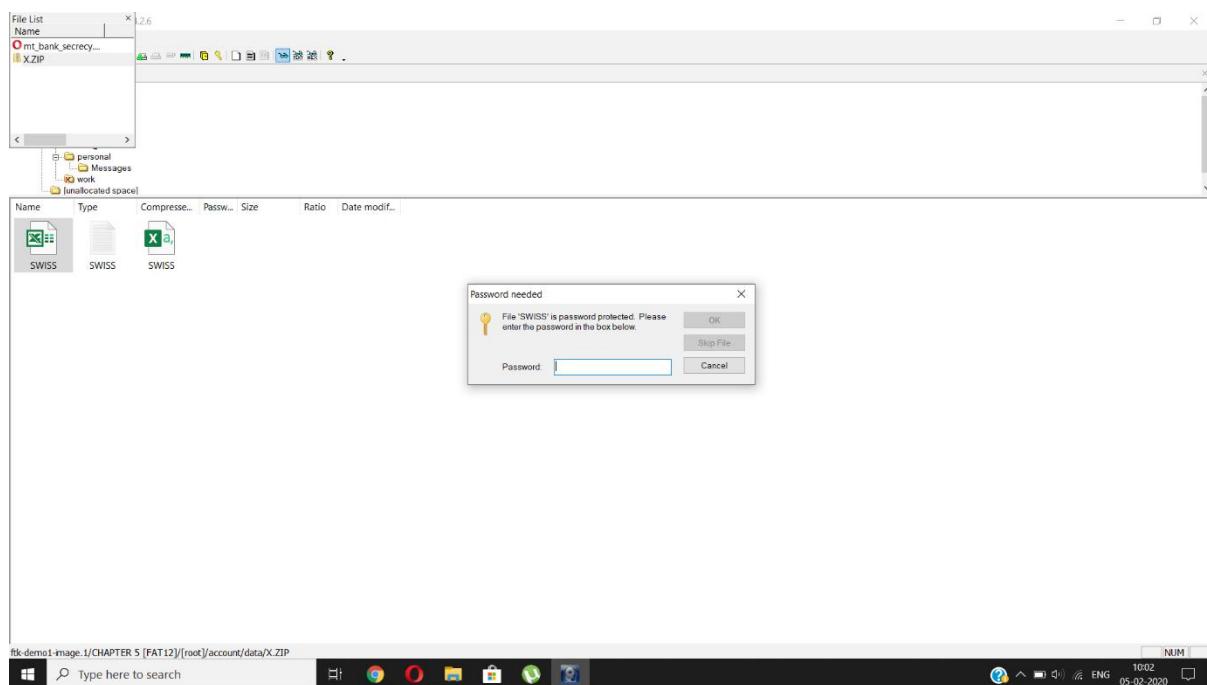
We have given a case of 2 people working in a company George and Martha.

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 hard drive 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.

For this we use FTK imager tool to recover deleted files and to investigate their case so as to find out how they did this crime.

1. Launch FTK Imager
2. Select File > Add Evidence Item
3. Select "image file" and proceed to add the file
4. Under the "Evidence Tree", right click your file and select Verify Drive/Image



AccessData FTK Imager 3.4.2.6

Evidence Tree

- CHAPTERS5[FAT12]
 - root
 - account
 - data
 - X ZIP
 - personal
 - Messages
 - wolf
 - [unallocated space]

Mr. Jones,
The password for your account is: couch
Please let us know if you need anything else.
Regards,
Sigor Krautfletz
Isle of Man Saving & Loan

File List

Name	Size	Type	Date Modif...
mt_bank_secrecy...	3	Regular File	15-02-2003
XZIP	7	Regular File	15-02-2003

ftk-demo1-image.1/CHAPTER 5 [FAT12]/[root]/account/data/mt_bank_secrecy.htm

Windows Taskbar: Type here to search, Start button, Task View, Chrome, File Explorer, Control Panel, System, Taskbar icons, Network, ENG, 1009, 05-02-2020

SWISS [Compatibility Mode] - Excel

saksham garg

File Home Insert Page Layout Formulas Data Review View Help Tell me what you want to do

Cut Copy Paste Format Painter Clipboard Font Alignment Number Styles Conditional Formatting Table Insert Delete Format Cells Sort & Filter Clear Editing

H9 : Janvier 29, 2002

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
1																						
2	Goneo Internationale																					
3	Autres liens																					
4																						
5	Account Number:	8882111																				
6	Les montants ont énumérés en des dollars des Etats-Unis																					
7	Quantité de dépôt	Argent Total Courant	Intérêt gagné à 6.533 pour cent	Date de dépôt																		
8	\$1,524.00	\$1,623.56	\$99.56	Janvier 29, 2002																		
9	\$15,886.00	\$18,655.59	\$1,037.96	Février 14, 2002																		
10	\$15,886.00	\$18,655.59	\$1,037.96	Mars 11, 2002																		
11	\$15,886.00	\$18,655.59	\$1,037.96	Avril 13, 2002																		
12	\$1,547.00	\$34,233.66	\$101.07	May 13, 2002																		
13	\$22,014.00	\$59,922.32	\$1,438.17	June 10, 2002																		
14	\$2,554.00	\$66,557.89	\$166.85	July 8, 2002																		
15	\$2,554.00	\$69,111.94	\$177.72	Septembre 23, 2002																		
16	\$2,412.00	\$10,856.98	\$157.58	Octobre 23, 2002																		
17	\$24,186.00	\$13,858.69	\$1,580.07	Septembre 12, 2002																		
18	\$2,541.00	\$15,296.43	\$166.00	Octobre 13, 2002																		
19	\$2,541.00	\$15,296.43	\$166.00	Novembre 10, 2002																		
20	\$24,632.00	\$22,865.79	\$1,609.21	Décembre 2, 2002																		
21	\$2,12,588.00	\$44,284.73	\$13,888.37	Janvier 24, 2003																		
22	\$24,553.00	\$4,97,655.84	\$1,604.05	Février 12, 2003																		
23	\$2,12,588.00	\$50,531.43	\$1,604.05	Mars 2, 2003																		
24	\$7,892.00	\$58,81,359.53	\$151.58	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	\$2,12,588.00	\$7,38,133.48	\$1,604.05	Juillet 13, 2003																		
28	\$59,311.00	\$7,17,735.39	\$3,874.79	Août 23, 2003																		
29	\$6,548.00	\$9,78,274.84	\$427.78	Septembre 24, 2003																		
30	\$64,156.00	\$10,9,979.55	\$3,538.01	Octobre 11, 2003																		
31	\$2,144.00	\$11,7,016.75	\$140.07	Novembre 2, 2003																		
32	\$2,12,588.00	\$13,18,47	\$2,387.68	Décembre 2, 2003																		
33	\$36,548.00	\$14,26,693.71	\$2,387.68	Janvier 20, 2004																		
34	\$2,31,455.00	\$17,6,410.24	\$15,120.96	Février 13, 2004																		
35	\$2,486.00	\$18,6,392.90	\$162.41	Mars 2, 2004																		
36	\$2,486.00	\$18,6,392.90	\$162.41	Avril 16, 2004																		
37	\$98,765.00	\$22,7,950.39	\$6,452.22	Mai 3, 2004																		
38	\$17,893.00	\$24,38,373.53	\$1,168.95	Jun 12, 2004																		
39	\$34,795.00	\$26,3,740.63	\$2,273.16	Juillet 4, 2004																		
40	\$44,892.00	\$26,9,346.33	\$3,598.09	Août 21, 2004																		
41	\$45,793.00	\$31,0,1319.80	\$2,991.40	Septembre 22, 2004																		

Swiss

Windows Taskbar: Type here to search, Start button, Task View, Chrome, File Explorer, Control Panel, System, Taskbar icons, Network, ENG, 1002, 05-02-2020

AccessData FTK Imager 3.4.2.6

E Evidence Tree

File List

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

Martha,

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

George

File List

Name	Size	Type	Date Modif..
p-021218.msg	1	Regular File	15-02-2003..
p-021229.msg	1	Regular File	15-02-2003..
m-021220.msg	1	Regular File	15-02-2003..
m-021230.msg	1	Regular File	15-02-2003..
msg5.txt	1	Regular File	15-02-2003..

ftk-demo1-image.1/CHAPTER 5 [FAT12]/[root]/persona/Messages/p-021218.msg

10:09 05-02-2020

AccessData FTK Imager 3.4.2.6

E Evidence Tree

File List

Merge

deposits. I encrypted this file so as to prevent anyone from reading them. If I have to flee when the auditor finds the missing money, you can meet me in Zurich on the 19 of January. y

File List

Name	Size	Type	Date Modif..
m-021220.msg	1	Regular File	15-02-2003..
m-021230.msg	1	Regular File	15-02-2003..
msg5.txt	1	Regular File	15-02-2003..
msg7.txt	1	Regular File	15-02-2003..

ftk-demo1-image.1/CHAPTER 5 [FAT12]/[root]/persona/Messages/msg7.txt

10:10 05-02-2020



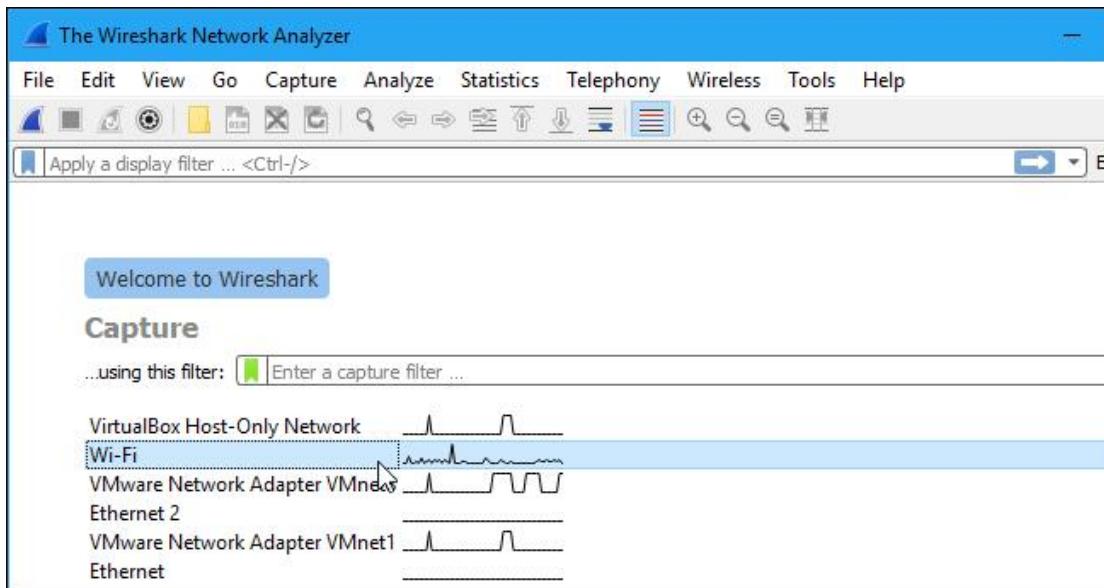
EXPERIMENT-6

Capturing and Analysis of Network Packets using WIRESHARK(Fundamentals)

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets.

Capturing Packets

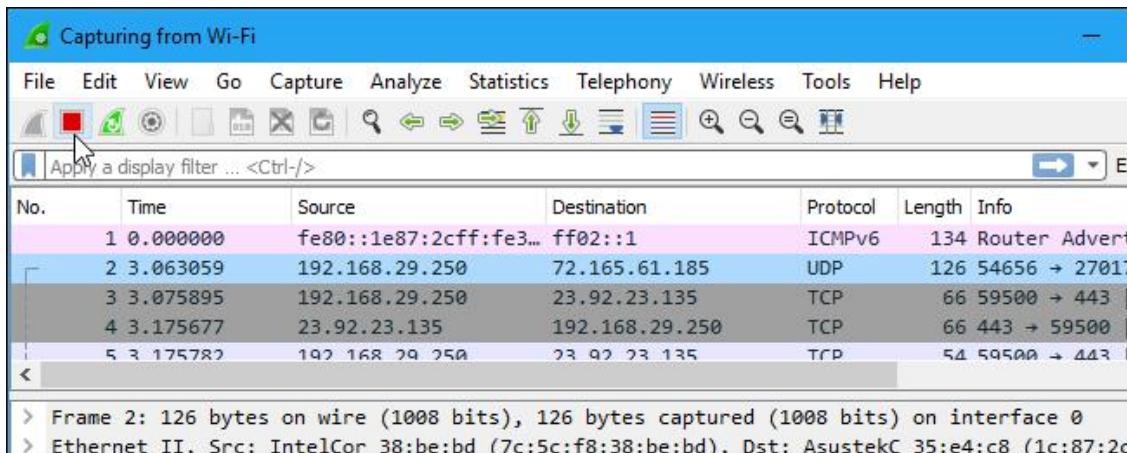
After downloading and installing Wireshark, you can launch it and double-click the name of a network interface under Capture to start capturing packets on that interface. For example, if you want to capture traffic on your wireless network, click your wireless interface. You can configure advanced features by clicking Capture > Options, but this isn't necessary for now.



As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

If you have promiscuous mode enabled—it's enabled by default—you'll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the “Enable promiscuous mode on all interfaces” checkbox is activated at the bottom of this window.

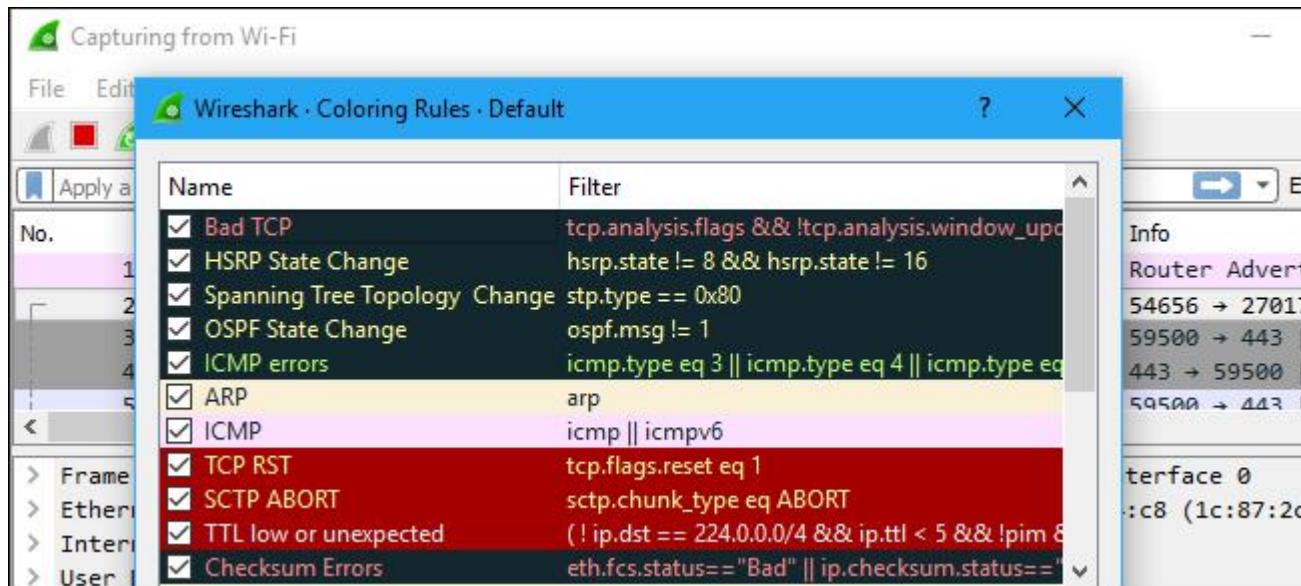
Click the red “Stop” button near the top left corner of the window when you want to stop capturing traffic.



Color Coding

You'll probably see packets highlighted in a variety of different colors. Wireshark uses colors to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors—for example, they could have been delivered out of order.

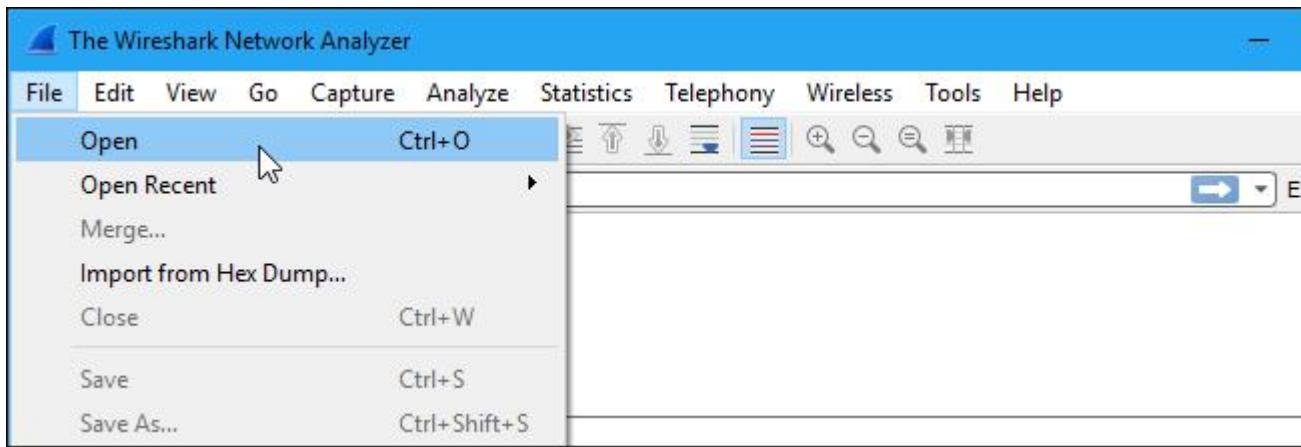
To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



Sample Captures

If there's nothing interesting on your own network to inspect, Wireshark's wiki has you covered. The wiki contains a [page of sample capture files](#) that you can load and inspect. Click File > Open in Wireshark and browse for your downloaded file to open one.

You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.



Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

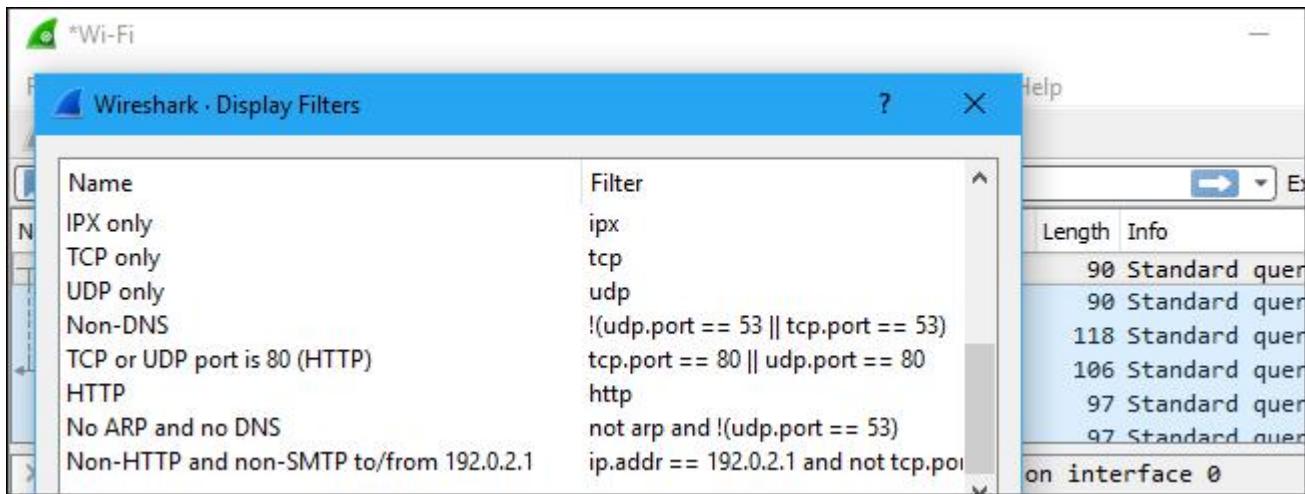
The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type “dns” and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.

A screenshot of the Wireshark interface. The title bar says "*Wi-Fi". The main window shows a list of network captures. A search bar at the top has "dns" typed into it. The table below lists four DNS packets (No. 305, 306, 307, 308) with details like Time, Source, Destination, Protocol (DNS), Length, and Info. The "Info" column shows "Standard quer".

No.	Time	Source	Destination	Protocol	Length	Info
305	5.248733	2601:1c0:cf00:8961::	2601:1c0:cf00:8961::	DNS	90	Standard quer
306	5.249092	2601:1c0:cf00:8961::	2601:1c0:cf00:8961::	DNS	90	Standard quer
307	5.269967	2601:1c0:cf00:8961::	2601:1c0:cf00:8961::	DNS	118	Standard quer
308	5.270325	2601:1c0:cf00:8961::	2601:1c0:cf00:8961::	DNS	106	Standard quer

You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

For more information on Wireshark's display filtering language, read the [Building display filter expressions](#) page in the official Wireshark documentation.



Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

You'll see the full TCP conversation between the client and the server. You can also click other protocols in the Follow menu to see the full conversations for other protocols, if applicable.

Close the window and you'll find a filter has been applied automatically. Wireshark is showing you the packets that make up the conversation.

tcp.stream eq 35							
No.	Time	Source	Destination	Protocol	Length	Info	
1054	2.798483	192.168.29.250	131.253.61.66	TCP	66	60375 → 443	
1078	2.891263	131.253.61.66	192.168.29.250	TCP	58	443 → 60375	
1079	2.891359	192.168.29.250	131.253.61.66	TCP	54	60375 → 443	
1080	2.891527	192.168.29.250	131.253.61.66	TLSv1.2	288	Client Hello	
1103	2.992980	131.253.61.66	192.168.29.250	TCP	1514	[TCP segment of a discontiguous packet]	
1104	2.992980	131.253.61.66	192.168.29.250	TCP	1514	[TCP segment of a discontiguous packet]	

Details for selected packet 1078:

- > Frame 1078: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
- > Ethernet II, Src: AsustekC_35:e4:c8 (1c:87:2c:35:e4:c8), Dst: IntelCor_38:be:bd (7c:5c:f8)
- > Internet Protocol Version 4, Src: 131.253.61.66, Dst: 192.168.29.250
- > Transmission Control Protocol, Src Port: 443, Dst Port: 60375, Seq: 0, Ack: 1, Len: 0

Inspecting Packets

Click a packet to select it and you can dig down to view its details.

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 35

No.	Time	Source	Destination	Protocol	Length	Info
1054	2.798483	192.168.29.250	131.253.61.66	TCP	66	60375 → 443
1078	2.891263	131.253.61.66	192.168.29.250	TCP	58	443 → 60375
1079	2.891359	192.168.29.250	131.253.61.66	TCP	54	60375 → 443
1080	2.891527	192.168.29.250	131.253.61.66	TLSv1.2	288	Client Hello

Frame 1054: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Interface id: 0 (\Device\NPF_{D32D7F0A-A9E8-44EE-88DC-DFD58F65ABA7})
Encapsulation type: Ethernet (1)
Arrival Time: Jun 9, 2017 12:40:04.140141000 Pacific Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1497037204.140141000 seconds

0000	1c 87 2c 35 e4 c8 7c 5c	f8 38 be bd 08 00 45 00	..,5.. \ .8....E.
0010	00 34 0b 5d 40 00 80 06	4f 85 c0 a8 1d fa 83 fd	.4.]@... 0.....
0020	3d 42 eb d7 01 bb 22 52	7b 69 00 00 00 00 80 02	=B...."R {i.....
0030	fa f0 48 ef 00 00 02 04	05 b4 01 03 03 08 01 01	..H.....
0040	04 02		..

Encapsulation type (frame.encap_type) Packets: 8136 · Displayed: 21 (0.3%)

You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 35

No.	Time	Source	Destination	Protocol	Length	Info
1054	2.798483	192.168.29.250	131.253.61.66	TCP	66	60375 → 443
1078	2.891263	131.253.61.66	192.168.29.250	TCP	58	443 → 60375
1079	2.891359	192.168.29.250	131.253.61.66	TCP	54	60375 → 443
1080	2.891527	192.168.29.250	131.253.61.66	TLSv1.2	288	Client Hello

Source Port: 60375

- Expand Subtrees Shift+Right
- Expand All Ctrl+Right
- Collapse All Ctrl+Left

Apply as Column

- Apply as Filter ▾ Selected (Selected)
- Prepare a Filter ▾ Not Selected
- Conversation Filter ▾ ...and Selected
- Colorize with Filter ▾ ...or Selected
- Follow ▾ ...and not Selected

Packets: 8136 · Displayed: 21 (0.2%)

Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.

EXPERIMENT-7

Analysis of 5 pcap files using WIRESHARK

All 5 Pcap file solutions are present

This was the only information found within all the pcap files

Ann Bed Pcap Solutions

1. The name of Ann's IM buddy is

Filter:	ip.addr eq 192.168.1.158	Expression...	Clear	Apply	Save
lo.	Time Source Destination	Protocol	Length	Info	
23	18.870898 192.168.1.158 64.12.24.50	SSL	60	Continuation Data	
24	18.871477 64.12.24.50 192.168.1.158	TCP	60	https > 51128 [ACK] Seq=1 Ack=7 Win=64240 Len=0	
25	33.914966 192.168.1.158 64.12.24.50	SSL	243	Continuation Data	
26	33.915486 64.12.24.50 192.168.1.158	TCP	60	https > 51128 [ACK] Seq=1 Ack=196 Win=64240 Len=0	
27	34.006599 192.168.1.158 64.12.24.50	SSL	94	Continuation Data	
28	34.006604 64.12.24.50 192.168.1.158	TCP	60	https > 51128 [ACK] Seq=1 Ack=236 Win=64240 Len=0	
29	34.023247 64.12.24.50 192.168.1.158	SSL	263	Continuation Data	
31	34.025537 64.12.24.50 192.168.1.158	SSL	92	Continuation Data	
32	34.026804 192.168.1.158 64.12.24.50	TCP	60	51128 > https [ACK] Seq=236 Ack=210 Win=62780 Len=0	
33	34.026809 192.168.1.158 64.12.24.50	TCP	60	51128 > https [ACK] Seq=236 Ack=248 Win=62742 Len=0	
90	56.425051 192.168.1.158 239.255.255.250	SSDP	174	M-SEARCH * HTTP/1.1	
91	57.427165 192.168.1.158 239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1	
92	58.458768 192.168.1.158 64.12.24.50	SSL	182	Continuation Data	
93	58.461856 64.12.24.50 192.168.1.158	TCP	60	https > 51128 [ACK] Seq=248 Ack=364 Win=64240 Len=0	
94	58.568705 64.12.24.50 192.168.1.158	SSL	263	Continuation Data	
95	58.568716 192.168.1.158 64.12.24.50	TCP	60	51128 > https [ACK] Seq=248 Ack=364 Win=64240 Len=0	
Frame 27: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)					
Ethernet II, Src: Hewlett-_45:a4:bb (00:12:79:45:a4:bb), Dst: VMware_b0:8d:62 (00:0c:29:b0:8d:62)					
Internet Protocol Version 4, Src: 192.168.1.158 (192.168.1.158), Dst: 64.12.24.50 (64.12.24.50)					
Version: 4					
Header Length: 20 bytes					
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))					
Total Length: 80					
0000	00 0c 29 b0 8d 62 00 12 79 45 a4 bb 08 00 45 00	..).,b., yE....E.			
0010	00 50 ab 3d 40 00 40 06 74 e6 c0 a8 01 9e 40 0c	.P.=@. @. t...;@.			
0020	18 32 c7 b8 01 bb 33 6b d3 86 07 e9 60 db 50 18	.2....3k .b.;....P.			
0030	f5 3c 77 dc 00 00 2a 02 00 62 00 22 00 04 00 14	.<w...? .b.;....			
0040	00 00 00 00 46 00 00 00 00 00 00 00 00 01F.			
0050	0b 53 65 63 35 35 38 75 73 65 72 31 00 00	.sec558user1..			

Sec558user1

2. The first comment in the captured IM conversation is

Filter: ip.addr eq 192.168.1.158					
No.	Time	Source	Destination	Protocol	Length Info
23	18.870898	192.168.1.158	64.12.24.50	SSL	60 Continuation Data
24	18.871477	64.12.24.50	192.168.1.158	TCP	60 https > 51128 [ACK] Seq=1 Ack=7 Win=64240 Len=0
25	33.914966	192.168.1.158	64.12.24.50	SSL	243 Continuation Data
26	33.915486	64.12.24.50	192.168.1.158	TCP	60 https > 51128 [ACK] Seq=1 Ack=196 Win=64240 Len=0
27	34.006599	192.168.1.158	64.12.24.50	SSL	94 Continuation Data
28	34.006604	64.12.24.50	192.168.1.158	TCP	60 https > 51128 [ACK] Seq=1 Ack=236 Win=64240 Len=0
29	34.023247	64.12.24.50	192.168.1.158	SSL	263 Continuation Data
31	34.025537	64.12.24.50	192.168.1.158	SSL	92 Continuation Data
32	34.026800	192.168.1.158	64.12.24.50	TCP	60 51128 > https [ACK] Seq=236 Ack=210 Win=62780 Len=0
33	34.026809	192.168.1.158	64.12.24.50	TCP	60 51128 > https [ACK] Seq=236 Ack=248 Win=62742 Len=0
90	56.425051	192.168.1.158	239.255.255.250	SSDP	174 M-SEARCH * HTTP/1.1
91	57.427165	192.168.1.158	239.255.255.250	SSDP	175 M-SEARCH * HTTP/1.1
92	58.458768	192.168.1.158	64.12.24.50	SSL	182 Continuation Data
93	58.461856	64.12.24.50	192.168.1.158	TCP	60 https > 51128 [ACK] Seq=248 Ack=364 Win=64240 Len=0
94	58.568705	64.12.24.50	192.168.1.158	SSL	263 Continuation Data
95	59.568716	64.12.24.50	192.168.1.158	TCP	60 51128 > https [ACK] Seq=248 Ack=374 Win=62742 Len=0

Frame 25: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
 Ethernet II, Src: Hewlett_-45:a4:bb (00:12:79:45:a4:bb), Dst: VMware_b0:8d:62 (00:0c:29:b0:8d:62)
 Internet Protocol version 4, Src: 192.168.1.158 (192.168.1.158), Dst: 64.12.24.50 (64.12.24.50)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
 Total Length: 229

```
0030 f5 3c d0 8c 00 00 2a 02 00 61 00 b7 00 04 00 06 .<....?..a....  

0040 00 00 00 00 00 45 34 36 32 38 37 37 38 00 00 01 .....E46 28778...  

0050 0b 53 65 63 35 35 38 75 73 65 72 31 00 02 00 8f .Sec558u ser1...  

0060 05 01 00 04 01 01 02 01 01 00 83 00 00 00 00 .....  

0070 48 65 72 65 27 73 20 74 68 65 20 73 65 63 72 65 Here's t he secre  

0080 74 20 72 65 63 69 70 65 28 2e 2e 20 49 20 6a 75 t recipe ... I ju  

0090 73 74 20 64 6f 77 6e 6c 6f 61 64 65 64 20 69 74 st downl oaded it  

00a0 20 66 72 6f 6d 20 74 68 65 20 66 69 6c 65 20 73 from th e file s  

00b0 65 72 65 65 72 2e 20 4a 75 73 74 20 63 6f 70 79 erver. J ust copy  

00c0 20 74 6f 20 61 20 74 68 75 6d 62 20 64 72 69 76 to a th umb driv  

00d0 65 20 61 6e 64 20 79 6f 75 27 72 65 20 67 6f 6f e and yo u're goo  

00e0 64 20 74 6f 20 67 6f 20 26 67 74 3b 3a 2d 29 00 d to go &gt;:-).  

00f0 03 00 00 .....
```

3. The name of the file that Ann transferred is

Filter: ip.addr eq 192.168.1.158					
No.	Time	Source	Destination	Protocol	Length Info
107	61.051425	Dell_4d:4f:ae	Broadcast	ARP	60 Who has 192.168.1.158? Tell 192.168.1.159
108	61.051429	Hewlett_-45:a4:bb	dell_4d:4f:ae	ARP	60 192.168.1.158 is at 00:12:79:45:a4:bb
109	61.052925	192.168.1.158	192.168.1.158	TCP	62 csmplockmgr > aol [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
110	61.052930	192.168.1.158	192.168.1.158	TCP	62 aol > csmplockmgr [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
111	61.054660	192.168.1.159	192.168.1.158	TCP	60 csmplockmgr > aol [ACK] Seq=1 Ack=1 Win=64240 Len=0
112	61.054884	192.168.1.158	192.168.1.159	TCP	310 aol > csmplockmgr [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=256
113	61.064823	192.168.1.159	64.12.25.91	TLSV1	110 Application Data
114	61.065468	64.12.25.91	192.168.1.159	TCP	60 https > sweetware-apps [ACK] Seq=896 Ack=96 Win=64240 Len=0
115	61.144314	192.168.1.159	64.12.25.91	TLSV1	143 Application Data
116	61.144758	64.12.25.91	192.168.1.159	TCP	60 https > sweetware-apps [ACK] Seq=896 Ack=185 Win=64240 Len=0
117	61.155756	192.168.1.159	192.168.1.158	TCP	310 csmplockmgr > aol [PSH, ACK] Seq=1 Ack=257 Win=63984 Len=256
118	61.155760	192.168.1.158	192.168.1.159	TCP	60 aol > csmplockmgr [ACK] Seq=257 Ack=257 Win=6432 Len=0
119	61.270615	192.168.1.158	192.168.1.159	TCP	1514 aol > csmplockmgr [ACK] Seq=257 Ack=257 Win=6432 Len=1460
120	61.270620	192.168.1.158	192.168.1.159	TCP	1514 aol > csmplockmgr [ACK] Seq=1717 Ack=257 Win=6432 Len=1460
121	61.270623	192.168.1.159	192.168.1.158	TCP	60 csmplockmgr > aol [ACK] Seq=257 Ack=3177 Win=64240 Len=0

Frame 117: 310 bytes on wire (2480 bits), 310 bytes captured (2480 bits)
 Ethernet II, Src: dell_4d:4f:ae (00:21:70:4d:4f:ae), Dst: Hewlett_-45:a4:bb (00:12:79:45:a4:bb)
 Internet Protocol version 4, Src: 192.168.1.159 (192.168.1.159), Dst: 192.168.1.158 (192.168.1.158)
 Version: 4
 Header length: 20 bytes
 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
 Total Length: 296

```
0050 00 01 00 00 2e e8 00 00 2e e8 00 00 00 00 b1 64 .....d  

0060 00 00 00 00 00 00 00 00 00 00 00 00 ff ff .....Cool F  

0070 00 00 00 00 00 00 00 00 00 43 6f 6f 20 46 .....ilexFer.....  

0080 69 6c 65 58 66 65 72 00 00 00 00 00 00 00 00 00 iflexFer.....  

0090 00 00 00 00 00 00 00 00 00 20 10 11 00 00 00 .....  

00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  

00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  

00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  

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  

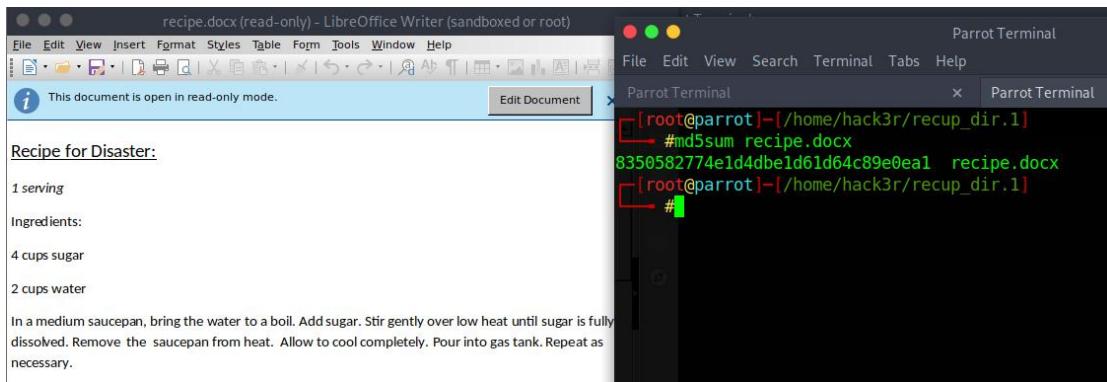
0100 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 x.....  

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 .....
```

Recipe.doc

4. The MD5 sum of the file is



5. The secret recipe is

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.

Ping Pcap Solutions

1. Type of ICMP traffic shown: Echo Request / Reply

```

Frame 192: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 1
Interface id: 1 (\Device\NPF_{D282B257-0DB6-4718-8451-167FF884D55D})
    Interface name: \Device\NPF_{D282B257-0DB6-4718-8451-167FF884D55D}
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 21, 2012 14:51:55.050942000 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1350811315.050942000 seconds
    [Time delta from previous captured frame: 0.010872000 seconds]
    [Time delta from previous displayed frame: 0.010872000 seconds]
    [Time since reference or first frame: 24.758288000 seconds]
    Frame Number: 192
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: CiscoSrv 27:6d:2f (24:76:7d:27:6d:2f), Dst: Azurewaw 6a:24:9f (74:f0:6d:6a:24:9f)
0000  74 f0 6d 6a 24 9f 24 76 7d 27 6d 2f 08 00 45 00 t-mj$ $v }'m/..E
0010  00 3c 4b 31 00 00 3c 01 df 7e 59 cf 38 8c c0 a8 <K1..< ~Y.8...
0020  01 0e 00 00 55 5a 00 01 00 01 61 62 63 64 65 66 ...UZ... abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuvwxyz
0040  77 61 62 63 64 65 66 67 68 69 wabcefg hi

```

```

Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0x555a [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 1 (0x0001)
  Sequence number (LE): 256 (0x0100)
  [Request frame: 181]
  [Response time: 10.872 ms]
  Data (32 bytes)
    Data: 6162636465666768696a6b6c6d6e6f707172737475767761...
    Length: 321
0000 74 f0 6d 6a 24 9f 24 76 7d 27 6d 2f 08 00 45 00 t m$ $v }'m/..E.
0010 00 3c 4b 31 00 00 3c 01 df 7e 59 cf 38 8c c0 a8 <K1..< ..~Y.8...
0020 01 0e 00 00 55 5a 00 01 00 01 61 62 63 64 65 66 ...UZ... abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuvwxyz
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Internet Protocol Version 4, Src: 89.207.56.140, Dst: 192.168.1.14
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    0000 00.. = Differentiated Services Codepoint: Default (0)
    .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 60
  Identification: 0x4b31 (19249)
  Flags: 0x0000
    0... .... .... = Reserved bit: Not set

0000 74 f0 6d 6a 24 9f 24 76 7d 27 6d 2f 08 00 45 00 t m$ $v }'m/..E.
0010 00 3c 4b 31 00 00 3c 01 df 7e 59 cf 38 8c c0 a8 <K1..< ..~Y.8...
0020 01 0e 00 00 55 5a 00 01 00 01 61 62 63 64 65 66 ...UZ... abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuvwxyz
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Ethernet II, Src: CiscoSpv_27:6d:2f (24:76:7d:27:6d:2f), Dst: Azurewav_6a:24:9f (74:f0:6d:6a:24:9f)
  Destination: Azurewav_6a:24:9f (74:f0:6d:6a:24:9f)
    Address: Azurewav_6a:24:9f (74:f0:6d:6a:24:9f)
    .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
    .... ..0. .... .... .... = IG bit: Individual address (unicast)
  Source: CiscoSpv_27:6d:2f (24:76:7d:27:6d:2f)
    Address: CiscoSpv_27:6d:2f (24:76:7d:27:6d:2f)
    .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
    .... ..0. .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 89.207.56.140, Dst: 192.168.1.14
    0100 .... = Version: 4

0000 74 f0 6d 6a 24 9f 24 76 7d 27 6d 2f 08 00 45 00 t m$ $v }'m/..E.
0010 00 3c 4b 31 00 00 3c 01 df 7e 59 cf 38 8c c0 a8 <K1..< ..~Y.8...
0020 01 0e 00 00 55 5a 00 01 00 01 61 62 63 64 65 66 ...UZ... abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuvwxyz
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

```

2. Frame no. 15 Indicates something funny might be going on.

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

```

Frame 15 : 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits) on
Interface id: 1 (\Device\NPF_{D282B257-0DB6-4718-8451-167FF884D55D})
    Interface name: \Device\NPF_{D282B257-0DB6-4718-8451-167FF884D55D}
Encapsulation type: Ethernet (1)
Arrival Time: Oct 21, 2012 14:51:33.734469000 IST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1350811293.734469000 seconds
[Time delta from previous captured frame: 0.164406000 seconds]
[Time delta from previous displayed frame: 0.164406000 seconds]
[Time since reference or first frame: 3.441815000 seconds]
Frame Number: 22
Frame Length: 212 bytes (1696 bits)

0000 ff ff ff ff ff 74 f0 6d 6a 24 9f 08 00 45 00 . . t mJS -E
0010 00 c6 71 3c 00 00 80 11 44 8d c0 a8 01 0e c0 a8 . q< . D . .
0020 01 ff 19 f6 19 f6 00 b2 8f de 00 00 00 a6 00 00 . . . . . .
0030 00 04 00 00 00 00 00 00 00 08 00 00 00 00 18 4d 00 . . . . . M
0040 63 00 4e 00 41 00 55 00 6e 00 69 00 71 00 75 00 c-N-A-U n-i-q-u-
0050 65 00 49 00 64 00 0b 00 00 00 24 00 00 00 65 31 e-I-d... .$.e1
0060 38 30 30 61 36 39 2d 36 35 38 62 2d 34 34 66 33 800a69-6 58b-44f3
0070 2d 61 33 66 63 2d 36 34 31 32 32 66 32 62 39 62 -a3fc-64 122f2b9b
0080 66 30 01 00 00 00 18 4d 00 63 00 4e 00 41 00 55 f0.....M .c-N[A-U
0090 00 6e 00 69 00 71 00 75 00 65 00 49 00 64 00 0b .n-i-q-u .e-I-d..
00a0 00 00 00 24 00 00 00 62 39 63 35 33 34 31 36 2d ...$.b 9c53416-
00b0 33 37 34 31 2d 34 62 39 36 2d 38 30 64 39 2d 61 3741-4b9 6-80d9-a
00c0 30 31 31 38 31 63 36 37 32 62 34 01 7b de f7 bd 01181c67 2b4.{...
00d0 00 00 00 23 . . . #
```

2. Application layer protocol hidden in icmp traffic ie. Payload is ssh
 3. The tool most likely generated this traffic is ICMP Tunnel
 4. True Destination IP is: 192.168.5.217

An external host accessible through 192.168.5.217

5. Session Identifier for each packet in format of 1111

```
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: Azurewave_f0:30:c0 (e0:b9:a5:f0:30:c0)
Sender IP address: 192.168.1.19
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.1
```

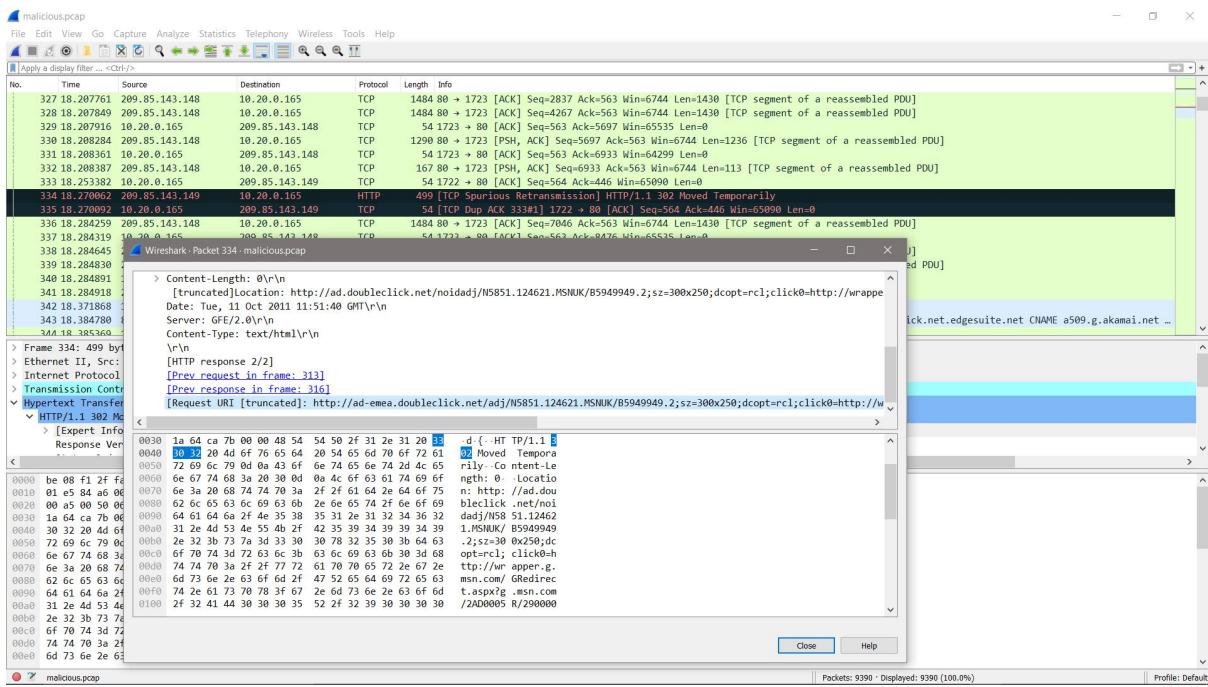
Malicious Pcap Solutions

1. The complete URI of the original web request that led to the client being compromised is,

http://ad-

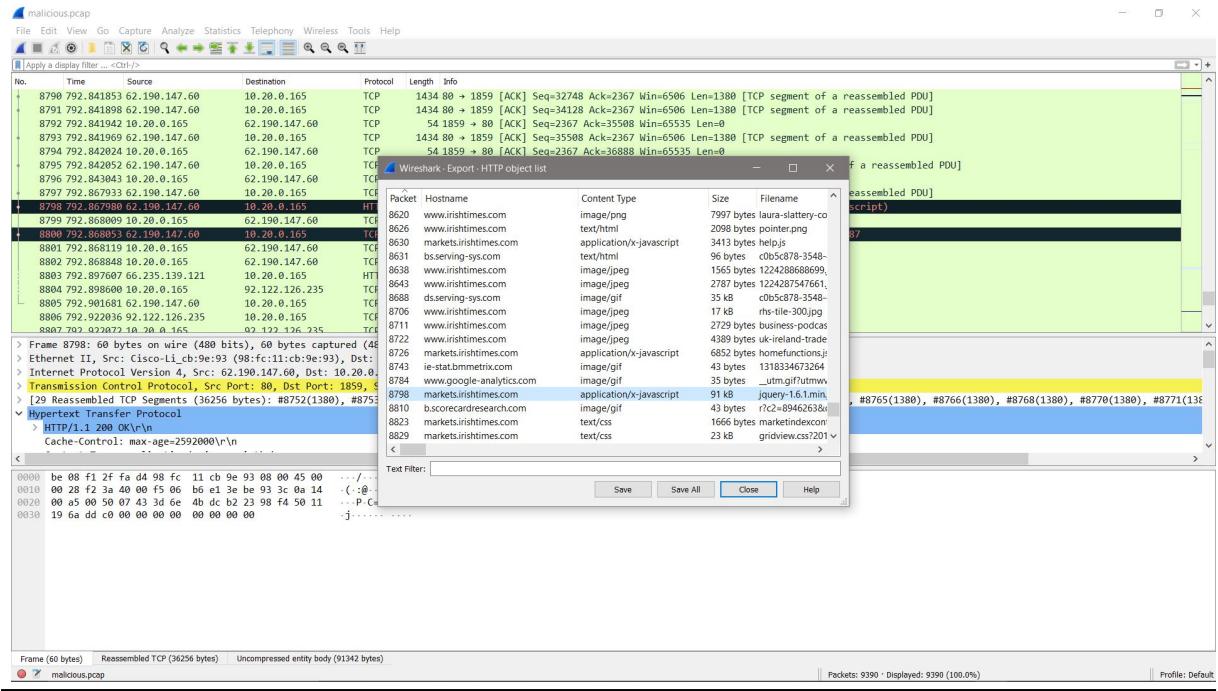
emea.doubleclick.net/adj/N5851.124621.MSNUK/B5949949.2;sz=300x250;dcop
t=rcl;click0=http://wrapper.g.msn.com/GRedirect.aspx?g.msn.com/2AD0005R/2
9000000000099086.1?!&&PID=9240833&UIT=G&TargetID=100008621&A]

http://10.20.0.111:8080/banking.htm



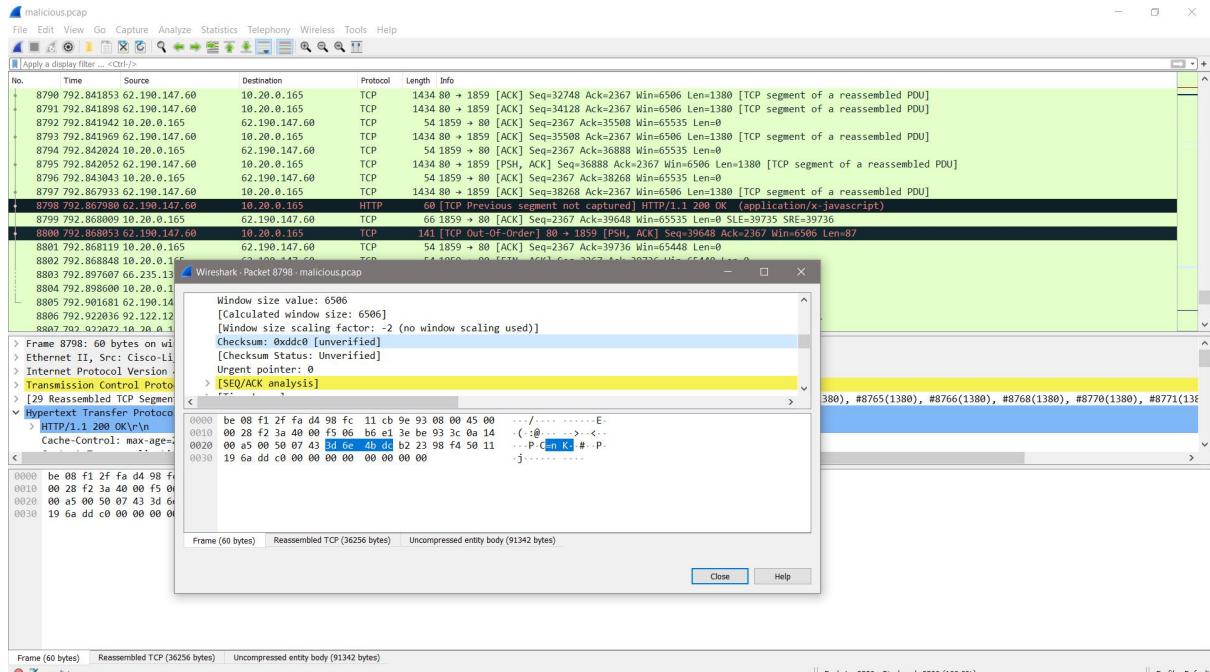
This can be found when we examine the first suspicious packet that uses Hyper Text Transfer Protocol under Hypertext Transfer Protocol tab in the Packet details pane.

2. The file type requested in the final web request from the malicious server was a gif file as we can see below,



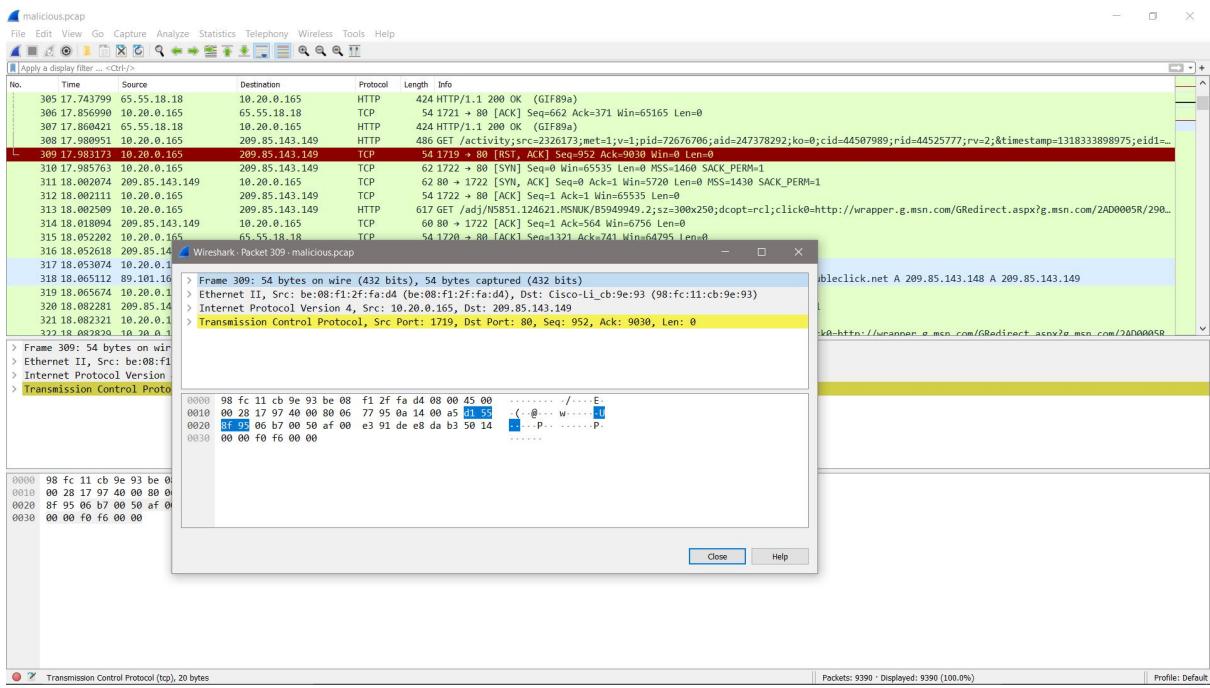
This can be found by finding out the file requested by the last frame under the HTTP object list which shows the name of the file along with the extension and other details.

3. The SHA1 Hash of the requested file to the malicious server is 0xddc0.



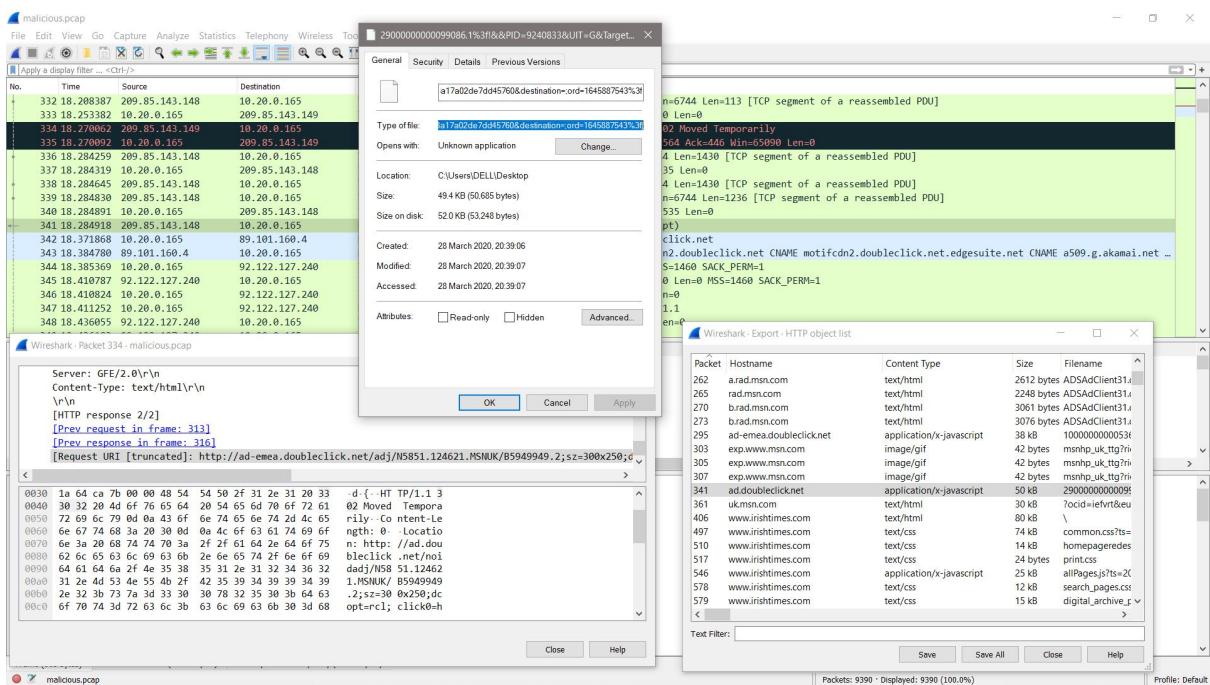
Can be found by going in the Packet details pane of the 8790th frame and checking it's checksum value.

4. The number of the first frame that indicates that the client has been attacked is 4722.



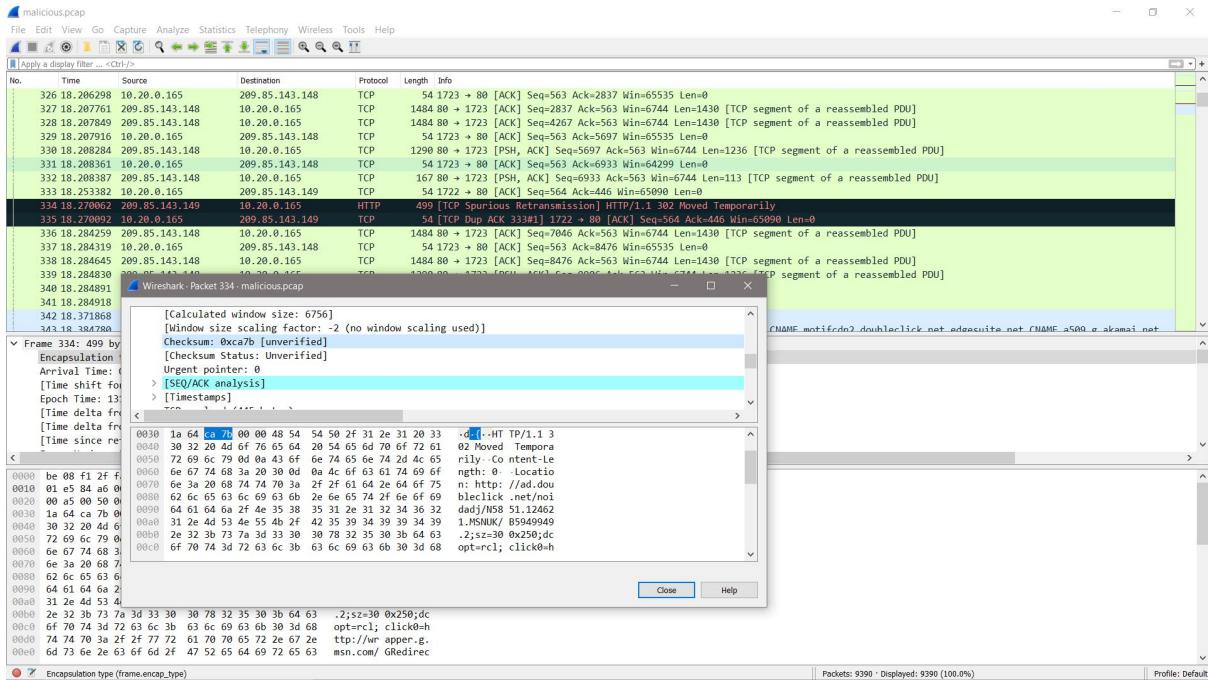
5. The file that the malicious server sends the client is a type of windows executable file.

1%3F!&&PID=9240833&UIT=G&TARGETID=100008621&AN=1645887543 &PG=UK9REN&ASID=85E54A since it's extension is .1%3f!&&PID=9240833&UIT=G&TargetID=100008621&AN=1645887543& PG=UK9REN&ASID=85e54a8ea63a43e8a17a02de7dd45760&destination=;ord =1645887543%3f.



Here we can see the extension of the file as well as how it was discovered.

6. The SHA1 hash of the malicious file which we found out in the previous question is 7afc1f67e627abb4786e5596843f9d790be81a34



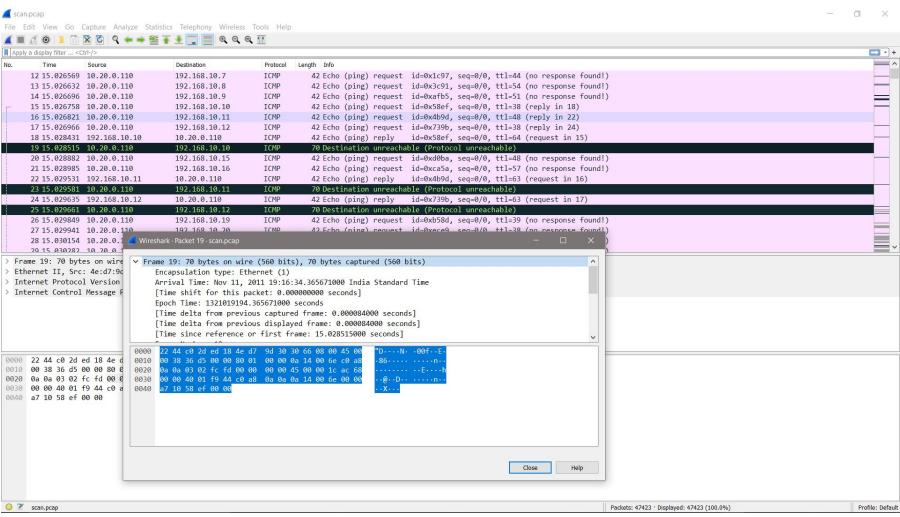
We can find this out by checking the checksum of the frame we received the file from.

7. The Vulnerable Software here clearly was the browser application IE6 used by the client since the malicious file entered the system exploiting the vulnerability of the application.

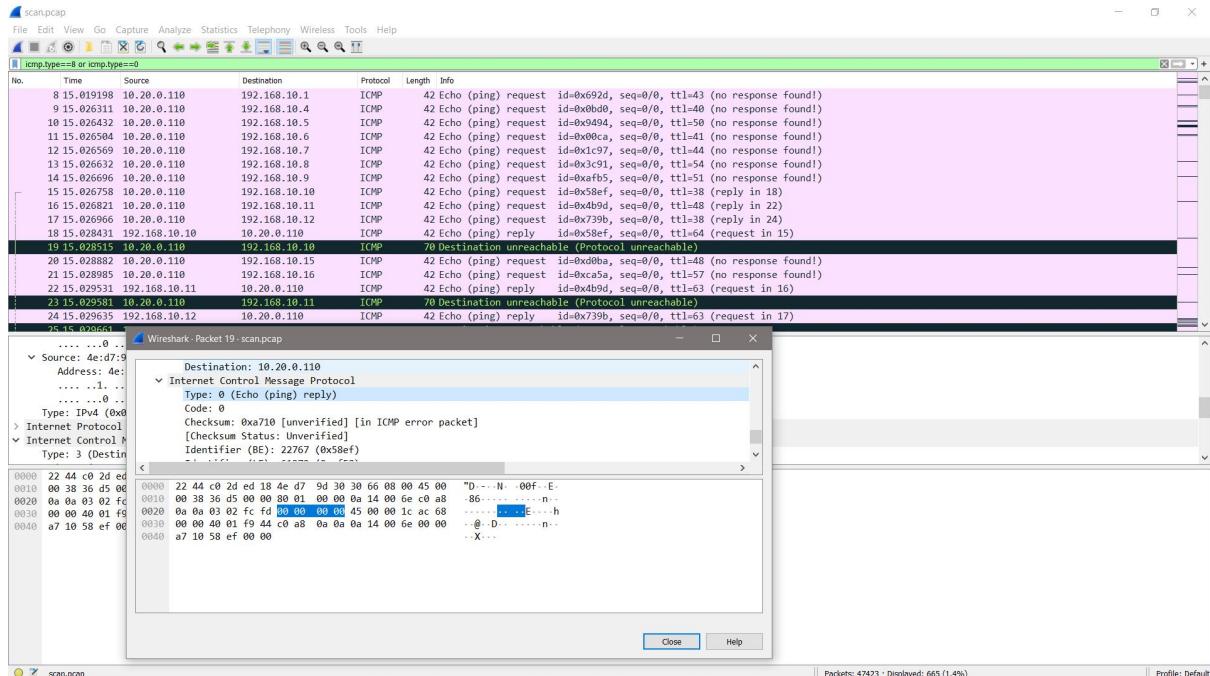
8. This is a “Gain Privileges” vulnerability. To get the corresponding CVE security bulletin, we check what kind of vulnerability this is. Since we have established that the type of vulnerability exploited is a “Gain Privileges” vulnerability, we check the database of CVE and match the columns with the file we are analysing. Doing this, the CVE security bulletin can be CVE-2005-1790.

Scan Pcap Solutions

1. The tool used to generate this traffic is the “ping”.
2. The Frame which first shows unusual behaviour is Frame number 8.



3. This Frame constitutes the beginning of an ICMP Ping Sweep Attack.



4. sU switch was removed from the command to improve the speed.

5. sS was the switch added to final scan.

Access Pcap Solutions

1. The SSID and BSSID of his access point are:

SSID: Ment0rNet

BSSID: 00:23:69:61:00:d0

```
1 0.000000 Cisco-Li_61:00:d0 Broadcast 802.11 105 Beacon frame, SN=3583, FN=0, Flags=..  
2 0.007098 BelkinIn_63:83:26 (... 802.11 10 Acknowledgement, Flags=.....  
3 0.011195 SenaoInt_33:a9:55 (... 802.11 10 Acknowledgement, Flags=.....  
4 0.059323 SenaoInt_33:a9:55 (... 802.11 10 Acknowledgement, Flags=.....  
5 0.064957 SenaoInt_33:a9:55 (... 802.11 10 Acknowledgement, Flags=.....  
6 0.068024 Sonicwal_53:71:15 (... 802.11 10 Acknowledgement, Flags=.....  
7 0.071007 SenaoInt_33:a9:55 (... 802.11 10 Acknowledgement, Flags=.....  
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)  
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)  
Transmitter address: Cisco-Li_61:00:d0 (00:23:69:61:00:d0)  
Source address: Cisco-Li_61:00:d0 (00:23:69:61:00:d0)  
BSS Id: Cisco-Li_61:00:d0 (00:23:69:61:00:d0)  
1 0.000000 Cisco-Li_61:00:d0 Broadcast 802.11 105 Beacon frame, SN=3583, FN=..  
2 0.007098 BelkinIn_63:83:26 (... 802.11 10 Acknowledgement, Flags=...  
3 0.011195 SenaoInt_33:a9:55 (... 802.11 10 Acknowledgement, Flags=...  
4 0.059323 SenaoInt_33:a9:55 (... 802.11 10 Acknowledgement, Flags=...  
5 0.064957 SenaoInt_33:a9:55 (... 802.11 10 Acknowledgement, Flags=...  
6 0.068024 Sonicwal_53:71:15 (... 802.11 10 Acknowledgement, Flags=...  
7 0.071007 SenaoInt_33:a9:55 (... 802.11 10 Acknowledgement, Flags=...  
Beacon Interval: 0.102400 [Seconds]  
↳ Capabilities Information: 0x0411  
↳ Tagged parameters (69 bytes)  
↳ Tag: SSID parameter set: Ment0rNet
```

2. Time for packet capture is 414s

No.	Time	Source	Destination	Protocol	Length	Info
1330...	413.542139		SenaoInt_33:a9:55 (... 802.11	10	Ackn	
1330...	413.543160		SenaoInt_33:a9:55 (... 802.11	10	Ackn	
1330...	413.551866		SenaoInt_33:a9:55 (... 802.11	10	Ackn	
1330...	413.5558010		SenaoInt_33:a9:55 (... 802.11	10	Ackn	
1330...	413.574904	SenaoInt_05:cb:11	SenaoInt_33:a9:55 (... 802.11	16	Req	
1330...	413.576954	SenaoInt_05:cb:11	SenaoInt_33:a9:55 (... 802.11	16	Req	

[Time since reference or first frame: 413.576954000 seconds]

3. 59274 WEP-encrypted data frames are there total in the packet capture

\$ tshark -r evidence08.pcap -R '((wlan.fc.type_subtype == 0x20) &&

(wlan.fc.protected == 1)) && (wlan.bssid == 00:23:69:61:00:d0)' | wc -l

```
$ tshark -r evidence08.pcap -R 'wlan.fc.type_subtype==0x20 && wlan.fc.protected==1  
&& wlan.bssid==00:23:69:61:00:d0' | wc -l  
59274
```

4. 29719 unique WEP initialization vectors (IVs) are there total in the packet capture related to Joe's access point

\$ tshark -r evidence08.pcap -R '(wlan.bssid == 00:23:69:61:00:d0) &&

wlan.wep.iv' -T fields -e wlan.wep.iv | sort -u | wc -l

5. The MAC address of the station executing the Layer 2 attacks

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

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

a) 14133 By the attacker station.

\$ tshark -r evidence08.pcap -R '(wlan.bssid == 00:23:69:61:00:d0) && (wlan.sa

```
== 1c:4b:d6:69:cd:07) && wlan.wep.iv' -T fields -e wlan.wep.iv|sort -u|wc -l
```

b) 15587 By all other stations combined

```
$ tshark -r evidence08.pcap -R '(wlan.bssid == 00:23:69:61:00:d0) && (wlan.sa != 1c:4b:d6:69:cd:07) && wlan.wep.iv' -T fields -e wlan.wep.iv|sort -u|wc -l
```

7. D0:E5:9E:B9:04 was the WEP key of Joe's WAP

```
$ aircrack-ng -b 00:23:69:61:00:d0 evidence08.pcap
```

8. They administrative username and password of the targeted wireless access point

username: admin

passphrase: admin

9. The WAP administrative passphrase changed to :

passphrase: hahp0wnedJ00

EXPERIMENT-8

Email Forensics

8.A

- Mail Service Providers

A mailbox provider, mail service provider or, somewhat improperly, email service provider is a provider of email hosting. It implements email servers to send, receive, accept, and store email for other organizations or end users, on their behalf.

Some e-mail providers :

- Email protocols

POP3

POP3 stands for Post Office 3 protocol. POP simply reaches out to the mail server and brings back the mail contents. This is a simple yet standardized way which allows users to access mailboxes and quickly download messages to their device.

With POP3, users can configure the server settings. This can be used to allow mail copies to be left on the server or move all emails without leaving any copy on the server. This is usually configurable in most cases. The biggest advantage of POP3 is the low dependency over the Internet. Users can download all emails and read them at leisure even if they are accessing this offline.

The way these emails are stored in local depends on the email client. For instance, Outlook utilizes .pst, while Thunderbird uses .mbox. This is a good option in case you choose to read emails offline. Apart from this, this helps you reduce the server space by storing messages locally.

The default ports for POP3 are:

Port 110 – This is the default non-encrypted port.

Port 995 – This is the default port for secure connections.

IMAP

This stands for Internet Message Access Protocol. This again is a standard protocol for accessing emails and is a client/server protocol. Here the emails are received and held by the Internet server. Unlike POP, this does not move the emails. The biggest difference between POP3 and IMAP is the mail sync up. POP3 assumes that a user will be connected to a single device. However, IMAP is suitable for different devices simultaneously.

IMAP requires users to be constantly connected to the Internet. When a user accesses the mailbox, the user is actually connected to an external server. This is more beneficial when there are multiple users. IMAP can work over a relatively low internet connection since it only downloads email messages from the server when a user has requested to read a specific email.

The default ports for IMAP are:

Port 143 – This is the default non-encrypted port.

Port 993 – This is default port for secure connections.

SMTP

This stands for Simple Mail Transfer Protocol. This is a standard protocol for sending emails over the Internet. This is a protocol which is used by a Mail Transfer Agent to deliver emails to a recipient's email server. This is a protocol which defines mail sending and cannot be used for mail receiving.

SMTP is the most commonly used protocol for mail transfer between two servers. This requires no authentication to function, unlike POP3 and IMAP. Certain Internet Service Providers block the default port 25 of SMTP. In such cases, the mail server also provides an alternate secondary port.

The default port for SMTP are:

Port 25 – This is the default non-encrypted port.

Port 465/ 587 – This is default port for secure connections.

HTTP

This is a commonly known protocol and stands for HyperText Transfer Protocol. This is not an email specific protocol. However, HTTP is used for email access using web-based emails. Hotmail or Gmail are examples of using HTTP as an email protocol. This is used to compose and retrieve emails from a web-based account.

The default port for HTTP are:

Port 80 – This is default non-encrypted port.

Port 443 – This is default port for secure connections.

- Recovering emails

Limitations:

This will only work for emails that are removed from the "Deleted Items" folder.

Emails are only stored for 14 days after permanent deletion.

Windows: How to recover deleted mail in windows

Step 1- Open Outlook.

Step 2- Select the "Deleted Items" folder.

Step 3- Go to the "Tools >> Recover Deleted Items from server"

Step 4- Select the email(s) that you would like to recover.

Step 5- Click the "Recover Selected Items" button (the icon is an email message with an arrow).

Step 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.)

- Analyzing email header

An email consists of three vital components: the envelope, the header(s), and the body of the message. The envelope is something that an email user will never see since it is part of the internal process by which an email is routed. The body is the part that we always see as it is the actual content of the message contained in the email. The header(s), the third component of an email, is perhaps a little more difficult to explain, though it is arguably the most interesting part of an email.

Header

In an e-mail, the body (content text) is always preceded by header lines that identify particular routing information of the message, including the sender, recipient, date and subject. Some headers are mandatory, such as the FROM, TO and DATE headers. Others are optional, but very commonly used, such as SUBJECT and CC. Other headers include the sending time stamps and the receiving time stamps of all mail transfer agents that have received and sent the message. In other words, any time a message is transferred from one user to another (i.e. when it is sent or forwarded), the message is date/time stamped by a mail transfer agent (MTA) - a computer program or software agent that facilitates the transfer of email message from one computer to another. This date/time stamp, like FROM, TO, and SUBJECT, becomes one of the many headers that precede the body of an email.

To really understand what an email header is, you must see one. Here is an example of a full email header*:

Return-Path: <example_from@dc.edu>

X-SpamCatcher-Score: 1 [X]

Received: from [136.167.40.119] (HELO dc.edu)

by fe3.dc.edu (CommuniGate Pro SMTP 4.1.8)

with ESMTP-TLS id 61258719 for example_to@mail.dc.edu; Mon, 23 Aug 2004
11:40:10 -0400

Message-ID: <4129F3CA.2020509@dc.edu>

Date: Mon, 23 Aug 2005 11:40:36 -0400

From: Taylor Evans <example_from@dc.edu>

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.1)
Gecko/20020823 Netscape/7.0

X-Accept-Language: en-us, en

MIME-Version: 1.0

To: Jon Smith <example_to@mail.dc.edu>

Subject: Business Development Meeting

Content-Type: text/plain; charset=us-ascii; format=flowed

Content-Transfer-Encoding: 7bit

* email headers should always be read from bottom to top.

Fortunately, most of this information is hidden inside the email with only the most relevant or mandatory headers appearing to the user. Those headers that we most often see and recognize are bolded in the above example.

Header Characteristics

A single email header has some important characteristics, including perhaps the most important part of an email - this is the KEY:VALUE pairs contained in the header. Looking at the above, you can tell some of the KEY:VALUE pairs used. Here is a breakdown of the most commonly used and viewed headers, and their values:

- From: sender's name and email address (IP address here also, but hidden)
- To: recipient's name and email address
- Date: sent date/time of the email
- Subject: whatever text the sender entered in the Subject heading before sending

Headers Provide Routing Information

Besides the most common identifications (from, to, date, subject), email headers also provide information on the route an email takes as it is transferred from one computer to another. As mentioned earlier, mail transfer agents (MTA) facilitate email transfers. When an email is sent from one computer to another it travels through a MTA. Each time an email is sent or forwarded by the MTA, it is

stamped with a date, time and recipient. This is why some emails, if they have had several destinations, may have several RECEIVED headers: there have been multiple recipients since the origination of the email. In a way it is much like the same way the post office would route a letter: every time the letter passes through a post office on its route, or if it is forwarded on, it will receive a stamp. In this case the stamp is an email header.

When viewed in their entirety, these multiple recipient headers will look like this in an email:

```
Received: from tom.bath.dc.uk ([138.38.32.21] ident=yalrla9a1j69szla2ydr)
by steve.wrath.dc.uk with esmtp (Exim 3.36 #2)id 19OjC3-00064B-00
for example_to@imaps.bath.dc.uk; Sat, 07 Jun 2005 20:17:35 +0100
```

```
Received: from write.example.com ([205.206.231.26])
by tom.wrath.dc.uk with esmtp id 19OjBy-0001lb-3V
for example_to@bath.ac.uk; Sat, 07 Jun 2005 20:17:30 +0100
```

```
Received: from master.example.com (lists.example.com [205.206.231.19])
by write.example.com (Postfix) with QMQP
id F11418F2C1; Sat, 7 Jun 2005 12:34:34 -0600 (MDT)
```

In the example shown above, there are three Received: stamps. Reading from the bottom upwards, you can see who sent the message first, next and last, and you can see when it was done. This is because every MTA that processed the email message added a Received: line to the email's header. These Received: lines provide information on where the message originated and what stops it made (what computers) before reaching its final destination. As the example shows, these Received: lines provide the email and IP address of each sender and recipient. They also provide the date and time of each transfer. The lines also indicate if the email address was part of an email list. It is all this information that is valued by computer programmers and IT department associates when making efforts to track and stop SPAM email message. And it is this information that arguably makes headers the most important part of an email.

8.B

Case Study: Wes Mantooth Solution

1. Details regarding email categories

Users->Wes Mantooth->AppData->Local->Microsoft->Outlook...

Outlook.pst(converted it into pdf and got emails)

A. John Washer and Mantooth emailed each other several times discussing about different ways to catch quick money (check washing project and selling drugs)

B. Rasco Badguy emailed Wes Mantooth about Bujumbura Africa meeting.

C. Wes Mantooth also emailed about NZ's trade show.

2. Look and bookmark 10 email messages

These are the some messages found in inbox folder and to be bookmarked.

Screenshot of a file explorer window showing the contents of the Outlook PST file. The left pane shows a tree view of folders: Mantooth, AppData, Local, Microsoft, Outlook, Windows, Windows Mail, Backup, Local Folders, Deleted Items, Drafts, Inbox, and Junk E-mail. The right pane is titled "File List" and displays a table of files:

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	8/4/2007 4:08:3...
OC130270-0000000D.eml	4	Regular File	7/24/2007 9:02:...
10AB12E1-00000012.eml	3	Regular File	7/25/2007 11:5...
1A3A3A70-00000013.eml	19	Regular File	7/25/2007 11:4...
1B5C05E6-00000007.eml	16	Regular File	6/20/2007 5:47:...
25BB4381-00000005.eml	3	Regular File	4/13/2007 12:2...
26FC5471-00000004.eml	9	Regular File	4/12/2007 11:0...
2A29541D-0000000E.eml	14	Regular File	7/24/2007 9:38:...
31D0562C-00000001.eml	24	Regular File	2/27/2007 10:4...
3376666D-0000000A.eml	768	Regular File	7/13/2007 10:1...
40A511AF-00000008.eml	768	Regular File	7/12/2007 11:2...
43467A94-00000010.eml	17	Regular File	7/25/2007 11:4...
458C76A0-0000000C.eml	1,612	Regular File	7/13/2007 10:3...
61A02D20-0000000F.eml	41	Regular File	7/25/2007 11:4...
7C58013C-00000011.eml	70	Regular File	7/25/2007 11:5...

The bottom pane shows the raw message content of the selected file (61A02D20-0000000F.eml), which includes headers and body text:

```

boundary="-----_NextPart_001_006D_01C7C3C7.9400D820"

-----_NextPart_001_006D_01C7C3C7.9400D820
Content-Type: text/plain;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Sweet!

If that turns out to be too risky, a budy of mine showed me how to rig =
the machines to keep the cards... Then we shoulder surf the pin and get =
the card when they leave!

He got this from a SPAM chainletter!

I love it!

```

3. Email regarding Bujumbura, Africa



Wed 8/1/2007 3:09 PM

Rasco Badguy <txkidd@swbell.net>

Letter

To : chkwasher@comcast.net; dollarhyde86@comcast.net; molarmen420@hotmail.com; skimmerman27@hotmail.com

Message

Confidential Business Letter.doc (29 KB)

Guys,

Been working on a letter that I think will get us some working capital. I have a buddy in Bujumbura Africia that has a re-mailer program that will send this out. Read it and let me know what you think.

R~

A. Email sent on Wednesday 8/1/2007 at 3.09pm

B. Parties associated with the mail were:

- a. chkwasher@comcast.net - John Washer
- b. Dollarhyde86@comcast.net - Wes Mantooth
- c. Molarmen420@hotmail.com -
- d. Skimmerman27@hotmail.com - David Thomas

C. Yes, there was an attachment. It was a confidential business letter.

D. 66.196.96.95 Email server ip-address

E. Microsoft -- Outlook

4. Real names with the mail-ids associated are :

chkwasher@comcast.net - John Washer

Dollarhyde86@comcast.net - Wes Mantooth

Molarmen420@hotmail.com -

Skimmerman27@hotmail.com - David Thomas

toothfairy@mentaldental.com - Wes's Mom

txkidd@swbell.net - Rasco Badguy

Smee.rox@gmail.com - Mr Smee

5. Mom's mail sent by mantooth to his mom

Thu 7/12/2007 7:37 PM
 Wes Mantooth <dollarhyde86@comcast.net>
Hey Mom
To toothfairy@mentaldental.com
[Message](#) [Wes.jpg \(79 KB\)](#)

Hey there mom. How is it going?

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

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 p

Love ya!

6. Regarding the wedding announcement his mother wanted to see him . A message was conveyed by his dad for sending a picture of his.

7. Joan is one of the contacts of Wes Mantooth. We can see his details in address book of Wes Mantooth. There are also his personal details of business,mobile number etc., It is mentioned that Joan is excellent source of for checks. He works in ARYBS Company.

8. Mantooth's dad was released from jail. Dear Sweetie.doc .

9. Users->Wes Mantooth->AppData->Local->Microsoft->Outlook...

Outlook.pst(converted it into pdf and got emails) one of the screenshots for example from pdf.

Mantooth Case Outlook.pdf

No results < > Options

ts

From: Wes Mantooth <dollarhyde86@comcast.net>
To: 'John Washer'
Date: 6/21/2007 11:26:44 PM
Subject: RE: Whats up in D town?
Attachments: Pharmacy.vcs

It works EXACTLY the same. I have been doing quit a bit of research on it.
You would be amazed what information you can get from those who would try and stop you!
I am going to NZ for a trade show. Lots of free schwag!
You should come!
See the attached cal event.
Later

From: John Washer [mailto:chkwasher@comcast.net]
Sent: Thursday, June 21, 2007 3:09 PM
To: Wes Mantooth
Subject: Re: Whats up in D town?

So.. how are you going to get the writing off these?
The usual method?
Does it work the same with scripts as checks?
<http://celtickane.com/projects/washing/>

----- Original Message -----
From: Wes Mantooth
To: John Washer
Sent: Thursday, June 21, 2007 3:06 PM
Subject: RE: Whats up in D town?

Your crazy!
You are going to blow your self up!
I am sticking with my method...
I horked another today from the pharm counter... this lady is a mess. She just leaves this stuff lying around!

□

From: John Washer [mailto:chkwasher@comcast.net]
Sent: Thursday, June 21, 2007 12:02 PM
To: Wes Mantooth

10. Yes, there is an email sent by David Thomas to Wes mantooth regarding ATM rigging. The name Rasco is also mentioned in the email.

Wed 7/11/2007 4:27 PM
John Washer <chkwasher@comcast.net>
Re: New Venture
To: Wes Mantooth; Mr Smee

Message [ATM_THEFTS1.ppt \(558 KB\)](#)

Sweet!
If that turns out to be too risky, a budy of mine showed me how to rig the machines to keep the cards... Then we shoulder surf the pin and get the card when they leave!
He got this from a SPAM chainletter!
I love it!

11. Washer's AIM username was: Washergonebad .

EXPERIMENT-9

Web Browser Forensics

9.A Browser Forensics Analysis is a separate, large area of expertise. Web browsers are used in mobile devices, tablets, netbooks, desktops, etc.

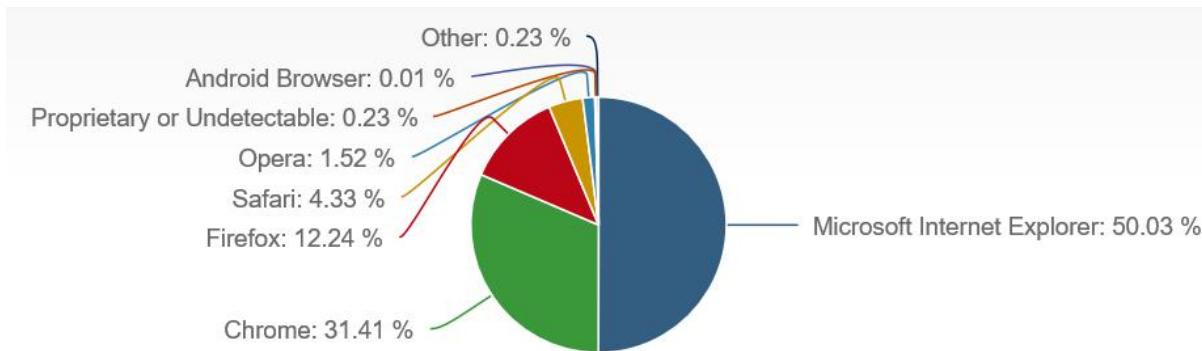
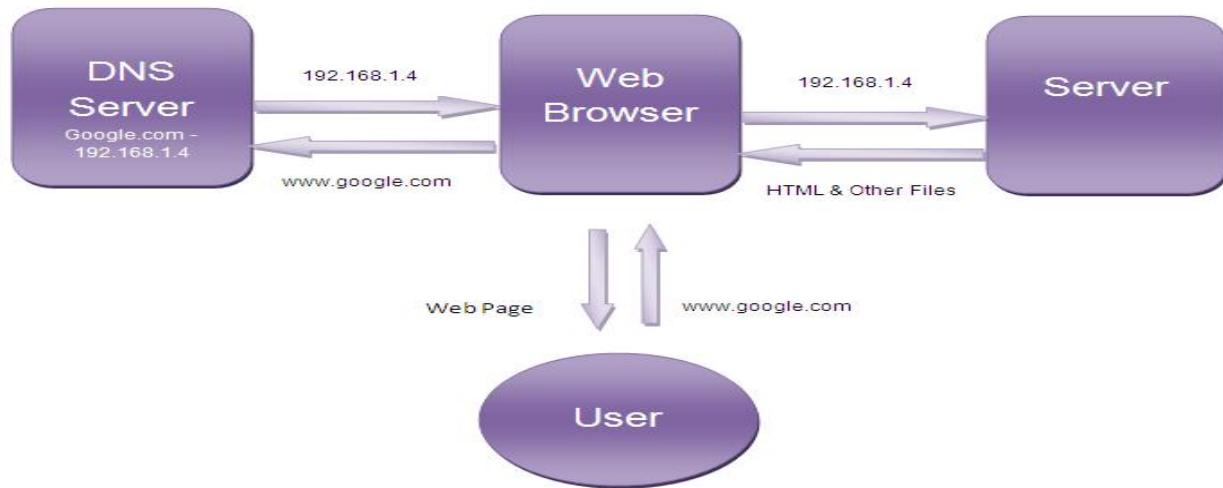


Table 2. File Location in the Web Browser Operating System

Web Browser	Operating System	File Path
Internet Explorer	Windows 95/98	C:\Temporary Internet Files\Content.ie5 C:\Cookies C:\History\History.ie5
	Windows 2000/XP	C:\Documents and Settings%\username%\Local Settings\Temporary Internet Files\Content.ie5 C:\Documents and Settings%\username%\Cookies C:\Documents and Settings%\username%\Local Settings\History\history.ie5
	Windows Vista, 7 and latest version	C:\Users%\username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\ C:\Users%\username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\
	Linux	/home/\$USER/.mozilla/firefox/\$PROFILE.default/places.sqlite
Firefox	MacOS-X	/Users/\$USER/Library/Application Support/Firefox/Profiles/\$PROFILE.default/places.sqlite
	Windows XP	C:\Documents and Settings%\username%\Application Data\Mozilla\Firefox\Profiles%\PROFILE%.default\places.sqlite
	Windows Vista, 7 and latest version	C:\Users%\USERNAME%\AppData\Roaming\Mozilla\Firefox\Profiles%\PROFILE%.default\places.sqlite
	MacOS-X	/Users/\$USER/Library/Safari/ /Users/\$USER/Library/Caches/com.apple.Safari/
Safari	Windows XP	C:\Documents and Settings%\username%\Application Data\Apple Computer\Safari\ C:\Documents and Settings%\username%\Local Settings\Application Data\Apple Computer\Safari\
	Windows 7	C:\Users%\username%\AppData\Roaming\Apple Computer\Safari\ C:\Users%\username%\AppData\Local\Apple Computer\Safari\
Opera	Linux	/home/\$USER/.opera/
	MacOS-X	/Users/\$USER/Library/Opera/
	Windows XP	C:\Documents and Settings%\username%\Application Data\Opera\Opera\
	Windows Vista, 7 and latest version	C:\Users%\username%\AppData\Roaming\Opera\Opera\
Google Chrome	Linux	/home/\$USER/.config/google-chrome/Default/Preferences
	MacOS-X	/Users/\$USER/Library/Application Support/Google/Chrome/Default/Preferences
	Windows XP	C:\Documents and Settings%\username%\Local Settings\Application Data\Google\Chrome\User Data\Default\Preferences
	Windows Vista, 7 and latest version	C:\Users%\username%\AppData\Local\Google\Chrome\User Data\Default\Preferences

- **Web Browser working**

A browser is a software application used to locate, retrieve and display content on the World Wide Web, including Web pages, images, video and other files. As a client/server model, the browser is the client run on a computer that contacts the Web server and requests information. The Web server sends the information back to the Web browser which displays the results on the computer or other Internet-enabled device that supports a browser.

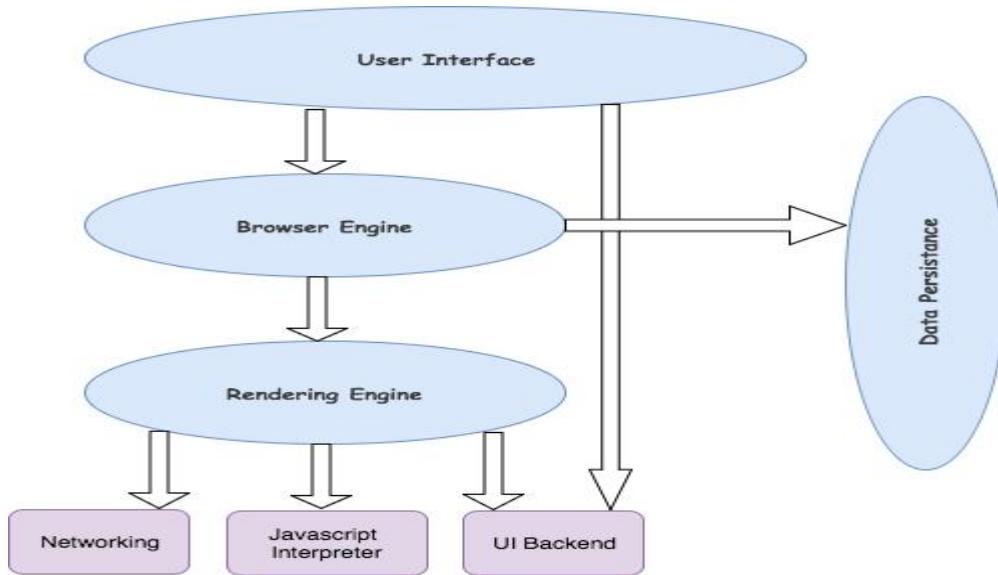


Today's browsers are fully-functional software suites that can interpret and display HTML Web pages, applications, JavaScript, AJAX and other content hosted on Web servers. Many browsers offer plug-ins which extend the capabilities of the software so it can display multimedia information (including sound and video), or the browser can be used to perform tasks such as videoconferencing, to design web pages or add anti-phishing filters and other security features to the browser.

A browser is a group of structured codes which together performs a series of tasks to display a web page on the screen. According to the tasks they perform, these codes are made as different components.

High-level architecture of browser

The below image shows the main components of a web browser:



Main components of the browser

1. **The User Interface:** The user interface is the space where User interacts with the browser. It includes the address bar, back and next buttons, home button, refresh and stop, bookmark option, etc. Every other part, except the window where requested web page is displayed, comes under it.
2. **The Browser Engine:** The browser engine works as a bridge between the User interface and the rendering engine. According to the inputs from various user interfaces, it queries and manipulates the rendering engine.
3. **The Rendering Engine:** The rendering engine, as the name suggests is responsible for rendering the requested web page on the browser screen. The rendering engine interprets the HTML, XML documents and images that are formatted using CSS and generates the layout that is displayed in the User Interface. However, using plugins or extensions, it can display other types data also. Different browsers use different rendering engines:
 - * Internet Explorer: Trident
 - * Firefox & other Mozilla browsers: Gecko
 - * Chrome & Opera 15+: Blink
 - * Chrome (iPhone) & Safari: Webkit
4. **Networking:** Component of the browser which retrieves the URLs using the common internet protocols of HTTP or FTP. The networking component

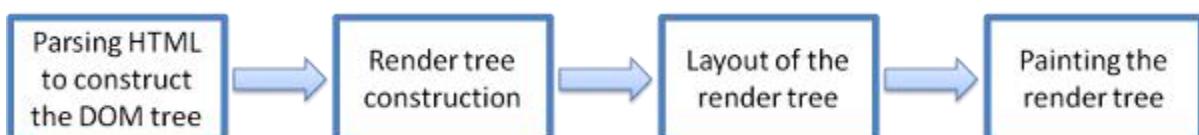
handles all aspects of Internet communication and security. The network component may implement a cache of retrieved documents in order to reduce network traffic.

5. **JavaScript Interpreter:** It is the component of the browser which interprets and executes the javascript code embedded in a website. The interpreted results are sent to the rendering engine for display. If the script is external then first the resource is fetched from the network. Parser keeps on hold until the script is executed.
6. **UI Backend:** UI backend is used for drawing basic widgets like combo boxes and windows. This backend exposes a generic interface that is not platform specific. It underneath uses operating system user interface methods.
7. **Data Persistence/Storage:** This is a persistence layer. Browsers support storage mechanisms such as localStorage, IndexedDB, WebSQL and FileSystem. It is a small database created on the local drive of the computer where the browser is installed. It manages user data such as cache, cookies, bookmarks and preferences.

An important thing to note here is that in web browsers such as Google Chrome each tab runs in a separate process(multiple instances of rendering engine).

Rendering engine

The networking layer will start sending the contents of the requested documents to the rendering engine in chunks of 8KBs.



Rendering engine basic flow

The rendering engine parses the chunks of HTML document and convert the elements to DOM nodes in a tree called the “**content tree**” or the “**DOM tree**”. It also parses both the external CSS files as well in style elements.

While the DOM tree is being constructed, the browser constructs another tree, the **render tree**. This tree is of visual elements in the order in which they will be

displayed. It is the visual representation of the document. The purpose of this tree is to enable painting the contents in their correct order. Firefox calls the elements in the render tree “frames”. WebKit uses the term renderer or render object.

After the construction of the render tree, it goes through a “**layout process**” of the render tree. When the renderer is created and added to the tree, it does not have a position and size. The process of calculating these values is called layout or reflow. This means giving each node the exact coordinates where it should appear on the screen. The position of the root renderer is 0,0 and its dimensions are the viewport—the visible part of the browser window. All renderers have a “layout” or “reflow” method, each renderer invokes the layout method of its children that need layout.

The next stage is **painting**. In the painting stage, the render tree is traversed and the renderer’s “paint()” method is called to display content on the screen. Painting uses the UI backend layer.

The rendering engine always tries to display the contents on the screen as soon as possible for better user experience. It does not wait for the HTML parsing to complete before starting to build and layout the render tree. It parses and displays the content it has received from the network, while rest of the contents stills keeps coming from the network.

- **Forensics activities on browser**

Encryption of data

Part of the data in web browsers is encrypted (for example, passwords to websites). Internet Explorer on Microsoft EDGE uses the Data Protection Application Programming Interface. The DPAPI mechanism appeared in Windows 2000 and is used to protect stored passwords and confidential information on the computer. This mechanism includes the functions of encryption and decryption of data and RAM.

You need a user password to decrypt the encrypted data. If the password is logged into your account using the login and the password, the operating system uses the hash of the password to decrypt the encrypted data.

As a rule, data encryption is carried out using the SHA1 algorithm, however, in some cases, the data is encrypted using a less crypto-resistant algorithm.

Difficulties of web browsers forensic analysis

An examiner can have the following difficulties when analyzing web browsers:

- Many browsers, lots of data
- Different data
- Encryption used to protect user data
- User's use of Private mode (or Incognito mode), in which the examined computer does not have web browser artifacts.

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
- Screenshots
- Financial info
- Form values (Searches, Autofill)
- Downloaded files (Downloads)
- Favorites

Tools for Analysis:

Commonly WEFA, NetAnalaysis, Browser History Examiner, FTK and Encase are software used for analyzing web browsers in digital forensics examinations. In this chapter features of specified web browser analyze tools are demonstrated [7].

1. IEF (Internet Evidence Finder)

IEF is a software with license fee produced by Magnet forensics company. Personal computers are used in the process of examinations of smart phones and tablets by experts. With its different models, it presents the characteristics like examining internet TV series, analysis of traces obtained from mobile applications. It is used on Windows and MacOs operating systems.

2. WEFA

WEFA is a free web browser analyze tool. It runs on Windows NT and later versions. Supports Internet Explorer(~11), Mozilla Firefox, Apple Safari, Opera, Chromium, Google Chrome, Google Chrome Canary, Comodo Dragon, CoolNovo(ChromePlus), Swing browsers. For these browsers WEFA offers various methods to perform analysis from an active system or an image disk. These methods include gathering the web browser's cache, cookies, internet history, download history, session data, temporary internet files, and the timesheet data information. The obtained data can be displayed in timeline view, HTML view or URL parameters view. Searches can be made in obtained data by date, key word or regular expressions. Also deleted data can be recovered, index.dat file can be analyzing in detail and classification and analysis of user behaviors can be made. CSV formatted reports can be generated according to these data.

3. NetAnalysis

NetAnalysis is a licensed tool developed by Digital Detective company for digital examining of web browsers. And supports Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari and Opera bowsers. It allows the examination of Internet history, cache, cookies and other components. And it has an effective reporting feature that allows quickly gathering evidence according to user behavior. Also this software has effective analytical tools for decoding and understanding data. At the same time, it has ability to use SQL queries to identify related evidence. Also it can be used to recover deleted web browser components

4. Browser History Examiner

Browser History Examiner is a licensed tool developed by Foxton Forensics Company and it extracts and analyzes web history. It supports Chrome, Firefox, Internet Explorer and Edge web browsers. And it can analyze a lot of data type as downloads, cache data and visited URL files. Internet activities in a specific timeline can be traced with web site timeline feature. Data can be analyzed by using various filters like key word list and time-date range with advanced filtering feature. Image files saved in the browser cache can be easily shown in thumbnail galleries with cache image viewer feature. Web sites stored in browser cache can be reconstructed and analyzed with cache web page viewer feature. Different time zone conversions can be performed with Time Zone and DST Configuration feature. And all obtained data from these features are reported.

5. FTK

FTK is one of the tools developed to analyze systems entirely. It enables to analyze web browser data with its features. Web browser history is virtualized in detail. Internet Explorer, Firefox, Chrome, Safari and Opera browsers are supported. Also, deleted web browser data can be recovered by FTK. This software also has a feature to report analysis results.

6. Encase

Encase system is an analysis tool developed to examine systems entirely. It enables to examine web browser data with its features. With the help of a simple script, all browser history, cookies and cache files are copied into a file by using 3rd party software. Internet explorer, Firefox, Chrome / Chromium, Opera and Safari are supported in Windows, UNIX and Mac operating systems. Also it enables to recover deleted internet components. Obtained data can be analyzed by filtering according to key word and time parameters.

WEFA, NetAnalysis and History Examiner are developed especially for performing digital analysis of web browsers. But, FTK and EnCase applications are developed to examine files and systems. This software also has features as analyzing web history and holistic analysis.

4. Conclusion

Web browser analysis is one of the most important processes in digital forensics. Most of the crimes committed through computer systems is performed via a web browsers and a lot of crimes are revealed by this analysis. Digital forensics experts must know how web browsers save data in different operating systems to be able to collect evidence from web browsers. Obtaining search history of the suspect, search words, visited URLs, download history and cache data is very important for gathering evidence. Information which obtained from user files reveals whether the offense occurred or not. Therefore, experts must analyze browser data correctly.

In this paper it is shown how most commonly used web browsers store data, what information can be recover or analyze and how different operating systems store records. Besides, applications which can be used by experts who perform analysis in this field, are introduced. Thus, it is put forward which data will be obtained and analyzed by expert in this field.

- Cache / Cookies analysis

- Cookies

Cookies are text files used to give feedback from the user to the server. When performing some actions with a web resource (viewing web links,

downloading files, etc.), these actions are registered in a cookie that is secretly sent by the server to the user's computer. With this web resource, the server has the ability to find out what actions the user has taken on previous visits to this web resource.

\Users\%UserProfile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxx
x.default\cookies.sqlite (Firefox, Windows)

\Users\%UserProfile%\AppData\Local\Google\Chrome\User
Data\Default\Cookies.db (Google Chrome, Windows)

\Windows\Cookies\ (Windows 98) (Internet Explorer)

\Documents and Settings\Administrator\Cookies (Windows 2000, Windows
XP) (Internet Explorer)

\Users\%UserProfile%\AppData\Roaming\Microsoft\Windows\Cookies
(Windows 7) (Internet Explorer)

\Users\Default\AppData\Roaming\Microsoft\Windows\Cookies (Windows
7) (Internet Explorer)

- **Cache**

\Users\%UserProfile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxx
x.default\cache2\entries Firefox (Windows)

\Users\%UserProfile%\AppData\Local\Google\Chrome\User
Data\Default\Cache\ (Google Chrome, Windows)

\Users\%UserProfile%\AppData\Local\Google\Chrome\User
Data\Default\GPUCache\ (Google Chrome, Windows)

\Users\%UserProfile%\AppData\Local\Google\Chrome\User
Data\Default\Media Cache\ (Google Chrome, Windows)

\Users\%UserProfile%\AppData\Roaming\Opera Software\Opera
Stable\ShaderCache\GPUCache\data_3 (Opera, Windows)

- **Last Internet activity**

Some important paths in internet activities :

- **Searches**

\Users\%UserProfile%\AppData\Local\Google\Chrome\User
Data\Default\Web Data (Google Chrome, Windows)

- **Most Visited sites**

\Users\%UserProfile%\Library\Safari\TopSites.plist (Safari, MacOS)

- **Last Session**

\Users\%UserProfile%\AppData\Local\Google\Chrome\User
Data\Default\Last Session (Google Chrome, Windows)

\Users\%UserProfile%\AppData\Roaming\Opera Software\Opera
Stable\Last Session (Opera, Windows)

\Users\%UserProfile%\Library\Safari\LastSession.plist (Safari, MacOS)

- **Last Tabs**

\Users\%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\Last Tabs (Google Chrome, Windows)

\Users\%UserProfile%\AppData\Roaming\Opera Software\Opera Stable\Last Tabs (Opera, Windows)

- **Current Tabs**

\Users\%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\Current Tabs (Google Chrome, Windows)

\Users\%UserProfile%\AppData\Roaming\Opera Software\Opera Stable\Current Tabs (Opera, Windows)

- **Current Session**

\Users\%UserProfile%\AppData\Local\Google\Chrome\User Data\Default\Current Session (Google Chrome, Windows)

- **Session**

\Users\%UserProfile%\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3

d8bbwe\AC\MicrosoftEdge\User\Default\Recovery\Active\{07677C23-6987-4777-B133-5AC24BD039F5}.dat (Microsoft EDGE, Windows)

\Users\%UserProfile%\AppData\Roaming\Opera Software\Opera Stable\Current Session (Opera, Windows)

- **Session Recovery**

\Users\%UserProfile%\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3

d8bbwe\AC\MicrosoftEdge\User\Default\Recovery\Active\{A7D7A4FC-7458-11E6-9BCD-000C29566E3E}.dat (Microsoft EDGE, Windows)

\Users\%UserProfile%\AppData\Roaming\Mozilla\Firefox\Profiles\xxxxxxx.x.default\sessionstore.js

(Firefox, Windows)

9.B

Case Study : Granny Clampet Solution

1. All the registry files are exported from the evidence provided.

2.

 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/

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?

 Save Directory

REG_SZ

C:\Documents and Settings\Granny\My Documents\

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 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. Portable devices

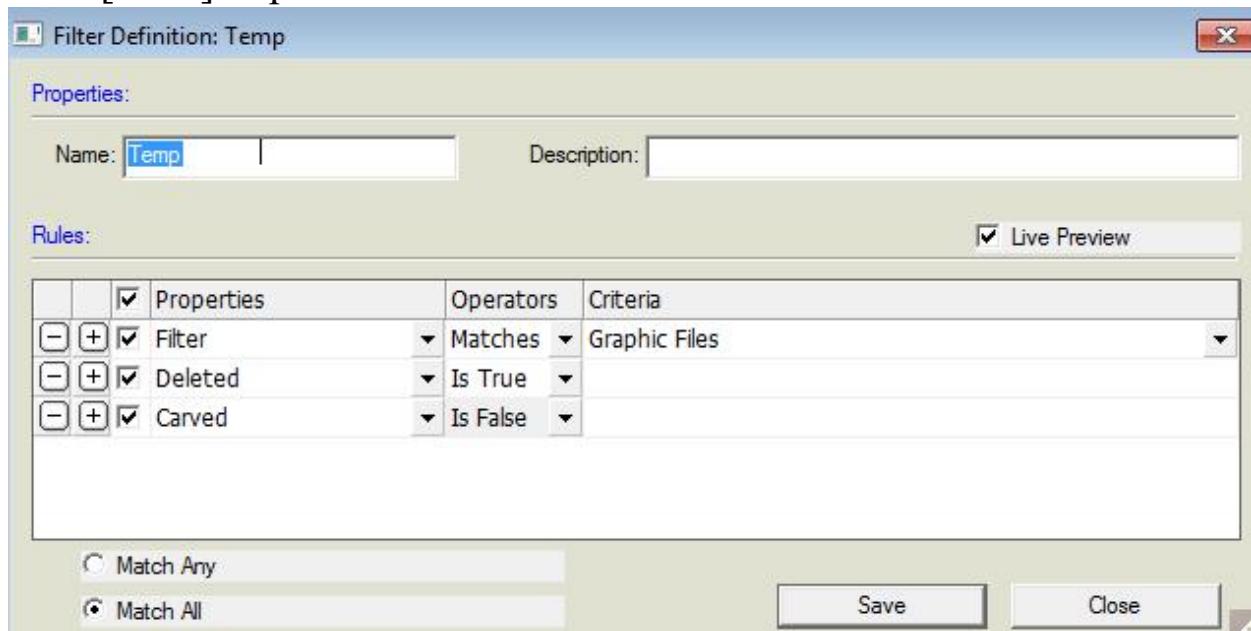


system[2310].tmp\ControlSet001\Enum\USBSTOR

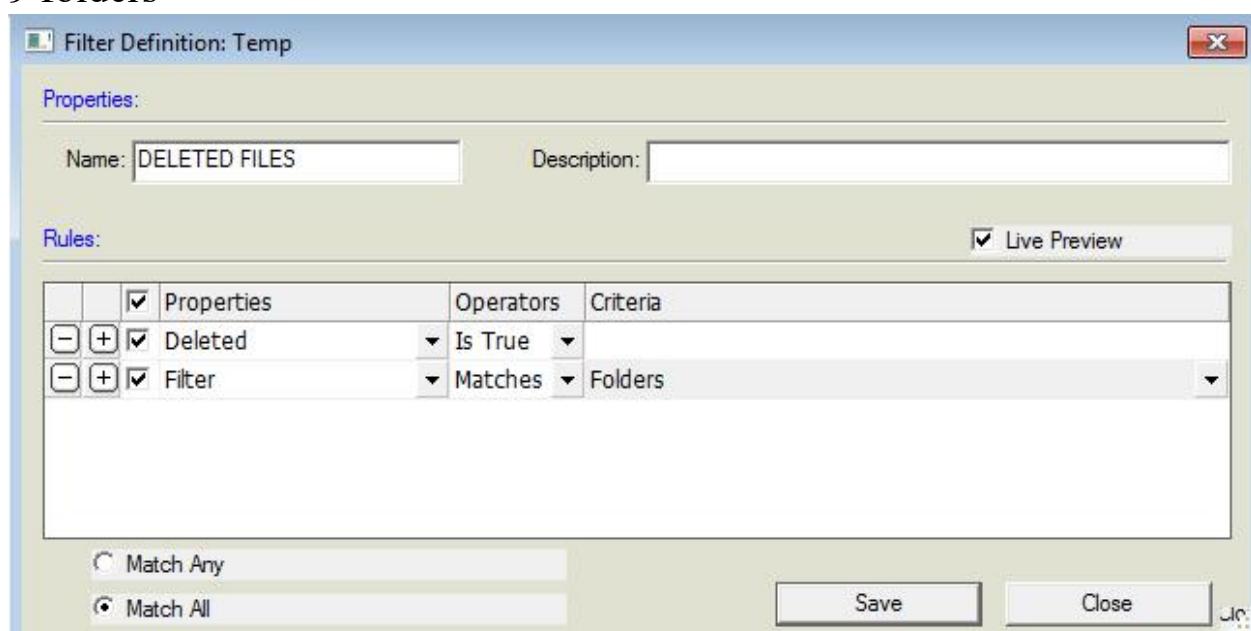
C. Document when Granny last logged on to this machine.

7/3/2009 23:10:23 UTC

SAM[2320].tmp\SAM\Domains\Account\Users\000003EE



9 folders



Four Folders

D. Generate a Report based on the System 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

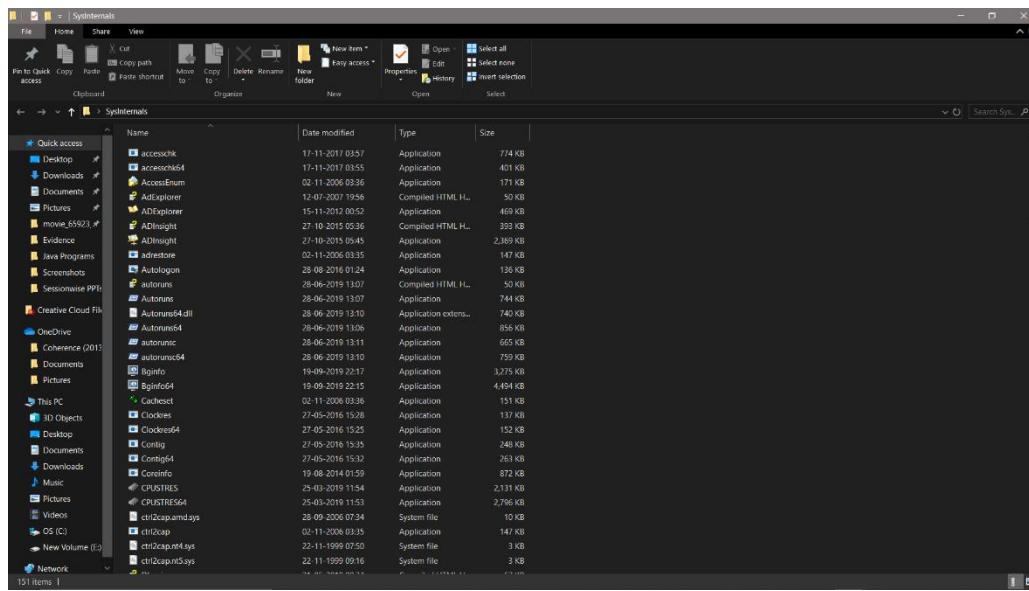
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

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

Using Sisinternals tools for Network Tracking and Process Monitoring

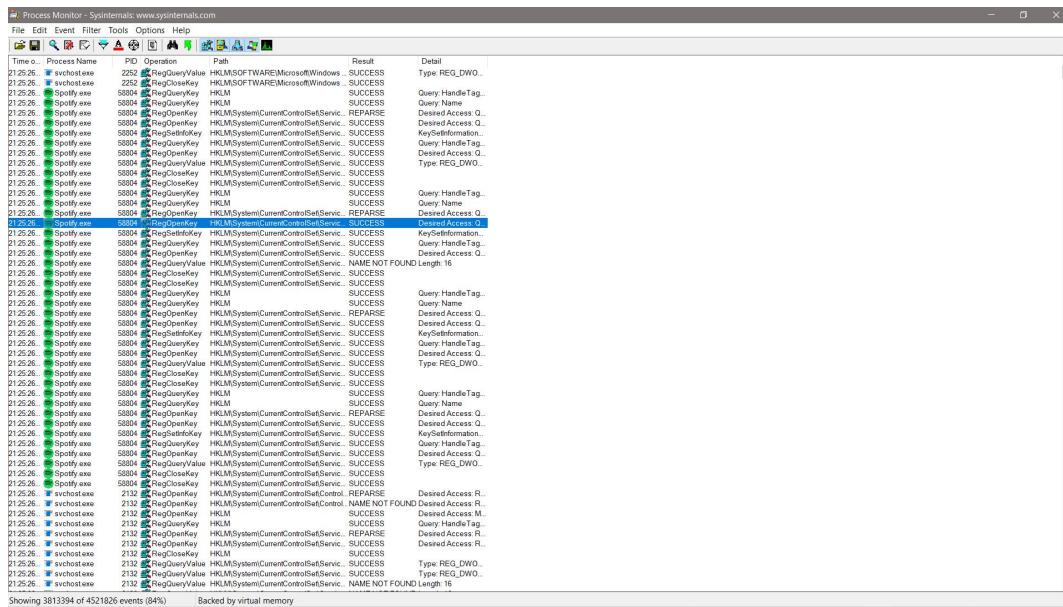
To download the SysInternals tools we can go to Microsoft's official site to download the SysInternals Suite package which contains all of the SysInternals tools.



In the above picture we can see some of the various variety of tools we are provided with in the SysInternals Suite package.

Capture Live Processes:

Now, to monitor live processes of the system we use the application ‘Process Monitor’ which can be found as Procmon64 in the package.



The above image shows the processes captured in this session in the Process Manager. These are all the live process running right now on the system.

Now, to have a simplified view of the live processes running we can use the ‘Process Tree’. We can access it by going to the ‘Tools’ drop-down menu and click ‘Process Tree’ or pressing CTRL+ T.

The screenshot shows the 'Process Tree' window with the following details:

Process	Description	Image Path	Life Time	Company
ModuleCoreService.exe (412)	McAfee Module C...	C:\Program Files\...		McAfee, LLC.
ModuleCoreService.exe (5)	McAfee Module C...	C:\Program Files\...		McAfee, LLC.
conhost.exe (53956)	Console Window ...	C:\WINDOWS\syst...		Microsoft Corpor
PnkBstrA.exe (4140)		C:\WINDOWS\Sys...		
PEFService.exe (4148)	McAfee PEF Servi...	C:\Program Files\...		McAfee, Inc.
AGSService.exe (4176)	Adobe Genuine S...	C:\Program Files (...		Adobe Systems.
svchost.exe (4184)	Host Process for ...	C:\WINDOWS\syst...		Microsoft Corpor
svchost.exe (4220)	Host Process for ...	C:\WINDOWS\Sys...		Microsoft Corpor
GameManagerService.exe (4240)	GameManagerSer...	C:\Program Files (...		Razer Inc
RazerCentralService.exe (4260)	Razer Central Serv...	C:\Program Files (...		Razer Inc.
runSW.exe (4300)		C:\Windows\runS...		
SmartByteNetworkService.exe	SmartByte Networ...	C:\Program Files\...		Rivet Networks
SynTPEnhService.exe (4340)	64-bit Synaptics P...	C:\Program Files\...		Synaptics Incorp
SynTPEnh.exe (46652)	Synaptics TouchP...	C:\Program Files\...		Synaptics Incorp
AGMService.exe (4424)	Adobe Genuine S...	C:\Program Files (...		Adobe Systems.
WavesSysSvc64.exe (4464)	WavesSysSvc Se...	c:\Program Files\...		Waves Audio Ltc

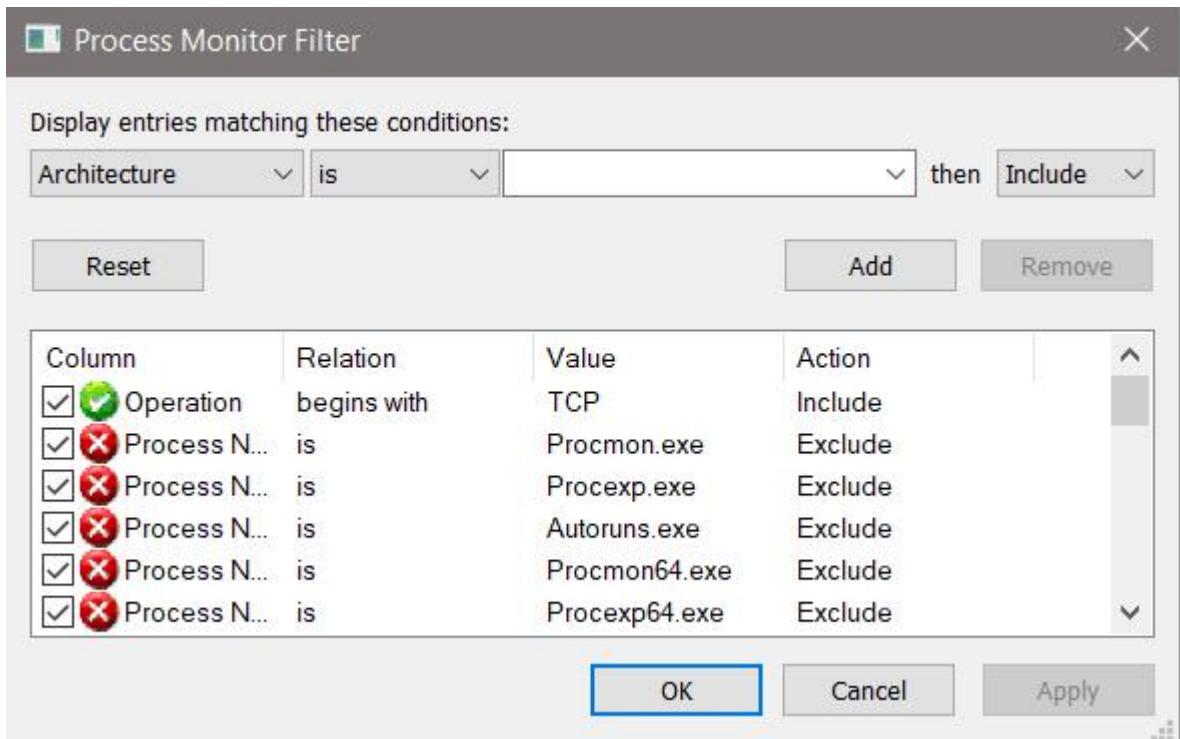
Description:
Company:
Path: Idle
Command:
User:
PID: 0 Started: 15-03-2020 18:28:13

Go To Event Include Process Include Subtree Close

The picture above shows the Process Tree of my system. These are some of the live processes.

Capture TCP/UDP Packets:

Process Monitor can also be used to capture TCP Packets. To do this, first we need to apply the filter of including TCP packets in the capture and excluding lsass.exe and svchost.exe for better functioning and capture of our processes.



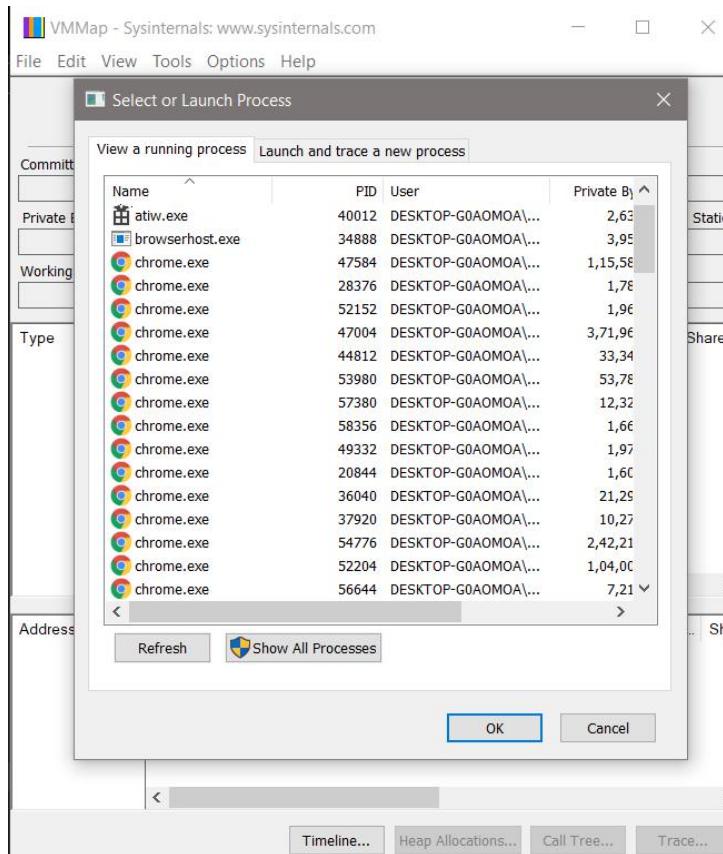
The above picture shows that the filters have been applied using the Process Monitor Filter.

So, now when we capture the packets it will only show the packets that follow the TCP protocol as we can see in the picture below.

Time o...	Process Name	PID	Operation	Path	Result	Detail
21:59:37...	Spotify.exe	58804	TCP Receive	DESKTOP-G0AOMOA:64843 -> 47.224.1...	SUCCESS	Length: 31, seqnum...
21:59:38...	Spotify.exe	58804	TCP Receive	DESKTOP-G0AOMOA:64844 -> 2600:190...	SUCCESS	Length: 0, seqnum: ...
21:59:38...	Spotify.exe	58804	TCP Disconnect	DESKTOP-G0AOMOA:64844 -> 2600:190...	SUCCESS	Length: 0, seqnum: ...
21:59:49...	chrome.exe	37920	TCP Receive	DESKTOP-G0AOMOA:64842 -> del03s0...	SUCCESS	Length: 56, seqnum...
21:59:49...	chrome.exe	37920	TCP Disconnect	DESKTOP-G0AOMOA:64842 -> del03s0...	SUCCESS	Length: 0, seqnum: ...
22:00:08...	Spotify.exe	58804	TCP Send	DESKTOP-G0AOMOA:64843 -> 47.224.1...	SUCCESS	Length: 35, startim...
22:00:08...	Spotify.exe	58804	TCP TCPCopy	DESKTOP-G0AOMOA:64843 -> 47.224.1...	SUCCESS	Length: 31, seqnum...
22:00:08...	Spotify.exe	58804	TCP Receive	DESKTOP-G0AOMOA:64843 -> 47.224.1...	SUCCESS	Length: 31, seqnum...
22:00:08...	chrome.exe	44812	TCP Disconnect	DESKTOP-G0AOMOA:64832 -> laureate...	SUCCESS	Length: 0, seqnum: ...
22:00:08...	chrome.exe	44812	TCP Disconnect	DESKTOP-G0AOMOA:64831 -> laureate...	SUCCESS	Length: 0, seqnum: ...
22:00:09...	chrome.exe	44812	TCP Connect	DESKTOP-G0AOMOA:64851 -> 161.69.2...	SUCCESS	Length: 0, mss: 137...
22:00:09...	chrome.exe	44812	TCP Connect	DESKTOP-G0AOMOA:64852 -> 161.69.2...	SUCCESS	Length: 0, mss: 137...
22:00:09...	chrome.exe	44812	TCP Send	DESKTOP-G0AOMOA:64851 -> 161.69.2...	SUCCESS	Length: 536, startim...
22:00:09...	chrome.exe	44812	TCP Receive	DESKTOP-G0AOMOA:64851 -> 161.69.2...	SUCCESS	Length: 1370, seqn...
22:00:09...	chrome.exe	44812	TCP Receive	DESKTOP-G0AOMOA:64851 -> 161.69.2...	SUCCESS	Length: 1370, seqn...
22:00:09...	chrome.exe	44812	TCP Receive	DESKTOP-G0AOMOA:64851 -> 161.69.2...	SUCCESS	Length: 1370, seqn...
22:00:09...	chrome.exe	44812	TCP Receive	DESKTOP-G0AOMOA:64851 -> 161.69.2...	SUCCESS	Length: 436, seqnu...
22:00:09...	chrome.exe	44812	TCP Send	DESKTOP-G0AOMOA:64852 -> 161.69.2...	SUCCESS	Length: 536, startim...
22:00:09...	chrome.exe	44812	TCP Receive	DESKTOP-G0AOMOA:64852 -> 161.69.2...	SUCCESS	Length: 1370, seqn...
22:00:09...	chrome.exe	44812	TCP Receive	DESKTOP-G0AOMOA:64852 -> 161.69.2...	SUCCESS	Length: 1370, seqn...
22:00:09...	chrome.exe	44812	TCP Receive	DESKTOP-G0AOMOA:64852 -> 161.69.2...	SUCCESS	Length: 1370, seqn...
22:00:09...	chrome.exe	44812	TCP Receive	DESKTOP-G0AOMOA:64852 -> 161.69.2...	SUCCESS	Length: 436, seqnu...

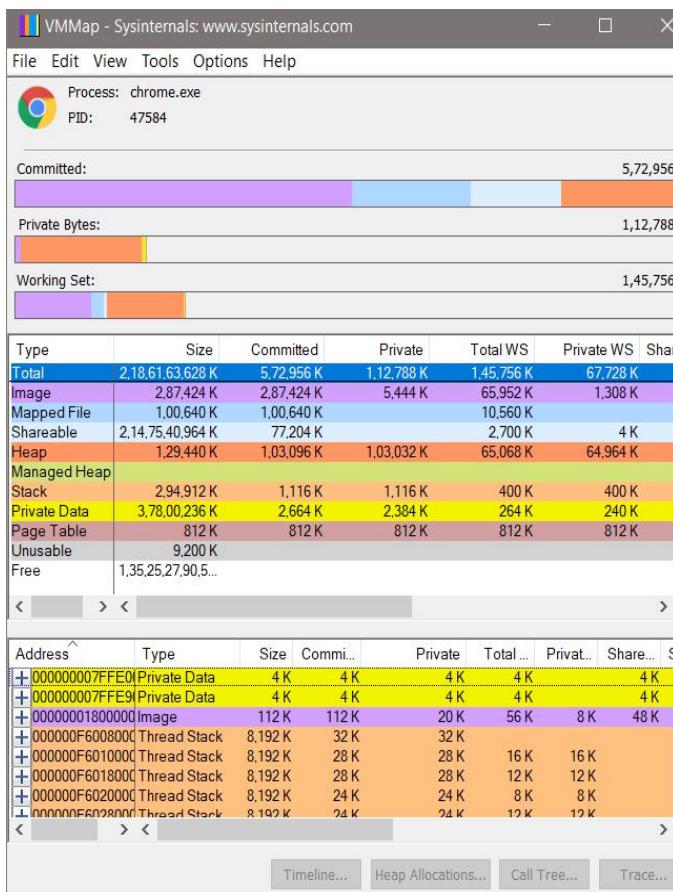
Monitor Virtual Memory:

To Monitor Virtual Memory using a SysInternals tool, we have to use VMMap. 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*'.

Now once we click '*Okay*' we will see the able to see the memory occupied by the process as shown in the picture below.



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.

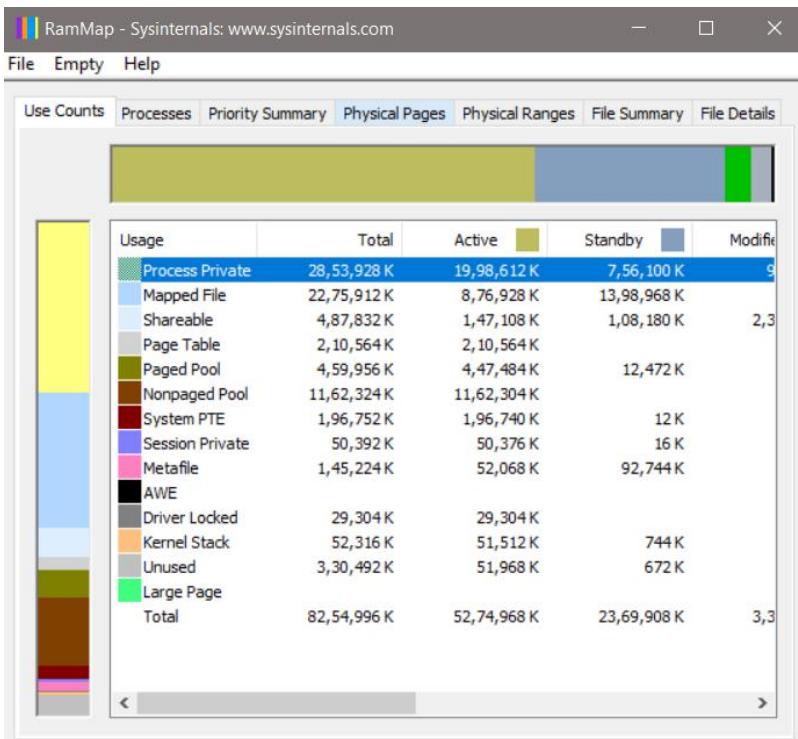
The screenshot shows the Disk Monitor application interface. At the top, it displays the process name as "Disk Monitor" and PID as "47584". Below this is a table of disk activity logs:

#	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

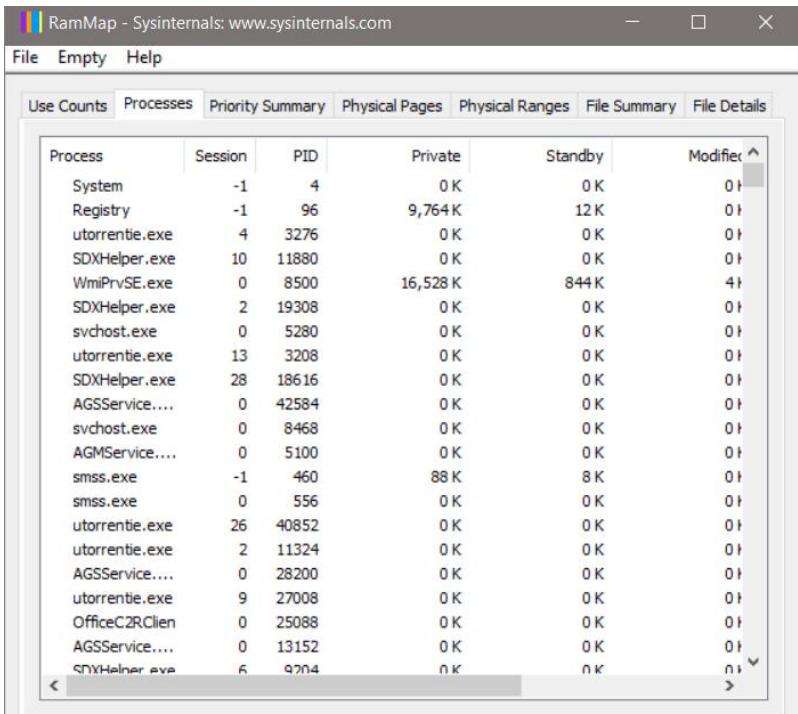
Therefore, as we can see in the image above these are some of the process that are running in the Hard Disk.

Monitor Cache Memory:

We know that cache memory is stored in RAM. Therefore, we need to use RAMMap to monitor Cache Memory. We can find this in the SysInternals 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.

THE END