PRACTICAL NO. 1

Aim:

Creating a Forensic Image using FTK Imager/Encase Imager:

- Creating Forensic Image
- Check Integrity of Data
- Analyze Forensic Image

In this Practical we are going to use the FTK Imager to create Images of the evidences

Go to File → Create Disk Image

Select the source evidence type

Here we are going to select the physical drive and proceed Then we browse the location of the Pen drive and click Finish

Now we add the location to create images

In this we are going to select the **raw (dd)** format

And now we fill the details required for the case

Create a folder to save the images to store in the system disk as the pen drive size cannot be stored in the same drive

Then paste that location to save the images and click Finish

Then Click on Start and wait until the imaging is done

Now it will verify

This is the Hash Value CheckSum given if it matches the original values then the evidence is original if not the evidence is been misplaced

We take the image summary

Now we are going to view the images in the FTK

Imager Go to File

Then select the type of the evidence here it is Image File

Give the directory of the images created using the FTK Imager and click Finish

Here we can see the data shown by the FTK Imager

AccessData FTK Imager 3.4.3.3
File View Mode Help
Evidence Tree
290723.001
Partition 1 [29339MB]
MADDY 48 [FAT32]
[root]
System Volume Information
[unallocated space]
Unpartitioned Space [basic disk]
[unallocated space]
File List
Name Size Type Date Modified
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Int... Custom Conte...
Cursor pos = 0; phy sec = 0
290723.001
NUM

AccessData FTK Imager 3.4.3.3
File View Mode Help
Evidence Tree
290723.001
Partition 1 [29339MB]
MADDY 48 [FAT32]
[root]
System Volume Information
[unallocated space]
Unpartitioned Space [basic disk]
[unallocated space]
File List
Name Size Type Date Modified
IndexerVolumeGuid 1 Regular File 29-08-2023 10:...
IndexerVolumeGuid.Fi... 16 File Slack
WPSettings.dat 1 Regular File 29-08-2023 10:...
WPSettings.dat.FileSlack 16 File Slack
Custom Content Sources
Evidence:File System|Path|File Options

PRACTICAL NO. 2

Aim:

Data Acquisition:

- Perform data acquisition using:
- USB Write Blocker + Encase Imager
- SATA Write Blocker + Encase Imager
- Falcon Imaging Device

USB Writer Blocker + Encase Imager

Hardware and Paid Softwares https://www.getfastforensics.com/write-blockers https://www.amazon.com/usb-writeblocker/s?k=usb+write+blocker&language=en_US&currency=INR http://www.orionforensics.com/forensics-tools/orion-usb-write-blocker/ **For Open Source Software** https://sourceforge.net/projects/usbwriteblockerforwind ows8/ **Encase Imager**

Encase is a forensic suite produced by Guidance Software (now part of OpenText) that is popular with commercial providers. A standard license comes in at around $3500 around ₹289242 **Overview PDF for the Encase Imager** https://www.opentext.com/assets/documents/en-US/pdf/opentext-po-encase- forensicen.pdf https://www.forensicstore.com/product/encase-

forensic-v8-06/ **YouTube link to see the working of the Encase Imager**

https://www.youtube.com/watch?v=obmRoD3ChSc

Here is an Overview of the Encase Imager

https://www.hackingarticles.in/forensic-imagingencase/ SATA Write Blocker + Encase Imager

Overview of Write Blockers

https://linuxhint.com/best_hardware_write_blockers/

https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-programcftt/cftt- technical/hardware Setup of the Write Blocker https://www.youtube.com/watch?v=Kmm8iaa76rQ

Falcon Imaging Device

About Info of the Falcon Imaging Device https://www.logicube.com/shop/forensic-falcon-neo/ http://www.edasfox.com/product/forensic-falcon-neo/ https://www.secureindia.in/?page_id=1068

Prices of the Falcon Imaging Device https://www.indiamart.com/proddetail/forensic-

falcon-

2850471543448.html

Documentation and Videos for Demonstration of the Working of the Flacon Imaging

Device https://www.forensicfocus.com/articles/how-to-create-a-logical-image-on-falcon-neo/

https://www.forensicfocus.com/articles/how-to-image-to-a-network-repository-withlogicubes-forensic- falcon-neo/

https://www.forensicfocus.com/articles/how-to-use-the-file-browser-feature-in-

logicubesforensic-falcon- neo/ https://www.youtube.com/watch?v=YSLSi1QpjUs

https://www.youtube.com/watch?v=rZLndjf1hPs

SELECT MODE
x
DRIVE TO FILE
FILE TO FILE
PARTITION TO FILE
NET TRAFFIC TO FILE
DRIVE TO DRIVE
FILE TO DRIVE
OK

PRACTICAL NO. 3

Aim:

Analyze the memory dump of a running computer system.

- Extract volatile data, such as open processes, network connections, and registry information.

Open Process

Go to Sysinternal Suite **ProcMon** Right Click on it and **Open As Administrator**

Network Connections

Go to SysinternalSuite

- TCPview

Registry Information

Click on **Search Bar** on the **Taskbar** Type **Regedit** Click on **Registry Editor**

View the desired registries to be analyzed

PRACTICAL NO. 4

Aim:

Capturing and analyzing network packets using WireShark (Fundamentals):

- Identification the live network
- Capture Packets
- Analyze the captured packets

In this practical only **identification**, **capturing** and **analysis** is done. We will also **solve some cases to understand the practical clearly.** ***Identifying the Live Networks***

We are using **WireShark**, an application used to identify, capture and analyze the network traffics.

Capturing Network

We are now going to capture a network of Ethernet

As soon as you single-click on your network interface's name, you can see how the packets are working in real time. WireShark will capture all the packets going in and out of our systems.

Analyze the Captured Packets

Color Coding Different packets are seen highlighted in various different colors. This is WireShark's way of displaying traffic to help you easily identify the types of it.

Default colors are:

- Light Purple color for TCP traffic
- Light Blue color for UDP traffic
- Black color identifies packets with errors Example these packets are delivered in an unordered manner. Click on View Colorize Conversation New Coloring Rule

Here we can see the Default Colors given for every **Packet Capturing**

Now we analyze data using filters provided in the WireShark application write the following commands in the given area to apply filter

No.	Time	Source	Destination	Protocol	Length	Host	Server	Referer	Info
1	0.000000	HuaweiTe_9d:bb:d0	Broadcast	ARP	60				Who has 49.248.73.
2	0.095299	192.168.10.28	142.250.199.130	TLSv1.2	55				
3	0.097731	142.250.199.130	192.168.10.28	TCP	66				443 → 50164 [ACK]
4	0.199439	HuaweiTe_9d:bb:d0	Broadcast	ARP	60				Who has 49.248.73.
5	0.269636	Micro-St_60:2a:5b	Broadcast	ARP	60				Who has 192.168.10
6	0.497308	CompalIn_fb:47:4f	Broadcast	ARP	60				Who has 192.168.10
7	0.497309	CompalIn_fb:47:4f	Broadcast	ARP	60				Who has 192.168.10
8	1.129070	192.168.10.104	192.168.10.255	BROWSER	248				Domain/Workgroup A
9	1.269718	Micro-St_60:2a:5b	Broadcast	ARP	60				Who has 192.168.10

<u>Display filter command</u>

1. Display packets based on specific IP-address
   - ip.addr == 192.0.2.1

2. Display packets which are coming from specific IP-address **O** ip.src == 192.168.10.28

3. Display packets which are having specific IP-address destination **O** ip.dst == 192.168.10.28

4. Display packets which are using http protocol
   - http

5. Display packets which are using http request
   - http.request

6. Display packets which are using TCP protocol
   - tcp

7. Display packets having no error connecting to server
   - http.response.code==200

8. Display packets having port number 80, 443 ✪
   tcp.port==80 || udp.port==443

9. Display packets which that contains keyword facebook **O** tcp contains facebook

Now we are going to perform a **Case Study**

AIM:

Analyze the packets provided in lab and solve the questions using Wireshark

1. What web server software issued by go.microsoft.com?

Analysis –

The domain name be found from host header so we will set host header column where we will see all domain name. Select any HTTP request and expand the Hypertext Transfer Protocol then right click on Host header and then Apply as Column

First find the requests from **HTTP** and click on and **request** then on the **lower table of details** Select on

HyperText Transfer Protocol **Host** and **Right Click** on that and Select **Apply as Filter**

Now we can see the **Host**

Right click on the **selected packet** and then select **Follow** ⇒ **TCP stream**

2. About what cell phone problem is the client concerned?

<u>Analysis</u> –

Client talking about cell so we search for cell keyword in whole packets. We will use regular express for searching the cell keyword. Apply frame matches "()"

In the **<u>search frame</u>** type **frame matches "microsoft"**

After applying the filter now, we will start to check every HTTP request. We noticed in the first HTTP request microsoft keyword is in URL and it was about Microsoft Edge connection.

3. According to http, what data will TCP show?

<u>Analysis</u> –

As we did in the last challenge, we will **apply a regular express filter** for the Google **keyword**. **Apply frame matched "http"** .

Select the packet and **expand the Hypertext Transfer Protocol** tab **right click** on **Transmission Control Protocol Go to Protocol Preferences** and **check Allow subdissector** to resemble TCP stream with HTTP spanning bodies.

Now **Go to file** and **select Export Objects** ⍰ **HTTP**. It will save all objects from the packet.

Click on save all.

After checking it seems only the packets transfer were to connect the machine to the internet.

4. How many web servers are running Microsoft?

<u>Analysis</u> –

The web server name can be retrieved from **<u>HTTP response header</u>**. So will apply filter **http.response** and we can see all http response packets.

Now we will set the server header as column select any packet and right click on it then select Apply as Column.

Now can see the server column where all server name is showing.

Now we have to check how many Apache packets are there we can't count manually for each packet so we will apply another filter **http.server contains "Microsoft"**

After applying filter **<u>Go to Statistics</u>** → **<u>Endpoints</u>**

It will show all connections.

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
4.150.240.254	27	3646	14	1859	13	1787	—	—	—	—
8.8.8.8	40	5928	20	4410	20	1518	—	—	—	—
10.1.6.13	5	330	0	0	5	330	—	—	—	—
10.90.90.90	30	10 k	30	10 k	0	0	—	—	—	—
13.107.3.254	32	10 k	19	8572	13	1674	—	—	—	—
13.107.5.93	88	28 k	51	22 k	37	5790	—	—	—	—
13.107.6.254	35	11 k	21	10 k	14	1740	—	—	—	—
13.107.42.18	1,518	1518 k	1,138	1477 k	380	41 k	—	—	—	—
13.107.136.254	33	10 k	20	8630	13	1678	—	—	—	—
13.107.213.48	7	378	0	0	7	378	—	—	—	—
13.107.246.48	7	378	0	0	7	378	—	—	—	—
13.107.246.68	40	11 k	20	9191	20	2444	—	—	—	—
13.232.28.114	78	15 k	26	8343	52	7056	—	—	—	—
14.142.64.16	10	660	0	0	10	660	—	—	—	—
15.206.237.184	36	7828	16	3212	20	4616	—	—	—	—
20.42.65.90	53	22 k	27	7039	26	15 k	—	—	—	—
20.42.73.27	199	38 k	101	15 k	98	22 k	—	—	—	—
20.50.201.200	28	10 k	14	7594	14	2828	—	—	—	—
20.189.173.7	36	17 k	17	11 k	19	6607	—	—	—	—
20.189.173.11	107	22 k	56	11 k	51	11 k	—	—	—	—
20.189.173.14	1,415	853 k	782	113 k	633	739 k	—	—	—	—
20.197.103.14	186	82 k	96	55 k	90	26 k	—	—	—	—
20.198.118.190	49	12 k	25	8121	24	4405	—	—	—	—

Check the limit to display filter then it will show the actual Microsoft connections. Now there are showing 223 connections but will exclude 4.150.240.254 because it is client's IP not a server IP so there are actual 222 Microsoft servers.

Wireshark · Endpoints · Ethernet

Ethernet · 61 | IPv4 · 223 | IPv6 · 53 | TCP · 763 | UDP · 845

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
3.34.242.126	28	7978	17	6121	11	1857	—	—	—	—
4.150.240.254	27	3646	14	1859	13	1787	—	—	—	—
8.8.8.8	138	18 k	69	12 k	69	5466	—	—	—	—
10.1.6.13	5	330	0	0	5	330	—	—	—	—
10.90.90.90	36	12 k	36	12 k	0	0	—	—	—	—
13.71.55.58	45	13 k	20	9612	25	4327	—	—	—	—
13.78.111.198	209	126 k	115	23 k	94	103 k	—	—	—	—
13.107.3.254	32	10 k	19	8572	13	1674	—	—	—	—
13.107.5.93	88	28 k	51	22 k	37	5790	—	—	—	—
13.107.6.254	35	11 k	21	10 k	14	1740	—	—	—	—
13.107.42.18	1,518	1518 k	1,138	1477 k	380	41 k	—	—	—	—
13.107.136.254	33	10 k	20	8630	13	1678	—	—	—	—
13.107.213.48	7	378	0	0	7	378	—	—	—	—
13.107.246.48	7	378	0	0	7	378	—	—	—	—
13.107.246.68	40	11 k	20	9191	20	2444	—	—	—	—
13.115.74.94	31	11 k	19	9405	12	2019	—	—	—	—
13.228.126.19	24	8599	12	6287	12	2312	—	—	—	—
13.232.28.114	280	87 k	97	51 k	183	35 k	—	—	—	—
13.251.69.8	23	8215	11	6338	12	1877	—	—	—	—
14.142.64.16	10	660	0	0	10	660	—	—	—	—
15.206.237.184	36	7828	16	3212	20	4616	—	—	—	—
18.66.41.26	27	10 k	14	8877	13	1855	—	—	—	—
18.66.53.65	131	52 k	72	36 k	59	16 k	—	—	—	—

Name resolution Limit to display filter

CONCLUSION:

We have successfully analyzed the packets provided and solved the questions using WireShark

PRACTICAL NO. 5

Aim:

Using Sysinternals tools for Network Tracking and Process Monitoring:

- Check Sysinternals tools
- Monitor Live Processes
- Capture RAM
- Capture TCP/UDP packets
- Monitor Hard Disk
- Monitor Virtual Memory
- Monitor Cache Memory

Let Check If the **Sysinternal Suite** is **Available** on the **System** ***Check SysInternals Tools***

STEPS

Google ❼ sysinternal tools

If **Available** Then **Skip** the **Installation Part**

Let's Install the **Sysinternal Suite** for **Windows** We

can download the zip file from the given link

https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite

Then Extract the file to the desired directory

<u>Monitor Live Processes</u>

Process Monitor is an advanced monitoring tool for Windows that show real-time file system. Registry and process/thread activity. It combines the features of two legacy SysInternals utilities, Filemon and Regmon, and adds an extensive list of enhancements including rich non-destructive filtering, comprehensive event properties such as session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more.

<u>STEPS</u>

Sysinternal ❼ procmon

Then allow the permissions and then Select all the processes to be viewed

Then Click on Apply and then OK Then see the displayed Processes

Capture RAM

RAMMap is an advanced physical memory usage analysis utility for Windows Vista and higher. It presents usage information in different ways on its several different tabs:

- **Use Counts**: usage summary by type and paging list
- **Processes**: process working set sizes
- **Priority Summary**: prioritized standby list sizes
- **Physical Pages**: per-page use for all physical memory
- **Physical Ranges**: physical memory addresses
- **File Summary**: file data in RAM by file
- **File Details**: individual physical pages by file

STEPS

Sysinternal ❼ RAMMap

Then allow the permissions and view the mapping

Usage	Total	Active	Standby	Modified	Modified ...	Transition	Zeroed	Free	Bad
Process Private	32,13,936 K	30,54,888 K	972 K	1,58,056 K		20 K			
Mapped File	77,83,948 K	6,93,888 K	70,89,580 K	480 K					
Shareable	3,06,216 K	1,67,764 K	1,844 K	1,36,608 K					
Page Table	1,41,444 K	1,41,444 K							
Paged Pool	8,21,936 K	7,99,892 K	164 K	21,880 K					
Nonpaged Pool	5,17,552 K	5,17,552 K							
System PTE	4,42,736 K	4,42,736 K							
Session Private	320 K	320 K							
Metafile	24,34,692 K	56,928 K	23,77,764 K						
AWE									
Driver Locked	21,824 K	21,824 K							
Kernel Stack	75,160 K	74,896 K		264 K					
Unused	7,25,652 K	13,752 K					6,69,752 K	42,148 K	
Large Page									
Total	1,64,85,416 K	59,85,884 K	94,70,324 K	3,17,288 K		20 K	6,69,752 K	42,148 K	

<u>Capture TCP/UDP packets</u>

TCPView is Windows program that will show you detailed listening's of all TCP and UDP endpoints on your system, including the local and remote addresses and the state of TCP connections.

Using TCPView:

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

Using Tcpvcon

Tcpvcon using is similar to that of the built-in Windows netstat utility

Usage

Tcpvcon [-a] [-c] [-n] [process name or PID]

<u>STEPS</u>

Download TCPView

```
C:\SysinternalsSuiteNEW\tcpv

Tcpvcon.exe v4.19 - Sysinternals TcpVcon
Copyright (C) 1996-2023 Mark Russinovich & Bryce Cogswell
Sysinternals - www.sysinternals.com

[TCP] epmd.exe
        PID:    6732
        State:  ESTABLISHED
        Local:  D-24
        Remote: localhost
[TCP] [System Process]
        PID:    0
        State:  TIME_WAIT
        Local:  d-24.asccl.com
        Remote: d-23
[TCP] [System Process]
        PID:    0
        State:  TIME_WAIT
        Local:  d-24.asccl.com
        Remote: d-23
[TCP] [System Process]
        PID:    0
        State:  TIME_WAIT
        Local:  d-24.asccl.com
        Remote: d-23
[TCP] erl.exe
        PID:    6256
        State:  ESTABLISHED
        Local:  D-24
        Remote: localhost
```

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

4 TCP v4 6 TCP v6 4 UDP v4 6 UDP v6 Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	1328	TCP	Listen	0.0.0.0	135	0.0.0.0	0	29-08-2023 07:05:11	RpcSs
System	4	TCP	Listen	192.168.10.28	139	0.0.0.0	0	29-08-2023 08:36:37	System
System	4	TCP	Listen	192.168.44.1	139	0.0.0.0	0	29-08-2023 08:36:35	System
System	4	TCP	Listen	192.168.80.1	139	0.0.0.0	0	29-08-2023 08:36:35	System
vmware-authd.exe	5800	TCP	Listen	0.0.0.0	902	0.0.0.0	0	29-08-2023 07:05:12	VMAuthdService
vmware-authd.exe	5800	TCP	Listen	0.0.0.0	912	0.0.0.0	0	29-08-2023 07:05:12	VMAuthdService
sqlservr.exe	8936	TCP	Listen	127.0.0.1	1434	0.0.0.0	0	29-08-2023 07:05:15	MSSQLSERVER
mysqld.exe	4652	TCP	Listen	0.0.0.0	3306	0.0.0.0	0	29-08-2023 07:05:13	MySQL
epmd.exe	6996	TCP	Listen	0.0.0.0	4369	0.0.0.0	0	29-08-2023 07:05:13	
epmd.exe	6996	TCP	Established	127.0.0.1	4369	127.0.0.1	49694	29-08-2023 07:05:13	
svchost.exe	10804	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	29-08-2023 08:36:32	CDPSvc
erl.exe	6756	TCP	Listen	127.0.0.1	5984	0.0.0.0	0	29-08-2023 07:05:14	
emlproxy.exe	4496	TCP	Listen	127.0.0.1	17400	0.0.0.0	0	29-08-2023 07:05:11	Core Mail Protection
mongod.exe	4688	TCP	Listen	127.0.0.1	27017	0.0.0.0	0	29-08-2023 07:05:12	MongoDB
lsass.exe	688	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	29-08-2023 07:05:11	
wininit.exe	936	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	29-08-2023 07:05:11	
svchost.exe	1944	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	29-08-2023 07:05:11	Schedule
svchost.exe	2980	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	29-08-2023 07:05:11	EventLog
spoolsv.exe	4164	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	29-08-2023 07:05:11	Spooler

Endpoints: 117 | Established: 15 | Listening: 37 | Time Wait: 9 | Close Wait: 6 | Update: 2 sec | States: (All)

TCPView - Sysinternals: www.sysinternals.com

File Edit View Process Connection Options Help

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
svchost.exe	6108	UDP		127.0.0.1	51273	*		29-08-2023 08:36:36	SSDPSRV
WINWORD.EXE	5704	UDP		127.0.0.1	51807	*		29-08-2023 07:08:11	WINWORD.EXE
svchost.exe	2140	UDP		127.0.0.1	52266	*		29-08-2023 07:05:13	netprofm
dasHost.exe	3764	UDP		0.0.0.0	61128	*		29-08-2023 08:36:46	
chrome.exe	15968	UDP		0.0.0.0	5353	*		29-08-2023 08:36:46	chrome.exe
chrome.exe	15968	UDP		0.0.0.0	5353	*		29-08-2023 08:36:46	chrome.exe
chrome.exe	15968	UDP		0.0.0.0	5353	*		29-08-2023 08:36:46	chrome.exe
svchost.exe	1536	UDPv6		::	123	*		29-08-2023 08:37:16	W32Time
svchost.exe	4544	UDPv6		::	500	*		29-08-2023 07:05:11	IKEEXT
svchost.exe	6108	UDPv6		::1	1900	*		29-08-2023 08:36:35	SSDPSRV
svchost.exe	6108	UDPv6		fe80::3b4f:9f72:34ab:146	1900	*		29-08-2023 08:36:35	SSDPSRV
svchost.exe	6108	UDPv6		fe80::3b4f:9f72:34ab:146	1900	*		29-08-2023 08:36:35	SSDPSRV
svchost.exe	6108	UDPv6		fe80::3b4f:9f72:34ab:146	1900	*		29-08-2023 08:36:35	SSDPSRV
dasHost.exe	3764	UDPv6		::	3702	*		29-08-2023 08:36:46	
dasHost.exe	3764	UDPv6		::	3702	*		29-08-2023 08:36:46	
svchost.exe	4544	UDPv6		::	4500	*		29-08-2023 07:05:11	IKEEXT
chrome.exe	15968	UDPv6		::	5353	*		29-08-2023 08:36:46	chrome.exe
svchost.exe	1772	UDPv6		::	5353	*		29-08-2023 08:36:37	Dnscache
chrome.exe	15968	UDPv6		::	5353	*		29-08-2023 08:36:46	chrome.exe

Endpoints: 122 Established: 15 Listening: 37 Time Wait: 10 Close Wait: 6 Update: 2 sec States: (All)

Monitor Hard Disk

DiskMon is an application that logs and displays all hard disk activity on a Windows system **STEPS**

Download DiskMon ❼ Run as Administrator

Disk Monitor - Sysinternals: www.sysinternals.com

File Edit Options Help

#	Time	Duration (s)	Disk	Request	Sector	Length
345	42.980874	0.00000000	1	Write	377607112	160
346	42.980944	0.00000000	1	Write	377481320	8
347	42.981136	0.00000000	1	Write	377481184	8
348	42.982512	0.00000000	0	Write	6104864	32
349	42.982624	0.00000000	0	Write	6102944	8
350	42.996067	0.00000000	0	Write	6102808	8
351	46.014710	0.00000000	1	Write	399863448	72
352	46.058413	0.00000000	1	Write	399589248	48
353	46.058442	0.00000000	1	Write	391426624	128
354	46.058714	0.00000000	1	Write	377481192	8
355	46.059206	0.00000000	1	Write	391426624	8
356	46.059389	0.00000000	1	Write	377481328	8
357	46.060474	0.00000000	1	Write	88806120	8
358	46.060509	0.00000000	1	Write	88806200	8
359	46.060598	0.00000000	1	Write	88806232	8
360	46.060707	0.00000000	1	Write	88806384	8
361	46.060842	0.00000000	1	Write	88806432	16
362	46.060890	0.00000000	1	Write	88806528	16
363	46.060918	0.00000000	1	Write	88806568	8
364	46.060950	0.00000000	1	Write	88806608	8
365	46.060986	0.00000000	1	Write	88806664	8
366	46.061018	0.00000000	1	Write	88806744	8
367	46.061050	0.00000000	1	Write	88806904	8
368	46.061078	0.00000000	1	Write	88806920	8
369	46.061110	0.00000000	1	Write	88807104	8
370	46.061142	0.00000000	1	Write	88807312	16
371	46.061171	0.00000000	1	Write	88807504	8
372	46.061203	0.00000000	1	Write	88807536	8
373	46.061232	0.00000000	1	Write	88807576	8
374	46.061264	0.00000000	1	Write	374822856	8
375	46.061312	0.00000000	1	Write	377481200	8
376	46.061651	0.00000000	1	Write	377481328	8
377	46.352349	0.00000000	1	Write	139327088	8
378	46.828643	0.00000000	1	Write	427564056	104
379	46.828838	0.00000000	1	Write	377481200	40
380	46.829600	0.00000000	1	Write	21384496	64
381	46.830454	0.00000000	1	Write	230977264	56
382	46.830467	0.00000000	1	Write	254829232	48
383	46.830592	0.00000000	1	Write	377481360	8

Monitor Virtual Memory

VMMap is a process virtual and physical memory analysis. It shows a breakdown of a process's committed virtual memory types as well as the amount of physical memory working set assigned by the operating system to those types.

STEPS

Sysinternal ❼ VMMap

Monitor Cache Memory

CacheSet is an applet that allows you to manipulate the working the set parameters of the system file cahce. Unlike CacheMan, CacheSet runs on all versions and will work without modifications on new Service Pack releases.

Give all the permissions and Click on Agree

Click on apply

After applying the changes

Cacheset - http://www.sysinternals.com
Cache Information
Current size
476128 KB
Peak size
534772 KB
Adjust Cache Settings
Working set minumum
1024
KB
Working set maximum
4194300
KB
Apply
Clear
Reset
Cancel
SysInternals

PRACTICAL NO. 6

Aim:

Recovering and Inspecting deleted files

- Check for Deleted Files
- Recover the Deleted Files
- Analyzing and Inspecting the recovered files
- Perform this using recovery option in ENCASE and also Perform manually through command line

In this Practical we are going to use the Autopsy, an application used to check, recover, analyze and inspect the deleted files using the Image evidence created

Open Autopsy and Click on New Case

Give a case name and browse the destination to save the autopsy file

Then give the case number and the details as per the case number when performing the FTK Imager Practical 1

Select on Disk Image or VM File and Click Next

Give the destination of the image and click next

Select the ingest module and click next

See the acknowledgement and click finish

Now we check the files recovered

We see the Deleted Files

Now We Extract/Recover some deleted files

Set a directory for the recovered files

Now we Generate a Report of the Autopsy done

Select a type to store the data and click next. Here we are going to generate the report in Excel.

Now select all results this will generate all the reports and click finish. The other option only generate the report for tagged one only.

Click on close and open the excel from the directory it is stored

	A	B
1	Summary	
2		
3	Case Name:	290723
4	Case Number:	290723
5	Examiner:	Maddy
6	Number of Images:	1

Summary | Tagged Files | Tagged Results

	A	B	C	D	E	F	G	H
1	Date Taken	Device Manufacturer	Device Model	Latitude	Longitude	Altitude	Source File	Tags
2	2022-06-10 18:10:21 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610181021.jpg	
3	2022-06-10 18:10:27 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610181027.jpg	
4	2022-06-10 18:10:30 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610181030.jpg	
5	2022-06-10 18:10:34 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610181034.jpg	
6	2022-06-10 18:23:26 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0000000.jpg	
7	2022-06-10 18:24:07 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0005120.jpg	
8	2022-06-10 18:24:13 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0012256.jpg	
9	2022-06-10 18:24:17 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0016320.jpg	
10	2022-06-10 18:24:37 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0020864.jpg	
11	2022-06-10 18:34:20 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610183420.jpg	
12	2022-06-10 18:34:25 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610183425.jpg	
13	2022-06-10 18:34:37 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610183437.jpg	
14	2022-06-10 18:34:53 IST	realme	realme 6				/img_04092023_masood.001/vol_vol2/IMG20220610183453.jpg	

	A	B	C	D	E	F
1	E-Mail To	E-Mail From	Subject	Date Sent	Date Received	Path
2	'5amspade@myway.com'	Jim Shu: Jim_shu@comcast.net	RE: Bike spec's	2006-12-04 07:39:00 IST	2006-12-04 07:39:00 IST	\\Top of Personal Folders\Sent Items
3	'5amspade@myway.com'	Jim Shu: Jim_shu@comcast.net	RE: Bike spec's	2006-12-04 07:39:00 IST	2006-12-04 07:39:00 IST	\\Top of Personal Folders\Sent Items
4	'5amspade@myway.com'	Jim Shu: Jim_shu@comcast.net	RE: Bike spec's	2006-12-04 08:37:00 IST	2006-12-04 08:37:00 IST	\\Top of Personal Folders\Deleted Items
5	'5amspade@myway.com'	Jim Shu: Jim_shu@comcast.net	RE: Bike spec's	2006-12-04 08:37:00 IST	2006-12-04 08:37:00 IST	\\Top of Personal Folders\Deleted Items
6	'baspen99@aol.com'	Jim Shu: Jim_shu@comcast.net	RE: Waiting	2006-12-07 07:51:00 IST	2006-12-07 07:51:00 IST	\\Top of Personal Folders\Sent Items
7	'baspen99@aol.com'	Jim Shu: Jim_shu@comcast.net	RE: Waiting	2006-12-07 07:51:00 IST	2006-12-07 07:51:00 IST	\\Top of Personal Folders\Sent Items
8	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Activate your account	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
9	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Activate your account	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
10	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:07:00 IST	2006-12-08 05:07:00 IST	\\Top of Personal Folders\Sent Items
11	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:07:00 IST	2006-12-08 05:07:00 IST	\\Top of Personal Folders\Sent Items
12	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
13	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
14	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
15	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
16	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:09:00 IST	2006-12-08 05:09:00 IST	\\Top of Personal Folders\Sent Items
17	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bicycle offer	2006-12-08 05:09:00 IST	2006-12-08 05:09:00 IST	\\Top of Personal Folders\Sent Items
18	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:07:00 IST	2006-12-08 05:07:00 IST	\\Top of Personal Folders\Sent Items
19	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:07:00 IST	2006-12-08 05:07:00 IST	\\Top of Personal Folders\Sent Items
20	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
21	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:08:00 IST	2006-12-08 05:08:00 IST	\\Top of Personal Folders\Sent Items
22	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:09:00 IST	2006-12-08 05:09:00 IST	\\Top of Personal Folders\Sent Items
23	'jim_shu1@yahoo.com'	Jim Shu: Jim_shu@comcast.net	FW: Bike spec's	2006-12-08 05:09:00 IST	2006-12-08 05:09:00 IST	\\Top of Personal Folders\Sent Items

	A	B	C
1	Email Addresses		
2	%@clients.l.google.com		
3	Preview	Source File	Tags
4	lients.l.google.com«%@clients.l.google.com«%hclients.l.google.	/img_04092023_masood.001/vol_vol2//$Unalloc/Unalloc_1878_3915776_1077723136	
5	lients.l.google.com«%@clients.l.google.com«%hclients.l.google.	/img_04092023_masood.001/vol_vol2/$OrphanFiles/_LLPLA~1.PCA	
6	lients.l.google.com«%@clients.l.google.com«%hclients.l.google.	/img_04092023_masood.001/vol_vol2/$OrphanFiles/_ROTEU~1.EXE	
7	lients.l.google.com«%@clients.l.google.com«%hclients.l.google.	/img_04092023_masood.001/vol_vol2/$OrphanFiles/aftnndbn.umd	
8			
9	-239034676-0-1001@flonetwork.com		
10	Preview	Source File	Tags
11	jjjz4znt«-239034676-0-1001@flonetwork.com«>[work.com>[4676-0	/img_04092023_masood.001/vol_vol2//$Unalloc/Unalloc_1878_3915776_1077723136	
12	jjjz4znt«-239034676-0-1001@flonetwork.com«>[work.com>[4676-0	/img_04092023_masood.001/vol_vol2/_S/Proteus 8.11 SP0 Pro HomeMade Electronics.exe	
13			
14	200612032123.609457386a225c@rly-xm04.mx.aol.com		
15	Preview	Source File	Tags
16	-0500in-reply-to: <«200612032123.609457386a225c@rly-xm04.mx.aol.com«>x-mb-message-sourc	/img_04092023_masood.001/vol_vol2//$Unalloc/Unalloc_1878_3915776_1077723136	
17	-0500in-reply-to: <«200612032123.609457386a225c@rly-xm04.mx.aol.com«>x-mb-message-sourc	/img_04092023_masood.001/vol_vol2/_S/Proteus 8.11 SP0 Pro HomeMade Electronics.exe	
18			
19	20061204013940.a88906765f@mprdmxin.myway.com		
20	Preview	Source File	Tags
21	etmail.comcast.net<«20061204013940.a88906765f@mprdmxin.myway.com«>mail.comcast.net000	/img_04092023_masood.001/vol_vol2//$Unalloc/Unalloc_1878_3915776_1077723136	
22	; 7bitmessage-id: <«20061204013940.a88906765f@mprdmxin.myway.com«>date: sun, 3 dec	/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0333408.pst	

Summary | EXIF Metadata | E-Mail Messages | Keyword Hits | Accounts_Email | Extension Misi ...

	A	B	C	D
1	Review Status	ID	Tags	
2	Undecided	5amspade@myway.com		
3	Undecided	5amspade@myway.com		
4	Undecided	baspen99@aol.com		
5	Undecided	baspen99@aol.com		
6	Undecided	jim_shu1@yahoo.com		
7	Undecided	jim_shu1@yahoo.com		
8	Undecided	jim_shu@comcast.net		
9	Undecided	jim_shu@comcast.net		
10	Undecided	martha.dax@superiorbicycles.biz		
11	Undecided	martha.dax@superiorbicycles.biz		
12	Undecided	terrysadler@goowy.com		
13	Undecided	terrysadler@goowy.com		
14				

A1 | File

	A	B	C	D
1	File	Extension	MIME Type	Path
2	AC19.gpj	gpj	image/jpeg	/img_04092023_masood.001/vol_vol2/$OrphanFiles/_IM_SH~1.PST/AC19.gpj
3	AC19.gpj	gpj	image/jpeg	/img_04092023_masood.001/vol_vol2//$CarvedFiles/f0333408.pst/AC19.gpj
4				
5				

PRACTICAL NO. 7

Aim:

Steganography Detection

- Detect hidden information or files within digital images using steganography analysis tools.
- Extract and examine the hidden content.

In this Practical we are going to use the **SteganPEG** to check the hidden files in the given

Image Create a folder to keep the image and message file and store the txt file and image Open the SteganPEG and give a password and browse the path of the image

First we are going to add some files in the captured image

Save the stegged image

Open the saved image with the assigned password and view the image with hidden files

Now we are going to do the <u>stegging process</u> using <u>Command Prompt</u> and <u>viewing</u> the Image using the <u>WinRAR</u>

Make a zip file of the text file

Go to **<u>Command Prompt</u>** and **<u>Type</u>** the **<u>Syntax</u>**

C:\Users\bmm\Desktop\New Folder>copy/b stegprac.jpg + stegpractxt.rar

Then create a shortcut for WinRAR on the desktop

Then open the image using the shortcut

Right Click on the image ❼ **Open with** ❼ **Choose another app**

Select **Choose another app** ❼ **choose an app on your pc**

Then **Desktop** ❼ **Shortcut created of WinRAR** and **Select Just Once**

View the Extracted File

PRACTICAL NO. 8

Aim:

Mobile Device Forensics

- Perform a forensic analysis of a mobile device, such as a smartphone or tablet.
- Retrieve call logs, text messages, and other relevant data for investigative purposes.

Practical:

In this Practical we are going to perform the mobile forensic using the MOBILedit Forensic toolkit

We are going to download the MOBILedit toolkit

Got to the link https://www.mobiledit.com/connection-kit

Then Click on **Online Store** then Scroll down to the Products

The Price is given below. It is around $1000

Then we go to the software

The price is given below. It starts from $99 to few Thousands of Dollars

Now we are going to start the Practical

Click on **connect** and **Select the type of forensic device** to work with. Here we are going with **<u>Phone</u>**

Click **Next** and **Select the type of Connection** with the **Mobile Phone.** Here we are going to Select **Cable Connection** and click Next

Click **Next** and let it **Scan the Device**, If ***Found*** click **Next**, If ***Not Found*** **Perform these steps and Retry** **"Go to Phone Settings and open Developer Option and Enable it, and then Allow USB Debugging"**

Then connect it with a connector for efficient data recovery

We got a device connected

This is the device we are going to use and click on next

Fill the details and browse a directory to store the logs

Then Click on Next then Select the **Acquisition** we want Here **we are going to acquire all the data from the device**

Click on Yes and Wait for the Acquisition to be completed

Open the **Case** and **Organize** and decide the **Format** in which we need the **Acquisition**

Fill in the details of the Investigator

Select the type of format to display the data. Here we are going to display it in Excel.

A Success Message will be Prompted

Now we are going to **view** and **analyze** the **data acquired** form the **Performed Acquisition**

We have performed of Two Mobile Devices The
First One is the Oppo Reno 2

Second One is the One+ 9

Display of the First Device Oppo Reno 2

Here we can see the Phonebook of the device

And here we can see the Call Logs

And here we can see the messages on the device

Display of the Second Device One+ 9

Here we can see the Files ❼Internal Storage ❼DCIM ❼ Camera

Here we can see the Files ❼Internal Storage ❼ Pictures

Now we are going to **Generate** and **Analyze** the **Report**

This is the **data.log** file we created before we started the **Acquisition**

PRACTICAL NO. 9

Aim:

Email Forensics

- Analyze email headers and content to trace the origin of suspicious emails.
- Identify potential email forgeries or tampering

Here we are going to use the AccessData FTK

FTK can filter or find files specific to e-mail clients and servers.
You can configure these filters when you enter search parameters.
Because of Jim's responses to a poor performance review, the CEO of Superior Bicycles,Martha Dax, suspects he might have obtained sensitive information about the company's business model that he's leaking to a competitor.
Martha asked her CIO, to have an IT employee copy the Outlook .pst file from Jim Shu's old computer to a USB drive.
To process this investigation, we need to examine the Jim_shu's.pst file, locate the message, and export it for further analysis of its header to see how Jim might have received it.

Recovering Email

Start **AccessData FTK** and click **Start a new case**, then click **OK**.

Click **Next** until you reach the **Refine Case** - **Default dialog box** Click the **Email Emphasis button**, and then click **Next**

Create a new File

Fill the details of the Examiner

Click on all the options and Click Next

Select all the options

Now we have reached the Email Emphasis section

Click Next until you reach the **Add Evidence** to **Case dialog box**, and then click the **Add Evidence button**. In the **Add Evidence** to **Case dialog box**, click the **Individual File option button**, and then click **Continue**.

In the Select **File dialog box**, **navigate to your work folder**, click the **Jim_shu's.pst file**, and then click **Open**.

Give some data

Complete the steps and Click on Next

Click on finish and see the data

When the Add Evidence to Case dialog box opens, click Next. In the Case summary dialog box, click Finish. When FTK finishes processing the file, in the main FTK window, click the Email Messages button, and then click the Full Path column header to sort the records.

For email recovery follow following steps: Click the E-Mail tab. In the tree view, click to expand all folders, and then click the Deleted Items folder.

Select any message say Message0001 right click and select option Launch Detached Viewer and you can see detail of deleted message.

For analyzing header follow following steps: Click the E-Mail tab. In the tree view, click to expand all folders, and then click the Inbox folder. In the File List pane at the upper right, click Message0003; as shown in the pane at the bottom, it's from Sam and is addressed to Jim_shu@comcast.net.

Right-click on any message say Message0003 in the File List pane and click Export File. In the Export Files dialog box, click OK.

FTK saves exported files in the HTML format with no extension.

Right-click the Message0003 file and click Rename. Type Message0003.html and press Enter

Double-click Message0003.html to view it in a Web browser.

Conversation Topic: Bike spec's Sender Name: Sam Received By: Jim Shu Delivery Time: 04-12-2006 07:44:02 Creation Time: 04-12-2006 07:46:48 Modification Time: 08-12-2006 05:09:12 Submit Time: 04-12-2006 07:44:14 Flags: 1 = Read Size: 6456 Received: from myway.com (nn1.excitenetwork.com[207.159.120.55](untrusted sender)) by alnrmxc23.comcast.net (alnrmxc23) with ESMTP id <20061204021402a2300j90t3e>; Mon, 4 Dec 2006 02:14:02 +0000 X-Originating-IP: [207.159.120.55] Received: by mprdmxin.myway.com (Postfix, from userid 110) id 63B6067669; Sun, 3 Dec 2006 21:14:14 -0500 (EST) To: Jim_shu@comcast.net Subject: RE: Bike spec's Received: from [24.18.24.250] by mprdmailfe3.nwk.myway.com via HTTP; Sun, 03 Dec 2006 21:14:14 EST X-AntiAbuse: This header was added to track abuse, please include it with any abuse report X-AntiAbuse: ID = f869dfbea97fe07b9eab2f865d19b540 Reply-to: 5amspade@myway.com From: "Sam"<5amspade@myway.com> MIME-Version: 1.0 X-Sender: 5amspade@myway.com X-Mailer: PHP Content-Type: text/plain; charset="US-ASCII" Content-Transfer-Encoding: 7bit Message-Id: <20061204021414.63B6067669@mprdmxin.myway.com> Date: Sun, 3 Dec 2006 21:14:14 -0500 (EST) We might be able to go $4000 if it is good. Is it? Sam --- On Sun 12/03, Jim Shu < Jim_shu@comcast.net > wrote: From: Jim Shu [mailto: Jim_shu@comcast.net] To: 5amspade@myway.com Date: Sun, 3 Dec 2006 18:09:06 -0800 Subject: RE: Bike spec's How much are you willing to pay me to get these plans to you?Jim-----Original Message-----From: Sam [mailto:5amspade@myway.com] Sent: Sunday, December 03, 2006 5:40 PMTo: jim_shu@comcast.netSubject: Bike spec'sDo you have them yet?I've got people in Asia ready to duplicate them?Sam_____No banners. No pop-ups. No kidding.Make My Way your home on the Web - http://www.myway.com _____ No banners. No pop-ups. No kidding. Make My Way your home on the Web - http://www.myway.com

PRACTICAL NO. 10

Aim:

Web Browser Forensics

- Analyze browser artifacts, including history files, bookmarks, and download records.
- Analyze cache and cookies data to reconstruct user-browsing history and identify visited websites or online activities.
- Extract the relevant log or timestamp file, analyze its contents and interpret the timestamp data to determine the user's last internet activity and associated details.

We are going to use the **Browser History Examiner** Run it as Administrator..

It is a **Paid Software** but has a **free–trail to get a total of 25 records from all the browsers in the device**

Click on Continue Trail

Click OK

This is the Interface of the

Application Go to File ❼ Capture

History

We are going to capture from this device only Select on that and click Next

Select the Browser we want the history and give a directory to save those history extracted files

Here we can see the websites visited

Here we can see the bookmarks

Here we can see the browser settings

Here we can see the cached files

Here we can see the cached images

Here we can the cached webpages

Here we can see the cookies stored

Here we can see the emails used for logins

Here we can see the favicons

Here we can see the searches

Here we see the thumbnails

Here we can see the websites visits