



Digital Forensics(7906ICT)

Major Assignment

Nihar Vyas
s5317069

Master Of Cyber Security

Task-1

Evidence A – A disk image of an old laptop computer found in an abandoned car near the airport.

1. Who is the owner of the laptop?

➔ Disc image analysis showed that, based on user account information and the majority of log-in counts, Peter is the owner of the laptop.

Command: `rip.pl -r /mnt/windows_mount/WINDOWS/system32/config/software -p winver`

```
copyright 2020 Quantum Analytics Research, LLC
sansforensics@siftworkstation: /cases
$ rip.pl -r /mnt/windows_mount/WINDOWS/system32/config/software -p winver
Launching winver v.20200525
winver v.20200525
(Software) Get Windows version & build info

ProductName           Microsoft Windows XP
CSDVersion             Service Pack 3
BuildLab               2600.xpsp.080413-2111
RegisteredOrganization
RegisteredOwner        Peter
InstallDate            2023-08-20 05:56:08Z
```

2. What programs have been installed on the laptop? What recent programs have been run?

➔ This is a list of the installed programmes together with the date of their most recent run. Which are:

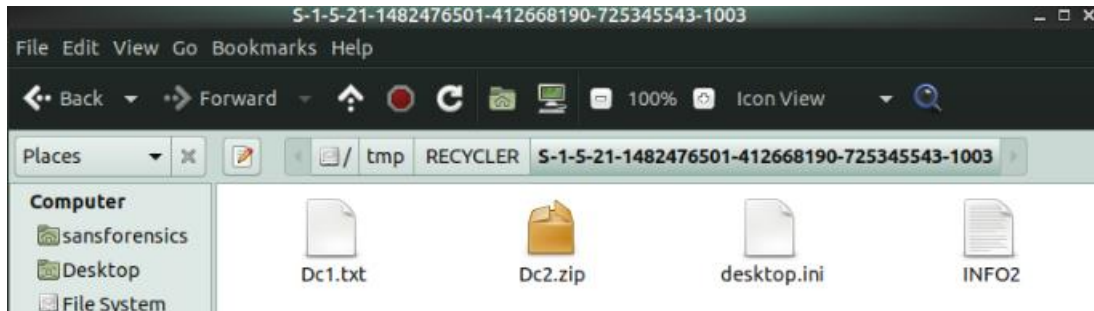
- 7-zip
- Messenger
- VMware
- Adobe
- Netmining
- IrfanView
- MSN
- VideoLAN

Command: `[ls -l]` is performed once we change the directory to `/windows_mount/Program Files`

```
sansforensics@siftworkstation: /mnt/windows_mount/Program Files
$ ls -l
total 88
drwxrwxrwx 1 root root 4096 Aug 20 06:32 7-Zip
drwxrwxrwx 1 root root  0 Aug 20 06:33 Adobe
drwxrwxrwx 1 root root 4096 Aug 20 06:33 'Common Files'
drwxrwxrwx 1 root root  0 Aug 20 05:54 'ComPlus Applications'
drwxrwxrwx 1 root root 4096 Aug 20 05:55 'Internet Explorer'
drwxrwxrwx 1 root root 4096 Aug 20 06:34 IrfanView
drwxrwxrwx 1 root root 4096 Aug 20 05:54 Messenger
drwxrwxrwx 1 root root  0 Aug 20 05:55 'microsoft frontpage'
drwxrwxrwx 1 root root 4096 Aug 20 05:54 'Movie Maker'
drwxrwxrwx 1 root root 4096 Aug 20 06:37 'Mozilla Firefox'
drwxrwxrwx 1 root root 4096 Aug 20 06:37 'Mozilla Maintenance Service'
drwxrwxrwx 1 root root  0 Aug 20 05:54 MSN
drwxrwxrwx 1 root root  0 Aug 20 05:54 'MSN Gaming Zone'
drwxrwxrwx 1 root root 4096 Aug 20 05:54 NetMeeting
drwxrwxrwx 1 root root 4096 Aug 20 05:54 'Online Services'
drwxrwxrwx 1 root root 4096 Aug 20 05:54 'Outlook Express'
drwxrwxrwx 1 root root  0 Aug 20 05:57 'Uninstall Information'
drwxrwxrwx 1 root root  0 Aug 20 06:36 VideoLAN
drwxrwxrwx 1 root root  0 Aug 20 05:58 VMware
drwxrwxrwx 1 root root 4096 Aug 20 05:55 'Windows Media Player'
drwxrwxrwx 1 root root 4096 Aug 20 05:54 'Windows NT'
drwxrwxrwx 1 root root  0 Aug 20 05:54 WindowsUpdate
drwxrwxrwx 1 root root  0 Aug 20 05:55 xerox
```

3. Recover any files in the recycle bin.
➔ There are 4 files which have been recovered from the recycle bin.

```
sansforensics@siftworkstation: /cases/7906ICT-EvidenceA
$ ts_k_recover -e -b 512 -o 56 7906ICT-EvidenceA.dd /tmp/
Files Recovered: 12202
```



4. Is there evidence that the owner of the laptop has committed a crime?

- ➔ No, there isn't any concrete proof that Peter, the owner of the laptop, has done anything illegal, but based on my review of the material, he is definitely a primary suspect because the device has some traceable information about the kidnapping.

Evidence B – Network capture of a suspected criminal gang hideout.

5. Who are the people communicating in the transmission? When does the first transmission begin and the last transmission finish?

- Marko, Birdie, Ahmed, Gregor, and Raman are the individuals who are in communication during the transmission.

- ➔ The communication began at 21-08-2023 07:30 and the last message was at 21-08-2023 07:39.

```

0.3.~.=...3. KA.YYc...3.E+..w+...3.y.oIK.....w...Z#.....w...%./y.;...42["msg",{"chan":1,"msg":{"ty
pe":"error","text":"Ali: Nickname is already in use.", "showInactive":true,"from":{"id":15,"previews":[]},"self":false,"time":"2023-08-
21T07:25:31.282Z"}}].M42["nick",{"network":"acefd45-06e8-48bb-ac23-271428653207","nick":"Birdie"}]...F..F..3..y6..K4..3.....3
...u..3..D..+v...3..1z5..z..3..u...".3.....3..i..[.....3.....?.....3..r.DmP...+N=1...~.42["msg",{"chan":1,"msg":{"text
":"You're now known as Ahmed","from":{"id":16,"previews":[]},"type":"message","self":false,"time":"2023-08-21T07:29:26.362Z"}}].L42["n
ick",{"network":"acefd45-06e8-48bb-ac23-271428653207","nick":"Ahmed"}]...[P..IR...3..RG...E...3..AA...3.....8.5..8...3..A4..sw3..3..b.
...P...3..E...3..6...u...3..c...3..8...H...$3...~.42["msg",{"chan":1,"msg":{"type":"error","text":"Messages can not
be sent to lobbies.", "from":{"id":17,"previews":[]},"self":false,"time":"2023-08-21T07:33:15.540Z"}}].AB.os@...3.....3.....
$.0...6...%..(y.Y...P.#...~.42["join",{"network":"acefd45-06e8-48bb-ac23-271428653207","chan":{"name":"#RuedParadis2","state":1,
"id":2,"messages":{"totalMessages":0,"key":"","topic":"","type":"channel","firstUnread":0,"unread":0,"highlight":0,"users":[]},"index
":1}]}~.42["msg",{"chan":2,"msg":{"from":{"mode":"","nick":"Ahmed"},"time":"2023-08-21T07:34:02.083Z","hostname":"Birdie@127.0.0.1",
"type":"join","self":true,"id":18,"previews":[],"text":"","id":18}]]..42["users",{"chan":2}]]..42["users",{"chan":2}]]..w...u...?@;$.%...42["open
",{"B~.%1.....M<.h<.x...R...J42["names",{"id":2,"users":[{"nick":"Ahmed","mode":"@","lastMessage":0}]]..J42["names",
{"id":2,"users":[{"nick":"Ahmed","mode":"@","lastMessage":0}]]..J42["names",{"id":2,"users":[{"nick":"Ahmed","mode":"@","lastMessage":
0}]]...~.42["msg",{"chan":2,"msg":{"type":"message","text":"nt", "from":{"id":19,"previews":[]},"self":false,"time":"2023-08-21T
07:34:03.085Z"}}]...~.42["msg",{"chan":2,"msg":{"from":{"mode":"","nick":"Raman"},"time":"2023-08-21T07:34:19.574Z","hostname":"user4@12
7.0.0.1","type":"join","self":false,"id":20,"previews":[]},"text":"","id":20}]]..42["users",{"chan":2}]]...4.P$.P.u42["names",{"id":2,"users":[]
{"nick":"Ahmed","mode":"@","lastMessage":0},"nick":"Raman","mode":"","lastMessage":0}]]...T...~.3...
.....~.42["msg",{"chan":2,"msg":{"from":{"mode":"","nick":"Ahmed"},"type":"message","time":"2023-08-21T07:34:34.413Z","text":
"Get Marko","self":true,"highlight":false,"users":[]},"id":21,"previews":[]}}]...~.42["msg",{"chan":2,"msg":{"from":{"mode":"","nick":"Ram
an"},"type":"message","time":"2023-08-21T07:34:45.981Z","text":"What...s the matter?","self":false,"highlight":false,"users":[]},"id":22
,"previews":[]}}]...v

```

6. What browsers, operating systems, and IP addresses are used by the communication endpoints?

- ➔ The picture below displays the IP address used, the operating system (Ubuntu Linux), and the browser that was used:

➔ Upon observing the dialogue, I may conclude that each participant is a member of the same criminal organisation.

[illegible]

Evidence C – A memory dump of a personal laptop.

9. What applications are running on the memory dump computer?

➔ The list of programmes that are open on the memory dump machine is provided below.

- Firefox
- Thunderbird
- Mynotepad++
- ResouceHacker
- Etc.

Command: vol.py -f 7906ICT-Evidence.vmem --profile=Win7SP1x64 pslist

samforensics\fwk\Taskstation:									
Volatility Framework 2.6.1									
File	FPID	Thds	Hnds	Sess	Mow64	Start	Exit		
\\.\ffffffffff3b0b35f0	System	4	0	92	556	-----	2023-08-21 13:05:34 UTC+0000		
\\.\ffffffffff32b2c93f	smss.exe	264	4	2	299	-----	2023-08-21 13:05:34 UTC+0000		
\\.\ffffffffff32b2c83f70	csrss.exe	352	340	9	470	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	csrss.exe	404	348	74	480	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff80d4e445d0	csrss.exe	412	396	11	452	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	csrss.exe	468	396	3	111	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	services.exe	584	604	0	0	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	lsass.exe	512	604	0	722	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	lsass.exe	508	604	0	722	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	524	604	10	157	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	692	604	7	297	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	744	604	2	254	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	852	604	27	590	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	904	584	36	981	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	944	584	14	84	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	988	584	19	759	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	1036	584	17	383	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	1148	584	11	87	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	explorer.exe	1152	1132	25	712	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	explorer.exe	1252	1152	2	39	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	cmd.exe	1260	1152	7	39	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	spoolsv.exe	1384	104	13	270	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	spoolsv.exe	1384	104	0	0	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	1380	104	18	315	-----	2023-08-21 13:05:35 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	1640	584	3	84	-----	2023-08-21 13:05:37 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	1648	584	11	272	-----	2023-08-21 13:05:37 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	2020	624	9	196	-----	2023-08-21 13:05:37 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	2268	584	13	189	-----	2023-08-21 13:05:37 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	2476	584	14	149	-----	2023-08-21 13:05:37 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	2484	584	11	583	-----	2023-08-21 13:05:42 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	2632	584	13	414	-----	2023-08-21 13:05:42 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	2584	584	0	0	-----	2023-08-21 13:05:42 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	2856	624	9	220	-----	2023-08-21 13:05:43 UTC+0000		
\\.\ffffffffff32b2c83f70	svchost.exe	2976	584	9	355	-----	2023-08-21 13:05:4		

10. What web pages has the memory dump computer visited recently?

➔ This proof includes two different web browsers: Firefox and Internet Explorer. Nevertheless, I was able to use the command below to get the history of the Firefox web page; unfortunately, Internet Explorer was not included in the results of the IEHISTORY function.

➔ Search history is listed below:

- Taken mills
- Paris
- Rue du Paradis
- Missing persons
- Protect your privacy and browse faster with Firefox features.

Command: vol.py -f 7906ICT-EvidenceC.vmem --profile=Win75P1X64 firefoxhistory

UserPerformanceFrameworkStatistics:											
5 volpy -f PMHICT-EvidenceC:\vmen -profile=Win7P3id64 firefohistory											
Volatility Foundation Volatility Framework 2.6.1											
100											
Item	Type	Favicon	ID	Frequency	Last Visit	Date	GUID	Foreign Count	Title	Rev Host	Visits
17	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:16:39.728000	hrefCJfVw4d	0	taken mills - Google Search	mc.elgogw.www.	1
16	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:16:39.728000	hrefCJfVw4d	0	paris - Google Search	mc.elgogw.www.	1
15	https://www.croodapardis.com/en/		0	0	100	2023-08-21 13:16:32.727900	838u5l_2w_1	0	Rue du Paradis	mc.elgogw.ltdr.apoder.www.	1
14	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:16:32.955000	t_eG6WpLXxk	0		mc.elgogw.www.	1
13	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:16:32.356000	8F1v4v2Cz7B9	0	rue du paradis - Google Search	mc.elgogw.www.	1
12	https://www.google.com/search?q=missing-persons&rlz=C360007f-8		0	0	100	2023-08-21 13:16:55.375000	8e_v1808Cvjd	0	missing persons - Google Search	mc.elgogw.www.	1
11	https://www.mozilla.org/en-US/firefox/45.0.1/firstrun/		0	0	100	2023-08-21 13:18:05.836000	CaLCP3o50F	0	Protect your privacy and browse faster with Firefox features	gro.allizon.www.	1
10	https://www.mozilla.org/en-US/firefox/45.0.1/firstrun/		0	0	100	2023-08-21 13:18:05.836000	CaLCP3o50F	0	Welcome to Firefox	gro.allizon.www.	1
9	https://www.mozilla.org/en-US/firefox/45.0.1/firstrun/		0	0	100	2023-08-21 13:18:05.836000	CaLCP3o50F	0		gro.allizon.www.	1
8	place:folder-80000&ns=MozillaFolder-4M1-128&ns=MozillaFolder-4M1-128&ns=MozillaFolder-4M1-128&ns=MozillaFolder-4M1-128		0	0	100	2023-08-21 13:18:05.836000	CaLCP3o50F	0		gro.allizon.www.	1
7	place:sort-80000&ns=MozillaFolder-4M1-128&ns=MozillaFolder-4M1-128&ns=MozillaFolder-4M1-128&ns=MozillaFolder-4M1-128		0	0	100	2023-08-21 13:18:05.836000	CaLCP3o50F	0		gro.allizon.www.	1
6	https://www.mozilla.org/en-US/about/		0	0	100	2023-08-21 13:18:05.836000	CaLCP3o50F	0		gro.allizon.www.	1
5	https://www.mozilla.org/en-US/about/		0	0	100	2023-08-21 13:18:05.836000	CaLCP3o50F	0		gro.allizon.www.	1
4	https://www.mozilla.org/en-US/about/		0	0	100	2023-08-21 13:18:05.836000	CaLCP3o50F	0		gro.allizon.www.	1
3	https://www.mozilla.org/en-US/about/		0	0	100	2023-08-21 13:18:05.836000	CaLCP3o50F	0		gro.allizon.www.	1
2	https://www.mozilla.org/en-US/about/		0	0	100	2023-08-21 13:18:05.836000	CaLCP3o50F	0		gro.allizon.www.	1
1	https://www.mozilla.org/en-US/about/		0	0	100	2023-08-21 13:18:05.836000	CaLCP3o50F	0		gro.allizon.www.	1
17	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0	taken mills - Google Search	mc.elgogw.www.	1
16	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0		mc.elgogw.www.	1
15	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0		mc.elgogw.www.	1
14	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0		mc.elgogw.www.	1
13	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0		mc.elgogw.www.	1
12	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0		mc.elgogw.www.	1
11	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0		mc.elgogw.www.	1
10	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0		mc.elgogw.www.	1
9	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0		mc.elgogw.www.	1
8	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0		mc.elgogw.www.	1
7	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0		mc.elgogw.www.	1
6	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0		mc.elgogw.www.	1
5	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0		mc.elgogw.www.	1
4	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0		mc.elgogw.www.	1
3	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0		mc.elgogw.www.	1
2	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0		mc.elgogw.www.	1
1	https://www.google.com/search?q=takenmills&rlz=C360007f-8		0	0	100	2023-08-21 13:18:19.728000	hrefCJfVw4d	0		mc.elgogw.www.	1

11. What is email address of the owner of the memory dump computer and are they connected to the case?

➔ The memory dump, which belongs to Patrice Saint-Clair (owner), has the email address cm363478@gmail.com.

```
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\saint-clair\AppData\Roaming
CommonProgramFiles=C:\Program Files (x86)\Co
nProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=WIN
Spec=C:\Windows\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\Users\saint-clair
LOCALAPPDATA=C:\Users\sain
Local
LOGONSERVER=\\WIN-OI7C6DKJET9
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\Windows\system32;C:\Windows;C:\Windows\
vPROCESSOR_ARCHIT
q=Intel64 Family 6 Model 158 Stepping 10, GenuineIntel
PROCESSOR_LEVEL=6
PROC
C:\Users\SAINT~1\AppData\Local\Temp
TMP=C:\Users\SAINT~1\AppData\Local\Temp
USERDOMAIN=WIN-OI7C6DKJET9
USERNAME=saint-
E=C:\Users\saint-clair
windir=C:\Windows
windows_tracing_flags=3
windows_tracing_logfile=C:\BVTBin\Tests\installpackage\
205#
```

```
user_pref("mail.server.server1.userName", "cm363478@gmail.com");
user_pref("mail.smtpserver.smtp1.username", "cm363478@gmail.com");
3478@gmail.com
```

12. What is password of the memory dump computer?

Ans: TheGodfather is the password of the Patrice Saint-Clair's laptop.

Code: vol.py -f 7906ICT-EvidenceC.vmem --profile=Win7SP1x64 lsadump

```
sansforensics@siftworkstation: /cases/7906ICT-EvidenceC
$ vol.py -f 7906ICT-EvidenceC.vmem --profile=Win7SP1x64 lsadump
Volatility Foundation Volatility Framework 2.6.1
DefaultPassword
0x00000000 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000010 54 00 68 00 65 00 47 00 6f 00 64 00 66 00 61 00 T.h.e.G.o.d.f.a.
0x00000020 74 00 68 00 65 00 72 00 00 00 00 00 00 00 00 00 t.h.e.r.....

DPAPI_SYSTEM
0x00000000 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0x00000010 01 00 00 00 d4 65 ec 0e 46 23 52 6e f3 fc a5 39 .....e..F#Rn...9
0x00000020 cd 41 35 85 7a b5 b1 30 43 03 3e 32 93 e3 44 76 .A5.z..0C.>2..Dv
0x00000030 07 a6 d7 1c 19 f2 17 94 64 e9 2d ad 00 00 00 00 .....d.-.....

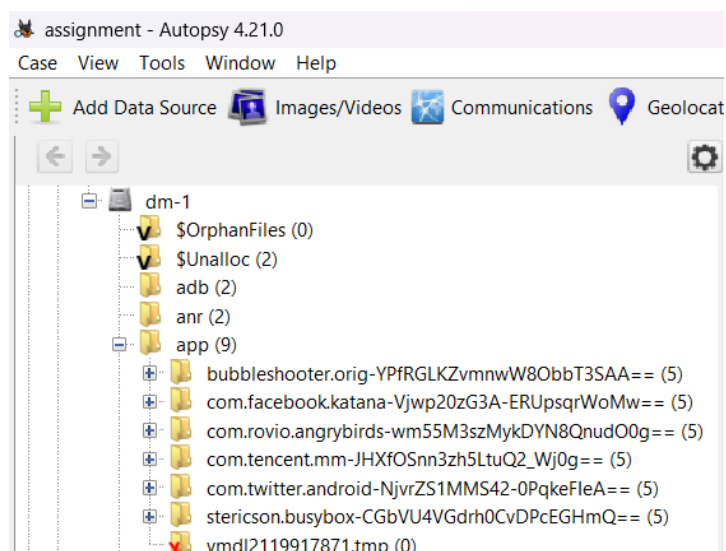
sansforensics@siftworkstation: /cases/7906ICT-EvidenceC
$
```

Evidence D – A disk image of a damaged mobile phone found in the daughter's hotel apartment.

13. What are the non-stock applications installed on the phone?

➔ Following an analysis of the evidence, the non-stock uses are:




- Bubblesooter
- Angrybirds
- Tencent
- Twitter
- Busybox



```
root@siftworkstation:/mnt/e01/system# cd app
root@siftworkstation:/mnt/e01/system/app# ls
BasicDreams          CtsShimPrebuilt      LicenseChecker        SecureElement
Bluetooth            Drive                 LiveWallpapersPicker  SimAppDialog
BluetoothMidiService EasterEgg              Maps                  Traceur
BookmarkProvider     ExactCalculator       Music2                 Videos
Browser2             GoogleContactsSyncAdapter NexusWallpapersStubPrebuilt WallpaperBackup
BuiltInPrintService  GoogleExtShared       NFCNci                 WallpapersBReel
CalendarGooglePrebuilt GoogleHindiIME         PacProcessor           WallpapersUsTwo
Camera2              GooglePinyinIME       PartnerBookmarksProvider WAPPushManager
CaptivePortalLogin   GooglePrintRecommendationService Photos                 WebViewStub
CarrierDefaultApp    GoogleTTS              PrebuiltBugle          YouTube
CertInstaller        HTMLViewer            PrebuiltDeskClockGoogle
Chrome               KeyChain              PrebuiltGmail
CompanionDeviceManager LatinIMEGooglePrebuilt PrintSpooler
root@siftworkstation:/mnt/e01/system/app#
```

14. Who is in the contacts list? What messages and calls have been sent and received by the phone?

➔ The phone has multiple messages and just three contacts (see images below):

Table	Thumbnail	Summary					
Source Name	S	C	O	Name	Phone Number	Email	Data Source
 contacts2.db			1	Amanda Goldman	1 834-524-325	sr8640171@gmail.com	dm-1
 contacts2.db			1	Dad	1 802-342-233		dm-1
 contacts2.db			0	Mum	1 845-345-343		dm-1

A	B	C	D	E	F	G	H	I	J
Source Na	Message T	Date/Time	Read	Direction	From Phone Number	To Phone Number	Text	Thread ID	Data Sourc
mmssms.d Android M 2023-08-2	1	Outgoing			27fc813e-3d84-4bf2-9554-a7	1834524325	What are your cousins names?	7ff7568f-077b-45a3-83fc-< dm-1	
mmssms.d Android M 2023-08-2	1	Incoming			1834524325	27fc813e-3d84-4bf2-9554-a7	Beth and Bronte. Why do you ask?	7ff7568f-077b-45a3-83fc-< dm-1	
							I had to tell Dad that we were going to Paris with your cousins before he would		
mmssms.d Android M 2023-08-2	1	Outgoing			27fc813e-3d84-4bf2-9554-a7	1834524325	sign the permission form.	7ff7568f-077b-45a3-83fc-< dm-1	
mmssms.d Android M 2023-08-2	1	Incoming			1834524325	27fc813e-3d84-4bf2-9554-a7	How uncool.	7ff7568f-077b-45a3-83fc-< dm-1	
mmssms.d Android M 2023-08-2	1	Outgoing			27fc813e-3d84-4bf2-9554-a7	1834524325	He signed it! He signed it! We are going!!!!!!	7ff7568f-077b-45a3-83fc-< dm-1	
mmssms.d Android M 2023-08-2	1	Outgoing			27fc813e-3d84-4bf2-9554-a7	1802342233	Hey Dad, made it to Paris	7ff7568f-077b-45a3-83fc-< dm-1	
mmssms.d Android M 2023-08-2	1	Incoming			1802342233	27fc813e-3d84-4bf2-9554-a7	You be careful honey. Let me know when you get to the apartment.	7ff7568f-077b-45a3-83fc-< dm-1	
mmssms.d Android M 2023-08-2	1	Incoming			1802342233	27fc813e-3d84-4bf2-9554-a7	I rang before and you didn't answer	7ff7568f-077b-45a3-83fc-< dm-1	
							Donâ€™t worry. The people here are so friendly. We met a guy Peter who is going		
mmssms.d Android M 2023-08-2	1	Outgoing			27fc813e-3d84-4bf2-9554-a7	1802342233	to give us a lift.	7ff7568f-077b-45a3-83fc-< dm-1	
mmssms.d Android M 2023-08-2	1	Outgoing			27fc813e-3d84-4bf2-9554-a7	1802342233	Dad there's someone here.	7ff7568f-077b-45a3-83fc-< dm-1	
mmssms.d Android M 2023-08-2	1	Incoming			1802342233	27fc813e-3d84-4bf2-9554-a7	The cousins are back?	7ff7568f-077b-45a3-83fc-< dm-1	
mmssms.d Android M 2023-08-2	1	Outgoing			27fc813e-3d84-4bf2-9554-a7	1802342233	No. Dad, they're coming. They have Amanda.	7ff7568f-077b-45a3-83fc-< dm-1	
mmssms.d Android M 2023-08-2	1	Incoming			1802342233	27fc813e-3d84-4bf2-9554-a7	How many people are there?	7ff7568f-077b-45a3-83fc-< dm-1	
mmssms.d Android M 2023-08-2	1	Outgoing			27fc813e-3d84-4bf2-9554-a7	1802342233	Three, four. I don't know.	7ff7568f-077b-45a3-83fc-< dm-1	
							Go to the next bedroom. Get under the bed. Now, the next part is very important.		
mmssms.d Android M 2023-08-2	1	Incoming			1802342233	27fc813e-3d84-4bf2-9554-a7	They are going to take you. Shout out everything you see about them. Hair color,	7ff7568f-077b-45a3-83fc-< dm-1	
mmssms.d Android M 2023-08-2	1	Outgoing			27fc813e-3d84-4bf2-9554-a7	1802342233	They're there. I can hear them.	7ff7568f-077b-45a3-83fc-< dm-1	
mmssms.d Android M 2023-08-2	1	Incoming			1802342233	27fc813e-3d84-4bf2-9554-a7	Put the phone closer so I can hear.	7ff7568f-077b-45a3-83fc-< dm-1	
mmssms.d Android M 2023-08-2	1	Outgoing			27fc813e-3d84-4bf2-9554-a7	1802342233	They're leaving. I think they're...Beard. Six feet. Tattoo right hand, moon and star.	7ff7568f-077b-45a3-83fc-< dm-1	

15. What Internet searches has the owner of the phone made?

➔ I have history file containing the history of Chrome browser (data/com.android.chrome/app_chrome/Default/History) from the damaged phone, the visited websites are shown below:

libgeswapers-jni.so	DistanceImage Positioning «History» MaskImage RowL... /img_vda1/system/lib/libgeswapers-jni.so	2020-08-05 11:06:52 AEST	2020-08-05 11:06:52 AEST
History	«History» /img_vda1/data/com.android.chrome/app_chrome/De...	2023-08-20 14:27:12 AEST	2023-08-20 14:27:12 AEST
NOTICE.xml	documentation, and revision «History» Some improvem... /img_vda1/etc/NOTICE.xml.gz/NOTICE.xml	0000-00-00 00:00:00	0000-00-00 00:00:00
History-journal	«History»-journal /img_vda1/data/com.android.chrome/app_chrome/De...	2023-08-20 15:13:34 AEST	2023-08-20 15:13:34 AEST
History-journal-slack	«History»-journal-slack /img_vda1/data/com.android.chrome/app_chrome/De...	2023-08-20 15:13:34 AEST	2023-08-20 15:13:34 AEST
sh	storysearch-«History»-downsearch-«History»-upset-arg... /img_vda1/system/bin/sh	2020-08-05 11:06:16 AEST	2020-08-05 11:06:16 AEST
Telecom.apk	your contacts and call «History» when connectedPairing /img_vda1/system/priv-app/Telecom/Telecom.apk	2020-08-05 11:13:04 AEST	2020-08-05 11:13:04 AEST

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Table «Hex» 9 entries Page 1 of 1 Export to CSV									
id	url	title	visit_count	typed_co...	last_v...				
1	https://www.google.com/search?q=Paris&oeq=Paris&oeq=chrome.6957/03.12050/7&client=	Paris - Google Search	3	0	1333				
2	https://www.google.com/url?r=https://en.m.wikipedia.org/wiki/Paris&oeq=U0ved=2&hJKEwJl Paris - Wikipedia	Paris - Wikipedia	1	0	1333				
3	https://en.m.wikipedia.org/wiki/Paris	Paris - Wikipedia	1	0	1333				
4	https://www.google.com/search/client=ms-unknown&oeq=ss=558490629&oeq=u2+tour&oeq=u2+tour - Google Search	U2 + Tour - Google Search	2	0	1333				
5	https://www.google.com/url?r=https://www.u2.com/tour/boa+U0ved=2&hJKEwJlYuaA... U2 + Tour	U2 + Tour	1	0	1333				
6	https://www.u2.com/tour/	U2 + Tour	1	0	1333				
7	https://www.google.com/search/client=ms-unknown&oeq=ss=558490629&oeq=Paris+metro... Paris metro - Google Search	Paris metro - Google Search	1	0	1333				
8	https://www.google.com/url?r=https://www.ratp.fr/en/plan-metro&oeq=U0ved=2&hJKEwJlR3 Metro map of Paris and the Île-de-France region RATP	Metro map of Paris and the Île-de-France region RATP	1	0	1333				
9	https://www.ratp.fr/en/plan-metro	Metro map of Paris and the Île-de-France region RATP	1	0	1333				

16. Is there other evidence on the phone that might indicate the role of the owner in the daughter's disappearance?

➔ No, there isn't any evidence that sheds any light on the disappearance. The study suggests that the daughter's phone may be the cause of the absence, so there aren't any more details or connections to the case.

Source Na	Message T	Date/Time Read	Direction	From Phone Number	To Phone Number	Text
mmssms.d Android M	2023-08-2		1 Outgoing	27fc813e-3d84-4bf2-9554-a7	1834524325	What are your cousins names?
mmssms.d Android M	2023-08-2		1 Incoming	1834524325	27fc813e-3d84-4bf2-9554-a7	Beth and Bronte. Why do you ask?
mmssms.d Android M	2023-08-2		1 Outgoing	27fc813e-3d84-4bf2-9554-a7	1834524325	I had to tell Dad that we were going to Paris with your cousins before he would sign the permission form.
mmssms.d Android M	2023-08-2		1 Incoming	1834524325	27fc813e-3d84-4bf2-9554-a7	How uncool.
mmssms.d Android M	2023-08-2		1 Outgoing	27fc813e-3d84-4bf2-9554-a7	1834524325	He signed it! He signed it! We are going!!!!!!
mmssms.d Android M	2023-08-2		1 Outgoing	27fc813e-3d84-4bf2-9554-a7	1802342233	Hey Dad, made it to Paris
mmssms.d Android M	2023-08-2		1 Incoming	1802342233	27fc813e-3d84-4bf2-9554-a7	You be careful honey. Let me know when you get to the apartment.
mmssms.d Android M	2023-08-2		1 Incoming	1802342233	27fc813e-3d84-4bf2-9554-a7	I rang before and you didn't answer
mmssms.d Android M	2023-08-2		1 Outgoing	27fc813e-3d84-4bf2-9554-a7	1802342233	Don't worry. The people here are so friendly. We met a guy Peter who is going to give us a lift.
mmssms.d Android M	2023-08-2		1 Outgoing	27fc813e-3d84-4bf2-9554-a7	1802342233	Dad there's someone here.
mmssms.d Android M	2023-08-2		1 Incoming	1802342233	27fc813e-3d84-4bf2-9554-a7	The cousins are back?
mmssms.d Android M	2023-08-2		1 Outgoing	27fc813e-3d84-4bf2-9554-a7	1802342233	No. Dad, they're coming. They have Amanda.
mmssms.d Android M	2023-08-2		1 Incoming	1802342233	27fc813e-3d84-4bf2-9554-a7	How many people are there?
mmssms.d Android M	2023-08-2		1 Outgoing	27fc813e-3d84-4bf2-9554-a7	1802342233	Three, four. I don't know.
mmssms.d Android M	2023-08-2		1 Incoming	1802342233	27fc813e-3d84-4bf2-9554-a7	Go to the next bedroom. Get under the bed. Now, the next part is very important. They are going to take you. Shout out everything you see about them. Hair color, eye color, tall, short, scars. Anything you see. You understand?
mmssms.d Android M	2023-08-2		1 Outgoing	27fc813e-3d84-4bf2-9554-a7	1802342233	They're there. I can hear them.
mmssms.d Android M	2023-08-2		1 Incoming	1802342233	27fc813e-3d84-4bf2-9554-a7	Put the phone closer so I can hear.
mmssms.d Android M	2023-08-2		1 Outgoing	27fc813e-3d84-4bf2-9554-a7	1802342233	They're leaving. I think they're...Beard. Six feet. Tattoo right hand, moon and star.

ADDITIONAL QUESTIONS

17. Conduct a timeline analysis of the pieces of evidence.

The screenshot shows the Timeline-Editor application. The main window displays a list of events with columns for Date/Time, Event Type, Description, Tagged, and Hash Hit. The events are sorted by date, showing a range from May 2020 to August 2023. The interface includes a sidebar with filters (Must include text, Must be tagged, Must have hash hit, Limit data sources to) and a bottom section with a hex view and various toolbars for navigation and analysis.

➔ Above mentioned screenshot is for mobile forensics analysis. I can say that most of the event is happening between 8 May 2020, 6:21:11 am to 20 Aug 2023 3:37: 08 pm

Timeline - Editor

Timeline x

Display Times In: Local Time Zone GMT / UTC

View Mode: Counts Details List

29,952 events

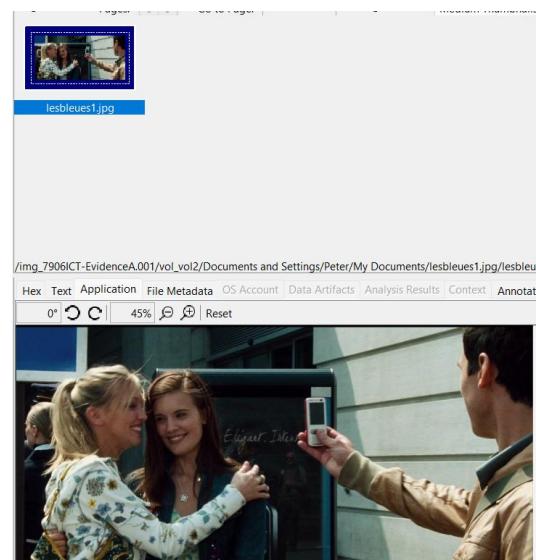
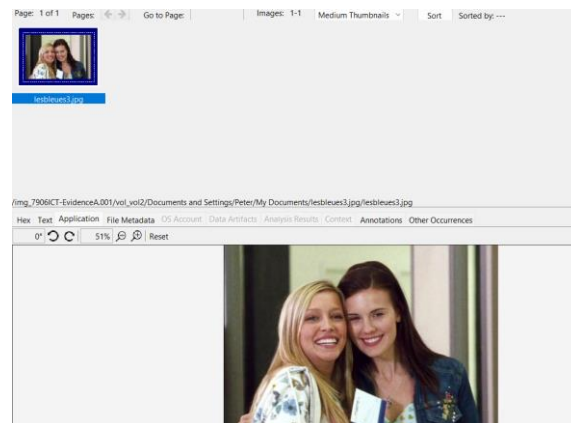
Date/Time	Event Type	Description	Tagged	Hash Hit
2006-08-16 21:08:49	Document Last Saved	Document Last Saved : :		
2006-08-16 21:08:49	Document Created	Document Created : :		
2006-08-16 21:09:20	Document Last Saved	Document Last Saved : :		
2006-08-16 21:09:20	Document Created	Document Created : :		
2007-04-02 23:34:02	_M	/Program Files/Messenger/xpmsgcr.chm		
2007-04-02 23:37:24	_M	/Program Files/Messenger/fvback.gif		
2007-04-02 23:37:28	_M	/Program Files/Messenger/type.wav		
2007-05-15 13:38:22	_M	/WINDOWS/system32/spool/drivers/w32x86/3/PSSCRIPT.HLP		
2007-05-15 13:38:24	_M	/WINDOWS/system32/spool/drivers/w32x86/3/PSSCRIPT.NTF		
2007-06-25 22:39:02	_M	/Program Files/Windows Media Player/Skins/Revert.wmz/pl_restoremin_btgrp_hover.bmp		
2007-06-25 22:39:02	_M	/Program Files/Windows Media Player/Skins/Revert.wmz/pl_restoremin_btgrp_down.bmp		
2007-06-25 22:39:02	_M	/Program Files/Windows Media Player/Skins/Revert.wmz/volume_thumb_on.bmp		
2007-06-25 22:39:02	_M	/Program Files/Windows Media Player/Skins/Revert.wmz/volume_slider_on.bmp		
2007-06-25 22:39:02	_M	/Program Files/Windows Media Player/Skins/Revert.wmz/pl_z.bmp		
2007-06-25 22:39:02	_M	/Program Files/Windows Media Player/Skins/Revert.wmz/volume_thumb_hover.bmp		
2007-06-25 22:39:02	_M	/Program Files/Windows Media Player/Skins/Revert.wmz/pause_down.bmp		
2007-06-25 22:39:02	_M	/Program Files/Windows Media Player/Skins/Revert.wmz/eq_hslider_thumb_down.bmp		
2007-06-25 22:39:02	_M	/Program Files/Windows Media Player/Skins/Revert.wmz/player_disable.bmp		
2007-06-25 22:39:02	_M	/Program Files/Windows Media Player/Skins/Revert.wmz/eq_vslider_thumb_disabled.bmp		
2007-06-25 22:39:02	_M	/Program Files/Windows Media Player/Skins/Revert.wmz/eq_vslider_thumb_disabled.bmp		

Start: 16 Dec 2005, 11:26:42 am End: 21 Aug 2023, 1:53:48 am

➔ Above mentioned screenshot is for Evidence A I can say that most of the event happened between 16 Dec 2005, 11:26:42 am to 21 Aug 2023, 1:53:48 am.

18. Provide a brief final analysis of the evidence and your conclusions.

Evidence A: Two photos, "lesbleus3" and "lesbleus1," were found, which translate to "THE BLUE ONE" in French. It is significant that Kim is wearing a blue jacket in one of these photos, indicating prior knowledge about her.



Evidence B: The taxi driver, Peter, is initially portrayed as friendly and helpful. However, it is later revealed that he is connected to the human traffickers who abducted Kim and Amanda. Furthermore, a .txt file on Peter's laptop contains the address "Level 5 Hoffman Hotel, 26 Av Kleber 75116 Paris, France." A map image sent by Raman is believed to correspond to this address.

address.txt		0	2023-08-20 16:38:28 AEST
desktop.ini		0	2023-08-20 16:20:06 AEST
fifa.jpg		0	2023-08-20 16:18:26 AEST

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis Results

StringsExtracted TextTranslation

Page: 1 of 1 PageMatches on page: - of - Match100%

Level 5 Hoffman Hotel, 26 Av. Kléber, 75116 Paris, France

-----METADATA-----

Evidence C: Emails suggest a connection between the owner, Patrice, and an individual named Marko. While the content of their communication is unknown, it appears that Patrice is waiting for Marko to complete the abduction task, implying his involvement with the criminal operation.

```
user_pref("mail.server.server1.userName", "cn363478@gmail.com");
user_pref("mail.smtpserver.smtp1.username", "cn363478@gmail.com");
3478@gmail.com
2023 Google LLC 1600 Amphitheatre Parkway, Mountain View, CA 94043Updating our Google Account inactivity policyGoogle Accounts Team <no-reply@accounts.google.com> undefinedcn363478@gmail.com undefined
cn363478@gmail.com
<https://accounts.google.com/AccountChooser?Email=cn363478@gmail.com&continue=https://myaccount.google.com/alert/nt/1692623524000?rfn%3D127%26rfnc%3D1%26eid%3D663880662732590837%26et%3D0>
2023 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USAsecurity alertGoogle <no-reply@accounts.google.com> undefinedcn363478@gmail.com undefined
cn363478@gmail.com
<https://accounts.google.com/AccountChooser?Email=cn363478@gmail.com&continue=https://myaccount.google.com/alert/nt/1692623512744?rfn%3D325%26rfnc%3D1%26eid%3D8135379664817103574%26et%3D0>
2023 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USAsecurity alertGoogle <no-reply@accounts.google.com> undefinedcn363478@gmail.com undefined
On Mon, 21 Aug 2023 at 18:29, Patrice Saint-Clair <cn363478@gmail.com>Check notepad for MessageMarko Dushku <hs1615717@gmail.com> undefinedPatrice Saint-Clair <cn363478@gmail.com> undefined
cn363478@gmail.com
<https://accounts.google.com/AccountChooser?Email=cn363478@gmail.com&continue=https://myaccount.google.com/alert/nt/1692685627000?rfn%3D325%26rfnc%3D1%26eid%3D3574682928082999683%26et%3D0>
2023 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USAsecurity alertGoogle <no-reply@accounts.google.com> undefinedcn363478@gmail.com undefined
cn363478@gmail.com
emailhs1615717@gmail.com
emailcn363478@gmail.com(
emailhs1615717@gmail.com
emailcn363478@gmail.com
(END)
```

Evidence D: Mobile messages reveal that Peter randomly met Kim and Amanda. This indicates that Peter had prior knowledge of the victims, as they were targeted by the human traffickers. The messages further implicate Raman as a key figure in the operation, as he is directing Marko and providing critical updates.

mmssms.db		Android Message	2023-08-20 14:48:46 AEST	1	27fc813
mmssms.db		Android Message	2023-08-20 14:49:11 AEST	1	27fc813

HexTextApplicationSource File MetadataOS AccountData ArtifactsAnalysis ResultsContextAccounts

Result: 12 of 21Result

From: 27fc813e-3d84-4bf2-9554-a713049fd8e1
To: 1802342233
CC:
Subject:

HeadersTextHTMLRTFAttachments (0)Accounts

Don't worry. The people here are so friendly. We met a guy Peter who is going to give us a lift.

Analysis and Conclusions: The presence of photos on Peter's laptop indicating Kim's attire, along with mobile messages suggesting he had met them randomly, raises suspicion that he had prior knowledge of the victims. This implies a premeditated plan for their abduction.

Raman's involvement is significant, as he appears to be the orchestrator of the operation. He is in constant communication with Marko, providing instructions and sharing a distorted map image that likely corresponds to the abduction location.

Patrice, the owner mentioned in the email communication, is possibly associated with the criminal operation. Although the content of their communication is not available, Patrice seems to be awaiting updates from Marko, indicating his dependence on the gang's activities.

19. Provide advice to Bryan Mills about the identification and collection methods for each specific evidence item.

➔ In the digital forensics investigation involving four separate pieces of evidence, various tools are employed to extract critical information. In Evidence A, Sleuth Kit and FTK Imager are used to gather user profiles, analyze the Windows registry for system configurations and software details, extract file metadata for timeline establishment, recover deleted files, and facilitate overall forensic analysis.

➔ Evidence B, Wireshark and Network Miner are utilized to identify communicating parties, transmission timing, browsers, operating systems, and IP addresses involved in network traffic, pinpoint sent files, and unveil relationships among participants.

➔ Evidence C involves the use of Sleuth Kit and the Volatility Framework to identify running applications, analyze web browsing history, discover email addresses and their relevance to the case, and recover passwords.

➔ Evidence D is examined using Autopsy, which helps identify non-stock applications, access contacts, messages, and call logs, trace internet searches, and uncover potential evidence pertaining to the owner's role in a particular situation. It's imperative to stress that all these investigations must be carried out in a forensically sound manner, adhering to legal standards and preserving the chain of custody, preferably by law enforcement or trained digital forensics experts, especially in cases involving potential criminal activity.

Task-2

Topic: Disk Forensics and File Carving in Digital Forensics Investigations

Introduction

Digital forensics plays a pivotal role in modern law enforcement and legal proceedings, aiding in the identification and prosecution of individuals involved in various cybercrimes and criminal activities. Disk forensics, a subfield of digital forensics, focuses on the examination and analysis of digital storage media like hard drives, USB devices, and mobile phones to recover valuable evidence. It is an essential aspect of any digital forensic investigation because it helps uncover crucial information, such as files, user activity, and system configurations, which can be used as evidence in a court of law. One key technique within disk forensics is "File Carving," which involves extracting files from unallocated disk space, file fragments, or damaged storage devices. This article explores the importance of disk forensics and the specific methodology of file carving in a real-world case.

Usefulness of Disk Forensics

Disk forensics is invaluable in various scenarios, including cybercrime investigations, corporate espionage, data theft, intellectual property disputes, and more. It helps in the recovery of digital evidence, which is often crucial for building a case or establishing the guilt or innocence of suspects. Disk forensics can provide insights into user actions, including files accessed, deleted, or modified, web browsing history, and communication records, making it an essential component of digital investigations.

When is Disk Forensics Used?

Criminal Investigations: Law enforcement agencies use disk forensics to gather evidence related to various crimes, such as cyberattacks, financial fraud, and child exploitation cases.

Civil Litigation: In civil lawsuits, parties may use disk forensics to uncover electronic evidence that supports their claims.

Data Recovery: Disk forensics can help recover data from damaged or corrupted storage devices in personal or business contexts.

Evidence Acquisition

Proper evidence acquisition is paramount in maintaining the integrity of digital evidence. It involves the careful collection of data from the suspect's digital storage devices without tampering with or altering the original data. Techniques used to ensure the preservation of digital evidence include:

Disk Imaging:

Disk imaging is the process of creating a bit-by-bit copy of the original storage device, ensuring that the integrity of the original evidence is preserved. A popular tool for this purpose is "dd," a command-line utility in Unix-based systems. For example, in our case, the damaged mobile phone found at the daughter's hotel apartment was imaged using the "dd" command to create a forensically sound copy of the device's data.

Write-Blocking:

Write-blocking hardware or software is employed to prevent any writes to the storage device during acquisition. This prevents the contamination of evidence during the acquisition process. In the case

mentioned, a hardware write blocker was used to ensure that no data could be written back to the mobile phone during imaging.

Forensic Analysis:

Forensic analysis in disk forensics involves the examination of acquired disk images to uncover relevant information and evidence. This analysis often includes the process of file carving, which is a technique for recovering files from unallocated disk space or fragmented files. Several algorithms, techniques, and methods are used to conduct the analysis:

File Carving:

File carving is a crucial aspect of disk forensics and involves extracting files from unallocated space or damaged storage devices. It works by identifying file headers and footers and then reconstructing the file based on this information. For instance, if a file's header and footer can be found in unallocated space, a file carving tool can reconstruct the entire file. In our investigation, file carving was essential to recover deleted or damaged files from the mobile phone's storage.

Keyword and Pattern Searching:

Forensic analysts may use keyword and pattern searching to identify specific data within disk images. This can be useful in finding text documents, emails, or other information related to the case. For instance, searching for keywords like "history" or "web history" may reveal relevant data on the mobile phone.

File Metadata Analysis:

File metadata, including timestamps (creation, modification, and access times), can provide crucial information about the sequence of events and user activities. In our case, analyzing file metadata helped establish a timeline of actions related to the daughter's disappearance.

Data Recovery:

Disk forensics tools and techniques enable data recovery from damaged or partially overwritten files. This is important for retrieving evidence that may have been deliberately or accidentally deleted.

Forensic Tools

There are various forensic tools available to aid in disk forensics and file carving. Each has its advantages and disadvantages, and the choice of tool depends on the specific requirements of the case. Here are a few tools used in our investigation:

The Sleuth Kit:

The Sleuth Kit is an open-source software library and collection of command-line digital forensic tools. It is advantageous for its open-source nature, but it requires expertise to use effectively. Sleuth Kit was used in our case for tasks such as file system analysis and file recovery.

FTK Imager:

FTK Imager, developed by AccessData, is a user-friendly graphical tool for acquiring disk images and viewing their contents. Its advantages include ease of use and a user-friendly interface, making it suitable for investigators with varying levels of expertise.

Autopsy:

Autopsy is another open-source digital forensics platform that is used for disk analysis. It offers a web-based interface and features like file carving, keyword searching, and timeline analysis. Its open-source nature allows for extensive customization and community support.

Conclusions

In conclusion, disk forensics, particularly file carving, plays a pivotal role in digital investigations, enabling the recovery of vital evidence from digital storage devices. Proper evidence acquisition, involving techniques like disk imaging and write-blocking, ensures the integrity of the collected data. Forensic analysis techniques, including file carving, keyword and pattern searching, and file metadata analysis, help uncover evidence in a forensically sound manner. Various tools are available, each with its advantages and disadvantages, providing flexibility in investigations.

As technology advances, the field of disk forensics continues to evolve. Future directions may involve improved tools and techniques for analyzing solid-state drives (SSDs), cloud-based storage, and IoT devices. It is crucial for digital forensic investigators to stay updated and adapt to emerging technologies to remain effective in their roles.

In the case at hand, the combination of sound evidence acquisition, effective forensic analysis, and the use of appropriate forensic tools based on the specific requirements of the case proved essential in identifying and prosecuting those involved in the daughter's disappearance. This underscores the importance of disk forensics and file carving in modern investigative practices and legal proceedings.

References

Autopsy. (2019, August 12). Autopsy; Basis Technology. <https://www.autopsy.com/>

BibGuru. (n.d.). Bibguru.com. Retrieved October 16, 2023, from <https://app.bibguru.com/>

Chandel, R. (2020, November 6). Comprehensive guide on FTK Imager. Hacking Articles. <https://www.hackingarticles.in/comprehensive-guide-on-ftk-imager/>

Fox, N. (2022, April 12). How to use Volatility for memory forensics and analysis. Varonis.com. <https://www.varonis.com/blog/how-to-use-volatility>

FTK® imager. (2023, May 26). Exterro. <https://www.exterro.com/ftk-imager>

Open source digital forensics. (n.d.). Sleuthkit.org. Retrieved October 16, 2023, from <https://www.sleuthkit.org/>

The Volatility Foundation - open source memory forensics. (n.d.). Volatilityfoundation. Retrieved October 16, 2023, from <https://www.volatilityfoundation.org/>

(N.d.). Openai.com. Retrieved October 16, 2023, from <https://chat.openai.com/>