

ICT30010 Capstone Lab Assignment

Investigator: Wong Jin Tao

Image analysed: ImaHacker.E01

Environment: Kali Linux

Date Completed: 28/6/2025

Contents

1. Introduction	3
1.1 Evidence received from police and colleagues	3
2. Chain of Custody	3
3. Preparation	3
3.1 Image Verification	3
3.2 Determine Partitions on Disk Image	5
3.3 Mount the Partition	5
3.4 Checking the Disk Image Time Zone	6
3.5 Examination with Autopsy Forensic Browser	6
3.5.1 Setup for Autopsy	6
3.5.2 Setup for Timeline Analysis	7
4. Alleged Hacking Events	8
4.1 Scenario 1 – “Hackable” Company (hackable.com.au)	8
4.2 Scenario 2 – Website attack	11
4.3 Scenario 3 – Unauthorised access to Facebook	16
4.4 Scenario 4 - Find the collaborator with the suspect	20
5. Forensic Report	25
1. Introduction	25
2. Evidence & Chain of Custody	25
Received from Police:	25
Received from Colleague, Troy:	25
Chain of Custody:	25
3. Tools and Methodology	26
3.1 Partition and Time Zone Information	26
4. Forensic Analysis	26
4.1 Scenario 1 – Hackable.com.au Defacement (4 May 2010)	26
4.2 Scenario 2 – Website Attack (4 March 2009, 2:22 AM)	27
4.3 Scenario 3 – Unauthorised access to Facebook account	28
4.4 Collaborator Communications (hidemyass.com)	29
5. Overall Conclusion	30
6. Glossary	30

1. Introduction

This technical report outlines the detailed forensic process undertaken to investigate allegations against Imanuel Leet-Hacker (Ima Hacker) concerning three primary incidents, which are the defacement of the Hackable website, a second website attack, and the unauthorised access of a Facebook account. Additionally, the investigation aimed to identify any evidence of communication with a suspected collaborator using hidemyass.com as an email dropbox.

1.1 Evidence received from police and colleagues

- A forensic image of the suspect's computer (ImaHacker.E01)
- Exhibit 1: Screenshot of Hackable's web server after compromise
- Exhibit 2: Image placed on "Somepoor victim" Facebook page
- A timeline CSV (timeline.csv) (MD5: 9574ac771fdeeeb9a95d8dda5ed1749a)

The investigation was conducted using Kali Linux, Autopsy, RegRipper, Wireshark, and other forensic tools to extract, analyse, and correlate digital artefacts with the alleged incidents. This report documents the environment setup, evidence acquisition, tool usage, commands executed, and analysis steps taken to ensure reproducibility, transparency, and alignment with forensic best practices.

The findings from this investigation are presented with clear technical details and are organised according to each scenario in the capstone lab requirements, ensuring they align with the assessment criteria while demonstrating rigorous forensic methodology.

2. Chain of Custody

The forensic image ImaHacker.E01 was received from the police in October 2010 via a secure institutional download link and verified using an MD5 hash check to confirm integrity before analysis. The image was mounted using ewfmount on Kali Linux in a read-only environment, ensuring that no alterations occurred during the examination.

The evidence items were securely stored on the forensic analysis system and accessed using Autopsy, RegRipper, Wireshark, and command-line forensic tools while maintaining strict evidence integrity throughout the analysis in alignment with forensic best practices.

3. Preparation

3.1 Image Verification

The disk image is not a standard "dd" (raw disk image). I have instead been provided with a compressed Expert Witness Format (EWF, also known as EnCase format, or E01) disk image.

1. First, I copy the file to the Kali-share folder, whose path is /mnt/Kali-share.
2. I opened the terminal in Kali and ran “cd /mnt/Kali-share”.
3. I ran the command “pwd” to make sure I am in the correct path.
4. I ran the command “sudo apt install libewf-tools” to install the EWF tools.
5. I ran the command “ewfinfo ImaHacker.E01” to display metadata information about the disk image
 - a. The sector size (bytes per sector) for the forensic image is 512 bytes.
 - b. The disk image size (media size) is 20 Gigabytes.
 - c. Acquisition Date is Wed 25 May 2011 22:58:54.
 - d. Operating System is Windows 7.

```
(kali@kali)-[/mnt/Kali-share]
$ ewfinfo ImaHacker.E01
ewfinfo 20140816

Acquiry information
Description:          ImaHacker
Evidence number:      Capstone Lab
Notes:               Ima Hacker's PC - Seized 15/10/10
Acquisition date:    Wed May 25 22:58:54 2011
System date:         Wed May 25 22:58:54 2011
Operating system used: Windows 7
Software version used: 6.18
Password:            N/A
Extents:             0

EWF information
File format:         unknown
Sectors per chunk:   64
Error granularity:   64
Compression method:  deflate
Compression level:   best compression
Set identifier:      51303450-b036-4164-a371-2c076515f1f1

Media information
Media type:          fixed disk
Is physical:         yes
Bytes per sector:    512
Number of sectors:   41943040
Media size:          20 GiB (21474836480 bytes)

Digest hash information
MD5:                 16dc3a3dcdb703e62f5b3dbe3b4ab8a10
SHA1:                b4da388ef7196fed5bbd60a0b2497f19b94407ef
```

Picture 1: Metadata information of the disk image

6. I ran the command “ewfverify ImaHacker.E01” to verify that the hash contained within the E01 file is correct.
 - a. The MD5 hash stored in the file is the same as the MD5 hash calculated over the data.

```
Read: 20 GiB (21474836480 bytes) in 1 minute(s) and 52 second(s) with 182 MiB/s (191739611 bytes/second).

MD5 hash stored in file:          16dc3a3dcdb703e62f5b3dbe3b4ab8a10
MD5 hash calculated over data:    16dc3a3dcdb703e62f5b3dbe3b4ab8a10

Additional hash values:
SHA1:  b4da388ef7196fed5bbd60a0b2497f19b94407ef

ewfverify: SUCCESS
```

Picture 2: The successful result of the verification

3.2 Determine Partitions on Disk Image

- I ran the command “`mmls ImaHacker.E01`” to determine the partitions. Below is the table that shows all the partitions on the disk image:

Partition Number	Partition Type	Start Sector	End Sector	Total Sector	Total Size (MB)
000	Primary Table	00	00	1	0.00049
001	Unallocated	00	62	63	0.031
002	NTFS/ exFaT	63	41913584	41913522	20465.59
003	Unallocated	41913585	41943039	29455	14.38

Table 1: Partition table on Disk Image

```
(kali㉿kali)-[/mnt/Kali-share]
$ mmls ImaHacker.E01
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

    Slot      Start      End      Length    Description
000:  Meta      0000000000  0000000000  0000000001  Primary Table (#0)
001:  _____  0000000000  0000000062  0000000063  Unallocated
002:  000:000    0000000063  0041913584  0041913522  NTFS / exFAT (0x07)
003:  _____  0041913585  0041943039  0000029455  Unallocated
```

Picture 3: Partitions in Disk Image

3.3 Mount the Partition

- I made a new directory by running the command “`mkdir /mnt/Kali-share/Data`”.
- I ran the command “`sudo ewfmount ImaHacker.E01 /mnt/Kali-share/Data`” to make the raw disk image within the E01 file available.
- I verified the mount occurred correctly by running the command “`sudo ls -l /mnt/Kali-share/Data`”, which had a file named “`ewf1`”

```
(kali㉿kali)-[/mnt/Kali-share]
$ sudo ls -l /mnt/Kali-share/Data
total 0
-r--r--r-- 1 root root 21474836480 Jun 27 15:33 ewf1
```

Picture 4: verification for the file named “ewf1”

- Here are the steps that I used to mount the partition contained within the raw disk image
 - I calculated the starting offset, which is **32256** (starting sector x sector size).
 - I made a new directory by running the command “`mkdir /mnt/Kali-share/windows_mount`”
 - I ran the command “`sudo mount -t ntfs -o ro,loop,offset=32256,show_sys_files /mnt/Kali-share/Data/ewf1 /mnt/Kali-share/windows_mount`” to mount the partition read-only.

- d. I ran the command “ls /mnt/Kali-share/windows_mount” to make sure the mount occurred correctly.

```
$ ls /mnt/Kali-share/windows_mount
'AttrDef' '$Bitmap' '$Extend' '$MFT' '$Secure' '$Volume' boot.ini 'Documents and Settings'
'$BadClus' '$Boot' '$LogFile' '$MFTMirr' '$UpCase' AUTOEXEC.BAT CONFIG.SYS IO.SYS

MSDOS.SYS ntldr 'Program Files' 'System Volume Information' WINDOWS
NTDETECT.COM pagefile.sys RECYCLER Toolz
```

Pictures 5&6: Verification of the files in windows_mount

3.4 Checking the Disk Image Time Zone

12. I used a forensic tool named RegRipper to check the registry.
- I installed the RegRipper by using the command “sudo apt install regripper”
 - I ran the RegRipper tool over the system registry hive by executing the command:
“sudo perl rip.pl -r /mnt/Kali-share/windows_mount/WINDOWS/system32/config/system -f system > /mnt/Kali-share/system.txt”
 - I ran the command “more /mnt/Kali-share/system.txt” to view the created report.
 - Under the “TimeZoneInformation key” heading, the current standard time zone was **AUS Eastern Standard Time**

```
TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time 2010-05-04 12:32:28Z
DaylightName → AUS Eastern Standard Time
StandardName → AUS Eastern Standard Time
Bias → -600 (-10 hours)
ActiveTimeBias → -600 (-10 hours)

usb v.20200515
(System) Get USB key info
```

Picture 7: Current standard time zone

3.5 Examination with Autopsy Forensic Browser

3.5.1 Setup for Autopsy

- I ran the command “sudo cp /usr/bin/mactime /usr/bin/mactime-sleuthkit” and “sudo cp /usr/bin/ils /usr/bin/ils-sleuthkit” to setup the Autopsy.
- I ran the command “sudo autopsy” to start the forensic tool.
- I opened Firefox, entered on URL <http://localhost:9999/autopsy>
 - I created a new case named Capstone
 - I clicked “Add Host” to add details of the PC seized from Ima Hacker

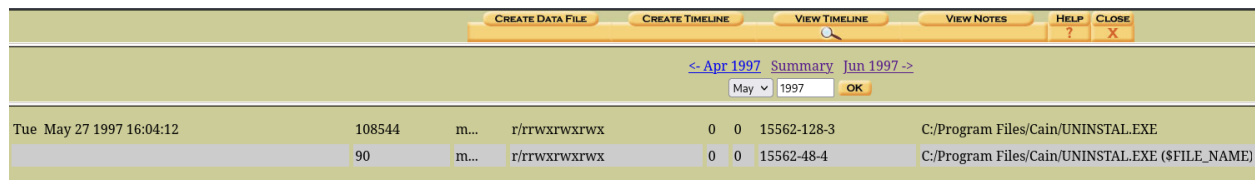
- i. I set the host name to "Ima Hacker" and the time zone to "Australia/Melbourne" (without the quotes).
 - ii. This configuration ensures that all timestamps in the analysis are interpreted according to the local time zone of the suspect system, automatically handling Australian Eastern Standard Time (AEST; UTC+10:00) and Australian Eastern Daylight Time (AEDT; UTC+11:00) based on the evidence dates.
- c. I clicked "Add Image", then "Add Image file" to add the image file.
 - i. Under "Location", I entered `/mnt/Kali-share/ImaHacker.E01`
 - ii. For "Type", I chose "Disk" and left the import method as "Symlink"
- d. In the "Host Manager", I selected the "C:" volume, and clicked the analyse button.



Picture 8: Autopsy Host Manager Screen Showing C: Volume for ImaHacker.E01

3.5.2 Setup for Timeline Analysis

16. On the host manager screen, I clicked the "File Activity Time Lines" button, then clicked the "Create Data File" button.
 - a. I selected the "C:/ ImaHacker.E01-63-41913584" volume, and once the data file process completed, I left the default values and created the timeline named "timeline.txt"



Picture 9: Timeline Analysis in Autopsy

4. Alleged Hacking Events

4.1 Scenario 1 – “Hackable” Company (hackable.com.au)

17. I clicked “File Analysis” to view the files inside the C: volume, and I used the search function to find related files by typing “hackable”

All files with 'hackable' in the name

[SHOW ALL FILES](#)

Error Parsing File (invalid characters?)
: V/V 17520: \$OrphanFiles 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0000-00-00 00:00:00 (UTC) 0 0 0

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
d / d		C:/Documents and Settings/Ima Hacker/My Documents/server.hackable	2010-05-04 23:35:36 (AEST)	2010-08-06 00:55:47 (AEST)	2010-05-04 23:35:36 (AEST)	2010-05-04 23:32:06 (AEST)	56	0	0	15424-144-9
r / r		C:/Documents and Settings/Ima Hacker/Recent/server.hackable.lnk	2010-05-04 23:35:36 (AEST)	2010-05-04 23:35:36 (AEST)	2010-05-04 23:35:36 (AEST)	2010-05-04 23:32:16 (AEST)	476	0	0	16138-128-1
r / r		C:/Program Files/Nmap/server.hackable.com.au.xml	2010-05-04 22:46:44 (AEST)	2010-05-04 22:46:44 (AEST)	2010-05-04 22:46:44 (AEST)	2010-05-04 22:46:44 (AEST)	11217	0	0	12102-128-4

Picture 10: Search result of “hackable”

- I noticed that there is a file inside C:/ Documents and Settings/ Ima Hacker/ My Documents/server.hackable/ and navigated into the path.
- I saw an HTML document named “PAWNED, again!.htm”, and the data inside was the same as the provided Exhibit 1, which is a screenshot of Hackable’s web server after compromised.

ASCII String Contents Of File: C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/PAWNED, again!.htm

```
<html><head>
<meta http-equiv="content-type" content="text/html; charset=ISO-8859-1">
<title>PAWNED, again!</title>
</head><body>
<h1>I've been hacked (again)</h1>
<p>L33t haxors rule!</p>

<p>(and because my backup user had a crap password. IPCScan saved the day!)</p>
</body></html>
```

Picture 11: Content of the PAWNED, again!.htm

- I found a document named “users.txt” that showed a bunch of users' details
 - I found that two account users named “IUSR_VICTIM” and “IWAM_VICTIM” accessed the website anonymously.

User	Fullname	Comment	SID	Req. Pass. Change	Pass Never Expire
Administrator	Administrator	Built-in account for administering the computer/domain	S-1-5-21-343818398-527237240-1801674531-500	No	Yes 2004/07/21 - 14:57 Active
backup	backup	system backup account	S-1-5-21-343818398-527237240-1801674531-1005	No	Yes 2011/04/26 - 08:24 Active
dave	dave shaver	dave is such a GOARMY fan	S-1-5-21-343818398-527237240-1801674531-1003	No	Yes 2009/07/14 - 05:11 Active
Guest	Guest	Built-in account for guest access to the computer/domain	S-1-5-21-343818398-527237240-1801674531-501	Yes	Yes 1970/01/1 - 00:00 Disabled
IUSR_VTICTIM	IUSR_VTICTIM	Internet Guest Account Built-in account for anonymous access to Internet Information Services	S-1-5-21-343818398-527237240-1801674531-1000	Yes	Yes 2011/04/26 - 08:24 Active
IWAM_VTICTIM	IWAM_VTICTIM	Launch IIS Process Account Built-in account for Internet Information Services to start out of process applications	S-1-5-21-343818398-527237240-1801674531-1001	Yes	Yes 2009/07/14 - 04:39 Active
lance	lance mueller		S-1-5-21-343818398-527237240-1801674531-1004	No	Yes 1970/01/1 - 00:00 Active
ric	ric stonesifer	this is rics account	S-1-5-21-343818398-527237240-1801674531-1002	No	Yes 1970/01/1 - 00:00 Active

Picture 12: Content of users.txt

- d. I found a picture named “win2000.gif” in the C:/ Documents and Settings/ Ima Hacker/ My Documents/ server.hackable /PAWNED, again! Files/, which is the same as in Exhibit 1.



Picture 13: same thumbnail as the thumbnail in Exhibit 1

- e. After that, I returned to the previous directory and found the Nmap tools folder. In C:/ Documents and Settings/ Ima Hacker/.zenmap/, I found two text files, which were “recent_scans.txt” and “target_list.txt”
- The “recent_scans.txt” showed at Zenmap (Nmap) was used on the suspect’s device to scan the host server.hackable.com.au
 - The “target_list.txt” showed the scan target, which is server.hackable.com.au

Contents Of File: C:/Documents and Settings/Ima Hacker/.zenmap/recent_scans.txt

C:\Program Files\Nmap\server.hackable.com.au.xml

Picture 14: Content of recent_scans.txt

```
Contents Of File: C:/Documents and Settings/Ima Hacker/.zenmap/target_list.txt  
  
server.hackable.com.au
```

Picture 15: Content of target_list.txt

- f. In the “C:/Program Files/ Nmap” (from Picture 10), I found the server.hackable.com.au.xml, and it showed the details about port scanning on server.hackable.com.au

```
Initiating ARP Ping Scan at 22:41  
Scanning server.hackable.com.au (192.168.75.129) [1 port]  
Completed ARP Ping Scan at 22:41, 0.19s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 22:41  
Completed Parallel DNS resolution of 1 host. at 22:41, 0.17s elapsed  
Initiating SYN Stealth Scan at 22:41  
Scanning server.hackable.com.au (192.168.75.129) [1000 ports]  
Discovered open port 139/tcp on 192.168.75.129  
Discovered open port 21/tcp on 192.168.75.129  
Discovered open port 80/tcp on 192.168.75.129  
Discovered open port 445/tcp on 192.168.75.129  
Discovered open port 443/tcp on 192.168.75.129  
Discovered open port 135/tcp on 192.168.75.129  
Discovered open port 1025/tcp on 192.168.75.129  
Discovered open port 1026/tcp on 192.168.75.129  
Completed SYN Stealth Scan at 22:41, 0.09s elapsed (1000 total ports)  
Initiating Service scan at 22:41  
Scanning 8 services on server.hackable.com.au (192.168.75.129)  
Completed Service scan at 22:42, 106.13s elapsed (8 services on 1 host)  
Initiating OS detection (try #1) against server.hackable.com.au (192.168.75.129)
```

Picture 16: Port scanning on server.hackable.com.au

18. For the timeline analysis, I set the date to May 2010, as mentioned, the Hackable company website was hacked on 4th May 2010.

- a. On Tue, 4th May 2010 22:40:48, suspect run a scan by using zenmap.exe

Tue May 04 2010 22:40:48	46592	.a..	r/rrwxrwxrwx	0 0	14981-128-3	C:/Program Files/Nmap/zenmap.exe
-----------------------------	-------	------	--------------	-----	-------------	----------------------------------

Picture 17: Time and Date when the Zenmap was executed

56	mac.	d/drwxrwxrwx	0 0	15288-144-6	C:/Documents and Settings/Ima Hacker/.zenmap
22	...b	r/rrwxrwxrwx	0 0	5415-128-4	C:/Documents and Settings/Ima Hacker/.zenmap/target_list.txt
96	macb	r/rrwxrwxrwx	0 0	5415-48-2	C:/Documents and Settings/Ima Hacker/.zenmap/target_list.txt (\$FILE_NAME)
48	...b	r/rrwxrwxrwx	0 0	5417-128-5	C:/Documents and Settings/Ima Hacker/.zenmap/recent_scans.txt
98	macb	r/rrwxrwxrwx	0 0	5417-48-2	C:/Documents and Settings/Ima Hacker/.zenmap/recent_scans.txt (\$FILE_NAME)

Picture 18: Files that were investigated previously appeared in timeline

- a. On Tue, 4th May 2010 22:46:44, the server.hackable.com.au.xml has been created

Tue May 04 2010 22:46:44	11217	mach	r/rwxrwxrwx	0 0	12102-128-4	C:/Program Files/Nmap/server.hackable.com.au.xml
	118	mach	r/rwxrwxrwx	0 0	12102-48-2	C:/Program Files/Nmap/server.hackable.com.au.xml (\$FILE_NAME)

Picture 19: Time and date the XML file was created

- b. On Tue, 4th May 2010 23:32:16, users.txt was likely accessed by the suspect.

Tue May 04 2010 23:32:16	1239	mach	r/rwxrwxrwx	0 0	15427-128-3	C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/users.txt
	84	mach	r/rwxrwxrwx	0 0	15427-48-2	C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/users.txt (\$FILE_NAME)
	704	mach	r/rwxrwxrwx	0 0	15552-128-4	C:/Documents and Settings/Ima Hacker/Recent/users.txt.lnk
	92	mach	r/rwxrwxrwx	0 0	15552-48-2	C:/Documents and Settings/Ima Hacker/Recent/users.txt.lnk (\$FILE_NAME)
	476	...b	r/rwxrwxrwx	0 0	16138-128-1	C:/Documents and Settings/Ima Hacker/Recent/server.hackable.lnk
	104	...b	r/rwxrwxrwx	0 0	16138-48-2	C:/Documents and Settings/Ima Hacker/Recent/server.hackable.lnk (\$FILE_NAME)

Picture 20: Suspect got the users.txt file

- c. On Tue, 4th May 2010 23:35:36, the “PAWNED, again!.htm” has been accessed

Tue May 04 2010 23:35:36	56	m.c.	d/drwxrwxrwx	0 0	15424-144-9	C:/Documents and Settings/Ima Hacker/My Documents/server.hackable
	4670	mach	r/rwxrwxrwx	0 0	15657-128-3	C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/PAWNED, again!.files/win2000.gif
	88	mach	r/rwxrwxrwx	0 0	15657-48-2	C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/PAWNED, again!.files/win2000.gif (\$FILE_NAME)
	152	m.cb	d/drwxrwxrwx	0 0	15771-144-1	C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/PAWNED, again!.files
	106	mach	d/drwxrwxrwx	0 0	15771-48-2	C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/PAWNED, again!.files (\$FILE_NAME)
	663	mach	r/rwxrwxrwx	0 0	16135-128-4	C:/Documents and Settings/Ima Hacker/Recent/PAWNED, again!.htm.lnk
	110	mach	r/rwxrwxrwx	0 0	16135-48-2	C:/Documents and Settings/Ima Hacker/Recent/PAWNED, again!.htm.lnk (\$FILE_NAME)
	340	...b	r/rwxrwxrwx	0 0	16137-128-1	C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/PAWNED, again!.htm
	26	...b	r/rwxrwxrwx	0 0	16137-128-4	C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/PAWNED, again!.htm.Zone.Identifier
	102	mach	r/rwxrwxrwx	0 0	16137-48-2	C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/PAWNED, again!.htm (\$FILE_NAME)
	476	mac.	r/rwxrwxrwx	0 0	16138-128-1	C:/Documents and Settings/Ima Hacker/Recent/server.hackable.lnk
	104	mac.	r/rwxrwxrwx	0 0	16138-48-2	C:/Documents and Settings/Ima Hacker/Recent/server.hackable.lnk (\$FILE_NAME)

Picture 21: PAWNED, again!.htm

4.2 Scenario 2 – Website attack

19. From timeline analysis, I set the date to March 2009 as mentioned the website attack occurred on 4th March, 2009

- a. First, I scrolled to the time when the attack occurred, but there was nothing that happened at 2:22 am

Wed Mar 04 2009 02:20:18	256	m.c.	d/drwxrwxrwx	0 0	12270-144-1	C:/WINDOWS/Microsoft.NET
	56	m.c.	d/drwxrwxrwx	0 0	12272-144-7	C:/WINDOWS/Microsoft.NET/Framework/v2.0.50727
	56	m.c.	d/d-wx-wx-wx	0 0	12818-144-5	C:/WINDOWS/assembly
	176	mac.	d/drwxrwxrwx	0 0	12999-144-6	C:/WINDOWS/assembly/NativeImages_v2.0.50727_32
	48	mac.	d/drwxrwxrwx	0 0	13000-144-1	C:/WINDOWS/assembly/NativeImages_v2.0.50727_32/Temp
	89756	mac.	r/rwxrwxrwx	0 0	13008-128-4	C:/WINDOWS/Microsoft.NET/Framework/v2.0.50727/ngen_service.log
	304	mach	d/drwxrwxrwx	0 0	13342-144-1	C:/WINDOWS/assembly/NativeImages_v2.0.50727_32/System.Web.Services
	104	mach	d/drwxrwxrwx	0 0	13342-48-2	C:/WINDOWS/assembly/NativeImages_v2.0.50727_32/System.Web.Services (\$FILE_NAME)
	1945600	mach	r/rwxrwxrwx	0 0	13344-128-4	C:/WINDOWS/assembly/NativeImages_v2.0.50727_32/System.Web.Services/b47f2438f4bc0344a2eee6c1653fd1fe/System.Web.Services.ni.dll
	118	mach	r/rwxrwxrwx	0 0	13344-48-5	C:/WINDOWS/assembly/NativeImages_v2.0.50727_32/System.Web.Services/b47f2438f4bc0344a2eee6c1653fd1fe/System.Web.Services.ni.dll (\$FILE_NAME)
	0	..c	r/r--x--x--x	0 0	13345-128-1	C:/WINDOWS/assembly/NativeImages_v2.0.50727_32/index1b.dat
	0	mach	r/r--x--x--x	0 0	13348-128-1	C:/WINDOWS/assembly/NativeImages_v2.0.50727_32/index1c.dat
	88	mach	r/r--x--x--x	0 0	13348-48-2	C:/WINDOWS/assembly/NativeImages_v2.0.50727_32/index1c.dat (\$FILE_NAME)
	296	mach	d/drwxrwxrwx	0 0	13349-144-1	C:/WINDOWS/assembly/NativeImages_v2.0.50727_32/System.Web.Services/b47f2438f4bc0344a2eee6c1653fd1fe
	130	mach	d/drwxrwxrwx	0 0	13349-48-2	C:/WINDOWS/assembly/NativeImages_v2.0.50727_32/System.Web.Services/b47f2438f4bc0344a2eee6c1653fd1fe (\$FILE_NAME)
Wed Mar 04 2009 02:29:07	234914	...b	r/rwxrwxrwx	0 0	13286-128-3	C:/WINDOWS/Prefetch/Layout.ini

Picture 22: No result on 4th March, 2009 at 2:22 am

b. Before 2:22 am,

- i. I found that there is a file named “hackthissite-mission4” at 1:48:50 am and 1:49:18 am

Wed Mar 04 2009 01:48:50	12837	...b	r/rwxrwxrwx	0 0	11328-128-4	C:/RECYCLER/S-1-5-21-1935655697-1757981266-725345543-1003/Dc1.html
	82	...b	r/rwxrwxrwx	0 0	11328-48-6	C:/RECYCLER/S-1-5-21-1935655697-1757981266-725345543-1003/Dc1.html (\$FILE_NAME)
	568	...b	r/rwxrwxrwx	0 0	11329-128-1	C:/Documents and Settings/Ima Hacker/Recent/hackthissite-mission4.lnk
	116	...b	r/rwxrwxrwx	0 0	11329-48-2	C:/Documents and Settings/Ima Hacker/Recent/hackthissite-mission4.lnk (\$FILE_NAME)
Wed Mar 04 2009 01:49:09	12837	m...	r/rwxrwxrwx	0 0	11328-128-4	C:/RECYCLER/S-1-5-21-1935655697-1757981266-725345543-1003/Dc1.html
	82	mac.	r/rwxrwxrwx	0 0	11328-48-6	C:/RECYCLER/S-1-5-21-1935655697-1757981266-725345543-1003/Dc1.html (\$FILE_NAME)
Wed Mar 04 2009 01:49:18	568	m.c.	r/rwxrwxrwx	0 0	11329-128-1	C:/Documents and Settings/Ima Hacker/Recent/hackthissite-mission4.lnk
	116	mac.	r/rwxrwxrwx	0 0	11329-48-2	C:/Documents and Settings/Ima Hacker/Recent/hackthissite-mission4.lnk (\$FILE_NAME)

Picture 23: Timeline for “hackthissite-mission4”

- ii. I found the suspect was browsing “www.blackhatworld” at 1:52:07am

Wed Mar 04 2009 01:52:07	273	m.cb	r/rwxrwxrwx	0 0	11352-128-1	C:/Documents and Settings/Ima Hacker/Cookies/ima hacker@www.blackhatworld[1].txt
	136	mach	r/rwxrwxrwx	0 0	11352-48-2	C:/Documents and Settings/Ima Hacker/Cookies/ima hacker@www.blackhatworld[1].txt (\$FILE_NAME)
	169798	...b	r/rwxrwxrwx	0 0	11360-128-5	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/CJIP4PUH/21313-change-referrer-anything-testing-out[1].htm
	164	mach	r/rwxrwxrwx	0 0	11360-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/CJIP4PUH/21313-change-referrer-anything-testing-out[1].htm (\$FILE_NAME)

Picture 24: Browsed blackhatworld

- iii. I found the suspect was browsing Stack Overflow at 1:54:58 am

Wed Mar 04 2009 01:54:58	2642	mac.	r/rwxrwxrwx	0 0	11458-128-4	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/EVKTON8H/adzerk1_2_4_43,adzerk2_2_17_45,adzerk3_2_4_44[1].htm
	775	mac.	r/rwxrwxrwx	0 0	11463-128-4	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/EVKTON8H/5526bf57d5775d0233f70dcb93b2bb2b[1].png
	498	mach	r/rwxrwxrwx	0 0	11465-128-1	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/EVKTON8H/8d1dc85bd2d8ed3a2074b9728fdaa55[1].png
	144	mach	r/rwxrwxrwx	0 0	11465-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/EVKTON8H/8d1dc85bd2d8ed3a2074b9728fdaa55[1].png (\$FILE_NAME)
	1363	mach	r/rwxrwxrwx	0 0	11466-128-4	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/IZQDETYP/0640a421d5d39fe474dc8214a3e97bb4[1].png
	144	mach	r/rwxrwxrwx	0 0	11466-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/IZQDETYP/0640a421d5d39fe474dc8214a3e97bb4[1].png (\$FILE_NAME)
	417	m.c.	r/rwxrwxrwx	0 0	11467-128-1	C:/Documents and Settings/Ima Hacker/Cookies/ima hacker@stackoverflow[1].txt
	128	mac.	r/rwxrwxrwx	0 0	11467-48-2	C:/Documents and Settings/Ima Hacker/Cookies/ima hacker@stackoverflow[1].txt (\$FILE_NAME)

Picture 25: Browsed Stack Overflow

- iv. I found the suspect was accessing “secfox-turn-firefox-into-an-ultimate-hacking-tool-parts-1[1].htm” at 1:55:51am

Wed Mar 04 2009 01:53:51	46700	...	r/rwxrwxrwx	0	0	11508-128-4	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/IZQDETYP/books[1].png
	90	...	r/rwxrwxrwx	0	0	11508-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/IZQDETYP/books[1].png (\$FILE_NAME)
	51198	...	r/rwxrwxrwx	0	0	11509-128-4	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/IZQDETYP/books[2].png
	90	macb	r/rwxrwxrwx	0	0	11509-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/IZQDETYP/books[2].png (\$FILE_NAME)
	4673	macb	r/rwxrwxrwx	0	0	11510-128-4	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/IZQDETYP/books[1].jpg
	90	macb	r/rwxrwxrwx	0	0	11510-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/IZQDETYP/books[1].jpg (\$FILE_NAME)
	6179	macb	r/rwxrwxrwx	0	0	11511-128-4	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/IZQDETYP/books[2].jpg
	90	macb	r/rwxrwxrwx	0	0	11511-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/IZQDETYP/books[2].jpg (\$FILE_NAME)
	84608	...	r/rwxrwxrwx	0	0	11513-128-5	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/UDM5CTEP/secfox-turn-firefox-into-an-ultimate-hacking-tool-part-1[1].htm
	192	macb	r/rwxrwxrwx	0	0	11513-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/UDM5CTEP/secfox-turn-firefox-into-an-ultimate-hacking-tool-part-1[1].htm (\$FILE_NAME)
	40064	macb	r/rwxrwxrwx	0	0	11515-128-5	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/UDM5CTEP/v2mncore_1366ad1369e871103f89fdaa63928e9c[2].js
	160	macb	r/rwxrwxrwx	0	0	11515-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/UDM5CTEP/v2mncore_1366ad1369e871103f89fdaa63928e9c[2].js (\$FILE_NAME)

Picture 26: Timeline that shows a website related to hacking tools

- v. I found the suspect was accessing a website related to apphack at 1:56 am

Wed Mar 04 2009 01:56:00	0	macb	r/rwxrwxrwx	0	0	11481-128-1	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/UDM5CTEP/books[1].htm
	90	macb	r/rwxrwxrwx	0	0	11481-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/UDM5CTEP/books[1].htm (\$FILE_NAME)
	412	...	r/rwxrwxrwx	0	0	11522-128-1	C:/Documents and Settings/Ima Hacker/Cookies/ima hacker@a4apphack[1].txt
	120	...	r/rwxrwxrwx	0	0	11522-48-2	C:/Documents and Settings/Ima Hacker/Cookies/ima hacker@a4apphack[1].txt (\$FILE_NAME)
Wed Mar 04 2009 01:56:01	927	macb	r/rwxrwxrwx	0	0	11525-128-5	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/UDM5CTEP/external-tracking.min[2].js
	120	macb	r/rwxrwxrwx	0	0	11525-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/UDM5CTEP/external-tracking.min[2].js (\$FILE_NAME)

Picture 27: Timeline that shows a website related to apphack

- vi. I found that the suspect was using Fiddler at 1:59:32 am

Wed Mar 04 2009 01:59:32	56	m.c.	d/d-wx-wx-wx	0	0	10290-144-6	C:/Documents and Settings/Ima Hacker/Favorites
	318	macb	r/rwxrwxrwx	0	0	11724-128-1	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/IZQDETYP/favicon[1].ico
	94	macb	r/rwxrwxrwx	0	0	11724-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/IZQDETYP/favicon[1].ico (\$FILE_NAME)
	225	m.cb	r/rwxrwxrwx	0	0	11725-128-4	C:/Documents and Settings/Ima Hacker/Favorites/Fiddler Web Debugger - links.url
	130	macb	r/rwxrwxrwx	0	0	11725-48-2	C:/Documents and Settings/Ima Hacker/Favorites/Fiddler Web Debugger - links.url (\$FILE_NAME)

Picture 28: Timeline that shows the suspect using Fiddler

- c. After 2:22 am,

- i. I found that the suspect was accessing “hackthissite-mission5.html” at 2:29:21 am

Wed Mar 04 2009 02:29:21	115514	...	r/rwxrwxrwx	0	0	13347-128-5	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/EVKT0N8H/{mod_poly,mod_dir}[1].js
	122	macb	r/rwxrwxrwx	0	0	13347-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/EVKT0N8H/{mod_poly,mod_dir}[1].js (\$FILE_NAME)
Wed Mar 04 2009 02:29:22	115514	mac.	r/rwxrwxrwx	0	0	13347-128-5	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/EVKT0N8H/{mod_poly,mod_dir}[1].js
Wed Mar 04 2009 02:44:09	568	macb	r/rwxrwxrwx	0	0	13154-128-1	C:/Documents and Settings/Ima Hacker/Recent/hackthissite-mission5.html.lnk
	126	macb	r/rwxrwxrwx	0	0	13154-48-2	C:/Documents and Settings/Ima Hacker/Recent/hackthissite-mission5.html.lnk (\$FILE_NAME)

Picture 29: Timeline about hackthissite-mission5.html

- ii. I found that the suspect was viewing the captured packet by using Fiddler2 at 2:44:20 am

Wed Mar 04 2009 02:44:20	480	macb	d/drwxrwxrwx	0 0	13350-144-1	C:/Documents and Settings/Ima Hacker/My Documents/Fiddler2
	82	macb	d/drwxrwxrwx	0 0	13350-48-2	C:/Documents and Settings/Ima Hacker/My Documents/Fiddler2 (\$FILE_NAME)
	360	macb	d/drwxrwxrwx	0 0	13351-144-1	C:/Documents and Settings/Ima Hacker/My Documents/Fiddler2/Captures
	82	macb	d/drwxrwxrwx	0 0	13351-48-2	C:/Documents and Settings/Ima Hacker/My Documents/Fiddler2/Captures (\$FILE_NAME)
	48	macb	d/drwxrwxrwx	0 0	13352-144-1	C:/Documents and Settings/Ima Hacker/My Documents/Fiddler2/Captures/Requests
	82	macb	d/drwxrwxrwx	0 0	13352-48-2	C:/Documents and Settings/Ima Hacker/My Documents/Fiddler2/Captures/Requests (\$FILE_NAME)
	48	m.cb	d/drwxrwxrwx	0 0	13353-144-1	C:/Documents and Settings/Ima Hacker/My Documents/Fiddler2/Captures/Responses
	84	macb	d/drwxrwxrwx	0 0	13353-48-2	C:/Documents and Settings/Ima Hacker/My Documents/Fiddler2/Captures/Responses (\$FILE_NAME)
	264	...b	d/drwxrwxrwx	0 0	13354-144-1	C:/Documents and Settings/Ima Hacker/My Documents/Fiddler2/Scripts
	80	macb	d/drwxrwxrwx	0 0	13354-48-2	C:/Documents and Settings/Ima Hacker/My Documents/Fiddler2/Scripts (\$FILE_NAME)

Picture 30: Timeline of the fiddler capture

iii. I found that the suspect was browsing “admin.hackthissite” at 2:50:18 am

Wed Mar 04 2009 02:50:18	202	macb	r/rwxrwxrwx	0 0	13361-128-1	C:/Documents and Settings/Ima Hacker/Cookies/ima hacker@admin.hackthissite[1].txt
	138	macb	r/rwxrwxrwx	0 0	13361-48-2	C:/Documents and Settings/Ima Hacker/Cookies/ima hacker@admin.hackthissite[1].txt (\$FILE_NAME)

Picture 31: Timeline about the admin.hackthissite

20. From File Analysis, I found 5 files by using the keyword “hackthissite”

r / r	C:/Documents and Settings/Ima Hacker/Cookies/ima hacker@hackthissite[2].txt	2009-03-04 03:02:09 (AEDT)	2009-03-04 03:02:09 (AEDT)
r / r	C:/Documents and Settings/Ima Hacker/Cookies/ima hacker@admin.hackthissite[1].txt	2009-03-04 02:50:18 (AEDT)	2009-03-04 02:50:18 (AEDT)
r / r	C:/Documents and Settings/Ima Hacker/My Documents/Wireshark/nmap hackthissite.org	2010-01-03 06:19:20 (AEDT)	2010-01-03 06:19:20 (AEDT)
r / r	C:/Documents and Settings/Ima Hacker/Recent /hackthissite-mission4.lnk	2009-03-04 01:49:18 (AEDT)	2010-05-04 23:00:03 (AEST)
r / r	C:/Documents and Settings/Ima Hacker/Recent /hackthissite-mission5.html.lnk	2009-03-04 02:44:09 (AEDT)	2009-03-04 02:44:09 (AEDT)

Picture 32: Files that have been found using the keyword

a. I found the imahacker@admin.hackthissite[1].txt that previously showed in the timeline

Contents Of File: C:/Documents and Settings/Ima Hacker/Cookies/ima hacker@admin.hackthissite[1].txt
phpAds_blockAd[32]
1303767555
admin.hackthissite.org/
1024
3461227392
30147573
1344787712
29989903
*

Picture 33: Content of imahacker@admin.hackthissite[1].txt

b. In the Hex display, I found the original path for “hackthissite-mission4” and “hackthissite-mission5” in the MS shortcut file type

```

000000E0: 1000 0000 0043 3A5C 446F 6375 6D65 6E74 .....C:\Document
000000F0: 7320 616E 6420 5365 7474 696E 6773 5C49 s and Settings\I
00000100: 6D61 2048 6163 6865 725C 4465 7368 746F ma Hacker\Deskto
00000110: 705C 6861 6368 7468 6973 7369 7465 2D6D p\hackthissite-m
00000120: 6973 7369 6F6E 342E 6874 6D6C 0000 2500 ssion4.html..%.

```

```

000000D0: 7500 0000 1100 0000 0300 0000 45C0 EBE8 u.....E...
000000E0: 1000 0000 0043 3A5C 446F 6375 6D65 6E74 .....C:\Document
000000F0: 7320 616E 6420 5365 7474 696E 6773 5C49 s and Settings\I
00000100: 6D61 2048 6163 6865 725C 4465 7368 746F ma Hacker\Deskto
00000110: 705C 6861 6368 7468 6973 7369 7465 2D6D p\hackthissite-m
00000120: 6973 7369 6F6E 352E 6874 6D6C 0000 2500 ssion5.html..%.

```

Pictures 34 & 35: Original Path for “hackthissite-mission”

- c. I navigated to the original file path for both “hackthissite-mission”, and I did not find any files related

r/r	Cain.lnk	01:38:30 (AEST)	02:44:11 (AEST)	01:38:30 (AEST)
		2010-05-04	2010-08-06	2010-05-04
		23:21:50 (AEST)	00:56:36 (AEST)	23:21:50 (AEST)
r/r	Hacked_Notification.jpg	2010-08-06	2010-08-06	2010-08-06
		01:38:32 (AEST)	01:38:36 (AEST)	01:38:36 (AEST)
r/r	Hacked_Notification.jpg:Zone.Identifier	2010-08-06	2010-08-06	2010-08-06
		01:38:32 (AEST)	01:38:36 (AEST)	01:38:36 (AEST)
r/r	Nmap - Zenmap GUI.lnk	2009-06-13	2010-08-06	2009-06-13
		00:16:51 (AEST)	00:56:36 (AEST)	00:16:51 (AEST)

Picture 36: No file that contains hackthissite-mission

- d. I navigated to the C:/RECYCLER/S-1-5-21-1935655697-1757981266-725345543-1003/ INFO2, and I found the deleted “hackthissite-mission” files.

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * Add Note	
File Type: Windows Recycle Bin INFO2 file (Win2k - WinXP)	
Hex Contents Of File: C:/RECYCLER/S-1-5-21-1935655697-1757981266-725345543-1003/INFO2	
00000000: 0500 0000 2200 0000 2200 0000 2003 0000"....
00000010: E85D AA03 433A 5C44 6F63 756D 656E 7473	..C:\Documents
00000020: 2061 6E64 2053 6574 7469 6E67 735C 496D	and Settings\Im
00000030: 6120 4861 6368 6572 5C44 6573 6874 6F70	a Hacker\Desktop
00000040: 5C68 6163 6874 6869 7373 6974 652D 6D69	\hackthissite-mi
00000050: 7373 696F 6E34 2E68 746D 6C00 0000 0000	ssion4.html.....
00000060: 0000 0000 0000 0000 0000 0000 0000 0000

```

00000970: 0000 0000 433A 5C44 6F63 756D 656E 7473 ....C:\Documents
00000980: 2061 6E64 2053 6574 7469 6E67 735C 496D and Settings\Im
00000990: 6120 4861 6368 6572 5C44 6573 6874 6F70 a Hacker\Desktop
000009A0: 5C68 6163 6874 6869 7373 6974 652D 6D69 \hackthissite-mi
000009B0: 7373 696F 6E35 2E68 746D 6C00 0000 0000 ssion5.html.....

```

Pictures 37 & 38: Original Path for hackthissite-mission in INFO2

21. I found 5 files by using the keyword “fiddler” and I navigated to “C:/Documents and Settings/ Ima Hacker/ My Documents/Fiddler2Captures”. There are no documents inside the Requests and Responses folder.

Current Directory: [C:/ /Documents and Settings/ /Ima Hacker/ /My Documents/ /Captures/](#)

[ADD NOTE](#) [GENERATE MD5 LIST OF FILES](#)

DEL	Type dir / in	NAME	WRITTEN	ACCESSED
	d / d	../	2009-03-04 02:44:20 (AEDT)	2009-03-04 02:44:20 (AEDT)
	d / d	../	2009-03-04 02:44:20 (AEDT)	2009-03-04 02:44:20 (AEDT)
	d / d	Requests/	2009-03-04 02:44:20 (AEDT)	2009-03-04 02:44:20 (AEDT)
	d / d	Responses/	2009-03-04 02:44:20 (AEDT)	2009-03-04 02:59:03 (AEDT)

Picture 39: No documents inside either folder

4.3 Scenario 3 – Unauthorised access to Facebook

22. I typed the ID 100002369565636 in the search bar and found a picture that is the same as Exhibit 2.


DEL	Type dir / in	NAME	WRITTEN
	r / r	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/UDM5CTEP/211272_100002369565636_3948015_n[1].jpg	2010-08-06 01:38:47 (AEST)

ASCII ([display - report](#)) * Hex ([display - report](#)) * ASCII Strings ([display - report](#))

File Type: JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment

C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/UDM5CTEP/211272_100002369565636_3948015_n[1].jpg

Thumbnail: [View Full Size Image](#)



Picture 40: Result after searching with ID

23. I used the search function to find related files by typing “Brisbane”

DEL	Type dir / in	NAME	WRITTEN	ACCESSED	CHANGED
	d / d	C:/Documents and Settings/Ima Hacker/My Documents/Brisbane 2010	2010-10-14 03:10:57 (AEDT)	2010-10-14 03:10:57 (AEDT)	2010-10-14 03:10:57 (AEDT)
	r / r	C:/Documents and Settings/Ima Hacker/Recent/Brisbane 2010.lnk	2010-10-14 03:12:27 (AEDT)	2010-10-14 03:12:27 (AEDT)	2010-10-14 03:12:27 (AEDT)

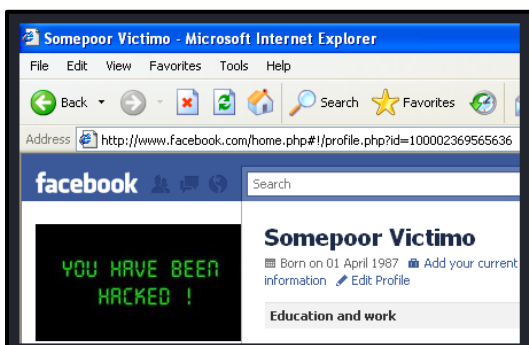
Picture 41: Result after searching withBrisbane

- a. I navigated to C:/Documents and Settings/Ima Hacker/ Brisbane2010 and found three files.

DEL	Type	NAME	WRITTEN	ACCESSED	CHANGED	CREATED	SIZE	UID	GID	META
	dir / in									
	d / d	..	2010-07-30 00:18:56 (AEST)	2010-10-14 02:43:59 (AEDT)	2010-07-30 00:18:56 (AEST)	2009-02-16 04:02:15 (AEDT)	56	0	0	10274-144-6
	d / d	.	2010-10-14 03:10:57 (AEDT)	2010-10-14 03:10:57 (AEDT)	2010-10-14 03:10:57 (AEDT)	2010-07-30 00:18:51 (AEST)	56	0	0	16727-144-8
	r / r	hotel_dump_including_email_and_facebook.pcap	2010-08-06 01:24:09 (AEST)	2010-10-14 02:44:40 (AEDT)	2010-10-14 02:44:42 (AEDT)	2010-08-06 01:24:08 (AEST)	24135176	0	0	16141-128-4
	r / r	hotel_dump.pcap	2010-07-30 00:19:05 (AEST)	2010-10-14 03:09:55 (AEDT)	2010-10-14 03:09:55 (AEDT)	2010-07-30 00:19:05 (AEST)	7626338	0	0	16728-128-4
	r / r	victim's facebook.bmp	2010-08-06 01:40:05 (AEST)	2010-10-14 02:44:32 (AEDT)	2010-08-06 01:40:05 (AEST)	2010-08-06 01:40:05 (AEST)	364986	0	0	17314-128-4

Picture 42: Files show in directory

- b. I exported "victim's_facebook.bmp" and opened it with the image viewer. I found that Exhibit 2 was a part of the picture.



Picture 43: Somepoor Victim Facebook has been hacked

- c. I exported hotel_dump.pcap and opened it with Wireshark
- I applied a filter: dhcp
 - The suspect's machine was already operating with IP 192.168.17.129 and issued a DHCP Inform at 2010-07-29 10:05:38, indicating active use of this address.

dhcp										
No.	Time	Source	Destination	Protocol	Length	Info				
1	2010-07-29 10:04:32.395536	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x16bf0ca7				
5	2010-07-29 10:04:33.404050	192.168.17.254	192.168.17.130	DHCP	342	DHCP Offer - Transaction ID 0x16bf0ca7				
6	2010-07-29 10:04:33.416140	0.0.0.0	255.255.255.255	DHCP	350	DHCP Request - Transaction ID 0x16bf0ca7				
7	2010-07-29 10:04:33.416624	192.168.17.254	192.168.17.130	DHCP	342	DHCP ACK - Transaction ID 0x16bf0ca7				
44	2010-07-29 10:05:38.669926	192.168.17.129	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xe8053c33				
45	2010-07-29 10:05:38.670841	192.168.17.254	192.168.17.129	DHCP	342	DHCP ACK - Transaction ID 0xe8053c33				
60	2010-07-29 10:05:42.658134	192.168.17.129	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xe8053c33				
61	2010-07-29 10:05:42.658354	192.168.17.254	192.168.17.129	DHCP	342	DHCP ACK - Transaction ID 0xe8053c33				
16054	2010-07-29 10:17:06.354319	192.168.17.128	192.168.17.254	DHCP	342	DHCP Request - Transaction ID 0x6a2d835b				
16055	2010-07-29 10:17:06.354437	192.168.17.254	192.168.17.128	DHCP	342	DHCP ACK - Transaction ID 0x6a2d835b				

Picture 44: DHCP traffic in the packet file

- d. I exported hotel_dump_including_email_and_facebook.pcap and opened it with Wireshark
- I applied filter: http.cookie contains "c_user=100002369565636" and http.host contains "facebook", and found that the session was hijacked by the suspect

http.cookie contains "c_user=100002369565636" and http.host contains "facebook"						
No.	Time	Source	Destination	Protocol	Length	Info
47086	2010-08-05	11:20:36.209180	192.168.17.129	69.171.224.42	HTTP	585 GET /update_security_info.php HTTP/1.1
47157	2010-08-05	11:20:37.158286	192.168.17.129	69.171.224.42	HTTP	569 GET /images/icons/email.png HTTP/1.1
47209	2010-08-05	11:20:37.434349	192.168.17.129	69.171.224.42	HTTP	572 GET /images/icons/verified.gif HTTP/1.1
47330	2010-08-05	11:20:37.701258	192.168.17.129	69.171.224.42	HTTP	573 GET /images/cc_logos/secure.png HTTP/1.1
47375	2010-08-05	11:20:38.199968	192.168.17.129	220.233.2.219	HTTP	739 GET /common/history_manager.php? index=0 HTTP/1.1
47418	2010-08-05	11:20:46.073326	192.168.17.129	69.171.224.42	HTTP	1151 GET /home.php HTTP/1.1
47489	2010-08-05	11:20:55.118071	192.168.17.129	69.171.224.42	HTTP	630 GET /images/wizard/nuxwizard_profile_picture.gif HTTP/1.1
47545	2010-08-05	11:20:55.401371	192.168.17.129	69.171.224.42	HTTP	620 GET /images/welcome/welcome_mobile.png HTTP/1.1
47750	2010-08-05	11:20:56.689039	192.168.17.129	69.171.224.42	HTTP	620 GET /ajax/contextual_help.php?_a=1&set_name=global HTTP/1.1
47756	2010-08-05	11:20:57.103908	192.168.17.129	69.171.224.42	HTTP	621 GET /ajax/contextual_help.php?_a=1&set_name=welcome HTTP/1.1
47760	2010-08-05	11:20:57.363464	192.168.17.129	69.171.224.42	HTTP	163 POST /ajax/autoset_timezone_ajax.php?__a=1 HTTP/1.1 (application/x-www-form-urlencoded)

Picture 45: Sessions that have been hijacked by the suspect

- ii. I applied filter: frame contains "@yahoo.com" and found out the suspect already compromised the somepoorvictim@yahoo.com.au

frame contains "@yahoo.com"						
No.	Time	Source	Destination	Protocol	Length	Info
46040	2010-08-05	11:18:16.241980	192.168.17.129	69.147.94.41	POP	88 C: USER somepoorvictim@yahoo.com.au
46054	2010-08-05	11:18:17.837700	69.147.94.41	192.168.17.129	POP	1126 S: +OK 10469 octets
46065	2010-08-05	11:18:18.048671	69.147.94.41	192.168.17.129	POP	738 S: DATA fragment, 684 bytes
46081	2010-08-05	11:18:19.074047	69.147.94.41	192.168.17.129	POP	590 S: +OK 8938 octets
46090	2010-08-05	11:18:19.082781	69.147.94.41	192.168.17.129	POP	590 S: DATA fragment, 536 bytes
46108	2010-08-05	11:18:19.706904	69.147.94.41	192.168.17.129	POP	590 S: +OK 13915 octets
46117	2010-08-05	11:18:19.715615	69.147.94.41	192.168.17.129	POP	590 S: DATA fragment, 536 bytes
46124	2010-08-05	11:18:19.722248	69.147.94.41	192.168.17.129	POP	590 S: DATA fragment, 536 bytes
46147	2010-08-05	11:18:20.358533	69.147.94.41	192.168.17.129	POP	1514 S: +OK 11042 octets
46153	2010-08-05	11:18:20.363938	69.147.94.41	192.168.17.129	POP	1126 S: DATA fragment, 1072 bytes
46156	2010-08-05	11:18:20.365867	69.147.94.41	192.168.17.129	POP	590 S: DATA fragment, 536 bytes
46933	2010-08-05	11:20:12.325284	192.168.17.129	69.147.94.41	POP	88 C: USER somepoorvictim@yahoo.com.au
46952	2010-08-05	11:20:13.846106	69.147.94.41	192.168.17.129	POP	590 S: +OK 4472 octets
46961	2010-08-05	11:20:13.853690	69.147.94.41	192.168.17.129	POP	590 S: DATA fragment, 536 bytes

Picture 46: Post Office Protocol file

24. From the timeline analysis, I set the time to August 2010, as mentioned, the unauthorised access to Facebook happened on 6th August 2010
- a. I found the suspect executed the Nmap tools for port scanning on 6th August 2010, 12:52:30 am

Fri Aug 06	650	...	r/rwxrwxrwx	0 0	15165-128-4	C:/Documents and Settings/Ima Hacker/Start Menu/Programs/Nmap/Nmap - Zenmap GUI.lnk
2010 00:52:30						

Picture 47: Timeline of Nmap tools being used

- b. I found the suspect had downloaded the Firesheep, which is used for session hijacking, on 6th August 2010, 12:55:46 am

Fri Aug 06	104	...	r/rwxrwxrwx	0 0	16766-48-7	C:/Documents and Settings/Ima Hacker/My Documents/Downloads/firesheep-0.1-1.xpi (\$FILE_NAME)
2010 00:55:46						

Picture 48: Firesheep download by the suspect

- c. I found the hotel_dump_including_email_and_facebook.pcap created on 6th August 2010, 1:24:08 am

Fri Aug 06 2010 01:24:08	814	...	r/rwxrwxrwx	0 0	11123-128-4	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/CJIP4PUH/nopic_64[1].gif
	28805	...	r/rwxrwxrwx	0 0	11158-128-4	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/UDM5CTEP/CA89EBO1.css
	42	macb	r/rwxrwxrwx	0 0	15553-128-1	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/EVKTON8H/Blank_1x1[1].gif
	98	macb	r/rwxrwxrwx	0 0	15553-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/EVKTON8H/Blank_1x1[1].gif (\$FILE_NAME)
	7808	macb	r/rwxrwxrwx	0 0	16139-128-5	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/IZQDEYTP/uh_utils-1.3.0[1].js
	106	macb	r/rwxrwxrwx	0 0	16139-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/IZQDEYTP/uh_utils-1.3.0[1].js (\$FILE_NAME)
	729	macb	r/rwxrwxrwx	0 0	16140-128-4	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/UDM5CTEP/c8ad9845c9414424cb5854238af212b0_1[1].gif
	148	macb	r/rwxrwxrwx	0 0	16140-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/UDM5CTEP/c8ad9845c9414424cb5854238af212b0_1[1].gif (\$FILE_NAME)
	24135176	...b	r/rwxrwxrwx	0 0	16141-128-4	C:/Documents and Settings/Ima Hacker/My Documents/Brisbane 2010/hotel dump including email and facebook.pcap
	154	macb	r/rwxrwxrwx	0 0	16141-48-2	C:/Documents and Settings/Ima Hacker/My Documents/Brisbane 2010/hotel dump including email and facebook.pcap (\$FILE_NAME)

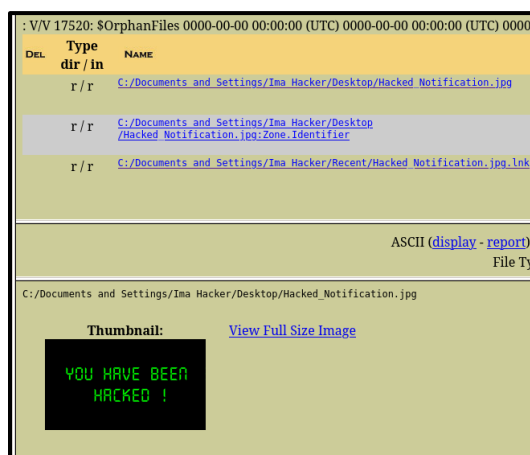
Picture 49: Timeline of the Packet file created

- d. I found the file that showed “You’ve been hacked!” and the Hacked_Notification.jpg on 6th August 2010, 1:33:51 am

Fri Aug 06 2010 01:33:44	152	...	d/rwxrwxrwx	0 0	15771-144-1	C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/PAWNED, again!.files
Fri Aug 06 2010 01:33:51	883	...b	r/rwxrwxrwx	0 0	16946-128-4	C:/Documents and Settings/Ima Hacker/Recent/You've been hacked! - Inbox - 'Yahoo!7 Mail'.htm.lnk
	170	...b	r/rwxrwxrwx	0 0	16946-48-2	C:/Documents and Settings/Ima Hacker/Recent/You've been hacked! - Inbox - 'Yahoo!7 Mail'.htm.lnk (\$FILE_NAME)

	41504	...b	r/rwxrwxrwx	0 0	17275-128-4	C:/Documents and Settings/Ima Hacker/Desktop/Hacked_Notification.jpg
	26	...b	r/rwxrwxrwx	0 0	17275-128-5	C:/Documents and Settings/Ima Hacker/Desktop/Hacked_Notification.jpg:Zone.Identifier
	112	macb	r/rwxrwxrwx	0 0	17275-48-2	C:/Documents and Settings/Ima Hacker/Desktop/Hacked_Notification.jpg (\$FILE_NAME)
	553	...b	r/rwxrwxrwx	0 0	17276-128-1	C:/Documents and Settings/Ima Hacker/Recent/Hacked_Notification.jpg.lnk
	120	...b	r/rwxrwxrwx	0 0	17276-48-2	C:/Documents and Settings/Ima Hacker/Recent/Hacked_Notification.jpg.lnk (\$FILE_NAME)

Pictures 50 & 51: Timeline of the Picture and file that same as in Exhibit 2



Picture 52: Hack_Notification.jpg

- e. I found the suspect viewed the same image associated with the account, proving the profile was accessed on 6th August 2010, 1:38:47 am

Fri Aug 06 2010 01:38:46	6374	...b	r/rwxrwxrwx	0 0	17283-128-4	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/UDM5CTEP/211272_100002369565636_3948015_n[1].jpg
	144	macb	r/rwxrwxrwx	0 0	17283-48-2	C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/UDM5CTEP/211272_100002369565636_3948015_n[1].jpg (\$FILE_NAME)

Picture 53: Timeline of the suspect accessing the victim's account

- f. I found the “victim’s facebook.bmp” on 6th August 2010, 1:40:05 am

Fri Aug 06 2010 01:40:05	464	ma..	r/rtwxrwxrwx	0 0	17118-128-1	C:/System Volume Information/_restore{B6B28996-CAB8-4AFC-A54A-607873F6C717}/RP4/A0000179.lnk
	90	mac.	r/rtwxrwxrwx	0 0	17118-48-4	C:/System Volume Information/_restore{B6B28996-CAB8-4AFC-A54A-607873F6C717}/RP4/A0000179.lnk (\$FILE_NAME)
	748	...b	r/rtwxrwxrwx	0 0	17202-128-4	C:/Documents and Settings/Ima Hacker/Recent/victim's facebook.bmp.lnk
	116	...b	r/rtwxrwxrwx	0 0	17202-48-2	C:/Documents and Settings/Ima Hacker/Recent/victim's facebook.bmp.lnk (\$FILE_NAME)
	364986	m.cb	r/rtwxrwxrwx	0 0	17314-128-4	C:/Documents and Settings/Ima Hacker/My Documents/Brisbane 2010/victim's facebook.bmp
	108	mach	r/rtwxrwxrwx	0 0	17314-48-2	C:/Documents and Settings/Ima Hacker/My Documents/Brisbane 2010/victim's facebook.bmp (\$FILE_NAME)
	760	ma.b	r/rtwxrwxrwx	0 0	17315-128-4	C:/System Volume Information/_restore{B6B28996-CAB8-4AFC-A54A-607873F6C717}/RP4/A0000178.lnk
	90	mach	r/rtwxrwxrwx	0 0	17315-48-5	C:/System Volume Information/_restore{B6B28996-CAB8-4AFC-A54A-607873F6C717}/RP4/A0000178.lnk (\$FILE_NAME)

Picture 54: Timeline of victim's facebook.bmp

4.4 Scenario 4 - Find the collaborator with the suspect

25. Back to the Kali terminal, I ran the command "`cd /mnt/Kali-share/windows_mount`" to change into the directory where I mounted the forensic image.
26. searched the files named *.pst or *.dbx in the email databases on the suspect computer to find the email between the suspect and the collaborator.
 - a. By running the command "`find -iname "*.dbx" -o -iname "*.pst"`", I located some email databases in the "Ima Hacker" folder.

```
(kali@kali)~/mnt/Kali-share/windows_mount
$ find -iname "*.dbx" -o -iname "*.pst"
./Documents and Settings/Ima Hacker/Local Settings/Application Data/Identities/{6FE73E6F-28AF-4574-90D1-A0B477E9D564}/Microsoft/Outlook Express/Deleted Items.dbx
./Documents and Settings/Ima Hacker/Local Settings/Application Data/Identities/{6FE73E6F-28AF-4574-90D1-A0B477E9D564}/Microsoft/Outlook Express/Drafts.dbx
./Documents and Settings/Ima Hacker/Local Settings/Application Data/Identities/{6FE73E6F-28AF-4574-90D1-A0B477E9D564}/Microsoft/Outlook Express/Folders.dbx
./Documents and Settings/Ima Hacker/Local Settings/Application Data/Identities/{6FE73E6F-28AF-4574-90D1-A0B477E9D564}/Microsoft/Outlook Express/Inbox.dbx
./Documents and Settings/Ima Hacker/Local Settings/Application Data/Identities/{6FE73E6F-28AF-4574-90D1-A0B477E9D564}/Microsoft/Outlook Express/Offline.dbx
./Documents and Settings/Ima Hacker/Local Settings/Application Data/Identities/{6FE73E6F-28AF-4574-90D1-A0B477E9D564}/Microsoft/Outlook Express/Outbox.dbx
./Documents and Settings/Ima Hacker/Local Settings/Application Data/Identities/{6FE73E6F-28AF-4574-90D1-A0B477E9D564}/Microsoft/Outlook Express/Pop3uidl.dbx
./Documents and Settings/Ima Hacker/Local Settings/Application Data/Identities/{6FE73E6F-28AF-4574-90D1-A0B477E9D564}/Microsoft/Outlook Express/Sent Items.dbx
```

Picture 55: Email databases are located

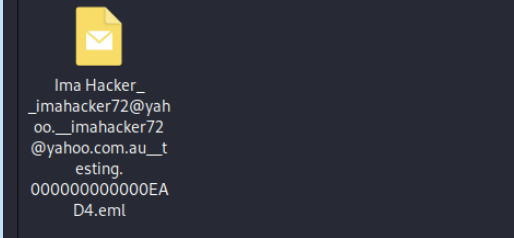
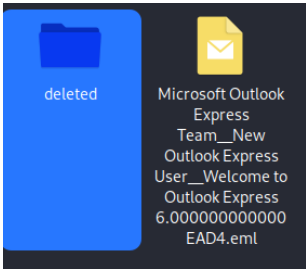
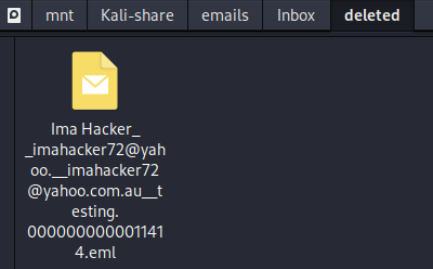
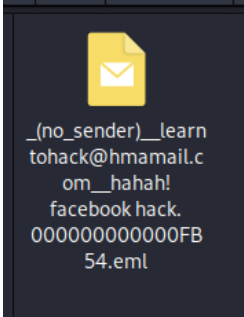
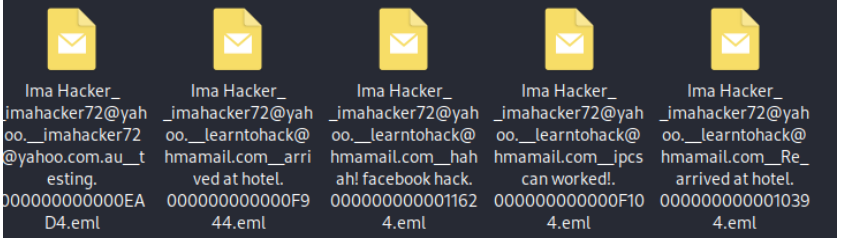
27. I used the undbx tools to extract the contents
 - b. I created a new directory by running the command "`mkdir /mnt/Kali-share/emails`"
 - c. I installed the undbx tools by running the command "`sudo apt install undbx`"
 - d. I extracted the individual emails from the .dbx files by running the command "`undbx -r /mnt/Kali-share/windows_mount/Documents\ and\ Settings/Ima\ Hacker/Local\ Settings/Application\ Data/Identities/{6FE73E6F-28AF-4574-90D1-A0B477E9D564}/Microsoft/Outlook\ Express /mnt/Kali-share/emails`"

```
UnDBX v0.21 (Dec 26 2022)
Scanning Deleted Items.dbx: 100.0%
Recovering 1 deleted message fragments with offset 0 from Deleted Items.dbx to /mnt/Kali-share/emails/Deleted Items/deleted: 100.0%
1 deleted message fragments recovered, 0 errors
Scanning Drafts.dbx: 100.0%
Scanning Folders.dbx: 100.0%
Scanning Inbox.dbx: 100.0%
Recovering 1 messages with offset 0 from Inbox.dbx to /mnt/Kali-share/emails/Inbox: 100.0%
1 messages recovered, 0 errors
Recovering 1 deleted message fragments with offset 0 from Inbox.dbx to /mnt/Kali-share/emails/Inbox/deleted: 100.0%
1 deleted message fragments recovered, 0 errors
Scanning Offline.dbx: 100.0%
Scanning Outbox.dbx: 100.0%
Recovering 1 deleted message fragments with offset 0 from Outbox.dbx to /mnt/Kali-share/emails/Outbox/deleted: 100.0%
1 deleted message fragments recovered, 0 errors
Scanning Pop3uidl.dbx: 100.0%
Scanning Sent Items.dbx: 100.0%
Recovering 5 messages with offset 0 from Sent Items.dbx to /mnt/Kali-share/emails/Sent Items: 100.0%
5 messages recovered, 0 errors
Extracted 8 out of 8 DBX files
```

Picture 56: Extracted the individual emails

28. I used the GUI to navigate to the path `/mnt/Kali-share/emails` to view the extracted files.

a. Output:

Directory	Files inside the directory
Deleted Item/deleted	<div>mnt Kali-share emails Deleted Items deleted</div> 
Drafts	None
Folders	None
Inbox	<div>mnt Kali-share emails Inbox deleted</div>  
Offline	None
Outbox/deleted	
Pop3uidl	none
Sent Item	<div>mnt Kali-share emails Sent Items</div> 

29. I found that the suspect had sent 4 emails to the same email address, which is `learntohack@hmamail.com`, which is the collaborator who uses the website `hidemyass.com`

- a. The first email showed the suspect arrived at the Brisbane hotel on 30 July 2010, 00:18:35

```
From: "Ima Hacker" <imahacker72@yahoo.com.au>
To: <learntohack@hmamail.com>
Subject: arrived at hotel
Date: Fri, 30 Jul 2010 00:18:35 +1000
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="-----_NextPart_000_0008_01CB2F7C.C0377060"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

This is a multi-part message in MIME format.

-----_NextPart_000_0008_01CB2F7C.C0377060
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Hey,

Just got to the hotel in brissie and connected my pc - looks like =
they're only using a network hub! I can see everyone else's traffic, =
it's awesome!

Looks like one guy is working going to be on the gold coast, soon - =
judging by his browsing history!

Might try that firesheep thing you were telling me about later, see if I =
can get into any accounts!
```

From:	imahacker72@yahoo.com.au>
To:	learntohack@hmamail.com
Subject:	arrived at hotel
Date:	Fri, 30 July 2010 00:18:35 +1000 (AEST)
Content-Type:	multipart/alternative
Email Client:	Microsoft Outlook Express 6.00

Table 2: Metadata

- b. The second email related to scenario 3, which showed that the suspect had compromised the victim's Facebook account

```

From: "Ima Hacker" <imahacker72@yahoo.com.au>
To: <learntohack@hmamail.com>
Subject: hahah! facebook hack
Date: Fri, 6 Aug 2010 01:41:25 +1000
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="-----_NextPart_000_0003_01CB3508.7B0EF760"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

This is a multi-part message in MIME format.

-----=_NextPart_000_0003_01CB3508.7B0EF760
Content-Type: multipart/alternative;
        boundary="-----_NextPart_001_0004_01CB3508.7B0EF760"

-----=_NextPart_001_0004_01CB3508.7B0EF760
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

pwned the guys facebook, too... so easy to reset passwords once you've =
got access to their email.

```

From:	imahacker72@yahoo.com.au>
To:	learntohack@hmamail.com
Subject:	hahah! facebook hack
Date:	Fri, 6 Aug 2010 01:41:25 +1000 (AEST)
Content-Type:	multipart/mixed
Email Client:	Microsoft Outlook Express 6.00

Table 3: Metadata

- c. The third email is related to scenario 1, which showed the suspect has compromised the hackable company web server

```

From: "Ima Hacker" <imahacker72@yahoo.com.au>
To: <learntohack@hmamail.com>
Subject: ipcsan worked!
Date: Tue, 4 May 2010 23:30:35 +1000
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="-----_NextPart_000_0006_01CAEBE1.CBB92D40"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

This is a multi-part message in MIME format.

-----=_NextPart_000_0006_01CAEBE1.CBB92D40
Content-Type: text/plain;
        charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Hey, ipcsan worked!

I got into that hackable server. I can't believe their backup password =
was "backup"! how lame...

```


From:	imahacker72@yahoo.com.au>
To:	learntohack@hmamail.com
Subject:	ipscan worked
Date:	Tue, 4 May 2010 23:30:35 +1000 (AEST)
Content-Type:	Multipart/alternative
Email Client:	Microsoft Outlook Express 6.00

Table 4: Metadata

- d. The fourth email is related to scenario 3, which showed the suspect planning to hijack someone's account

```

From: "Ima Hacker" <imahacker72@yahoo.com.au>
To: <learntohack@hmamail.com>
Subject: Re: arrived at hotel
Date: Fri, 6 Aug 2010 01:28:24 +1000
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="-----_NextPart_000_0008_01CB3506.A9AACC90"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.2180
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2180

This is a multi-part message in MIME format.

-----_NextPart_000_0008_01CB3506.A9AACC90
Content-Type: text/plain;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

Don't know what's wrong with that firesheep program - couldn't get it to =
work. It picked up some guy logging into yahoo, but came up with "error" =
and didn't let me hijack his session.

Maybe it only works on wifi?

Still, he also checked his email via pop, so scored his password that =
way!

Some people are so dumb!

```

From:	imahacker72@yahoo.com.au>
To:	learntohack@hmamail.com
Subject:	Re: arrived at hotel
Date:	Fri, 6 Aug 2010 01:28:24 +1000 (AEST)
Content-Type:	Multipart/alternative
Email Client:	Microsoft Outlook Express 6.00

Table 5: Metadata

5. Forensic Report

ICT30010 – Capstone Forensic Investigation Report

Subject: Imanuel Leet-Hacker (aka Ima Hacker)

Investigator: Wong Jin Tao

Date of Investigation: 28 June 2025

Image Analysed: ImaHacker.E01

1. Introduction

This report presents the findings from a digital forensic investigation into a series of cyber incidents attributed to Imanuel Leet-Hacker, known online as "Ima Hacker." The investigation involved analysis of a forensic image of the suspect's system and addressed four key allegations:

- A defacement of **Hackable.com.au** on **4 May 2010**
- An alleged second website attack on **4 March 2009**
- A **Facebook account takeover** traced to a Brisbane hotel on **6 August 2010**
- Suspected **communication with a collaborator** using a **hidemyass.com** email dropbox

Each scenario has been investigated with digital evidence recovered and analysed using professional forensic tools. This report outlines all findings, including timelines, recovered artefacts, and analysis conclusions.

2. Evidence & Chain of Custody

Received from Police:

- **Disk image:** ImaHacker.E01 (MD5 verified)
- **Exhibit 1:** Screenshot of hacked Hackable.com.au web server
- **Exhibit 2:** Image placed on the victim's Facebook page
- **Timeline file:** timeline.csv (MD5: 9574ac771fdeeeb9a95d8dda5ed1749a)

Received from Colleague, Troy:

- A "Super Timeline" (Timescanner output) provided by colleague Troy via email.

Chain of Custody:

Upon receipt, all evidence was transferred to a secure forensic workstation with read-only access. The MD5 hash of the ImaHacker.E01 file was verified using `ewfverify`, confirming file integrity. The image was mounted using `ewfmount`, and partition analysis was conducted using

mmls. Throughout the investigation, artefacts were handled according to digital forensic best practices to preserve metadata and ensure admissibility of evidence in court.

3. Tools and Methodology

3.1 Partition and Time Zone Information

- Partition information was retrieved using mmls to determine the partition of the disk image, and the relevant NTFS partition (002) was mounted using the appropriate offset for analysis.

Partition Number	Partition Type	Start Sector	End Sector	Total Sector	Total Size (MB)
000	Primary Table	00	00	1	0.00049
001	Unallocated	00	62	63	0.031
002	NTFS/ exFaT	63	41913584	41913522	20465.59
003	Unallocated	41913585	41943039	29455	14.38

Table 6: Partition in disk image

- The timezone of the suspect's system was identified using the RegRipper tool on the system registry hive. The output confirmed the system was configured to **AUS Eastern Standard Time (AEST)**, which corresponds to UTC+10:00. All timestamps in this investigation were interpreted accordingly to match the local settings of the suspect's machine.
- The following forensic tools and techniques were employed:
 - Disk Imaging & Mounting:** ewfinfo, ewfverify, mmls, mount
 - Timeline Analysis:** Autopsy timeline tool and Timescanner CSV
 - Registry Analysis:** RegRipper
 - Network Capture Analysis:** Wireshark with filters (http.cookie, frame contains)
 - Email Extraction:** undbx for .dbx recovery
 - Keyword Searches:** Terms like facebook, hackable, Brisbane, hackthissite

4. Forensic Analysis

4.1 Scenario 1 – Hackable.com.au Defacement (4 May 2010)

Evidence and Timeline:

- An HTML file named **PAWNED, again!.htm** was discovered at C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/.

- The contents of this file matched the defaced version of Hackable.com.au shown in Exhibit 1. Also located in the same folder was a **win2000.gif** image, which was visually consistent with the image on the hacked web page.
- A **users.txt** file containing usernames was found in the same directory. This file likely contains account credentials harvested from the compromised server.
- Further artefacts uncovered include two Zenmap files: **recent_scans.txt** and **target_list.txt**, indicating that the suspect performed reconnaissance on **server.hackable.com.au**. A port scan configuration file **server.hackable.com.au.xml** was generated shortly afterwards.
- **recent_scans.txt** and **target_list.txt**, indicating that the suspect performed reconnaissance on **server.hackable.com.au**. A port scan configuration file **server.hackable.com.au.xml** was generated shortly afterwards.
- Autopsy's timeline tool showed the following sequence:
 - 22:40 – Zenmap (zenmap.exe) was launched.
 - 22:46 – server.hackable.com.au.xml created.
 - 23:30 – Email sent referencing successful scan.
 - 23:32 – users.txt accessed.
 - 23:35 – PAWNED, again!.htm file opened.

Analysis:

- This sequence demonstrates clear progression from reconnaissance to defacement. The timestamped file creation and access history corresponds with the system tools used. Additionally, an email sent to **learntohack@hmamail.com** included phrases referencing the scan results, confirming that the suspect reported the success to a collaborator.

Conclusion:

- The evidence confirms that the suspect performed reconnaissance using Zenmap, created and accessed files used in the website defacement, and communicated the success of the operation.

4.2 Scenario 2 – Website Attack (4 March 2009, 2:22 AM)

Evidence and Timeline:

- **No direct activity** occurred at the exact time of the alleged attack (2:22 AM).
- However, the timeline surrounding this event suggests the system was in active use:
 - **01:48–01:59** – Access to hackthissite missions, blackhatworld, and Stack Overflow.
 - **01:59** – Fiddler tool launched, indicating network traffic analysis.
 - **02:29** – Next recorded activity with hackthissite-mission5.html accessed
- Deleted artefacts in the `C:/RECYCLER/INFO2` confirmed the previous existence of files such as hackthissite-mission4 and hackthissite-mission5.

Analysis:

- The active usage of hacking-related websites and tools before and after 2:22 AM strongly suggests that the system was not idle.
- No evidence was found to support the claim that the user was absent or the machine was shut down during the window in question.

Conclusion:

- Although there is no exact activity at 2:22 AM, continuous system usage before and after, combined with the nature of accessed content, disputes the suspect's alibi of being elsewhere at the time.

4.3 Scenario 3 – Unauthorised access to Facebook account

Evidence and Timeline:

- The investigation revealed that `victim's_facebook.bmp` matched the altered image shown in Exhibit 2. The image was found in a folder labelled `Brisbane2010`, which also contained packet capture files `hotel_dump.pcap` and `hotel_dump_including_email_and_facebook.pcap`.
- Network logs showed:
 - **29 July 2010, 10:05:38** – DHCP INFORM from suspect's device (IP 192.168.17.129), proving device use at the hotel.
 - **6 August 2010, 00:55** – Firesheep downloaded (a session hijacking tool).
 - **6 August 2010, 01:24** – PCAP containing Facebook session cookies (`c_user`, `xs`) created.
 - **6 August 2010, 01:33–01:38** – Access to the victim's profile and creation of an edited image.
 - **6 August 2010, 01:41** – Email sent to `learntohack@hmamail.com` with subject: "hahah! Facebook hack"

Analysis

- Firesheep enables the interception of unsecured HTTP cookies to hijack sessions. The session cookies for the victim's Facebook account were captured and used to access the account without login credentials. The rapid sequence from tool download to PCAP creation, image editing, and email reporting further supports the allegation.

Conclusion:

- Digital evidence, including PCAP analysis, session hijacking tools, and resulting artefacts, confirms that the suspect hijacked a Facebook session and posted unauthorised content.

4.4 Collaborator Communications (hidemyass.com)

Evidence and Timeline:

- Using undbx, Outlook Express .dbx email files were extracted and reviewed. Four key emails were found sent from **imahacker72@yahoo.com.au** to **learntohack@hmamail.com**:
 - **30 July 2010, 00:18** – "Arrived at hotel" — confirms presence in Brisbane.
 - **4 May 2010, 23:30** – "ipscan worked" — refers to a successful Hackable scan.
 - **6 August 2010, 01:28** – Planning message for session hijack.
 - **6 August 2010, 01:41** – Confirmation of Facebook hack
- Each email had metadata confirming timestamps, content, and the identity of the sender and recipient.

Analysis

- The emails align precisely with key events in each scenario. The subject lines and timing match known activities. The use of hmamail.com, an anonymising email service, further suggests intent to conceal identity and coordination between the suspect and collaborator.

Conclusion:

- Consistent, timestamped communication referencing each incident confirms collaboration. The suspect used an email to coordinate and report activities.

5. Overall Conclusion

The forensic investigation confirms the involvement of the suspect in multiple unauthorised activities:

- The defacement of Hackable.com.au using tools and artefacts present on the system.
- A questionable alibi for the 4 March 2009 attack, undermined by adjacent system activity.
- Unauthorised access to a Facebook account using Firesheep and network session hijacking.
- Ongoing, real-time collaboration with an associate via email, directly referencing each incident.

All findings are supported by a combination of file system evidence, network analysis, and email communications. Evidence integrity was maintained throughout the investigation, making this report suitable for legal proceedings.

6. Glossary

- **PCAP:** Packet Capture file, used to store network traffic data.
- **Firesheep:** A network analysis tool used to hijack web sessions over unencrypted Wi-Fi.
- **RegRipper:** A tool used to extract and analyse Windows registry data.
- **Zenmap/Nmap:** Network scanning tools used to map hosts and services.
- **E01:** A forensic disk image format, also known as Expert Witness Format.
- **MD5 Hash:** A unique value used to verify file integrity.
- **.dbx:** Microsoft Outlook Express email storage file.
- **Autopsy:** A digital forensics platform for disk image analysis.
- **DHCP INFORM:** A message sent by a client to obtain local network configuration parameters.
- **Session Hijacking:** A security attack where a user session is taken over by an unauthorised party.