E-Forensic (ICT30010) Capstone Report

Name: SM Ragib Rezwan

ID: 103172523

On 19th May 2022, at 6:30PM AEST, the police had asked for my assistance in verifying whether certain alleged hacking events had occurred (see in the table below), in order to prosecute Imanuel Leet-Hacker. For this, they had provided me with a Forensic image in Expert Witness Disk Image Format (EWF) (ie the E01 file extension), alongside two exhibits (screenshot of hackable's website after compromise and image placed on "Somepoor Victim"'s Facebook page) via 3 different download links from a canvas webpage (URL: https://swinburne.instructure.com/courses/40722/assignments/422273).

Event number	Event brief Description
1	Whether or not Hackable company's website had been hacked by culprit on 4th May 2010
2	Whether or not culprit had hacked another website on 4th March 2009 at 2:22am
3	Whether or not culprit had accessed Somepoor Victim's Facebook account without permission on 6th August 2010 while staying at a hotel in Brisbane
4	Whether or not culprit has a collaborator who uses hidemyass.com as an email dropbox

Upon receiving the evidence, I extracted them from their respective links and copied them to the forensic workstation where I immediately ran relevant hash functions (using the terminal) on each evidence received and noted them down in the table below:

Evidences	MD5 value	SHA1 value
ImaHacker.E01 (forensic image received from the police)	16dc3a3dcb703e62f5b3dbe3b4ab8a10	b4da388ef7196fed5bbd60a0b2497f19b94407ef
Exhibit 1 (Hackable's website screenshot picture)	cec89fe25b60e9635ae849f2e24fdbb3	702f692dda66025b81e480872b277378251b809f
Exhibit 2 (Somepoor Victim's Facebook page)	5674005e22027fd893c8fbc74752bd01	2aa6b6e43500ec9e6410ed613fe35776df145f0e

After this, at 6:35pm, I also used a forensic tool (ewfverify) to ensure hash contained within the forensic image was accurate. There, the hash values found were same as the ones mentioned in the table, ensuring chain of continuity had been maintained in transferring of the forensic image.

Here are the pictures of the two exhibits that have been received:

[Exhibit 1: screenshot of hackable's website after compromise]

[Exhibit 2: image placed on "Somepoor Victim"'s Facebook page]

After a while, at 6:40pm, I had received a detailed timeline in the form of Timescanner Super Timeline from Troy as a Microsoft Excel Comma Separated Values File (i.e. files with extension .csv) as an email attachment alongside its MD5 value. So I immediately copied it to the forensic workstation and re-ran the hash to ensure chain of custody was properly maintained. Its hash value had been unchanged and so it was confirmed.

	MD5 written in Capstone Lab Scenario	**MD5 found after receiving**
Timeline.csv	9574ac771fdeeeb9a95d8dda5ed1749a	9574ac771fdeeeb9a95d8dda5ed1749a

Details of the partition contained within the image, and determination of the seized devices time zone

After this, at 6:45PM, I utilized another forensic tool (mmls) on the forensic image to find details of partitions contained in the image, which I have noted in the table below for later use:

Partition Number	**Partition Type**	**Start Sector**	**End Sector**	**Total Sector**	**Total size (MB)**
1	NTFS	63	41913584	41913522	21,459,723,264

Moreover, it also had a sector size of: **512 bytes**

Later on, at 6:50PM, I utilized a different forensic tool (rip.pl) to get the time zone information of the seized device which I noted in the table below:

Time Zone	**AUS Eastern Standard Time (UTC+10)**

After this, at 6:55PM, I used the start sector (**63**) and sector size (**512**) to find the starting offset in bytes (**32,256**) which I then used (in addition to the time zone difference) to mount the forensic image on the Autopsy forensic tool. After this, all preparatory stages had been done and so I began my investigation.

[Note:** During the investigation, I had noticed a discrepancy in time between the events occurring in the Super timeline and on the forensic image (shown by autopsy) by 1 hour 53 seconds (i.e. Dc1.html file's creation in Recycler occurred at 2009-03-04 **"00:48:50"** on autopsy but had occurred on same day at **"01:49:43"** in the super timeline). Thus I had reduced the timing of all events in the Super Timeline by that time in order to maintain continuity with the timings observed in autopsy browser**]

[Note:

For each investigation event report, I have broken them down in the following manner:

How I located the evidence

To note the background information given to me and the way I had proceeded to find all the evidence

Overall evidence list

To sum up all the important/ relevant evidences to my investigation

Overall Summary (keeping timelines relative to that of the autopsy browser)

*To give a simplified overall of how the series of events that had taken place**]***

Evidence and Explanation for the alleged "Hackable" attack:

How I located the evidence:

For this investigation, I had been given the exhibit1 and the fact that it had occurred on 4th May 2010 on hackable's website. Thus I utilized a forensic tool (autopsy) to search for a file named "hackable" and noted down the results found in the table below:

File path	Written	Accessed	Changed	Created	Size (byte)	Meta
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	15424-144-9
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	16138-128-1
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	12102-128-4

Since the first file was a directory, I used the same forensic tool to open it which provided me with the following file which I had also noted in the table below:

File path	Written	Accessed	Changed	Created	Size (byte)	Meta
C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/PAWNED, again!.htm	2010-05-04 23:35:37 (AEST)	2010-05-04 23:35:37 (AEST)	2010-05-04 23:35:37 (AEST)	2010-05-04 23:35:36 (AEST)	340	16137-128-1
C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/PAWNED, again!.htm:Zone.Identifier	2010-05-04 23:35:37 (AEST)	2010-05-04 23:35:37 (AEST)	2010-05-04 23:35:37 (AEST)	2010-05-04 23:35:36 (AEST)	26	16137-128-4
C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/PAWNED, again!_files	2010-05-04 23:35:36 (AEST)	2010-08-06 01:33:44 (AEST)	2010-05-04 23:35:36 (AEST)	2010-05-04 23:35:36 (AEST)	152	15771-144-1
C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/users.txt	2010-05-04 23:32:16 (AEST)	2010-05-04 23:32:16 (AEST)	2010-05-04 23:32:16 (AEST)	2010-05-04 23:32:16 (AEST)	1239	15427-128-3

Going through file “PAWNED, again!.htm”, I noticed that it was extremely similar to the file in the Exhibit1 provided by the police, missing only the picture. So I noted it down in the suspicious file

Furthermore I also found a picture link in the previous htm file which lead me to the following file inside “PAWNED, again!_files/”:

File path	Written	Accessed	Changed	Created	Size (byte)	Meta
C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/PAWNED, again!_files/win2000.gif	2010-05-04 23:35:36 (AEST)	2010-05-04 23:35:36 (AEST)	2010-05-04 23:35:36 (AEST)	2010-05-04 23:35:36 (AEST)	4670	15657-128-3

Opening it using the same forensic tool (autopsy) revealed the picture that had been present on the webpage displayed in Exhibit 1. So I noted it down as another suspicious file.

After this I looked though the User.txt file too and noticed that it contained a list of users along with their SSIDs which I noted in the table below before noting it down as another suspicious file.

The information present in the User.txt file:

User	Full name	Comment	SID	Req. Pass. Change	Pass Never Expire	Last logon	Status
Administrator	***N/A***	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	***N/A***	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	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	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

After that, I checked other files too and noticed that in "C:/Program Files/Nmap/server.hackable.com.au.xml", there was report of NMAP running on server.hackable.com.au from the computer in the forensic image, alongside sending information to "PAWNED!" .Now, NMAP is a tool that scans through all ports to find vulnerabilities in a network. So I noted it down as another suspicious file.

After finishing that, I still used the same forensic tool to do a "keystring" search (searching using a string like a phrase or word) using "hackable", order to see whether I missed anything. Then I found the following file that contains all sent emails from Ima Hacker's email:

"C:/Documents and Settings/Ima Hacker/Local Settings/Application Data/Identities/{6FE73E6F-28AF-4574-90D1-A0B477E9D564}/Microsoft/Outlook Express/Sent Items.dbx"

In there an email had been sent from Ima Hacker's email address to learntohack@hmamail.com on 4th May 2010 at 23:30:35, stating that "he had gotten into hackable server using "ipcscan" using their backup password and was now playing around". So I noted down that email details as a suspicious email and the file details as a suspicious file

File path	Written date	Accessed Date	Changed date	Created date	File size (byte)	Meta
C:/Documents and Settings/Ima Hacker/Local Settings/Application Data/Identities/{6FE73E6F-28AF-4574-90D1-A0B477E9D564}/Microsoft/Outlook Express/Sent Items.dbx	2010-10-14 02:18:38 (AEST)	2010-10-14 02:18:38 (AEST)	2010-10-14 02:18:38 (AEST)	2010-05-04 22:57:32 (AEST)	207572	15284-128-4

Email details:

To	From	Date	Subject	X-Mailer
<learntohack@hmamail.com>	"Ima Hacker" <imahacker72@yahoo.com.au>	4 May 2010 23:30:35	ipcscan worked!	Microsoft Outlook Express 6.00.2900.2180

Since, there was a mention of “ipcscan”, which is a brute force password cracking tool; I used the same forensic tool to do a file scan of that name which loaded up the following files which I have noted in the table below:

File path	Written	Accessed	Changed	Created	Size (byte)	Meta
C:/Documents and Settings/Ima Hacker/My Documents/Downloads/ipcscan.rar	2010-05-04 23:16:37 (AEST)	2010-08-06 00:56:41 (AEST)	2010-05-04 23:16:37 (AEST)	2010-05-04 23:16:36 (AEST)	61418	15430-128-4
C:/Documents and Settings/Ima Hacker/My Documents/Downloads/ipcscan.rar:Zone.Identifier	2010-05-04 23:16:37 (AEST)	2010-08-06 00:56:41 (AEST)	2010-05-04 23:16:37 (AEST)	2010-05-04 23:16:36 (AEST)	26	15430-128-8
C:/Toolz/ipcscan	2010-05-04 23:19:47 (AEST)	2010-05-04 23:19:47 (AEST)	2010-05-04 23:19:47(AEST)	2010-05-04 23:19:42 (AEST)	480	15540-144-1
C:/Toolz/ipcscan/IpcScan-gui.exe	2002-10-12 13:14:32 (AEST)	2010-05-04 23:24:17 (AEST)	2010-05-04 23:40:20 (AEST)	2010-05-04 23:19:47 (AEST)	143360	15546-128-4
C:/WINDOWS/Prefetch/IPCSCAN-GUI.EXE-1C4F985C.pf	2010-05-04 23:24:27 (AEST)	2010-05-04 23:24:27 (AEST)	2010-05-04 23:24:27 (AEST)	2010-05-04 23:24:27 (AEST)	9914	15551-128-4

Then I opened the ipcscan directory and found that there was a file called ipcpass.dic (which contained place holders to enter password and list of usernames) and ipcuser.dic (which contained a list of possible users). Alongside that, I also noticed that there was a GUI there too named IpcScan-gui.exe which also had been run on that day. So I noted down all their details as suspicious files as well.

After that I looked through the Super timeline and noticed that before all of these at 22:15:33 *(after converting the time to autopsy’s time)*, the “Parosproxy.org - Web Application Security” webpage had

been bookmarked (it is a website that uses tools to do penetration testing for web applications). So I noted those details in the table below:

date	time	time zone	MACB	source	source type	type	user	host
5/4/2010	22:15:33	Australia/Melbourne	M...	WEBHIST	Firefox History	Content Modification Time	-	L33TPC

short	description	version	Filename	inode	notes
Bookmarked Parosproxy.org - Web Application Security (http://www.parosproxy.o...	Bookmark URL Parosproxy.org - Web Application Security (http://www.parosproxy.org/) [Parosproxy.org - Web Application Security] visit count 1	2	TSK:/Documents and Settings/Ima Hacker/Application Data/Mozilla/Firefox/Profiles/65qsm3on.default/places.sqlite	13487	-

format	Extra
sqlite/firefox_history	host: gro.yxorpsorap.www.; schema_match: True; sha256_hash: 2cce74fb6cac7c0c8e50316ada07237900af752680e8ab634b32b515ce82a7e1

Overall Evidence list:

A. Overall suspicious files list/table for event 1: (follow suspicious file format from other labs)

File path	Written date	Accessed Date	Changed date	Created date	File size (byte)	Meta
C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/PAWNED, again!_files/win2000.gif	2010-05-04 23:35:36 (AEST)	2010-05-04 23:35:36 (AEST)	2010-05-04 23:35:36 (AEST)	2010-05-04 23:35:36 (AEST)	4670	15657-128-3
C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/users.txt	2010-05-04 23:32:1	2010-05-04 23:32:16	2010-05-04 23:32:1	2010-05-04 23:32:1	1239	15427-128-3

	6 (AEST)	(AEST)	6 (AEST)	6 (AEST)		
C:/Documents and Settings/Ima Hacker/My Documents/server.hackable/PAWNED, again!.htm	2010-05-04 23:35:37 (AEST)	2010-05-04 23:35:37 (AEST)	2010-05-04 23:35:37 (AEST)	2010-05-04 23:35:36 (AEST)	340	16137-128-1
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	12102-128-4
C:/Toolz/ipcscan/ipcpass.dic	2007-03-02 14:53:02 (AEST)	2010-05-04 23:19:47 (AEST)	2010-05-04 23:19:47 (AEST)	2010-05-04 23:19:47 (AEST)	591	15545-128-1
C:/Toolz/ipcscan/IpcScan-gui.exe	2002-10-12 13:14:32 (AEST)	2010-05-04 23:24:17 (AEST)	2010-05-04 23:40:20 (AEST)	2010-05-04 23:19:47 (AEST)	143360	15546-128-4
C:/Toolz/ipcscan/ipcuser.dic	2005-07-25 15:44:09 (AEST)	2010-05-04 23:19:47 (AEST)	2010-05-04 23:19:47 (AEST)	2010-05-04 23:19:47 (AEST)	93	15547-128-1
C:/Documents and Settings/Ima Hacker/Local Settings/Application Data/Identities/{6FE73E6F-28AF-4574-90D1-A0B477E9D564}/Microsoft/Outlook Express/Sent Items.dbx	2010-10-14 02:18:38 (AEST)	2010-10-14 02:18:38 (AEST)	2010-10-14 02:18:38 (AEST)	2010-05-04 22:57:32 (AEST)	207572	15284-128-4

B. Suspicious Email details:

To	From	Date	Subject	X-Mailer
<learntohack@hmamail.com>	"Ima Hacker" <imahacker72@yahoo.com.au>	4 May 2010 23:30:35	ipcscan worked!	Microsoft Outlook Express 6.00.2900.2180

C. Relevant Timeline Information:

date	Time (readjusted to autopsy	time zone	MACB	source	source type	type	user	host

	timings)							
5/4/2010	22:15:33	Australia/Melbourne	M...	WEBHIST	Firefox History	Content Modification Time	-	L33TPC

short	description	version	Filename	inode	notes
Bookmarked Parosproxy.org - Web Application Security (http://www.parosproxy.o...	Bookmark URL Parosproxy.org - Web Application Security (http://www.parosproxy.org/) [Parosproxy.org - Web Application Security] visit count 1	2	TSK:/Documents and Settings/Ima Hacker/Application Data/Mozilla/Firefox/Profiles/65qsm3on.default/places.sqlite	13487	-

format	Extra
sqlite/firefox_history	host: gro.yxorpsorap.www.; schema_match: True; sha256_hash: 2cce74fb6cac7c0c8e50316ada07237900af752680e8ab634b32b515ce82a7e1

Overall Summary (keeping timelines relative to that of the autopsy browser)

So, on 4th May 2010, at first Parosproxy webpage had been browsed and then bookmarked. Then, NMap program had been run, which had been used to find vulnerabilities in the hackable website.

After that a ipcscan software had been downloaded as a file with ".rar" extension (which is a program file used to brute force passwords).Once it was done, it had been extracted to C:/Toolz/ipcscan file. Then, relevant username and password files to set up in the ipcscan file, before running the GUI of ipcscan.

After that, an email had been sent from imahacker's email account (imahacker72@yahoo.com.au) to his possible collaborator learntohack@hmamail.com where the sender spoke about "being able to use ipscan to get into hackable's server using their backup password" and "was just playing around now".

Then, a list of authorized users, SIDs and other details from hackable's website had been copied and pasted into a text file called Users.txt.

After that, webpage shown in Exhibit 1 had been created (using files "PAWNED, again!.htm" and "win2000.gif") and uploaded on the hackable's website.

So, keeping all evidences in mind and the order of events, the attack on hackable's website had indeed occurred.

Relevant evidence and the explanation of findings that supports or refutes the hacker's alibi for the alleged "second" website attack

How I located the evidence:

For this investigation, I had been informed that a similar website attack had occurred on 4th March 2009 at 2:22AM where the Ima Hacker had stated to be out shopping at a local 24 hours convenience store. So I began by looking through the super timeline and also the corresponding artifacts on the forensic image using forensic tool (autopsy) in order to see everything that had been done around that timeframe

[Note: *Since I am keeping the times relative to the forensic image, the super timeline times had been corrected by reducing "**1hr 53 seconds**" from each. Furthermore, this would put the incident to occur at "**1:21:07AM**" on the same day where Ima Hacker claimed to be out shopping, with respect to forensic image time on autopsy***.]***

[Note: *Since I had used the super timeline from the very start for this investigation, the evidence had been noted in order of events occurring. But giving timeline evidence under each and every statement took too much space and made it difficult to read. Thus to keep things clear, I have taken all evidences and placed them in their respective tables in the "overall evidence" section**]***

On 0:22:37, a news webpage on NimeMSN.com regarding Jquery.iepnghack had been opened, which is an article regarding where plugins used to commit a hack on jquery (used in Javascipts running on webpages) using pictures. So, I noted the information regarding it in the suspicious timeline details table.

After that at, at 0:38:15, a site called "hackthissite" had been entered, which is a website set up in order to allow ethical hackers to develop their skills. So, I noted it down in the suspicious timeline details table. Furthermore, I also noted down the index.dat (i.e. the file that contained the cache data) as a suspicious file

Later on, at 0:44:01, that site had been visited again, this time as an admin to view a picture. So I noted it down in the table as well (it also stored information in the index.dat).

After that, at 0:44:57, a mission noted as the first mission in the basic part on the webpage had been accessed, which I also noted down in the table (it also stored information in the index.dat).

Next, at 0:46:35, a mission noted as the third mission in the basic part on the webpage had been accessed, which I also noted down in the table (it also stored information in the index.dat).

Next, at 0:47:33, a mission noted as the fourth mission in the basic part on the webpage had been accessed, which I also noted down in the table (it also stored information in the index.dat).

After that, at 0:48:50, html file (webpage file) containing mission 4 information from the website had been deleted on the computer. This made me curious, so I used forensic tool (autopsy) to access the file

where I noticed that it was a hacking activity which had been completed. So I noted down both in the timeline table and also in the suspicious deleted file table.

Next, at 0:49:49 a mission noted as the fifth mission in the basic part on the webpage had been accessed, which I also noted down in the table (it also stored information in the index.dat).

Then at 0:51:13 a search had been performed in Google on how to “change http of referrer” which I noted down in the table.

Then at 0:54:33, a site called “fiddler2” had been accessed. It is software used to tool to log, inspect and “fiddle” with incoming or outgoing data from a client computer to the internet. So I also noted it down in the table.

After that at 0:54:41, a Google search had been made regarding “windows hacking tool to change http header” information and at 0:55:33, another Google search had been made about “http traffic interception and modification”. So I also noted these down in the table.

Later on at 0:55:38, an article on site called “a4apphack” had been accessed which spoke about using “secfox to turn firefox into an ultimate hacking tool”. So I noted it down in the table.

Then at 0:55:59, “getfiddler” website had been accessed in order to get “fiddler2setup.exe” file. So it had been noted down in the table as well.

So, I looked through the forensic image using a forensic tool (autopsy) and noticed that file called fiddler2 had been created in Program files at 00:57:50. Since I knew what it is usually used for, I noted down its details as a suspicious file.

Then from 1:19:25 to 1:28:29, a gap in the timeline had been noticed when no operations had been performed on the computer in the forensic image. This has been around the time when the attack had been thought to have taken place.

Similarly, another gap had been noticed from 1:28:31 to 1:43:07 where no operation had been performed on the computer.

Then at 1:56:33, a download page for software called “burp” on “portswigger” website had been accessed. It is software used to test web applications in order to find vulnerabilities. So I noted down that detail in the table as well. Alongside that, I used the forensic tool (autopsy) and found that it had been downloaded as a zip file called “burpsuite_v1.3.03[1].zip” at 01:58:11. So I noted that detail in the suspicious file table.

After that, at 1:58:15 and 1:58:26, the hackthissite website’s admin part had been accessed again in order to access files named scanner and learnsecurityonline (cache again stored in index.dat file)

After that, from 2:01:41-48, dotnetfx, hackthissite-mission5, burpsuite_v1 and its zip had been deleted. So I noted down those information in the timeline table and also in the deleted files table.

Overall Evidence list:

A. Suspicious timeline details:

date	time	time zone	MACB	source	source type	type	user	host
3/4/2009	0:22:37	Australia/Melbourne	.A..	WEBHIST	MSIE Cache File URL record	Last Access Time	-	L33TPC
3/4/2009	0:38:15	Australia/Melbourne	....	WEBHIST	MSIE Cache File URL record	Last Checked Time	-	L33TPC
3/4/2009	0:44:01	Australia/Melbourne	....	WEBHIST	MSIE Cache File URL record	Last Checked Time	-	L33TPC
3/4/2009	0:44:57	Australia/Melbourne	....	WEBHIST	MSIE Cache File URL record	Last Checked Time	-	L33TPC
3/4/2009	0:46:35	Australia/Melbourne	.A..	WEBHIST	MSIE Cache File URL record	Last Access Time	-	L33TPC
3/4/2009	0:47:33	Australia/Melbourne	.A..	WEBHIST	MSIE Cache File URL record	Last Access Time	-	L33TPC
3/4/2009	0:48:50	Australia/Melbourne	M...	RECBIN	Recycle Bin	Content Deletion Time	-	L33TPC
3/4/2009	0:49:49	Australia/Melbourne	.A..	WEBHIST	MSIE Cache File URL record	Last Access Time	-	L33TPC
3/4/2009	0:51:13	Australia/Melbourne	....	WEBHIST	MSIE Cache File URL record	Last Checked Time	-	L33TPC
3/4/2009	0:54:33	Australia/Melbourne	.A..	WEBHIST	MSIE Cache File URL record	Last Access Time	-	L33TPC
3/4/2009	0:54:41	Australia/Melbourne	.A..	WEBHIST	MSIE	Last	-	L33TPC

					Cache File URL record	Access Time		
3/4/2009	0:55:33	Australia/Melbourne	....	WEBHIST	MSIE Cache File URL record	Expiration Time	-	L33TPC
3/4/2009	0:55:38	Australia/Melbourne	.A..	WEBHIST	MSIE Cache File URL record	Last Access Time	-	L33TPC
3/4/2009	0:55:59	Australia/Melbourne	.A..	WEBHIST	MSIE Cache File URL record	Last Access Time	-	L33TPC
3/4/2009	1:56:33	Australia/Melbourne	.A..	WEBHIST	MSIE Cache File URL record	Last Access Time	-	L33TPC
3/4/2009	1:58:15	Australia/Melbourne	....	WEBHIST	MSIE Cache File URL record	Last Checked Time	-	L33TPC
3/4/2009	1:58:26	Australia/Melbourne	.A..	WEBHIST	MSIE Cache File URL record	Last Access Time	-	L33TPC
3/4/2009	2:01:41	Australia/Melbourne	M...	RECBIN	Recycle Bin	Content Deletion Time	-	L33TPC
3/4/2009	2:01:44	Australia/Melbourne	M...	RECBIN	Recycle Bin	Content Deletion Time	-	L33TPC
3/4/2009	2:01:46	Australia/Melbourne	M...	RECBIN	Recycle Bin	Content Deletion Time	-	L33TPC
3/4/2009	3:02:48	Australia/Melbourne	M...	RECBIN	Recycle Bin	Content Deletion Time	-	L33TPC

short	**description**	**version**	**filename**	**inode**	**notes**
Location:	Location:	2	TSK:/Doc	1	-

http://ninemsn.com.au/js/jquery.iepnghack.1.6.js?v=1 Cached file: I...	http://ninemsn.com.au/js/jquery.iepnghack.1.6.js?v=1 Number of hits: 1 Cached file: IZQDETYP\jquery.iepnghack.1.6[1].js Cached file size: 4780 HTTP headers: HTTP/1.1 200 OK - Content-Length: 4780 - Content-Type: application/x-javascript -		uments and Settings/ Ima Hacker/Local Settings/ Temporary Internet Files/Content.IE5/index.dat	0 3 4 0	
Location: http://www.hackthissite.org/images/bullet_triangle_green.png Cached...	Location: http://www.hackthissite.org/images/bullet_triangle_green.png Number of hits: 3 Cached file: IZQDETYP\bullet_triangle_green[1].png Cached file size: 512 HTTP headers: HTTP/1.1 200 OK - ETag: "f7d84-200-44326a95b6500" - Content-Length: 512 - Content-Type: image/png - - ~U:ima hacker -	2	TSK:/Documents and Settings/ Ima Hacker/Local Settings/ Temporary Internet Files/Content.IE5/index.dat	1 0 3 4 0	-
Location: http://admin.hackthissite.org/ads/adimage.php?filename=468x60_codes...	Location: http://admin.hackthissite.org/ads/adimage.php?filename=468x60_codescan.jpg&contenttype=jpeg Number of hits: 3 Cached file: UDM5CTEP\adimage[1].jpg Cached file size: 26676 HTTP headers: HTTP/1.1 200 OK - Content-Length: 26676 - Content-Type: image/jpeg; name=468x60_codescan.jpg - - ~U:ima hacker -	2	TSK:/Documents and Settings/ Ima Hacker/Local Settings/ Temporary Internet Files/Content.IE5/index.dat	1 0 3 4 0	-
Location: view-source:http://www.hackthissite.org/missions/basic/1/ Cached fi...	Location: view-source:http://www.hackthissite.org/missions/basic/1/ Number of hits: 1 Cached file: CJIP4PUH\1[1] Cached file size: 13022	2	TSK:/Documents and Settings/ Ima Hacker/Local	1 0 3 4 0	-

			Settings/ Temporary Internet Files/Content.IE5/index.dat		
Location: view-source:http://www.hackthissite.org/missions/basic/3/ Cached fi...	Location: view-source:http://www.hackthissite.org/missions/basic/3/ Number of hits: 1 Cached file: EVKT0N8H\3[1] Cached file size: 12496	2	TSK:/Documents and Settings/ Ima Hacker/Local Settings/ Temporary Internet Files/Content.IE5/index.dat	1034 0	-
Location: view-source:http://www.hackthissite.org/missions/basic/4/ Cached fi...	Location: view-source:http://www.hackthissite.org/missions/basic/4/ Number of hits: 1 Cached file: EVKT0N8H\4[1] Cached file size: 12839	2	TSK:/Documents and Settings/ Ima Hacker/Local Settings/ Temporary Internet Files/Content.IE5/index.dat	1034 0	-
Deleted file: C:\Documents and Settings\Ima Hacker\Desktop\hackthissite-missi...	DC1 -> C:\Documents and Settings\Ima Hacker\Desktop\hackthissite-mission4.html (from drive: C)	2	TSK:/RECYCLER/S-1-5-21-1935655697-1757981266-725345543-1003/INFO2	1134 3	-
Location: view-source:http://www.hackt	Location: view-source:http://www.hackthissite.org/missions/ba	2	TSK:/Documents	10	-

hissite.org/missions/basic/5/ Cached fi...	sic/5/ Number of hits: 1 Cached file: UDM5CTEP\5[1] Cached file size: 12649		and Settings/ Ima Hacker/Local Settings/ Temporary Internet Files/Content.IE5/index.dat	3 4 0	
Location: http://www.google.com.au/search?hl=en&source=hp&q=change+http+refer...	Location: http://www.google.com.au/search?hl=en&source=hp&q=change+http+referrer&meta=&aq=o&aqi=&aql=&oq= Number of hits: 3 Cached file: IZQDETYP\search[1].htm Cached file size: 29290 HTTP headers: HTTP/1.1 200 OK - Content-Length: 29290 - Content-Type: text/html -	2	TSK:/Documents and Settings/ Ima Hacker/Local Settings/ Temporary Internet Files/Content.IE5/index.dat	1 0 3 4 0	-
Location: http://www.fiddler2.com/fiddler2/ Cached file: IZQDETYP\fiddler2[1]...	Location: http://www.fiddler2.com/fiddler2/ Number of hits: 1 Cached file: IZQDETYP\fiddler2[1].htm Cached file size: 5543 HTTP headers: HTTP/1.1 200 OK - MicrosoftOfficeWebServer: 5.0_Pub - X-Powered-By: ASP.NET - Content-Length: 5543 - Content-Type: text/html; Charset=utf-8 - - ~U:ima hacker -	2	TSK:/Documents and Settings/ Ima Hacker/Local Settings/ Temporary Internet Files/Content.IE5/index.dat	1 0 3 4 0	-
Location: http://www.google.com.au/search?q=windows+hacking+tool+change+http+...	Location: http://www.google.com.au/search?q=windows+hacking+tool+change+http+headers&hl=en&source=hp&aq=f&aqi=&aql=&oq= Number of hits: 2 Cached file: CJIP4PUH\search[3].htm Cached file size: 31411 HTTP headers: HTTP/1.1 200 OK - Content-Length: 31411 - Content-Type: text/html -	2	TSK:/Documents and Settings/ Ima Hacker/Local Settings/	1 0 3 4 0	-

			Temporary Internet Files/Content.IE5/index.dat		
Location: http://www.google.com.au/search?q=http+traffic+intercept+and+modify...	Location: http://www.google.com.au/search?q=http+traffic+intercept+and+modify&hl=en&prmd=ivns&ei=Fvy1Te6LMZGuvgPxiMG6Dw&start=10&sa=N Number of hits: 2 Cached file: CJIP4PUH\search[4].htm Cached file size: 30540 HTTP headers: HTTP/1.1 200 OK - Content-Length: 30540 - Content-Type: text/html -	2	TSK:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/index.dat	1034 0	-
Location: http://a4apphack.com/featured/secfox-turn-firefox-into-an-ultimate-...	Location: http://a4apphack.com/featured/secfox-turn-firefox-into-an-ultimate-hacking-tool-part-1 Number of hits: 3 Cached file: UDM5CTEP\secfox-turn-firefox-into-an-ultimate-hacking-tool-part-1[1].htm Cached file size: 84608 HTTP headers: HTTP/1.1 200 OK - Content-Length: 84608 - Content-Type: text/html -	2	TSK:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/index.dat	1034 0	-
Location: http://www.getfiddler.com/dl/Fiddler2Setup.exe Cached file: IZQDETY...	Location: http://www.getfiddler.com/dl/Fiddler2Setup.exe Number of hits: 1 Cached file: IZQDETYP\Fiddler2Setup[1].exe Cached file size: 639824 HTTP headers: HTTP/1.1 200 OK - ETag: "f2e033-9c350-4a1b49dd4d940" - Content-Length: 639824 - Keep-Alive: timeout=2 max=100 - Content-Type: application/x-msdownload - - ~U:ima hacker -	2	TSK:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/index.dat	1034 0	-

Location: http://portswigger.net/burp/download.html Cached file: UDM5CTEP\dow...	Location: http://portswigger.net/burp/download.html Number of hits: 1 Cached file: UDM5CTEP\download[2].htm Cached file size: 6027 HTTP headers: HTTP/1.1 200 OK - ETag: "f5005f-178b-4ccd4330" - Content-Length: 6027 - Keep-Alive: timeout=5 max=60 - Content-Type: text/html - - ~U:ima hacker -	2	TSK:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/index.dat	103440	-
Location: http://admin.hackthissite.org/ads/adimage.php?filename=scanner358x5...	Location: http://admin.hackthissite.org/ads/adimage.php?filename=scanner358x52.gif&contenttype=gif Number of hits: 22 Cached file: EVKT0N8H\adimage[1].gif Cached file size: 15516 HTTP headers: HTTP/1.1 200 OK - Content-Length: 15516 - Content-Type: image/gif; name=scanner358x52.gif - - ~U:ima hacker -	2	TSK:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/index.dat	103440	-
Location: http://admin.hackthissite.org/ads/adimage.php?filename=learnsecurit...	Location: http://admin.hackthissite.org/ads/adimage.php?filename=learnsecurityonline.gif&contenttype=gif Number of hits: 3 Cached file: CJIP4PUH\adimage[2].gif Cached file size: 20084 HTTP headers: HTTP/1.1 200 OK - Content-Length: 20084 - Content-Type: image/gif; name=learnsecurityonline.gif - - ~U:ima hacker -	2	TSK:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/index.dat	103440	-
Deleted file: C:\Documents and Settings\Ima Hacker\Desktop\dotnetfx.exe	DC3 -> C:\Documents and Settings\Ima Hacker\Desktop\dotnetfx.exe (from drive: C)	2	TSK:/RECYCLER/S-1-5-21-1935655697-1757981	113443	-

			266-7253455 43-1003/INFO2		
Deleted file: C:\Documents and Settings\Ima Hacker\Desktop\hackthissite-missi...	DC4 -> C:\Documents and Settings\Ima Hacker\Desktop\hackthissite-mission5.html (from drive: C)	2	TSK:/RECYCLER/S-1-5-21-1935655697-1757981266-7253455 43-1003/INFO2	1 1 3 4 3	-
Deleted file: C:\Documents and Settings\Ima Hacker\Desktop\burpsuite_v1.3.03	DC5 -> C:\Documents and Settings\Ima Hacker\Desktop\burpsuite_v1.3.03 (from drive: C)	2	TSK:/RECYCLER/S-1-5-21-1935655697-1757981266-7253455 43-1003/INFO2	1 1 3 4 3	-
Deleted file: C:\Documents and Settings\Ima Hacker\Desktop\burpsuite_v1.3.03.zip	DC6 -> C:\Documents and Settings\Ima Hacker\Desktop\burpsuite_v1.3.03.zip (from drive: C)	2	TSK:/RECYCLER/S-1-5-21-1935655697-1757981266-7253455 43-1003/INFO2	1 1 3 4 3	-

format	Extra
msiecf	cache_directory_index: 1; cache_directory_name: IZQDETYP; cached_filename: jquery.iepnghack.1.6[1].js; recovered: False; sha256_hash: 2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90
msiecf	cache_directory_index: 1; cache_directory_name: IZQDETYP; cached_filename: bullet_triangle_green[1].png; recovered: False; sha256_hash:

	2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90
msiecf	cache_directory_index: 2; cache_directory_name: UDM5CTEP; cached_filename: adimage[1].jpg; recovered: False; sha256_hash: 2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90
msiecf	cache_directory_index: 3; cache_directory_name: CJIP4PUH; cached_filename: 1[1]; recovered: False; sha256_hash: 2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90
msiecf	cache_directory_index: 0; cache_directory_name: EVKT0N8H; cached_filename: 3[1]; recovered: False; sha256_hash: 2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90
msiecf	cache_directory_index: 0; cache_directory_name: EVKT0N8H; cached_filename: 4[1]; recovered: False; sha256_hash: 2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90
recycle_bin_info2	drive_number: 2; file_size: 16384; sha256_hash: e0b531d60b7f93fa72e046e6fb4b1e29604efb9743bd5b3b3718aca5805ee396
msiecf	cache_directory_index: 2; cache_directory_name: UDM5CTEP; cached_filename: 5[1]; recovered: False; sha256_hash: 2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90
msiecf	cache_directory_index: 1; cache_directory_name: IZQDETYP; cached_filename: search[1].htm; recovered: False; sha256_hash: 2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90
msiecf	cache_directory_index: 1; cache_directory_name: IZQDETYP; cached_filename: fiddler2[1].htm; recovered: False; sha256_hash: 2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90
msiecf	cache_directory_index: 3; cache_directory_name: CJIP4PUH; cached_filename: search[3].htm; recovered: False; sha256_hash: 2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90
msiecf	cache_directory_index: 3; cache_directory_name: CJIP4PUH; cached_filename: search[4].htm; recovered: False; sha256_hash: 2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90
msiecf	cache_directory_index: 2; cache_directory_name: UDM5CTEP; cached_filename: secfox-turn-firefox-into-an-ultimate-hacking-tool-part-1[1].htm; recovered: False; sha256_hash: 2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90
msiecf	cache_directory_index: 1; cache_directory_name: IZQDETYP; cached_filename: Fiddler2Setup[1].exe; recovered: False; sha256_hash: 2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90
msiecf	cache_directory_index: 2; cache_directory_name: UDM5CTEP; cached_filename: download[2].htm; recovered: False; sha256_hash: 2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90
msiecf	cache_directory_index: 0; cache_directory_name: EVKT0N8H; cached_filename: adimage[1].gif; recovered: False; sha256_hash: 2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90
msiecf	cache_directory_index: 3; cache_directory_name: CJIP4PUH; cached_filename: adimage[2].gif; recovered: False; sha256_hash: 2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90
recycle_bin_info2	drive_number: 2; file_size: 23511040; sha256_hash: e0b531d60b7f93fa72e046e6fb4b1e29604efb9743bd5b3b3718aca5805ee396

recycle_bin_info2	drive_number: 2; file_size: 16384; sha256_hash: e0b531d60b7f93fa72e046e6fb4b1e29604efb9743bd5b3b3718aca5805ee396
recycle_bin_info2	drive_number: 2; file_size: 2908160; sha256_hash: e0b531d60b7f93fa72e046e6fb4b1e29604efb9743bd5b3b3718aca5805ee396
recycle_bin_info2	drive_number: 2; file_size: 2617344; sha256_hash: e0b531d60b7f93fa72e046e6fb4b1e29604efb9743bd5b3b3718aca5805ee396

B. Suspicious file table:

File path	Written date	Accessed Date	Changed date	Created date	File size (byte)	Meta
C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/index.dat	2010-10-14 02:18:31 (AEST)	2009-02-16 03:02:15 (AEST)	2010-10-14 02:18:31 (AEST)	2009-02-16 03:02:15 (AEST)	1638400	10340-128-4
C:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/CJIP4PUH/burpsuite_v1.3.03[1].zip	2009-03-04 01:58:18 (AEST)	2009-03-04 01:58:18 (AEST)	2009-03-04 01:58:18 (AEST)	2009-03-04 01:58:11 (AEST)	2616070	13561-128-4
C:/Program Files/Fiddler2	2009-03-04 00:57:59 (AEST)	2010-10-14 01:57:39 (AEST)	2009-03-04 00:57:59 (AEST)	2009-03-04 00:57:50 (AEST)	56	11572-144-5

C. Suspicious deleted file table:

File path	Written date	Accessed Date	Changed date	Created date	File size (byte)	Meta
C:/RECYCLER/S-1-5-21-1935655697-1757981266-725345543-1003/Dc1.html	2009-03-04 00:49:09 (AEST)	2009-03-04 00:49:32 (AEST)	2009-03-04 00:49:43 (AEST)	2009-03-04 00:48:50 (AEST)	12837	11328-128-4
C:/RECYCLER/S-1-5-21-1935655697-1757981266-725345543-	2009-03-04 01:07:22 (AEST)	2009-03-04 01:07:22 (AEST)	2009-03-04 02:02:34 (AEST)	2009-03-04 01:07:17 (AEST)	23510720	11948-128-3

1003/Dc3.exe						
C:/RECYCLER/S-1-5-21-1935655697-1757981266-725345543-1003/Dc4.html	2009-03-04 00:51:23 (AEST)	2009-03-04 02:02:35 (AEST)	2009-03-04 02:02:37 (AEST)	2009-03-04 00:51:13 (AEST)	12647	11353-128-4
C:/RECYCLER/S-1-5-21-1935655697-1757981266-725345543-1003/Dc5.03	2009-03-04 01:58:42 (AEST)	2010-10-14 02:10:57 (AEST)	2009-03-04 02:02:39 (AEST)	2009-03-04 01:58:42 (AEST)	56	13572-144-6
C:/RECYCLER/S-1-5-21-1935655697-1757981266-725345543-1003/Dc6.zip	2009-03-04 01:58:22 (AEST)	2009-03-04 02:02:40 (AEST)	2009-03-04 02:02:41 (AEST)	2009-03-04 01:58:20 (AEST)	2616070	13562-128-4

Overall Summary (keeping timelines relative to that of the autopsy browser)

[Note: *Since the attack had been pinpointed to have occurred at a certain time of the day, I have also included all the timings of events here in the summary*]

On 0:22:37, a news webpage on NimeMSN.com regarding Jquery.iepnghack had been opened, which is an article regarding where plugins used to commit a hack on jquery using pictures. The, at 0:38:15, a site called hackthissite had been entered, which is a website set up in order to allow ethical hackers to develop their skills. Later on, at 0:44:01, that site had been visited again, this time as an admin to view a picture. After that, from 0:44:57 to 0:47:33, basic mission 1,3,4 from part of the website had been accessed. After that, at 0:48:50, html file (webpage file) containing mission 4 information from the website had been deleted on the computer after completion of task. Next, at 0:49:49 a mission noted as the fifth mission in the basic part on the webpage had been accessed

Then at 0:51:13 a search had been performed in Google on how to “change http of referrer”. Then at 0:54:33, a site called “fiddler2” had been accessed. It is software used to tool to log, inspect and “fiddle” with incoming or outgoing data from a client computer to the internet. After that at 0:54:41, a search had been made in Google regarding “windows hacking tool to change http header” and at 0:55:33, another Google search had been made about “http traffic interception and modification”

Later on at 0:55:38, an article on site called a4apphack had been accessed which spoke about using “secfox to turn firefox into an ultimate hacking tool”

Then at 0:55:59, getfiddler had been accessed in order to get fiddler2setup.exe file to download and use fiddler2.

After that two gaps had been noticed between 1:19:25 to 1:28:29, and 1:28:31 to 1:43:07 where no operation had been performed on the computer. This corresponded to the time when the hack should have occurred.

Then at 1:56:33, a download page for software called “burp” from “portswigger” had been accessed. It is software used to test web applications in order to find vulnerabilities.

After that, at 1:58:15 and 1:58:26, the hackthissite website’s admin part had been accessed again in order to access files named scanner and learnsecurityonline (cache again stored in index.dat file)

After that, from 2:01:41-48, dotnetfx, hackthissite-mission5, burpsuite_v1 and its zip had been deleted.

So, to conclude, Ima Hacker had not hacked any website using similar attack on the exact date and time provided by the police and had instead been away from his computer. But just before and after the given time, he had downloaded hacking tools whilst trying to hack the “hackable” website (in order to complete the missions provided there) in order to develop his hacking skills and had also deleted files related to it afterwards to cover his tracks.

Evidence and explanation for the alleged Facebook account takeover:

How I located the evidence:

The police had informed me that Somepoor victim (somepoorvictim@yahoo.com.au) had unauthorized access his Facebook account (ID: 100002369565636) on 6th Aug 2010 whilst staying at Hotel in Brisbane, at the same time when Ima Hacker had been staying there.

So, I started by using forensic tool (autopsy) to check for files with name Brisbane, which provided me with the following file directory

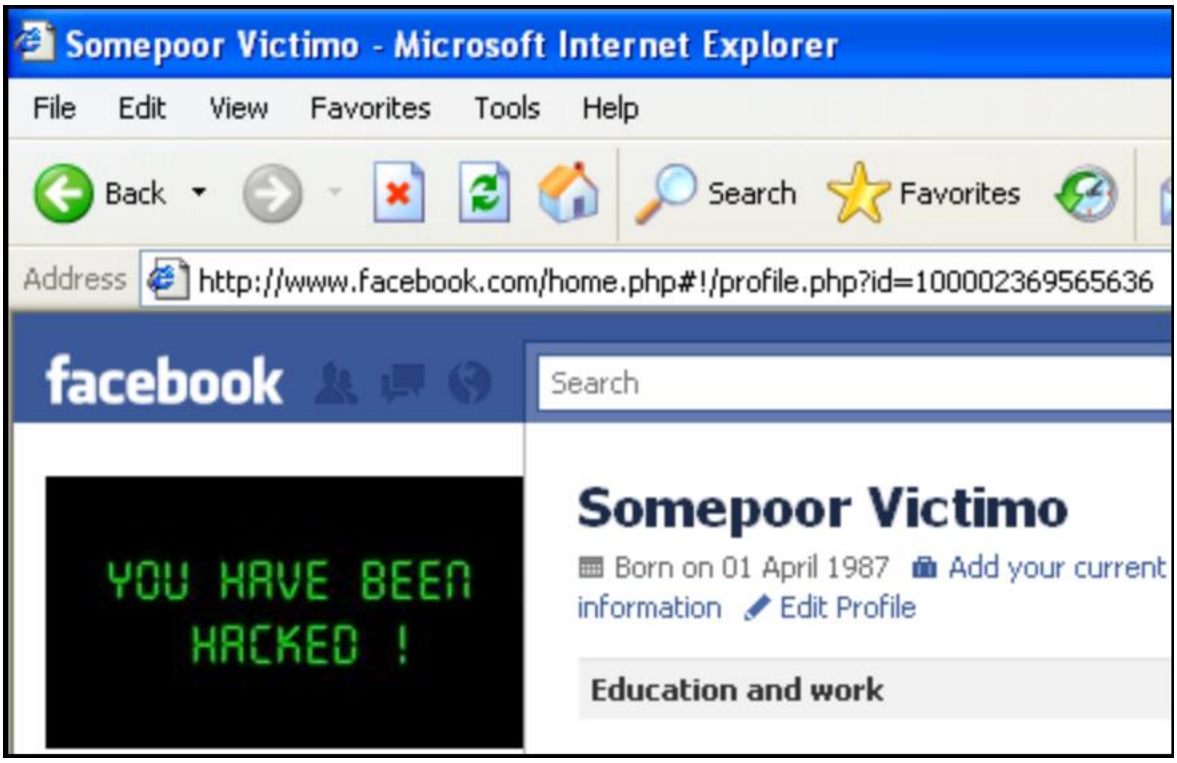
File name or path	Written date	Accessed Date	Changed date	Created date	File size (byte)	Meta
C:/Documents and Settings/Ima Hacker/My Documents/Brisbane 2010	2010-10-14 02:10:57 (AEST)	2010-10-14 02:10:57 (AEST)	2010-10-14 02:10:57 (AEST)	2010-07-30 00:18:51 (AEST)	56	16727-144-8

Opening the folder Brisbane 2010 led me to the following list of files:

File path	Written date	Accessed Date	Changed date	Created date	File size (byte)	Meta
C:/Documents and	2010-08-06	2010-10-14	2010-10-14	2010-08-06	24135176	16141-

Settings/Ima Hacker/My Documents/Brisbane 2010/hotel dump including email and facebook.pcap	01:24:09 (AEST)	01:44:40 (AEST)	01:44:42 (AEST)	01:24:08 (AEST)		128-4
C:/Documents and Settings/Ima Hacker/My Documents/Brisbane 2010/hotel dump.pcap	2010-07-30 00:19:05 (AEST)	2010-10-14 02:09:55 (AEST)	2010-10-14 02:09:55 (AEST)	2010-07-30 00:19:05 (AEST)	7626338	16728-128-4
C:/Documents and Settings/Ima Hacker/My Documents/Brisbane 2010/victim's facebook.bmp	2010-08-06 01:40:05 (AEST)	2010-10-14 01:44:32 (AEST)	2010-08-06 01:40:05 (AEST)	2010-08-06 01:40:05 (AEST)	364986	17314-128-4

Seeing the name of the third file, I became curious and used another forensic tool (ewfmount and mount) to mount the forensic image and open it using GUI. This led me to the following picture below:



[Figure: Image of the file victim's facebook.bmp]

Here it can be noticed that the Somepoor Victim's id (100002369565636) is present in the Facebook's profile id written in the address bar. Furthermore, the webpage had similar name to that of somepoor victim alongside the picture of "You have been hacked" which is same as that seen in Exhibit 2. So I noted down that file as a suspicious file.

Then I opened the other two files and noticed that they were Wireshark files and contained internet activities. So I utilized forensic tool (autopsy) to open these files. There I found certain packets (via filtering with somepoor victim's yahoo email address and Facebook id) carrying data related to somepoor victim's yahoo and Facebook. So I noted the suspicious information that I had found inside those packets in the tables below

Email details found in the packet:

To	**From**	**Date**	**Subject**	**X-Mailer**
Somepoor Victimo <somepoorvictim@yahoo.com.au>	Facebook < password+zj4o6tts=4t9@facebookmail.com>	Tue, 26 Apr 2011 03:20:58 -0700 (PDT)	You requested a new Facebook password	Zuck Mail [version 1.00]
<somepoorvictim@yahoo.com.au>	Yahoo! <mailbot@yahoo.com>	Tue, 26 Apr 2011 02:23:53 -0700 (PDT)	Welcome to Yahoo!	N/A
somepoorvictim@yahoo.com.au	Facebook <confirm+Ac29tZXBvb3J2aWN0aW1AeWFob28uY29tLmF1@facebookmail.com>	Tue, 26 Apr 2011 03:10:54 -0700 (PDT)	Just one more step to get started on Facebook	Zuck Mail [version 1.00]
Somepoor Victimo <somepoorvictim@yahoo.com.au>	Facebook <update+zj4o6tts=4t9@facebookmail.com>	Tue, 26 Apr 2011	Welcome to Facebook	Zuck Mail [version

		03:10:54 -0700		1.00]
Somepoor Victimo <somepoorvictim@yahoo.com.au>	Facebook <update+zj4o6tts=4t9@facebookmail.com>	Tue, 26 Apr 2011 03:15:10 -0700 (PDT)	Getting back onto Facebook	Zuck Mail [version 1.00]

With email contents regarding, “resetting facebook password”, “Welcoming somepoor to yahoo email”, “Confirmation code for signing up on facebook” “Welcoming somepoor to facebook”

Moreover, after the “resetting facebook password” email had been received in the yahoo email, 4 emails had also been deleted from it, before server had signed off.

Furthermore, the following email Username and password was also found in the packets:

USER	**PASS**
somepoorvictim@yahoo.com.au	8WXyk5W8

Moreover, the following suspicious details were also found in the packets data:

GET	**Accept**	**Referrer**	**Accept-Language**	**Accept-Encoding:**	**User-Agent**	**Host**	**Connection**
GET /rsrc.php/v1/yt/r/ip1sk_hStb2.css HTTP/1.1	*/*	http://www.facebook.com/login.php?email=somepoorvictim%40yahoo.com.au	en-us	gzip, deflate	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)	b.static.ak.fbcdn.net	Keep-Alive
GET	*/	http://www.facebook.com/login	en-	gzip,	Mozill	b.static.	Kee

/rsrc.php/v1/ym/r/Dev2iAkOGvH.css HTTP/1.1	*	.php?email=somepoorvictim%40yahoo.com.au	us	deflate	a/4.0 (compatible; MSIE 6.0; Windows NT 5.1)	ak.fbcdn.net	p-Alive
/ping/GSN-584610-Q/28774711/1701737132/0.4561285205793827/blur HTTP/1.1	*/*	http://pinglio.com/2010/11/how-to-install-and-use-firesheep/	en-us	gzip, deflate	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.16) Gecko/20110319 Firefox/3.6.16	data.gosquared.com	keep-alive

X-Apparently-To	Date and time	Received-SPF
somepoorvictim@yahoo.com.au via 98.138.85.215	Tue, 26 Apr 2011 03:10:55 -0700 (PDT)	pass (mta148.mail.ac4.yahoo.com: domain of confirm+ac29tzxbvb3j2awn0aw1aewfob28uy29tlmf1@facebookmail.com designates 66.220.144.142 as permitted sender)
somepoorvictim@yahoo.com.au via 98.138.85.210	Tue, 26 Apr 2011 03:10:56 -0700 (PDT)	pass (mta1081.mail.mud.yahoo.com: domain of update+zj4o6tts=4t9@facebookmail.com designates 66.220.144.151 as permitted sender)

[Note: *all the dates provided in the wireshark packet were inaccurate. Thus had to look through other evidences and the super timeline to set up the timeline*]

Since, the victim's yahoo email had been accessed; I used the forensic tool (autopsy) to look through the emails sent by Ima Hacker (file details noted in the table below) and filter out emails that he had sent while being in the hotel. There I found certain emails which I noted down in the suspicious emails table.

File name or path	Written date	Accessed Date	Changed date	Created date	File size (byte)	Meta
C:/Documents and Settings/Ima Hacker/Local Settings/Application Data/Identities/{6FE73E6F-28AF-4574-90D1-A0B477E9D564}/Microsoft/Outlook Express/Sent Items.dbx	2010-10-14 02:18:38 (AEST)	2010-10-14 02:18:38 (AEST	2010-10-14 02:18:38 (AEST)	2010-05-04 22:57:32 (AEST)	207572	15284-128-4

To	From	Date	Subject	X-Mailer
<learntohack@hmamail.com>	"Ima Hacker" <imahacker72@yahoo.com.au>	Fri, 30 Jul 2010 00:18:35 +1000	arrived at hotel	Microsoft Outlook Express 6.00.2900.2180
<learntohack@hmamail.com>	"Ima Hacker" <imahacker72@yahoo.com.au>	Fri, 6 Aug 2010 01:28:24 +1000	Re: arrived at hotel	Microsoft Outlook Express 6.00.2900.2180
<learntohack@hmamail.com>	"Ima Hacker" <imahacker72@yahoo.com.au>	Fri, 6 Aug 2010 01:41:25 +1000	hahah! facebook hack	Microsoft Outlook Express 6.00.2900.2180

Here, the content of the emails were regarding the following information respectively,

> "got to hotel, could see everyone's traffic as the hotel only used a network hub and planned to try firesheep thing if he could get into any accounts"
>
> "couldn't get firesheep to hijack the session of a person logging into yahoo, but got his password as the person had checked his email via pop"

> “pawned that guy’s facebook too by resetting his password using the email which [he] had already gotten access to beforehand”

Furthermore, for the last email, an attachment had also been sent which had the name “Hacked_Notification.jpg”. So I used the forensic tool (autopsy)’s file search to find out what it is. It was a picture similar to that shown in exhibit 2. So I noted down the file details in the suspicious file table.

[Figure: Hacked_Notification.jpg**]**

Firesheep is an extension for Firefox web browser that uses a packet sniffer to intercept unencrypted traffic and thus can be used to automate session hijacking attacks on unsecure Wi-Fi networks. Since its name had come up again, I used the forensic tool (autopsy) to search for file with that that name. Although these popped up several files, I noticed that most of these were files inside located in the same directory. Thus I noted down those directory names as suspicious files. Furthermore, I also noted down the installation file and prefetch file (as installation file can say when the file had been downloaded on to the computer and prefetch file can say the last time it had been run).

After this I looked through the super timeline in order to see how the things that had taken place and get an accurate timeline of how the events had proceeded. For this I used the email correspondence and firesheep download timings to get an idea of which point of time to look around.

[Note: *since timeline is “**1hr 53sec**” ahead of autopsy timings, I had adjusted the timings accordingly to correspond with the autopsy timings*]

In the timeline, several things had taken place. From there I only noted the events that took place which had not been detected in the previous evidences. For those events, I noted a brief summary of the things that had happened below and detailed information in the timeline table:

Before the attack, the following things had occurred:

A Google search had been on “firesheep how to”

A website called “codebutler” had been accessed for firesheep

A Google search had been made on “how to install and use firesheep”

Using “pinglio” to learn “how to install and use firesheep”

A Google search had been made on “how to hijack facebook using firesheep”

Attempting to login to Facebook using “codebutler” and “pinglio” and failing

Later on, just opening somepoor’s yahoo, a file had been deleted from Brisbane folder

After gaining access to somepoor’s facebook:

A Google search had been made on “I’ve been hacked image”

Somepoor’s facebook profile pic had been opened again

From the timeline, I had noticed a webpage file had been deleted from Brisbane 2010 which had the following name “You've been hacked! - Inbox - 'Yahoo!7 Mail'.htm” before being deleted to recycler as “DC33”. So I noted the deleted file as a suspicious file.

Overall Evidence list:

A. Suspicious file list:

File path	Written date	Accessed Date	Changed date	Created date	File size (byte)	Meta
C:/Documents and Settings/Ima Hacker/My Documents/Brisbane 2010/hotel dump including email and facebook.pcap	2010-08-06 01:2	2010-10-14 01:44:40	2010-10-14 01:4	2010-08-06 01:2	24135176	16141-128-4

	4:09 (AEST)	(AEST)	4:42 (AEST)	4:08 (AEST)		
C:/Documents and Settings/Ima Hacker/My Documents/Brisbane 2010/hotel dump.pcap	2010-07-30 00:19:05 (AEST)	2010-10-14 02:09:55 (AEST)	2010-10-14 02:09:55 (AEST)	2010-07-30 00:19:05 (AEST)	7626338	16728-128-4
C:/Documents and Settings/Ima Hacker/My Documents/Brisbane 2010/victim's facebook.bmp	2010-08-06 01:40:05 (AEST)	2010-10-14 01:44:32 (AEST)	2010-08-06 01:40:05 (AEST)	2010-08-06 01:40:05 (AEST)	364986	17314-128-4
C:/Documents and Settings/Ima Hacker/Desktop/Hacked_Notification.jpg	2010-08-06 01:38:32 (AEST)	2010-08-06 01:38:36 (AEST)	2010-08-06 01:38:36 (AEST)	2010-08-06 01:38:30 (AEST)	41504	17275-128-4
C:/Documents and Settings/Ima Hacker/Application Data/Mozilla/Firefox/Profiles/65qsm3on.default/extensions/firesheep@codebutler.com	2010-08-06 00:58:43 (AEST)	2010-10-14 01:57:40 (AEST)	2010-08-06 00:58:43 (AEST)	2010-08-06 00:58:43 (AEST)	56	13478-144-6
C:/Documents and Settings/Ima Hacker/Application Data/Mozilla/Firefox/Profiles/65qsm3on.default/extensions/firesheep@codebutler.com/platform/Darwin_x86-gcc3/firesheep-backend.dSYM	2010-08-06 00:58:43 (AEST)	2010-08-06 00:58:43 (AEST)	2010-08-06 00:58:43 (AEST)	2010-08-06 00:58:43 (AEST)	152	16783-144-1
C:/Documents and Settings/Ima Hacker/My Documents/Downloads/firesheep-0.1-1.xpi	2010-08-06	2010-08-06 00:5	2010-08-06	2010-08-06	3082723	16766-128-4

	00:56:07 (AEST)	6:07 (AEST)	00:56:07 (AEST)	00:55:47 (AEST)		
C:/WINDOWS/Prefetch/FIRESHEEP-BACKEND.EXE-3A5BA61B.pf	2010-08-06 01:07:25 (AEST)	2010-08-06 01:07:25 (AEST)	2010-08-06 01:07:25 (AEST)	2010-08-06 00:58:48 (AEST)	19660	7487-128-4

B. Suspicious Email list:

To	From	Date	Subject	X-Mailer
Somepoor Victimo <somepoorvictim@yahoo.com.au>	Facebook < password+zj4o6tts=4t9@facebookmail.com>	Tue, 26 Apr 2011 03:20:58 -0700 (PDT) (times taken from wireshark)	You requested a new Facebook password	Zuck Mail [version 1.00]
<somepoorvictim@yahoo.com.au>	Yahoo! <mailbot@yahoo.com>	Tue, 26 Apr 2011 02:23:53 -0700 (PDT) (times taken from wireshark)	Welcome to Yahoo!	N/A
somepoorvictim@yahoo.com.au	Facebook <confirm+Ac29tZXBvb3J2aWN0aW1AeWFob28uY29tLmF1@facebookmail.com>	Tue, 26 Apr 2011 03:10:54 -0700 (PDT) (times taken from wireshark)	Just one more step to get started on Facebook	Zuck Mail [version 1.00]
Somepoor Victimo <somepoorvictim@y	Facebook <update+zj4o6tts=4t9@facebookmail.com>	Tue, 26 Apr 2011	Welcome to	Zuck Mail

ahoo.com.au>		03:10:54 -0700	Facebook	[version 1.00]
Somepoor Victimo <somepoorvictim@yahoo.com.au>	Facebook <update+zj4o6tts=4t9@facebookmail.com>	Tue, 26 Apr 2011 03:15:10 -0700 (PDT)	Getting back onto Facebook	Zuck Mail [version 1.00]
<learntohack@hmamail.com>	"Ima Hacker" <imahacker72@yahoo.com.au>	Fri, 30 Jul 2010 00:18:35 +1000	arrived at hotel	Microsoft Outlook Express 6.00.2900.2180
<learntohack@hmamail.com>	"Ima Hacker" <imahacker72@yahoo.com.au>	Fri, 6 Aug 2010 01:28:24 +1000	Re: arrived at hotel	Microsoft Outlook Express 6.00.2900.2180
<learntohack@hmamail.com>	"Ima Hacker" <imahacker72@yahoo.com.au>	Fri, 6 Aug 2010 01:41:25 +1000	hahah! facebook hack	Microsoft Outlook Express 6.00.2900.2180

C. Suspicious information in the wireshark files (as seen in autopsy)

USER	PASS
somepoorvictim@yahoo.com.au	8WXyk5W8

GET	Accept	Referer	Accept-Language	Accept-Encoding:	User-Agent	Host	Connection
GET /rsrc.php/v1/yt/r/ip1sk_hStb2.css HTTP/1.1	*/*	http://www.facebook.com/login.php?email=somepoorvictim%40yahoo.com.au	en-us	gzip, deflate	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)	b.static.ak.fbcdn.net	Keep-Alive
GET /rsrc.php/v1/ym/r/Dev2iAkOGvH.css HTTP/1.1	*/*	http://www.facebook.com/login.php?email=somepoorvictim%40yahoo.com.au	en-us	gzip, deflate	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)	b.static.ak.fbcdn.net	Keep-Alive
/ping/GSN-584610-Q/28774711/1701737132/0.4561285205793827/blur HTTP/1.1	*/*	http://pinglio.com/2010/11/how-to-install-and-use-firesheep/	en-us	gzip, deflate	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.16) Gecko/20110319 Firefox/3.6.16	data.gosquared.com	keep-alive

X-Apparently-To	Date and time	Received-SPF
somepoorvictim@yahoo.com.au via 98.138.85.215	Tue, 26 Apr 2011 03:10:55 -0700 (PDT)	pass (mta148.mail.ac4.yahoo.com: domain of confirm+ac29tzxbvb3j2awn0aw1aewfob28uy29tlmf1@facebookmail.com designates 66.220.144.142 as permitted sender)
somepoorvictim@yahoo.com.au via 98.138.85.210	Tue, 26 Apr 2011 03:10:56 -0700 (PDT)	pass (mta1081.mail.mud.yahoo.com: domain of update+zj4o6tts=4t9@facebookmail.com designates 66.220.144.151 as permitted sender)

D. Suspicious Timeline events:

date	time	timezone	MACB	source	sourcetype	type	user	host
8/6/2010	0:05:09	Australia/Melbourne	.A..	WEBHIST	Firefox Cache	Last Visited Time	-	L33TPC
8/6/2010	0:05:22	Australia/Melbourne	.A..	WEBHIST	Firefox Cache	Last Visited Time	-	L33TPC
8/6/2010	0:05:25	Australia/Melbourne	.A..	WEBHIST	Firefox Cache	Last Visited Time	-	L33TPC
8/6/2010	0:05:26	Australia/Melbourne	.A..	WEBHIST	Firefox Cache	Last Visited Time	-	L33TPC
8/6/2010	0:05:27	Australia/Melbourne	.A..	WEBHIST	Firefox Cache	Last Visited Time	-	L33TPC
8/6/2010	0:05:29	Australia/Melbourne	.A..	WEBHIST	Firefox Cache	Last Visited Time	-	L33TPC
8/6/2010	0:06:36	Australia/Melbourne	.A..	WEBHIST	Firefox Cache	Last Visited Time	-	L33TPC
8/6/2010	0:34:55	Australia/Melbourne	M...	RECBIN	Recycle Bin	Content Deletion	-	L33TPC

						Time		
8/6/2010	0:37:11	Australia/Melbourne	.A..	WEBHIST	Firefox Cache	Last Visited Time	-	L33TPC
8/6/2010	0:37:55	Australia/Melbourne	....	WEBHIST	MSIE Cache File URL record	Last Checked Time	-	L33TPC

short	**Description**	**version**	**filename**	**inode**	**notes**
[HTTP/1.1 200 OK] GET "HTTP:http://www.google.com.au/search?q=firesheep+how+t...	Fetched 1 time(s) [HTTP/1.1 200 OK] GET "HTTP:http://www.google.com.au/search?q=firesheep+how+to&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a"	2	TSK:/Documents and Settings/Ima Hacker/Local Settings/Application Data/Mozilla/Firefox/Profiles/65qsm3on.default/Cache/_CACHE_001_	15283	-
[HTTP/1.1 200 OK] GET "HTTP:http://codebutler.com/firesheep"	Fetched 1 time(s) [HTTP/1.1 200 OK] GET "HTTP:http://codebutler.com/firesheep"	2	TSK:/Documents and Settings/Ima Hacker/Local Settings/Application Data/Mozilla/Firefox/Profiles/65qsm3on.default/Cache/_CACHE_001_	15283	-
[HTTP/1.1 302 Found] GET "HTTP:http://www.go	Fetched 1 time(s) [HTTP/1.1 302 Found] GET "HTTP:http://www.google.com.au/url?sa=t&source=web&cd=6&ved=0CDsQFjAF&url=http%3A%2F%2Fpinglio.com%2F2010%2F11%2Fhow-to-install-and-use-firesheep%2F&ei=Rpm2TdWPJIaIvgPdqtGiAw&usg=AFQjCNEMK	2	TSK:/Documents and Settings/Ima Hacker/Local	15283	-

ogle.com.au/url?sa=t&source=web&c…	sXxsppTEUIuBLKe0g2FfYDdBg"		Settings/Application Data/Mozilla/Firefox/Profiles/65qsm3on.default/Cache/_CACHE_001_		
[HTTP/1.1 200 OK] GET "HTTP:http://pinglio.com/2010/11/how-to-install-and-use...	Fetched 1 time(s) [HTTP/1.1 200 OK] GET "HTTP:http://pinglio.com/2010/11/how-to-install-and-use-firesheep/"	2	TSK:/Documents and Settings/ImaHacker/Local Settings/Application Data/Mozilla/Firefox/Profiles/65qsm3on.default/Cache/_CACHE_001_	152833	-
[HTTP/1.1 200 OK] GET "HTTP:http://www.pcworld.com/article/209333/how_to_hija...	Fetched 1 time(s) [HTTP/1.1 200 OK] GET "HTTP:http://www.pcworld.com/article/209333/how_to_hijack_facebook_using_firesheep.html"	2	TSK:/Documents and Settings/ImaHacker/Local Settings/Application Data/Mozilla/Firefox/Profiles/65qsm3on.default/Cache/_CACHE_001_	152833	-
[HTTP/1.1 200 OK] GET "HTTP:http://www.facebook.com/extern/login_status.ph?a...	Fetched 1 time(s) [HTTP/1.1 200 OK] GET "HTTP:http://www.facebook.com/extern/login_status.php?api_key=9cccf2c9570e99aeb7ea4a7284b957a1&app_id=9cccf2c9570e99aeb7ea4a7284b957a1&channel_url=http%3A%2F%2Fstatic.ak.fbcdn.net%2Fconnect%2Fxd_proxy.php%3Fversion%3D0%23cb%3Df2118b3a1651dee%26origin%3Dhttp%253A%252F%252Fcodebutler.com%252Ff1e12dbcabb65dc%26relation%3Dparent.parent%26transport%3Dpostmessage&display=hidden&extern=2&locale=en_US&method=auth.status&next=http%3A%2F%2Fstatic.ak.fbcdn.net%2Fconnect%2Fxd_proxy.php%3Fversion%3D0%23cb%3Df32a4e2dd629546%26origin%3Dhttp%253A%252F%252Fcodebutler.com%252Ff1e12dbcabb65dc%26relation%3Dparent%26transport%3Dpostmessage%26frame%3Df2ccda6a7ba7204%26result%3D%2522xxRESULTTOKENxx%2522&no_	2	TSK:/Documents and Settings/ImaHacker/Local Settings/Application Data/Mozilla/Firefox/Profiles/65qsm3on.default/Cache/_CACHE_002_	153324	-

	session=http%3A%2F%2Fstatic.ak.fbcdn.net%2Fconnect%2Fxd_proxy.php%3Fversion%3D0%23cb%3Df2286917da8d48a%26origin%3Dhttp%253A%252F%252Fcodebutler.com%252Ff1e12dbcabb65dc%26relation%3Dparent%26transport%3Dpostmessage%26frame%3Df2ccda6a7ba7204&no_user=http%3A%2F%2Fstatic.ak.fbcdn.net%2Fconnect%2Fxd_proxy.php%3Fversion%3D0%23cb%3Df29e60e86194b4c%26origin%3Dhttp%253A%252F%252Fcodebutler.com%252Ff1e12dbcabb65dc%26relation%3Dparent%26transport%3Dpostmessage%26frame%3Df2ccda6a7ba7204&ok_session=http%3A%2F%2Fstatic.ak.fbcdn.net%2Fconnect%2Fxd_proxy.php%3Fversion%3D0%23cb%3Df1c6d46a22bd62%26origin%3Dhttp%253A%252F%252Fcodebutler.com%252Ff1e12dbcabb65dc%26relation%3Dparent%26transport%3Dpostmessage%26frame%3Df2ccda6a7ba7204&sdk=joey&session_version=3"				
[HTTP/1.1 200 OK] GET "HTTP:http://www.facebook.com/extern/login_status.php?a...	Fetched 1 time(s) [HTTP/1.1 200 OK] GET "HTTP:http://www.facebook.com/extern/login_status.php?api_key=113869198637480&app_id=113869198637480&channel_url=http%3A%2F%2Fstatic.ak.fbcdn.net%2Fconnect%2Fxd_proxy.php%3Fversion%3D0%23cb%3Df268a6a7485c968%26origin%3Dhttp%253A%252F%252Fpinglio.com%252Ff2d8f5888a4dc38%26relation%3Dparent.parent%26transport%3Dpostmessage&display=hidden&extern=2&locale=en_US&method=auth.status&next=http%3A%2F%2Fstatic.ak.fbcdn.net%2Fconnect%2Fxd_proxy.php%3Fversion%3D0%23cb%3Df26dce17a90032%26origin%3Dhttp%253A%252F%252Fpinglio.com%252Ff2d8f5888a4dc38%26relation%3Dparent%26transport%3Dpostmessage%26frame%3Df12f2c6090c30e4%26result%3D%2522xxRESULTTOKENxx%2522&no_session=http%3A%2F%2Fstatic.ak.fbcdn.net%2Fconnect%2Fxd_proxy.php%3Fversion%3D0%23cb%3Df29665961b2465a%26origin%3Dhttp%253A%252F%252Fpinglio.com%252Ff2d8f5888a4dc38%26relation%3Dparent%26transport%3Dpostmessage%26frame%3Df12f2c6090c30e4&no_user=http%3A%2F%2Fstatic.ak.fbcdn.net%2Fconnect%2Fxd_proxy.php%3Fversion%3D0%23cb%3Df324349148336c%26origin%3Dhttp%253A%252F%252Fpinglio.com%252Ff2d8f5888a4dc38%26relation%3Dparent%26transport%3Dpostmessage%26frame%3Df12f2c6090c30e4&ok_session=http%3A%2F%2Fstatic.ak.fbcdn.net%2Fconnect%2Fxd_proxy.php%3Fversion%3D0%23cb%3Df27331b00299628%26origin%3Dhttp%253A%252F%252Fpinglio.com%252Ff2d8f5888a4dc38%26relation%3Dparent%26transport%3Dpostmessage%26frame%3Df12f2c6090c30e4&sdk=joey&session_version=3"	2	TSK:/Documents and Settings/Ima Hacker/Local Settings/Application Data/Mozilla/Firefox/Profiles/65qsm3on.default/Cache/_CACHE_002_	15324	-
Deleted file: C:\Documents and Settings\Im	DC33 -> C:\Documents and Settings\Ima Hacker\My Documents\Brisbane 2010\You've been hacked! - Inbox - 'Yahoo!7 Mail'.htm (from drive: C)	2	TSK:/RECYCLER/S-1-5-21-1935655697-1757981266	11343	-

a Hacker\My Documents \Brisbane 2010...			-725345543-1003/INFO2		
[HTTP/1.1 302 Found] GET "HTTP:http ://www.go ogle.com/s earch?q=i% 27ve+been +hac...	Fetched 1 time(s) [HTTP/1.1 302 Found] GET "HTTP:http://www.google.com/search?q=i%27ve+been+hacked+image&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a"	2	TSK:/Documents and Settings/Ima Hacker/Local Settings/Application Data/Mozilla/Firefox/Profiles/65qsm3on.default/Cache/_CACHE_001_	1552833	-
Location: http://profile.ak.fbcdn.net/hprofile-ak-snc4/211272_1000023695656 36...	Location: http://profile.ak.fbcdn.net/hprofile-ak-snc4/211272_100002369565636_3948015_n.jpg Number of hits: 4 Cached file: UDM5CTEP\211272_100002369565636_3948015_n[1].jpg Cached file size: 6374 HTTP headers: HTTP/1.1 200 OK - Content-Type: image/jpeg - X-Backend: hs752.snc6 - X-Blockid: 211272 - X-Orig-Cache-by: 016 - Content-Length: 6374 - - ~U:ima hacker -	2	TSK:/Documents and Settings/Ima Hacker/Local Settings/Temporary Internet Files/Content.IE5/index.dat	103400	-

format	Extra
firefox_cache	data_size: 23027; info_size: 260; location: 0; major: 1; minor: 12; request_size: 127; sha256_hash: f0c8fece1730384028d4d19786d251cde1a6741290d1f4fce6a6a2a1800b3580; version: 1
firefox_cache	data_size: 69506; info_size: 526; location: 0; major: 1; minor: 12; request_size: 37; sha256_hash: f0c8fece1730384028d4d19786d251cde1a6741290d1f4fce6a6a2a1800b3580; version: 1
firefox_cache	data_size: 0; info_size: 294; location: 0; major: 1; minor: 12; request_size: 213; sha256_hash: f0c8fece1730384028d4d19786d251cde1a6741290d1f4fce6a6a2a1800b3580; version: 1
firefox_cache	data_size: 8069; info_size: 397; location: 0; major: 1; minor: 12; request_size: 66; sha256_hash: f0c8fece1730384028d4d19786d251cde1a6741290d1f4fce6a6a2a1800b3580;

	version: 1
firefox_cache	data_size: 20884; info_size: 402; location: 0; major: 1; minor: 12; request_size: 87; sha256_hash: f0c8fece1730384028d4d19786d251cde1a6741290d1f4fce6a6a2a1800b3580; version: 1
firefox_cache	data_size: 58; info_size: 231; location: 0; major: 1; minor: 12; request_size: 1441; sha256_hash: 06bd2c7e792dd0c9183d1b2b46ce340b19a4b065eb2130cba75bd4c8b9f8a464; version: 1
firefox_cache	data_size: 58; info_size: 231; location: 0; major: 1; minor: 12; request_size: 1391; sha256_hash: 06bd2c7e792dd0c9183d1b2b46ce340b19a4b065eb2130cba75bd4c8b9f8a464; version: 1
recycle_bin_info2	drive_number: 2; file_size: 0; sha256_hash: e0b531d60b7f93fa72e046e6fb4b1e29604efb9743bd5b3b3718aca5805ee396
firefox_cache	data_size: 0; info_size: 383; location: 0; major: 1; minor: 12; request_size: 132; sha256_hash: f0c8fece1730384028d4d19786d251cde1a6741290d1f4fce6a6a2a1800b3580; version: 1
msiecf	cache_directory_index: 2; cache_directory_name: UDM5CTEP; cached_filename: 211272_100002369565636_3948015_n[1].jpg; recovered: False; sha256_hash: 2327d0e33de92e156a0c10174b702b980fdf4d5ba701acf02ee0d5cbe674ab90

E. Suspicious Deleted file list:

File name or path	Written date	Accessed Date	Changed date	Created date	File size (byte)	Meta
C:/RECYCLER/S-1-5-21-1935655697-1757981266-725345543-1003/Dc33.htm	2010-08-06 01:35:19 (AEST)	2010-08-06 01:35:19 (AEST)	2010-08-06 01:35:48 (AEST)	2010-08-06 01:35:19 (AEST)	0	17116-128-1

Overall Summary (keeping timelines relative to that of the autopsy browser)

On the first day Ima Hacker arrived at hotel (many days before day of the attack), he had sent an email to learntohack@hmamail.com saying that "he has gained access to the network and could see everyone's traffic"

On the day of the attack, at first a Google search had been made on "firesheep how to". Then firesheep in the codebutler website had been accessed. After that, a Google search had been made on "how to install and use firesheep". Then a pinglio website article "how to install and use firesheep" had been accessed. After that a pcworld website's article "how to hijack

facebook using firesheep" had been accessed. Later on, a Facebook login page had been attacked using codebutler and pinglio respectively, but both cases had failed.

After that, a different approach had been tried in which somepoor's yahoo email's username and password had been stolen with the help of wireshark. Soon after, an email to had been sent to learntohack@hmamail.com saying that "he couldn't get firesheep to hijack the session of a person logging into yahoo, but got his password as the person had checked his email via pop."

Later on, somepoor's yahoo email's username and password had been used access his yahoo email in order to reset the password set on somepoor's Facebook account and access it.

During that time a file had been deleted which had the following title: "You've been hacked! - Inbox - 'Yahoo!7 Mail'.htm" which was quite similar to the information shown in the exhibit 2, but in text instead of picture.

After that, 4 emails had also been deleted from somepoor's yahoo email, before being signed off and accessing somepoor's Facebook account

Then a Google search had been made for pictures saying "You have been hacked" and a picture was downloaded and saved as Hacked_Notification.jpg. Then that picture was uploaded to somepoor's Facebook page.

After that a screenshot of somepoor's Facebook page had been taken and saved as victim's facebook.bmp. During this time, an email had been sent to learntohack@hmamail.com saying that "the facebook account had been hacked by using the person's yahoo account to reset the facebook's password" along with the Hacked_Notification.jpg as an attachment

So overall, yes Ima Hacker had indeed accessed somepoor victim's Facebook account without authority (by using the victim's yahoo email) while somepoor had stayed in the hotel in Brisbane.

Explanation of the communication method between the hacker and the collaborator and use of “hidemyass”:

How I located the evidence:

I had been informed that Ima Hacker may had a collaborator who used website hidemyass.com (it is an anonymous email service) as an email dropbox to communicate with him and had been tasked to find the collaborator’s email address and any email communication.

So I used the forensic tool (autopsy) to search for files with names hidemyass. But no such file had been found. So I tried doing a string search with it instead, but still nothing was found.

So I looked about it online and found out that it uses an acronym “hma”. This made me remember the learntohack@hmamail.com that Ima Hacker had been communicating with during attack1 (on hackable’s website) and just before and during the attack 3 (somepoor’s Facebook attack in Brisbane hotel). Thus I quickly noted down the emails sent by Ima Hacker to that email address, noting them down as suspicious emails.

Furthermore, I had also used the forensic tool (autopsy) to check all the other emails Ima Hacker had sent (by checking Sent Items.bdx in Microsoft outlook folder), but didn’t find anything else related to hidemyass or hma, other than those email correspondence. So I noted down that file details as suspicious file

Overall Evidence list:

A. Suspicious Emails:

To	From	Date	Subject	X-Mailer
<learntohack@hmamail.com>	"Ima Hacker" <imahacker72@yahoo.com.au>	4 May 2010 23:30:35	ipcscan worked!	Microsoft Outlook Express 6.00.2900.2180
<learntohack@hmamail.com>	"Ima Hacker" <imahacker72@yahoo.com.au>	Fri, 30 Jul 2010	arrived at	Microsoft

		00:18:35 +1000	hotel	Outlook Express 6.00. 2900. 2180
<learntohack@hmamail.com>	"Ima Hacker" <imahacker72@yahoo.com.au>	Fri, 6 Aug 2010 01:28:24 +1000	Re: arrived at hotel	Microsoft Outlook Express 6.00. 2900. 2180
<learntohack@hmamail.com>	"Ima Hacker" <imahacker72@yahoo.com.au>	4 May 2010 23:30:35	ipcscan worked!	Microsoft Outlook Express 6.00. 2900. 2180

B. Suspicious file:

File name or path	Written date	Accessed Date	Changed date	Created date	File size (byte)	Meta
C:/Documents and Settings/Ima Hacker/Local Settings/Application Data/Identities/{6FE73E6F-28AF-4574-90D1-A0B477E9D564}/Microsoft/Outlook Express/Sent Items.dbx	2010-10-14 02:18:38 (AEST)	2010-10-14 02:18:38 (AEST)	2010-10-14 02:18:38 (AEST)	2010-05-04 22:57:32 (AEST)	207572	15284-128-4

Overall Summary (keeping timelines relative to that of the autopsy browser)

Overall Ima Hacker had a collaborator who had used the email address learntohack@hmamail.com. Ima Hacker had used that email in order to send 4 messages which have been mentioned briefly in the evidence above and also in their relevant scenario. In those emails, he had said the following information:

A. “he had gotten into hackable server using ipscan using their backup password “backup” and was just playing around now”
B. “he had connected his pc to the network in hotel in Brisbane and could see everyone’s traffic and that he would try using firesheep thing soon”
C. “firesheep didn’t work as he wasn’t able to hijack the session but he has been able to gain the person’s email address and password”
D. “he had pawned that guy’s facebook too by using reset password feature using that person’s email address” and had also sent the attachment “Hacked_Notification.jpg” on the last email

Conclusion:

Overall, I had finished my investigation at 10:55PM (AEST) and had found detailed proof which showed that the 3 of the 4 alleged hacking events had indeed occurred and had been committed by Ima Hacker, all of which had been noted in details in each event. But the 2nd event of “similar website hacking attack at 2:22 AM on 4th March 2009” had not occurred (although hacking events had indeed taken place before and after the noted time on that day)

Furthermore, I had also done a final hash of all the exhibits provided to me, including the forensic image, from the police and the Timescanner super timeline from Troy and it had remained same. This showed that the evidence had not been modified during my investigation. Now I am going to handover the report to the police for their prosecution.