Ishika Batra

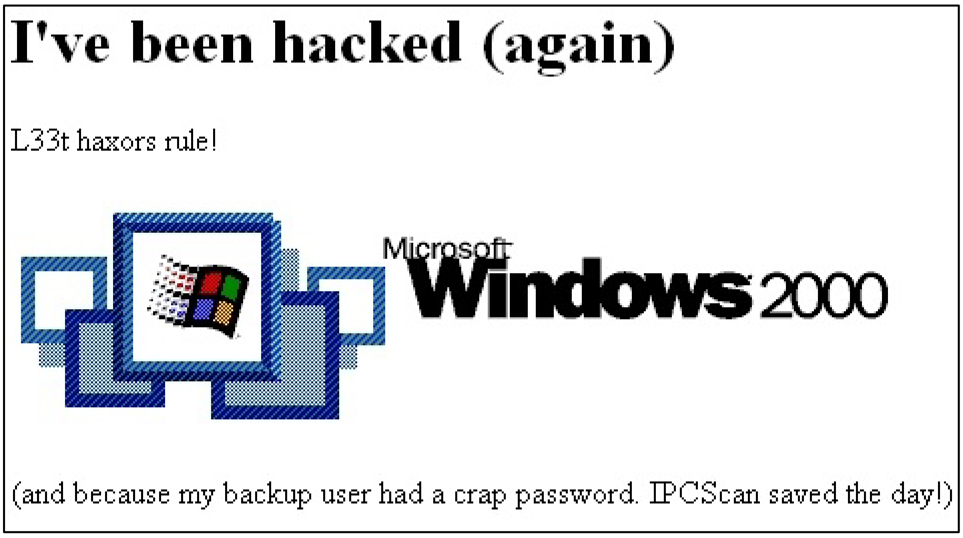
103126718

ICT30010 E-Forensics Fundamentals

Capstone Report

Scenario-

In October 2010, a warrant was executed on the residence of Imanuel Leet-Hacker (aka Ima Hacker), after police received numerous reports of hacking activities tracing back to his IP address. **On 5 May,2022, at 6:30PM**, I was provided a download link to access the forensic image **(ImaHacker.E01**), which the police have created, to make investigation of a computer that was believed to be used for most of his hacking activities. Besides the forensic image, police have also provided me with the following two exhibits-



I've been hacked (again)

L33t haxors rule!

(and because my backup user had a crap password. IPCScan saved the day!)

Figure 1: Hackable's webserver front page

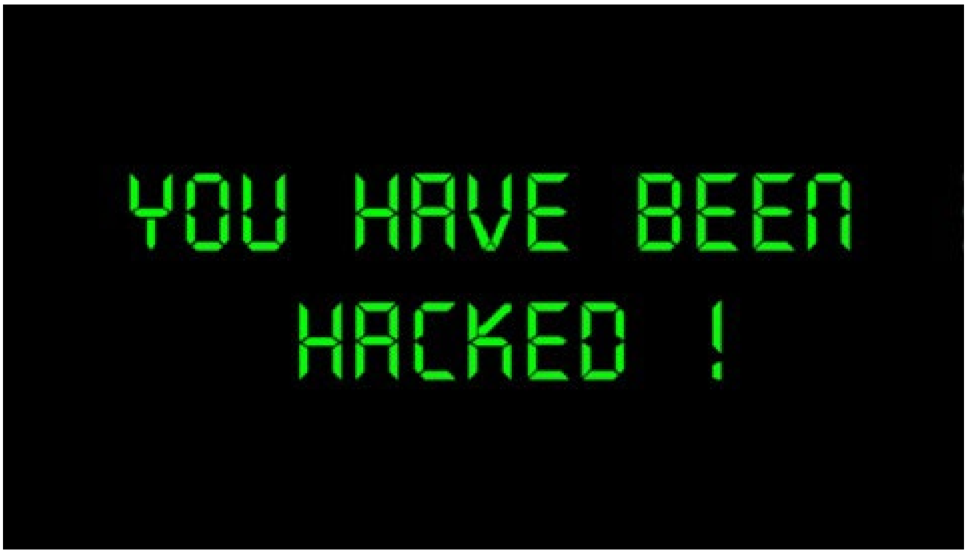


Figure 2: Image file uploaded to Somepoor Victim's Facebook

On reviewing the forensic image my colleague Troy has generated a **detailed timeline** of system events in the form of "Timescanner Super Timeline" that contains operating system artefacts and internet history relevant to my investigation, this was provided to me via email from Troy on the **same day at 6:40PM**.

In this report I will be providing detailed evidence which will prove whether Ima Hacker was involved in the four scenarios of “hackable.com.au” got hacked, second website attack, Facebook account hack and whether he communicated with the collaborator.

Intended Audience-

Police, Lawyers, judges, another forensic examiner, and other non-technical people.

Tools used-

WireShark
This is a network protocol analyzer giving the user access to examine what’s happening in their network on a microscopic level.

Command prompt
A command line interface included in Microsoft Windows.

RegRipper
RegRipper is a tool which extracts pre-defined registry keys and creates a report

Autopsy
This is a digital forensics platform and graphical interface to the Sleuth kit and other digital forensics tools. Used by law enforcements, military and corporate examiners to be able to investigate what happened on computers.

Forensic Analysis-

1. On 23 May 2022 at 8:30pm, I started the investigation on SIFT Workstation and copied the forensic image provided in a new folder, **capstoneFiles**, in the virtual machine.
2. At 8:40pm, I changed the time and date settings of the virtual machine manually to Melbourne which made it equal to the current time zone.
3. On the same day at 8:45pm, I used some forensic tools (EWF tools-> *EWF files are a type of disk image, i.e., files that contain the contents and structure of an entire data storage device, a disk volume, or (in some cases) a computer's physical memory (RAM).)* to check that there is no change in the image during the process of copying. The process was successful, and the hash values of the file was verified. The details are mentioned below:

Acquiry Information		
	Description	ImaHacker
	Evidence Number	Capstone Lab
	Notes	Ima Hacker’s PC – Seized 15/10/10
	Acquisition Date	Thu May 26 12:58:54 2011
	System Date	Thu May 26 12:58:54 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
	Bytes per sector	512 bytes
	Number of sectors	41943040
	Media Size	20 GB (21474836480 bytes)
Digest hash information		

	MD5	16dc3a3dcb703e62f5b3dbe3b4ab8a10
	SHA1	b4da388ef7196fed5bbd60a0b2497f19b94407ef

4. At 8:50pm I identified the partition of the forensic image and got the following information:

Partition name	Partition Type	Start Sector	End Sector	Total Sectors	Total Size (MB)
ImaHacker.E01	NTFS (0x07)	63	41,913,584	41,913,522	20,465 MB

5. At 8:55pm, I accessed the raw disk image contained within E01 and mounted the file in */mnt/windows_mount* in read only format so that I do not override any information in it and it is easily accessible via GUI.

6. At 9pm, I ran the RegRipper tool over the system registry to examine the window registry settings.

7. From the registry, I noted the TimeZoneInformation key and noted the following:

LastWriteTime	DaylightName	StandardName
Thu Jan 1 00:00:00 1970 (UTC)	AUS Eastern Standard Time	AUS Eastern Standard Time

8. At 9:05pm, I tried to locate any common type of email database- Microsoft outlook or Outlook express using some tools in command prompt. In the result of this search, I located 8 emails in- *./Documents and Settings/Ima Hacker/Local Settings/Application Data/Identities/{6FE73E6F-28AF-4574-90D1-A0B477E9D564}/Microsoft/Outlook Express/*
9. I installed an email extraction tool (undbx-0.21) to extract the email files and created a new folder(**emails**) to store these emails in it.
10. At 9:10pm, I created a new case in Autopsy Forensic Browser to start the investigation of the cases.

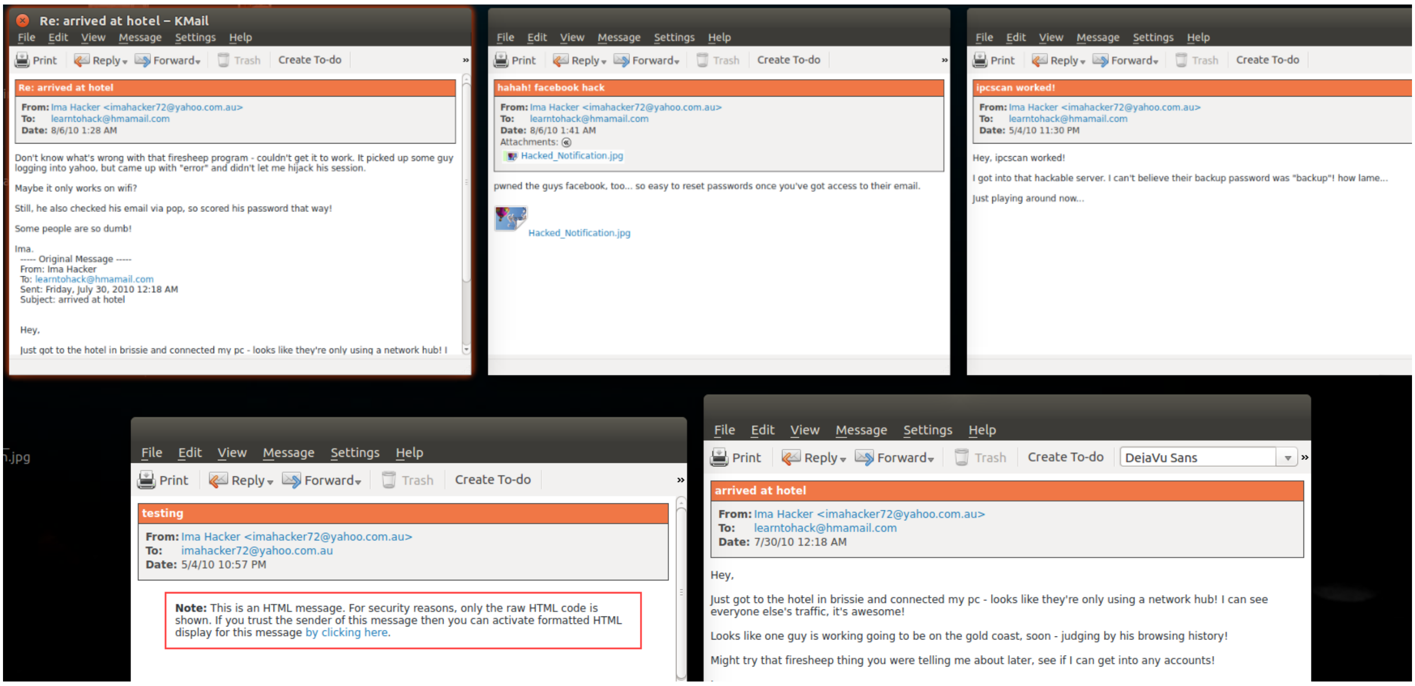
Cases:

Case 1- Involvement of Ima Hacker and Collaborator

After a suspicious belief of Ima Hacker is involved with another collaborator. It is believed he uses a website named hidmyass.com as an email dropbox where his friends and other hackers are able to communicate with each other. This investigation is conducted to provide evidence of such activity.

I navigated to the emails folder in GUI and searched all the folders and got just 1 email in the deleted folder, inbox and outbox and 5 in the sent items.

The email in the deleted folder was a self-ping testing email which imahacker72@yahoo.com.au sent to himself. The email in the inbox was sent from Microsoft outlook to the newly joined users. Four of the emails in the sent items are sent from imahacker72@yahoo.com.au to learntohack@hmamail.com on different days mostly giving information about where he is and what is he planning to do.


Re: arrived at hotel – KMail
File Edit View Message Settings Help
Print Reply Forward Trash Create To-do
DejaVu Sans
.jpg

Re: arrived at hotel

From: Ima Hacker <imahacker72@yahoo.com.au>
To: learntohack@hmamail.com
Date: 8/6/10 1:28 AM

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!

Ima.
----- Original Message -----
From: Ima Hacker
To: learntohack@hmamail.com
Sent: Friday, July 30, 2010 12:18 AM
Subject: arrived at hotel

Hey,

Just got to the hotel in brissie and connected my pc - looks like they're only using a network hub! I

hahah! facebook hack

From: Ima Hacker <imahacker72@yahoo.com.au>
To: learntohack@hmamail.com
Date: 8/6/10 1:41 AM
Attachments:
Hacked_Notification.jpg

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

Hacked_Notification.jpg

ipcscan worked!

From: Ima Hacker <imahacker72@yahoo.com.au>
To: learntohack@hmamail.com
Date: 5/4/10 11:30 PM

Hey, ipcscan worked!

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

Just playing around now...

testing

From: Ima Hacker <imahacker72@yahoo.com.au>
To: imahacker72@yahoo.com.au
Date: 5/4/10 10:57 PM

Note: This is an HTML message. For security reasons, only the raw HTML code is shown. If you trust the sender of this message then you can activate formatted HTML display for this message by clicking here.

arrived at hotel

From: Ima Hacker <imahacker72@yahoo.com.au>
To: learntohack@hmamail.com
Date: 7/30/10 12:18 AM

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!

Figure 3: Emails in the sent items folder

Ima Hacker communicates with only one person and informs him about the attacks he did or his plannings who is learntohack@hmamail.com and the hmamail service is provided by HideMyAss and thus Ima Hacker is involved with a collaborator.

Case 2- Hackable's website Attack

This investigation is conducted after a company named "Hackable (hackable.com.au)" provided logs to the police which stated that their website was hacked on the 4th of May 2010 (Time not provided). They stated that the IP address traced back to the suspect Ima Hacker.

On 23 May 2022, at 10:00pm, I created a filesystem timeline in the autopsy for the day of attack i.e., 4th May 2010 and started checking it. Exactly at 10:46:44pm in the timeline, server.hackable.com.au was mentioned and it was showing that a file was created related to that.

I searched for "hackable.com.au" in the file name search to find some evidence in this case as the website was named hackable.com.au and I got an xml file(**server.hackable.com.au.xml**) which showed that the hacker was using the IP address - 192.168.75.129 and was initiating a scan at 22:41 on the same day. The hacker was also scanning open ports in the server. The details of server.hackable.com.au.xml are-

File Name	Last Accessed	Last Changed	Created	Path
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)	C:/Program Files/Nmap/server.hackable.com.au.xml

I also searched for server.hackable in the file name search and discovered a new directory. I checked that directory and got four useful files in it.These are the following:

File name	Last Accessed	Last Modified	Created	Location
PAWNED, again! .htm	2010-05-04 23:35:37 (AEST)	2010-05-04 23:35:37 (AEST)	2010-05-04 23:35:36 (AEST)	C:/ /Documents and Settings/ /Ima Hacker/ /My Documents/
win2000.gif (inside PAWNED, again!_files directory)	2010-05-04 23:35:36 (AEST)	2010-05-04 23:35:36 (AEST)	2010-05-04 23:35:36 (AEST)	C:/ /Documents and Settings/ /Ima Hacker/ /My Documents/ /server.hackablePAWNED, again!_files/
users.txt	2010-05-04 23:32:16 (AEST)	2010-05-04 23:32:16 (AEST)	2010-05-04 23:32:16 (AEST)	C:/ /Documents and Settings/ /Ima Hacker/ /My Documents/

One of the files- “users.txt” stored the details of the users (SSIDs,username, active times etc.) which would the hacker probably got from the scan on the server. One of the files was an html file name “pawned, again.htm” which was the html file that had the exact message and image that was provided to me by the police (exhibit 1). The other file stored a gif- “win2000.gif” which was the image used in the html file (pawned, again!.htm).
The last file was “pawned, again!.html:Zone.Identifier”. A file with a "Zone.Identifier" extension contains information about another file. It describes the security zone associated with the file, which may the Internet, local intranet, trusted site, or restricted site. The ZoneId for this file is 3 which stands for Internet. This means pawned, again!.htm is downloaded from Internet and saved in the local disk of the computer automatically. It is mentioned in one of the emails to the collaborator that the working of ipscan helped Ima Hacker to hack the server so in the autopsy timeline I started finding “ipscan” and it noticed that at 11:16:36 pm, the Ipscan.rar was downloaded and after extracting finally the ipscan was accessed in GUI at 11:19:47pm and the IP addresses or open ports of the server were scanned by it.

These evidences makes the fact evident enough to support the alleged “Hackable” attack.

Case 3- Similar Website Attack

This investigation is conducted after a similar website attack was held as Hackable’s website Attack, which occurred on the 4th of March 2009 approximately at 2:22am. The suspect stated that he was shopping at a local 24-hour convenience store at that very moment and had no knowledge of such an attack occurring.

In the timeline provided by my colleague Troy, I checked the entries of this date (4th March 2009) for few hours earlier and later the provided time of attack and found put that before the attack, Ima Hacker was normally searching on Internet- used google, yahoo, Hotmail, blackhat, Facebook, updated his window, checking images on Hackthissite.org etc. Then he did normal search and at 1:19:40 an image was downloaded called Hacker_Wallpaper_1.png which when I searched in autopsy was in his computer.

At 1:10:59am, a search was started for bottle shops and at 1:13:10am and then at 2:13:09am a search on google maps which came out to be “tottenham+cellars +west+foo...”. In the result of search google maps showed the way to Tottenham Cellars West Footscray Victoria. Between 2:20:18am to 2:29:22am there is no activity noted in the timeline. Even after 2:29:22am, opening some images, bookmarking websites, using hack this site and yahoo etc. are noted in the timeline and no such proof of hacking the website at 2:22am. There are not much evidences and it cannot be concluded that the suspect is involved in this attack.

Case 4- Somepoor Victim’s Facebook Hacked

This investigation is conducted after the victim “Somepoor Victim” stated that he had unauthorized access to his Facebook account which holds a Facebook Account ID of **100002369565636** on the 6th of August 2010. It is stated that this was traced back to a hotel located in Brisbane. It is believed that Ima Hacker was residing at this hotel at that point of time. Hotel provided no resource to help with this case.

As suggested by Troy, Ima Hacker seemed to like Wireshark, so I started my investigation by searching “.pcap” files in the file name in autopsy and found two useful pcap files(hotel dump.pcap and hotel dump including email and facebook.pcap) and their directory(Brisbane 2010) and following are their details:

File Name	Last Accessed	Last Modified	Created	Location
hotel dump including email and facebook.pcap	2010-10-14 02:44:40 (AEDT)	2010-10-14 02:44:42 (AEDT)	2010-08-06 01:24:08 (AEST)	C:/ /Documents and Settings/ /Ima Hacker/ /My Documents/ /Brisbane 2010/
hotel dump.pcap	2010-10-14 03:09:55 (AEDT)	2010-10-14 03:09:55 (AEDT)	2010-07-30 00:19:05 (AEST)	C:/ /Documents and Settings/ /Ima Hacker/ /My Documents/ /Brisbane 2010/

I searched for this folder in GUI and got three files- two of the pcap files and an image – “victim’s facebook.bmp”, This image is a screenshot which shows that the same exhibit (exhibit 2) provided by the police to me appears on the somepoor victim’s facebook page when opened.The details of the image file are-

Name	Location	Type	Size	Accessed	Modified
victim's facebook.bmp	/home/sansforensics/Desktop/mount_points/windows_mount/Documents and Settings/Ima Hacker/My Documents/Brisbane 2010	Windows BMP image (image/bmp)	365.0 kB (364,986 bytes)	Thu, Oct 14 2010 02:44:32	Fri, Aug 6 2010 01:40:05

The exact copy of exhibit 2 provided to me by the police was also found on Desktop of Ima Hacker while I was searching for some proofs in GUI.The details of the following are-

Name	Location	Type	Size	Accessed	Modified
Hacked_Notification.jpg	/home/sansforensics/Desktop/mount_points/windows_mount/Documents and Settings/Ima Hacker/Desktop	JPEG Image (image/jpeg)	41.5 kB (41,504 bytes)	Fri, Aug 6 2010 01:38:36	Fri, Aug 6 2010 01:38:32

I investigated the “hotel dump.pcap” and on filtering the result on basis of pop as it is indicated in the emails of Ima Hacker that “pop” helped him in getting the password of somepoorvictim’s email. I got the username and password of Ima Hacker’s email. The packets were captured on 30 July 2010 and the details are-

No.	Time	Source	Destination	Protocol	Length	Info
670	12:06:42am	192.168.17.130	69.147.94.41	POP	85	C:USER imahacker72@yahoo.com.au
673	12:06:43am	192.168.17.130	69.147.94.41	POP	69	C: PASS hs6AS8Oc

The packets also captured the email which Ima Hacker sent to the collaborator on 30 July 2010, in which he writes that he is in a hotel in Brisbane and can see everyone's traffic and is planning to use firesheep(*Firesheep* uses packet sniffers to hijack unencrypted session cookies across websites like Facebook.) to get into user accounts. The packet details are:

No.	Time	Source	Destination	Protocol	Length	Info
16205	12:18:38am	192.168.17.130	209.191.106.133	SMTP	978	C: DATA fragment, 924 bytes

I investigated the "hotel dump including email and facebook.pcap" file. I filtered the wireshark results on the basis of pop and the very first packet shows that somepoor victim received a pop from yahoo to login on 06/08/2010 at 01:18:16 am and the username was entered at this time. The packet details for the same are-

No.	Time	Source	Destination	Protocol	Length	Info
46040	01:18:16 am	192.168.17.129	69.147.94.41	POP	88	C: USER somepoorvictim@yahoo.com.au

The password was entered at 01:18:16am which was 8WXyk5W8 and the packet details are-

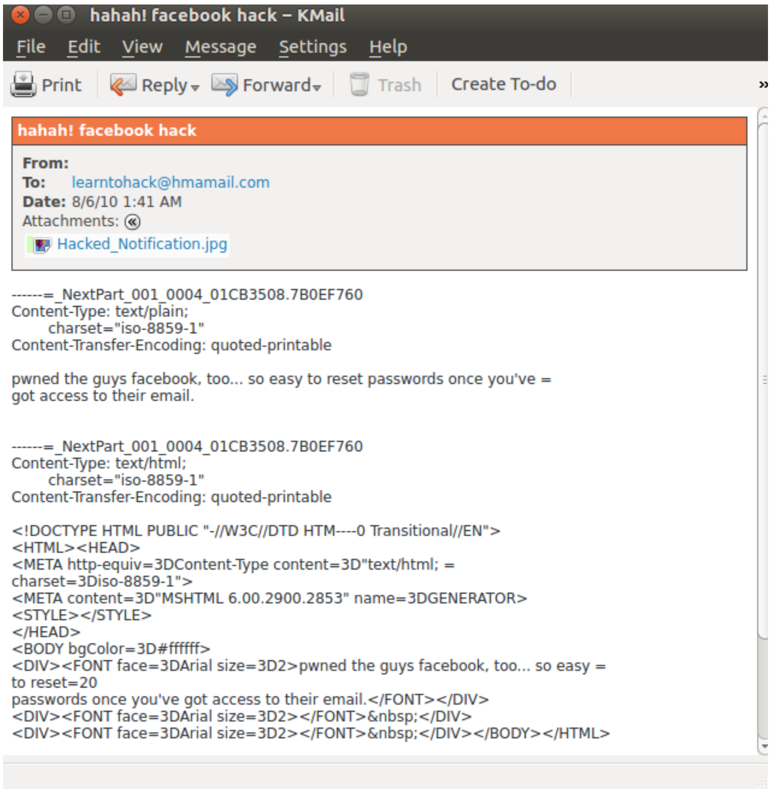
No.	Time	Source	Destination	Protocol	Length	Info
46043	01:18:16 am	192.168.17.129	69.147.94.41	POP	69	C: PASS 8WXyk5W8

There is another packet which has the information that the somepoor victim received an email from facebook in which facebook has sent a login link and then another packet has the password recovery link(contained the text- *" Hi Somepoor ,…. You recently asked to reset your Facebook password…" .)*
at 01:18:20am on 6 August 2010. This is how the new password for facebook was set.

To verify the results of the wireshark packets, I searched for the ID of somepoor victim (100002369565636) in the timeline provided by Troy and got seven results. The records above the facebook recovery were related to yahoo pops, the events occurring in these are already evident in the wireshark packets.

The first record of this ID in the history of Ima Hacker was on 01/01/2009 at 11:00:00 am. The other entry was on 06/08/2010 at 01:37:09am where the account was recovered and at 01:37:58 a picture was uploaded on it. At 05/10/2011 the account of somepoor victim was used again at 08:38:12pm.

This is a deleted email which was sent to learntohack@hmamail.com on the on *8/6/2010 at 1:41 AM*. when Facebook of somepoorvictim was hacked and it is mentioned in the email that the guys facebook has been pawned as the access to his email was got first which made the hacking easy. This email also has an attachment which is the same image that is saved on Ima Hacker's desktop. These all evidence support the accusation on the suspect.


hahah! facebook hack – KMail
File Edit View Message Settings Help
Print
Reply
Forward
Trash
Create To-do

hahah! facebook hack

From:
To: learntohack@hmamail.com
Date: 8/6/10 1:41 AM
Attachments:
Hacked_Notification.jpg

```
------=_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.


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

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTM----0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=3DContent-Type content=3D"text/html; =
charset=3Diso-8859-1">
<META content=3D"MSHTML 6.00.2900.2853" name=3DGENERATOR>
<STYLE></STYLE>
</HEAD>
<BODY bgColor=3D#ffffff>
<DIV><FONT face=3DArial size=3D2>pwned the guys facebook, too... so easy =
to reset=20
passwords once you've got access to their email.</FONT></DIV>
<DIV><FONT face=3DArial size=3D2></FONT>&nbsp;</DIV>
<DIV><FONT face=3DArial size=3D2></FONT>&nbsp;</DIV></BODY></HTML>
```

Figure 4: Email to the collaborator telling him the success of facebook hacking

In the end to ensure the integrity and that nothing has changed during this process, I verified the hash value of the forensic image.

Conclusion-

In this detailed forensic analysis, the emails, Wireshark tool, autopsy and the command line tools altogether helped me to come up to the conclusion on 27 May 2022 at 01:30:24pm that Ima Hacker had a collaborator(hidemyass) with whom he communicated via email and his email address is – learntohack@hmamail.com . There are enough evidences to support that the alleged attack on the website- hackable.com.au, somepoor Victime's facebook account were hacked by Ima Hacker's system. There were not enough evidence to support that Ima Hacker was involved in the second website attack on 4 March 2009.