**//write all in words in the end. Do not give the screenshot pictures as then troy will cut marks!!!**

1.Your explanation of all the evidence received from the Police, how and when it was received and how you handled continuity (chain of custody) of the digital evidence. (1 mark)

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 the Forensic image of the computer seized from residence of the culprit, 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:

|  |  |  |
| --- | --- | --- |
|  | MD5 value | SHA1 value |
|  |  |  |
| Exhibit 1 (Hackable’s website screenshot picture) | cec89fe25b60e9635ae849f2e24fdbb3 | 702f692dda66025b81e480872b277378251b809f |
| Exhibit 2 (Somepoor Victim’s facebook page) | 5674005e22027fd893c8fbc74752bd01 | 2aa6b6e43500ec9e6410ed613fe35776df145f0e |

Moreover, here are the pictures of the two exhibits that have been received:



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



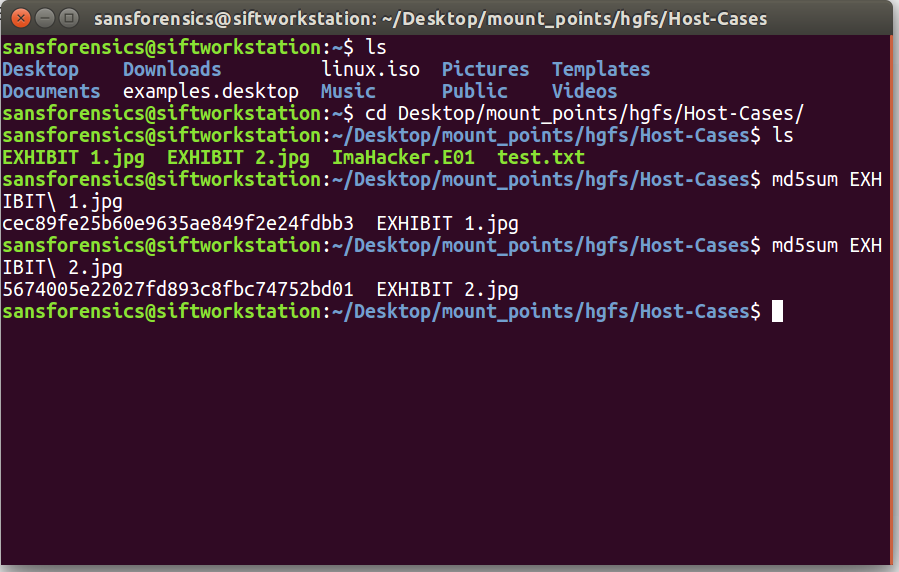
[Exhibit 2: image placed on “Somepoor Victim”’s facebook page]

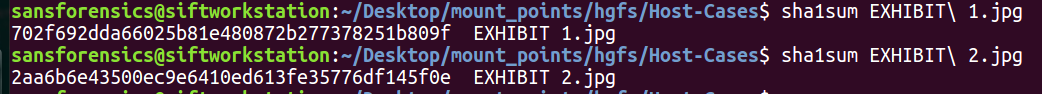
2. Your explanation of the item received from your colleague Troy, how and when it was received and how you handled continuity (chain of custody) of the item. (1 mark)

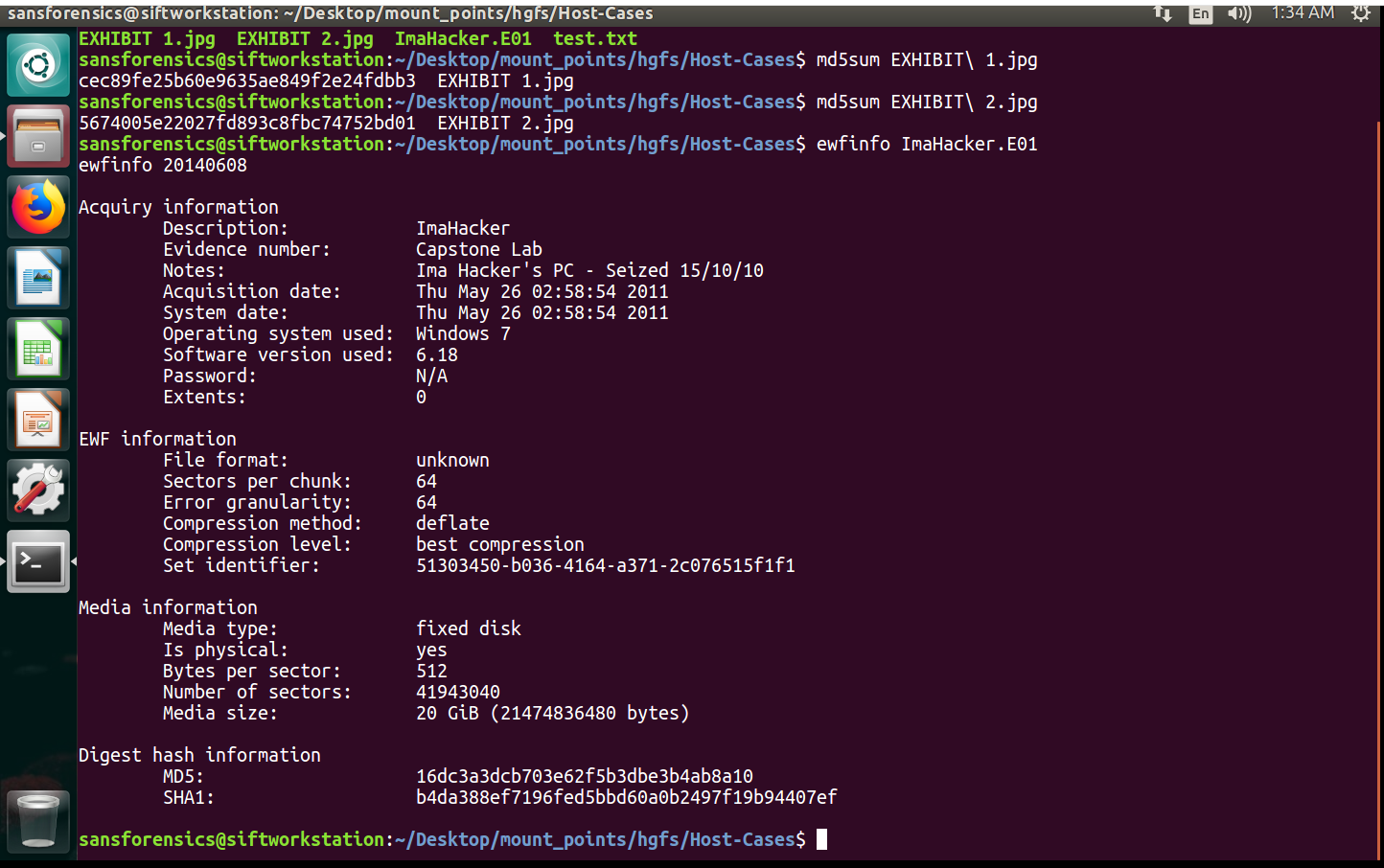
(ALL hashes LIST both obtained and also checked by self:)

. Disk image “ImaHacker.E01” – Downloaded from Canvas

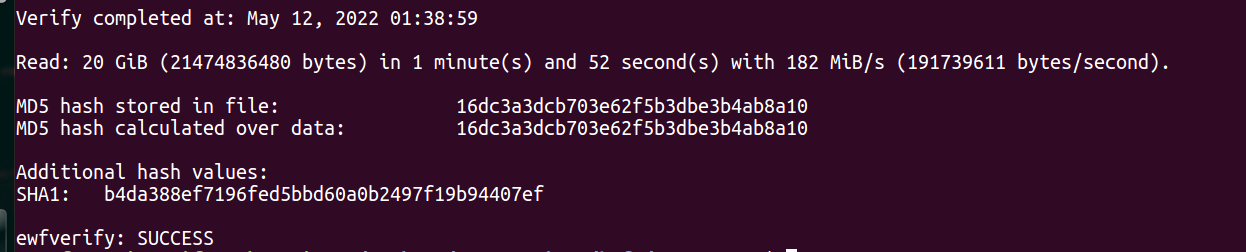
Timeline of system events “timeline.csv” - Email (MD5: 9574ac771fdeeeb9a95d8dda5ed1749a)



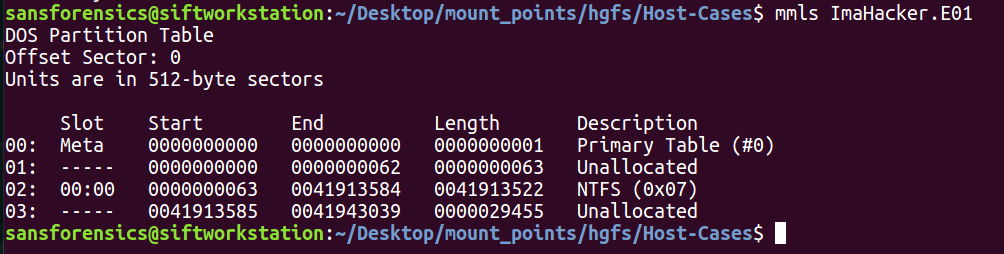




Also did ewfverify to ensure hash contained within was correct..

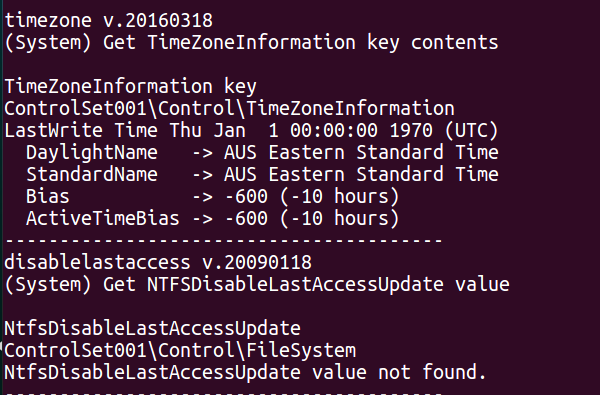


3. Details of the partition contained within the image, and determination of the seized devices time zone (2marks)

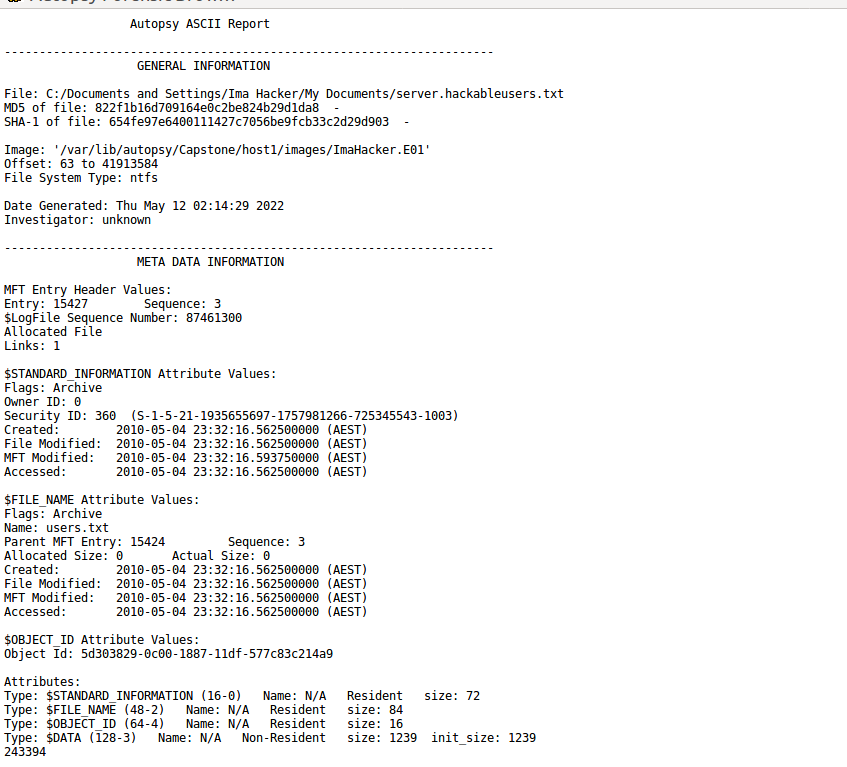


(make partition table format using those datas)

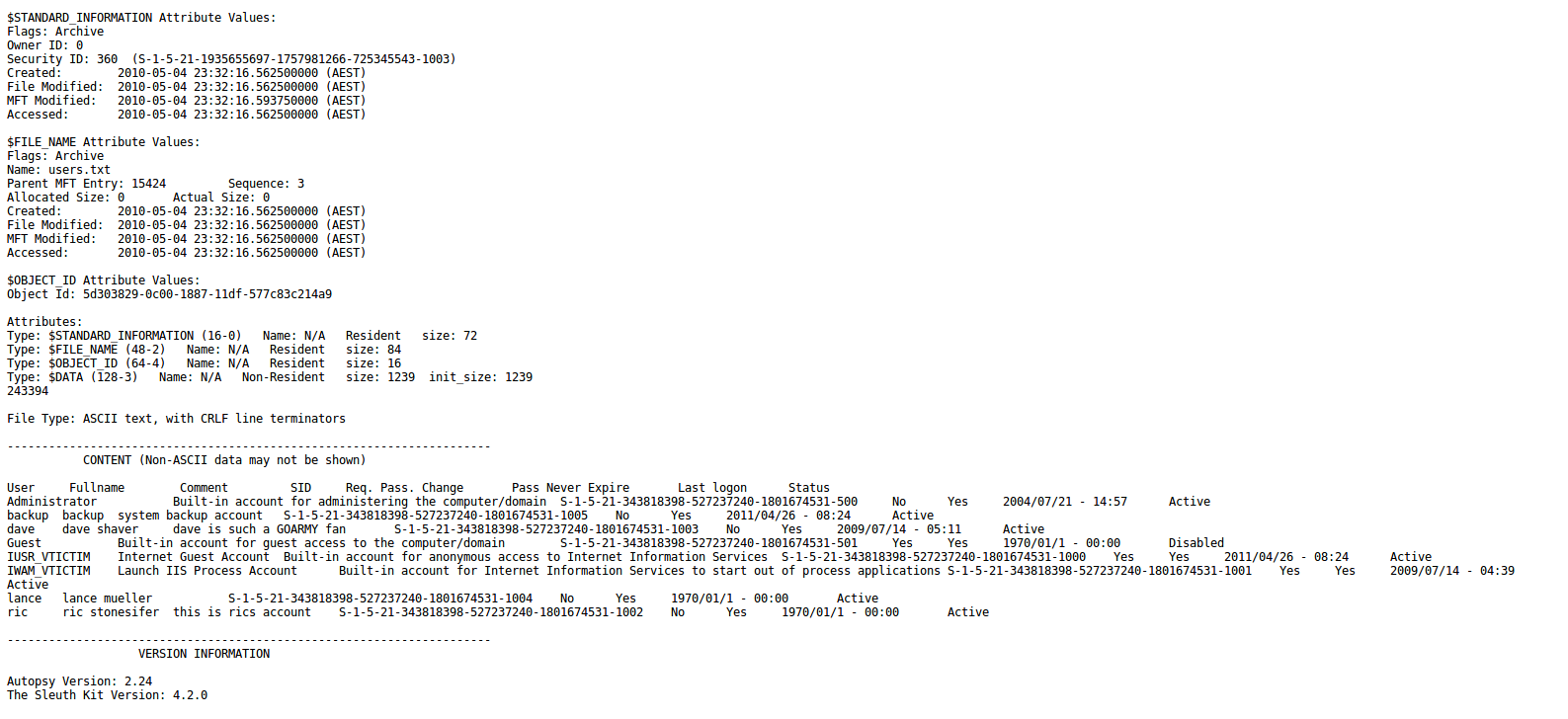
63\*512= 32,256 (starting offset)

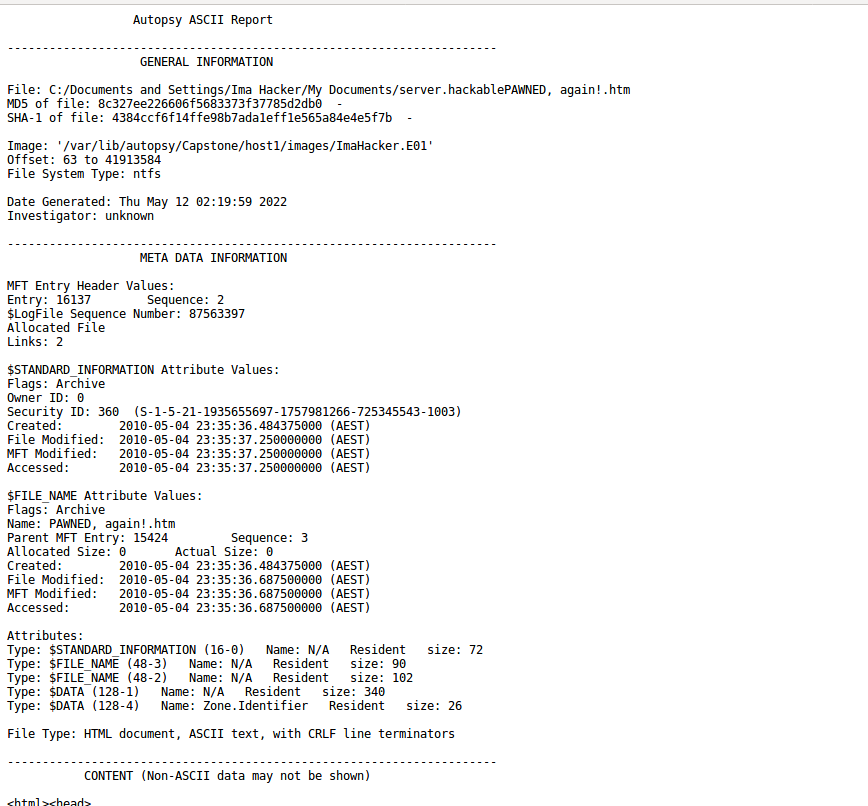


4. Evidence and explanation for the alleged "Hackable" attack (5 marks)



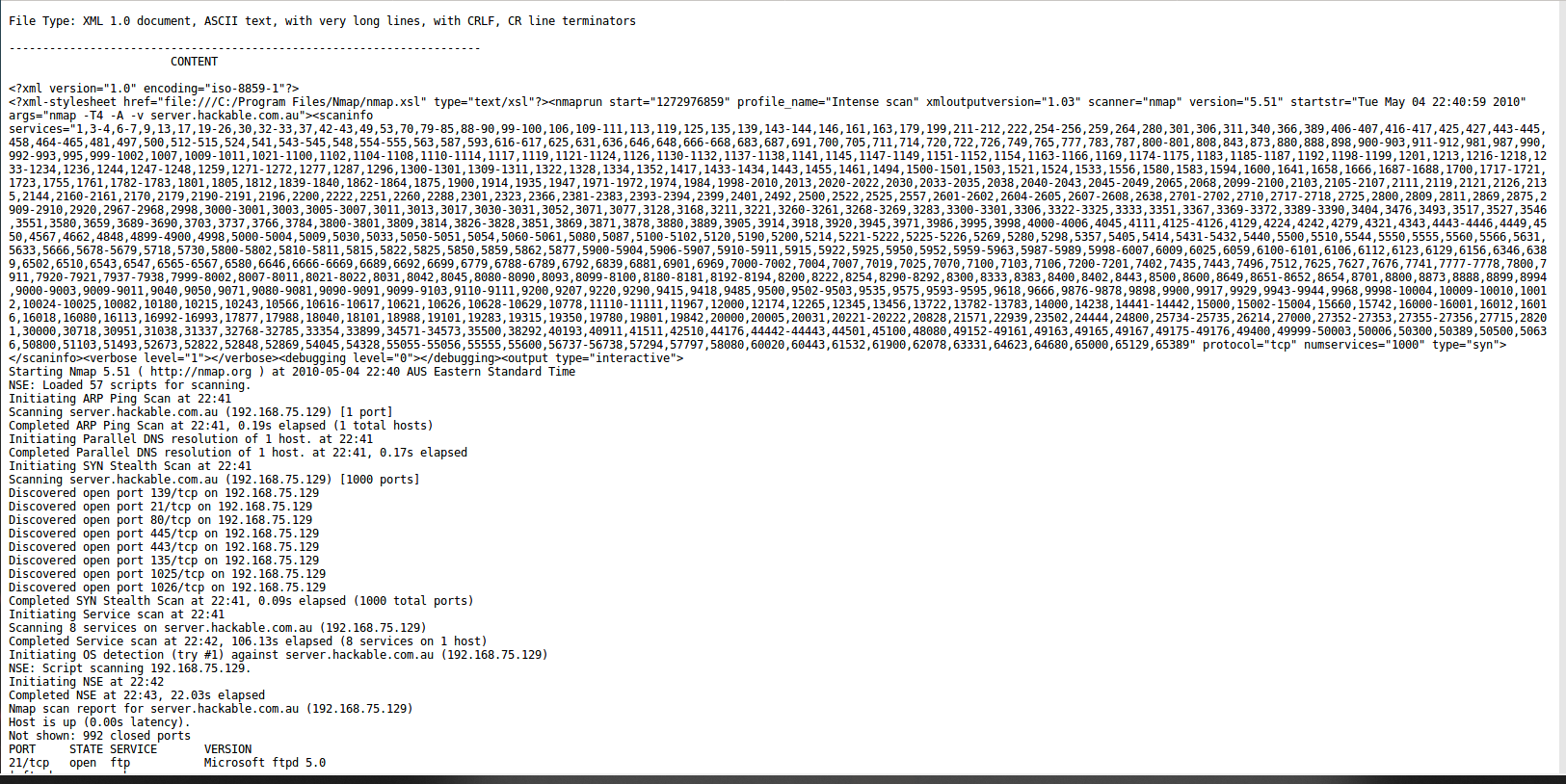
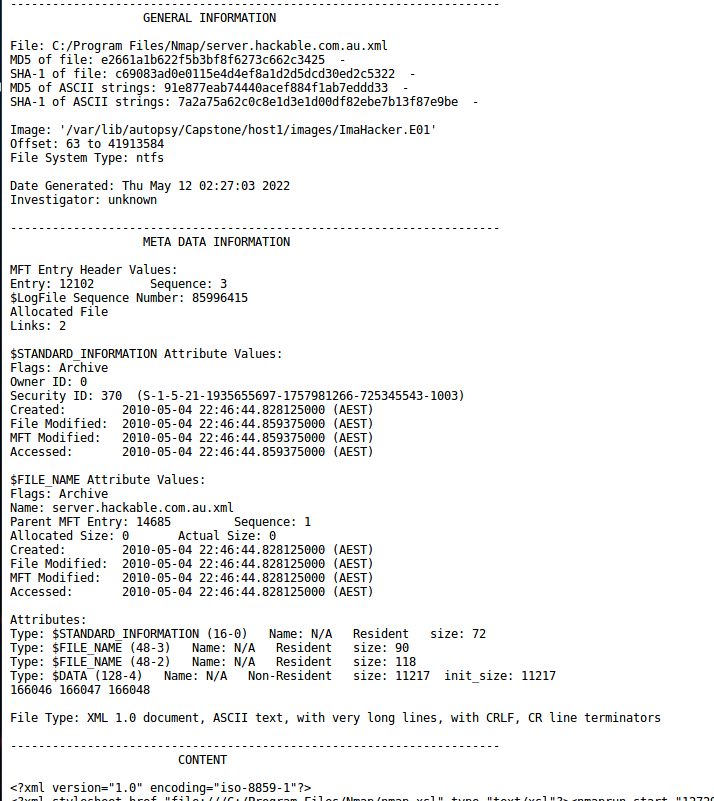
So he attacked and gained access to list of user names





Also he did an nmap attack which

“This program scans the network that a computer is connected to and outputs a list of ports, device names, operating systems, and several other identifiers that help the user understand the details behind their connection status. Nmap can be used by hackers to gain access to uncontrolled ports on a system”



(he attacked at: 22:46:44 2010-05-04 using an NMAP Attack on hackable’s website

At 23:32:16 2010-05-04 he stole users list from the hackable’s website

At 23:35:36 he made(use different wording as he could have downloaded too) the gif file for the logo

At 23:35:36 he also made the webpage that can be seen in exibit 1

(issue is that the md5 and sha1 doesn’t match with that of exibit, so try to find the main webpage on his pc and not just separate parts)

(see everything he did from 22:46:44 to 23:35:36 and see 1 hr before and after the thing in wireshark)

5. Relevant evidence and the explanation of your findings that supports or refutes the hacker’s alibi for the alleged “second” website attack (3 marks)

On that day at 00:48:50, he had visited a site called hackThisSite (maybe, may not be relevant)

6. Evidence and explanation for the alleged Facebook account takeover (5 marks)

recent.capture\_file: C:\Documents and Settings\Ima Hacker\My Documents\Wireshark\Testing pings.pcap

recent.capture\_file: C:\Documents and Settings\Ima Hacker\My Documents\Brisbane 2010\hotel dump.pcap

recent.capture\_file: C:\Documents and Settings\Ima Hacker\My Documents\Brisbane 2010\hotel dump including email and facebook.pcap

He looked up how to attack a fb using firesheep on 26th April 2011 10:07:15 GMT (probably not related to this dude as the fb has occurred in 2010 not 2011) (maybe this is the attack, but he maybe used smth to change to the time settings??) (found the actual time firesheep had been downloaded

Then used it to display a cookie in fb that said “Facebook does not have a P3P policy. Learn why here: <http://fb.me/p3p>”.

Then he got the yahoo email of the victim and used it so send an email seemingly from zukerburg for a fb notification that welcomed him to fb

Then later on he also gave a link to poorvictim for reclogging into his fb account

Then he used these to gain access to the fb account and change the password by requesting for a new password

Later when the email came back to the poorvictim, he accessed and deleted that email before the victim could see it

7. Explanation of the communication method between the hacker and the collaborator including an assessment regarding the use of hidemyass (1 mark)

8. The inclusion of relevant evidence from Timescanner super timeline in your findings (1 mark)

9. Your ability to stick to the facts, and explain your processes and findings in non-technical (but still accurate!) language (2marks) (.5 Reduction for each non-factual statement)

10. Overall presentation of your report (1 mark)