Name: S M Ragib Rezwan
ID: 103172423
Course name: eForensic Fundamentals

Assesment1-Lab 3 Report:

- On 17th March 2022 (Thursday) at around 6:30pm, GoodChem Company hired me to find out whether or not an intellectual property has been stolen from their company.

- At that moment in time, they had given me a zip file named "lab3.tar.gz" which had the following files:
    - A forensic image of the USB drive
    - A text file containing the MD5 hash values of the forensic image
    - A test file containing a list of known files and their MD5 hash values

- Alongside this, (at the same time) they had also provided a set of entries from their server's access logs which they had deemed suspicious.

Date/Time	User	File Accessed	Description
1/Mar/2010 3:04pm	FThompson	GoodChemClientList.xls	a List of all GoodChem's current clients
31/Mar/2010 3:29pm	FThompson	GoodChem Inventory.xls	a list of GoodChem's inventory and current prices
17/Mar/2010 4:15pm	FThompson	Users Summary.xls	a summary of GoodChem user accounts by department
23/Mar/2010 10:38am	FThompson	GoodChemUsers.xls	a list of all usernames and passwords to GoodChem's main database

- So, with all these information, I started my investigation at 6:35pm where I made a new folder "lab3" in the cases directory to store the zip file "lab3.tar.gz". There I had unzipped the file to see the forensic image "lab3.dd".

- Then, at around 6:40pm, I used a forensic tool (md5sum) to compare the hash values between the "lab3.dd" file and the value of the hash provided by the company in the text file, ensuring they were the same.

  (same hash value means data stored in the forensic image is same as that before and no change had occurred to the data)

- After that, at around 6:45pm, I used a forensic tool (fdisk) to find out the partitions on the disk image:
  There it had a sector size of 512 bytes.
  And its partition had the following details:

Partition	Partition Type (e.g. NTFS/FAT)	Start Sector	End Sector	Total Sectors	Total Size (MB)
lab3.dd 1	FAT32	63	3968054	3967992	1937

[Note: here total size came 1937.4960 MB so rounded it off to 1937 MB for ease of view]

- After that, at around 6:50pm, I used a forensic tool (sudo mount) to mount the partition in a read only manner using the starting offset 32256 (in byte) and pre-created mount point directory.
  (I did this to ensure that I access the data in a read only manner and not alter it in any way)

- At 6:55pm, I started to work to see if there had been any files deleted. So at that point in time, I went inside the mount point and noted down directories and number of files in each directories seen from the GUI or user point of view.

- Next, at 7:00pm, I utilized a forensic tool (sleuth kit's "fls") to see all the directories.

[Note: here I had failed at first due to lack of information (starting offset number of partition, the file system type being observed and imagetype). Thus I had to go through the manual to modify the command to look for the file system of fat32 (as noted in partition type before) along with offset (the start sector value noted in partition beforehand) and the type of image it is.]

[Note: the modified command (if needed): fls –f fat32 –i raw –o 63 lab3.dd]

- So, at 7:10pm, I utilized the same forensic tool to run the modified command. This had brought up the following a list of directories and folders including their iNode number which I noted down for later use:

Name	iNode number
Internet Pics	5
Powerpoints	7
Programs	9
Word doc	11

- After this, at 7:15pm, I used the same forensic tool (with the "Word doc" directory's iNode) to go into the "Word docs" directory and see the list of files located in each directory (in order to compare with the original list of files seen in the GUI). There I noticed two deleted files and noted their name and iNode number down:

Name	iNode number
GoodChemUsers.xls	209298
GoodChemUsersSummary.xls	209301

- So I set out to recover those deleted files at 7:20pm. There, I used forensic tool (icat with file's Inode Numbers and file name) to output the information stored in the deleted files to different file names, in the same mounted directory. Then I utilized the OpenOffice application calc present in the VM to open those files to ensure that the information stored in the deleted files has been restored.

- Since it looked like an excel spreadsheet information, at 7:25pm, I used a forensic tool to run a MD5 hash function on those two deleted files and compared those values with that in the list provided by the company. There I found that it does indeed match two of their files (GoodChemUsers.xls and GoodChemUsersSummary.xls).

  (This means that the information contained in the two deleted files were exactly same as the ones on those two files. This also means the files had been deleted from the Word docs directory in order to hide themselves in the forensic image.)

  So, I quickly, I noted their iNode values and numbers in the undeleted files table:

Name	iNode number
GoodChemUsers.xls	209298
GoodChemUsersSummary.xls	209301

- After this, at 7:30pm, I also utilized a forensic tool (istat with iNode values) to find the file's first sector number (i.e. where it is located), size and the written, accessed and created dates and times and noted them down.

File Name	iNode number	First sector number	Size	Written	Accessed	Created
GoodChemUsers.xls	209298	27528	27648	2010-03-17 08:24:46 (UTC)	2010-03-31 00:00:00 (UTC)	2010-03-31 03:28:22 (UTC)
GoodChemUsersSummary.xls	209301	27584	22016	2010-03-17 08:24:36 (UTC)	2010-03-31 00:00:00 (UTC)	2010-03-31 03:28:22 (UTC)

- Then, at 7:35pm, I used the forensic tool (fls) once more to verify that no other deleted items are present in other directories.

- After this, at 7:40pm, I used the forensic tool (sorter) to sort through the files and categorized them based on their signature (in case the files have been renamed to have the wrong extension to hide the fact that they are actually another type of file) and placed them in sorter directory.

- At the same time, I immediately moved to the sorter directory and ran the command to create a summary of the files discovered and noted the results onto the table below:

File type	Image files	Document types
Number of files	12	8

- Then, at 7:45pm, I used the forensic tool to view the text file containing all image information and also opened those files to ensure they can be viewed as image. After that, I also repeated the same with the document type files. There I noticed that the sorter wasn't able to properly extract information from the powerpoint files, but was able to extract the metadata from the word docs and also from the recently recovered excel sheets.

- Since the information from the powerpoints weren't properly displayed, at 7:50pm I had gone back and opened the file. There I noticed that it opened in calc (an open office

application) instead of as a powerpoint which was quite strange. So, I decided to look deeper.

- Thus, at around 7:55pm, I used a forensic tool (xxd) to see the first 16 bits of all the powerpoint files. There all of them had the matching signature and also had the "D0CF 11E0" in the first few bytes.

  (Although these are usually found in different MS office documents, they are also found in documents that use CDF. So their files types couldn't be confirmed in this way.)

- So, at 8:00pm, I used a modification of that forensic tool to see the ending part of the suspicious "awesomejokes.pps" file, while avoiding lines containing all zeroes (just to see the data at the end). There I noticed words pop up including "ms excel", "spreadsheet",etc.

  (This made me realize that it might actually be an excel file in disguise.)

- Hence, at 8:05pm, I decided to check my thought by copying the files into my cases directory with the .xls ending (spreadsheet extension). Then I made a hash file of the information in it and checked it with the list of hash files and file names provided by the company. There I noticed that the hash had matched with the company's "GoodChemClientList.xls".

  (This means the file has been renamed to hide itself in the powerpoint directory of the forensic image.)

- So I noted down its current name, iNode number and then also used the forensic tool (using that iNode number) to find the file's size and written, accessed and created date and times and noted them down as well in the renamed files list:

File Name	iNode number	Size	Written	Accessed	Created
awesomejokes.pps	6926	798720	2010-03-01 09:36:42 (UTC)	2010-03-02 00:00:00 (UTC)	2010-03-01 03:05:17 (UTC)

- After this, at 8:10pm, I began looking for the file file. Since the company had told me the name of the person who wrote the document (Keith Falce), alongside some of the items that were on the inventory list (Tegin Pellets, Tegobetaine, peanut), I had used a text document to create a keyword list with those specific words noted in new lines.

- Then, at 8:13pm I used the forensic tool to create a searchable list of strings (ie any group of characters like words or sentences) present in the entire forensic image, saving them to lab3.str file.

- Once this was done, at around 8:15pm, I used the file created at 8:10pm (one with specific keywords) to search through the list of strings present in the file created at 8:13pm (file with all groups of characters in the forensic image) and noted the offset of the search hits/outcomes. Then I used the file offset, sector size and sector offset of volume boot record to calculate the logical sector.

Offset	Logical sector
14140433	27555

- Once this was done, at around 8:20pm, I used the forensic tool to find the iNode value of the offset that had been found in the search hit before. Then I used another forensic tool to find the file name belonging to the iNode value. This resulted in the file name "GoodChemUsers.xls" which we had already found beforehand.

  (This made me realize that it was just a false positive.)

- So, at 8:25pm, I tried an alternative method where I directly searched the file name (goodcheminventory.xls) in the text file made at 8:13 (file with groups of characters in the forensic image) just to see if there is any hit with it. Surprisingly, there were two hits returned by the search this time with certain byte offset. So I calculated their logical sector too before noting it down in the table below:

Byte Offset	Logical sector (offset/sector size)
13958686	27,200
14124159	27,523

- Then i ran the forensic tool (ifind) with these values from the logical sector, thinking there would be an iNode value and hence a specific file associated with them. Unfortunately, the tool reported that no current, deleted or recoverable files were associated with those two values.

- So, at 8:30pm, I instead used another forensic tool (blkcat) to see the data around those two sectors (in hex format) where the search had been hit. There I noticed that "GoodChemInventory.xls" had indeed appeared there alongside letters "PK" just before and after it.

(Since "PK" header is commonly associated with zip files, I thought maybe the files had been zipped.)

- Furthermore, I know that zip files usually begin with both "PK" and either 0405, 0506 or 0607. Since that was the case for the first hit on the search performed in the previous step, I decided to copy the content of the sector there using another forensic tool (alongside physical sector number of first hit and sector count), and then passed it to a new zip file called "inventory.zip"

[note: this is the process of copying contents of a sector to find a deleted file is known as file carving]

- Then, at 8:35pm, I unzipped the file and noticed that "GoodChemInventory.xls" was being unzipped (ie inflated). This was the same file name as the 4th file that had been accessed. So to be absolutely sure, I ran a hash function on that file and checked it with the list of hash and file names provided by the company. It was a match with the "GoodChemInventory.xls" file from the company and thus it has been located. It had been zipped up and unallocated to hide its existence and thus had to be "carved out" of the sectors (after searching for the filename), in order to find it in the forensic image and recreate it.

- So I noted down the file type, start sector, sector length, and size for the curved file. Furthermore, I also noted down the file name, size and modified date of the content present in the carved file.

For carved file:

File Type	Start Sector	Length (byte)	Size (byte)
ZIP	27263	324	165888

For contents of carved file:

Name (with file type)	Size (byte)	Date/Time
GoodChemInventory.xls	511488	March 17, 2010

- Then I verified the hash values of the files to ensure they are still the same.

Overall, I have completed my investigation on 17th March 2022 (Thursday) at 8:40pm and have located all the files from the suspicious server access logs on the forensic image file provided to me while ensuring that no content on any of the files have been altered by me or my tools.