(examples format)

1. On Wednesday 4rd of May, 2011 at approximately 7:03pm, I …..

2. At 7:06pm, I ……

23. On Friday 6th of May, 2011 at approximately 9:27am, I recovered ……. the file details are as follows:

Then boxes for undeleted files, renamed files and so on…

No need to say exact commands used. Instead say that u used a forensic tool to do…. (ie the purpose of the command)

“It is important that opinions and other suppositions are not part of your report. Statements like “Fred saved the file at 12:03pm” is a conclusion not based entirely on the evidence you were provided. A better statement might be “the file had a created date of 12:03pm”. “

Currently writing in q/a format as uncertain of report format:

You will be marked on:

1. Your explanation what you received, how and when received the forensic evidence, how you handled continuity of the evidence. (1 mark)

**I have received a zip file containing forensic image of a USB drive, a text file containing MD5 hash value for the forensic image and a text file containing a list of known files(GoodChemClientList.xls, GoodChemInventory.xls,GoodChemUsersSummary.xlxs,GoodChemUsers.xls) from the GoodChem company along with their MD5 hash value on 17/3/2022 at 6:30pm AEST.**

**I had handled the continuity of the evidence by unzipping the folder and running a hash function on the forensic image and comparing the value obtained to previously given hash value to ensure data has not been modified in any way. (same hash value means data stored in the forensic image is same as that before and no change had occurred to the data). But before doing this, I had also set up the shared folder setup between the VM and the windows OS, to make it easy to transfer the zip file to the VM for examination.**

**Furthermore, I have also done a similar check of the hash function at the very end to ensure the data in the forensic image has not been altered by my actions. There the hash function values were still same as that given in the starting zip file, ensuring data hasn’t been altered.**

2. The details of the partition you located within the forensic image. (1 mark)

**I had only located a single partition in the disk which had the following details:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Partition** | **Partition**  **Type (e.g. NTFS/FAT)** | **Start Sector** | **End Sector** | **Total Sectors** | **Total Size (MB)** |
| **lab3.dd 1** | **W95 FAT32** | **63** | **3968054** | **3967992** | **1937** |

**The disk also had the sector size of 512 byte**

**[Note: here total size came 1937.4960 mb so rounded it off to 1937 mb]**

3. Your ability to locate the two deleted files, detailing the details of the files, how they were hidden within in the forensic image and the explanation of the processes you used to locate them. (2 marks)

**In order to locate the deleted files, I had to perform the following sequence of steps:**

1. **Mounting the partition using the starting offset value (calculated using starting sector and sector size) and the mount point of the disk (had to create a new one beforehand). I had done this to ensure I access the data in a read only manner and not alter it in any way**
2. **Then 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.**
3. **Then I utilized a forensic tool (sleuth kit)’s command line to see all the directories. But there I had failed at first due to lack of information (starting offset number of partition, the fie 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]**

**This had brought up 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** |

1. **Then I went into each directory and repeated the command with slight modification (determined by the iNode number of the directory) to see the files located in each directory to compared with the original list of files seen in step2.**

**There I noticed two files that had been deleted in the Word Docs directory and noted down their names and iNode number:**

|  |  |
| --- | --- |
| **Name** | **iNode number** |
| **GoodChemUsers.xls** | **209298** |
| **GoodChemUsersSummary.xls** | **209301** |

1. **Since, the deleted files had been located, I set out to recover them. There (for both deleted files), I had used the forensic tool’s icat command (using their own iNode number 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.**
2. **Since it looked like an excel spreadsheet information, I had then run a 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 means the files had been deleted from the Word docs directory in order to hide themselves in the forensic image.**
3. **Once this was confirmed, I noted their iNode values and numbers in the undeleted files table**

|  |  |
| --- | --- |
| **Name** | **iNode number** |
| **GoodChemUsers.xls** | **209298** |
| **GoodChemUsersSummary.xls** | **209301** |

1. **After this, I also utilized the forensic tool once more, running its istat command (with the upper two file’s iNode values ) to find the file’s first sector number (ie where it is located), size and the written, accessed and created dates and times and noted them down.**

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

1. **After all this was done, I once more verified that no other deleted items where present in other directories using the forensic tool**

4. Your ability to locate the renamed file, detailing the details of the files, how it was hidden within in the forensic image and the explanation of the processes you used to locate it. (2 marks)

**In order to locate the renamed files, I had done the following set of steps:**

1. **I had used the forensic tool to sort through the files and categorize 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.**
2. **After this, I moved to the sorter directory and ran the command to create a summary of the files discovered. This showed the fact that there were 12 image files and 8 document type files and stored all their metadata in respective txt files.**
3. **Then I used to command to view the txt file containing all image information and also opened those files to ensure they can be viewed as image.**
4. **Once this was confirmed I repeated the same with the txt files containing all documents information. 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, I had gone back and opened the files. There I noted that the file “awesomejokes.pps” was opening in calc instead of as a powerpoint document.**

1. **So, I decided to take a closer look by going into the powerpoint directory and checking the first 16 bytes of all the documents using the forensic tool.**

**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 can’t be confirmed in this way.**

1. **Thus I decided to look at the ending (last section) of the “awesomejokes.pps” (the file that opened in calc instead of powerpoint), instead of its starting, while avoiding lines containing all zeroes, just to see the data at the last section. There I noticed words pop up including ms excel, spreadsheet,etc which made me realize that it might actually be an excel file.**
2. **Thus 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.**

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

5. Your ability to locate the carved file, detailing the details of the file, how it was hidden within in the forensic image and the explanation of the processes you used to locate it. (2 marks)

**I had followed the following steps in order to locate the carved files:**

1. **Since the company had told me 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 txt document to create a keyword list with those specific words noted in new lines.**
2. **Then 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**
3. **Once this was done, I used the file created in step 1 to search through the list of strings present in the file created in step 2 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.**

**Once this was done, 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, making me realize that it was just a false positive.**

1. **So I tried an alternative method where I directly searched the file name (goodcheminventory.xls) in the txt file formed in step 2 just to see if there is any hit with it. Surprisingly, there were two hits returned by the search this time, with byte offset of 13958686, 14124159. So I calculated their logical sectors which were 27,200 and 27,523 respectively and ran the forensic tool with these values, hoping there would be a iNode value and file associated with them. Unfortunately, the tool reported that no current, deleted or recoverable files were associated with those two values.**
2. **So, I instead used another forensic tool 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. So, the keyword search we did in step 3 hadnt found it as the file had been compressed!**
3. **Now, I know that zip files usually begins with both “PK” and either 0405, 0506 or 0607. Since that was the case for the first hit on the search performed in step 4, I decided to copy the content of the sector there using another forensic tool, physical sector number of first hit (logical sector +63) and sector count (sector of search hit1 –sector of search hit2 +1), 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]**

1. **Then I unzipped the file and noted and 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 For contents of carved file**

|  |  |
| --- | --- |
| **File type** | **ZIP** |
| **Start Sector** | **27263** |
| **Length (sector)** | **324** |
| **Size** | **165888** |

|  |  |
| --- | --- |
| **Name** | **GoodChemInventory.xls** |
| **Size** | **511488** |
| **Date/Time** | **March 17 2010** |

6. Your ability to stick to the facts and explain your processes and findings in non-technical (but still accurate!) language and the overall presentation of the report (2 marks