|  |  |
| --- | --- |
| **Student Num**O**b**f**e**fi**r**c**:**ial (Closed) - Non Sensitive | **Seat Number:** |
| **Student Name:** | **Module Group:** |



**Digital Forensics**

Year 2/3 (2021/22), Semester 4/6

**School of InfoComm Technology**

(Diploma in Cybersecurity & Digital Forensics) (Diploma in Information Technology)

COMMON TEST

Date: 15 Dec 2021 (Wed)

Time: 4.00 PM – 5.30 PM

INSTRUCTIONS TO CANDIDATES:

1. Write your Student Number, Name, Module Group and Seat Number CLEARLY in the boxes provided above.
2. This paper consists of 18 pages including this cover page. Check carefully to make sure your set is complete.
3. There are FIVE questions. Answer **ALL** questions.

**GRADE**

DF (CSF, IT) - 1 - AY21/22 Sem 4/6

Last update: 28/11/2022

There are FIVE questions. Answer **ALL** questions. QUESTION 1 (20 marks)

Mike has just joined Goodworks Pte Ltd as a Forensics Investigator and was involved in a case involving a possible unlawful disclosure of company’s confidential materials by one of its employees, Jason Ong.

Mike arrived at the company and was given accessed to Jason’s office. He noticed a powered-on laptop on the desk. The laptop was connected to the company’s main network server. Mike connected an external hard disk (HDD1) to the laptop and copied the laptop’s hard disk contents to it. After completion, he powered off the laptop.

Amongst the items found on the desk include a couple of DVDs, a thumb drive, an iPhone10 smartphone, a digital clock, a musical coffee mug and some printed papers on a printer. Mike seized and tagged all these items, put them in a sturdy box, and sealed the box to be transported later to the forensics lab. After completing the search at the office, Mike placed the sturdy box in the car boot.

At the forensics lab, Mike stored the seized evidence in a locked cabinet. Next, he connected the external hard disk (HDD1) directly to the forensic workstation to create a forensic image (evidence file). He performed analysis, searched, and bookmarked the evidence file with necessary keywords using EnCase.

Prior to the investigation, the company has informed Mike that MS Outlook and Skype for Business were commonly used for correspondence as well. An important file, *financial\_blueprint.vsd,* was seemingly to have been missing from Jason’s laptop.

1. For each of the following digital forensics processes, identify **TWO** mistakes Mike may have made while handling the case. Suggest the correct step(s) that should have been taken for each mistake identified.

(6 marks)

|  |  |  |
| --- | --- | --- |
| **Processes** | **Mistakes Made** | **Correct Steps** |
| Identification and Seizure of Evidence | Mike placed the evidence into a sturdy box  Mike placed the sturdy box into the car boot | Mike should have placed the evidence into an antistatic bag to prevent more electronic interference to the evidence.  Placed in separate evidence bags  Mike should not place the evidence into the car boot but instead place it at the backseat of the car due to the higher temperature. |

QUESTION 1 (cont.)

|  |  |  |
| --- | --- | --- |
| Evidence Acquisition | Mike connected the external hard disk (HDD1) directly to the forensic workstation to create a forensic image  Mike did not check the hash values between the files during the acquisition stage and proceeded to conduct the analysis  Copied the laptop’s hard disk contents to external hard disk (HDD1) which may have been contaminated | Mike should connect a write blocker between the external hard disk and the forensics workstation.  Mike should check the hash value of the bit stream copies of evidence on a forensically clean device created has the same hash values as the device seized before continuing to analyze the file.  Should not be using his own HDD storafe devices for storing evidence file must be forensically clean. |
| Documentation | Mike did not note down the exact location of where each evidence was seized.  Mike did not document the chain of custody for each of the evidence starting from the time of evidence seizure  Power off laptop without hesitation | Mike should note down and take a photograph to show where the exact location of the device was.  Mike should document the chain of custody from when he seized the data using the format of XXX-yyyy/mm/dd-evidence number-Serial number. Mike should also note down the timing of where the evidence is as of the timing.  Should have taken a photo or recording of the screen. |

1. Based on the case description, identify **ONE** type of data for each of the following categories of forensic data.

(3 marks)

|  |  |
| --- | --- |
| **Categories of Forensic Data** | **Data Identified from Case** |
| Active Data | evidence file  Files and programs used by the MS Outlook and Skype Data / Files from the laptop / OS Files |
| Latent Data | *financial\_blueprint.vsd* |
| Archival Data | external hard disk (HDD1)  Data from the external Hard disk  Data on DVDs  Data on thumb drive |

QUESTION 1 (cont.)

1. Mike performed analysis on the evidence file using keyword search. Suggest any **FOUR**

relevant keywords that Mike could use.

(2 marks)



Jason Ong

MS Outlook

Skype for Business

Financial\_blueprint.vsd

Goodworks Pte Ltd

Suspect’s Email Address

1. Generally, there are three types of forensic images Mike could create. Briefly describe any

**TWO** types of forensic images.

(4 marks)

Complete Disk. Complete Disk imaging is the forensic image of capturing the entire hard disk storage image. Most preferred as it is the most comprehensive because it contains the bit stream copy of the entire disk.

Logical. Logical Imaging is the extraction of specific files and is usually used when the device storage is too large to do a complete disk imaging. Only certain files are acquired.

1. Explain what would be the best course of action Mike could take if he noticed that the iPhone10 was still on and he wished to acquire the phone data.

(3 marks)



Mike can do a Complete disk acquisition on the iphone 10 by connecting it to a physical image acquisition tool to image the iphone 10 into a forensically clean storage device.

The phone should be left on to prevent any volatile data that may be lost. The phone should be connected to the battery source and isolated from the cell tower by placing it in a Faraday bag, set the phone to airplane mode and disabling communication systems

1. Discuss what must be done in order to assure the court of law that the evidence is authentic. Provide any **TWO** necessary information that must be included.

(2 marks)



There should be 2 bit stream copies of the original device and the analysis should be done on the bit stream copies where as the original evidence should be used to just generate the hash values which match the 2 bit streams and should be stored at a location that is only accessible by the authorized personnel. There should also be a chain of custody record of who had the device, the timeframe of when the device is with the other stated person, the purpose of them retrieving the device, and at what time.

There should be a chain of custody form with the date, incident type, custodian and reason, description of evidence and location.

QUESTION 2 (20 marks)

A Korean bank’s employee, Kim has been accused of stealing company’s confidential data while serving her resignation period. Joseph, a Forensic Investigator, is taking charge of the investigation. The suspect, Kim, denied any wrongdoings and claimed that her account had been hacked, resulting in the data theft.

Joseph acquired both volatile and non-volatile contents of the suspect’s Windows 10 computer and begun his investigation at the forensic lab. Joseph discovered a suspicious email that showed a file attachment with the Korean name 비밀 문서 (translated to “*secret document”*). He tried to perform Keyword (String) search using Search Options shown in Figure 2 to find the file, but was unsuccessful.

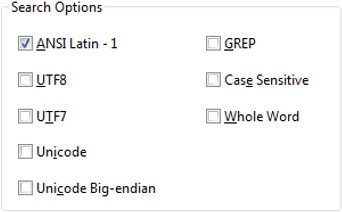


Figure 2: Search Options

Joseph had also discovered that multiple storage devices had been connected to the suspect’s computer, and a file named *Familyphoto.jpg* was copied to an external storage device. He performed Signature Analysis and noticed “mismatch” result in the file signature and extension of *Familyphoto.jpg*. The signature showed that it is a Portable Document Format (PDF) formatted file instead.

1. Explain how Joseph can investigate Windows logon activities, to verify if the suspect’s account has been hacked as claimed.

(3 marks)

Joseph can use the security logs logged in the event logs and refer to the code on the method of logging in. The method of interest is likely using a remote login.

Joseph can check Windows Security event log to verify if there are multiple failed logon attempts. There is a possibility that bure-force attack has taken pplace on the suspect’s computer in the event of multiple failed logon attempts.

QUESTION 2 (cont.)

1. Briefly explain which file Joseph could examine to confirm the last logoff time of the suspect’s account. Suggest the Operating System based tool to view this file.

(3 marks)

|  |
| --- |
| Joseph can examine the NTUSER.dat file. As the NTUSER.dat file is modified only when the user logs out or shuts down the device, the last modified time will be the last logoff time of the suspect’s user account.  Joseph can examine the NTUSER.DAT file in the root folder. The last written time can be used to possibly determine when the user last logged out.  The registry viewer could be used to view NTUSER.DAT file. |

1. Explain the possible reason why Joseph could not find the file 비밀 문서 (secret document). Give ONE suggestion to increase his chance of locating the file and explain why this is necessary.

(4 marks)

|  |
| --- |
| One reason why Joseph may not be able to find the file is because the character encoding may not be supported in ANSI Latin-1. Instead of just checking ANSI Latin-1, UTF 7 and UTF 8 character encoding can also be checked.  As keyword search will only work if the encoding method is correct, therefore if Joseph chose the ANSI Latin-1 encoding method, there will not ne any resultabnt search hits. In this case, the file seemed to be encoded using Korean characters, so if Joseph searcheds using ASCII, he will not find the file.  Joseph can increase his chances by selecting UTF7, UTF8 and Unicode in the search options.  Unicode uses 8-, 16- or 32-bit characrters for electronic text that includes every written alphabet in existence. |

1. What could be the intention of the suspect when the *Familyphoto.jpg* file is found to have mismatch in the signature and extension?

(2 marks)

|  |
| --- |
| The intention of the suspect when the Familyphoto.jpg file has a mismatch in the signature and extension is to conceal the data possibly stored in the original file.  The Suspect may be trying to hide the file by naming the file extension to something else that does not attract attention. |

QUESTION 2 (cont.)

1. Joseph would like to extend his investigation into the slack space of the acquired Windows 10 computer. Calculate the slack space created for the *Familyphoto.jpg* file of 7,000 bytes, written onto the hard disk for a cluster size of 8 sectors. Clearly show your working and answer in bytes.

(5 marks)

|  |
| --- |
| 512 x 8 = 4096  (2)(4096) – 7000 = 1192bytes  Sector size = 512 bytes  Cluster size = 8 x 512 = 4096bytes  2 clusters are required to howld the Familyphoto.jpg  (2)(4096) – 7000 = 1192bytes |

1. Joseph tried to look for a deleted file using “\xFF\xD8\xFF\xE0” as the search expression. He found the file as shown in Figure 2(f) below:

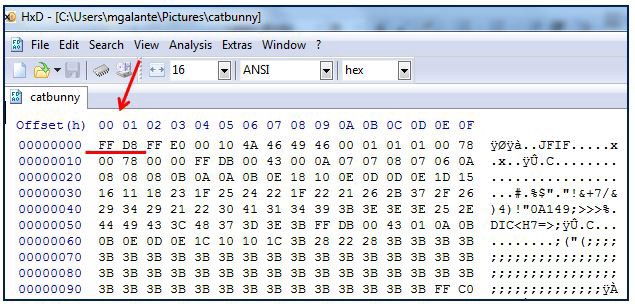


Figure 2(f): Searching for a Deleted File

Briefly explain the extraction method which Joseph had performed. What file type was he searching for?

(3 marks)

|  |
| --- |
| The extraction method Joseph has performed is file carving. The type of file Joseph is looking for is an image file.  Joseph has performed “File Carving” extraction method using the known header (File signature) to search on the evidence file.  He was looking for a JPEG file. |

QUESTION 3 (20 marks)

You have been engaged by CCN bank to perform an investigation on its Human Resource staff’s laptop which is suspected of being infected with malware.

After conducting interviews with the Human Resource staff, you realized that the owner of the laptop, Jane, had recently received a job application email with an attached resume file. She had opened the file without suspecting that it could be infected with malware. Through other interviews with the bank’s IT staff, you gathered information of the bank’s network infrastructure as shown in Figure 3. You suspected that the attacker has accessed other systems in the domain through Jane’s infected laptop.

You acquired the volatile as well as non-volatile data from Jane’s laptop and seized the laptop back to the forensic lab for further investigation.

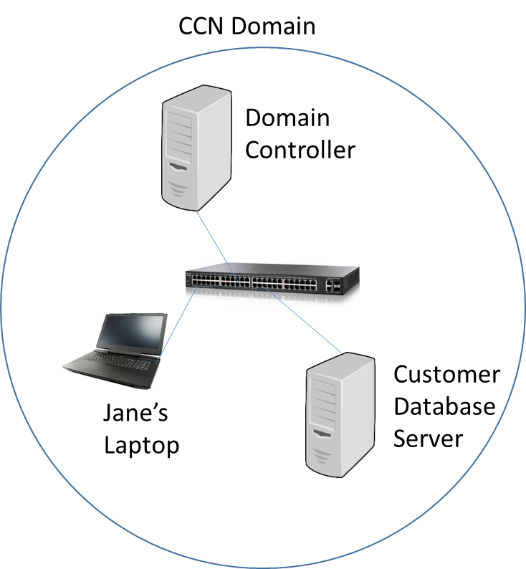


Figure 3: Partial Network Diagram of CCN Bank

1. From the acquired forensic image of Jane’s laptop hard disk, you found a suspicious email with an attachment named *JobApp.docx*. You would like to quickly search for the file to perform further analysis. Suggest and explain TWO extraction methods that you would use to locate the file in Jane’s hard disk. Assume that Jane has not deleted the file.

(4 marks)

|  |
| --- |
| Two extraction methods are keyword search and searching using the file signature.  The keyword search can be used with the keyword JobApp.docx. The keyword search will match the content and name of the file with the keyword specified and it will show the files which have result hits.  The searching using the file signature will look for all files with the same signature with the one specified.  Metadata by using the filename and MAC timestamp to search for the file since this information are available.  String or keyword search to make sure the use of file names and patterns in the file names for searching |

QUESTION 3 (cont.)

1. You had found the file *JobApp.docx* and suspected that the file has been renamed to make it look like a legitimate job application letter. Explain what you can do to confirm your suspicion.

(3 marks)

|  |
| --- |
| To confirm the suspicion, file signature analysis can be used to check if the file was renamed. By checking the file signature, the file extension will be shown.  Perform file signature analysis to verify the actual file type by comparing the file signature at the header with the extension. |

1. Upon further investigation, it appeared that the attacker had taken control of Jane’s laptop to remotely access the Customer Database Server using stolen credentials. The volatile data shows that a Remote Desktop Protocol (RDP) client was running.

Given the following Logon Types in Table 3(c), explain which Logon Type had taken place?

(3 marks)

|  |  |
| --- | --- |
| **Type** | **Code** |
| Interactive | 2 |
| Network | 3 |
| Batch | 4 |
| Service | 5 |
| Proxy | 6 |
| Unlock | 7 |
| NetworkCleartext | 8 |
| NewCredentials | 9 |
| RemoteInteractive | 10 |
| CacheInteractive | 11 |

Table 3(c): Logon Types

|  |
| --- |
| The Network type of Login with code 2 has taken place. As the Remote Desktop Protocol runs through the internet, it uses the Network login instead of the interactive login and batch and service login are used by the system.  The logon type is with code 10 has taken place. RDP client is used to remotely access Customer Database Server. |

QUESTION 3 (cont.)

1. Besides *JobApp.docx*, you are also trying to search for a file that could potentially contain the confidential data that the attacker has copied from Customer Database Server. You suspected that the file has been deleted and proceed to examine the $Recycle.Bin of the acquired evidence file, as shown in Figure 3(d) below.

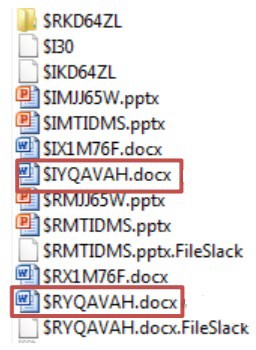


Figure 3(d): Files in $Recycle.Bin

Explain in what way the two files ($IYQAVAH.docx and $RYQAVAH.docx) are related, and what information they contain.

(4 marks)

|  |
| --- |
| $IYQAVAH and $RYQAVAH are related as the $RYQAVAH is the renamed version of the original file and the $IYQAVAH is the file with the location data of where the file is stored.  When a file is sent to $Recycle.Bin for Windows Vista/7/8/10 Operating System, it is renamed to $R followed by a set of random characters, followed by the original file extension. A matching file is created as $I is followed by the same random characters and extension as the $R file.  The $R file contains the actual file content.  The $I file contains the original filename/path and file size and the date and tie that the file was moved to the Recycle Bin. |

1. The file that you are looking for could not be found in the search of the recycle bin. Propose and explain clearly another search method to attempt and how you can use this method to recover this deleted file.

(3 marks)

|  |
| --- |
| Another search method that can be used is the searching of unallocated space. As the unallocated space may contain reminiscence of the previous files. Using file carving to search for a sequence of bytes matching the file header of the docx file.  Search for the file in the Unallocated and slack space using keyword such as customer names or other particulars that can be found in the Customer Database Server. You will probably need permission and help from CCN bank to obtain these keywords. |

QUESTION 3 (cont.)

1. You are investigating on Jane’s browsing activities and looked into the Internet Properties of Internet Explorer (IE), as shown in Figure 3(f).

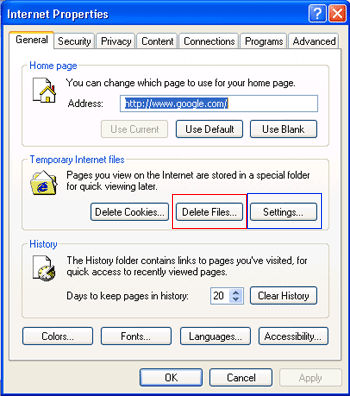


Figure 3(f): Internet Properties of Internet Explorer (IE)

Briefly explain why the Temporary Internet files (TIF) are placed under the Low folder.

(3 marks)

|  |
| --- |
| The Temporary Internet Files are placed in the Low folder based on the security configuration for the browser.  Temporary Internet Files (TIF) are placed under the Low folder as Microsoft use the Low folder to protect system against malware. Data in this folder runs at the lowest possible level of integrity to minimize the execution of malware. |

QUESTION 4 (20 marks)

During a forensics investigation, you are tasked to examine 2 computers, Computer A and Computer B respectively. Figure 4(a) shows a screen shot of Computer A’s Disk management.

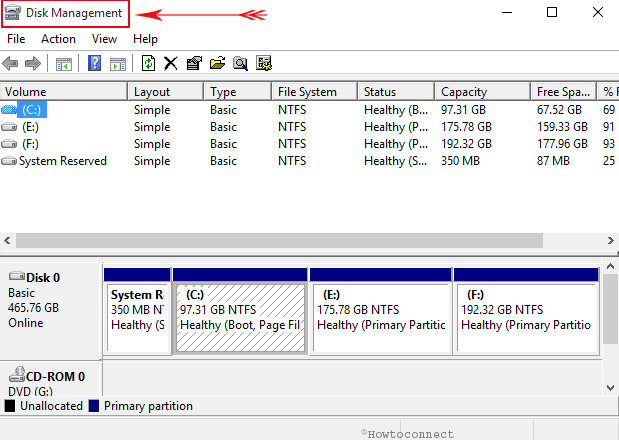


Figure (4(a) Disk Management view of Computer A

1. Based on Figure 4(a), complete the table below

(4 marks)

|  |  |  |
| --- | --- | --- |
|  | Number of drives/volumes | Name(s) of drive/volume |
| Number of Physical drive(s) | 1 | Disk 0 |
| Number of Logical volume(s) | 4 | C:, E, F:, System Reserved |

QUESTION 4 (cont.)

1. Figure 4(b) depicts the MBR of Computer B. The partition table is highlighted.

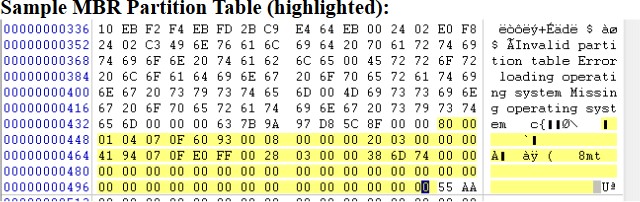




Figure 4(b): MBR of Computer B A partition record consists of the following information:

* 1. Status (1 byte, 80=Yes, 00=No)
  2. Starting sector on CHS format (3 bytes) (C-Cylinder, H-Head, S-Sector)
  3. Partition Type (1 byte)
  4. Ending Sector on CHS format (3 bytes) (C-Cylinder, H-Head, S-Sector)
  5. Relative Sector offset (4 bytes)
  6. Total Sectors of partition (4 bytes)
     1. Complete the following Partition Table entries based on the information provided.

(4 marks)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Partition Type** | **Name** | **Status** | **Starting Sector**  **(CHS)** | **Ending Sector**  **(CHS)** | **Relative Sector Offset**  **(CHS)** | **Total Size of partition**  **(In sectors)** |
| 07 | NTFS | (80) | 00:01:04 | 0F:60:93 | 00:08:00:00 | (00:20:03:00 ) |
| 07 | NTFS | (00) | 00:41:94 | (0F:E0:FF) | 00:28:03:00 | 00:38:6D:74 |
| 00 | None | 00 | 00:00:00 | 00:00:00 | 00:00:00:00 | 00:00:00:00 |
| 00 | None | 00 | 00:00:00 | 00:00:00 | 00:00:00:00 | 00:00:00:00 |

QUESTION 4 (cont.)

(b)

* + 1. How many partitions are formatted on Computer B’s hard disk? What file system is used for each partition?

(2 marks)

|  |
| --- |
| 2 partitions running NTFS |

* + 1. Which is the bootable partition? Explain your answer.

(2 marks)

|  |
| --- |
| The first partition as the status code is 80 which refers to the active partition. |

* + 1. Calculate the size (represented in GB) of the first partition.

(4 marks)

|  |
| --- |
| 204800 \* 512 = 20485600  20485600/(1024\*\*3) =0.0977GB  204800 \* 512 = 104857600  104857600/(1024\*\*3) = 0.0977GB |

* + 1. What could you conclude about Computer B based on the Hex 55 AA at the end of the MBR?

(2 marks)

|  |
| --- |
| The MBR signature is valid and the hard drive is bootable.  The hex decimal 55AA indicates that computer B is able to boot properly |

QUESTION 4 (cont.)

(b)

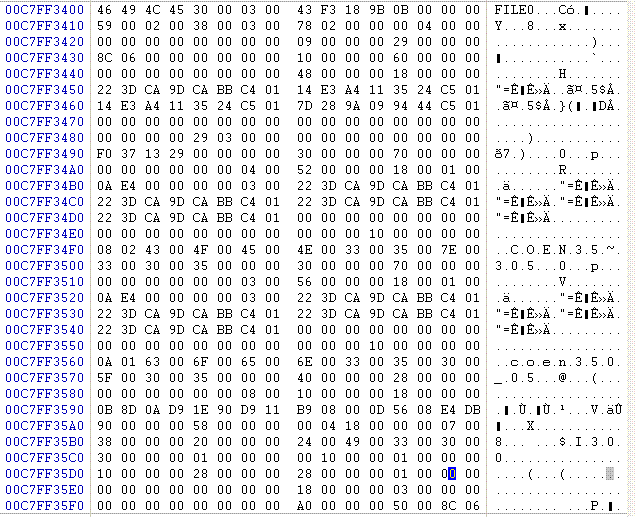
* + 1. MBR contains the master boot code. Explain how would Computer B boot based on the information contained in the master boot code and the partition table in 4(b)(i).

(2 marks)

|  |
| --- |
| Computer B will check the Master Boot Record and look for the active partition which is the first partition of Computer B. It will than find the starting sector of the partition and load a copy of the boot sector into the memory. It will than transfer the executable code into the boot sector.  Scans the partition table for the active partition  Finds the starting sector of the active partition  Loads a copy of the boot sector (in VBR) from the active partition into memory (RAM)  Transfer control to the executable code in the boot sector. |

QUESTION 5 (20 marks)

A forensic investigator, Tom is examining a computer formatted with NTFS file system. Figure 5- 1 shows an entry in Master File Table (MFT) and Figure 5-2 shows the list of NTFS attributes.



**Byte offset 0x38**

Figure 5-1: An Entry in Master File Table (MFT)

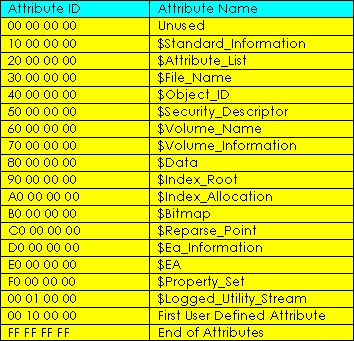


Figure 5-2: NTFS Attributes

QUESTION 5 (cont.)

1. Answer the following questions based on Figure 5-1 and 5-2.

(15 marks)

|  |  |
| --- | --- |
|  | Answers |
| (i) Byte offset of the first attribute | 0x38 |
| (ii) Name of the first attribute | $Standard\_Information |
| (iii) Length of the first attribute | 96 bytes  0x60 |
| (iv) Byte offset of the second attribute | 0x98 |
| (v) Name of the second attribute | $File\_Name |
| (vi) Name of the object (file/folder) | COEN35~305  COEN35 (shortened name always end with a tilde (~)) |
| (vii) Byte offset of the third attribute | 0x108 |
| (viii) Name of the third attribute and content of this attribute | $File\_Name  COEN350\_05  This is another file name entry, this specifies the long file name content is coen350\_05 |
| (ix) Why this attribute is necessary? | The file name is more than 8 characters or consists of a special character. Which in this case the file consists of a special character ‘~’ and more than 8 characters.  If the filename is longer than 8 characters or contains special characters, windows will also create a DOS compatible name ns save this as a 2nd $File\_Name attribute. |
| (x) Does this entry specify a file or a folder? Explain | The entry specifies a folder as the next attribute is a $Object\_ID  This is a folder name as there is no extension |
| (xi) List the names of the remaining three attributes | $Object\_ID  $Index\_Root  $Index\_Allocation |

QUESTION 5 (cont.)

1. Illustrate the above MFT entry with the aid of a well-labeled diagram. Your diagram should be as specific as possible, showing all the relevant fields and length of the entry (in bytes).

(5 marks)

|  |
| --- |
|  |

\*\* END OF PAPER \*\*