Student Number:	**Seat Number:**
Student Name:	**Module Group:**

NGEE ANN POLYTECHNIC

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	

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 evidences 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.

(a) 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		

QUESTION 1 (cont.)

(a)

Evidence Acquisition		
Documentation		

(b) 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	
Latent Data	
Archival Data	

QUESTION 1 (cont.)

(c) Mike performed analysis on the evidence file using keyword search. Suggest any **FOUR** relevant keywords that Mike could use.

(2 marks)

(d) Generally, there are three types of forensic images Mike could create. Briefly describe any **TWO** types of forensic images.

(4 marks)

(e) 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)

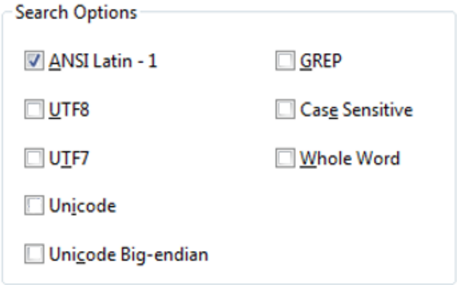
(f) Discuss what must be done in order to assure the court of law that the evidence is authentic. Provide any **TWO** necessary information that must be included.

(2 marks)

<u>QUESTION 2</u> (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.



Search Options

☑ ANSI Latin - 1
□ UTF8
□ UTF7
□ Unicode
□ Unicode Big-endian
□ GREP
□ Case Sensitive
□ Whole Word

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.

(a) Explain how Joseph can investigate Windows logon activities, to verify if the suspect's account has been hacked as claimed.

(3 marks)

QUESTION 2 (cont.)

(b) 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)

(c) 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)

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

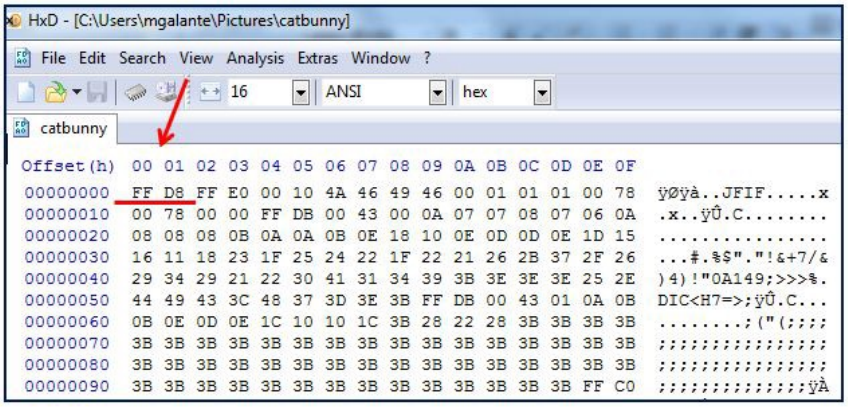
(2 marks)

QUESTION 2 (cont.)

(e) 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)

(f) 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:



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 01 00 78  ÿØÿà..JFIF.....x
00000010  00 78 00 00 FF DB 00 43 00 0A 07 07 08 07 06 0A  .x..ÿÛ.C........
00000020  08 08 08 0B 0A 0A 0B 0E 18 10 0E 0D 0D 0E 1D 15  ................
00000030  16 11 18 23 1F 25 24 22 1F 22 21 26 2B 37 2F 26  ...#.%$"."!&+7/&
00000040  29 34 29 21 22 30 41 31 34 39 3B 3E 3E 3E 25 2E  )4)!"0A149;>>>%.
00000050  44 49 43 3C 48 37 3D 3E 3B FF DB 00 43 01 0A 0B  DIC<H7=>;ÿÛ.C...
00000060  0B 0E 0D 0E 1C 10 10 1C 3B 28 22 28 3B 3B 3B 3B  ........;("(;;;;
00000070  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  ;;;;;;;;;;;;;;;;
00000080  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B  ;;;;;;;;;;;;;;;;
00000090  3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B 3B FF C0  ;;;;;;;;;;;;;;ÿÀ
```

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)

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.

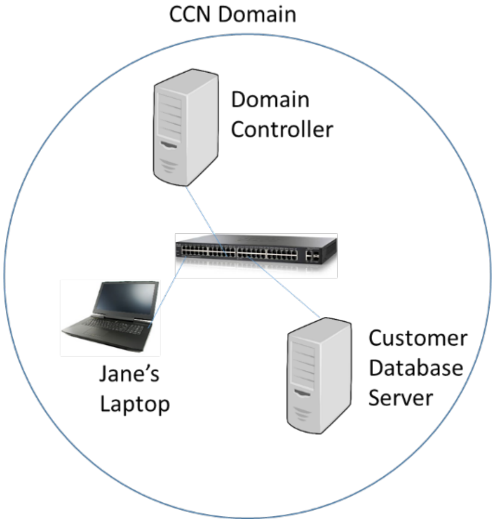


Figure 3: Partial Network Diagram of CCN Bank

(a) 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)

<u>QUESTION 3</u> (cont.)

(b) 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)

(c) 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?

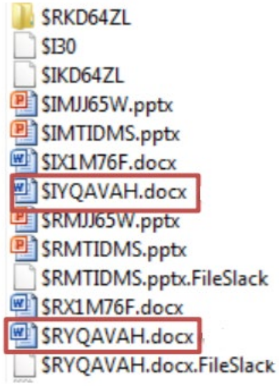
(3 marks)

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

QUESTION 3 (cont.)

(d) 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.



```
$RKD64ZL
$I30
$IKD64ZL
$IMJJ65W.pptx
$IMTIDMS.pptx
$IX1M76F.docx
$IYQAVAH.docx
$RMJJ65W.pptx
$RMTIDMS.pptx
$RMTIDMS.pptx.FileSlack
$RX1M76F.docx
$RYQAVAH.docx
$RYQAVAH.docx.FileSlack
```

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.

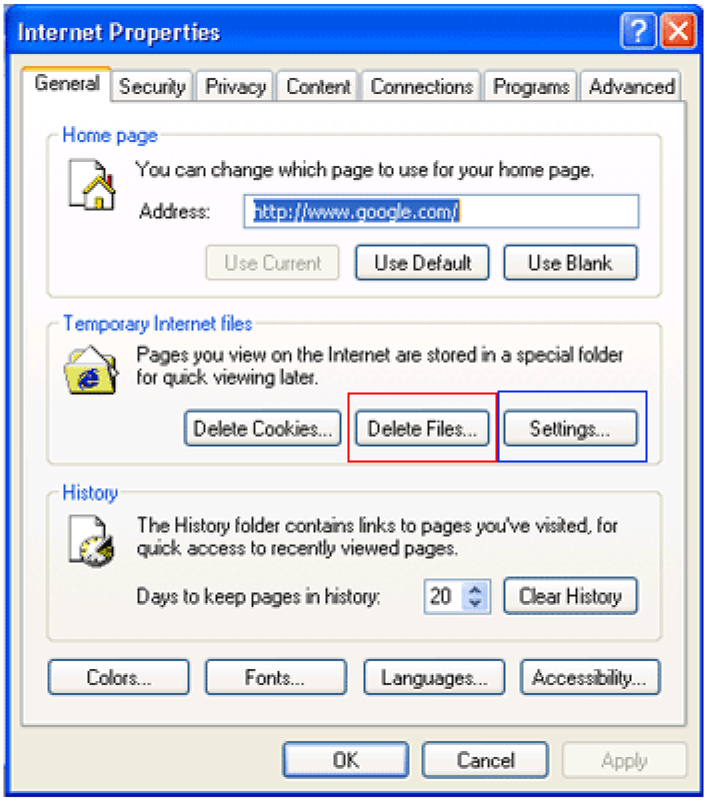
(4 marks)

(e) 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)

QUESTION 3 (cont.)

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



You can change which page to use for your home page.

Address: http://www.google.com/

Pages you view on the Internet are stored in a special folder for quick viewing later.

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

Days to keep pages in history: 20

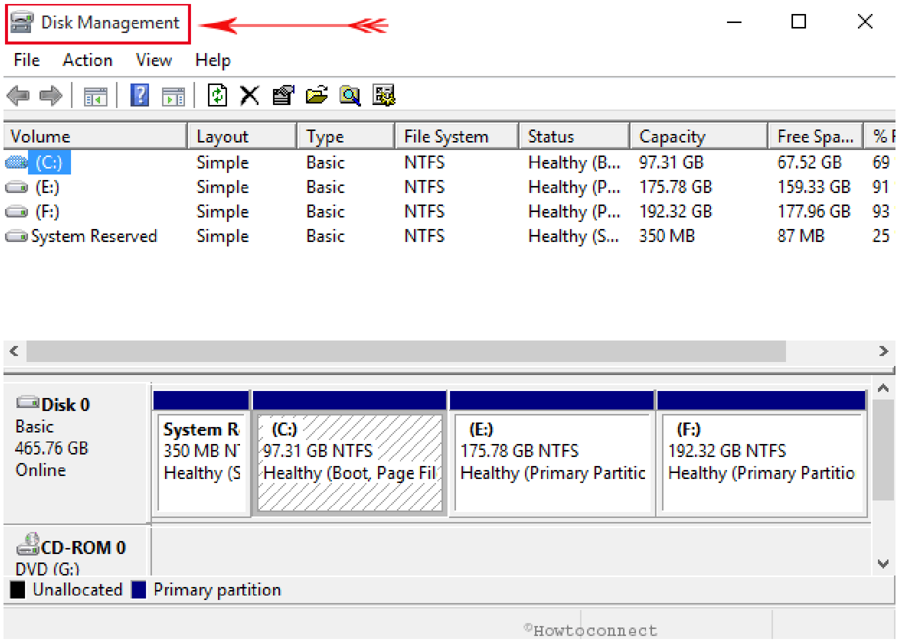
Figure 3(f): Internet Properties of Internet Explorer (IE)

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

(3 marks)

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.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% F
(C:)	Simple	Basic	NTFS	Healthy (B...	97.31 GB	67.52 GB	69
(E:)	Simple	Basic	NTFS	Healthy (P...	175.78 GB	159.33 GB	91
(F:)	Simple	Basic	NTFS	Healthy (P...	192.32 GB	177.96 GB	93
System Reserved	Simple	Basic	NTFS	Healthy (S...	350 MB	87 MB	25

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

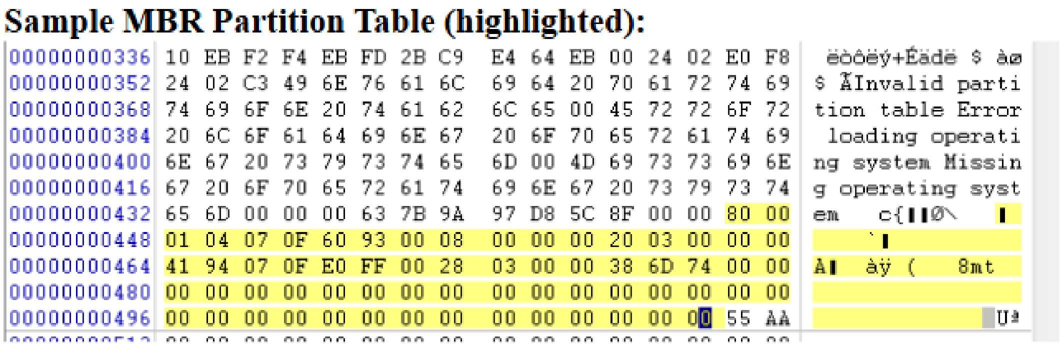
(a) Based on Figure 4(a), complete the table below

(4 marks)

	Number of drives/volumes	Name(s) of drive/volume
Number of Physical drive(s)		
Number of Logical volume(s)		

QUESTION 4 (cont.)

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



Sample MBR Partition Table (highlighted):

```
00000000336  10 EB F2 F4 EB FD 2B C9  E4 64 EB 00 24 02 E0 F8   ëòôëý+Éäd ë $ àø
00000000352  24 02 C3 49 6E 76 61 6C  69 64 20 70 61 72 74 69  $ ÃInvalid parti
00000000368  74 69 6F 6E 20 74 61 62  6C 65 00 45 72 72 6F 72  tion table Error
00000000384  20 6C 6F 61 64 69 6E 67  20 6F 70 65 72 61 74 69   loading operati
00000000400  6E 67 20 73 79 73 74 65  6D 00 4D 69 73 73 69 6E  ng system Missin
00000000416  67 20 6F 70 65 72 61 74  69 6E 67 20 73 79 73 74  g operating syst
00000000432  65 6D 00 00 00 63 7B 9A  97 D8 5C 8F 00 00 80 00  em   c{  Ø\
00000000448  01 04 07 0F 60 93 00 08  00 00 00 20 03 00 00 00       `
00000000464  41 94 07 0F E0 FF 00 28  03 00 00 38 6D 74 00 00  A   àÿ (   8mt
00000000480  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000000496  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 AA                U ª
```

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)

(i) 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	( )	00:01:04	0F:60:93	00:08:00:00	( )
07	NTFS	( )	00:41:94	( )	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)

(ii) How many partitions are formatted on Computer B’s hard disk? What file system is used for each partition?

(2 marks)

(iii) Which is the bootable partition? Explain your answer.

(2 marks)

(iv) Calculate the size (represented in GB) of the first partition.

(4 marks)

(v) What could you conclude about Computer B based on the Hex 55 AA at the end of the MBR?

(2 marks)

QUESTION 4 (cont.)

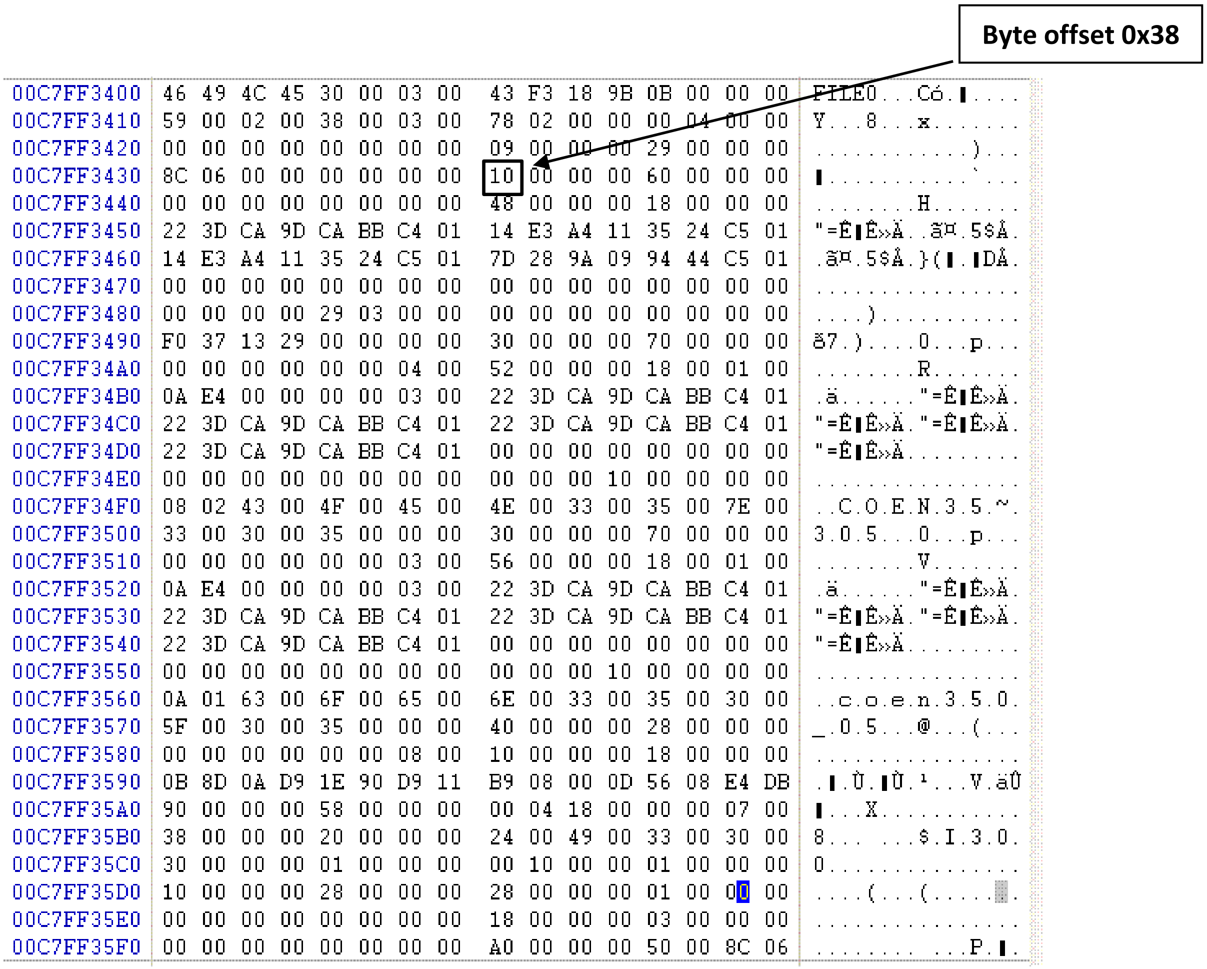
(b)

(vi) 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)

QUESTION 5 (20 marks)

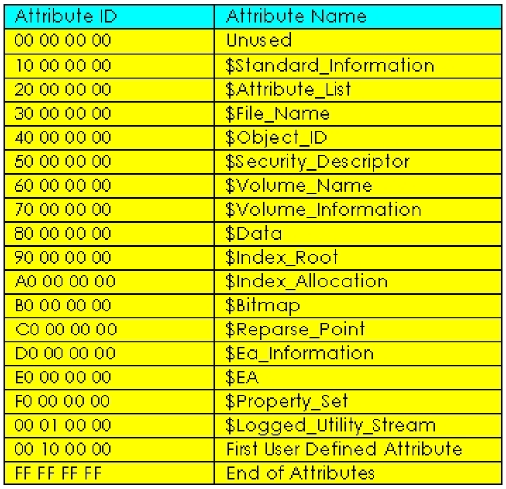
A forensic investigator, Tom is examining a computer formatted with NTFS file system. Figure 5-1 shows an entry in Master File Table (MFT) and Figure 5-2 shows the list of NTFS attributes.



Byte offset 0x38

```
00C7FF3400  46 49 4C 45 30 00 03 00  43 F3 18 9B 0B 00 00 00  FILE0...Có.▌....
00C7FF3410  59 00 02 00 38 00 03 00  78 02 00 00 00 04 00 00  Y...8...x.......
00C7FF3420  00 00 00 00 00 00 00 00  09 00 00 00 29 00 00 00  ............)...
00C7FF3430  8C 06 00 00 00 00 00 00  10 00 00 00 60 00 00 00  ▌...........`...
00C7FF3440  00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00  ........H.......
00C7FF3450  22 3D CA 9D CA BB C4 01  14 E3 A4 11 35 24 C5 01  "=Ê▌Ê»Ä..ã¤.5$Å.
00C7FF3460  14 E3 A4 11 35 24 C5 01  7D 28 9A 09 94 44 C5 01  .ã¤.5$Å.}(▌.▌DÅ.
00C7FF3470  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00C7FF3480  00 00 00 00 29 03 00 00  00 00 00 00 00 00 00 00  ....)...........
00C7FF3490  F0 37 13 29 00 00 00 00  30 00 00 00 70 00 00 00  ð7.)....0...p...
00C7FF34A0  00 00 00 00 00 00 04 00  52 00 00 00 18 00 01 00  ........R.......
00C7FF34B0  0A E4 00 00 00 00 03 00  22 3D CA 9D CA BB C4 01  .ä......"=Ê▌Ê»Ä.
00C7FF34C0  22 3D CA 9D CA BB C4 01  22 3D CA 9D CA BB C4 01  "=Ê▌Ê»Ä."=Ê▌Ê»Ä.
00C7FF34D0  22 3D CA 9D CA BB C4 01  00 00 00 00 00 00 00 00  "=Ê▌Ê»Ä.........
00C7FF34E0  00 00 00 00 00 00 00 00  00 00 00 10 00 00 00 00  ................
00C7FF34F0  08 02 43 00 4F 00 45 00  4E 00 33 00 35 00 7E 00  ..C.O.E.N.3.5.~.
00C7FF3500  33 00 30 00 35 00 00 00  30 00 00 00 70 00 00 00  3.0.5...0...p...
00C7FF3510  00 00 00 00 00 00 03 00  56 00 00 00 18 00 01 00  ........V.......
00C7FF3520  0A E4 00 00 00 00 03 00  22 3D CA 9D CA BB C4 01  .ä......"=Ê▌Ê»Ä.
00C7FF3530  22 3D CA 9D CA BB C4 01  22 3D CA 9D CA BB C4 01  "=Ê▌Ê»Ä."=Ê▌Ê»Ä.
00C7FF3540  22 3D CA 9D CA BB C4 01  00 00 00 00 00 00 00 00  "=Ê▌Ê»Ä.........
00C7FF3550  00 00 00 00 00 00 00 00  00 00 00 10 00 00 00 00  ................
00C7FF3560  0A 01 63 00 6F 00 65 00  6E 00 33 00 35 00 30 00  ..c.o.e.n.3.5.0.
00C7FF3570  5F 00 30 00 35 00 00 00  40 00 00 00 28 00 00 00  _.0.5...@...(...
00C7FF3580  00 00 00 00 00 00 08 00  10 00 00 00 18 00 00 00  ................
00C7FF3590  0B 8D 0A D9 1E 90 D9 11  B9 08 00 0D 56 08 E4 DB  .▌.Ù.▌Ù.¹...V.äÛ
00C7FF35A0  90 00 00 00 58 00 00 00  00 04 18 00 00 00 07 00  ▌...X...........
00C7FF35B0  38 00 00 00 20 00 00 00  24 00 49 00 33 00 30 00  8... ...$.I.3.0.
00C7FF35C0  30 00 00 00 01 00 00 00  00 10 00 00 01 00 00 00  0...............
00C7FF35D0  10 00 00 00 28 00 00 00  28 00 00 00 01 00 00 00  ....(...(.......
00C7FF35E0  00 00 00 00 00 00 00 00  18 00 00 00 03 00 00 00  ................
00C7FF35F0  00 00 00 00 00 00 00 00  A0 00 00 00 50 00 8C 06  ........ ...P.▌.
```

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



Attribute ID	Attribute Name
00 00 00 00	Unused
10 00 00 00	$Standard_Information
20 00 00 00	$Attribute_List
30 00 00 00	$File_Name
40 00 00 00	$Object_ID
50 00 00 00	$Security_Descriptor
60 00 00 00	$Volume_Name
70 00 00 00	$Volume_Information
80 00 00 00	$Data
90 00 00 00	$Index_Root
A0 00 00 00	$Index_Allocation
B0 00 00 00	$Bitmap
C0 00 00 00	$Reparse_Point
D0 00 00 00	$Ea_Information
E0 00 00 00	$EA
F0 00 00 00	$Property_Set
00 01 00 00	$Logged_Utility_Stream
00 10 00 00	First User Defined Attribute
FF FF FF FF	End of Attributes

Figure 5-2: NTFS Attributes

QUESTION 5 (cont.)

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

(15 marks)

	Answers
(i) Byte offset of the first attribute	
(ii) Name of the first attribute	
(iii) Length of the first attribute	
(iv) Byte offset of the second attribute	
(v) Name of the second attribute	
(vi) Name of the object (file/folder)	
(vii) Byte offset of the third attribute	
(viii) Name of the third attribute and content of this attribute	
(ix) Why this attribute is necessary?	
(x) Does this entry specify a file or a folder? Explain	
(xi) List the names of the remaining three attributes	

QUESTION 5 (cont.)

(b) 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 **