Thapar Institute of Engineering and Technology

Department of Computer Science and Engineering

Mid Semester Examination(MST-MAKE UP 2023)

BE. (3rd Year CSE/COE)
Date & Time: 17 April 2023, 5:30 PM.
Duration: 2Hrs
Total Marks: 25
Instructions: *Attempt any 5 Questions.*

Course Code: UCS648
Course Name: Cyber Forensics
Faculty: Dr. Jaskirat Singh

Q1a. What is Criminal Profiling? When does Criminal Profiling should be applied by the investigator? **(1 marks)**

Q1b. Consider the following scenarios:

Scenario1: The customers of DBI bank in mumbai have been victim of fake fixed deposit fraud. All the employees were trapped into the fraud scheme after getting information from the fake banners pasted near the bank premises. Earlier similar frauds have also been reported by the clients of Crompton Bank in Agra and Ballarpur Bank in Orissa.

Scenario2: A RAT malware has been found on the PC of the head of the Research and Development department of DRDO. All the PC of Simulation and Modelling LAB have been found to be infected by the same malware.

Explain the profiling method that the investigator should apply in both the scenario. With respect to the applied profiling method, which information does the investigator should collect. **(4 marks)**

Q2a. Explain in detail how investing a computer machine in a switched OFF state is different from investigating a machine in switched ON state? **(4 marks)**

Q2b. How subpoena is different from a Warrant? **(1 marks)**

Q3a. Bipul, age 45, is a native of Bhiki Village, Punjab and is popularly as "lotteryking". He has been held by the law enforcement for duping local people by selling fake lottery tickets to them. He gets the fake tickets design file through emails from his associates in other countries and he prints the fake ticket from his own color photocopier machine. The investigators seized his laptop and photocopier machine. The following snapshot of the system with windows operating system and a volume size of 2GB was documented by Investigators:

C:\Windows\system32>fsutil fsinfo ntfsinfo c: NTFS Volume Serial Number : 0xf4ca5d7cca5d3c54 Version : 3.1 Number Sectors : 0x00000000078fd7ff, Physical Sector : 0x0000000000800, Total Clusters : 0x0000000006f1faff, Free Clusters : 0x00000000000e8821 , Total Reserved : 0x0000000000000910 , Mft Valid Data Length : 0x000000000196c0000, Physical Cluster : 0x0000000000002000 Mft Start Lcn : 0x00000000000c0000 Mft2 Start Lcn : 0x000000000097ffff Mft Zone Start : 0x0000000000051f920 Mft Zone End : 0x0000000000051f9a0 RM Identifier: 0652C3D3-7AA9-11DA-ACAC-C80AA9F2FF32.

Analysing the forensic image of the harddisk, a file named "money to lotteryking.txt" (Figure 1) was recovered which was found to be deleted a day before his arrest. Investigators are now interested in knowing: How much is the slack space. Also, they are interested in finding what message is circulated in the file. Help the investigators in answering these questions. **(5 marks)**

money to lotteryking.txt

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	4D	4F	4E	45	59	20	48	41	53	20	42	45	45	4E	20	54
00000016	52	41	4E	53	46	45	52	45	44	20	54	4F	20	59	4F	55
00000032	52	20	41	43	43	4F	55	4E	54	20	20	20	20	20	20	20
00000048	20	20	20	20	20											

Figure 1. Snapshot of the recovered file

Q4(a) Explain the statement "digital evidence is intangible". What are the requirements for digital evidence to be admissible in court **(2 marks)**

4(b) Explain how disk imaging is different from normal copying **(3 marks)**

Q5a. To prevent the integrity of evidence, explain what steps does the investigator should take? **(1.5 marks)**

Q5b. John was involved with embezzling of company funds of worth 500 crores. The money was transferred online through using a virtual private network. The machine has been seized and investigation has been initiated. Write down the steps and techniques that can be used to solve this case. **(3.5 marks)**

Roll No_____

Thapar Institute of Engineering and Technology
Department of Computer Science and Engineering
END Semester Examination EVEN2023

BE. (3rd Year CSE/COE)
Date & Time: 15 MAY 2023, 2:00PM.
Duration: 3Hrs
Total Marks: 40

Course Code: UCS648
Course Name: Cyber Forensics
Faculty: Dr. Jaskirat Singh (JAS)

Instructions: *Attempt all Questions.*

Q1. **(a)** Explain in detail how organization policy can facilitate the investigative process? **(3 marks)**
(b) Discuss what type of crimes are categorized as non-violent cybercrimes **(2 marks)**

Q2. Bipul, is undergoing trial for selling fake IPL tickets at Mohali Cricket Stadium. He was nabbed by the mohali police with the help of a informer who bait bipul to sell a ticket to him. During investigation, Bipul told the law enforcement that he used to print the fake tickets at home. The investigators have seized bipul laptop and color printer. The following snapshot of the system was documented by the Investigators:

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

I:\Windows\system32>fsutil fsinfo ntfsinfo I:
NTFS Volume Serial Number :       0x9c823fad823f8ab2
Version :                         3.1
Number Sectors :                  0x000000001efd57ff
Total Clusters :                  0x0000000003dfaaff
Free Clusters  :                  0x0000000000d1cbe1
Total Reserved :                  0x00000000000007d0
Bytes Per Sector  :               0x400
Bytes Per Cluster :               0x2000
Bytes Per FileRecord Segment    : 1024
Clusters Per FileRecord Segment : 0
Mft Valid Data Length :           0x0000000041880000
Mft Start Lcn  :                  0x000000000000c0000
Mft2 Start Lcn :                  0x0000000000000002
Mft Zone Start :                  0x000000000004f3c00
Mft Zone End   :                  0x000000000004f4f00
Encription :                      Enabled
Cipher:                           ROT2 on English Alphabets
Text Encoding:                    Windows(ANSI)
```

Analyzing the forensic image of the harddisk, Large no of files named in a sequential order, i.e. "ticket_no_4300.txt" to "ticket_no_4320.txt" were found to be deleted. The most recent file "ticket_no_4320.txt" was found to be deleted just day before Bipul was arrested. Investigators have recovered the deleted file "ticket_no_4320.txt" file as shown below:

ticket_no_4320.txt

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00000000	4E	67	69	6B	76	6B	6F	63	76	67	20	76	6B	65	6D	67
00000010	76	20	68	71	74	20	4B	52	4E	20	6F	63	76	65	6A	20
00000020	63	76	20	6F	71	6A	63	6E	6B	20	64	67	76	79	67	67
00000030	70	20	76	79	71	20	76	67	63	6F	75					

The Investigators are interested in knowing the contents of this file **(4 marks)** and how much is the space of this file **(1 marks).** Help the investigators in answering these questions.

Q3.**(a)** Explain what are the different ways by which data can be hidden in a digital crime? **(3 marks)**

Q3.**(b)** The NTFS file system views each file (or folder) as a set of file attributes. Explain the different attributes of the file record in NTFS file system? **(2 marks)**

Q4. **(a)** Explain in detail the steps involved in the prosecution of the cybercrime case? **(3.5 marks)**
(b) What are the problems faced in solving the computer based crime? **(1.5 marks)**

Roll No_____

Q5. (a) What aspects of the evidence needs to be proven for it to be admissible in court? **(2 marks)**

(b) The Investigator should be aware about the laws of the jurisdiction. Explain the different types of law? **(2 marks)**

(c) The Complainant has been constantly receiving communications over the email from the defendant council to withdraw the case against the defendant in an ongoing trial. The defendant had approached the court for the same. Explain specifically how the complainant can get relief from the court. **(1 marks)**

Q6. The forensic disk image of the suspect machine having ntfs file system has been captured. The first sector of the physical disk has been extracted as follows:

```
30 45 63 32 2E 00 00 08 A3 00 7E 01 00 00 00 20
11 00 0B FA FF BA 00 08 00 00 00 23 D3 00 80 20
21 00 07 FE FF AE 00 04 00 00 00 44 E7 00 00 30
30 66 64 54 3D AC 00 04 00 00 00 33 A4 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA
```

You as investigator have been asked to dissect the following raw bytes and report vital information required for locating data records in disk volumes. **(5 marks)**

```
EB 52 90 4E 54 46 53 20 20 20 20 00 08 10 00 00
00 00 00 00 00 F8 00 00 3F 00 FF 00 00 08 00 00
00 00 00 00 80 00 00 00 FF 43 E7 00 00 00 00 00
00 00 0D 00 00 00 00 00 02 00 00 00 00 00 00 00
F6 00 00 00 01 00 00 00 FD 5C 5D AE 94 5D AE 26
00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07
1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E
54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB
55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC
18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13
9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3
0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8
66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8
4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D
66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16
68 07 BB 16 68 70 0E 16 68 09 00 66 53 66 53 66
55 16 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF
28 10 B9 D8 0F FC F3 AA E9 5F 01 90 90 66 60 1E
06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00
00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E
00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F
0F 82 16 00 66 FF 06 11 00 03 16 0F 00 8E C2 FF
0E 16 00 75 BC 07 1F 66 61 C3 A0 F8 01 E8 09 00
A0 FB 01 E8 03 00 F4 EB FD B4 01 8B F0 AC 3C 00
74 09 B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 41 20
64 69 73 6B 20 72 65 61 64 20 65 72 72 6F 72 20
6F 63 63 75 72 72 65 64 00 0D 0A 42 4F 4F 54 4D
47 52 20 69 73 20 6D 69 73 73 69 6E 67 00 0D 0A
42 4F 4F 54 4D 47 52 20 69 73 20 63 6F 6D 70 72
65 73 73 65 64 00 0D 0A 50 72 65 73 73 20 43 74
72 6C 2B 41 6C 74 2B 44 65 6C 20 74 6F 20 72 65
73 74 61 72 74 0D 0A 00 8C A9 BE D6 00 00 55 AA
```

Q7. Explain in detail the steps required to secure the evidence? **(5 marks)**

Q8. (a) Explain the difference between physical and digital evidence? **(2 marks)**

(b) Explain how software write blocking is implemented? **(3 marks)**