ofc

Thapar Institute of Engineering and Technology

Department of Computer Science and Engineering

Mid Semester Examination (MST- EVEN2023)

BE. (3rd Year CSE/COE)
Date & Time: 6 March 2023, 3:30 PM.
Duration: 2Hrs
Total Marks: 25

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

Instructions: *Attempt all 5 Questions.* ***Each question is of 5 marks.***

Q1(a) Explain how disk imaging is different from normal copying (2 marks)

1(b) Explain Inductive and Deductive profiling with the help of an example? (3 marks)

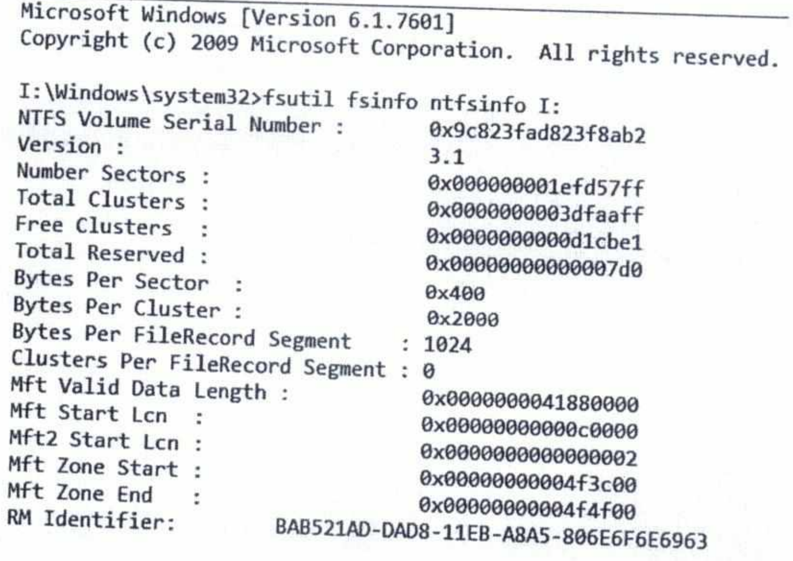
Q2(a) Describe the steps to investigate a cyber crime incident in Business Organizations?(3 marks)

2(b) Explain what are the contents of chain of custody and its importance in any case? (2 marks)

Q3(a)Translational Health Science and Technology Institute(THSTI), Ministry of Science and Technology, Government of India deals with producing biomedical innovations for human health. The research team of the scientists has developed first indigenous vaccine against rotavirus that serves to protect against severe diarrhea in children. The vaccine formulation got leaked in the public domain. The laptop of one of the research scholar working on the same project was seized by the Incidence Response Team (IRT). IRT team found a malware program running as a process id=943. Explain the different forensic investigation techniques that can be utilized by the investigator in this case? (3 marks)

3(b) Explain how disk imaging is different from normal copying (2 marks)

Q4. Harjeet is a native of Ambala, Haryana and is undergoing trial for selling fake railway tickets at Ambala Railway Station. He was nabbed by the Ambala railway police with the help of a informer who bait harjeet to sell a ticket from Ambala to Amritsar. During investigation, harjeet told the law enforcement that he used to get the fake tickets design file through whatsapp messages from his friend Bipul who runs a photograph printing shop in Amritsar. He used to print the fake ticket from his own color photocopier machine. The investigators have seized harjeet laptop and photocopier machine. The following snapshot of the system with windows operating system with ntfs file system on volume I: of size 100GB was documented by the Investigators:

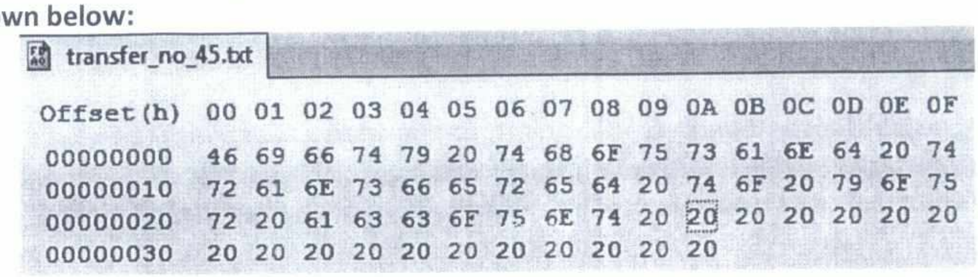


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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  :                  0x00000000000c0000
Mft2 Start Lcn :                  0x0000000000000002
Mft Zone Start :                  0x00000000004f3c00
Mft Zone End   :                  0x00000000004f4f00
RM Identifier:          BAB521AD-DAD8-11EB-A8A5-806E6F6E6963
```

Ofc

Analyzing the forensic image of the harddisk, Large no of files named in a sequential order from 1 to 45 , i.e. “transfer_no_1.txt” to "transfer_no_45.txt" were found to be deleted. The most recent file "transfer_no_45.txt" was found to be deleted just day before Harjeet was arrested. Investigators have recovered the deleted file "transfer_no_45.txt" file as shown below:



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

00000000   46 69 66 74 79 20 74 68 6F 75 73 61 6E 64 20 74
00000010   72 61 6E 73 66 65 72 65 64 20 74 6F 20 79 6F 75
00000020   72 20 61 63 63 6F 75 6E 74 20 20 20 20 20 20 20
00000030   20 20 20 20 20 20 20 20 20 20 20
```

The Investigators are interested in knowing the contents of this file and how much is the slack space of this file. Help the investigators in answering these questions.

Q5(a) Explain the steps that needs to be taken by the crime scene technician if the system is in switched OFF state. (3 marks)

5(b) Explain How a fraudulent ponzi scheme is different from a pyramid scheme (1 marks)?

5(c) Explain How cyber fraud is different from cyber threat (1 marks)?