Roll No____________________

# Thapar Institute of Engineering and Technology
## Department of Computer Science and Engineering
## END Semester Examination EVEN2022

**BE. (3rd Year CSE/COE)** **Course Code:** UCS648

**Date & Time:** 2~~6~~7 MAY 2022, 11:15 AM. **Course Name:** Cyber Forensics

**Duration:** 2Hrs **Faculty:** Dr. Jaskirat Singh (JAS)

**Total Marks:** 35

***Instructions:*** *Attempt all 5 Questions.*

**Q1a.** The forensic investigator must be aware of the ways by which the data (indicators) could possibly be hidden by the suspect. Explain what are the ways by which forensic investigator could find the data associated with the crime. **4 marks**

**Q1b.** Explain what is Host Protected Area(HPA). **2 marks**

**Q1c.** Joseph works with finance company rocket finance. He deleted a file “list_final” having list of clients from his laptop. The file was located at location E:\customer\list_final.doc. what is the renamed version of the deleted file if list_final.doc is the 4th file to get deleted. **1 marks**

**Q2.** The forensic disk image of the suspect machine has been captured. The partition table entries in the MBR are as follows:

```
20 55 53 42 2E 00 00 00 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 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA
```

You as investigator has been asked to dissect the following raw bytes and report vital information required for locating data records. **7 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
```

Roll No____________________

**Q3a.** In a computer crime case, the evidence can be of what different types? **2 marks**

**Q3b.**What is the difference between interview and interrogation. Explain the different methods to interrogation. **3 marks**

**Q3c.** List out the organizations involved in formulation of standard methods for collection and analysis of digital evidence. **2 mark**

**Q4a.** Bipul has filed a consumer case related to deficiency of service with his internet service provider – Speed Communications ltd. He is getting threatening phone calls and text messages from the circle manager of Speed Communications ltd. to withdraw the legal case from the court. How can the judiciary help Bipul in this scenario? **1 mark**

**Q4b.** What are the investigative tools investigators can use to investigate a case? **3 marks**

**Q4c.** Explain the structure of the Master Boot Record of the disk formatted with NTFS file system? **3 marks**

**Q5.** Explain in detail the steps involved in the investigation of the cybercrime case? **7 marks**