CE1.3-R4: CYBER FORENSICS & LAW

NOTE:

1. **Answer question 1 and any FOUR from questions 2 to 7.**
2. **Parts of the same question should be answered together and in the same sequence.**

Time: 3 Hours **Total Marks: 100**

1.

a) Discuss the features and limitation of FAT, FAT16, FAT32 and NTFS file systems.
b) List the rules of digital evidence that should be looked into for ensuring its usefulness.
c) Explain in brief various anti-forensic techniques used by perpetrators.
d) How a bad extension in the file name is identified using tools as well as the correction of the same is done?
e) Explain the importance of "Chain of Custody of Digital Evidence" during the digital forensic investigations. Design a form for recording it.
f) List the do's, do not's along with necessary precautions to be followed, while carrying out analysis of a digital evidence.
g) Define the digital forensics along with the processes involved in the digital forensic investigations.

(7x4)

2.

a) What happens if a computer with 'Windows OS' goes into 'hibernation' mode? Describe the significance of hibernation in digital forensic analysis.
b) Explain the types of digital evidences. Describe the tools to collect volatile evidence from a suspected computer.
c) Many of our normal daily activities in life, we leave a digital trail. Consider one typical day in your life as an example and briefly describe six digital trails left by you through your activities.

(7+5+6)

3.

a) Explain the legal formalities associated with the seizing and preserving of digital data storage device from a suspected computer system.
b) Describe the role of Windows Registry in digital forensic investigations.
c) What do you mean by 'integrity' of digital evidence? What are the guidelines and best practices to be followed to maintain the integrity of the evidence? How the same can be verified by analysts at any stage of digital forensic investigations?

(4+7+7)

4.

a) Describe any five methods used by perpetrators to hide or disguise files in digital data storage devices? What are the general counters measures taken by cyber forensic analysts to handle them?
b) What is a bit stream copy of data from a digital data storage device? How is it different from a copy or backup? Describe its usefulness in digital forensic analysis. Name the tools to make a bit stream copy.
c) Describe the investigation and analysis of the cyber-crimes associated with the social networking websites.

(5+8+5)

5.

a) What is the role of a 'First Responder' in digital forensic investigation? Describe the tools and equipment required by a first responder in the toolkit to be possessed while visiting the cyber-crime site.
b) Describe the various functions of an integrated digital forensic toolkit. Give the names of two such toolkits which are well known to the Indian Compute Forensic Community.

c) During the e-mail investigations, how will you find the details in respect of the source of an e-mail? What are the other resources required to verify these details?

(6+8+4)

6.

a) What can happen if a seized original digital data storage device is analysed directly? Which legal issues could be associated in such circumstance? Describe the solution to overcome these legal issues.

b) Which section of Indian IT Act provides the details in respect of level of police officer who can handle a cyber-crime? Discuss the activities which can be performed by the police official at the site of cyber-crime.

c) Which section of Indian IT Act is used to handle the criminal cases of Cyber Terrorism? Describe the section in detail providing the acts of cyber terrorism and punishments.

(8+5+5)

7. In the context of Digital Forensic Analysis, write short notes on:

a) Digital Steganography

b) CDR analysis with tool

c) Slack Space in a file

(6+6+6)