CE1.3-R4: CYBER FORENSIC & 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) Which are the time stamps maintained by the file system for a file on digital data storage media? How are these time stamps useful in digital forensic investigations? What are the legal issues associated with these time stamps?

b) What do you understand by 'Message-ID' and 'ESMTP ID'? How can these be viewed? How are these useful in digital forensic investigations?

c) Explain five rules of digital evidence.

d) List out various cyber-crimes covered under erstwhile Section 66A of Indian Information Technology Act. Why was the same scrapped by Honourable Supreme Court of India?

e) What is 'Social Engineering Attack' and how is it carried out? Explain any five common social engineering attacks and the tips to avoid victimisation by the same.

f) What is e-mail spoofing? How is e-mail spoofing done?

g) What are 'Call Details Records'? Why and who maintain these? How these records are useful in investigation of crimes?

(7x4)

2.

a) How can Digital Signatures be used by the sender of a digital document to make it confidential? How can the receiver use digital signatures to verify (i) integrity and (ii) confidentiality of the digital document received?

b) How can you find the list of USB devices that were used in past on a windows computer system as well as the date stamp for the last use of the same?

c) Explain various 'Anti-forensic' tricks generally adopted by the cyber criminals.

(7+6+5)

3.

a) Explain the sections along with the contents and tables that should be available in a standard Digital Forensic Analysis Report for a typical cyber-crime analysis carried out in digital forensic lab.

b) Explain the process of digital forensic investigation of an E-mail. Generally, what is the purpose of such investigation? Explain the evidences that can be extracted from an E-Mail?

c) What do you understand by 'Metadata', 'File Headers' and 'File Carving'? How are these useful in digital forensic investigations? Explain the use of any three File Carving Tools.

(8+5+5)

4.

a) What is Cyber Terrorism? Which are the typical infrastructures targeted by the Cyber Terrorists? Which section of Indian Information Technology Act covers the criminal activity related to Cyber Terrorism? What is the punishment prescribed under Indian IT Act for activity of Cyber Terrorism?

b) What is a 'Rainbow Table'? How is the same used in Cyber Forensic Analysis?

c) Illustrate the procedure with any tool for capturing the RAM data from alive computer.

(7+6+5)

5.

a) List and explain the necessary steps in making a digital forensic image of a suspected digital data storage media, starting from its receipt in the digital forensic lab including chain of custody and case documentation for preparing the digital forensic analysis report.

b) Write a short note on Network Forensics. List at least one tool, which could be used to capture and analyse the network traffic and the approaches to store and analyse the captured data.

c) A physically damaged hard disk is seized from the crime scene and it is noticed that its magnetic platters are intact. Explain the methodology to be adopted in a lab to prepare its digital forensic image.

(6+7+5)

6.

a) What are the general criteria for acceptability of a digital forensic software tool in a court of law? What are the general conditions defined by NIST for accepting the validity of a digital forensic software tool?

b) List out the necessary features that should be available in a typical integrated Computer Forensic Toolkit to be used for data acquisition and analysis of a digital data storage media.

c) Explain 'Cluster' and 'Slack Space' and their importance in digital forensic investigations.

(6+6+6)

7. In the context of digital forensic analysis, write short notes on the following:

a) Bulk_extractor

b) Windows Registry Analysis

c) Internet Evidence Finder.

(6+6+6)