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)   List the rules of Computer forensics.
b)   Explain the important features of Coroner's toolkit.
c)   Differentiate between public key cryptography and Private key cryptography.
d)   Explain the applications of network forensics toolkit.
e)   Explain the role and significance of accreditation standards in Cyber forensics.
f)   Distinguish between deleted file and deleted partition recovery procedures.
g)   Explain common law privacy.

                                                                                                        (7x4)

2.
a)   Explain Windows Registry. Discuss about the uses of windows registry, where in normal scenario, information retrieval is impossible.
b)   Explain cyber crime investigation process using cyber forensic techniques in detail.

                                                                                                        (9+9)

3.   Review the tools for following cyber forensics applications-
a)   Data Acquisition
b)   Capturing of RAM data and analysis
c)   Cryptanalysis
d)   Steganography

                                                                                                        (18)

4.
a)   What is 'File Carving'? How it is done and what is its utility in computer forensics.
b)   Discuss the various attacks in detail:-
        i)   Spoofing
        ii)   Hijacked Session Attacks
        iii)   Cyber Stalking

                                                                                                        (9+9)

5.
a)   Explain the accreditation standards for the following:
        i)   Evidence Control Checklist,
        ii)   Quality Assurance Checklist
b)   Differentiate between data recovery in Linux and Data Recovery in Windows O.S.

                                                                                                        (9+9)

6.
a)   What is Backtracking? Explain Forensic Discovery and Analysis Using Backtrack.
b)   Explain the following Law in respect to Cyber Security:
        i)   Constitutional Law
        ii)   Corporate Law

                                                                                                        (9+9)

7.   Write short note on **any three**:-
a)   Data Imaging and duplication
b)   Anti-Forensics
c)   e-mail investigation
d)   Manipulating File Systems

                                                                                                        (3x6)