Paper ID : 261564

Subject Code:BCAI061

Roll No:													

BTECH
(SEM. VI) THEORY EXAMINATION 2025-26
CYBER FORENSIC ANALYTICS

TIME: 3 HRS **M.MARKS: 70**

Note: Attempt all Sections. In case of any missing data; choose suitably.

SECTION A

1. Attempt *all* questions in brief. **02 x 7 = 14**

Q no.	Question	CO	Level
a.	Explain the security challenges involved in eCash systems.	1	K1
b.	What is cyber terrorism and cyber warfare?	1	K1
c.	Explain the importance of digital devices in cyber forensics.	2	K1
d.	What are DoS and DDoS attacks?	2	K1
e.	Explain the concepts of cyber investigation and network investigation.	3	K1
f.	Define evidence and digital evidence.	4	K1
g.	Explain the concept of electronic governance (e-Governance).	5	K1

SECTION B

2. Attempt any *three* of the following: **07 x 3 = 21**

a.	Explain the concept of cyber space and discuss how cyber crimes differ from traditional crimes.	1	K3
b.	What is data carving in cyber forensics? Explain different data carving techniques used to recover deleted or hidden files.	2	K2
c.	Discuss the importance of audit logs in cyber investigations. Explain the methods used for investigating audit logs to identify suspicious activities.	3	K3
d.	Discuss the importance of contextual information in evidence analysis and cyber crime investigations.	4	K2
e.	Explain the objectives and key features of the Information Technology Act 2000 in regulating cyber activities and cyber crimes in India.	5	K2

SECTION C

3. Attempt any *one* part of the following: **07 x 1 = 07**

a.	Describe different types of cyber financial frauds, including ATM frauds, phishing, and phreaking. Suggest preventive measures against them.	1	K2
b.	Explain the working of key loggers and email frauds as practical cyber crime techniques. How can individuals and organizations protect themselves from such attacks?	1	K3

4. Attempt any *one* part of the following: **07 x 1 = 07**

a.	Explain the concept of steganography and its role in cyber crime. How do forensic investigators detect hidden information in digital media?	2	K2
b.	Differentiate between Trojans, Backdoors and Botnets. Explain how these malware attacks affect computer systems and networks.	2	K3

Roll No:													

BTECH
(SEM. VI) THEORY EXAMINATION 2025-26
CYBER FORENSIC ANALYTICS

TIME: 3 HRS **M.MARKS: 70**

---

5. Attempt any *one* part of the following: **07 x 1 = 07**

a.	Explain the concept of profiling in cyber investigations. How are cyber criminal profiling and stylometric techniques used to identify suspects?	3	K2
b.	Differentiate between warranted searches and warrantless searches in cyber investigations. Discuss the legal and ethical challenges involved.	3	K3

6. Attempt any *one* part of the following: **07 x 1 = 07**

a.	Describe the role of evidence management in cyber forensics. Explain the procedures followed during pre-search activities and on-scene activities.	4	K2
b.	Discuss the practical applications of digital evidence analysis and network analysis in identifying and prosecuting cyber criminals.	4	K2

7. Attempt any *one* part of the following: **07 x 1 = 07**

a.	What are electronic signature certificates? Explain the procedure for obtaining and using them in secure online communication.	5	K2
b.	Describe the penalties and compensation provisions under the Information Technology Act 2000 for cyber offences and data breaches.	5	K3