PSG COLLEGE OF ARTS & SCIENCE
(AUTONOMOUS)

BVoc DEGREE EXAMINATION MAY 2022
(Sixth Semester)

Branch – **NETWORKING AND MOBILE APPLICATIONS**

DISCIPLINE SPECIFIC ELECTIVE – II: CYBER FORENSICS

Time: Three Hours Maximum: 75 Marks

SECTION-A (10 Marks)
Answer **ALL** questions
ALL questions carry **EQUAL** marks (10 x 1 = 10)

1. Which of the following enables attackers to gain control over the computer by exploiting the vulnerabilities in the software
   (i) Web Jacking (iii) XSS attack
   (ii) Theft of FTP passwords (iv) Exploit kits
2. Which of the following is an example of Data espionage?
   (i) Cybercrime against person (iii) Cybercrime against nation
   (ii) Cybercrime against property (iv) All these
3. Which of the following is a form of Pharming?
   (i) Online fraud (iii) system interference
   (ii) Copyright – and trademark-related offence (iv) data interference
4. Which includes rogue security software and tech support scams
   (i) Scareware (iii) Screen Lockers
   (ii) Encrypting Ransomware (iv) BitCoin
5. Which forensic tool helps to collect useful evidence?
   (i) mgrep (iii) nshark
   (ii) shark (iv) ngrep
6. Which reveals to the analyst any unauthorized changes made to system binaries?
   (i) Timeline analysis (iii) System file Analysis
   (ii) Volatile evidence analysis (iv) data recovery analysis
7. Which among the following is the first action performed while booting to ensure the presence and functionality of the core components?
   (i) Power on Self Test (iii) Plug on Self Test
   (ii) Power on System Test (iv) Plug on System Test
8. How Timestamp is updated when the file or directory is written in inode
   (i) Updated (U) (iii) Modified (M)
   (ii) Wrote (W) (iv) Changed (C)
9. Which algorithm is used for computing the condensed representation of a message or a data file?
   (i) CRC32 (iii) MD5
   (ii) E01 (iv) SHA
10. Which of the following is analysed by emailTrackerPro?
    (i) routes of network (iii) routes of email
    (ii) email protocols (iv) email headers

Cont...

SECTION - B (25 Marks)

Answer **ALL** questions

ALL questions carry **EQUAL** Marks (5 x 5 = 25)

11. a) Examine the different types of cybercrime.

(OR)

b) What do means Mens rea and Actusreus in cybercrime? How are they applicable to cybercrime?

12. a) What is infringing on property rights? List its types.

(OR)

b) Outline the deep web and its challenges.

13. a) Describe the methods employed in forensics analysis.

(OR)

b) Examine the stages of Incident Handling

14. a) Compare physical and digital evidence.

(OR)

b) D the components of FAT file system.

15. a) Infer the forensics tools used in password recovery.

(OR)

b) Mention the role of the forensic analyst in analysis.

SECTION -C (40 Marks)

Answer **ALL** questions

ALL questions carry **EQUAL** Marks (5 x 8 = 40)

16. a) Summarize the tools used in cybercrime.

(OR)

b) Analyze the factors influencing the cybercrime with its challenges.

17. a) Inspect the various cybercrime against property.

(OR)

b) Explain ransomware attack.

18. a) Summarize the steps involved in forensic investigation.

(OR)

b) Discuss the stages of mobile forensics.

19. a) Discuss the phases of evidence collection procedure.

(OR)

b) Explain how the browser artifacts of different operating system can be collected as evidence.

20. a) Examine the forensic tools used for analysing the network.

(OR)

b) Explain RAM analysis with volatility.

Z-Z-Z END