Register No.: …… Name: ……..

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

SECOND SEMESTER M.C.A DEGREE EXAMINATION (Regular), JULY 2022

(2021 SCHEME)

Course Code: **21CA204-E**

Course Name: **Ethical Hacking and Cyber Forensics**

Max. Marks: **60** **Duration: 3 Hours**

PART A

(Answer all questions. Each question carries 3 marks)

1. What is a keylogger? How do hackers use keyloggers to steal passwords?
2. Write notes on footprinting in ethical hacking.
3. Analyse the vulnerabilities of embedded operating systems.
4. Write an overview of network protection systems.
5. How digital forensics can help after a cyber-attack?
6. Discuss the importance of law enforcement agency investigation.
7. What is the importance of data acquisition in digital forensics? Briefly explain any three key points.
8. Examine the need of image acquisition in digital forensics.
9. Summarize the tasks performed by digital forensics tools.
10. Write short notes on: i) OSForensics ii) Network Miner

PART B

(Answer one full question from each module, each question carries 6 marks)

MODULE I

11. Illustrate operating system vulnerability with suitable example. (6)

OR

12. a) How hackers use social engineering as a tool for attack? (2)
    b) Discuss the types of port scanning. How do you prevent port scanning attacks? (4)

MODULE II

13. Describe any two methods of hacking wireless networks. (6)

OR

14. a) What is cross-site scripting (XSS)? Describe how XSS works. (4)

b) Summarize the possible attacks on web servers. (2)

MODULE III

15. a) Write notes on digital forensics resources. (3)
    b) Elaborate the role of private sector investigations in digital forensics. (3)

OR

16. What is digital investigation? Explain the different ways of conducting digital investigation. (6)

MODULE IV

17. What is digital evidence? Elaborate on the storage formats for digital evidence. (6)

OR

18. Elaborate the steps for validating data acquisitions. How will you find the best acquisition method? (6)

MODULE V

19. a) Illustrate any two forensics software tools used for forensic investigation. (4)
    b) Write notes on forensic workstations. (2)

OR

20. List and elaborate on the methods for validating and testing forensic software. (6)

****