P.G. DIPLOMA IN INFORMATION SECURITY (PGDIS)

Term-End Examination

June 2021

MSEI-027 : DIGITAL FORENSICS

Time : 2 hours *Maximum Marks : 50*

Note :

*Section A – Answer **all** the objective type questions.*

*Section B – Answer **all** the very short answer type questions.*

*Section C – Answer any **two** questions out of three short answer type questions.*

*Section D – Answer any **two** questions out of three long answer type questions.*

SECTION A

Attempt all the following questions. *10×1=10*

1. The _____ refers to handing over the results of private investigations to the authorities because of indications of criminal activity. *1*

2. A/An _____ is a form of internet text messaging or synchronous conferencing. *1*

3. Class 1 bluetooth devices have the range of _____ metres. *1*

4. RAID stands for _____ . *1*

5. PUK stands for _____ . *1*

6. _____ are computers that excel at executing many different computer programs at the same time. *1*

7. _____ field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death. *1*

8. _____ is a digital object that contains reliable information that supports or refutes a hypothesis. *1*

9. A Multi-Media Card (MMC) is a solid state disk card with _____ number of pins connector. *1*

10. AAA Protocol/Service in RADIUS stands for _____ . *1*

SECTION B

Attempt all the questions. *5×2=10*

11. Define Ad hoc mode of operation. *2*

12. Explain Active and Passive Reconnaissance in Hacking. *2*

13. Define Cloning in Forensic Analysis. *2*

14. Define 'Copy of the drive' and 'Imaging of the drive'. *2*

15. Define honey potting. *2*

SECTION C

Attempt 2 out of 3 short answer type questions. *2×5=10*

16. Explain Money Laundering and Phishing. *5*

17. Explain the process of LOG File Analysis. How can deleted files be reconstructed ? *5*

18. What are the legal issues involved in the seizure of computer equipment ? *5*

SECTION D

Attempt 2 out of 3 long answer type questions. *2×10=20*

19. Explain Intrusion Detection System. How is it different from Firewall ? Define IPS. *10*

20. Explain the needs which are required for conducting an effective investigation for cyber crime. *10*

21. Describe procedure of RAM forensics, Hard Disk forensics and Mobile forensics. *10*