BE/Sem VII/Comp/Digital Forensic/25.11.16

NOV-2016

QP CODE : 725003

(3 Hours) **[Total Marks 80**

N.B. (1) Question No. 1 is **Compulsory**.
(2) Attempt any **THREE** questions out of remaining five questions.
(3) Assume any suitable data if required with justification.

Q. 1 a) What do you mean by incident response methodology? Explain all components of it. 10

b) What do you mean by digital evidence? What are the challenges involved in evidence handling? 10

Q. 2 a) List and explain in brief steps taken to collect live data from UNIX system. 10

b) Explain procedure to investigate routers. 10

Q .3 a) Explain the terms : i) DMCA (ii) CFAA (iii) CANSpam 10

b) What are the steps involved in forensic analysis? Explain each in brief. 10

Q. 4 a) What are various hacking tools? Explain any two in details. 10

b) Explain the bodies of law. Explain the levels of law. 10

Q. 5 a) Write the differences between: 10
(i) netcat and cryptcat (ii) Virus and Worms.

b)Explain procedure for recording cryptographic checksums of critical files. What are the advantages of it ? 10

Q. 6 Answer **any four**: 20
a) Write short notes on Evidence Validation.
b) Explain the terms ; Forensic Duplicate, Qualified Forensic Duplicate .
c) Write short notes on Internet Fraud.
d) Explain techniques used to recover the deleted files.
e) Explain the storage layer of the file system.
f) Explain levels of culpability.
