BRAINWARE UNIVERSITY

Term End Examination 2023
Programme – B.Sc.(ANCS)-Hons-2020
Course Name – Digital Forensics
Course Code - BNCSC602
(Semester VI)

Full Marks : 60 **Time : 2:30 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A
(Multiple Choice Type Question) 1 x 15=15

1. *Choose the correct alternative from the following :*

(i) Develop the private networks can be a richer source of evidence than the Internet because _____

a) They retain data for longer periods of time
b) Owners of private networks are more cooperative with law enforcement
c) Private networks contain a higher concentration of digital evidence
d) All of the above

(ii) Summarize that computer forensics involves all of the following stated activities except _____

a) Extraction of computer data
b) Interpretation of computer data
c) Preservation of computer data
d) Manipulation of computer data

(iii) Define digital forensics _____

a) The process of analyzing digital data to investigate and prevent cybercrime.
b) The process of recovering deleted files and folders.
c) The process of monitoring employee internet activity.
d) The process of performing computer repairs and maintenance.

(iv) Define the Long form of DFI _____

a) Digital Forensic Investigation
b) Digital Fraud Industry
c) Defining Form In
d) None

(v) Select the form of electronic evidence _____

a) Hard Drive
b) E-mail
c) Either A or B
d) Both A and B

(vi) Tell the digital evidence are used to established a credible link between _____

a) Attacker and victim and the crime scene
b) Attacker And information
c) Either A or B
d) Both A and B

(vii) Define that which of the following is not type of volatile evidence _____

a) Routing Tables
b) Main Memory
c) Log Files
d) Cached Data

(viii) Choose what are the difficulties in handling Digital Evidence _____

a) Easy to destroy
b) Easy to sustain
c) Hard to get
d) None of the above.

(ix) Identify that to crack the password you need cracking tool such as

a) LC4
b) John The Ripper
c) pwdump
d) All of the above

(x) Classify a scientific truth attempts to identify roles that are universally true. Legal judgment, on The other hand, has a standard of proof in criminal prosecutions of

a) Balance of probabilities
b) Beyond a reasonable doubt
c) Acquittal
d) None of the above

(xi) Choose which of the following is a passive online attack _____

a) Password guessing
b) Network sniffing
c) Brute-force attack
d) Dictionary attack

(xii) Discover that private networks can be a richer source of evidence than the Internet because

a) They retain data for longer periods of time
b) Owners of private networks are more cooperative with law enforcement
c) Private networks contain a higher concentration of digital evidence
d) All the above

(xiii) Choose in forensic duplication, the_____ of every file should be compared with a known set of hases and ignore any matches

a) Forensic hashes
b) Cryptography
c) MD5 hashes
d) Active hashes

(xiv) Choose WPA2 provides security in _____

a) Wi-fi
b) Ethernet
c) Bluetooth
d) None of the above

(xv) Identify that which is the legal form of hacking based on which jobs are provided in IT industries and firms

a) Cracking
b) Non ethical Hacking
c) Ethical hacking
d) Hactivism

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Define retrieved communication. (3)
3. Discuss the sources of potential evidence. (3)
4. Discover the logical structure of a hard disk. (3)
5. Define IIS Logs. (3)
6. Summarize mobile os for forensic purposes. (3)

OR

Conclude Integrated Circuit Card Identification. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Explain file carving. (5)
8. Summarize the types of malware analysis. (5)
9. Estimate the top threats for targetting mobile devices (5)
10. Explain the process of search and seizure. (5)
11. Explain the different types of densities on a hard disk. (5)

12. Explain indicators of a web attack. (5)

OR

Explain apache web server architecture. (5)

****