BRAINWARE UNIVERSITY

Term End Examination 2023-2024
Programme – B.Sc.(ANCS)-Hons-2020/B.Sc.(ANCS)-Hons-2021
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) How would you define that in computer intrusions the attacker will be leave multiple traces of there presence in.

   a) File System
   b) Registry
   c) System Logs
   d) All of these.

(ii) Define the full form of IMAP.

   a) Internet Message Access Protocol
   b) Internet Mail Agent Protocol
   c) Internet Mail Access Protocol
   d) None of these.

(iii) For which having a member of the search team trained to handle digital evidence that _____ .

   a) Can reduce the number of people who handle the evidence
   b) Can serve to streamline the presentation of the case
   c) Can reduce the opportunity for opposing counsel to impugn the integrity of the Evidence
   d) All of these

(iv) Name a digital investigator pursuing a line of investigation in a case because that line of Investigation proved successful in two previous cases is an example of _____ .

   a) Logical reasoning
   b) Common sense
   c) Preconceived theory
   d) Investigator's intuition

(v) Apply to the text, the most common mistake that prevents evidence seized from Being admitted is _____ .

   a) Uninformed consen
   b) Forcible entry
   c) Obtained without authorization
   d) None of these

(vi) Identify to obtaining a warrant, an investigator must convince the judge on all of the following Points except _____ .

   a) Evidence of a crime is in existence
   b) A crime has been committed

c) The owner or resident of the place to be searched is likely to have committed The crime

d) The evidence is likely to exist at the place to be searched

(vii) Tell that evidence contained in a document provided to prove that statements made in court are True is referred to as _____.

a) Inadmissible evidence

b) Illegally obtained evidence

c) Hearsay evidence

d) Direct evidence

(viii) Select that the digital forensics is all of them except _____ .

a) Extraction of computer data

b) Preservation of computer data

c) Interpretation of computer data

d) Manipulation of computer data

(ix) Identify the full form of IDIP.

a) Integrated Digital Investigation Process

b) Integrated Data Investigator Process

c) Integrated Digital Investigator Process

d) Independent Digital Investigator Process

(x) There are three c's in computer forensics, which is one of the three?

a) Control

b) Chance

c) Chains

d) Core

(xi) Define a valid definition of digital evidence is _____.

a) Data stored or transmitted using a computer

b) Information of probative value

c) Digital data of probative value

d) Any digital evidence on a computer

(xii) Which of following are unethical norms for investigator?

a) Uphold any relevant evidence

b) Declare any confidential matters or knowledge.

c) Distort or falsify education, training, credentials

d) All of these.

(xiii) Construct that deleted files is a common technique used in computer forensics is the recovery of deleted files.

a) True

b) False

c) Can be true or false

d) Can not say

(xiv) Choose the most common storage device for the personal computer is the _____.

a) Hard disk drive

b) USB thumb drive

c) Floppy disk

d) Zip disk

(xv) Identify a set of instructions compiled into a program that performs a particular task is known as.

a) Hardware

b) Central processing unit

c) Software

d) Motherboard

Group-B
(Short Answer Type Questions)   3 x 5=15

2. Define the objectives of computer forensics.   (3)
3. Define the roles of digital evidence.   (3)
4. Explain data analysis.   (3)
5. Illustrate data carving.   (3)
6. Summarize mobile phone forensic.   (3)

OR

Summarize SIMcon.   (3)

Group-C
(Long Answer Type Questions)   5 x 6=30

7. Justify the importance of analyzing malware. (5)
8. Describe IT Act 2000. (5)
9. Define different types of cyber-attacks. (5)
10. Explain data acquisition. (5)
11. Explain different types of data acquisition. (5)
12. Summarize different types of password cracking techniques. (5)

OR

Summarize the challenges of web application forensics. (5)

****