JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATIONS-2022

B.Tech-6th Semester (CS/IT)

COURSE CODE: 19B1WCI631 MAX. MARKS: 35

COURSE NAME: Digital forensics

COURSE CREDITS: 2 MAX. TIME: 2 Hour

Note: *All questions are compulsory. Marks are indicated against each question in square brackets.*

Q1. You are using Disk Manager to view primary and extended partitions on a suspect's drive. The program reports the extended partitions total size as larger than the sum of the sizes of logical partitions in this extended partition. Justify the following term:

1. The disk is corrupted.
2. There's a hidden partition.
3. Nothing; this is what you had expect to see.
4. The drive is formatted incorrectly.
5. Password is unknown. [5]

Q2. In the war of Russia and Ukraine cyber attackers try to loss each other in cyber space. Justify the following loses face by both country and classify the type of attacks in each prospect:

1. Gain the information of secret mission
2. Financial crisis
3. Identification of High level personnel's
4. Minimization of Bandwidth utilization and stop proper communication
5. Authenticity of information [5]

Q3. Interpret and validate the result of forensic analysis, you should do which of the following

1. Calculate the hash value with two different tools.

2. Use a different tool to compare the results of evidence you find.
3. Repeat the steps used to obtain the digital evidence, using the same tool, and recalculate?

[6]

Q4. Discuss recent trends in mobile forensic techniques to search the seizure electronic evidence and list out forensic tools with each step of forensic analysis. [5]

Q5. In recent scenario of government examination, it's difficult to prevent paper leaking by cyber attackers. As a cyber expert classify the type of threats and its solution with proper forensic tools? [6]

Q6. Explain volatile data collection for window operating system [3]

Q7. Write Short notes:

1. Trace the crime which has been happened through email.
2. Network analysis tools
3. IDS
4. Malware
5. Password Cracking [5]