Center of Cyber Security, Department of Computer Science and Engineering **Name:**

Institute of Technical Education & Research, SOA Deemed to be University **Regd. No.:**

QUIZ

Digital Forensic Workshop (CSE 3156)

Programme: B.Tech. (CSE Cyber Security) **Semester: 5th**

Full marks: __ **Time:** $\frac{1}{4}$ hours

Date: 04/10/2024 **Quiz No.:** 1

1. Which feature distinguishes dc3dd from dd?

   (a) dc3dd can only copy files, while dd can clone disks

   (b) dc3dd provides error correction and hashing capabilities, while dd does not

   (c) dc3dd has a graphical interface, while dd is command-line based

   (d) dc3dd is slower than dd

2. What is the primary purpose of the dd command in Unix/Linux systems?

   (a) Network troubleshooting

   (b) Disk cloning and data conversion

   (c) Creating user accounts

   (d) Monitoring system performance

3. What command is used to specify the configuration file when running Scalpel?

   (a) scalpel -c <config_file>

   (b) scalpel -f <config_file>

   (c) scalpel -o <output_directory>

   (d) scalpel –config <config_file>

4. Which command option in Scalpel is used to define the output directory for recovered files?

   (a) -d <output_directory>

   (b) -o <output_directory>

   (c) -r <output_directory>

   (d) –output <output_directory>

5. Which command option in Foremost specifies the maximum size of the output files created during recovery?

   (a) -m <size>

   (b) -s <size>

   (c) -l <size>

   (d) –max-size <size>

6. What does the -i option in Foremost specify?

   (a) The input file or disk image to be analyzed

   (b) The output format of the recovered files

   (c) The number of threads to use during recovery

   (d) The log file to record recovery progress

7. What will be the output of below code snippet:

```
result = subprocess.run(
["md5sum", file_path],
stderr=subprocess.PIPE,
text=True               )
print(result.stdout)
```

   (a) 128 bit hash of the specified file

   (b) syntax error

   (c) 256 bit hash of the specified file

   (d) no output without syntax error

8. Why is a hash check required when downloading a malware-affected memory dump file?

   A. To prevent corruption during download and ensure the file is intact.

   B. To verify that the downloaded file contains malware.

   C. To ensure that the memory dump file is not modified or tampered with.

   D. To confirm the file's integrity, authenticity, and prevent any manipulation.

   E. To check if the malware is removed from the file.

(a) Only A
(b) Only B
(c) Both A and C
(d) A, C, and D
(e) B and E

9. What is a hash collision, and why is it a concern in cryptography?

A. When two different inputs produce the same hash value, making it hard to distinguish between the two.

B. When a hash function generates an incorrect hash value, leading to data corruption.

C. When the hash length is too long, causing slow performance.

D. When a hash value cannot be verified due to network errors.

(a) Only A
(b) Only B
(c) Both A and C
(d) A and D
(e) None of the above

10. What is the primary function of Bulk Extractor in digital forensics?

A. To analyze memory dumps for running processes and hidden malware.

B. To extract useful information such as email addresses, URLs, and credit card numbers from disk images or data files.

C. To perform a full disk encryption of files to prevent data leaks.

D. To recover deleted files from storage devices for forensic analysis.

(a) Only A
(b) Only B
(c) Both A and C
(d) B and D
(e) None of the above