QUIZ

Digital Forensic Workshop (CSE 3156)

Programme: B.Tech. (CSE Cyber Security) **Semester: 5th**
Full marks: __ **Time:** $\frac{1}{3}$ hours
Date: 07/11/2024 **Quiz No.:** 2

---

1. Which tool is the Autopsy forensic browser primarily based on?
   (a) Volatility
   (b) The Sleuth Kit
   (c) FTK Imager
   (d) EnCase

2. In Autopsy, which of the following tabs provides details on when files were last written, accessed, changed, and created?
   (a) File Activity
   (b) Directory Structure
   (c) File Analysis
   (d) Metadata Overview

3. Which option in Autopsy allows investigators to analyze an image file without copying or moving it?
   (a) Import Method
   (b) Symlink
   (c) Hash Database
   (d) Evidence Link

4. The Autopsy forensic browser interface can be accessed via:
   (a) Command prompt only
   (b) The localhost web link on port 9999
   (c) SSH on port 22
   (d) A dedicated Autopsy application

5. In Volatility, which plugin is used to list the active processes in a memory dump?
   (a) procdump
   (b) dlllist
   (c) pslist
   (d) sockets

6. What is the purpose of the 'meta' number in Autopsy?
   (a) It tracks user activity.
   (b) It is the metadata ID that identifies file information in the file system.
   (c) It provides a backup of all deleted files.
   (d) It stores hashes for file integrity.

7. Which Volatility plugin would you use to generate exe and dat files from the raw files?
   (a) dumpfiles
   (b) sockets
   (c) netscan
   (d) memdump

8. When creating a case in Autopsy, the investigator can specify which of the following optional settings?
   (a) Encryption method
   (b) Investigator's email address
   (c) Time zone and hash database paths
   (d) Case size limit

9. Which Autopsy feature allows investigators to search for deleted files specifically?
   (a) Directory Seek
   (b) ALL DELETED FILES
   (c) EXPAND DIRECTORIES
   (d) File Carving

10. In Volatility 3, which plugin provides details on DLLs loaded by processes?

(a) dlllist
(b) modules
(c) lsmod
(d) psxview

11. What is the primary purpose of the swap_digger tool in digital forensics?
    (a) To analyze and recover deleted files from the main file system
    (b) To extract potentially sensitive data from Linux swap space
    (c) To create backups of important files
    (d) To identify network anomalies in system memory

12. Which of the following data types is swap_digger most likely to locate within the swap partition?
    (a) Installed software versions
    (b) Network packet captures
    (c) Sensitive information like passwords and encryption keys
    (d) System error logs