Alexander Cannell

CSIS 3700

Professor Barker

Chapter 7: Review Questions

1. What are the five required functions for computer forensics tools?

- Reporting
-Reconstruction
-Acquisition
-Validation
-Extraction
-Discrimination

3. What two data-copying methods are used in software data acquisitions?

c) Logical And Physical

5. Hashing, filtering, and file header analysis make up which function of computer forensics tools?

A)Validation and Discrimination

7. When considering new forensics software, you should do which of the following?

C) Test and Validate the software

8. What are the sub functions of the extraction function?

-Data Viewing
-Keyword Searching
-Decompressing
-Carving
-Decrypting
-Bookmarking

10. Hash values are used for which of the following purposes?

B) Filtering known good files from potentially suspicious data
D)Validating that the original data hasn't changed

11. What's the name of the NIST project established to collect all known hash values for commercial software and OS files?

-National Software Reference Library (NSRL)

15. which of the following is true of most drive imaging tools?

A)They perform the same function as a backup.
B) they ensure that the original drive doesnt become corrupt and damage the digital evidence.
C) They create a copy of the original Drive.

16. The standards for testing forensics tools are based on which criteria?

C)ISO 17025

17. Which of the following tools can examine files created by WINZIP?

A) FTK