Alexander Cannell
11/27/2012
CSIS 3700

Chapter 9 Review:

1. which of the following represents known files you can eliminate from an investigation?

B) Files associated with an application
C) System files the OS uses

2. for which of the following reasons should you wipe a target drive?

D) Both To ensure the quality of the digital evidence you acquire and to make sure unwanted data isnt retained on the drive

3. FTK'S known file filter (KFF) can be used for which of the following purposes?

A) Filter known program files from view
C) Compare hash values of known files to evidence files

8. **Scope creep** happens when an investigation goes beyond the bounds of its original description.

9. Suppose you're investigating an e-mail harassment case. Generally, is collecting evidence for this type of case easier for an internal corporate investigation or a criminal investigation?

C) Internal corporate investigation because corporate investigators typically have ready access to company records

10. You're 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. What might you infer from this information?

B) There's a hidden partition

11. Commercial encryption programs often rely on a technology known as **Key Escrow** to recover files if a password or passphrase is lost.

12. Steganography is used for which of the following purposes?

B) Hiding Data

14. Which of the following statements about HDHOST is true?

A) It can be used to access a suspect's computer remotely
B) It requires installing the DiskExplorer program corresponding to the suspect's file system
D) It works over both serial and TCP/IP interfaces

15. Which of the following tools is most helpful in accessing clusters marked as "bad" on a disk?

A) Norton Disk Edit