Alexander Cannell

10/08/2012

CSIS 3700

Chapter 5 Review:

1. Corporate investigations are typically easier than law enforcement investigations for which of the following reasons?

A. Most companies keep inventory databases of all hardware and software used.

4. As a corporate investigator, you can become an agent of law enforcement when which of the following happens?

A. you begin to take orders from a police detective without a warrant or subpoena.

B. Your internal investigation has concluded, and you have filed a criminal complaint and turned over the evidence to law enforcement.

6. If a suspect computer is located in an area that might have toxic chemicals, you must do which of the following?

A. Coordinate with the hazmat team.

C. Assume the suspect computer is contaminated.

7. what are the three rules for a forensic hash?

-the hash changes with the file

-It can't be predicted

-no files have the same hash

8. In forensic hashes, a collision occurs when _____.

files have the same hash values.

9. list three items that should be in an initial response field kit.

-Camera for photographing the evidence.

-Notebook to take notes on how you retrieve the evidence.

-evidence tags to tag the evidence.

10. when you arrive at the scene, why should you extract only those items you need to acquire evidence?

to prevent evidence destruction, and to keep track of all you evidence supplies at the scene.

12. if a suspect computer is running windows 2000, which of the following can you perform safely?

B. Disconnecting power

14. which of the following techniques might be used in convert surveillance?

A. Key logging

B. Data Sniffing

16. list two hashing algorithms commonly used for forensic purposes.

- Message Digest 5(MD5)

-Secure Hash Algorithm Version 1(SHA-1)