

ECCouncil

312-49V10 Exam

Computer Hacking Forensic Investigator (CHFI-v10)

Questions & Answers

Demo

Version: 5.0

Topic 1, Exam Pool A

Question: 1

When an investigator contacts by telephone the domain administrator or controller listed by a Who is lookup to request all e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?

- A. Title 18, Section 1030
- B. Title 18, Section 2703(d)
- C. Title 18, Section Chapter 90
- D. Title 18, Section 2703(f)

Answer: D

Question: 2

Item 2If you come across a sheepdip machine at your client site, what would you infer?

- A. A sheepdip coordinates several honeypots
- B. A sheepdip computer is another name for a honeypot
- C. A sheepdip computer is used only for virus-checking.
- D. A sheepdip computer defers a denial of service attack

Answer: C

Question: 3

In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?

- A. rules of evidence
- B. law of probability
- C. chain of custody
- D. policy of separation

Answer: C

Question: 4

How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?

- A. 128
- B. 64
- C. 32
- D. 16

Answer: C

Question: 5

You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years.

You navigate to `archive.org` and view the HTML code of `news.com`. You then navigate to the current `news.com` website and copy over the source code. While searching through the code, you come across something abnormal: What have you found?

- A. Web bug
- B. CGI code
- C. Trojan.downloader
- D. Blind bug

Answer: A
