



## **EC-COUNCIL 312-49**

**Exam Name:** *Computer Hacking Forensic Investigator*

**Q & A :** 141 Q&As

***Pdf Demo***

### **Quality and Value for the 312-49 Exam**

[Just4Exams Practice Exams](#) for EC-COUNCIL Certified Ethical Hacker 312-49 are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development.

### **100% Guarantee to Pass Your 312-49 Exam**

If you do not pass the Certified Ethical Hacker 312-49 exam on your first attempt using our Just4Exams **312-49 testing engine and pdf study guide**, we will give you a FULL REFUND of your purchasing fee.

### **Downloadable, Interactive 312-49 Testing engines and PDF Version**

Our Exam Preparation Material provides you everything you will need to take a [Certified Ethical Hacker certification](#) examination. Details are researched and produced by [EC-COUNCIL Certification](#) Experts who are constantly using industry experience to produce precise, and logical.

#### **Free 312-49 Exams:**

***This is demo only, this pdf do not include the questions and answers picture***

Exam : EC-Council 312-49

Title : Computer Hacking Forensic Investigator

1. You are assisting in the investigation of a possible Web Server Hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a porno graphic web site. The company checked the web server and nothing appears wrong. When you type in the IP address of the web site in your browser everything appears normal. What is the name of the attack that affects the DNS cache of the name resolution servers, resulting in those servers directing users to the wrong web site?

- A. ARP Poisoning
- B. DNS Poisoning
- C. HTTP redirect attack

D. IP Spoofing

Answer: B

2. As a CHFI professional, which of the following is the most important to your professional reputation?

A. Your Certifications

B. The correct, successful management of each and every case

C. The fee that you charge

D. The friendship of local law enforcement officers

Answer: B

3. Microsoft Outlook maintains email messages in a proprietary format in what type of file?

A. .email

B. .mail

C. .pst

D. .doc

Answer: C

4. Hackers can gain access to Windows Registry and manipulate user passwords, DNS settings, access rights or others features that they may need in order to accomplish their objectives. One simple method for loading an application at startup is to add an entry (Key) to the following Registry Hive:

A. HKEY\_LOCAL\_MACHINEhardwarewindowsstart

B. HKEY\_LOCAL\_USERSSoftware|MicrosoftoldVersionLoad

C. HKEY\_CURRENT\_USERMicrosoftDefault

D. HKEY\_LOCAL\_MACHINESoftwareMicrosoftCurrentVersionRun

Answer: D

5. In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation.

What assistance can the ISP provide?

A. The ISP can investigate anyone using their service and can provide you with assistance

B. The ISP can investigate computer abuse committed by their employees, but must preserve the privacy of their customers and therefore cannot assist you without a warrant

C. The ISP can't conduct any type of investigations on anyone and therefore can't assist you

D. ISP's never maintain log files so they would be of no use to your investigation

Answer: B

6. The efforts to obtain information before a trial by demanding documents, depositions, questioned and answers written under oath, written requests for admissions of fact and examination of the scene is a description of what legal term?

A. Detection

B. Hearsay

C. Spoliation

D. Discovery

Answer: D

7. The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?

A. Any data not yet flushed to the system will be lost

B. All running processes will be lost

C. The /tmp directory will be flushed

D. Power interruption will corrupt the pagefile

Answer: AB

8. Law enforcement officers are conducting a legal search for which a valid warrant was obtained. While conducting the search, officers observe an item of evidence for an unrelated crime that was not included in the warrant. The item was clearly visible to the officers and immediately identified as evidence. What is the term used to describe how this evidence is admissible?

A. Plain view doctrine

B. Corpus delicti

C. Locard Exchange Principle

D. Ex Parte Order

Answer: A

9. You are a computer forensics investigator working with local police department and you are called to assist in an investigation of threatening emails. The complainant has printer out 27 email messages from the suspect and gives the printouts to you. You inform her that you will need to examine her computer because you need access to the \_\_\_\_\_ in order to track the emails back to the suspect.

- A. Routing Table
- B. Firewall log
- C. Configuration files
- D. Email Header

Answer: D

10. You are working as an independent computer forensics investigator and receive a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a simple backup copy of the hard drive in the PC and put it on this drive and requests that you examine that drive for evidence of the suspected images. You inform him that a simple backup copy will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceedings?

- A. Bit-stream Copy
- B. Robust Copy
- C. Full backup Copy
- D. Incremental Backup Copy

Answer: A

More [312-49 Braindumps](#) Information

**Related 312-49 Exams**

EC0-350    312-49    312-50    EC0-349

**Other EC-COUNCIL Exams**

EC0-479    412-79    EC0-232    EC0-349    EC0-350  
312-50    312-49