



# EC1-349<sup>Q&As</sup>

Computer Hacking Forensic Investigator Exam

**Pass EC-COUNCIL EC1-349 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/ec1-349.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





### QUESTION 1

If you discover a criminal act while investigating a corporate policy abuse, it becomes a public-sector investigation and should be referred to law enforcement?

- A. True
- B. False

Correct Answer: A

---

### QUESTION 2

Jason, a renowned forensic investigator, is investigating a network attack that resulted in the compromise of several systems in a reputed multinational's network. He started Wireshark to capture the network traffic. Upon investigation, he found that the DNS packets travelling across the network belonged to a non-company configured IP. Which of the following attack Jason can infer from his findings?

- A. DNS Poisoning
- B. Cookie Poisoning Attack
- C. DNS Redirection
- D. Session poisoning

Correct Answer: A

---

### QUESTION 3

You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive footprinting against their Web servers. What tool should you use?

- A. Dig
- B. Ping sweep
- C. Netcraft
- D. Nmap

Correct Answer: C

---

### QUESTION 4

When the operating system marks cluster as used, but does not allocate them to any file, such clusters are known as \_\_\_\_\_.



- A. Lost clusters
- B. Bad clusters
- C. Empty clusters
- D. Unused clusters

Correct Answer: A

---

#### QUESTION 5

Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test. The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

- A. False negatives
- B. True negatives
- C. True positives
- D. False positives

Correct Answer: A

[EC1-349 PDF Dumps](#)

[EC1-349 VCE Dumps](#)

[EC1-349 Practice Test](#)