



# 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

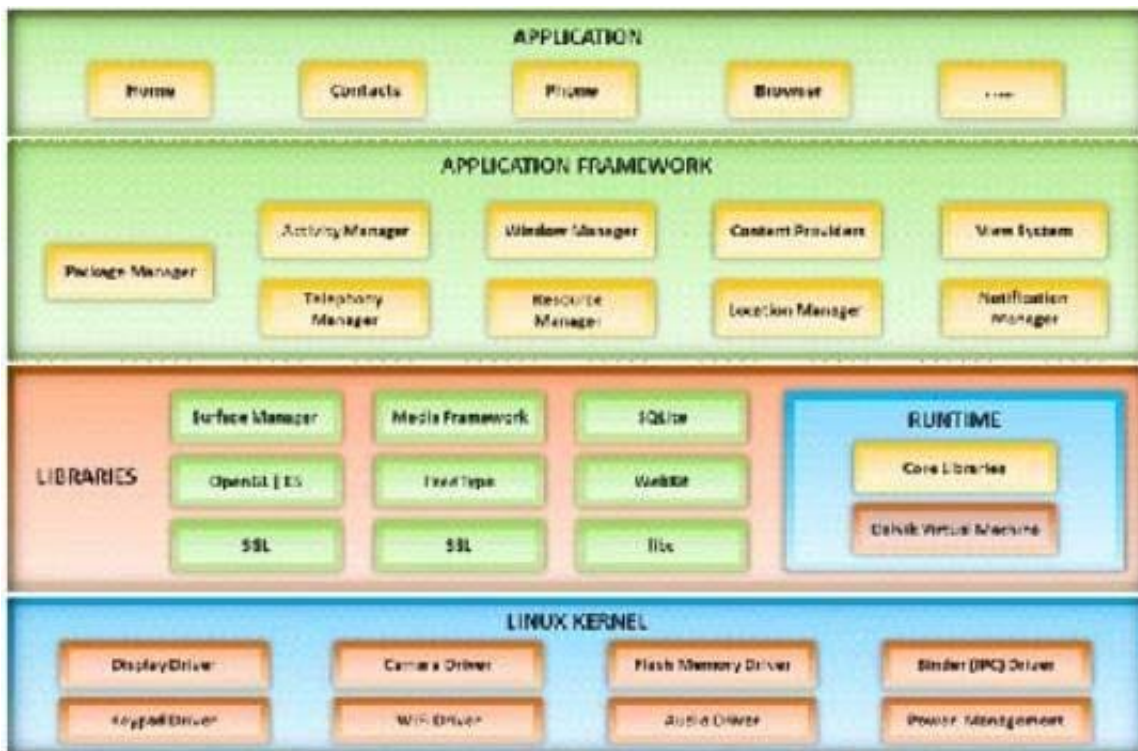
Which of the following statements is incorrect related to acquiring electronic evidence at crime scene?

- A. Sample banners are used to record the system activities when used by the unauthorized user
- B. In warning banners, organizations give clear and unequivocal notice to intruders that by signing onto the system they are expressly consenting to such monitoring
- C. The equipment is seized which is connected to the case, knowing the role of the computer which will indicate what should be taken
- D. At the time of seizing process, you need to shut down the computer immediately

Correct Answer: D

### QUESTION 2

A mobile operating system manages communication between the mobile device and other compatible devices like computers, televisions, or printers.



Which mobile operating system architecture is represented here?

- A. webOS System Architecture
- B. Symbian OS Architecture
- C. Android OS Architecture



D. Windows Phone 7 Architecture

Correct Answer: C

---

### QUESTION 3

Identify the attack from following sequence of actions? Step 1: A user logs in to a trusted site and creates a new session Step 2: The trusted site stores a session identifier for the session in a cookie in the web browser Step 3: The user is tricked to visit a malicious site Step 4: the malicious site sends a request from the user's browser using his session cookie

- A. Web Application Denial-of-Service (DoS) Attack
- B. Cross-Site Scripting (XSS) Attacks
- C. Cross-Site Request Forgery (CSRF) Attack
- D. Hidden Field Manipulation Attack

Correct Answer: C

---

### QUESTION 4

What must an investigator do before disconnecting an iPod from any type of computer?

- A. Unmount the iPod
- B. Mount the iPod
- C. Disjoin the iPod
- D. Join the iPod

Correct Answer: A

---

### QUESTION 5

While looking through the IIS log file of a web server, you find the following entries: What is evident from this log file?

```
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index.asp
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /login.asp?username=if ((select user)='sa' ,
select 1 else select 1/0
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Developments/index_02.jpg
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index_04.jpg
```

- A. Web bugs
- B. Cross site scripting
- C. Hidden fields



D. SQL injection is possible

Correct Answer: D

[Latest EC1-349 Dumps](#)

[EC1-349 Practice Test](#)

[EC1-349 Study Guide](#)