

**Boost up Your Certification Score**

# **EC Council**

## **112-53**

**EC-Council Digital Forensics Essentials (DFE)**



**For More Information – Visit link below:**

**<https://www.examsboost.com/>**

### **Product Version**

- ✓ **Up to Date products, reliable and verified.**
- ✓ **Questions and Answers in PDF Format.**

# Latest Version: 6.0

## Question: 1

Which of the following artifacts can be analyzed in Windows forensics to determine a user's browsing activity? (Select all that apply)

- A. Cache
- B. Cookies
- C. History files
- D. Firewall logs

**Answer: A,B,C**

## Question: 2

Which of the following are considered non-volatile information in Windows forensics? (Select two)

- A. Browser cookies
- B. RAM data
- C. Windows event logs
- D. Running processes

**Answer: A,C**

## Question: 3

What is the significance of identifying the entry point of a malware program during static analysis?

- A. It determines how the malware is activated.
- B. It reveals the malware's uninstallation procedure.
- C. It helps in identifying the software that the malware intends to mimic.
- D. It indicates the malware's compatibility with various operating systems.

**Answer: A**

## Question: 4

Which of the following are common techniques used in dynamic malware analysis? (Select two)

- A. Analyzing registry changes during execution
- B. Disassembling the malware code
- C. Monitoring network activity
- D. Creating a disk image

**Answer: A,C**

### Question: 5

Which of the following is an example of an anti-forensics technique?

- A. File compression
- B. Data obfuscation
- C. Disk defragmentation
- D. Evidence collection

**Answer: B**

### Question: 6

Which of the following are essential components of a forensic readiness policy? (Select two)

- A. A defined process for collecting digital evidence
- B. Immediate public disclosure of all evidence collected
- C. Regular audits of the forensic readiness plan
- D. Immediate destruction of evidence after analysis

**Answer: A,C**

### Question: 7

What role do IoCs play in network forensics?

- A. They provide definitive proof of a network intrusion.
- B. They act as early warning signs of potential security incidents.
- C. They serve as legal evidence in court proceedings.
- D. They are used to optimize network performance.

**Answer: B**

### Question: 8

What is a unique characteristic of the Mac OS booting process compared to Windows and Linux?

- A. Use of BIOS
- B. Use of an entirely graphical interface
- C. Requirement for internet connection
- D. Utilization of EFI instead of a traditional BIOS

**Answer: D**

### Question: 9

In the context of malware forensics, what does network behavior analysis aim to identify?

- A. The best network protocols for efficient data transfer
- B. Malware communication with command and control servers
- C. The optimal network topology for enterprise security
- D. Network components that need upgrading

**Answer: B**

### Question: 10

Which of the following are objectives during the postinvestigation phase? (Select two)

- A. Ensuring all evidence is returned to rightful owners
- B. Updating investigation policies based on recent experiences
- C. Planning the press conference for case disclosure
- D. Archiving all documentation and evidence properly

**Answer: B,D**

# Thank You for Trying Our Product

For More Information – **Visit link below:**

**<https://www.examsboost.com/>**

15 USD Discount Coupon Code:

**G74JA8UF**

## FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**



Visit us at: <https://www.examsboost.com/test/112-53>