



# 212-89<sup>Q&As</sup>

EC-Council Certified Incident Handler

## Pass EC-COUNCIL 212-89 Exam with 100% Guarantee

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

<https://www.geekcert.com/212-89.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

Digital evidence must:

- A. Be Authentic, complete and reliable
- B. Not prove the attackers actions
- C. Be Volatile
- D. Cast doubt on the authenticity and veracity of the evidence

Correct Answer: A

---

#### QUESTION 2

Removing or eliminating the root cause of the incident is called:

- A. Incident Eradication
- B. Incident Protection
- C. Incident Containment
- D. Incident Classification

Correct Answer: A

---

#### QUESTION 3

The individual who recovers, analyzes, and preserves computer and related materials to be presented as evidence in a court of law and identifies the evidence, estimates the potential impact of the malicious activity on the victim, and assesses the intent and identity of the perpetrator is called:

- A. Digital Forensic Examiner
- B. Computer Forensic Investigator
- C. Computer Hacking Forensic Investigator
- D. All the above

Correct Answer: D

---

#### QUESTION 4

Preventing the incident from spreading and limiting the scope of the incident is known as:

- A. Incident Eradication



- B. Incident Protection
- C. Incident Containment
- D. Incident Classification

Correct Answer: C

---

#### QUESTION 5

Insiders may be:

- A. Ignorant employees
- B. Carless administrators
- C. Disgruntled staff members
- D. All the above

Correct Answer: D

[Latest 212-89 Dumps](#)

[212-89 PDF Dumps](#)

[212-89 Exam Questions](#)