



IIO-001

(Certified Information Forensics Investigator)

Total Questions: 229

Last Updated: Nov 23, 2007

Document version: 8.27.11

Thanks for purchasing techXams' Study Guide,

techXams' I10-001 study guide is a comprehensive compilation of questions and answers that have been developed by our team of certified professionals. In order to prepare for the actual exam, all you need is to study the content of this guide. An average of approximately 10 to 20 hours should be spent to study this guide and you will surely pass your exam. It's our guarantee.

Disclaimer

Neither this guide nor any material in this guide is sponsored, endorsed or affiliated with any of the respective vendor. All trademarks are properties of their respective owners.

Guarantee

If you study this guide properly and still unable to pass the exam, please send us a scanned copy of your official score at: refund@techeXams.ws. We will happily reimburse the cost of this study guide or send you an exchange of study guide of your choice free of cost.

Feedback

If you find any possible improvement, then please do let us know. We are always interested in improving the quality of this product. Feedback can be send at: feedback@techeXams.ws

Copyright

techXams holds the copyright of this material. techXams grants you a limited license to view and study this material, either for personal or commercial use. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Question: 1

Firewalls are an excellent source of:

- A. Details of system usage
- B. Details of protocol usage
- C. Forensic Evidence for malicious attacks
- D. Port/service mappings

Answer: C

Question: 2

What technique of layered security design will allow for both investigation and recovery after an incident?

- A. RI Technology
- B. Highly available systems
- C. Overlap design approach
- D. Honeypot placement

Answer: B

Question: 3

If a CIFI violates the ISFA code of Ethics, her CIFI certification can be immediately revoked.

- A. True
- B. False

Answer: B

Question: 4

The 1st amendment allows hackers to exercise free speech by altering content on websites to express opposing viewpoints.

- A. True
- B. False

Answer: B

Question: 5

The term "Browser Artifacts" refer to:

- A. Web browser cache, cookies, favorites, history, auto complete information
- B. Older web browser applications that have little or no security and allow for unchecked use
- C. Older web browser applications that can be used as a surveillance tool for investigators due to their lack of security

2

D. Web browser cookies

Answer: A

Question: 6

All of the following

- A. Internal audit
- B. External audit
- C. Thorough audit
- D. 3rd party audit

Answer: C

Question: 7

In selecting Forensic
standard for authentication

- A. The same for all cases because a record must be maintained
- B. Much more complex than for a crime the
- C. To convert the data into a format presented as evidence
- D. To ensure the data is accurate

of a crime the

does not vary simply
 m.
 of the process.
 language to be
 of evidence collection.

Answer: C

Question: 8

"Interesting data" is

- A. Data relevant to the investigation
- B. Data that is not relevant to the investigation
- C. Data that is not relevant to the investigation
- D. Data that is not relevant to the investigation

Answer: A

Question: 9

Social engineer is legal in the United States, United Kingdom, Japan, France, Germany, Spain, Italy, China, India, South Africa, New Zealand, Singapore, Malaysia, Australia, and Canada as long as the social engineer does not:

- A. Attempt to extract corporate secrets
- B. Lie
- C. Apply the Frye Scenario
- D. Live outside those countries

I10-001 Demo Exam

Question: 10

Drive geometry refers to

- A. The algorithms used to store data
- B. The functional components of a drive
- C. Physical dimensions of the drive
- D. The depth of the drive

Answer: A

Question: 11

Which of the following is not a characteristic of a digital signature?

- A. Cannot be easily forged
- B. Is not time sensitive
- C. Should follow a specific standard
- D. Must be decrypted to be used

Answer: B

Question: 12

Embedding a serial number into a document is called

- A. Hashing
- B. Steganography
- C. Message Digest
- D. Imprinting

Answer: C