

312-49

ECCouncil

Computer Hacking Forensic Investigator

OfficialCerts.com is a reputable IT certification examination guide, study guides and audio exam provider. We ensure that you pass your 312-49 exam in first attempt and also get high scores to acquire ECCouncil certification.

If you use OfficialCerts 312-49 Certification questions and answers, you will experience actual 312-49 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our ECCouncil exam prep covers over 95% of the questions and answers that may be appeared in your 312-49 exam. Every point from pass4sure 312-49 PDF, 312-49 review will help you take ECCouncil 312-49 exam much easier and become ECCouncil certified.

Here's what you can expect from the OfficialCerts ECCouncil 312-49 course:

- * Up-to-Date ECCouncil 312-49 questions as experienced in the real exam.*
- * 100% correct ECCouncil 312-49 answers you simply can't find in other 312-49 courses.*
- * All of our tests are easy to download. Your file will be saved as a 312-49 PDF.*
- * ECCouncil 312-49 brain dump free content featuring the real 312-49 test questions.*

ECCouncil 312-49 certification exam is of core importance both in your Professional life and ECCouncil certification path. With ECCouncil certification you can get a good job easily in the market and get on your path for success. Professionals who passed ECCouncil 312-49 exam training are an absolute favorite in the industry.

You will pass ECCouncil 312-49 certification test and career opportunities will be open for you.

<http://janetdailey.com/?certs=exams.asp?examcode=312-49>



QUESTION: 1

What is the First Step required in preparing a computer for forensics investigation?

- A. Do not turn the computer off or on, run any programs, or attempt to access data on a computer
- B. Secure any relevant media
- C. Suspend automated document destruction and recycling policies that may pertain to any relevant media or users at Issue
- D. Identify the type of data you are seeking, the Information you are looking for, and the urgency level of the examination

Answer: A

QUESTION: 2

Network forensics can be defined as the sniffing, recording, acquisition and analysis of the network traffic and event logs in order to investigate a network security incident.

- A. True
- B. False

Answer: A

QUESTION: 3

Which of the following commands shows you the names of all open shared files on a server and number of file locks on each file?

- A. Net sessions
- B. Net file
- C. Netconfig
- D. Net share

Answer: B

QUESTION: 4

The Recycle Bin exists as a metaphor for throwing files away, but it also allows user to retrieve and restore files. Once the file is moved to the recycle bin, a record is added to the log file that exists in the Recycle Bin. Which of the following files contains records that correspond to each deleted file in the Recycle Bin?

- A. INFO2 file
- B. INFO1 file
- C. LOGINFO2 file
- D. LOGINFO1 file

Answer: A

QUESTION: 5

Email archiving is a systematic approach to save and protect the data contained in emails so that it can be accessed fast at a later date. There are two main archive types, namely Local Archive and Server Storage Archive. Which of the following statements is correct while dealing with local archives?

- A. It is difficult to deal with the webmail as there is no offline archive in most cases. So consult your counsel on the case as to the best way to approach and gain access to the required data on servers
- B. Local archives do not have evidentiary value as the email client may alter the message data
- C. Local archives should be stored together with the server storage archives in order to be admissible in a court of law
- D. Server storage archives are the server information and settings stored on a local system whereas the local archives are the local email client information stored on the mail server

Answer: A

QUESTION: 6

Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages, to go to (instead of the sender's address)?

- A. Errors-To header
- B. Content-Transfer-Encoding header
- C. Mime-Version header
- D. Content-Type header

Answer: A

QUESTION: 7

Which of the following commands shows you all of the network services running on Windows- based servers?

- A. Net start
- B. Net use
- C. Net Session
- D. Net share

Answer: A

QUESTION: 8

Email archiving is a systematic approach to save and protect the data contained in emails so that it can be easily accessed at a later date.

- A. True
- B. False

Answer: A

QUESTION: 9

Which of the following commands shows you the NetBIOS name table each?

OfficialCerts.com Certification Exam Full Version Features;

- Verified answers researched by industry experts.
- Exams **updated** on regular basis.
- Questions, Answers are downloadable in **PDF** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success **Guarantee**.
- **Fast**, helpful support 24x7.

View list of All exams we offer;

<http://www.officialcerts.com/allexams.asp>

To contact our Support;

<http://www.officialcerts.com/support.asp>

View FAQs

<http://www.officialcerts.com/faq.asp>

Download All Exams Samples

<http://www.officialcerts.com/samples.asp>

To purchase Full Version and updated exam;

<http://www.officialcerts.com/allexams.asp>



Shop now using **PayPal**



3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google	

You have made the
Right Choice

You are becoming member of most comprehensive, accurate, highest quality and lowest cost certification resource in the world.

