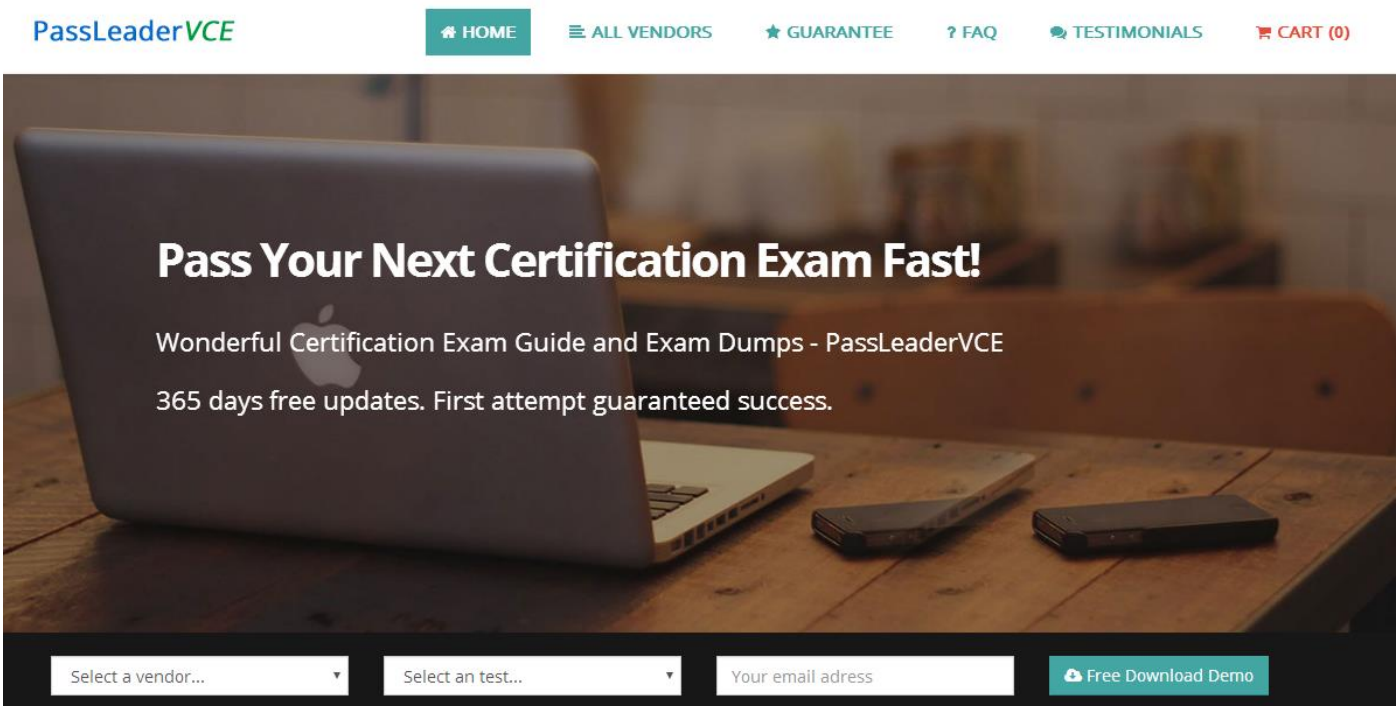
PassleaderVCE



http://www.passleadervce.com/

Wonderful Certification Exam Guide and Exam Dumps- PassLeaderVCE

Exam : **EC1-349**

Title : Computer Hacking Forensic Investigator Exam (EC1-349)

Vendors : EC-COUNCIL

Version : DEMO

NO.1 WPA2 provides enterprise and Wi-Fi users with stronger data protection and network access control which of the following encryption algorithm is used DVWPA2?
A. RC4-CCMP
B. RC4-TKIP
C. AES-CCMP
D. AES-TKIP
Answer: C

NO.2 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

NO.3 Which of the following is not a part of the technical specification of the laboratory-based imaging
system?
A. High performance workstation PC
B. Remote preview and imaging pod
C. Anti-repudiation techniques
D. very low image capture rate
Answer: D

NO.4 Email archiving is a systematic approach to save and protect the data contained in emails so that
it can tie easily accessed at a later date.
A. True
B. False
Answer: A

NO.5 Computer forensics report provides detailed information on complete computer forensics investigation process. It should explain how the incident occurred, provide technical details of the incident and should be clear to understand. Which of the following attributes of a forensics report can render it inadmissible in a court of law?
A. It includes metadata about the incident
B. It includes relevant extracts referred to In the report that support analysis or conclusions
C. It is based on logical assumptions about the incident timeline
D. It maintains a single document style throughout the text
Answer: C

NO.6 Data acquisition system is a combination of tools or processes used to gather, analyze and record

Information about some phenomenon. Different data acquisition system are used depends on the location, speed, cost. etc. Serial communication data acquisition system is used when the actual location of the data is at some distance from the computer. Which of the following communication standard is used in serial communication data acquisition system?
A. RS422
B. RS423
C. RS232
D. RS231
Answer: C

NO.7 Smith, as a part his forensic investigation assignment, has seized a mobile device. He was asked
to recover the Subscriber Identity Module (SIM card) data the mobile device. Smith found that the SIM was protected by a Personal identification Number (PIN) code but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He unsuccessfully tried three PIN numbers that blocked the SIM card. What Jason can do in this scenario to reset the PIN and access SIM data?
A. He should contact the device manufacturer for a Temporary Unlock Code (TUK) to gain access to the SIM
B. He cannot access the SIM data in this scenario as the network operators or device manufacturers have no idea about a device PIN
C. He should again attempt PIN guesses after a time of 24 hours
D. He should ask the network operator for Personal Unlock Number (PUK) to gain access to the SIM
Answer: D

NO.8 When dealing with the powered-off computers at the crime scene, if the computer is switched off,
turn it on
A. True
B. False
Answer: B

NO.9 Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where, “X” represents the _____.
A. Drive name
B. Sequential number
C. Original file name's extension
D. Original file name
Answer: A

NO.10 During the seizure of digital evidence, the suspect can be allowed touch the computer system.
A. True

B. False
Answer: B