Financial Forensic Accounting Qualification

Digital Forensics

Sample Questions and Answers

ISCA Financial Forensic Accounting Qualification – Digital Forensics

Question	Answer	Explanation
1. What does ETL stand for in relation to the data analytics process? a. Educate-Translate-Learn b. Evaluate-Transact-Leverage c. Estimate-Threshold-Limit d. Extract-Transform-Load	d	ETL (Extract, Transform and Load) is a process in data warehousing responsible for pulling data out of the source systems and placing it into a data warehouse.
2. The CEO of a company reported that someone has logged into his laptop, most likely via Remote Desktop. As an investigator, what should you do first? a. Start forensic preservation of the CEO's laptop and arrange for an interview with the CEO to obtain more information b. Use Excel to generate statistics on the logs c. Connect the laptop to the network and perform a network capture to detect anomalous connections. d. None of the above	a	Forensic preservation takes time and should commence after the investigator has confirmed the facts about the incident.
3. Although the Windows operating system removed the EMF file upon a successful print job, the investigator may still recover the file as a result of a search on its unique header information in areas such as unallocated clusters or swap file. a. True b. False	a	Even though Windows will delete the EMF file after a print job has been completed, forensic software may still be used to recover the file by doing a search of its unique header information.

Question	Answer	Explanation
4. You have received a suspicious spoofing email in your inbox, how do you determine if it is a phishing email? a. The email is using SMTP protocol b. The time that you received this email is fishy c. In the email content you are told to deliver a package to someone you have not met d. The email address in the From field is not a legitimate email address	d	Phishing attempts involve the use of a sender's email address that is similar to, but not the same as a company's official email address.
5. Which of the following constitutes post-incident activities? I. Perform a root-cause analysis II. Review the firewall logs for anomalies III. Review the procedures in performing the recovery IV. Perform a rebuild of the application server a. III and IV b. II and III c. I and III d. I and IV	c	A follow up is needed following the recovery of an incident to verify that the incident has been mitigated, the adversary has been removed and additional counter measures are being implemented. This step usually involves a combination of additional monitoring, network/host sweeps looking for new breaches and beach heads, and auditing the network (e.g. Pen Test and Compliance) to ensure that the new security mechanisms are in place and are functioning properly.