WGU Master's Course C702 - Forensics and Network Intrusion

A software company suspects that employees have set up automatic corporate email forwarding to their personal inboxes against company policy. The company hires forensic investigators to identify the employees violating policy, with the intention of issuing warnings to them.

Which type of cybercrime investigation approach is this company taking?

A Civil
B Criminal
C Administrative
D Punitive Correct answer- C

Which model or legislation applies a holistic approach toward any criminal activity as a criminal operation?

A Enterprise Theory of Investigation
B Racketeer Influenced and Corrupt Organizations Act
C Evidence Examination
D Law Enforcement Cyber Incident Reporting Correct answer- A

What does a forensic investigator need to obtain before seizing a computing device in a criminal case?

A Court warrant
B Completed crime report
C Chain of custody document
D Plaintiff's permission Correct answer- A

Which activity should be used to check whether an application has ever been installed on a computer?

A Penetration test
B Risk analysis
C Log review
D Security review Correct answer- C

Which characteristic describes an organization's forensic readiness in the context of cybercrimes?

A It includes moral considerations.
B It includes cost considerations.
C It excludes nontechnical actions.
D It excludes technical actions. Correct answer- B

A cybercrime investigator identifies a Universal Serial Bus (USB) memory stick containing emails as a primary piece of evidence.

Who must sign the chain of custody document once the USB stick is in evidence?

A Those who obtain access to the device
B Anyone who has ever used the device
C Recipients of emails on the device
D Authors of emails on the device Correct answer- A

Which type of attack is a denial-of-service technique that sends a large amount of data to overwhelm system resources?

A Phishing
B Spamming
C Mail bombing
D Bluejacking Correct answer- C

Which computer crime forensics step requires an investigator to duplicate and image the collected digital information?

A Securing evidence
B Acquiring data
C Analyzing data
D Assessing evidence Correct answer- B

What is the last step of a criminal investigation that requires the involvement of a computer forensic investigator?

A Analyzing the data collected
B Testifying in court
C Assessing the evidence
D Performing search and seizure Correct answer- B

How can a forensic investigator verify an Android mobile device is on, without potentially changing the original evidence or interacting with the operating system?

A Check to see if it is plugged into a computer
B Tap the screen multiple times
C Look for flashing lights

D Hold down the power button Correct answer- C

What should a forensic investigator use to protect a mobile device if a Faraday bag is not available?

A Aluminum foil
B Sturdy container
C Cardboard box
D Bubble wrap Correct answer- A

Which criterion determines whether a technology used by government to obtain information in a computer search is considered innovative and requires a search warrant?

A Availability to the general public
B Dependency on third-party software
C Implementation based on open source software
D Use of cloud-based machine learning Correct answer- A

Which situation allows a law enforcement officer to seize a hard drive from a residence without obtaining a search warrant?

A The computer is left unattended.
B The front door is wide open.
C The occupant is acting suspicious.
D The evidence is in imminent danger. Correct answer- D

Which legal document contains a summary of findings and is used to prosecute?

A Investigation report
B Search warrant
C Search and seizure
D Chain of custody Correct answer- A

What should an investigator use to prevent any signals from reaching a mobile phone?

A Faraday bag
B Dry bag
C Anti-static container
D Lock box Correct answer- A

A forensic investigator is called to the stand as a technical witness in an internet payment fraud case.

Which behavior is considered ethical by this investigator while testifying?

A Providing and explaining facts found during the investigation
B Interpreting the findings and offering a clear opinion to the jury
C Helping the jury arrive at a conclusion based on the facts
D Assisting the attorney in compiling a list of essential questions Correct answer- A

A government agent is testifying in a case involving malware on a system.

What should this agent have complied with during search and seizure?

A Fourth Amendment
B Stored Communications Act
C Net Neutrality Bill
D Federal Rules of Evidence Correct answer- A

Which path should a forensic investigator use to look for system logs in a Mac?

A /var/log/cups/access_log
B /var/log/
C /var/audit/
D /var/log/install.log Correct answer- B

Which tool should a forensic investigator use to view information from Linux kernel ring buffers?

A arp
B dmesg
C fsck
D grep Correct answer- B

A forensic investigator makes a bit-stream copy of a Windows hard drive that has been reformatted. The investigator needs to locate only the Adobe PDF files on the hard drive.

Which tool should this investigator use?

A Quick Recovery
B Handy Recovery
C EaseUS Data Recovery
D Stellar Data Recovery Correct answer- C

Which hexadecimal value should an investigator search for to find JPEG images on a device?

A 0x424D
B 0xD0CF11E0A1B11AE1
C 0x504B030414000600