|  |
| --- |
| **Which of the following statements pertaining to First Response is true?** |
| |  | | --- | | First Response is a part of the investigation phase | | First Response is a part of the pre-investigation phase | | First Response is neither a part of pre-investigation phase nor a part of investigation phase. It only involves attending to a crime scene first and taking measures that assist forensic investigators in executing their tasks in the investigation phase more efficiently | | First Response is a part of the post-investigation phase | |

|  |
| --- |
| **A breach resulted from a malware attack that evaded detection and compromised the machine memory without installing any software or accessing the hard drive. What technique did the adversaries use to deliver the attack?** |
| |  | | --- | | Trojan | | JavaScript | | Fileless | | Spyware | |

|  |
| --- |
| **Rule 1002 of Federal Rules of Evidence (US) talks about \_\_\_\_\_\_** |
| |  | | --- | | Admissibility of duplicates | | Admissibility of other evidence of contents | | **Requirement of original** | | Admissibility of original | |

|  |
| --- |
| **In which IoT attack does the attacker use multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks?** |
| |  | | --- | | **Sybil attack** | | Replay attack | | Jamming attack | | Blueborne attack | |

|  |
| --- |
| **Maria has executed a suspicious executable file in a controlled environment and wants to see if the file adds/modifies any registry value after execution via Windows Event Viewer. Which of the following event ID should she look for in this scenario?** |
| |  | | --- | | **Event ID 4657** | | Event ID 4624 | | Event ID 7040 | | Event ID 4688 | |

|  |
| --- |
| **Which of the following statements is true with respect to SSDs (solid-state drives)?** |
| |  | | --- | | **Faster data access, lower power usage, and higher reliability are some of the major advantages of SSDs over HDDs** | | Like HDDs, SSDs also have moving parts | | SSDs contain tracks, clusters, and sectors to store data | | SSDs cannot store non-volatile data | |

|  |
| --- |
| **Which of the following is a requirement for senders as per the CAN-SPAM act?** |
| |  | | --- | | Senders should never share their physical postal address in the email | | **Senders cannot use misleading or false header information** | | Emails must not contain information regarding how to stop receiving emails from the sender in future | | Senders must use deceptive subject lines | |

|  |
| --- |
| **An investigator seized a notebook device installed with a Microsoft Windows OS. Which type of files would support an investigation of the data size and structure in the device?** |
| |  | | --- | | HFS and GNUC | | Ext2 and Ext4 | | **NTFS and FAT** | | APFS and HFS | |

|  |
| --- |
| **What is the extension used by Windows OS for shortcut files present on the machine?** |
| |  | | --- | | .pf | | .log | | .dat | | .**lnk** | |

|  |
| --- |
| **During a forensic investigation, a large number of files were collected. The investigator needs to evaluate ownership and accountability of those files. Therefore, he begins to identify attributes such as "author name,” "organization name,” "network name,” or any additional supporting data that is meant for the owner's identification purpose. Which term describes these attributes?** |
| |  | | --- | | Data index | | **Metadata** | | Data header | | Metabase | |

|  |
| --- |
| **Frank, a cloud administrator in his company, needs to take backup of the OS disks of two Azure VMs that store business-critical data. Which type of Azure blob storage can he use for this purpose?** |
| |  | | --- | | Append blob | | Block blob | | **Page blob** | | Medium blob | |

|  |
| --- |
| **A file requires 10 KB space to be saved on a hard disk partition. An entire cluster of 32 KB has been allocated for this file. The remaining, unused space of 22 KB on this cluster will be identified as \_\_\_\_\_\_\_\_.** |
| |  | | --- | | Swap space | | Cluster space | | Sector space | | **Slack space** | |

|  |
| --- |
| **In Java, when multiple applications are launched, multiple Dalvik Virtual Machine instances occur that consume memory and time. To avoid that, Android implements a process that enables low memory consumption and quick start-up time. What is the process called?** |
| |  | | --- | | **Zygote** | | Media server | | Daemon | | Init | |

|  |
| --- |
| **A clothing company has recently deployed a website on its latest product line to increase its conversion rate and base of customers. Andrew, the network administrator recently appointed by the company, has been assigned with the task of protecting the website from intrusion and vulnerabilities. Which of the following tool should Andrew consider deploying in this scenario?** |
| |  | | --- | | Kon-Boot | | CryptaPix | | **ModSecurity** | | Recuva | |

|  |
| --- |
| **During an investigation, Noel found a SIM card from the suspect's mobile. The ICCID on the card is 8944245252001451548. What does the first four digits (89 and 44) in the ICCID represent?** |
| |  | | --- | | TAC and industry identifier | | Issuer identifier number and TAC | | Country code and industry identifier | | **Industry identifier and country code** | |

|  |
| --- |
| **Jack is reviewing file headers to verify the file format and hopefully find more information of the file. After a careful review of the data chunks through a hex editor; Jack finds the binary value 0xffd8ff. Based on the above information, what type of format is the file/image saved as?** |
| |  | | --- | | ASCII | | **JPEG** | | BMP | | GIF | |

|  |
| --- |
| **While collecting active transaction logs using SQL Server Management Studio, the query Select \* from ::fn\_dblog(NULL, NULL) displays the active portion of the transaction log file. Here, what does assigning NULL values imply?** |
| |  | | --- | | Start and end points for log files are not specified | | Start and end points for log sequence numbers are zero | | Start and end points for log files are zero | | **Start and end points for log sequence numbers are not specified** | |

|  |
| --- |
| **Which of the following Windows event logs record events related to device drives and hardware changes?** |
| |  | | --- | | Forwarded events log | | **System log** | | Security log | | Application log | |

|  |
| --- |
| **Malware analysis can be conducted in various manners. An investigator gathers a suspicious executable file and uploads it to VirusTotal in order to confirm whether the file is malicious, provide information about its functionality, and provide information that will allow to produce simple network signatures. What type of malware analysis was performed here?** |
| |  | | --- | | Hybrid | | Volatile | | Static | | **Dynamic** | |

|  |
| --- |
| **An investigator is checking a Cisco firewall log that reads as follows: Aug 21 2019 09:16:44: %ASA-1-106021: Deny ICMP reverse path check from 10.0.0.44 to 10.0.0.33 on interface outside  What does %ASA-1-106021 denote?** |
| |  | | --- | | Type of request | | Type of traffic | | Firewall action | | ***Mnemonic message*** | |

|  |
| --- |
| **A forensic examiner encounters a computer with a failed OS installation and the master boot record (MBR) or partition sector damaged. Which of the following tools can find and restore files and information in the disk?** |
| |  | | --- | | NetCat | | R-Studio | | **Helix** | | Wireshark | |

|  |
| --- |
| **Which set of anti-forensic tools/techniques allows a program to compress and/or encrypt an executable file to hide attack tools from being detected by reverse-engineering or scanning?** |
| |  | | --- | | Botnets | | **Packers** | | Emulators | | Password crackers | |

|  |
| --- |
| **According to RFC 3227, which of the following is considered as the most volatile item on a typical system?** |
| |  | | --- | | Archival media | | Temporary system files | | **Registers and cache** | | Kernel statistics and memory | |

|  |
| --- |
| **Which Federal Rule of Evidence speaks about the Hearsay exception where the availability of the declarant is immaterial and certain characteristics of the declarant such as present sense impression, excited utterance, and recorded recollection are also observed while giving their testimony?** |
| |  | | --- | | **Rule 803** | | Rule 804 | | Rule 801 | | Rule 802 | |

|  |
| --- |
| **A call detail record (CDR) provides metadata about calls made over a phone service. From the following data fields, which one is not contained in a CDR.** |
| |  | | --- | | Phone number receiving the call | | **The language of the call** | | A unique sequence number identifying the record | | The call duration | |

|  |
| --- |
| **Cybercriminals sometimes use compromised computers to commit other crimes, which may involve using computers or networks to spread malware or illegal information. Which type of cybercrime stops users from using a device or network, or prevents a company from providing a software service to its customers?** |
| |  | | --- | | Malware attack | | Ransomware attack | | **Denial-of-Service (DoS) attack** | | Phishing | |

|  |
| --- |
| **A computer forensics investigator or forensic analyst is a specially trained professional who works with law enforcement as well as private businesses to retrieve information from computers and other types of data storage devices. For this, the analyst should have an excellent working knowledge of all aspects of the computer. Which of the following is not a duty of the analyst during a criminal investigation?** |
| |  | | --- | | To fill the chain of custody | | ***To enforce the security of all devices and software in the scene*** | | To recover data from suspect devices | | To dismantle and rebuild the system when the data is damaged | |

|  |
| --- |
| **Adam is thinking of establishing a hospital in the US and approaches John, a software developer to build a site and host it for him on one of the servers, which would be used to store patient health records. He has learned from his legal advisors that he needs to have the server’s log data reviewed and managed according to certain standards and regulations. Which of the following regulations are the legal advisors referring to?** |
| |  | | --- | | Electronic Communications Privacy Act | | Data Protection Act of 2018 | | **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** | | Payment Card Industry Data Security Standard (PCI DSS) | |

|  |
| --- |
| **Data is striped at a byte level across multiple drives, and parity information is distributed among all member drives. What RAID level is represented here?** |
| |  | | --- | | RAID Level 5 | | RAID Level 1 | | **RAID Level 3** | | RAID Level 0 | |
| **Brian has the job of analyzing malware for a software security company. Brian has setup a virtual environment that includes virtual machines running various versions of OSes. Additionally, Brian has setup separated virtual networks within this environment. The virtual environment does not connect to the company’s intranet nor does it connect to the external Internet. With everything setup, Brian now received an executable file from client that has undergone a cyberattack. Brian ran the executable file in the virtual environment to see what it would do. What type of analysis did Brian perform?** |
| |  | | --- | | Static malware analysis | | Status malware analysis | | **Dynamic malware analysis** | | Static OS analysis | |

|  |
| --- |
| **Data density of a disk drive is calculated by using \_\_\_\_\_\_\_\_\_\_** |
| |  | | --- | | Track density, areal density, and slack density. | | **Track density, areal density, and bit density**. | | Track space, bit area, and slack space. | | Slack space, bit density, and slack density. | |

|  |
| --- |
| **Which of the following directory contains the binary files or executables required for system maintenance and administrative tasks on a Linux system?** |
| |  | | --- | | /sbin | | /usr | | /lib | | /bin | |

|  |
| --- |
| **Williamson is a forensic investigator. While investigating a case of data breach at a company, he is maintaining a document that records details such as the forensic processes applied on the collected evidence, particulars of people handling it, the dates and times when it is being handled, and the place of storage of the evidence. What do you call this document?** |
| |  | | --- | | **Chain of custody** | | Log book | | Authorization form | | Consent form | |

|  |
| --- |
| **You are a forensic investigator who is analyzing a hard drive that was recently collected as evidence. You have been unsuccessful at locating any meaningful evidence within the file system and suspect a drive wiping utility may have been used. You have reviewed the keys within the software hive of the Windows registry and did not find any drive wiping utilities. How can you verify that drive wiping software was used on the hard drive?** |
| |  | | --- | | Load various drive wiping utilities offline, and export previous run reports | | ***Check the list of installed programs*** | | Document in your report that you suspect a drive wiping utility was used, but no evidence was found | | Look for distinct repeating patterns on the hard drive at the bit level | |

|  |
| --- |
| **“No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court” – this principle is advocated by which of the following?** |
| |  | | --- | | **The Association of Chief Police Officers (ACPO) Principles of Digital Evidence** | | Scientific Working Group on Imaging Technology (SWGIT) | | Locard’s exchange principle | | FBI Cyber Division | |

|  |
| --- |
| **What command-line tool enables forensic investigator to establish communication between an Android device and a forensic workstation in order to perform data acquisition from the device?** |
| |  | | --- | | APK Analyzer | | Xcode | | SDK Manager | | **Android Debug Bridge** | |

|  |
| --- |
| **You are the incident response manager at a regional bank. While performing routine auditing of web application logs, you find several attempted login submissions that contain the following strings:**  **< SCRIPT type="text/javascript" > var adr = '../evil.php?cakemonster=' + escape(document.cookie); < /SCRIPT >**  **What kind of attack has occurred?** |
| |  | | --- | | Cross-site request forgery | | Buffer overflow | | Cross-site scripting | | SQL injection | |

|  |
| --- |
| **To understand the impact of a malicious program after the booting process and to collect recent information from the disk partition, an investigator should evaluate the content of the:** |
| |  | | --- | | UEFI | | MBR | | GRUB | | BIOS | |

|  |
| --- |
| **Place the following in order of volatility from most volatile to the least volatile.** |
| |  | | --- | | Register and cache, temporary file systems, routing tables, disk storage, archival media | | **Registers and cache, routing tables, temporary file systems, disk storage, archival media** | | Registers and cache, routing tables, temporary file systems, archival media, disk storage | | Archival media, temporary file systems, disk storage, archival media, register and cache | |

|  |
| --- |
| **Steve thought it would be funny to make some changes on Tom’s computer at their office. Steve went into the Microsoft Windows registry and changed the keyboard mapping configuration on Tom’s computer. Now Tom is unable to log into his computer because of the changes. Could Steve’s actions warrant a cybercrime investigation?** |
| |  | | --- | | No, because this scenario describes a corporate investigation | | No, because there is no company policy that prohibits computer pranks on co-workers | | **Yes, because modifying computer software is always treated as a federal offense** | | Yes, because Steve performed a denial-of-service attack on Tom’s computer | |

|  |
| --- |
| **Which of the following attacks refers to unintentional download of malicious software via the Internet? Here, an attacker exploits flaws in browser software to install malware merely by the user visiting the malicious website.** |
| |  | | --- | | Internet relay chats | | **Drive-by downloads** | | Malvertising | | Phishing | |

|  |
| --- |
| **An investigator is examining a file to identify any potentially malicious content. To avoid code execution and still be able to uncover hidden indicators of compromise (IOC), which type of examination should the investigator perform:** |
| |  | | --- | | Dynamic analysis | | Threat analysis | | Threat hunting | | **Static analysis** | |

|  |
| --- |
| **SO/IEC 17025 is an accreditation for which of the following:** |
| |  | | --- | | Encryption | | Chain of custody | | CHFI issuing agency | | **Forensics lab licensing** | |

|  |
| --- |
| **Consider a scenario where a forensic investigator is performing malware analysis on a memory dump acquired from a victim’s computer. The investigator uses Volatility Framework to analyze RAM contents; which plugin helps investigator to identify hidden processes or injected code/DLL in the memory dump?** |
| |  | | --- | | malscan | | pslist | | mallist | | **malfind** | |

|  |
| --- |
| **Harry has collected a suspicious executable file from an infected system and seeks to reverse its machine code to instructions written in assembly language. Which tool should he use for this purpose?** |
| |  | | --- | | **Ollydbg** | | HashCalc | | oledump | | BinText | |

|  |
| --- |
| **Sally accessed the computer system that holds trade secrets of the company where she is employed. She knows she accessed it without authorization and all access (authorized and unauthorized) to this computer is monitored.To cover her tracks, Sally deleted the log entries on this computer. What among the following best describes her action?** |
| |  | | --- | | Network intrusion | | Brute-force attack | | Password sniffing | | **Anti-forensics** | |

|  |
| --- |
| **Matthew has been assigned the task of analyzing a suspicious MS Office document via static analysis over an Ubuntu-based forensic machine. He wants to see what type of document it is, whether it is encrypted, or contains any flash objects/VBA macros. Which of the following python-based script should he run to get relevant information?** |
| |  | | --- | | oleid.py | | oleform.py | | oledir.py | | **pdfid.py** | |

|  |
| --- |
| **Simona has written a regular expression for the detection of web application-specific attack attempt that reads as /((\%3C)|<)((\%2F)|\/)\*[a-z0-9\%]+((\%3E)|>)/ix. Which of the following does the part ((\%3E)|>) look for?** |
| |  | | --- | | Opening angle bracket or its hex equivalent | | Alphanumeric string or its hex equivalent | | **Closing angle bracket or its hex equivalent** | | Forward slash for a closing tag or its hex equivalent | |

|  |
| --- |
| **Tony, an email marketing professional, is accused of enticing people to reveal their personal information such as banking credentials, credit card details, bank balance, etc., via phishing emails. What type of investigation will apply to Tony’s case?** |
| |  | | --- | | Administrative | | None of these | | **Criminal** | | Civil | |

|  |
| --- |
| **When investigating a system, the forensics analyst discovers that malicious scripts were injected into benign and trusted websites. The attacker used a web application to send malicious code, in the form of a browser side script, to a different end-user. What attack was performed here?** |
| |  | | --- | | **Cross-site scripting attack** | | Brute-force attack | | SQL injection attack | | Cookie poisoning attack | |

|  |
| --- |
| **Which of these Windows utility help you to repair logical file system errors?** |
| |  | | --- | | Disk cleanup | | Resource Monitor | | Disk defragmenter | | **CHKDSK** | |

|  |
| --- |
| **You are a digital forensic investigator at a large pharmaceutical company. You are responding to a security incident where you have found a computer on the scene, and you believe the computer contains evidence that is valuable to the case. The computer is running, but the screen is blank. What should you do first?** |
| |  | | --- | | **Move the mouse slightly to wake the computer up** | | Unplug the computer | | Gather the appropriate report forms, pens, and memory capture tools | | Press a single key on the keyboard, and document which key was pressed | |

|  |
| --- |
| **Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?** |
| |  | | --- | | Surface Manager | | **OpenGL/ES and SGL** | | WebKit | | Media framework | |

|  |
| --- |
| **Storage location of Recycle Bin for NTFS file systems (Windows Vista and later) is located at:** |
| |  | | --- | | Drive:\REYCLED | | Drive:\RECYCLE.BIN | | **Drive:\$Recycle.Bin** | | Drive:\RECYCLER | |

|  |
| --- |
| **Before accessing digital evidence from victims, witnesses, or suspects, on their electronic devices, what should the investigator do first to respect legal privacy requirements?** |
| |  | | --- | | Remove the battery or turn-off the device | | Notify the fact to the local authority or employer | | Protect the device against external communication | | **Obtain a formal written consent to search** | |

|  |
| --- |
| **Cloud forensic investigations impose challenges related to multi-jurisdiction and multi-tenancy aspects. To have a better understanding of the roles and responsibilities between the cloud service provider (CSP) and the client, which document should the forensic investigator review?** |
| |  | | --- | | Service level agreement | | Service level management | | National and local regulation | | Key performance indicator | |

|  |
| --- |
| **William is examining a log entry that reads 192.168.0.1 - - [18/Jan/2020:12:42:29 +0000] "GET / HTTP/1.1" 200 1861. Which of the following logs does the log entry belong to?** |
| |  | | --- | | The combined log format of Apache access log | | IIS log | | Apache error log | | ***The common log format of Apache access log*** | |

|  |
| --- |
| **Fill in the missing Master Boot Record component. 1. Master boot code 2. Partition table 3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| |  | | --- | | **Disk signature** | | Boot loader | | Signature word | | Volume boot record | |

|  |
| --- |
| **This is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted. Which among the following is suitable for the above statement?** |
| |  | | --- | | **Hearsay rule** | | Rule 1001 | | Limited admissibility | | Testimony by the accused | |

|  |
| --- |
| **After a successful data exfiltration attack against your organization, you are conducting an internal investigation and suspect a significant portion of evidence exists on an end-user’s personal laptop. You want to be sure not to tip-off the laptop’s owner that an investigation is being conducted. What is the best option to obtain the evidence?** |
| |  | | --- | | Request the laptop owner to voluntarily surrender it | | **Obtain a search warrant** | | Confiscate the laptop | | Obtain a subpoena | |

|  |
| --- |
| **Recently, an internal web app that a government agency utilizes has become unresponsive. Betty, a network engineer for the government agency, has been tasked to determine the cause of the web application’s unresponsiveness. Betty launches Wireshark and begins capturing the traffic on the local network. While analyzing the results, Betty noticed that a syn flood attack was underway. How did Betty know a syn flood attack was occurring?** |
| |  | | --- | | Wireshark capture does not show anything unusual and the issue is related to the web application | | Wireshark capture shows multiple ACK requests and SYN responses from single/multiple IP address(es) | | **Wireshark capture shows multiple SYN requests and ACK responses from single/multiple IP address(es)** | | Wireshark capture shows multiple SYN requests and RST responses from single/multiple IP address(es) | |

|  |
| --- |
| **Choose the layer in iOS architecture that provides frameworks for iOS app development?** |
| |  | | --- | | Media services | | Core OS | | **Cocoa Touch** | | Core services | |

|  |
| --- |
| **Mark works for a government agency as a cyber-forensic investigator. He has been given the task of restoring data from a hard drive. The partition of the hard drive was deleted by a disgruntled employee in order to hide their nefarious actions. What tool should Mark use to restore the data?** |
| |  | | --- | | Diskmon | | EFSDump | | R-Studio | | Diskview | |

|  |
| --- |
| **Which of the following tools is used to dump the memory of a running process, either immediately or when an error condition occurs?** |
| |  | | --- | | **Belkasoft Live RAM Capturer** | | FATKit | | CacheInf | | Coreography | |

|  |
| --- |
| **Which of the following methods of mobile device data acquisition captures all the data present on the device, as well as all deleted data and access to unallocated space?** |
| |  | | --- | | Manual acquisition | | Logical acquisition | | Direct acquisition | | Physical acquisition | |

|  |
| --- |
| **Ronald, a forensic investigator, has been hired by a financial services organization to investigate an attack on their MySQL database server, which is hosted on a Windows machine named WIN-DTRAI83202X. Ronald wants to retrieve information on the changes that have been made to the database. Which of the following files should Ronald examine for this task?** |
| |  | | --- | | WIN-DTRAI83202X-bin.nnnnnn | | relay-log.info | | WIN-DTRAI83202Xslow.log | | WIN-DTRAI83202Xrelay-bin.index | |

|  |
| --- |
| **At a trading organization, three employees received email from a senior official at ABC bank asking them to urgently fill customer-specific details at the bank's website. As the organization already has a partnership with the bank, all the employees visited the website and updated customer-related information, such as their bank account details, confidential documents, and credit card information. After a day, all the concerned customers complained that large amount of money has been spent using their credit cards and they cannot log into their bank accounts. What kind of attack is this?** |
| |  | | --- | | Whaling | | Mail bombing | | **Spear phishing** | | Email spamming | |

|  |
| --- |
| **In forensics, \_\_\_\_\_\_\_\_\_ are used to view stored or deleted data from both files and disk sectors.** |
| |  | | --- | | Hash algorithms | | SIEM tools | | Host interfaces | | **Hex editors** | |

|  |
| --- |
| **In forensics, \_\_\_\_\_\_\_\_\_ are used to view stored or deleted data from both files and disk sectors.** |
| |  | | --- | | Hash algorithms | | SIEM tools | | Host interfaces | | Hex editors | |

|  |
| --- |
| **Which of the following applications will allow a forensic investigator to track the user login sessions and user transactions that have occurred on an MS SQL Server?** |
| |  | | --- | | Notepad++ | | **ApexSQL Audit** | | Event Log Explorer | | netcat | |

|  |
| --- |
| **An investigator needs to perform data acquisition from a storage media without altering its contents to maintain the integrity of the content. The approach adopted by the investigator relies upon the capacity of enabling read-only access to the storage media. Which tool should the investigator integrate into his/her procedures to accomplish this task?** |
| |  | | --- | | **Write block**er | | Backup tool | | Data duplication tool | | BitLocker | |

|  |
| --- |
| **Assume there is a file named myfile.txt in C: drive that contains hidden data streams. Which of the following commands would you issue to display the contents of a data stream?** |
| |  | | --- | | C:\MORE < myfile.txt:stream1 | | **C:\>ECHO text\_message > myfile.txt:stream1** | | echo text > program:source\_file | | myfile.dat:stream1 | |

|  |
| --- |
| **Which of the following is considered as the starting point of a database and stores user data and database objects in an MS SQL server?** |
| |  | | --- | | ibdata1 | | Transaction log data files (LDF) | | **Primary data files (MDF)** | | Application data files (ADF) | |

|  |
| --- |
| **You are an information security analyst for a national retain chain. The organization has a web server which provides customer reports to internal users for marketing purposes. You are analyzing IIS logs on the web server and find the following log entry:  #Software: Microsoft Internet Information Services 7.5 #Version 1.0 #Date 2020-04-28 11:50:54 #Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) sc-status sc-substatus sc-win32-status time-taken 2020-04-28 11:50:54 192.168.1.39 GET /Data/Files/customer\_report.xlsx 80 - 192.168.1.200/Mozilla/5.0+(Macintosh;+Intel+Mac+OS+X+10\_7\_2) +AppleWebKit/535.51.22+(KHTML,+like+Gecko)+Version/5.1.1 +Safari/534.51.22 200 0 0 54  Based on the contents of this log entry, what occurred?** |
| |  | | --- | | A user at IP address 192.168.1.200 requested the customer\_report.xlsx file and the web server at IP address 192.168.1.39 processed the request | | A user at IP address 192.168.1.39 requested the customer\_report.xlsx file and the web server at IP address 192.168.1.200 failed to process the request | | A user at IP address 192.168.1.200 requested the customer\_report.xlsx file and the web server at IP address 192.168.1.39 failed to process the request | | **A user at IP address 192.168.1.39 requested the customer\_report.xlsx file and the web server at IP address 192.168.1.200 processed the request** | |

|  |
| --- |
| **Jacob, a cybercrime investigator, joined a forensics team to participate in a criminal case involving digital evidence. After the investigator collected all the evidence and presents it to the court, the judge dropped the case and the defense attorney pressed charges against Jacob and the rest of the forensics team for unlawful search and seizure. What forensics privacy issue was not addressed prior to collecting the evidence?** |
| |  | | --- | | None of these | | Compliance with the Third Amendment of the U.S. Constitution | | **Compliance with the Fourth Amendment of the U.S. Constitution** | | Compliance with the Second Amendment of the U.S. Constitution | |

|  |
| --- |
| **The working of the Tor browser is based on which of the following concepts?** |
| |  | | --- | | Both static and default routing | | Default routing | | Static routing | | **Onion routing** | |

|  |
| --- |
| **Which of the following malware targets Android mobile devices and installs a backdoor that remotely installs applications from an attacker-controlled server?** |
| |  | | --- | | XcodeGhost | | Felix | | **xHelper** | | Unflod | |

|  |
| --- |
| **Edgar is part of the FBI’s forensic media and malware analysis team; he is analyzing a current malware and is conducting a thorough examination of the suspect system, network, and other connected devices. Edgar’s approach is to execute the malware code to know how it interacts with the host system and its impacts on it. He is also using a virtual machine and a sandbox environment.**  **What type of malware analysis is Edgar performing?** |
| |  | | --- | | Static analysis | | Malware disassembly | | VirusTotal analysis | | **Dynamic malware analysis/behavioral analysis** | |

|  |
| --- |
| **Which of the following is the most effective tool for acquiring volatile data from a Windows-based system?** |
| |  | | --- | | Ethereal | | **Helix** **Live** | | Coreography | | Datagrab | |

|  |
| --- |
| **On NTFS file system, which of the following tools can a forensic investigator use in order to identify timestomping of evidence files?** |
| |  | | --- | | analyzeMFT | | Exiv2 | | wbStego | | **Timestomp** | |

|  |
| --- |
| **Which of the following registry components (cells) contains registry key information and includes offsets to other cells as well as the LastWrite time for the key?** |
| |  | | --- | | **Key cell** | | Security descriptor cell | | Value cell | | Value list cell | |

|  |
| --- |
| **Fred, a cybercrime investigator for the FBI, finished storing a solid-state drive in a static resistant bag and filled out the chain of custody form. Two days later, John grabbed the solid-state drive and created a clone of it (with write blockers enabled) in order to investigate the drive. He did not document the chain of custody though. When John was finished, he put the solid-state drive back in the static resistant and placed it back in the evidence locker. A day later, the court trial began and upon presenting the evidence and the supporting documents, the chief justice outright rejected them. Which of the following statements strongly support the reason for rejecting the evidence?** |
| |  | | --- | | Write blockers were used while cloning the evidence | | Block clones cannot be created with solid-state drives | | John investigated the clone instead of the original evidence itself | | **John did not document the chain of custody** | |

|  |
| --- |
| **Which following forensic tool allows investigator to detect and extract hidden streams on NTFS drive?** |
| |  | | --- | | analyzeMFT | | **Stream Detector** | | TimeStomp | | Autopsy | |

|  |
| --- |
| **A forensic analyst has been tasked with investigating unusual network activity inside a retail company’s network. Employees complain of not being able to access services, frequent rebooting, and anomalies in log files. The investigator requested log files from the IT administrator and after carefully reviewing them, he finds the following log entry:**  **https://www.eccexam.com/DOCS/uzx6wQF2Um7b/Tests/YuDtUpdhk7tT/Q9.JPG**  **What type of attack was performed on the companies’ web application?** |
| |  | | --- | | Directory transversal | | **SQL injection** | | Unvalidated input | | Log tampering | |

|  |
| --- |
| **A cybercriminal is attempting to remove evidence from a Windows computer. He deletes the file evidence1.doc, sending it to Windows Recycle Bin. The cybercriminal then empties the Recycle Bin. After having been removed from the Recycle Bin, what will happen to the data?** |
| |  | | --- | | ***The data will be moved to new clusters in unallocated space*** | | The data will remain in its original clusters until it is overwritten | | The data will become corrupted, making it unrecoverable | | The data will be overwritten with zeroes | |

|  |
| --- |
| **Which layer in the IoT architecture is comprised of hardware parts such as sensors, RFID tags, and devices that play an important role in data collection?** |
| |  | | --- | | Application layer | | **Edge technology layer** | | Middleware layer | | Access gateway layer | |

|  |
| --- |
| **Jeff is a forensics investigator for a government agency’s cyber security office. Jeff is tasked with acquiring a memory dump of a Windows 10 computer that was involved in a DDoS attack on the government agency’s web application. Jeff is onsite to collect the memory. What tool could Jeff use?** |
| |  | | --- | | RAMMapper | | Memcheck | | Volatility | | ***Autopsy*** | |

|  |
| --- |
| **Chloe is a forensic examiner who is currently cracking hashed passwords for a crucial mission and hopefully solve the case. She is using a lookup table used for recovering a plain text password from cipher text; it contains word list and brute-force list along with their computed hash values. Chloe is also using a graphical generator that supports SHA1. a. What password technique is being used? b. What tool is Chloe using?** |
| |  | | --- | | **a. Rainbow Tables b. Winrtgen** | | a. Cain & Able b. Rten | | a. Brute-force b. MScache | | a. Dictionary attack b. Cisco PIX | |

|  |
| --- |
| **The information security manager at a national legal firm has received several alerts from the intrusion detection system that a known attack signature was detected against the organization’s file server. What should the information security manager do first?** |
| |  | | --- | | Disconnect the file server from the network | | Manually investigate to verify that an incident has occurred | | Report the incident to senior management | | Update the anti-virus definitions on the file server | |

|  |
| --- |
| **Which “Standards and Criteria” under SWDGE states that “the agency must use hardware and software that are appropriate and effective for the seizure or examination procedure”?** |
| |  | | --- | | Standards and Criteria 1.7 | | **Standards and Criteria 1.5** | | Standards and Criteria 1.6 | | Standards and Criteria 1.4 | |

|  |
| --- |
| **For the purpose of preserving the evidentiary chain of custody, which of the following labels is not appropriate?** |
| |  | | --- | | ***Relevant circumstances surrounding the collection*** | | General description of the evidence | | SSN of the person collecting the evidence | | Exact location the evidence was collected from | |

|  |
| --- |
| **Web browsers can store relevant information from user activities. Forensic investigators may retrieve files, lists, access history, cookies, among other digital footprints. Which tool can contribute to this task?** |
| |  | | --- | | Most Recently Used (MRU) list | | Task Manager | | Google Chrome Recovery Utility | | MZCacheView | |

|  |
| --- |
| **Donald made an OS disk snapshot of a compromised Azure VM under a resource group being used by the affected company as a part of forensic analysis process. He then created a vhd file out of the snapshot and stored it in a file share and as a page blob as backup in a storage account under different region. What is the next thing he should do as a security measure?** |
| |  | | --- | | Create another VM by using the snapshot | | Delete the snapshot from the source resource group | | Delete the OS disk of the affected VM altogether | | Recommend changing the access policies followed by the company | |

|  |
| --- |
| **Which OWASP IoT vulnerability talks about security flaws such as lack of firmware validation, lack of secure delivery, and lack of anti-rollback mechanisms on IoT devices?** |
| |  | | --- | | Insecure data transfer and storage | | Insecure default settings | | Use of insecure or outdated components | | **Lack of secure update mechanism** | |

|  |
| --- |
| **Robert needs to copy an OS disk snapshot of a compromised VM to a storage account in different region for further investigation. Which of the following should he use in this scenario?** |
| |  | | --- | | Azure Monitor | | ***Azure Portal*** | | Azure CLI | | Azure Active Directory | |

|  |
| --- |
| **Consider a scenario where the perpetrator of a dark web crime has uninstalled Tor browser from their computer after committing the crime. The computer has been seized by law enforcement so they can investigate it for artifacts of Tor browser usage. Which of the following should the investigators examine to establish the use of Tor browser on the suspect machine?** |
| |  | | --- | | Security logs | | Swap files | | Files in Recycle Bin | | **Prefetch files** | |

|  |
| --- |
| **"To ensure that the digital evidence is collected, preserved, examined, or transferred in a manner safeguarding the accuracy and reliability of the evidence, law enforcement, and forensics organizations must establish and maintain an effective quality system" is a principle established by:** |
| |  | | --- | | **SWGDE** | | EC-Council | | NIST | | NCIS | |

|  |
| --- |
| **During the course of his investigation, Vincent came across a situation where he needs to run a packet sniffing tool on a Linux-based machine to monitor the network traffic. Which tool should Vincent choose in this case?** |
| |  | | --- | | Balbuzard | | **Tcpdump** | | CurrPorts | | DumpIt | |

|  |
| --- |
| **You are an information security analyst at a large pharmaceutical company. While performing a routine review of audit logs, you have noticed a significant amount of egress traffic to various IP addresses on destination port 22 during off-peak hours. You researched some of the IP addresses and found that many of them are in Eastern Europe. What is the most likely cause of this traffic?** |
| |  | | --- | | The organization’s primary internal DNS server has been compromised and is performing DNS zone transfers to malicious external entities | | Data is being exfiltrated by an advanced persistent threat (APT) | | Malicious software on internal system is downloading research data from partner SFTP servers in Eastern Europe | | Internal systems are downloading automatic Windows updates | |

|  |
| --- |
| **Which standard is used during a judicial trial to assess whether an expert witness's scientific testimony is based on scientifically valid reasoning that can adequately be applied (admissible) to the facts under consideration?** |
| |  | | --- | | Joiner Standard | | **Daubert Standard** | | Dunn Standard | | Carmichael Standard | |

|  |
| --- |
| **Debbie has obtained a warrant to search a known pedophile’s house. Debbie went to the house and executed the search warrant to seize digital devices that have been recorded as being used for downloading illicit images. She seized all digital devices except a digital camera. Why did she not collect the digital camera?** |
| |  | | --- | | The digital camera was old, had a cracked screen, and did not have batteries. Therefore, it could not have been used in a crime. | | **The digital camera was not listed as one of the digital devices in the warrant** | | The vehicle Debbie was using to transport the evidence was already full and could not carry more items | | Debbie overlooked the digital camera because it is not a computer system | |

|  |
| --- |
| **During an investigation, the first responders stored mobile devices in specific containers to provide network isolation. All the following are examples of such pieces of equipment, except for:** |
| |  | | --- | | Wireless StrongHold bag | | RF shield box | | Faraday bag | | **VirtualBox** | |

|  |
| --- |
| **This law sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.** |
| |  | | --- | | **The CAN-SPAM act** | | Federal Spam act | | European Anti-Spam act | | Telemarketing act | |

|  |
| --- |
| **"In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to explain his/her actions and the impact of those actions on the evidence, in the court.” Which ACPO principle states this?** |
| |  | | --- | | Principle 3 | | **Principle 2** | | Principle 4 | | Principle 1 | |

|  |
| --- |
| **An investigator wants to extract passwords from SAM and System Files. Which tool can the investigator use to obtain a list of users, passwords, and their hashes in this case?** |
| |  | | --- | | **PWdump7** | | Nuix | | HashKey | | FileMerlin | |

|  |
| --- |
| **An EC2 instance storing critical data of a company got infected with malware. The forensics team took the EBS volume snapshot of the affected instance to perform further analysis and collected other data of evidentiary value. What should be their next step?** |
| |  | | --- | | They should terminate the instance after taking necessary backup | | They should pause the running instance | | They should keep the instance running as it stores critical data | | They should terminate all instances connected via the same VPC | |

|  |
| --- |
| **When installed on a Windows machine, which port does the Tor browser use to establish a network connection via Tor nodes?** |
| |  | | --- | | 49667/49668 | | 7680 | | **9150/915**1 | | 49664/49665 | |

|  |
| --- |
| **What does Locard's Exchange Principle state?** |
| |  | | --- | | Digital evidence must have some characteristics to be disclosed in the court of law | | Any information of probative value that is either stored or transmitted in a digital form | | Forensic investigators face many challenges during forensics investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidence | | **Anyone, or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave** | |

|  |
| --- |
| **Which of the following tools will allow a forensic investigator to acquire the memory dump of a suspect machine so that it may be investigated on a forensic workstation to collect evidentiary data like processes and Tor browser artifacts?** |
| |  | | --- | | Hex Editor | | Bulk Extractor | | DB Browser SQLite | | **Belkasoft Live RAM Capturer and AccessData FTK Imager** | |

|  |
| --- |
| **\_\_\_\_\_\_\_\_\_ allows a forensic investigator to identify the missing links during investigation.** |
| |  | | --- | | Chain of custody | | **Evidence reconstruction** | | Evidence preservation | | Exhibit numbering | |