Question #1 *Topic 1*

A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation?

A. Image the disk and try to recover deleted files

B. Seek the help of co-workers who are eye-witnesses

C. Check the Windows registry for connection data (you may or may not recover)

D. Approach the website's administrator for evidence

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #2

Topic 1

You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

A. The registry

B. The swap file

C. The recycle bin

D. The metadata

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

Which of the following are small pieces of data sent from a website and stored on the user's computer by the user's web browser to track, validate, and maintain specific user information?

A. Temporary Files

B. Open files

C. Cookies

D. Web Browser Cache

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

Depending upon the jurisdictional areas, different laws apply to different incidents. Which of the following law is related to fraud and related activity in connection with computers?

A. 18 USC §1029

B. 18 USC §1030

C. 18 USC §1361

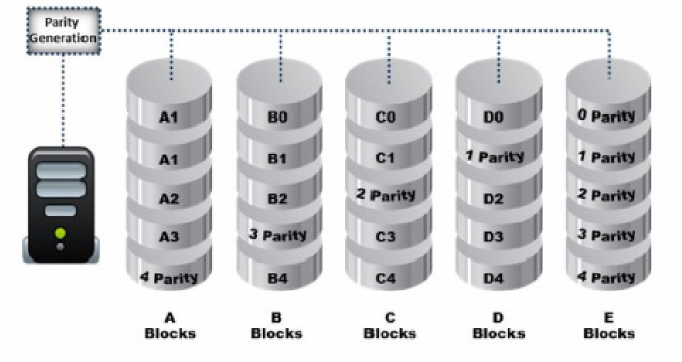
D. 18 USC §1371

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

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?

A. RAID Level 0

B. RAID Level 5

C. RAID Level 3

D. RAID Level 1

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

Charles has accidentally deleted an important file while working on his Mac computer. He wants to recover the deleted file as it contains some of his crucial business secrets. Which of the following tool will help Charles?

A. Xplico

B. Colasoft's Capsa

C. FileSalvage

D. DriveSpy

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

Jason discovered a file named $RIYG6VR.doc in the C:\$Recycle.Bin\<USER SID>\ while analyzing a hard disk image for the deleted data. What inferences can he make from the file name?

A. It is a doc file deleted in seventh sequential order

B. RIYG6VR.doc is the name of the doc file deleted from the system

C. It is file deleted from R drive

D. It is a deleted doc file

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and to execute commands outside of the web server's root directory?

A. Parameter/form tampering

B. Unvalidated input

C. Directory traversal

D. Security misconfiguration

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

Annie is searching for certain deleted files on a system running Windows XP OS. Where will she find the files if they were not completely deleted from the system?

A. C: $Recycled.Bin

B. C: \$Recycle.Bin

C. C:\RECYCLER

D. C:\$RECYCLER

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

Which of the following files stores information about a local Google Drive installation such as User email ID, Local Sync Root Path, and Client version installed?

A. filecache.db

B. config.db

C. sigstore.db

D. Sync_config.db

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

An expert witness is a _________________ who is normally appointed by a party to assist the formulation and preparation of a party's claim or defense.

A. Expert in criminal investigation

B. Subject matter specialist

C. Witness present at the crime scene

D. Expert law graduate appointed by attorney

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

Smith, a network administrator with a large MNC, was the first to arrive at a suspected crime scene involving criminal use of compromised computers. What should be his first response while maintaining the integrity of evidence?

A. Record the system state by taking photographs of physical system and the display

B. Perform data acquisition without disturbing the state of the systems

C. Open the systems, remove the hard disk and secure it

D. Switch off the systems and carry them to the laboratory

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?

A. HIPAA

B. GLBA

C. SOX

D. FISMA

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

Jacky encrypts her documents using a password. It is known that she uses her daughter's year of birth as part of the password. Which password cracking technique would be optimal to crack her password?

A. Rule-based attack

B. Brute force attack

C. Syllable attack

D. Hybrid attack

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

Which of the following Event Correlation Approach is an advanced correlation method that assumes and predicts what an attacker can do next after the attack by studying the statistics and probability and uses only two variables?

A. Bayesian Correlation

B. Vulnerability-Based Approach

C. Rule-Based Approach

D. Route Correlation

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #16

Topic 1

Smith, as a part his forensic investigation assignment, seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data in 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 made three unsuccessful attempts, which blocked the SIM card. What can Jason do in this scenario to reset the PIN and access SIM data?

A. He should contact the network operator for a Temporary Unlock Code (TUK)

B. Use system and hardware tools to gain access

C. He can attempt PIN guesses after 24 hours

D. He should contact the network operator for Personal Unlock Number (PUK)

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

Amber, a black hat hacker, has embedded a malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

A. Click-jacking

B. Compromising a legitimate site

C. Spearphishing

D. Malvertising

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Netstat is a tool for collecting information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics. Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?

A. netstat – r

B. netstat – ano

C. netstat – b

D. netstat – s

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

Billy, a computer forensics expert, has recovered a large number of DBX files during the forensic investigation of a laptop. Which of the following email clients can he use to analyze the DBX files?

A. Microsoft Outlook

B. Eudora

C. Mozilla Thunderbird

D. Microsoft Outlook Express

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

To which phase of the Computer Forensics Investigation Process does the Planning and Budgeting of a Forensics Lab belong?

A. Post-investigation Phase

B. Reporting Phase

C. Pre-investigation Phase

D. Investigation Phase

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

Identify the file system that uses $BitMap file to keep track of all used and unused clusters on a volume.

A. NTFS

B. FAT

C. EXT

D. FAT32

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?

A. OpenGL/ES and SGL

B. Surface Manager

C. Media framework

D. WebKit

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #23 Topic 1

You are assigned a task to examine the log files pertaining to MyISAM storage engine. While examining, you are asked to perform a recovery operation on a MyISAM log file. Which among the following MySQL Utilities allow you to do so?

A. mysqldump

B. myisamaccess

C. myisamlog

D. myisamchk

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #24

Topic 1

Gary is checking for the devices connected to USB ports of a suspect system during an investigation. Select the appropriate tool that will help him document all the connected devices.

A. DevScan

B. Devcon

C. fsutil

D. Reg.exe

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

An International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:

A. Type Allocation Code (TAC)

B. Integrated Circuit Code (ICC)

C. Manufacturer Identification Code (MIC)

D. Device Origin Code (DOC)

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

The Apache server saves diagnostic information and error messages that it encounters while processing requests. The default path of this file is usr/local/apache/logs/error.log in Linux. Identify the Apache error log from the following logs.

A. http://victim.com/scripts/..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1

B. [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration: /export/home/live/ap/htdocs/test

C. 127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700]"GET /apache_pb.gif HTTP/1.0" 200 2326

D. 127.0.0.1 - - [10/Apr/2007:10:39:11 +0300]] [error] "GET /apache_pb.gif HTTP/1.0" 200 2326

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

Which part of Metasploit framework helps users to hide the data related to a previously deleted file or currently unused by the allocated file.

A. Waffen FS

B. RuneFS

C. FragFS

D. Slacker

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

Event correlation is the process of finding relevance between the events that produce a final result. What type of correlation will help an organization to correlate events across a set of servers, systems, routers and network?

A. Same-platform correlation

B. Network-platform correlation

C. Cross-platform correlation

D. Multiple-platform correlation

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

What malware analysis operation can the investigator perform using the jv16 tool?

A. Files and Folder Monitor

B. Installation Monitor

C. Network Traffic Monitoring/Analysis

D. Registry Analysis/Monitoring

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #30

Topic 1

Which command can provide the investigators with details of all the loaded modules on a Linux-based system?

A. list modules -a

B. lsmod

C. plist mod -a

D. lsof -m

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

Examination of a computer by a technically unauthorized person will almost always result in:

A. Rendering any evidence found inadmissible in a court of law

B. Completely accurate results of the examination

C. The chain of custody being fully maintained

D. Rendering any evidence found admissible in a court of law

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

The Recycle Bin exists as a metaphor for throwing files away, but it also allows a 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

B. INFO1

C. LOGINFO1

D. LOGINFO2

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

A Linux system is undergoing investigation. In which directory should the investigators look for its current state data if the system is in powered on state?

A. /auth

B. /proc

C. /var/log/debug

D. /var/spool/cron/

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a "simple backup copy" of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a "simple backup copy" will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

A. Robust copy

B. Incremental backup copy

C. Bit-stream copy

D. Full backup copy

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

An investigator enters the command sqlcmd -S WIN-CQQMK62867E -e -s"," -E as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E" represent?

A. Name of the Database

B. Name of the SQL Server

C. Operating system of the system

D. Network credentials of the database

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

Robert is a regional manager working in a reputed organization. One day, he suspected malware attack after unwanted programs started to popup after logging into his computer. The network administrator was called upon to trace out any intrusion on the computer and he/she finds that suspicious activity has taken place within Autostart locations. In this situation, which of the following tools is used by the network administrator to detect any intrusion on a system?

A. Hex Editor

B. Internet Evidence Finder

C. Process Monitor

D. Report Viewer

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

What do you call the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents?

A. Windows Services Monitoring

B. System Baselining

C. Start-up Programs Monitoring

D. Host integrity Monitoring

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

Which of the following statements is true regarding SMTP Server?

A. SMTP Server breaks the recipient’s address into Recipient’s name and his/her designation before passing it to the DNS Server

B. SMTP Server breaks the recipient's address into Recipient’s name and recipient’s address before passing it to the DNS Server

C. SMTP Server breaks the recipient’s address into Recipient’s name and domain name before passing it to the DNS Server

D. SMTP Server breaks the recipient’s address into Recipient’s name and his/her initial before passing it to the DNS Server

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

Which ISO Standard enables laboratories to demonstrate that they comply with quality assurance and provide valid results?

A. ISO/IEC 16025

B. ISO/IEC 18025

C. ISO/IEC 19025

D. ISO/IEC 17025

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

Which of these Windows utility help you to repair logical file system errors?

A. Resource Monitor

B. Disk cleanup

C. Disk defragmenter

D. CHKDSK

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

Identify the term that refers to individuals who, by virtue of their knowledge and expertise, express an independent opinion on a matter related to a case based on the information that is provided.

A. Expert Witness

B. Evidence Examiner

C. Forensic Examiner

D. Defense Witness

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 1*

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, assigning NULL values implies?

A. Start and end points for log sequence numbers are specified

B. Start and end points for log files are not specified

C. Start and end points for log files are specified

D. Start and end points for log sequence numbers are not specified

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #43 *Topic 1*

An attacker successfully gained access to a remote Windows system and plans to install persistent backdoors on it. Before that, to avoid getting detected in future, he wants to cover his tracks by disabling the last-accessed timestamps of the machine. What would he do to achieve this?

A. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 0

B. Run the command fsutil behavior set disablelastaccess 0

C. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 1

D. Run the command fsutil behavior set enablelastaccess 0

Suggested Answer: *C -*
Reference https://www.techrepublic.com/article/tech-tip-disable-the-last-access-update/

Currently there are no comments in this discussion, be the first to comment!

Question #44 *Topic 1*

POP3 is an Internet protocol, which is used to retrieve emails from a mail server. Through which port does an email client connect with a POP3 server?

A. 110

B. 143

C. 25

D. 993

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 1*

James, a hacker, identifies a vulnerability in a website. To exploit the vulnerability, he visits the login page and notes down the session ID that is created. He appends this session ID to the login URL and shares the link with a victim. Once the victim logs into the website using the shared URL, James reloads the webpage (containing the URL with the session ID appended) and now, he can browse the active session of the victim. Which attack did James successfully execute?

A. Cross Site Request Forgery

B. Cookie Tampering

C. Parameter Tampering

D. Session Fixation Attack

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

What does Locard's Exchange Principle state?

A. Any information of probative value that is either stored or transmitted in a digital form

B. Digital evidence must have some characteristics to be disclosed in the court of law

C. Anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave

D. Forensic investigators face many challenges during forensics investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidence

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #47 *Topic 1*

You are asked to build a forensic lab and your manager has specifically informed you to use copper for lining the walls, ceilings, and floor. What is the main purpose of lining the walls, ceilings, and floor with copper?

A. To control the room temperature

B. To strengthen the walls, ceilings, and floor

C. To avoid electromagnetic emanations

D. To make the lab sound proof

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #48

Topic 1

Which tool allows dumping the contents of process memory without stopping the process?

A. psdump.exe

B. pmdump.exe

C. processdump.exe

D. pdump.exe

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

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?

A. The common log format of Apache access log

B. IIS log

C. The combined log format of Apache access log

D. Apache error log

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #50 Topic 1

In a Filesystem Hierarchy Standard (FHS), which of the following directories contains the binary files required for working?

A. /mnt

B. /sbin

C. /media

D. /proc

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #51 *Topic 1*

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?

A. NetCat

B. Helix

C. R-Studio

D. Wireshark

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #52 *Topic 1*

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?

A. echo text > program:source_file

B. C:\>ECHO text_message > myfile.txt:stream1

C. C:\MORE < myfile.txt:stream1

D. myfile.dat:stream1

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #53

Topic 1

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?

A. WIN-DTRAI83202X-bin.nnnnnn

B. WIN-DTRAI83202Xslow.log

C. relay-log.info

D. WIN-DTRAI83202Xrelay-bin.index

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #54 *Topic 1*

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?

A. Insecure default settings

B. Use of insecure or outdated components

C. Lack of secure update mechanism

D. Insecure data transfer and storage

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #55

Topic 1

Which of the following malware targets Android mobile devices and installs a backdoor that remotely installs applications from an attacker-controlled server?

A. Unflod

B. Felix

C. XcodeGhost

D. xHelper

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #56 *Topic 1*

Which of the following tools is used to dump the memory of a running process, either immediately or when an error condition occurs?

A. CacheInf

B. FATKit

C. Belkasoft Live RAM Capturer

D. Coreography

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #57 *Topic 1*

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?

A. Authorization form

B. Consent form

C. Chain of custody

D. Log book

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #58 *Topic 1*

Which of the following is a requirement for senders as per the CAN-SPAM act?

A. Emails must not contain information regarding how to stop receiving emails from the sender in future

B. Senders should never share their physical postal address in the email

C. Senders cannot use misleading or false header information

D. Senders must use deceptive subject lines

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #59 *Topic 1*

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?

A. Delete the OS disk of the affected VM altogether

B. Delete the snapshot from the source resource group

C. Recommend changing the access policies followed by the company

D. Create another VM by using the snapshot

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #60 *Topic 1*

Identify the location of Recycle Bin on a Windows 7 machine that uses NTFS file system to store and retrieve files on the hard disk.

A. Drive:\RECYCLER

B. Drive:\RECYCLED

C. Drive:\$Recycle.Bin

D. C:\RECYCLED

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #61 *Topic 1*

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"?

A. Standards and Criteria 1.4

B. Standards and Criteria 1.5

C. Standards and Criteria 1.6

D. Standards and Criteria 1.7

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #62 *Topic 1*

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.

A. A unique sequence number identifying the record

B. The call duration

C. Phone number receiving the call

D. The language of the call

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #63

Topic 1

"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?

A. Principle 1

B. Principle 2

C. Principle 3

D. Principle 4

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #64 *Topic 1*

On NTFS file system, which of the following tools can a forensic investigator use in order to identify timestomping of evidence files?

A. Exiv2

B. analyzeMFT

C. Timestomp

D. wbStego

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #65 *Topic 1*

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?

A. oleid.py

B. oleform.py

C. oledir.py

D. pdfid.py

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #66 *Topic 1*

Before accessing digital evidence from victims, witnesses, or suspects, on their electronic devices, what should the investigator do first to respect legal privacy requirements?

A. Protect the device against external communication

B. Remove the battery or turn-off the device

C. Notify the fact to the local authority or employer

D. Obtain a formal written consent to search

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #67 *Topic 1*

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?

A. Metadata

B. Metabase

C. Data index

D. Data header

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #68 *Topic 1*

Derrick, a forensic specialist, was investigating an active computer that was executing various processes. Derrick wanted to check whether this system was used in an incident that occurred earlier. He started inspecting and gathering the contents of RAM, cache, and DLLs to identify incident signatures. Identify the data acquisition method employed by Derrick in the above scenario.

A. Dead data acquisition

B. Non-volatile data acquisition

C. Static data acquisition

D. Live data acquisition

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #69 *Topic 1*

When analyzing logs, it is important that the clocks of all the network devices are synchronized. Which protocol will help in synchronizing these clocks?

A. UTC

B. PTP

C. UCT

D. NTP

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #70 *Topic 1*

What happens to the header of the file once it is deleted from the Windows OS file systems?

A. The OS replaces the entire hex byte coding of the file

B. The hex byte coding of the file remains the same, but the file location differs

C. The OS replaces the second letter of a deleted file name with a hex byte code: Eh5

D. The OS replaces the first letter of a deleted file name with a hex byte code: E5h

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #71 *Topic 1*

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 ____________.

A. Swap space

B. Cluster space

C. Slack space

D. Sector space

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #72 *Topic 1*

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?

A. Access gateway layer

B. Application layer

C. Edge technology layer

D. Middleware layer

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #73 *Topic 1*

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?

A. DB Browser SQLite

B. Belkasoft Live RAM Capturer and AccessData FTK Imager

C. Bulk Extractor

D. Hex Editor

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #74 *Topic 1*

"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?

A. FBI Cyber Division

B. Scientific Working Group on Imaging Technology (SWGIT)

C. The Association of Chief Police Officers (ACPO) Principles of Digital Evidence

D. Locard's exchange principle

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #75 *Topic 1*

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?

A. National and local regulation

B. Service level agreement

C. Key performance indicator

D. Service level management

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!