1. Common types of cyber crimes
    a. Phishing
    b. Cyber Extortion(ransomware)
    c. Data breach
    d. Identity theft
    e. Harassment
2. Common web application threats/attacks - Source OWASP
    a. A01:2021-Broken Access Control
    b. A02:2021-Cryptographic Failures
    c. A03:2021-Injection
    d. A04:2021-Insecure Design
    e. A05:2021-Security Misconfiguration
    f. A06:2021-Vulnerable and Outdated Components
    g. A07:2021-Identification and Authentication Failures
    h. A08:2021-Software and Data Integrity Failures
    i. A09:2021-Security Logging and Monitoring Failures
    j. A10:2021-Server-Side Request Forgery
3. Challenges in web application forensics
   https://info-savvy.com/understand-web-applications-architecture-in-forensic-investigation/
    a. Web applications are often business-critical, thus making it difficult for the investigators to create their forensic image that requires the site to be down for some time for completing the process. This makes it difficult for the investigators to capture volatile data including processes, port/network connections, logs of memory dumps, and user logs during the time of the incident analysis.
    b. When a website attack occurs, the investigators need to gather the digital fingerprints left by the attacker. Then, they need to collect the following data fields associated with each HTTP request made to the website in order to get an insight of the attack performed.
    c. Most of the web applications restrict access to HTTP information, such as the full set of HTTP headers and the request body without which all the HTTP headers will look alike. This makes it impossible for the investigators to differentiate valid HTTP requests from the malicious ones.
4. What is anti-forensics and what are some common techniques?
   https://cisomag.eccouncil.org/6-anti-forensic-techniques-that-every-digital-forensic-investigator-dreads/
    a. Encryption
    b. Program Packers
    c. Overwriting data
    d. Onion Routing

    e. Steganography
    f. Changing Timestamps
5. What is network forensics and what are some of the challenges?
    a. Network forensics is a sub-branch of the practice of digital forensics itself a branch of forensic science - whereby experts and law enforcement look into technology or data that may contain evidence of a crime or attribute evidence to suspects, cross-reference statements or check alibis. Network forensics, unsurprisingly, refers to the investigation and analysis of all traffic going across a network suspected of use in cyber crime, say the spread of data-stealing malware or the analysis of cyber attacks.
    b. Some of the key challenges include high storage speed, the requirement of ample storage space, data integrity, data privacy, access to IP address, and location of data extraction.
6. What is the difference between post-mortem and real-time analysis?
    a. A post-mortem is held after an incident has taken place (in this case, a security breach of some type). The security team sits down with the rest of the organization (or the affected team) and talks through what happened, identifies causes, lessons learned, and how to move forward.
    b. Real-time network traffic analysis helps engineers, operators, administrators, and analysts better identify anomalies and suspicious traffic patterns that could be an indication of compromise (IOC) or an infrastructure component malfunctioning.
7. What are some examples of volatile data and non-volatile data?
    a. Volatile Memory: It is the memory hardware that fetches/stores data at a high-speed. It is also referred to as temporary memory. The data within the volatile memory is stored till the system is capable of, but once the system is turned off the data within the volatile memory is deleted automatically. RAM (Random Access Memory) and Cache Memory are some common examples of volatile memory. Here, data fetch/store is fast and economical.
    b. Non-Volatile Memory: It is the type of memory in which data or information is not lost within the memory even if power is shut-down. ROM (Read Only Memory) is the most common example of non-volatile memory. It's not economical and slow in fetch/store as compared to volatile memory however it stores a higher volume of data. All such information that needs to be stored for an extended amount of time is stored in non-volatile memory. Non-volatile memory has a huge impact on a system's storage capacity.
8. What are the types of forensic data acquisition?
    a. There are different types of data acquisition methods including logical disk-to-disk file, disk-to-disk copy, sparse data copy of a file or folder, and disk-to-image file.
9. What are TOR relays and how do they work?
   https://medium.com/coinmonks/tor-nodes-explained-580808c29e2d
    a. What is an Entry/Guard Relay? It is the entry point to the TOR Network. Each client that wants to connect to the TOR network will first connect to the guard node meaning, they can see the real IP Address of the client who is attempting to

connect. The list of guard nodes is available in the public list of TOR nodes and are updated almost every minute. Few websites to check the currently available guard nodes and their details are dan.me.uk/, torstatus.blutmagie.de/, check.torproject.org/. There are cases where attackers have control or observe certain relays and they can be used to see the victim's browsing. Also, when you try changing the circuit in your current session, it only changes the relays and not the guard node (in order to protect against known anonymity-breaking attacks). The guard node typically changes every 2–3 months.

b. What is a Middle Relay? Middle relays cover most part of the Tor circuit in any given transmission. They consist of relays through which data is passed in encrypted format and no node knows more than its predecessor and descendant. All the available middle relay nodes show themselves to the guard and exit nodes so that any may connect to them for transmission. Even if any middle relay is known to transmit malicious traffic (such as the attacker's exploit or the attack itself) they're not held responsible as they're neither the source nor destination of the traffic. A middle relay will never be allowed to act as an exit node. It is most suitable for users who want to utilize TOR from home or workplace (if it's allowed).

c. What is an Exit Relay? The exit relay is the final relay in the TOR circuit. They are the nodes that send the data to the destination and are often considered the culprit because the Exit node is perceived as the origin of the traffic. Therefore, the exit node's IP will be directly visible to the destination and often receive multiple complaints, legal notices, take down notices etc. In order to host an End node one must be ready to handle problems such as, Legal issues like take-downs or DMCA notices, Own a dedicated IP and make sure their reverse DNS is easily discovered, setting up an Exit Node Hosting notice (the most important step) etc.

10. What is a TOR bridge node?
    a. Bridge nodes are the nodes which are not listed on the public directory of TOR nodes. Most of the entry and exit nodes are publicly available on the internet and therefore they can be blocked if one wishes to restrict the usage of TOR. Many ISPs, Corporate Organizations and even Governments have filters set to ban the usage of TOR. For example, the Chinese government has blocked all publicly available nodes on their country level firewall. To avoid such a scenario, there are Bridge nodes. You will need to follow a different configuration settings in order to connect to the TOR network via a Bridge node.
11. What is the internal architecture of MySQL?
    a. MySQL parses queries to create an internal structure (the parse tree), and then applies a variety of optimizations. These can include rewriting the query, determining the order in which it will read tables, choosing which indexes to use, and so on.
12. What is fileless malware and what is the infection chain of fileless malware?

a. Fileless malware is a type of malicious software that uses legitimate programs to infect a computer. It does not rely on files and leaves no footprint, making it challenging to detect and remove.

13. What is the Dark Web and what are some of the dangers?
    a. The dark web refers to sites that are not indexed and only accessible via specialized web browsers. Significantly smaller than the tiny surface web, the dark web is considered a part of the deep web.
    b. A December 2014 study by Gareth Owen from the University of Portsmouth found that the most commonly hosted type of content on Tor was child pornography, followed by black markets, while the individual sites with the highest traffic were dedicated to botnet operations. Many whistleblowing sites maintain a presence as well as political discussion forums. Sites associated with Bitcoin, fraud-related services, and mail order services are some of the most prolific.
14. How do you browse the Dark Web safely?
    a. The dark web, also known as darknet websites, are accessible only through networks such as TOR ("The Onion Routing" project) that are created specifically for the dark web.
    https://www.torproject.org/
15. What is the structure of a data directory?
    a. The MySQL data directory contains all of the databases and tables managed by the server. In general, these are organized into a tree structure that is implemented in straightforward fashion by taking advantage of the hierarchical structure of the UNIX or Windows file systems:
        - Each database corresponds to a directory under the data directory.
        - Tables within a database correspond to files in the database directory.
16. What is cloud computing?
    a. Cloud computing is the on-demand delivery of IT resources over the Internet with pay-as-you-go pricing. Instead of buying, owning, and maintaining physical data centers and servers, you can access technology services, such as computing power, storage, and databases, on an as-needed basis from a cloud provider.
17. What are the types of cloud computing services?
    a. There are 3 main types of cloud computing services:
        - Infrastructure-as-a-Service (IaaS)
        - Platforms-as-a-Service (PaaS)
        - Software-as-a-Service (SaaS)
18. What are the types of cloud deployment models?
    a. Different types of cloud computing deployment models are:
        1. Public cloud
        2. Private cloud
        3. Hybrid cloud
        4. Community cloud
        5. Multi-cloud
19. What are the common cloud threats/attacks?

https://www.blumira.com/top-cloud-security-threats/

a. Misconfigured cloud services
b. Data loss
c. API vulnerabilities
d. Malware infections
e. Insufficient identity and access management controls

20. What are the parts of an email message?
    a. The pattern that defines an email is known as Request for Comment (RFC). Basically, RFC5321 provides information about the envelope and the transmission protocol for an email while RFC5322 addresses the format.

Term	Letter	Email
RFC5321	Recipient	Envelope Recipient
RFC5321	Sender	Envelope Sender, Bounce Address, Return Path
RFC5322	Recipient	Header To, Header Recipient
RFC5322	Sender	Header From, Header Sender
RFC5322	Date	Header Date
RFC5322	Subject	Header Subject

21. What is malware and what are the components of malware?
    a. Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for “malicious software.” Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware.
        - Payload: This is the core component of malware, designed to execute its actual motive
        - Obfuscator: Usually a packer or protector for encrypting or compressing the malware
        - Persistence: How the malware manages to stay in the system
        - Stealth component: Hides the malware from antivirus and other tools, and security analysts
        - Armoring: Protects the malware from being easily identified by researchers
        - Command and control (C&C): This is the control center for the malware
22. What are some common malware families?
    a. Worms, viruses, trojans, backdoors, and ransomware are some of the most common types of malware.
23. What are some common techniques used to distribute malware across the web?
    a. Phishing emails.
    b. Remote Desktop Protocol.

    c. Drive-by downloads from a compromised website.
    d. USB and Removable Media.
24. How do fileless malware attacks work? (i.e.- memory exploits)
    a. Fileless malware is a type of malicious activity that uses native, legitimate tools built into a system to execute a cyber attack. Unlike traditional malware, fileless malware does not require an attacker to install any code on a target's system, making it hard to detect. This fileless technique of using native tools to conduct a malicious attack is called "living off the land."
25. What is IoT and the architecture of IoT devices?
    a. The Internet of Things (IoT) describes the network of physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools.
    b. An IoT Architecture is a system of numerous elements such as sensors, actuators, protocols, cloud services, and layers that make up an IoT networking system. It generally consists of differentiated layers that enable administrators to evaluate, monitor, and maintain the system's consistency. As with any system design plan, it also requires a strategy for integration with your organization's existing infrastructure and systems.
26. What are common IoT security threats/attacks?
    a. Lack of physical hardening.
    b. Insecure data storage and transfer.
    c. Lack of visibility and device management.
    d. Botnets.
    e. Weak passcodes.
    f. Insecure ecosystem interfaces.
    g. AI-based attacks.
27. What is NAS and SAN storage?
    a. A NAS is a single storage device that serves files over Ethernet and is relatively inexpensive and easy to set up, while a SAN is a tightly coupled network of multiple devices that work with block-based data and is more expensive and complex to set up and manage.
28. What is RAID?
    a. Redundant Array of Independent/Inexpensive Disks (RAID) is a technology that allows storing data across multiple hard drives. The purpose of RAID is to achieve data redundancy to reduce data loss and, in a lot of cases, improve performance. The best way to get in on the RAID action is with a NAS.
29. What is the boot process for Windows, Linux, and Mac OS?
    a. Windows
        - PreBoot: POST or Power-On Self-Test loads firmware settings. It checks for a valid disk system, and if the system is good to go for the next phase. If the computer has a valid MBR, i.e., Master Boot Record, the boot process moves further and loads Windows Boot Manager.

- Windows Boot Manager: This step determines if you have multiple OS installed on your computer. If yes, then it offers a menu with the names of the OSs. When you select the OS, it will load the right program, i.e., Winload.exe to boot you into the correct OS.
- Windows OS Loader: Like its name, WinLoad.exe loads important drivers to kick start the Windows Kernel. The kernel uses the drivers to talk to the hardware and do the rest of the things required for the boot process to continue.
- Windows NT OS Kernel: This is the last stage that picks up the Registry settings, additional drivers, etc. Once that has been read, the control is taken by the system manager process. It loads up the UI, the rest of the hardware and software. That's when you finally get to see your Windows 10 Login screen.

b. Linux
   - BIOS stands for Basic Input/Output System. In simple terms, the BIOS loads and executes the Master Boot Record (MBR) boot loader.
   - MBR stands for Master Boot Record, and is responsible for loading and executing the GRUB boot loader.
   - GRUB Sometimes called GNU GRUB, which is short for GNU GRand Unified Bootloader, is the typical boot loader for most modern Linux systems. The GRUB splash screen is often the first thing you see when you boot your computer. It has a simple menu where you can select some options. If you have multiple kernel images installed, you can use your keyboard to select the one you want your system to boot with. By default, the latest kernel image is selected.
   - Kernel is often referred to as the core of any operating system, Linux included. It has complete control over everything in your system. In this stage of the boot process, the kernel that was selected by GRUB first mounts the root file system that's specified in the grub.conf file. Then it executes the /sbin/init program, which is always the first program to be executed. You can confirm this with its process id (PID), which should always be 1.
   - Init - At this point, your system executes runlevel programs. At one point it would look for an init file, usually found at /etc/inittab to decide the Linux run level.
   - Runlevel programs depending on which Linux distribution you have installed, you may be able to see different services getting started. For example, you might catch 'starting sendmail …. OK.'

c. Mac Boot Process
   - Boot ROM Initialization - As soon as you press the Power button to turn your Mac on, it sends the electrical signals to the Main Logic Board (also called Motherboard) which initializes the small program code called BootROM and makes the memory(RAM) usable. BootROM controls two other subprograms called POST and EFI.

- Executing Boot Loader - Once the macOS partition has been selected, Boot ROM passes the control over to the Boot Loader file called Boot.efi (earlier known as BootX) which is located in /System/Library/CoreServices folder on the root partition. Once the Boot.efi file (Boot Loader) is found, it draws the “Apple logo” on the screen. The primary job of this Boot.efi file is to load the essential kernel extensions (hardware drivers also known as kexts) from its cache folder
- Kernel Initialization and Rooting - At this stage, enough drivers are loaded for the kernel to find the root device. Once the root device is found, the kernel roots itself off of BSD and mounts the system partition as the root, or top-level, file system which is also known as rooting. After the root partition is mounted, the kernel passes the control over to the root system processes which show the login screen and create user interface and environment.This process is known as System Initialization.
- System Initialization - This is the stage where the dark gray Apple logo is replaced by the login window or the user’s desktop background if the auto login is enabled.

30. What is the Android architecture and what are some common threats/attacks to Android devices?
    a. The main components of android architecture are following:-
        - Applications
        - Application Framework
        - Android Runtime
        - Platform Libraries
        - Linux Kernel
    b. Common Threats/Attacks
       https://www.hackeracademy.org/top-10-android-attacks-hackers-use-in-2021/
        - Untrusted APKS
        - Android Attacks using SMS
        - Email
        - Android Attacks using App Sandboxing issues
        - Rooting
        - Spying Apps
        - Android Attacks using Fork bomb attack
        - Phishing Attack
        - Smudge attacks
        - Droid Dream
31. What is the iOS architecture and what are some common threats/attacks to iOS devices?
    a. Core OS
        - All the iOS technologies are built on the low level features provided by the Core OS layer. These technologies include Core Bluetooth Framework, External Accessory Framework, Accelerate Framework, Security Services Framework, Local Authorisation Framework etc.

b. Core Services
    - The technologies in the Core Services layer are called *core services* because they provide essential services to apps but have no direct bearing on the app's user interface. In general, these technologies are dependent on frameworks and technologies in the two lowest layers of OS X—that is, the Core OS layer and the Kernel and Device Drivers layer.
c. Media
    - The media layer enables all the graphics, audio and video technology of the system.
d. Cocoa Touch
    - User interface framework provided by Apple for building software applications for products like iPhone, iPad and iPod Touch. It is primarily written in Objective C language and is based on Mac OS X.

32. Where can you find evidence on mobile devices?
    a. Data on a mobile phone can be found in a number of locations: SIM card, external storage card, and phone memory. In addition, the service provider also stores communication-related information. The book primarily focuses on data acquired from the phone memory. Mobile device data extraction tools recover data from the phone's memory. Even though data recovered during a forensic acquisition depends on the mobile model, in general, the data in the next set of bullet items is common across all models and useful as evidence.
        - Address Book: This stores contact names, numbers, e-mail addresses, and so on
        - Call History: This contains dialed, received, missed calls, and call durations
        - SMS: This contains sent and received text messages
        - MMS: This contains media files such as sent and received photos and videos
        - E-mail: This contains sent, drafted, and received email messages
        - Web browser history: This contains the history of websites that were visited
        - Photos: This contains pictures that are captured using the mobile phone camera, those downloaded from the Internet, and the ones transferred from other devices
        - Videos: This contains videos that are captured using the mobile camera, those downloaded from the Internet, and the ones transferred from other devices
        - Music: This contains music files downloaded from the Internet and those transferred from other devices
        - Documents: This contains documents created using the device's applications, those downloaded from the Internet, and the ones transferred from other devices
        - Calendar: This contains calendar entries and appointments

- Network communication: This contains GPS locations
- Maps: This contains looked-up directions, and searched and downloaded maps
- Social networking data: This contains data stored by applications, such as Facebook, Twitter, LinkedIn, Google+, and WhatsApp
- Deleted data: This contains information deleted from the phone

33. What is a SIM card?
    a. A SIM card, also called a subscriber identity module or subscriber identification module, is a small memory card that contains unique information that identifies it to a specific mobile network. This card allows subscribers to use their mobile devices to receive calls, send SMS messages, or connect to mobile internet services.
34. What are common log files you can obtain in a forensic investigation?
    a. The application log, network log, operating system log, and database log produce valuable information for a forensic investigation.
35. What is the ELF_LOGFILE_HEADER structure?
    a. The ELF_LOGFILE_HEADER structure is used at the beginning of an event log to define information about the event log.
        - HeaderSize - The size of the header structure. The size is always 0x30.
        - Signature - The signature is always 0x654c664c, which is ASCII for eLfL.
        - MajorVersion - The major version number of the event log. The major version number is always set to 1.
        - MinorVersion - The minor version number of the event log. The minor version number is always set to 1.
        - StartOffset - The offset to the oldest record in the event log.
        - EndOffset - The offset to the ELF_EOF_RECORD in the event log.
        - CurrentRecordNumber - The number of the next record that will be added to the event log.
        - OldestRecordNumber - The number of the oldest record in the event log. For an empty file, the oldest record number is set to 0.
        - MaxSize - The maximum size, in bytes, of the event log. The maximum size is defined when the event log is created. The event-logging service does not typically update this value, it relies on the registry configuration. The reader of the event log can use normal file APIs to determine the size of the file. For more information about registry configuration values, see Eventlog Key.
        - Flags - The status of the event log. This member can be one of the following values:
            1. ELF_LOGFILE_HEADER_DIRTY 0x0001 - Indicates that records have been written to an event log, but the event log file has not been properly closed. For more information about this flag, see the Remarks section.
            2. ELF_LOGFILE_HEADER_WRAP 0x0002 - Indicates that records in the event log have wrapped.

3. ELF_LOGFILE_LOGFULL_WRITTEN 0x0004 - Indicates that the most recent write attempt failed due to insufficient space.
4. ELF_LOGFILE_ARCHIVE_SET 0x0008 - Indicates that the archive attribute has been set for the file. Normal file APIs can also be used to determine the value of this flag.

- Retention - The retention value of the file when it is created. The event-logging service does not typically update this value, it relies on the registry configuration. For more information about registry configuration values, see Eventlog Key.
- EndHeaderSize - The ending size of the header structure. The size is always 0x30.

36. What is the legal criteria for admitting logs as evidence?
    a. The USA – code title 28, section 1732 states that ' logs files are admissible as evidence if they are collected in the regular course of the business'.
37. What is the Web server architecture of IIS?
    a. IIS uses a request-processing architecture. It listens for HTTP requests (as well as requests for other protocols) before creating worker processes (w3wp.exe) to handle the request.
38. What is the Web server architecture of Apache?
    a. Apache is the web server that processes requests and serves web assets and content via HTTP. MySQL is the database that stores all your information in an easily queried format. PHP is the programming language that works with apache to help create dynamic web content
39. What are common hex values for image files?
    a. JPEG - FF D8 FF
    b. PNG - 50 4E 47
    c. GIF - 47 49 46
40. What is a WAF and how do they work?
    a. WAF -Web Application Firewall
    b. A WAF protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorized data from leaving the app.
41. What are the benefits/drawbacks to using a Web application firewall?
    a. Benefits:
        - Prevent attacks, including SQL injections, cross-site scripting (XSS) attacks, and distributed denial of service (DDoS) attacks
        - Stop customer data from being compromised, preserving confidence—and their patronage
        - Ensure compliance with regulations like HIPAA and PCI
        - Free up your team’s resources by automatically running security tests and monitoring traffic
    b. Drawbacks:
        - False positives

        - Insufficient Protection - Additionally, WAFs can not protect from design flaws such as Broken Access Control and Parameter Tampering.
        - Resource-hungry - WAFs consume many resources from the organization because they are complex to maintain, and the licenses are costly.

42. How is data stored in SQL server?
    a. Data files (.mdf) contain the actual data. Data in tables is stored in row and column format at the logical level, but physically it stores data in something called data pages. A data page is the fundamental unit of data storage in SQL Server and it is 8KB in size.
43. Where can you find evidence in a database?
    a. Volatile database data (sessions/connections, active requests, active users, memory, etc.)
    b. Transaction logs
    c. Database files
    d. SQL Server error logs
    e. System event logs
    f. Trace files
44. What are MySQL utility programs that can be used for forensic analysis? https://info-savvy.com/perform-mysql-forensics/
    a. Mysqldump
    b. mysqlaccess
    c. myisamlog
    d. myisamchk
    e. mysqlbinlog
    f. mysqldbexport
45. What is the chain of custody and why is it important? https://percipient.co/overview-the-three-types-of-forensic-collections-physical-vs-logical-vs-targeted/
    a. The chain of custody is the most critical process of evidence documentation. It is a must to assure the court of law that the evidence is authentic, i.e., it is the same evidence seized at the crime scene. It was, at all times, in the custody of a person designated to handle it and for which it was never unaccounted.
46. What types of images can you do in a forensic investigation?
    a. Physical Image - A physical device collection is a bit-by-bit copy of the device, i.e., an exact copy. Conducting physical imaging of a mobile device is the most thorough and acquires the greatest amount of data. It is used to acquire the entire physical volume of a drive. Physical forensic images capture deleted space, file fragments and provide access to deleted and encrypted data.
    b. Logical Image - A logical image of a device or hard drive captures all files visible to the user and typically does not recover deleted items, data in deleted areas of the device, nor does it collect file fragments.
    c. Targeted Image - A targeted collection is just what it sounds like: a forensic collection of specific files or folders relevant to a legal matter. This method is the least expensive because it collects the least amount of data and is best suited for

civil matters with cost sensitivity considerations, eDiscovery proportionality concerns or for subpoena responses.

47. What is the sleuth kit?
    a. The Sleuth Kit is a library and collection of Unix- and Windows-based utilities for extracting data from disk drives and other storage so as to facilitate the forensic analysis of computer systems.
48. What is Autopsy?
    a. Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.
49. What is Flare VM?
    a. FLARE VM is a freely available and open sourced Windows-based security distribution designed for reverse engineers, malware analysts, incident responders, forensicators, and penetration testers.
50. What is Remnux and what is it used for?
    a. REMnux® is a Linux toolkit for reverse-engineering and analyzing malicious software. REMnux provides a curated collection of free tools created by the community. Analysts can use it to investigate malware without having to find, install, and configure the tools.
51. What are SQL Server Trace Files?
    a. A file created when a trace is saved. In SQL Server Profiler, a file that defines the event classes and data columns to be collected in a trace. In SQL Server Profiler, a table that is created when a trace is saved to a table.
52. How do you do Windows Memory Analysis?
    a. WinPMEM is a tool used for obtaining memory images from Windows systems. It is an easy-to-use command line program which, by default, stores the resulting memory image in AFF4 format.
    b. Volatility is a tool that can be used to analyze a volatile memory of a system or an image from WinPMEM. With this easy-to-use tool, you can inspect processes, look at command history, and even pull files and passwords from a system without even being on the system.
53. What are some common areas in Windows Registry changed by malware?
    a. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
    b. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
    c. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
    d. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
54. How do you identify TOR Browser Artifacts and what kind of information can you get from TOR?
    a. When the Tor browser is installed on a Windows machine, it uses port 9150/9151 for establishing connections via Tor nodes. Forensic investigators can obtain the path from where the TOR browser is executed in the following Registry key: HKEY_USERS<SID>\SOFTWARE\Mozilla\Firefox\Launcher. The investigator

analyzes the ‘State’ file located in the path where the Tor browser was executed on a suspect machine.

55. What are Prefetch Files?
    a. Prefetch files are artifacts for forensic investigators trying to analyze applications that have been run on a system. Windows creates a prefetch file when an application is run from a particular location for the very first time. This is used to help speed up the loading of applications.
56. What is malware forensics?
    a. It is a way of finding, analyzing & investigating various properties of malware to seek out the culprits and reason for the attack. The method also includes tasks like checking out the malicious code, determining its entry, method of propagation, impact on the system, ports it tries to use etc. investigators conduct forensic investigation using different techniques and tools.
57. What are common challenges in analyzing malware?
    a. No guarantee to find everything built into the malware, sometimes interaction from the developers are needed to see what it can evolve to.
58. What is the difference between static and dynamic malware analysis?
    a. Static analysis is a process of analyzing a malware binary without actually running the code. Static analysis is generally performed by determining the signature of the binary file which is a unique identification for the binary file and can be done by calculating the cryptographic hash of the file and understanding each component.
    b. Dynamic analysis involves running the malware sample and observing its behavior on the system in order to remove the infection or stop it from spreading into other systems. The system is set up in a closed, isolated virtual environment so that the malware sample can be studied thoroughly without the risk of damage to your system.
59. What tools can be used for static and dynamic malware analysis?
    https://www.varonis.com/blog/malware-analysis-tools

    a. PeStudio
    b. Process Hacker
    c. Process Monitor (ProcMon)
    d. ProcDot
    e. Autoruns
    f. Fiddler
    g. Wireshark
    h. x64dbg
    i. Ghidra
    j. Radare2/Cutter
    k. Cuckoo Sandbox
60. What Happens When a File is Deleted in Windows?
    a. When you delete a file from a standard desktop computer, the file first gets moved to the “recycle bin” or the “trash,” which means only that you've placed the

intact data in a new directory. You erase the file when you empty your recycle bin. But even then, much of the information remains on the hard disk.

61. What is file carving?
    a. File carving is a process used in computer forensics to extract data from a disk drive or other storage device without the assistance of the file system that originally created the file. It is a method that recovers files at unallocated space without any file information and is used to recover data and execute a digital forensic investigation. It is also called “carving,” which is a general term for extracting structured data out of raw data, based on format specific characteristics present in the structured data. https://www.infosecinstitute.com/courses/computer-forensics-boot-camp/?utm_source=resources&utm_medium=infosec%20network&utm_campaign=course%20pricing&utm_content=hyperlink
62. How do you bypass Passwords on a Powered-off Computer? https://robertscocca.medium.com/cracking-windows-hashes-fb0af3108c0a
    a. Remove the hard drive and access the hash files through an external hdd usb device. Use a laptop/desktop that has KALI or the necessary tools to crack hashed passwords.
63. What is steganography?
    a. Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data.
64. What are alternate data streams?
    a. An Alternate Data Stream is a little-known feature of the NTFS file system. It has the ability of forking data into an existing file without changing its file size or functionality. Think of ADS as a ‘file inside another file’. ADS exists in all versions of Microsoft’s NTFS file system, and it has been available since Windows NT was released. It was originally intended to allow for compatibility with Macintosh’s Hierarchical File System (HFS). Currently, all Windows Operating Systems, including the latest Windows 11 OS, supports the ADS feature.
65. What are common tools for anti-forensics?
    a. Steganography Studio
    b. CryptaPix
    c. GiliSoft File Lock Pro
    d. wbStego
    e. Data Stash
    f. OmniHide PRO
    g. Masker
    h. Deep Sound
66. What is metadata and what forensic information does it contain?
    a. In the world of digital forensics, metadata is the data and information that is part of or attached to some other more obvious piece of data. We usually think of

metadata being associated with a particular file. Every file on a computer has some amount of metadata associated with it.

67. What are LNK files?
    a. An LNK file is a shortcut or "link" used by Windows as a reference to an original file, folder, or application, similar to an alias on the Macintosh platform. It contains the shortcut target type, location, and filename as well as the program that opens the target file and an optional shortcut key.
68. What are jump lists?
    a. Jump Lists maintain the records of recently accessed files and folders and group them as per application basis.
69. How do you conduct Linux memory forensics?
    a. Use LiME to acquire memory and dump it to a file
    b. Get Volatility and use it to analyze your memory dump
70. What are some of the challenges in mobile forensics for Android and iOS devices?
    a. Accidental wiping or resetting of data (or intentional wiping or resetting by a suspect, even from a remote location)
    b. Variations in hardware and software platforms and devices that investigators must understand and navigate.
    c. Password protection features, including fingerprint sensors and facial recognition software, that make access to the device a challenge.
    d. The danger of altering data on the device itself by simply powering it on or off, viewing different areas of the phone or background apps making modifications.
    e. Insufficient tools or resources by departments doing the investigating due to the sheer volume of different tools needed.
    f. Built-in security features, such as Android's encryption methods, that can be tricky or time-consuming for investigators to crack.
71. What are some common tools for network and host traffic analysis?
    a. Auvik.
    b. SolarWinds Network Traffic Analysis Tool.
    c. Paessler Network Analysis Tool.
    d. Wireshark.
    e. NetFort LANGuardian.
    f. Manage Engine NetFlow Analyzer.
    g. Nagios.
    h. Icinga.
72. How do you analyze network traffic for SYN flood attacks?
    a. Use of a device that collects network data through a SPAN port. Then using a tool such as Wireshark or Tshark to analyze the packets. Attacks can be limited by newer firewalls.
73. What is a SIEM?
    a. *SIEM* stands for security information and event management and provides organizations with next-generation detection, analytics and response.
    b. SIEM software works by collecting log and event data produced from applications, devices, networks, infrastructure, and systems to draw analysis and

provide a holistic view of an organization's information technology (IT). SIEM solutions can reside either in on-premises or cloud environments.

74. What is an EDR/XDR?
    a. XDR (extended detection and response) collects and automatically correlates data across multiple security layers – email, endpoint, server, cloud workload, and network. This allows for faster detection of threats and improved investigation and response times through security analysis.
75. How do you detect malware activity in network traffic (indicators)?
    a. Unusual outbound network traffic
    b. Anomalies in privileged user account activity
    c. Geographical irregularities
    d. Other log in red flags
    e. HTML response sizes
    f. Mismatched port-application traffic
    g. Suspicious registry or system file changes
    h. Domain Name System request anomalies
    i. Mobile device settings changes
    j. Aggregated data in the wrong place
    k. Web traffic with unhuman behavior
    l. Signs of distributed-denial-of-service (DDoS) attacks
    m. Changes in security rating
    n. Exposed credentials
    o. Changes in vendor security ratings
76. What is a rogue DNS server and how do you detect it?
    a. A rogue DNS server translates domain names of desirable websites (search engines, banks, brokers, etc.) into IP addresses of sites with unintended content, even malicious websites. Most users depend on DNS servers automatically assigned by their ISPs.
77. What is DNS hijacking/spoofing?
    a. DNS spoofing, also referred to as DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record, e.g. an IP address.
78. What are brute force attacks and how do you identify them in forensics?
    a. A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. Hackers work through all possible combinations hoping to guess correctly.
79. What are some common threats/attacks for wireless networks?
    a. Configuration Problems (Misconfigurations or Incomplete Configurations)
    b. Denial of Service
    c. Passive Capturing
    d. Rogue (or Unauthorized/Ad-Hoc) Access Points
    e. Evil Twin Attacks
    f. Hacking of Lost or Stolen Wireless Devices

    g. Freeloading
80. How do you detect a rogue access point?
    a. Rogue access point detection works through sensors and radio frequency. Wireless radios automatically scan the RF spectrum for access points transmitting on the same spectrum. The RF scans can discover third-party transmitters in addition to other radios.
81. How do you detect honeypots?
    a. The machine looks like it was just set up yesterday and the only thing it has on it besides default directories is a folder called "Sensitive" filled with page scans of old copies of 2600 and lists of misspelled names and address purporting to be employees of HB Gary.
    b. The mouse driver has the manufacturer labeled as "Microsoft SMS Solutions"
    c. You try to talk to the drive controller or any other DMA device and the computer begins responding weirdly.
    d. The CPUID op code places value 0x02 in EAX
    e. You do an RDTSC timing on an instruction sequence and the resulting value is some insane number.
    f. You try to make an HTTP connection to cnbc.com and get the error "cannot connect"
    g. The only printers installed on the machine have the word "generic" in their name.
    h. You give the command "net view" and get back the response "The list of servers for this workgroup is not currently available."
82. What is XSS, what are the types of XSS, and how do you identify XSS attacks?
    a. Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.
    b. Reflected XSS -> https://owasp.org/www-community/attacks/xss/#reflected-xss-attacks
    c. Stored XSS -> https://owasp.org/www-community/attacks/xss/#stored-xss-attacks
    d. DOM Based XSS -> https://owasp.org/www-community/attacks/DOM_Based_XSS
83. What is CSRF and how do you identify CSRF attacks?
    a. Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform. It allows an attacker to partly circumvent the same origin policy, which is designed to prevent different websites from interfering with each other.
    b. CSRF attacks can be identified using a Web Application Firewall with specific rules/alerts setup

84. What is a SQL injection attack, what are the types of SQL injection attacks, and how do you identify SQLi attacks?
    a. SQL injection is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution.
    b. SQL injections typically fall under three categories:
        - In-band SQLi (Classic)
        - Inferential SQLi (Blind)
        - Out-of-band SQLi
    c. Detection methods range from checking server logs to monitoring database errors. Most network intrusion detection systems (IDS) and network perimeter firewalls are not configured to review HTTP traffic for malicious SQL fragments, making it possible for an attacker to bypass network security boundaries. Web application firewalls (WAF) can be integrated into security solutions to filter HTTP requests that match SQLi attempts. But a WAF must be continuously updated to filter new techniques.
85. What are the types of command injection attacks?
    a. Command injection is a cyber attack that involves executing arbitrary commands on a host operating system (OS). Typically, the threat actor injects the commands by exploiting an application vulnerability, such as insufficient input validation.
86. How do you identify directory traversal attacks, parameter tampering attacks, command injection attacks, SQLi attacks, cookie poisoning attacks, XML external entity attacks, and Brute Force attacks?
    a. Web application firewall
87. How do you perform forensics on a WordPress website?
    a. Collect Activity Logs
    b. Use of the database files

88. What are some of the challenges in Dark Web Forensics?
    a. The difficulty in analyzing the activity on the dark net is that all of the users and services are anonymous. It is impossible for location or ownership to be established for any computer or person on the darknet, which is incredibly problematic for law enforcement who need to establish jurisdiction in order to act.
89. What are the steps to investigate email crimes?
    a. Email Header Analysis - Email headers contain important information including name of the sender and receiver, the path (servers and other devices) through which the message has traversed, etc. The vital details in email headers can help investigators and forensics experts in email investigation. For instance, the Delivered-To field contains the email address of the recipient and the Received-By field contains the last visited SMTP server's IP address, its SMTP ID, and the date and time at which the email is received. Similarly, the Received: from field may provide key details like IP address of sender and host name. Such information can be instrumental in identifying the culprit and collecting evidence.

b. Email Server Investigation - Email servers are investigated to locate the source of an email. If an email is deleted from client application, sender's or receiver's, then related ISP or Proxy servers are scanned as they usually save copies of emails after delivery. Servers also maintain logs that can be analyzed to identify the address of the computer from which the email originated. It's worth noting that HTTP and SMTP (common messaging initiation protocol) logs are archived frequently by large ISPs. If a log is archived then tracing relevant emails can take a lot of time and effort, as it requires decompressing and extraction techniques. So, it's best to examine the logs as soon as possible lest they are archived.
c. Investigation of Network Devices - In some cases, logs of servers aren't available. This can happen due to many reasons such as when servers aren't configured to maintain logs or when an ISP refuses to share the log files. In such an event, investigators can refer to the logs maintained by network devices such as switches, firewalls, and routers to trace the source of the email message.
d. Sender Mailer Fingerprints - X-headers are email headers that are added to messages along with standard headers like Subject and To. These are often added for spam filter information, authentication results, etc. and can be used to identify the software that's handling the email at the client such as Outlook or Opera Mail. X-originating-IP header can be used to find the original sender, i.e. IP address of the sender's computer.
e. Software Embedded Identifiers - Sometimes, the email software used by a sender can include additional information about the message and attached files in the email. It can be found in MIME content as a Transport Neutral Encapsulation Format (TNEF) or custom header. An in-depth analysis of these sections can reveal vital details related to sender like MAC addresses, Windows logon username of the sender, PST file names, and more.
f. Bait Tactics - Bait tactic is an email investigation technique that's used when the location of a suspect or cybercriminal is unknown. In this, the investigators send an email that contains a http: "<img src>" tag to the suspect. The image source is on a computer that's monitored by the investigators. When the suspect opens the email, the computer's IP address is registered in a log entry on the HTTP server that hosts the image. The investigators can use the IP address to track the suspect

90. How do you collect logs in Azure, AWS, Google Cloud?
    a. AWS
        - Activate Amazon CloudWatch Logs for your instances at the layer level in OpsWorks Stacks.
        - Monitor the logs for your instances in the CloudWatch console.
    b. Azure
        - Access Log Analytics from the Logs option on the Azure Monitor menu or from most other services in the Azure portal.
    c. Google Cloud

        - Google Cloud Console: In the Cloud Console, go to the Logging page. When in the Logs Viewer, select and filter your resource type from the first drop-down list.

91. How do you acquire a virtual machine image/snapshot in Azure, AWS, Google Cloud?
    a. Azure
        - From the Azure Portal, choose the VM to migrate, and then choose Disks. Select each disk (either OS or data) and choose Create Snapshot. On the completed snapshot resource, choose Export. This creates a URL that you can use to download the virtual image.
    b. AWS
        - To *export* your image, use the *export*-image command in your Amazon CLI. The *exported* file is written to the specified S3 bucket using the following S3 key: prefixexport-*ami*-id
    c. Google Cloud
        - You can export your image using either the Google Cloud CLI, or the Cloud Build API. Use the gcloud compute images export command to export your image. Replace the following: IMAGE_NAME : the name of the image to export.
        - https://cloud.google.com/compute/docs/images/export-image
92. How do you acquire a virtual machine snapshot using powershell?
    a. get-vm -location “My Lab” | New-Snapshot -Memory -Quiesce -Name *PrePatch*
    b. When the command above completes you will have a snapshot for each VM located in the “My Lab” folder. Each Snapshot will be named “Prepatch”.
93. How do you collect evidence from a smartwatch?
    a. Most swart watches are encrypted. Evidence can be collected from; third party apps that generate records or in the multiple clouds storing data and communications.
94. How do you collect evidence from Amazon Echo/smart speakers?
    a. Amazon and the owners of the device have to agree to have the recordings pulled from Amazon servers.
95. How do you analyze a suspicious document/pdf for malware?
    a. Reverse engineering the files with one of these tools:
        - IDA Pro
        - Ghidra
        - Binary Ninja
        - Hopper
        - Radare2
96. How do you analyze the behavior of a system when performing dynamic malware analysis (i.e.- monitor Registry for artifacts, monitor processes/services, startup programs, event logs in Windows, API calls, monitoring device drivers, monitoring files and folders, monitoring network ports (open ports), DNS, etc)?
    a. Dynamic analysis—also called malware behavior analysis—runs the malware program to examine its behavior. Of course, running a piece of malware always carries some risk, so dynamic analysis must be performed in a safe environment.

A “sandbox” environment is a virtual system that is isolated from the rest of the network and can run malware without risk to production systems. After the analysis is done, the sandbox can be rolled back to its original state without permanent damage.

97. How would you analyze Emotet malware on a system?
    - Build a VM that does not have access to a network, file sharing disabled.
    - Deploy the malware.
    - Also a service like https://any.run/ can be used.
98. What are common tools you can use for analyzing non-volatile data and volatile data on a system?
    a. FTK Imager
    b. Pro Discover
    c. Win32dd
    d. Nigilant32
    e. Memoryze
    f. Helix3 (dd).
99. What are common tools you can use for forensic analysis of Windows, Linux, and Mac OS systems?
    a. Disk analysis: Autopsy/the Sleuth Kit
    b. Image creation: FTK imager
    c. Memory forensics: volatility
    d. Windows registry analysis: Registry recon
    e. Network analysis: Wireshark
    f. Linux and Mac distributions: CAINE
100. What are native Windows and Linux tools that can be used for forensic and/or malware analysis?
    a. Windows
        - Sysinternals
    b. Linux
        - Htop
        - Tcpdump
        - Perf
        - netstat
101. What are some tools for carving files in Windows?
    a. EVTXtract

       https://github.com/williballenthin/EVTXtract

    b. bulk_extractor

       https://github.com/simsong/bulk_extractor

    c. Scalpel

       https://github.com/sleuthkit/scalpel
102. What are common tools for recovering deleted partitions?

a. MiniTool Partition Wizard Free (How to recover lost or deleted partition)

   https://www.partitionwizard.com/help/partition-recovery.html

b. Piriform Recuva Free

   http://www.piriform.com/recuva

c. AccessData FTK (Forensic ToolKit)

   http://accessdata.com/product-download

d. Testdisk
   http://www.cgsecurity.org/wiki/TestDisk_Download

103. What are common tools you can use for password cracking?
   a. Hashcat
   b. John the Ripper
   c. Brutus
   d. Wfuzz
   e. THC Hydra
   f. Medusa
   g. OphCrack
   h. L0phtCrack
   i. Aircrack-ng - Wifi Cracking
104. What are common tools for steganography detection?
   a. Xstegsecret
   b. StegSecret
   c. StegAlyzerAS
   d. StegAiyzerRTS
   e. StegEx pose
   f. StegAiyzerS5
   g. Steganography Studio
   h. Virtual Steganographic Laboratory (VSL)
   i. Stegdetect
   j. ImgStegano
105. What are common tools for analyzing malware on Windows, Linux and Mac OS?
   a. Radare2
   b. Ghidra
106. How do you enumerate a USB with powershell?
   a. Enter the following command: Get-PnpDevice -PresentOnly | Where-Object { $_.InstanceId -match '^USB' }
107. What are some common tools to perform Windows memory and registry analysis?
   a. Memory - Volatility
      https://www.volatilityfoundation.org/
   b. Registry - RegRipper

108. What are some common tools to examine the cache, Cookie and history recorded in web browsers?
    a. Chrome/Chromium based browsers
        - https://github.com/obsidianforensics/hindsight
        - https://github.com/Tazeg/browserhistory
    b. Firefox/Safari
        - https://www.nirsoft.net/utils/browsing_history_view.html
    c. All browser types
        - https://www.sleuthkit.org/autopsy/
109. What are some common tools to Examine Windows Files and Metadata?
    a. Exiftool
110. What are some common tools to Examine ShellBags, LNK files and Jump Lists?
    a. https://ericzimmerman.github.io
        - JLECmd - Jump List parser
        - LECmd - Parse lnk files
        - JumpList Explorer - GUI based Jump List viewer
        - SBECmd - ShellBags Explorer, command line edition, for exporting shellbag data
111. What are some common tools to Collect Volatile Information on Linux?
    a. Acquire Volatile Memory Linux - https://github.com/microsoft/avml
    b. LiME - https://github.com/504ensicsLabs/LiME
112. What are some common tools to Collect Non-Volatile Information on Linux?
    a. Clone data to a USB device. Mount the drive and access it through a Linux machine.
113. What are some common Linux File system Analysis Tools?
    a. https://www.sans.org/tools/sift-workstation/
    File system support

        - NTFS (NTFS)
        - iso9660 (ISO9660 CD)
        - hfs (HFS+)
        - raw (Raw Data)
        - swap (Swap Space)
        - memory (RAM Data)
        - fat12 (FAT12)
        - fat16 (FAT16)
        - fat32 (FAT32)
        - ext2 (EXT2)
        - ext3 (EXT3)
        - ext4 (EXT4)
        - ufs1 (UFS1)
        - ufs2 (UFS2)
114. What are some common tools to Perform Linux Memory Forensics?

a. LiME (Linux Memory Extractor) Once known as DMD, this is a loadable kernel module which is one of the only available tools which will let you dump full memory captures from Android devices as well as Linux machines.
b. Volatility - It is a memory forensics framework that is capable of analyzing volatile RAM and page files.

115. How do you conduct APFS File System Analysis?
    a. https://cellebrite.com/en/digital-collector/
116. How do you parse metadata on Spotlight?
    a. https://github.com/ydkhatri/spotlight_parser
117. How do you conduct Incident Detection and Examination with SIEM tools?
    a. Collect logs and events from servers and desktops.
    b. Use the information gathered to find where the malware has spread.
118. How do you detect and Investigate Various Attacks on Web Applications?
    a. Static detection techniques
        - Web Server Logs
        - Application Server Logs
        - Web Application's custom audit trail
        - Operating system logs
    b. Dynamic detection technique
        - Web Application Firewall

119. What are some common tools to Identify TOR Artifacts?
    a. A Memory dump tool and hex editor to view TOR artifacts. Nothing is stored on the hard drive besides the browser.
120. What are some common tools to Acquire Memory Dumps?
    a. Windows
        - Process Hacker - https://github.com/processhacker/processhacker
        - Magnet RAM - https://www.magnetforensics.com/resources/magnet-ram-capture/
        - WinPmem - https://github.com/Velocidex/WinPmem/releases
    b. Linux
        - LiME Linux Memory Extractor - https://github.com/504ensicsLabs/LiME
121. What are some common tools to Examine the Memory Dumps?
    a. Redline -https://www.fireeye.com/services/freeware/redline.html
    b. Volatility - https://www.volatilityfoundation.org/
122. What are some common tools to Perform Static Malware Analysis?
    a. Cuckoo sandbox - https://cuckoosandbox.org/
    b. FLARE VM - https://www.mandiant.com/resources/flare-vm-update
123. What are some common tools to Analyze Suspicious Word and PDF documents?
    a. Remnux - https://remnux.org/
124. What are some common tools to conduct dynamic malware analysis on a host system?
    a. Network and service simulation - https://www.inetsim.org/
    b. Analyze Network Files - Wireshark - https://www.wireshark.org/download.html

c. Process monitoring - Process hacker - https://processhacker.sourceforge.io/downloads.php
d. System monitor - https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon
e. Malware Debugging - https://ghidra-sre.org/

125. What are some common tools to conduct dynamic malware analysis on a Network?
    a. Tshark/Wireshark
    b. InsetSim
126. What are some common tools to Perform Logical Acquisition on Android and iOS devices?
    a. iOS - https://libimobiledevice.org/
    b. Android - https://github.com/RealityNet/android_triage
127. What are some common tools to Perform Physical Acquisition on Android and iOS devices?
    a. https://cellebrite.com/wp-content/uploads/2021/12/SolutionOverview_CellebritePremium_LTR_2021_web.pdf
    b. There might be other solutions but rooting the device will be necessary
128. What are some common tools to Collect and Examine the Evidence Files on MSSQL Server?
    a. Along with the Volatile database data, Windows logs and Database plan cache, investigators can examine the following files to have an insight of the activities occurred on the database:
        - Database & logs files: \\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\ DATA*.MDF | *.LDF
        - Trace files: \\Microsoft SQL Server\MSSQL11.MSSQLSERVER \MSSQL\ LOG\LOG_#.TRC
        - SQL Server error logs: \\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\ LOG\ERRORLOG
129. What are some common tools to Acquire Deleted Emails?
    a. Outlook 2013 - Recovering deleted emails from PST file
    b. Outlook 2016 & 2019 - Recovering deleted emails from OST file
    c. Thunderbird - all emails of a particular mailbox are stored in a single MBOX file
    d. Possibility of a local backup if there is a local client e.g. Thunderbird and Outlook
130. What are some common tools to Perform Forensics on IoT devices?
    a. This is a difficult task because IoT devices are all built differently. Depending on the product they may store the data on power off and not cycle the memory often, but this is not a guarantee.
        - Log analysis for network layer
        - Cache and memory analysis for sensing layer
        - Fingerprint collection at the Interface layer