**SECTION A**

**Very Short Answer Questions**

**Attempt all questions (7\*2=14)**

1. **Who is expert witness? What is the role of expert witness?**

An expert witness is a person with specialized knowledge, skills, or experience in a particular field who is called upon to provide testimony in legal proceedings. Their role is to offer an informed opinion to help the court understand complex technical or scientific issues.

1. **Define Chain of custody?**

Chain of custody refers to the documented process that records the sequence of custody, control, transfer, analysis, and disposition of physical or electronic evidence. It ensures the integrity and traceability of the evidence from the time it is collected until it is presented in court.

1. **What is the purpose of encryption? What impact does it have on digital forensics?**

The purpose of encryption is to protect data by converting it into a coded format that can only be accessed by authorized individuals with the decryption key. In digital forensics, encryption can complicate the investigation process by making it difficult to access and analyze the encrypted data without the proper decryption key.

1. **Define digital evidence. List out source of it.**

Digital evidence is any information stored or transmitted in digital form that can be used in a court of law. Sources of digital evidence include computers, mobile devices, network servers, cloud storage, emails, social media, and digital cameras.

1. **What are the characteristics of cloud computing?**

Characteristics of cloud computing include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. These allow for flexible, scalable, and efficient resource usage.

1. **What is Database Forensics? mention some Database Forensics Tools**

Database forensics involves the examination of databases and their metadata to uncover evidence of tampering, unauthorized access, or other malicious activities. Some database forensics tools include:

ApexSQL Audit

DBForge Studio

Redgate SQL Monitor

1. **Define cookies and cache?**

Cookies: Small pieces of data stored by a web browser that track user activity and preferences on websites.

Cache: A storage layer that temporarily holds frequently accessed data to speed up subsequent access to the same data.

**SECTION B**

**Short Answer Questions**

**Attempt any seven (7) questions out of nine (9) questions (7\*8=56)**

1. **What is code of Ethics? Explain Computer forensic investigator should and should not.**

A Code of Ethics is a set of principles and guidelines designed to help professionals conduct their work with integrity, honesty, and fairness. In digital forensics, it ensures that investigators adhere to legal and ethical standards.

A Computer Forensic Investigator should:

* Maintain Integrity: Always act with honesty and integrity, ensuring that all findings are accurate and truthful.
* Follow legal procedures and obtain proper authorization before accessing data.
* Ensure the integrity and confidentiality of the evidence.
* Document all actions taken during the investigation.
* Keep updated with current laws and regulations related to digital forensics.
* Stay Competent: Continuously update their skills and knowledge to keep up with advancements in technology and forensic methods.

A Computer Forensic Investigator should not:

* Alter or tamper with the evidence.
* Share confidential information without proper authorization.
* Use the obtained data for personal gain or unauthorized purposes.
* Exceed their professional competence or qualifications.
* Ignore the legal rights of individuals under investigation.
* Show Bias: Avoid any conflicts of interest or bias in their investigations.

1. **Explain how you will deal with these iterns briefly while you seize.**
   1. **Dealing with powered ON Laptops.**

Capture a screenshot of the current state, if possible.

Disconnect the power supply carefully, preventing loss of volatile data.

Document the state of the laptop, including any open applications.

* 1. **Dealing with powered OFF computer.**

Leave the computer powered off to avoid altering the data.

Label all cables and connections before disconnecting them.

Physically secure the device and transport it to the lab for further analysis.

Note the hardware configuration and any connected peripherals.

* 1. **Dealing with powered ON Computers.**

Photograph or document the current state of the screen.

Consider performing a live capture if volatile data is crucial.

Ensure the computer is disconnected from any network.

Power down the computer following standard forensic procedures, ensuring data preservation.

* 1. **Dealing with networked computers.**

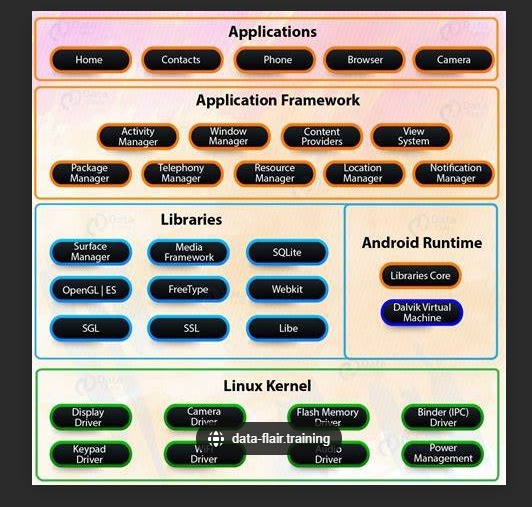
Disconnect the network cable to prevent remote tampering.

Document the network connections and any active sessions.

Capture volatile data, such as active network connections or running processes.

1. **What is Operating System? Explain Android architecture with neat diagram.**

An Operating System (OS) is software that manages hardware and software resources and provides services for computer programs. It acts as an intermediary between the user and the computer hardware, ensuring that applications run smoothly and efficiently.



Applications: Applications are the top layer of the Android architecture. These are the end-user applications that you interact with on your device, such as messaging apps, browsers, games, and social media apps. They are built using the Android SDK and run within the Android runtime environment. [Applications are designed to provide specific functionalities and can be downloaded from the Google Play Store or other sources1](https://play.google.com/store/apps?hl=en_US)[2](https://www.pcmag.com/picks/best-android-apps).

Application Framework: The application framework provides a set of APIs that developers can use to build applications. It includes various services and systems that manage the basic functions of the device. Key components of the application framework include:

* Activity Manager: Manages the lifecycle of applications and provides a common navigation backs tack.
* Content Providers: Manage access to a structured set of data.
* Resource Manager: Provides access to non-code resources such as strings, color settings, and user interface layouts.
* Notification Manager: Allows applications to display alerts and notifications to the user.
* [View System: Provides the building blocks for creating the user interface, including buttons, text fields, and other UI elements](https://play.google.com/store/apps?hl=en_US)[3](https://www.geeksforgeeks.org/android-development-frameworks/)[4](https://devathon.com/blog/top-best-android-frameworks-for-app-development/).

Libraries: Android libraries are collections of pre-written code that developers can use to add functionality to their applications without writing code from scratch. These libraries can include everything from user interface components to networking and database management tools. Examples of popular Android libraries include:

* Retrofit: A type-safe HTTP client for Android and Java.
* Glide: An image loading and caching library.
* [Room: A database library that provides an abstraction layer over SQLite to allow for more robust database access while harnessing the full power of SQLite](https://play.google.com/store/apps?hl=en_US)[5](https://developer.android.com/studio/projects/android-library)[6](https://android-arsenal.com/).

Android Runtime (ART): Executes Android applications..ART is the managed runtime used by applications and some system services on Android. It replaces the older Dalvik runtime and offers several improvements:

* Ahead-of-Time (AOT) Compilation: Compiles apps into native machine code upon installation, improving performance and reducing power consumption.
* Improved Garbage Collection: Enhances memory management and reduces the impact of garbage collection on app performance.
* [Better Debugging Support: Provides more accurate profiling and debugging features](https://play.google.com/store/apps?hl=en_US)[7](https://en.wikipedia.org/wiki/Android_Runtime)[8](https://source.android.com/docs/core/runtime).

Linux Kernel

The Linux kernel is the core of the Android operating system. It provides essential system services such as process management, memory management, and hardware abstraction. The Android kernel is based on the upstream Linux Long Term Supported (LTS) kernel, with additional patches and modifications to support Android-specific features. Key functions of the Linux kernel in Android include:

* Security: Implements security features such as SE Linux to enforce security policies.
* Power Management: Manages power consumption to extend battery life.
* [Hardware Abstraction: Provides a layer of abstraction between the hardware and the software, allowing Android to run on a wide variety of devices](https://play.google.com/store/apps?hl=en_US)[9](https://source.android.com/docs/core/architecture/kernel)[10](https://en.wikipedia.org/wiki/Android_%28operating_system%29).

These components work together to create a robust and flexible platform for developing and running applications on Android devices.

1. **What is Hashing? Explain with example how to obtain a Digital Hash.**

Hashing is a process that converts input data into a fixed-size string of characters, usually a Hash code, through a mathematical algorithm called as hash function. he output, called a "hash value" or "digest," is unique to the original data, meaning even a small change in the input will produce a drastically different hash. Hashing is widely used in digital forensics to verify data integrity, ensure that data has not been altered, and to securely store passwords.

* 1. Command-Line Tools

sha256sum, md5sum, sha1sum: Built-in utilities to generate SHA-256, MD5, and SHA-1 hashes, respectively. Example command:

2. Graphical User Interface (GUI) Tools

* HashMyFiles (Windows): A lightweight tool that can calculate MD5, SHA-1, and SHA-256 hashes for files. You can select files and folders through the interface, and it will generate hashes for them.
* 7-Zip (Windows): Primarily a file compression tool, but it also provides an option to calculate CRC-32, SHA-1, and SHA-256 hashes through its file manager.
  + Right-click a file > Select “CRC SHA” > Choose the desired hashing algorithm.
* HxD (Windows): A hex editor that also offers hashing capabilities for files. It supports MD5, SHA-1, SHA-256, and more.
* HashTab (Windows): A shell extension that adds a "File Hashes" tab to the properties dialog of files, allowing you to view MD5, SHA-1, CRC32, and other hashes.

Steps to Generate a Hash from a File

* Open the File: The file is read in binary mode to ensure that all data is accurately processed, regardless of the file type or content.
* Read the Data: The entire contents of the file are read into memory. For large files, this may be done in chunks to manage memory usage.
* Apply the Hashing Algorithm: A hashing algorithm (such as MD5, SHA-1, SHA-256) processes the file’s data. This algorithm converts the input data into a fixed-size string of characters (the hash).
* Generate the Hash Value: The hashing algorithm produces a hash value, which is a unique string of characters representing the file’s data. Even a small change in the file’s content will result in a completely different hash value.

Example:

Consider a file named document.txt.

Use a tool like SHA256sum to generate a hash.

Command: sha256sum document.txt

Output: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 document.txt

The resulting string is the digital hash, ensuring that if the file changes, the hash will differ.

1. **What are the guidelines for writing a good forensic report?**

* Clarity: Use clear, concise language that is easy to understand, avoiding jargon where possible.
* Accuracy: Ensure all facts and findings are correct, backed by evidence.
* Completeness: Cover all relevant aspects of the investigation, including the methods used, findings, and conclusions.
* Objectivity: Report findings impartially, without bias or opinion.
* structure: Structure the report logically with sections like introduction, methodology, analysis, and conclusion.
* Evidence: Include all supporting evidence, with proper documentation and chain of custody.
* Legal Compliance: Adhere to legal standards and guidelines relevant to the case.
* Summary: Provide an executive summary for quick reference by non-technical readers.

1. **What are common Windows File Systems explain.**

Common Windows File Systems

Windows operating systems support several file systems, each with its own characteristics and use cases. Here are the most common ones:

1. NTFS (New Technology File System)

NTFS is the default file system for modern Windows operating systems.

Features:

* Large File and Volume Support: Can handle very large files and volumes, making it suitable for modern storage needs. File Size Theoretically up to 16 EB (exabytes), practically up to 256 TB and Volume Size Limit: Theoretically up to 256 TB, practically up to 8 PB (petabytes)
* File Permissions and Security: Supports file-level security, permissions, and encryption, enhancing data protection.
* Journaling: Keeps track of changes, which helps in recovering data in case of a system crash.
* [Compression: Allows for file and folder compression to save disk space](https://www.makeuseof.com/ntfs-fat-exfat-windows-10-file-systems-explained/).

1. FAT32 (File Allocation Table 32)

Introduction: An older file system introduced with Windows 95, FAT32 is widely used for compatibility with various devices

Features:

* Wide Compatibility: Works with almost all operating systems, including Windows, macOS, Linux, and many embedded systems.
* [Limitations: Supports a maximum file size of 4GB and a maximum partition size of 8TB, which can be restrictive for modern usage](https://www.makeuseof.com/ntfs-fat-exfat-windows-10-file-systems-explained/)[1](https://www.makeuseof.com/ntfs-fat-exfat-windows-10-file-systems-explained/)[2](https://www.pcmag.com/how-to/fat32-vs-exfat-vs-ntfs-which-format-is-best-for-your-storage-drive). It does not support advanced features like file permissions or encryption.
* [Use Cases: Commonly used for USB flash drives and memory cards due to its compatibility](https://www.makeuseof.com/ntfs-fat-exfat-windows-10-file-systems-explained/).

3. exFAT (Extended File Allocation Table)

* Introduction: Introduced by Microsoft in 2006, exFAT is designed to bridge the gap between FAT32 and NTFS.

File Size Limit: Up to 16 EB

Volume Size Limit: Up to 128 PB

* Features:
  + Large File and Volume Support: Supports larger files and volumes than FAT32, without the overhead of NTFS.
  + Compatibility: Widely supported across different operating systems, making it ideal for external drives and flash storage.
  + [No Journaling: Unlike NTFS, exFAT does not support journaling, which can affect data recovery](https://www.makeuseof.com/ntfs-fat-exfat-windows-10-file-systems-explained/)[1](https://www.makeuseof.com/ntfs-fat-exfat-windows-10-file-systems-explained/)[2](https://www.pcmag.com/how-to/fat32-vs-exfat-vs-ntfs-which-format-is-best-for-your-storage-drive).

4. ReFS (Resilient File System)

* Introduction: Developed by Microsoft to improve upon NTFS, ReFS is designed for high availability and data integrity.

File Size Limit: Theoretically up to 35 PB

Volume Size Limit: Theoretically up to 35 PB

* Features:
  + Data Integrity: Uses checksums to detect and correct data corruption.
  + Scalability: Supports very large volumes and files, making it suitable for large-scale data storage.
  + [Performance: Optimized for performance in specific scenarios, such as virtualized environments](https://www.makeuseof.com/ntfs-fat-exfat-windows-10-file-systems-explained/)[4](https://sysadmin.co.in/windows-file-systems-everything-you-need-to-know/).

1. **What do you mean by web security? Explain how and what security testing tools are used to perform Security testing for Web Applications.**

Web security refers to the practices and measures taken to protect websites and web applications from various threats and vulnerabilities. It involves safeguarding data and resources from attacks that could compromise the confidentiality, integrity, and availability of web applications. Web security aims to prevent unauthorized access, data breaches, and other malicious activities that could impact users or the functionality of the web application.

Key Aspects of Web Security:

* Authentication: Verifying the identity of users accessing the system.
* Authorization: Ensuring users have permission to access specific resources.
* Encryption: Protecting data in transit and at rest to prevent unauthorized access.
* Input Validation: Checking user inputs to prevent injection attacks.
* Session Management: Securing user sessions to prevent hijacking.
* Error Handling: Properly managing errors to avoid revealing sensitive information

Security testing tools are essential for identifying and mitigating vulnerabilities in web applications. Here are some commonly used tools:

OWASP ZAP (Zed Attack Proxy):

* Description: An open-source tool for finding vulnerabilities in web applications.
* Features: Automated scanners, passive scanning, and a variety of tools for manual testing.
* Use Case: Ideal for developers and testers to identify security issues during the development process.

Burp Suite:

* Description: A comprehensive platform for web application security testing.
* Features: Includes tools for scanning, crawling, and exploiting vulnerabilities.
* Use Case: Widely used by security professionals for penetration testing and vulnerability assessment.

Nmap:

* Description: A network scanning tool that helps discover hosts and services on a network.
* Features: Port scanning, service detection, and vulnerability detection.
* Use Case: Useful for mapping the attack surface and identifying open ports and services.

Acunetix:

* Description: A web vulnerability scanner that detects and reports on a wide range of web application vulnerabilities.
* Features: Automated scanning, detailed reports, and integration with CI/CD pipelines.
* Use Case: Suitable for both small developers and large enterprises to ensure web application security.

Wireshark:

* Description: A network protocol analyzer that captures and interacts with network traffic in real-time.
* Features: Deep inspection of hundreds of protocols, live capture, and offline analysis.
* Use Case: Useful for analyzing network traffic and identifying potential security issues.

1. **What is password cracking? Describe password-cracking techniques?**

Password cracking is the process of recovering passwords from data stored or transmitted by computer systems, often used by attackers to gain unauthorized access to systems and data. It can also be employed by security professionals to test the strength of passwords and identify vulnerabilities.

Brute-force attacks involve trying all possible combinations of characters until the correct password is found, which can be very time-consuming. This method guarantees that the password will eventually be discovered, but it can be extremely time-consuming, especially for long and complex passwords. The effectiveness of brute-force attacks is directly related to the length and complexity of the password; the more characters and types of characters (letters, numbers, symbols) involved, the longer the attack will take.

Dictionary attacks use a precompiled list of common passwords and phrases to guess the password, making them faster but less effective against complex passwords that are not included in the dictionary. The success of this technique depends on the quality and comprehensiveness of the dictionary used, which typically includes common passwords, variations, and phrases.

Rainbow table attacks utilize precomputed tables of hash values for all possible password combinations. These tables allow for rapid comparison of hashed passwords to find matches, significantly speeding up the cracking process compared to brute-force methods.

Phishing involves tricking users into revealing their passwords through deceptive emails or websites, relying on social engineering. This technique relies heavily on social engineering, exploiting human trust and error rather than technical vulnerabilities. Phishing attacks can be highly effective if the user is not cautious, as they often mimic trusted entities like banks or online services.

Social engineering manipulates people into divulging confidential information by exploiting psychological manipulation rather than technical hacking. Techniques can include impersonating a trusted individual, creating a sense of urgency, or leveraging social norms to persuade the target to reveal their password. This method bypasses technical security measures entirely, relying on human interaction and psychology. Social engineering is often used in combination with other techniques to gain initial access or gather additional information.

Malware can be used to capture passwords by infecting a user’s device and recording keystrokes or other sensitive information. Keyloggers, a type of malware, record every keystroke made on a device, including passwords. Other types of malware might capture screenshots, steal stored passwords, or exploit vulnerabilities to gain access to password data. The effectiveness of malware depends on its ability to remain undetected and the sophistication of the security measures in place on the target device. Malware attacks can be highly effective but require the attacker to successfully deliver and install the malicious software on the victim’s device.

1. **What is partition? Mention its type and explain each of them.**

A partition is a division of a computer's hard drive into separate sections, each functioning as an independent disk. It allows the operating system to manage information in separate sections. This division helps in organizing data, improving performance, and managing multiple operating systems on a single physical drive. Partitions are essential for setting up a file system and storing data efficiently.

Types of Partitions:

Primary Partition: A primary partition is a bootable partition that can contain an operating system. A hard drive can have up to four primary partitions, or three primary partitions and one extended partition. Typically used to install operating systems. Each primary partition can be set as active, meaning the system can boot from it.

Extended Partition: An extended partition is a special type of partition that can hold multiple logical partitions. Unlike primary partitions, an extended partition itself is not bootable. Only one extended partition is allowed per disk. Used to overcome the limitation of having only four primary partitions. It allows the creation of multiple logical partitions within it, which can be used for data storage.

Logical Partition: Logical partitions are subdivisions within an extended partition. They function like primary partitions but are not bootable. Used for organizing data, such as separating system files from user files, or for different types of data storage (e.g., documents, media files).

**SECTION C**

**Long Answer Questions**

**Attempt any two (2) questions out of three (3) questions (2\*15=30)**

1. **a. What is volatile evidence? How is it useful in computer forensic investigation? Explain the method and tools for capturing volatile data. [10]**

Volatile evidence refers to data that is temporary and can be lost if the power is removed from the device containing it. This type of evidence is often stored in volatile memory (RAM) or other temporary storage locations, such as caches and registers. Examples of volatile evidence include running processes, network connections, system logs, and active user sessions.

Usefulness in Computer Forensic Investigation:

Insight into Current Activity: Volatile evidence provides a snapshot of the system's state at the time of the incident, offering insights into current activities, active processes, and network connections.

Detection of Malware: It can help in identifying malware that is running in memory, which might not be present on the disk.

Uncovering User Actions: It can reveal recent user actions, open files, and running applications, which can be crucial in understanding the context of the incident.

Methods for Capturing Volatile Data:

* Memory Dump: Capturing a complete or partial dump of the system’s RAM to analyze the data later. Tools like DumpIt and Belkasoft RAM Capturer are used to create a snapshot of the system’s RAM, which can then be analyzed for volatile data.
* Network Traffic Capture: Monitoring and capturing network packets to analyze ongoing communication and identify suspicious activities. Tools like Wireshark can capture network traffic in real-time, providing insights into active connections and data transfers.
* Process List and System Information (live response): Collecting information about currently running processes, services, and system configurations. This involves collecting data from a running system without shutting it down. Tools like FTK Imager and Volatility can be used to capture memory dumps and analyze them.
* System Commands: Commands like netstat, ps, and ifconfig can be used to gather information about network connections, running processes, and network interfaces.

Tools for Capturing Volatile Data:

* FTK Imager: Can be used to capture memory images.
* DumpIt: A lightweight tool for creating memory dumps on Windows systems.
* Volatility: An open-source tool used for analyzing memory dumps and extracting information from them.
* Wireshark: Used for capturing and analyzing network traffic.
* Sysinternals Suite (e.g., Process Explorer, TCPView): Useful for examining active processes, network connections, and system information.

1. **b. What are the roles and responsibilities of forensics Investigator?[5]**

* Evidence Collection: Identify, collect, and preserve digital evidence in a manner that maintains its integrity and admissibility in court.
* Analysis: Examine digital evidence to uncover relevant information, detect anomalies, and reconstruct events related to the investigation.
* Documentation: Maintain detailed records of the evidence handling process, including chain of custody, methods used, and findings.
* Collaboration: Working closely with law enforcement, attorneys, and other professionals to build a strong case.
* Reporting: Prepare comprehensive forensic reports that summarize findings, methodologies, and conclusions in a clear and professional manner.
* Testifying: Provide expert testimony in legal proceedings to explain the forensic analysis and the significance of the evidence.

1. **You have been hired as a malware analyst for an organization. Your job is to perform malware analysis for the organization. There are a few scoped machines which have been affected by malware. Consider the different dynamic and static malware analysis techniques you will use to investigate these machines. [15]**

As a malware analyst, my role involves using both static and dynamic analysis techniques to thoroughly investigate the affected machines and understand the nature of the malware.

Static analysis involves examining the malware without executing its code. This method is useful for quickly identifying the malware’s characteristics and potential behavior. Key techniques include:

1. File Fingerprinting: This involves calculating the hash value of the malware file to identify it uniquely. Tools like MD5 and SHA-256 are commonly used for this purpose.
2. Disassembly: Using tools like IDA Pro or Ghidra, you can convert the malware’s binary code into human-readable assembly code. This helps in understanding the malware’s functionality and identifying any malicious instructions.
3. String Analysis: Extracting readable strings from the malware file using tools like Strings can reveal useful information such as URLs, IP addresses, and commands used by the malware.
4. Signature-Based Detection: Comparing the malware’s code against a database of known malware signatures using antivirus tools like ClamAV can quickly identify known threats.
5. [Packer Detection: Identifying whether the malware is packed or obfuscated using tools like PEiD can help in understanding how the malware attempts to evade detection](https://www.bitdefender.com/blog/businessinsights/the-differences-between-static-malware-analysis-and-dynamic-malware-analysis/)[1](https://www.bitdefender.com/blog/businessinsights/the-differences-between-static-malware-analysis-and-dynamic-malware-analysis/)[2](https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/).

Dynamic analysis involves executing the malware in a controlled environment to observe its behavior. This method provides deeper insights into the malware’s actions and interactions with the system. Key techniques include:

1. Sandboxing: Running the malware in a sandbox environment, such as Cuckoo Sandbox, allows you to safely observe its behavior without risking the host system. This can reveal actions like file creation, network connections, and registry modifications.
2. Behavioral Analysis: Monitoring the malware’s behavior using tools like Process Monitor and Wireshark helps in understanding how the malware interacts with the system and network. This can uncover hidden processes, data exfiltration attempts, and other malicious activities.
3. Memory Analysis: Capturing and analyzing the system’s memory while the malware is running using tools like Volatility can reveal hidden code, injected processes, and other in-memory artifacts that are not visible on disk.
4. [Network Traffic Analysis: Observing the network traffic generated by the malware using tools like Wireshark can help identify command and control servers, data exfiltration, and other network-based activities2](https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/)[3](http://www.differencebetween.net/technology/difference-between-static-malware-analysis-and-dynamic-malware-analysis/).

Combining Static and Dynamic Analysis

Combining both static and dynamic analysis techniques provides a comprehensive understanding of the malware. Static analysis helps in quickly identifying known threats and understanding the malware’s structure, while dynamic analysis reveals the actual behavior and impact of the malware on the system. [By using both approaches, you can effectively identify, analyze, and mitigate the malware threat, ensuring the security of the organization’s systems and data1](https://www.bitdefender.com/blog/businessinsights/the-differences-between-static-malware-analysis-and-dynamic-malware-analysis/)[2](https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/).

1. **Suppose a person expressing unrestrained words of hate and malice in Tiktok against the minor girl so what evidence is required to report the cybercrime case and as a cyber-crime investigator, what tasks would you perform to solve the case. [15]**

To report a cybercrime case involving hate speech on TikTok, you need to gather specific evidence:

* Screenshots: Capture screenshots of the offensive content, including the username, date, and time including the exact posts, comments, or videos containing hate speech. Ensure the evidence includes timestamps and any visible user identifiers.
* Video Recordings: Record the videos showing the hate speech.
* Metadata: Collect metadata associated with the posts, such as timestamps and location data.

This can help establish the timeline and context of the offending content. If available, gather details about the devices used to create or access the offensive content, including IP addresses or device identifiers.

* User Information: Collect information about the user posting the content, such as their profile details and any other identifying information.
* Communication Records: If available, gather records of any interactions between the offender and the victim. If the hate speech was communicated through direct messages or private chats, obtain records of these interactions, including message content and sender/receiver details.
* Witness Statements: Collect statements from witnesses who observed the offensive content or interacted with the offender. Obtain a statement from the minor victim or their guardians, detailing the nature and impact of the hate speech.

As a cyber-crime investigator, your tasks would include:

* Evidence Collection and security: Secure and preserve all digital evidence to prevent tampering or loss. Use forensic tools to capture and archive screenshots, videos, and metadata.
* Document Chain of Custody: Maintain a detailed chain of custody for all collected evidence to ensure its integrity and admissibility in court.
* Content Analysis: Examine the offensive content to understand its nature, context, and impact. Assess whether it violates laws or platform policies related to hate speech.
* Profile Analysis: Investigate the offending user’s profile to gather more information about their online behavior and connections.
* Collaboration: Work with TikTok’s legal team and law enforcement to obtain additional information and support. Provide them with evidence of the hate speech and request assistance in identifying the user and taking appropriate action.
* Reporting: Compile a detailed report outlining the findings, including evidence of the hate speech, user identification, and the impact on the victim. Include recommendations for legal action.
* Legal Proceedings: Assist in the legal process by providing expert testimony and supporting the prosecution
* Safety Measures: Advise on measures to enhance the victim’s safety and privacy, such as reporting the incident to the platform, adjusting privacy settings, and avoiding further contact with the offender.