SECTION A

Very Short Answer Questions

Attempt all seven (7) questions [2 × 7 = 14]

**A. What are Bad Sectors?**

Bad sectors are areas on a hard disk drive or other storage devices that are physically damaged or have become unreadable. Data stored in these sectors may be lost or corrupted, and the system may experience errors when trying to access them.

**B. List Different Types of Network Attacks.**

1. **Denial of Service (DoS) Attack:** Overloads a network or system, causing it to become unresponsive.
2. **Man-in-the-Middle Attack:** An attacker intercepts and possibly alters the communication between two parties.
3. **Phishing Attack:** Deceptive attempts to obtain sensitive information by masquerading as a trustworthy entity.
4. **SQL Injection:** Inserting malicious SQL queries into input fields to manipulate or access databases.

**C. What is the Importance of Cybercrime Investigation?**

Cybercrime investigation is crucial for identifying and apprehending perpetrators of online crimes, protecting sensitive data, maintaining the integrity of digital systems, and ensuring that justice is served. It also helps in mitigating damage and preventing future cyber threats.

**D. What is the Difference Between Threat, Vulnerability, and Attack?**

* **Threat:** A potential danger that could exploit a vulnerability to cause harm, such as malware or hackers.
* **Vulnerability:** A weakness in a system that can be exploited by a threat, like outdated software or weak passwords.
* **Attack:** The actual act of exploiting a vulnerability, such as launching malware or a phishing scam.

**E. Explain the Function of SQL Server Management Studio (SSMS).**

SQL Server Management Studio (SSMS) is a tool used to configure, manage, and administer all components within Microsoft SQL Server. It provides a graphical interface for running queries, designing databases, and performing administrative tasks such as backing up and restoring databases.

**F. Original Evidence Should NEVER Be Used for Analysis. Provide Your Thought Process for Agreement or Disagreement.**

**Agreement:** Original evidence should never be used for analysis to preserve its integrity and admissibility in court. Working on copies ensures that the original data remains unaltered and intact, avoiding any potential tampering or contamination.

**G. Mention Some Cloud Computing Threats.**

1. **Data Breaches:** Unauthorized access to sensitive data stored in the cloud.
2. **Insecure APIs:** Vulnerabilities in cloud service APIs that can be exploited by attackers.
3. **Data Loss:** Accidental or malicious deletion of data without adequate backup.

**Account Hijacking:** Unauthorized access to cloud accounts through phishing or weak credentials.

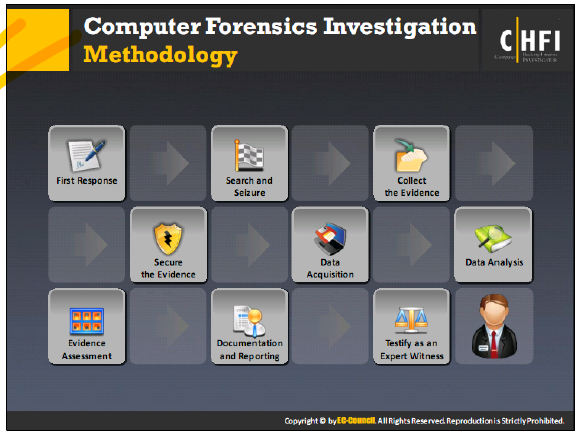
SECTION B

Short Answer Questions

Attempt only seven (7) questions out of eight (9) questions [7 × 8 = 56]

Q. 1   (Unit 1: Forensic Science)

Explain the basic steps of the Digital Forensic Investigation Process?



Q. 2    (Unit 1: Forensic Science)

You are taking an interview of forensics investigators to hire in your organization, what are

the different traits, roles, and responsibilities you will search on him/her during the

Process?

 **Traits:**

* **Attention to Detail:** A forensic investigator must be meticulous, noticing minor details that could be crucial.
* **Integrity and Ethics:** High ethical standards are essential as the investigator deals with sensitive and potentially incriminating information.
* **Analytical Thinking:** Ability to analyze complex data and situations to draw logical conclusions.
* **Communication Skills:** Clear communication is crucial for explaining technical findings to non-technical stakeholders, including in court.

 **Roles:**

* **Evidence Collection:** The investigator must be skilled in gathering digital evidence without compromising its integrity.
* **Analysis:** Expertise in analyzing various forms of digital data, including logs, emails, and files.
* **Reporting:** Ability to prepare comprehensive and understandable reports that can be used in legal proceedings.
* **Testimony:** Serve as an expert witness, providing testimony in court about the findings and methods used in the investigation.

 **Responsibilities:**

* **Maintaining Chain of Custody:** Ensuring that evidence is handled properly to maintain its admissibility in court.
* **Using Forensic Tools:** Proficiency with tools such as EnCase, FTK, or Autopsy for analyzing digital evidence.
* **Staying Updated:** Keeping up with the latest trends and threats in cybercrime and digital forensics techniques.
* **Collaboration:** Working with law enforcement, legal teams, and other stakeholders during an investigation.

Q. 3   (Unit 2: Regulations, Policies, and Ethics)

You have hired a digital forensics expert for setting up a computer forensic Lab. Briefly

describes different items that you will take into account and build a computer forensic Lab.

 **Forensic Workstations:** High-performance computers equipped with forensic software for analyzing digital evidence.

 **Write Blockers:** Devices that prevent data from being altered on storage media during analysis.

 **Secure Storage:** Safes or locked cabinets for storing digital evidence to maintain its integrity and chain of custody.

 **Forensic Software:** Licenses for industry-standard forensic tools like EnCase, FTK, and X-Ways Forensics.

 **Network Analysis Tools:** Tools such as Wireshark or NetFlow analyzers for investigating network-related crimes.

 **Imaging Tools:** Devices and software for creating bit-by-bit copies of storage media, ensuring exact replicas of original data.

 **Clean Room:** A dust-free environment for handling and analyzing sensitive hardware, such as damaged hard drives.

 **Training and Documentation:** Continuous training for staff on the latest forensic techniques and maintaining thorough documentation of all procedures.

Q. 4 (Unit 2: Regulations, Policies, and Ethics)

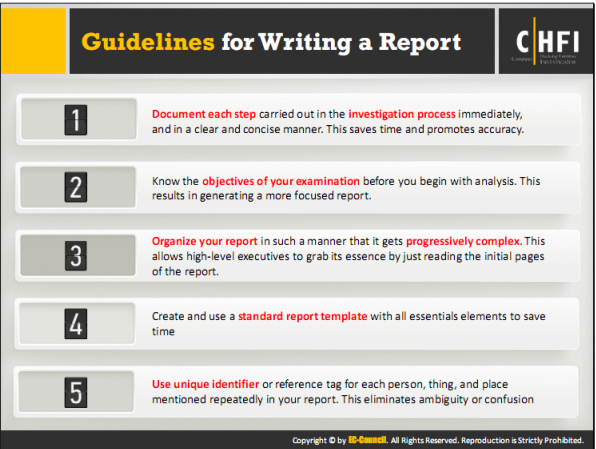
Explain different steps that are involved while performing an investigation of email crimes

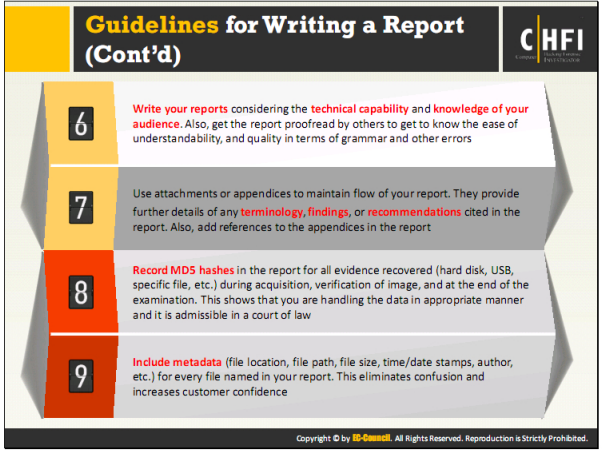
and violations.



Q. 5 (Unit 2: Regulations, Policies, and Ethics)

What are the guidelines for writing a good forensic report?



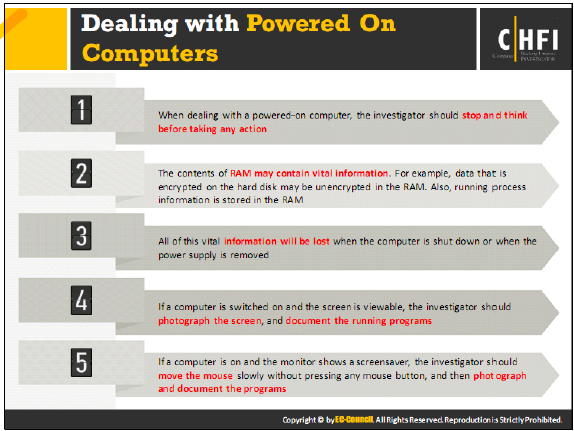


Q.6 (Unit 3: Digital Evidence)

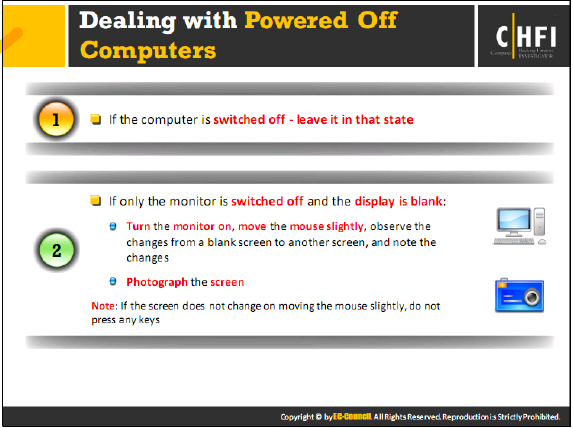
When you are conducting a forensics investigation explain how you will deal with these

items briefly

● Dealing with powered on computers



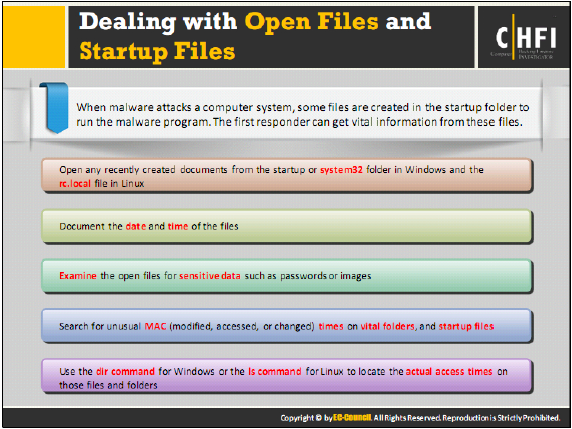
● Dealing with powered off computers



● Dealing with networked computers



● Dealing with network open and startup files



Q.7( Unit 4:Procedure and Methodology)

Why is chain of custody important? Explain what happens when a chain of custody is

Broken?

 **Importance:**

* **Legal Admissibility:** The chain of custody ensures that the evidence presented in court is the same as when it was first collected, preserving its integrity.
* **Accountability:** It provides a clear record of who handled the evidence, when, and under what conditions, which is crucial in legal proceedings.
* **Protection Against Tampering:** A well-maintained chain of custody reduces the risk of evidence tampering, loss, or contamination.

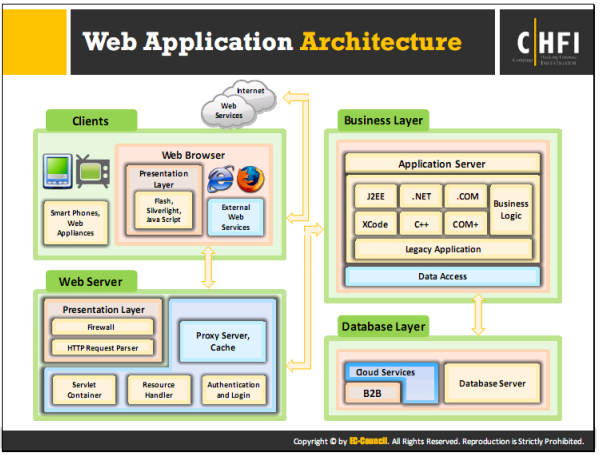
 **Consequences of a Broken Chain of Custody:**

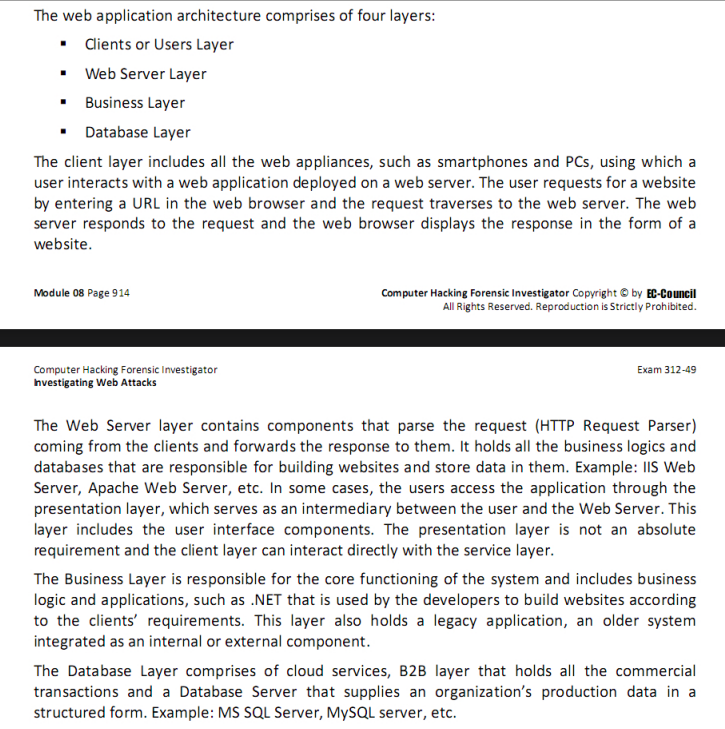
* **Evidence Exclusion:** If the chain of custody is broken, the evidence may be deemed inadmissible in court, potentially weakening the case.
* **Legal Challenges:** Opposing counsel may challenge the validity of the evidence, arguing that it could have been tampered with or altered.
* **Loss of Credibility:** The integrity of the investigation and the credibility of the forensic examiner may be called into question, undermining the overall investigation.

Q. 8   ( Unit 5:Digital Forensics)

Explain Web Application Architecture. Why log is important in forensic investigation?

Explain with some log files stored in apache web server.





 **Importance of Logs in Forensic Investigation:**

* **Activity Tracking:** Logs provide a record of all actions taken on a system, including user activities, errors, and system events, which are crucial for reconstructing incidents.
* **Evidence Collection:** Logs can serve as evidence in identifying unauthorized access, data breaches, and other malicious activities.
* **Incident Response:** Logs help in detecting and responding to security incidents by providing real-time or near-real-time information.

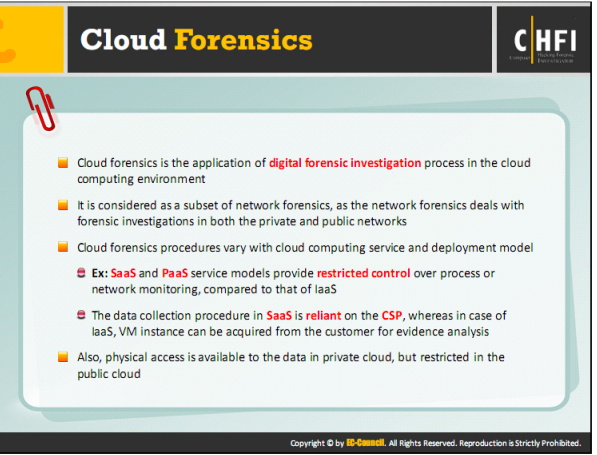
 **Apache Web Server Logs:**

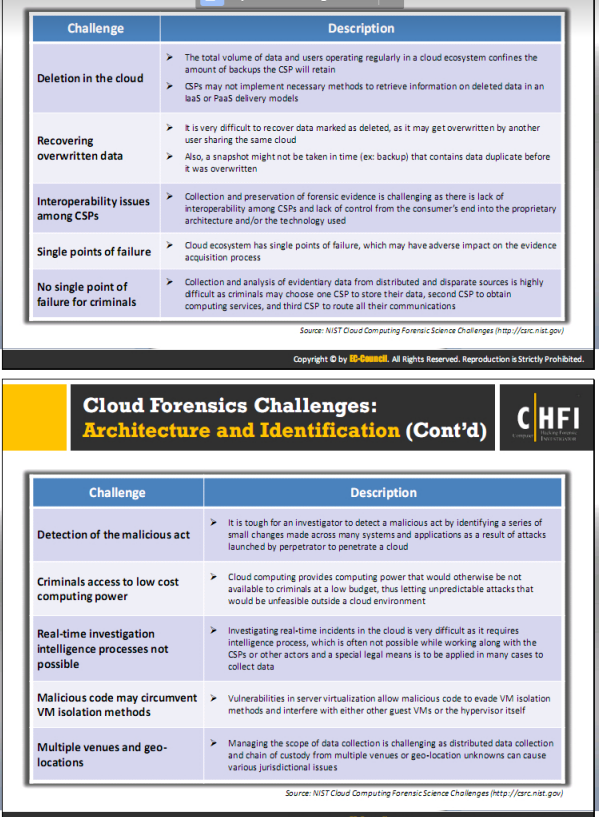
* **Access Logs:** Record every request made to the server, including IP address, request type, response status, and user-agent.
* **Error Logs:** Document any errors encountered by the server, such as failed requests, server crashes, or application errors.
* **Custom Logs:** Can be configured to capture specific events or data, depending on the server's configuration needs.

Q. 9  (Unit 5:Digital Forensics)

What do you understand about cloud forensics and describe different challenges that are

faced by investigators while performing cloud forensics?





Group C

Long Analytical or Case Question

Attempt any two (2) questions out of three (3) questions [2 × 15 = 30]

Q. 1  (Unit 1: Forensic Science,Unit 2: Regulations, Policies, and Ethics, Unit 3: Digital

Evidence,Unit 4:Procedure and Methodology, Unit 5:Digital Forensic)

Suppose you were recently hired for a new position as the computer forensics specialist at

a medium sized communications company. You have been asked to prepare a presentation

to the BOD on your main duties for the company and how your position could help achieve

business goals based on security and confidentiality. You are also aware that the company

has just had some issues with employee complaints of ongoing sexual harassment over

email and instant messaging systems but has been unable to obtain adequate evidence of

any kind.

A. Explain the basic primary tasks, high – level investigation processes, and challenges

of a computer forensics specialist.

1. **Primary Tasks:**
   * **Evidence Collection:** Gathering digital evidence from various sources like computers, emails, networks, and storage devices.
   * **Analysis:** Examining the collected evidence using specialized tools to uncover relevant information.
   * **Reporting:** Documenting findings in a clear, concise manner for use in legal proceedings or internal investigations.
   * **Preservation:** Ensuring that evidence is preserved in its original state to maintain its integrity throughout the investigation.
2. **High-Level Investigation Processes:**
   * **Identification:** Determine what digital evidence is relevant to the case.
   * **Collection:** Securely collect the evidence, ensuring that it is not altered during the process.
   * **Preservation:** Maintain the integrity of the evidence through secure storage and documentation.
   * **Analysis:** Use forensic tools to examine the evidence, looking for relevant data, patterns, and connections.
   * **Reporting:** Compile a report that presents the findings in a clear and legally admissible format.
3. **Challenges:**
   * **Encryption:** Dealing with encrypted data that may be inaccessible without proper keys.
   * **Data Volume:** Managing large volumes of data that require extensive processing time.
   * **Volatile Data:** Capturing data that may be lost if the system is powered down or altered.

**Legal Constraints:** Navigating legal issues, such as jurisdiction and privacy concerns, that can impact evidence collection and analysis.

B. Provide an overview of how computing devices are used in crimes of today and how

these crimes can affect a company data and information.

1. **Use of Computing Devices in Crimes:**
   * **Phishing Attacks:** Criminals use emails to deceive employees into providing sensitive information or clicking on malicious links.
   * **Insider Threats:** Employees may misuse their access to company systems to steal or alter data.
   * **Data Breaches:** Hackers can exploit vulnerabilities in company systems to gain unauthorized access to sensitive information.
   * **Social Engineering:** Criminals manipulate employees into divulging confidential information.
2. **Impact on Company Data and Information:**
   * **Data Loss:** Breaches can lead to the loss of sensitive customer or company data.
   * **Financial Loss:** Cybercrimes can result in significant financial losses due to fraud, theft, or fines.
   * **Reputation Damage:** Data breaches and cybercrimes can severely damage a company’s reputation, leading to loss of customer trust.
   * **Operational Disruption:** Cyberattacks can disrupt business operations, leading to downtime and productivity loss.

C. Discuss how computer forensics investigations pertain the law and trying of cases.

(5+5+5)

1. **Legal Relevance:**
   * **Admissibility:** Digital evidence must be collected and preserved in a manner that ensures it is admissible in court.
   * **Compliance:** Investigations must comply with laws and regulations regarding data privacy, evidence handling, and cybersecurity.
2. **Investigation Pertaining to Law:**
   * **Chain of Custody:** Maintaining a clear record of evidence handling to ensure its integrity and admissibility in legal proceedings.
   * **Forensic Reports:** Providing clear, detailed, and accurate reports that can be used by legal teams to build a case.

**Collaboration with Law Enforcement:** Working closely with legal authorities to ensure that all actions are legally justified and that evidence can be used effectively in court.

Q.2 (Unit 4:Procedure and Methodology)

You are working as a forensics investigator expert at MNO college. You have been recently

onboarded last week. All of sudden you come across a situation where you have to perform

a computer forensics investigation process. Describe briefly the methodology of the

computer forensics investigation you will go through to handle the incident. (15)

1. **Identification:**
   * **Incident Identification:** Identify the scope and nature of the incident. Determine what digital assets (e.g., computers, networks, storage devices) are involved.
   * **Stakeholder Communication:** Notify relevant stakeholders and establish a communication plan.
2. **Preparation:**
   * **Tool Selection:** Select appropriate forensic tools and resources based on the type of incident.
   * **Legal Preparation:** Ensure that you have the necessary legal authorization to collect and analyze evidence.
3. **Evidence Collection:**
   * **Securing the Scene:** Secure the affected area to prevent tampering or loss of evidence.
   * **Data Acquisition:** Collect volatile and non-volatile data from the affected systems. This may include memory dumps, disk images, and network logs.
   * **Chain of Custody:** Document every step in the evidence collection process, ensuring a clear chain of custody.
4. **Preservation:**
   * **Data Integrity:** Store collected data in a secure, unaltered state. Use hashing techniques to ensure data integrity.
   * **Secure Storage:** Ensure that all evidence is securely stored, with access restricted to authorized personnel only.
5. **Analysis:**
   * **Data Examination:** Use forensic tools to analyze the collected data. Look for signs of tampering, unauthorized access, or malicious software.
   * **Correlation:** Correlate evidence from different sources to build a comprehensive understanding of the incident.
   * **Reporting Findings:** Document findings in a clear and concise manner, suitable for both technical and non-technical audiences.
6. **Reporting:**
   * **Forensic Report:** Prepare a detailed report outlining the investigation process, findings, and conclusions. Include any recommendations for preventing future incidents.
   * **Legal Collaboration:** Work with legal teams to ensure that the report meets all legal requirements and can be used effectively in court if necessary.
7. **Presentation of Evidence:**
   * **Court Testimony:** If required, prepare to present evidence and testify in court as an expert witness.

**Stakeholder Briefing:** Provide a debrief to stakeholders, outlining the incident, findings, and recommended actions.

Q.3 (Unit 3: Digital Evidence)

You have been hired as a malware analyst for an educational organization. Your job is to

perform malware analysis for the organization. There are a few scoped machine which has

been affected by malware. What different dynamic and static malware analysis techniques

you will use to investigate these machines. (8+7)

**Dynamic Malware Analysis:**

* **Definition:** Dynamic analysis involves running the malware in a controlled environment to observe its behavior in real-time.
* **Sandboxing:** Execute the malware in a sandboxed environment to monitor its actions without risking the system.
* **Behavior Monitoring:** Track the malware's interactions with the file system, network, registry, and other system components.
* **Network Traffic Analysis:** Capture and analyze network traffic generated by the malware to detect any malicious communication.
* **API Calls Observation:** Monitor API calls made by the malware to understand how it interacts with the operating system and software.

**Static Malware Analysis:**

* **Definition:** Static analysis involves examining the malware's code without executing it.
* **Disassembly:** Use a disassembler to convert the malware's binary code into human-readable assembly code.
* **String Analysis:** Search for readable strings within the malware code, which might provide clues about its functionality or origin.
* **File Structure Analysis:** Examine the structure of the malware file, including headers, sections, and resources.
* **Signature Matching:** Compare the malware's code against known malware signatures using antivirus or specialized tools to identify common traits or previously known variants.
* **Hashing:** Generate hashes of the malware file to compare with known malicious files in databases.