**What is Malware Analysis?**

[Malware](https://www.crowdstrike.com/cybersecurity-101/malware/) analysis is the process of understanding the behavior and purpose of a suspicious file or URL. The output of the analysis aids in the detection and mitigation of the potential threat.

The key benefit of malware analysis is that it helps [incident responders](https://www.crowdstrike.com/cybersecurity-101/incident-response/) and security analysts:

* Pragmatically triage incidents by level of severity
* Uncover hidden indicators of compromise (IOCs) that should be blocked
* Improve the efficacy of IOC alerts and notifications
* Enrich context when [threat hunting](https://www.crowdstrike.com/cybersecurity-101/threat-hunting/)

## Types of Malware Analysis

The analysis may be conducted in a manner that is static, dynamic or a hybrid of the two.

### **Static Analysis**:

### Basic static analysis does not require that the code is actually run. Instead,**static analysis examines the file for signs of malicious intent**.

### It can be useful to identify malicious infrastructure, libraries or packed files.

### Technical indicators are identified such as file names, hashes, strings such as IP addresses, domains, and file header data can be used to determine whether that file is malicious.

### Code Disassembly: Use disassemblers like IDA Pro, Ghidra, or Radare2 to convert machine code into assembly language for manual analysis.

### String Analysis: Identify and analyze strings within the binary, including hardcoded IP addresses, URLs, encryption keys, and other relevant information.

Tool: Flare VM, pestudio

### **Dynamic Analysis**: **Dynamic malware analysis executes suspected malicious code in a safe environment called a sandbox.** This closed system enables security professionals to watch the malware in action without the risk of letting it infect their system or escape into the enterprise network.

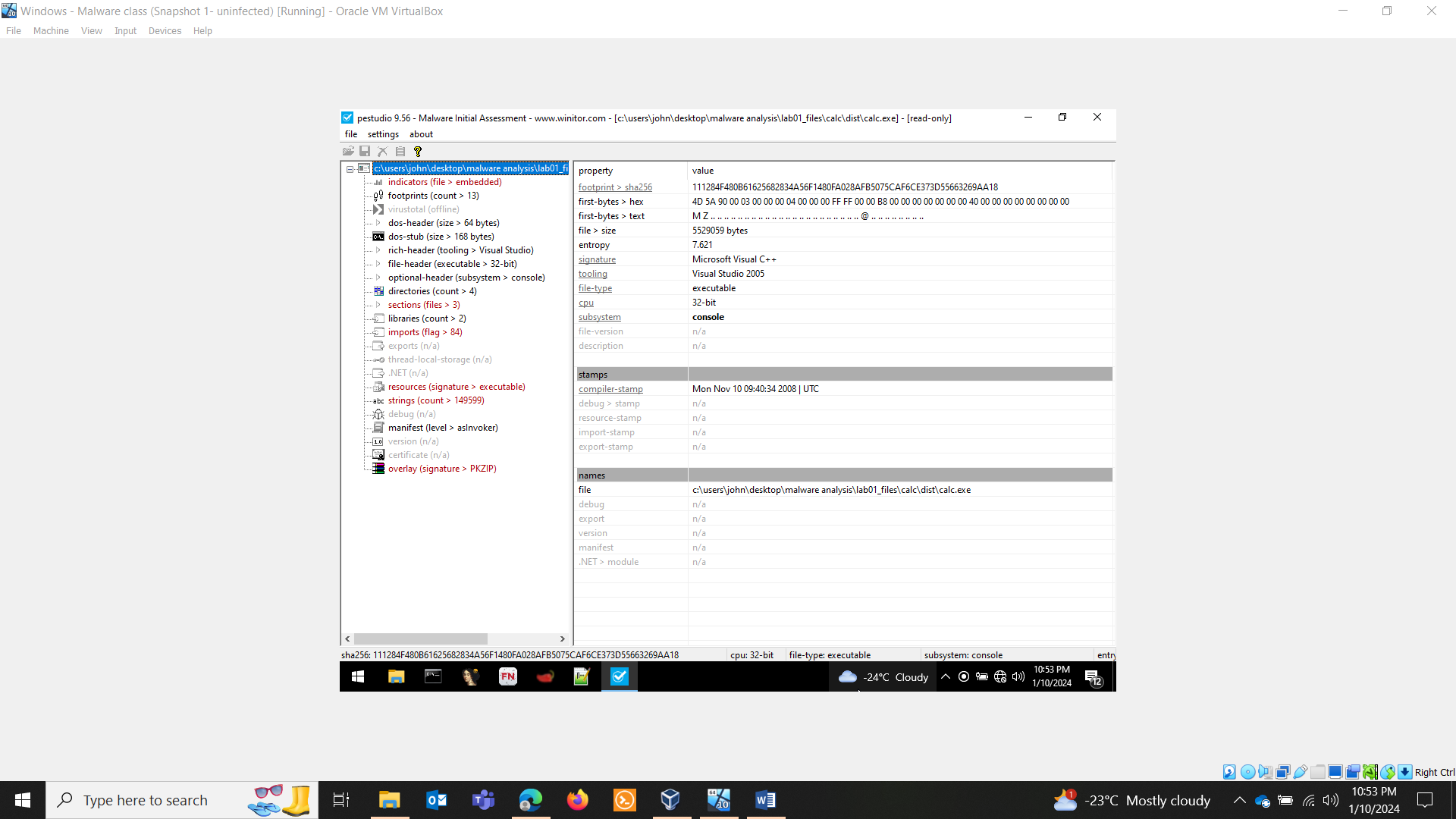
Example: Sandbox:cuckoo

FILE ANALYSIS:

File analysis in static analysis involves examining the characteristics and content of a malware file without executing it. This method helps analysts understand the file's structure, identify potential indicators of compromise (IoCs), and gather information about the malware's behavior. Here are key aspects of file analysis in static malware analysis:

* File Header Analysis: Examine the file header to gather information about the file format, such as the file type, version, and architecture. Malware authors may manipulate headers to evade detection.
* File Size and Entropy: Analyze the file size and entropy to identify anomalies. Unusually large or small file sizes or irregular entropy may indicate obfuscation or packing.
* Strings Analysis: Extract and analyze ASCII and Unicode strings embedded within the binary. This can reveal hardcoded IP addresses, URLs, registry keys, and other information that may be critical for understanding the malware's functionality.
* Checksums and Hash Values: Calculate and compare checksums (MD5, SHA-1, SHA-256) and hash values to identify known malware samples or detect changes in the file over time.
* Resource Analysis: Examine embedded resources such as images, icons, or configuration files. Malware might hide components within these resources.
* File Type Verification: Confirm that the file type matches the expected format. Some malware may use file extensions to masquerade as legitimate files.
* Check for Known Vulnerabilities: Identify whether the file exploits known vulnerabilities. This is particularly important for analyzing files that may serve as vectors for attacks.
* File Compression and Encryption: Determine whether the file is compressed or encrypted. Some malware may use encryption to conceal its true nature.

PESTUDIO:



STRING ANALYSIS:

* Use tools like strings command in Linux/Unix or dedicated binary analysis tools to extract ASCII and Unicode strings from the malware binary.
  + Command:
    - strings malware.exe | grep http
    - strings malware.exe > output.txt
    - Decode the string.
    - Identify C2C servers.
  + You can use grep command or findstr command if you are targeting a keyword.

**Network Traffic Analysis**: Monitor network communications to identify communication patterns, command and control servers, and data exfiltration.