Malware Analysis Proof of Concept (PoC)

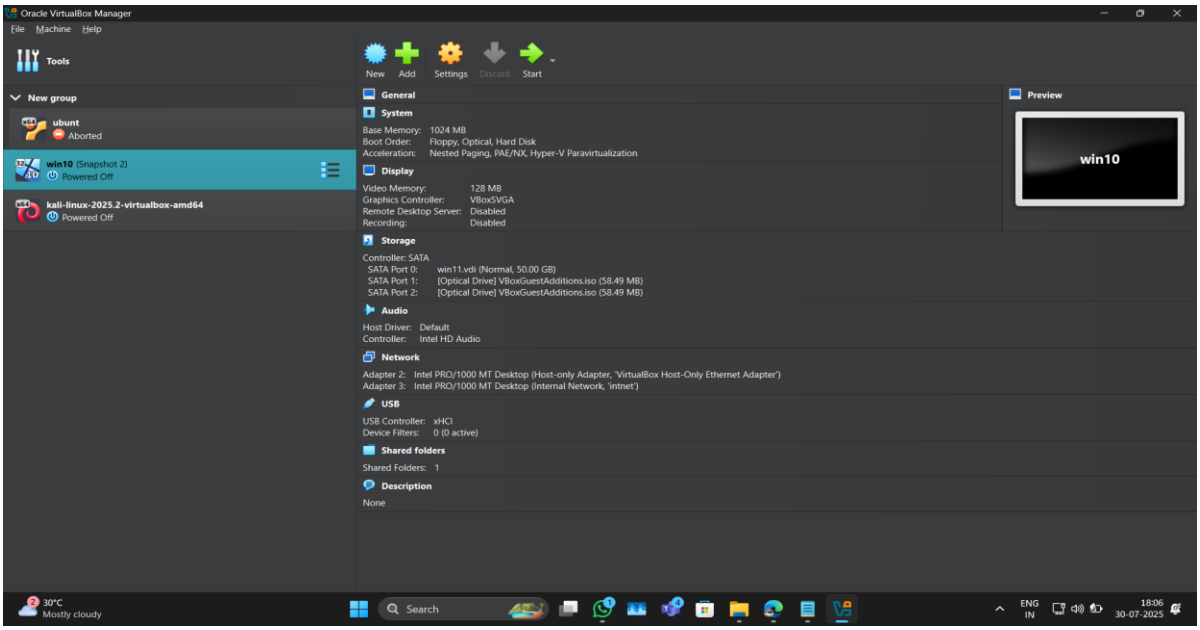
Lab Setup

Isolated Lab Environment:

1. **Host OS:** Windows 10 64-bit (for virtualization and sharing tools)
2. **VM Software:** Oracle VirtualBox
3. **VM1 (Attacker):** Kali Linux
4. **VM2 (Victim):** Windows 10 32-bit (Isolated and without internet)

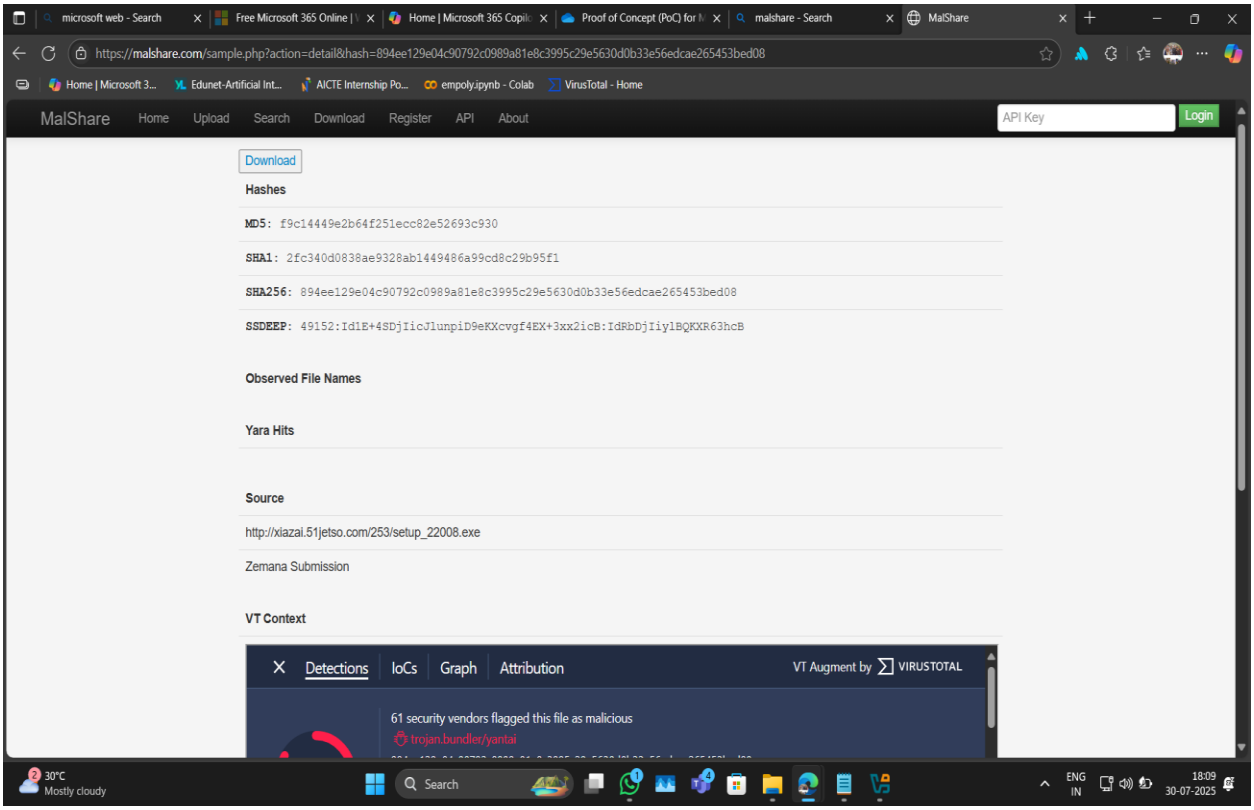
Steps:

- Install Oracle VirtualBox
- Create VM for Kali Linux
- Create VM for Windows 10 32-bit
- Setup **Host-Only Adapter** on both machines for internal communication



Malware Sample Acquisition

1. Go to malshare.com
2. Search for hash:
   `894ee129e04c90792c0989a81e8c3995c29e5630d0b33e56edcae265453bed08`
3. Download file (saved as `.vir` extension)



4. Start Python server in Kali:

```
python3 -m http.server 8888
```

5. On Win10 VM:
   a. Open browser > http://<Kali-IP>:8888
   b. Download malware sample

Tools Setup

Tools to Use (All downloaded in Host Windows):

- Autoruns
- Process Explorer
- Process Monitor
- RegShot
- DIE (Detect It Easy)
- Resource Hacker
- Strings (Sysinternals)
- TDSSKiller
- WinHex

Note: all tools zip file - https://github.com/Nikhil2604Saini/Digisuraksha-parhari-foundation/tree/main/Cybersecurity-Internship-Program-2025/Week-2_Malware-IOC-APT28/Malware-Reports/malware%20analysis%20tool

Share Tools:

- Go to VirtualBox settings
- Devices > Shared Folder > Add tools folder as shared
- Access from `Z:` drive or `\\VBOXSVR\\<folder>` in VM

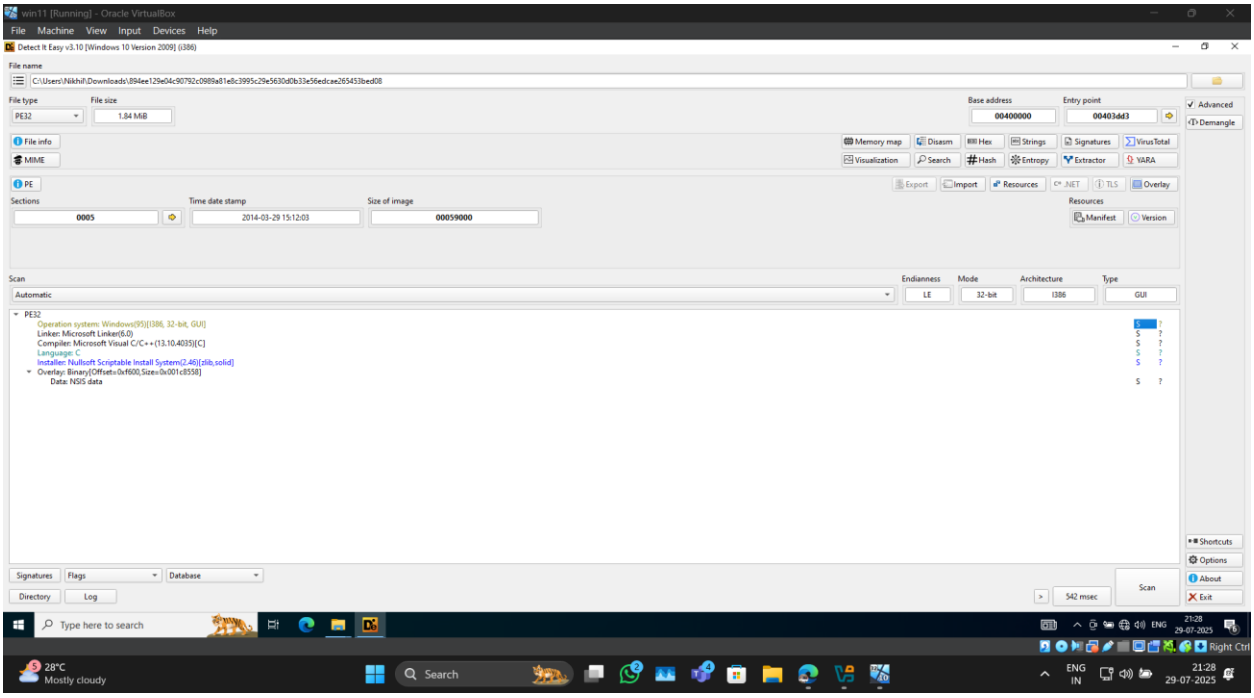
Static Analysis

Tools Used, Explanation and Steps:

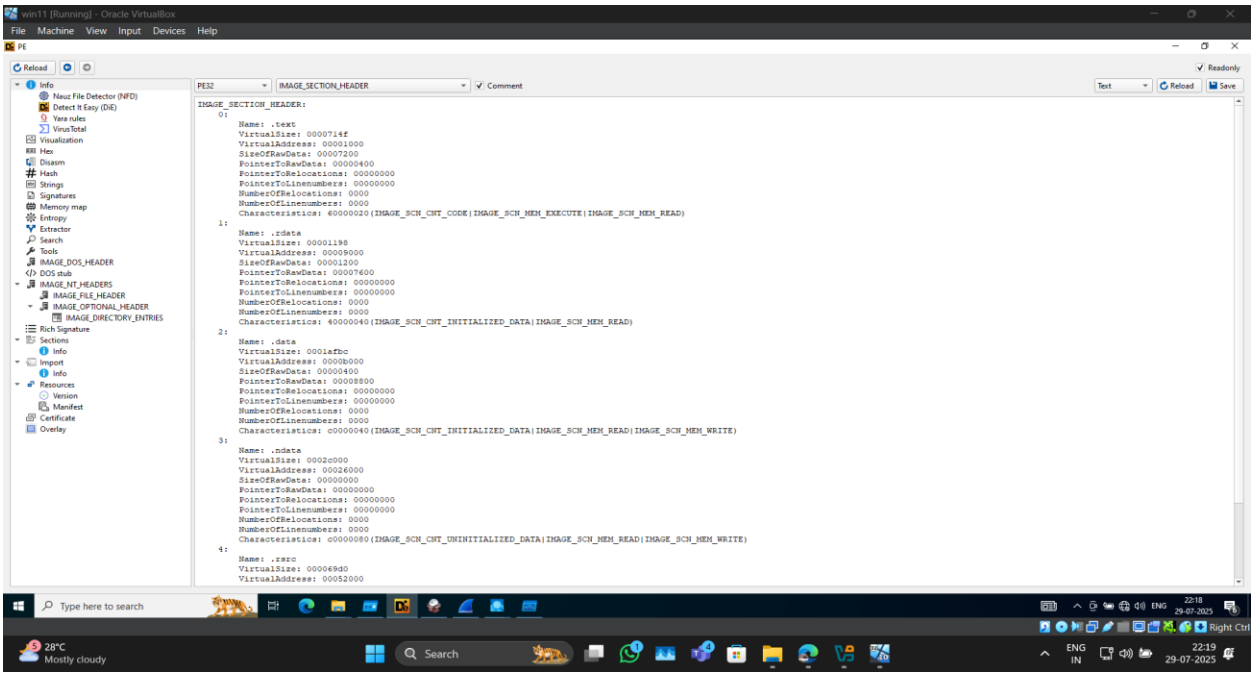
1. **DIE (Detect It Easy):**
    a. Purpose: Identifies if a binary is packed or obfuscated, shows compiler info.
    b. Steps:
        i. Open DIE.
        ii. Click 'File' > 'Open' and select malware `.exe`.
        iii. Review file type, entropy, packer and compiler info.

c. What We Learn: Detects packers (e.g., UPX), entropy (high = encrypted), compiler used.

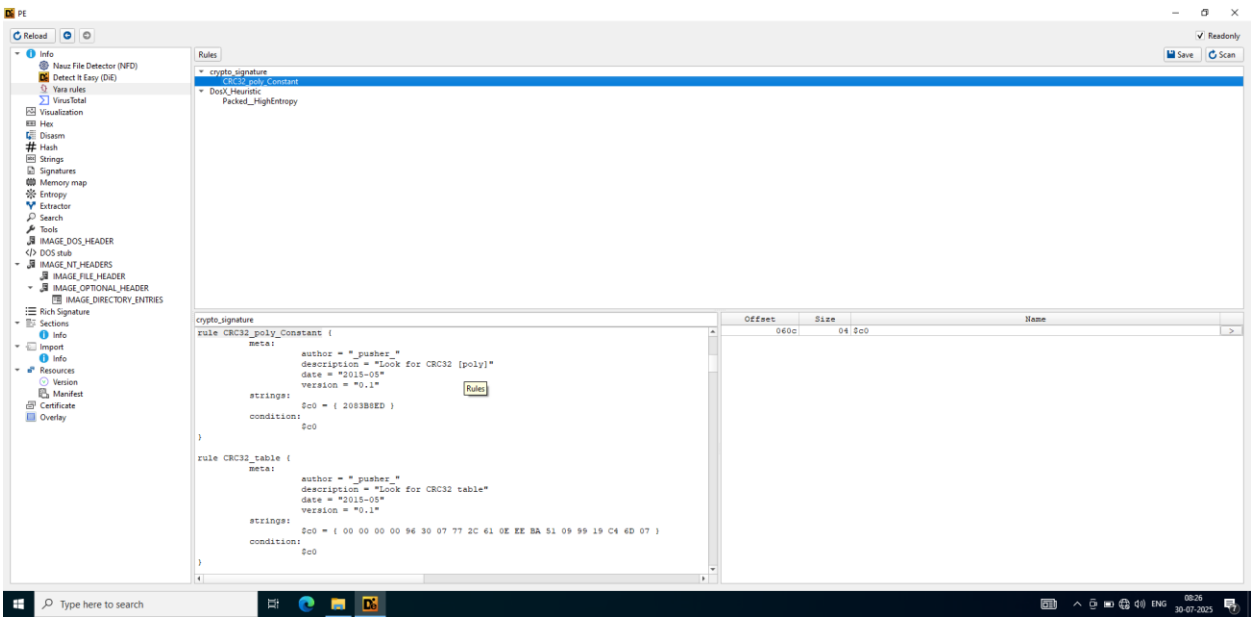
1.File Information(file type: PE32, Bass add.:00400000 , Entry point: 00403dd3)



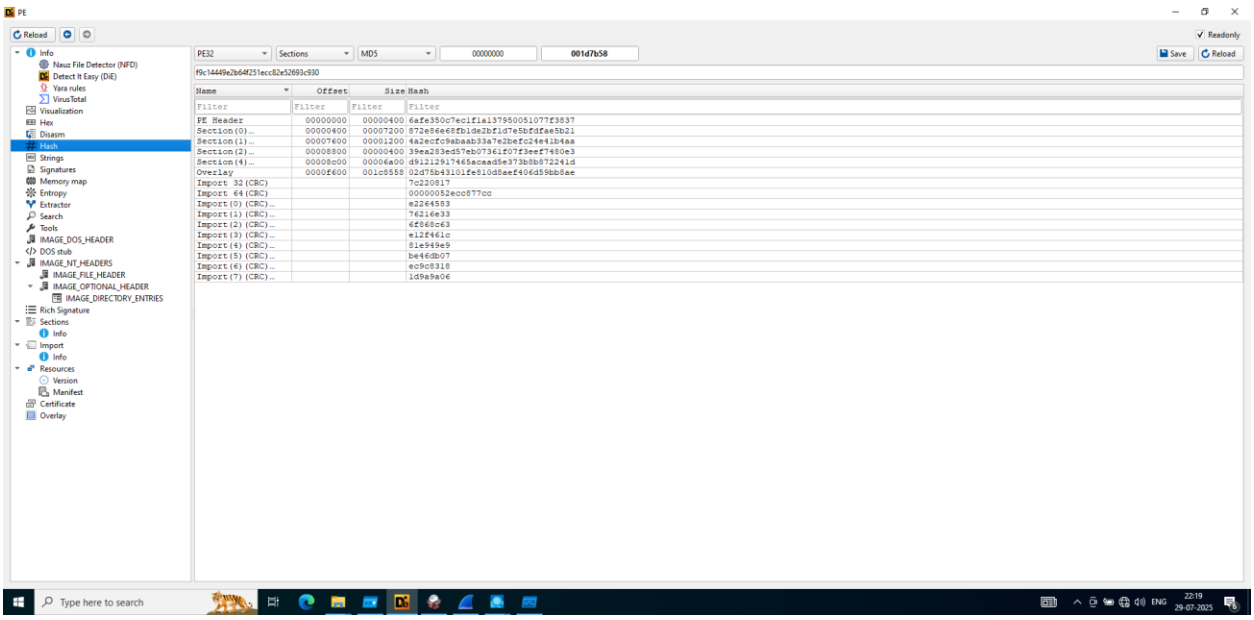
2.Section Header (.text, .rdata, .data, .ndata, .rsrc).



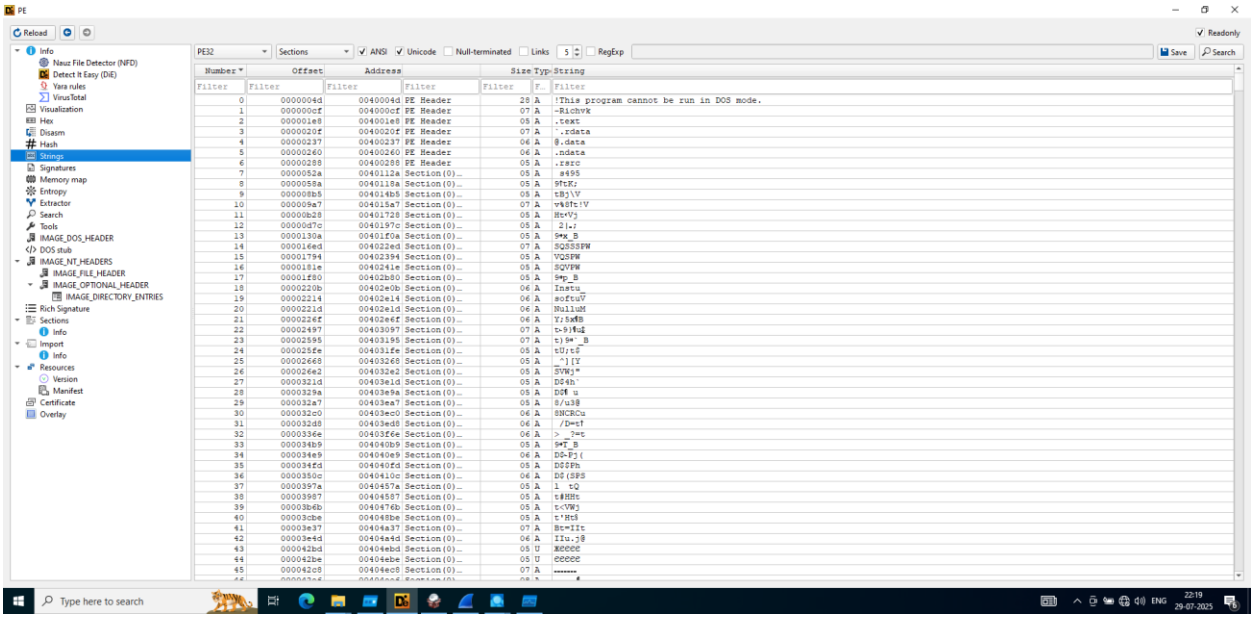
3.Yara rule



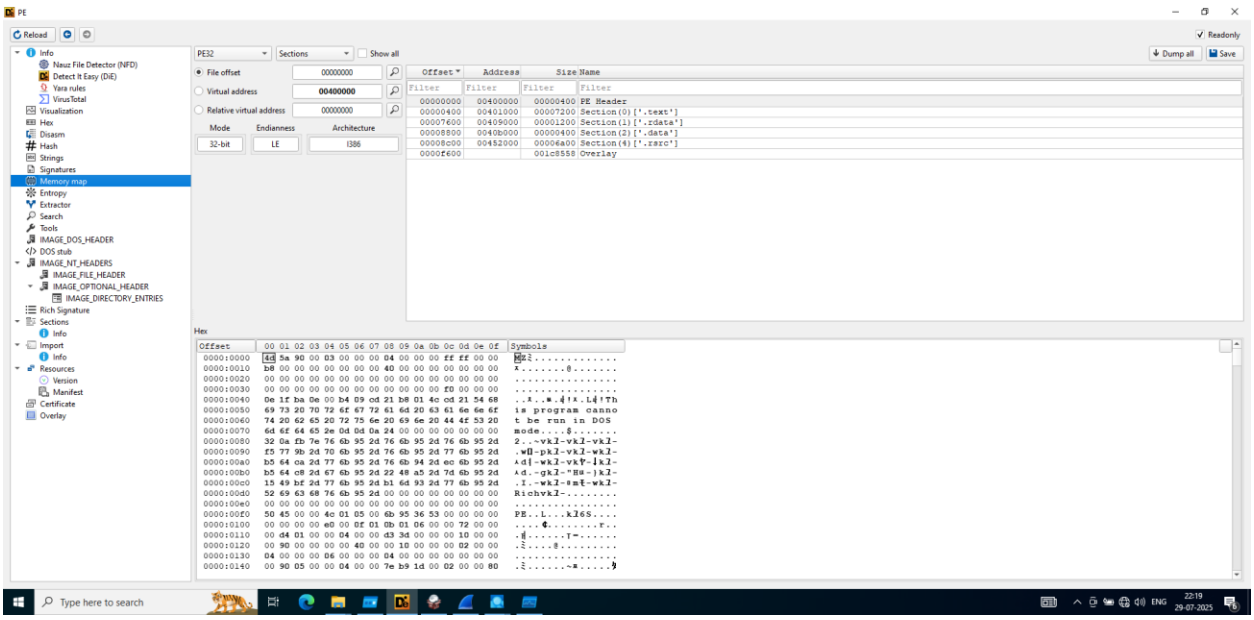
4.Hash



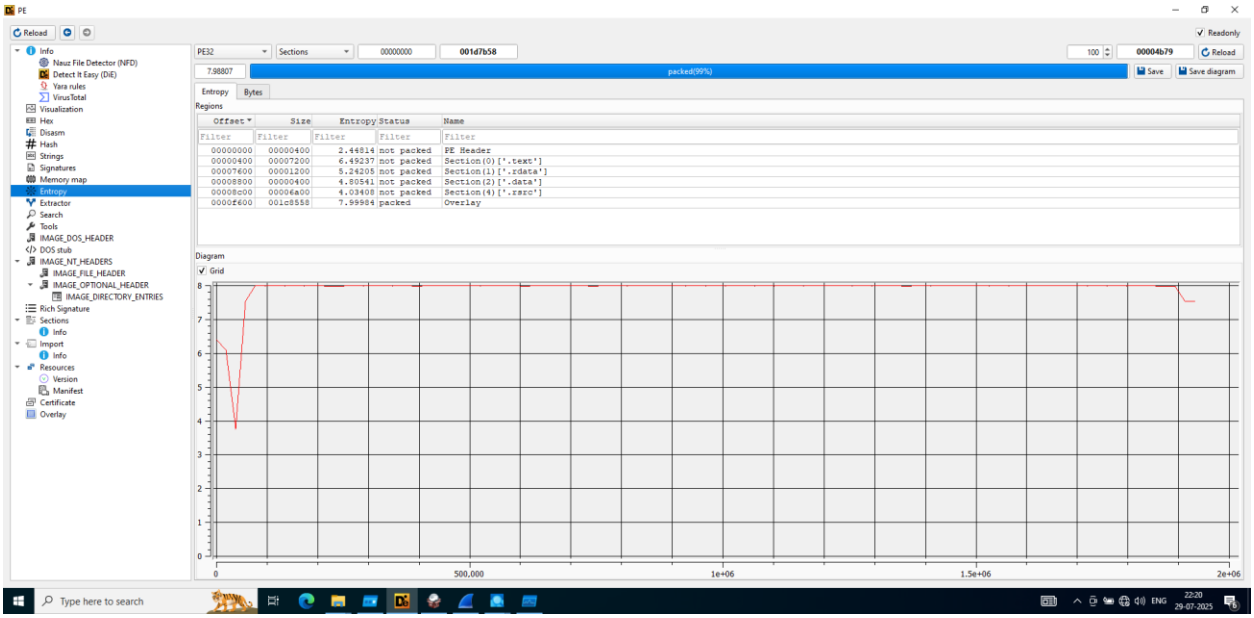
5.Strings



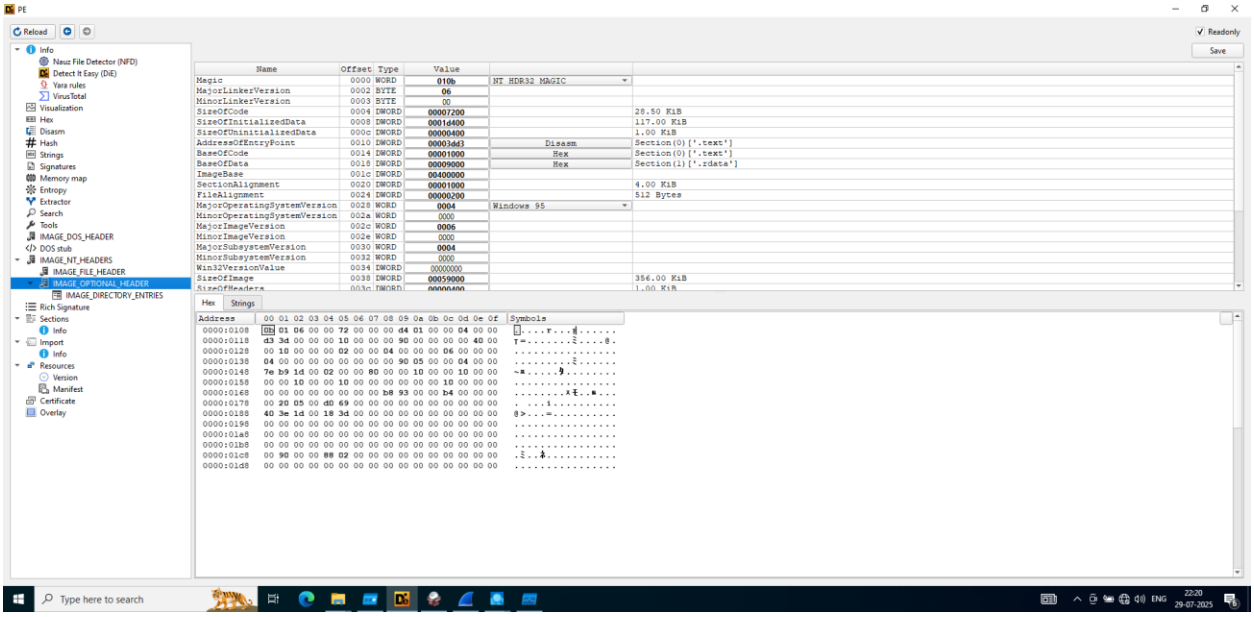
6.Memory mapping(Section address ,size ,name)



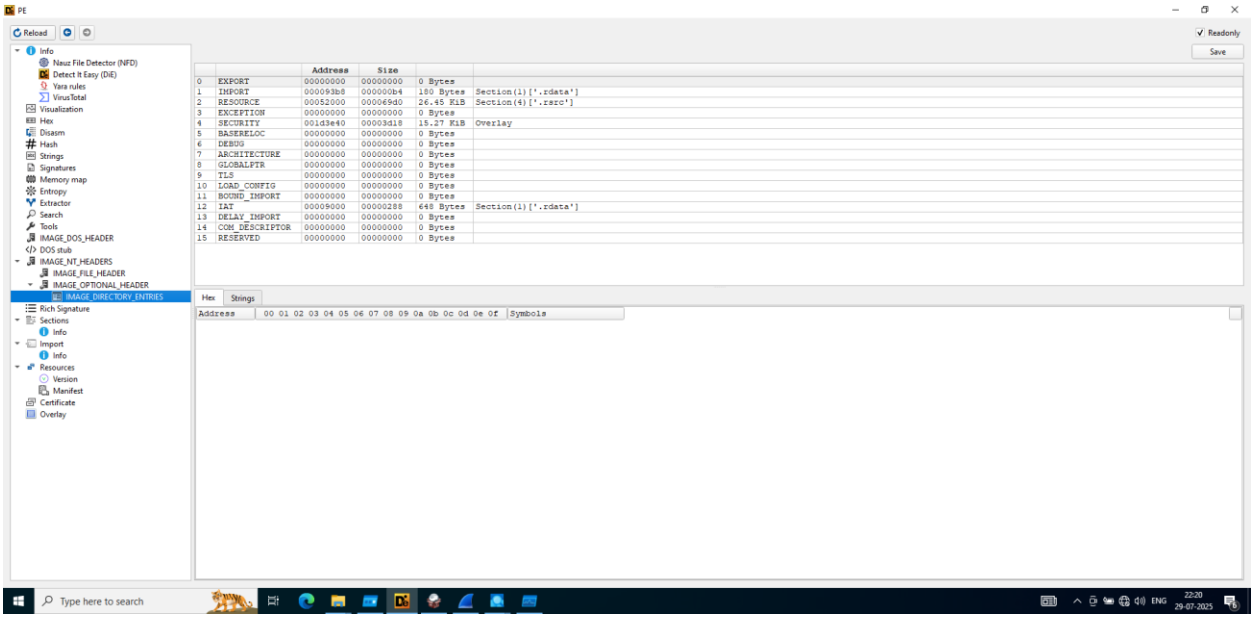
7.Entropy(hign entropy)



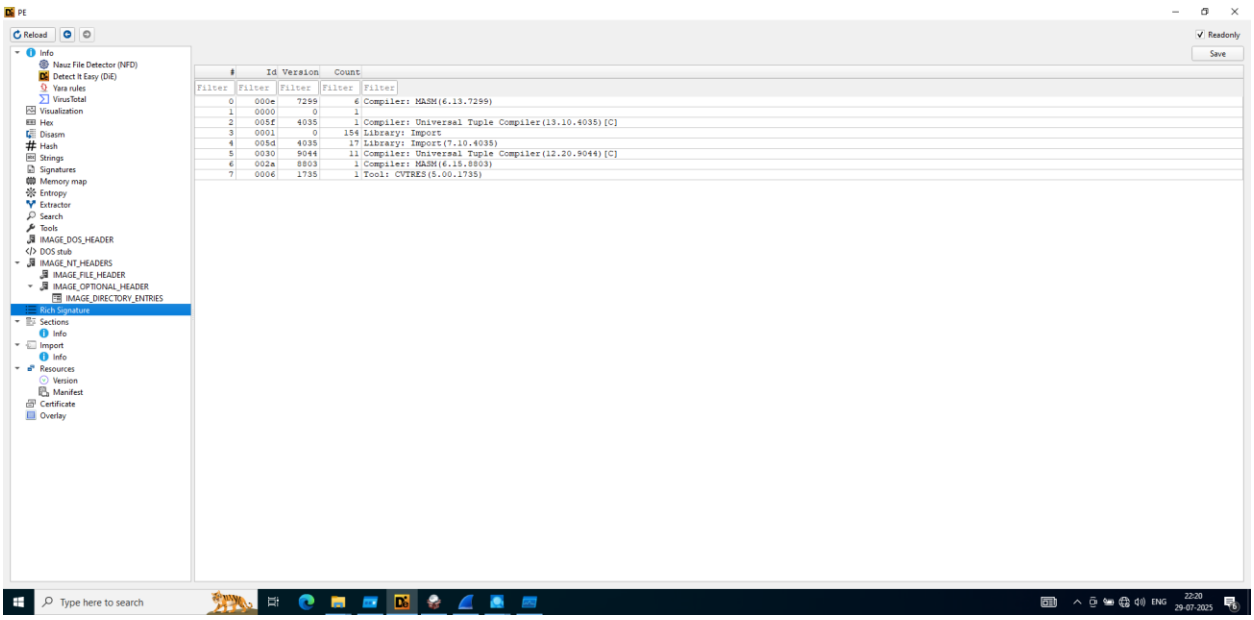
8.Image optional Header



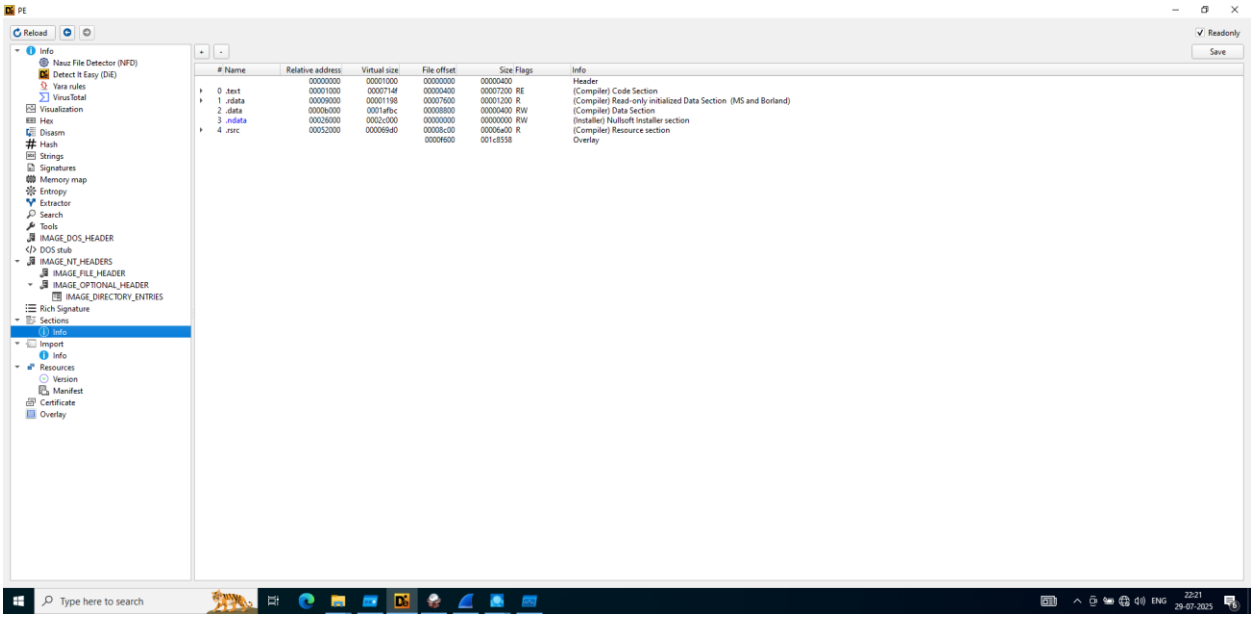
9.Image directory entry



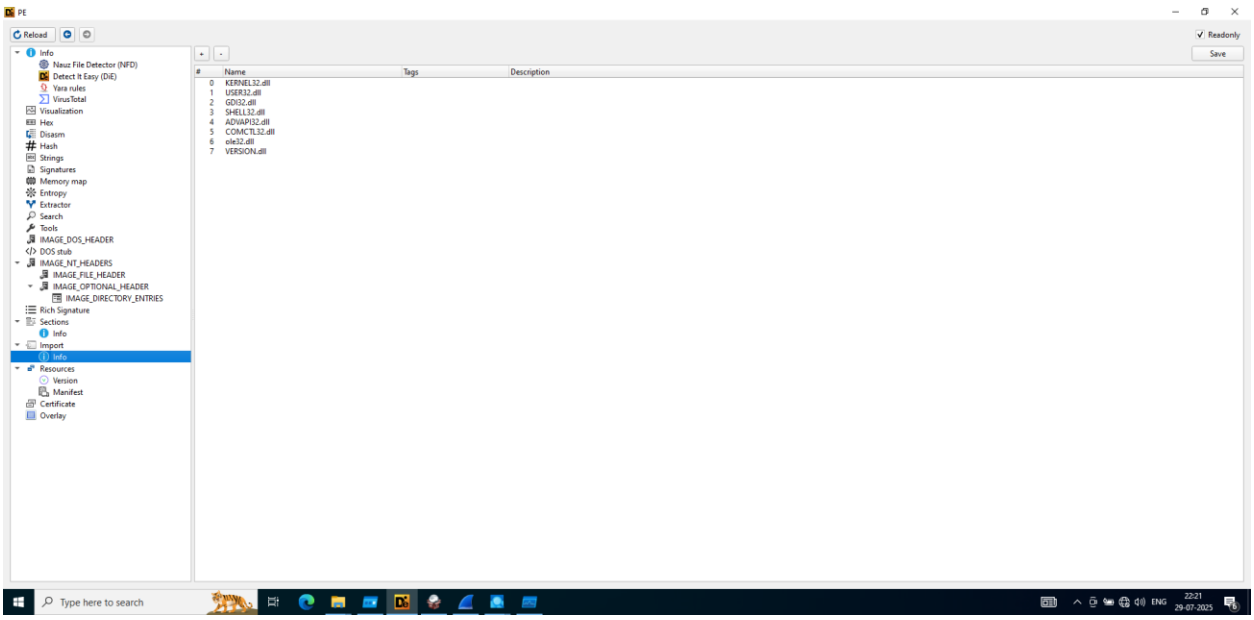
10.Rich Signature



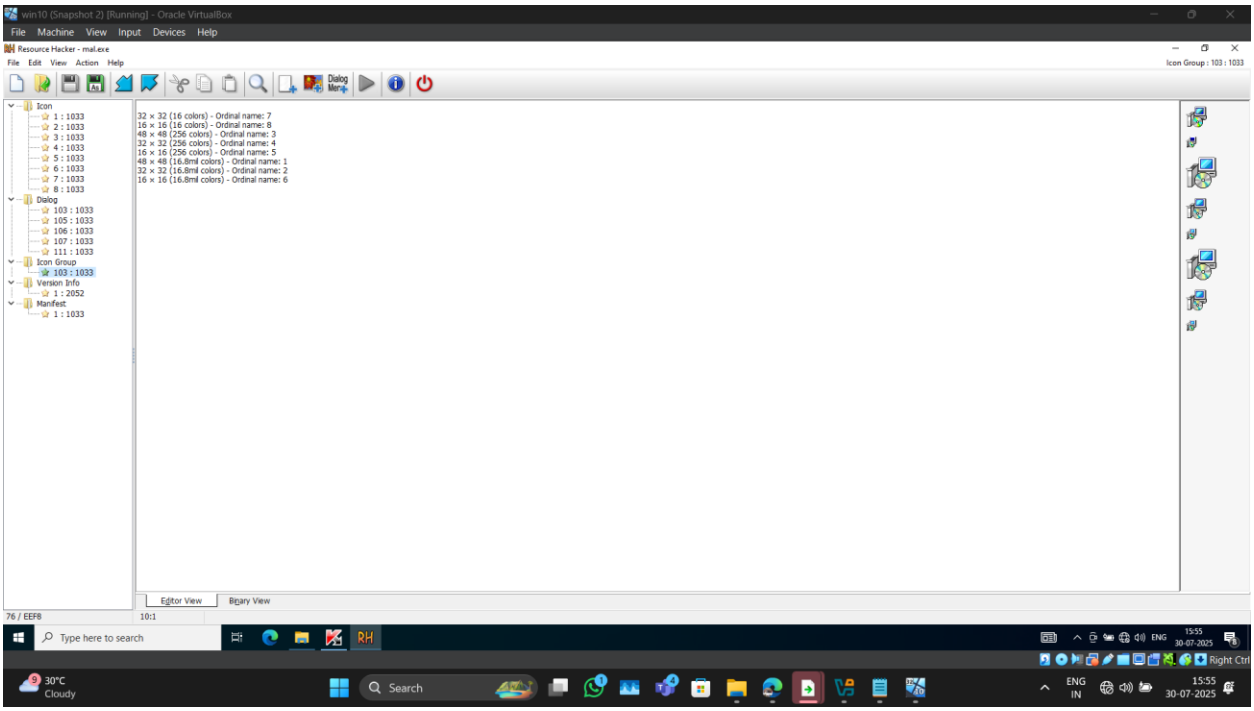
11.Section Information



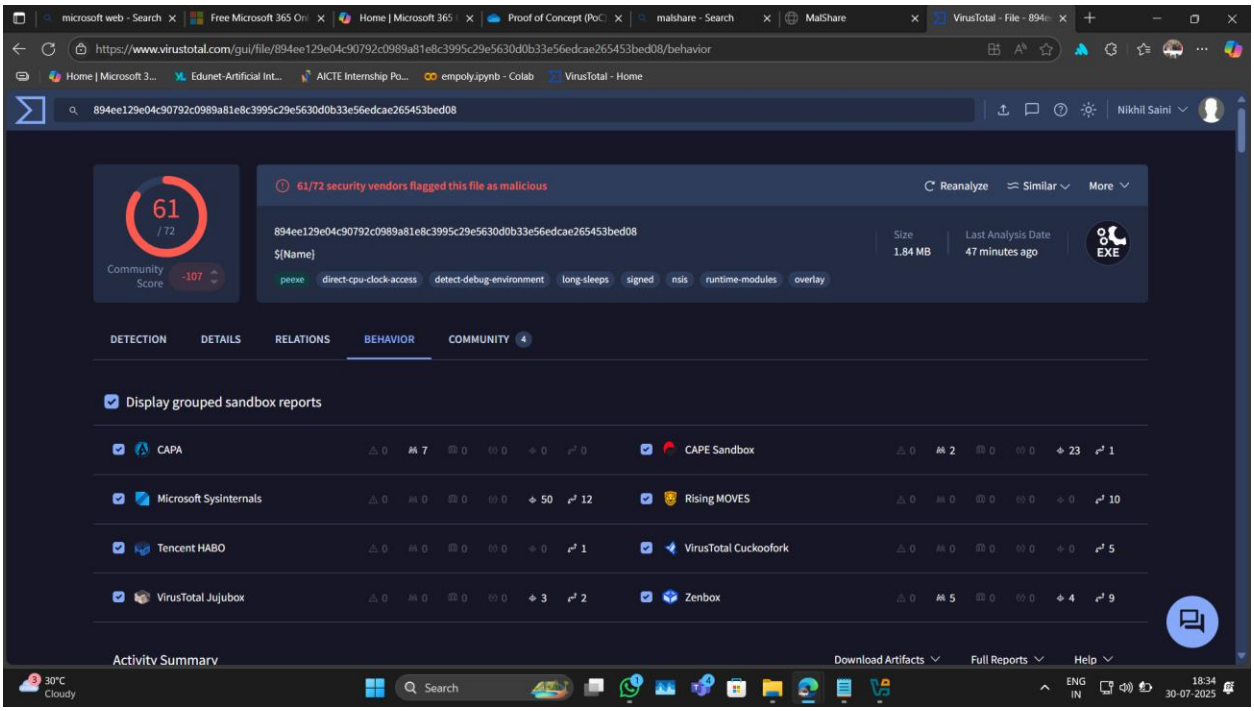
12.Import .dll information

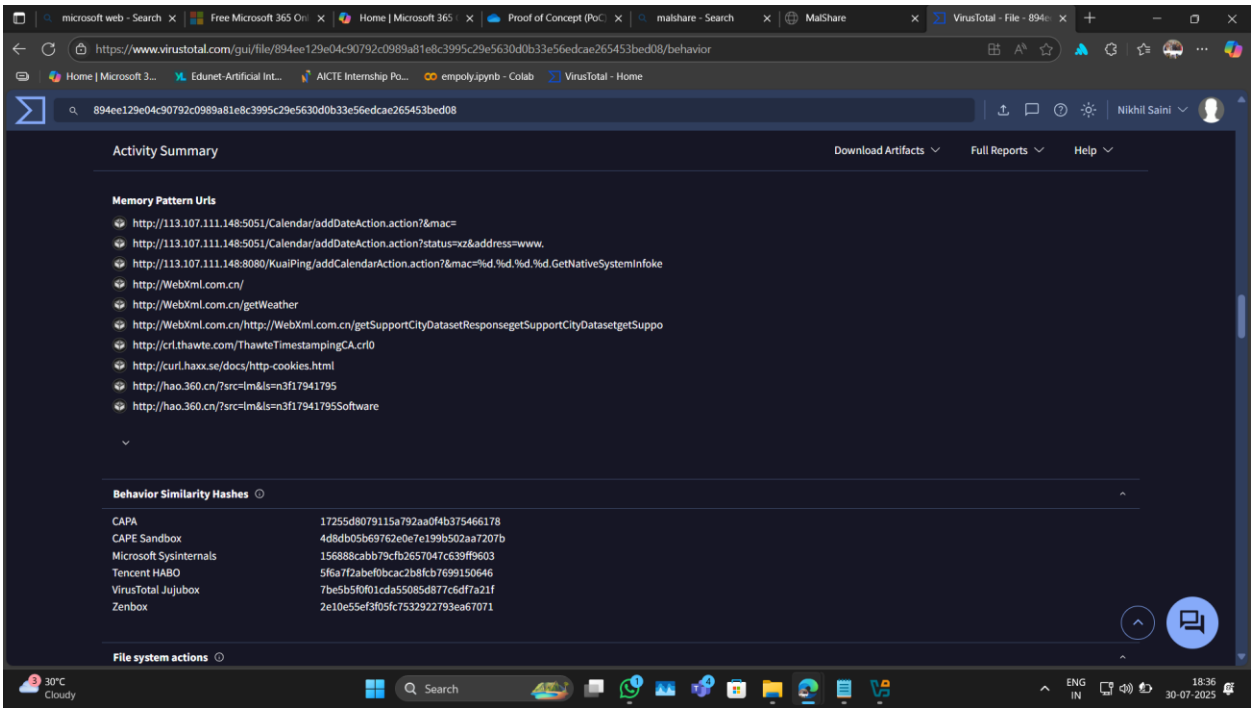


2. **Strings (Sysinternals):**
    a. Purpose: Extracts readable strings from binary files.
    b. Steps:
        i. Copy `strings.exe` and malware sample in same folder.
        ii. Run command: `strings malware_sample.exe > output.txt`
        iii. Open `output.txt` to inspect extracted data.
    c. What We Learn: Reveals IPs, URLs, filenames, commands, suspicious keywords.
3. **Resource Hacker:**
    a. Purpose: Views and edits executable resources (icons, metadata).
    b. Steps:
        i. Open Resource Hacker.
        ii. Load the malware file.
        iii. Browse through `Version Info`, `Manifest`, `Icon`, `String Table`.
    c. What We Learn: Fake company details, misleading info, embedded images or messages.



4. **WinHex:**
    a. Purpose: Examines raw hexadecimal data of binary files.
    b. Steps:
        i. Launch WinHex.
        ii. Click File > Open > Load malware sample.
        iii. Use Find (Ctrl+F) to search keywords like “http”, “cmd”, “exe”.
    c. What We Learn: Raw byte-level structure, signatures, and indicators not visible in high-level tools.
5. **Online Repositories (VirusTotal, MalwareBazaar, Vx-underground, Virus.exchange, Anu.run):**
    a. Purpose: Online services for malware intelligence.
    b. Steps:
        i. Search using malware hash.
        ii. Check detection rate, behavior reports, sandbox results.
        iii. Compare reports across platforms.
    c. What We Learn: Classification, threat level, network behavior, historical context.





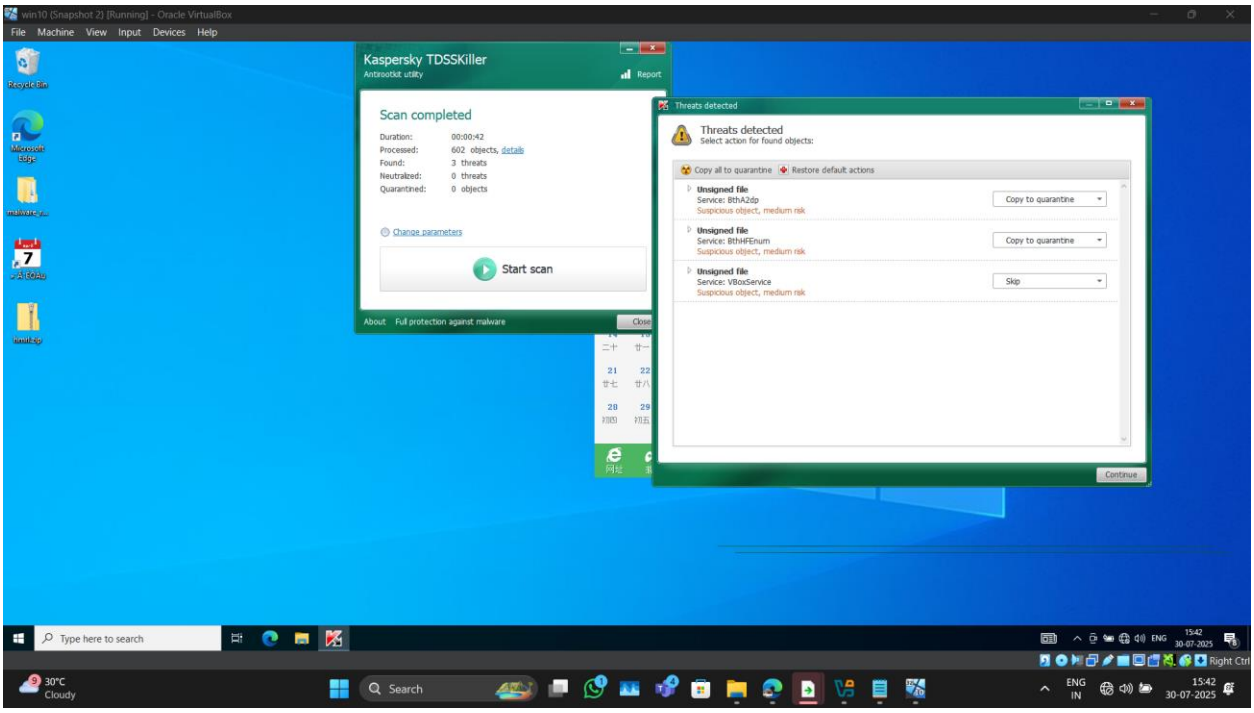
Note: for more info. Refer [VirusTotal - File - 894ee129e04c90792c0989a81e8c3995c29e5630d0b33e56edcae265453bed08]

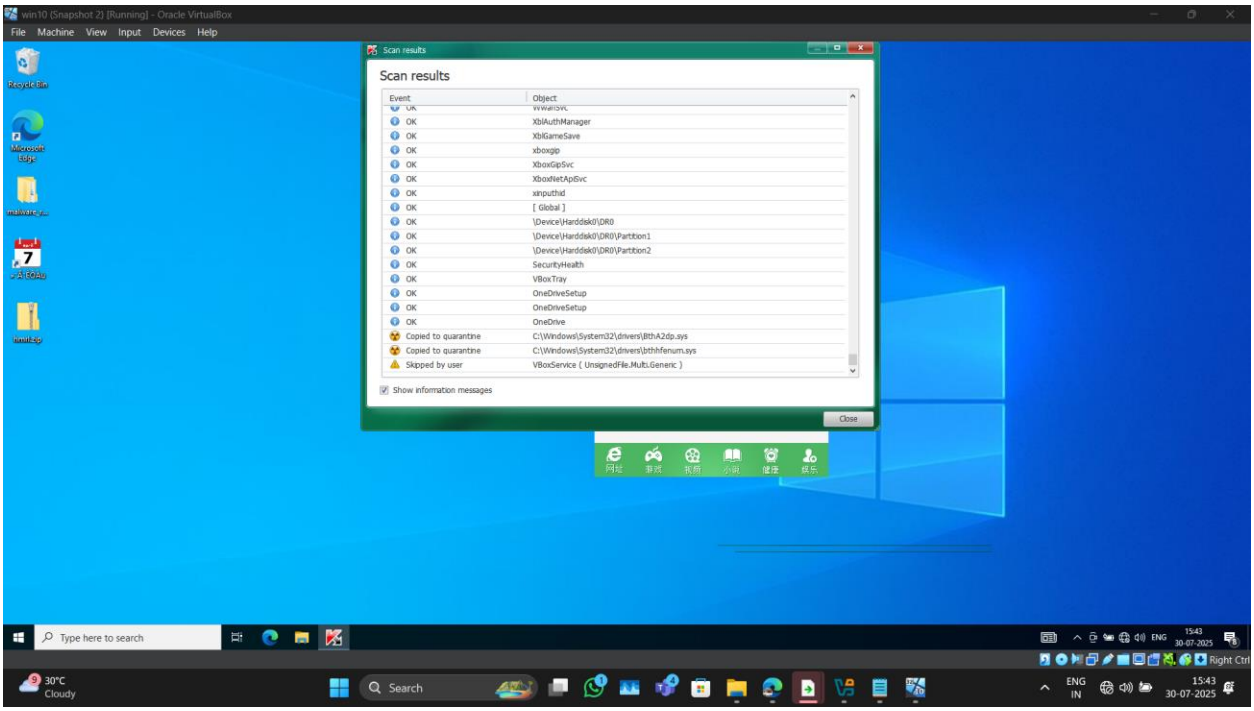
Dynamic Analysis

Tools Used, Explanation and Steps:

1. **Process Explorer (Sysinternals):**
    a. Purpose: Lists active processes with detailed info.
    b. Steps:
        i. Run as administrator.
        ii. Go to Options > Enable 'Verify Image Signatures'.
        iii. Sort by Company Name to highlight unsigned processes.
        iv. Look for suspicious, unknown, or unsigned entries.
    c. What We Learn: Hidden processes, parent-child relations, memory usage.
2. **Autoruns (Sysinternals):**
    a. Purpose: Displays all auto-starting programs.
    b. Steps:
        i. Launch Autoruns.
        ii. Review 'Logon', 'Scheduled Tasks', 'Services', and 'Drivers' tabs.
        iii. Highlight unfamiliar entries, check their paths and signatures.
    c. What We Learn: Persistence techniques used by malware.
3. **Process Monitor (Sysinternals):**
    a. Purpose: Captures real-time system activity.
    b. Steps:
        i. Launch ProcMon, press Ctrl+E to start logging.
        ii. Run the malware.
        iii. Press Ctrl+E again to stop.
        iv. Use filters (e.g., Process Name contains malware_sample.exe).
    c. What We Learn: Registry, file, and process events triggered by malware.
4. **RegShot:**
    a. Purpose: Compares registry before and after execution.
    b. Steps:
        i. Open RegShot.
        ii. Take Snapshot 1 before running malware.
        iii. Run malware and wait a few minutes.
        iv. Take Snapshot 2.
        v. Click ‘Compare’ and analyze differences.
    c. What We Learn: New/modified registry keys indicating persistence or configuration changes.

5. **TDSSKiller (Kaspersky):**
    a. Purpose: Rootkit detection and removal.
    b. Steps:
        i. Launch TDSSKiller.
        ii. Accept terms and click 'Start Scan'.
        iii. Wait for results.
        iv. Quarantine or delete detected files.
    c. What We Learn: Finds hidden malicious drivers, kernel-level threats.





File Transfer Recap

- Kali to Win10 VM:
  - Start server: `python3 -m http.server 8888`
  - Open `http://<Kali-IP>:8888` in Win10 VM browser
  - Download `.vir` file safely

Out files on :https://github.com/Nikhil2604Saini/Digisuraksha-parhari-foundation/tree/main/Cybersecurity-Internship-Program-2025/Week-2_Malware-IOC-APT28/Malware-Reports/malware_tools_report