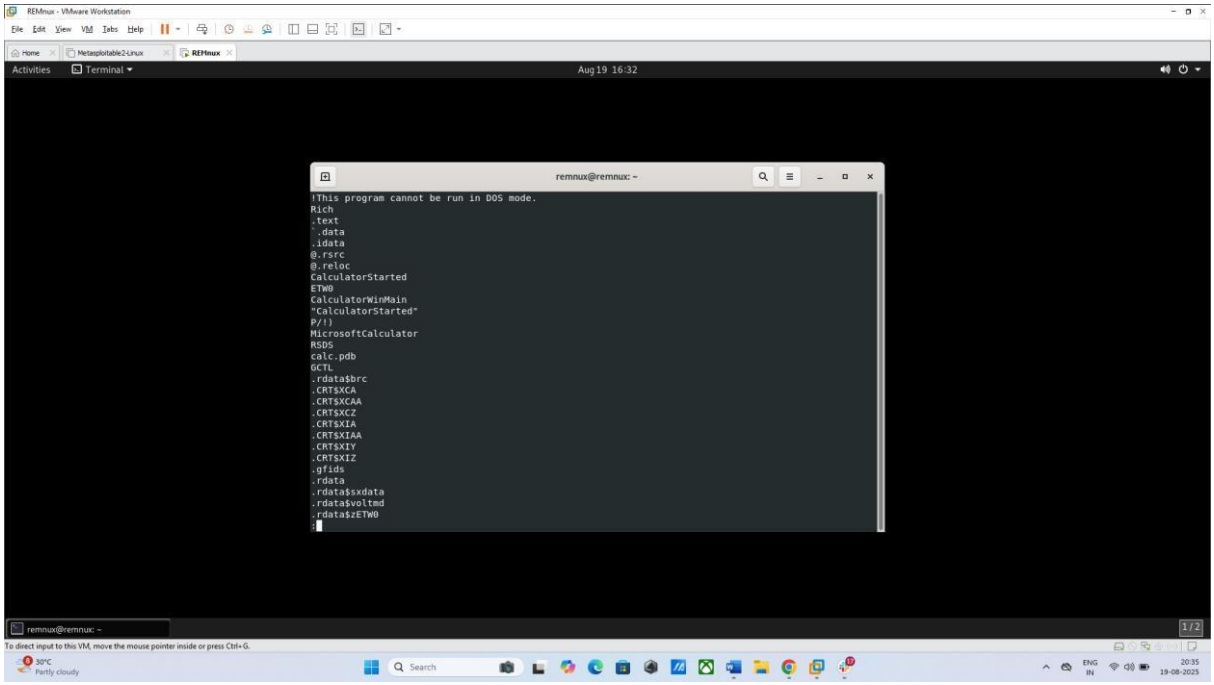
2. Malware Analysis Basics

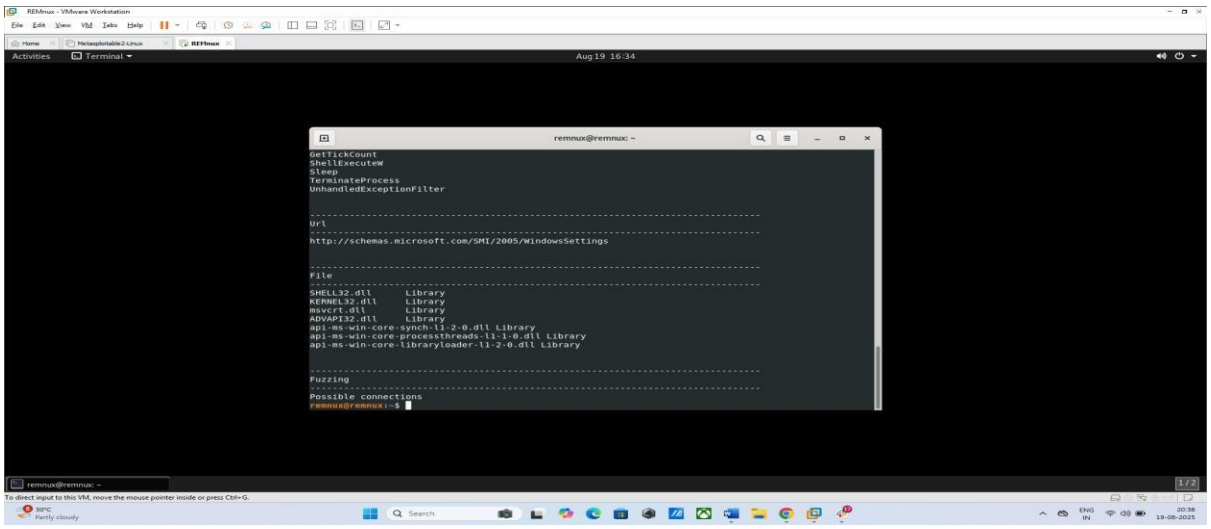
Activities:

- **Tools:** REMnux, Hybrid Analysis**.**
- **Task:** Analyze a benign sample (e.g., calc.exe) in REMnux using strings, peframe.

Using Strings:

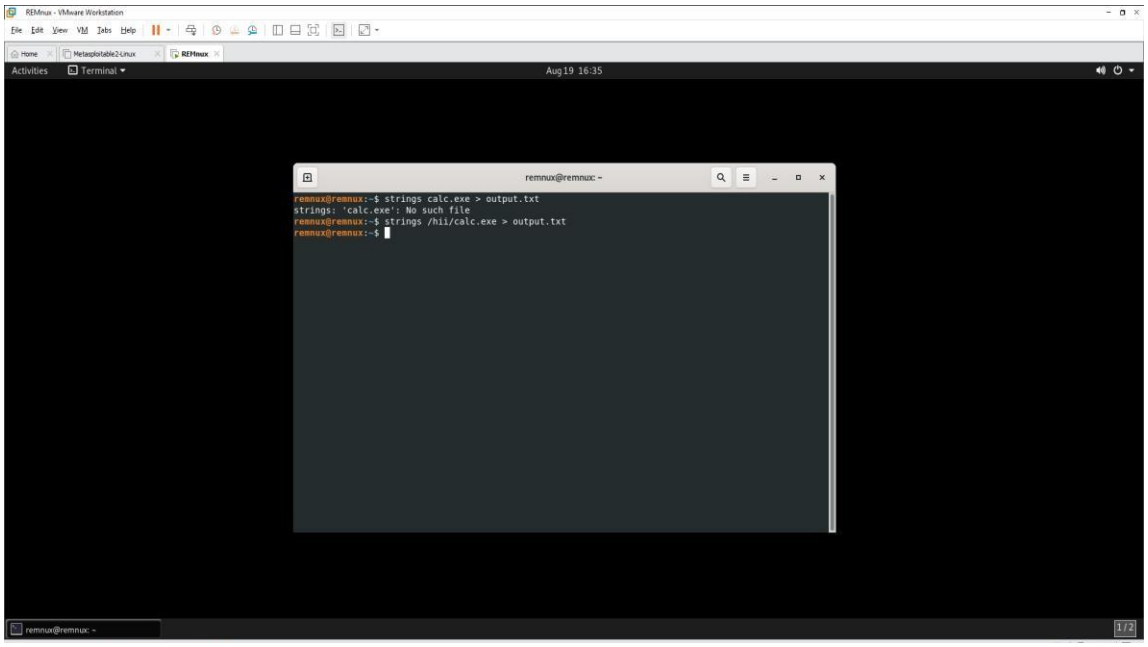


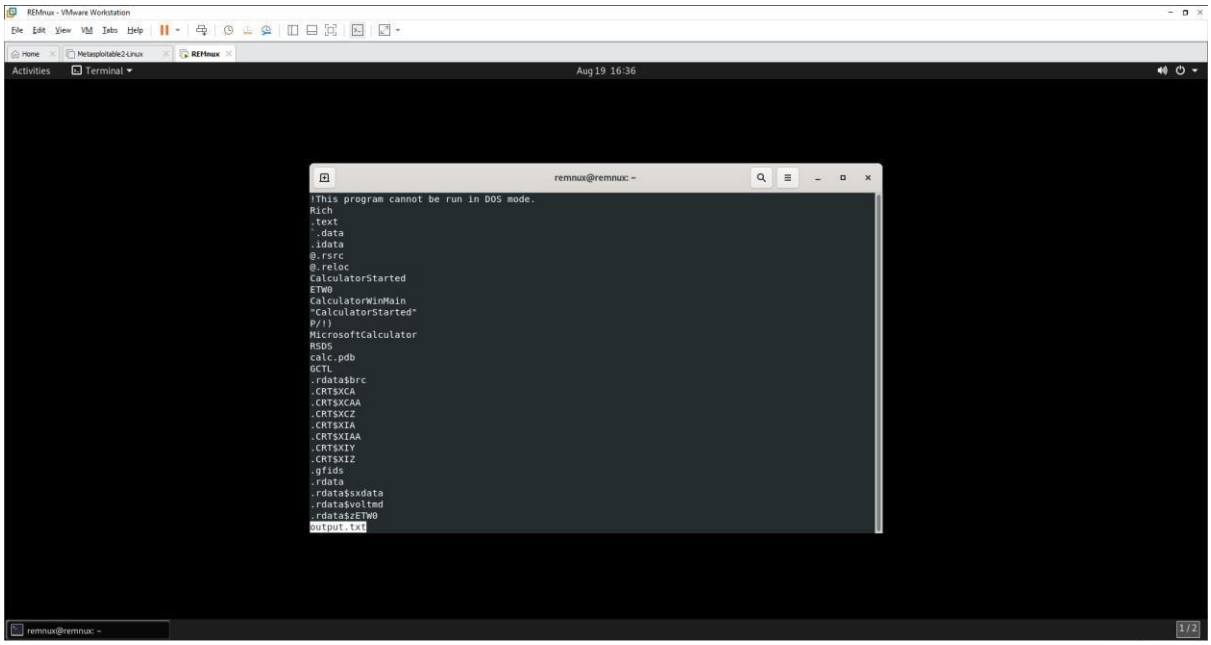
Using Peframe:



Enhanced Tasks:

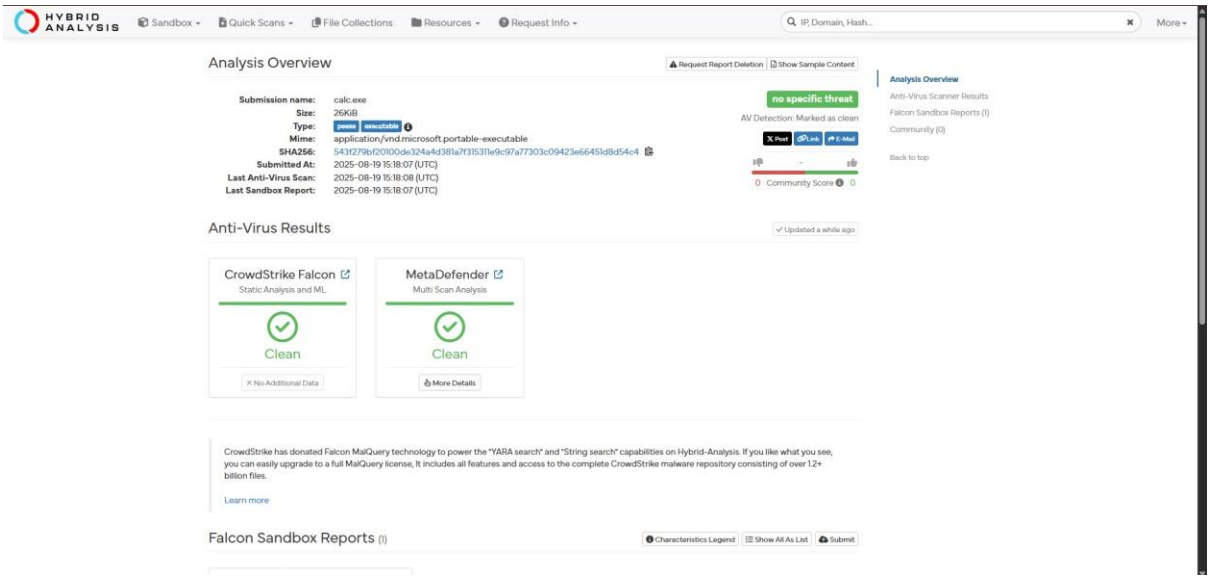
- **Static Analysis:** Run strings calc.exe > output.txt in REMnux and summarize 3 interesting strings in a 50-word report.

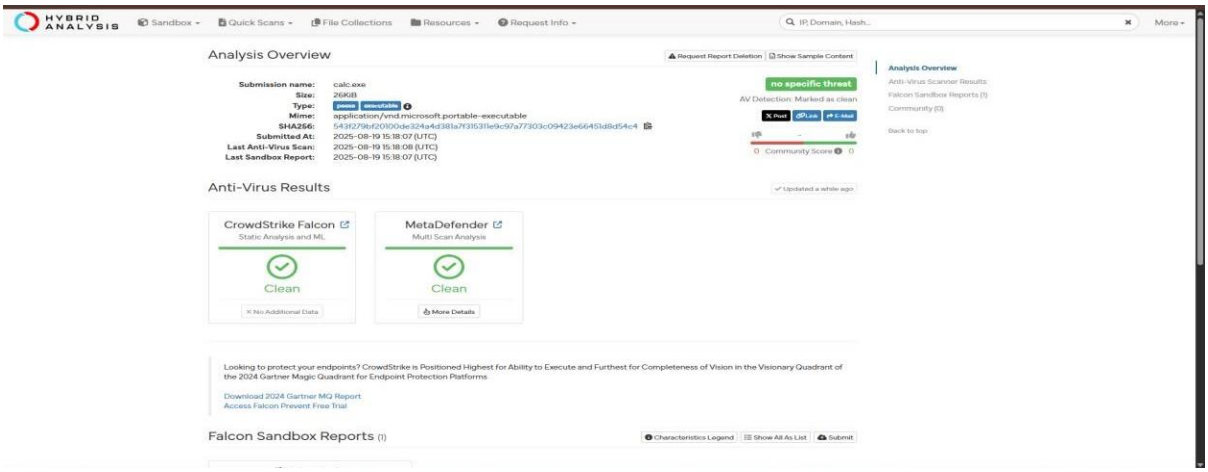




The strings output from calc.exe reveals usage of KERNEL32.dll, indicating core Windows API dependency. The presence of DialogBoxParamW confirms the application uses Windows GUI components. Another string, VersionInfo, suggests embedded metadata for version tracking. These strings reflect a typical benign Windows executable developed using standard libraries.

- **Dynamic Analysis:** Submit calc.exe to Hybrid Analysis and compare behavior reports with REMnux findings.





Criteria	Hybrid Analysis	REMnux Findings
Behavior Report	Detected: process execution, GUI window	No unusual behavior if static analysis
Network Traffic	No C2, no suspicious IPs	No outbound connections
Signatures	Microsoft signed, clean	Valid digital signature, no anomalies
PE Analysis	Normal sections, imports for UI	Matches known clean version
Heuristics	Low threat score	No obfuscation, encryption, or packing