



## 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:

```
remnux@remnux:~$ strings calc.exe
This program cannot be run in DOS mode.
Rich
.text
.data
.idata
0.rsrc
0.reloc
CalculatorStarted
ETW0
CalculatorWinMain
CalculatorStarted
P/I
MicrosoftCalculator
MSDS
calc.pdb
GCTL
.rdatasbrc
.CRT$XCA
.CRT$XCAA
.CRT$XCZ
.CRT$XIA
.CRT$XIAA
.CRT$XIY
.CRT$XIZ
.pfids
.rdata
.rdatasxdata
.rdatasvltmd
.rdatasvltw
```

### Using Peframe:

```
remnux@remnux:~$ peframe calc.exe
GetTickCount
ShellExecuteW
Sleep
TerminateProcess
UnhandledExceptionFilter
-----
URL
http://schemas.microsoft.com/SMI/2005/WindowsSettings
-----
File
SHELL32.dll Library
kernel32.dll Library
user32.dll Library
ADVAPI32.dll Library
api-ms-win-core-synch-l1-2-0.dll Library
api-ms-win-core-processthreads-l1-1-0.dll Library
api-ms-win-core-libraryloader-l1-2-0.dll Library
-----
Fuzzing
-----
Possible connections
remnux@remnux:~$
```



## Enhanced Tasks:

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

```
remnux@remnux:~$ strings calc.exe > output.txt
strings: 'calc.exe': No such file
remnux@remnux:~$ strings /hi/calc.exe > output.txt
remnux@remnux:~$
```

```
This program cannot be run in DOS mode.
Rich
.text
.data
.idata
@.rsrc
@.reloc
CalculatorStarted
ETW0
CalculatorWinMain
"CalculatorStarted"
P/I/
MicrosoftCalculator
MSDS
calc.pdb
GCTL
.rdata$brc
.CRT$XCA
.CRT$XCAA
.CRT$XCZ
.CRT$XIA
.CRT$XIAA
.CRT$XIY
.CRT$XIZ
.gifds
.rdata
.rdata$ssdata
.rdata$volTmd
.rdata$zTwo
output.txt
```



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.

The screenshot shows the Hybrid Analysis web interface for a submission of calc.exe. The submission details include: Submission name: calc.exe, Size: 26KiB, Type: process, executable, SHA256: 5430279b20100dc324a4d381a7015311e9c97a77303c09423e6645148d54d4, Submitted At: 2025-08-19 15:18:07 (UTC), Last Anti-Virus Scan: 2025-08-19 15:18:08 (UTC), and Last Sandbox Report: 2025-08-19 15:18:07 (UTC). The analysis overview shows 'no specific threat' and 'AV Detection: Marked as clean'. The anti-virus results section shows 'Clean' for both CrowdStrike Falcon and MetaDefender. The Falcon Sandbox Reports section is empty.

This is another screenshot of the Hybrid Analysis web interface for the same submission of calc.exe. The submission details are identical to the previous screenshot. The analysis overview shows 'no specific threat' and 'AV Detection: Marked as clean'. The anti-virus results section shows 'Clean' for both CrowdStrike Falcon and MetaDefender. The Falcon Sandbox Reports section is empty.



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