**Labs. Configuration Guide**

***for***

**Malware Investigation with Memory Forensic and Threat Hunting**

Contents

[Malware Analysis Sandbox and Tools Requirements: 3](#_Toc160287858)

[Malware Labs Configuration: 3](#_Toc160287859)

[Security Labs for Digital Payments-Configurations: 6](#_Toc160287860)

[Network Security Coding Snippets: 8](#_Toc160287861)

[Registration and Accounts Creations: 8](#_Toc160287862)

[Quantum Circuits, Algorithms and QML for Network Security (Extra Bites, Optional): 8](#_Toc160287863)

# Malware Analysis Sandbox and Tools Requirements:

Malware Analysis Labs of this workshop requires:

1. 1 Windows Virtual Machine - Sandbox and Digital Forensics Workstation
2. 1. Linux Virtual Machine - Sandbox and Forensics Workstation
3. 1 Windows and 1 Linux Workstations
4. Memory Forensics Tools, Forensics Images and Case Management Tools
5. Active Accounts in GitHub, ThreatConnect, Splunk Enterprise and Utility Tools
6. SDKs-Python, Java, Julia and PHP and IDEs- PyCharm and Jupyter Lab

# Malware Labs Configuration:

Follow the steps below to prepare Forensics Labs for this Workshop:

1. Create this folder, C:\MALWARE-INVESTIGATIONS-WORKSHOP in C-Drive
2. Clone all resources using git ***clone*** [***https://github.com/AmritChhetriB/MalwareAnalysisUsingMemoryForensics.git***](https://github.com/AmritChhetriB/MalwareAnalysisUsingMemoryForensics.git)
3. Configure Virtual Machines and Sandboxes mentioned above using Tools mentioned below
4. 1 Windows and Linux Workstations Malware Analysis-Tools:

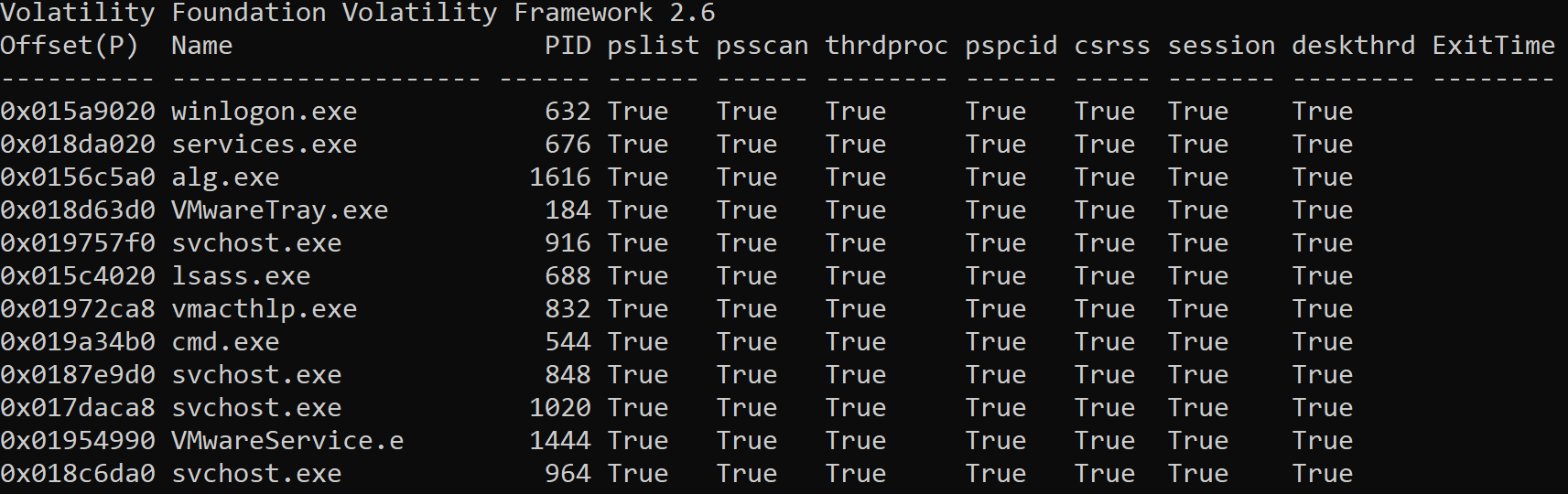
|  |  |  |  |
| --- | --- | --- | --- |
| **peripherals/Infrastructure** | **Peripherals/Infrastructure** | **Specifications** | **URLs** |
| **Virtual Machines** | 1 Windows Workstations(Victim Machine) | Window 10/11/2019 Pro 64x |  |
|  | 1 Windows Workstations(Sandbox) | Window 10/11/2019 Pro 64x | - |
|  | Linux Sandbox | RumNux | - |
|  |  | RUN.ANY | - |
| **Workstation Pre-requisites** | Operating System | Windows 10(Pro), 64-Bits | - |
|  | RAM | 8-12 GB | - |
|  | Storage/HDD | 30 GB |  |
|  | CPU | X86-64 Architecture |  |
|  | Network Bandwidth/Internet | Internet/LAN |  |
|  |  |  |  |



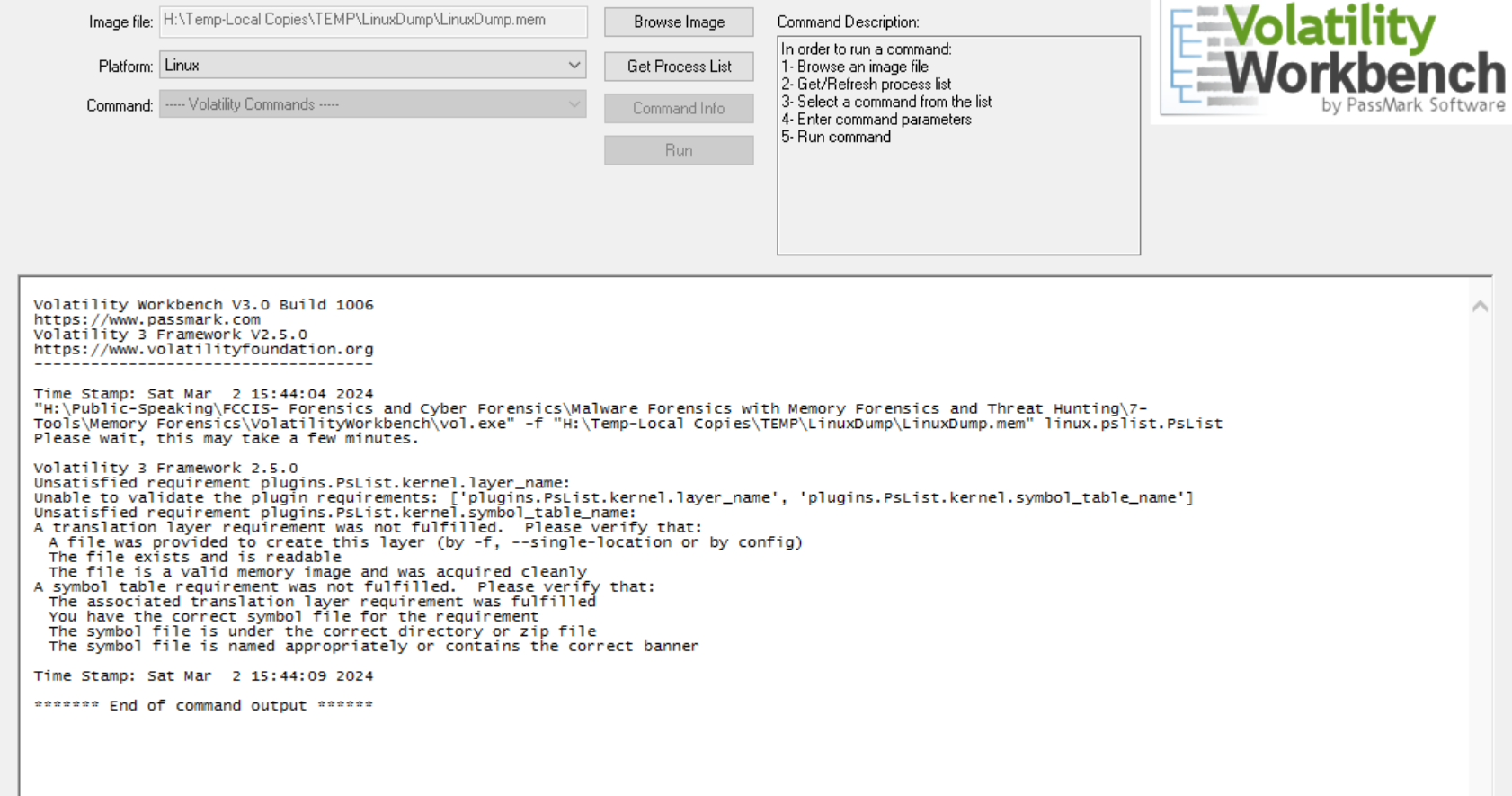
# Security Labs for Digital Payments-Configurations:

*Follow the steps below to install and configure all necessary tools. All details are for Tools for advanced settings.*

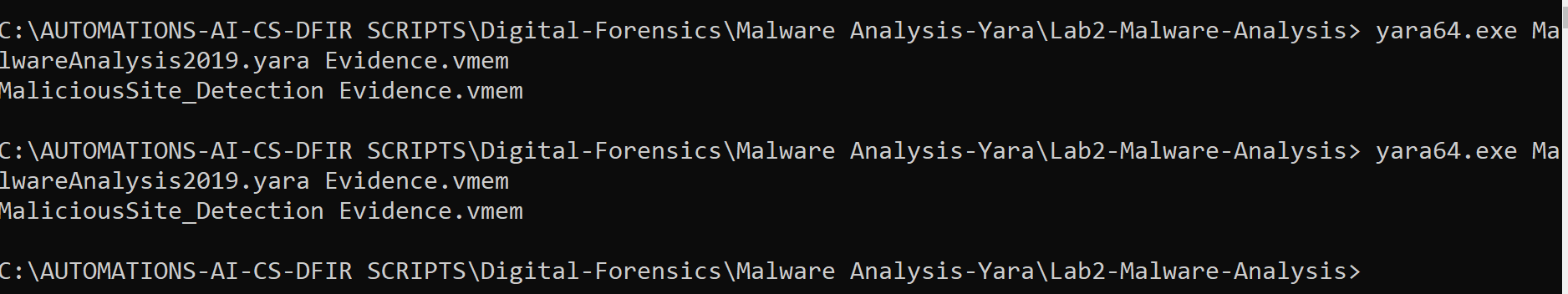
1. **Configuration of Volatility:**
   1. Download Volatility and extract inside ***C:\MALWARE-INVESTIGATIONS-WORKSHOP\FORENSIC-SCRIPTS-TOOLS***
   2. Then set ***C:\MALWARE-INVESTIGATIONS-WORKSHOP\FORENSIC-SCRIPTS-TOOLS\Memory-Forensics\volatility\_2.6\_win64\_standalone*** in PATH
   3. Download <https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples> and unzip inside evidence folder
   4. Run to check the configuration: ***volatility -f Evidence.vmem --profile=WinXPSP2x86 psxview***



* 1. Alternatively, download and use Volatility Workbench



1. **Configuration of Yara:**
   1. Download Yara from and extract and then extracted folder into PATH variable
   2. Run yara64.exe MalwareAnalysis2019.yara Evidence.vmem to test the configuration



# Network Security Coding Snippets:

* 1. Create a folder “Python4RNetworkSecurity” in a Drive and also install Git from URL given earlier
  2. Open Command Prompt and check out the code using ‘***git clone*** [***https://github.com/AmritChhetriB/MalwareAnalysis.git***](https://github.com/AmritChhetriB/MalwareAnalysis.git)***’***

# Registration and Accounts Creations:

1. Register Account with VirusTotal, Online Anti-Virus Solution powered by AI at https://www.virustotal.com/gui/
2. Account Registration for Cyber Crimes Reporting  
   Open <https://cybercrime.gov.in> in a Browser and complete the registration to get ready to report Digital Payments Crimes.

# Quantum Circuits, Algorithms and QML for Network Security (Extra Bites, Optional):

1. Create an account with IBM and login to IBM Quantum site to get API key
2. Install Jupyter Notebook and PyCharm( add qiskit plugin)
3. Use Q-Kit and Composer to design Quantum Circuits for different Algorithms and use Qiskit to write that Circuits Design into Quantum Algorithms.

# Yara Configuration:

Follow steps below to configure Yara in Standalone Mode:

1. **Yara Configuration on Windows:** 
   1. Get Yara Executable, yara-4.3.2-2150-win64.zip from
   2. **Keep Executable in PATH**
   3. **Prepare two files- Yara Rule and Text Evidence as given in folder**
      1. **Yara Rule: DetectionRule.yara**

rule MaliciousSite\_Detection

{

meta:

author = "Amrit Chhetri"

date = "07-01-2024"

Purose = "Malware Detection"

strings:

$MaliciousWeb1 = "www.xxx2.com"

$MaliciousWeb2 = "www.xxx1.com"

$Maliciousweb3 = "www.yyyy2.com"

$AttackerName1 = "hackx1203"

$AttackerName2 = "Hackor"

$AttackerName3 = "Hax"

condition:

any of them

// $MaliciousWeb1 and $MaliciousWeb2 and $MaliciousWeb2

}

* + 1. **Text Evidence:** **EvidenceURLs.txt**

www.xxx1.com

www.xxx2.com

www.xxx.com

hackx1203

Hackor

* 1. **And run** *yara64.exe MalwareAnalysis.yara Evidence.vmem*

1. **Running Yara with Volatility:** 
   1. volatility –f Evidence.vmem --profile=WinXPSP2x86 yarascan -Y "https:"
   2. volatility -f Evidence.vmem --profile=WinXPSP2x86 yarascan -p 1956 -Y "https:"
   3. volatility -f Evidence.vmem --profile=WinXPSP2x86 yarascan -Y "com"
   4. volatility –f Evidence.vmem --profile=WinXPSP2x86 yarascan -Y "172.16.98.1"
   5. volatility -f Evidence.vmem --profile=WinXPSP2x86 yarascan --yara-file=TrojanAnalysis.yara