Malware Analysis Bootcamp

Learning Malware Analysis The Right Way

Setting up our environment

Tools we will be using:

- Hypervisor - VirtualBox or VMware
- Windows 7 VM 32/64bit - 64 bit preferable.
- FLARE VM - Windows malware analysis distribution
    - Comes prepackaged with all the tools we need for malware analysis.

Note: Ensure you disable Windows Update and Windows Defender on your analysis VM.

Security guidelines

- Keep your Hypervisor updated.
- When executing malware ensure your network configuration is set to host-only.
- Do not plug any USB devices in to the VM.
- Make sure you download compressed and password protected samples to avoid accidental execution.
- Take snapshots!
- Do not store any valuable data on your analysis VM.
- Disable shared folders, before execution or analysis.