

Downloaded a fresh developer's evaluation vm from Microsoft https://aka.ms/windev_VM_vmware

Powered up as Windows 11 Pro vm in VMware Workstation 17 Pro but made no changes yet.

*NOTE – A simple hardware tweak or two goes a long way: Bumping the RAM to 8GB with 70-80GB storage and 2 NICs really streamlined everything. (Everything from installation to malware analysis was faster, plus deleting a NIC (the one set to NAT) after all your tools download feels way easier to me than reconfiguring the same NIC as well as your vm network adapter in the OS)

System > About

WinDev2212Eval
VMware7,1

Rename this PC



Device specifications

Copy



Device name	WinDev2212Eval
Processor	Intel(R) Core(TM) i9-10980HK CPU @ 2.40GHz 3.10 GHz (4 processors)
Installed RAM	8.00 GB
Device ID	74D6EDE2-1B8A-4509-BA74-7BCEA4622FFB
Product ID	00329-20000-00001-AA232
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Related links [Domain or workgroup](#) [System protection](#) [Advanced system settings](#)



Windows specifications

Copy



Edition	Windows 11 Enterprise Evaluation
Version	21H2
Installed on	1/3/2023
OS build	22000.1219
Experience	Windows Feature Experience Pack 1000.22000.1219.0

[Microsoft Services Agreement](#)

[Microsoft Software License Terms](#)

Downloaded FLAREv4 from source to the vm <https://github.com/mandiant/flare-vm/archive/refs/tags/v4.zip>

Decompressed and digested everything in the Readme.md instructions. Just do it. **Shameless shout out to the FLARE team for these hints; saved me some major time and headache!**

```
> **Note:** FLARE VM should ONLY be installed on a virtual machine!

* Prepare a Windows 10+ virtual machine
  * FLARE VM has been tested on [Windows 10 1809
    x64] (https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/) and `20H2`
  * We recommend:
    * Avoiding usernames containing a space or other special characters
    * Using a disk capacity of at least 70-80 GB and memory of at least 2 GB
  * Disable Windows Updates (at least until installation is finished)
    * https://www.windowscentral.com/how-stop-updates-installing-automatically-windows-10
  * Disable Tamper Protection and any Anti-Malware solution (e.g., Windows Defender), preferably
    via Group Policy.
    * Disabling Tamper Protection
      * https://support.microsoft.com/en-us/windows/prevent-changes-to-security-settings-with-tamper-protection-31d51aaa-645d-408e-6ce7-8d7f8e593f87
      * https://www.tenforums.com/tutorials/123792-turn-off-tamper-protection-windows-defender-antivirus.html
    * Disabling Windows Defender
      * https://stackoverflow.com/questions/62174426/how-to-permanently-disable-windows-defender-real-time-protection-with-gpo
      * https://www.windowscentral.com/how-permanently-disable-windows-defender-windows-10
      * https://github.com/jeremybeaume/tools/blob/master/disable-defender.ps1
  * Take a VM snapshot so you can always revert to a state before FLARE VM installation
* Open a `PowerShell` prompt as administrator
* Download the installation script
[ `installer.ps1` ] (https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1) to your
desktop
  * `(New-Object
    net.webclient).DownloadFile('https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1
    _','$([Environment]::GetFolderPath("Desktop"))\install.ps1')`
* Unblock the installation script by running:
  * `Unblock-File .\install.ps1`
* Enable script execution by running:
  * `Set-ExecutionPolicy Unrestricted`
* Finally, execute the installer script as follow:
  * `.\install.ps1`
  * You can also pass your password as an argument: `.\install.ps1 -password <password>`
```

Historically in PoSH, pushing “Set-ExecutionPolicy Unrestricted” as Administrator would get the script unblocked, but this time I had to scope the change to “Set-ExecutionPolicy -Scope CurrentUser Unrestricted” before it works.

To summarize steps taken against Defender via the more detailed Stack Overflow thread:

1. Disabled Resource Monitor
2. Disabled Tamper Protection
3. Enabled GPO “Turn off Real-time Protection” & rebooted
4. Enabled GPO “Turn off Microsoft Defender Antivirus” & rebooted
5. Verified DWORD “DisableAntiSpyware” value set to “1” (I previously turned it off in GUI)

```

PS C:\Users\User\Downloads\flare-vm-4\flare-vm-4> .\install.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\Users\User\Downloads\flare-vm-4\flare-vm-4\install.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): r
[+] Checking if script is running as administrator...
    [+] Running as administrator
[+] Checking if execution policy is unrestricted...
    [+] Execution policy is unrestricted
[+] Checking if Windows Defender Tamper Protection is disabled...
    [+] Tamper Protection is disabled
[+] Checking if Windows Defender service is disabled...
    [+] Defender is disabled
[+] Checking to make sure Operating System is compatible...
    [!] Windows version 22000 has not been tested. Tested versions: 17763, 19042
    [+] You are welcome to continue, but may experience errors downloading or installing packages
[-] Do you still wish to proceed? (Y/N): y|

```

At last, the install script will fully engage and present you with a GUI for granular control of tool packages:

Welcome to FLARE VM's custom installer. Please select your options below.
Default values will be used if you make no modifications.

Environment Variable Customization

%VM_COMMON_DIR%	%ProgramData%_VM Shared module and metadata for VM (e.g., config, logs, etc...)	Select Folder
%TOOL_LIST_DIR%	%ProgramData%\Microsoft\Windows\Start Menu\Programs\Tools Folder to store tool categories and shortcuts	Select Folder
%TOOL_LIST_SHORTCUT%	%UserProfile%\Desktop\Tools.lnk Shortcut to %TOOL_LIST_DIR%	Select Folder
%RAW_TOOLS_DIR%	%SystemDrive%\Tools Folder to store downloaded tools	Select Folder

Note: Metapackages may install in a different location (package author's decision)
Metapackages are wrappers around tools that install via dependencies

Package Installation Customization

Available to Install	To Install
asreproast.vm bytecodeviewer.vm exeinfope.vm fiddlerclassic.vm gobuster.vm hxd.vm libraries.python2.vm nmap.vm vbdec.vm	fakenet-ng.vm floss.vm ghidra.vm hashmyfiles.vm idafree.vm libraries.python3.vm map.vm networkminer.vm notepadplusplus.vm notepadpp.plugin.compare.vm npcab.vm ollydbg.ollydumpex.vm ollydbg.vm ollydbg2.ollydumpex.vm ollydbg2.vm pebear.vm peid.vm processdump.vm regshot.vm rundotnetdll.vm sysinternals.vm uniextract2.vm vcbuildtools.vm wireshark.vm
Total: 9	Total: 43

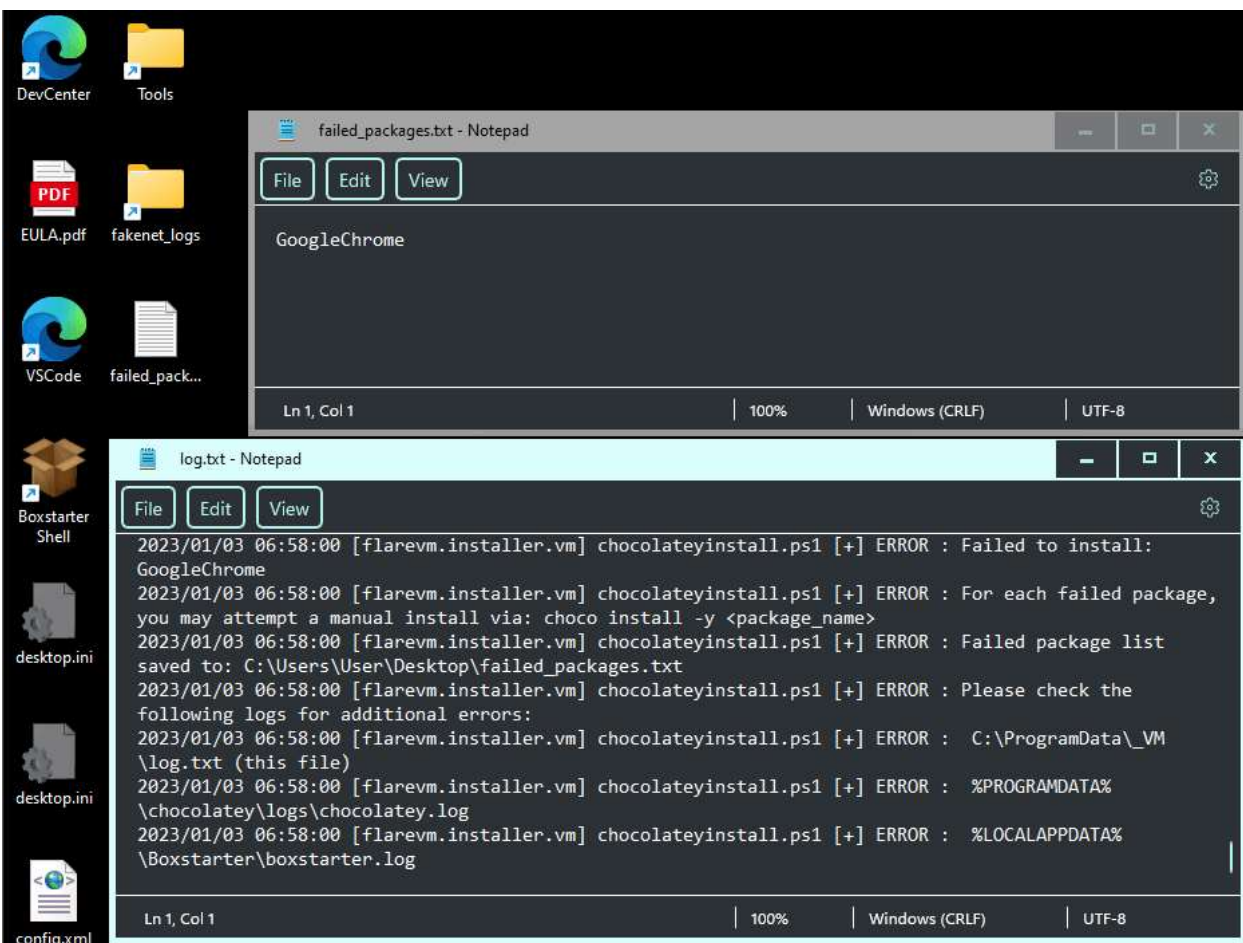
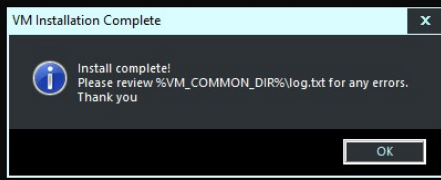
Reset

Let it ride and address any errors after you get the handy logs. Of course, I am not reporting a bug for Chrome. Just go get it!

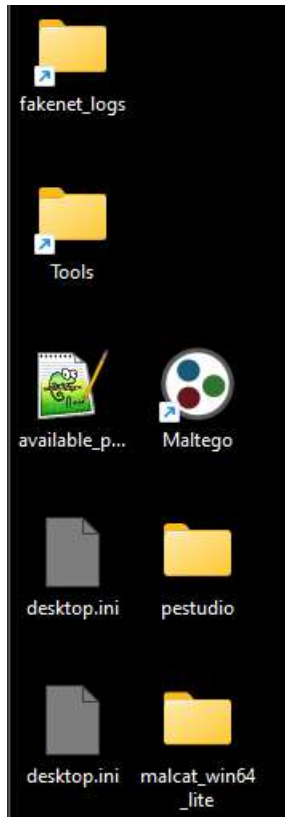
```
visualstudio2017-workload-vctools|1.3.3
visualstudio-installer|2.0.3
wireshark|4.0.2
wireshark.vm|4.0.2.20221221
x64dbg.ollydumpex.vm|1.80
x64dbg.vm|2021.05.08
x64dbgpy.vm|1.0.56.20211021
yara|4.2.3
yara.vm|4.2.3

2023/01/03 06:58:00 [flarevm.installer.vm] chocolateyinstall.ps1 [+] ERROR : Failed to install: GoogleChrome
2023/01/03 06:58:00 [flarevm.installer.vm] chocolateyinstall.ps1 [+] ERROR : For each failed package, you may attempt a
manual install via: choco install -y <package_name>
2023/01/03 06:58:00 [flarevm.installer.vm] chocolateyinstall.ps1 [+] ERROR : Failed package list saved to: C:\Users\User
\Desktop\failed_packages.txt
2023/01/03 06:58:00 [flarevm.installer.vm] chocolateyinstall.ps1 [+] ERROR : Please check the following logs for additio
nal errors:
2023/01/03 06:58:00 [flarevm.installer.vm] chocolateyinstall.ps1 [+] ERROR : C:\ProgramData\_VM\log.txt (this file)
2023/01/03 06:58:00 [flarevm.installer.vm] chocolateyinstall.ps1 [+] ERROR : %PROGRAMDATA%\chocolatey\logs\chocolatey
.log
2023/01/03 06:58:00 [flarevm.installer.vm] chocolateyinstall.ps1 [+] ERROR : %LOCALAPPDATA%\Boxstarter\boxstarter.log
[-] Please check the following logs for any errors:
[-] C:\ProgramData\_VM\log.txt
[-] %PROGRAMDATA%\chocolatey\logs\chocolatey.log
[-] %LOCALAPPDATA%\Boxstarter\boxstarter.log

1
True
```



It was only after all of this that I downloaded PeStudio <<https://www.winitor.com/download>> and MalCat <https://malcat.fr/latest/malcat_win64_lite.zip> to round out my ideal setup. I also decided to expand my investigative scope with Maltego <<https://www.maltego.com/downloads/>> for some OSINT-ing.



The only big tasks left were:

1. Snapshot
2. Remove bloatware
3. Disable autoruns such as Cortana
4. Tighten privacy settings
5. Disable the NAT'd NIC so I'm officially Host-only
6. Reboot
7. Finally, Snapshot my baseline system.

Happy hunting!