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, plus deleting a NIC set to NAT after all your tool downloads are done feels way easier to me than reconfiguring the same NIC as well as your Adapter Properties)

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. The stackoverflow thread on Defender really saved me some headache; shout out to the FLARE team for that hint!

```
> **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-antivi
      rus.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, running "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.

```
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
```

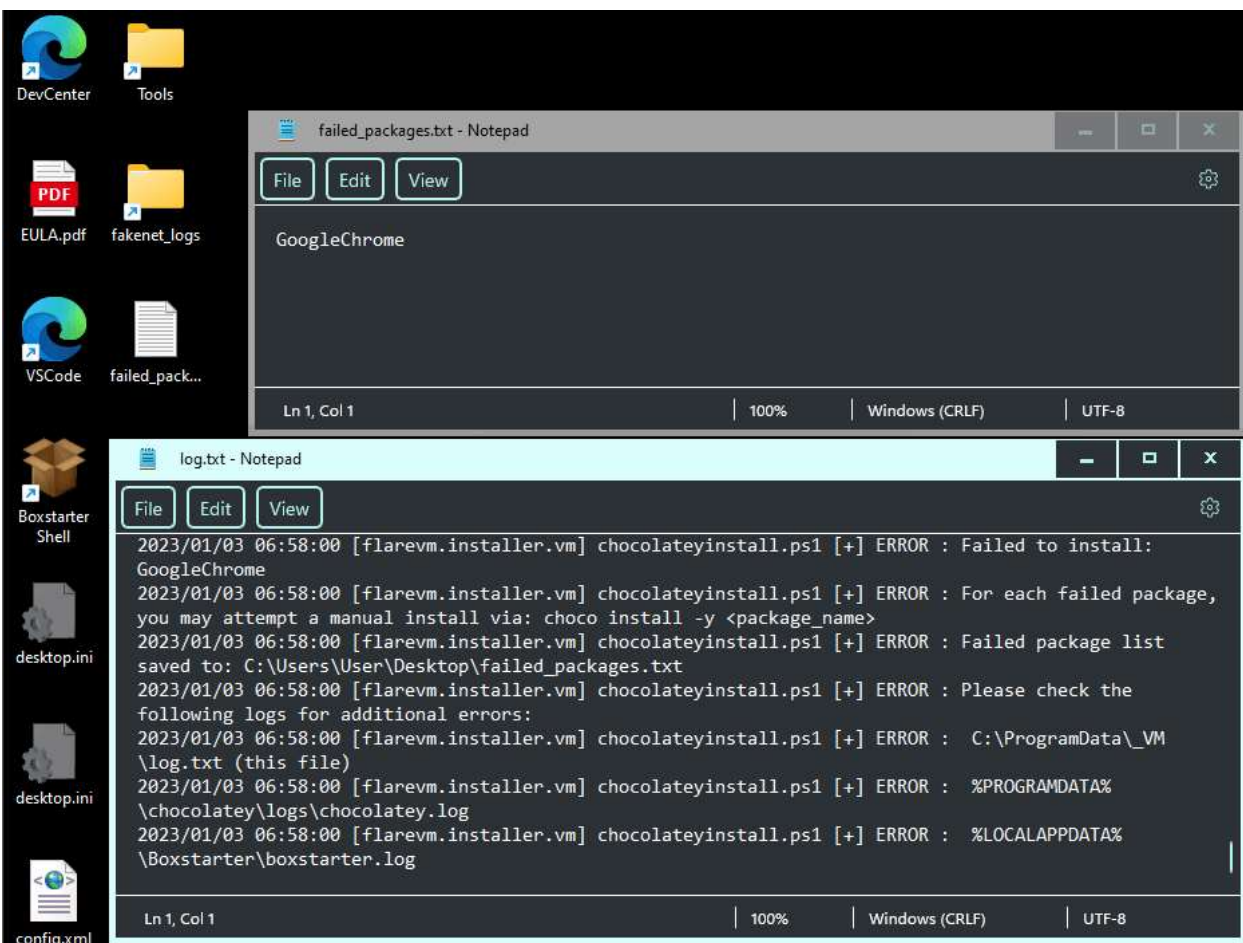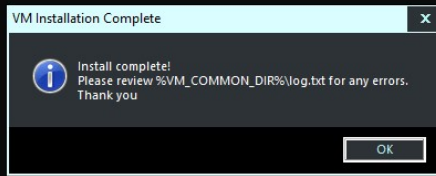At last, the install script will fully engage and present you with a GUI for granular control of tool packages:

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!

It was only after all of this that I downloaded PeStudio and MalCat to round out my ideal setup. The only big tasks left were Snapshot > Remove bloatware + disable autostarts + tighten privacy settings + disable 1 NIC so I'm officially Host-only + reboot > finally, Snapshot my baseline system.

Feel free to take it for a spin at your own risk. Happy hunting!

https://tinyurl.com/3xuajryt