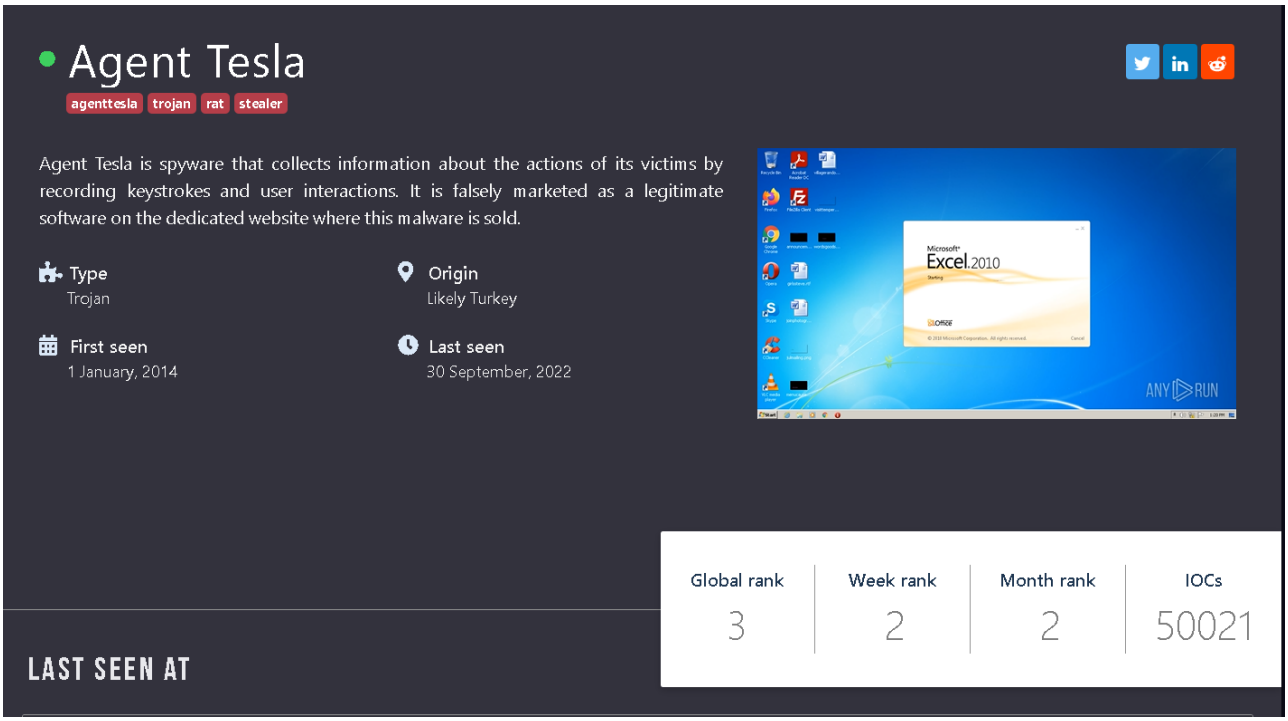
Worcester Polytechnic Institute
Department of Computer Science

Module 2: Volatility

Objectives

- Use the forensics tool Volatility to analyze a memory image, identifying the running processes using different plugins and comparing their results
- Recognize suspicious system processes by listing the DLLs, command lines, and handles for each process
- Analyze the registry information to identify the persistence mechanisms

You MUST use a Windows 7 virtual machine and NOT your host machine because this module requires downloading and running malware. This malware can record keystrokes so do NOT log into any websites after infecting the virtual machine.



Tasks

(If you are using the prepared virtual machine and have already used WinPMem on it in the previous module, skip to Task 1, step 6).

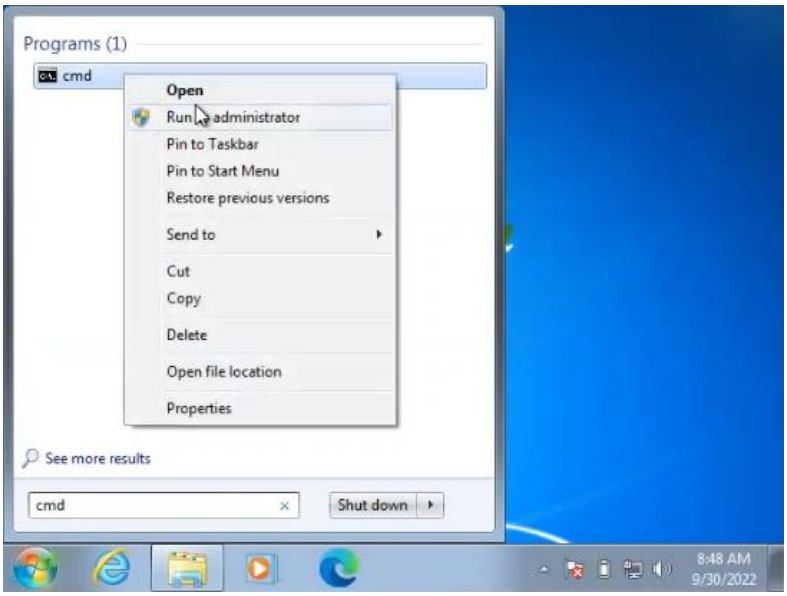
Task 0: Preparing a Windows 7 Virtual Machine

Follow the steps in Activity 10-1 to create a Windows 7 Virtual Machine.

Task 1: Preparing the clean and infected images.

1. We are going to use WinPmem to get a memory dump of our machine before we

infect it. Search “cmd” and right click it to run the command line as an administrator.



2. Once you are in the command line, navigate to the folder where you have WinPmem and run the command:

   (your version of winpmem).exe (name of your raw file).raw

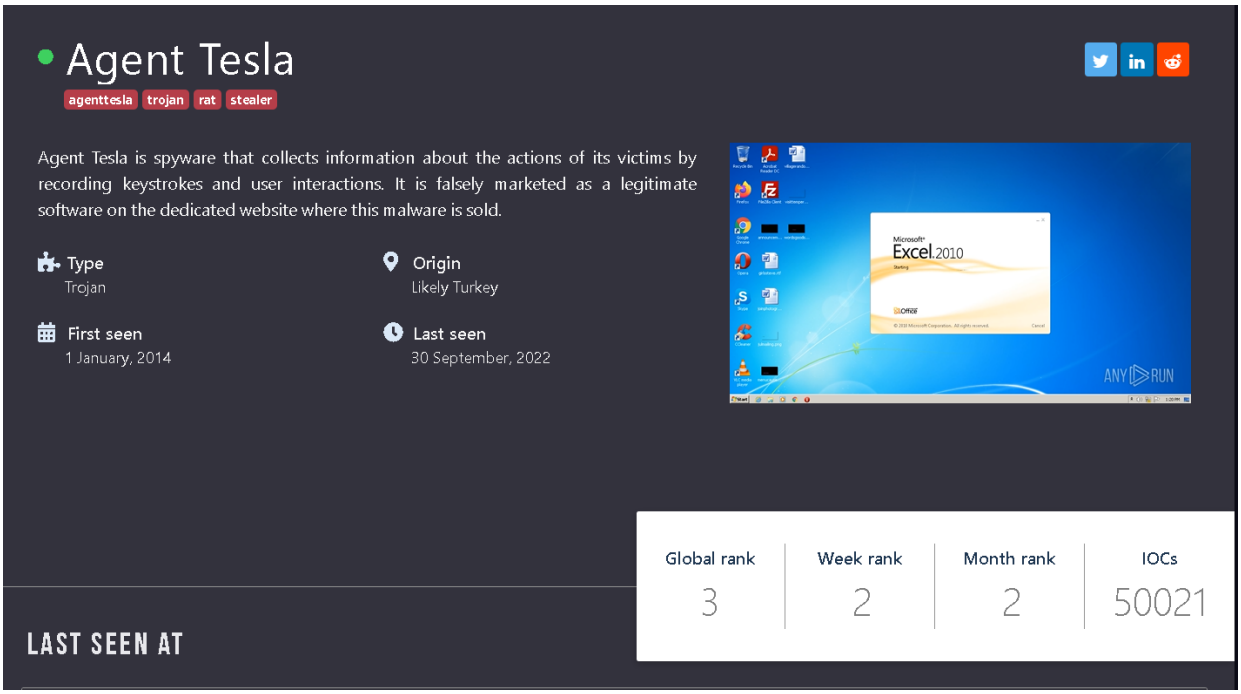
   In the following screenshot the version of winpmem we are using is winpmem_mini_x64_rc2 and we are naming our raw file “clean” so we entered “winpmem_mini_x64_rc2.exe clean.raw”

```
C:\Windows\system32>cd ..
C:\Windows>cd ..
C:\>cd Users\root\Desktop
```

```
C:\Users\root\Desktop>winpmem_mini_x64_rc2.exe clean.raw
```

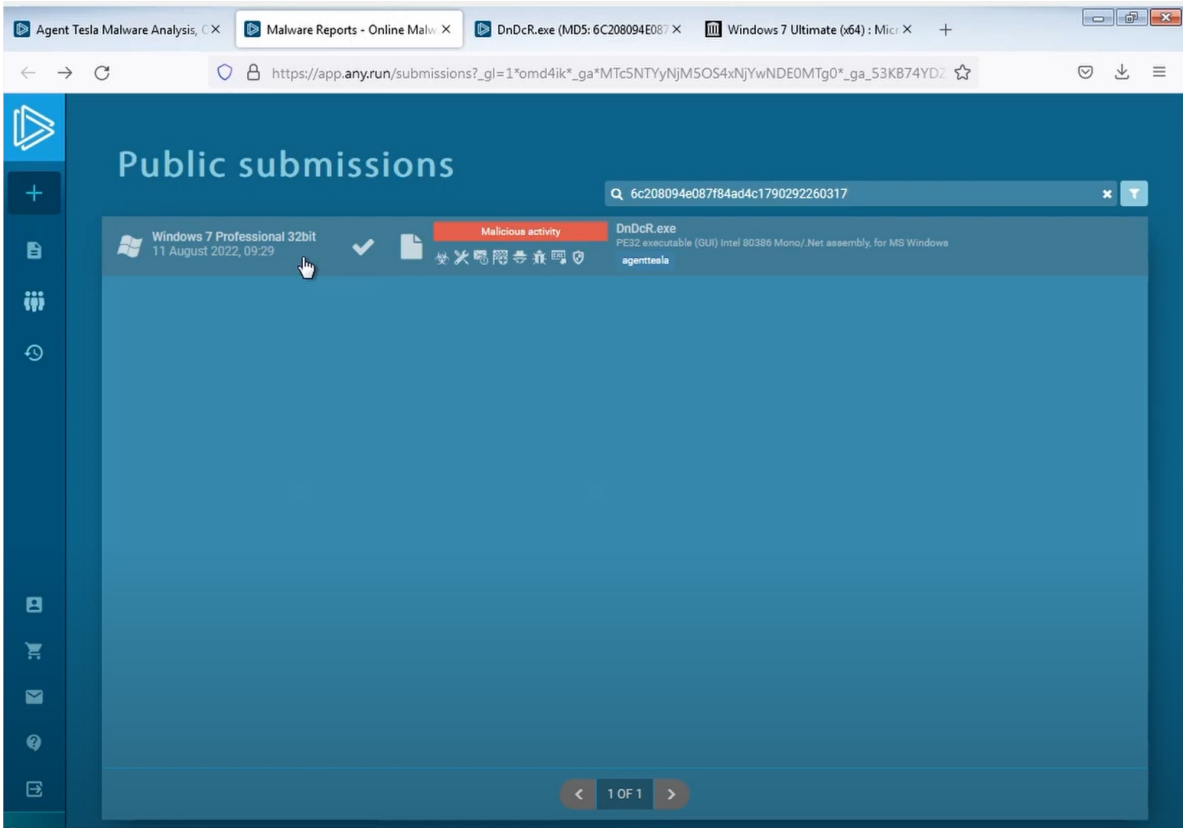
   Once it is done, you should now see the .raw file in the same location you have WinPMem downloaded.

3. Now we are going to download malware called “Agent Tesla”



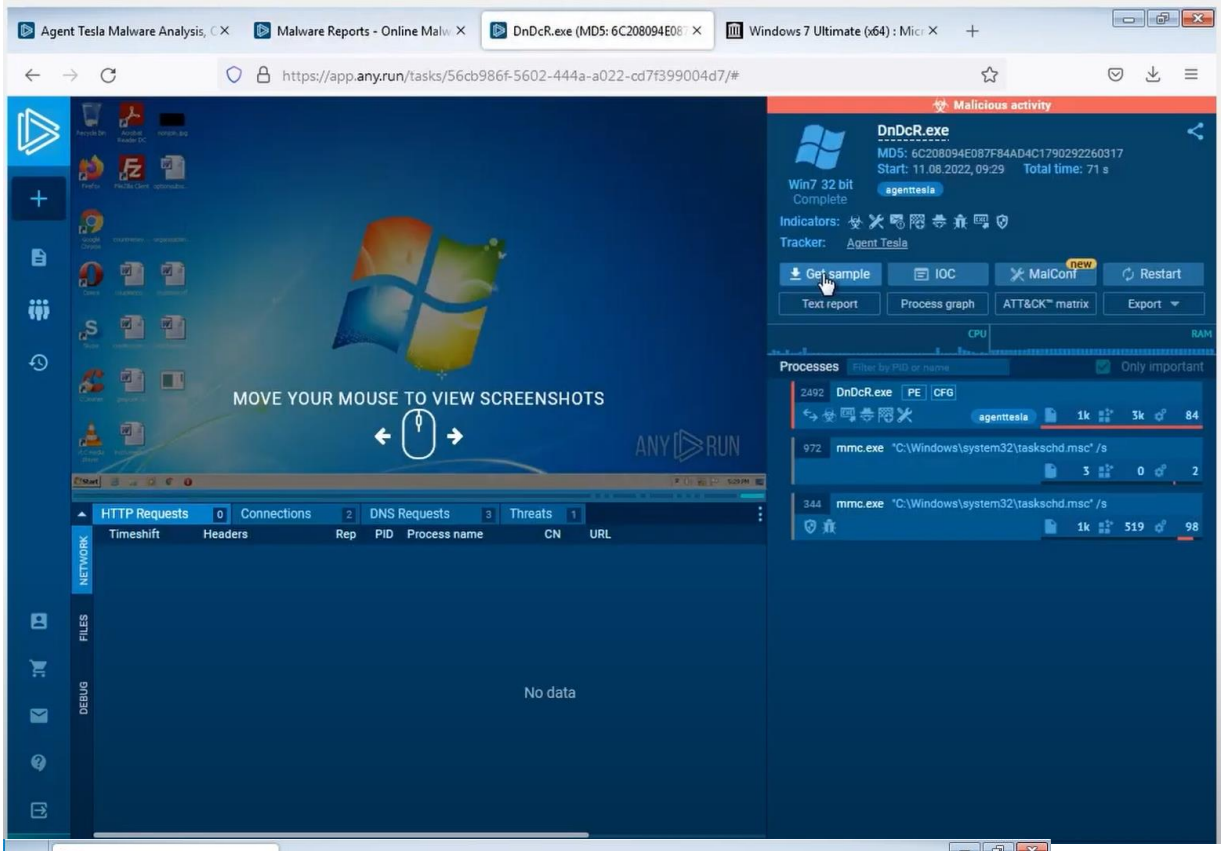
4. Go to https://app.any.run/submissions

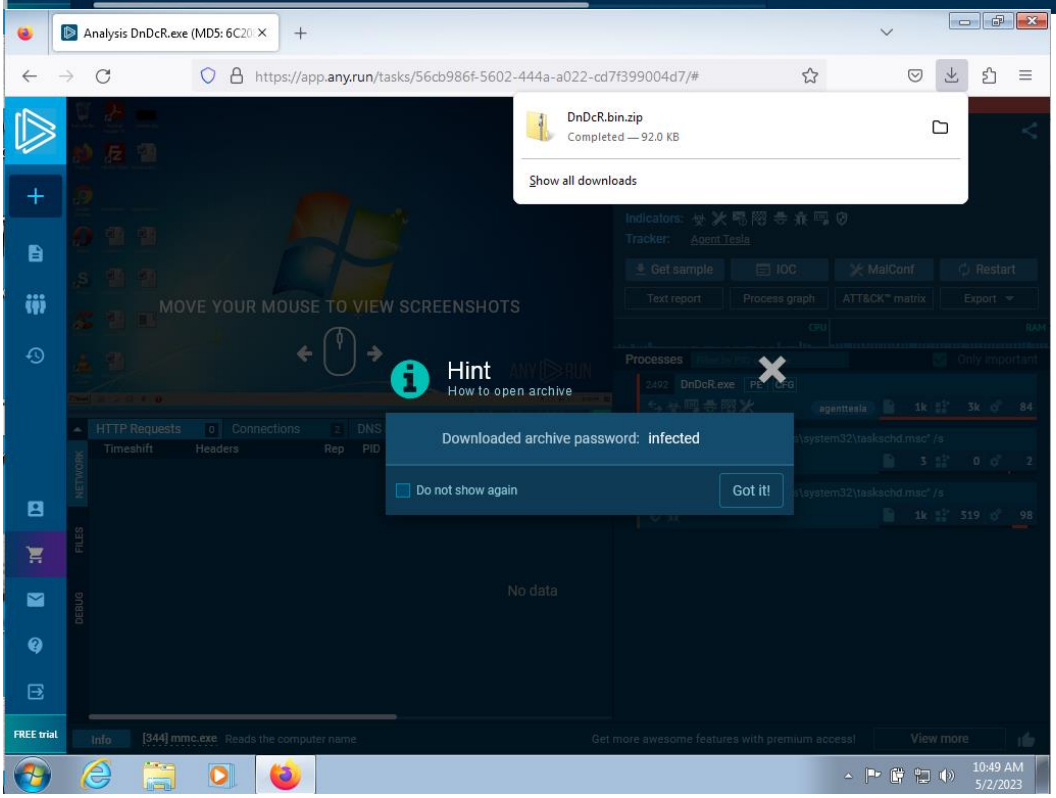
And search up this hash: 6c208094e087f84ad4c1790292260317



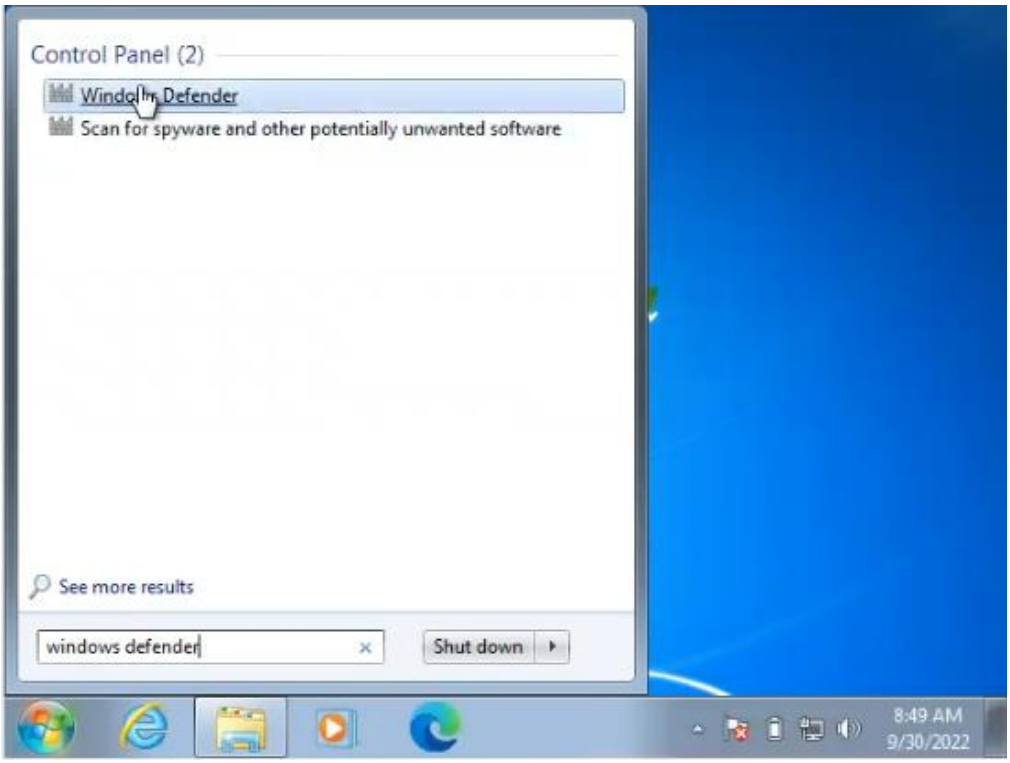
5. You will need an account to download the file. Once you have verified your email, click the DnDcR.exe file and click “Get Sample”. (Depending on the size of your screen, you may need to zoom in or out with the browser to see everything)

   Note that the password is “infected”.

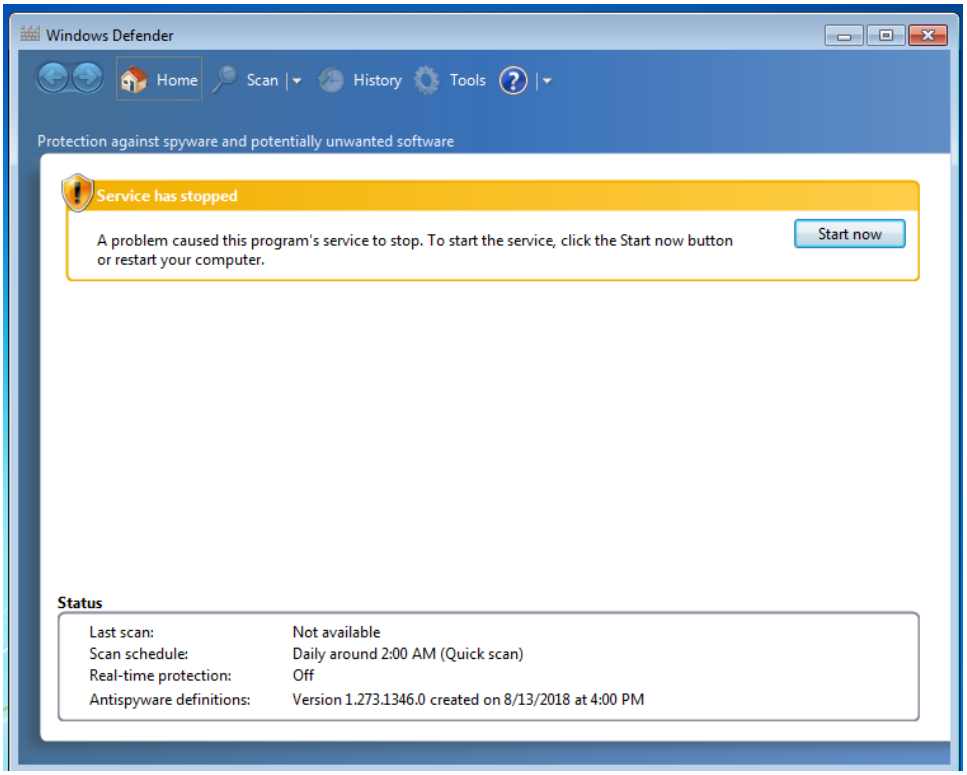




6. Now search for “Windows Defender” on your virtual machine and open it.

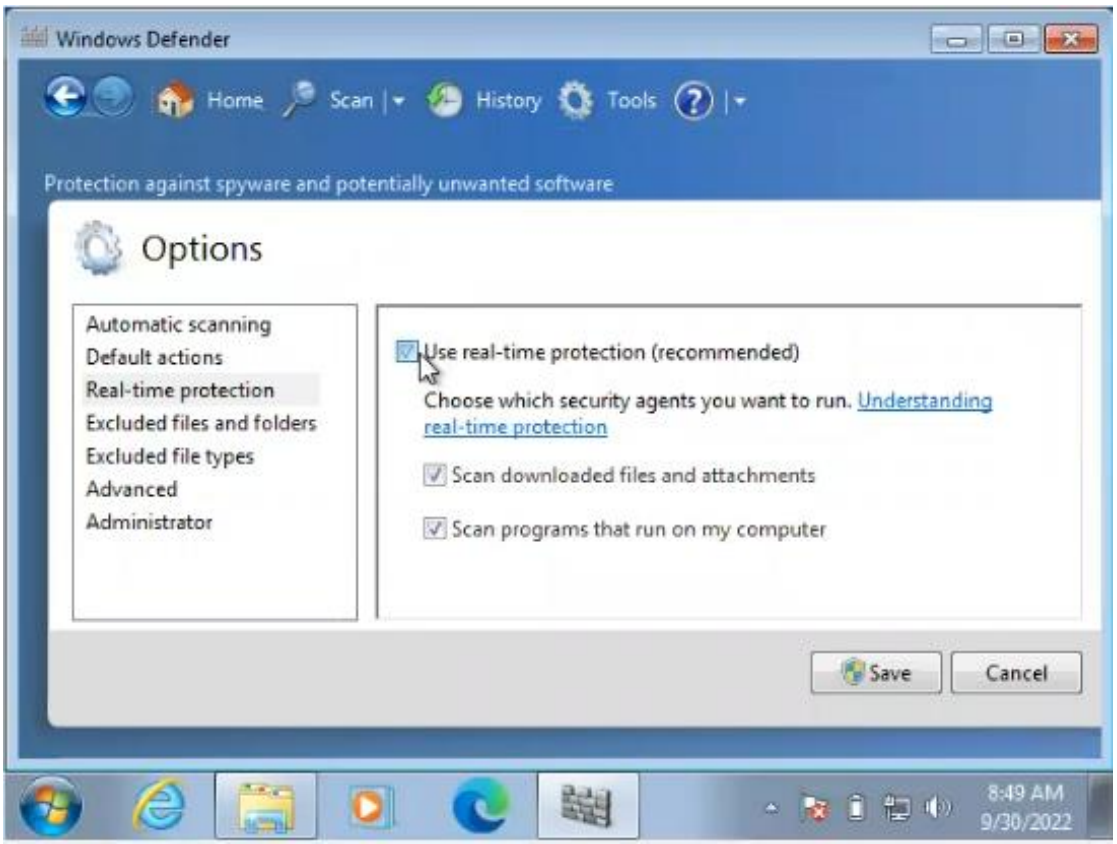


7. If you see this message, click “Start now”

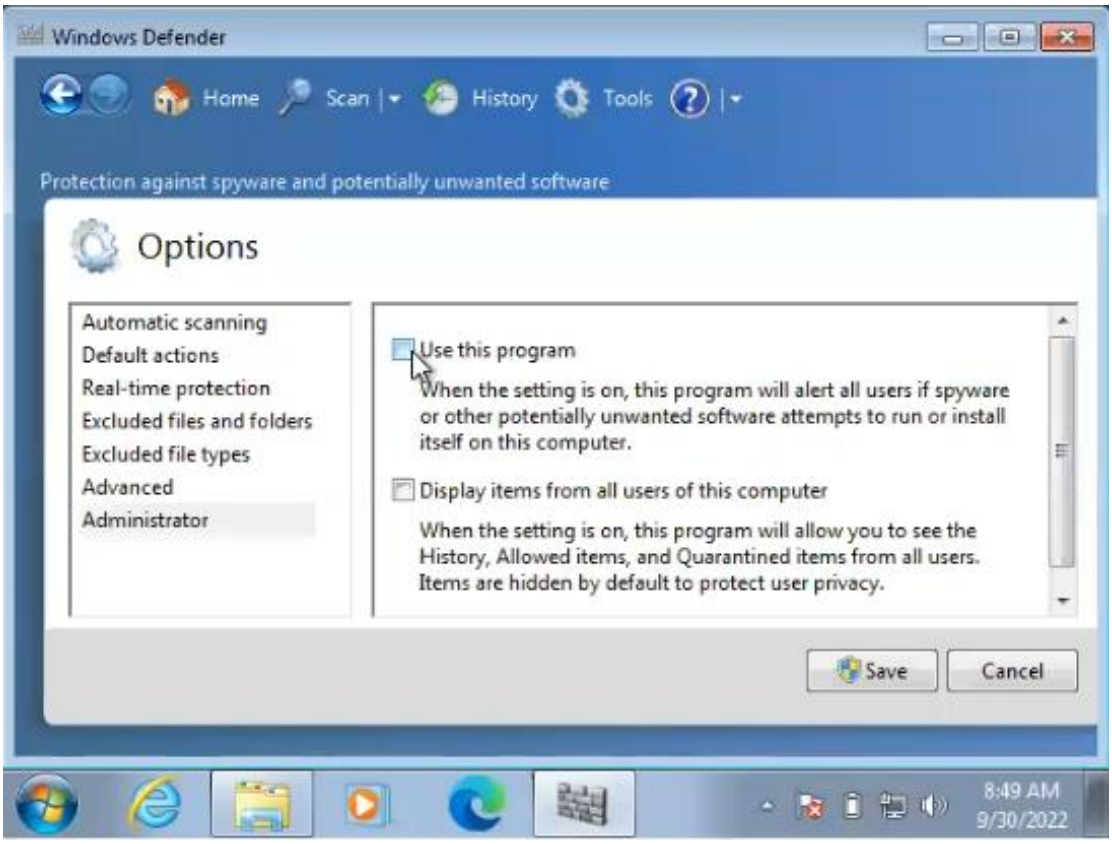


8. We need to make sure that Windows Defender will not turn on at all. Click “Tools” on the top and then click “Options”

9. Click “Real-time protection” and turn it off by unchecking “Use real-time protection”



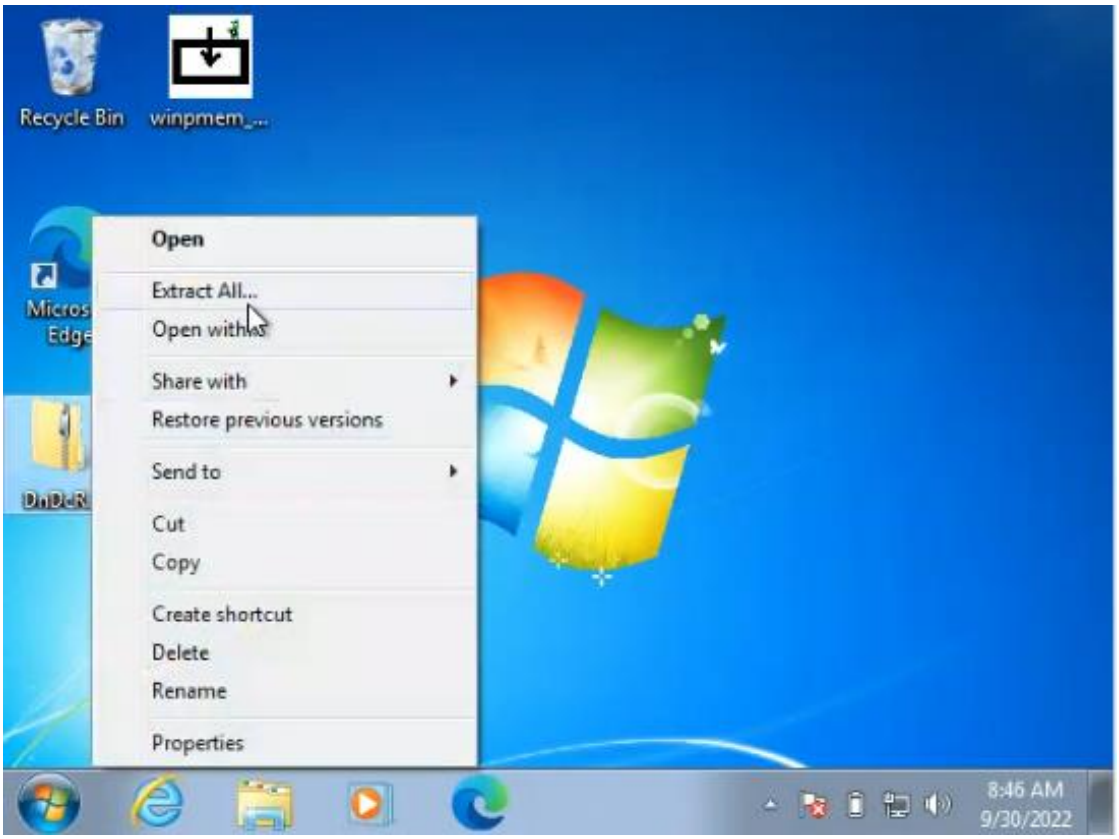
10. Now click “Administrator” and uncheck “Use this program”



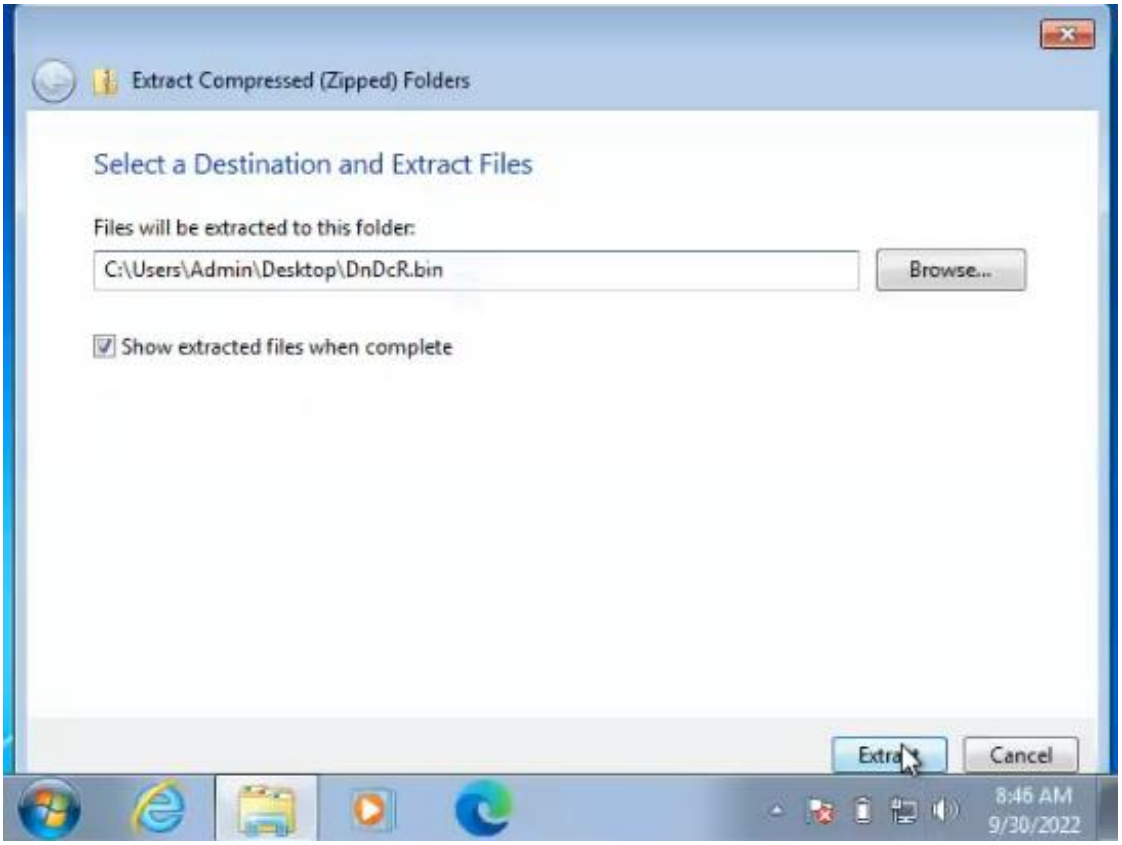
11. Now that we've gotten the memory dump of our clean machine and then turned off Windows Defender, let's extract our malware "Agent Tesla" that we previously downloaded.

(If you are using the prepared virtual machine, skip to step 13)

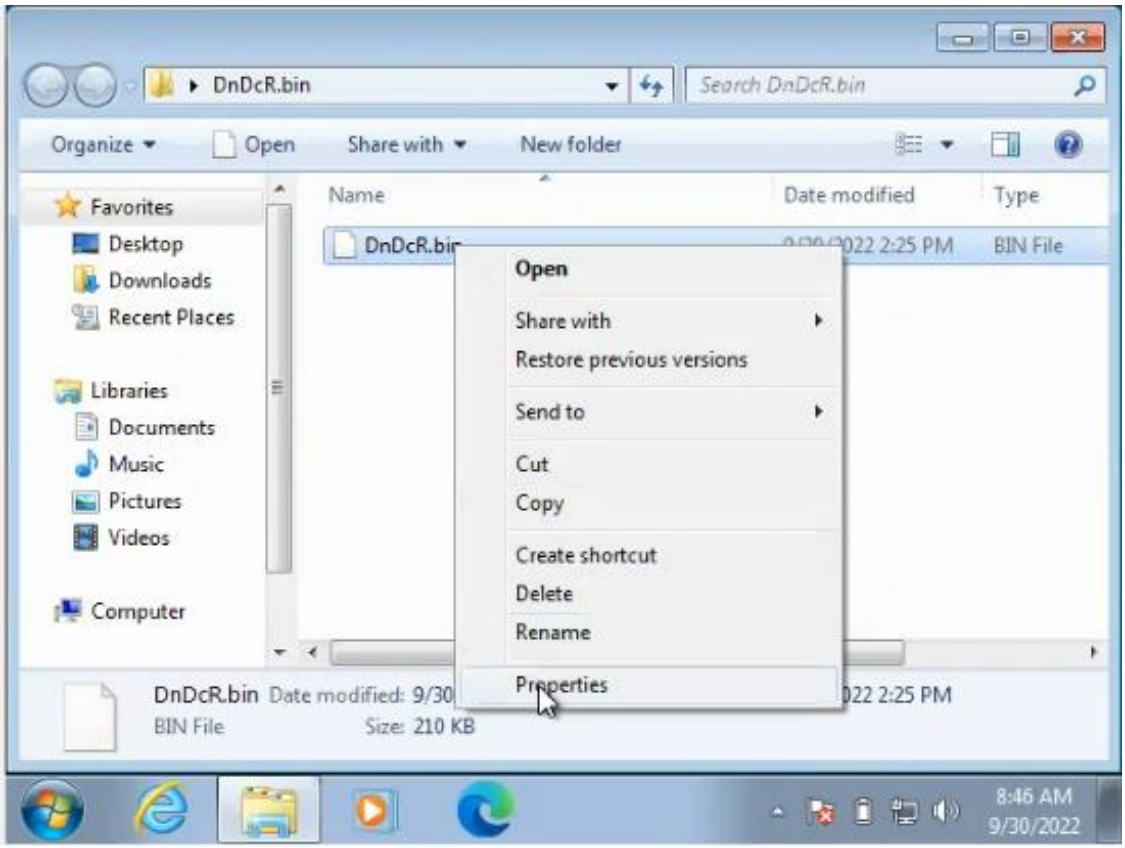
Right click the "DnDcR.bin" file and click "Extract All…"



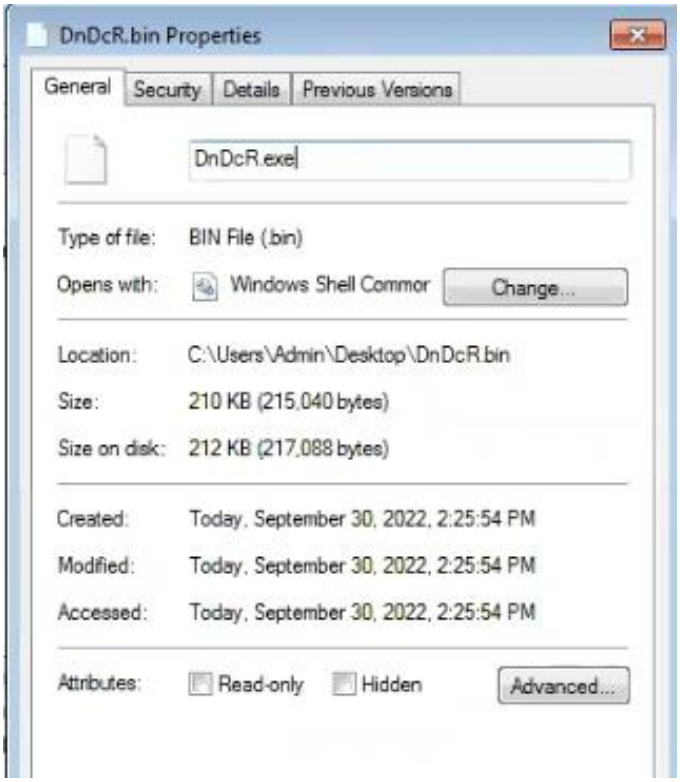
12. Click Extract. Remember the password is “infected”.



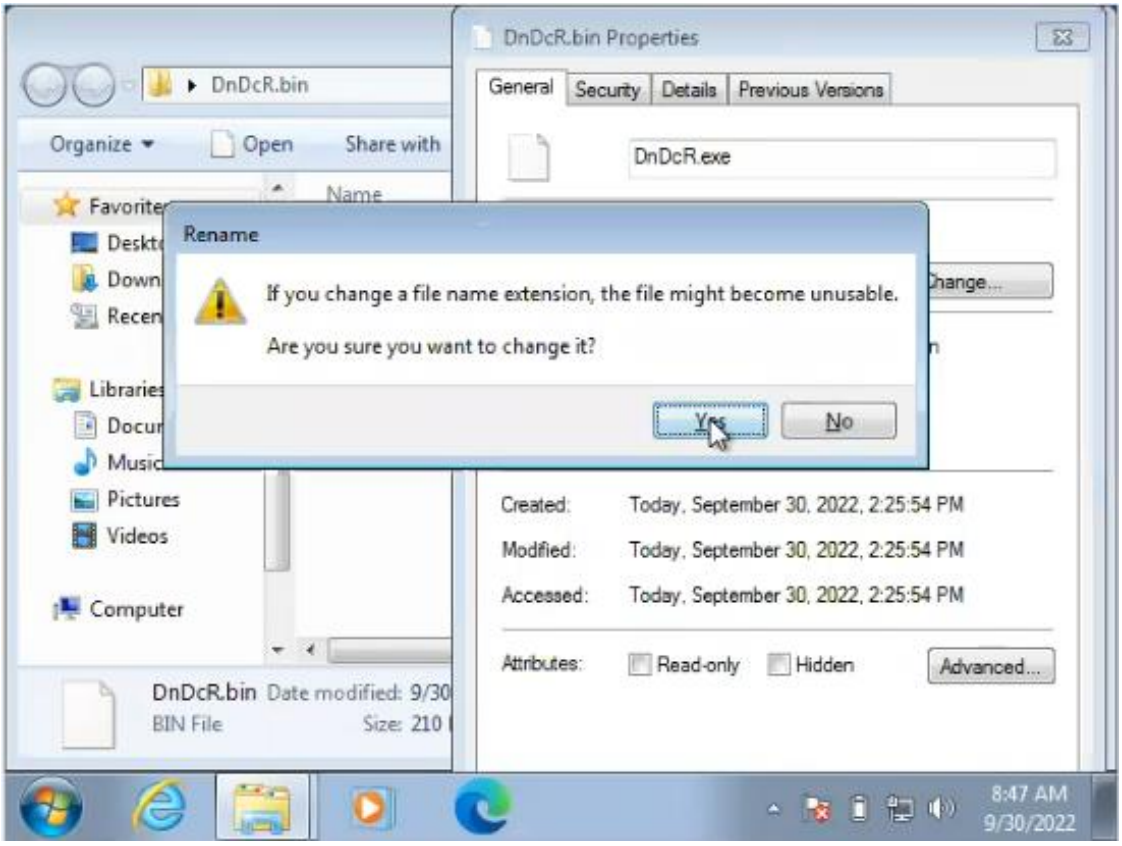
13. Once it is extracted, open the folder and right click the DnDcR.bin file and click “Properties”



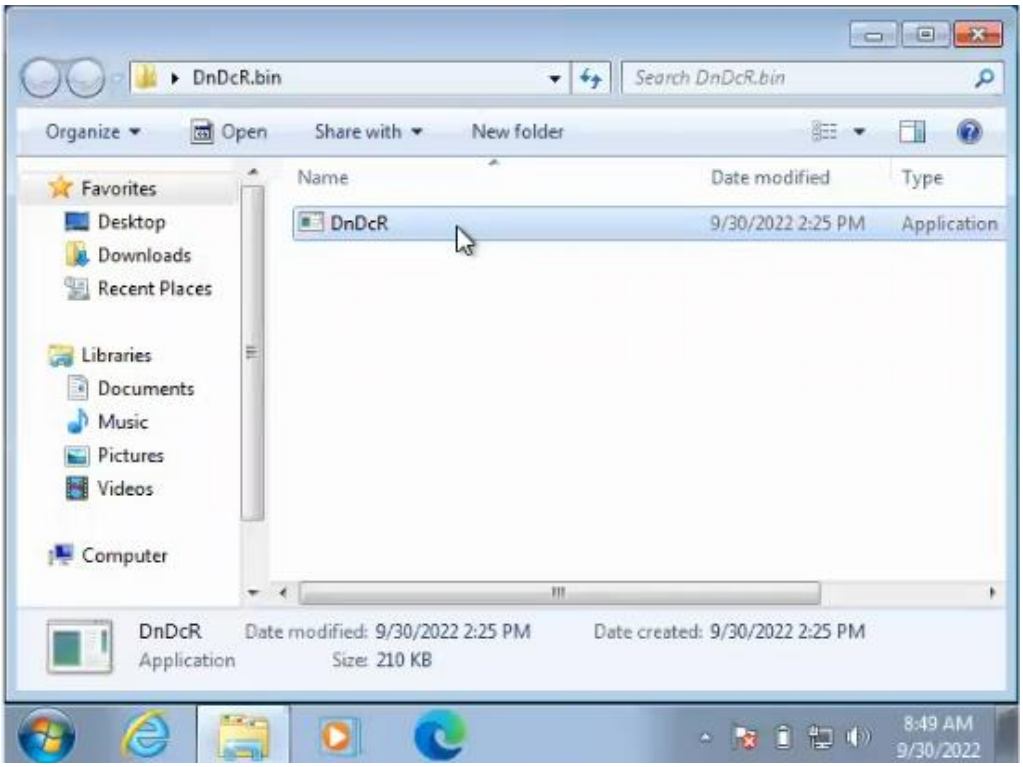
14. Now at the top of the window, change “DnDcR.bin” to “DnDcR.exe”



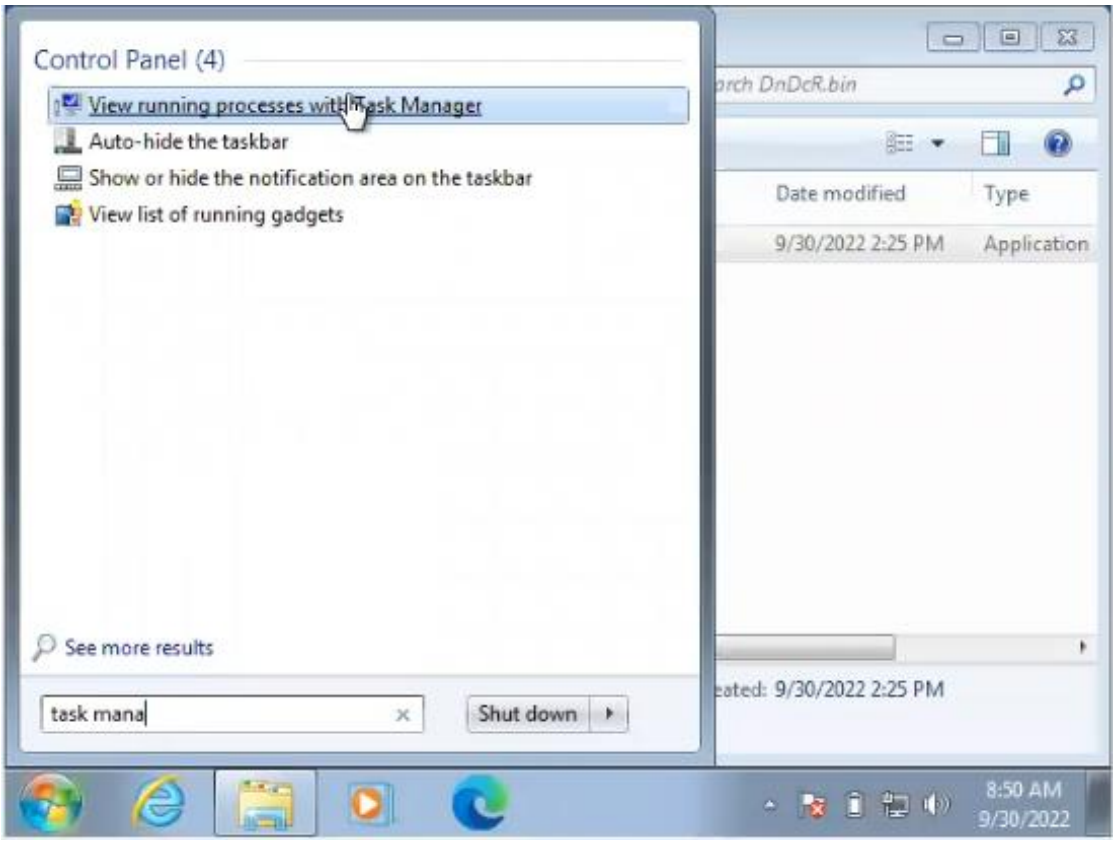
15. Now exit and click “Yes”



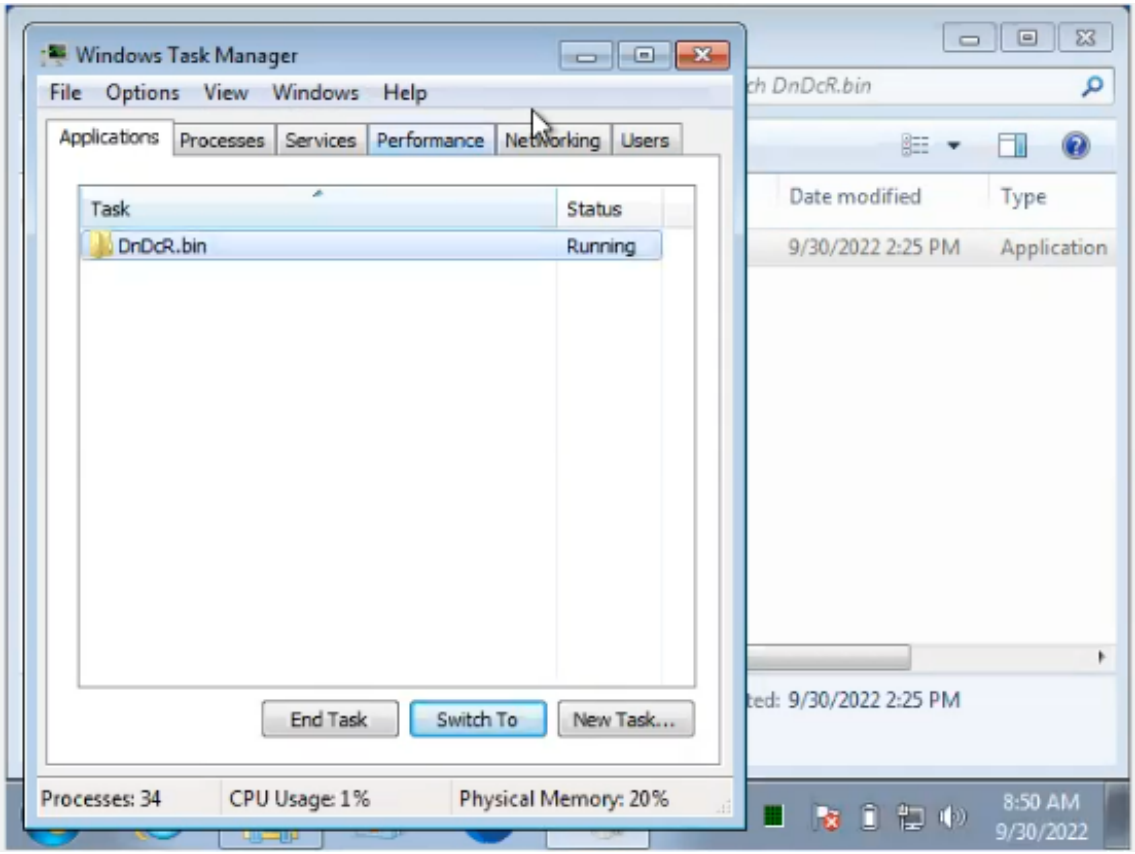
16. Now we can open our malware by double clicking it



17. Nothing will change visually, but we can verify our malware is running by searching up the task manager and clicking “View running processes with Task Manager”



18. Here we can see our malware is running



19. Now run the command line as an administrator again and type in the same WinPmem command but change the name of the raw file. In the following screenshot we are naming it “infected.raw”

```
C:\Windows\system32>cd ..

C:\Windows>cd ..

C:\>cd Users\root\Desktop
```

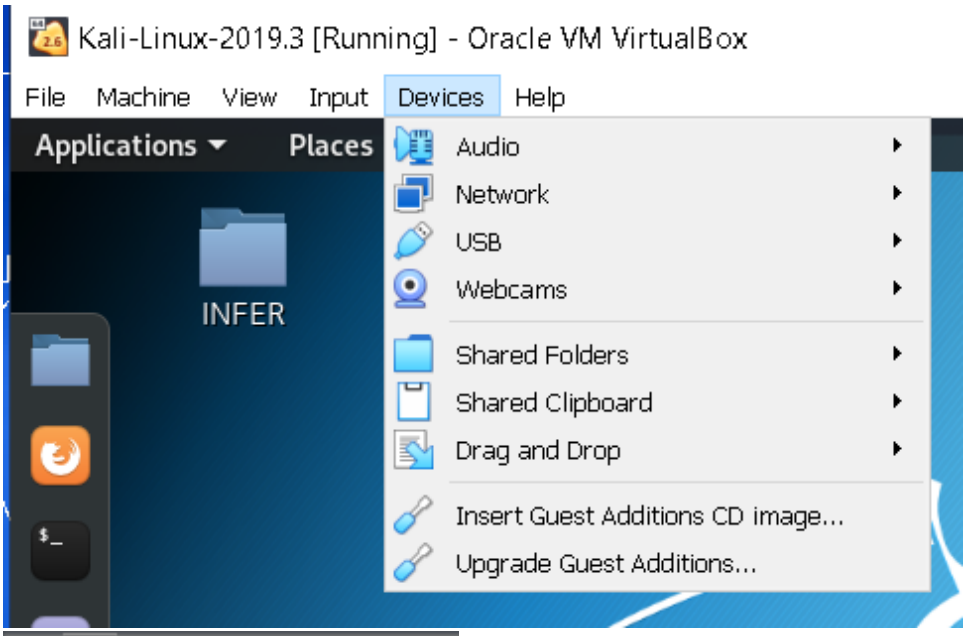
```
C:\Users\root\Desktop>winpmem_mini_x64_rc2.exe infected.raw
WinPmem64
Extracting driver to C:\Users\root\AppData\Local\Temp\pmeB4BF.tmp
Driver Unloaded.
Loaded Driver C:\Users\root\AppData\Local\Temp\pmeB4BF.tmp.
```

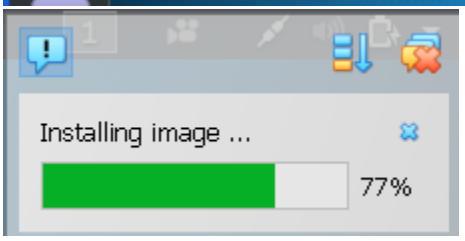
20. When you are done, you should have both a clean and infected raw file.

21. Move your clean and infected raw files to a kali linux virtual machine.

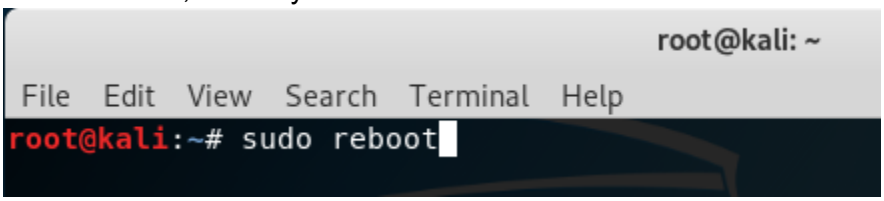
If you're using the prepared virtual machines, you can drag and drop it onto the prepared Kali linux machine by opening the Desktop directory on the Kali linux machine and dragging the file from the Windows 7 machine directly into that Desktop directory **then skip to step 23**.

If you are using a newer version of VirtualBox (such as 7.0.8), you will need to upgrade your Guest Additions to drag and drop your files. Click the Devices tab and select "Upgrade Guest Additions"





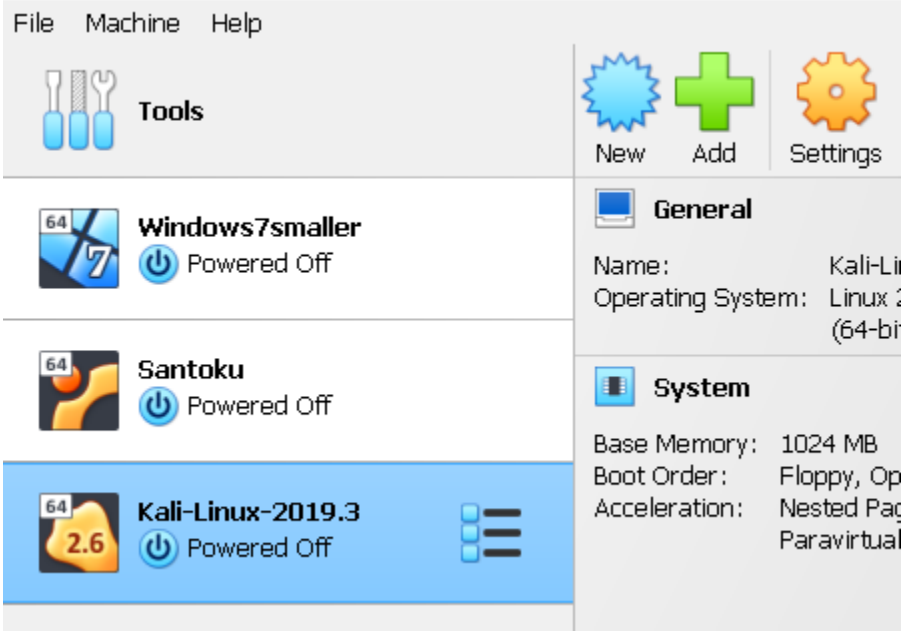
After it's done, reboot your virtual machine.



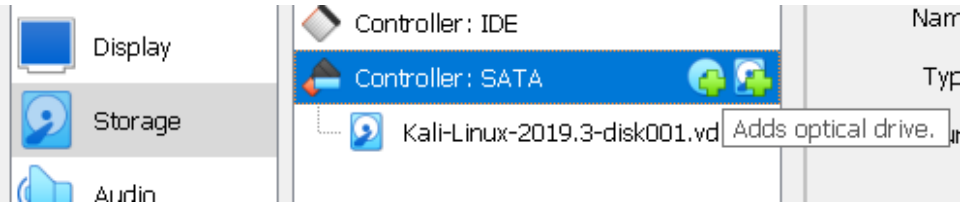
If upgrading your guest additions **didn't work**, here is a way to manually update them:

1.Power off the virtual machine

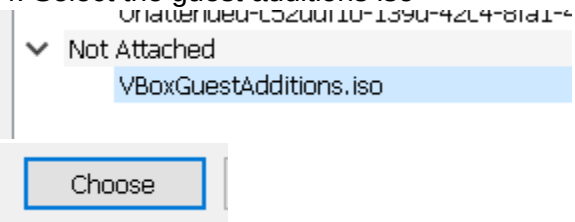
2. Go to settings



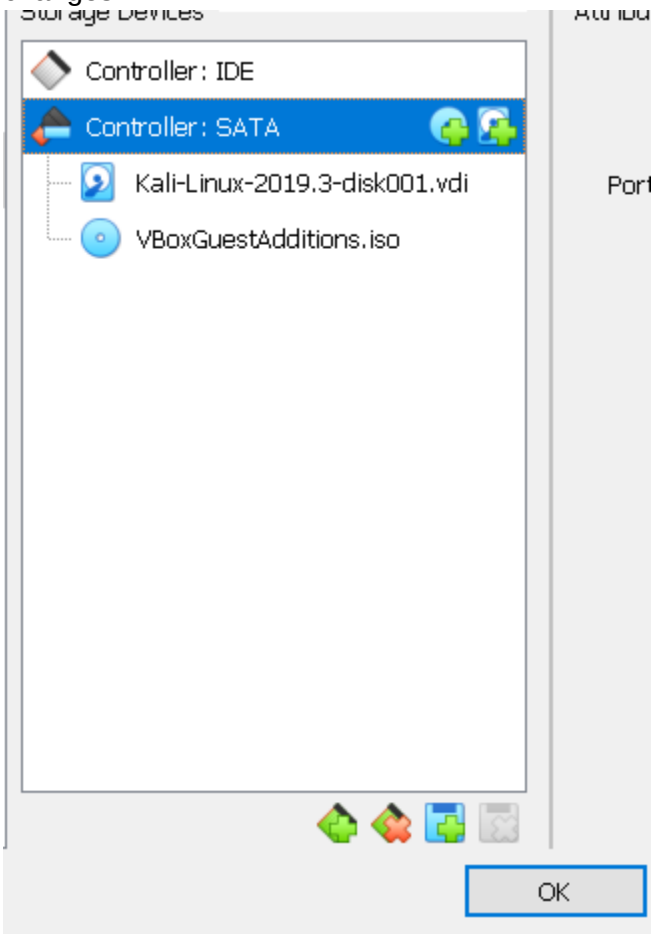
3. Go to storage and add an optical drive to IDE or SATA



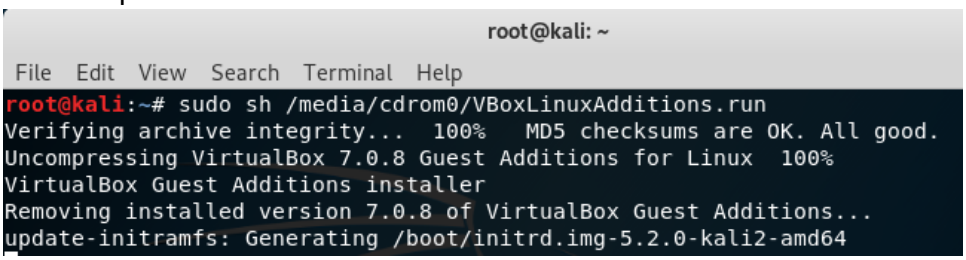
4. Select the guest additions iso



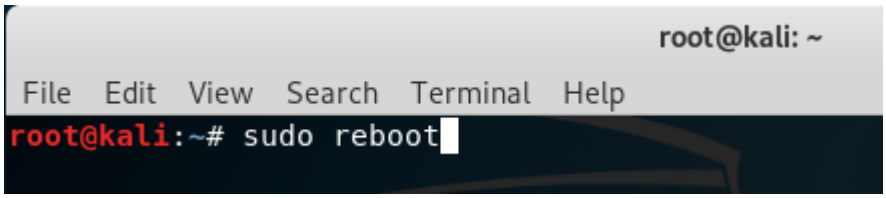
5. Now you should see the Guest Additions in the drive. Click OK to confirm your changes.



6. Now open the virtual machine and run the Guest Additions as an administrator

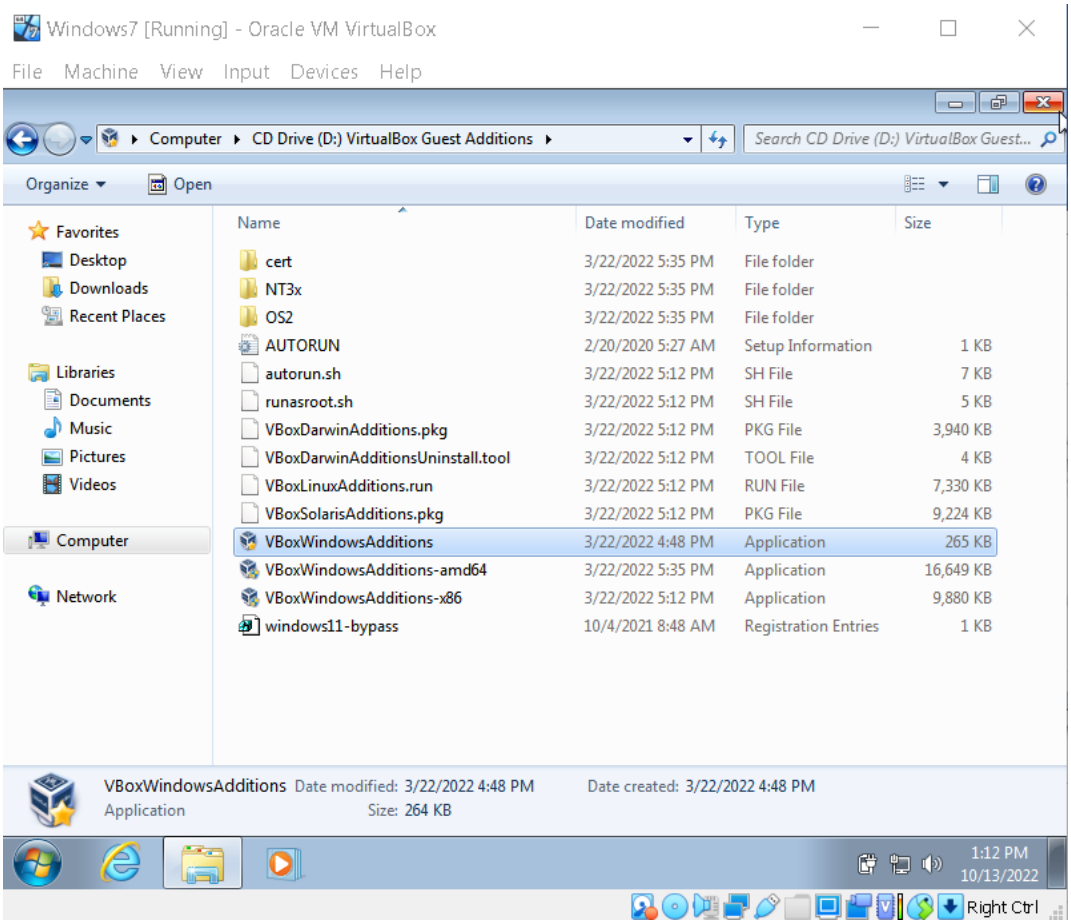


7. Then reboot the virtual machine

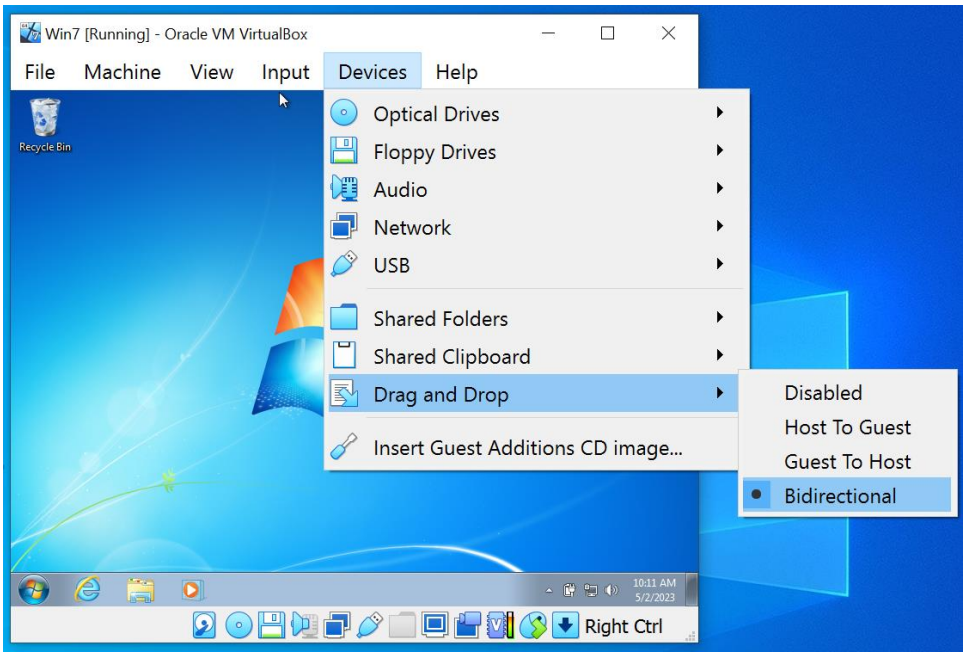


Otherwise if you are not using the premade virtual machines, to enable drag and drop, you will need to make sure Guest Additions are installed. If they are not, select Devices > Insert Guest additions

Now open your file explorer > Computer > CD Drive VirtualBox Guest Additions and install VBoxWindowsAdditions by right clicking it and running as administrator

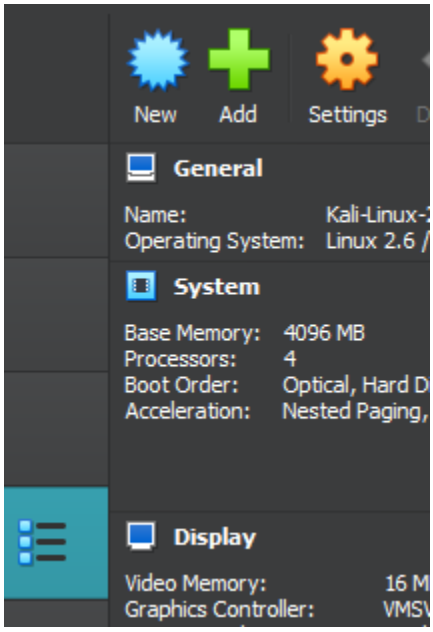


Now you can click Devices > Drag and Drop > Bidirectional

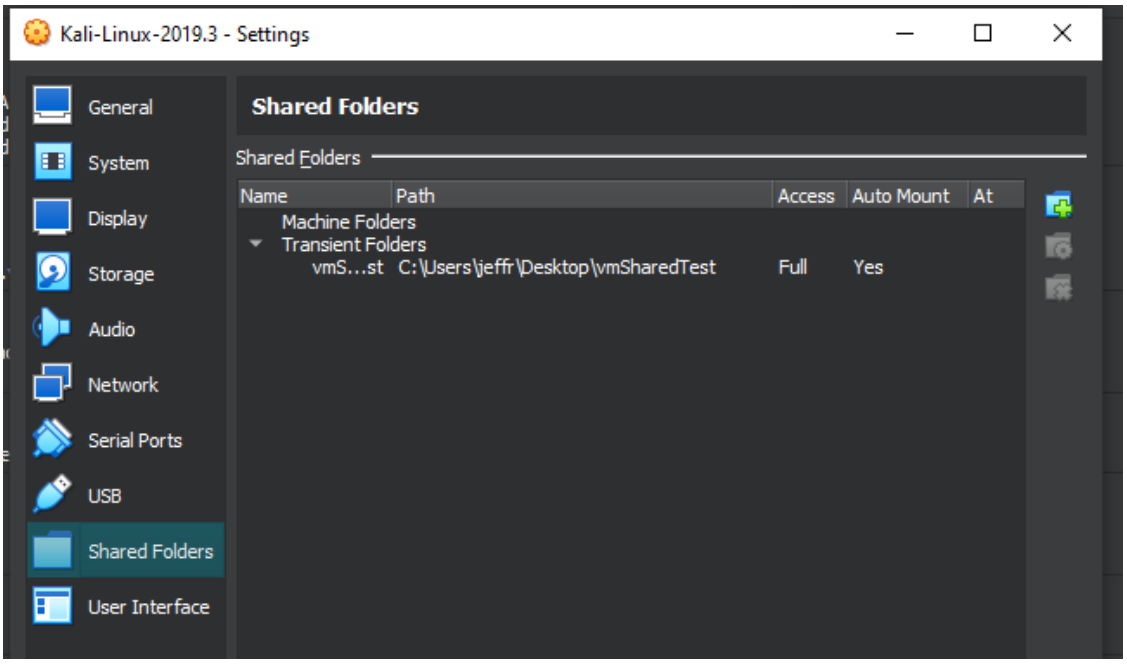


Please ask for help if you need it. If drag and drop still ends up not working on the kali vm, create a shared folder between your kali vm and your host machine. Do **NOT** log into any online file sharing services because Agent Tesla is malware and will keylog your credentials.

1. Create a folder on your host machine
2. Go to the settings of your kali vm

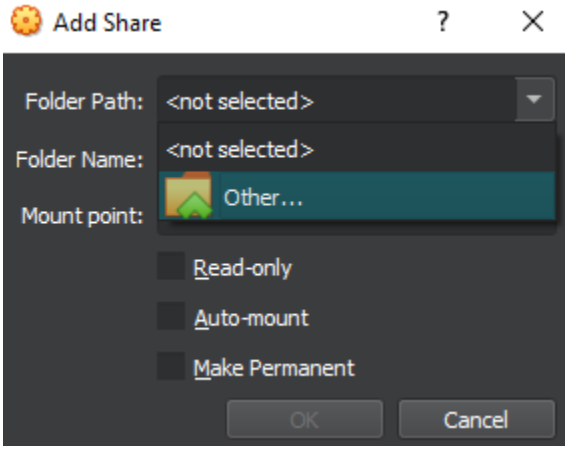


3. Go to the shared folders tab:

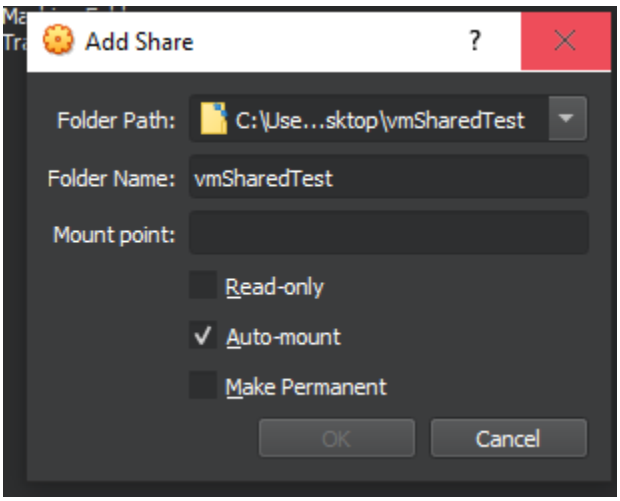


4. Click the add icon

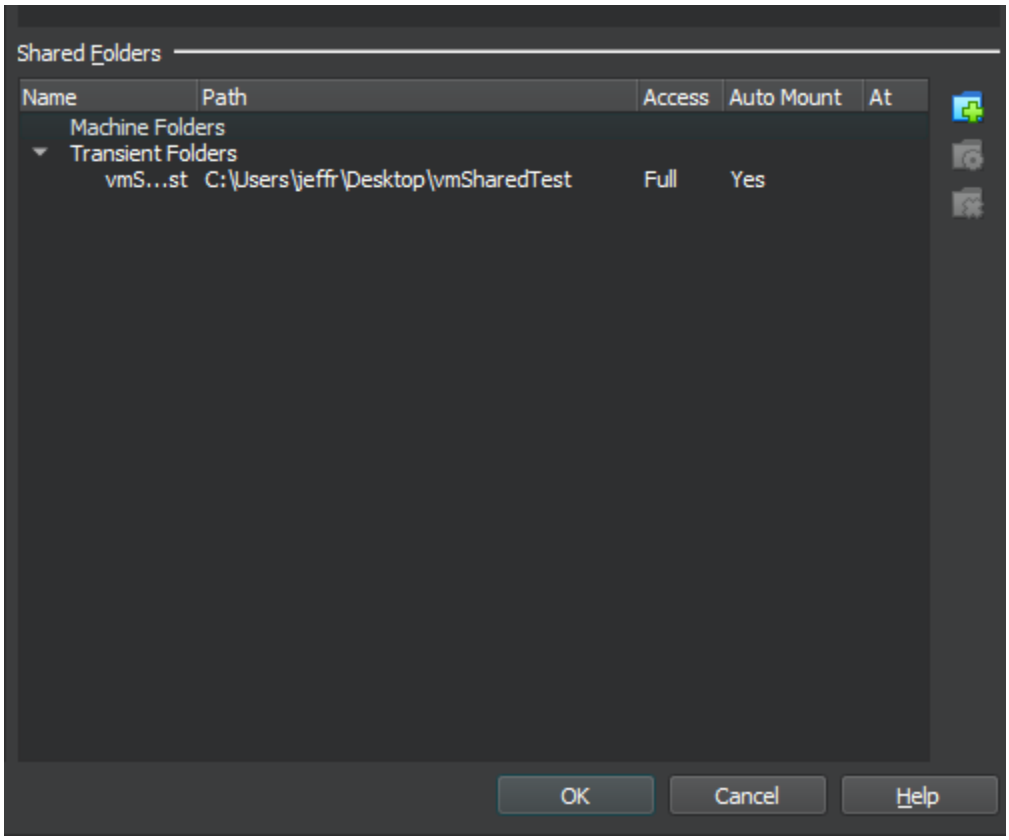
5. For folder path select “other” and find the folder you made on your host machine



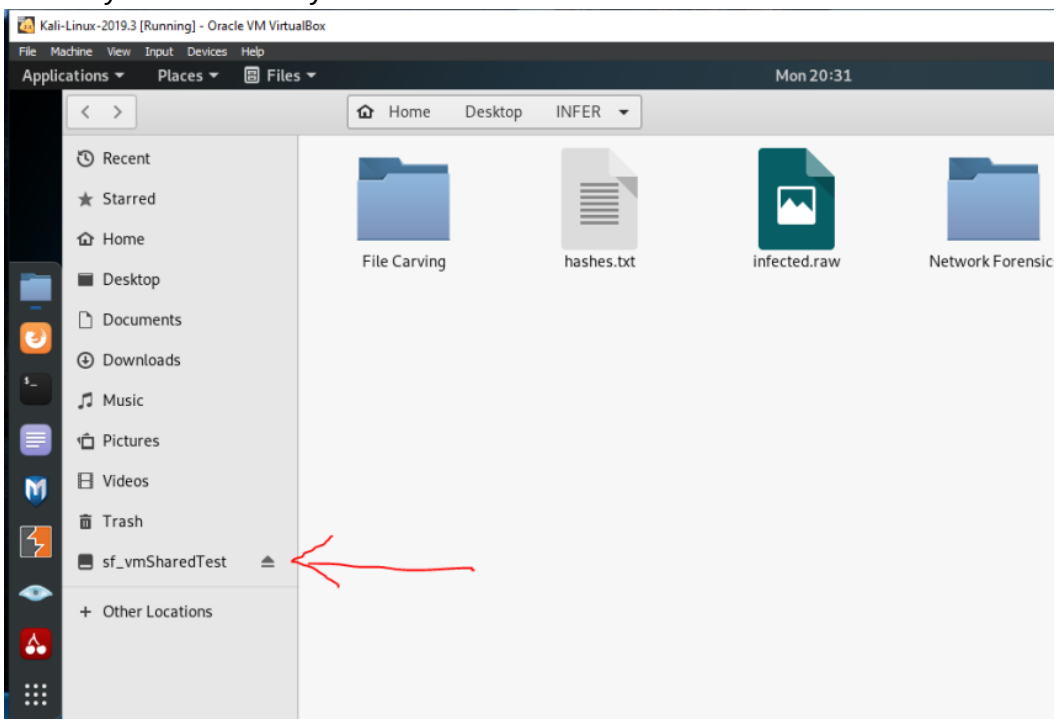
6. Select Auto-mount



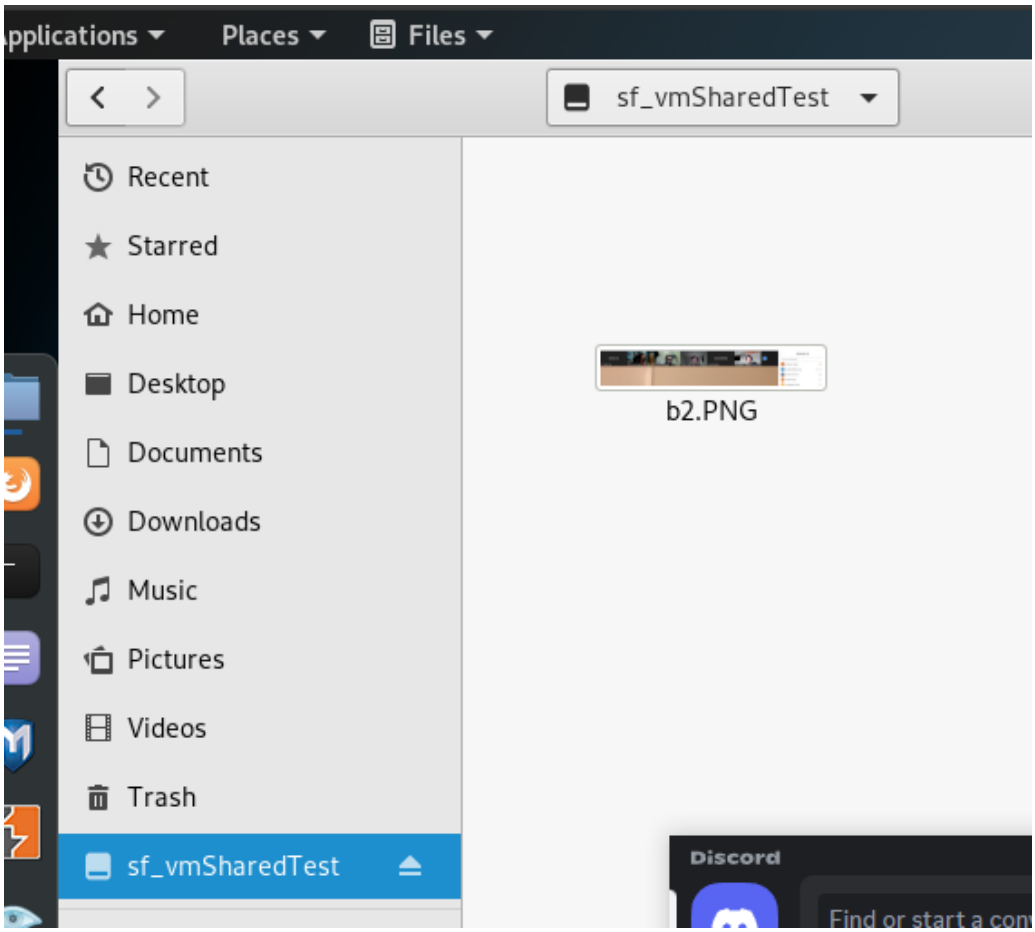
7. Click Ok and you should have something like this:



8. Now you should see your shared folder in the virtual machine



9. Now you can share files by putting files in the shared folder:



22. Now open up a new Kali Linux 2019 Virtual machine and run the following commands in the terminal to prepare the version of python and system dependencies that volatility requires:

    These commands install pip for python 2:

    1. sudo apt install -y python2 python2.7-dev libpython2-dev
    2. curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py
    3. sudo python2 get-pip.py
    4. sudo python2 -m pip install -U setuptools wheel

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# sudo apt install -y python2 python2.7-dev libpython2-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
libpython2-dev is already the newest version (2.7.16-1).
libpython2-dev set to manually installed.
python2 is already the newest version (2.7.16-1).
python2 set to manually installed.
python2.7-dev is already the newest version (2.7.16-3).
python2.7-dev set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali:~# curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.
py
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 1863k  100 1863k    0     0  1949k      0 --:--:-- --:--:-- --:--:-- 1947k
root@kali:~# sudo python2 get-pip.py
```

These commands install Volatility 2 and its Python dependencies:

5. python2 -m pip install -U distorm3 yara pycrypto pillow openpyxl ujson pytz ipython capstone

6. sudo python2 -m pip install yara

7. sudo ln -s /usr/local/lib/python2.7/dist-packages/usr/lib/libyara.so /usr/lib/libyara.so

8. python2 -m pip install -U git+https://github.com/volatilityfoundation/volatility.git

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
ERROR: You must give at least one requirement to install (see "pip help install"
)
root@kali:~# python2 -m pip install -U git+https://github.com/volatilityfoundati
on/volatility.git
DEPRECATION: Python 2.7 reached the end of its life on January 1st, 2020. Please
 upgrade your Python as Python 2.7 is no longer maintained. pip 21.0 will drop s
upport for Python 2.7 in January 2021. More details about Python 2 support in pi
p can be found at https://pip.pypa.io/en/latest/development/release-process/#pyt
hon-2-support pip 21.0 will remove support for this functionality.
Collecting git+https://github.com/volatilityfoundation/volatility.git
  Cloning https://github.com/volatilityfoundation/volatility.git to /tmp/pip-req
-build-I_psdh
  Running command git clone -q https://github.com/volatilityfoundation/volatilit
y.git /tmp/pip-req-build-I_psdh
Building wheels for collected packages: volatility
  Building wheel for volatility (setup.py) ... done
  Created wheel for volatility: filename=volatility-2.6.1-py2-none-any.whl size=
6563372 sha256=0da02315b8d43bca43d80d690ee4f02924de7d72a38ec685efe8ed45f85762bf
  Stored in directory: /tmp/pip-ephem-wheel-cache-yQcg07/wheels/7a/c4/2a/0a32e37
6b4c5a05335e0659f1633938e1f7ec4b2cd8708b7bc
Successfully built volatility
Installing collected packages: volatility
Successfully installed volatility-2.6.1
root@kali:~#
```

When you are done, you will have successfully installed volatility 2.6.1

Now navigate to where you had your infected raw file:

```
root@kali:~# ls
Desktop    Downloads   Music     Public     Videos
Documents  get-pip.py  Pictures  Templates
root@kali:~# cd Downloads
root@kali:~/Downloads# ls
infected.raw
```

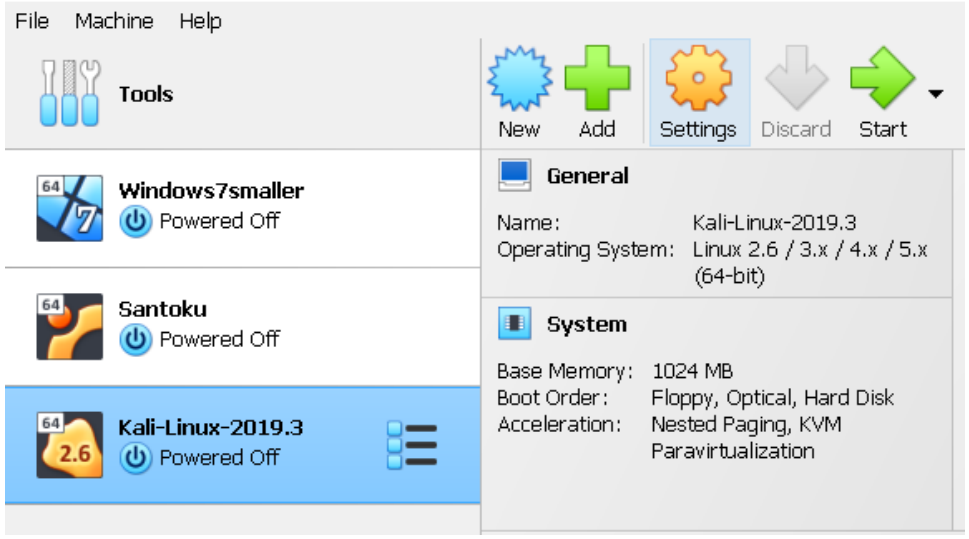
23. Before we can start analyzing anything, we need to get the profile of our raw file by entering:

    vol.py imageinfo -f <name of file or path to file>.raw

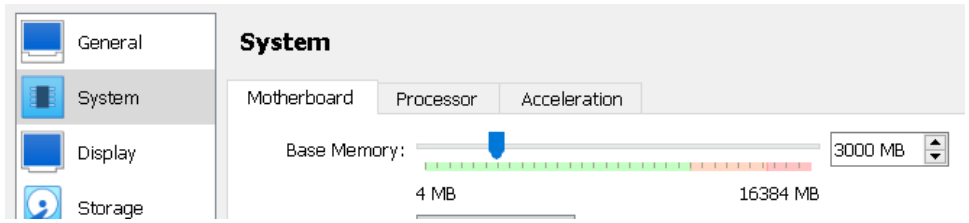
    Note: This step may be slow, be prepared to wait 5-10 minutes.

    If you would like to speed up the process, you can allocate more ram and processors to your Kali linux machine. This is optional, but highly recommended:

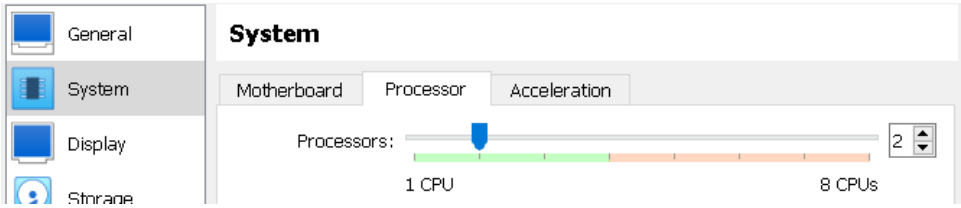
    1. Shut down the virtual machine
    2. Select your virtual machine and click settings



3. Go to system



As long as the system has already been shut down, you can adjust the base memory. 3000MB should be enough.



You can also add more processors. 2-4 should be enough.

When you are done, you can open your virtual machine back up.

The following screenshot had an infected raw file called “infected.raw” so the command used was:

vol.py imageinfo -f infected.raw

In the following screenshots the last profile in the list is used.

```
root@kali:~/Downloads# vol.py imageinfo -f infected.raw
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win200
8R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7S
P1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/Downloads/infected.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800029e9120L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff800029eb000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2022-09-30 15:51:34 UTC+0000
     Image local date and time : 2022-09-30 08:51:34 -0700
```

24. Let's run a process list on our infected file by entering the following command in the terminal:

    vol.py -f <name of file or path to file> --profile=<profile> pslist

```
root@kali:~/Downloads# vol.py -f infected.raw --profile=Win7SP1x64_23418 pslist
```

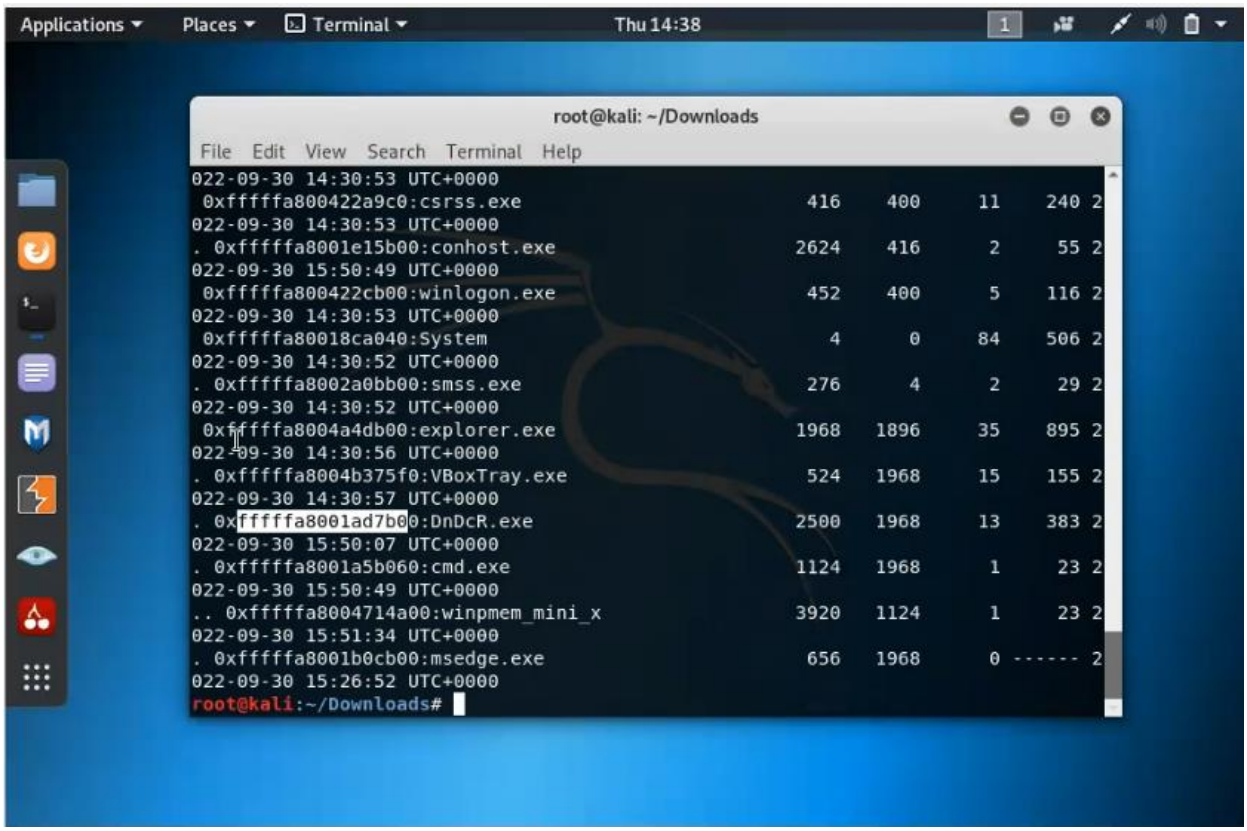
```
root@kali: ~/Downloads
File  Edit  View  Search  Terminal  Help
  0 2022-09-30 14:30:57 UTC+0000
0xfffffa8004b89b00 SearchIndexer.        2104    512     13      629      0
  0 2022-09-30 14:30:59 UTC+0000
0xfffffa8004a325f0 mscorsvw.exe          2332    512      6       82      0
  1 2022-09-30 15:24:59 UTC+0000
0xfffffa8004d9bb00 mscorsvw.exe          2132    512      5       75      0
  0 2022-09-30 15:24:59 UTC+0000
0xfffffa80019bf3d0 sppsvc.exe            1348    512      4      142      0
  0 2022-09-30 15:25:00 UTC+0000
0xfffffa8001b0cb00 msedge.exe             656   1968      0 --------      1
  0 2022-09-30 15:26:52 UTC+0000   2022-09-30 15:27:28 UTC+0000
0xfffffa8004584060 audiodg.exe            752    832      6      129      0
  0 2022-09-30 15:47:03 UTC+0000
0xfffffa8001ad7b00 DnDcR.exe             2500   1968     13      383      1
  1 2022-09-30 15:50:07 UTC+0000
0xfffffa800476f060 WmiPrvSE.exe          3612    620      8      251      0
  0 2022-09-30 15:50:08 UTC+0000
0xfffffa8001a5b060 cmd.exe               1124   1968      1       23      1
  0 2022-09-30 15:50:49 UTC+0000
0xfffffa8001e15b00 conhost.exe           2624    416      2       55      1
  0 2022-09-30 15:50:49 UTC+0000
0xfffffa8004714a00 winpmem_mini_x        3920   1124      1       23      1
  0 2022-09-30 15:51:34 UTC+0000
root@kali:~/Downloads#
```

Now we can see all of the processes. We can even see our malware DnDcR.exe that has a pid of 2500 (your pid may be different)

25. We can use the pstree command to see the parent child relationships of our processes:

```
root@kali:~/Downloads# vol.py -f infected.raw --profile=Win7SP1x64_23418 pstree
```

    vol.py -f <name of file or path to file> --profile=<profile> pstree



26. We are going to investigate our infected raw file by seeing if it output anything on the command line by entering the following command:

    vol.py -f <name of file or path to file> --profile=<profile> cmdline -p <PID>

By putting the pid of our malware at the end of the command, we can focus on the output of our malware:

```
root@kali:~/Downloads# vol.py -f infected.raw --profile=Win7SP1x64_23418 cmdline -p 2500
Volatility Foundation Volatility Framework 2.6.1
**************************************************************************
DnDcR.exe pid:   2500
Command line : "C:\Users\Admin\Desktop\DnDcR.bin\DnDcR.exe"
```

27. We are going to look at the environment variables of our malware by entering the following command with the malware's pid

    vol.py -f <name of file or path to file> --profile=<profile> envars -p <PID>

```
root@kali:~/Downloads# vol.py -f infected.raw --profile=Win7SP1x64_23418 envars -p 2500
```

28. To get the Dll list we are going to enter the following command:

    vol.py -f <name of file or path to file> --profile=<profile> dlllist -p <PID>

```
root@kali:~/Downloads# vol.py -f infected.raw --profile=Win7SP1x64_23418 dlllist -p 2500
```

29. To view the handles we are going to enter the following command:

    vol.py -f <name of file or path to file> --profile=<profile> handles -p <PID>

```
root@kali:~/Downloads# vol.py -f infected.raw --profile=Win7SP1x64_23418 handles -p 2500
```

You will be able to see what was granted access, such as keys and events

30. To view the privileges we are going to enter the following command:

    vol.py -f <name of file or path to file> --profile=<profile> privs -p <PID>

```
root@kali:~/Downloads# vol.py -f physmem.raw --profile=Win7SP1x64_23418 privs -p 2500
```

31. To recover passwords from our raw file, we need the profile we got from the imageinfo command (but it should not matter whether you use the clean or infected raw file, so you may use whichever you like)

```
root@kali:~/Downloads# vol.py imageinfo -f infected.raw
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win200
8R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7S
P1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/Downloads/infected.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800029e9120L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff800029eb000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2022-09-30 15:51:34 UTC+0000
     Image local date and time : 2022-09-30 08:51:34 -0700
```

    In these instructions the last suggested profile, Win2008R2SP1x64_23418, will be used (yours may be different)

32. Now use the hivelist command with the suggested profile to get the hive registry:

    vol.py -f <name of raw or path to raw> hivelist --profile=<profile>

```
root@kali: ~/Downloads
File  Edit  View  Search  Terminal  Help
root@kali:~/Downloads# vol.py -f infected.raw hivelist --profile=Win7SP1x64_2341
8
Volatility Foundation Volatility Framework 2.6.1
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a000fcc010 0x0000000010d7f010 \??\C:\Users\Admin\AppData\Local\Microsoft
\Windows\UsrClass.dat
0xfffff8a001035010 0x0000000018951010 \??\C:\System Volume Information\Syscache.
hve
0xfffff8a003e12010 0x000000002949e010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a003f00010 0x00000000274da010 \SystemRoot\System32\Config\SAM
0xfffff8a00000f010 0x000000002d2bd010 [no name]
0xfffff8a000024010 0x000000002d2c8010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a00004f010 0x000000002cdf3010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a0000fb010 0x0000000027fe7010 \SystemRoot\System32\Config\SECURITY
0xfffff8a0006be010 0x0000000029111010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a0006d2010 0x0000000028f48010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a000a43010 0x0000000048d1e010 \??\C:\Windows\ServiceProfiles\NetworkServ
ice\NTUSER.DAT
0xfffff8a000b01010 0x000000005438a010 \??\C:\Windows\ServiceProfiles\LocalServic
e\NTUSER.DAT
0xfffff8a000d4d010 0x0000000011a91010 \??\C:\Users\Admin\ntuser.dat
root@kali:~/Downloads#
```

33. Note the **Virtual** offset of SYSTEM and SAM (yours may be different)

    SYSTEM: 0xfffff8a000024010

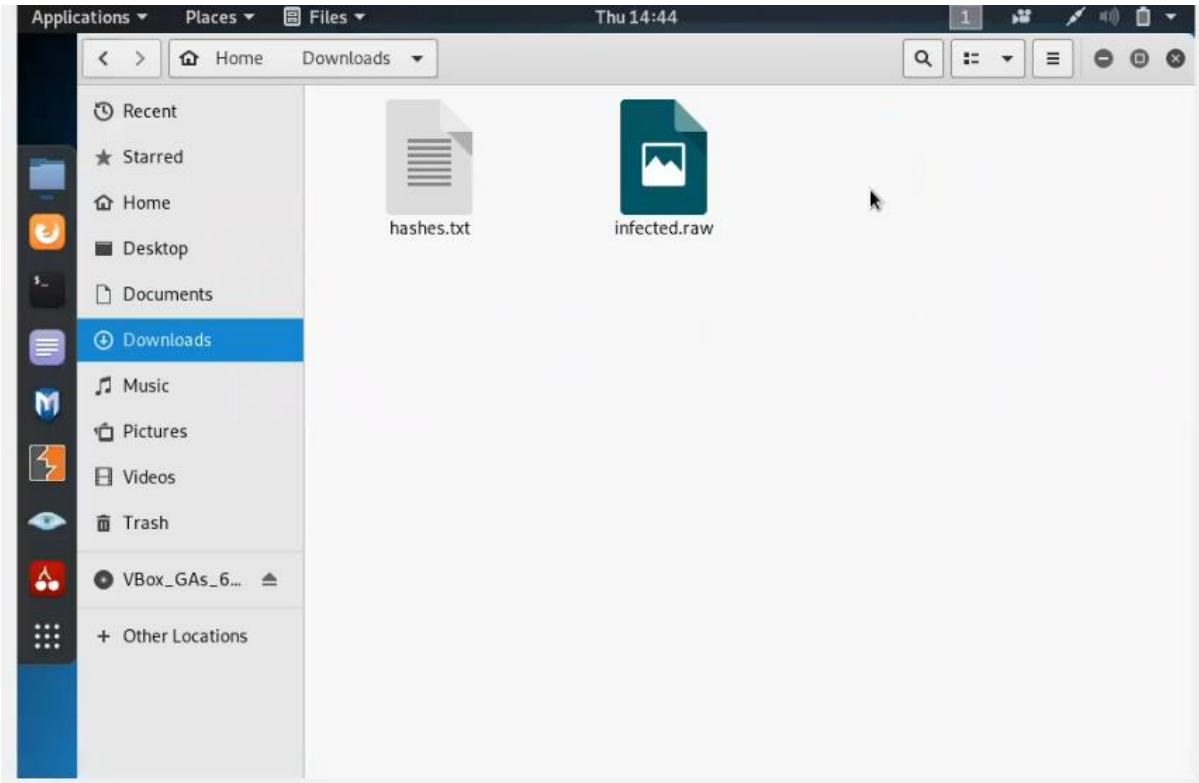
    SAM: 0xfffff8a002257410

34. Now use the profile, SYSTEM, and SAM for the hashdump command (the command is all 1 line)

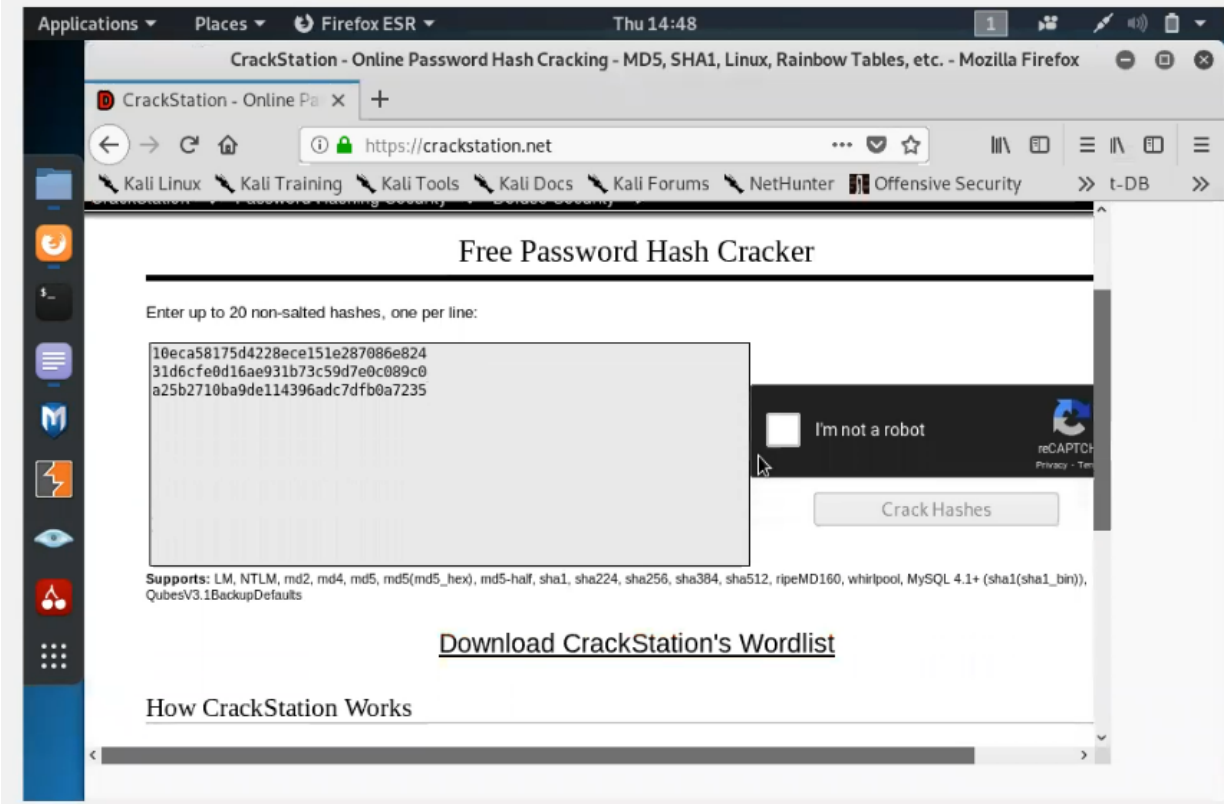
```
root@kali:~/Downloads# vol.py -f infected.raw --profile=Win7SP1x64_23418 hashdum
p -y 0xfffff8a000024010 -s 0xfffff8a003f00010 > hashes.txt
```

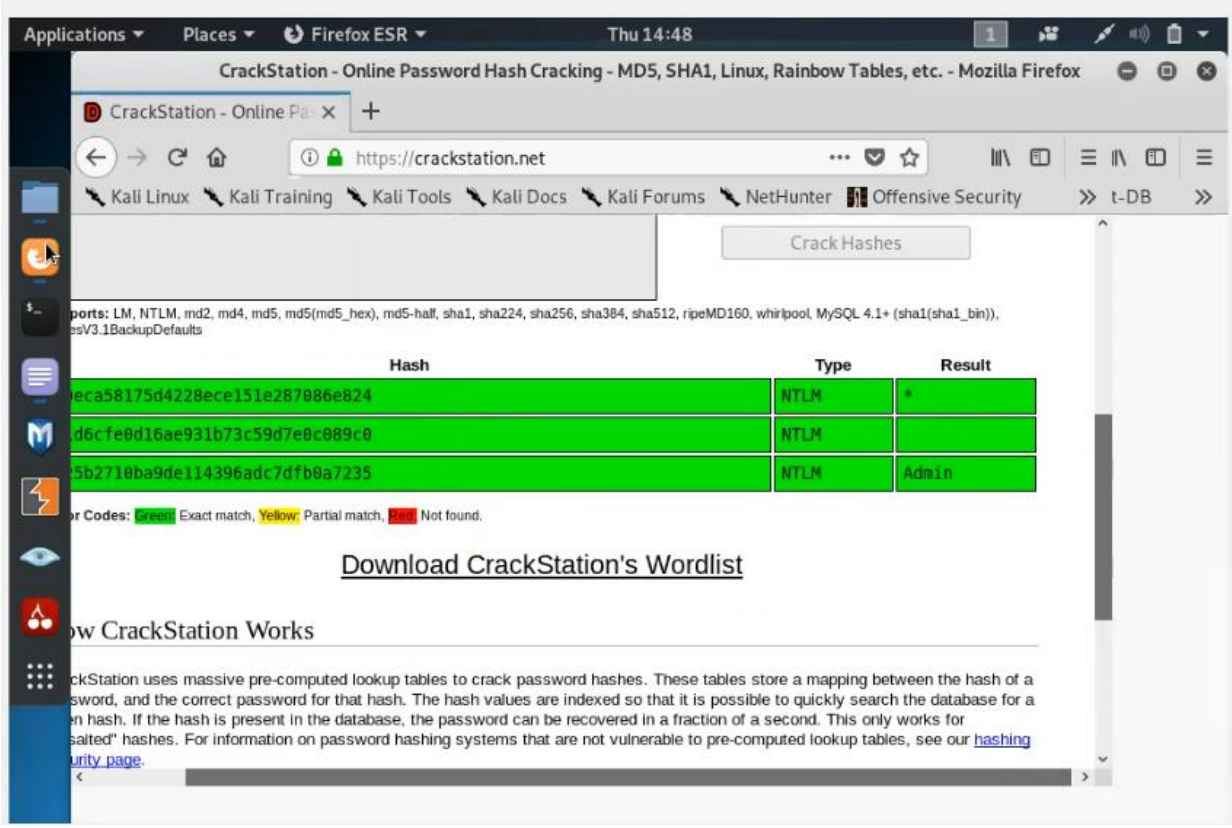
vol.py -f <name of raw or path to raw> --profile=<profile> hashdump –y <system offset> -s <sam offset> > hashes.txt

Now there will be a text file with hashes in the directory you had your raw file



35. Copy the hash between the last colons and use an online hash cracker to get the passwords




Applications
Places
Firefox ESR
Thu 14:48
CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. - Mozilla Firefox
CrackStation - Online Pa
https://crackstation.net
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
t-DB
Crack Hashes
ports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)),
esV3.1BackupDefaults
Hash
Type
Result
eca58175d4228ece151e287086e824
NTLM
*
d6cfe0d16ae931b73c59d7e0c089c0
NTLM
5b2710ba9de114396adc7dfb0a7235
NTLM
Admin
r Codes: Green: Exact match, Yellow: Partial match, Red: Not found.
Download CrackStation's Wordlist
ow CrackStation Works
ckStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a
sword, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a
n hash. If the hash is present in the database, the password can be recovered in a fraction of a second. This only works for
salted" hashes. For information on password hashing systems that are not vulnerable to pre-computed lookup tables, see our hashing
urity page.

Questions:

1. Explore the info on Agent Tesla on AnyRun. What was the threat verdict score the DnDcR.exe process received out of 100?
2. Provide screenshots of the PID list of both the clean and infected images to show that the malware is only running on the infected image.
3. Provide a screenshot of at least 3 potentially suspicious privileges the malware process had and explain how they could be suspicious or misused.
4. Why would it be important to see the parent and child processes of suspicious processes/malware?
5. Were you able to crack an exact match of your password? Provide a screenshot of your attempt.

Deliverable:

Explicitly answer all questions above one by one. Provide screenshots as necessary. You will be evaluated based on the correctness, completeness, clarity and quality of English writing.