WEEK 3 – TASK T3.1P

Pass Task.
Release Date: 22 July, Due Date: 5 August, End Date: 12 August.

Learning Outcomes

In this task, you will learn more about malware and malware analysis. You will get hands-on experience of analysing a malware that is running on a machine. This will complement the theoretical discussion about malware analysis in Week 2.

Instructions

Resources

An **answer sheet template** is available on OnTrack as a `**Resources**'. Please download the answer sheet and fill it with your answers. To upload on OnTrack, you need to convert the answer sheet template document to **PDF**. MS Word includes built-in PDF conversation capability.

All 7 questions and their sub-questions of this task must be attempted. If screenshots are required, please ensure that text in screenshots is readable.

Remember that troubleshooting technical problems is part of learning in this field. You must patiently work through issues and solve these. Tasks are not step-by-step guide. You need to be in the driver seat and learn concepts by doing – as you would when you start your future job (many times even your future supervisor doesn't know the answer to problems you face). After patent troubleshooting and research, if you need help:

Help is always available in SIT182. Please go to **Discussions** and ask your questions about this task in **Task 3.1P**. All students are encouraged to participate and help peers with their questions. Helping others is a great way to learn and think about aspects you may have overlooked. You can also seek help from tutors during online and face-to-face pracs. Please do not raise your questions through Teams, OnTrack, or Email.

References In cyber security, our preferred referencing style is **IEEE** – however, you are allowed to use any Deakin approved referencing style in this unit. Please refer to unit site > Content > Referencing - Hints & Tips for more information.

Setup (for working on your own machine – not for cyber lab)[1]:

You will need to a Windows 7 VM for this task. This Windows 7 is not activated and is provided by Microsoft for development and testing purposes. Please ensure that you do not use this VM for anything beyond this task given the potential security and privacy risks.

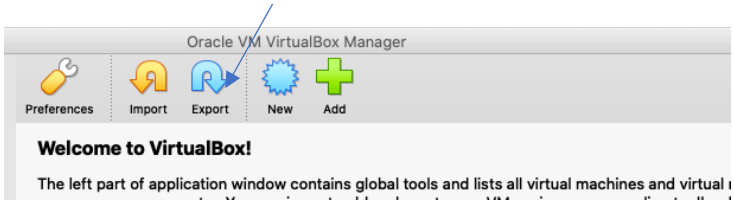
1. download the OVA file from any of the following links (file size: 5.3GB):

- https://drive.google.com/file/d/11PP-OwFqcZ6Udx8WJbLSrzuoKm6E1Y--/view?usp=sharing
- IE8 - Win7.ova

If clicking on the links didn't work, copy the links to your browser.

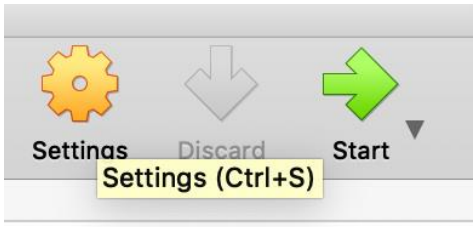
You will need to ensure that you have 10 GB available on your machine to download and run this VM.

2. **Import** the downloaded OVA file to VirtualBox. This is similar to how your imported Kali OVA file in Task 2.1P.



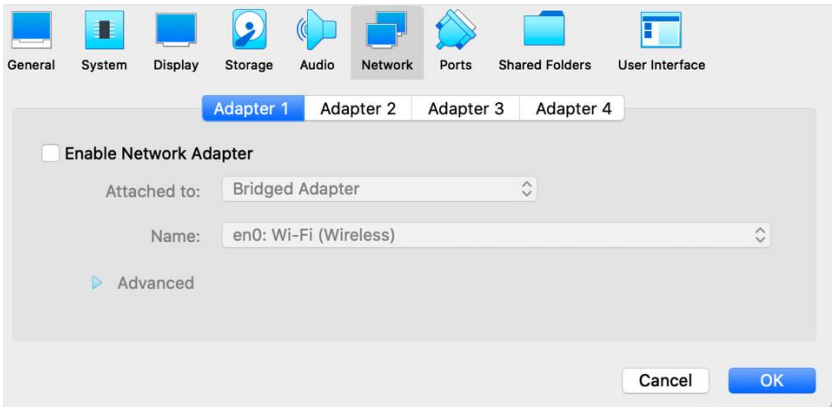
3. Given that this VM is used to run malware, you will need to ensure that is disconnected from network. Note that running the malware inside the VM will not affect your host OS.

Hence, BEFORE RUNNING THE VM after import, we need to disconnect it from network. For this, click on the VM in VirtualBox and then Settings.

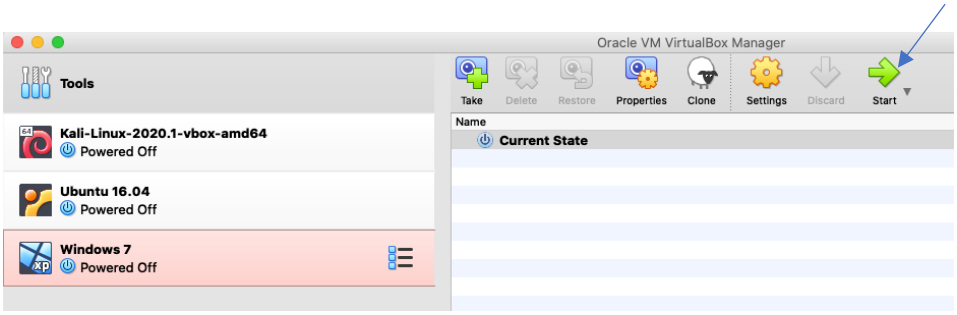


Click on the "Network" button and uncheck "Enable Network Adapter". Check Adapter 2-4 and make sure they are all disabled (i.e., no network access). Never connect with this Windows 7 VM to Internet. *(see the following screenshot)*

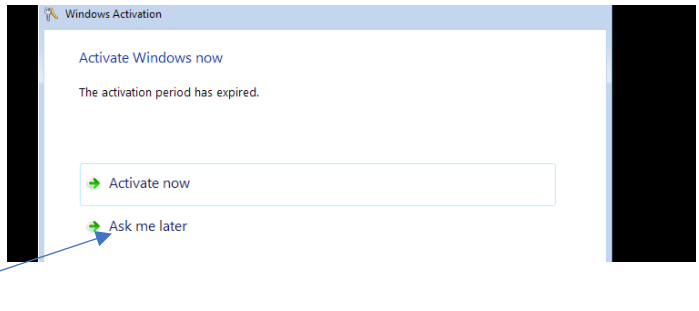
[1] If you are using cyber lab PCs, move to page 4.



4. Return to VirtualBox, pick Windows 7 VM, and Click on Start.

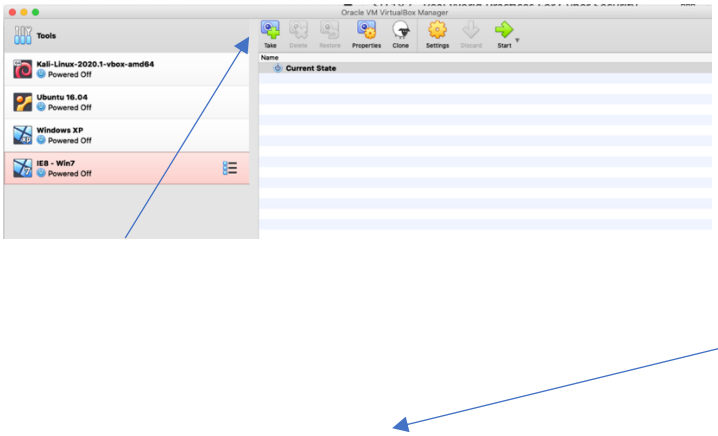


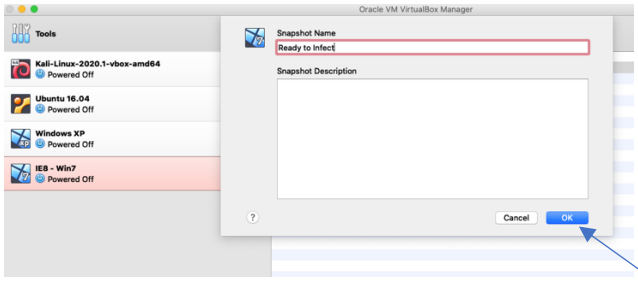
You may be prompted with an activation windows, please click on "Ask me later" – as mentioned, this is a development version of Microsoft Windows 7 and it should be used for test and development only.



Now that you have ensured the Windows 7 VM is working fine, shut down the Windows 7 VM.

5. Open VirtualBox. We need to take a snapshot of the VM before starting the task. Click on Snapshot (or, take snapshot), use `Ready to Infect' as snapshot name, and then press OK.

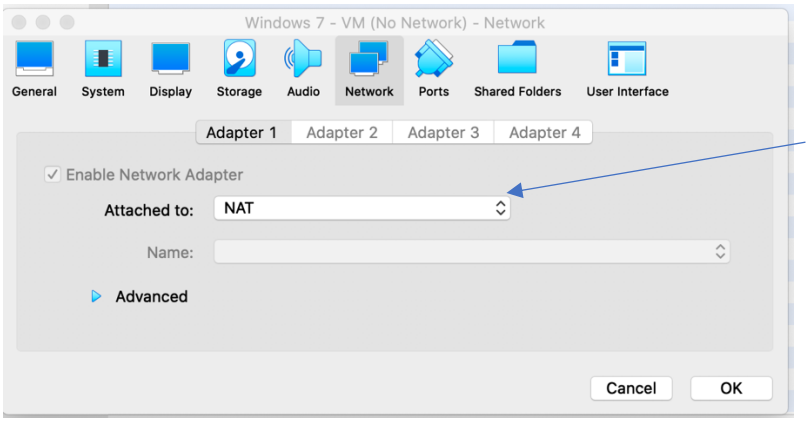




6. Now, run Windows 7 VM by clicking Start.

Setup (for cyber lab):

1. Open My Computer > Drive D > SIT182. In SIT182's folder, click on Windows 7 – VM (No Network) and import it.
2. Before starting the VM, open Settings and click on Network. Ensure that Adapter one is set to NAT.



Then, right-click on network setting in the bottom bar of VirtualBox window and click on "Connect Network Adapter"

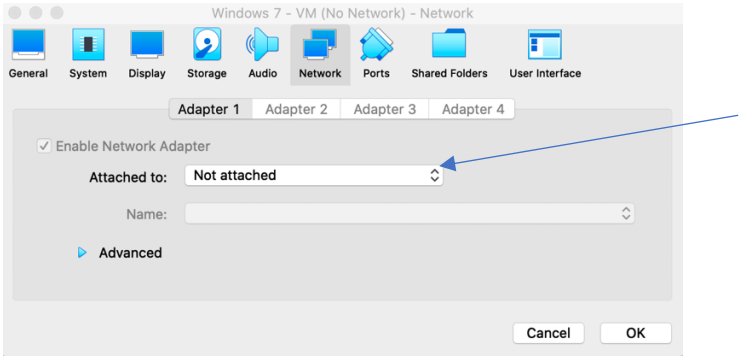
3. Run Windows 7 VM. Open Firefox and go to https://github.com/ytisf/theZoo/tree/master/malware/Binaries/Dyre

4. Locate Dyre. Click on the link and then Dyre.zip.Then, click on Download.

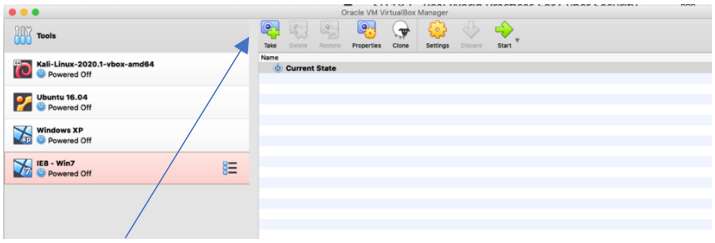
5. You also need to download Sigcheck.exe. For this, visit https://learn.microsoft.com/en-us/sysinternals/downloads/sigcheck and download the file.

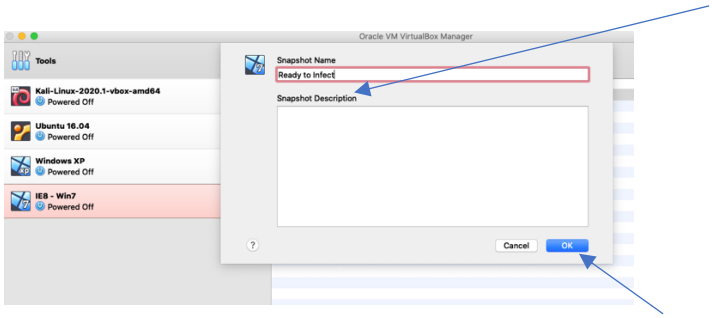
6. **As soon you finish downloading the file on your VM, you need to ensure that you the VM is disconnected from network. This is very important.**

7. Turn of the VM. Click on Settings for Windows 7 VM, Network, and then change the setting for adapter 1 to “not attached”.



8. Open VirtualBox. We need to take a snapshot of the VM before starting the task. Click on Snapshot (or, take snapshot), use `Ready to Infect’ as snapshot name, and then press OK.



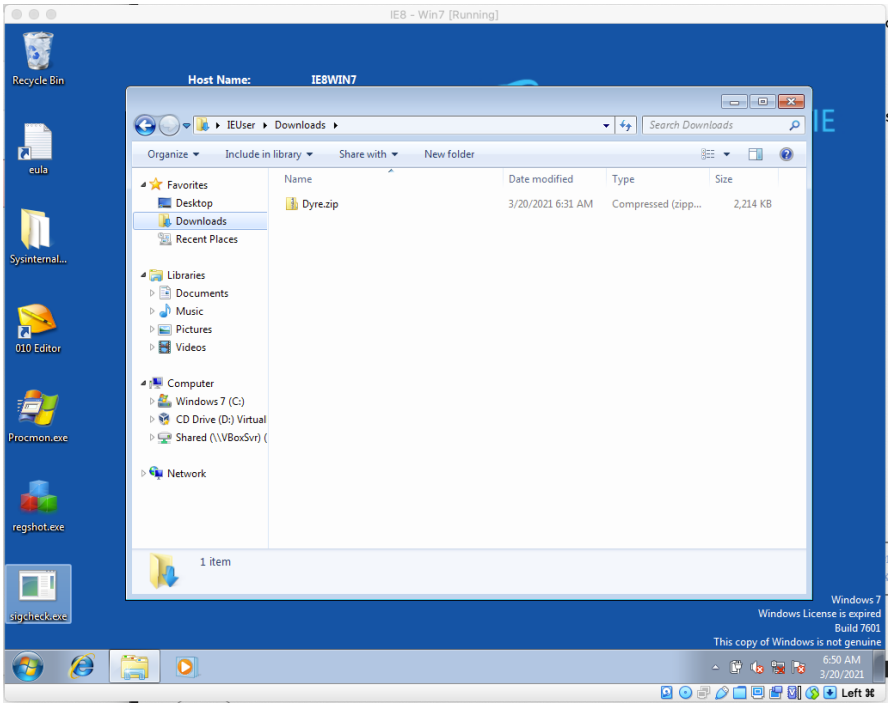


9. Now, run Windows 7 VM by clicking Start.

Let’s get started.

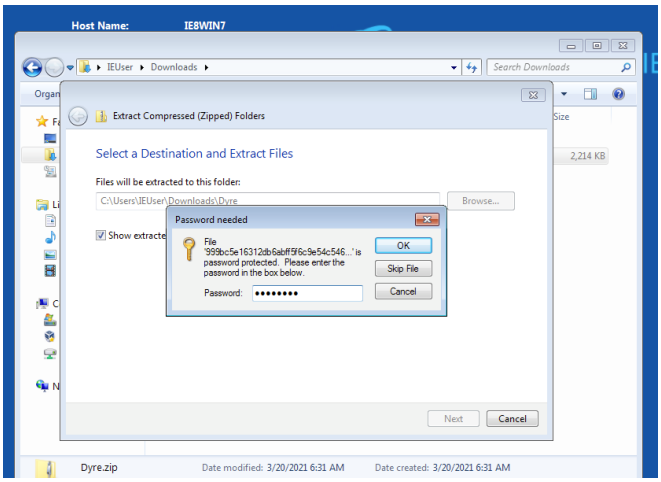
In Windows 7 VM, find the Download folder.

(Dyre.zip will be already downloaded and available for you if you are using Windows VM provided)



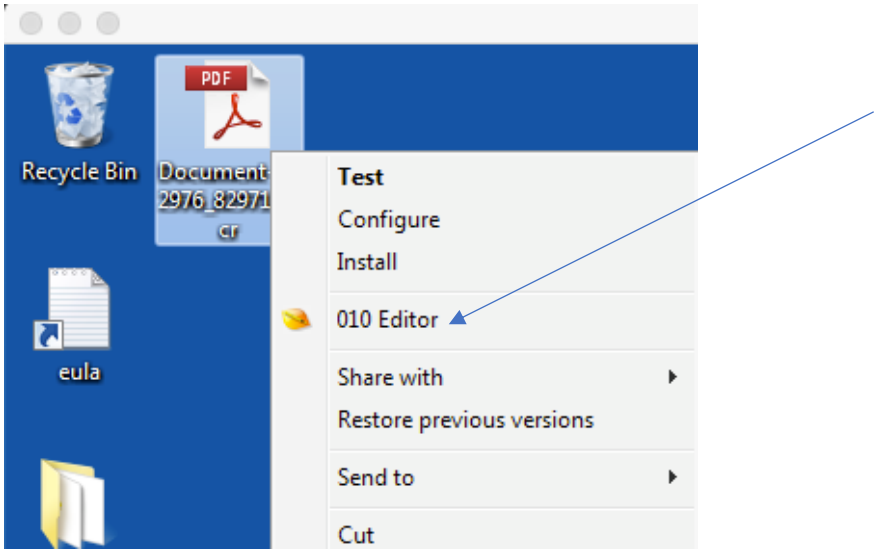
1. Unzip Dyre.zip by right-click and then “Extract All”

2. You will be required to provide a password to unzip the file. The password is “**infected**” (without quotes).

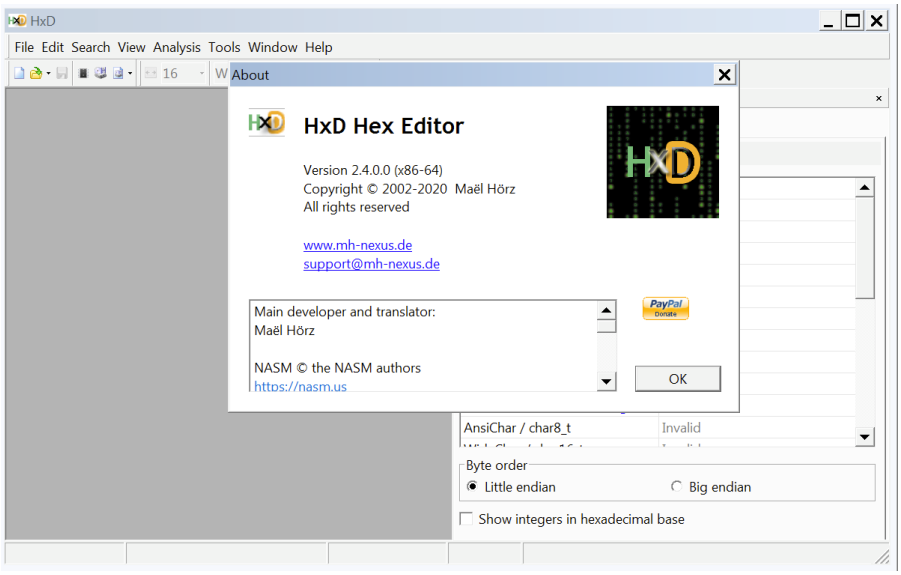


3. Navigate to the extracted folder (Dyre). The, `Original’ folder. Copy the PDF file “Document-772976_829712.scr” to Windows 7 VM desktop (i.e., not your host OS).

4. Right click on the PDF document you just copied and select `010 hex Editor’.



Important: if you are on campus and using cyber lab machines, use HxD. "010" is not available on lab machines.



Once you open the PDF file with a Hex Editor, you will notice that this file has an MZ header.

5. Close the hex editor (010 or HxD).

Task 1:

Investigate about `Dyre' malware and answer the following questions:

a. Explain in your own words about 'Dyre' malware.
b. What is a `polymorphic' virus and why Dyre is a polymorphic virus?
c. What type of malware is Dyre? *(Hint: refer to Week 2 lecture)*
d. What is Dyre's payload? What threat does it pose to a victim?

Task 2:

Investigate on Hex Editor and answer the following

a. What is a `Hexadecimal'
b. What does the `MZ header' indicate?

6. Click on Start and type CMD. Click on "cmd.exe".

7. Type "cd Desktop" to move to your desktop. Then run the command "**sigcheck.exe -h Document-772976_829712.scr > output1.txt**"

Tip: when typing the command, you can use [Tab] key for auto completion (see Task T2.1P and helpful tips on how to use CLI)

10. You will notice that the output1.txt is created on your VM's desktop. Click on the file and see its content.

. Close the hex editor

If you are in Cyber Lab and using VMs provided:

To run the Sigcheck command, open up CMD and change directory to where Sigcheck is downloaded to. For instance, let's assume the file is in Downloads folder of VM. In this case, the command becomes:

Cd Users\Administrator\Downloads\

Now, while you are in Downloads folder run:

sigcheck.exe -h \Users\Administrator\Desktop\Document-772976_829712.scr

Task 3:

Investigate the Sigcheck.exe tool by answering following questions:

a. What does the command `sigcheck.exe' do?
b. Include a screenshot of the content of "output1.txt" file on Windows 7 VM Desktop – *hint: you can use your host OS screenshot tools to capture.*

9. Navigate to your desktop. Now double click on "Procmon.exe" You should see the process monitor window pop up as the example below. Leave that running in the background.

10. Double click on "**Document-772976_829712.scr**" on your VM's desktop and then click `Run' (if prompted). Congratulations, your VM is now infected with Dyre Malware!
You will notice that the PDF file vanishes after this.

11. Wait about 10 seconds, then click the magnifier button  on the process monitor window to stop the monitoring.

12. In `Procmon", click tools->process tree to open the process tree window. On the left side of the process list, look for the process "**Document-772976_829712.scr**".

13. You'll notice that it created another process called "**googleupdaterr.exe**". Right click on the "Document-772976_829712.scr" process and select "Add process and children to Include filter" on the pop-up menu. Close the process tree window.

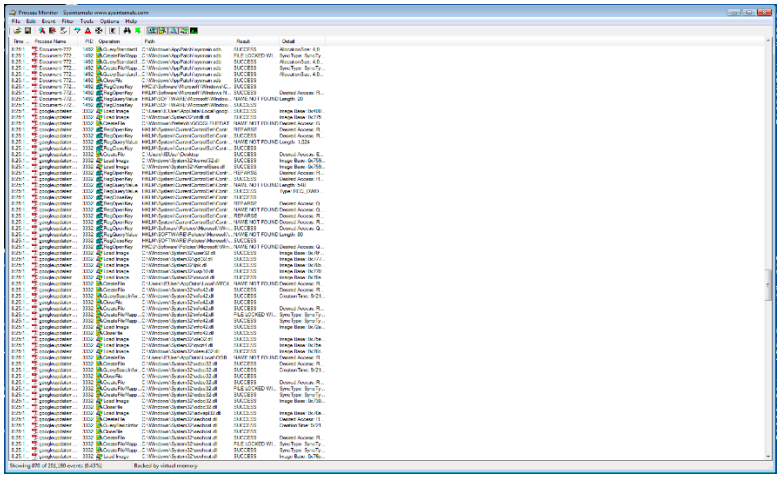
Task 4:

With reference to Week 2's lecture, answer the following:

a. Why a second process is added by `Dyre'?
b. What does it aim to accomplish?

14. You should see filtered results in the process monitor window of Procmon.

15. Locate the line that shows file googleupdaterr.exe was created and find the folder it was created in. You will need to look through Operation and Path in Procmon (patiently).



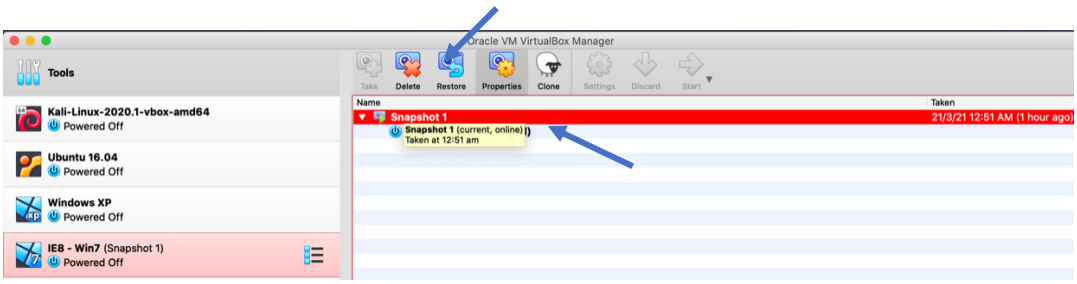
16. You will find that the newly created "googleupdaterr.exe" was stored somewhere in the Windows 7 VM. Go to that folder (once you locate it) and copy "googleupdaterr.exe" to your Desktop. Run the sigcheck for "googleupdaterr.exe" as you did in step 7: "**sigcheck.exe -h googleupdaterr.exe > output2.txt**"

Task 5:

Answer the below questions:

a. What is the path where googleupdaterr.exe is stored?
b. How does this hash stored in **output2.txt** compare with the hash stored in **output1.txt**? What does the comparison indicate?

17. Turn of the Windows 7 VM. We need to restore the VM to a previous state (before Dyre was executed) using the snapshot taken before. Click on the VM, find the snapshot taken earlier and click on Restore.

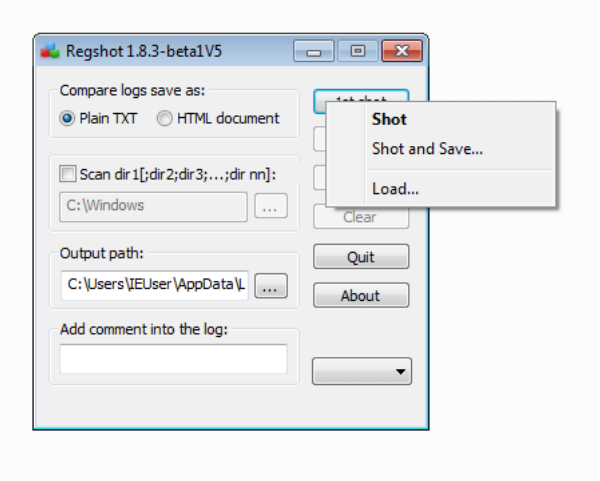


18. Run Windows 7 VM again. You will notice that all changes you made after snapshot have vanished (our time machine works!)

19. Extract Dyre again (available in Downloads folder of the VM). Password is "infected" (without quotes)

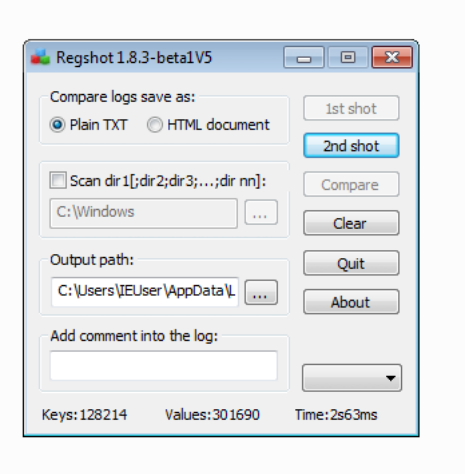
20. Run "regshot.exe" from VM's Desktop.

21. Click the 1st shot button available on regshot.exe interface.



22. Navigate to Downloads > Dyre > Original. Run "Document-772976_829712.scr". Congrats, your VM is once again compromised!

23. After about 10 seconds, click on 2nd shot in Regshot.



24. On Regshot, click on "Compare".

Task 6:

Answer the below questions on Windows Registry and Regshot.exe

a. What is `Windows Registry?' What is it used for?
b. How do you open Windows Registry in Windows 7 VM? Include screenshot of accessing the Windows Registry.
c. The malware analysis you tried in this task was `Static' or `Dynamic' – justify with reference to Week 2's lecture.

Task 7:

Research and Reflection

a. Refer to https://news.sophos.com/en-us/2020/05/22/the-ransomware-that-attacks-you-from-inside-a-virtual-machine/
Write a paragraph in your own words summarizing how the attack worked.

b. **Reflection**: Write a paragraph (100-200 words) summarizing what you learned in this week's task. How did task 3.1P complement the lecture content in Week 2?