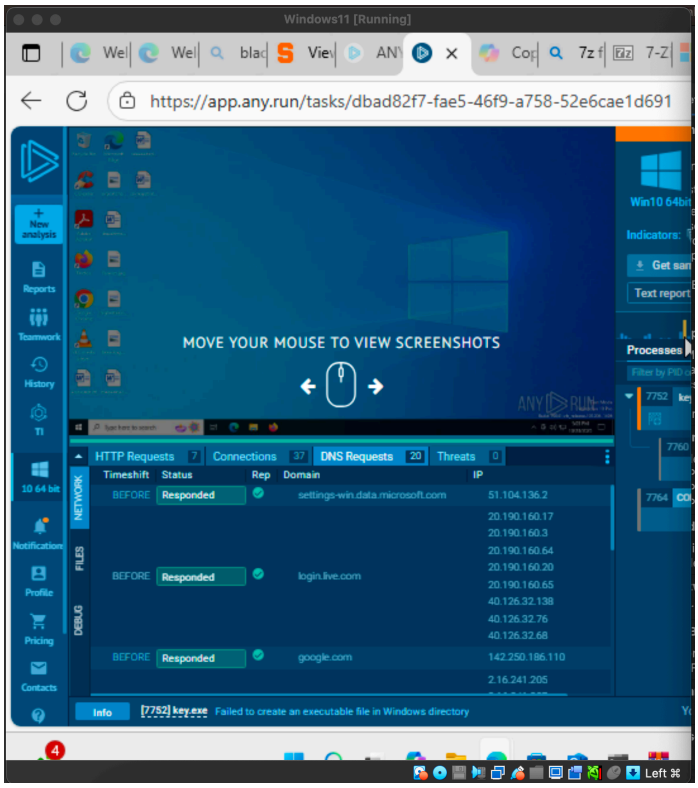
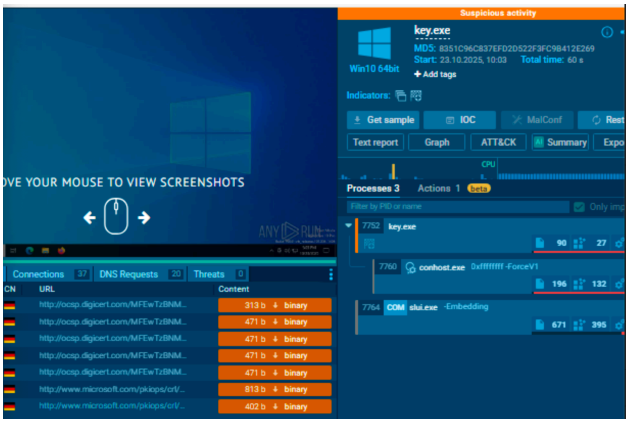
IOT InClass Exercise Week9-2
Lakshminath Reddy Alamuru
SUID: 367982169

Task1- Created the any run account.
Task2- Setup the VM for malware analysis. Created the new analysis session and opened the new analysis window.

Task3 - uploaded the key malware and ran the analsysis.

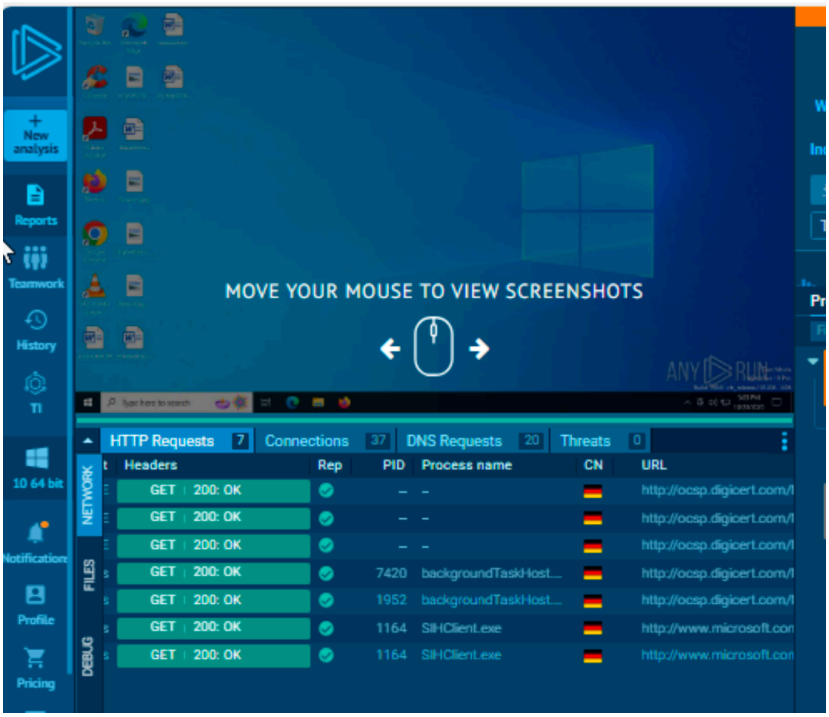


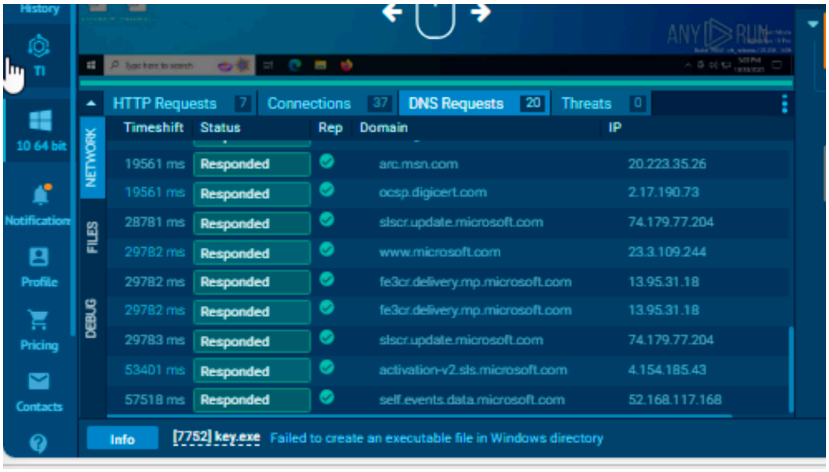
Task4 - Observed the process activity
I can see 3 process showed up here
Key.exe, Conhost.exe and slur.exe process clearly in the below screenshot.
Seems Conhost.exe is child process spawned



Task-5

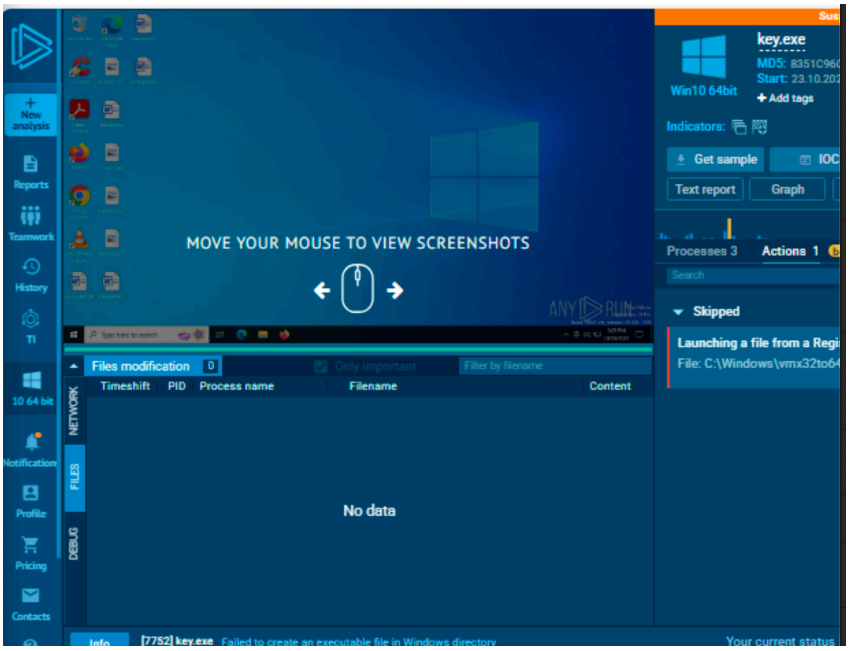
Checked Network behavio, it seems got response all ok200 for the HTTP requests, DNS requests and IP addresses associated to it





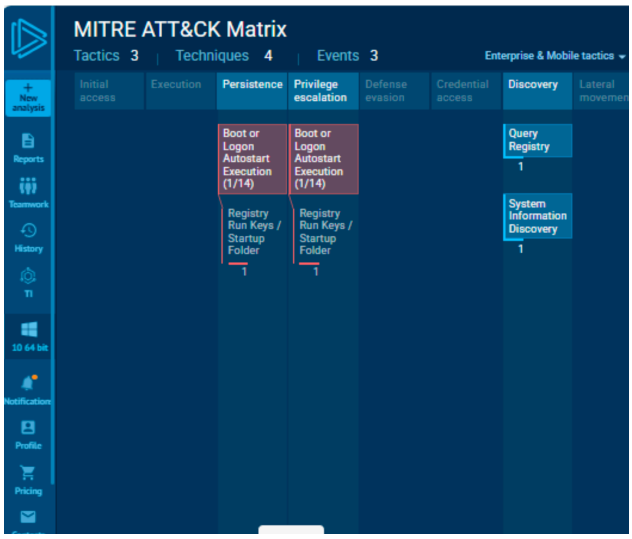
Task-6

In the files section, I didn't observe any files for modification. It shows that failed to create file in windows directory.

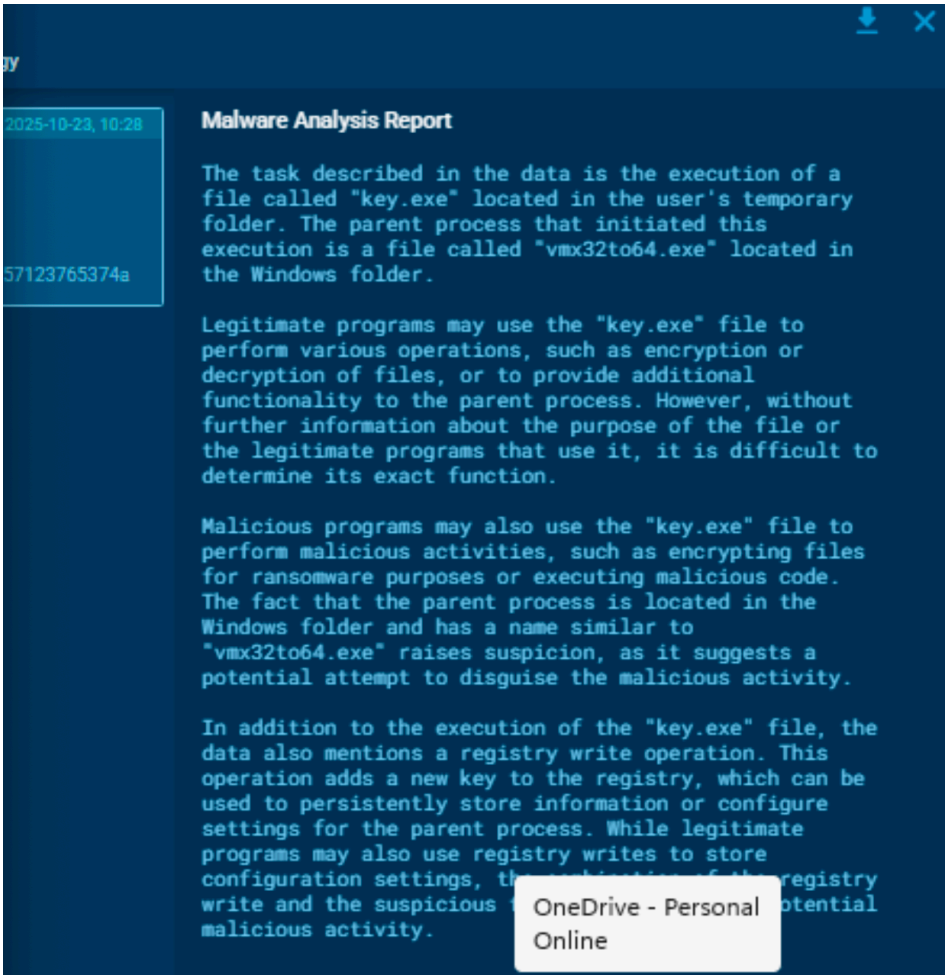


Task-7

I observed the persistence and privilege escalation for this file.



I have observed the summary by AI in the tool. Cliked on that tool
Got the below summary



Task-8
Report Findings below
Malware name : key.exe file
Malware Hash(MD5): 8351C96C837EFD2D522F3FFC98412E269

Malware activity: Trying to launch a file from registry key which is malicious activity here.
Observed Processs: key.exe, conhost.exe and slur.exe processes
Don’t observed any files in my case

Persistence techniques: Boot or Logon Autostart execution(Registry Run keys/ Startup folder)

Discovery : Query Registry, System information Recovery

Malware Analysis Report:

In addition to execution of the key.exe file, the data also mentions a registry write operation. This operation adds a new key to the registry, which can be used to persistently store information or configure settings for the parent process. While legitimate programs may also

use registry writes to store configuration settings, the combination of the registry write and the suspicious file name suggests a potential malicious activity.

Conclusion:

This assignment gave me the insights of any run software and how dynamic malware analysis happens for the provided key.exe file. It provided the detailed information about the file.