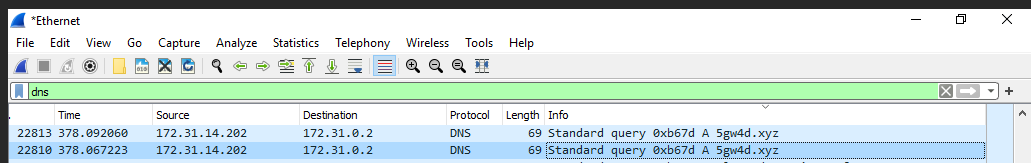
In this lab I will be using a Flare-Vm to perform a dynamic malware analysis.

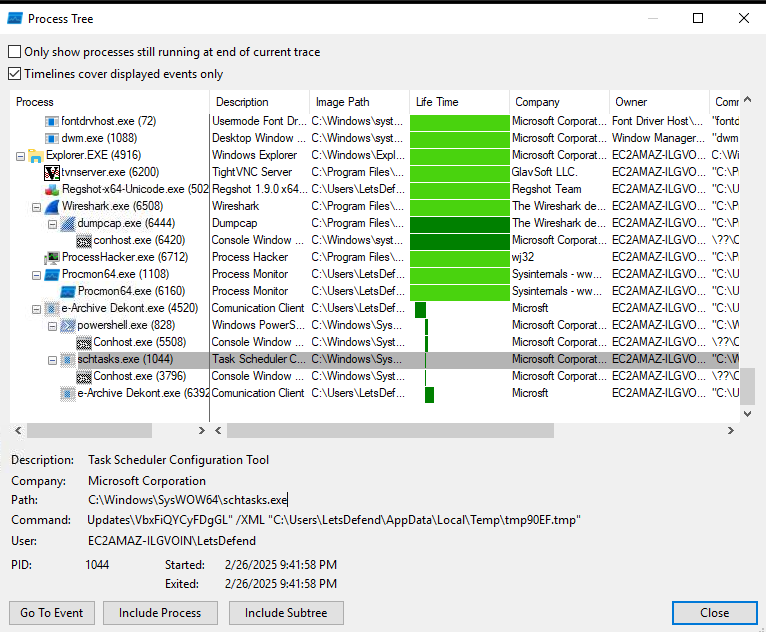
Beginning this lab I start both Process Hacker and Wireshark recording on ethernet to monitor the system.I also create a Regshot instance of the file system before the malware is executed. I then start Procmon and quickly change the malware file “e-ArchiveDekonot.bin” to an exe extension and run it as administrator.

1. What is the domain address where the "e-Archive Dekont" file sends the DNS request?

Stopping wireshark’s recording and sorting by DNS records I find that the malware sent a DNS request to 5gw4d.xyz.



1. File "e-Archive Dekont" has created a scheduled task. What is the action value of this task? (Full path)

When looking at Process Hacker, the malware seems like it has no malicious intent or child processes. However, this is misleading as Process Hacker shows what processes are happening in real time. Malware will quickly stop its child processes to avoid detection, which is where applications like Procmon come into play. Procmon records each instance of an event and how long it lived. Looking at procmon and sorting using the process tree, we see that “e-Archive Deknot” had several malicious child processes such as powershell and creating a scheduled task.

By checking the task scheduler we find a new task has been created which when the user logs on preforms the action “C:\Users\LetsDefend\AppData\Roaming\VbxFiQyCyFDgGL.exe”.

