**Name :- Kishan Lal**

**Course :- M.sc Digital Forensics & Information Security**

**Enrolment No. :- MSDFIS02**

**Subject :- Incident Response Management**

**Incident Response Management**

**Experiment :- 1**

**Title :-** Installation and Demonstration of Nmap

**Requirements :-** Laptop and Active Internet connection

**Objectives :-** Scanning DVWA

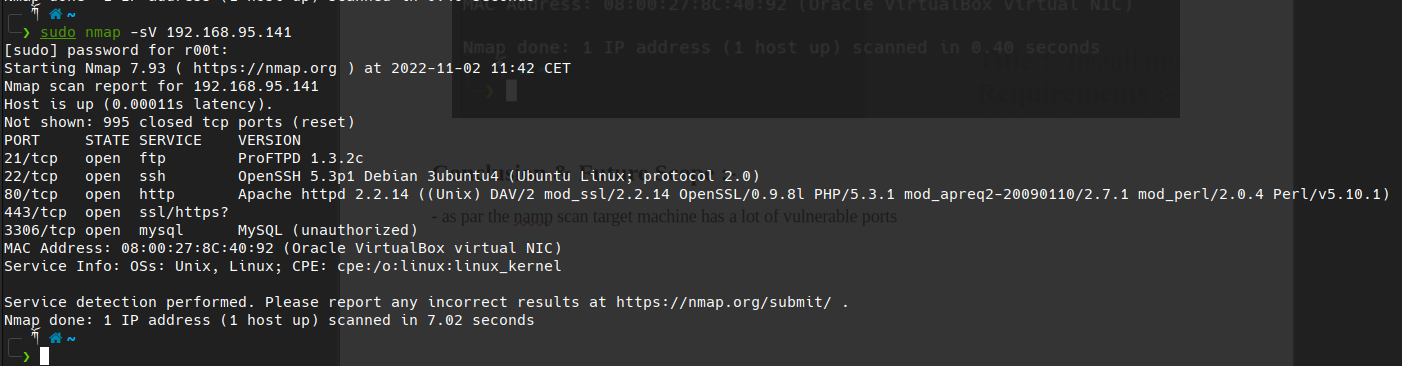
**Procedure :-**

1) Open up the Terminal in your Linux machine

2) type `**s*udo dnf install nmap***`

3) After installation scan the DVWA using `***sudo namp -sS 192.168.95.141***`

**Results :-**



**Conclusion & Future Scope :-**

**-** as par the namp scan target machine has a lot of vulnerable services open to attack for example here we have the open port of 21/tcp ProFTPD 1.3.2c which is vulnerable to the Remote Code Execution here is the [POC](https://www.exploit-db.com/exploits/15449).

**Incident Response Management**

**Experiment :- 2**

**Title :-** Installation and Demonstration of WireShark

**Requirements :-** Laptop and Active Internet connection

**Objectives :-** Network Sniffing

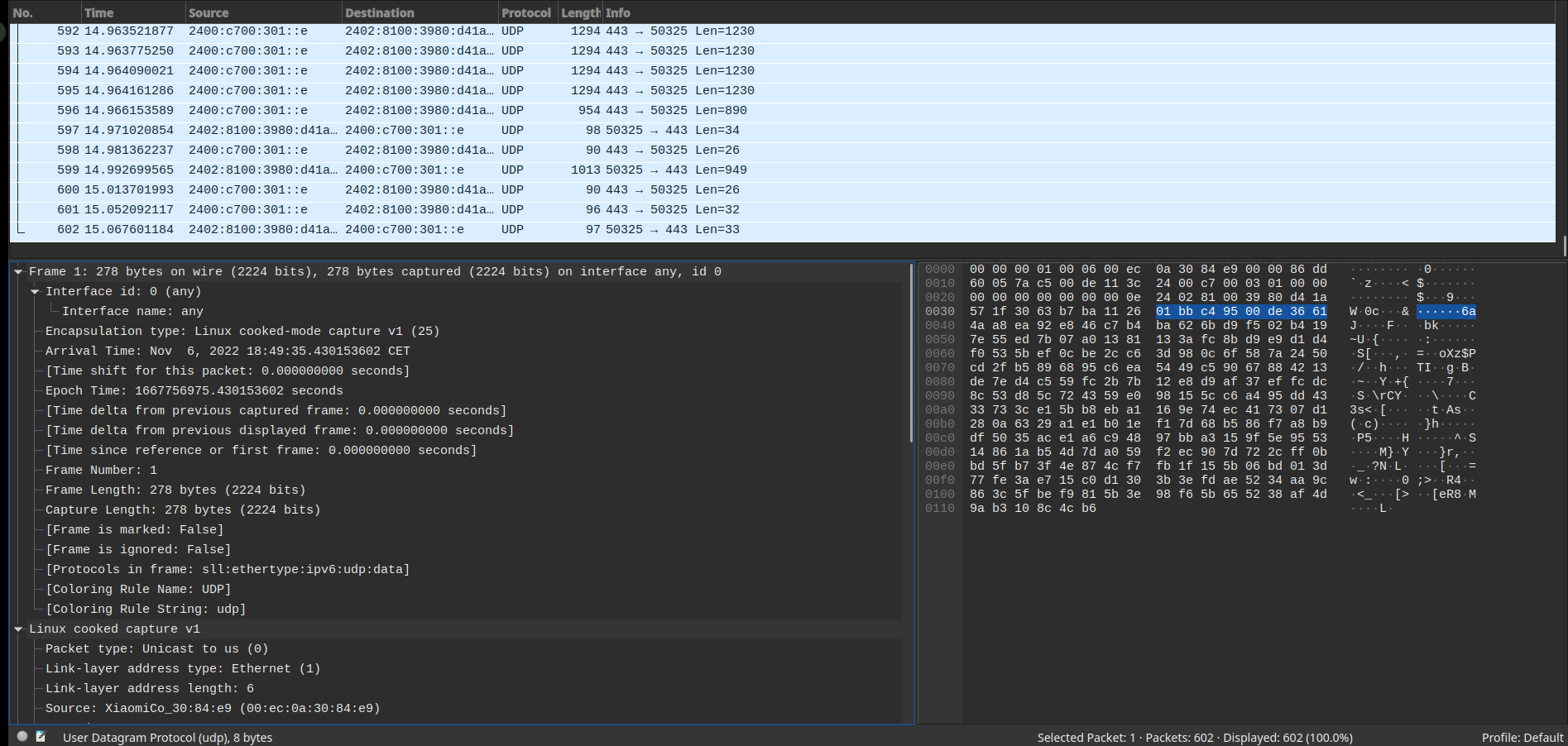
**Procedure :-**

1) Open up the Terminal in your Linux machine.

2) type `**s*udo dnf install Wireshark***`

3) After installation open up the **Wireshark** application and choose the interface.

**Results :-**



**Conclusion & Future Scope :-**

**-** as per the results we can see that through wireshark we can sniff the packets and analyse our network traffic.

- if we are performing the pen test against any company wireshark can help us find out if our tool are working find or not.

**Incident Response Management**

**Experiment :- 3**

**Title :-** Analyse and monitor system using event viewer

**Requirements :-** Windows OS

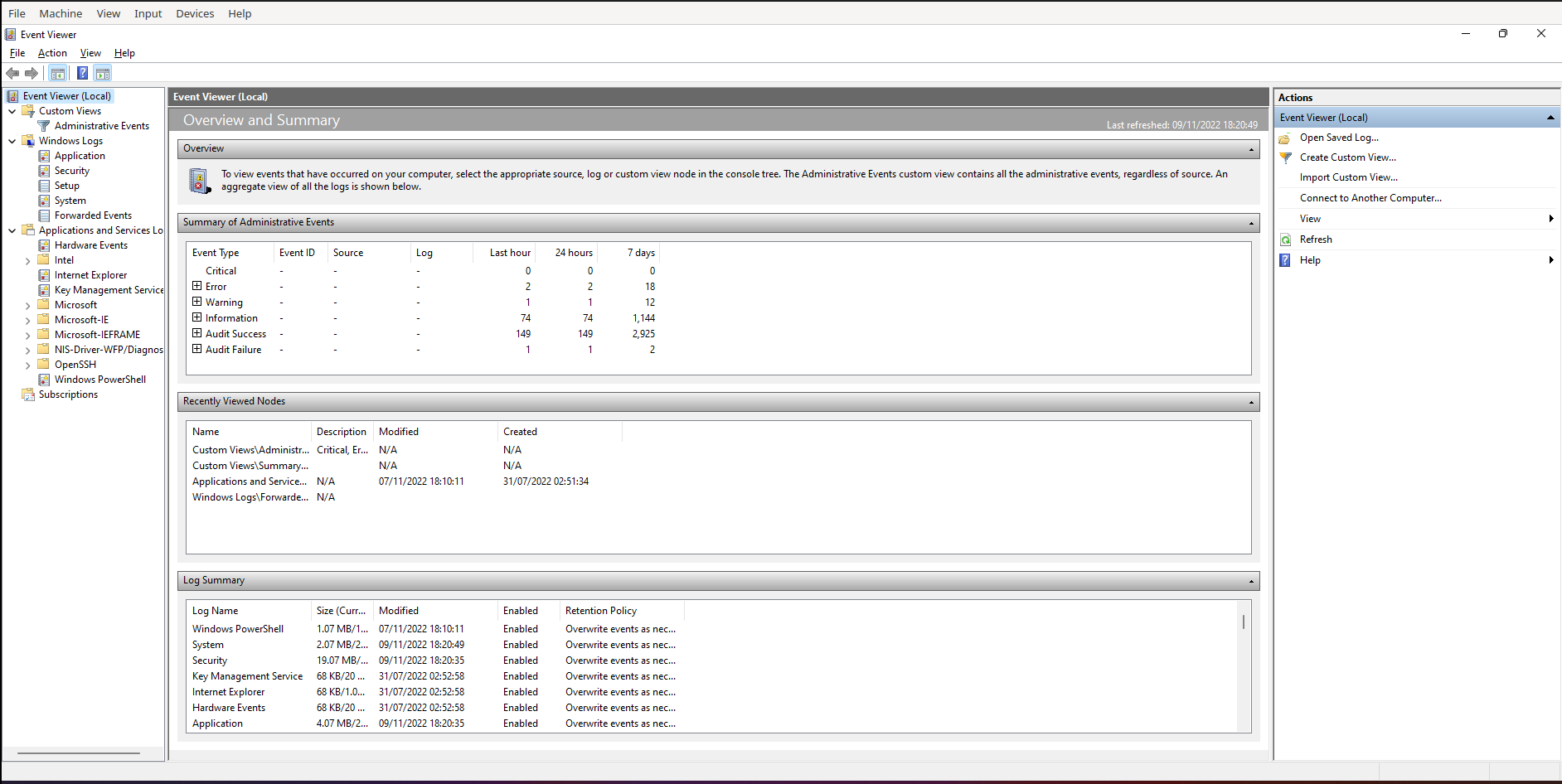
**Objectives :-** analysing our computer activities using event viewer

**Procedure :-**

1) Press the WIN-KEY + R

2) Type `**eventvwr**` in the Search Box

**Results :-**



**Conclusion & Future Scope :-**

- as per the results we can say that event viewer displays detailed information about significant events on your computer. Some of the information you will find are programs that don't start as expected, or automatically downloaded updates.

**Incident Response Management**

**Experiment :- 4**

**Title :-** Installation and Demonstration of Sysinternal tools

**Requirements :-** Laptop with windows OS and Active Internet connection

**Objectives :-** analysing our computer activities using sysinternal tools

**Procedure :-**

1) Open up the `**file explorer**` in you windows OS

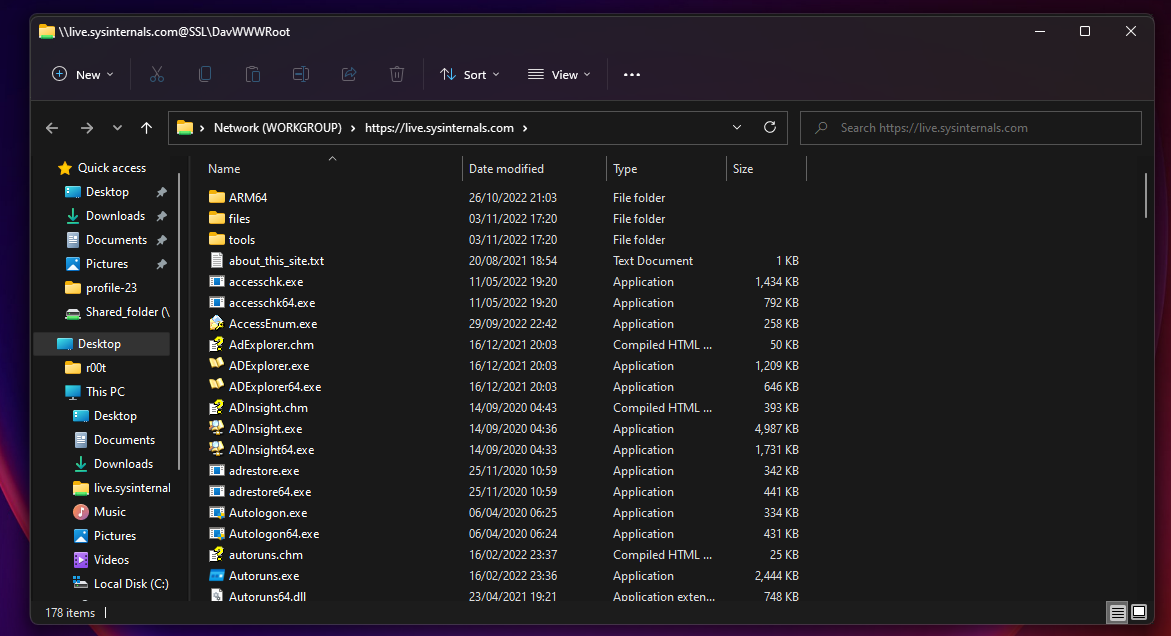
2) Right click on the `**file explorer**` and select the `**add network location**`

3) click on `**next`** and you will get asked to write the network address write this URL `[**https://live.sysinternals.com/**](https://live.sysinternals.com/)**`**

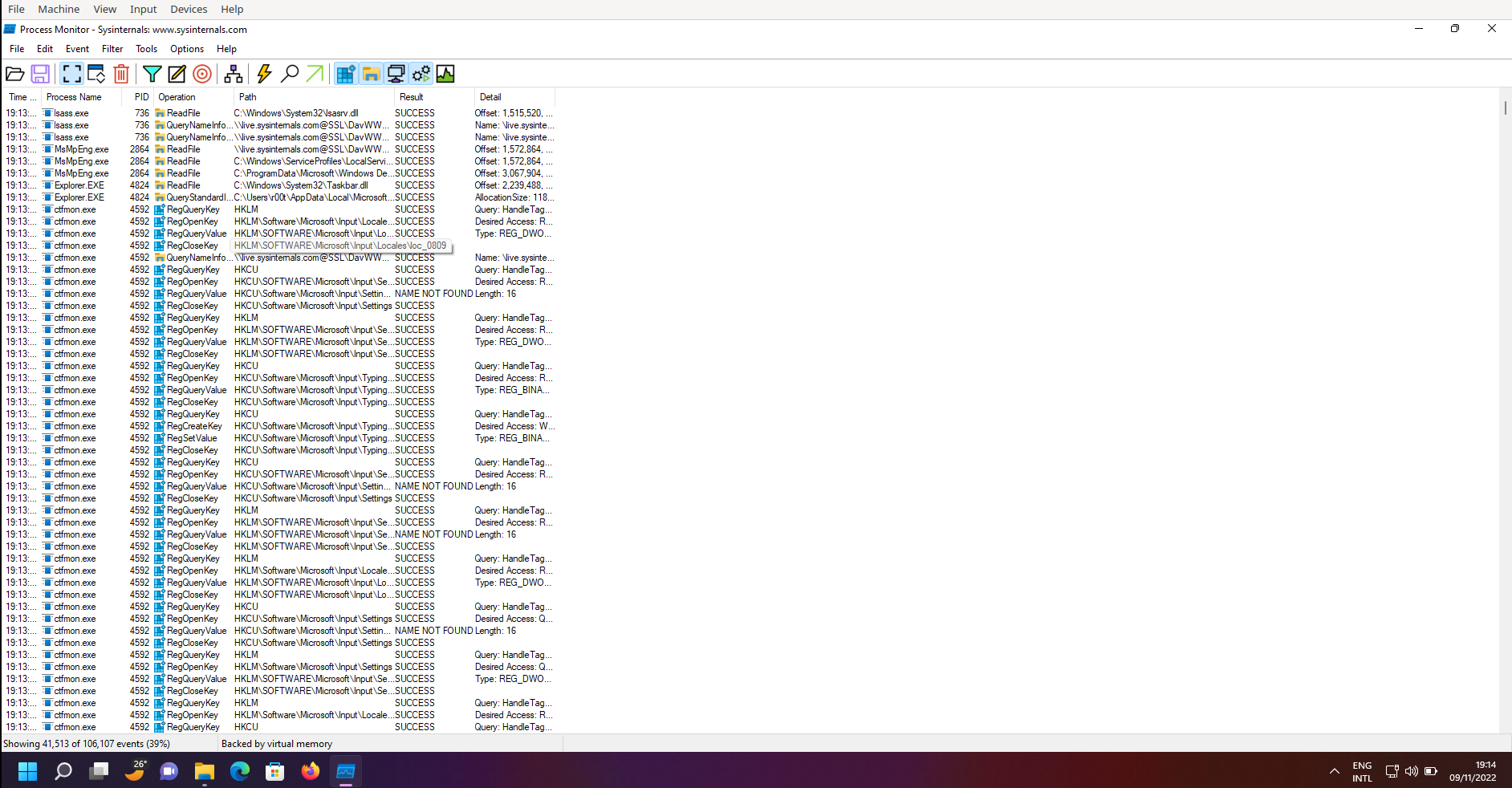
4) click on `**next**` and boom !!

5) you will get one network drive called `**live.sysinternals**` there you can find all the sysinternals tools.

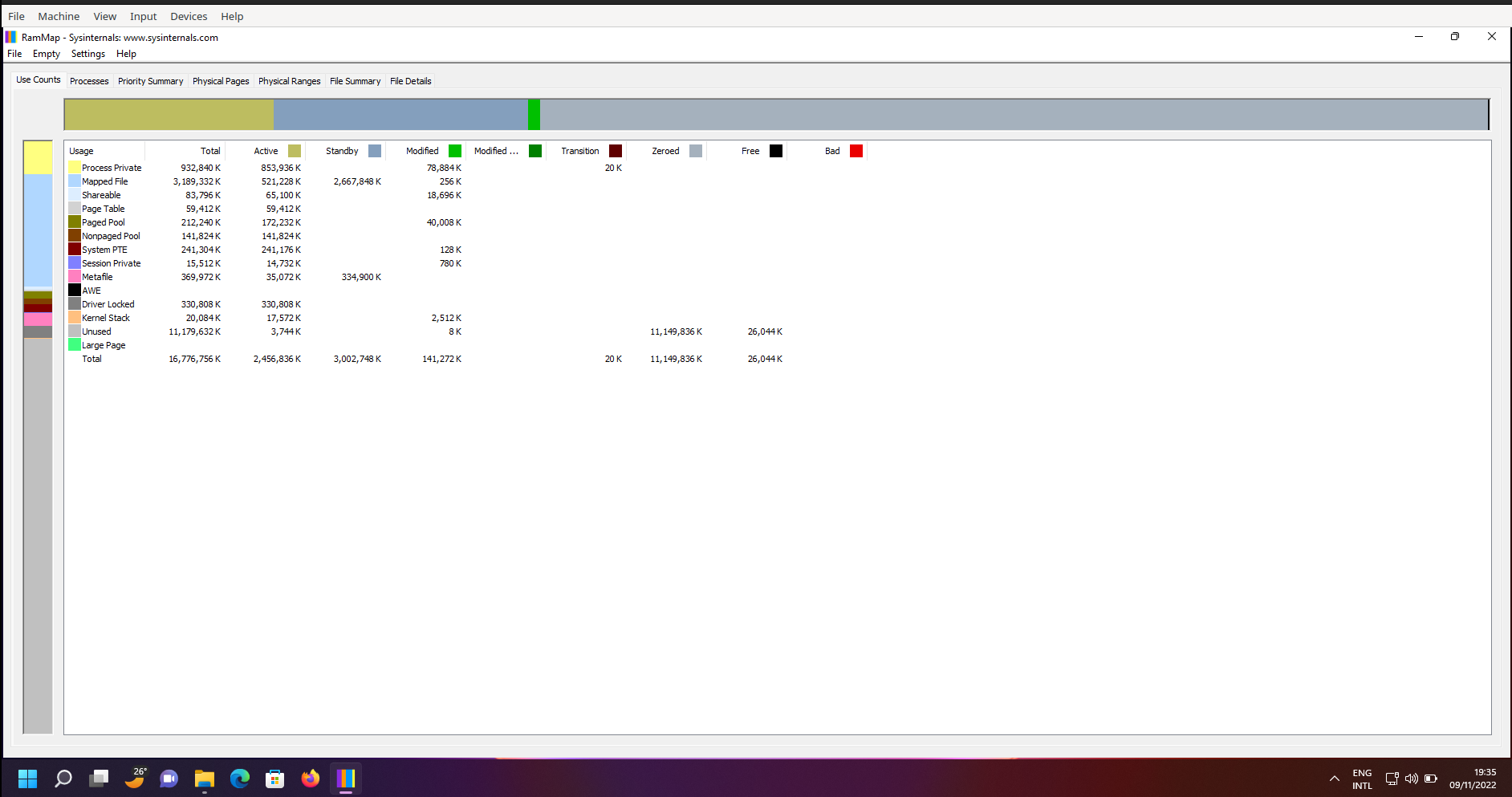
**Results :-**



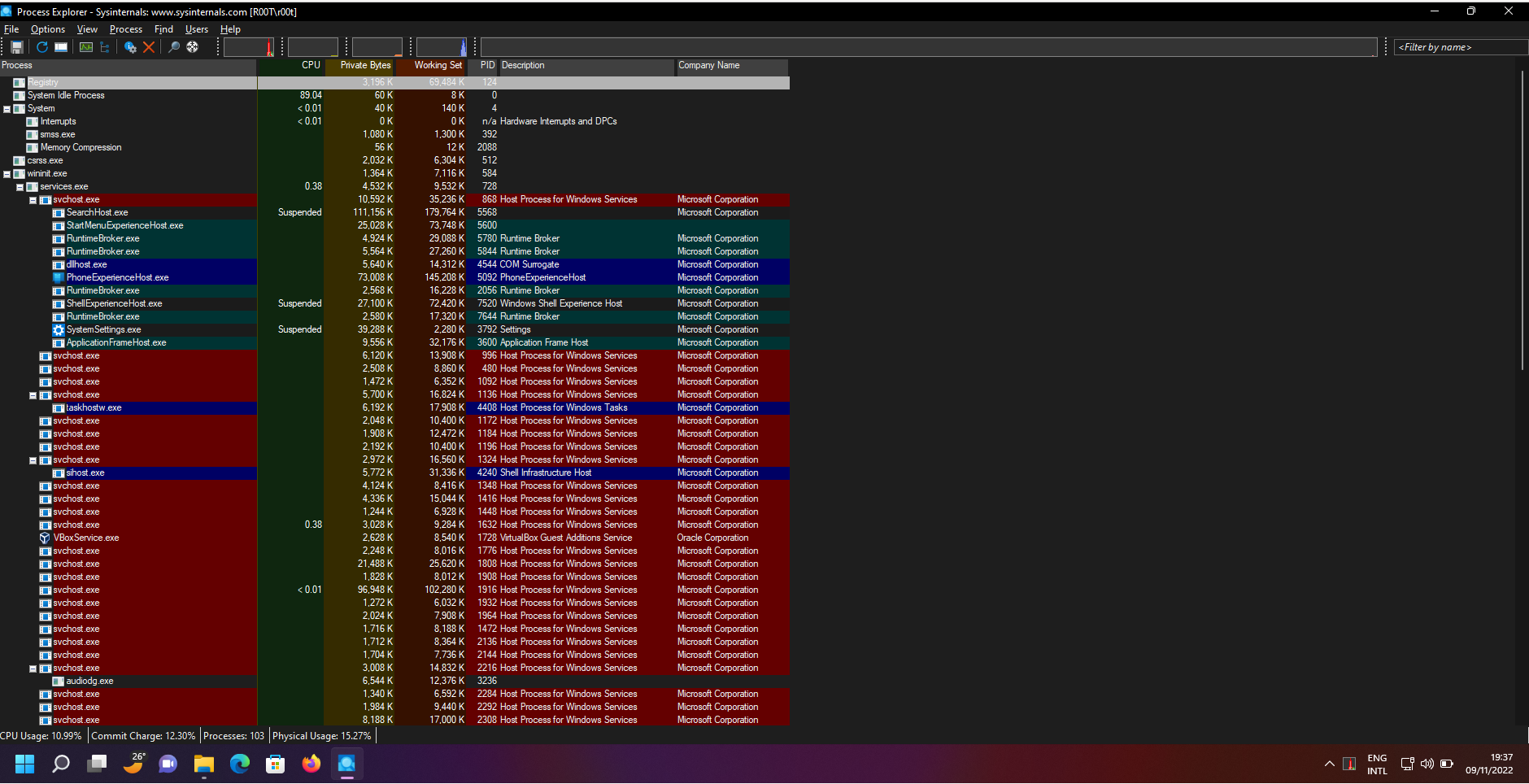
**procmon64.exe**



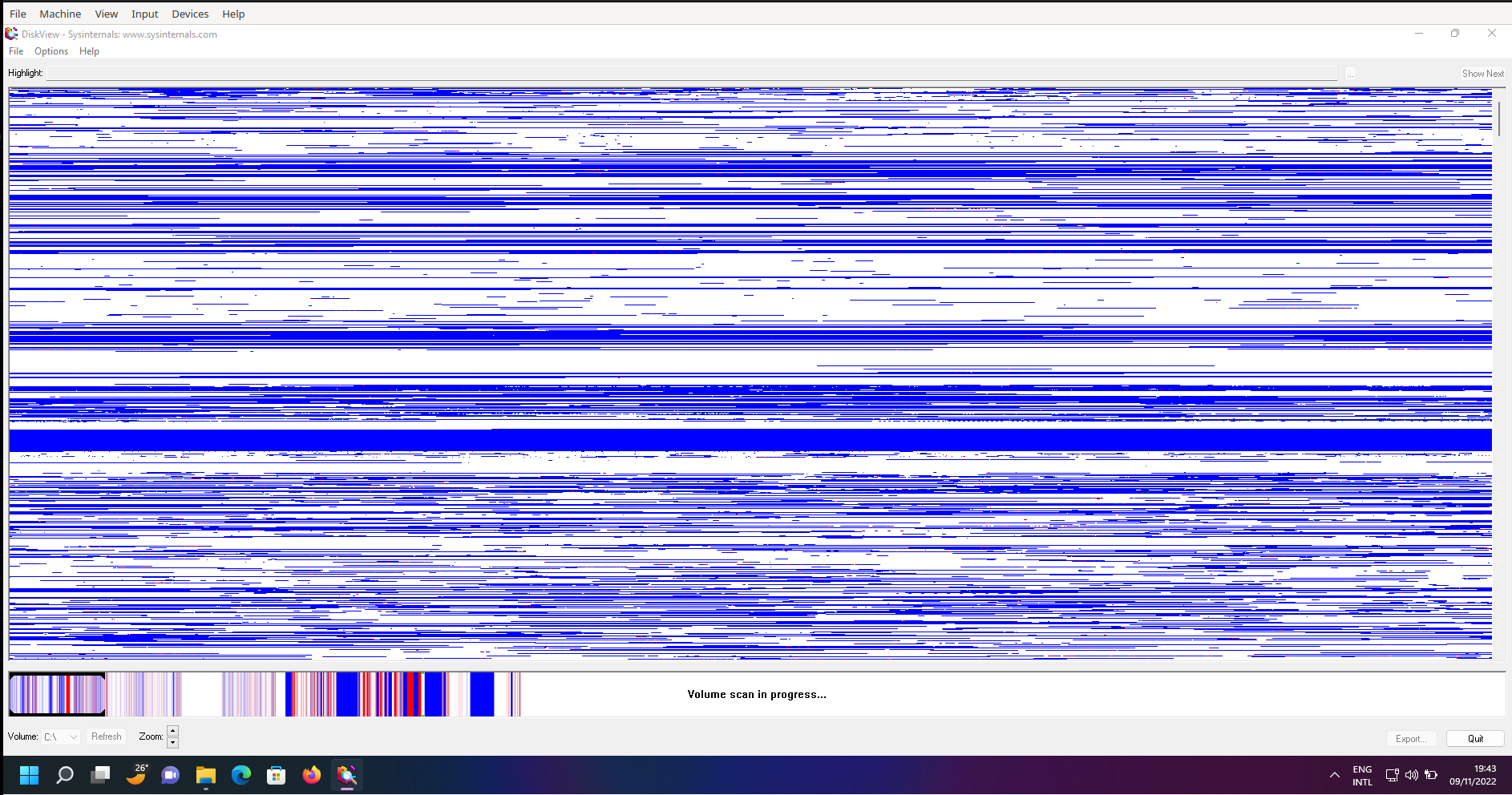
**rammap64.exe**

****

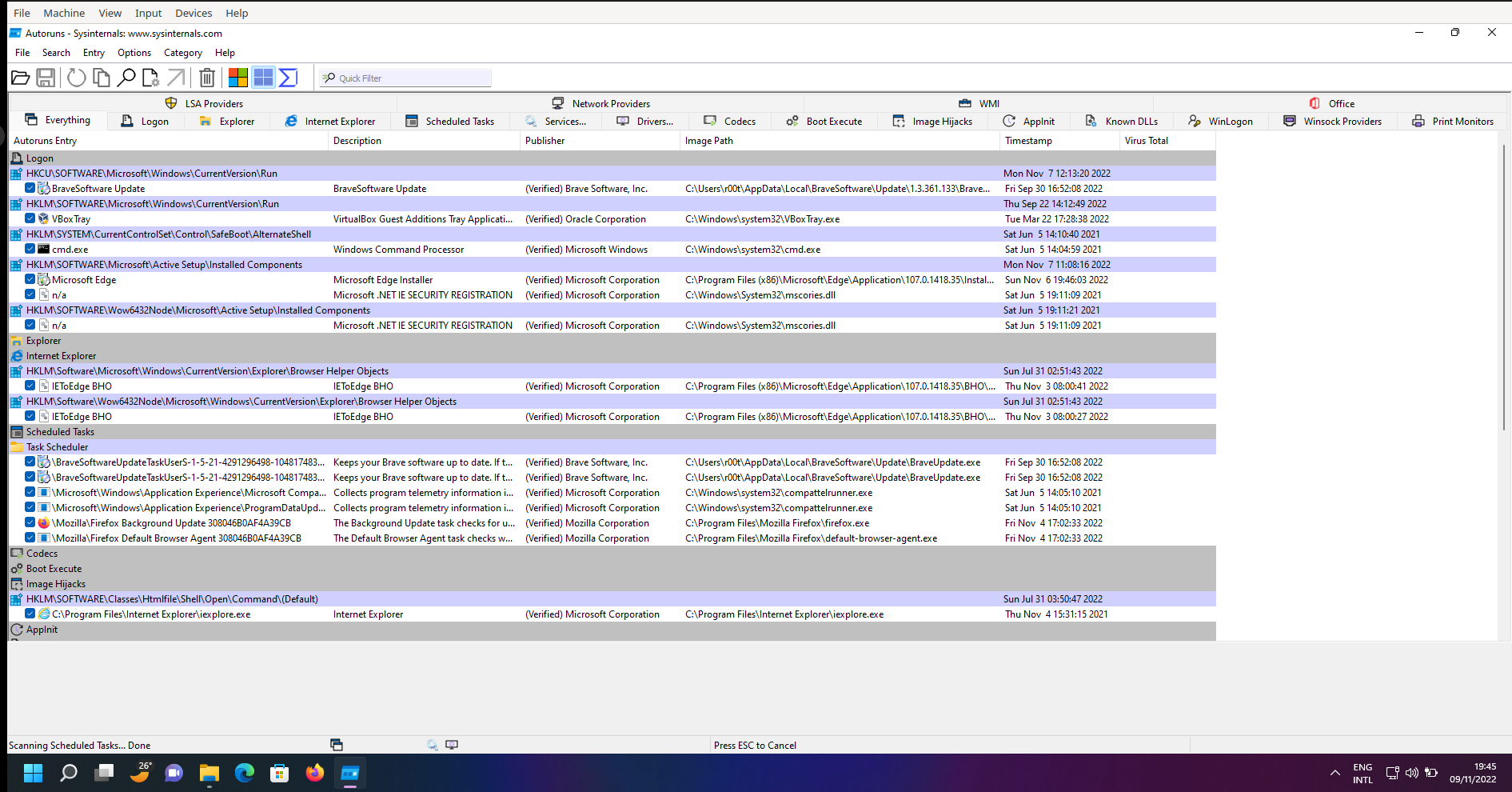
**procexp64.exe**

****

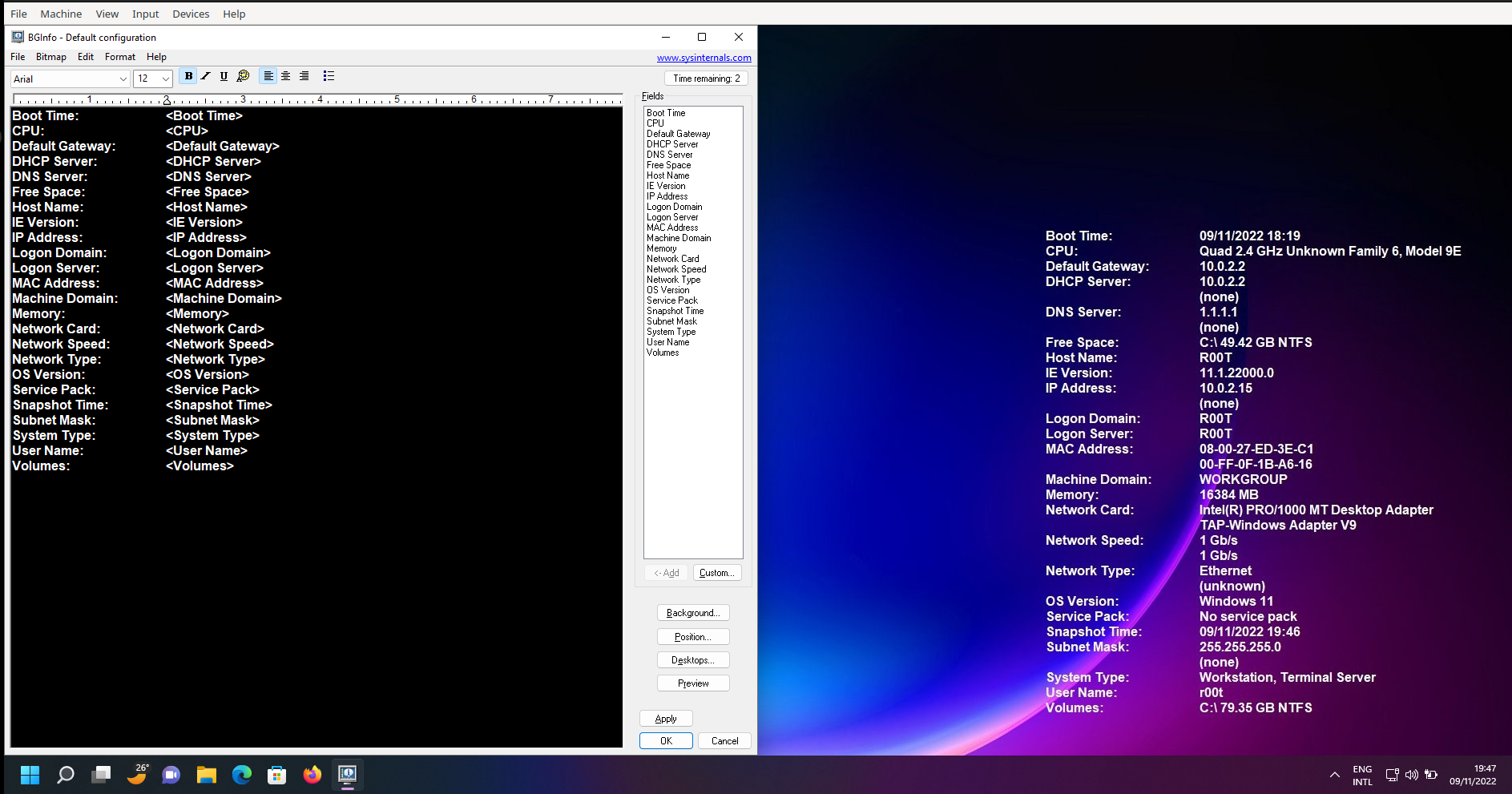
**Diskview64.exe**



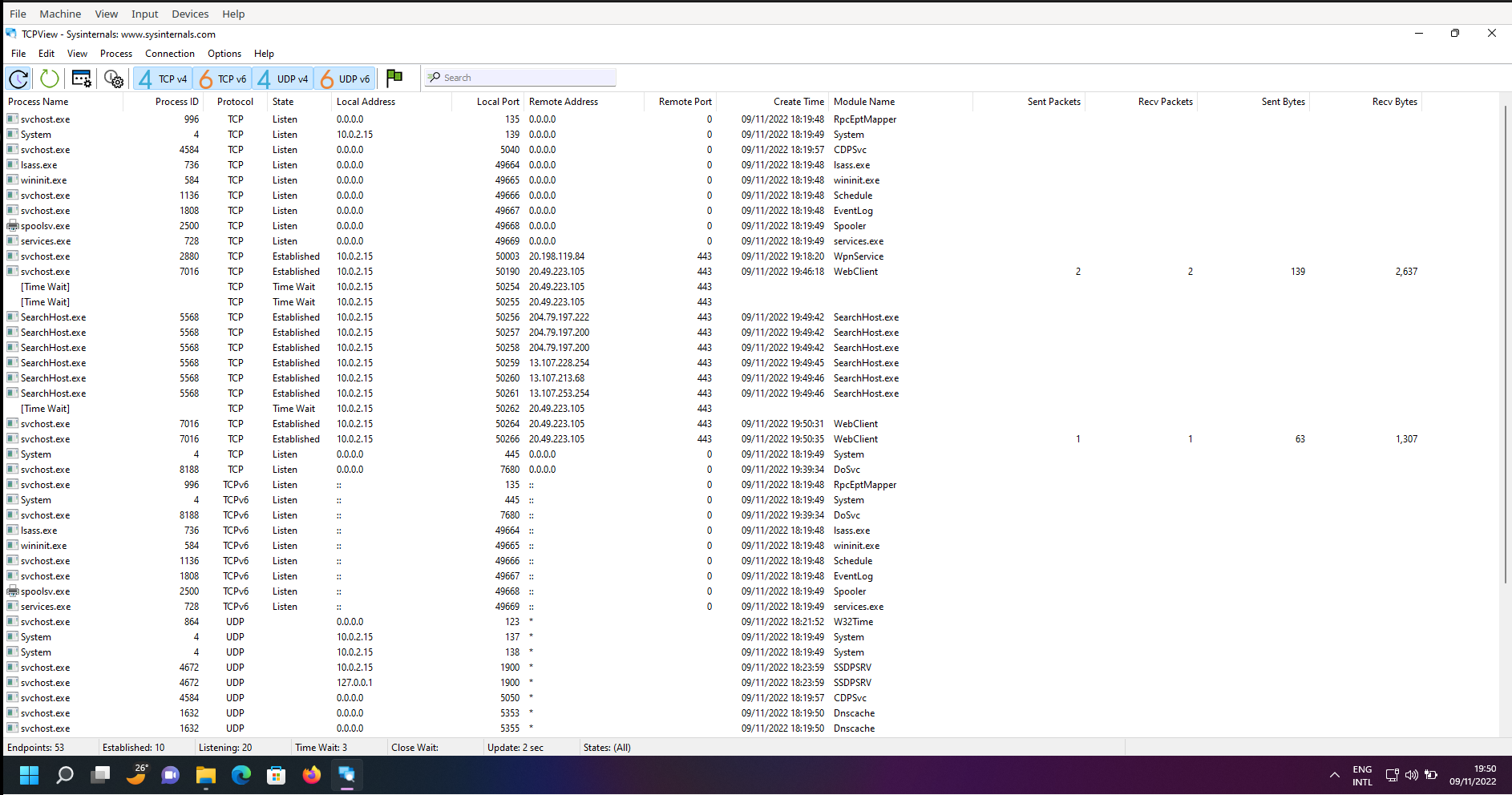
**autoruns64.exe**

****

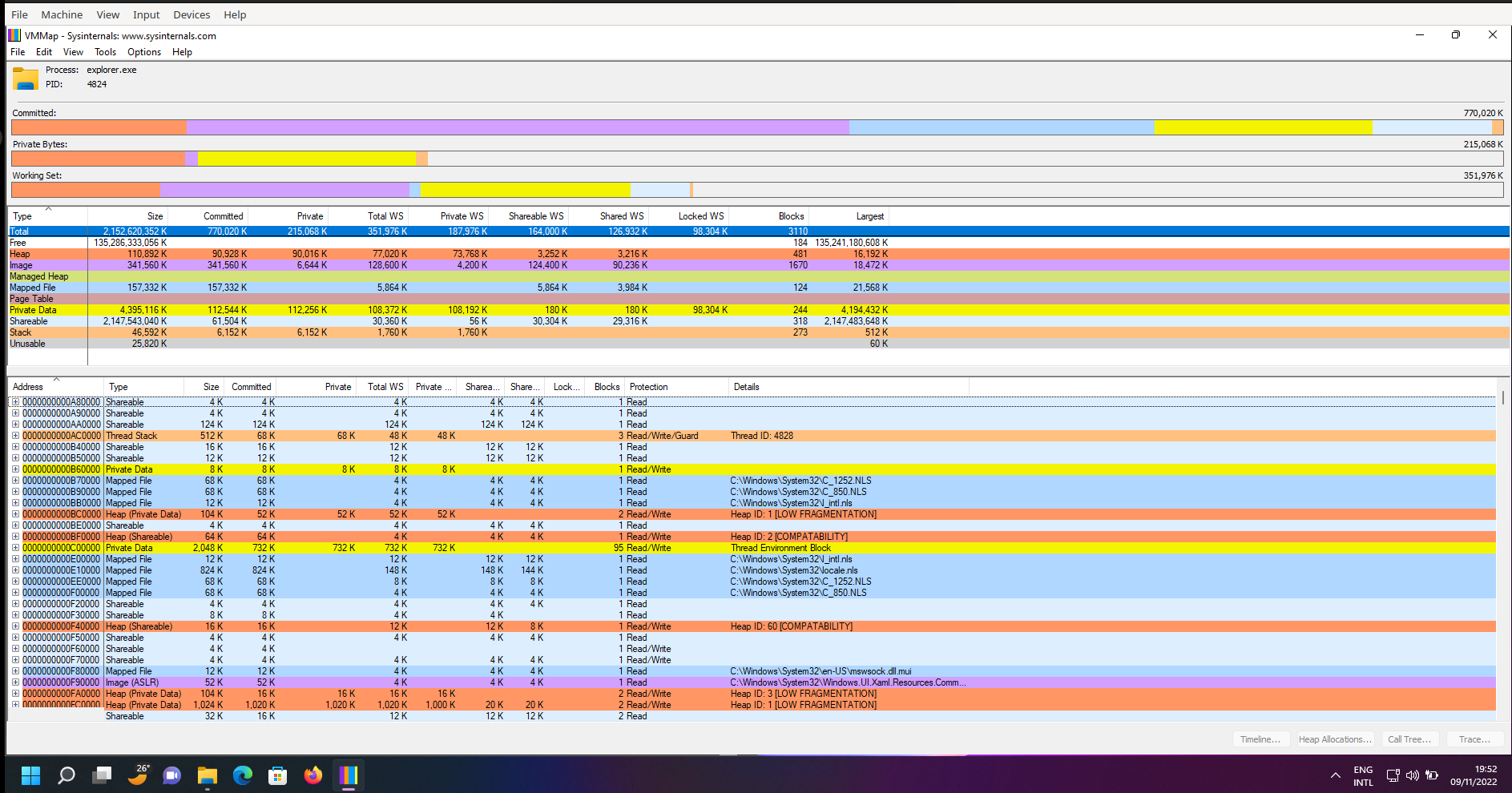
**bginfo64.exe**



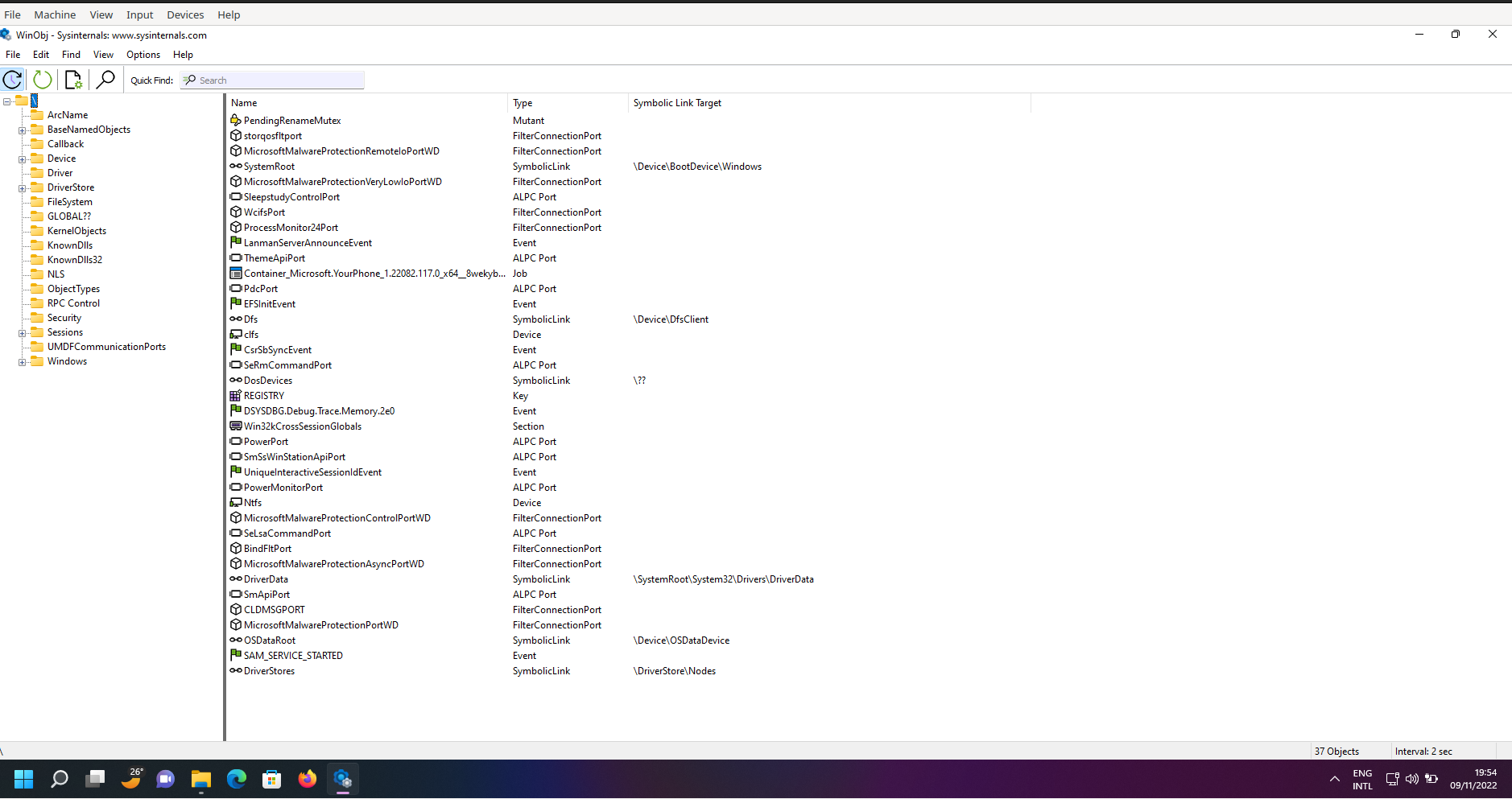
**tcpview64.exe**



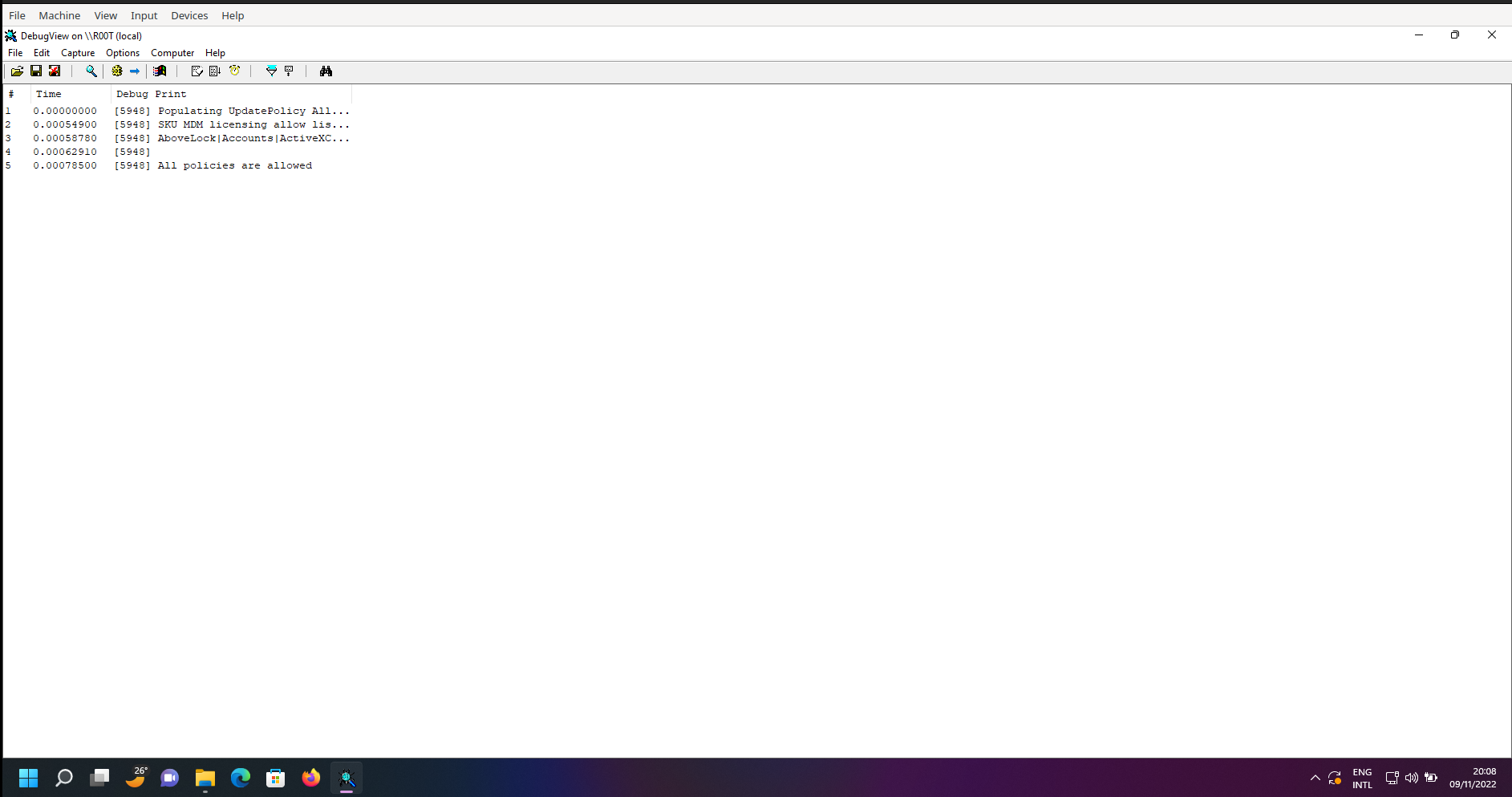
**vmmap64.exe**



**WinObj64.exe**

****

**dbgview64.exe**

****

**Conclusion & Future Scope :-**

**-** as per the results and demonstration we can conclude that sysinternals suite helps administrators to see disk usage by directory, measure network performance, remotely execute processes, dump event log records and much more

**Incident Response Management**

**Experiment :- 5**

**Title :-** Installation and Demonstration of snort

**Requirements :-** Linux Laptop and Active Internet connection

**Objectives :-** Implementing IDS policies

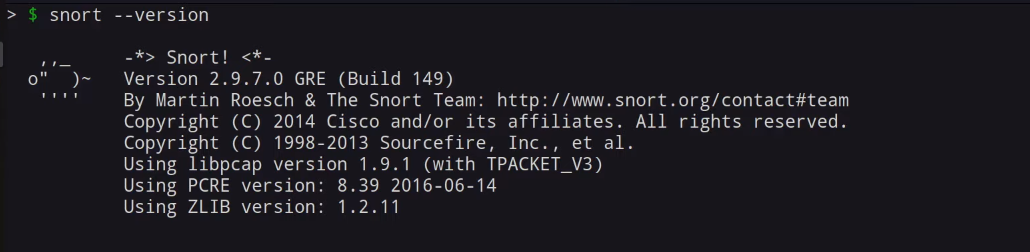
**Procedure :-**

1) Open up the Terminal in your Linux machine

2) type `**s*udo dnf install snort***`

3) go to the `/etc/snort/snort.conf` file here you can implement your own IDS/IPS rules

**Results :-**



**Conclusion & Future Scope :-**

**-** as per the results we conclude that snort is a foremost open source intrusion prevention system in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.