practice-1

1. Topic: network traffic analysis via packets capturing and detection of anomalies / possible attacks

- capturing and analyzing network traffic
- identifying normal communication patterns
- detecting possible anomalies or malicious activities
- using professional networking tools

Solution and practice

1. Installed and configured Wireshark in Windows (winget install Wireshark-Foundation.Wireshark)

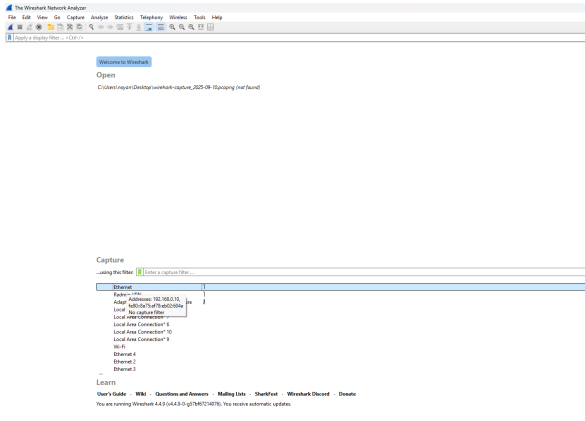
- source code: https://gitlab.com/wireshark/wireshark
- Wireshark in CLI form: tshark, tcpdump, or alternative
- However, Wireshark depricated native Python binding / API for interaction (reference: https://wiki.wireshark.org/python)
  - it is possible to use Lua (https://wiki.wireshark.org/lua)
  - that is why, downloaded additional library: pyshark (https://github.com/KimiNewt/pyshark)
  - network adapter need to be set in promiscuous mode for proper packat capture

2. setup environment for analysis:

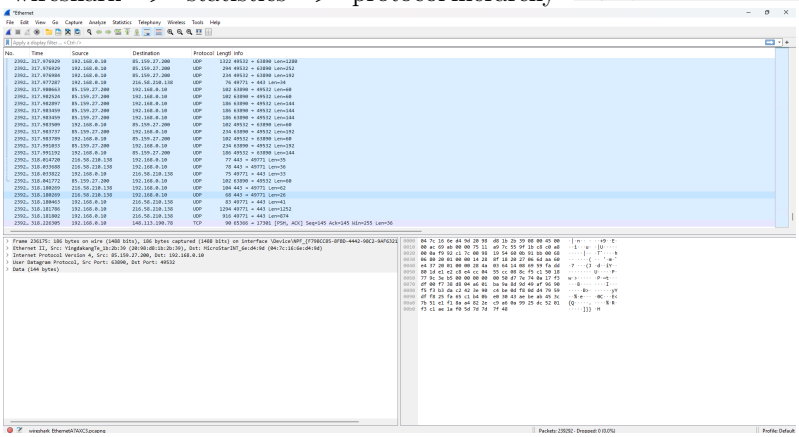
```
python3 -m venv venv
source .venv/bin/activate
pip install -r requirements.txt
```

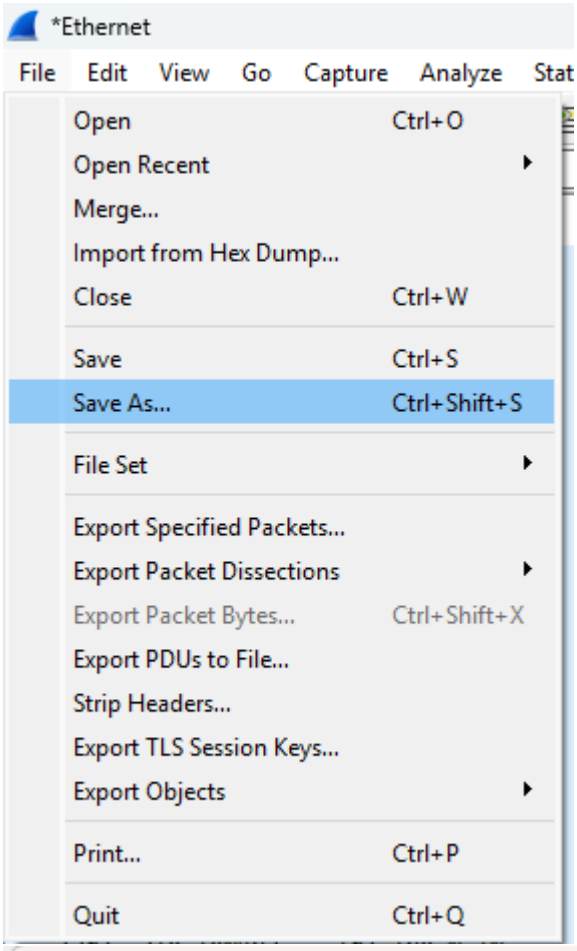
3. Captured traffic from Windows machine for 5+ minutes with web browsing, file downloads, DNS requests, VPN connection, etc.

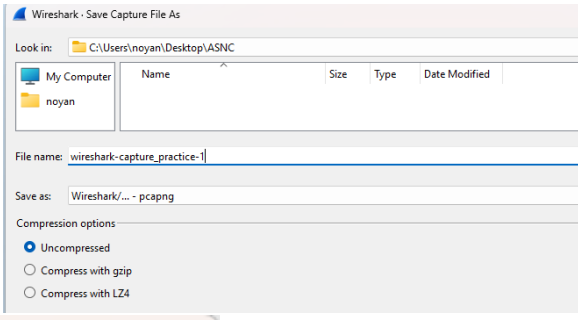
- or download traffic sample like https://www.wireshark.org/resources#sample-captures
- saved file in .pcap format in `/local_data`
- analyzed protcols: most frequent protocols in captured data in summary table (protocol / percentage of traffic)

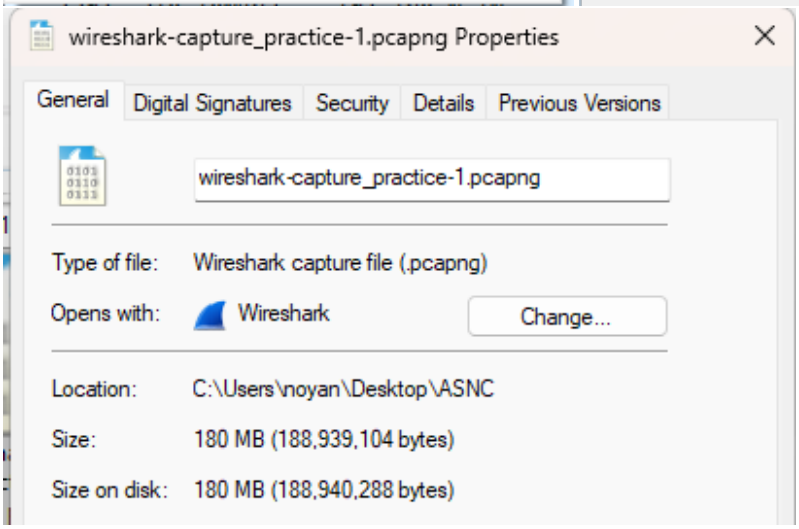


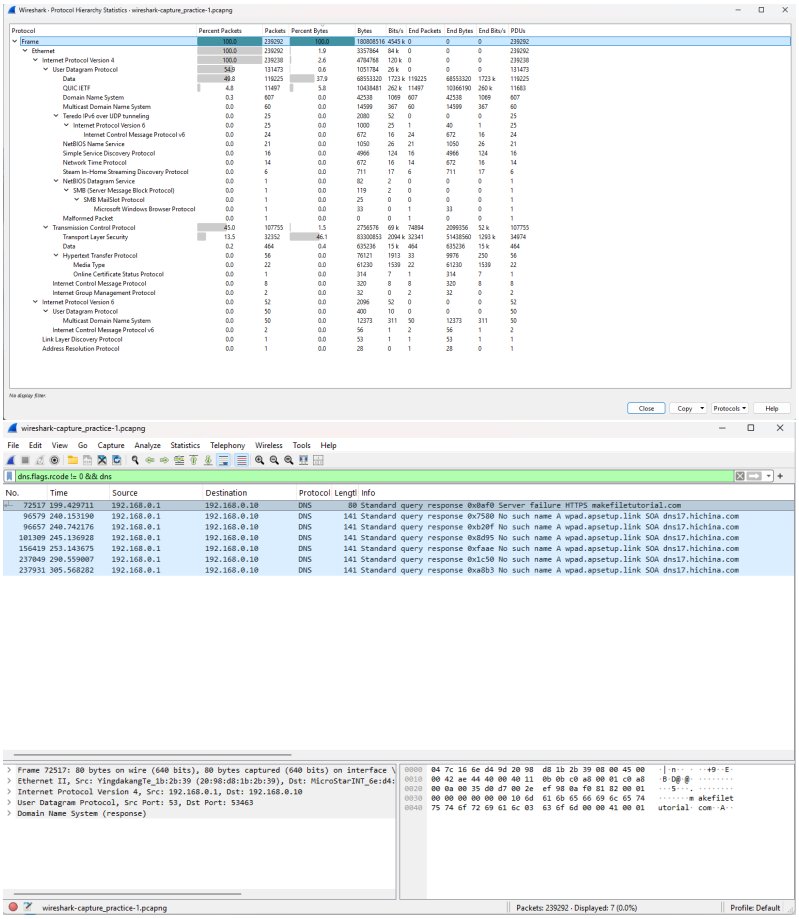
– “wireshark” -> “statistics” -> “protocol hierarchy”




*Ethernet
File
Edit
View
Go
Capture
Analyze
Stat
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Strip Headers...
Export TLS Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q

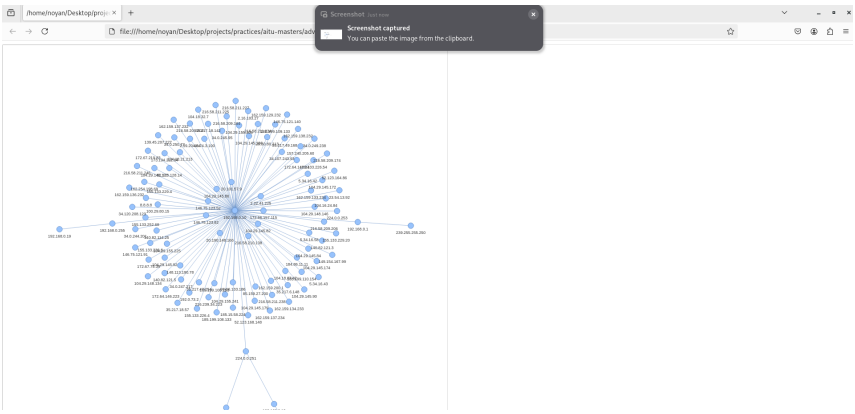

Wireshark · Save Capture File As
Look in: C:\Users\noyan\Desktop\ASNC
My Computer
noyan
Name
Size
Type
Date Modified
File name: wireshark-capture_practice-1
Save as: Wireshark/... - pcapng
Compression options
Uncompressed
Compress with gzip
Compress with LZ4


wireshark-capture_practice-1.pcapng Properties
General
Digital Signatures
Security
Details
Previous Versions
wireshark-capture_practice-1.pcapng
Type of file: Wireshark capture file (.pcapng)
Opens with: Wireshark
Change...
Location: C:\Users\noyan\Desktop\ASNC
Size: 180 MB (188,939,104 bytes)
Size on disk: 180 MB (188,940,288 bytes)



4. Anomaly and attack detection

- detecting possible anomalies in the traffic (e.g., repeated failed DNS requests, ARP spoofing attemps, unusual port scanning activity)
- suspicious flows with malicious activity
- provided practical graph representation in main.py to identify connections


/home/noyan/Desktop/proje
file:///home/noyan/Desktop/projects/practices/aitu-masters/adv
Screenshot Just now
Screenshot captured
You can paste the image from the clipboard.