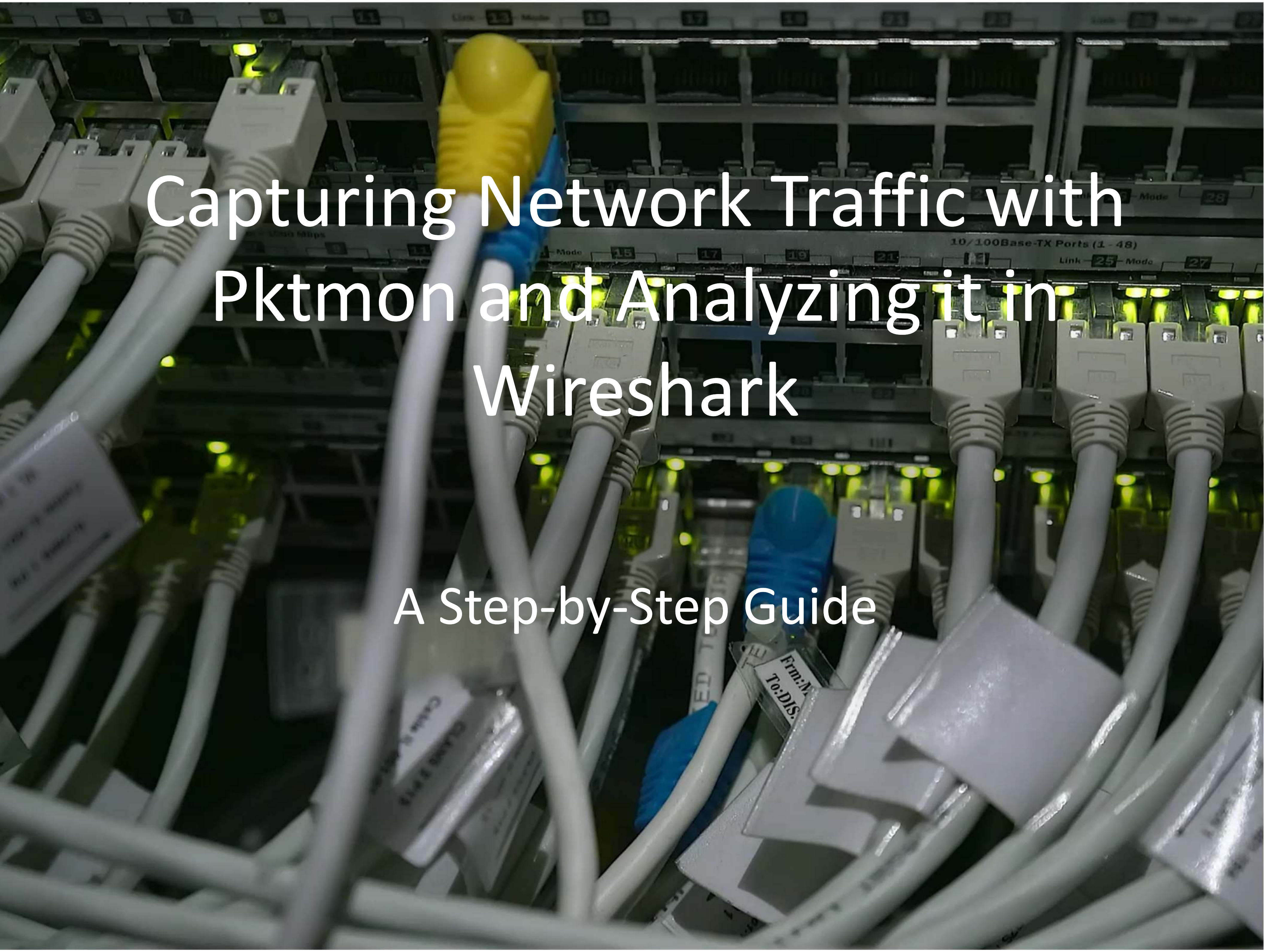


Capturing Network Traffic with Pktmon and Analyzing it in Wireshark

A Step-by-Step Guide

What is packet capture

- Logs all traffic that flows in and out of a machine
- Useful diagnostic tool when something is not working
- Wireshark is the most common tool

What is Pktmon?

Pktmon (Packet Monitor) is a built-in Windows network diagnostics tool.

Introduced in Windows 10 2004 update.

Installed on Server 2019 and later

Can capture, filter, and log network traffic.

Reduces the need to install and
patch Wireshark when packet capture is needed

Basic Traffic capture with Pktmon

Open	Open Command Prompt as Administrator.
Change	Change to the folder you want to use to store the capture
Logging	Start logging: pktmon start –c
Reproduce	Reproduce the issue
Validate	Validate capture by running pktmon counters
Logging	Stop logging: pktmon stop
Output	Output saved as .etl file in current directory.

Converting .etl to .pcapng or txt

Use the command: pktmon etl2pcapng pktmon.etl

File is created in current directory and can be sent to network or middleware for analysis

Use the command: pktmon etl2txt pktmon.etl

File can be opened in a text editor

Opening in Wireshark

- Open Wireshark.
- Load the .pcapng file: File > Open > Select pktmon.pcapng
- Analyze traffic using filters and protocol analyzers
- Example filters: ip.addr == 192.168.1.1, tcp.port == 80

Enhancing capture

- By default, only the first 128 bytes captured, Entire packet log using the command: pktmon start –c --pkt-size 0
- Analyzing all the data is like drinking from a fire hose
- Filters allow focus on what is needed
- Multiple filters can be added
- If a filer is not needed, you will need to clear and start over
- Specifying a nic may improve results

Filtering before capture

Filter created by pktmon filter add then a paramater as follows:

–t ICMP (TCP, UDP or protocol number)

-I 10.0.45.10 or 10.0.45.0/24 for IP or subnet

-p 443 or –p 80 443 for ports

Pktmon filter remove to clear

Selecting only one nic

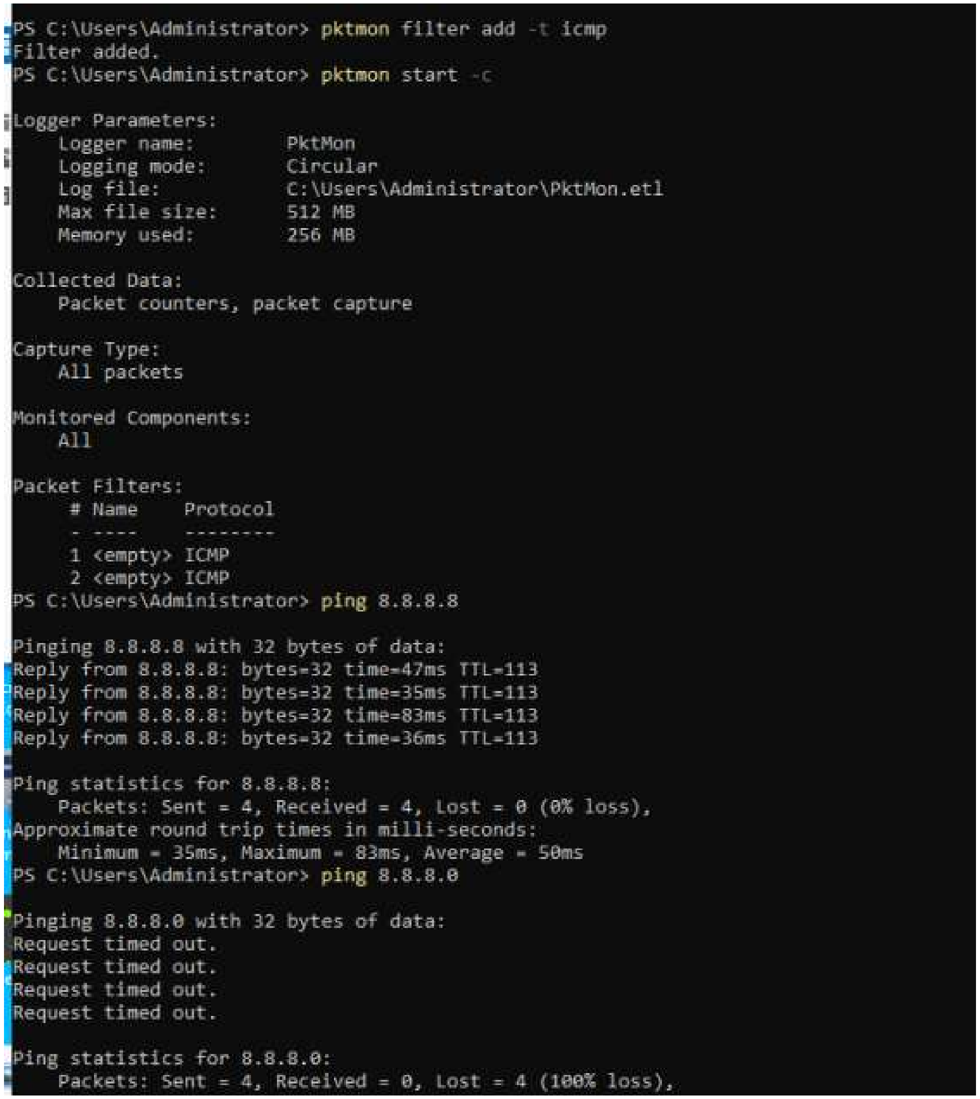
Allows more focus

pktmon list will show all present nics

Add –comp (ID number) to the end of the command to specify a nic

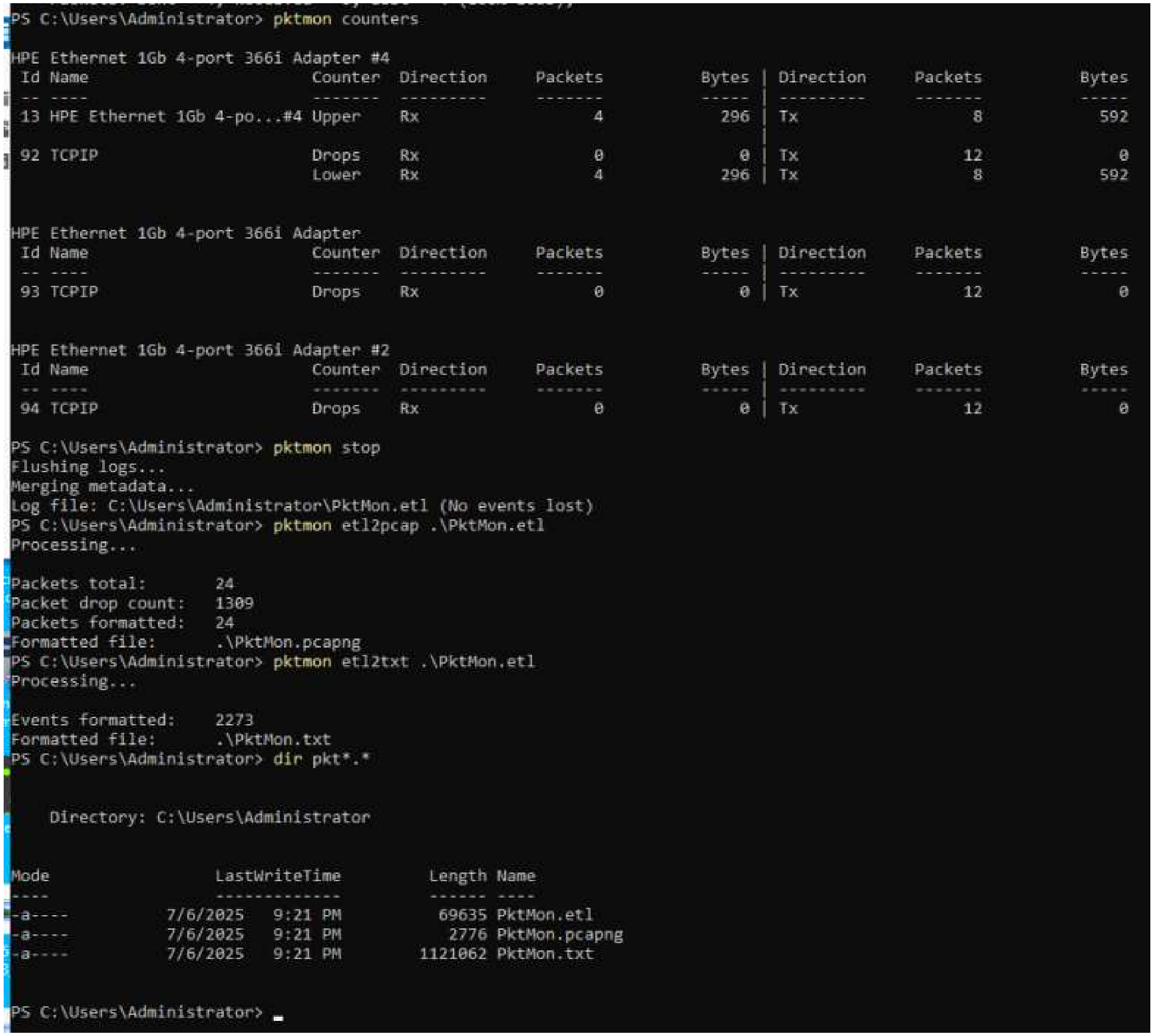
e.g. pktmon start -c --comp 15

Example



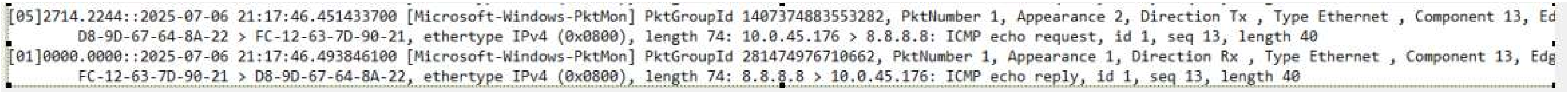
```
PS C:\Users\Administrator> pktmon filter add -t icmp
Filter added.
PS C:\Users\Administrator> pktmon start -c

Logger Parameters:
    Logger name:        PktMon
    Logging mode:       Circular
    Log file:           C:\Users\Administrator\PktMon.etl
    Max file size:      512 MB
    Memory used:        256 MB

Collected Data:
    Packet counters, packet capture

Capture Type:
    All packets

Monitored Components:
    All

Packet Filters:
     # Name    Protocol
     - ----    --------
     1 <empty> ICMP
     2 <empty> ICMP
PS C:\Users\Administrator> ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=47ms TTL=113
Reply from 8.8.8.8: bytes=32 time=35ms TTL=113
Reply from 8.8.8.8: bytes=32 time=83ms TTL=113
Reply from 8.8.8.8: bytes=32 time=36ms TTL=113

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 35ms, Maximum = 83ms, Average = 50ms
PS C:\Users\Administrator> ping 8.8.8.0

Pinging 8.8.8.0 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.0:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Example (2)

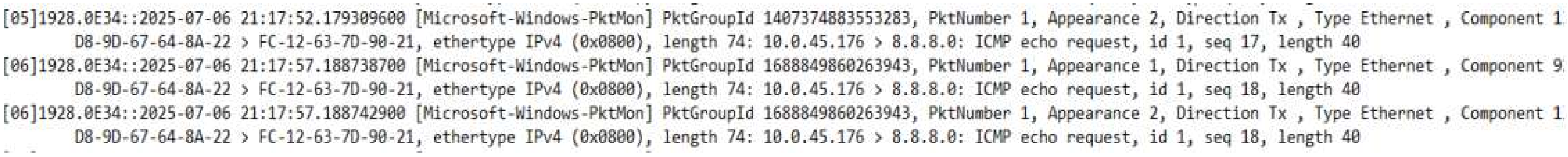


```
PS C:\Users\Administrator> pktmon counters

HPE Ethernet 1Gb 4-port 366i Adapter #4
 Id Name                       Counter  Direction     Packets           Bytes | Direction     Packets           Bytes
 -- ----                       -------  ---------     -------           ----- | ---------     -------           -----
 13 HPE Ethernet 1Gb 4-po...#4 Upper    Rx                  4             296 | Tx                  8             592
                                                                              |
 92 TCPIP                      Drops    Rx                  0               0 | Tx                 12               0
                               Lower    Rx                  4             296 | Tx                  8             592


HPE Ethernet 1Gb 4-port 366i Adapter
 Id Name                       Counter  Direction     Packets           Bytes | Direction     Packets           Bytes
 -- ----                       -------  ---------     -------           ----- | ---------     -------           -----
 93 TCPIP                      Drops    Rx                  0               0 | Tx                 12               0


HPE Ethernet 1Gb 4-port 366i Adapter #2
 Id Name                       Counter  Direction     Packets           Bytes | Direction     Packets           Bytes
 -- ----                       -------  ---------     -------           ----- | ---------     -------           -----
 94 TCPIP                      Drops    Rx                  0               0 | Tx                 12               0

PS C:\Users\Administrator> pktmon stop
Flushing logs...
Merging metadata...
Log file: C:\Users\Administrator\PktMon.etl (No events lost)
PS C:\Users\Administrator> pktmon etl2pcap .\PktMon.etl
Processing...

Packets total:       24
Packet drop count:   1309
Packets formatted:   24
Formatted file:      .\PktMon.pcapng
PS C:\Users\Administrator> pktmon etl2txt .\PktMon.etl
Processing...

Events formatted:    2273
Formatted file:      .\PktMon.txt
PS C:\Users\Administrator> dir pkt*.*


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          7/6/2025   9:21 PM          69635 PktMon.etl
-a----          7/6/2025   9:21 PM           2776 PktMon.pcapng
-a----          7/6/2025   9:21 PM        1121062 PktMon.txt


PS C:\Users\Administrator> _
```

Log Output

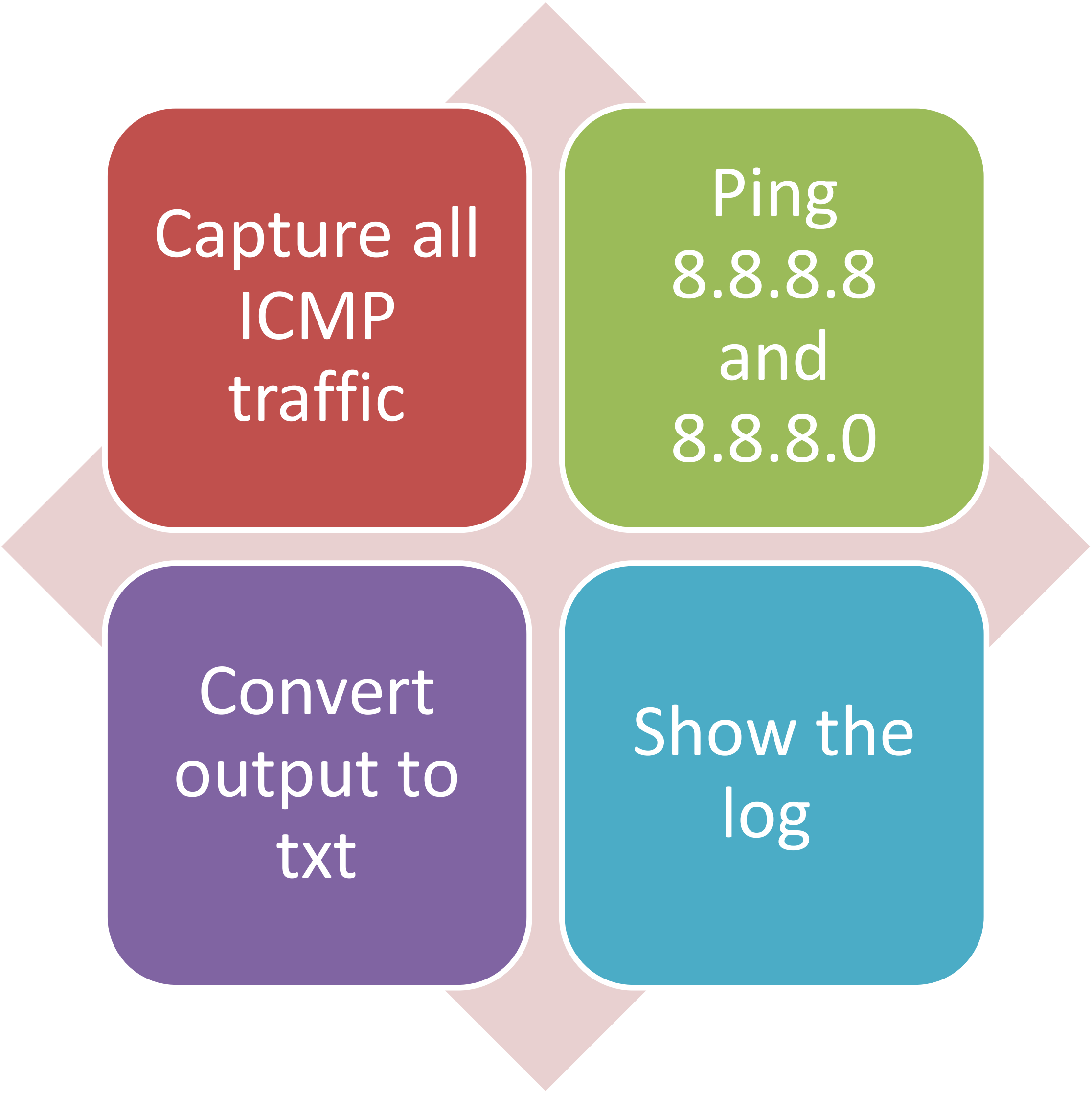


```
[05]2714.2244::2025-07-06 21:17:46.451433700 [Microsoft-Windows-PktMon] PktGroupId 1407374883553282, PktNumber 1, Appearance 2, Direction Tx , Type Ethernet , Component 13, Ed
        D8-9D-67-64-8A-22 > FC-12-63-7D-90-21, ethertype IPv4 (0x0800), length 74: 10.0.45.176 > 8.8.8.8: ICMP echo request, id 1, seq 13, length 40
[01]0000.0000::2025-07-06 21:17:46.493846100 [Microsoft-Windows-PktMon] PktGroupId 281474976710662, PktNumber 1, Appearance 1, Direction Rx , Type Ethernet , Component 13, Edg
        FC-12-63-7D-90-21 > D8-9D-67-64-8A-22, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.0.45.176: ICMP echo reply, id 1, seq 13, length 40
```



```
[05]1928.0E34::2025-07-06 21:17:52.179309600 [Microsoft-Windows-PktMon] PktGroupId 1407374883553283, PktNumber 1, Appearance 2, Direction Tx , Type Ethernet , Component 1
        D8-9D-67-64-8A-22 > FC-12-63-7D-90-21, ethertype IPv4 (0x0800), length 74: 10.0.45.176 > 8.8.8.0: ICMP echo request, id 1, seq 17, length 40
[06]1928.0E34::2025-07-06 21:17:57.188738700 [Microsoft-Windows-PktMon] PktGroupId 1688849860263943, PktNumber 1, Appearance 1, Direction Tx , Type Ethernet , Component 9
        D8-9D-67-64-8A-22 > FC-12-63-7D-90-21, ethertype IPv4 (0x0800), length 74: 10.0.45.176 > 8.8.8.0: ICMP echo request, id 1, seq 18, length 40
[06]1928.0E34::2025-07-06 21:17:57.188742900 [Microsoft-Windows-PktMon] PktGroupId 1688849860263943, PktNumber 1, Appearance 2, Direction Tx , Type Ethernet , Component 1
        D8-9D-67-64-8A-22 > FC-12-63-7D-90-21, ethertype IPv4 (0x0800), length 74: 10.0.45.176 > 8.8.8.0: ICMP echo request, id 1, seq 18, length 40
```

Demo



Capture all ICMP traffic

Ping 8.8.8.8 and 8.8.8.0

Convert output to txt

Show the log

Final notes

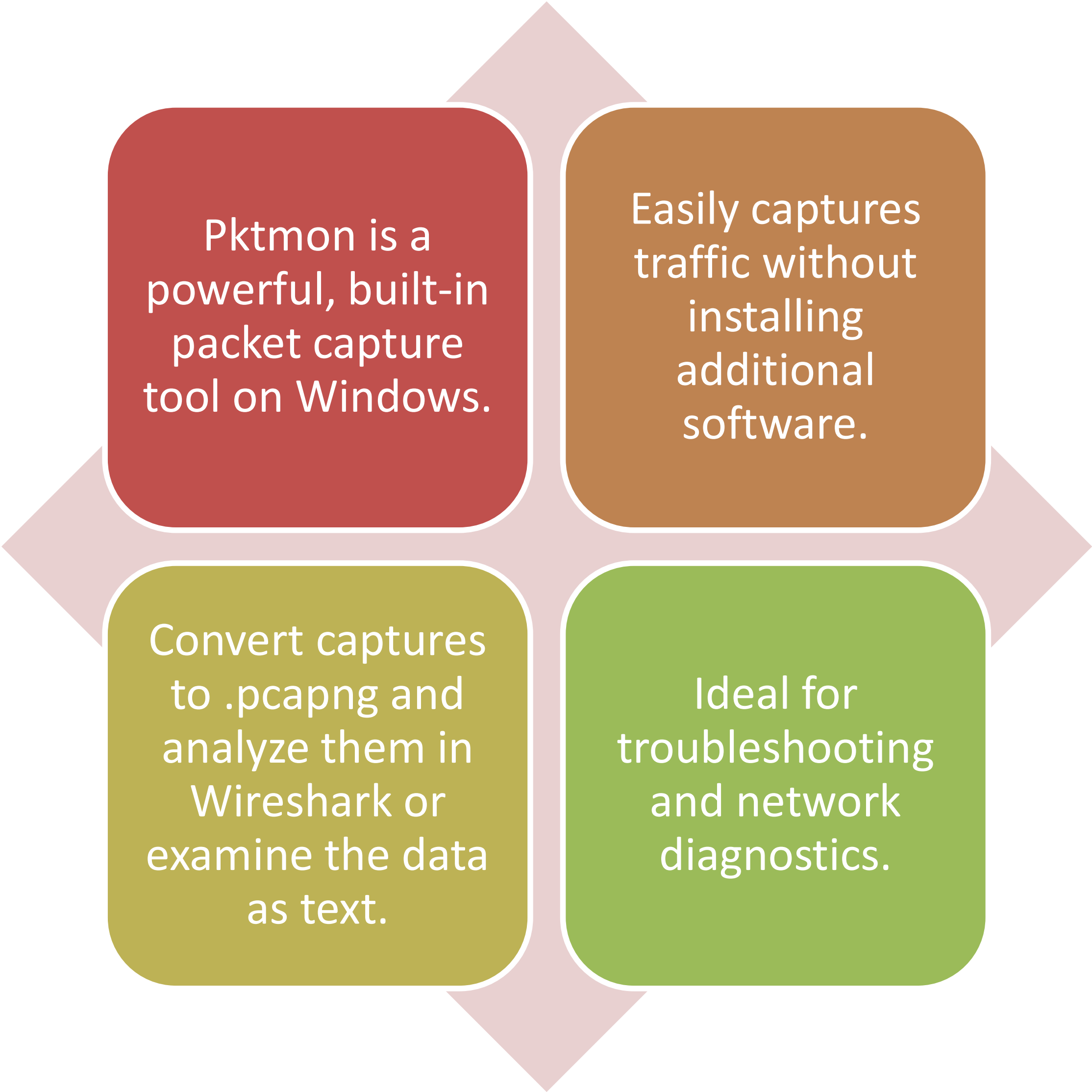
You may see retransmits if you don’t specify a NIC, those can be ignored

Specify the NIC for a cleaner output

Read the pktmon page for more details about how to use this tool.

This tool is not as robust as wireshark, we may still need wireshark in some cases

Summary



Pktmon is a powerful, built-in packet capture tool on Windows.

Easily captures traffic without installing additional software.

Convert captures to .pcapng and analyze them in Wireshark or examine the data as text.

Ideal for troubleshooting and network diagnostics.

Reference Page

- Microsoft pktmon: Packet Monitor (Pktmon) | Microsoft Learn
- Pktmon filters: Pktmon command formatting | Microsoft Learn