FORTINET
Training Institute

FORTINET
CERTIFIED
SOLUTION
SPECIALIST
Security
Operations

Security Operations Analyst

Attack Surface and Vectors

FortiAnalyzer 7.4

Last Modified: 22 January 2025

Reviewing Traffic Flows

Objectives

- Describe how to capture traffic on Fortinet devices
- Describe how to capture traffic on an endpoint
- Describe how to use Wireshark to analyze packet captures

Packet Capture—Introduction

- As a SOC analyst, you should know how to capture and review traffic flows, so that you can:
  - Analyze the traffic in real time or save a copy
  - Present evidence of a vulnerability or a suspected attack
  - Establish baselines for expected traffic flows

- To capture traffic on FortiAnalyzer and FortiGate on the CLI:

```
# diagnose sniffer packet <interface> '<filter>' <verbosity> <count> <timestamp>
```

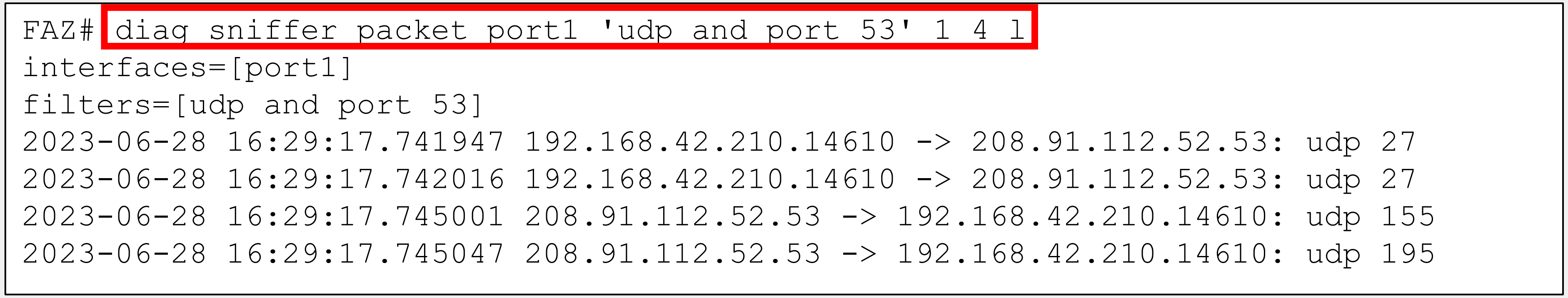
  - `<interface>` can be `any` or a specific interface (that is `port1` or `internal`)
  - `<filter>` follows tcpdump format
  - `<verbosity>` specifies how much information to capture
  - `<count>` the number of packets to capture
  - `<timestamp>` print time stamp information
    - `a` – prints absolute UTC timestamp
    - `l` – prints local timestamp

Training Institute

Packet Capture on FortiAnalyzer

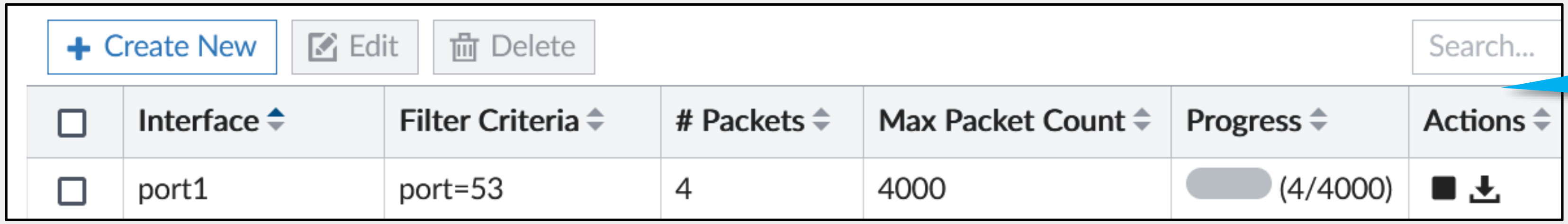
Example Sniffer	CLI Command to Use
DNS Traffic traversing port1, on level 1 verbosity, 4 packet limit, and in local system time	`# diagnose sniffer packet <interface> <filter> <level> <count> <timestamp>`

- Example output



```
FAZ# diag sniffer packet port1 'udp and port 53' 1 4 l
interfaces=[port1]
filters=[udp and port 53]
2023-06-28 16:29:17.741947 192.168.42.210.14610 -> 208.91.112.52.53: udp 27
2023-06-28 16:29:17.742016 192.168.42.210.14610 -> 208.91.112.52.53: udp 27
2023-06-28 16:29:17.745001 208.91.112.52.53 -> 192.168.42.210.14610: udp 155
2023-06-28 16:29:17.745047 208.91.112.52.53 -> 192.168.42.210.14610: udp 195
```

System Settings > Network



□	Interface	Filter Criteria	# Packets	Max Packet Count	Progress	Actions
□	port1	port=53	4	4000	(4/4000)	■ ⬇

Can also capture using the GUI

Packet Capture From the FortiGate CLI

Example Sniffer	CLI Command to Use
ICMP traffic to and from 10.0.10.254, on level 6 verbosity, with no packet limit, and in local system time	`# diagnose sniffer packet <interface> <filter> <level> <count> <timestamp>`

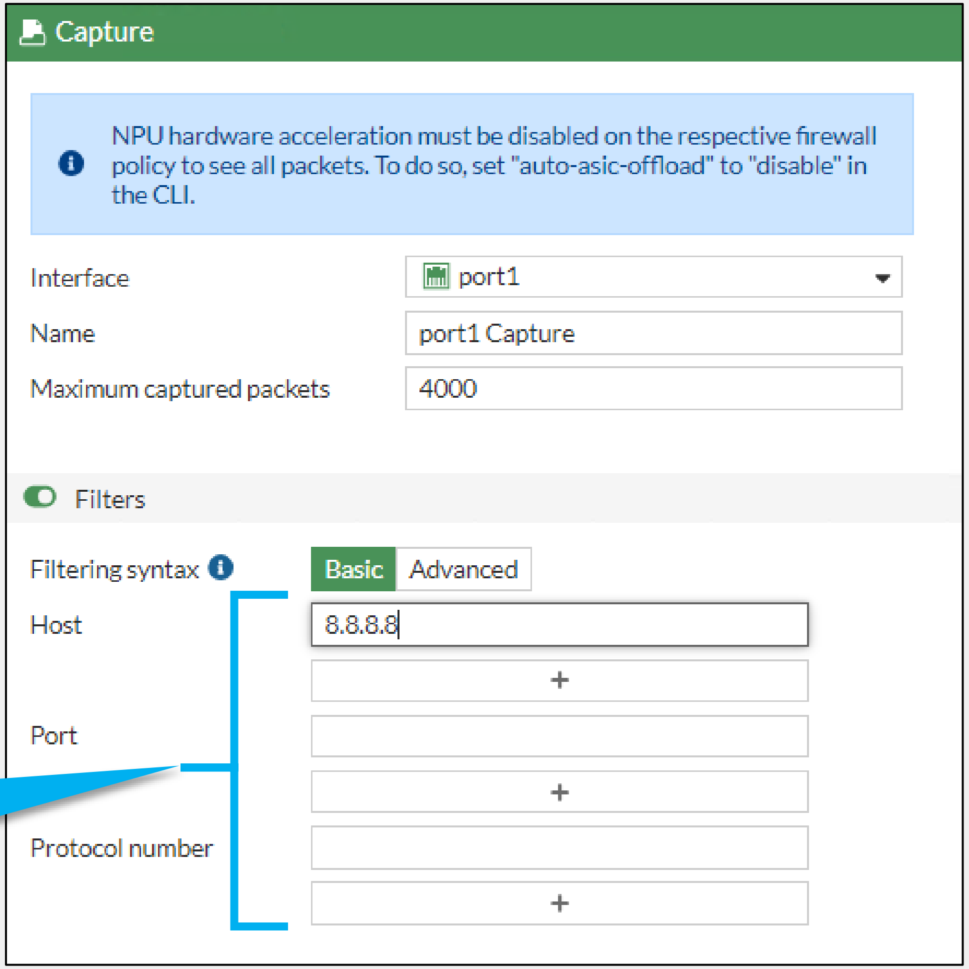
- Example output

```
FortiGate# diagnose sniffer packet Students "icmp and host 10.0.10.254" 6 0 l
2021-05-26 07:43:28.653443 Students -- 10.0.10.2 -> 10.0.10.254: icmp: echo request
0x0000   0009 0f09 0003 5c85 7e32 16a2 0800 4500        ......\.~2....E.
0x0010   0054 9fef 4000 4001 71ba 0a00 0a02 0a00        .T..@.@.q.......
0x0020   0afe 0800 cec5 1686 0001 905e ae60 dff0        ...........^.`..
0x0030   0900 0809 0a0b 0c0d 0e0f 1011 1213 1415        ................
0x0040   1617 1819 1a1b 1c1d 1e1f 2021 2223 2425        ............!"#$%
0x0050   2627 2829 2a2b 2c2d 2e2f 3031 3233 3435        &'()*+,-./012345
0x0060   3637
```

Packet Capture From the FortiGate GUI

- Automatically convert packet capture to PCAP (no conversion script required)
- Embedded real-time analysis page

Network > Diagnostics > Packet Capture



Capture

NPU hardware acceleration must be disabled on the respective firewall policy to see all packets. To do so, set "auto-asic-offload" to "disable" in the CLI.

Interface: port1

Name: port1 Capture

Maximum captured packets: 4000

Filters

Filtering syntax: [✓ Basic] Advanced

Host: 8.8.8.8

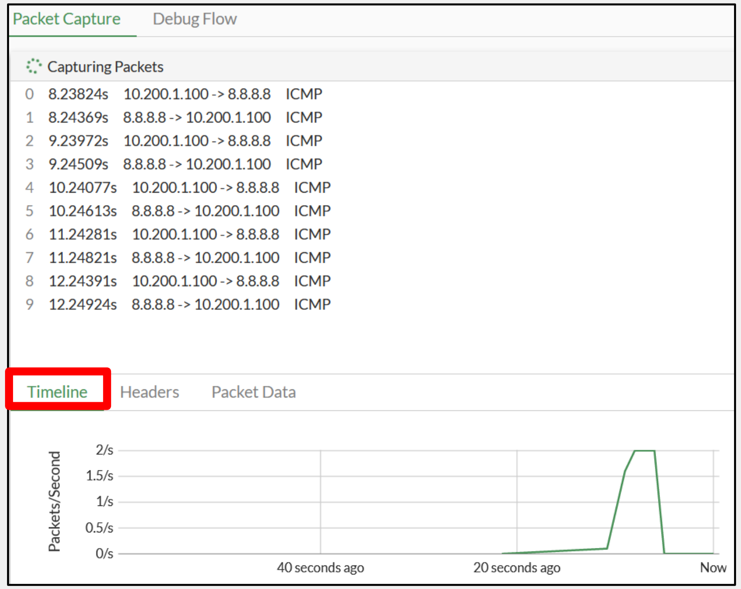
Port:

Protocol number:

Set up filter to narrow down packet capture as much as possible

Packet Capture From the FortiGate GUI (Contd)

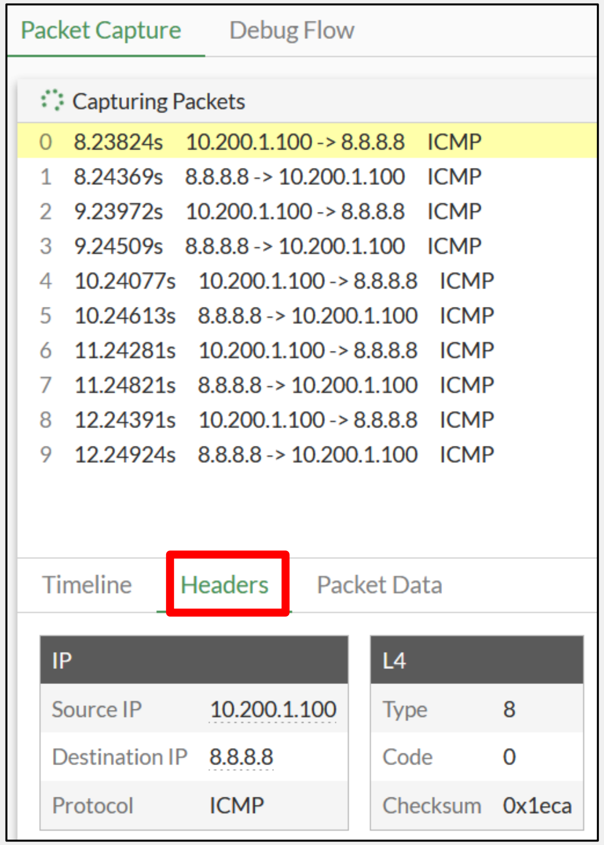
Packet Capture > Timeline



```
0  8.23824s   10.200.1.100 -> 8.8.8.8   ICMP
1  8.24369s   8.8.8.8 -> 10.200.1.100   ICMP
2  9.23972s   10.200.1.100 -> 8.8.8.8   ICMP
3  9.24509s   8.8.8.8 -> 10.200.1.100   ICMP
4  10.24077s  10.200.1.100 -> 8.8.8.8   ICMP
5  10.24613s  8.8.8.8 -> 10.200.1.100   ICMP
6  11.24281s  10.200.1.100 -> 8.8.8.8   ICMP
7  11.24821s  8.8.8.8 -> 10.200.1.100   ICMP
8  12.24391s  10.200.1.100 -> 8.8.8.8   ICMP
9  12.24924s  8.8.8.8 -> 10.200.1.100   ICMP
```

- Useful to identify important traffic events

Packet Capture > Headers



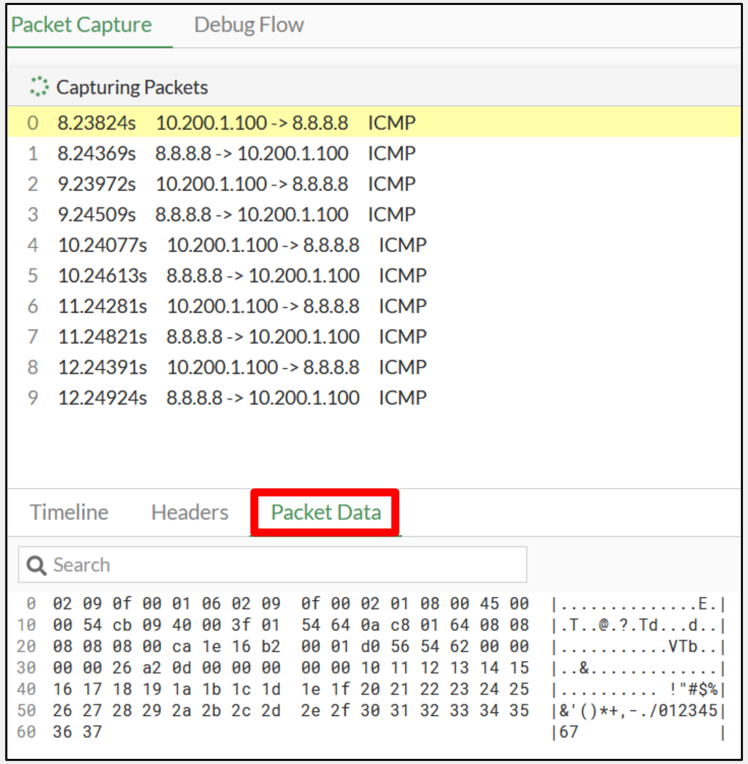
```
0  8.23824s   10.200.1.100 -> 8.8.8.8   ICMP
1  8.24369s   8.8.8.8 -> 10.200.1.100   ICMP
2  9.23972s   10.200.1.100 -> 8.8.8.8   ICMP
3  9.24509s   8.8.8.8 -> 10.200.1.100   ICMP
4  10.24077s  10.200.1.100 -> 8.8.8.8   ICMP
5  10.24613s  8.8.8.8 -> 10.200.1.100   ICMP
6  11.24281s  10.200.1.100 -> 8.8.8.8   ICMP
7  11.24821s  8.8.8.8 -> 10.200.1.100   ICMP
8  12.24391s  10.200.1.100 -> 8.8.8.8   ICMP
9  12.24924s  8.8.8.8 -> 10.200.1.100   ICMP
```

IP	
Source IP	10.200.1.100
Destination IP	8.8.8.8
Protocol	ICMP

L4	
Type	8
Code	0
Checksum	0x1eca

- Basic IP and layer 4 data

Packet Capture > Packet Data



```
0  8.23824s   10.200.1.100 -> 8.8.8.8   ICMP
1  8.24369s   8.8.8.8 -> 10.200.1.100   ICMP
2  9.23972s   10.200.1.100 -> 8.8.8.8   ICMP
3  9.24509s   8.8.8.8 -> 10.200.1.100   ICMP
4  10.24077s  10.200.1.100 -> 8.8.8.8   ICMP
5  10.24613s  8.8.8.8 -> 10.200.1.100   ICMP
6  11.24281s  10.200.1.100 -> 8.8.8.8   ICMP
7  11.24821s  8.8.8.8 -> 10.200.1.100   ICMP
8  12.24391s  10.200.1.100 -> 8.8.8.8   ICMP
9  12.24924s  8.8.8.8 -> 10.200.1.100   ICMP
```

```
 0  02 09 0f 00 01 06 02 09  0f 00 02 01 08 00 45 00  |..............E.|
10  00 54 cb 09 40 00 3f 01  54 64 0a c8 01 64 08 08  |.T..@.?.Td...d..|
20  08 08 08 00 ca 1e 16 b2  00 01 d0 56 54 62 00 00  |...........VTb..|
30  00 00 26 a2 0d 00 00 00  00 00 10 11 12 13 14 15  |..&.............|
40  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25  |.......... !"#$%|
50  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35  |&'()*+,-./012345|
60  36 37                                             |67              |
```

- Full packet data in HEX and ASCII formats

FORTINET
Training Institute

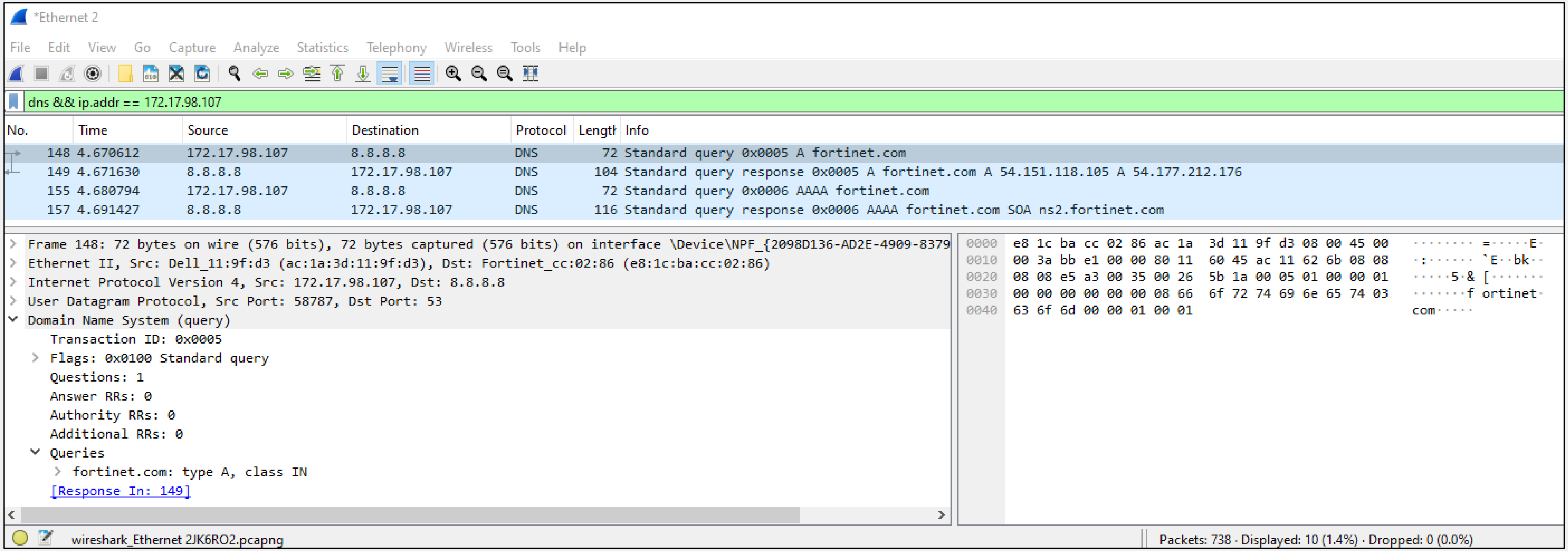
Packet Capture Verbosity Level

Level	IP Headers	Packet Payload	Ethernet Headers	Interface Name
1	•			
2	•	•		
3	•	•	•	
4	•			•
5	•	•		•
6	•	•	•	•

- FortiAnalyzer supports levels 1–3 only; FortiGate supports levels 1–6
- The most common levels are:
  - 4 – Prints the ingress and egress interfaces
    - You can verify how traffic is being routed, or if FortiGate is dropping packets
  - 3 or 6 – Prints the packet payload
    - You can convert this output to a PCAP file that you can open with a packet analyzer
  - If you don’t specify a level, the sniffer uses level `1` by default

Packet Capture on an Endpoint

Example Sniffer	Syntax Filter
On NIC Ethernet2: DNS traffic from and to host 172.17.98.107	`dns && ip.addr == 172.17.98.107`



```
dns && ip.addr == 172.17.98.107
```

```
No.   Time       Source          Destination     Protocol Length Info
  148 4.670612   172.17.98.107   8.8.8.8         DNS        72 Standard query 0x0005 A fortinet.com
  149 4.671630   8.8.8.8         172.17.98.107   DNS       104 Standard query response 0x0005 A fortinet.com A 54.151.118.105 A 54.177.212.176
  155 4.680794   172.17.98.107   8.8.8.8         DNS        72 Standard query 0x0006 AAAA fortinet.com
  157 4.691427   8.8.8.8         172.17.98.107   DNS       116 Standard query response 0x0006 AAAA fortinet.com SOA ns2.fortinet.com
```

```
> Frame 148: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{2098D136-AD2E-4909-8379
> Ethernet II, Src: Dell_11:9f:d3 (ac:1a:3d:11:9f:d3), Dst: Fortinet_cc:02:86 (e8:1c:ba:cc:02:86)
> Internet Protocol Version 4, Src: 172.17.98.107, Dst: 8.8.8.8
> User Datagram Protocol, Src Port: 58787, Dst Port: 53
v Domain Name System (query)
     Transaction ID: 0x0005
   > Flags: 0x0100 Standard query
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 0
   v Queries
      > fortinet.com: type A, class IN
     [Response In: 149]
```

```
0000  e8 1c ba cc 02 86 ac 1a  3d 11 9f d3 08 00 45 00   ········ =·····E·
0010  00 3a bb e1 00 00 80 11  60 45 ac 11 62 6b 08 08   ·:······ `E··bk··
0020  08 08 e5 a3 00 35 00 26  5b 1a 00 05 01 00 00 01   ·····5·& [·······
0030  00 00 00 00 00 00 08 66  6f 72 74 69 6e 65 74 03   ·······f ortinet·
0040  63 6f 6d 00 00 01 00 01                            com·····
```

wireshark_Ethernet 2JK6RO2.pcapng | Packets: 738 · Displayed: 10 (1.4%) · Dropped: 0 (0.0%)

FORTINET
Training Institute

Knowledge Check

1. Which packet capture method does not require a PCAP file conversion script?

   [✓ A. GUI]

   B. CLI

2. Which packet capture setting is different between FortiAnalyzer and FortiGate?

   A. Timestamp

   [✓ B. Verbosity]

Lesson Progress

- ✓ The Attack Surface
- ✓ Attack Vectors
- ✓ Reviewing Traffic Flows

Review

- ✓Describe how to capture traffic on Fortinet devices
- ✓Describe how to capture traffic on an endpoint
- ✓Describe how to use Wireshark to analyze packet captures