

[Open in app](#)

Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



TryHackMe | Wireshark: Packet Operations — Write-up

6 min read · Jun 29, 2023



igor_sec

Learn the fundamentals of packet analysis with Wireshark and how to find the needle in the haystack!

Link: <https://tryhackme.com/room/wiresharkpacketoperations>

“In this room, we will cover the fundamentals of packet analysis with Wireshark and investigate the event of interest at the packet-level. Note that this is the second room of the Wireshark room trio, and it is suggested to visit the first room ([Wireshark: The Basics](#)) to practice and refresh your Wireshark skills before starting this one.”

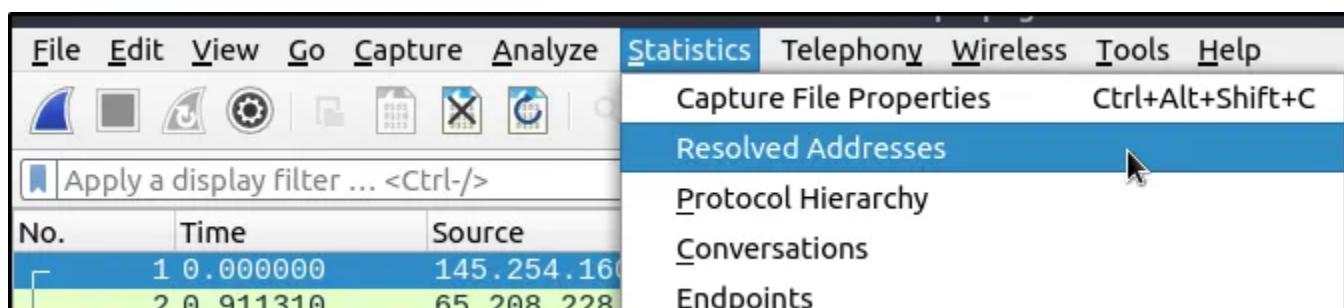
My write-up for the [Wireshark: The Basics](#) is found here <https://medium.com/@huglertomgaw/thm-wireshark-the-basics-9d5fa3c9a60e>

Task 2: Statistics | Summary

Investigate the resolved addresses. What is the IP address of the hostname starts with “bbc”?

Ans: 199.232.24.81

Go to Statistic then Resolved Addresses. Filter by typing the strings of the host name that we are after.

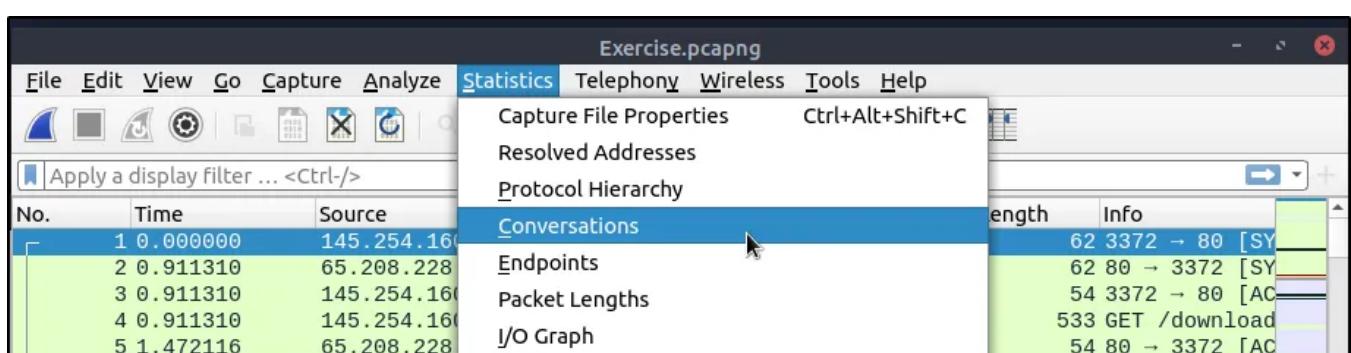


Wireshark · Resolved Addresses	
Hosts	Ports
<input type="text" value="bbc"/> All entries	
Address	Name
199.232.24.81	bbc.map.fastly.net

What is the number of IPv4 conversations?

Ans: 435

Go to Statistics then Conversations. IPv4 column contains all IPv4 conversations.

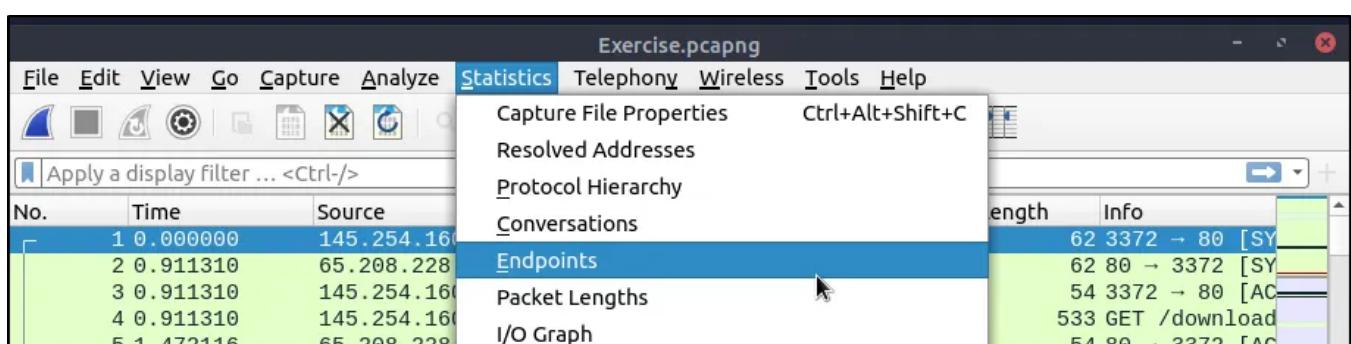


Wireshark · Conversations · Exercise.pcapng						
Ethernet · 25	IPv4 · 435	IPv6 · 4	TCP · 1490	UDP · 204		
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Pa
2.120.66.172	172.16.255.1	2	128	1	68	
4.2.2.2	192.168.43.9	6	588	3	294	
5.106.5.94	192.168.1.100	69	451	22	121	

How many bytes (k) were transferred from the “Micro-St” MAC address?

Ans: 7474

Go to Statistics then Endpoint.



Click the Name resolution to resolve host names of the endpoints.

Wireshark · Endpoints · Exercise.pcapng

Ethernet · 26	IPv4 · 436	IPv6 · 6	TCP · 2164	UDP · 224		
Address	▲ Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
Broadcast	81	18 k	0	0	81	18 k
fe:ff:20:00:01:00	43	25 k	23	22 k	20	2323
zte_2e:f0:5e	8527	831 k	3894	503 k	4633	327 k
LCFCHeFe_ce:28:5f	8571	844 k	4678	341 k	3893	503 k
Apple_13:c5:58	33	3180	18	1650	15	1530
RealtekU_12:35:03	30	2426	0	0	30	2426
RealtekU_12:35:02	1412	519 k	808	411 k	604	108 k
Micro-St_9a:f1:f5	10478	7474 k	4294	1083 k	6184	6390 k
IPv6mcast_fb	1	107	0	0	1	107
IPv6mcast_01	1	174	0	0	1	174
PcsCompu_cc:3f:1b	1444	522 k	636	111 k	808	411 k
02:c8:85:b5:5a:aa	58542	110 M	28971	2417 k	29571	107 M
02:46:92:ec:ed:bd	32	9973	16	7845	16	2128
02:45:a3:b1:8c:f1	58575	110 M	29590	107 M	28985	2425 k
MS-NLB-PhysServer-26...	33	3180	15	1530	18	1650

Name resolution Limit to display filter Endpoint Types ▾

[? Help](#) [Copy](#) [Map](#) [Close](#)

What is the number of IP addresses linked with “Kansas City”?

Ans: 4

Still on Endpoints, go to IPv4 tab then “City” column

Wireshark · Endpoints · Exercise.pcapng

Ethernet · 26	IPv4 · 436	IPv6 · 6	TCP · 2164	UDP · 224				
Address	▲ Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City
13.92.211.253	3	174	2	120	1	54	United States	Tappahannock
23.92.25.116	20	6593	10	5900	10	693	United States	Fremont
24.54.5.14	2	265	1	62	1	203	Canada	Mont-Tremblant
24.78.140.118	4	355	2	196	2	159	Canada	Winnipeg
24.192.137.36	2	679	1	605	1	74	United States	Warren
24.193.140.50	2	143	1	61	1	82	United States	Queens
34.117.237.239	28	4152	12	1861	16	2291	United States	Kansas City
34.120.208.123	23	3673	11	1045	12	2628	United States	Kansas City
34.120.237.76	7	618	3	276	4	342	United States	Kansas City
35.244.181.201	6	473	2	132	4	341	United States	Kansas City
37.59.43.136	108	7914	48	3768	60	4146	France	—

Which IP address is linked with “Blicnet” AS Organisation?

Ans: 188.246.82.7

Still on Endpoint, go to “As Organization” Column

Wireshark · Endpoints · Exercise.pcapng							
Ethernet · 26	IPv4 · 436	IPv6 · 6	TCP · 2164	UDP · 224			
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	AS Organization
97.103.179.155	2	259	1	62	1	197	BHN-33363
194.165.188.76	18	1456	7	490	11	966	BT Communications Ireland Limited
194.165.188.79	22	2256	10	937	12	1319	BT Communications Ireland Limited
188.246.82.7	2	137	1	61	1	76	Blicnet d.o.o.
212.8.163.80	20	1686	3	197	17	1489	British Telecommunications PLC

Task 3: Statistics | Protocol Details

What is the most used IPv4 destination address?

Ans: 10.100.1.33

Go to Statistics then IPv4 Statistics then All Addresses. Sort it by Count.

The screenshot shows the Wireshark interface with the Statistics menu open. The 'All Addresses' option under the IPv4 Statistics submenu is highlighted. The main pane displays a list of network conversations, and the details pane shows the raw hex and ASCII data for a selected packet.

Statistics Submenu:

- Capture File Properties
- Resolved Addresses
- Protocol Hierarchy
- Conversations
- Endpoints
- Packet Lengths
- I/O Graph
- Service Response Time
- DHCP (BOOTP) Statistics
- ONC-RPC Programs
- 29West
- ANCP
- BACnet
- Collectd
- DNS
- Flow Graph
- HART-IP
- HPFEEDS
- HTTP
- HTTP2
- Sametime
- TCP Stream Graphs
- UDP Multicast Streams
- F5
- IPv4 Statistics** (highlighted)
- All Addresses** (highlighted)
- Destinations and Ports
- IP Protocol Types
- Source and Destination Addresses

Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Destinations and Ports	81420				0.0000	100%	14.9200	442267516.890
10.100.1.33	29387				0.0000	36.09%	1.1100	568415475.093
TCP	29387				0.0000	100.00%	1.1100	568415475.093
10.10.57.178	28984				0.0000	35.60%	1.2100	568415512.371

What is the max service request-response time of the DNS packets?

Ans: 0.467897

Go to Statistics then DNS.

The screenshot shows the Wireshark interface with the 'Statistics' menu open. The 'DNS' option is highlighted. Other menu items include 'Capture File Properties', 'Resolved Addresses', 'Protocol Hierarchy', 'Conversations', 'Endpoints', 'Packet Lengths', 'I/O Graph', 'Service Response Time', 'DHCP (BOOTP) Statistics', 'ONC-RPC Programs', '29West', 'ANCP', 'BACnet', 'Collectd', and 'Flow Graph'. A context menu for a selected frame is also visible.

No.	Time	Source
1	0.000000	145.254.160
2	0.911310	65.208.228
3	0.911310	145.254.160
4	0.911310	145.254.160
5	1.472116	65.208.228
6	1.682419	65.208.228
7	1.812606	145.254.160
8	1.812606	65.208.228
9	2.012894	145.254.160
10	2.443513	65.208.228
11	2.553672	65.208.228
12	2.553672	145.254.160
13	2.553672	145.254.160
14	2.633787	65.208.228
15	2.814046	145.254.160

Frame 1: 62 bytes on wire (496 bits), 46 bytes captured (368 bits) on interface wireless at 192.168.1.10 (Intel PRO/100 MT Desktop) at 19:45:00.000000000000
Ethernet II, Src: Xerox_00:00:00 (08:00:22:00:00:00), Dst: 29West (08:00:22:00:00:00)

Wireshark · DNS · Exercise.pcapng								
Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burs
Class	171				0.0000	100.00%	0.1600	5684
IN	171				0.0000	100.00%	0.1600	5684
Service Stats	0				0.0000	100%	-	-
request-response time (secs)	85	0.07	0.000075	0.467897	0.0000		0.0800	5684
no. of unsolicited responses	0				0.0000		-	-
no. of retransmissions	0				0.0000		-	-

What is the number of HTTP Requests accomplished by “rad[.]msn[.]com?

Ans: 39

Go to Statistics then HTTP then Requests.

The screenshot shows the Wireshark interface with the 'Statistics' tab selected in the top menu bar. A context menu is open over a list of network packets, with the 'HTTP' submenu expanded. The 'Requests' option under the 'HTTP' submenu is highlighted with a blue selection bar. To the right of the menu, the packet list shows several entries, with the first few being:

- Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface wireless (mon0)
- Ethernet II, Src: Xerox_00:00:00 (00:0c:29:00:00:00), Dst: Microsoft_WPS_PtP (00:0c:29:00:00:01)
- Internet Protocol Version 4, Src: 145.254.160.1, Dst: 65.208.228.1
- Transmission Control Protocol, Src Port: 533 (TCP 533), Dst Port: 3372 (TCP 3372)

Look for the domain name and scroll all the way to the right.

Topic / Item	
▶	stork131.dropbox.com
▶	static.ak.fcdn.net
▶	spe.atdmt.com
▶	social.msn.com
▶	safebrowsing-cache.google.com
▶	s0.2mdn.net
▶	resource.ca.msn.com
▶	rad.msn.com
▶	profile.ak.fcdn.net

Wireshark · Requests · Exercise.pcapng						
	Count	Average	Min val	Max val	Rate (ms)	Percent
	2				0.0000	0.33%
	1				0.0000	0.16%
	6				0.0000	0.99%
	5				0.0000	0.82%
	3				0.0000	0.49%
	1				0.0000	0.16%
	5				0.0000	0.82%
	39				0.0000	6.40%
	6				0.0000	0.99%
	6				0.0000	0.99%

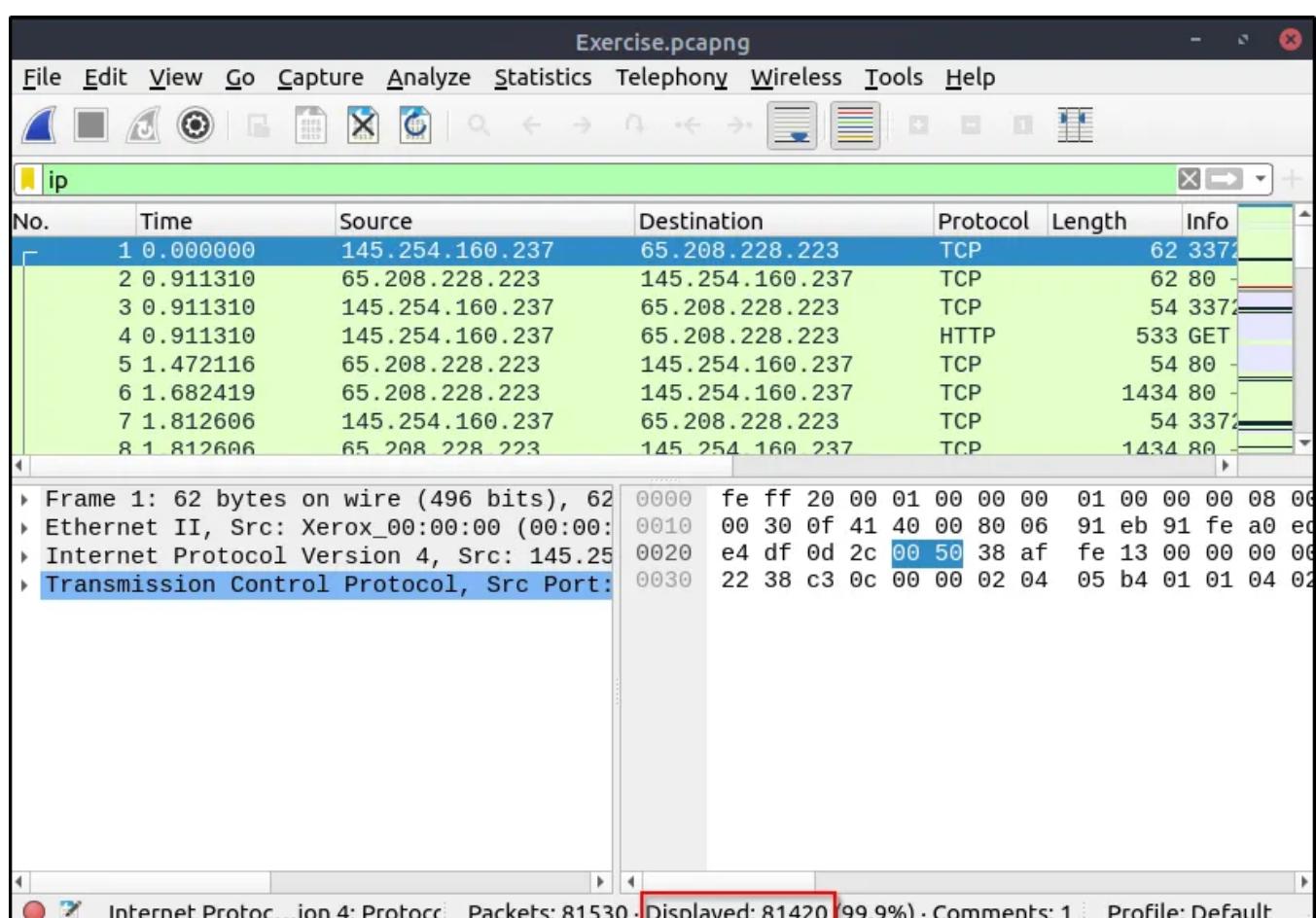
Task 5: Packet Filtering | Protocol Filters

What is the number of IP packets?

Ans: 84120

Filter out only packets with ip

```
ip
```



What is the number of packets with a “TTL value less than 10”?

Ans: 66

```
ip.ttl <= 10
```

Exercise.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.ttl <= 10

No.	Time	Source	Destination	Protocol	Length	Info
423	211538132.29...	192.168.3.131	239.255.255.250	SSDP	167	M-SE
424	211538132.29...	192.168.3.131	239.255.255.250	SSDP	165	M-SE
727	211538135.29...	192.168.3.131	239.255.255.250	SSDP	167	M-SE
728	211538135.29...	192.168.3.131	239.255.255.250	SSDP	165	M-SE
815	211538138.29...	192.168.3.131	239.255.255.250	SSDP	167	M-SE
816	211538138.29...	192.168.3.131	239.255.255.250	SSDP	165	M-SE
1932	211538145.75...	192.168.3.131	224.0.0.252	LLMNR	64	Stan
1941	211538145.85	192.168.3.131	224.0.0.252	LLMNR	64	Stan

Frame 423: 167 bytes on wire (1336 bits)
Ethernet II, Src: Micro-St_9a:f1:f5 (40:
Internet Protocol Version 4, Src: 192.16
User Datagram Protocol, Src Port: 57757,
Simple Service Discovery Protocol

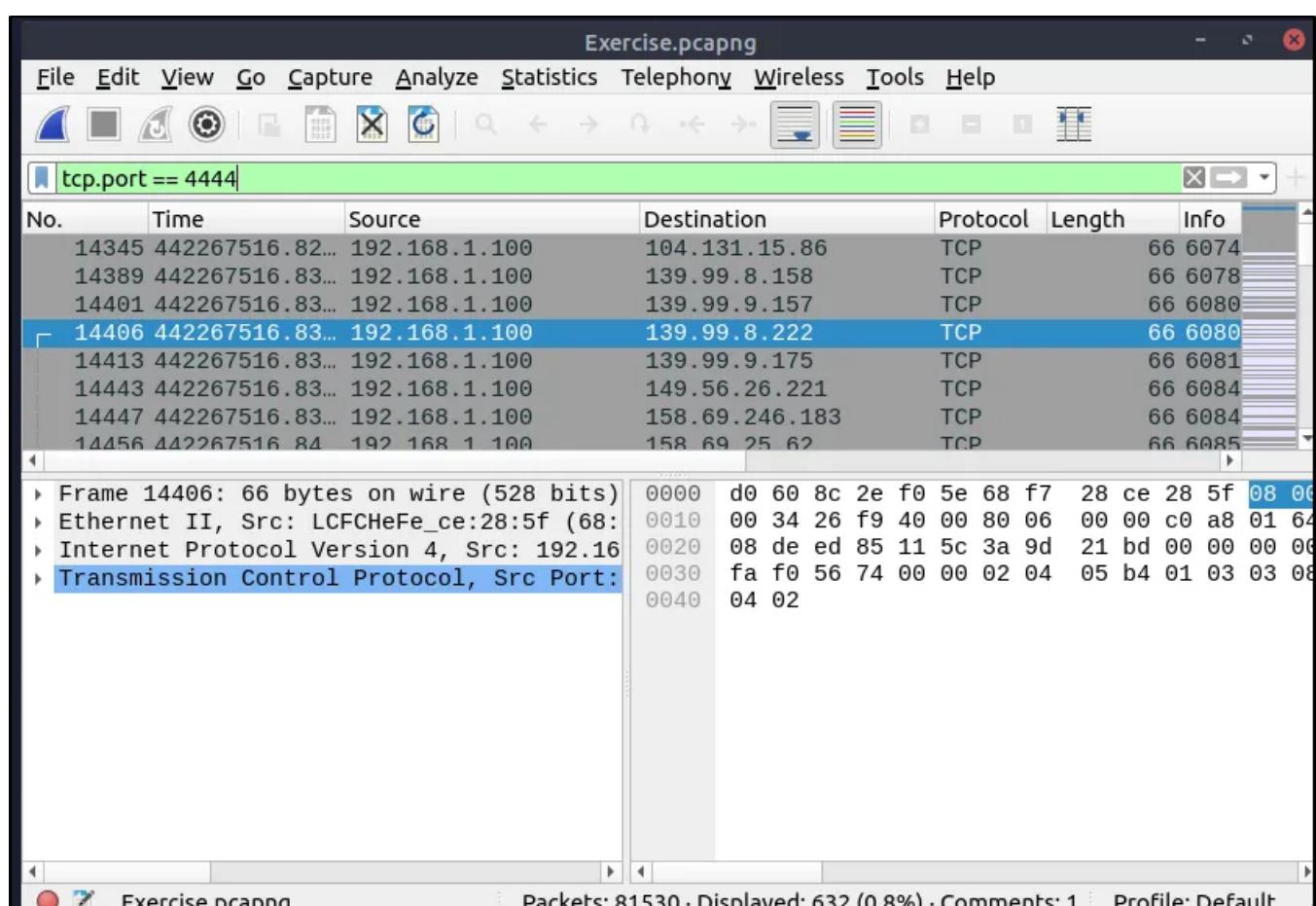
Hex	Dec
0000	01 00 5e 7f ff fa 40 61
0010	86 9a f1 f5 08 00 00 00
0020	00 99 68 f9 00 00 01 11
0030	9c 35 c0 a8 03 80 ff fa e1 9d 07 6c 00 85
0040	5e 7f 4d 2d 53 40 43 48 20 2a 20 48 54 54 50 2f 31 2e 31
0050	00 40 6f 73 74 3a 32 33 39 2e 32 35 35 2e 32 33
0060	32 35 30 3a 31 39 30 30 0d 0a 53 54 3a 70 3a 73 63 68 65 6d 61 73 2d 75 70 6e 70
0070	67 3a 64 65 76 69 63 65 3a 4d 65 64 69 6e 66 64 65 72 65 72 3a 31 0d 0a 4d 61 6e
0080	73 64 70 3a 64 69 73 63 6f 76 65 72 22 00 58 3a 33 0d 0a 0d 0a
0090	00 a0

Exercise.pcapng Packets: 81530 · Displayed: 66 (0.1%) · Comments: 1 · Profile: Default

What is the number of packets which uses “TCP port 4444”?

Ans: 632

```
tcp.port == 4444
```



What is the number of “HTTP GET” requests sent to port “80”?

Ans: 527

This filter joins two filters together. This filters out only “GET” http request method that uses tcp port 80.

```
http.request.method == "GET" && tcp.port == 80
```

The screenshot shows the Wireshark interface with the following details:

- Title Bar:** Exercise.pcapng
- Menu Bar:** File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help
- Toolbar:** Includes icons for file operations like Open, Save, Print, and various analysis tools.
- Display Filter:** http.request.method == "GET" && tcp.port == 80
- List View (No. column):** Shows packet numbers from 11539 to 11861.
- List View (Time column):** Shows timestamps for each packet.
- List View (Source column):** Shows source IP addresses (e.g., 192.168.3.131).
- List View (Destination column):** Shows destination IP addresses (e.g., 72.14.213.138).
- List View (Protocol column):** Shows the protocol (HTTP).
- List View (Length column):** Shows the length of the packets.
- List View (Info column):** Shows the content of the packets.
- Selected Item:** Hypertext Transfer Protocol
- Hex View:** Shows the raw hex and ASCII representation of the selected packet.
- Text View:** Shows the detailed structure of the selected packet.
- Status Bar:** Exercise.pcapng · Packets: 81530 · Displayed: 527 (0.6%) · Comments: 1 · Profile: Default

What is the number of “type A DNS Queries”?

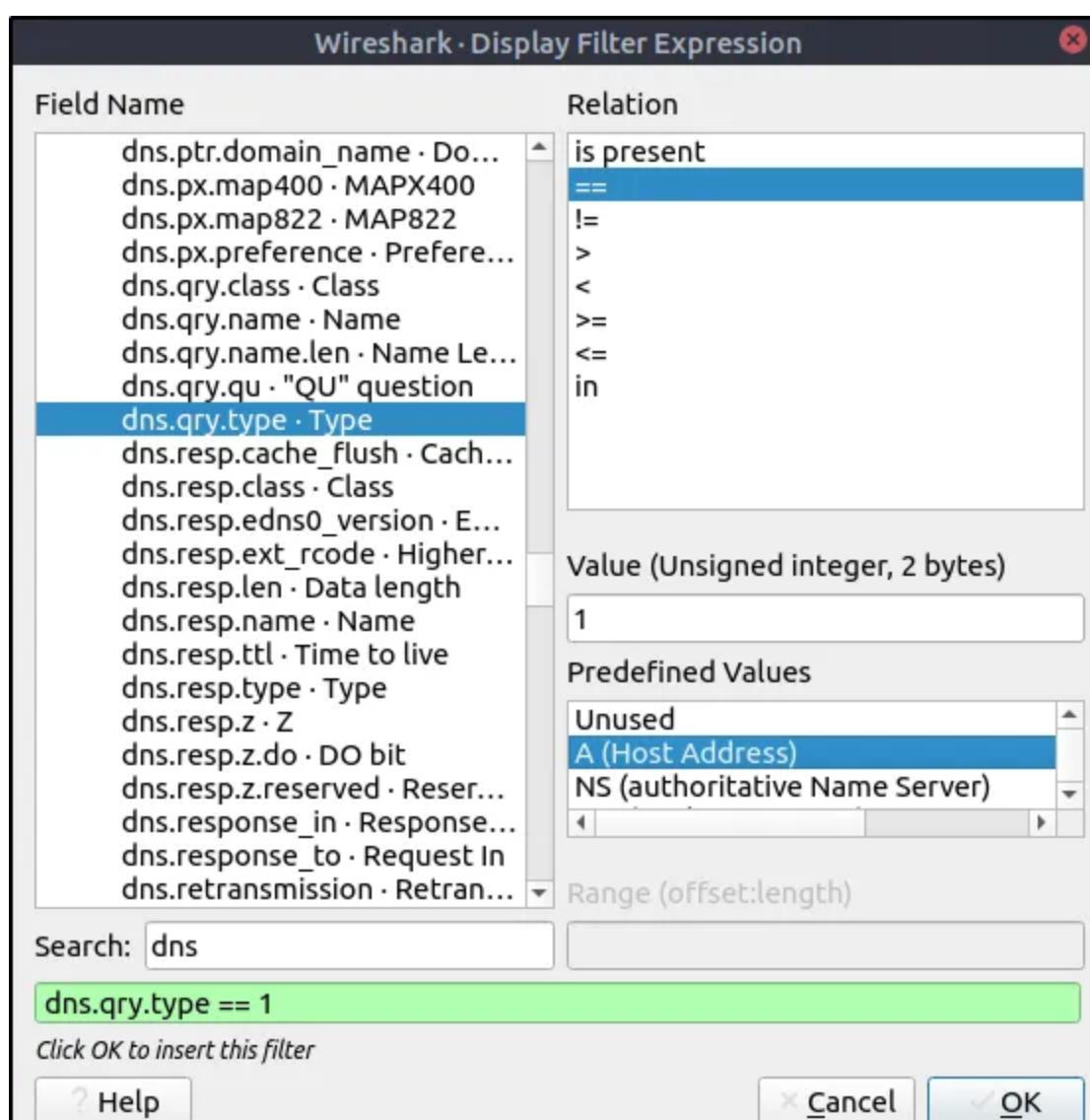
Ans: 51

Let's build a filter using the Display Filter Expression under the Analyze menu.

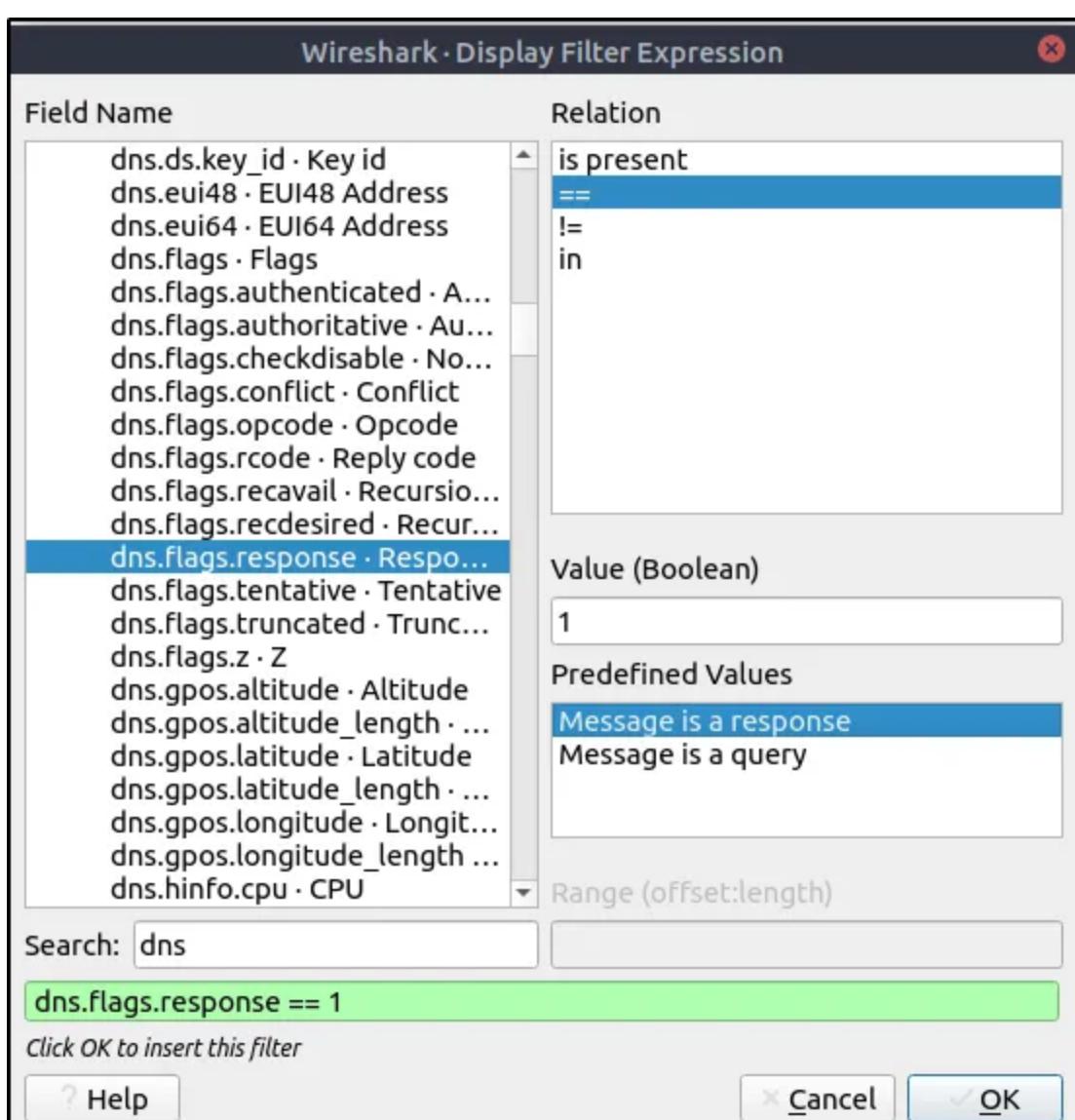
The screenshot shows the Wireshark interface with the Analyze menu open:

- Analyze Menu:** Display Filters..., Display Filter Macros..., Display Filter Expression... (selected), Apply as Column, Apply as Filter, Prepare a Filter.
- Display Filter:** http.request.method == "GET"
- List View:** Shows the first three packets of the filtered list.

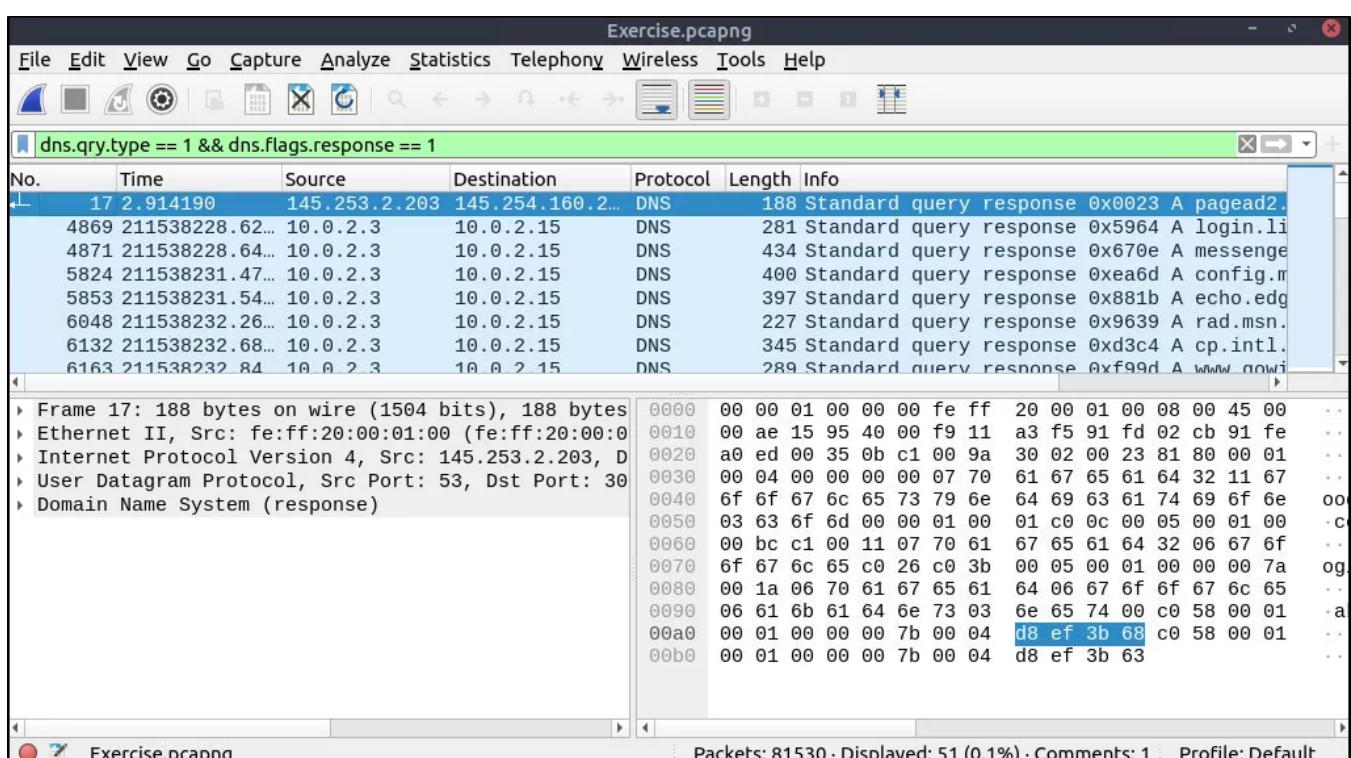
Search for dns then select dns.query.type A then click Ok.



Let's add another filter to show all DNS responses



```
dns.qry.type == 1 && dns.flags.response == 1
```



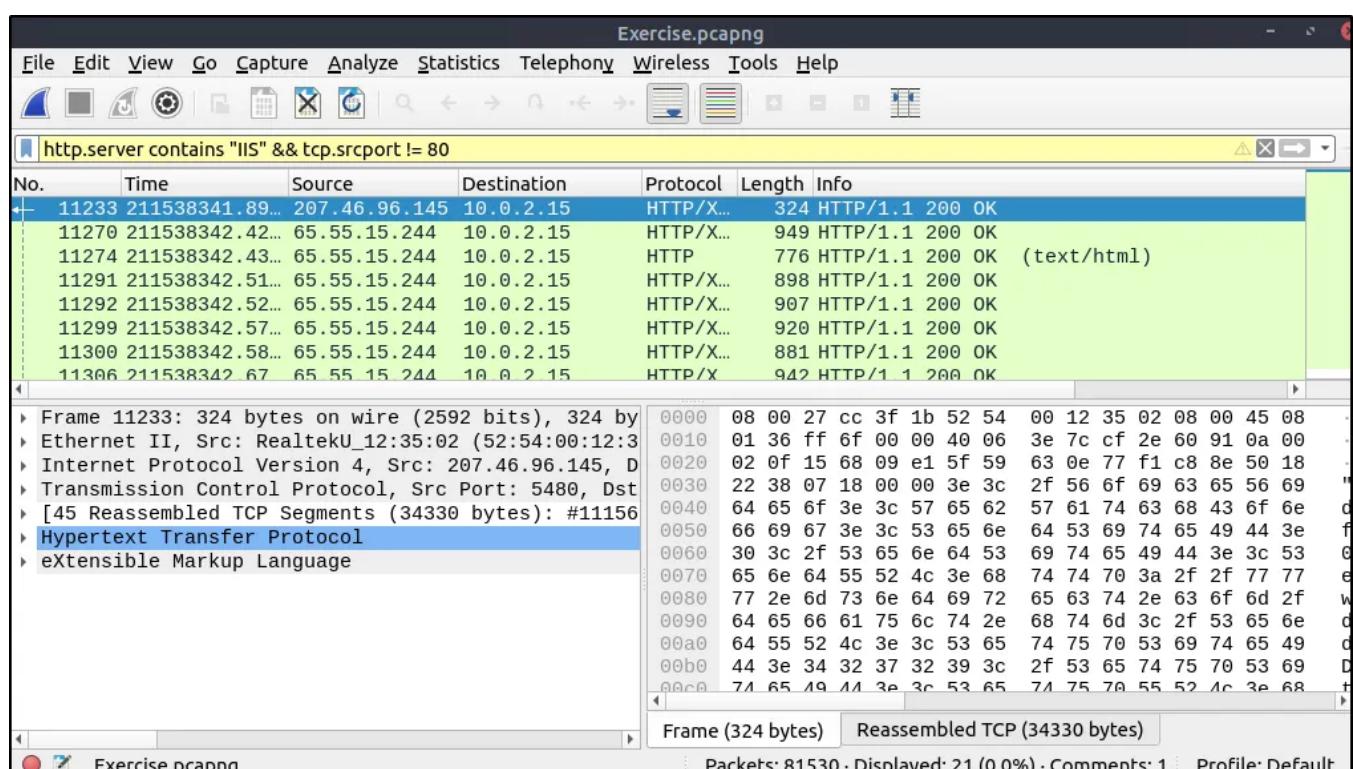
Task 6: Advanced Filtering

Find all Microsoft IIS servers. What is the number of packets that did not originate from “port 80”?

Ans: 21

This filters all http servers that contains the string “IIS” but excluding packets from source port 80.

```
http.server contains "IIS" && tcp.srcport != 80
```

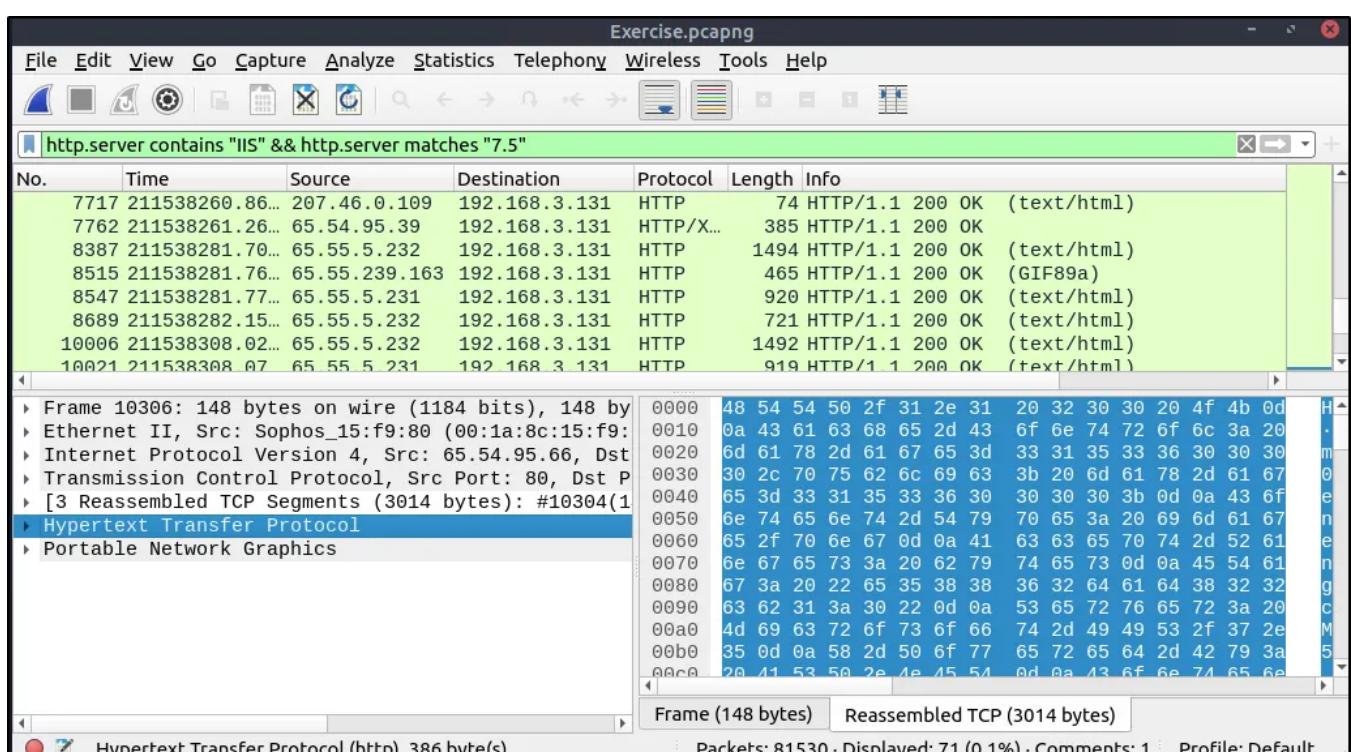


Find all Microsoft IIS servers. What is the number of packets that have “version 7.5”?

Ans: 71

The following filters all http server that contains “IIS” and matches the string “7.5”.

```
http.server contains "IIS" && http.server matches "7.5"
```

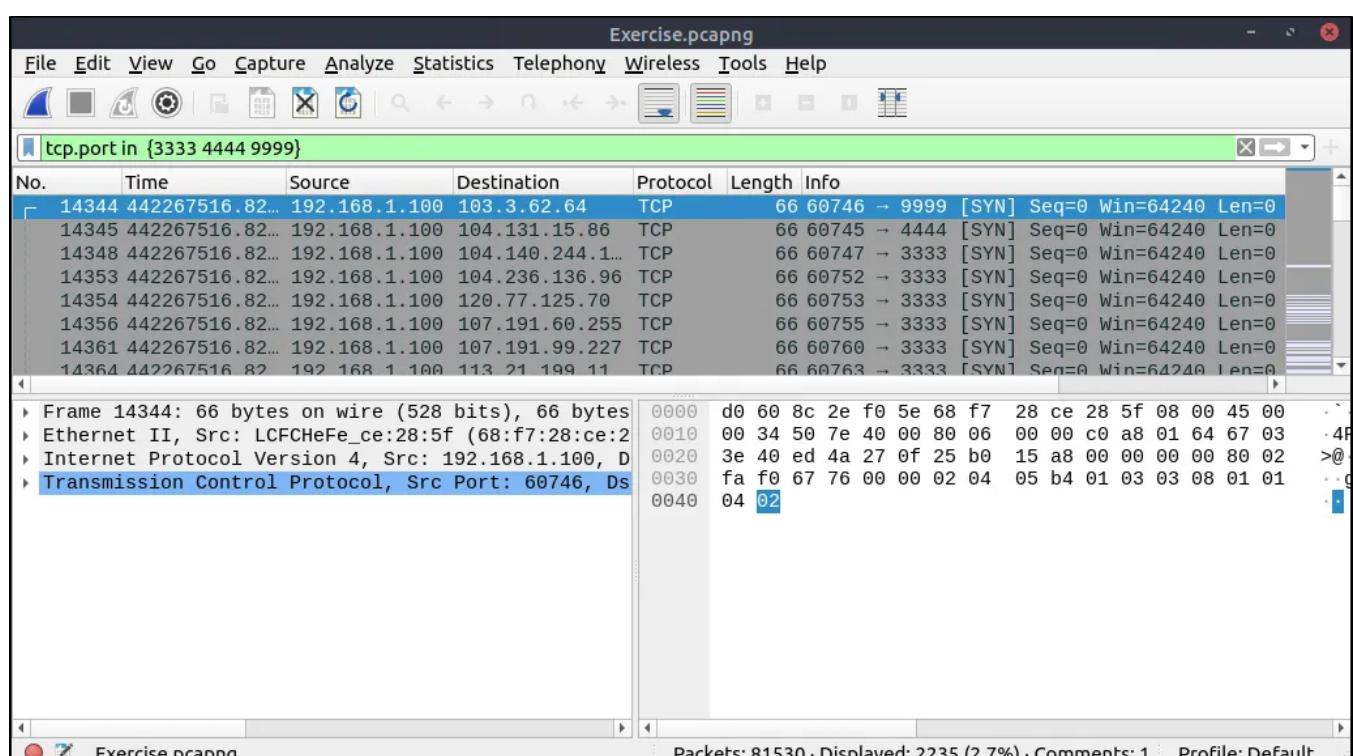


What is the total number of packets that use ports 3333, 4444 or 9999?

Ans: 2235

Use curly braces and put spaces between strings.

```
tcp.port in {3333 4444 9999}
```

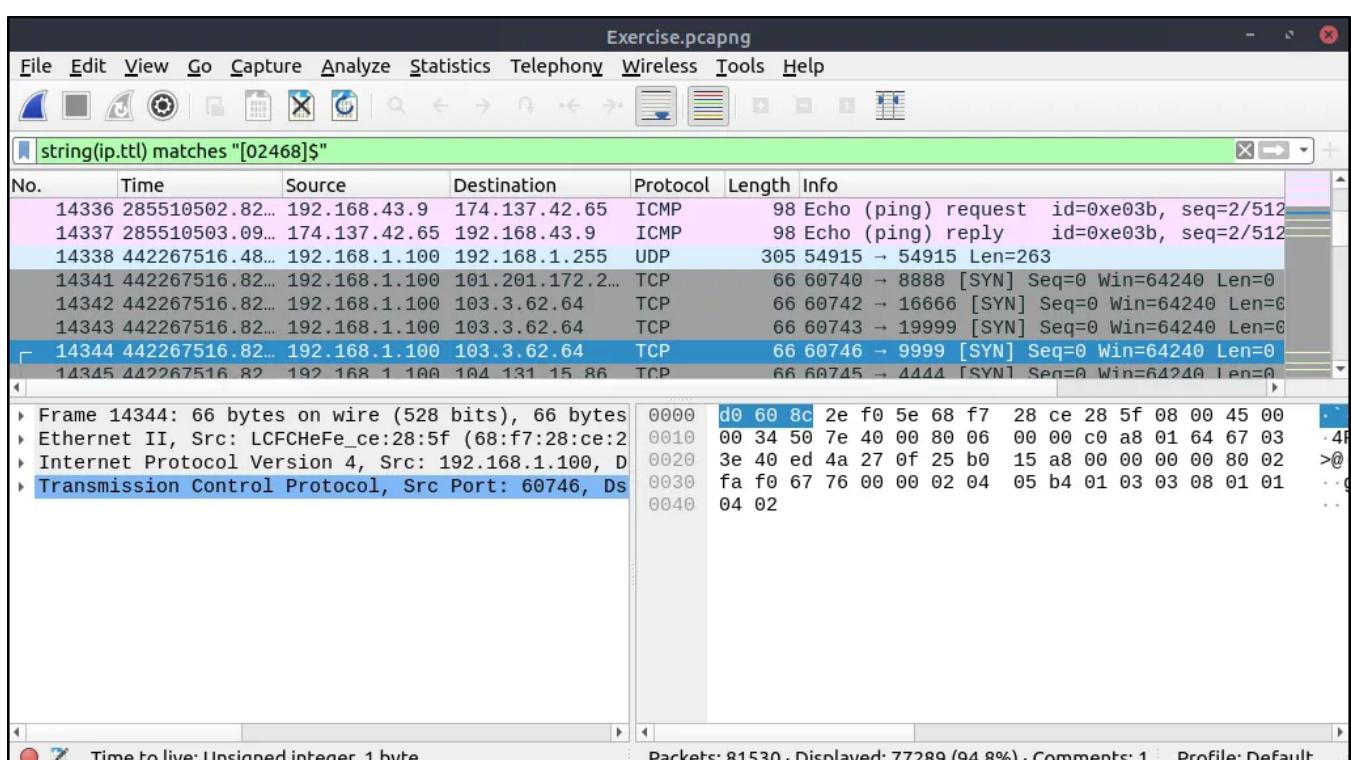


What is the number of packets with “even TTL numbers”?

Ans: 77289

What this filter does is, it will convert all ip.ttl fields to string values, and list ttl values only with even numbers.

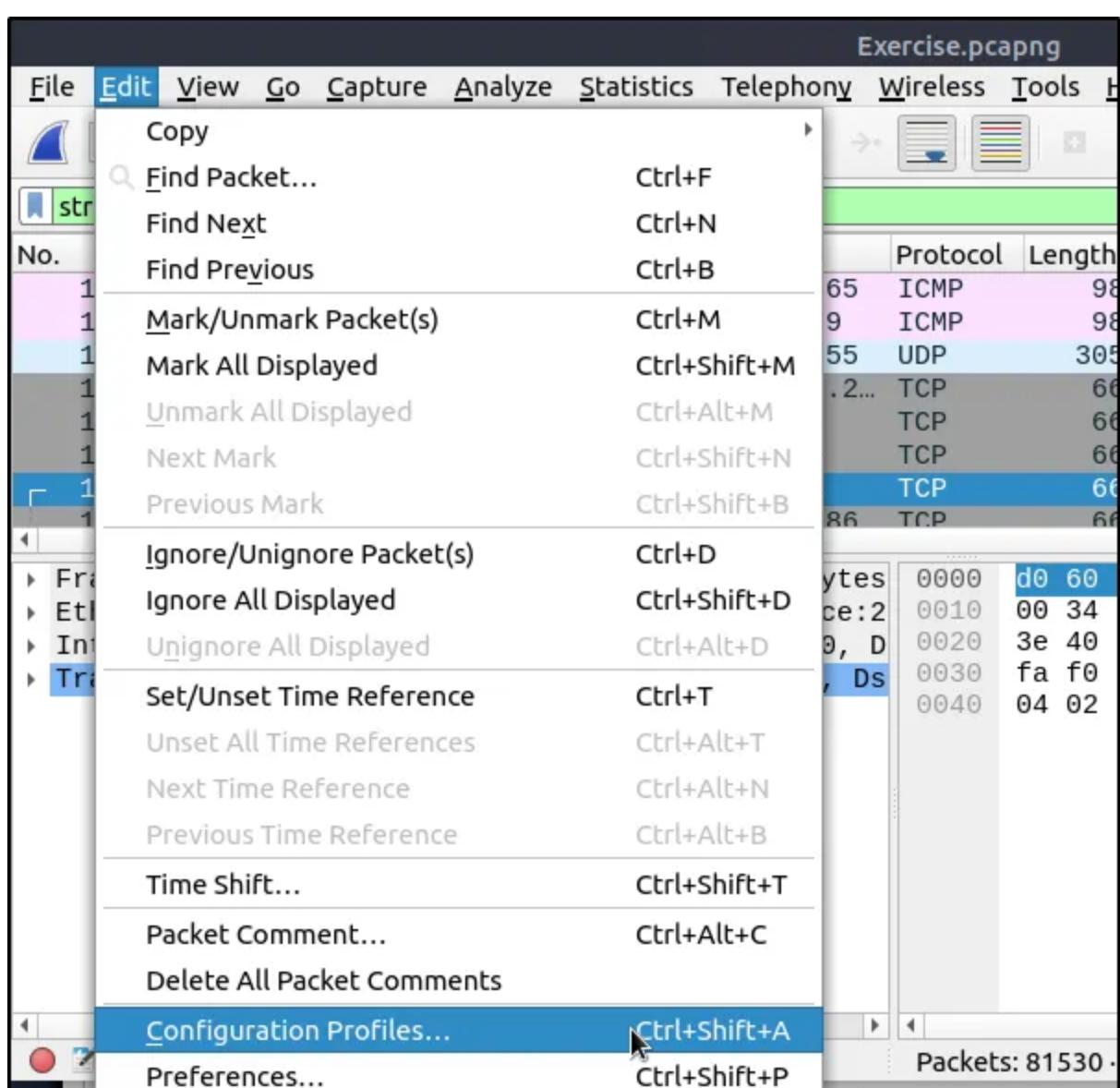
```
string(ip.ttl) matches "[02468]$"
```

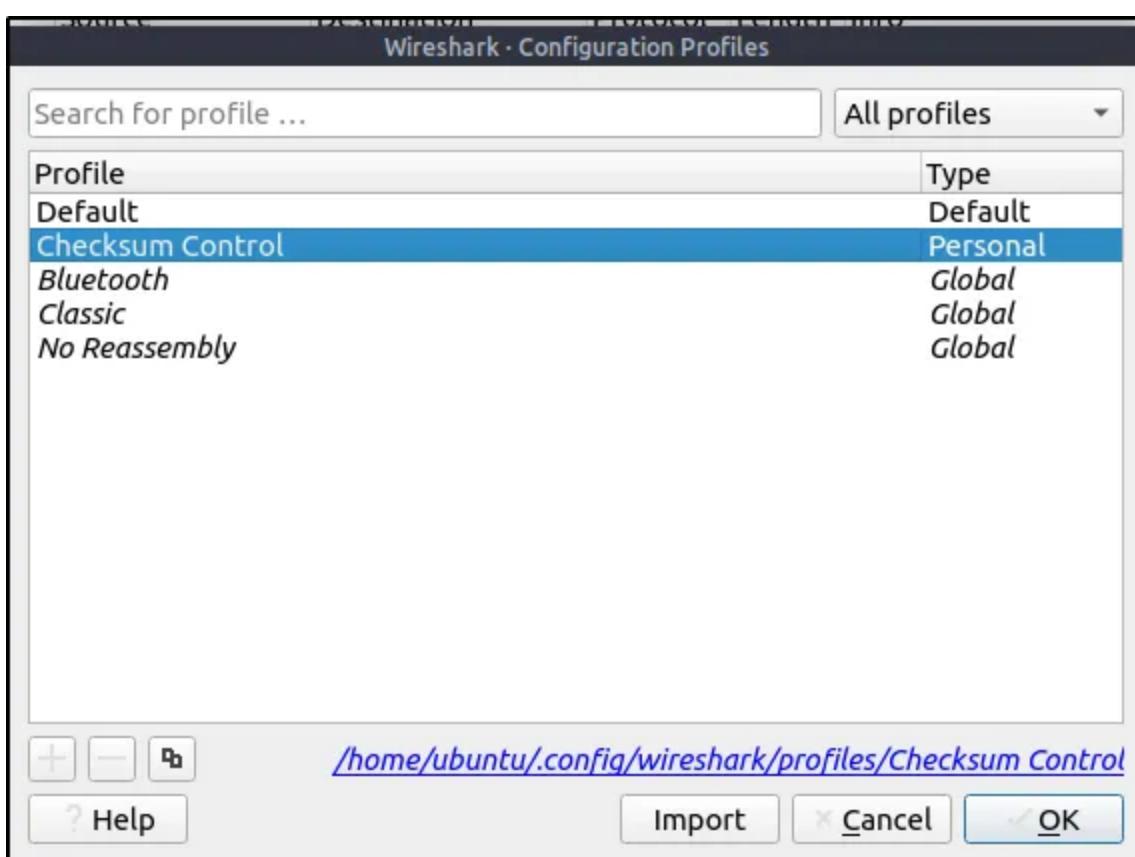


Change the profile to “Checksum Control”. What is the number of “Bad TCP Checksum” packets?

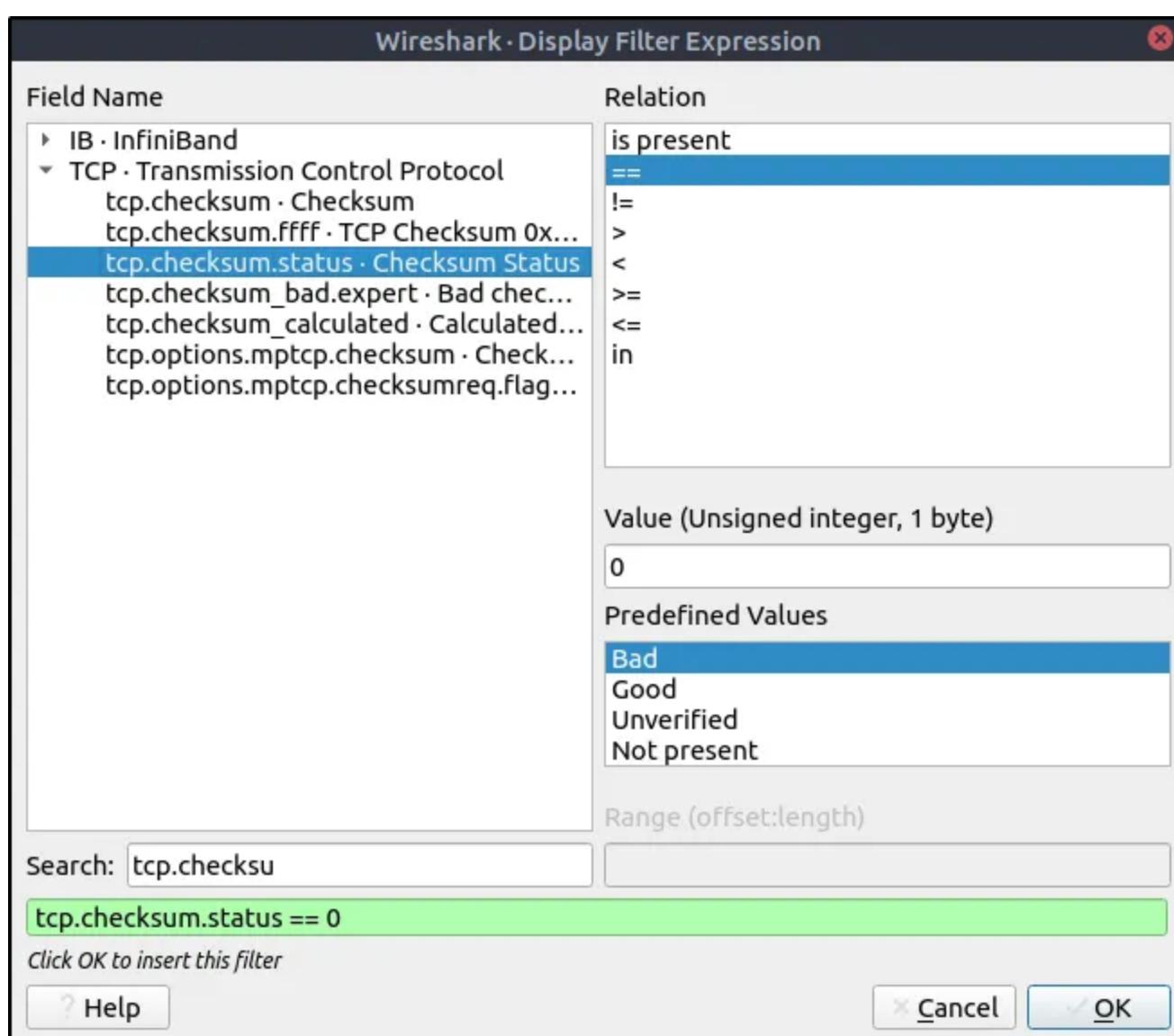
Ans: 34185

Go to **Edit** then **Configuration Profiles**. Select the “Checksum Control” profile listed.

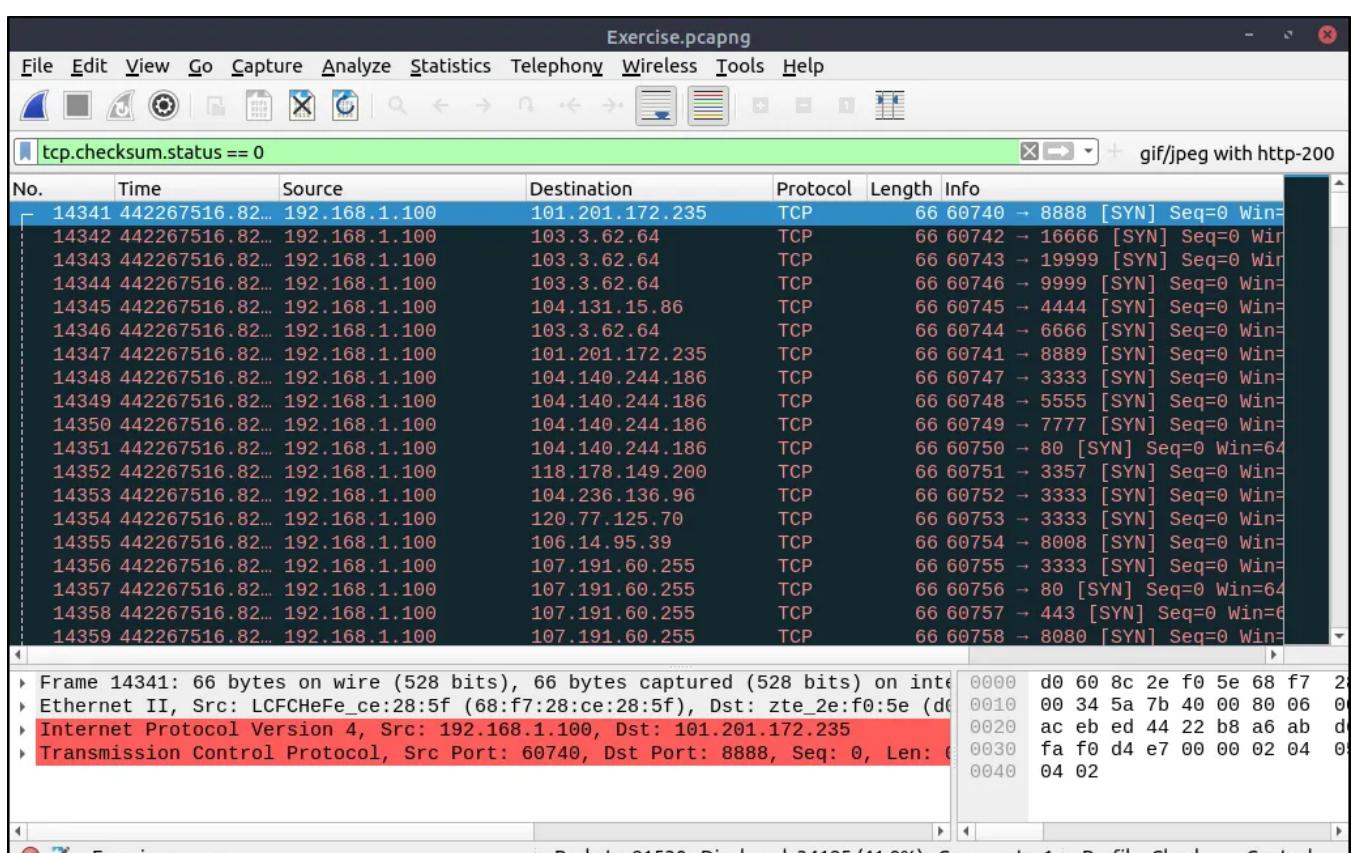




We will then open the Display Filter Expression window and create a filter for a bad tcp checksum.



```
tcp.checksum.status == 0
```



Use the existing filtering button to filter the traffic. What is the number of displayed packets?

Ans: 261

Click the button for the “Checksum Control” profile and it will populate the filter with the built-in filter.

Thanks for reading!

Happy learning :-)

[Wireshark](#)

[Tryhackme](#)

[Cybersecurity](#)

[Writeup](#)

[Learning](#)



[Follow](#)

Written by **igor_sec**

468 followers · 11 following

Responses (2)



Itsjustme



Galih Rakhmadi

Jul 24

Hi Mr. Igor, I really thank for the write up. Learned a lot about how to tackle the task correctly. I really am considering doing the write up like you. Once again really thank you for the best write up.

1



Ayouchka

Oct 6

great tks

More from **igor_sec**



 igor_sec

TryHackMe | Wireshark: The Basics

Learn the basics of Wireshark and how to analyse protocols and PCAPs.

Jun 23, 2023 145 6



 igor_sec

TryHackMe | Zeek

Introduction to hands-on network monitoring and threat detection with Zeek (formerly Bro).

· · · · · 125 3



 igor_sec

TryHackMe | Boogeyman 1

The room provided a phishing email, endpoint logs, and network traffic to analyze. By studying email headers, parsing JSON logs with JQ...

Nov 20, 2023 24 1



 igor_sec

TryHackMe | Wireshark: Traffic Analysis

Learn the basics of traffic analysis with Wireshark and how to find anomalies on your network!

Jun 29, 2023 115

See all from igor_sec

Recommended from Medium

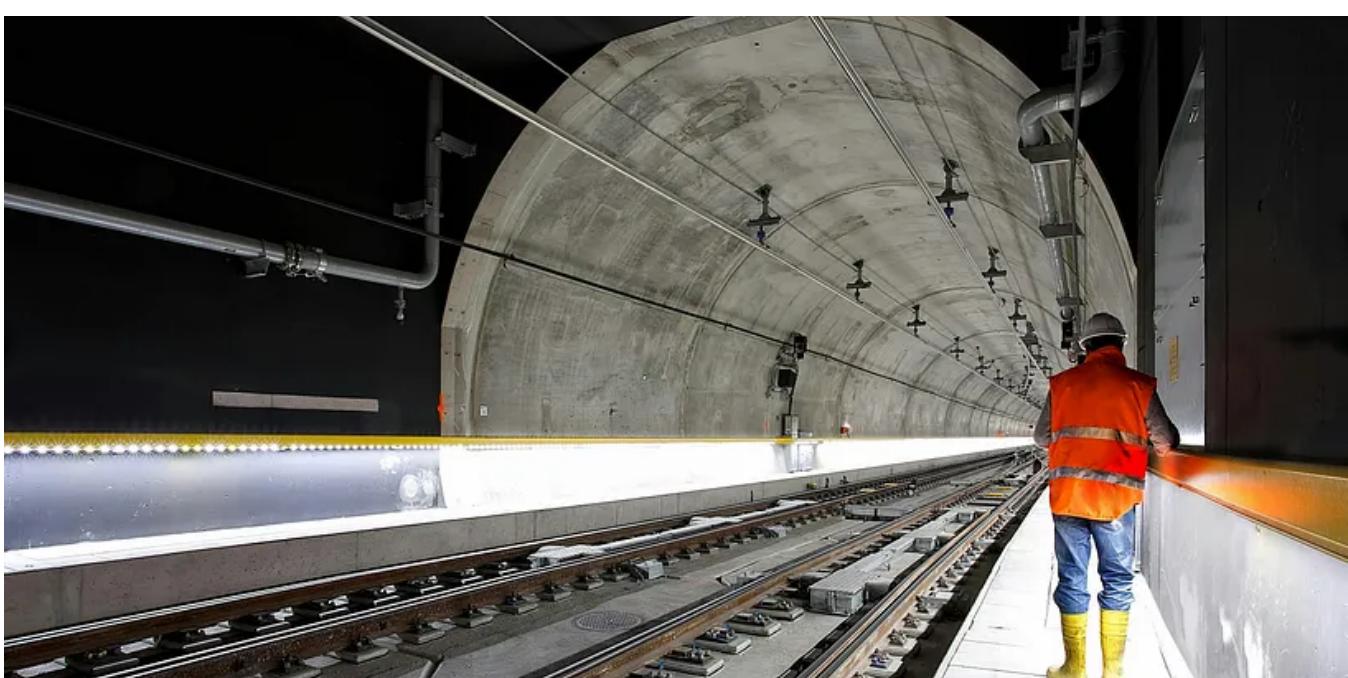


In T3CH by Axoloth

TryHackMe | Data Exfiltration Detection | WriteUp

Learn how to detect data exfiltration attempts in various network channels

Oct 3 50



 Tony Khalil Rodgers

Anti-Reverse Engineering

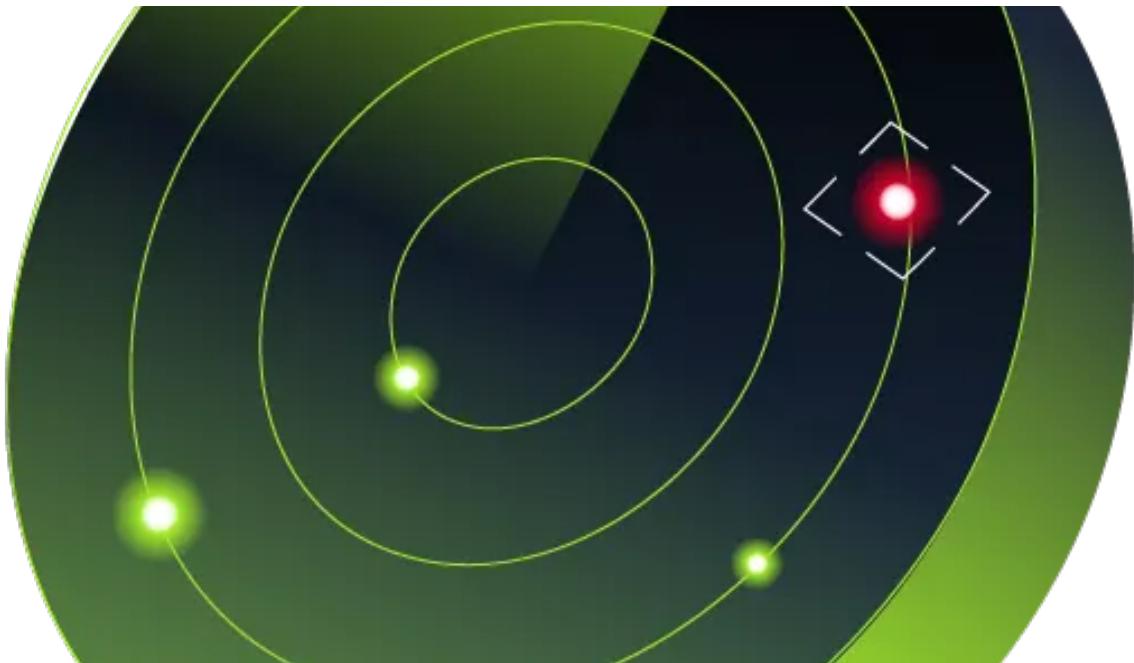
Anti-Reverse Engineering

 Sle3pyHead 🧑

Network Discovery Detection Walkthrough Notes | TryHackMe

Detect network scans and vulnerabilities using Zeek and Elastic.

Oct 2 5 1

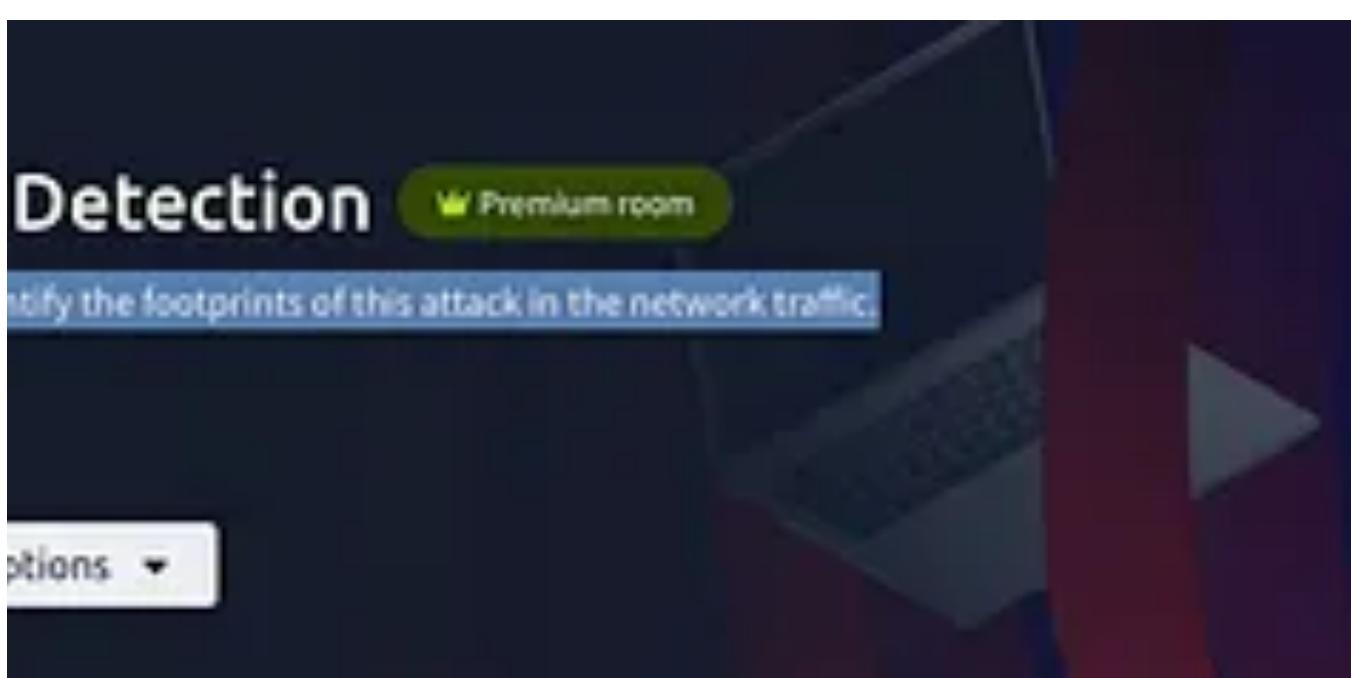


In System Weakness by Visir

Network Discovery Detection on TryHackMe: Identify Scanning Techniques

Internal scanning vs external scanning, what's a horizontal and vertical scanning technique

Oct 3 196 1



 In InfoSec Write-ups by THM{0x416469747961204D6163686972616A75}

Man-in-the-Middle Detection

Learn what MITM attack is, and how to identify the footprints of this attack in the network traffic.

Oct 9 18

 Robert Onyango

TryHackMe Write-up: Wireshark—The Basics

This is the second room of the Wireshark phase of my using TryHackMe rooms to train my SOC brain by understanding through practice how to...

Jun 13

See more recommendations