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."

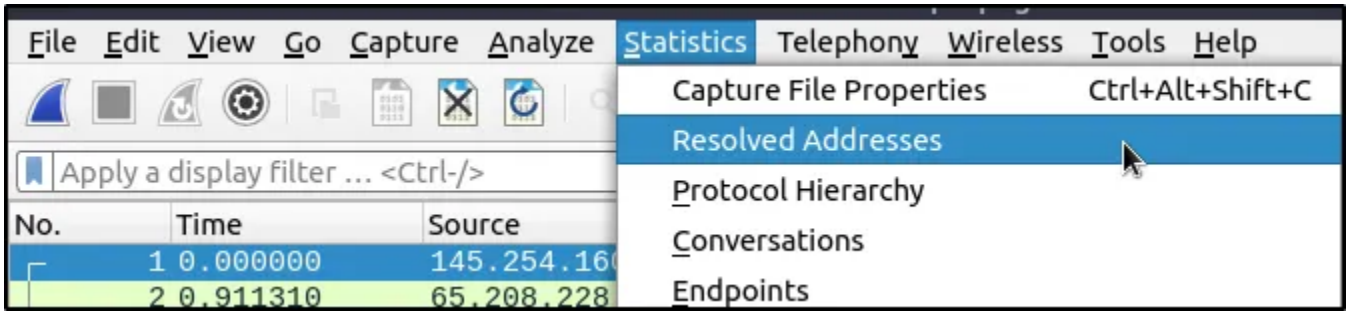
My write-up for the **Wireshark: The Basics** is found here https://medium.com/@huglertomgaw/thm-wireshark-the-basics-9d5fa3c9a60e

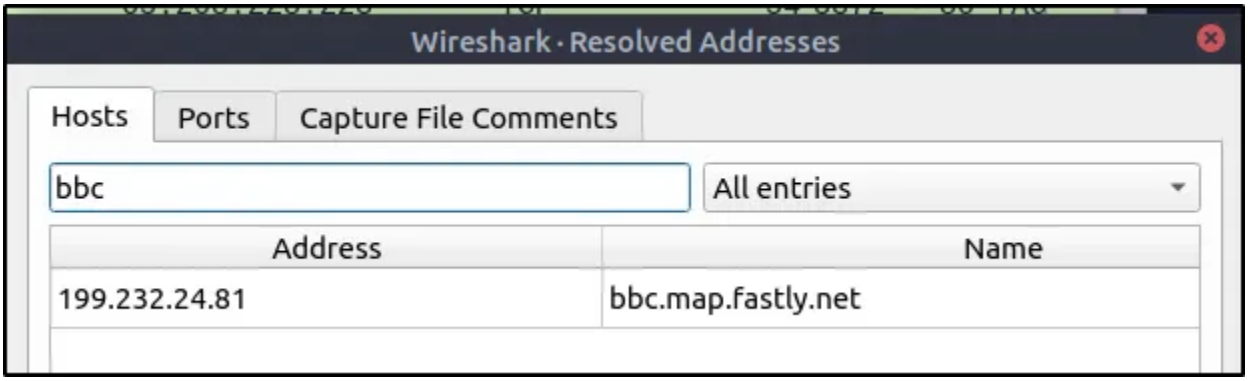
Task 2: Statistics | Summary

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.

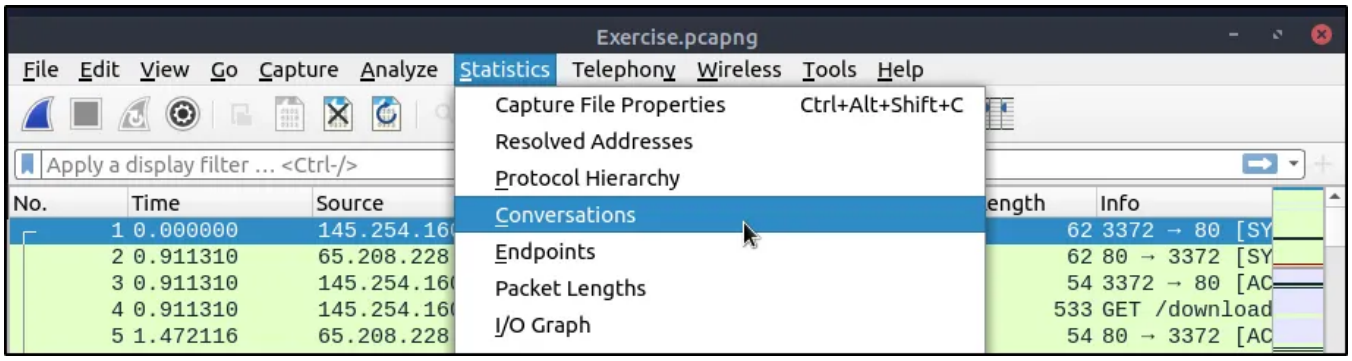


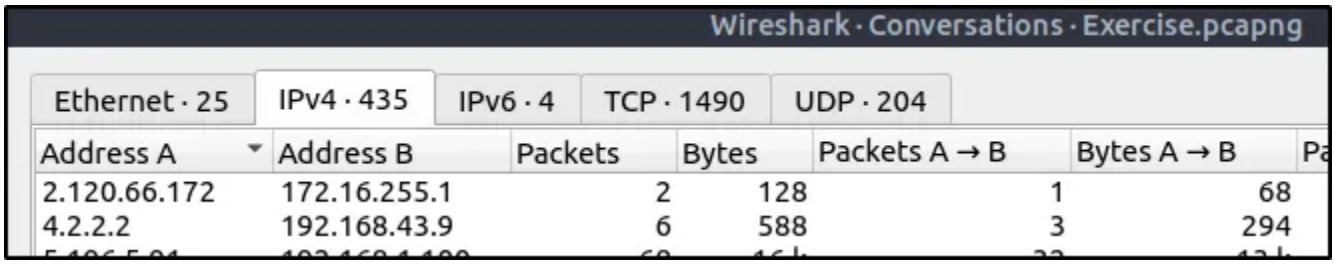


What is the number of IPv4 conversations?

Ans: 435

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

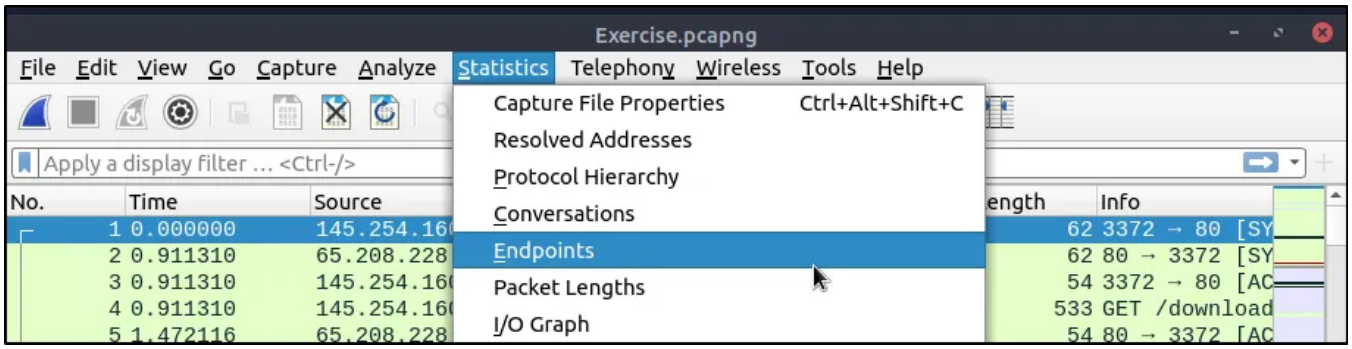




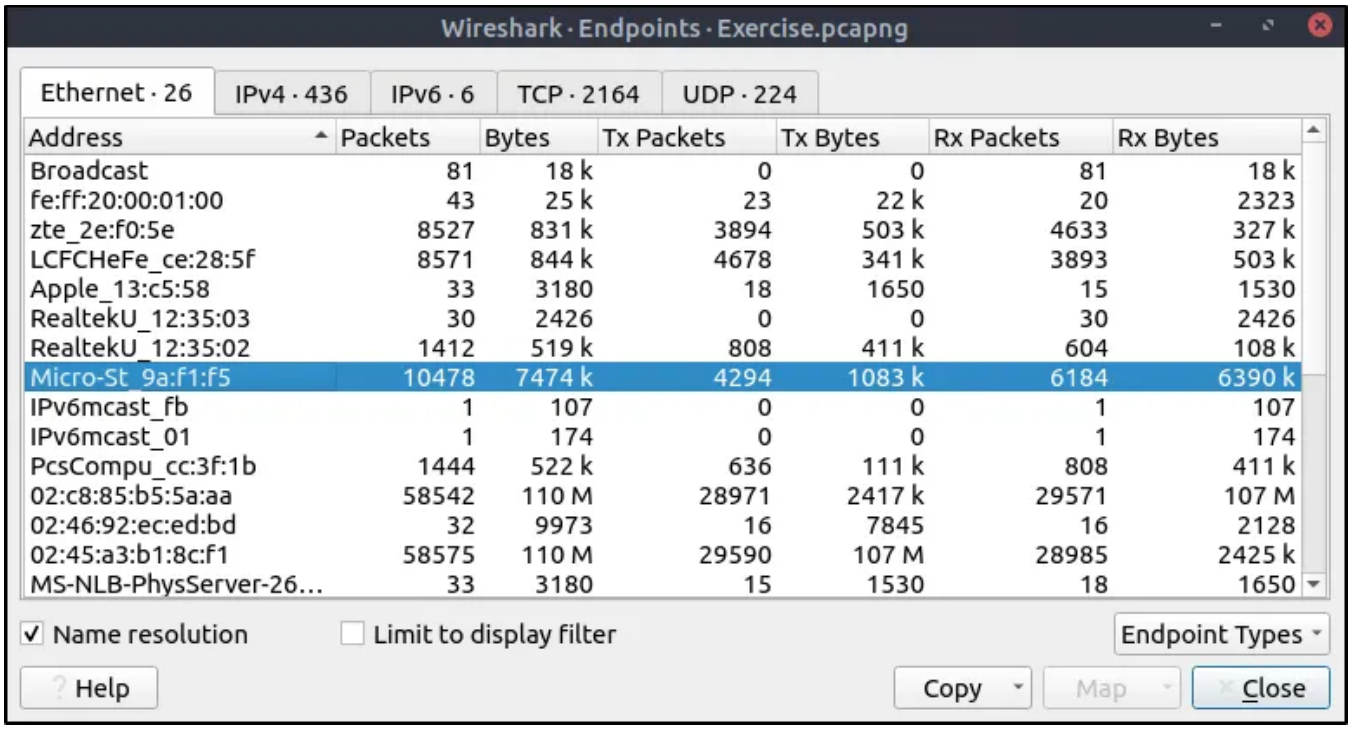
How many bytes (k) were transferred from the "Micro-St" MAC address?

Ans: 7474

Go to **Statistics** then **Endpoint.**



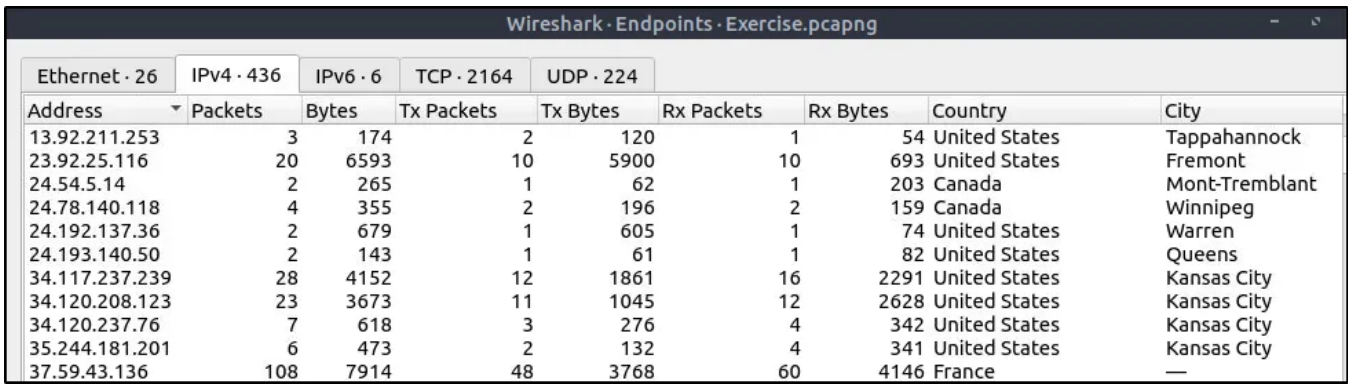
Click the Name resolution to resolve host names of the endpoints.



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

Ans: 4

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



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

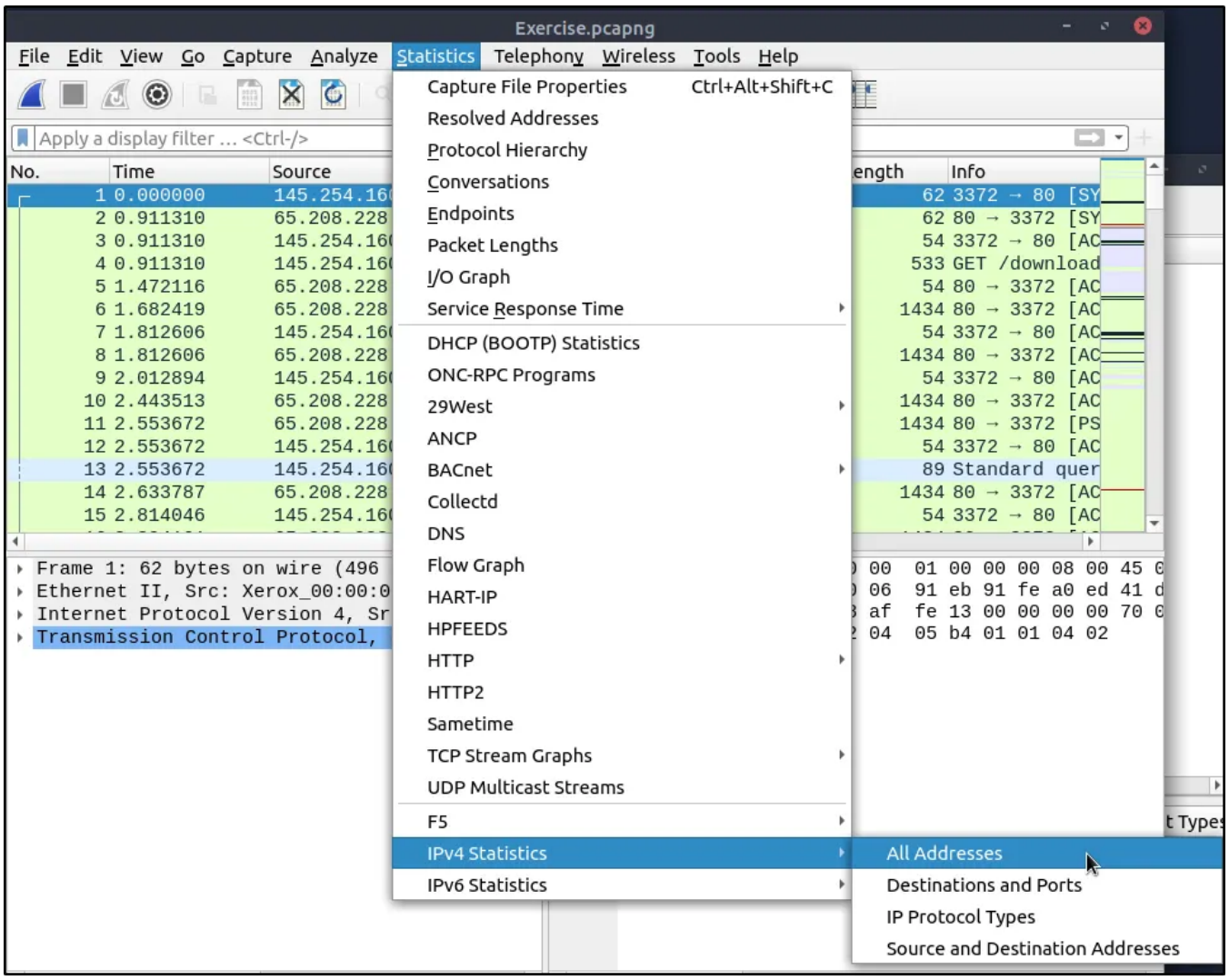
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	AS Organization
97.103.179.155	2	259	1	62	1	197	BHN-33363
194.165.188.76	18	1456	7	490	11	966	BT Communications Ireland Limited
194.165.188.79	22	2256	10	937	12	1319	BT Communications Ireland Limited
188.246.82.7	2	137	1	61	1	76	Blicnet d.o.o.
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.

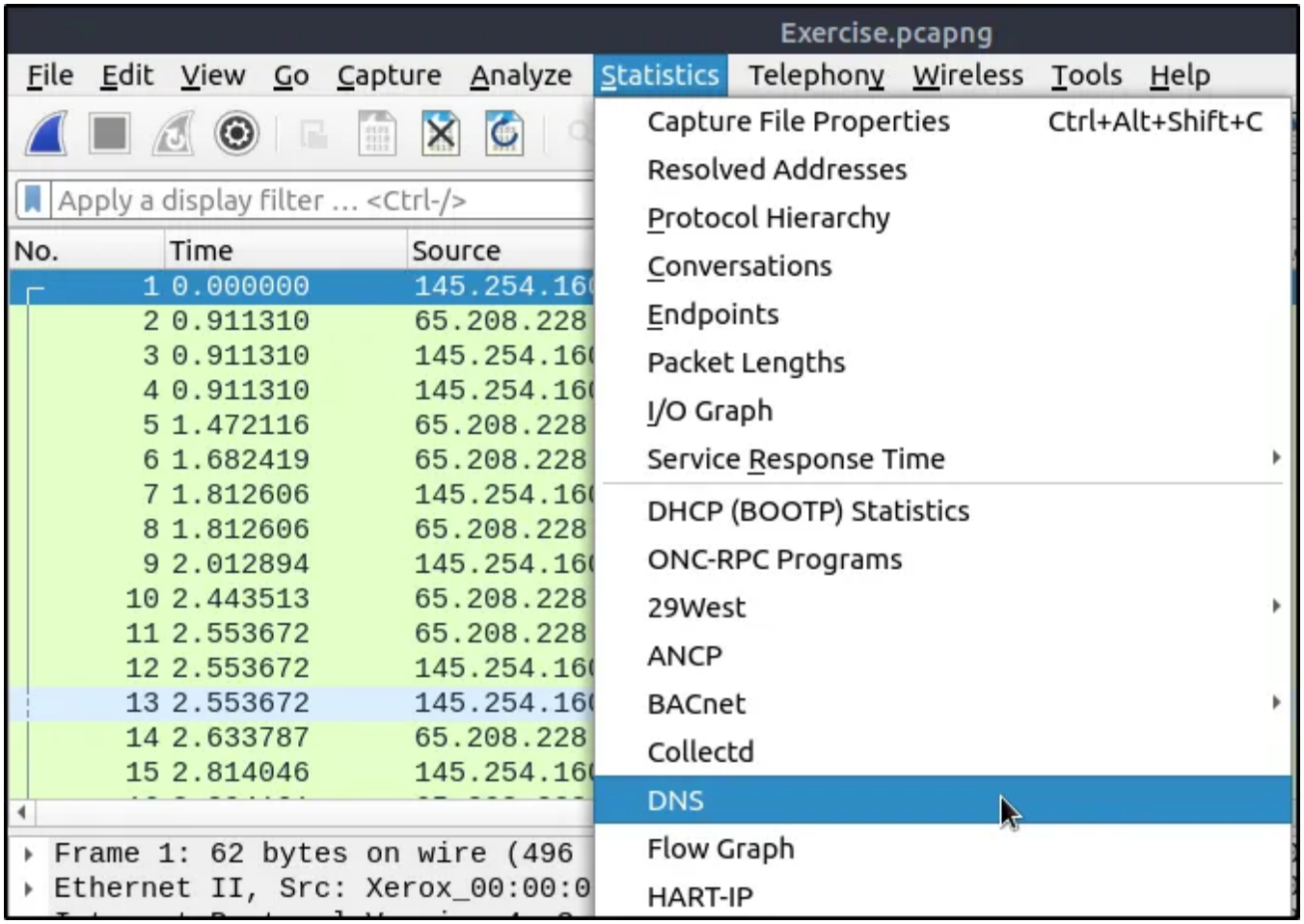


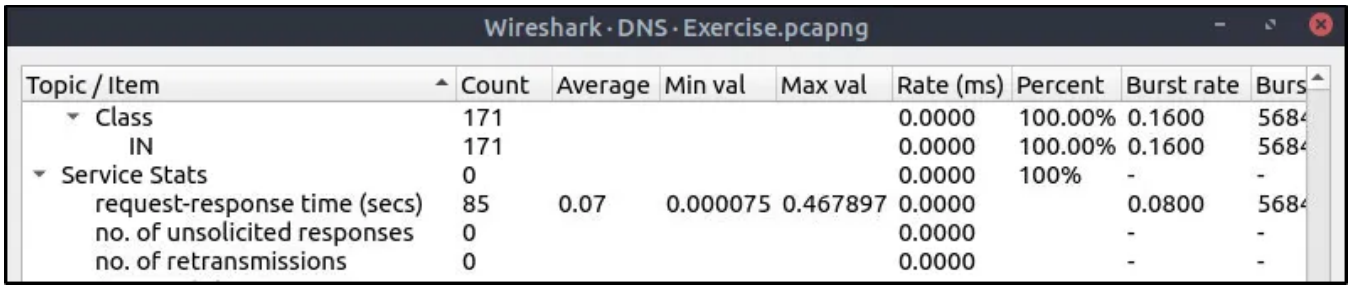
Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
Destinations and Ports	81420				0.0000	100%	14.9200	442267516.890
10.100.1.33	29387				0.0000	36.09%	1.1100	568415475.093
TCP	29387				0.0000	100.00%	1.1100	568415475.093
10.10.57.178	28984				0.0000	35.60%	1.2100	568415512.371

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

Ans: 0.467897

Go to **Statistics** then **DNS.**

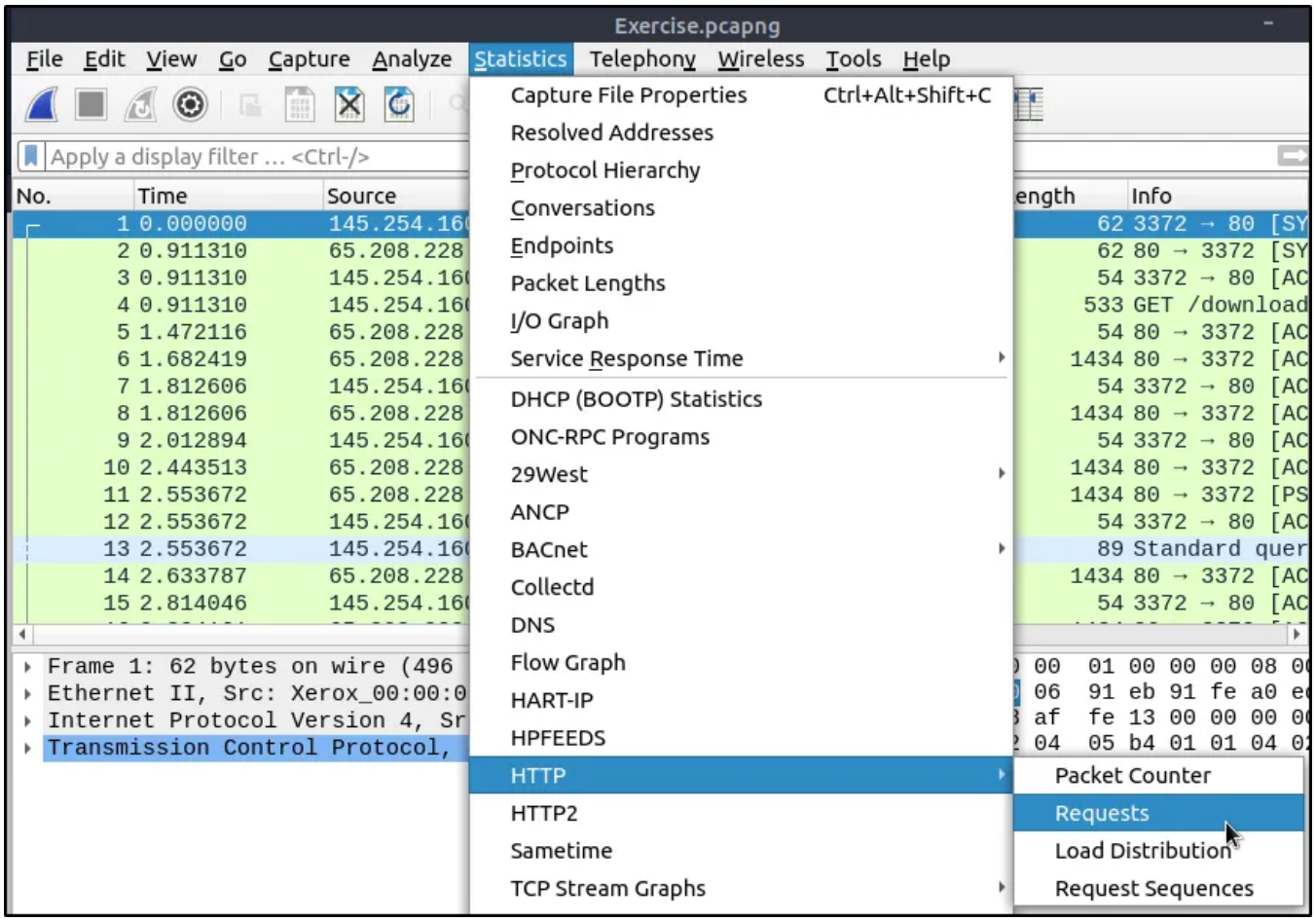




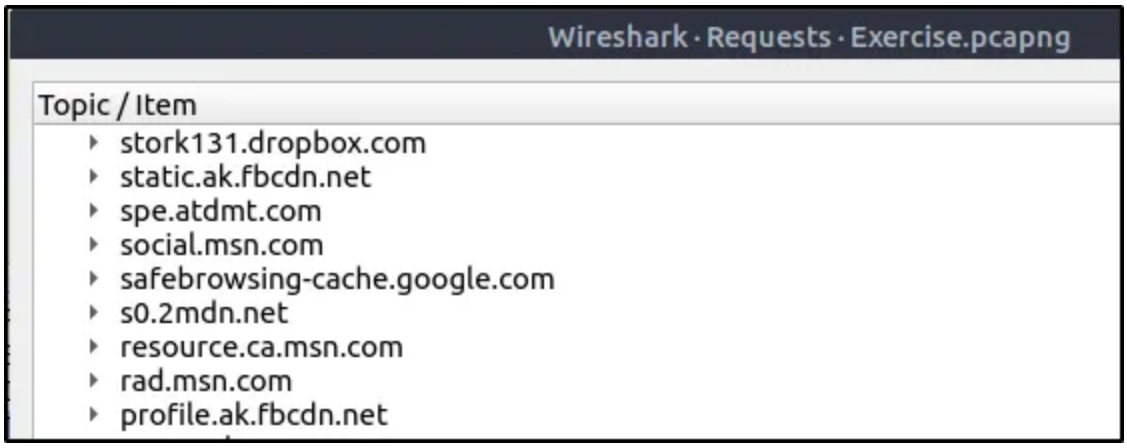
What is the number of HTTP Requests accomplished by "rad[.]msn[.]com?

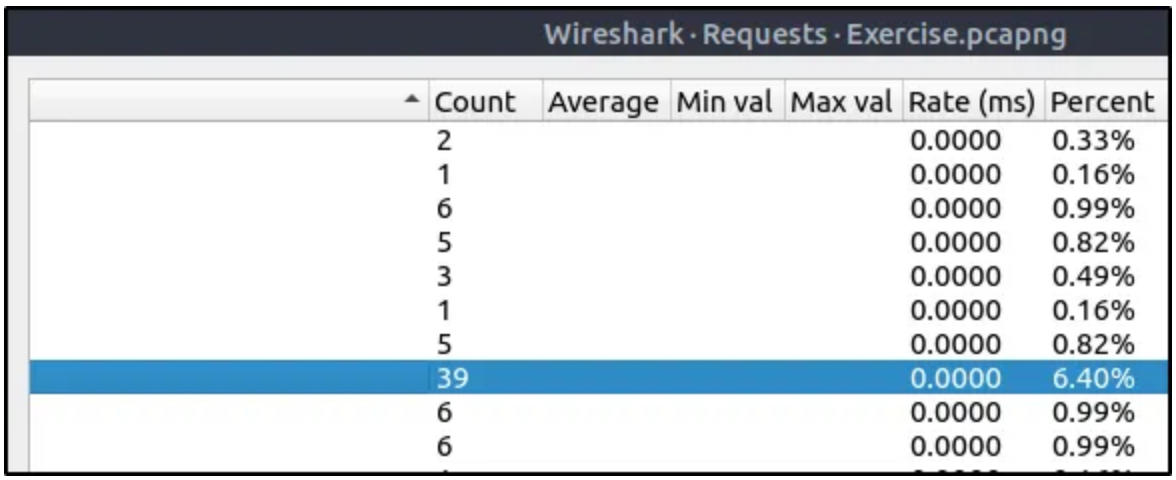
Ans: 39

Go to **Statistics** then HTTP then **Requests.**



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





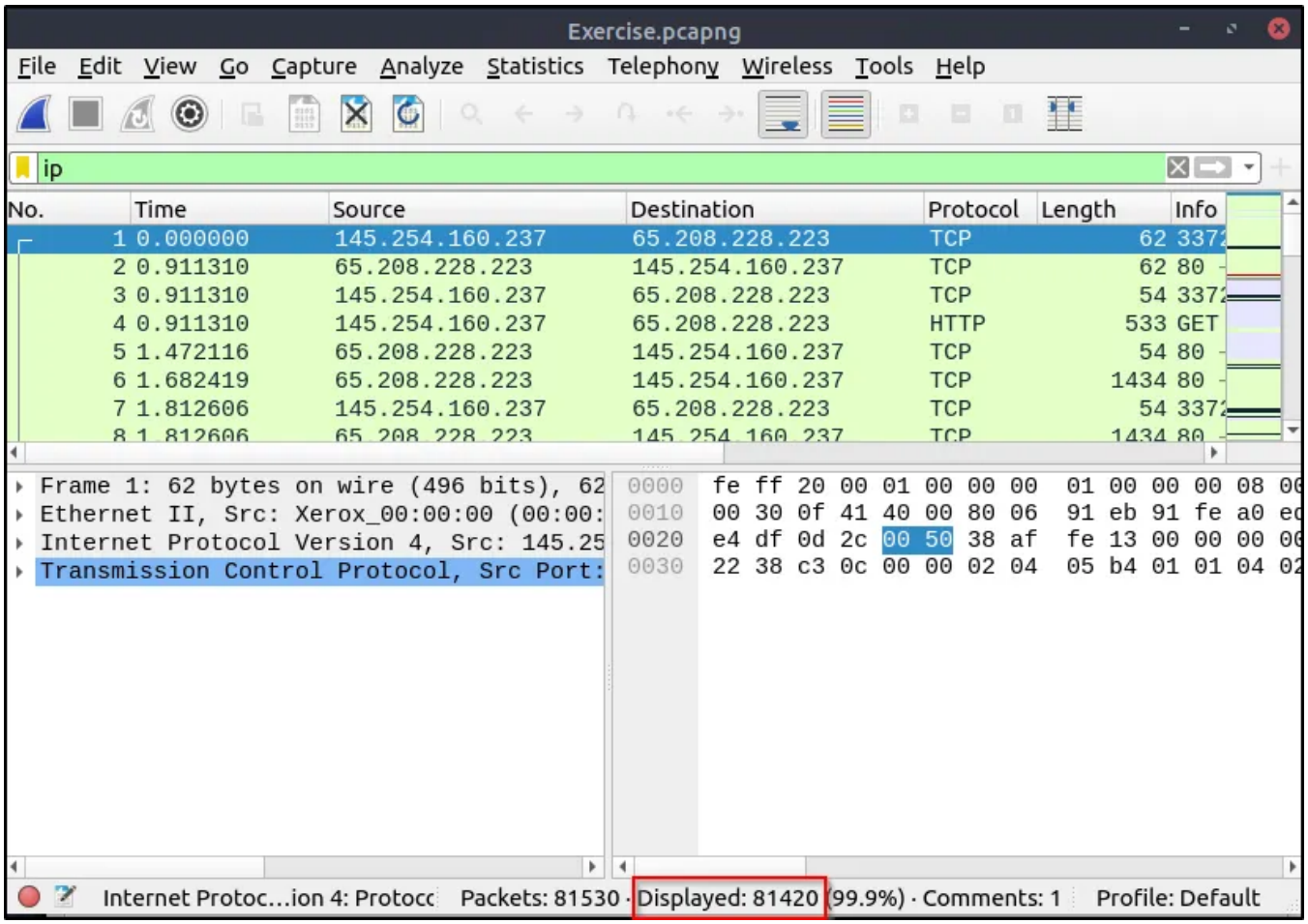
Task 5: Packet Filtering | Protocol Filters

What is the number of IP packets?

Ans: 84120

Filter out only packets with ip

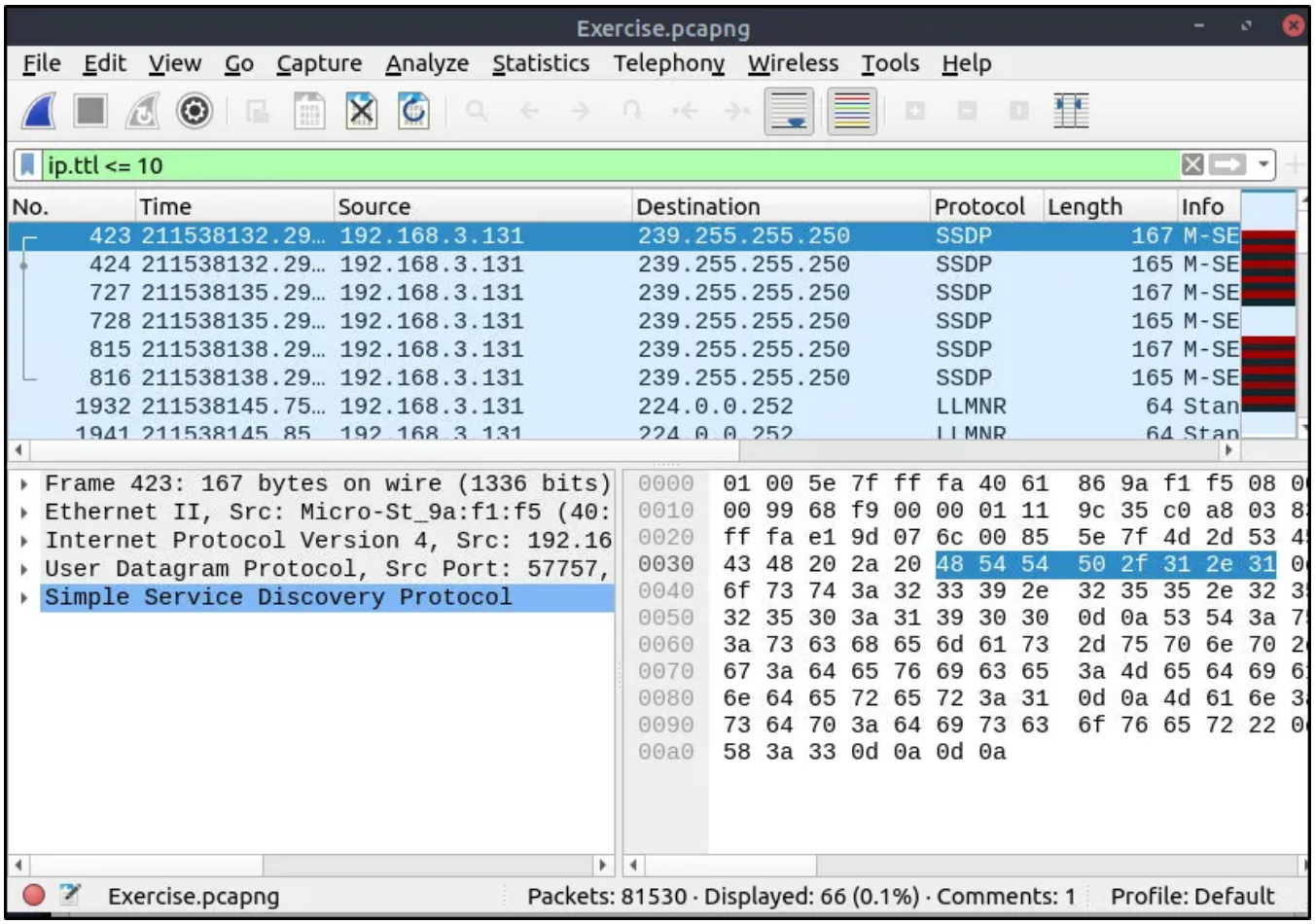
```
ip
```



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

Ans: 66

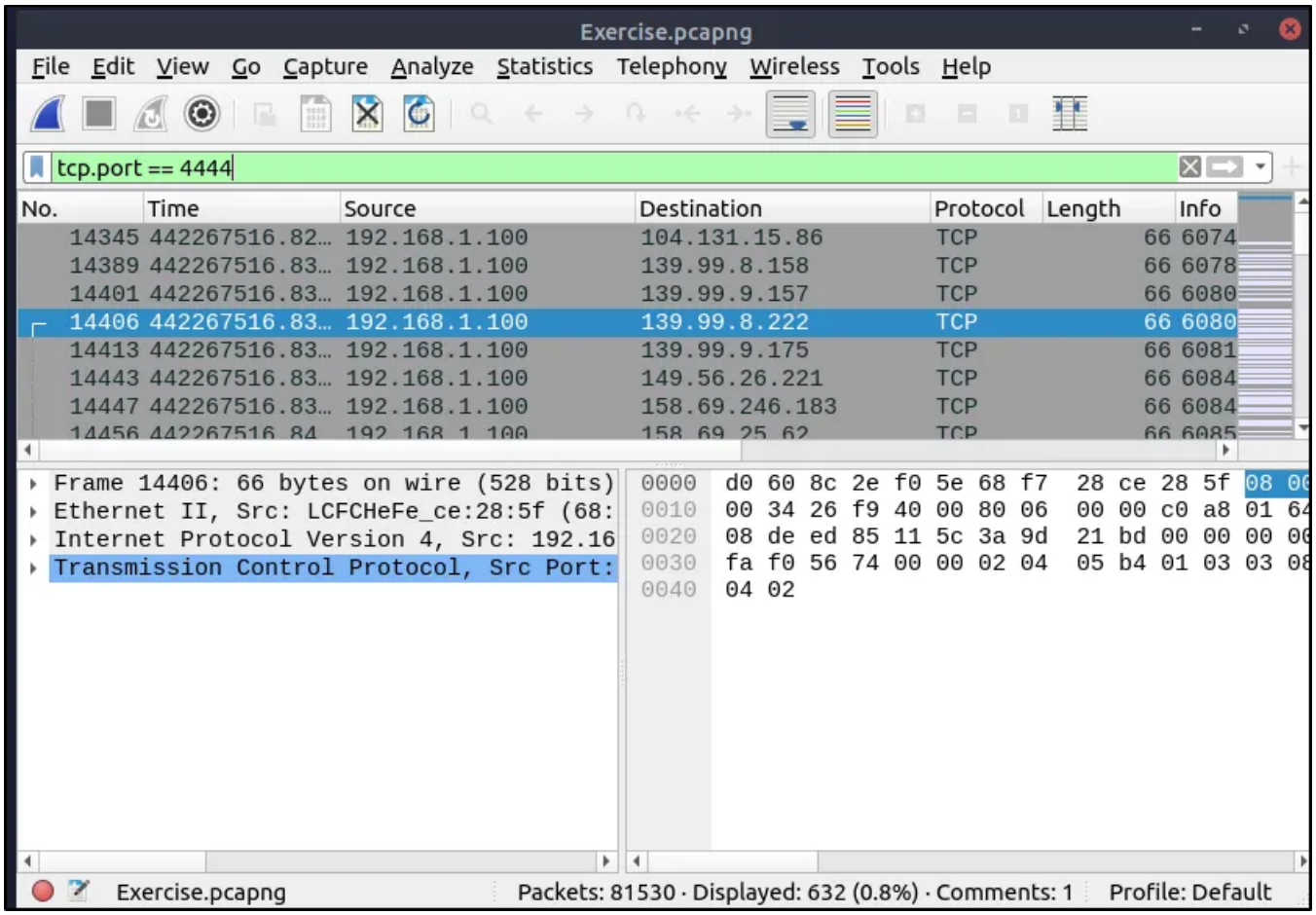
```
ip.ttl <= 10
```



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

Ans: 632

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

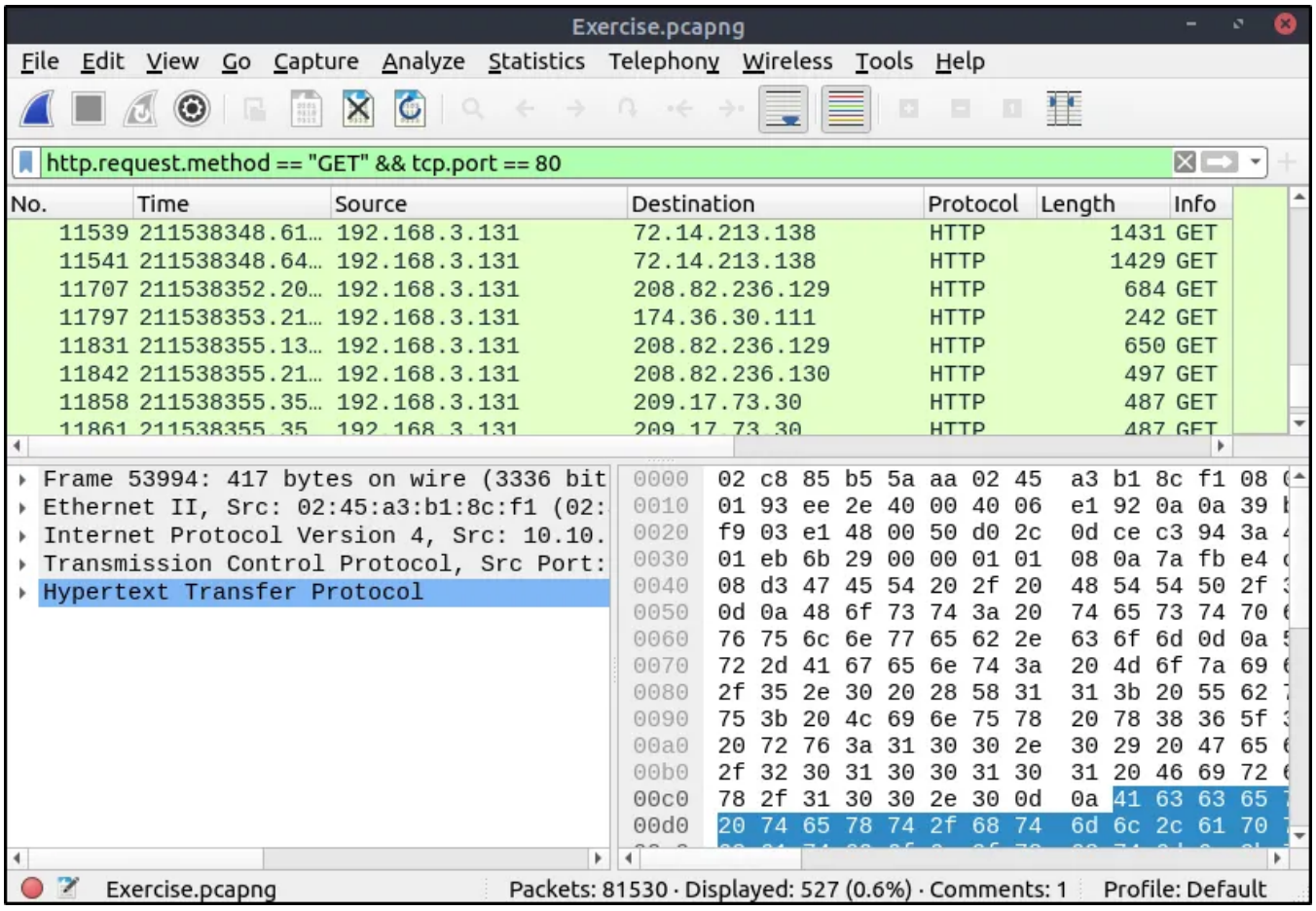


What is the number of "HTTP GET" requests sent to port "80"?

Ans: 527

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

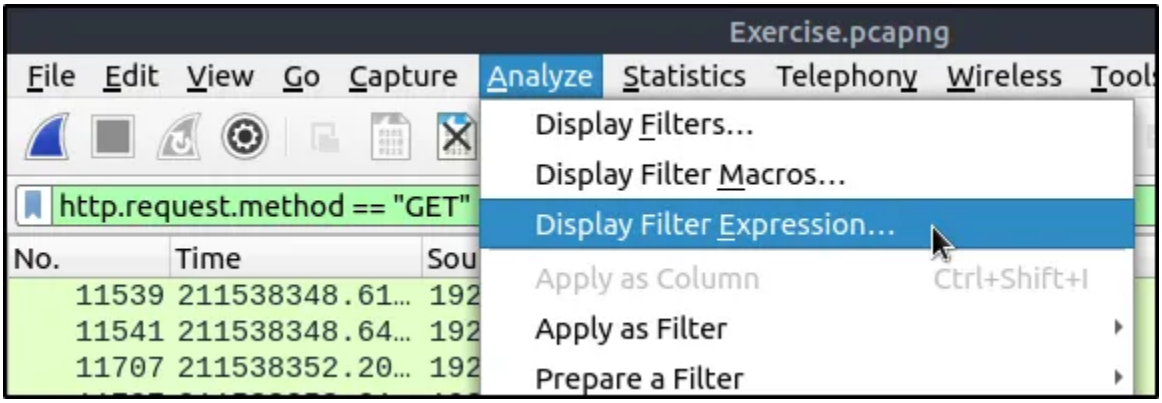
```
http.request.method == "GET" && tcp.port == 80
```



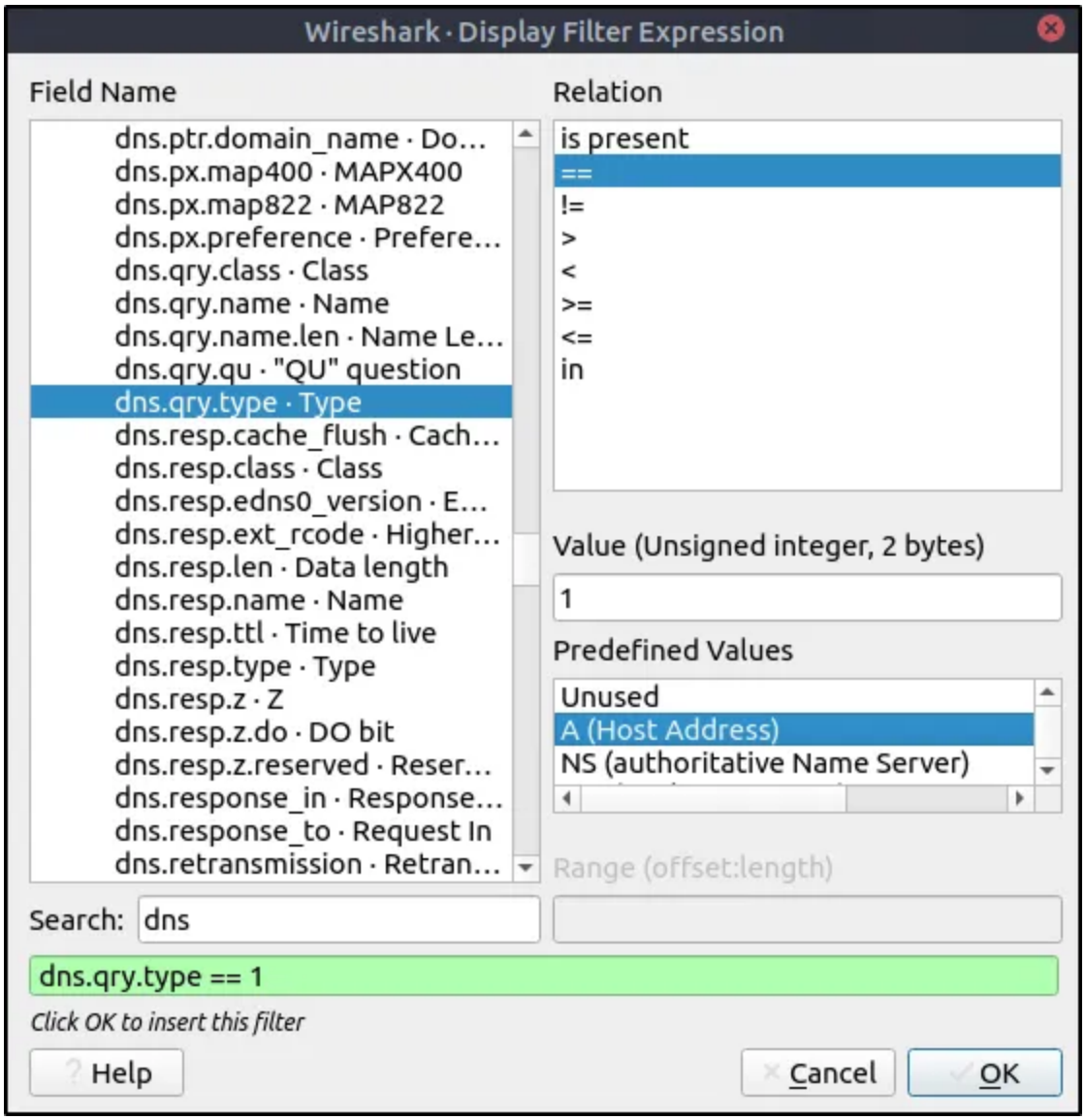
What is the number of "type A DNS Queries"?

Ans: 51

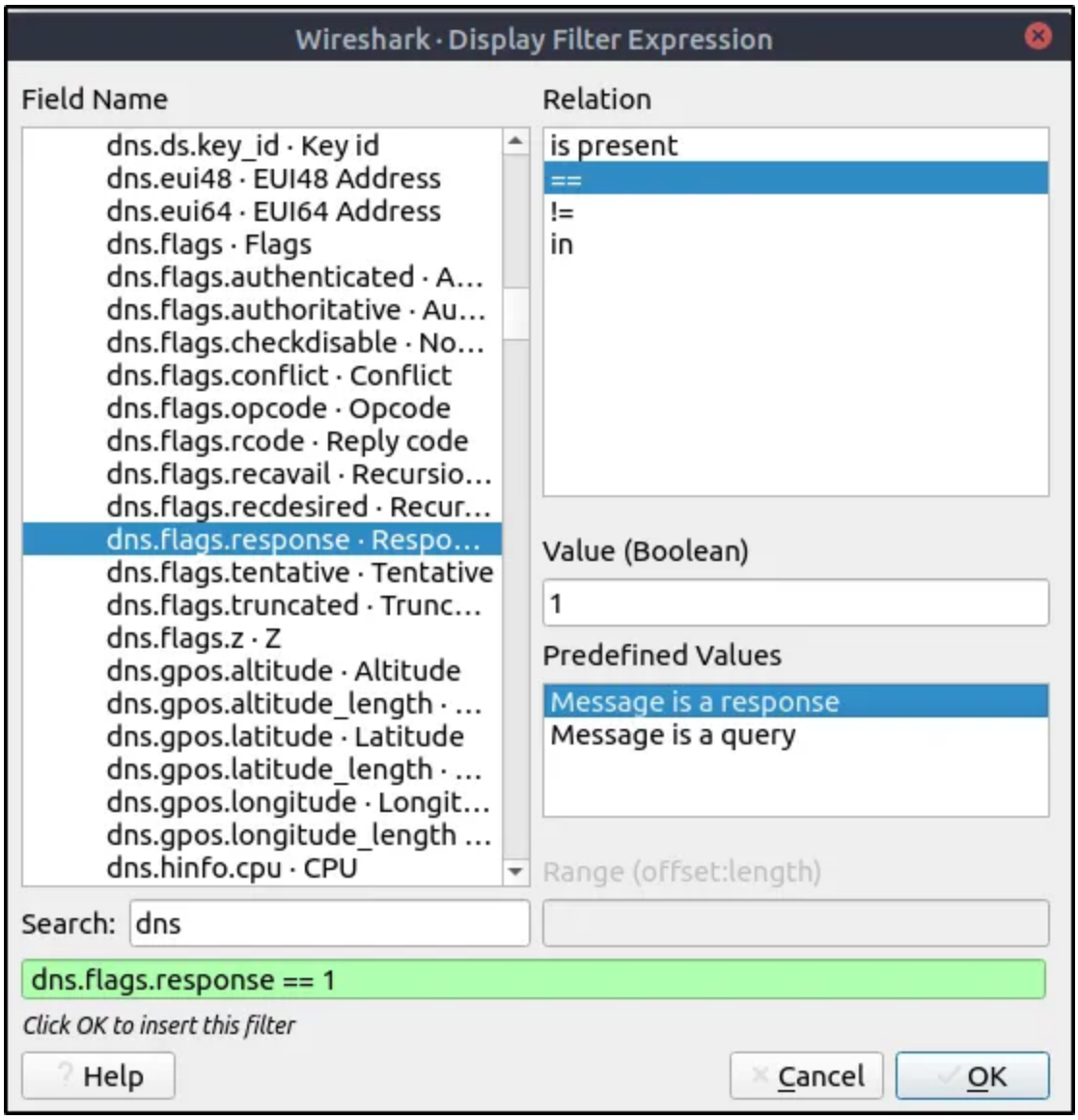
Let's build a filter using the Display Filter Expression under the **Analyze** menu.



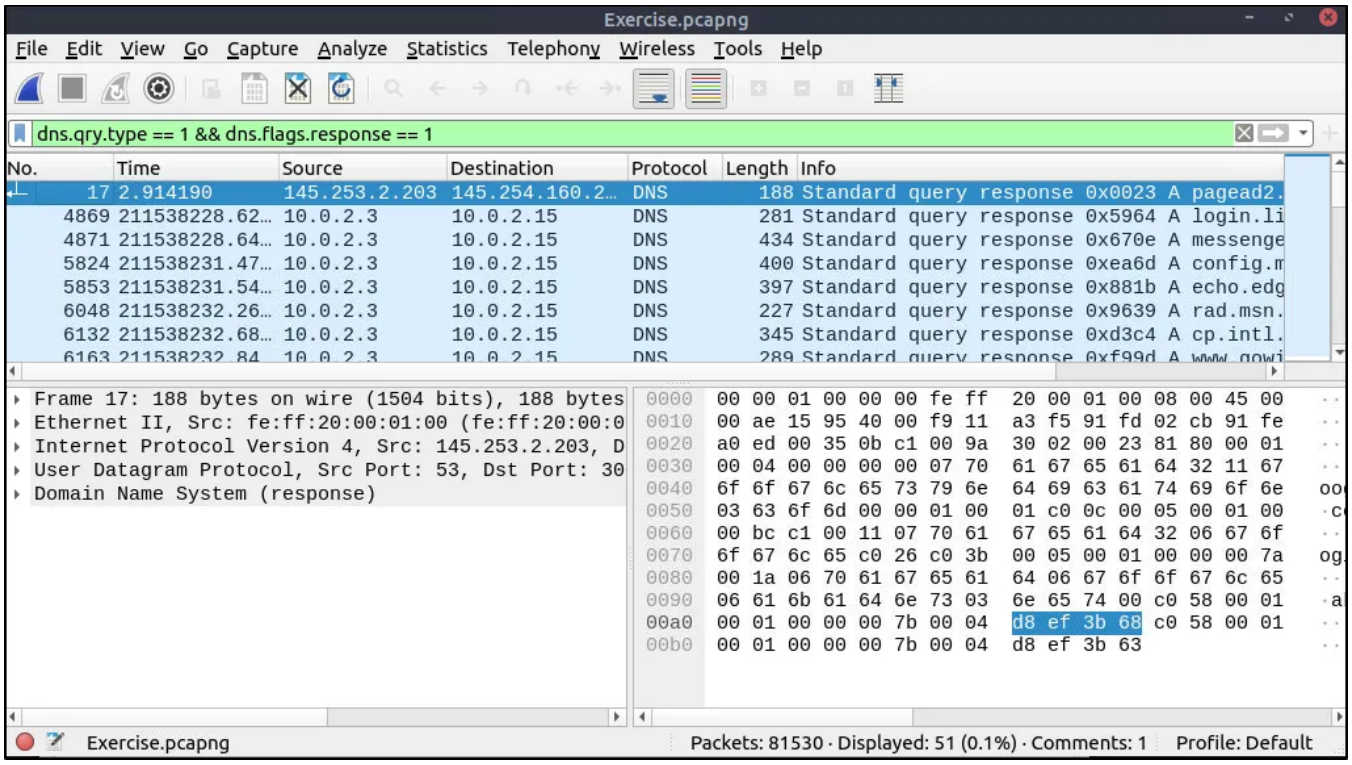
Search for **dns** then select **dns.query.type A** then click Ok.



Let’s add another filter to show all DNS responses




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



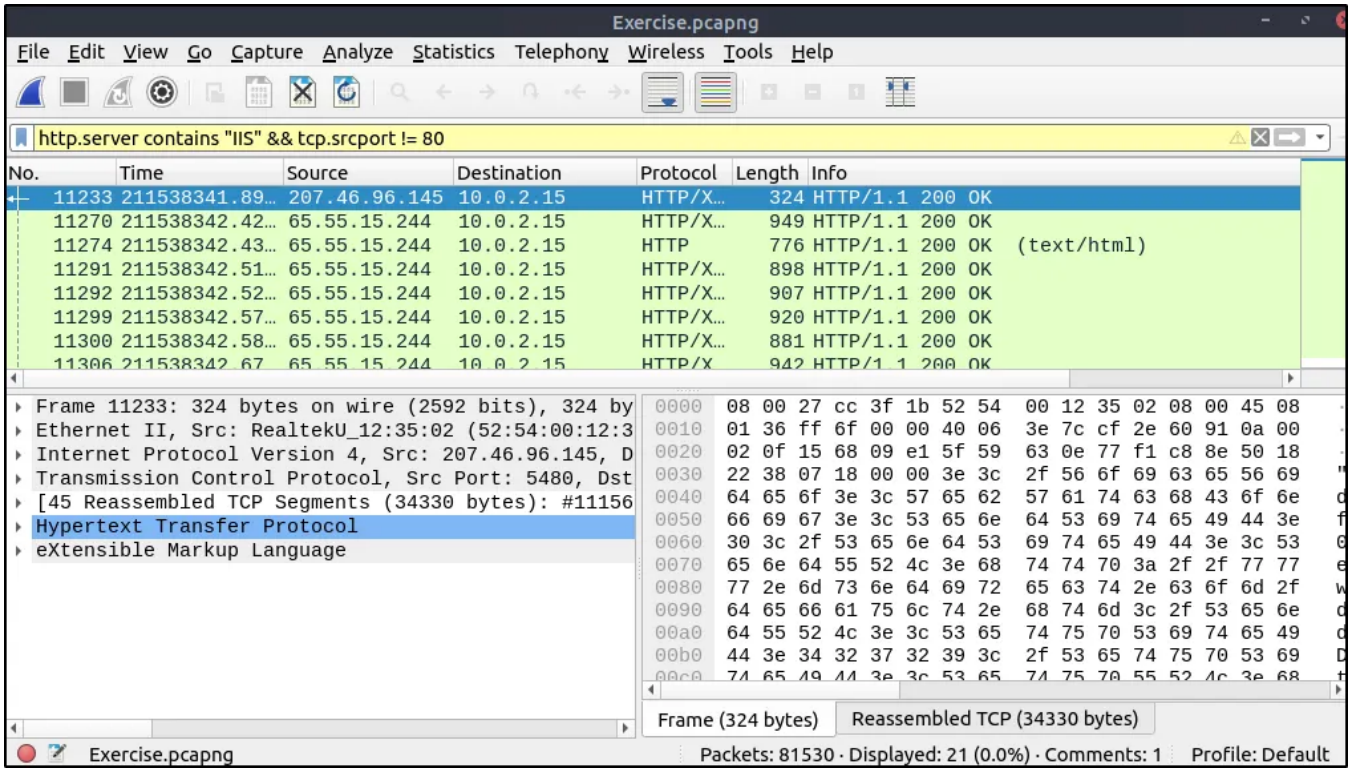
Task 6: Advanced Filtering

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
```

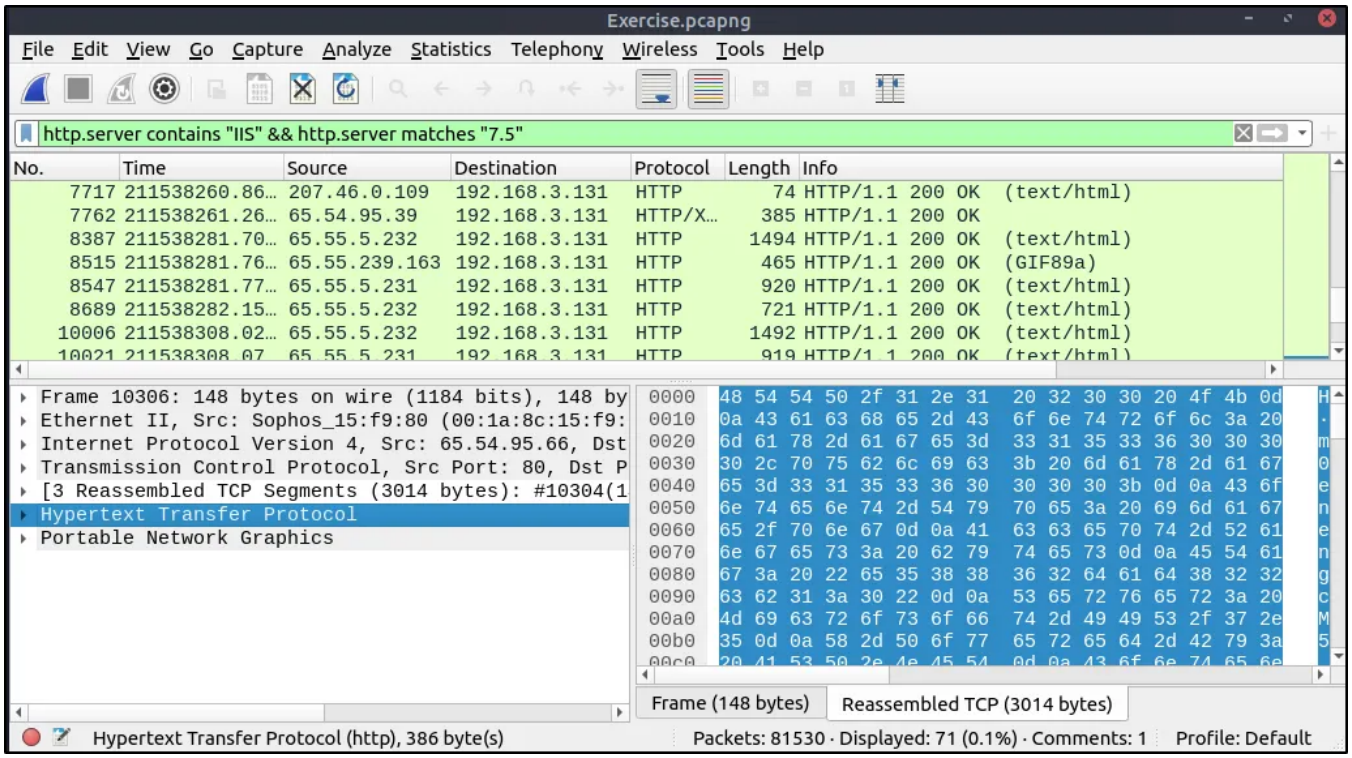


Find all Microsoft IIS servers. What is the number of packets that have "version 7.5"?

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"
```

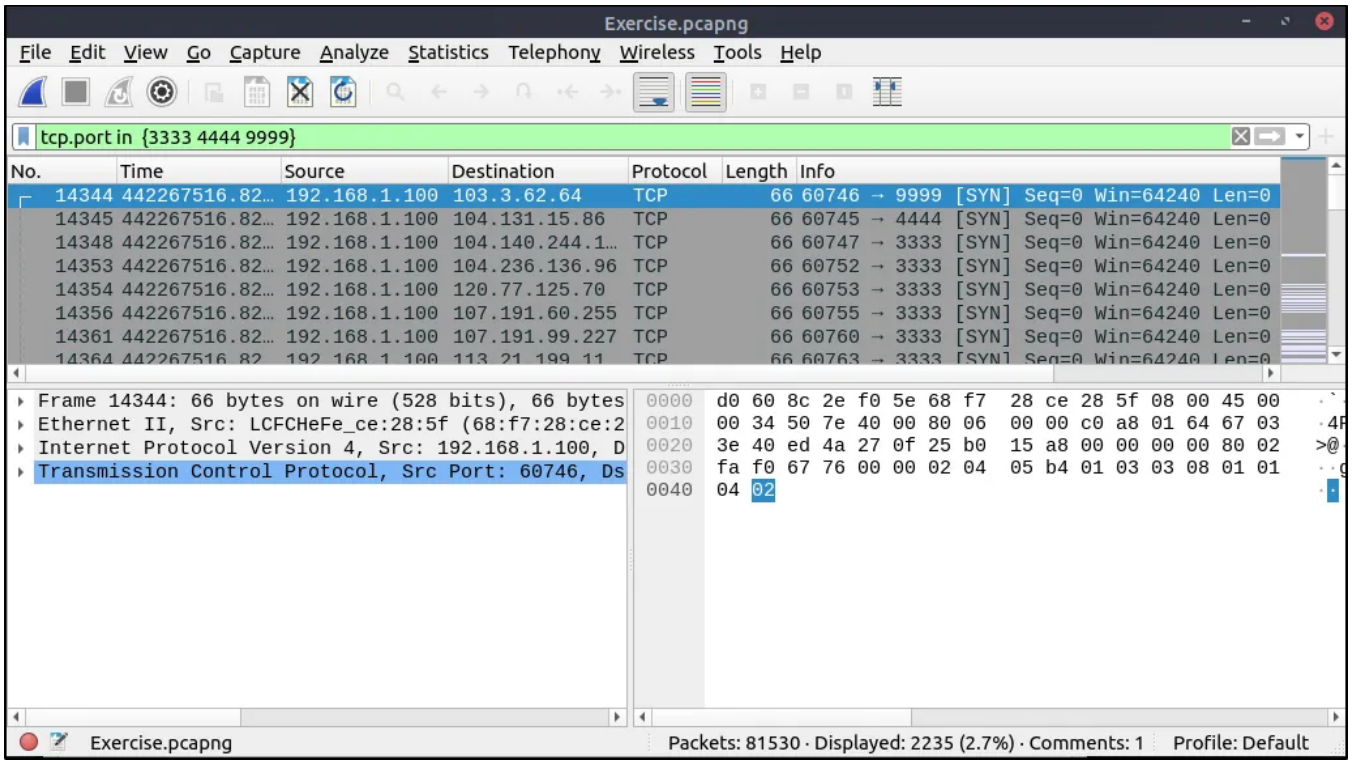


What is the total number of packets that use ports 3333, 4444 or 9999?

Ans: 2235

Use curly braces and put spaces between strings.

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

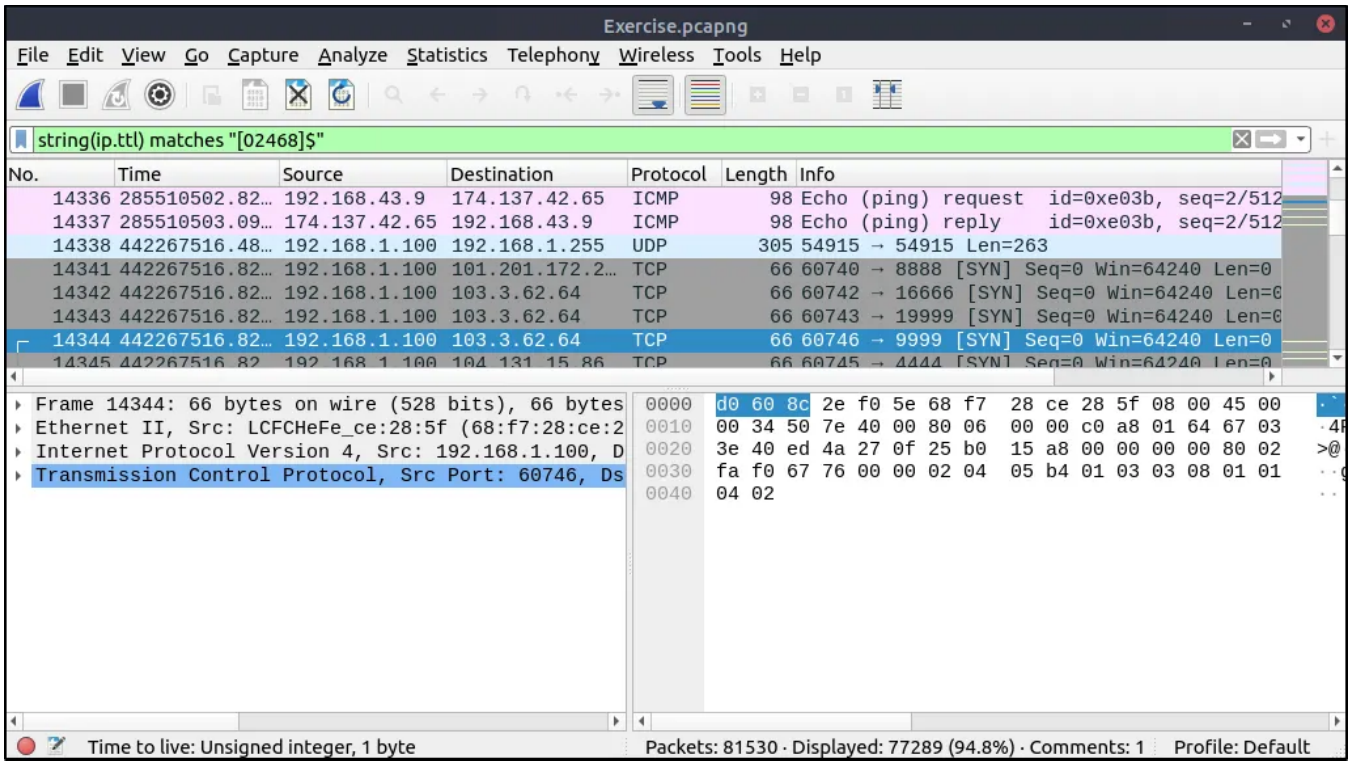


What is the number of packets with “even TTL numbers”?

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.

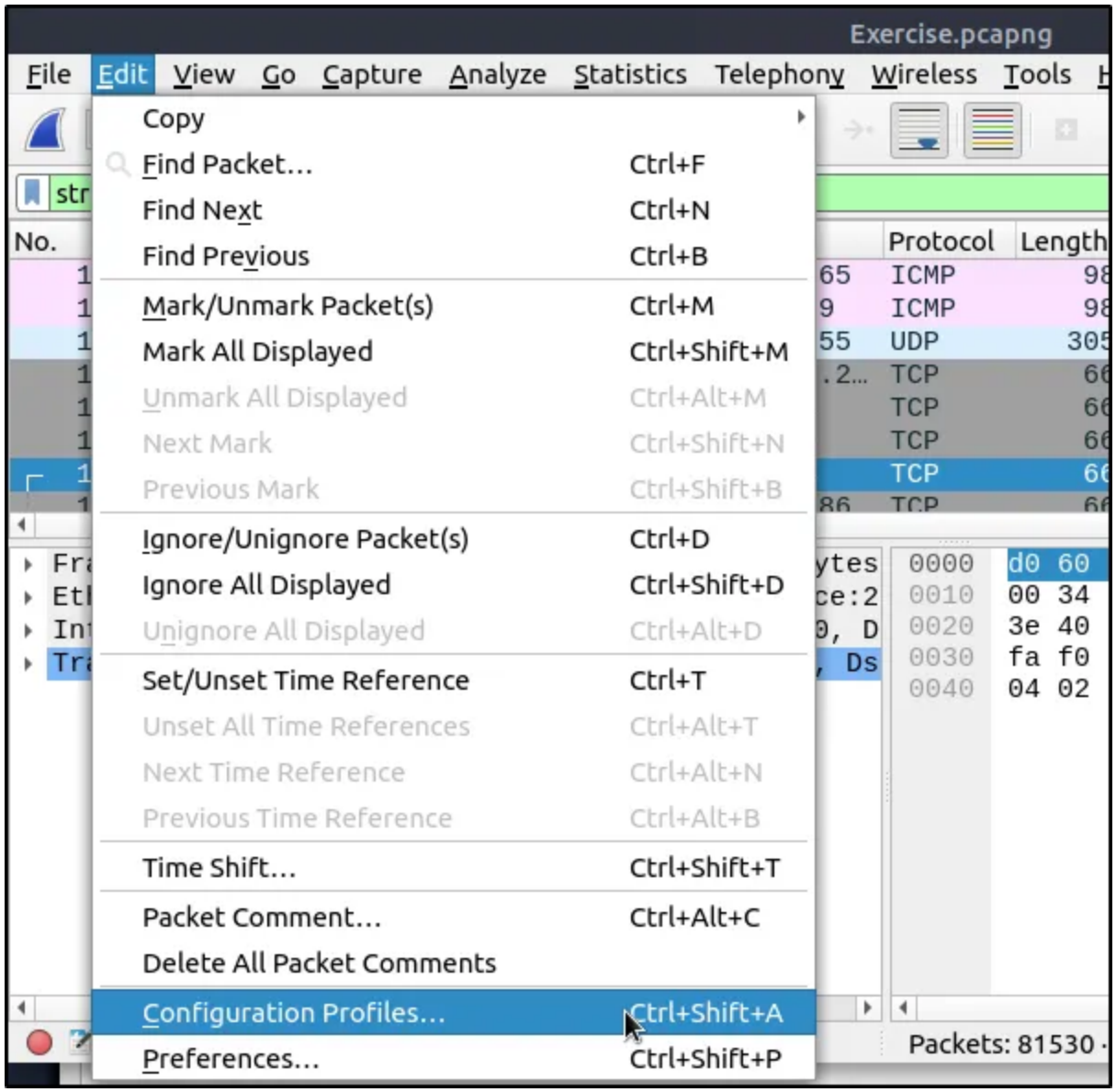
```
string(ip.ttl) matches "[02468]$"
```

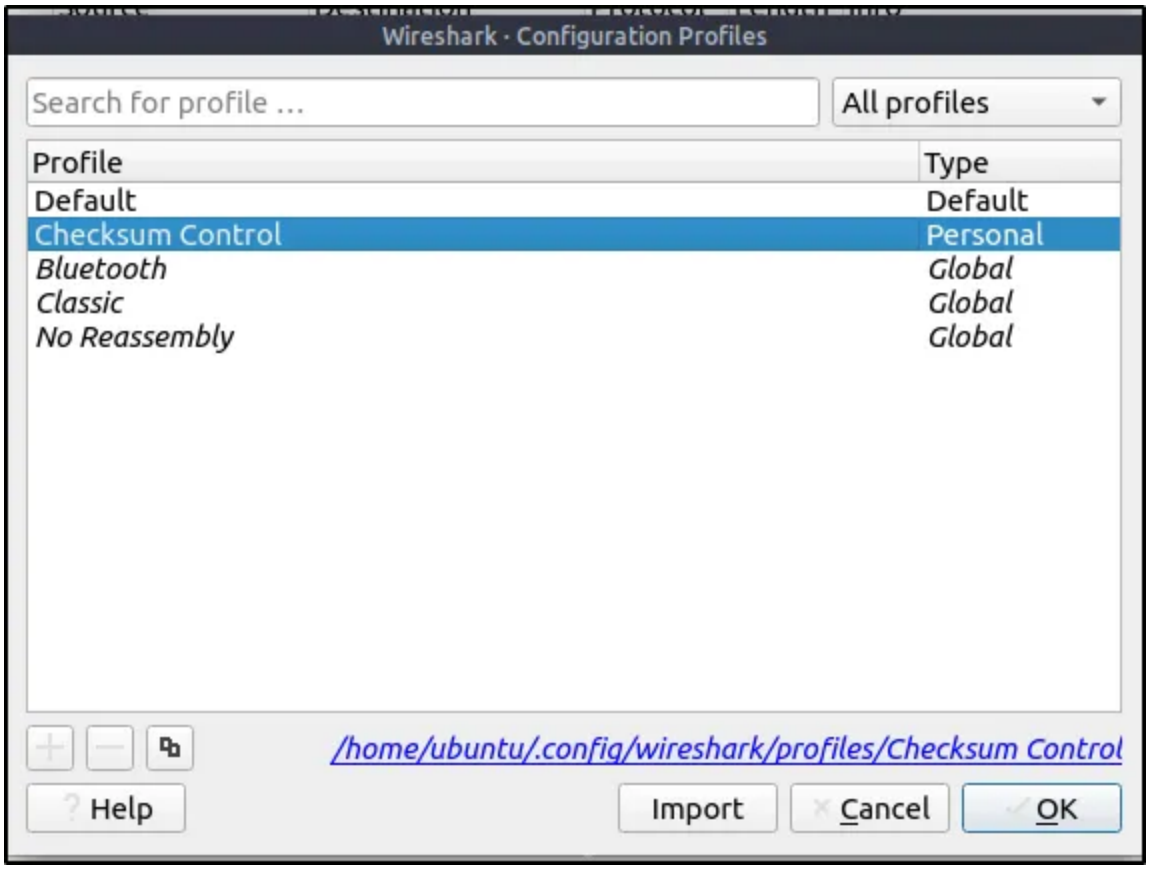


Change the profile to "Checksum Control". What is the number of "Bad TCP Checksum" packets?

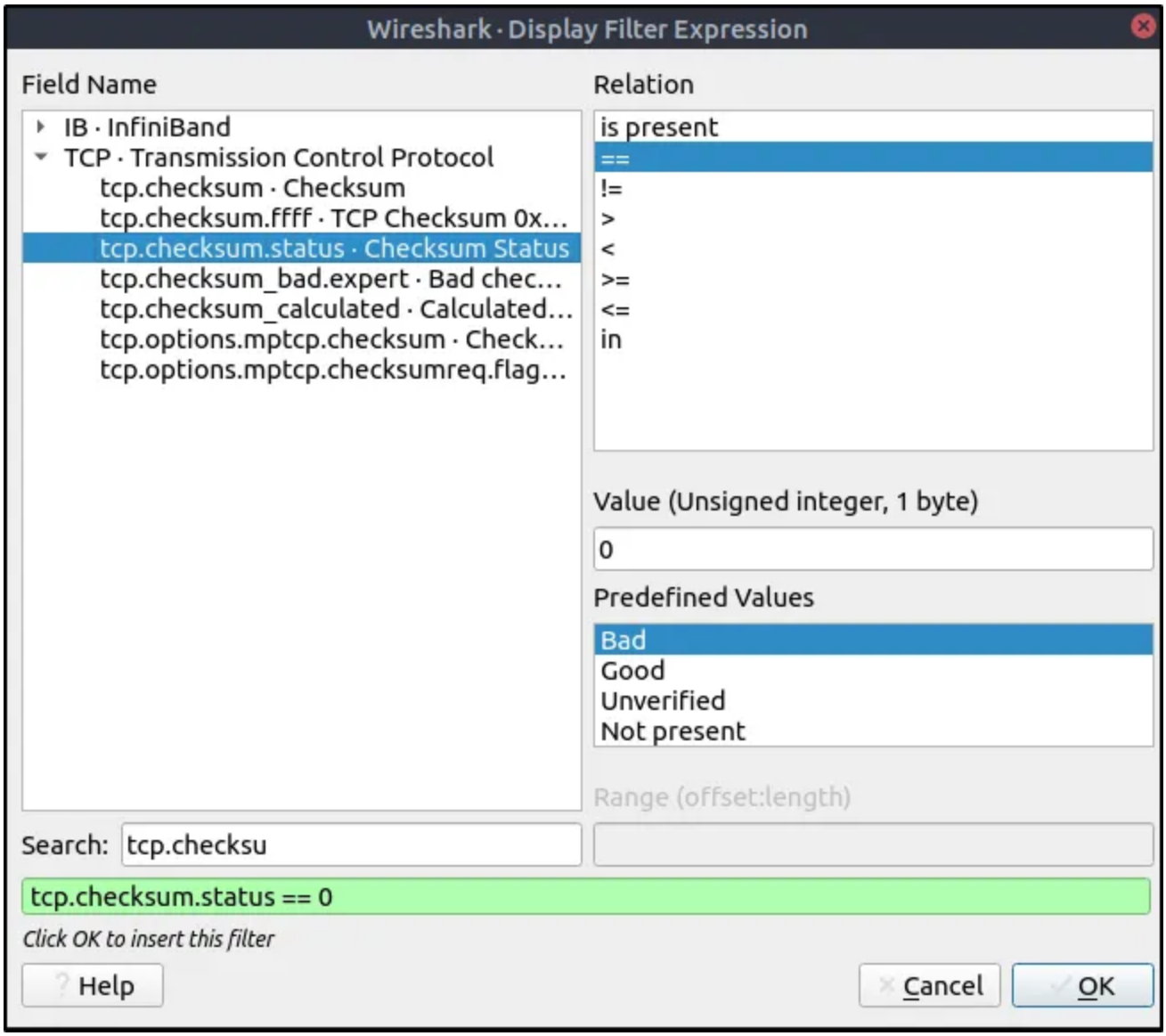
Ans: 34185

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

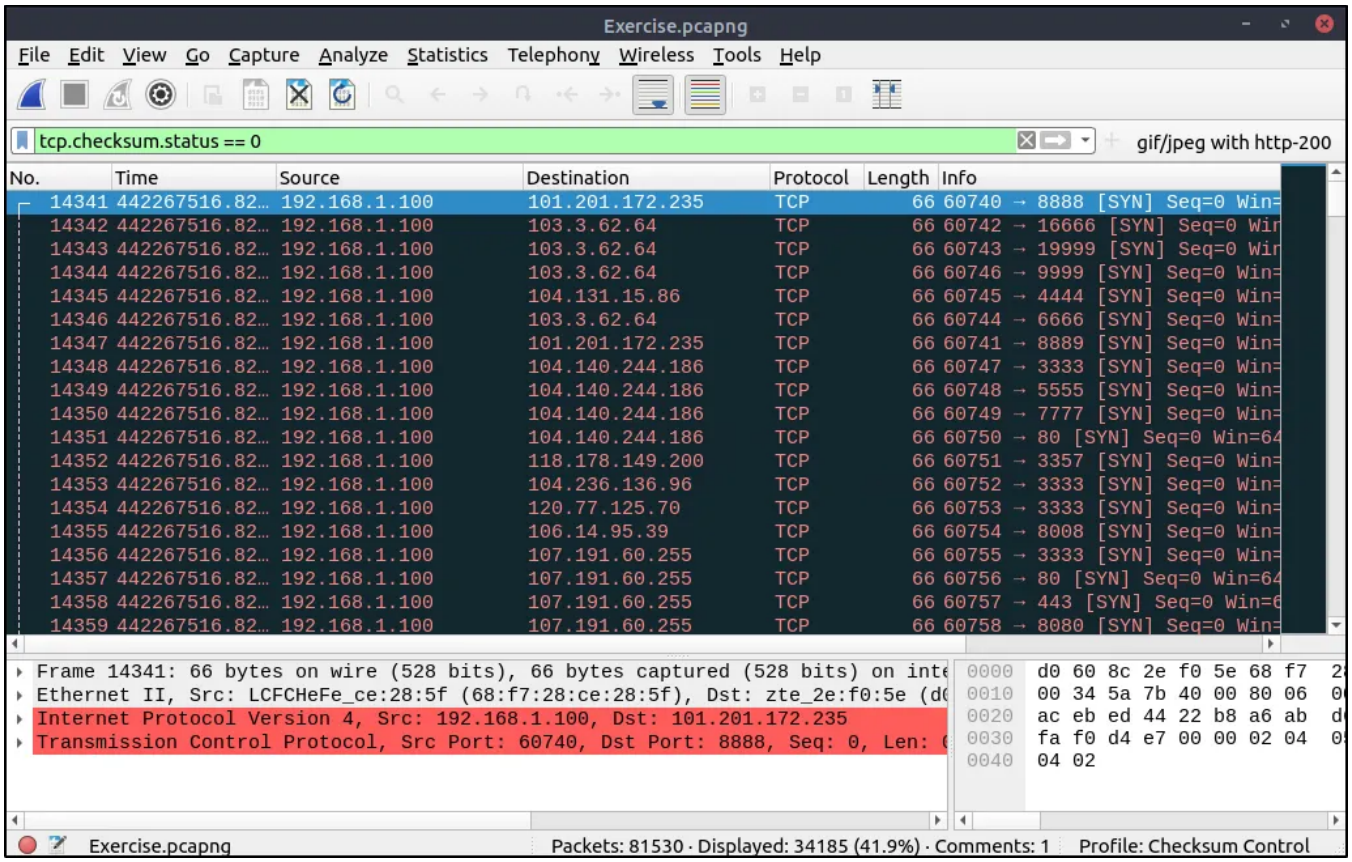

Exercise.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools
Copy
Find Packet... Ctrl+F
Find Next Ctrl+N
Find Previous Ctrl+B
Mark/Unmark Packet(s) Ctrl+M
Mark All Displayed Ctrl+Shift+M
Unmark All Displayed Ctrl+Alt+M
Next Mark Ctrl+Shift+N
Previous Mark Ctrl+Shift+B
Ignore/Unignore Packet(s) Ctrl+D
Ignore All Displayed Ctrl+Shift+D
Unignore All Displayed Ctrl+Alt+D
Set/Unset Time Reference Ctrl+T
Unset All Time References Ctrl+Alt+T
Next Time Reference Ctrl+Alt+N
Previous Time Reference Ctrl+Alt+B
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Delete All Packet Comments
Configuration Profiles... Ctrl+Shift+A
Preferences... Ctrl+Shift+P
No.
Protocol
Length
ICMP
UDP
TCP
0000 d0 60
0010 00 34
0020 3e 40
0030 fa f0
0040 04 02
Packets: 81530



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



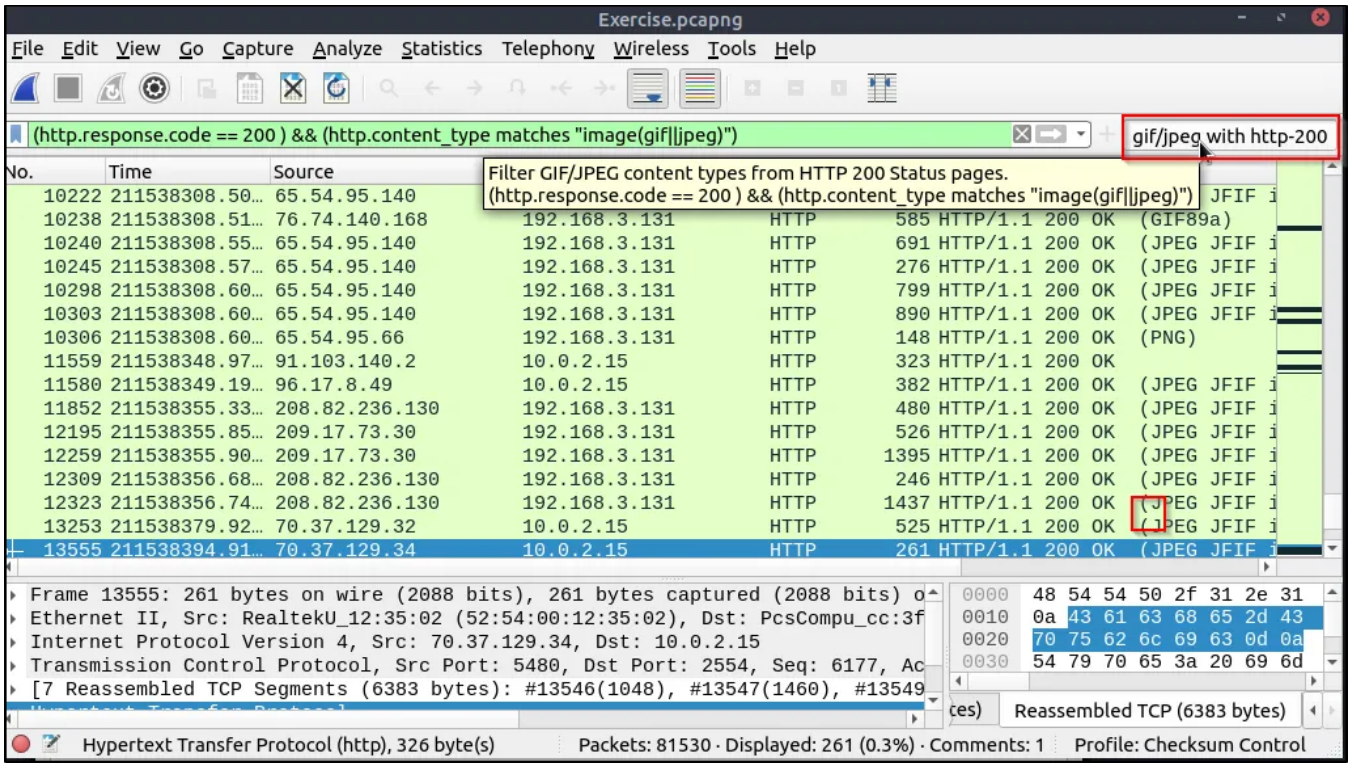

```
tcp.checksum.status == 0
```



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

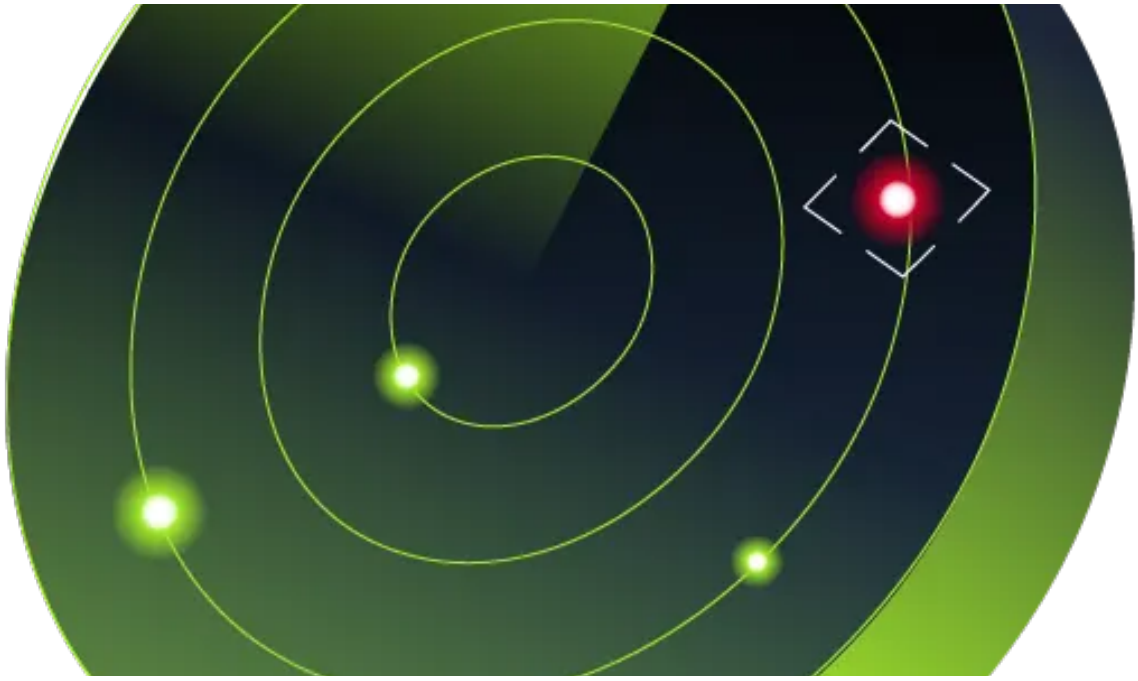
Anti-Reverse Engineering

Sle3pyHead

Network Discovery Detection Walkthrough Notes | TryHackMe

Detect network scans and vulnerabilities using Zeek and Elastic.

Oct 2 5 1

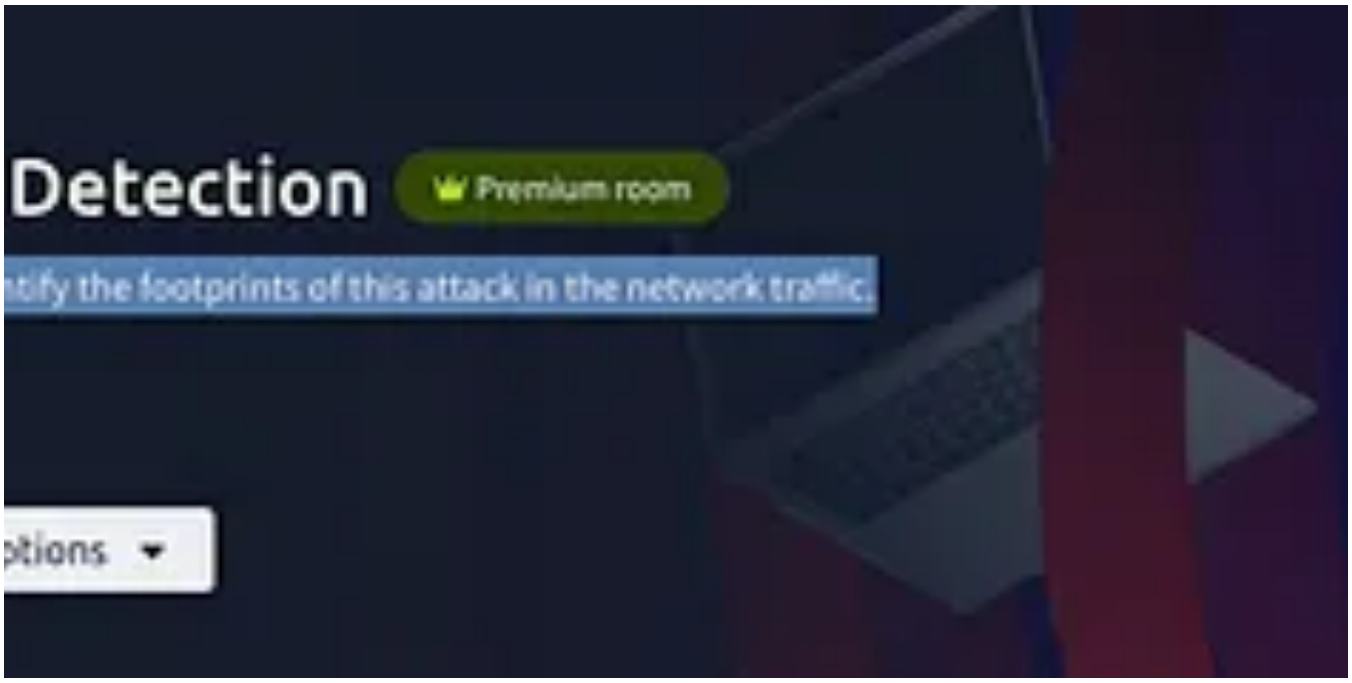


In System Weakness by Visir

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{0×416469747961204D6163686972616A75}

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