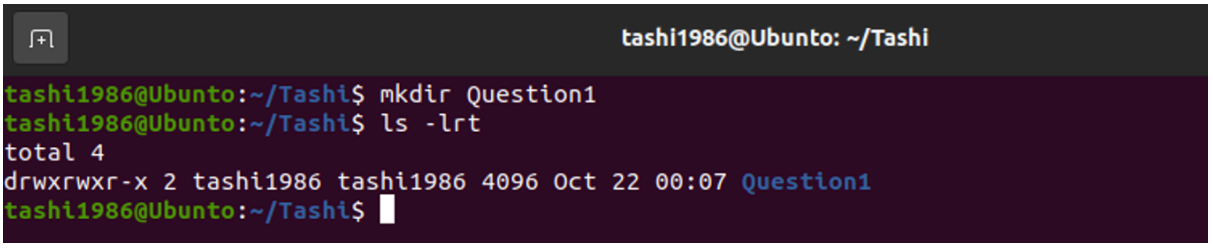
Question 1:

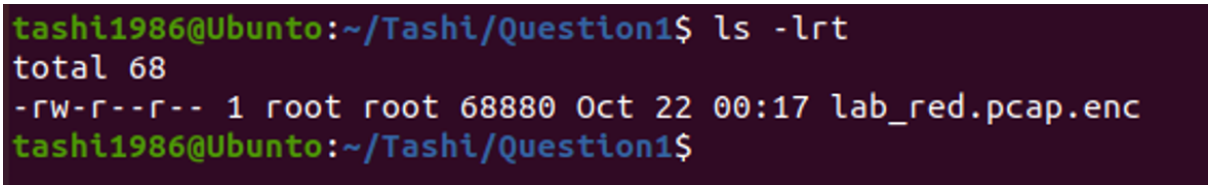
For Question 1, made a directory named Question1 as below:



Get the following file:

wget
https://github.com/SCH-IT-MurdochUni/NetworkingLabs/raw/refs/heads/main/Reusable_Learning_Objects/.test/.misc/lab_red.pcap.enc

Check the file: (file ***lab_red.pcap.enc*** will be generated)



You can decrypt it by adapting the following command for your purposes:

sudo openssl enc -d -aes-256-cbc -in lab_red.pcap.enc -out lab_red.pcap.enc.tar.bz2 -k '2aT9134fnBwC$'

The encrypted file gets decrypted as below:

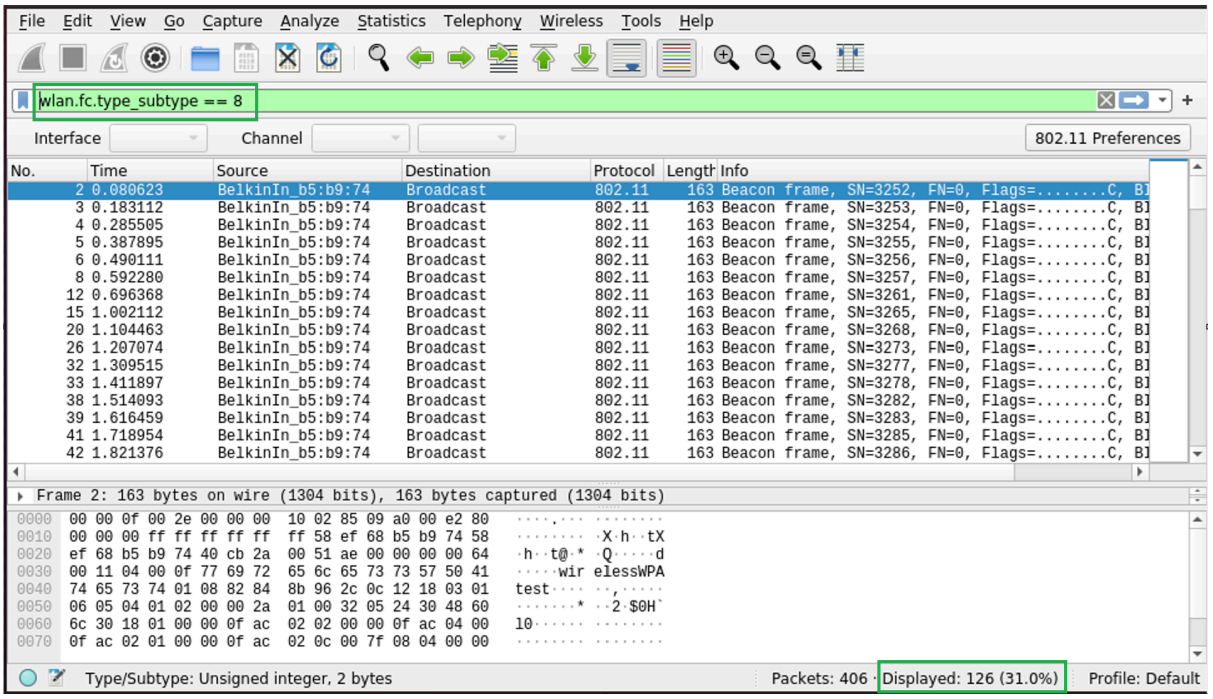
```
tashi1986@Ubunto:~/Tashi/Question1$ sudo openssl enc -d -aes-256-cbc -in lab_red.pcap.enc -out lab_red.pcap.enc.tar.bz2 -k '2aT9134fnBwC$'
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
tashi1986@Ubunto:~/Tashi/Question1$ ls -lrt
total 136
-rw-r--r-- 1 root root 68880 Oct 22 00:17 lab_red.pcap.enc
-rw-r--r-- 1 root root 68850 Oct 22 00:26 lab_red.pcap.enc.tar.bz2
tashi1986@Ubunto:~/Tashi/Question1$
```

What percentage of the frames are 802.11 beacons? Answer to 1 decimal place but do not include a % sign

Open the wireshark as: ***sudo wireshark lab_red.pcap.enc.tar.bz2***

```
tashi1986@Ubunto:~/Tashi/Question1$ sudo wireshark lab_red.pcap.enc.tar.bz2
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

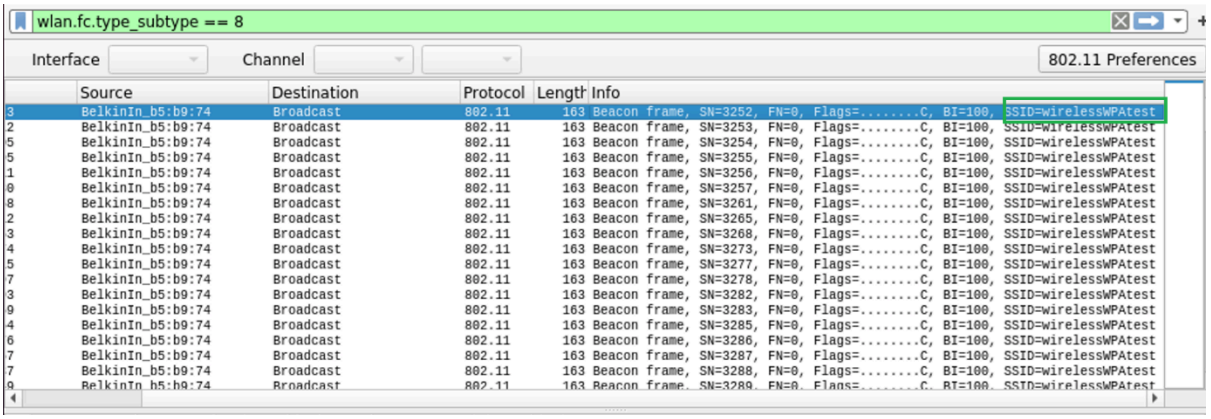
Filter it with 'wlan.fc.type_subtype == 8'



Answer: You can see the result value at the bottom: 31.0 % and so is the answer.

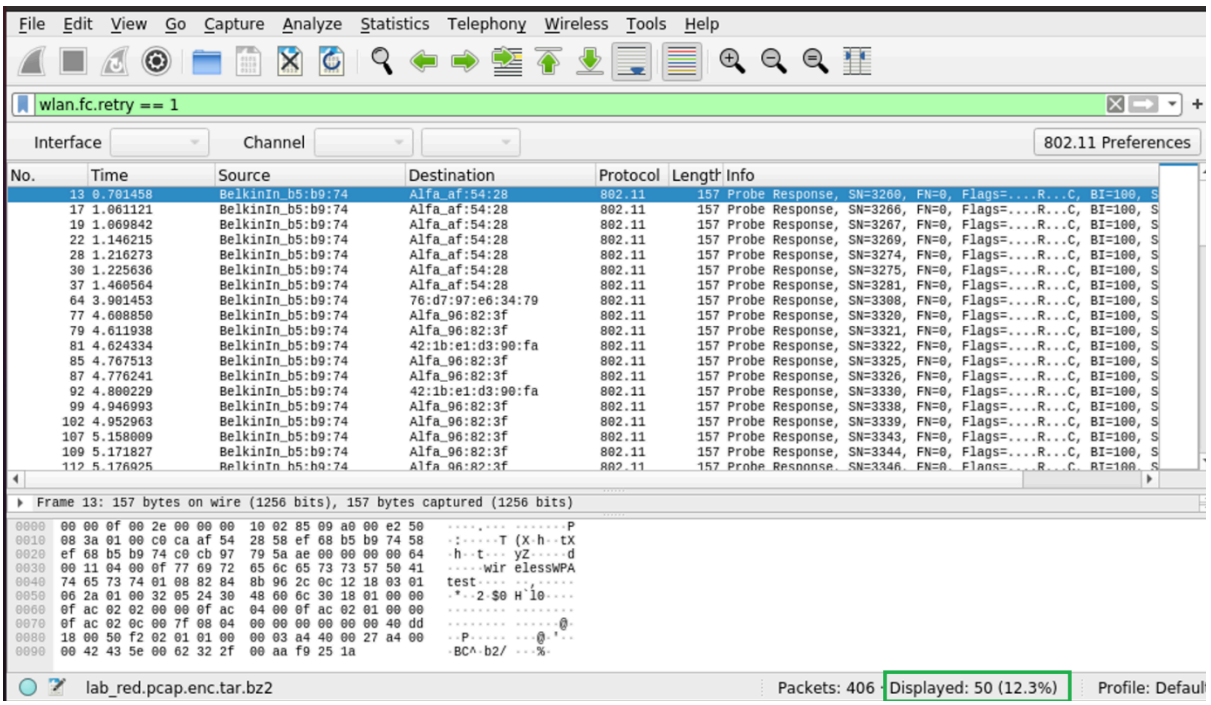
What is the SSID used?

Answer: WirelessWPAtest



How many frames have been reported as a retransmission? Enter a number:

Answer: 50



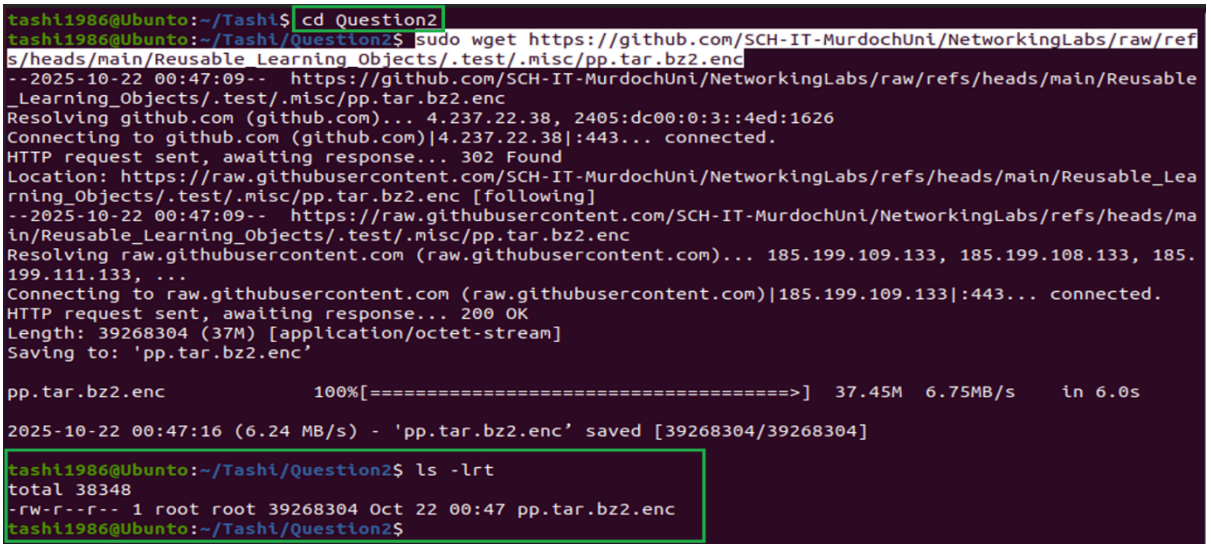
Question 2:

Made Question2 directory:

And get the encrypted file as below:

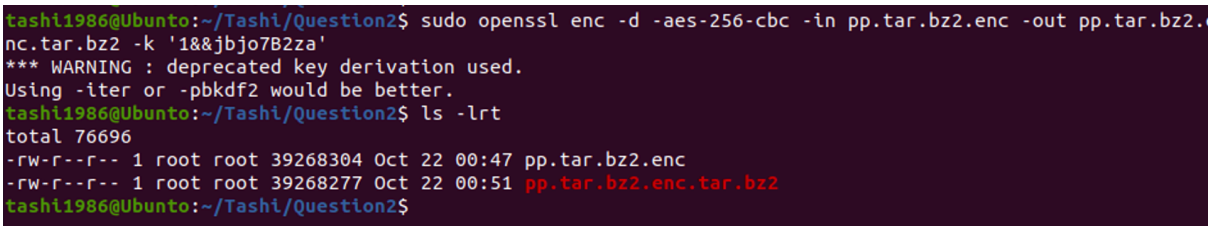
wget *https://github.com/SCH-IT-MurdochUni/NetworkingLabs/raw/refs/heads/main/Reusable_Learning_Objects/.test/.misc/pp.tar.bz2.enc*

and file pp.tar.bz2.enc will be downloaded as below:



Decrypt the file:

Sudo openssl enc -d -aes-256-cbc -in pp.tar.bz2.enc -out pp.tar.bz2.enc.tar.bz2 -k ‘1&&jbjo7B2za’

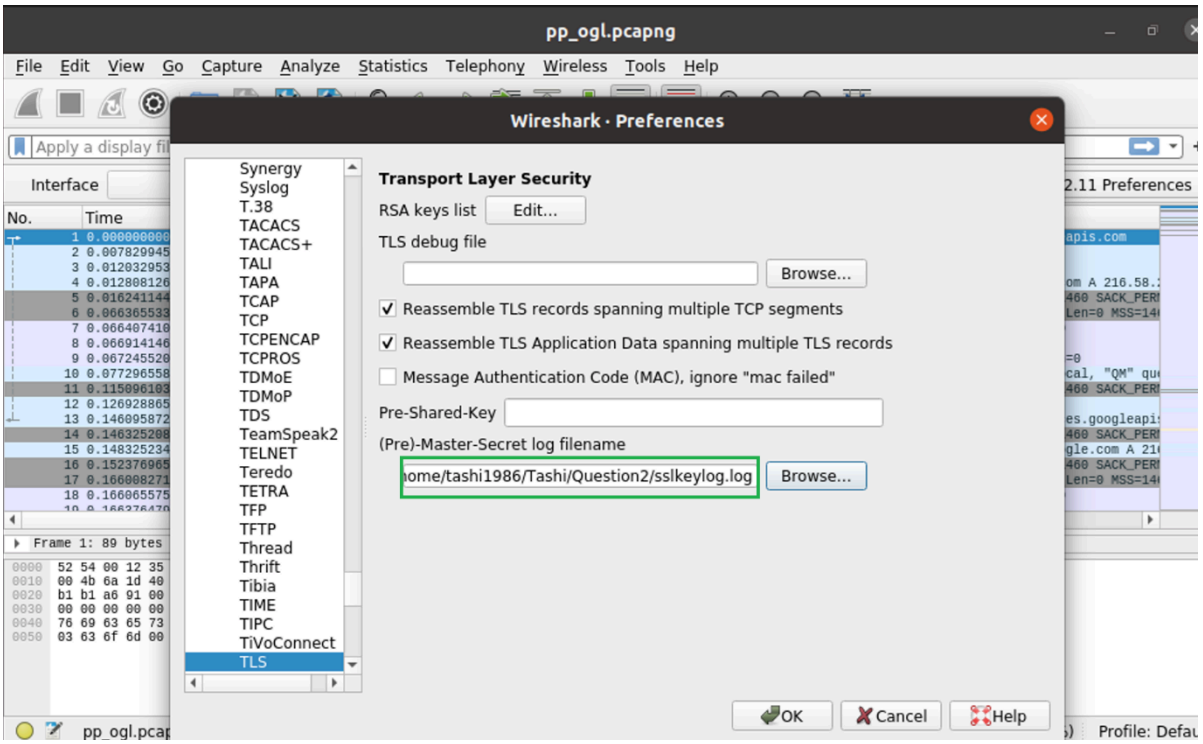


Post decryption, you will need to untar the file as below: ‘tar -xvf pp.tar.bz2.enc.tar.bz2’ and two more files will be generated:

```
tashi1986@Ubunto:~/Tashi/Question2$ tar -xvf pp.tar.bz2.enc.tar.bz2
pp_ogl.pcapng
sslkeylog.log
tashi1986@Ubunto:~/Tashi/Question2$ ls -lrt
total 116988
-rw-r--r-- 1 tashi1986 tashi1986 40707276 Aug 12  2019 pp_ogl.pcapng
-rw-r--r-- 1 tashi1986 tashi1986   547022 Aug 12  2019 sslkeylog.log
-rw-r--r-- 1 root      root      39268304 Oct 22 00:47 pp.tar.bz2.enc
-rw-r--r-- 1 root      root      39268277 Oct 22 00:51 pp.tar.bz2.enc.tar.bz2
tashi1986@Ubunto:~/Tashi/Question2$
```

Now open wireshark:

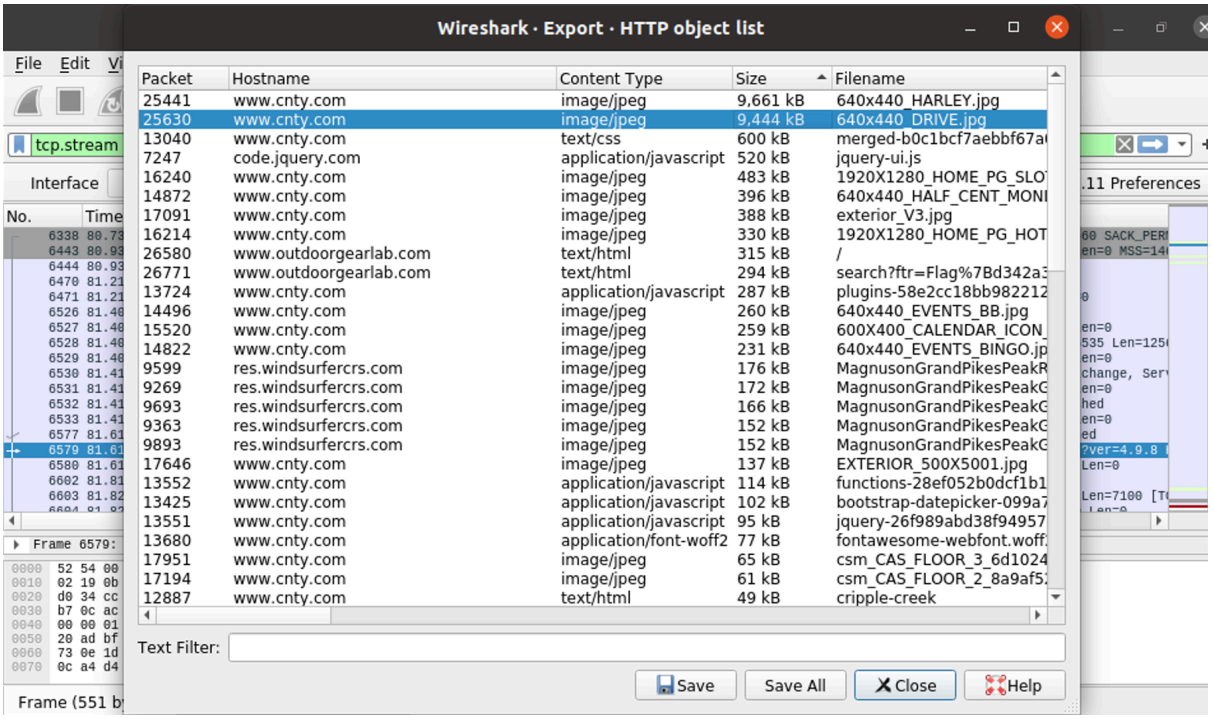
Go to Edit □ Preference □ Protocols □ TLS □ and select the sslkeylog.log file as below:



Click ok

Recover all of the HTTP objects. The second-largest file has three words in it. Write these three words below all lower case with no spaces

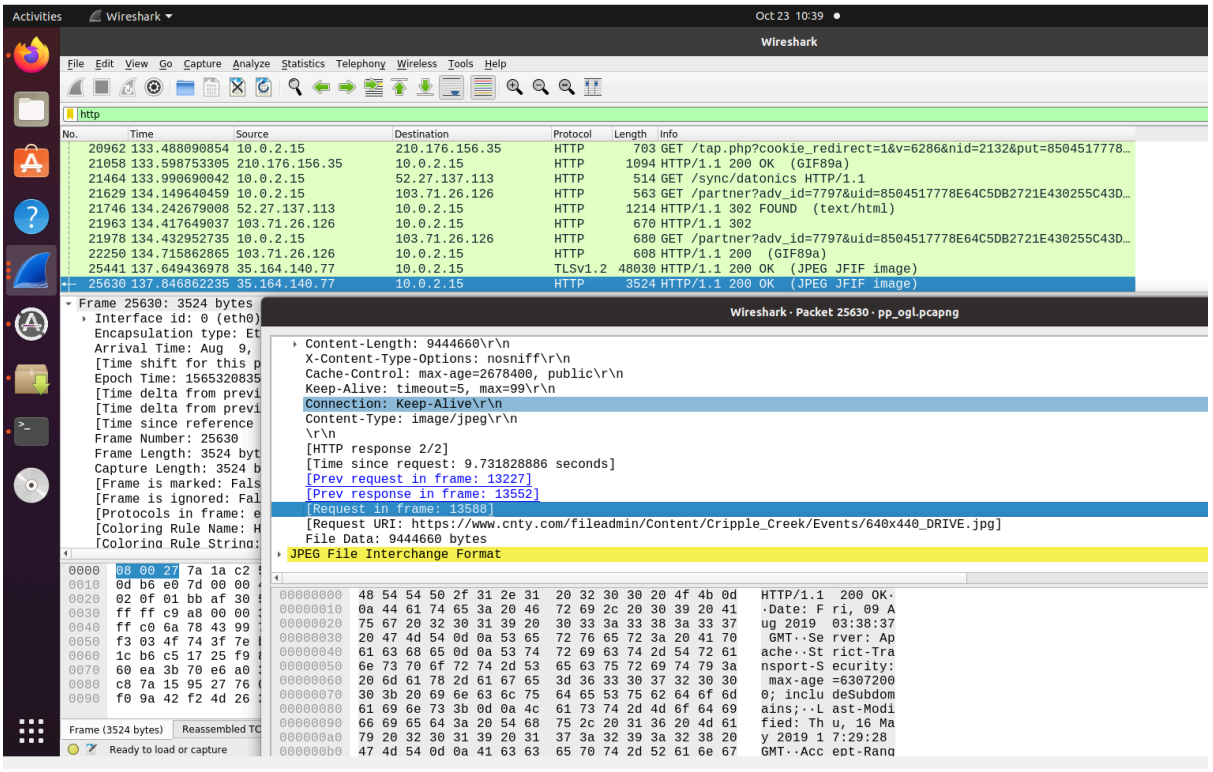
Go to File □ Export Objects □ HTTP (Then sort by size) and select the 2nd largest file and save it.



In ubuntu, open the saved image from deskop and you will see the image with three words that is drive your dream.

What frame number is this image requested in? Usually, in wireshark, the frame number is the left-most column. Requests from webpages are often HTTP Gets

Need to work on this: 13588



Question 3:

Get the file:

Decrypt the file:

Sudo openssl enc -d -aes-256-cbc -in eggtopia_anon_practice.pcap.bz2.enc -out eggtopia_anon_practice.pcap.bz2.enc.tar.bz2 -k ‘Psz#6j^3BqQl’

```
tashi1986@Ubunto:~/Tashi/Question3$ sudo openssl enc -d -aes-256-cbc -in eggtopia_anon_practice.pcap.bz2.
enc -out eggtopia_anon_practice.pcap.bz2.enc.tar.bz2 -k 'Psz#6j^3BqQl'
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
tashi1986@Ubunto:~/Tashi/Question3$ ls -lrt
total 2104
-rw-rw-r-- 1 tashi1986 tashi1986 1073792 Oct 22 23:37 eggtopia_anon_practice.pcap.bz2.enc
-rw-r--r-- 1 root      root      1073768 Oct 22 23:43 eggtopia_anon_practice.pcap.bz2.enc.tar.bz2
tashi1986@Ubunto:~/Tashi/Question3$
```

Open the file in Wireshark. If the data is encrypted, can you find the decryption key? You should use the password list here:

wget https://raw.githubusercontent.com/SCH-IT-MurdochUni/NetworkingLabs/refs/heads/main/Reusable_Learning_Objects/.test/.misc/leaked_password_list_clean.txt

A file named leaked_password_list_clean.txt will be generated as below:

```
tashi1986@Ubunto:~/Tashi/Question3$ sudo wget https://raw.githubusercontent.com/SCH-IT-MurdochUni/Network
ingLabs/refs/heads/main/Reusable_Learning_Objects/.test/.misc/leaked_password_list_clean.txt
--2025-10-22 23:44:24--  https://raw.githubusercontent.com/SCH-IT-MurdochUni/NetworkingLabs/refs/heads/ma
in/Reusable_Learning_Objects/.test/.misc/leaked_password_list_clean.txt
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.110.133, 185.
199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 776784 (759K) [text/plain]
Saving to: 'leaked_password_list_clean.txt’

leaked_password_list_clean 100%[===================================>] 758.58K  4.07MB/s    in 0.2s

2025-10-22 23:44:25 (4.07 MB/s) - 'leaked_password_list_clean.txt’ saved [776784/776784]

tashi1986@Ubunto:~/Tashi/Question3$ ls -lrt
total 2864
-rw-rw-r-- 1 tashi1986 tashi1986 1073792 Oct 22 23:37 eggtopia_anon_practice.pcap.bz2.enc
-rw-r--r-- 1 root      root      1073768 Oct 22 23:43 eggtopia_anon_practice.pcap.bz2.enc.tar.bz2
-rw-r--r-- 1 root      root       776784 Oct 22 23:44 leaked_password_list_clean.txt
tashi1986@Ubunto:~/Tashi/Question3$
```

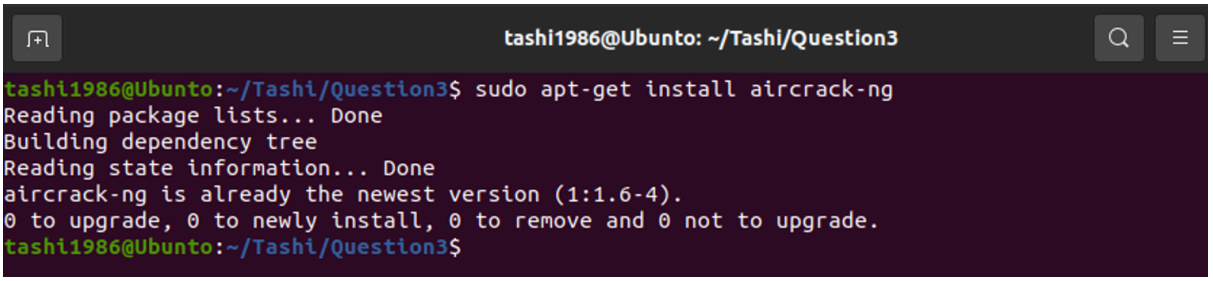
If you open the leaked_password_list_clean.txt, you can see the list of words, and now from these word you need to decrypt a password:

Cat leaked_password_list_clean.txt

```
040573
040563
04051964
04051961
04051954
040467
040465
04042010
04042008
040395
040369
040363
04032003
040295
040294
040275
040267
```

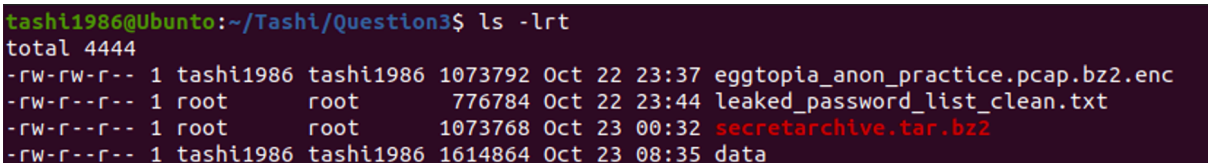
To get the decryption key, you will need to install aircrack-ng

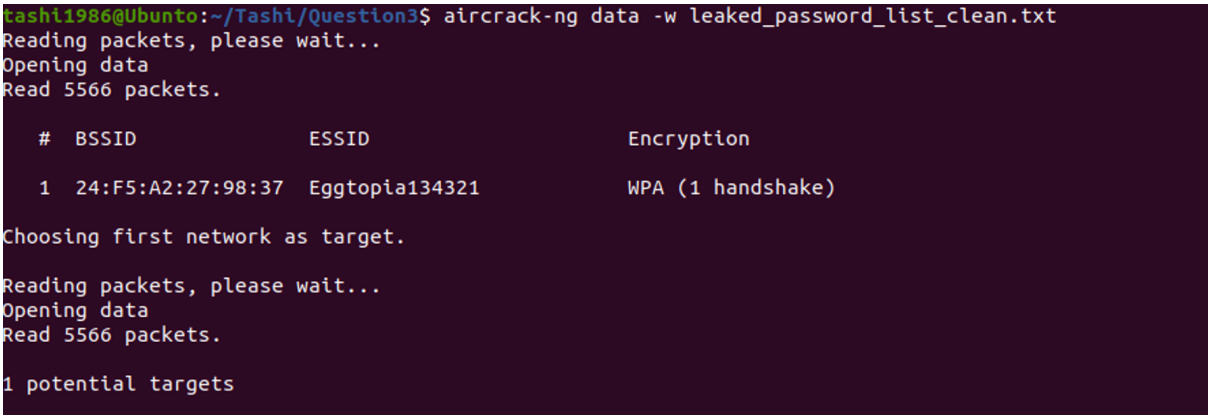
I have aircrack-ng already installed:

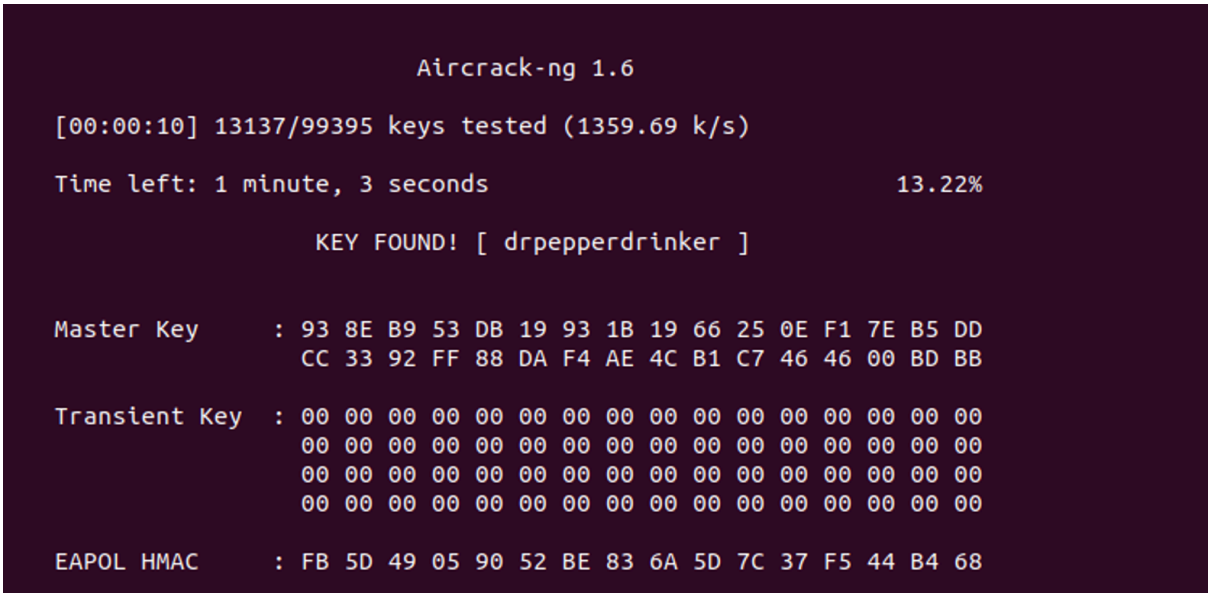


To decrypt use the below command:

You will need to untar the secretarchive.tar.bz2 file and will get the file ‘data’ as below:







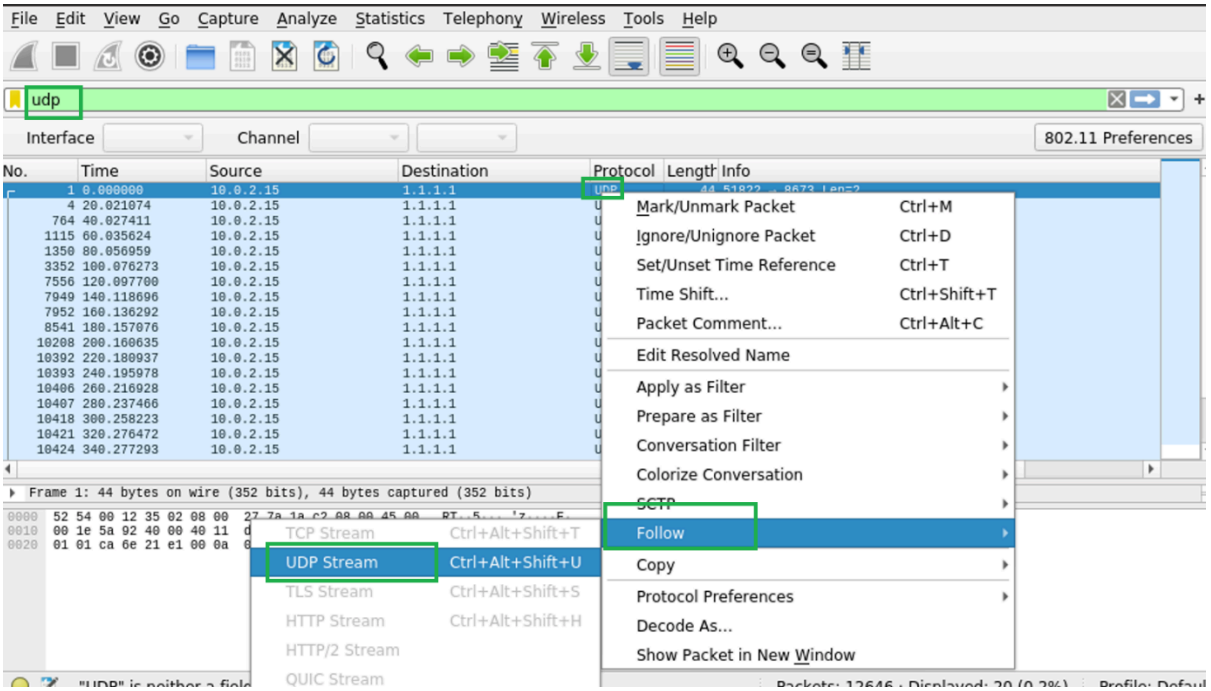
Question 4:

```
tashi1986@Ubunto:~/Tashi/Question4$ wget https://github.com/SCH-IT-MurdochUni/NetworkingLabs/raw/refs/hea
ds/main/Reusable_Learning_Objects/.test/.misc/2987.pcap.enc
--2025-10-23 00:05:16--  https://github.com/SCH-IT-MurdochUni/NetworkingLabs/raw/refs/heads/main/Reusable
_Learning_Objects/.test/.misc/2987.pcap.enc
Resolving github.com (github.com)... 4.237.22.38, 2405:dc00:0:3::4ed:1626
Connecting to github.com (github.com)|4.237.22.38|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/SCH-IT-MurdochUni/NetworkingLabs/refs/heads/main/Reusable_Lea
rning_Objects/.test/.misc/2987.pcap.enc [following]
--2025-10-23 00:05:17--  https://raw.githubusercontent.com/SCH-IT-MurdochUni/NetworkingLabs/refs/heads/ma
in/Reusable_Learning_Objects/.test/.misc/2987.pcap.enc
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.
199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13430768 (13M) [application/octet-stream]
Saving to: '2987.pcap.enc'

2987.pcap.enc              100%[===================================>]  12.81M  10.8MB/s    in 1.2s

2025-10-23 00:05:19 (10.8 MB/s) - '2987.pcap.enc' saved [13430768/13430768]
```

```
tashi1986@Ubunto:~/Tashi/Question4$ sudo openssl enc -d -aes-256-cbc -in 2987.pcap.enc -out 2987.pcap.enc
.tar.bz2 -k '9Edoo!Hib9dl'
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
tashi1986@Ubunto:~/Tashi/Question4$ ls -lrt
total 26232
-rw-rw-r-- 1 tashi1986 tashi1986 13430768 Oct 23 00:05 2987.pcap.enc
-rw-r--r-- 1 root      root      13430750 Oct 23 00:08 2987.pcap.enc.tar.bz2
tashi1986@Ubunto:~/Tashi/Question4$
```

Sudo wireshark 2987.pcap.enc.tar.bz2

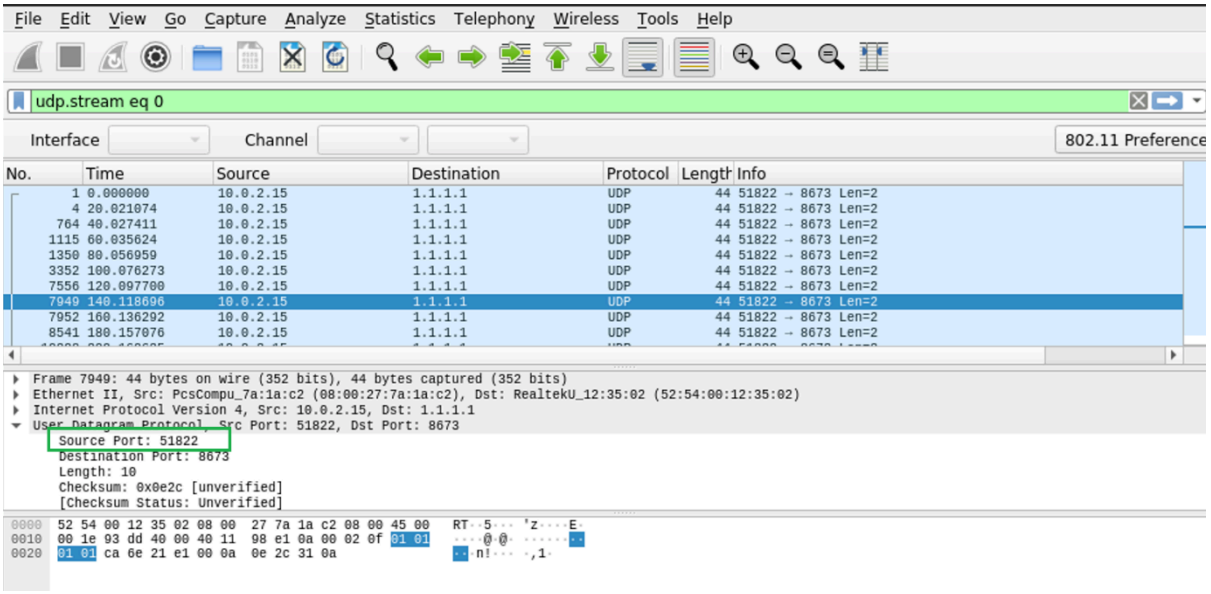
In wireshark filter it with UDP right click in UDP under Protocol field Follow UDP Stream



Enter the contents of the flag. Enter as a string of ascii chars only, no spaces or newlines.

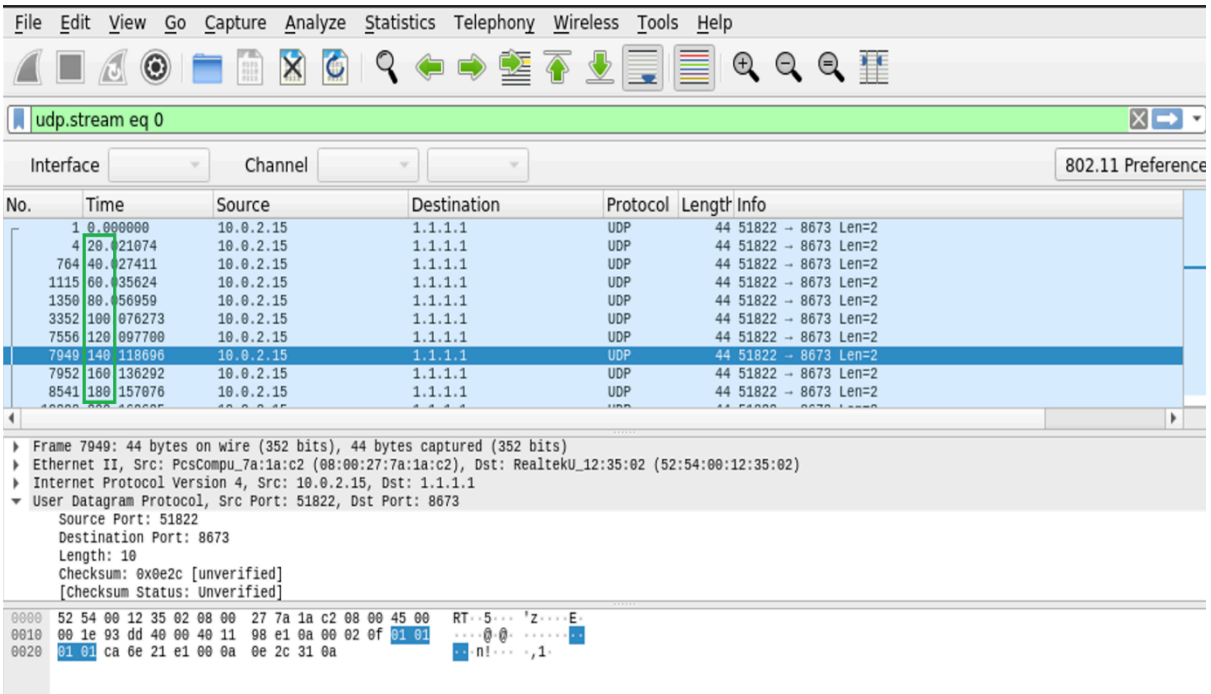
Answer: 10gQAZ%qgXX5

What is the source port in use to send this message:



Ans: port is 51822

There is a consistent time delay between messages, from the perspective of the packet capture, what is the delay between each of these messages:



Answer: 20

We can see hat the time difference between the each record is 20 and hence answer is 20