

Question 1:

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

```
tashi1986@Ubuntu:~/Tashi$ ls -lrt
total 4
drwxrwxr-x 2 tashi1986 tashi1986 4096 Oct 22 00:07 Question1
tashi1986@Ubuntu:~/Tashi$
```

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

```
tashi1986@Ubuntu:~/Tashi/Question1$ sudo wget https://github.com/SCH-IT-MurdochUni/NetworkingLabs/raw/refs/heads/main/Reusable_Learning_Objects/.test/.misc/lab_red.pcap.enc
[sudo] password for tashi1986:
Sorry, try again.
[sudo] password for tashi1986:
--2025-10-22 00:17:52-- https://github.com/SCH-IT-MurdochUni/NetworkingLabs/raw/refs/heads/main/Reusable_Learning_Objects/.test/.misc/lab_red.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_Learning_Objects/.test/.misc/lab_red.pcap.enc [following]
--2025-10-22 00:17:53-- https://raw.githubusercontent.com/SCH-IT-MurdochUni/NetworkingLabs/refs/heads/main/Reusable_Learning_Objects/.test/.misc/lab_red.pcap.enc
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.110.133, 185.199.111.133, 185.199.108.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.110.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 68880 (67K) [application/octet-stream]
Saving to: 'lab_red.pcap.enc'

lab_red.pcap.enc      100%[=====] 67.27K --KB/s    in 0.03s

2025-10-22 00:17:53 (2.35 MB/s) - 'lab_red.pcap.enc' saved [68880/68880]
```

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

```
tashi1986@Ubuntu:~/Tashi/Question1$ ls -lrt
total 68
-rw-r--r-- 1 root root 68880 Oct 22 00:17 lab_red.pcap.enc
tashi1986@Ubuntu:~/Tashi/Question1$
```

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:

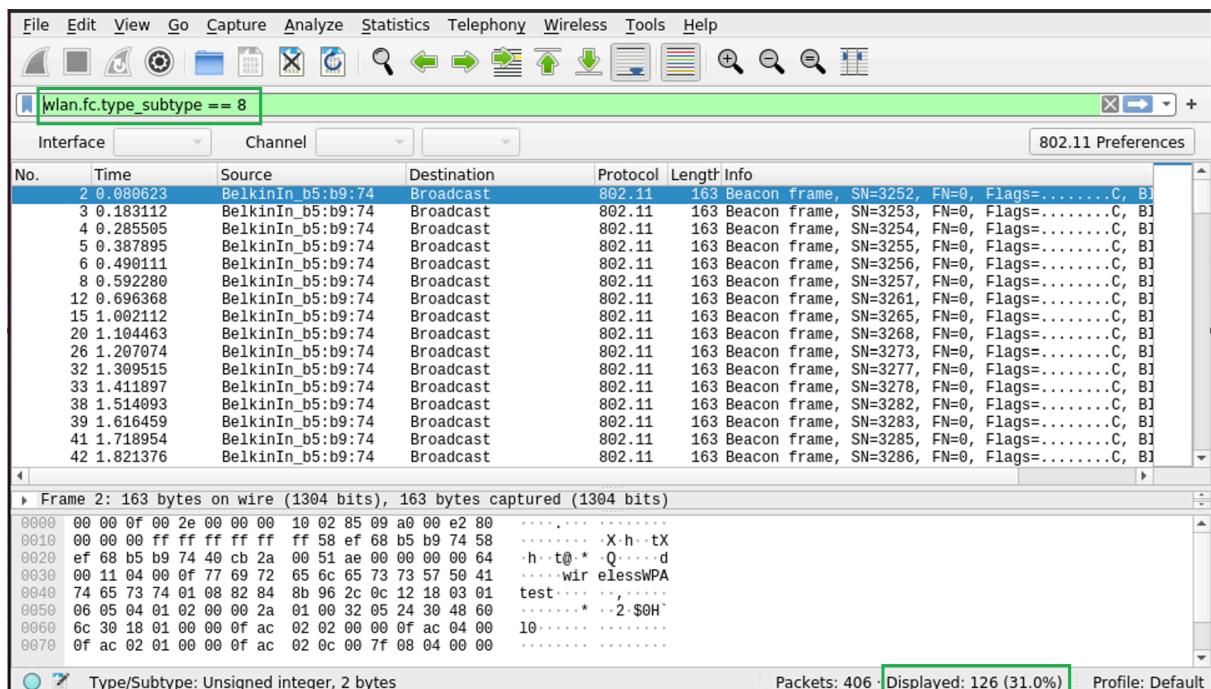
```
tashi1986@Ubuntu:~/Tashi/Question1$ sudo openssl enc -d -aes-256-cbc -in lab_red.pcap.enc -out lab_red.pcap.enc.tar.bz2 -k '2aT9134fnBwC$'  
*** WARNING : deprecated key derivation used.  
Using -iter or -pbkdf2 would be better.  
tashi1986@Ubuntu:~/Tashi/Question1$ ls -lrt  
total 136  
-rw-r--r--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

wlan.fc.type_subtype == 8						
	Interface	Channel	Protocol	Length	Info	802.11 Preferences
	Source	Destination	Protocol	Length	Info	
3	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3292, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
2	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3253, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
5	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3254, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
5	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3255, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
1	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3256, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
8	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3261, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
2	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3265, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
3	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3268, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
4	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3273, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
5	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3277, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
7	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3278, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
3	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3282, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
9	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3283, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
4	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3285, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
6	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3286, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
7	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3287, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
7	BelkinIn_b5:b9:74	Broadcast	802.11	163	Beacon frame, SN=3288, FN=0, Flags=.....C, BI=100, SSID=wirelessWPATest	
9	BelkinIn_h5:h9:74	Broadcast	802.11	163	Beacon frame, SN=3289, FN=0, Flags=.....C, BI=100, SSID=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:

```
tashi1986@Ubuntu:~/Tashi$ cd Question2
tashi1986@Ubuntu:~/Tashi/Question2$ sudo wget https://github.com/SCH-IT-MurdochUni/NetworkingLabs/raw/refs/heads/main/Reusable_Learning_Objects/.test/.misc/pp.tar.bz2.enc
--2025-10-22 00:47:09-- https://github.com/SCH-IT-MurdochUni/NetworkingLabs/raw/refs/heads/main/Reusable_Learning_Objects/.test/.misc/pp.tar.bz2.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_Learning_Objects/.test/.misc/pp.tar.bz2.enc [following]
--2025-10-22 00:47:09-- https://raw.githubusercontent.com/SCH-IT-MurdochUni/NetworkingLabs/refs/heads/main/Reusable_Learning_Objects/.test/.misc/pp.tar.bz2.enc
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.108.133, 185.199.111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 39268304 (37M) [application/octet-stream]
Saving to: 'pp.tar.bz2.enc'

pp.tar.bz2.enc          100%[=====] 37.45M  6.75MB/s   in 6.0s

2025-10-22 00:47:16 (6.24 MB/s) - 'pp.tar.bz2.enc' saved [39268304/39268304]

tashi1986@Ubuntu:~/Tashi/Question2$ ls -lrt
total 38348
-rw-r--r-- 1 root root 39268304 Oct 22 00:47 pp.tar.bz2.enc
tashi1986@Ubuntu:~/Tashi/Question2$
```

Decrypt the file:

Sudo openssl enc -d -aes-256-cbc -in pp.tar.bz2.enc -out pp.tar.bz2.enc.tar.bz2 -k
'1&&jbj07B2za'

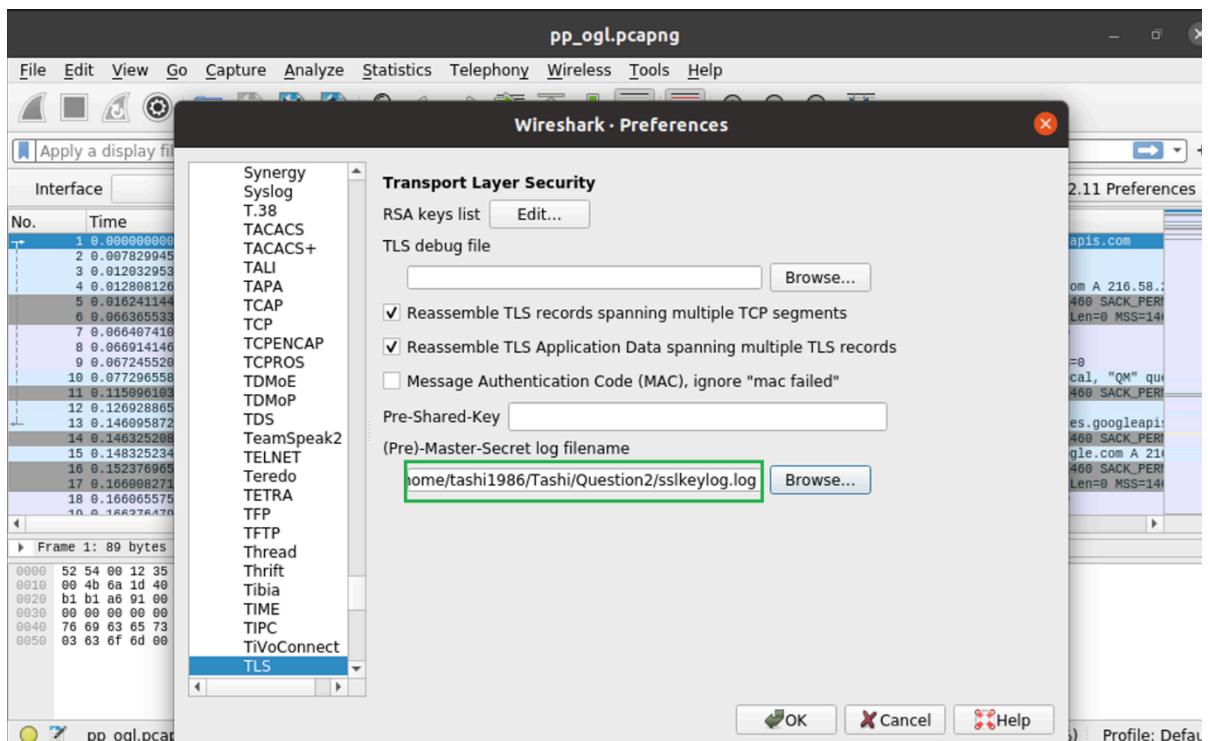
```
tashi1986@Ubuntu:~/Tashi/Question2$ sudo openssl enc -d -aes-256-cbc -in pp.tar.bz2.enc -out pp.tar.bz2.enc.tar.bz2 -k '1&&jbj07B2za'
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
tashi1986@Ubuntu:~/Tashi/Question2$ ls -lrt
total 76696
-rw-r--r-- 1 root root 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@Ubuntu:~/Tashi/Question2$
```

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@Ubuntu:~/Tashi/Question2$ tar -xvf pp.tar.bz2.enc.tar.bz2
pp_ogl.pcapng
sslkeylog.log
tashi1986@Ubuntu:~/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@Ubuntu:~/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.

Wireshark - Export - HTTP object list

Packet	Hostname	Content Type	Size	Filename
25441	www.cnty.com	image/jpeg	9,661 kB	640x440 HARLEY.jpg
25630	www.cnty.com	image/jpeg	9,444 kB	640x440 DRIVE.jpg
13040	www.cnty.com	text/css	600 kB	merged-b0c1bcf7aebbf67a
7247	code.jquery.com	application/javascript	520 kB	jquery-ui.js
16240	www.cnty.com	image/jpeg	483 kB	1920X1280_HOME_PG_SLO
14872	www.cnty.com	image/jpeg	396 kB	640x440_HALF_CENT_MONI
17091	www.cnty.com	image/jpeg	388 kB	exterior_V3.jpg
16214	www.cnty.com	image/jpeg	330 kB	1920X1280_HOME_PG_HOT
26580	www.outdoorgearlab.com	text/html	315 kB	/
26771	www.outdoorgearlab.com	text/html	294 kB	search?ftr=Flag%7Bd342a3
13724	www.cnty.com	application/javascript	287 kB	plugins-58e2cc18bb982212
14496	www.cnty.com	image/jpeg	260 kB	640x440_EVENTS_BB.jpg
15520	www.cnty.com	image/jpeg	259 kB	600X400_CALENDAR_ICON
14822	www.cnty.com	image/jpeg	231 kB	640x440_EVENTS_BINGO.jp
9599	res.windsurfercrs.com	image/jpeg	176 kB	MagnusonGrandPikesPeakKR
6532	res.windsurfercrs.com	image/jpeg	172 kB	MagnusonGrandPikesPeakC
6532	res.windsurfercrs.com	image/jpeg	166 kB	MagnusonGrandPikesPeakG
6533	res.windsurfercrs.com	image/jpeg	152 kB	MagnusonGrandPikesPeakC
6577	res.windsurfercrs.com	image/jpeg	152 kB	MagnusonGrandPikesPeakK
9893	res.windsurfercrs.com	image/jpeg	137 kB	EXTERIOR_500X5001.jpg
17646	www.cnty.com	application/javascript	114 kB	functions-28ef052b0dcf1b1
13552	www.cnty.com	application/javascript	102 kB	bootstrap-datepicker-099a7
13425	www.cnty.com	application/javascript	95 kB	jquery-26f989abd38f94957
13551	www.cnty.com	application/font-woff2	77 kB	fontawesome-webfont.woff
13680	www.cnty.com	image/jpeg	65 kB	csm_CAS_FLOOR_3_6d1024
17951	www.cnty.com	image/jpeg	61 kB	csm_CAS_FLOOR_2_8a9af5
17194	www.cnty.com	text/html	49 kB	cripple-creek
12887	www.cnty.com			

Frame Filter:

Frame (551 b)

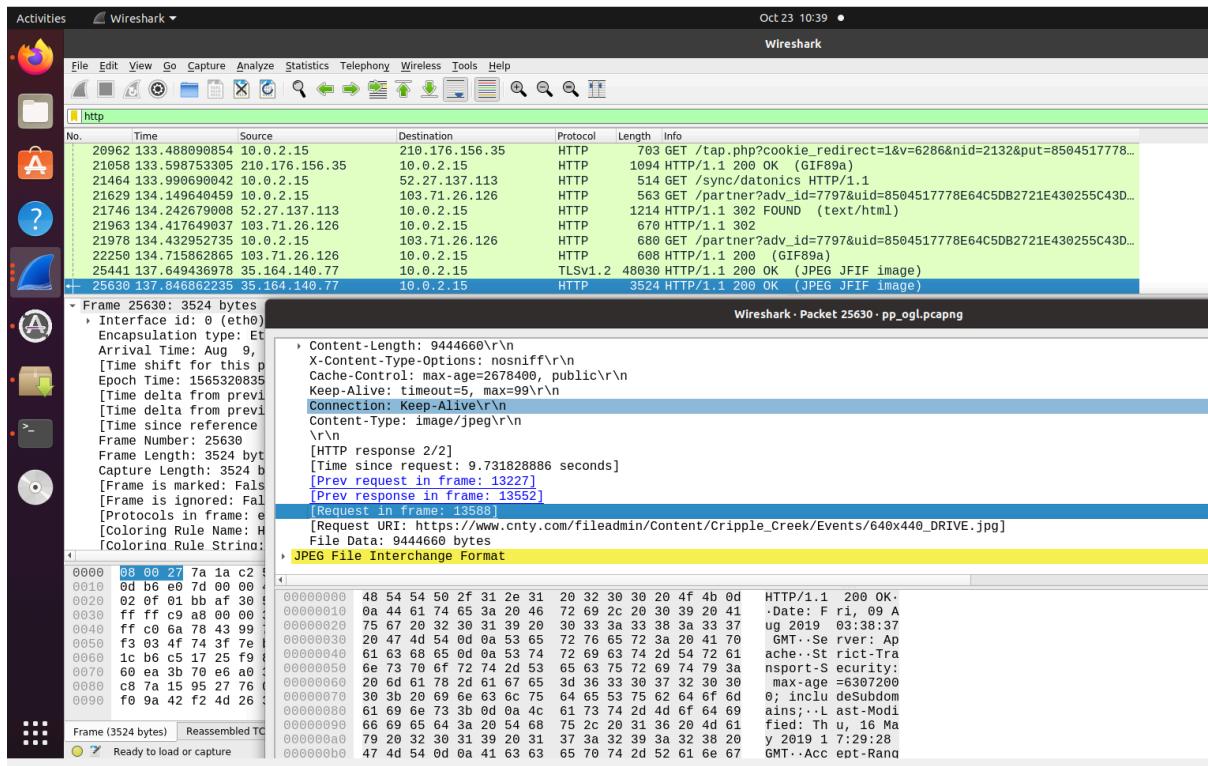
Save Save All Close Help

In ubuntu, open the saved image from desktop 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:

```
tashi1986@Ubuntu:~/Tashi/Question3$ sudo wget https://github.com/SCH-IT-MurdochUni/NetworkingLabs/raw/refs/heads/main/Reusable_Learning_Objects/.test/.misc/eggtopia_anon_practice.pcap.bz2.enc
--2025-10-22 23:10:28-- https://github.com/SCH-IT-MurdochUni/NetworkingLabs/raw/refs/heads/main/Reusable_Learning_Objects/.test/.misc/eggtopia_anon_practice.pcap.bz2.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_Learning_Objects/.test/.misc/eggtopia_anon_practice.pcap.bz2.enc [following]
--2025-10-22 23:10:29-- https://raw.githubusercontent.com/SCH-IT-MurdochUni/NetworkingLabs/refs/heads/main/Reusable_Learning_Objects/.test/.misc/eggtopia_anon_practice.pcap.bz2.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: 1073792 (1.0M) [application/octet-stream]
Saving to: 'eggtopia_anon_practice.pcap.bz2'

eggtopia_anon_practice.pcap 100%[=====] 1.02M 3.05MB/s in 0.3s

2025-10-22 23:10:30 (3.05 MB/s) - 'eggtopia_anon_practice.pcap.bz2' saved [1073792/1073792]
```

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@Ubuntu:~/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@Ubuntu:~/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@Ubuntu:~/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@Ubuntu:~/Tashi/Question3$ sudo wget https://raw.githubusercontent.com/SCH-IT-MurdochUni/NetworkingLabs/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/main/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@Ubuntu:~/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@Ubuntu:~/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:

```
tashi1986@Ubuntu: ~/Tashi/Question3$ sudo apt-get install aircrack-ng
Reading package lists... Done
Building dependency tree
Reading state information... Done
aircrack-ng is already the newest version (1:1.6-4).
0 to upgrade, 0 to newly install, 0 to remove and 0 not to upgrade.
tashi1986@Ubuntu:~/Tashi/Question3$
```

To decrypt use the below command:

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

```
tashi1986@Ubuntu:~/Tashi/Question3$ ls -lrt
total 4444
-rw-rw-r-- 1 tashi1986 tashi1986 1073792 Oct 22 23:37 eggtopia_anon_practice.pcap.bz2.enc
-rw-r--r-- 1 root      root      776784 Oct 22 23:44 leaked_password_list_clean.txt
-rw-r--r-- 1 root      root      1073768 Oct 23 00:32 secretarchive.tar.bz2
-rw-r--r-- 1 tashi1986 tashi1986 1614864 Oct 23 08:35 data
```

```
tashi1986@Ubuntu:~/Tashi/Question3$ aircrack-ng data -w leaked_password_list_clean.txt
Reading packets, please wait...
Opening data
Read 5566 packets.

#   BSSID           ESSID           Encryption
 1  24:F5:A2:27:98:37  Eggtopia134321          WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening data
Read 5566 packets.

1 potential targets
```

```
Aircrack-ng 1.6

[00:00:10] 13137/99395 keys tested (1359.69 k/s)

Time left: 1 minute, 3 seconds          13.22%

KEY FOUND! [ drpepperdrinker ]

Master Key      : 93 8E B9 53 DB 19 93 1B 19 66 25 0E F1 7E B5 DD
                  CC 33 92 FF 88 DA F4 AE 4C B1 C7 46 46 00 BD BB

Transient Key   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : FB 5D 49 05 90 52 BE 83 6A 5D 7C 37 F5 44 B4 68
```

Question 4:

```
tashi1986@Ubuntu:~/Tashi/Question4$ wget https://github.com/SCH-IT-MurdochUni/NetworkingLabs/raw/refs/heads/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/raw/refs/heads/main/Reusable_Learning_Objects/.test/.misc/2987.pcap.enc [following]
--2025-10-23 00:05:17-- https://raw.githubusercontent.com/SCH-IT-MurdochUni/NetworkingLabs/raw/refs/heads/main/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'

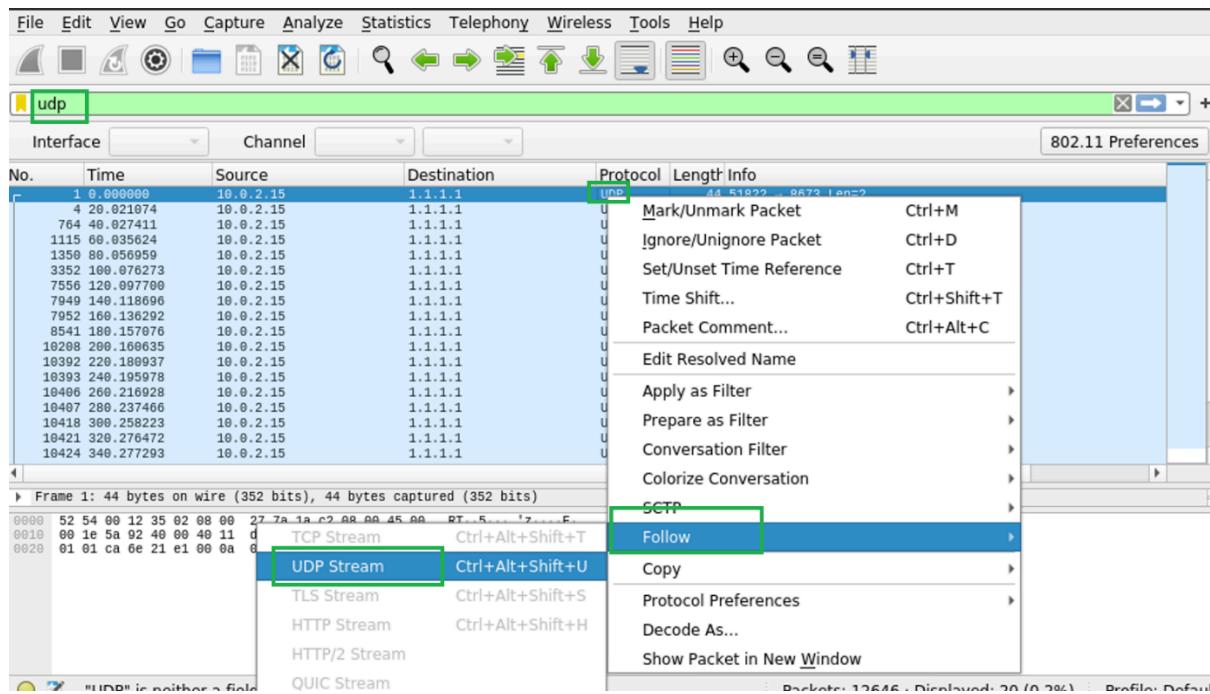
2987.pcap.enc          100%[=====] 12.81M 10.8MB/s   in 1.2s

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

```
tashi1986@Ubuntu:~/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@Ubuntu:~/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@Ubuntu:~/Tashi/Question4$
```

Sudo wireshark 2987.pcap.enc.tar.bz2

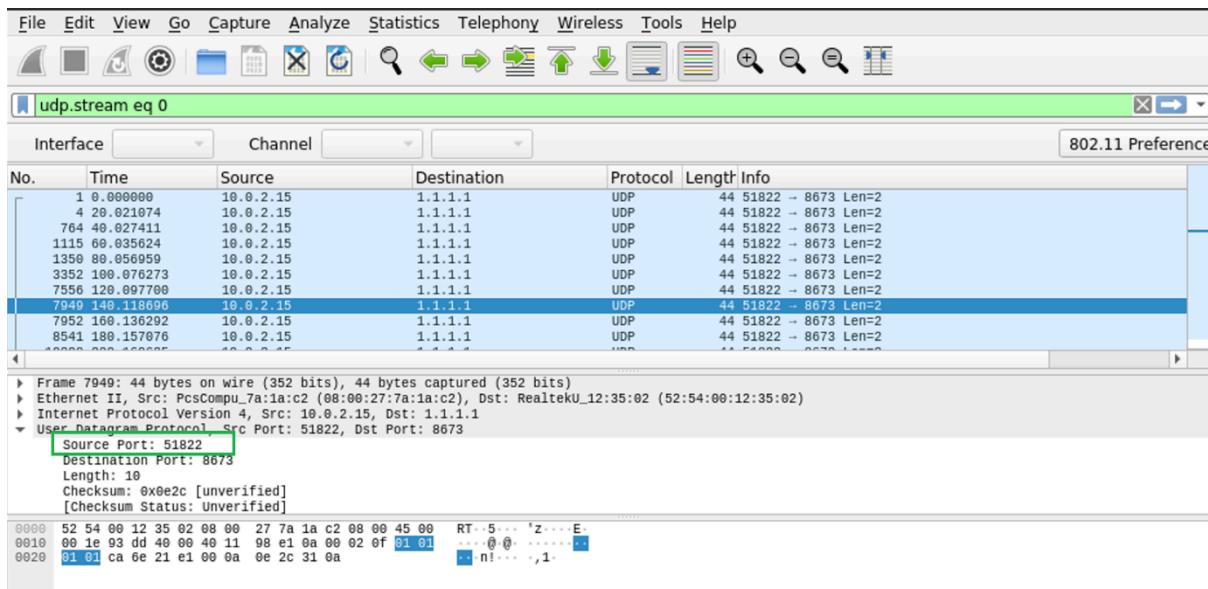
In wireshark filter it with UDP right click in UDP under Protocol field Follow UDP Stream



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

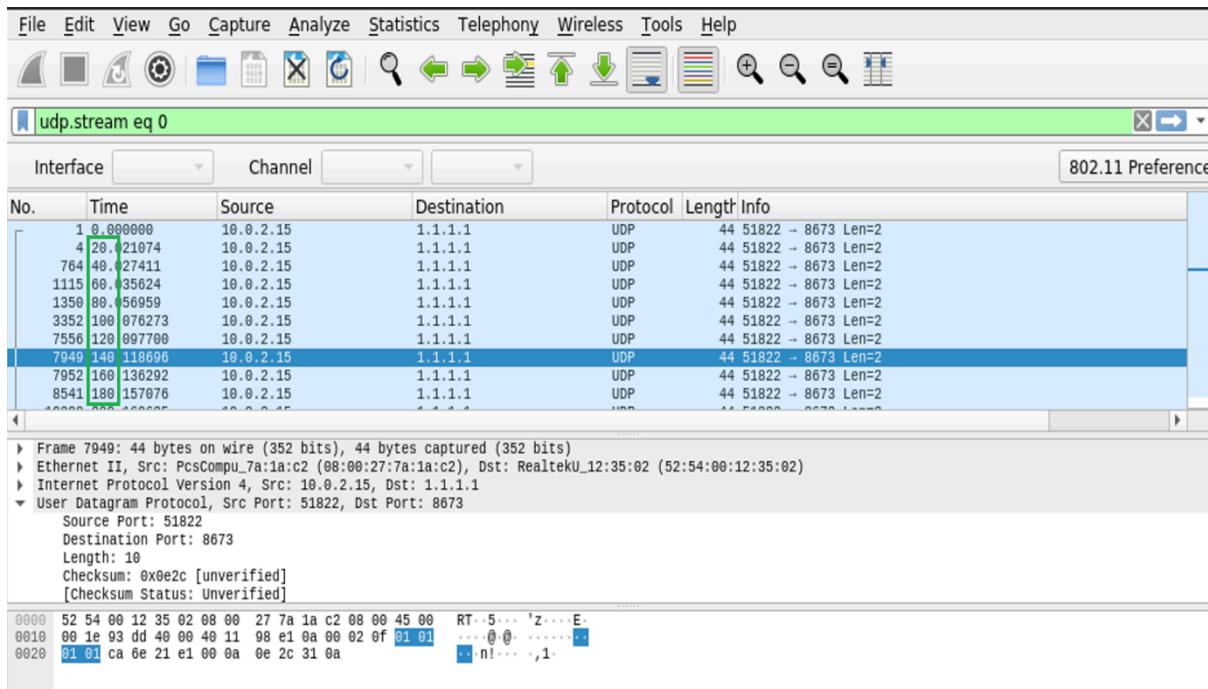
Answer: 10gQAZ%qgXX5

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