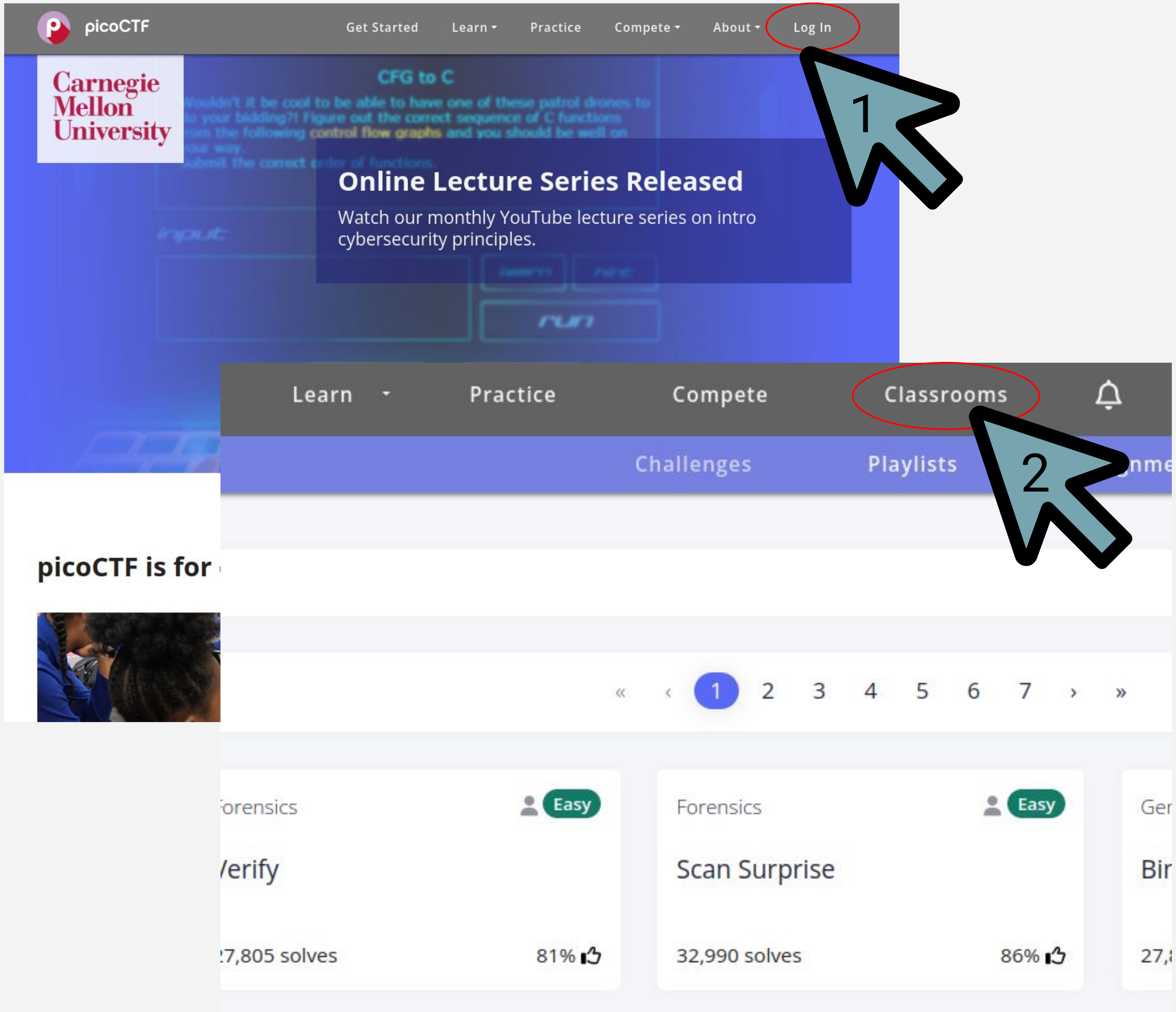
Introduction to Forensics

Today we’ll use:

→ https://picoctf.org/ Code: **CleCz0nr1**

→ https://wireshark.org/



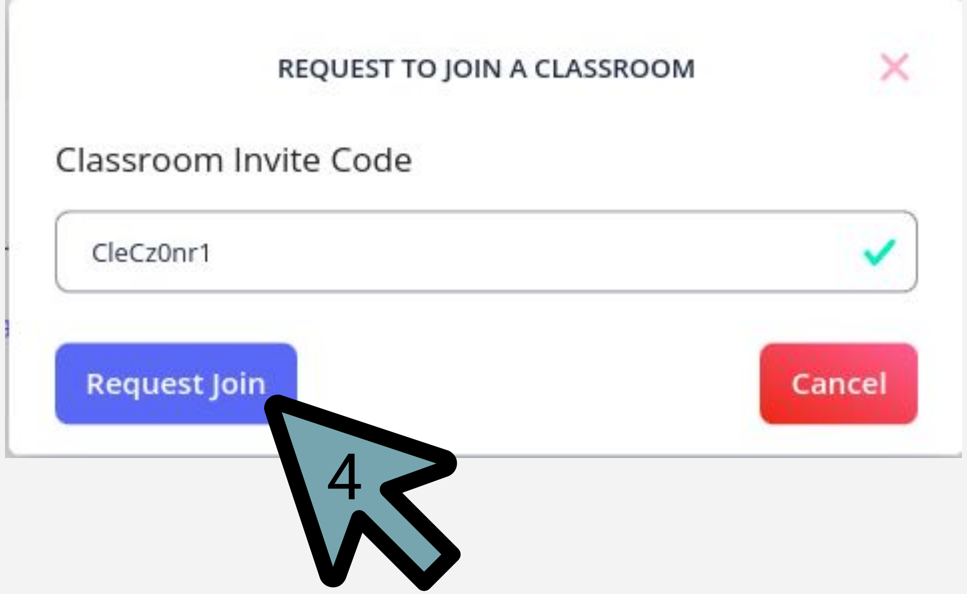
Carnegie Mellon University

Online Lecture Series Released

Watch our monthly YouTube lecture series on intro cybersecurity principles.

picoCTF is for

orensics Easy	Forensics Easy	Ger
/erify	Scan Surprise	Bir
ː7,805 solves 81%	32,990 solves 86%	27,

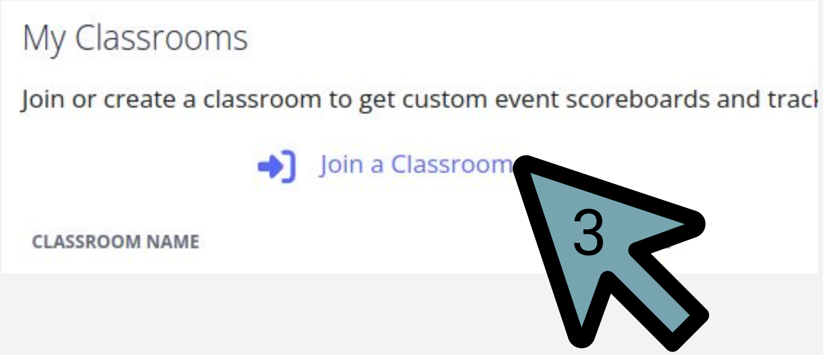


REQUEST TO JOIN A CLASSROOM

Classroom Invite Code

CleCz0nr1 ✓

Request Join   Cancel



My Classrooms

Join or create a classroom to get custom event scoreboards and tracl

Join a Classroom

CLASSROOM NAME

What is Forensics ?

Forensic science (wiki)

Forensic science is the application of science principles and methods to support legal decision-making in matters of criminal and civil law.

What is Cybersecurity Forensics ?

Cybersecurity Forensics

Cybersecurity Forensics focuses on gathering evidence present in **computer devices** that hold information electronically.

Types of Digital Evidence

- Internet Browsing History
- Log Files
- **Network Traffic**
- Cloud Storage Data
- IoT Device Data

Hackers find weaknesses in the computer world. In a dictionary, we can find two related definitions:

- An expert at programming and solving problems with a computer
- A person who illegally gains access to and sometimes tampers with information in a computer system

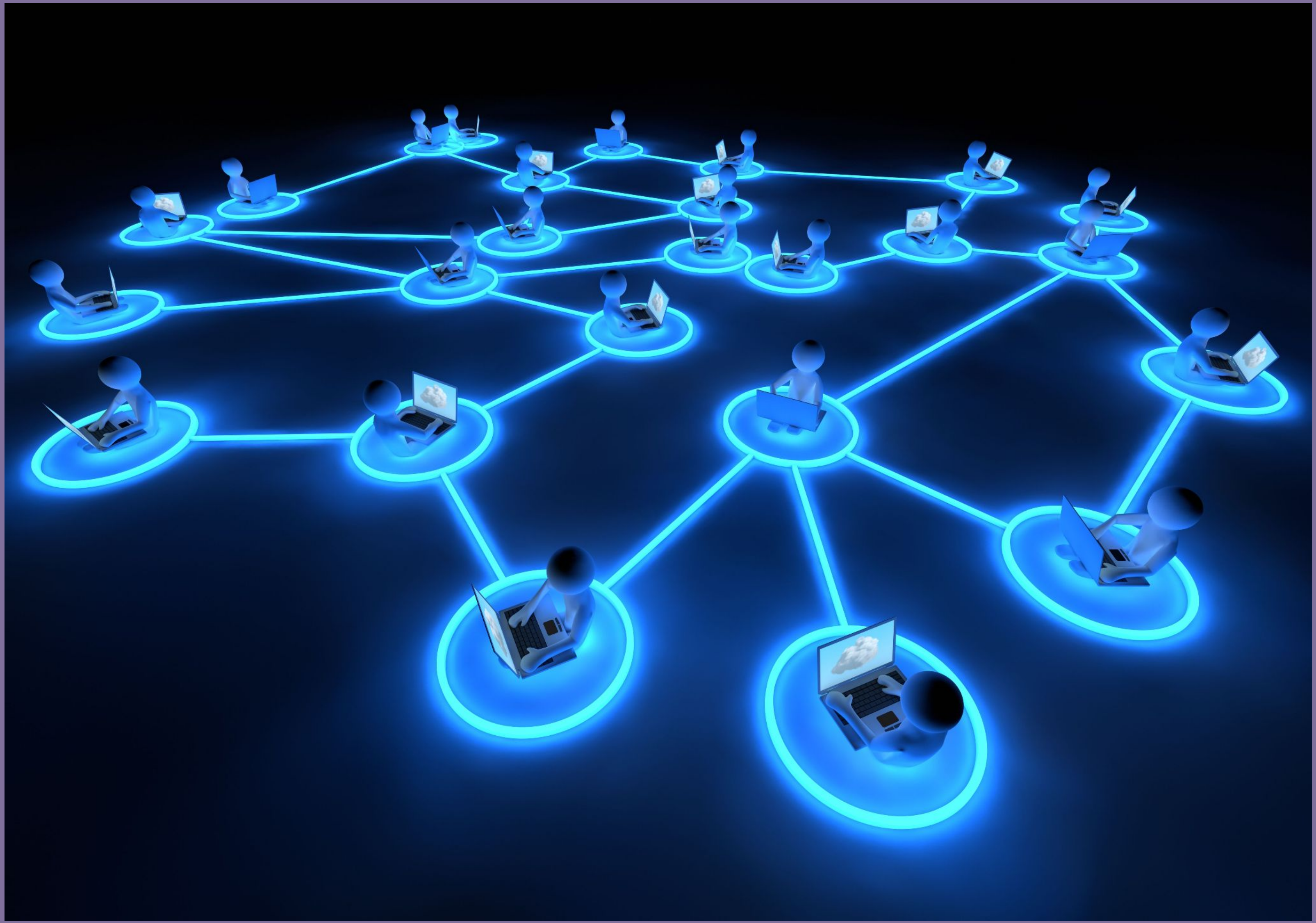
CTF (capture the flag)

- Competitions (cybersecurity challenges)
- Designed to test participants' skills
- Individuals or teams solve problems to find "flags," which are pieces of data that demonstrate successful exploitation or defense techniques.

Network Traffic

Network

A collection of interconnected devices that can communicate with each other to share resources, data, and services.



Packet or network analysis

This field of forensics concerns itself with understanding what has happened on a network through the examination of captured packets.

Packet

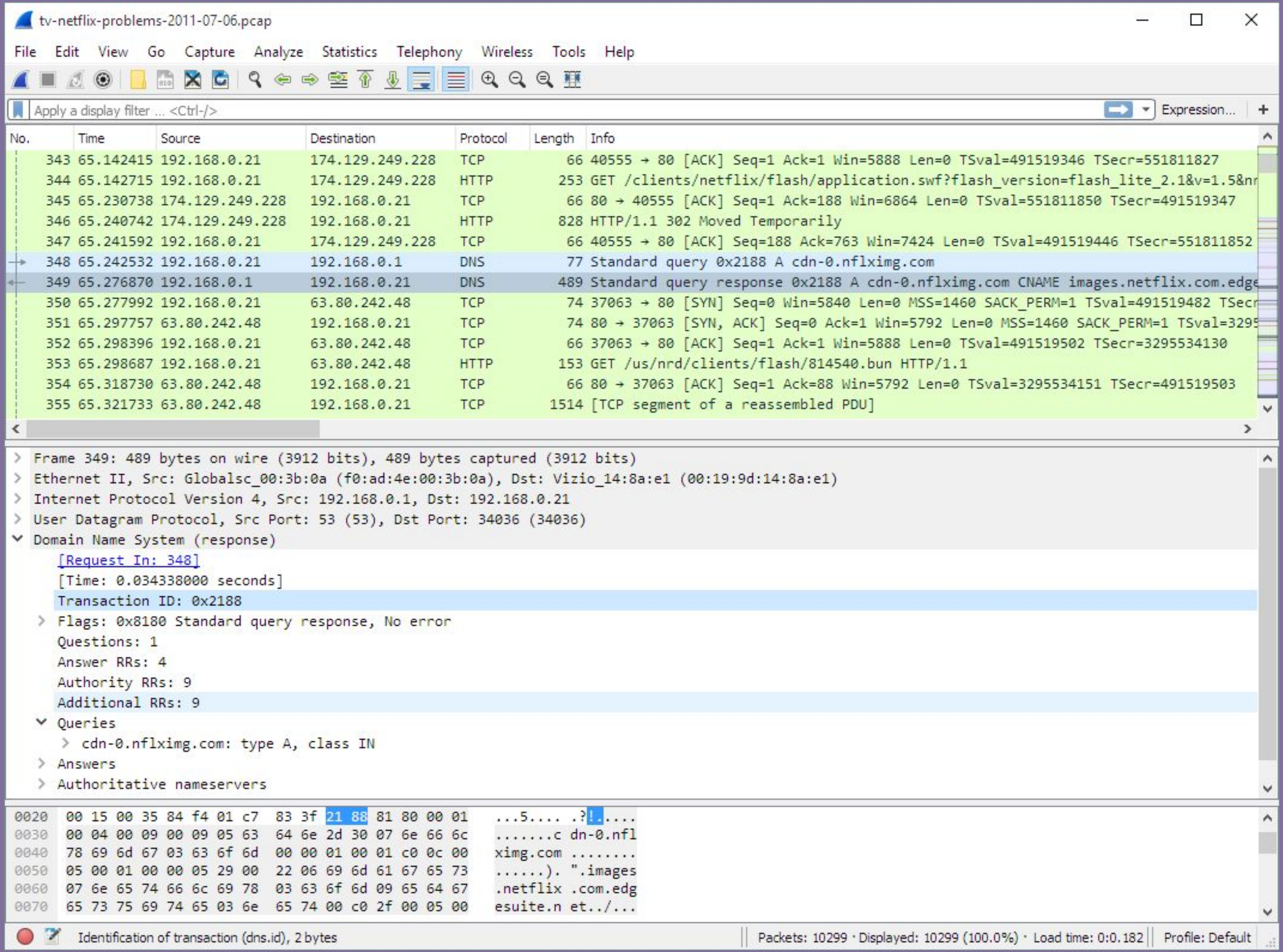
A basic unit of data that's grouped together and transferred over a computer network, typically a packet-switched network, such as the internet.

Wireshark

+

What Is Wireshark ?

Wireshark will help you **capture network packets** and display them at a granular level. It’s a software tool used to monitor the network traffic through a network interface.



```
No.   Time      Source          Destination     Protocol Length Info
  343 65.142415 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
  344 65.142715 192.168.0.21    174.129.249.228 HTTP      253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
  345 65.230738 174.129.249.228 192.168.0.21    TCP        66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
  346 65.240742 174.129.249.228 192.168.0.21    HTTP      828 HTTP/1.1 302 Moved Temporarily
  347 65.241592 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
  348 65.242532 192.168.0.21    192.168.0.1     DNS        77 Standard query 0x2188 A cdn-0.nflximg.com
  349 65.276870 192.168.0.1     192.168.0.21    DNS       489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
  350 65.277992 192.168.0.21    63.80.242.48    TCP        74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
  351 65.297757 63.80.242.48    192.168.0.21    TCP        74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
  352 65.298396 192.168.0.21    63.80.242.48    TCP        66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
  353 65.298687 192.168.0.21    63.80.242.48    HTTP      153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
  354 65.318730 63.80.242.48    192.168.0.21    TCP        66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
  355 65.321733 63.80.242.48    192.168.0.21    TCP      1514 [TCP segment of a reassembled PDU]
```

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

Identification of transaction (dns.id), 2 bytes

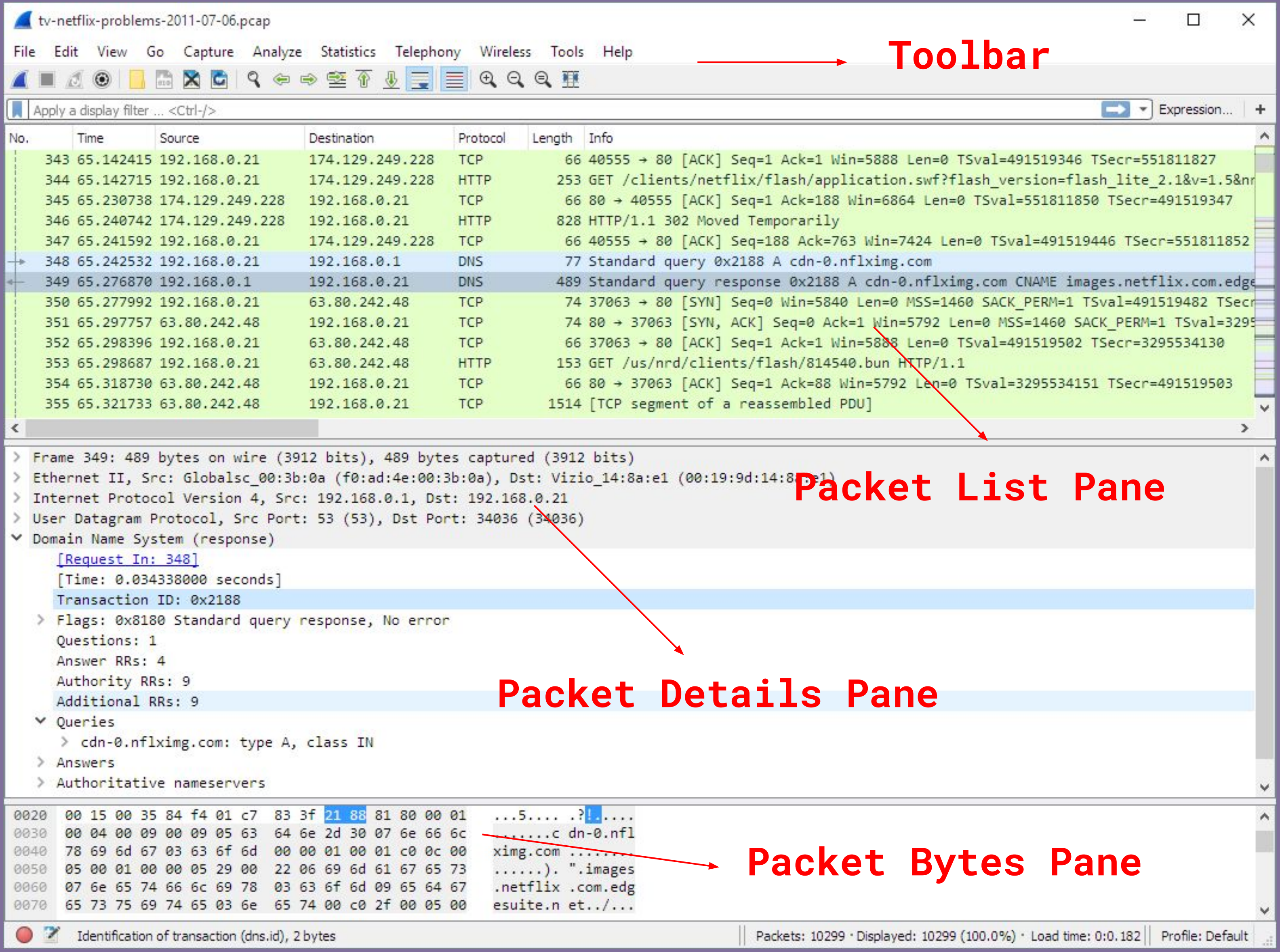
Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default

What is a PCAP file ?

What is a PCAP file ?

PCAP (packet capture) is an application programming interface (API) for capturing network traffic.

- .pcap is a file extension for packet captures
- A 100MB PCAP file contains tens of thousands of packets



Toolbar

```
No.   Time      Source          Destination     Protocol Length Info
  343 65.142415 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
  344 65.142715 192.168.0.21    174.129.249.228 HTTP      253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
  345 65.230738 174.129.249.228 192.168.0.21    TCP        66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
  346 65.240742 174.129.249.228 192.168.0.21    HTTP      828 HTTP/1.1 302 Moved Temporarily
  347 65.241592 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
  348 65.242532 192.168.0.21    192.168.0.1     DNS        77 Standard query 0x2188 A cdn-0.nflximg.com
  349 65.276870 192.168.0.1     192.168.0.21    DNS       489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
  350 65.277992 192.168.0.21    63.80.242.48    TCP        74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
  351 65.297757 63.80.242.48    192.168.0.21    TCP        74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
  352 65.298396 192.168.0.21    63.80.242.48    TCP        66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
  353 65.298687 192.168.0.21    63.80.242.48    HTTP      153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
  354 65.318730 63.80.242.48    192.168.0.21    TCP        66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
  355 65.321733 63.80.242.48    192.168.0.21    TCP      1514 [TCP segment of a reassembled PDU]
```

Packet List Pane

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

Packet Details Pane

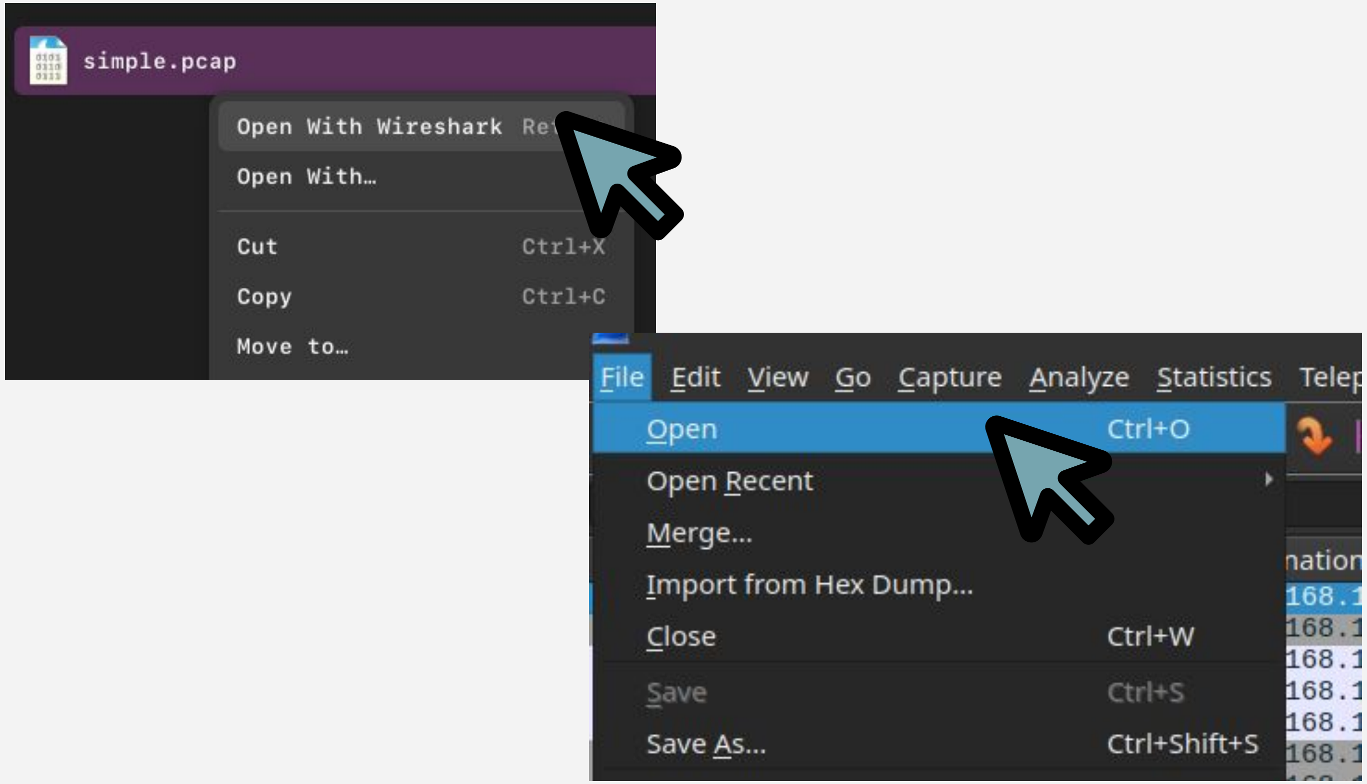
```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

Packet Bytes Pane

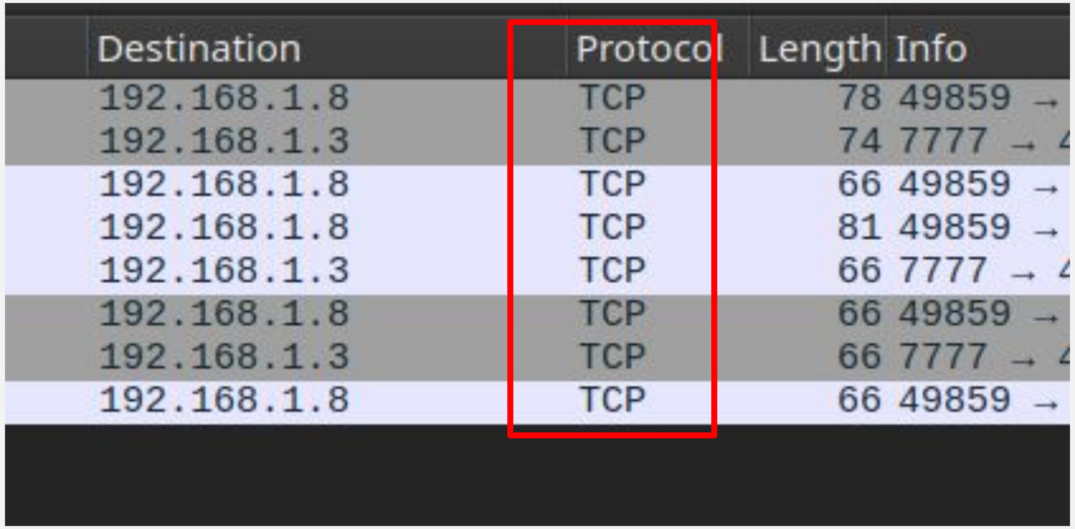
Identification of transaction (dns.id), 2 bytes | Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default

Exercise 1

1. Download: https://github.com/ieee-unipi-sb/Ethical-Hacking/tree/main/Workshop%201%20-%20Network%20Forensics/.pcap%20files
2. What protocol is most frequently used in this capture ?
3. What is the source/destination IP address ?
4. How many packets were captured in total ?
5. What is the size of the largest packet in this capture?

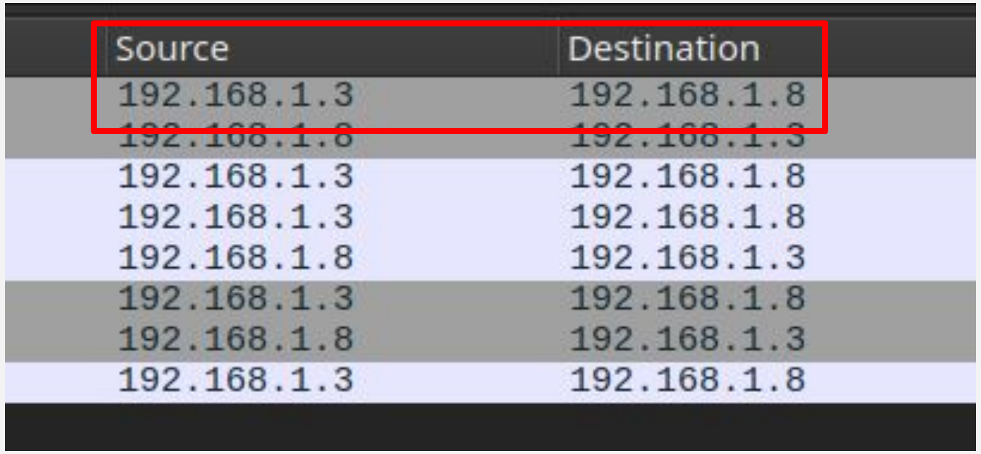


What networking protocol is used ?



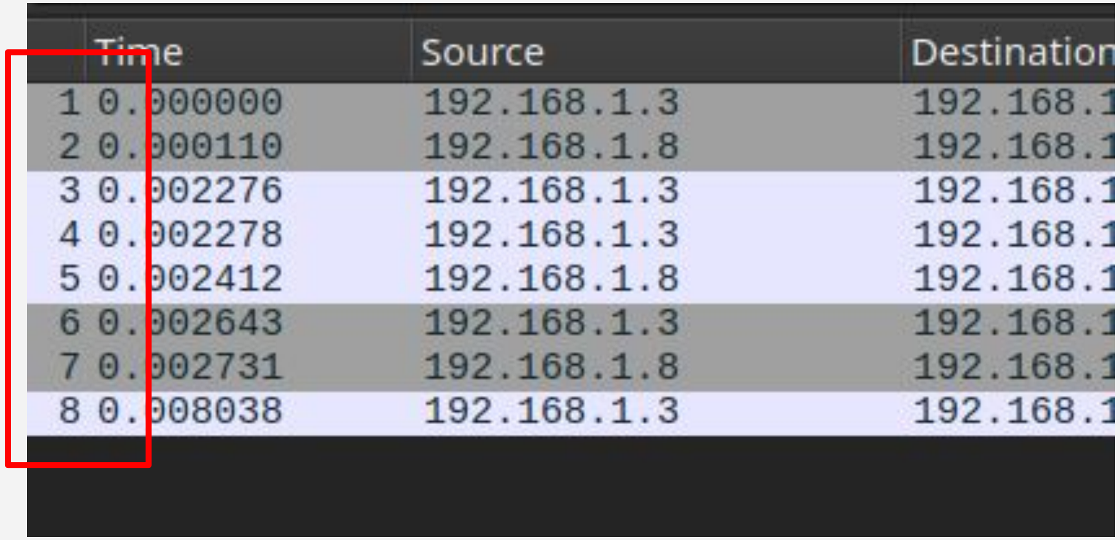
Destination	Protocol	Length	Info
192.168.1.8	TCP	78	49859 →
192.168.1.3	TCP	74	7777 → 4
192.168.1.8	TCP	66	49859 →
192.168.1.8	TCP	81	49859 →
192.168.1.3	TCP	66	7777 → 4
192.168.1.8	TCP	66	49859 →
192.168.1.3	TCP	66	7777 → 4
192.168.1.8	TCP	66	49859 →

What is the source/destination IP address ?



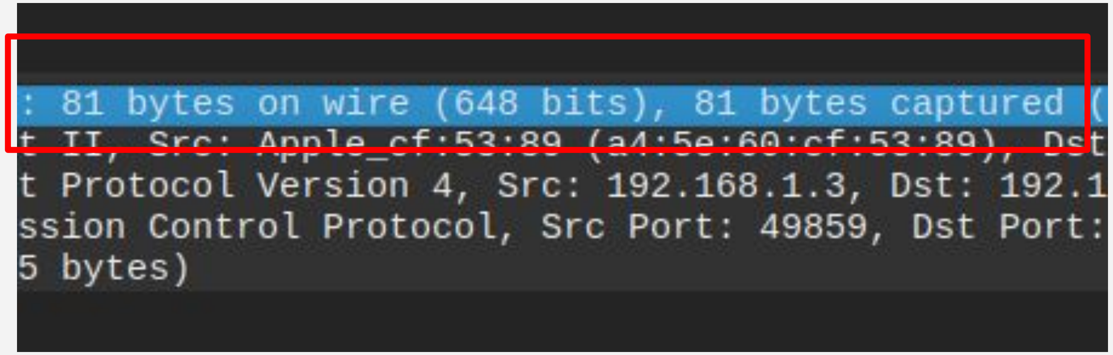
Source	Destination
192.168.1.3	192.168.1.8
192.168.1.8	192.168.1.3
192.168.1.3	192.168.1.8
192.168.1.3	192.168.1.8
192.168.1.8	192.168.1.3
192.168.1.3	192.168.1.8
192.168.1.8	192.168.1.3
192.168.1.3	192.168.1.8

How many packets are there ?



	Time	Source	Destination
1	0.000000	192.168.1.3	192.168.1
2	0.000110	192.168.1.8	192.168.1
3	0.002276	192.168.1.3	192.168.1
4	0.002278	192.168.1.3	192.168.1
5	0.002412	192.168.1.8	192.168.1
6	0.002643	192.168.1.3	192.168.1
7	0.002731	192.168.1.8	192.168.1
8	0.008038	192.168.1.3	192.168.1

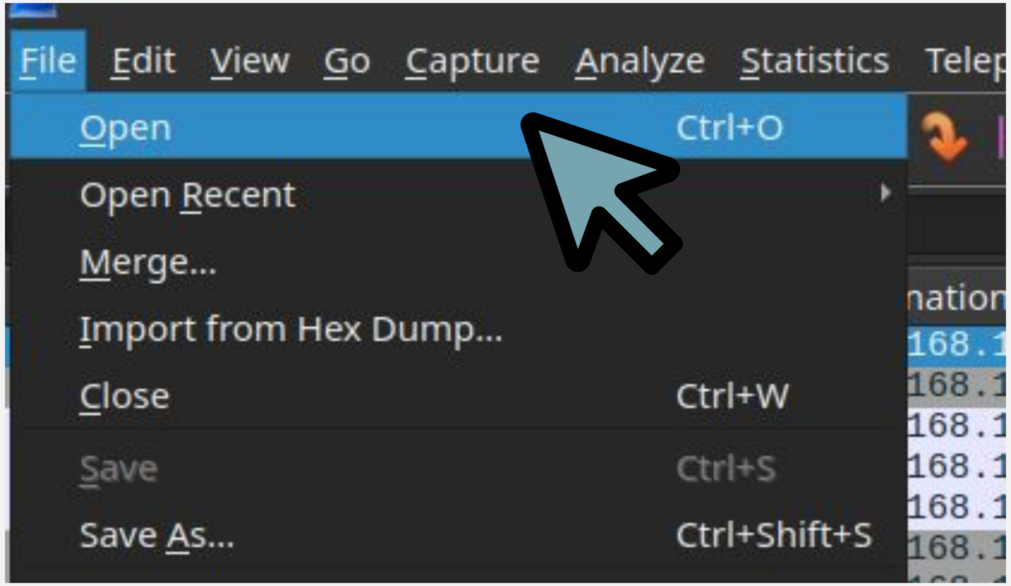
What is the size of the largest packet in this capture?



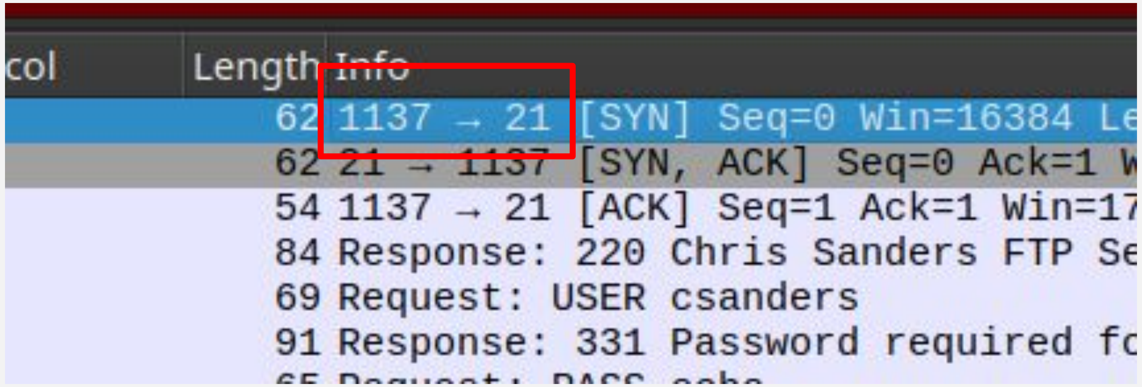
```
: 81 bytes on wire (648 bits), 81 bytes captured (
t II, Src: Apple_cf:53:89 (a4:5e:60:cf:53:89), Dst
t Protocol Version 4, Src: 192.168.1.3, Dst: 192.1
ssion Control Protocol, Src Port: 49859, Dst Port:
5 bytes)
```

Exercise 2

1. Download: https://github.com/ieee-unipi-sb/Ethical-Hacking/tree/main/Workshop%201%20-%20Network%20Forensics/.pcap%20files
2. What port number is the source using to communicate with the destination (1-to-3) ?
3. How many TCP connections were established during the capture?
4. What are the devices that communicate in the first TCP connection ?

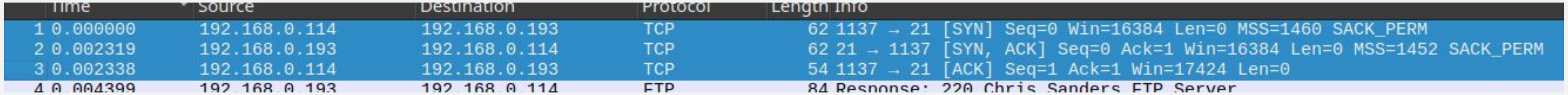


What port number is the source using to communicate with the destination

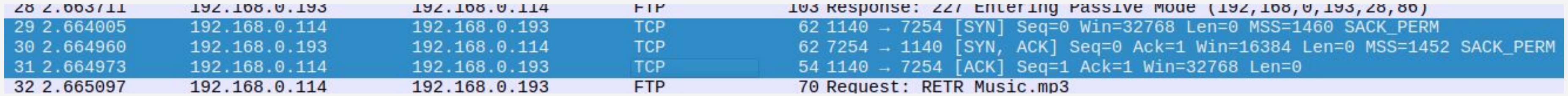


```
col          Length Info
                 62 1137 → 21 [SYN] Seq=0 Win=16384 Le
                 62 21 → 1137 [SYN, ACK] Seq=0 Ack=1 W
                 54 1137 → 21 [ACK] Seq=1 Ack=1 Win=17
                 84 Response: 220 Chris Sanders FTP Se
                 69 Request: USER csanders
                 91 Response: 331 Password required fo
                 65 Request: PASS echo
```

How many TCP connections were established during the capture?

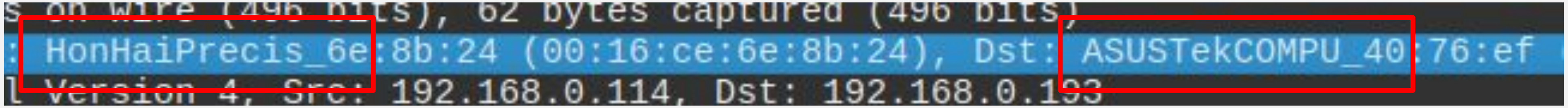


```
    Time          Source          Destination     Protocol  Length Info
  1 0.000000      192.168.0.114   192.168.0.193   TCP          62 1137 → 21 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
  2 0.002319      192.168.0.193   192.168.0.114   TCP          62 21 → 1137 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1452 SACK_PERM
  3 0.002338      192.168.0.114   192.168.0.193   TCP          54 1137 → 21 [ACK] Seq=1 Ack=1 Win=17424 Len=0
  4 0.004399      192.168.0.193   192.168.0.114   FTP          84 Response: 220 Chris Sanders FTP Server
```



```
 28 2.663711      192.168.0.193   192.168.0.114   FTP         103 Response: 227 Entering Passive Mode (192,168,0,193,28,86)
 29 2.664005      192.168.0.114   192.168.0.193   TCP          62 1140 → 7254 [SYN] Seq=0 Win=32768 Len=0 MSS=1460 SACK_PERM
 30 2.664960      192.168.0.193   192.168.0.114   TCP          62 7254 → 1140 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1452 SACK_PERM
 31 2.664973      192.168.0.114   192.168.0.193   TCP          54 1140 → 7254 [ACK] Seq=1 Ack=1 Win=32768 Len=0
 32 2.665097      192.168.0.114   192.168.0.193   FTP          70 Request: RETR Music.mp3
```

What are the devices that communicate in the first TCP connection ?



```
s on wire (496 bits), 62 bytes captured (496 bits)
: HonHaiPrecis_6e:8b:24 (00:16:ce:6e:8b:24), Dst: ASUSTekCOMPU_40:76:ef
l Version 4, Src: 192.168.0.114, Dst: 192.168.0.193
```

Extracting images/videos

STEP 1. Get your pcap file, and open it in Wireshark

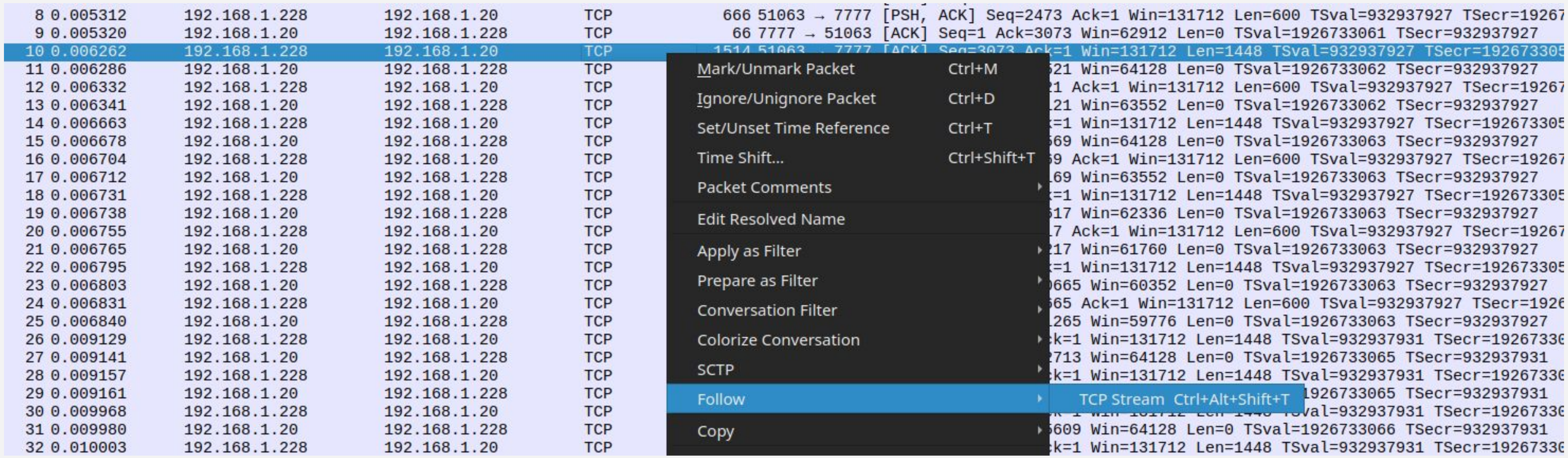
STEP 2. Find the packet

STEP 3. Right click “**Follow**” > “**TCP Stream**”

STEP 4. Click on “**Show data as**”

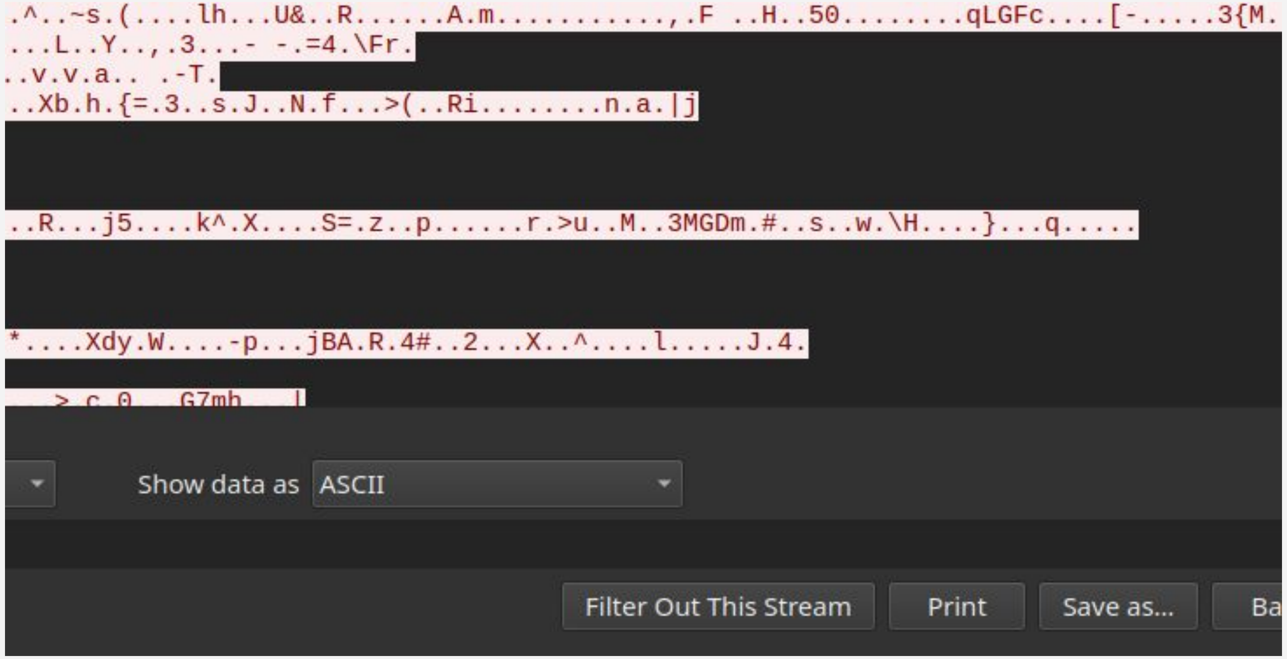
STEP 5. Select “**Raw**”

STEP 6. Select “**Save as**”



```
 8 0.005312   192.168.1.228   192.168.1.20    TCP        666 51063 → 7777 [PSH, ACK] Seq=2473 Ack=1 Win=131712 Len=600 TSval=932937927 TSecr=19267
 9 0.005320   192.168.1.20    192.168.1.228   TCP         66 7777 → 51063 [ACK] Seq=1 Ack=3073 Win=62912 Len=0 TSval=1926733061 TSecr=932937927
10 0.006262   192.168.1.228   192.168.1.20    TCP       1514 51063 → 7777 [ACK] Seq=3073 Ack=1 Win=131712 Len=1448 TSval=932937927 TSecr=192673305
11 0.006286   192.168.1.20    192.168.1.228   TCP                                   21 Win=64128 Len=0 TSval=1926733062 TSecr=932937927
12 0.006332   192.168.1.228   192.168.1.20    TCP                                   1 Ack=1 Win=131712 Len=600 TSval=932937927 TSecr=19267
13 0.006341   192.168.1.20    192.168.1.228   TCP                                   21 Win=63552 Len=0 TSval=1926733062 TSecr=932937927
14 0.006663   192.168.1.228   192.168.1.20    TCP                                   =1 Win=131712 Len=1448 TSval=932937927 TSecr=192673305
15 0.006678   192.168.1.20    192.168.1.228   TCP                                   69 Win=64128 Len=0 TSval=1926733063 TSecr=932937927
16 0.006704   192.168.1.228   192.168.1.20    TCP                                   9 Ack=1 Win=131712 Len=600 TSval=932937927 TSecr=19267
17 0.006712   192.168.1.20    192.168.1.228   TCP                                   169 Win=63552 Len=0 TSval=1926733063 TSecr=932937927
18 0.006731   192.168.1.228   192.168.1.20    TCP                                   =1 Win=131712 Len=1448 TSval=932937927 TSecr=192673305
19 0.006738   192.168.1.20    192.168.1.228   TCP                                   17 Win=62336 Len=0 TSval=1926733063 TSecr=932937927
20 0.006755   192.168.1.228   192.168.1.20    TCP                                   7 Ack=1 Win=131712 Len=600 TSval=932937927 TSecr=19267
21 0.006765   192.168.1.20    192.168.1.228   TCP                                   217 Win=61760 Len=0 TSval=1926733063 TSecr=932937927
22 0.006795   192.168.1.228   192.168.1.20    TCP                                   =1 Win=131712 Len=1448 TSval=932937927 TSecr=192673305
23 0.006803   192.168.1.20    192.168.1.228   TCP                                   0665 Win=60352 Len=0 TSval=1926733063 TSecr=932937927
24 0.006831   192.168.1.228   192.168.1.20    TCP                                   65 Ack=1 Win=131712 Len=600 TSval=932937927 TSecr=1926
25 0.006840   192.168.1.20    192.168.1.228   TCP                                   1265 Win=59776 Len=0 TSval=1926733063 TSecr=932937927
26 0.009129   192.168.1.228   192.168.1.20    TCP                                   k=1 Win=131712 Len=1448 TSval=932937931 TSecr=19267330
27 0.009141   192.168.1.20    192.168.1.228   TCP                                   2713 Win=64128 Len=0 TSval=1926733065 TSecr=932937931
28 0.009157   192.168.1.228   192.168.1.20    TCP                                   k=1 Win=131712 Len=1448 TSval=932937931 TSecr=19267330
29 0.009161   192.168.1.20    192.168.1.228   TCP                                                 1926733065 TSecr=932937931
30 0.009968   192.168.1.228   192.168.1.20    TCP                                                 val=932937931 TSecr=19267330
31 0.009980   192.168.1.20    192.168.1.228   TCP                                   5609 Win=64128 Len=0 TSval=1926733066 TSecr=932937931
32 0.010003   192.168.1.228   192.168.1.20    TCP                                   k=1 Win=131712 Len=1448 TSval=932937931 TSecr=19267330
```

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
TCP Stream Ctrl+Alt+Shift+T
Copy



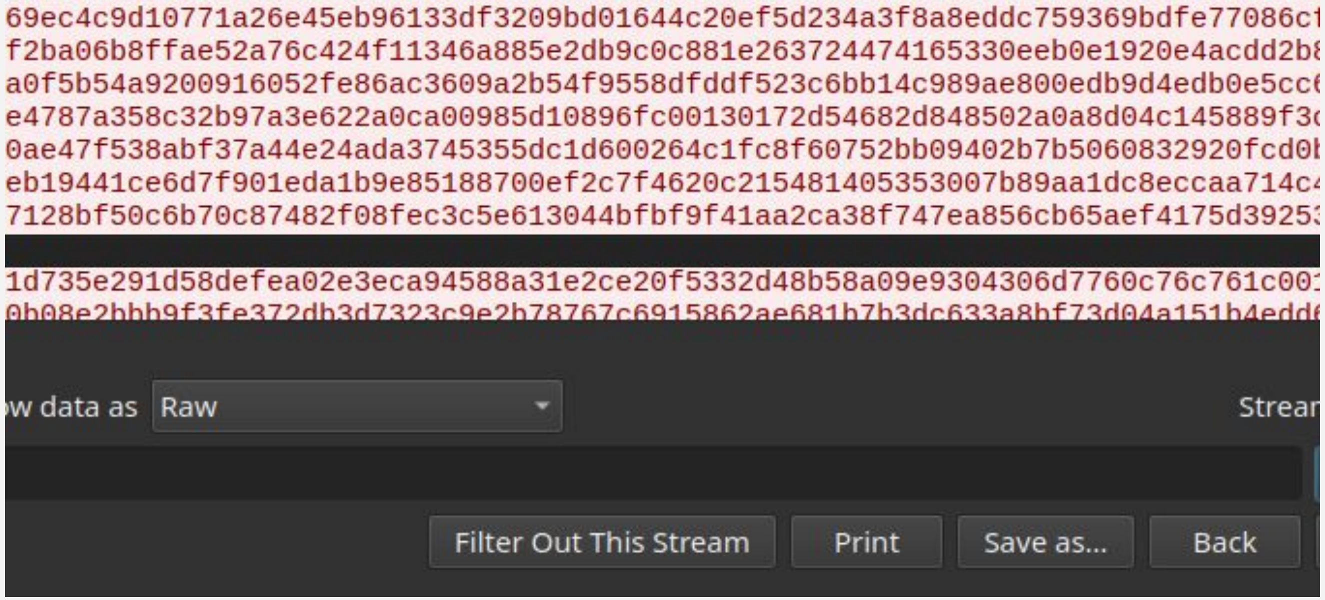
```
.^..~s.(....lh...U&..R......A.m...........,.F ..H..50........qLGFc....[-.....3{M.
...L..Y..,.3...- -.=4.\Fr.
..v.v.a.. .-T.
..Xb.h.{=.3..s.J..N.f...>(..Ri........n.a.|j


..R...j5....k^.X....S=.z..p......r.>u..M..3MGDm.#..s..w.\H....}...q.....


*....Xdy.W....-p...jBA.R.4#..2...X..^....l.....J.4.

...>.c.0....G7mh....|
```

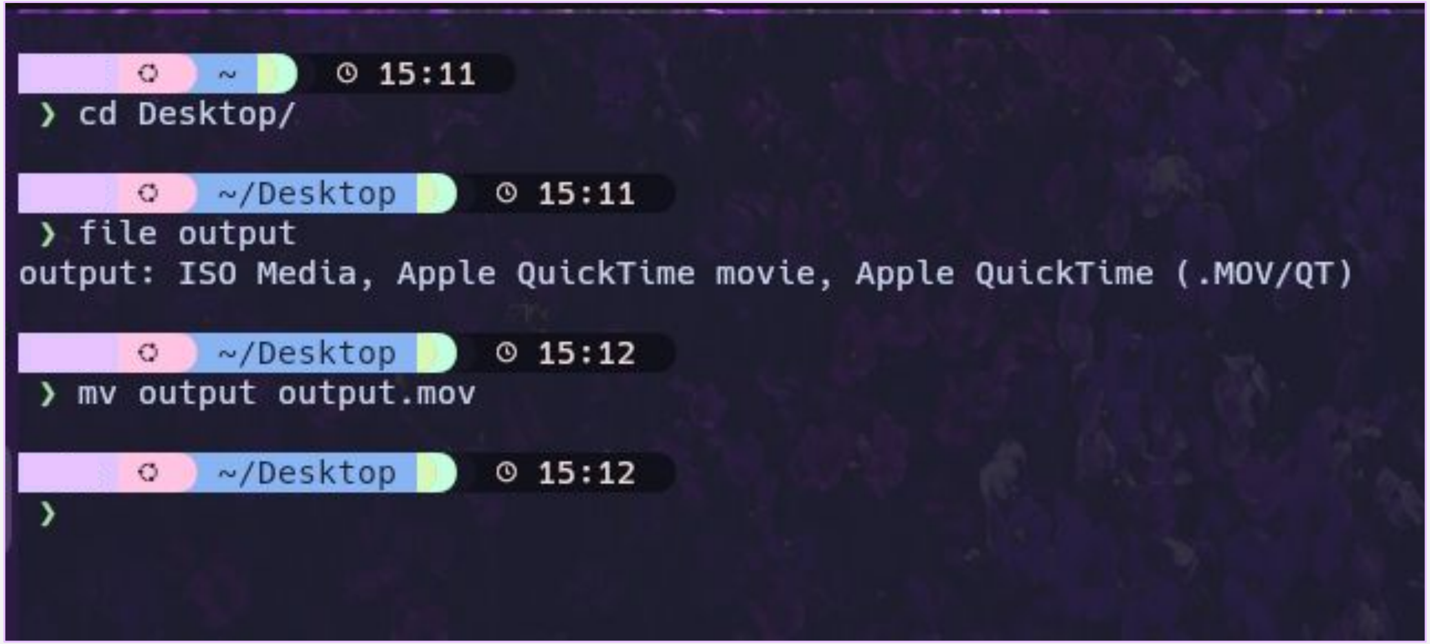
Show data as ASCII



```
69ec4c9d10771a26e45eb96133df3209bd01644c20ef5d234a3f8a8eddc759369bdfe77086cf
f2ba06b8ffae52a76c424f11346a885e2db9c0c881e263724474165330eeb0e1920e4acdd2b8
a0f5b54a9200916052fe86ac3609a2b54f9558dfddf523c6bb14c989ae800edb9d4edb0e5cc6
e4787a358c32b97a3e622a0ca00985d10896fc00130172d54682d848502a0a8d04c145889f3c
0ae47f538abf37a44e24ada3745355dc1d600264c1fc8f60752bb09402b7b5060832920fcd0b
eb19441ce6d7f901eda1b9e85188700ef2c7f4620c215481405353007b89aa1dc8eccaa714c4
7128bf50c6b70c87482f08fec3c5e613044bfbf9f41aa2ca38f747ea856cb65aef4175d3925

1d735e291d58defea02e3eca94588a31e2ce20f5332d48b58a09e9304306d7760c76c761c001
0b08e2bbb9f3fe372db3d7323c9e2b78767c6915862ae681b7b3dc633a8bf73d04a151b4edd6
```

w data as Raw



```
 ~  ◷ 15:11
❯ cd Desktop/

 ~/Desktop  ◷ 15:11
❯ file output
output: ISO Media, Apple QuickTime movie, Apple QuickTime (.MOV/QT)

 ~/Desktop  ◷ 15:12
❯ mv output output.mov

 ~/Desktop  ◷ 15:12
❯
```

“That’s all Folks!”

Thank you!

Credits

- https://en.wikipedia.org/wiki/Forensic_science
- https://www.techtarget.com/searchnetworking/definition/packet
- https://forensics.wiki
- https://primer.picoctf.org/
- https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it
- https://www.youtube.com/watch?v=Lj2DaFLRQVI