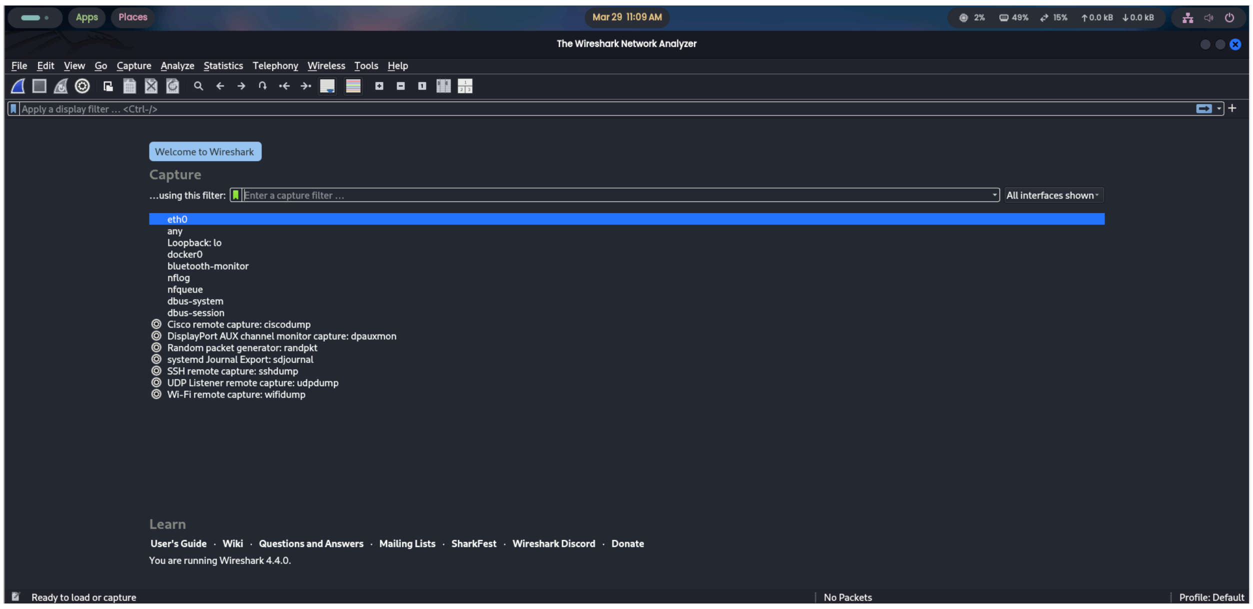
Code 200 [CyberStorm CTF]

What is this Code 200 and why is it the only thing that Nami keeps talking about? She makes it seem like its something gnarly and very hazardous for our ship. Is that true or is she just trying to hide yet another indulgent expenditure from the crew?

Reconnaissance and Enumeration [Phase 1]

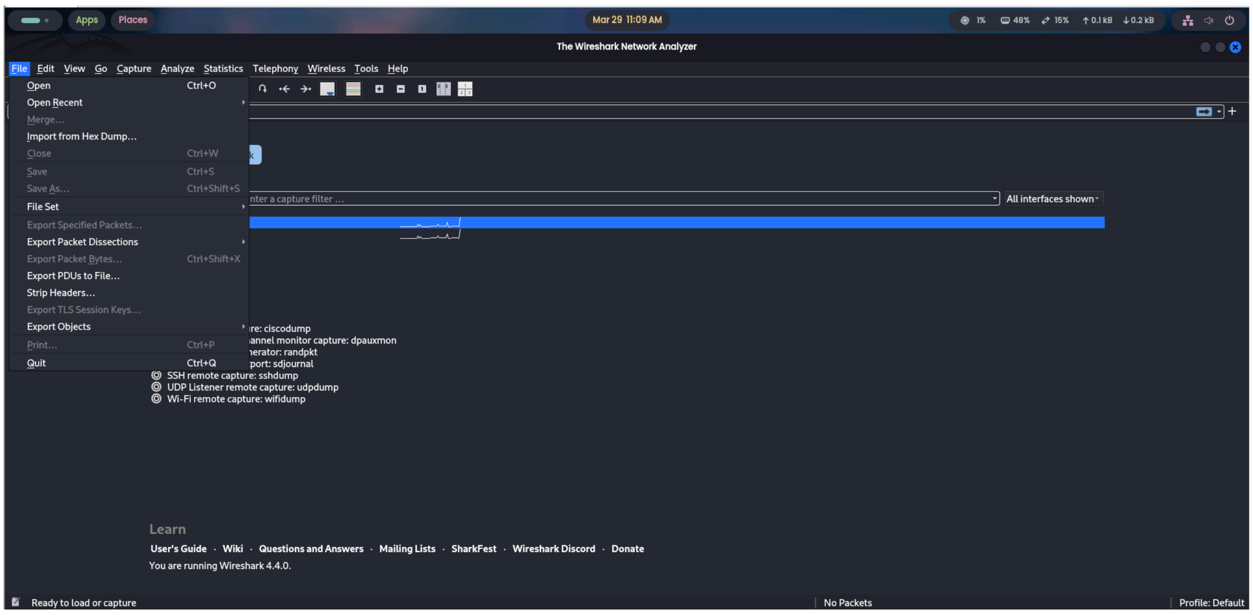
Importing the pcap file into Wireshark

command ⇒ wireshark



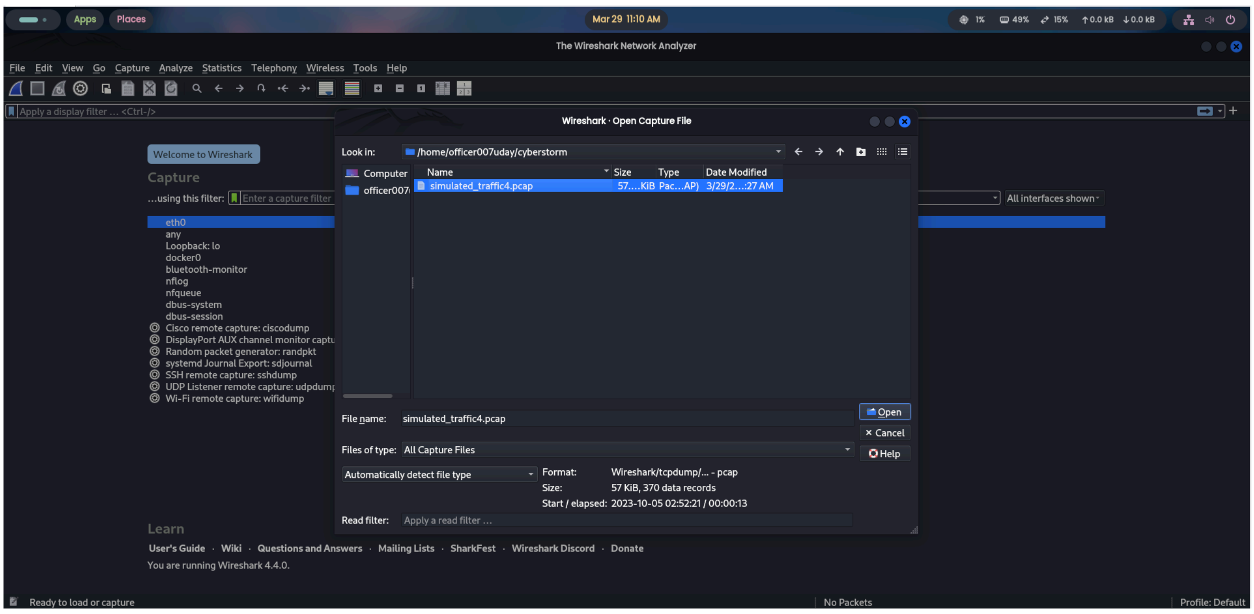
Apps
Places
Mar 29 11:09 AM
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Welcome to Wireshark
Capture
…using this filter:
Enter a capture filter …
All interfaces shown
eth0
any
Loopback: lo
docker0
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.4.0.
Ready to load or capture
No Packets
Profile: Default

Click on the top left side of the screen named as file to open the pcap file in wireshark



Apps
Places
Mar 29 11:09 AM
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge…
Import from Hex Dump…
Close Ctrl+W
Save Ctrl+S
Save As… Ctrl+Shift+S
File Set
Export Specified Packets…
Export Packet Dissections
Export Packet Bytes… Ctrl+Shift+X
Export PDUs to File…
Strip Headers…
Export TLS Session Keys…
Export Objects
Print… Ctrl+P
Quit Ctrl+Q
All interfaces shown
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.4.0.
Ready to load or capture
No Packets
Profile: Default

Click on the open and select your downloaded pcap file to start looking for the flag.



Wireshark · Open Capture File

Look in: /home/officer007uday/cyberstorm

Name	Size	Type	Date Modified
simulated_traffic4.pcap	57.…KiB	Pac…AP)	3/29/2…:27 AM

File name: simulated_traffic4.pcap

Files of type: All Capture Files

Automatically detect file type

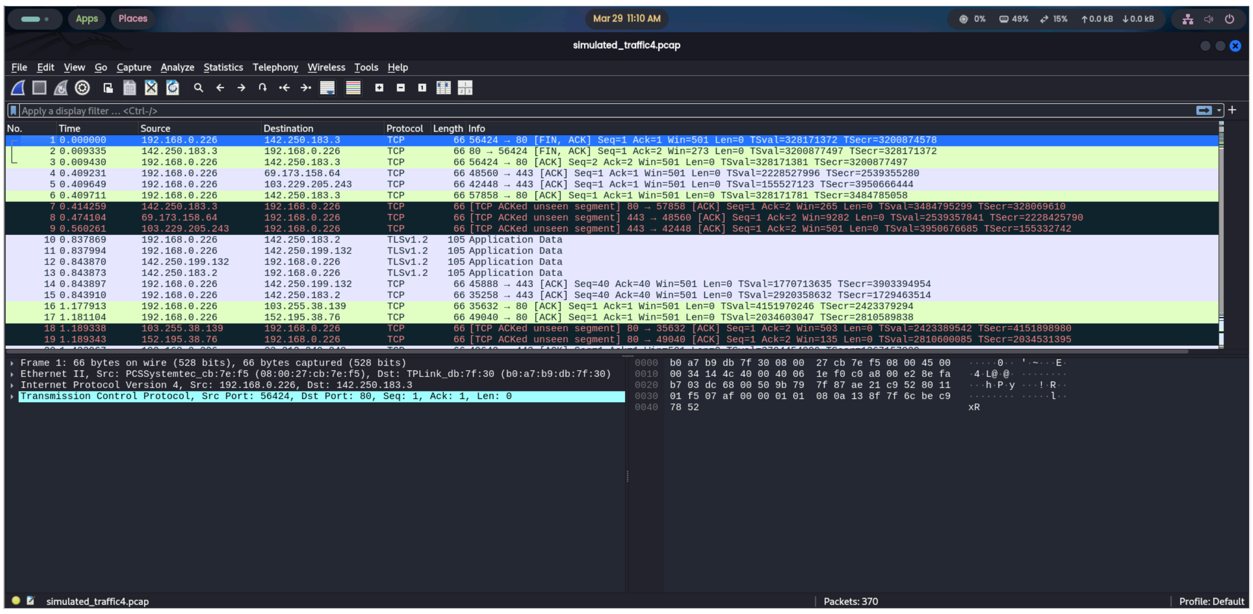
Format: Wireshark/tcpdump/… - pcap

Size: 57 KiB, 370 data records

Start / elapsed: 2023-10-05 02:52:21 / 00:00:13

Read filter: Apply a read filter …

You are running Wireshark 4.4.0.



simulated_traffic4.pcap

```
No. Time     Source          Destination     Protocol Length Info
  1 0.000000 192.168.0.226   142.250.183.3   TCP      66 56424 → 80 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=328171372 TSecr=3200874578
  2 0.009335 142.250.183.3   192.168.0.226   TCP      66 80 → 56424 [FIN, ACK] Seq=1 Ack=2 Win=273 Len=0 TSval=3200877497 TSecr=328171372
  3 0.009430 192.168.0.226   142.250.183.3   TCP      66 56424 → 80 [ACK] Seq=2 Ack=2 Win=501 Len=0 TSval=328171381 TSecr=3200877497
  4 0.409231 192.168.0.226   69.173.158.64   TCP      66 48560 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2228527996 TSecr=2539355280
  5 0.409649 192.168.0.226   103.229.205.243 TCP      66 42448 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=155527123 TSecr=3950666444
  6 0.409711 192.168.0.226   142.250.183.3   TCP      66 57858 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=328171781 TSecr=3484785058
  7 0.414259 142.250.183.3   192.168.0.226   TCP      66 [TCP ACKed unseen segment] 80 → 57858 [ACK] Seq=1 Ack=2 Win=265 Len=0 TSval=3484795299 TSecr=328069610
  8 0.474104 69.173.158.64   192.168.0.226   TCP      66 [TCP ACKed unseen segment] 443 → 48560 [ACK] Seq=1 Ack=2 Win=9282 Len=0 TSval=2539357841 TSecr=2228425790
  9 0.560261 103.229.205.243 192.168.0.226   TCP      66 [TCP ACKed unseen segment] 443 → 42448 [ACK] Seq=1 Ack=2 Win=501 Len=0 TSval=3950676685 TSecr=155332742
 10 0.837869 192.168.0.226   142.250.183.2   TLSv1.2 105 Application Data
 11 0.837994 192.168.0.226   142.250.199.132 TLSv1.2 105 Application Data
 12 0.843870 142.250.199.132 192.168.0.226   TLSv1.2 105 Application Data
 13 0.843873 142.250.183.2   192.168.0.226   TLSv1.2 105 Application Data
 14 0.843897 192.168.0.226   142.250.199.132 TCP      66 45888 → 443 [ACK] Seq=40 Ack=40 Win=501 Len=0 TSval=1770713635 TSecr=3903394954
 15 0.843910 192.168.0.226   142.250.183.2   TCP      66 35258 → 443 [ACK] Seq=40 Ack=40 Win=501 Len=0 TSval=2920358632 TSecr=1729463514
 16 1.177913 192.168.0.226   103.255.38.139  TCP      66 35632 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=4151970246 TSecr=2423379294
 17 1.181104 192.168.0.226   152.195.38.76   TCP      66 49040 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2034603047 TSecr=2810589838
 18 1.189338 103.255.38.139  192.168.0.226   TCP      66 [TCP ACKed unseen segment] 80 → 35632 [ACK] Seq=1 Ack=2 Win=503 Len=0 TSval=2423389542 TSecr=4151898980
 19 1.189343 152.195.38.76   192.168.0.226   TCP      66 [TCP ACKed unseen segment] 80 → 49040 [ACK] Seq=1 Ack=2 Win=135 Len=0 TSval=2810600085 TSecr=2034531395
```

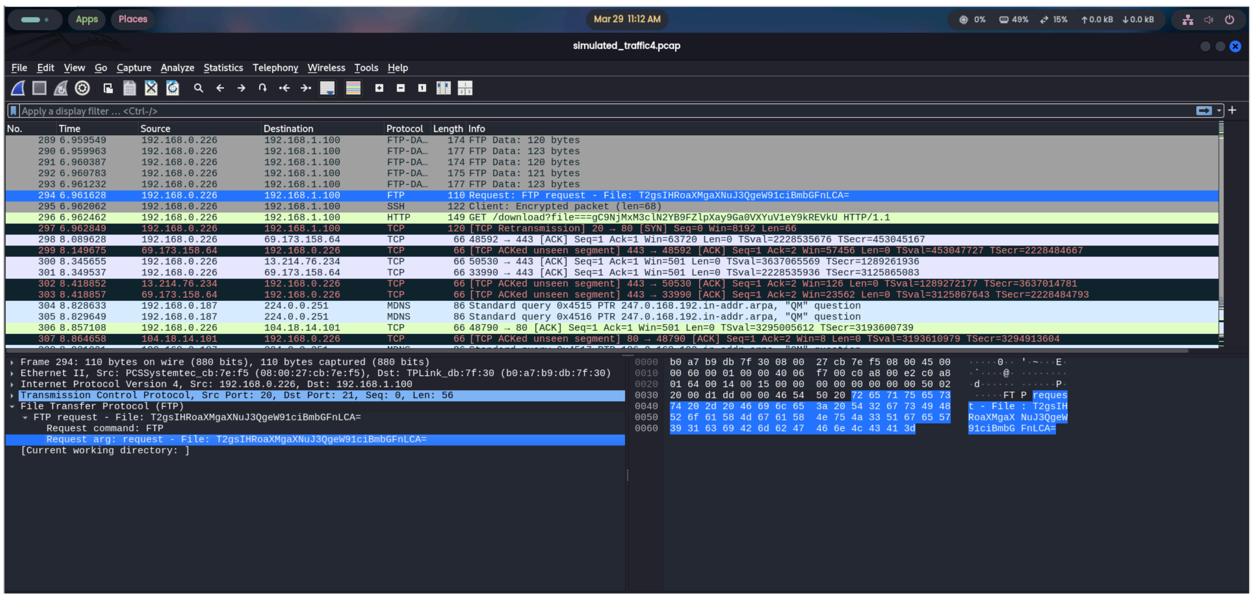
```
Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: PCSSystemtec_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: TPLink_db:7f:30 (b0:a7:b9:db:7f:30)
Internet Protocol Version 4, Src: 192.168.0.226, Dst: 142.250.183.3
Transmission Control Protocol, Src Port: 56424, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
```

```
0000  b0 a7 b9 db 7f 30 08 00  27 cb 7e f5 08 00 45 00   ·····0·· '·~···E·
0010  00 34 14 4c 40 00 40 06  1e f0 c0 a8 00 e2 8e fa   ·4·L@·@· ········
0020  b7 03 dc 68 00 50 9b 79  7f 87 ae 21 c9 52 80 11   ···h·P·y ···!·R··
0030  01 f5 07 af 00 00 01 01  08 0a 13 8f 7f 6c be c9   ········ ·····l··
0040  78 52                                              xR
```

Packets: 370

Now that we have imported our pcap file lets start going through it and see if there is something interesting that can be a flag.

Flag?

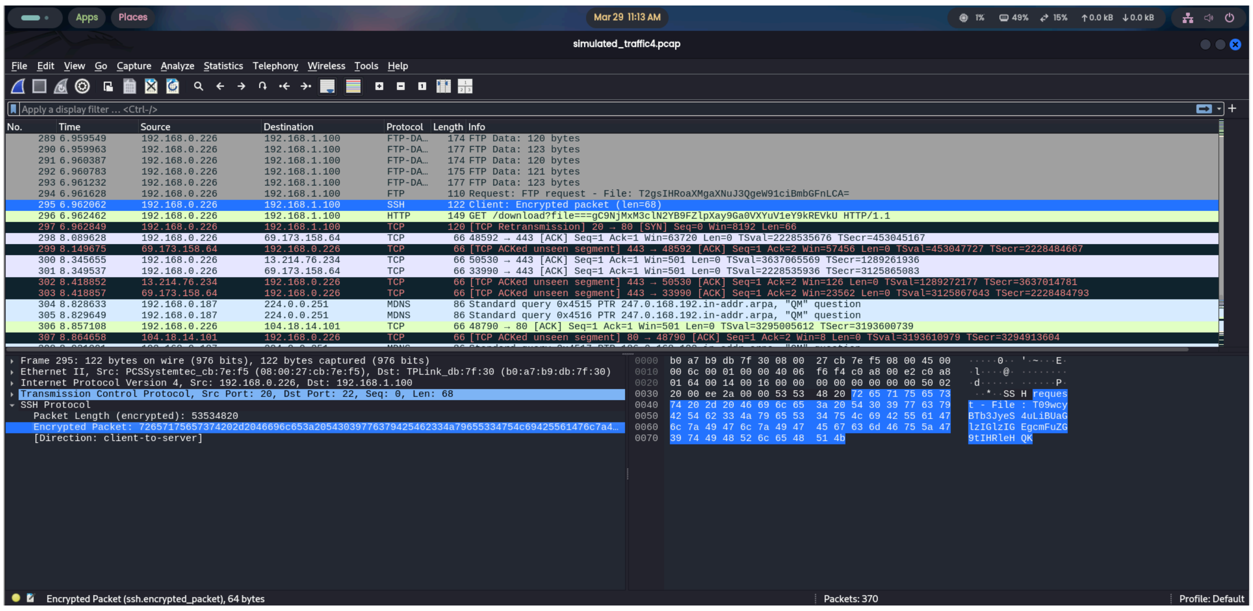


Apps
Places
Mar 29 11:12 AM
0%
49%
15%
↑0.0 kB
↓0.0 kB
simulated_traffic4.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time      Source           Destination      Protocol Length Info
  289 6.959549  192.168.0.226    192.168.1.100    FTP-DA…   174 FTP Data: 120 bytes
  290 6.959963  192.168.0.226    192.168.1.100    FTP-DA…   177 FTP Data: 123 bytes
  291 6.960387  192.168.0.226    192.168.1.100    FTP-DA…   174 FTP Data: 120 bytes
  292 6.960783  192.168.0.226    192.168.1.100    FTP-DA…   175 FTP Data: 121 bytes
  293 6.961232  192.168.0.226    192.168.1.100    FTP-DA…   177 FTP Data: 123 bytes
  294 6.961628  192.168.0.226    192.168.1.100    FTP       110 Request: FTP request - File: T2gsIHRoaXMgaXNuJ3QgeW91ciBmbGFnLCA=
  295 6.962062  192.168.0.226    192.168.1.100    SSH       122 Client: Encrypted packet (len=68)
  296 6.962462  192.168.0.226    192.168.1.100    HTTP      149 GET /download?file===gC9NjMxM3clN2YB9FZlpXay9Ga0VXYuV1eY9kREVkU HTTP/1.1
  297 6.962849  192.168.0.226    192.168.1.100    TCP       120 [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=66
  298 8.089628  192.168.0.226    69.173.158.64    TCP        66 48592 → 443 [ACK] Seq=1 Ack=1 Win=63720 Len=0 TSval=2228535676 TSecr=453045167
  299 8.149675  69.173.158.64    192.168.0.226    TCP        66 [TCP ACKed unseen segment] 443 → 48592 [ACK] Seq=1 Ack=2 Win=57456 Len=0 TSval=453047727 TSecr=2228484667
  300 8.345655  192.168.0.226    13.214.76.234    TCP        66 50530 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3637065569 TSecr=1289261936
  301 8.349537  192.168.0.226    69.173.158.64    TCP        66 33990 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2228535936 TSecr=3125865083
  302 8.418852  13.214.76.234    192.168.0.226    TCP        66 [TCP ACKed unseen segment] 443 → 50530 [ACK] Seq=1 Ack=2 Win=126 Len=0 TSval=1289272177 TSecr=3637014781
  303 8.418857  69.173.158.64    192.168.0.226    TCP        66 [TCP ACKed unseen segment] 443 → 33990 [ACK] Seq=1 Ack=2 Win=23562 Len=0 TSval=3125867643 TSecr=2228484793
  304 8.828633  192.168.0.187    224.0.0.251      MDNS       86 Standard query 0x4515 PTR 247.0.168.192.in-addr.arpa, "QM" question
  305 8.829649  192.168.0.187    224.0.0.251      MDNS       86 Standard query 0x4516 PTR 247.0.168.192.in-addr.arpa, "QM" question
  306 8.857108  192.168.0.226    104.18.14.101    TCP        66 48790 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3295005612 TSecr=3193600739
  307 8.864658  104.18.14.101    192.168.0.226    TCP        66 [TCP ACKed unseen segment] 80 → 48790 [ACK] Seq=1 Ack=2 Win=8 Len=0 TSval=3193610979 TSecr=3294913604
```

```
› Frame 294: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
› Ethernet II, Src: PCSSystemtec_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: TPLink_db:7f:30 (b0:a7:b9:db:7f:30)
› Internet Protocol Version 4, Src: 192.168.0.226, Dst: 192.168.1.100
› Transmission Control Protocol, Src Port: 20, Dst Port: 21, Seq: 0, Len: 56
⌄ File Transfer Protocol (FTP)
  ⌄ FTP request - File: T2gsIHRoaXMgaXNuJ3QgeW91ciBmbGFnLCA=
      Request command: FTP
      Request arg: request - File: T2gsIHRoaXMgaXNuJ3QgeW91ciBmbGFnLCA=
  [Current working directory: ]
```

```
0000  b0 a7 b9 db 7f 30 08 00  27 cb 7e f5 08 00 45 00   ·····0·· '·~···E·
0010  00 60 00 01 00 00 40 06  f7 00 c0 a8 00 e2 c0 a8   ·`····@· ········
0020  01 64 00 14 00 15 00 00  00 00 00 00 00 00 50 02   ·d······ ······P·
0030  20 00 d1 dd 00 00 46 54  50 20 72 65 71 75 65 73    ·····FT P reques
0040  74 20 2d 20 46 69 6c 65  3a 20 54 32 67 73 49 48   t - File : T2gsIH
0050  52 6f 61 58 4d 67 61 58  4e 75 4a 33 51 67 65 57   RoaXMgaX NuJ3QgeW
0060  39 31 63 69 42 6d 62 47  46 6e 4c 43 41 3d         91ciBmbG FnLCA=
```



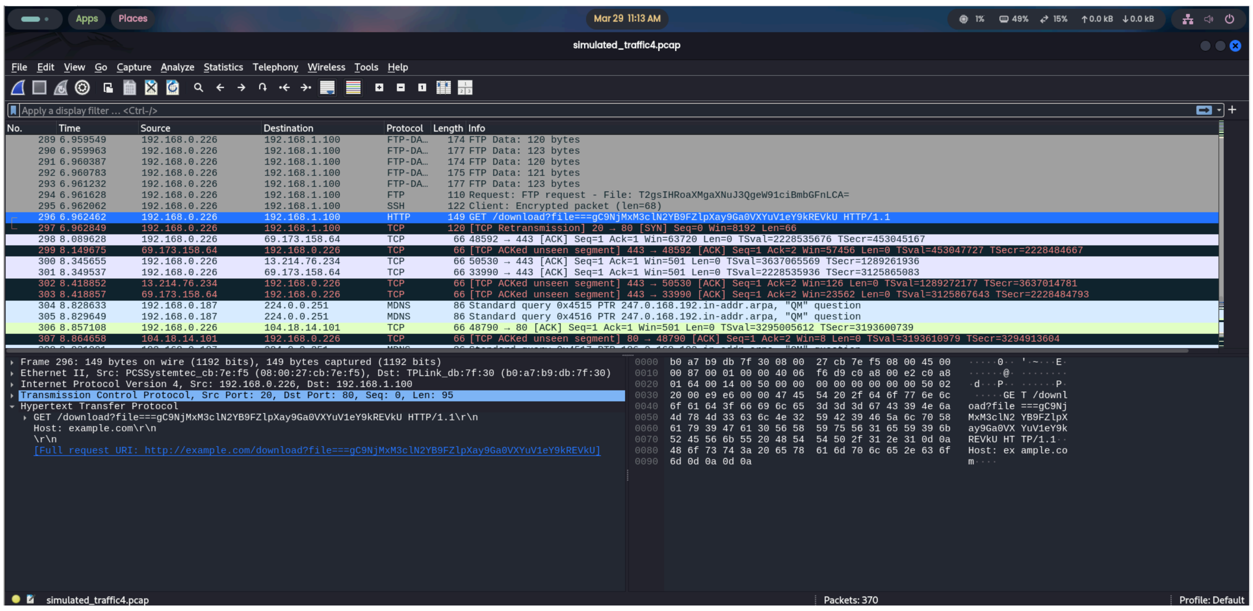
Apps
Places
Mar 29 11:13 AM
1%
49%
15%
↑0.0 kB
↓0.0 kB
simulated_traffic4.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time      Source           Destination      Protocol Length Info
  289 6.959549  192.168.0.226    192.168.1.100    FTP-DA…   174 FTP Data: 120 bytes
  290 6.959963  192.168.0.226    192.168.1.100    FTP-DA…   177 FTP Data: 123 bytes
  291 6.960387  192.168.0.226    192.168.1.100    FTP-DA…   174 FTP Data: 120 bytes
  292 6.960783  192.168.0.226    192.168.1.100    FTP-DA…   175 FTP Data: 121 bytes
  293 6.961232  192.168.0.226    192.168.1.100    FTP-DA…   177 FTP Data: 123 bytes
  294 6.961628  192.168.0.226    192.168.1.100    FTP       110 Request: FTP request - File: T2gsIHRoaXMgaXNuJ3QgeW91ciBmbGFnLCA=
  295 6.962062  192.168.0.226    192.168.1.100    SSH       122 Client: Encrypted packet (len=68)
  296 6.962462  192.168.0.226    192.168.1.100    HTTP      149 GET /download?file===gC9NjMxM3clN2YB9FZlpXay9Ga0VXYuV1eY9kREVkU HTTP/1.1
  297 6.962849  192.168.0.226    192.168.1.100    TCP       120 [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=66
  298 8.089628  192.168.0.226    69.173.158.64    TCP        66 48592 → 443 [ACK] Seq=1 Ack=1 Win=63720 Len=0 TSval=2228535676 TSecr=453045167
  299 8.149675  69.173.158.64    192.168.0.226    TCP        66 [TCP ACKed unseen segment] 443 → 48592 [ACK] Seq=1 Ack=2 Win=57456 Len=0 TSval=453047727 TSecr=2228484667
  300 8.345655  192.168.0.226    13.214.76.234    TCP        66 50530 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3637065569 TSecr=1289261936
  301 8.349537  192.168.0.226    69.173.158.64    TCP        66 33990 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2228535936 TSecr=3125865083
  302 8.418852  13.214.76.234    192.168.0.226    TCP        66 [TCP ACKed unseen segment] 443 → 50530 [ACK] Seq=1 Ack=2 Win=126 Len=0 TSval=1289272177 TSecr=3637014781
  303 8.418857  69.173.158.64    192.168.0.226    TCP        66 [TCP ACKed unseen segment] 443 → 33990 [ACK] Seq=1 Ack=2 Win=23562 Len=0 TSval=3125867643 TSecr=2228484793
  304 8.828633  192.168.0.187    224.0.0.251      MDNS       86 Standard query 0x4515 PTR 247.0.168.192.in-addr.arpa, "QM" question
  305 8.829649  192.168.0.187    224.0.0.251      MDNS       86 Standard query 0x4516 PTR 247.0.168.192.in-addr.arpa, "QM" question
  306 8.857108  192.168.0.226    104.18.14.101    TCP        66 48790 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3295005612 TSecr=3193600739
  307 8.864658  104.18.14.101    192.168.0.226    TCP        66 [TCP ACKed unseen segment] 80 → 48790 [ACK] Seq=1 Ack=2 Win=8 Len=0 TSval=3193610979 TSecr=3294913604
```

```
› Frame 295: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
› Ethernet II, Src: PCSSystemtec_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: TPLink_db:7f:30 (b0:a7:b9:db:7f:30)
› Internet Protocol Version 4, Src: 192.168.0.226, Dst: 192.168.1.100
› Transmission Control Protocol, Src Port: 20, Dst Port: 22, Seq: 0, Len: 68
⌄ SSH Protocol
    Packet Length (encrypted): 53534820
    Encrypted Packet: 72657175657374202d2046696c653a20543039776379425462334a79655334754c69425561476c7a4…
    [Direction: client-to-server]
```

```
0000  b0 a7 b9 db 7f 30 08 00  27 cb 7e f5 08 00 45 00   ·····0·· '·~···E·
0010  00 6c 00 01 00 00 40 06  f6 f4 c0 a8 00 e2 c0 a8   ·l····@· ········
0020  01 64 00 14 00 16 00 00  00 00 00 00 00 00 50 02   ·d······ ······P·
0030  20 00 ee 2a 00 00 53 53  48 20 72 65 71 75 65 73    ··*··SS H reques
0040  74 20 2d 20 46 69 6c 65  3a 20 54 30 39 77 63 79   t - File : T09wcy
0050  42 54 62 33 4a 79 65 53  34 75 4c 69 42 55 61 47   BTb3JyeS 4uLiBUaG
0060  6c 7a 49 47 6c 7a 49 47  45 67 63 6d 46 75 5a 47   lzIGlzIG EgcmFuZG
0070  39 74 49 48 52 6c 65 48  51 4b                     9tIHRleH QK
```

Encrypted Packet (ssh.encrypted_packet), 64 bytes
Packets: 370
Profile: Default



Apps
Places
Mar 29 11:13 AM
1%
49%
15%
↑0.0 kB
↓0.0 kB
simulated_traffic4.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time      Source           Destination      Protocol Length Info
  289 6.959549  192.168.0.226    192.168.1.100    FTP-DA…   174 FTP Data: 120 bytes
  290 6.959963  192.168.0.226    192.168.1.100    FTP-DA…   177 FTP Data: 123 bytes
  291 6.960387  192.168.0.226    192.168.1.100    FTP-DA…   174 FTP Data: 120 bytes
  292 6.960783  192.168.0.226    192.168.1.100    FTP-DA…   175 FTP Data: 121 bytes
  293 6.961232  192.168.0.226    192.168.1.100    FTP-DA…   177 FTP Data: 123 bytes
  294 6.961628  192.168.0.226    192.168.1.100    FTP       110 Request: FTP request - File: T2gsIHRoaXMgaXNuJ3QgeW91ciBmbGFnLCA=
  295 6.962062  192.168.0.226    192.168.1.100    SSH       122 Client: Encrypted packet (len=68)
  296 6.962462  192.168.0.226    192.168.1.100    HTTP      149 GET /download?file===gC9NjMxM3clN2YB9FZlpXay9Ga0VXYuV1eY9kREVkU HTTP/1.1
  297 6.962849  192.168.0.226    192.168.1.100    TCP       120 [TCP Retransmission] 20 → 80 [SYN] Seq=0 Win=8192 Len=66
  298 8.089628  192.168.0.226    69.173.158.64    TCP        66 48592 → 443 [ACK] Seq=1 Ack=1 Win=63720 Len=0 TSval=2228535676 TSecr=453045167
  299 8.149675  69.173.158.64    192.168.0.226    TCP        66 [TCP ACKed unseen segment] 443 → 48592 [ACK] Seq=1 Ack=2 Win=57456 Len=0 TSval=453047727 TSecr=2228484667
  300 8.345655  192.168.0.226    13.214.76.234    TCP        66 50530 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3637065569 TSecr=1289261936
  301 8.349537  192.168.0.226    69.173.158.64    TCP        66 33990 → 443 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=2228535936 TSecr=3125865083
  302 8.418852  13.214.76.234    192.168.0.226    TCP        66 [TCP ACKed unseen segment] 443 → 50530 [ACK] Seq=1 Ack=2 Win=126 Len=0 TSval=1289272177 TSecr=3637014781
  303 8.418857  69.173.158.64    192.168.0.226    TCP        66 [TCP ACKed unseen segment] 443 → 33990 [ACK] Seq=1 Ack=2 Win=23562 Len=0 TSval=3125867643 TSecr=2228484793
  304 8.828633  192.168.0.187    224.0.0.251      MDNS       86 Standard query 0x4515 PTR 247.0.168.192.in-addr.arpa, "QM" question
  305 8.829649  192.168.0.187    224.0.0.251      MDNS       86 Standard query 0x4516 PTR 247.0.168.192.in-addr.arpa, "QM" question
  306 8.857108  192.168.0.226    104.18.14.101    TCP        66 48790 → 80 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=3295005612 TSecr=3193600739
  307 8.864658  104.18.14.101    192.168.0.226    TCP        66 [TCP ACKed unseen segment] 80 → 48790 [ACK] Seq=1 Ack=2 Win=8 Len=0 TSval=3193610979 TSecr=3294913604
```

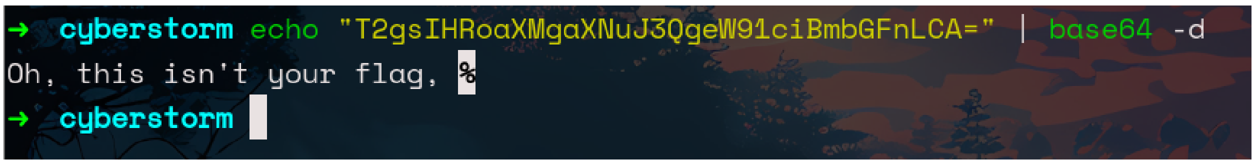
```
› Frame 296: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits)
› Ethernet II, Src: PCSSystemtec_cb:7e:f5 (08:00:27:cb:7e:f5), Dst: TPLink_db:7f:30 (b0:a7:b9:db:7f:30)
› Internet Protocol Version 4, Src: 192.168.0.226, Dst: 192.168.1.100
› Transmission Control Protocol, Src Port: 20, Dst Port: 80, Seq: 0, Len: 95
⌄ Hypertext Transfer Protocol
  › GET /download?file===gC9NjMxM3clN2YB9FZlpXay9Ga0VXYuV1eY9kREVkU HTTP/1.1\r\n
    Host: example.com\r\n
    \r\n
    [Full request URI: http://example.com/download?file===gC9NjMxM3clN2YB9FZlpXay9Ga0VXYuV1eY9kREVkU]
```

```
0000  b0 a7 b9 db 7f 30 08 00  27 cb 7e f5 08 00 45 00   ·····0·· '·~···E·
0010  00 87 00 01 00 00 40 06  f6 d9 c0 a8 00 e2 c0 a8   ······@· ········
0020  01 64 00 14 00 50 00 00  00 00 00 00 00 00 50 02   ·d···P·· ······P·
0030  20 00 e9 e6 00 00 47 45  54 20 2f 64 6f 77 6e 6c    ·····GE T /downl
0040  6f 61 64 3f 66 69 6c 65  3d 3d 3d 67 43 39 4e 6a   oad?file ===gC9Nj
0050  4d 78 4d 33 63 6c 4e 32  59 42 39 46 5a 6c 70 58   MxM3clN2 YB9FZlpX
0060  61 79 39 47 61 30 56 58  59 75 56 31 65 59 39 6b   ay9Ga0VX YuV1eY9k
0070  52 45 56 6b 55 20 48 54  54 50 2f 31 2e 31 0d 0a   REVkU HT TP/1.1··
0080  48 6f 73 74 3a 20 65 78  61 6d 70 6c 65 2e 63 6f   Host: ex ample.co
0090  6d 0d 0a 0d 0a                                     m····
```

After scrolling to the near bottom i found three requests first we have a base64 string that we got from FTP second we have a encrypted SSH string and at last we have a GET request and the value resembles base64 kind of if it was reversed. So lets see what are those starting with the base64's we got

1st Base64 (Flag?)

command ⇒ echo “your_base64_string” | base64 -d

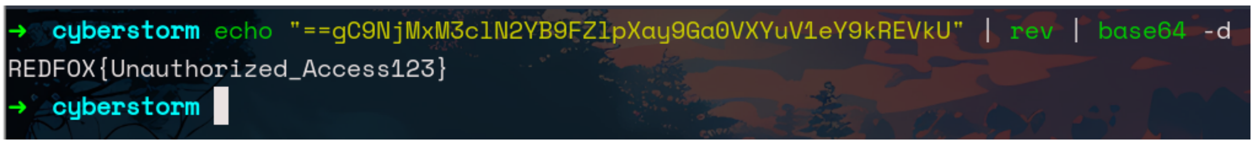


```
➜  cyberstorm echo "T2gsIHRoaXMgaXNuJ3QgeW91ciBmbGFnLCA=" | base64 -d
Oh, this isn't your flag, %
➜  cyberstorm
```

This was a bust maybe we look at the last reverse base64 string we got

2nd Base64 Flag

command ⇒ echo “your_base64_string” | rev | base64 -d



```
➜  cyberstorm echo "==gC9NjMxM3clN2YB9FZlpXay9Ga0VXYuV1eY9kREVkU" | rev | base64 -d
REDFOX{Unauthorized_Access123}
➜  cyberstorm
```

And as you can see we have got our flag lets submit this and move to our next challenge. But before that let me tell you what this command exactly does.

1. echo takes the string
2. | pipe is used to use multiple commands at once
3. rev is to reverse the string as it is not in proper base 64 from
4. and at last base64 -d to decode that string that is reversed from the echo