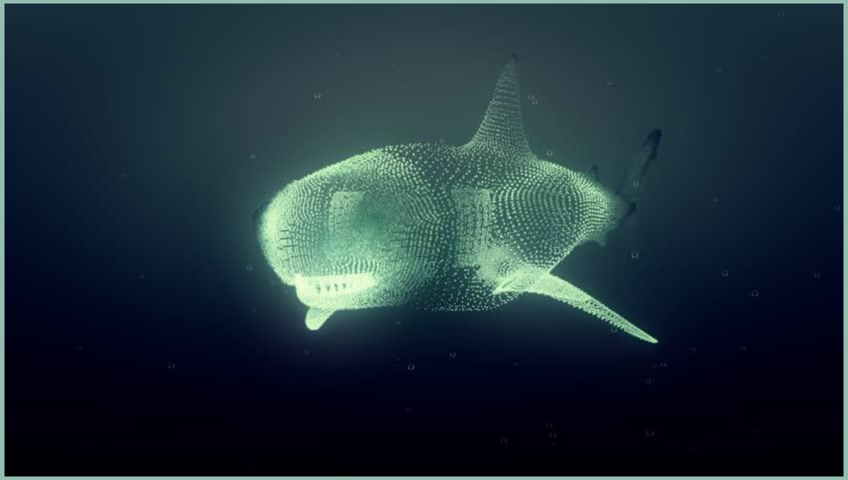
Intro Cybercamp



BACCC
BAY AREA
COMMUNITY COLLEGE CONSORTIUM

SUMMER CAMP

Network Forensics: Intro to Wireshark

Wireshark is a network packet analyzer

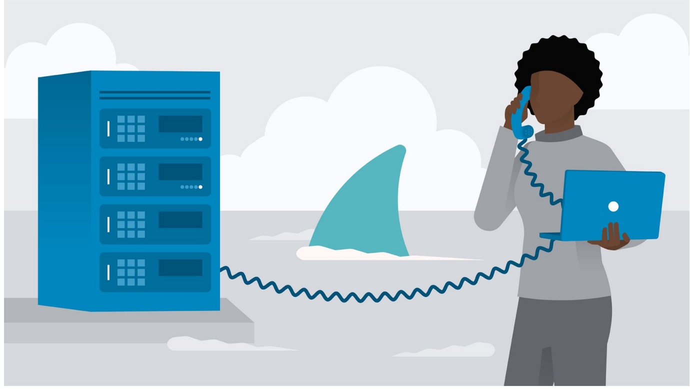
- Packet analyzers capture network packets and displays that packet data in as much detail as possible.
- Wireshark is perhaps one of the best open source packet analyzers available today.

Network Forensics: Intro to Wireshark

Wireshark is a powerful tool for network analysis. It can be used for things such as:

Security Tasks:

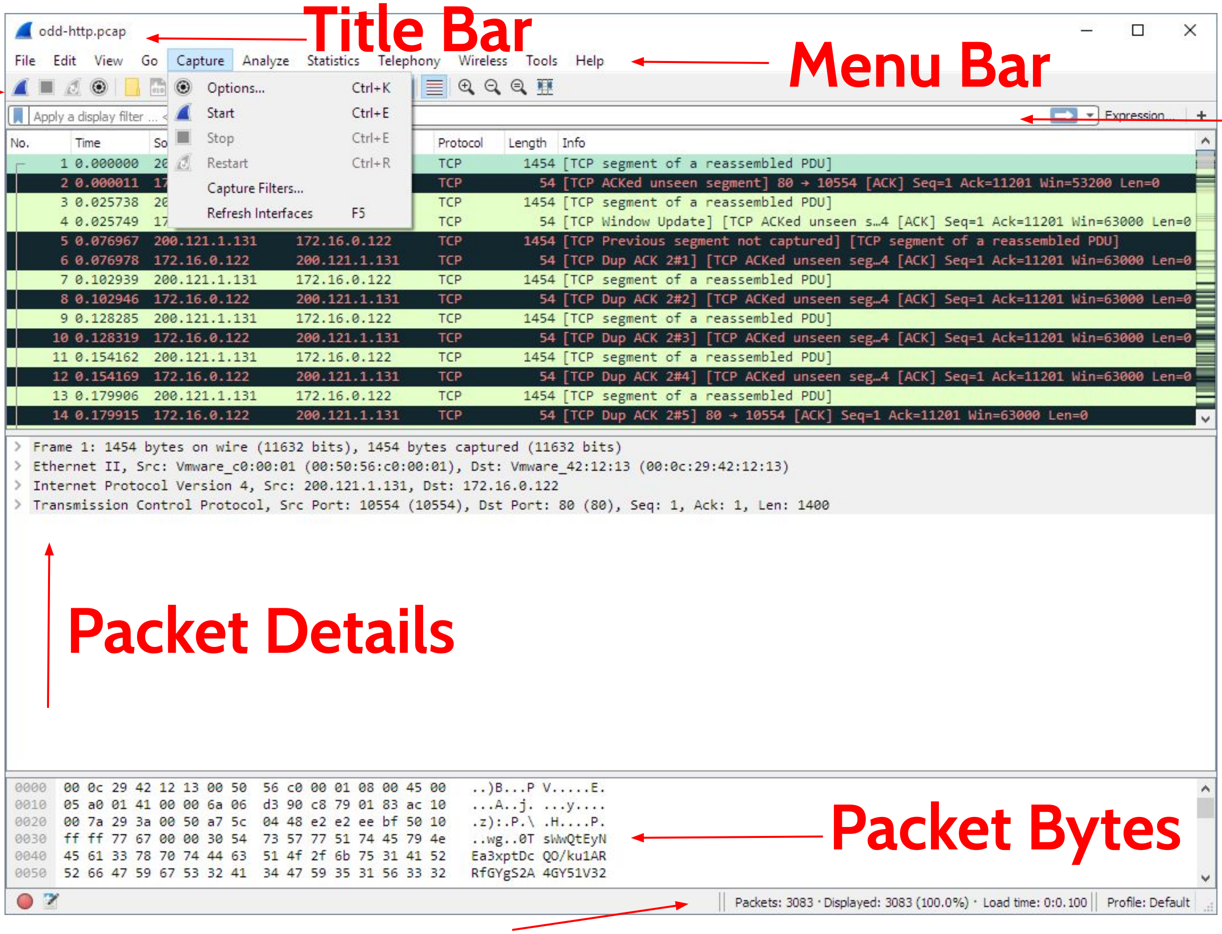
- Perform intrusion detection
- Identify and define malicious traffic signatures
- Log traffic for forensics examination
- Capture traffic as evidence
- Test firewall blocking
- Validate secure login and data traversal



Troubleshooting:

- Locate faulty network devices
- Identify device or software misconfiguration
- Measure high delays along a path
- Locate point of packet loss

Main Components of Wireshark



```
No.  Time       So                                   Protocol  Length Info
   1 0.000000   20                                   TCP        1454 [TCP segment of a reassembled PDU]
   2 0.000011   17                                   TCP          54 [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=53200 Len=0
   3 0.025738   20                                   TCP        1454 [TCP segment of a reassembled PDU]
   4 0.025749   17                                   TCP          54 [TCP Window Update] [TCP ACKed unseen s…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
   5 0.076967   200.121.1.131   172.16.0.122         TCP        1454 [TCP Previous segment not captured] [TCP segment of a reassembled PDU]
   6 0.076978   172.16.0.122    200.121.1.131        TCP          54 [TCP Dup ACK 2#1] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
   7 0.102939   200.121.1.131   172.16.0.122         TCP        1454 [TCP segment of a reassembled PDU]
   8 0.102946   172.16.0.122    200.121.1.131        TCP          54 [TCP Dup ACK 2#2] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
   9 0.128285   200.121.1.131   172.16.0.122         TCP        1454 [TCP segment of a reassembled PDU]
  10 0.128319   172.16.0.122    200.121.1.131        TCP          54 [TCP Dup ACK 2#3] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
  11 0.154162   200.121.1.131   172.16.0.122         TCP        1454 [TCP segment of a reassembled PDU]
  12 0.154169   172.16.0.122    200.121.1.131        TCP          54 [TCP Dup ACK 2#4] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
  13 0.179906   200.121.1.131   172.16.0.122         TCP        1454 [TCP segment of a reassembled PDU]
  14 0.179915   172.16.0.122    200.121.1.131        TCP          54 [TCP Dup ACK 2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
```

```
> Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)
> Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_42:12:13 (00:0c:29:42:12:13)
> Internet Protocol Version 4, Src: 200.121.1.131, Dst: 172.16.0.122
> Transmission Control Protocol, Src Port: 10554 (10554), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1400
```

```
0000  00 0c 29 42 12 13 00 50  56 c0 00 01 08 00 45 00   ..)B...P V.....E.
0010  05 a0 01 41 00 00 6a 06  d3 90 c8 79 01 83 ac 10   ...A..j. ...y....
0020  00 7a 29 3a 00 50 a7 5c  04 48 e2 e2 ee bf 50 10   .z):.P.\ .H....P.
0030  ff ff 77 67 00 00 30 54  73 57 77 51 74 45 79 4e   ..wg..0T sWwQtEyN
0040  45 61 33 78 70 74 44 63  51 4f 2f 6b 75 31 41 52   Ea3xptDc QO/ku1AR
0050  52 66 47 59 67 53 32 41  34 47 59 35 31 56 33 32   RfGYgS2A 4GY51V32
```

Packets: 3083 · Displayed: 3083 (100.0%) · Load time: 0:0.100 | Profile: Default

Title Bar

Menu Bar

Toolbar

Display Filte

Packet List

Packet Details

Packet Bytes

Status Bar

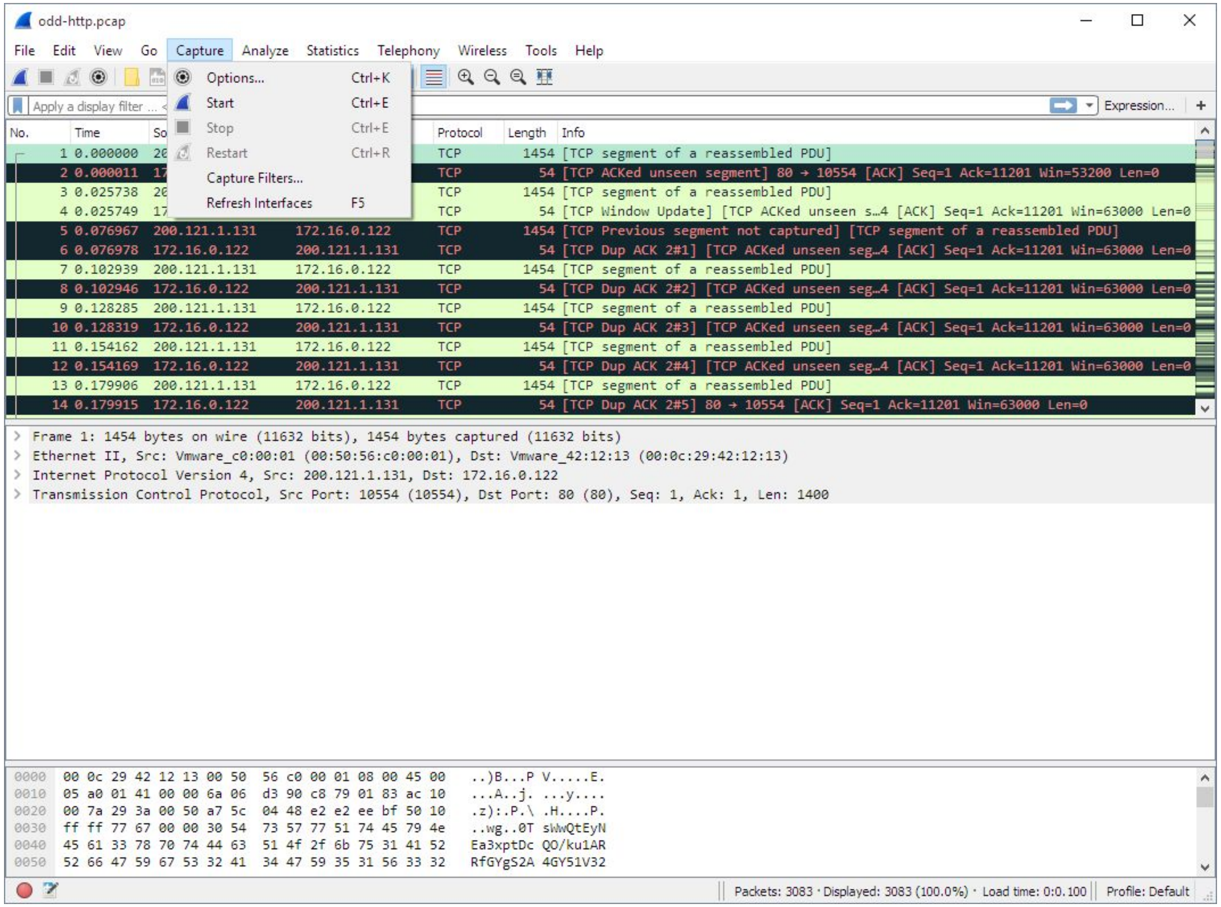
Using Wireshark: Starting a Capture

Start a Capture:

To start a new wireshark capture, choose the correct interface in Capture -> Options

Then select Start in the menu or toolbar

You will now start capturing network traffic until stopping the capture process.



```
No.     Time      So                                   Protocol  Length Info
     1 0.000000  20                                    TCP       1454 [TCP segment of a reassembled PDU]
     2 0.000011  17                                    TCP         54 [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=53200 Len=0
     3 0.025738  20                                    TCP       1454 [TCP segment of a reassembled PDU]
     4 0.025749  17                                    TCP         54 [TCP Window Update] [TCP ACKed unseen s…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
     5 0.076967  200.121.1.131    172.16.0.122         TCP       1454 [TCP Previous segment not captured] [TCP segment of a reassembled PDU]
     6 0.076978  172.16.0.122     200.121.1.131        TCP         54 [TCP Dup ACK 2#1] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
     7 0.102939  200.121.1.131    172.16.0.122         TCP       1454 [TCP segment of a reassembled PDU]
     8 0.102946  172.16.0.122     200.121.1.131        TCP         54 [TCP Dup ACK 2#2] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
     9 0.128285  200.121.1.131    172.16.0.122         TCP       1454 [TCP segment of a reassembled PDU]
    10 0.128319  172.16.0.122     200.121.1.131        TCP         54 [TCP Dup ACK 2#3] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
    11 0.154162  200.121.1.131    172.16.0.122         TCP       1454 [TCP segment of a reassembled PDU]
    12 0.154169  172.16.0.122     200.121.1.131        TCP         54 [TCP Dup ACK 2#4] [TCP ACKed unseen seg…4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
    13 0.179906  200.121.1.131    172.16.0.122         TCP       1454 [TCP segment of a reassembled PDU]
    14 0.179915  172.16.0.122     200.121.1.131        TCP         54 [TCP Dup ACK 2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
```

```
> Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)
> Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_42:12:13 (00:0c:29:42:12:13)
> Internet Protocol Version 4, Src: 200.121.1.131, Dst: 172.16.0.122
> Transmission Control Protocol, Src Port: 10554 (10554), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1400
```

```
0000  00 0c 29 42 12 13 00 50  56 c0 00 01 08 00 45 00   ..)B...P V.....E.
0010  05 a0 01 41 00 00 6a 06  d3 90 c8 79 01 83 ac 10   ...A..j. ...y....
0020  00 7a 29 3a 00 50 a7 5c  04 48 e2 e2 ee bf 50 10   .z):.P.\ .H....P.
0030  ff ff 77 67 00 00 30 54  73 57 77 51 74 45 79 4e   ..wg..0T sWwQtEyN
0040  45 61 33 78 70 74 44 63  51 4f 2f 6b 75 31 41 52   Ea3xptDc QO/ku1AR
0050  52 66 47 59 67 53 32 41  34 47 59 35 31 56 33 32   RfGYgS2A 4GY51V32
```

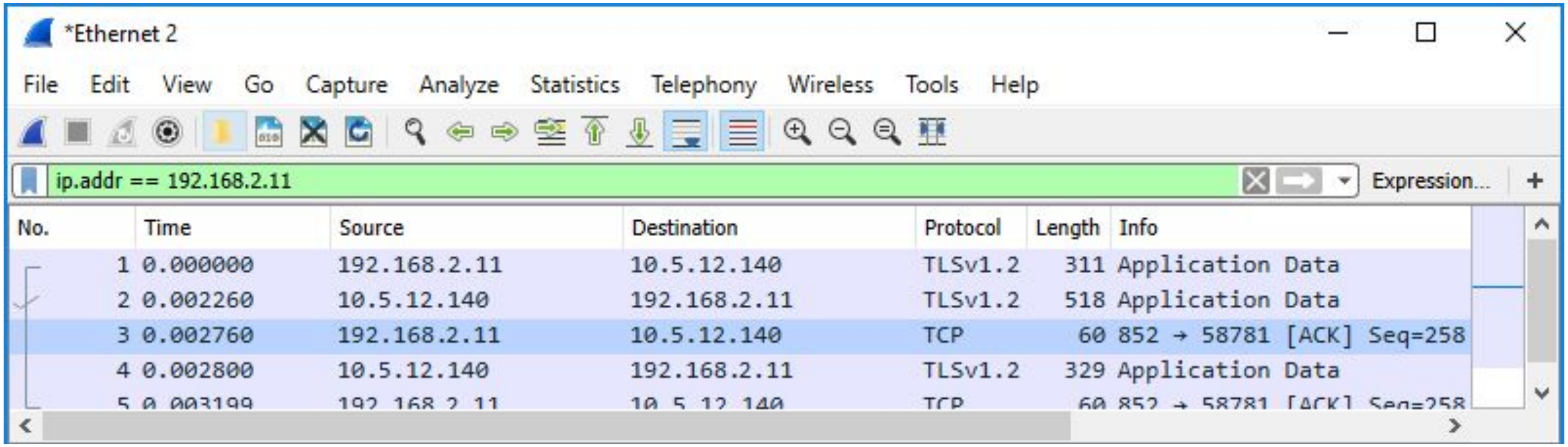
Packets: 3083 · Displayed: 3083 (100.0%) · Load time: 0:0.100 | Profile: Default

Using Wireshark: Displaying Filters

Display Filters:

- Do not limit saved packets
- Can be used with existing trace files and live captures
- All traffic is recorded for later use

The image below uses a display filter to search for packets with the ip address of 192.168.2.11



ip.addr == 192.168.2.11

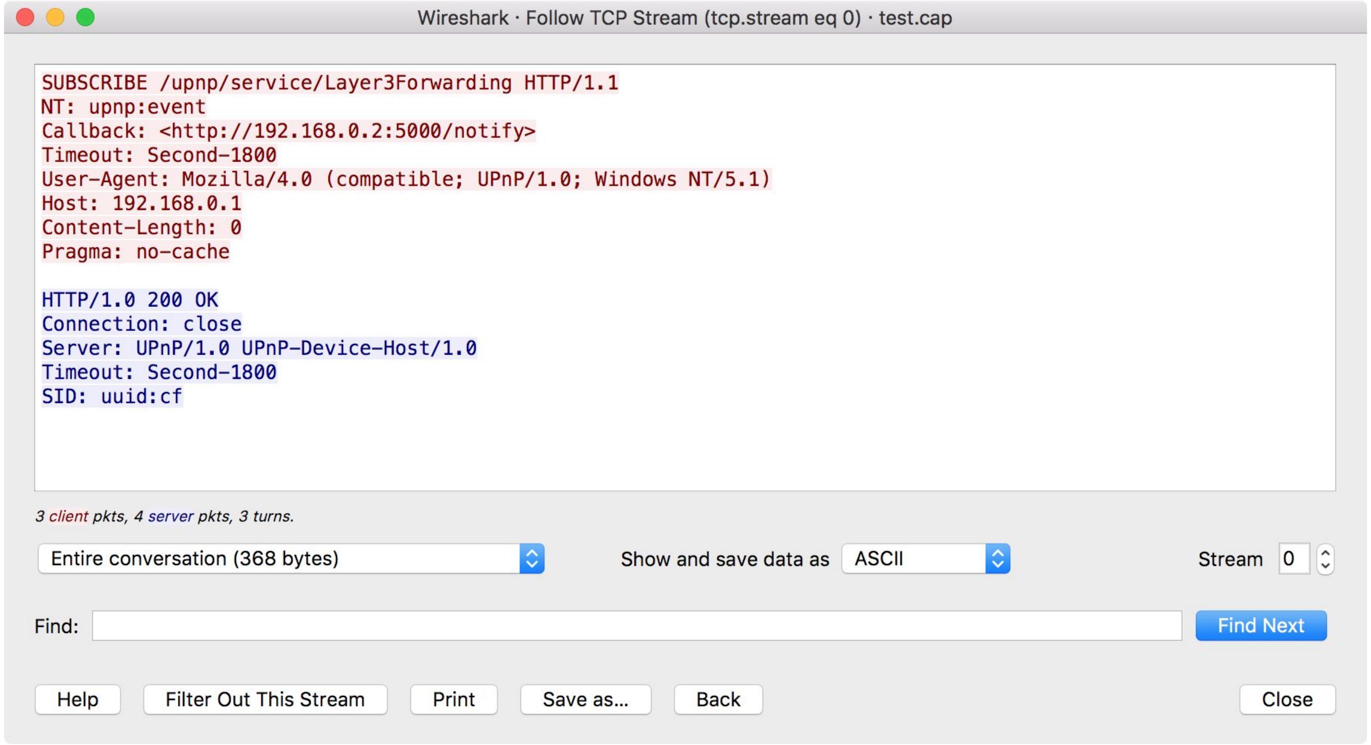
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.11	10.5.12.140	TLSv1.2	311	Application Data
2	0.002260	10.5.12.140	192.168.2.11	TLSv1.2	518	Application Data
3	0.002760	192.168.2.11	10.5.12.140	TCP	60	852 → 58781 [ACK] Seq=258
4	0.002800	10.5.12.140	192.168.2.11	TLSv1.2	329	Application Data
5	0.003199	192.168.2.11	10.5.12.140	TCP	60	852 → 58781 [ACK] Seq=258

Using Wireshark: Protocol Streams

It can be very helpful to see a protocol in the way that the application layer sees it. Perhaps you are looking for passwords in a Telnet stream, or you are trying to make sense of a data stream.

To follow a protocol stream:

1. Select a TCP, UDP, TLS, or HTTP packet in the packet list of the stream/connection you are interested in
2. Select the Follow TCP Stream menu item from the Wireshark Tools menu



Wireshark · Follow TCP Stream (tcp.stream eq 0) · test.cap

```
SUBSCRIBE /upnp/service/Layer3Forwarding HTTP/1.1
NT: upnp:event
Callback: <http://192.168.0.2:5000/notify>
Timeout: Second-1800
User-Agent: Mozilla/4.0 (compatible; UPnP/1.0; Windows NT/5.1)
Host: 192.168.0.1
Content-Length: 0
Pragma: no-cache

HTTP/1.0 200 OK
Connection: close
Server: UPnP/1.0 UPnP-Device-Host/1.0
Timeout: Second-1800
SID: uuid:cf
```

3 client pkts, 4 server pkts, 3 turns.

Entire conversation (368 bytes)

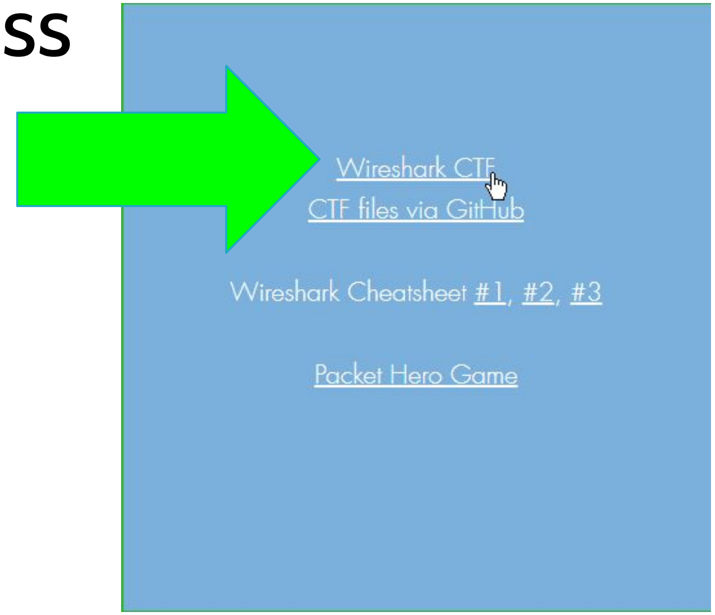
Show and save data as: ASCII

Stream: 0

Find:

Wireshark CTF

- Go to baycyber.net/intro
- Go to Day 4 “Wireshark”
- Click on “Wireshark CTF”
- Login to Netlab for access To Wireshark



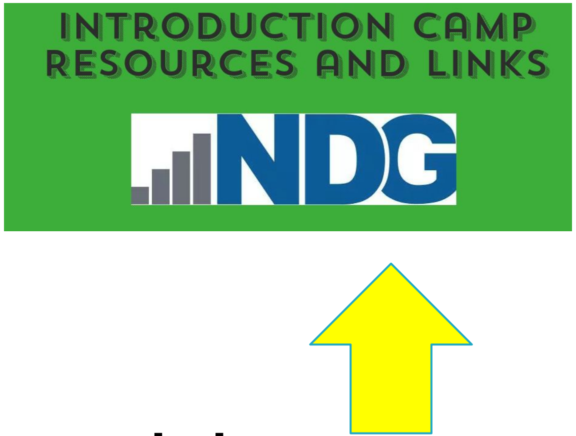
Wireshark CTF

CTF files via GitHub

Wireshark Cheatsheet #1, #2, #3

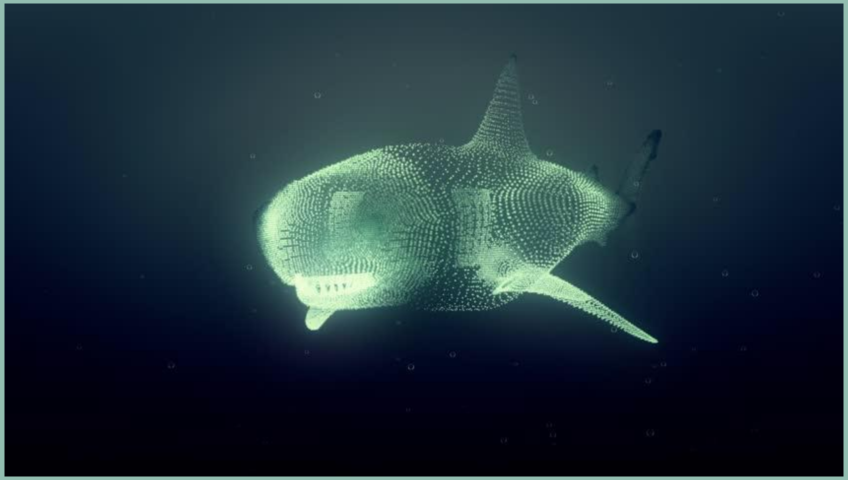
Packet Hero Game

Netlab Login



1. Log in to Netlab baycyber.net/intro
2. Click on the large “NDG” logo to access Netlab
   - See yellow arrow
3. Create a **Team Reservation** for **Cyber_Camp_2019_WireShark Access**
4. Play the Wireshark CTF!

Intro Cybercamp



BACCC
BAY AREA
COMMUNITY COLLEGE CONSORTIUM

SUMMER CAMP