



Cybersecurity 701

Wireshark Lab



Wireshark Materials

- Materials needed
 - Kali Linux Virtual Machine
 - Windows 7 Virtual Machine
- Software Tools used (From Kali Linux OS)
 - Wireshark (TCP/IP Packet Analyzer)



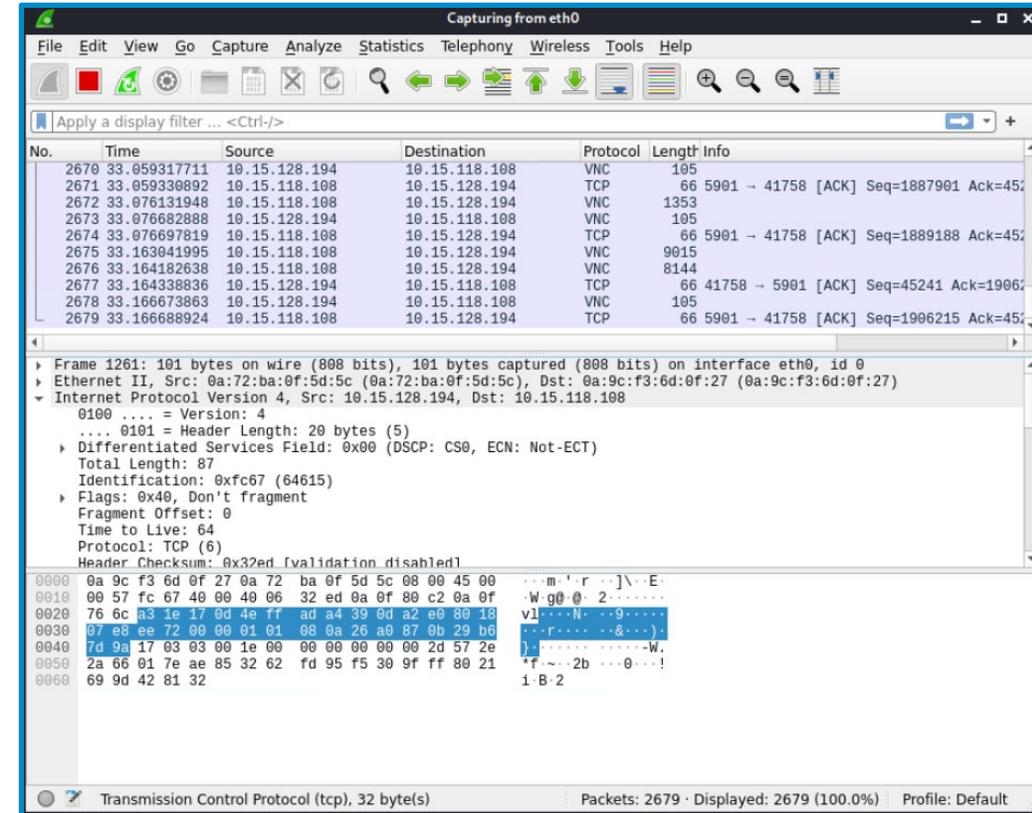
Objectives Covered

- Security+ Objectives (SY0-701)
 - Objective 4.9 - Given a scenario, use data sources to support an investigation.
 - Data sources
 - Packet captures



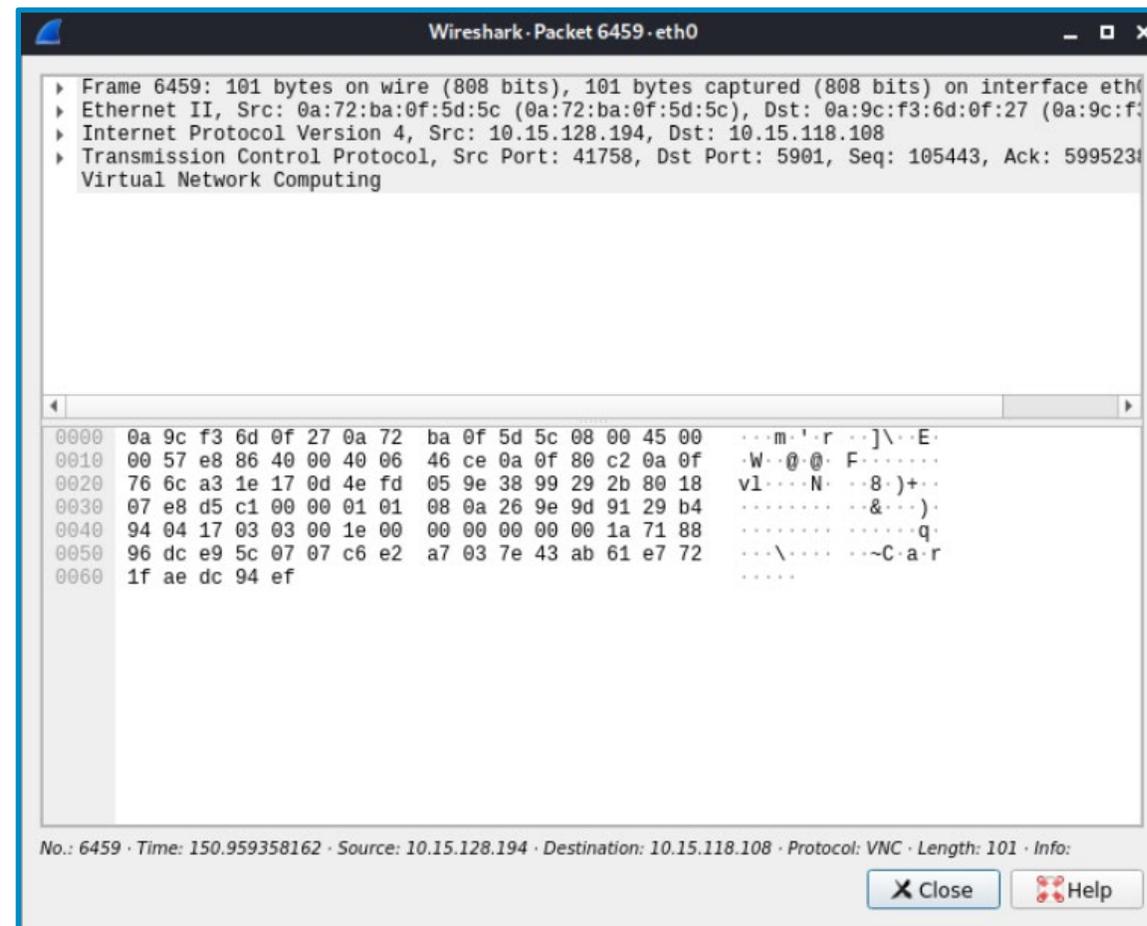
What is Wireshark?

- Wireshark is a network protocol analyzer
- Program that captures network traffic
 - Can capture packets from wired or wireless networks
 - Uses **pcap** to capture the packets
- Captures details from packets
 - Sender/Receiver IP Addresses
 - Type of packet
 - Protocol used
 - Packet contents
 - Much, much more



Wireshark Lab Overview

1. Set up Environments
2. Open Wireshark
3. Find Network Interface
4. Capture Packets
5. Analyze a Packet
6. Follow TCP Stream
7. Seeing a Capture



Set up Environments

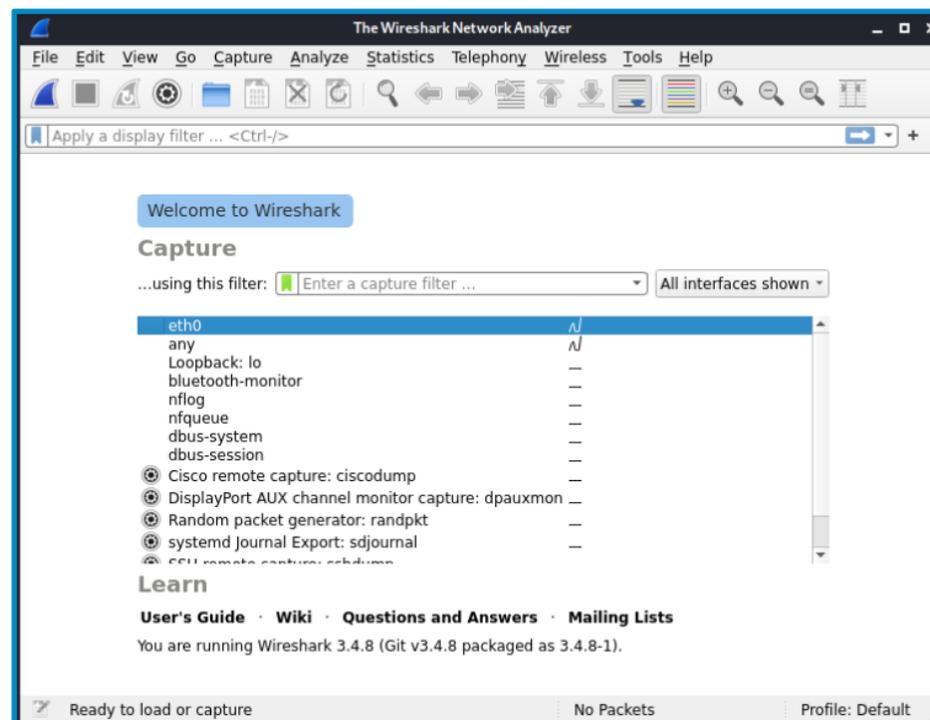
- Log into your range
- Open the Kali Linux and Windows 7 Environments
 - You should be on your Kali Linux Desktop
 - You should also be on your Windows 7 Desktop



Open Wireshark

- In Kali, open Terminal
- Use the following command to open the Wireshark application
sudo wireshark
- You should see Wireshark open

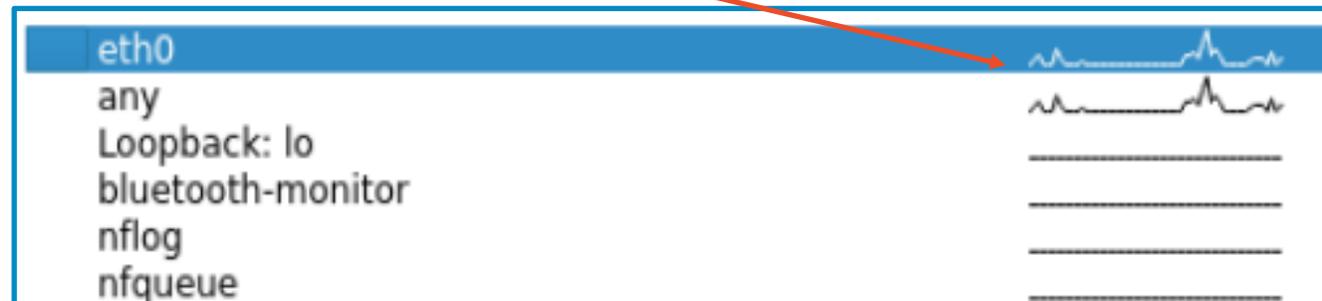
```
(kali@10.15.118.108) - [~]  
$ sudo wireshark
```



Find Network Interface

- Open a web browser
- Navigate to a couple of websites
- You should start to see Wireshark show some changes
- Notice which interface is showing more traffic while you are loading webpages

Lots of network traffic

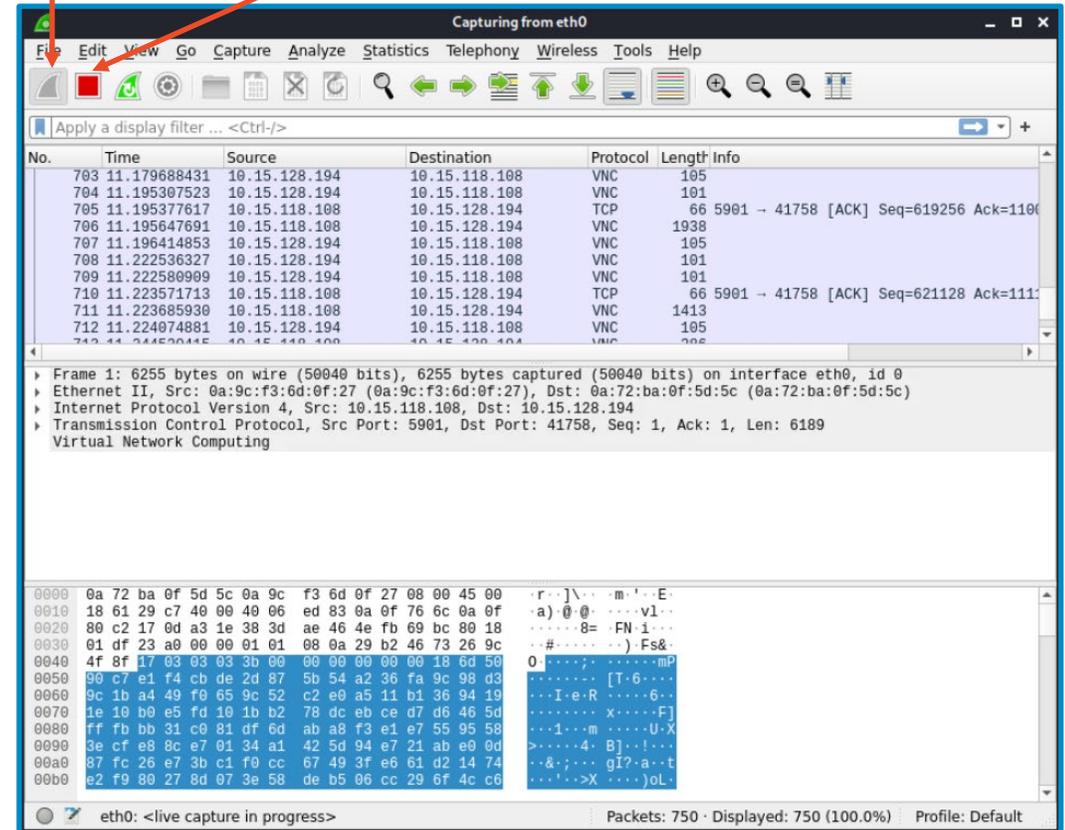


Capture Packets

- Select the active network
- Click the blue fin (top left) to start
- Visit a website in the browser
- Go back to Wireshark
- Click the Red box to stop capturing

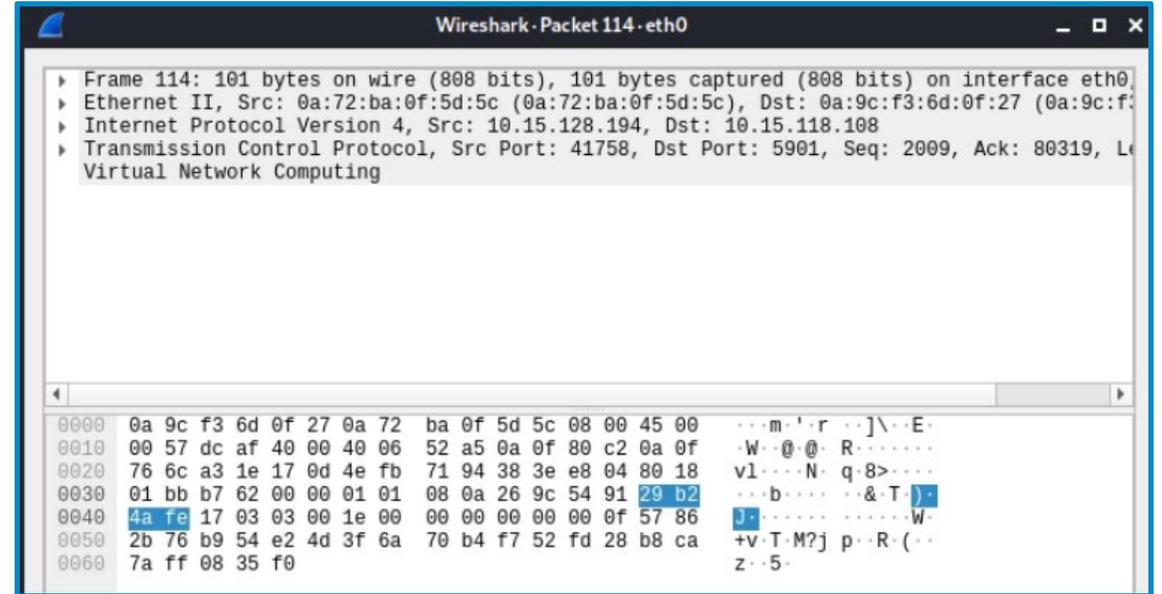
Starts Capture

Stops Capture



Analyze a Packet

- Double click on a packet
 - This will display the contents of the packet
- Find the following:
 - Length of the packet
 - Sender's and receiver's IP addresses
 - Protocol used
 - Source's MAC Address
 - Destination's MAC Address
 - Anything else?



Wireshark - Packet 114 - eth0

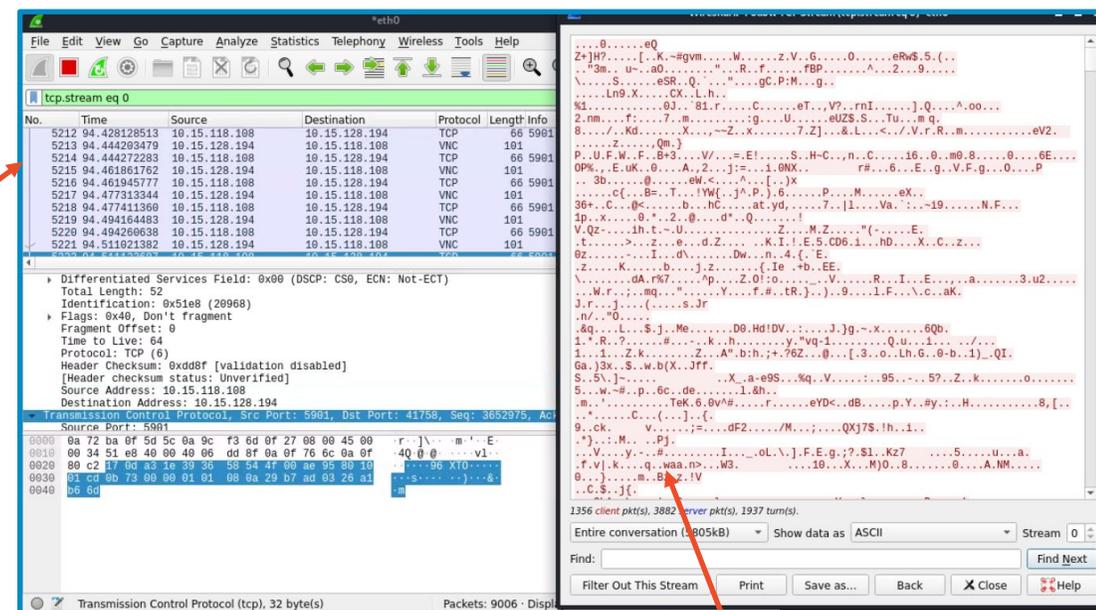
```
▶ Frame 114: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface eth0
▶ Ethernet II, Src: 0a:72:ba:0f:5d:5c (0a:72:ba:0f:5d:5c), Dst: 0a:9c:f3:6d:0f:27 (0a:9c:f3:6d:0f:27)
▶ Internet Protocol Version 4, Src: 10.15.128.194, Dst: 10.15.118.108
▶ Transmission Control Protocol, Src Port: 41758, Dst Port: 5901, Seq: 2009, Ack: 80319, Len: 101, Window: 65535,
  Virtual Network Computing
```

0000	0a 9c f3 6d 0f 27 0a 72 ba 0f 5d 5c 08 00 45 00	...m.'r...]\..E.
0010	00 57 dc af 40 00 40 06 52 a5 0a 0f 80 c2 0a 0f	·W·@·@·R·.....
0020	76 6c a3 1e 17 0d 4e fb 71 94 38 3e e8 04 80 18	v1...·N·q·8>.....
0030	01 bb b7 62 00 00 01 01 08 0a 26 9c 54 91 29 b2	...b...·&·T·)·
0040	4a fe 17 03 03 00 1e 00 00 00 00 00 0f 57 86	J·.....·W·
0050	2b 76 b9 54 e2 4d 3f 6a 70 b4 f7 52 fd 28 b8 ca	+v·T·M?j p·R·(·
0060	7a ff 08 35 f0	z··5·

Sample Packet

Follow TCP Stream

- Find a Packet
 - Find a TCP Protocol packet if possible
- Right-Click on the packet
- Go to the “follow” option
- Select the “TCP Stream” option
- The window shows all the data from this stream
 - Stream = multiple packets that makeup an exchange of data
- The main Wireshark window is displaying all the packets in this stream
- What are you seeing?
 - This is a webserver communicating with a browser
 - Each website you visit carries out a similar exchange



All the packets

Individual packet's data

Starting a Capture

- Start capturing data in Wireshark
- Open another Terminal
- Ping an IP Address of another device
 - `ping -c 5 <IP_Address>`
 - Let the ping run the 5 times
- Stop capturing data in Wireshark

```
(kali@10.15.118.108) - [~]
└─$ ping -c 5 10.15.112.18
PING 10.15.112.18 (10.15.112.18) 56(84) bytes of data.
64 bytes from 10.15.112.18: icmp_seq=1 ttl=128 time=1.48 ms
64 bytes from 10.15.112.18: icmp_seq=2 ttl=128 time=0.370 ms
64 bytes from 10.15.112.18: icmp_seq=3 ttl=128 time=0.335 ms
64 bytes from 10.15.112.18: icmp_seq=4 ttl=128 time=0.413 ms
64 bytes from 10.15.112.18: icmp_seq=5 ttl=128 time=0.546 ms
```



Viewing the Capture

- In Wireshark, search for the following in the display filter up top
 - `ip.addr == <IP Address>`
 - Use the IP Address of device you pinged

Display filter search

Ping

Response

No.	Time	Source	Destination	Protocol	Length	Info
165	3.179255736	10.15.118.108	10.15.112.18	ICMP	98	Echo (ping) request id=0x9f33, seq=1/2
166	3.180715046	10.15.112.18	10.15.118.108	ICMP	98	Echo (ping) reply id=0x9f33, seq=1/2
178	4.180915088	10.15.118.108	10.15.112.18	ICMP	98	Echo (ping) request id=0x9f33, seq=2/5
179	4.181258527	10.15.112.18	10.15.118.108	ICMP	98	Echo (ping) reply id=0x9f33, seq=2/5
211	5.212551454	10.15.118.108	10.15.112.18	ICMP	98	Echo (ping) request id=0x9f33, seq=3/7
212	5.212859161	10.15.112.18	10.15.118.108	ICMP	98	Echo (ping) reply id=0x9f33, seq=3/7
296	6.236569615	10.15.118.108	10.15.112.18	ICMP	98	Echo (ping) request id=0x9f33, seq=4/1
297	6.236956076	10.15.112.18	10.15.118.108	ICMP	98	Echo (ping) reply id=0x9f33, seq=4/1
473	7.260520282	10.15.118.108	10.15.112.18	ICMP	98	Echo (ping) request id=0x9f33, seq=5/1
474	7.261038490	10.15.112.18	10.15.118.108	ICMP	98	Echo (ping) reply id=0x9f33, seq=5/1

Questions to Ponder

- Why is there so much back and forth between the two IP addresses?
- Are there other packets being captured? If so, what do you think they're for?
- Do different actions on the Windows 7 machine result in different packet captures via Wireshark?

