Cybersecurity 701

Wireshark Lab

Wireshark Materials

- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine

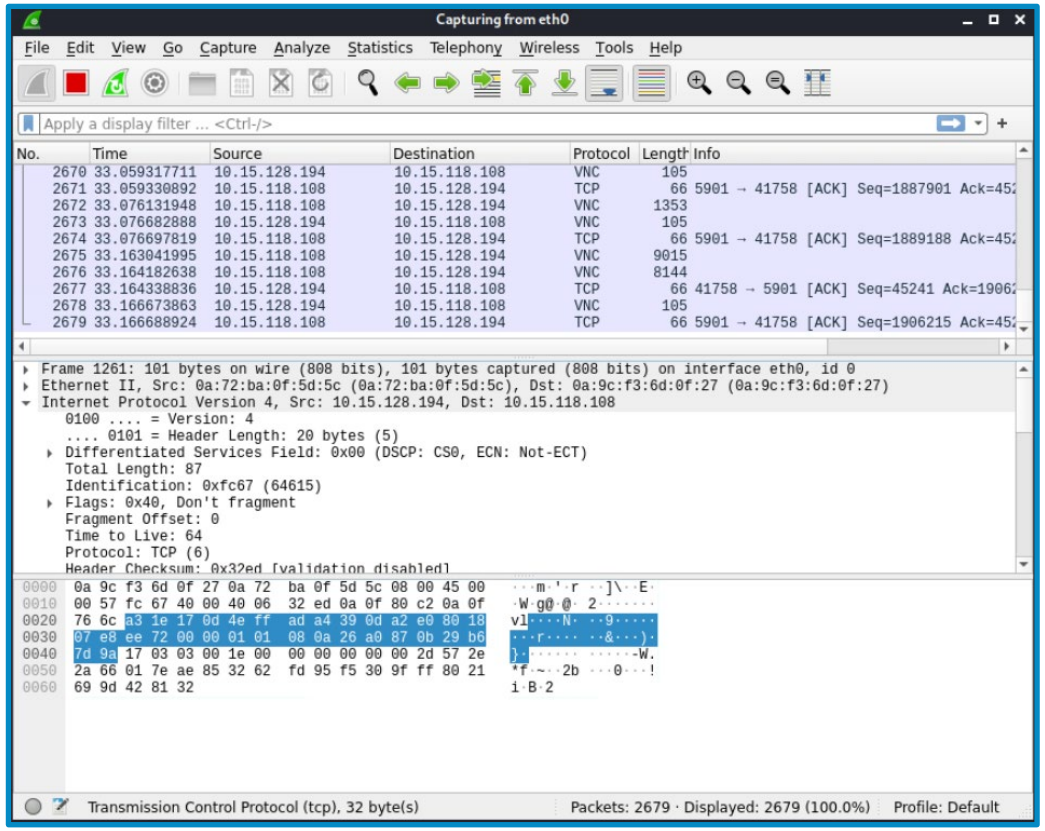
- Software Tools used (From Kali Linux OS)
  - Wireshark (TCP/IP Packet Analyzer)

Objectives Covered

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

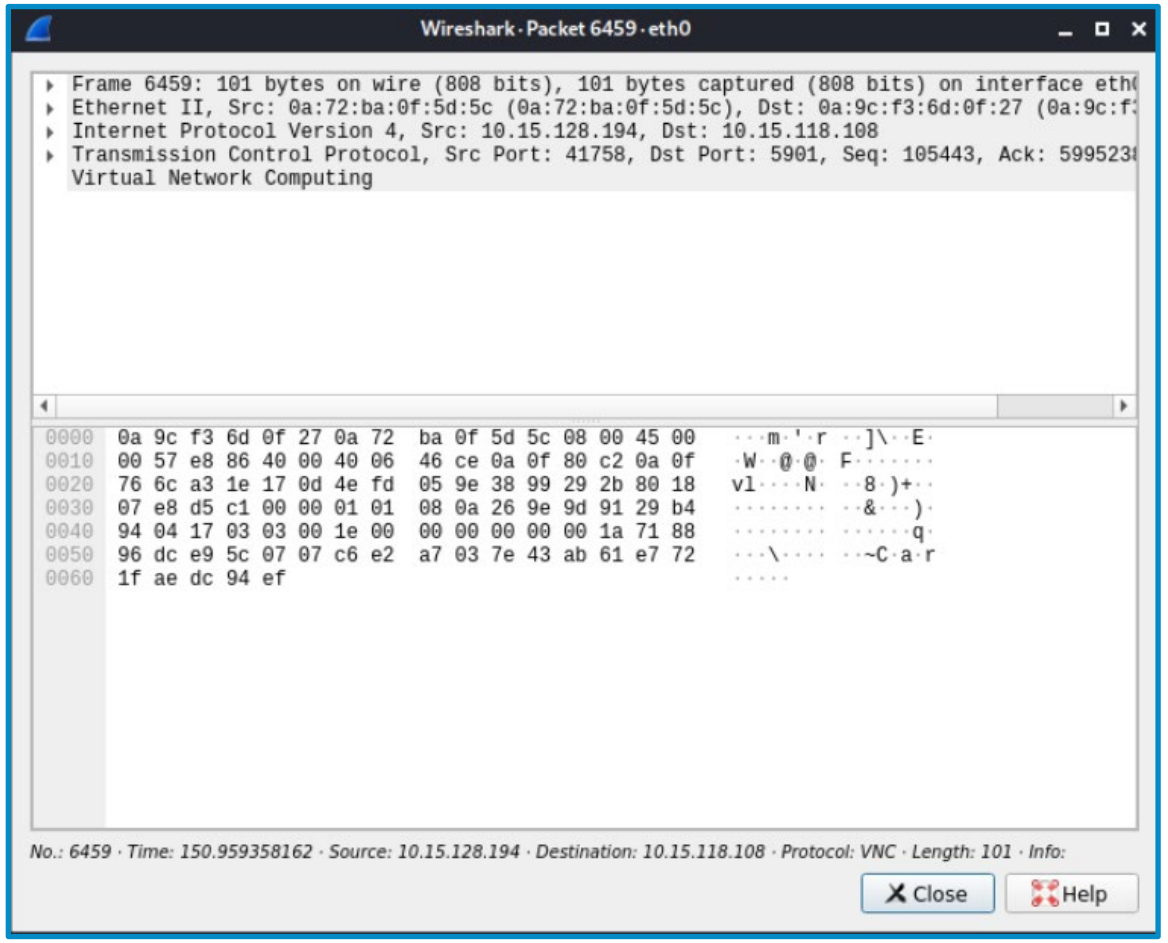
What is Wireshark?

- 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

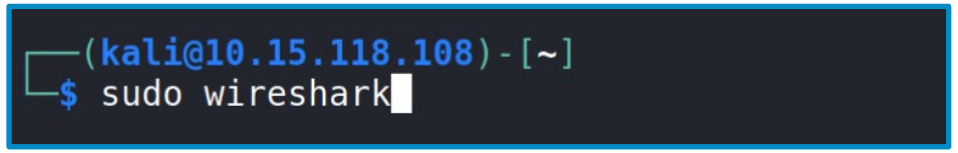
- Log into your range
- Open the Kali Linux and Windows 7 Environments
  - You should be on your Kali Linux Desktop
  - You should also be on your Windows 7 Desktop

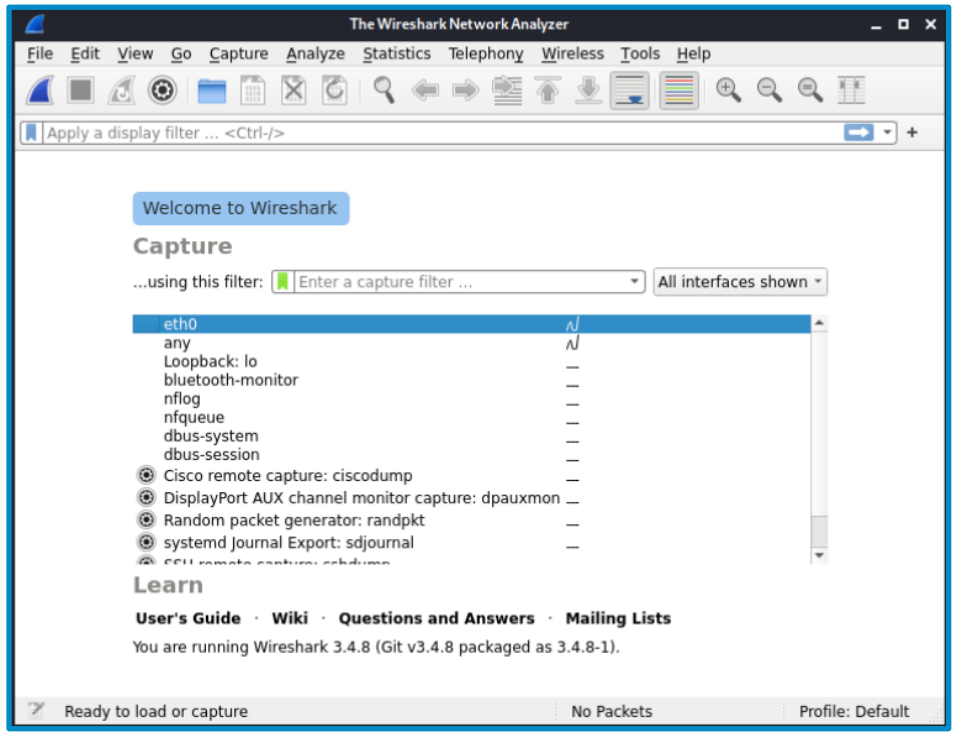
Open Wireshark

- In Kali, open Terminal
- Use the following command to open the Wireshark application

  `sudo wireshark`

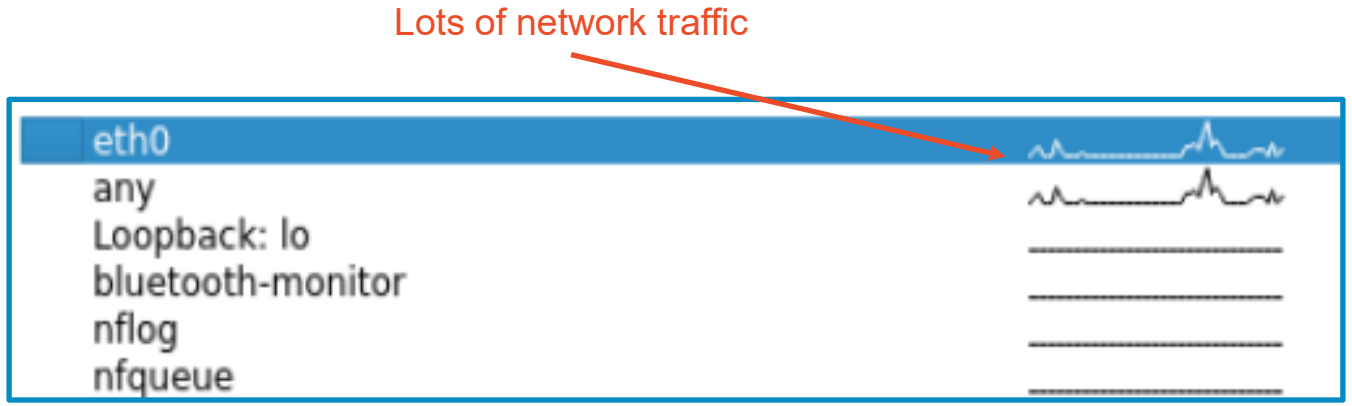
- You should see Wireshark open





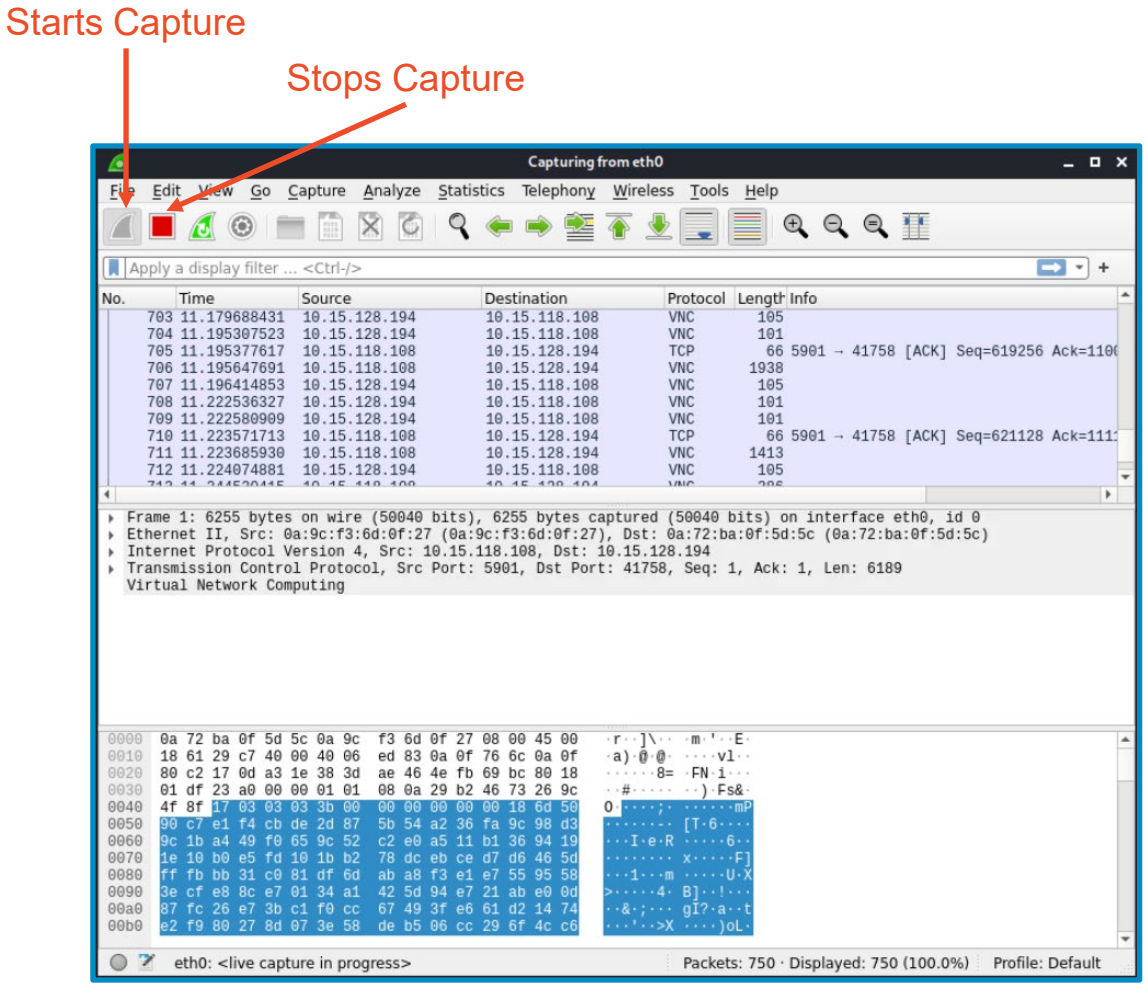
Find Network Interface

- 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



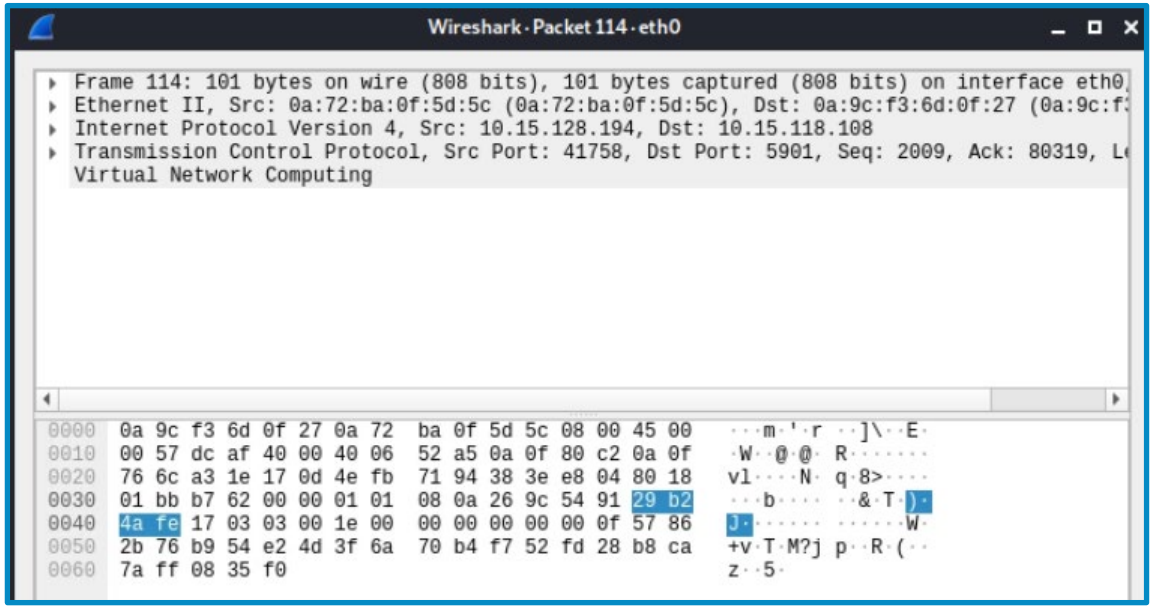
Capture Packets

- 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



Analyze a Packet

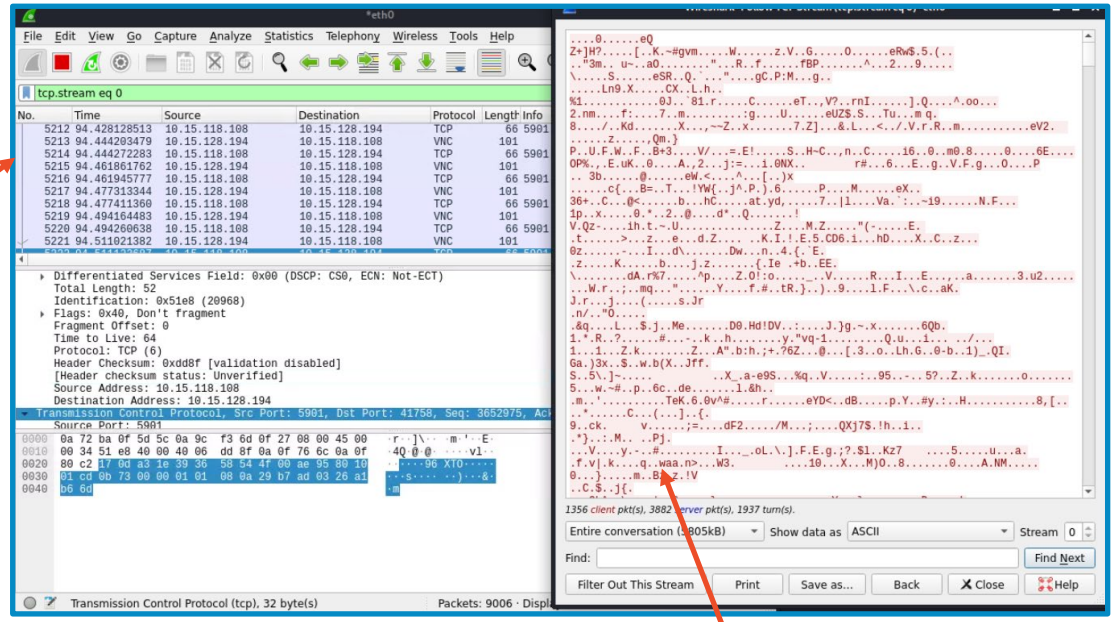
- Double click on a packet
  - This will display the contents of the packet
- Find the following:
  - Length of the packet
  - Sender's and receiver's IP addresses
  - Protocol used
  - Source’s MAC Address
  - Destination’s MAC Address
  - Anything else?



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



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

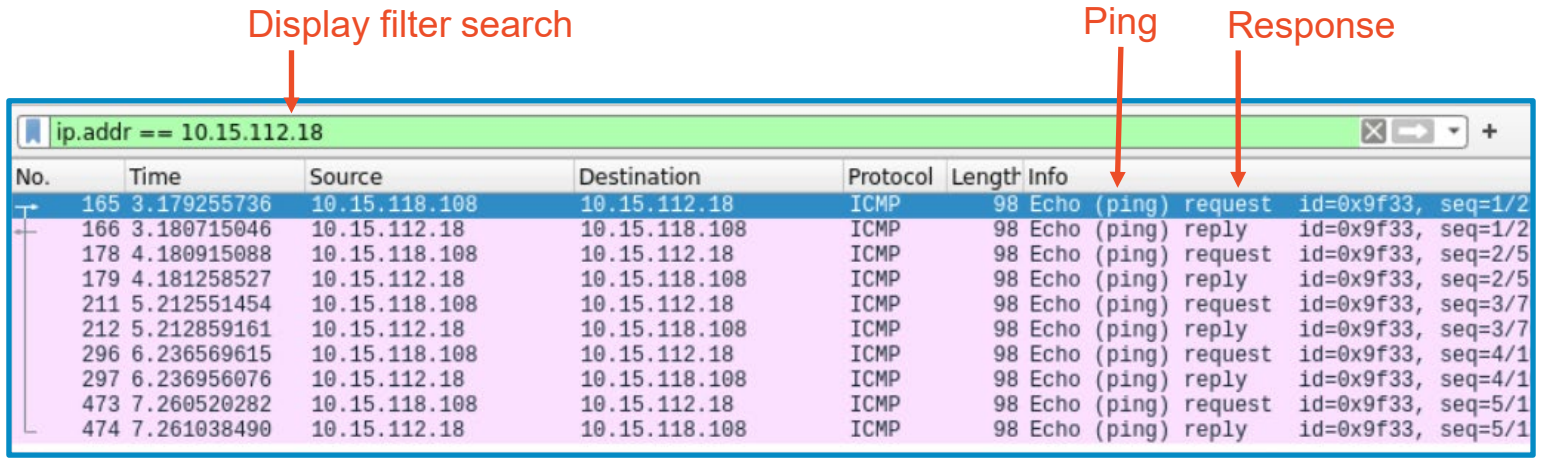
```
┌──(kali@10.15.118.108)-[~]
└─$ ping -c 5 10.15.112.18
PING 10.15.112.18 (10.15.112.18) 56(84) bytes of data.
64 bytes from 10.15.112.18: icmp_seq=1 ttl=128 time=1.48 ms
64 bytes from 10.15.112.18: icmp_seq=2 ttl=128 time=0.370 ms
64 bytes from 10.15.112.18: icmp_seq=3 ttl=128 time=0.335 ms
64 bytes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



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?