Northwest State Community College

Packet Capture Using Wireshark

Made possible through support from the National Science Foundation (NSF) award number 1800929

Objectives

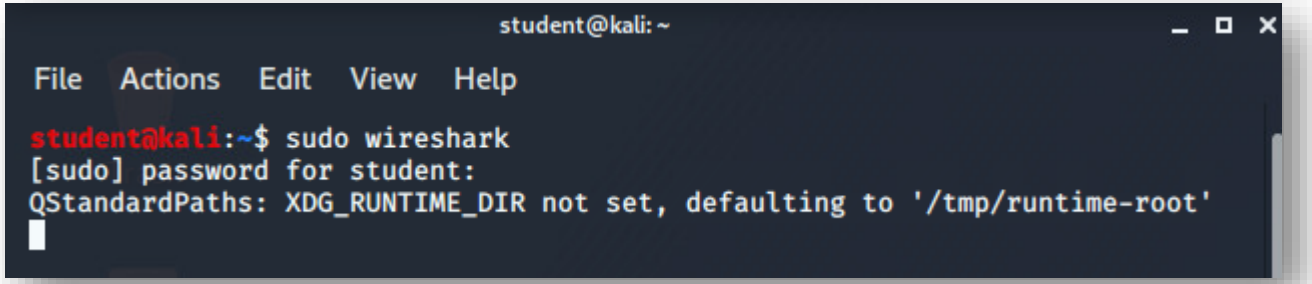
- Discuss the purpose of packet capture software such as Wireshark.
- Use Wireshark to capture network data.
- Explain the different ways Wireshark can present and format captured data.
- Control the display and capture of network data using filters.
- Discuss various ways networks and network devices can be manipulated to allow the capture of network traffic.

Wireshark Overview

- What is Wireshark?
  - Wireshark is software that allows us to view all data being transmitted on a network
  - Wireshark allows us to view fully decoded data or view data in its raw (binary) format
  - Wireshark is free, open-source software
  - Wireshark is available for multiple platforms (Linux, MAC, Windows)
    - https://www.wireshark.org

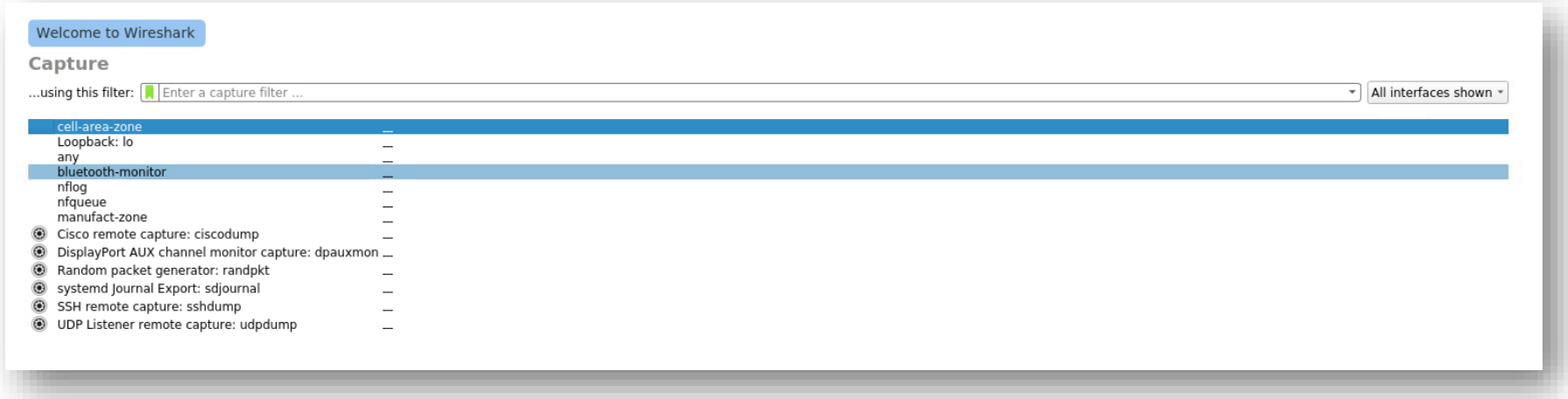
Wireshark Simple Usage

- Download and install
- Needs to be run as the super-user or permissions need to be configured to allow regular user access



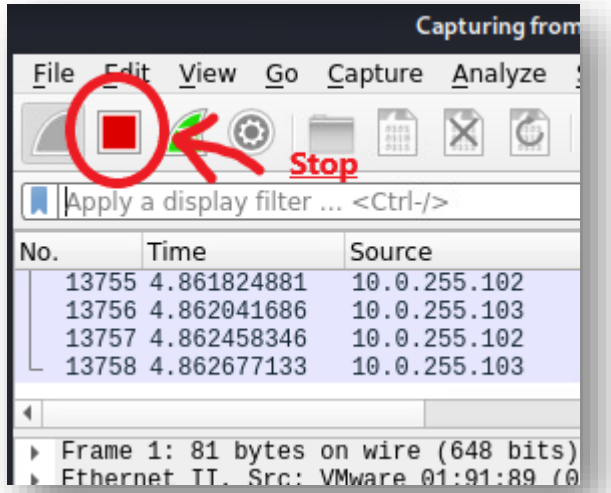
Wireshark Simple Usage

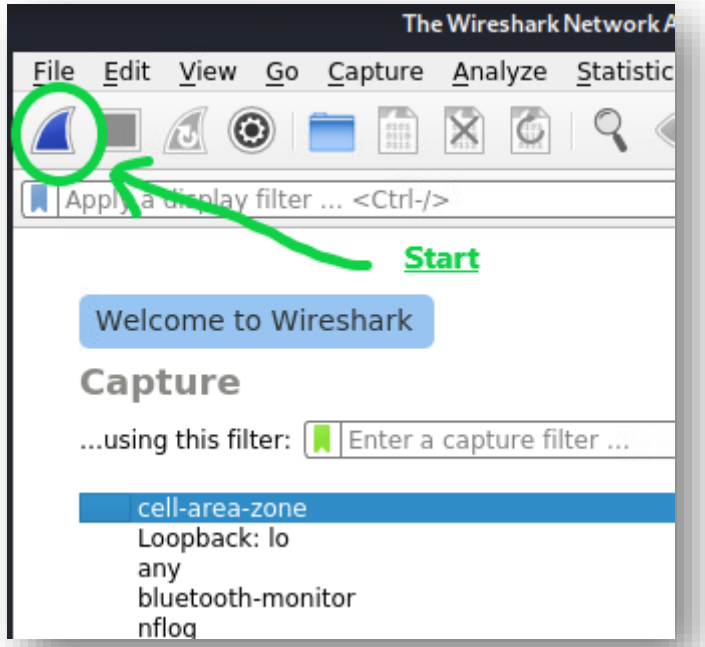
- Select the interface to be used to capture the data



Wireshark Simple Usage

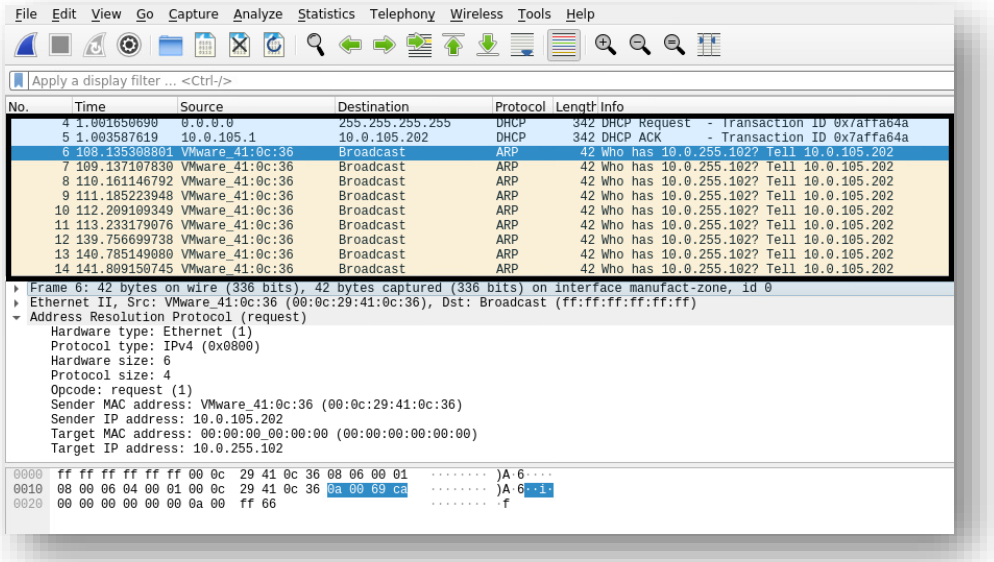
- Click the Start button to begin capture
- Click the Stop button to end capture





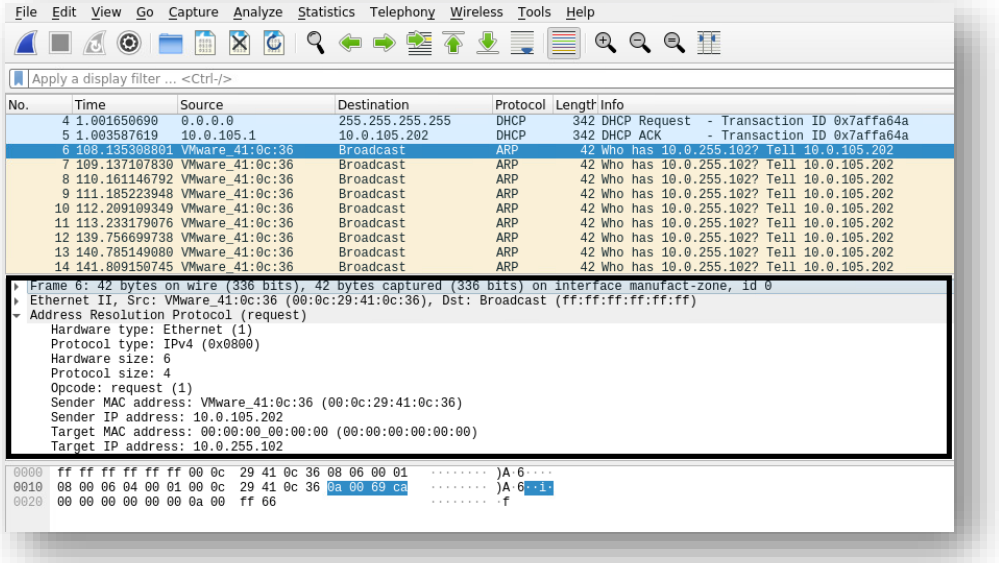
Wireshark Screen Layout

- When viewing a packet capture, the Wireshark screen is divided into three sections
- The top pane (packet list) shows an ordered list containing a summary of each packet captured



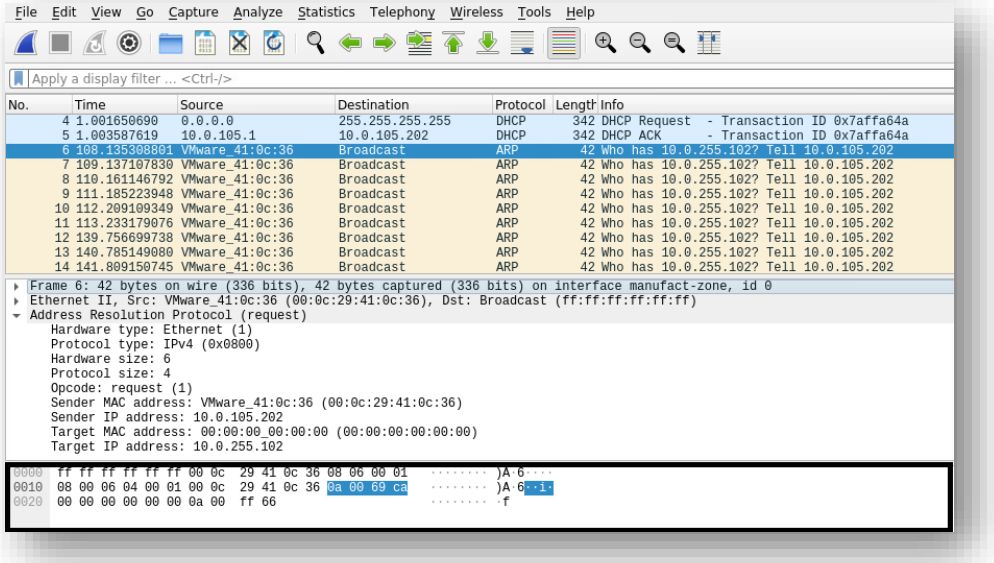
Wireshark Screen Layout

- When viewing a packet capture, the Wireshark screen is divided into three sections
- The middle pane (packet details) shows detailed and decoded data associated with the packet selected in the packet list pane
  - Some summary data listed in the packet details pane can be expanded to provide more detailed information about the section of the packet being displayed



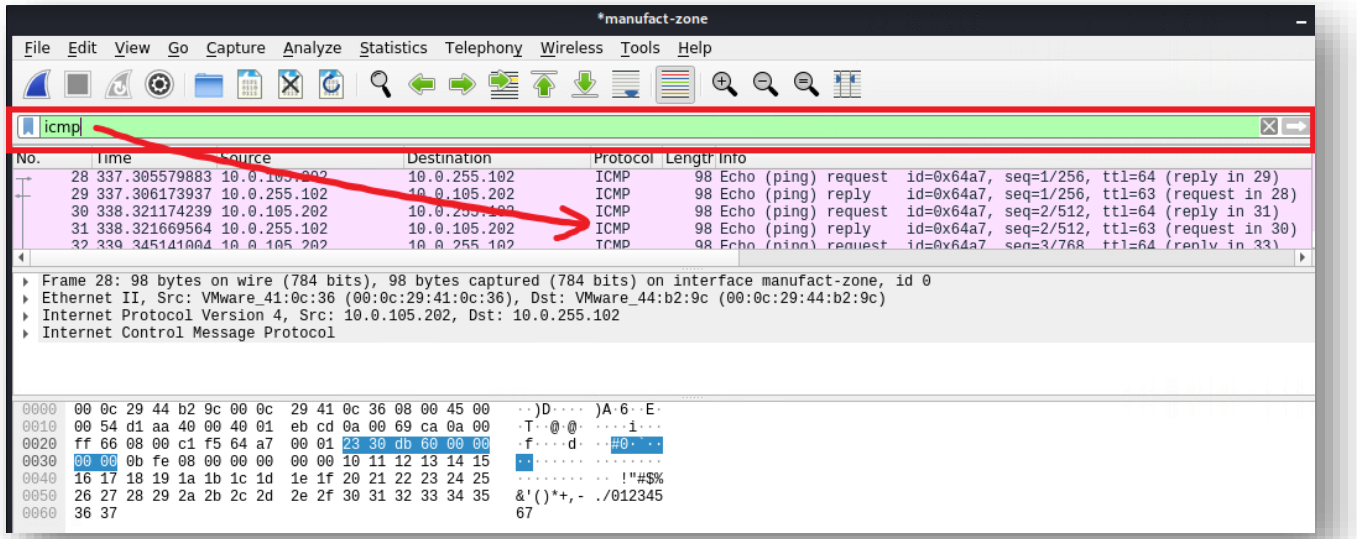
Wireshark Screen Layout

- When viewing a packet capture, the Wireshark screen is divided into three sections
- The bottom pane (packet bytes) shows the raw (binary) data associated with the packet selected in the packet list pane
  - If any decoded data is selected in the packet details pane the associated raw data will be highlighted in the packet bytes pane



Wireshark Filters

- Wireshark display filters can be typed into the filter toolbar to limit the data displayed and make it easier to view only specific packets



Wireshark Filters

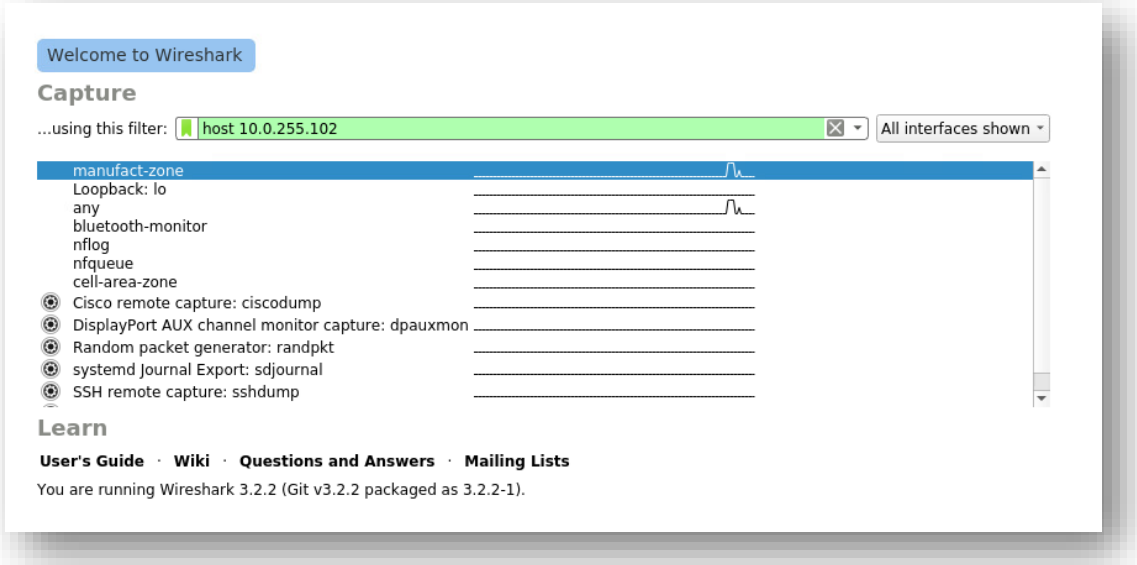
- Here are some example and commonly used display filters

Filter	Purpose
Protocol name (i.e. dhcp, icmp, telnet)	Display only data from packets which implement a specific protocol
ip.addr == 192.168.1.1	Display only data coming from or going to the IP address 192.168.1.1
ip.src == 10.0.255.10 and ip.dst == 10.0.105.202	Display only data coming from the IP address 10.0.255.10 AND going to the IP address 10.0.105.202

- For more information see https://wiki.wireshark.org/DisplayFilters

Wireshark Filters

- Wireshark also supports capture filters which can be applied prior to starting the data capture
- Wireshark capture filters limit the data before capture while display filters limit the amount data display after capture



Wireshark Filters

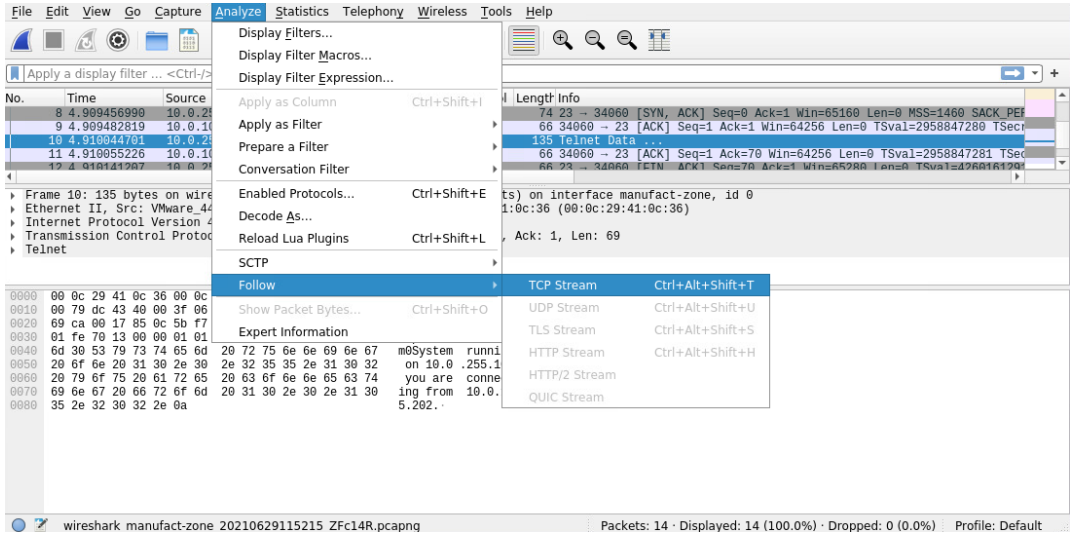
- Wireshark capture filters use a different syntax then display filters
- Wireshark capture filters use the pcap-filter syntax which is used by other network monitoring software packages such as the command line tcpdump program found on many Linux and Unix based systems
- For more information see https://wiki.wireshark.org/CaptureFilters

Filter Examples:

- Host: *host 192.168.1.2*
- HTTP: *tcp and port 80*
- Traffic between hosts: *ip host 192.168.1.1 and 192.168.1.2*
- Traffic from an host to another: *ip src 192.168.1.1 and dst 192.168.1.2*

Wireshark Follow Stream

- Wireshark has the capability to combine all the packets in a protocol stream together then display them on a single screen in several different formats

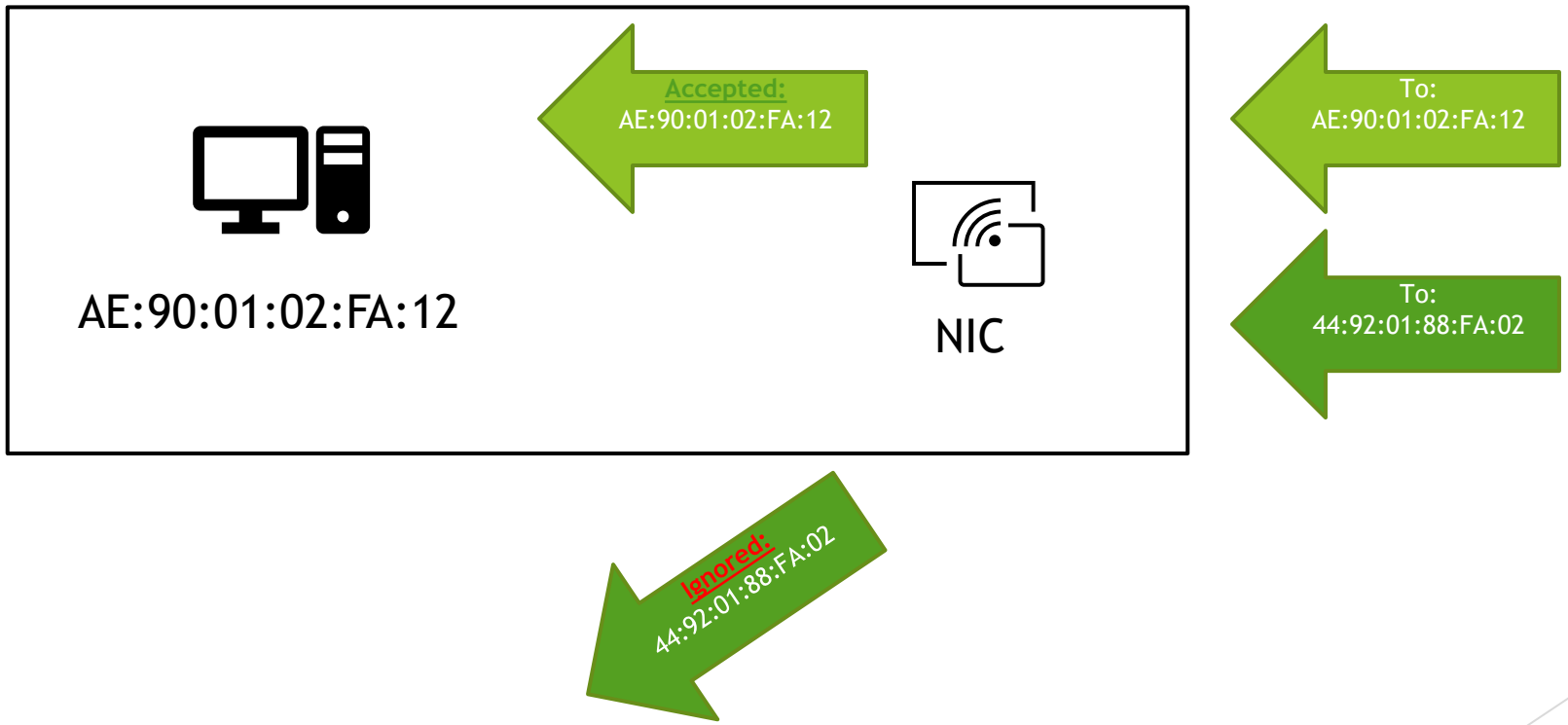


Wireshark Packet Files

- Wireshark has the ability open, decode and analyze data saved in a wide variety of formats for example:
  - Wireshark's native format is libpcap which can be generated by many programs and network devices
  - Microsoft Network Monitor captures
  - Oracle snoop and atmsnoop captures
  - Novell LANalyzer captures
  - pppd log files
  - IBM OS/400 communication traces
  - MPEG-2 transport streams

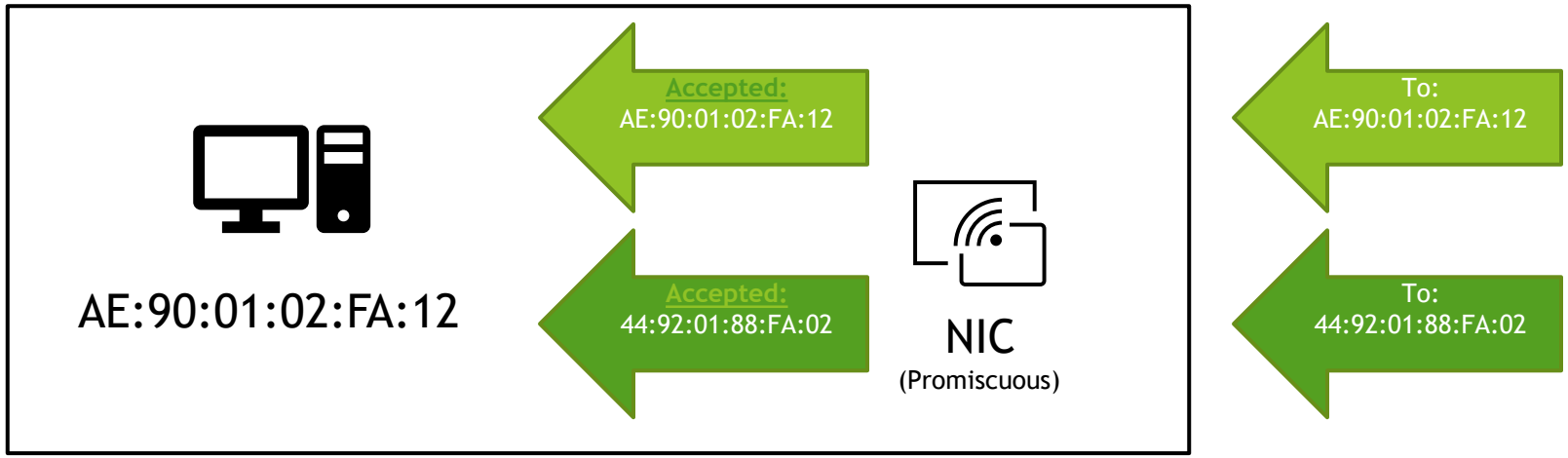
Wireshark Capture Problems

- Network interface cards (NIC) are designed to process network traffic addressed to themselves and discard all other network traffic



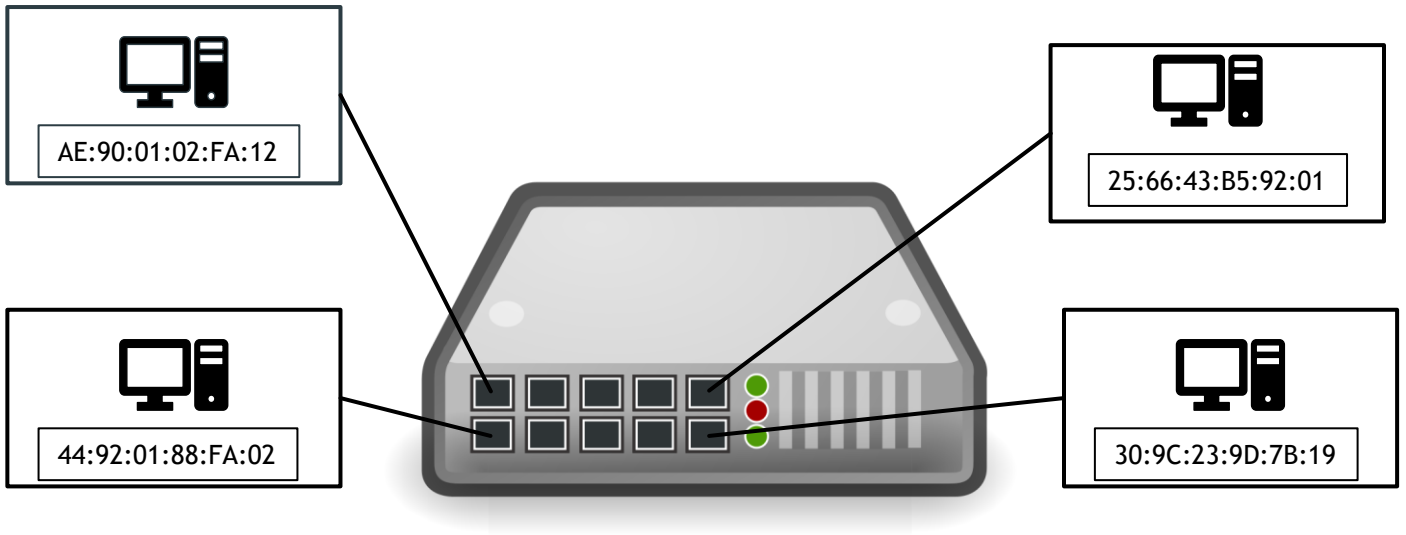
Wireshark Capture Problems

- To resolve this, some, but not all, network interface cards (NIC) can be configured to accept all traffic
  - Ethernet network cards may support promiscuous mode
  - Wireless network cards may support monitor mode



Wireshark Capture Problems

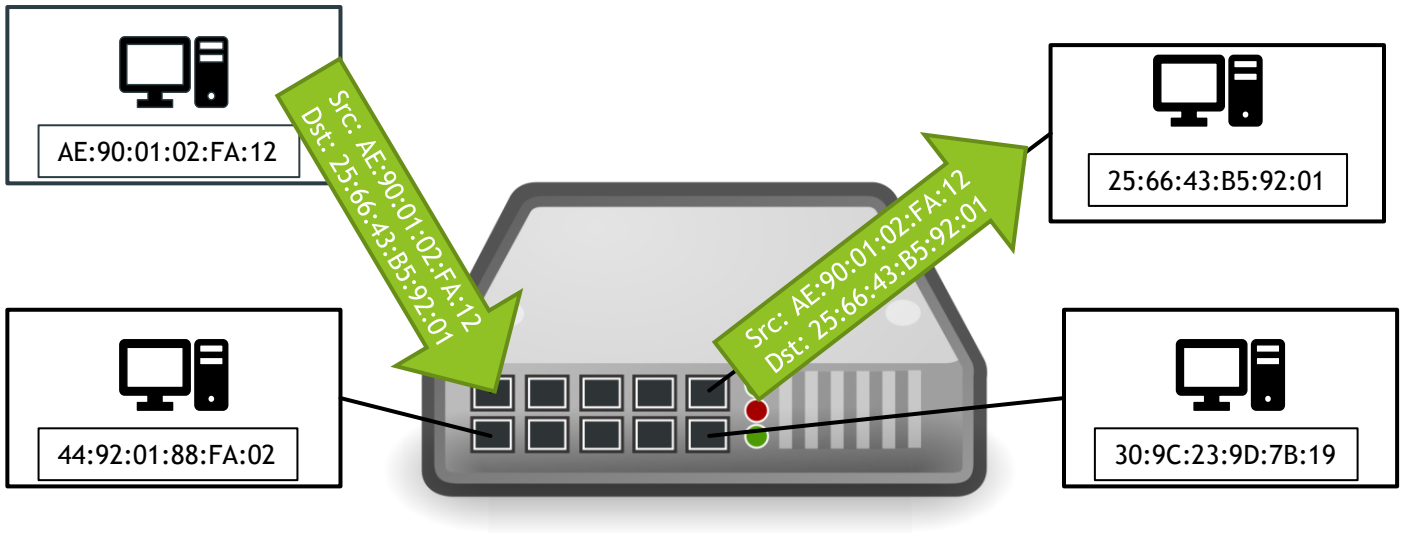
- Network switches are designed to learn the addresses of systems connected to each port and store that information in a MAC address table



Port	Address
1	AE:90:01:02:FA:12
2	44:92:01:88:FA:02
3	None
4	None
5	None
6	None
7	None
8	None
9	25:66:43:B5:92:01
10	30:9C:23:9D:7B:19

Wireshark Capture Problems

- Traffic is then forwarded out only on the port containing the system with the proper destination address
- Traffic from 192.168.1.101 to 192.168.1.109 would only be seen on ports 1 and 9



Port	Address
1	AE:90:01:02:FA:12
2	44:92:01:88:FA:02
3	None
4	None
5	None
6	None
7	None
8	None
9	25:66:43:B5:92:01
10	30:9C:23:9D:7B:19

Wireshark Capture Problems

- There are multiple ways to resolve this, the following methods are often used by network administrators to legally monitor network traffic
  - Many network switches provide a feature that can be configured to mirror traffic from one another monitor port
  - Devices called network taps can be purchased and inserted into network where the tap will copy all traffic received onto a monitor port

Wireshark Capture Problems

- There are multiple ways to resolve this, the following methods are used by hackers to illegally monitor network traffic
  - Some switches MAC tables can be overloaded which will cause it to forward traffic out on all ports
  - A technique known as ARP spoofing can fool the switch into thinking a port contains an address it does not

For More Information

- For further information go to https://www.nl.northweststate.edu/camo or contact:
  - Tony Hills – thills@northweststate.edu – 419-267-1354
  - Sarah Stubblefield – sstubblefield@northweststate.edu – 419-267-1512
  - Mike Kwiatkowski – mkwiatkowski@northweststate.edu – 419-267-1231

Made possible through support from the National Science Foundation (NSF) award number 1800929