

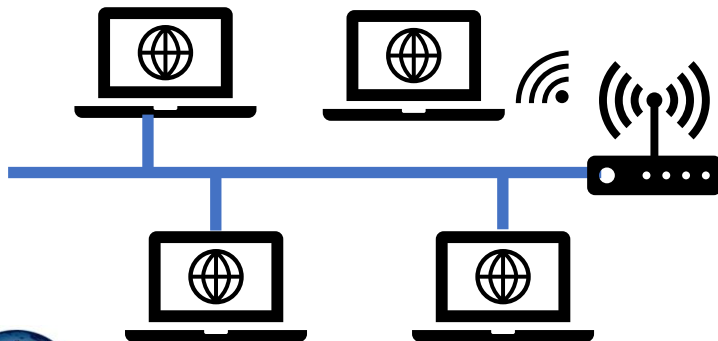
Introduction to Networks and Wireshark

Overview of Networking



UNIVERSITY OF MARYLAND
GLOBAL CAMPUS

What is a Network?



- When you connect two or more computers or devices, you have “networked” them together
- **Networks** can use wires and radio waves (wi-fi)
- Usually, you want or need more than two devices talking to each other
 - Introduce more networking hardware to help
 - A **router** symbol shows both wired and wireless network

Speaking the Same Language

- Information exchange must be done so that all parties can understand the information being shared
- What happens if you show up to a class and your teacher is speaking Korean and you only know French? How well does that information exchange work?
- There has to be an agreement on the language used for exchanging human information
- Computers are the same – they need to agree on how to exchange information
 - These **network protocols** provide a common “language” for how to communicate



Network Protocols

- Definition: A set of rules that governs the connection of computer systems to the internet (Oxford Dictionary)
- Ever heard of TCP/IP?
 - **TCP** = Transmission Control Protocol
 - **IP** = Internet Protocol
- The two protocols are used together to establish and maintain a network conversation
- TCP focuses on establishing and maintaining a **network connection**
 - Connection-oriented, knows if a packet is missing
- IP defines how computers send **packets** of data to each other

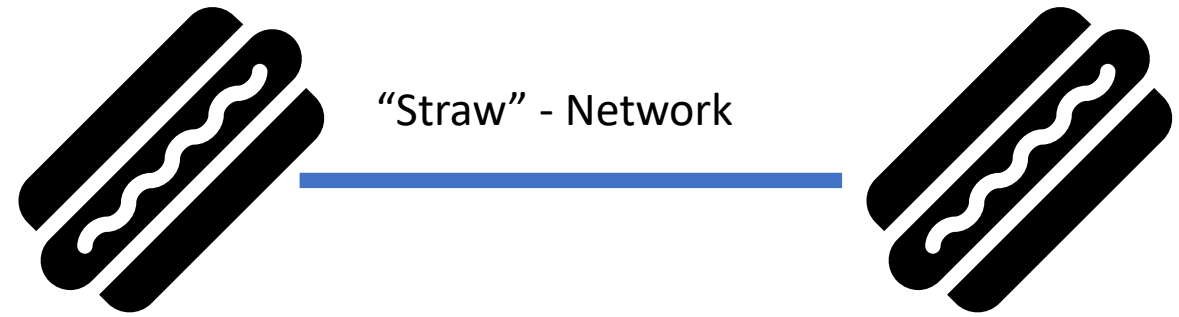


Network Protocols – Continued

- In addition to TCP, there is UDP
 - **UDP** = User Datagram Protocol
 - Unlike TCP, UDP doesn't guarantee that the packets will get to the right destinations.
 - UDP uses **IP** (Internet Protocol) as well
- UDP is connection-less
- UDP is less reliable than TCP
 - Relies on devices in between the sending and receiving computers to correctly get the data where it's supposed to go



Network Traffic



- **Packets** on a network are pieces of a file that sent over the network and re-assembled on the receiving side.
- Imagine the network is a straw and you want to push through a sandwich.
- How do you do it? One small piece (packet) at a time.

Network Data Packets Concept Map



Original Image

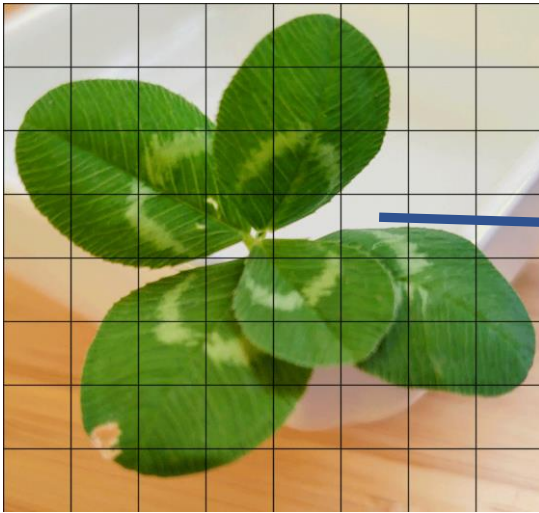


Image divided up into packet-sized data pieces

Individual Packet

IP sends
packet to
network

Network

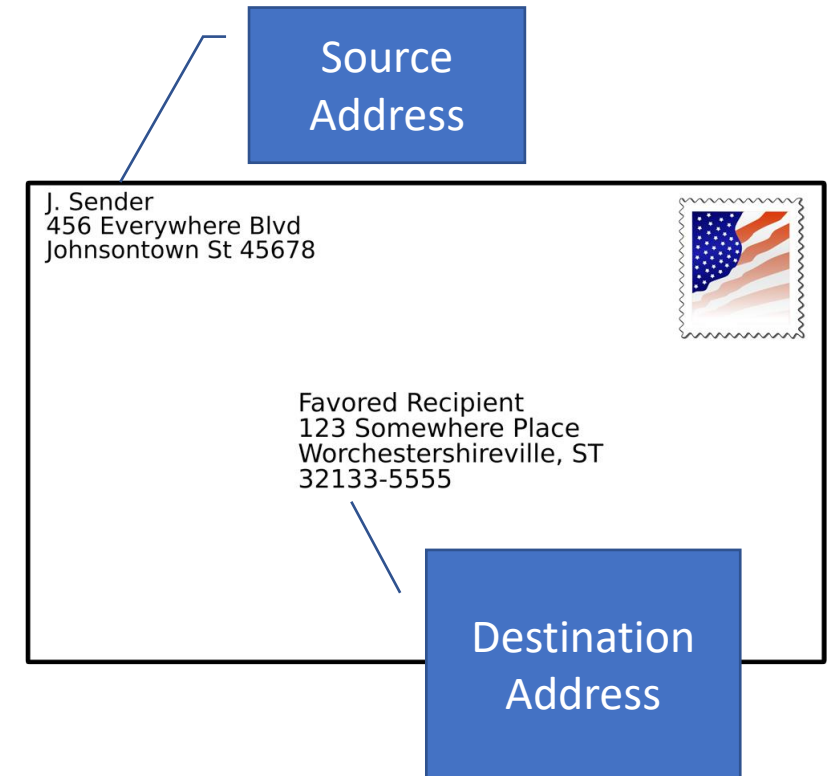


Packets get sent to destination

internet

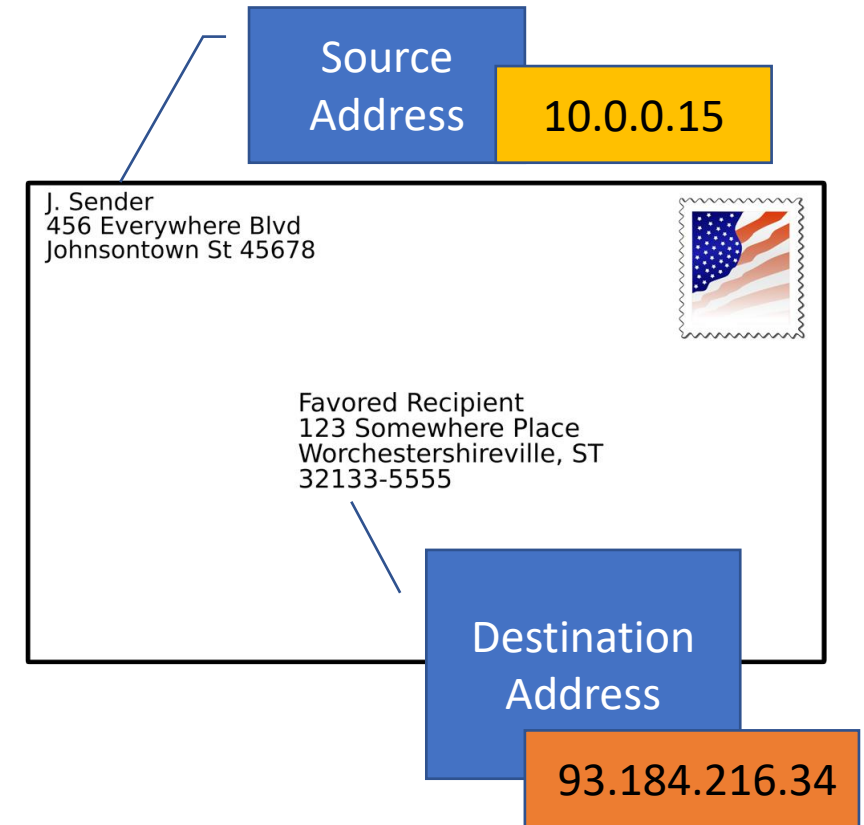
IP Addresses

- How does a packet know where it came from and where it's going to?
- Just like a letter, it uses addresses.
- **Source Address** - the IP address of where it's coming from (like a return address)
- **Destination Address** – the IP address of where it's going to



IP Addresses

- How does a packet know where it came from and where it's going to?
- Just like a letter, it uses addresses.
- **Source Address** - the IP address of where it's coming from (like a return address)
- **Destination Address** – the IP address of where it's going to



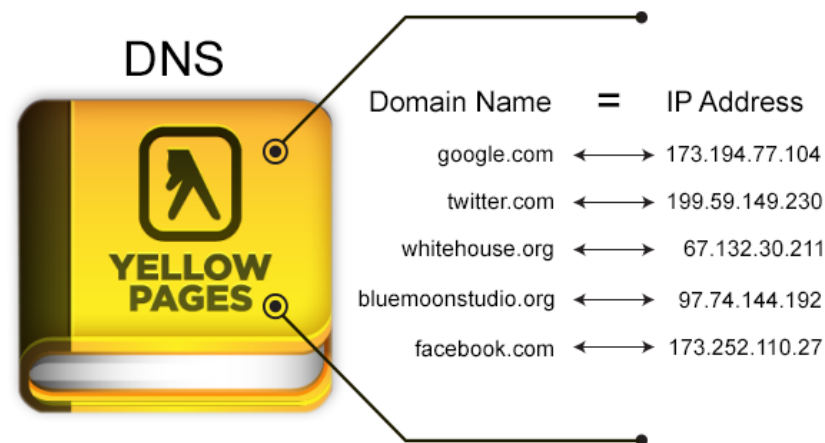
Other Identifiers – The MAC Address

- Computers are assigned IP addresses through software (changeable)
- The hardware has its own identifier, MAC address (non-changeable)
- Assigned at manufacture time, the first three bytes map to manufacturer (OUI listing)
- Can tell information about network hardware connected through the network traffic. The MAC address has (leaks) this information
- MAC addresses can be spoofed (faked), but generally the way to identify a specific physical network device



Not Lost in Translation

- How do you get from “example.com” to the IP address 93.184.216.34?
 - Answer: the **Domain Name System (DNS)**!
- DNS is like a phonebook for domain names mapped to IP addresses.



Ports

- Network ports indicate what type of service it is (email, file transfer, web).
- Typical ports used when browsing the internet
 - Resolving a URL (www.example.com) to an IP address (198.41.0.4) uses the **Domain Name System (DNS)** on port 53
 - Unencrypted website traffic (HTTP) – Port 80
 - Encrypted website traffic (HTTPS) – Port 443

Port Number	Usage
23	Telnet - Remote login service, unencrypted text messages
25	Simple Mail Transfer Protocol (SMTP) E-mail Routing
53	Domain Name System (DNS) service
80	Hypertext Transfer Protocol (HTTP) used in World Wide Web
110	Post Office Protocol (POP3) used by e-mail clients to retrieve e-mail from a server
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol (IMAP) Management of Digital Mail
161	Simple Network Management Protocol (SNMP)
194	Internet Relay Chat (IRC)
443	HTTP Secure (HTTPS) HTTP over TLS/SSL



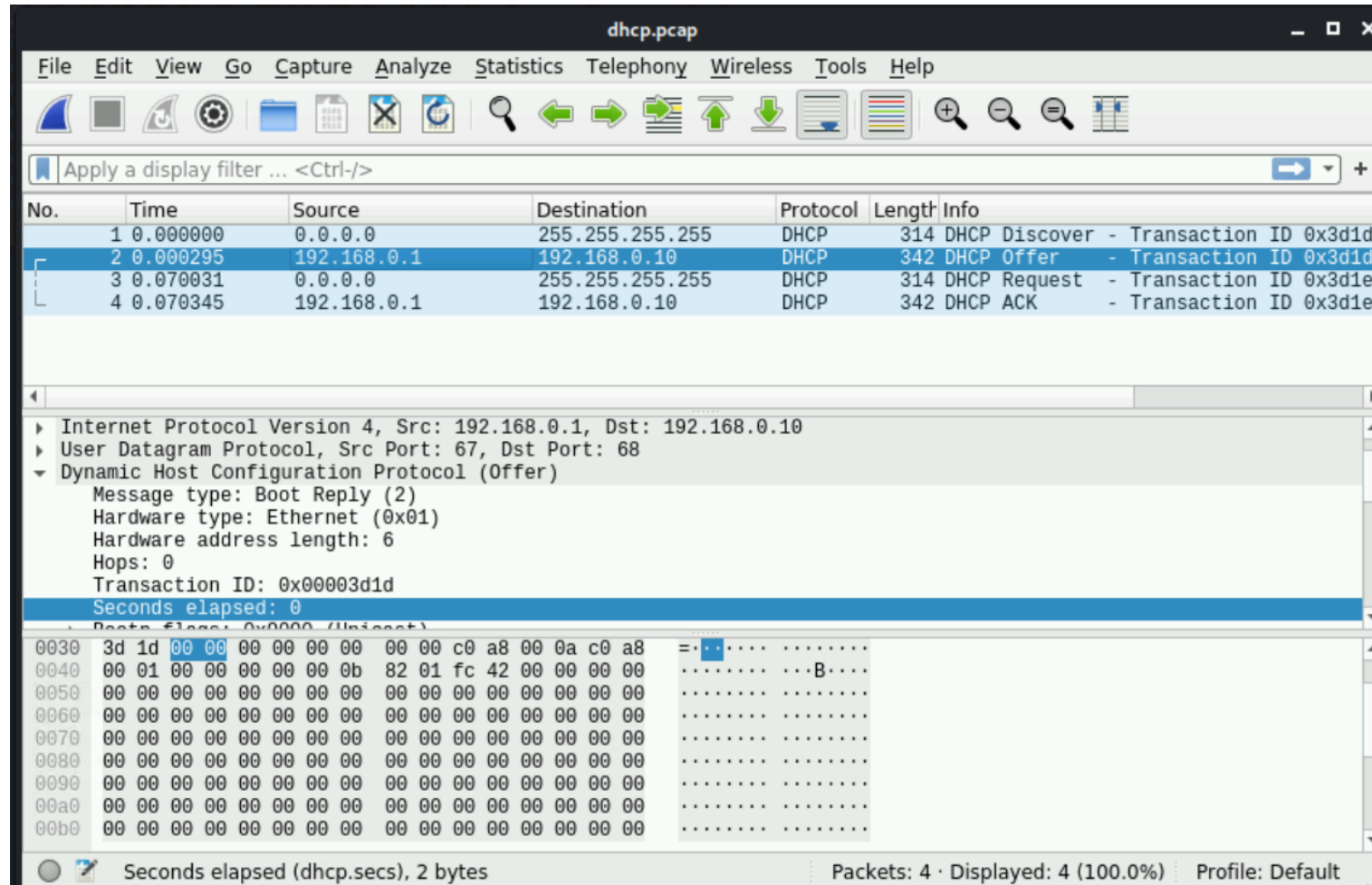
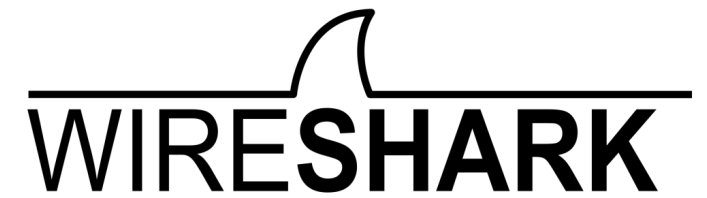
Do you think it's possible to analyze data sent over the network?




Wireshark

- Wireshark is a powerful analysis software that allows you to not only capture network and device packets, but to analyze them too (i.e., a packet analyzer).
- Remember - A packet is a fragment of data that is sent over a network from one machine to another. This data usually includes a *source port*, *source IP* address, *destination port*, *destination IP*, and other data that we will see in this lab.
- Wireshark allows a user to analyze the traffic traveling in and out of the machine, which can serve many uses.

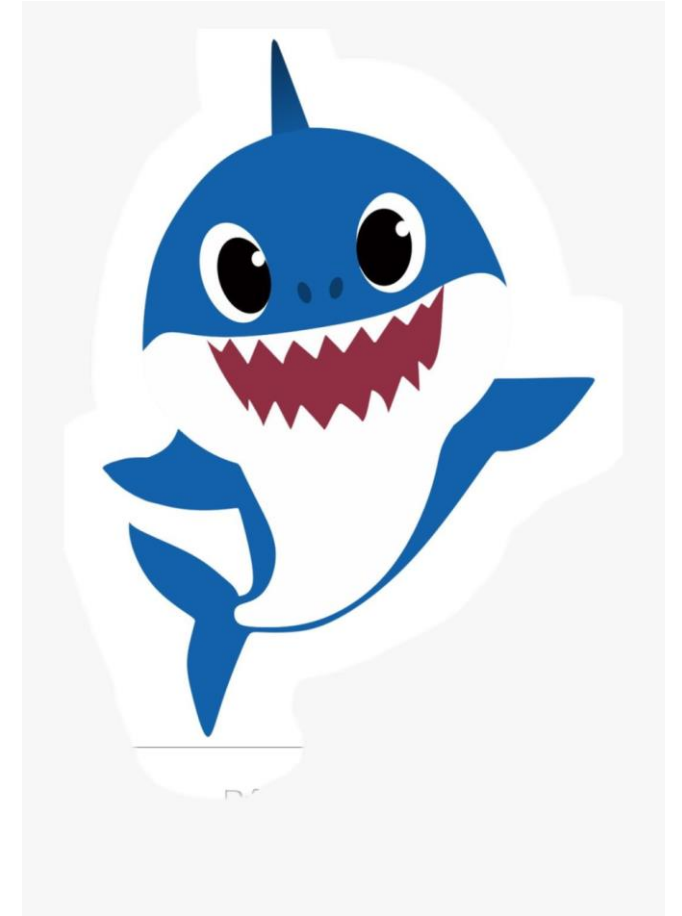
Wireshark



Attack of the Sharks


WIRESHARK

≠



Why Use Wireshark?

- Troubleshoot network connections.
- Filter data between two hosts to see a single network “conversation.”
- Comparing all “conversations” to discover bad actors or “bandwidth hogs.”
- Filter captured data to analyze specific protocols and ports being used.
- Analyze specific statistics about the traffic coming in and out of the system.

Adapted from © 2020 Virginia Cyber Range. Created by Thomas Weeks. [\(CC BY-NC-SA 4.0\)](#)



UNIVERSITY OF MARYLAND
GLOBAL CAMPUS

Wireshark Lab

- Wireshark allows you to view pieces of data (called packets) in real-time as they go in and out of a system and can be saved as packet capture or **pcap files**.
- In this lab, you will be analyzing packet capture files (network forensics).
- The objectives at the end of the lab is understand:
 - Wireshark overview
 - Analyzing DNS Packets
 - Name-to-IP address resolution
 - Wireless access points and identifiers



Debrief

