WEBER STATE UNIVERSITY

# Wireshark: A Beginners Intro

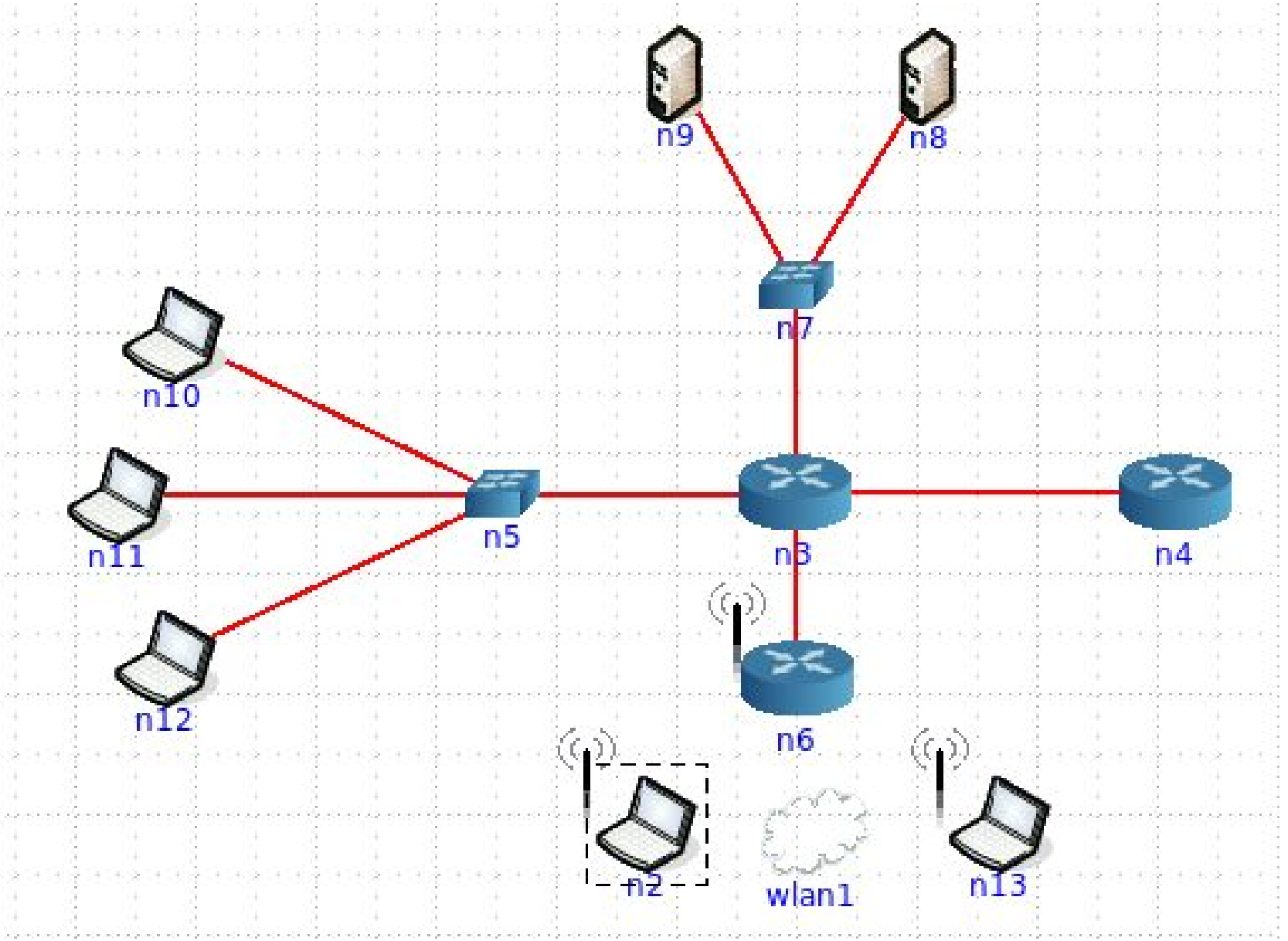
Kyle Feuz
School of Computing

# Introduction

- Download Wireshark and capture files
  - https://www.wireshark.org/download.html
  - http://icarus.cs.weber.edu/~kfeuz/downloads/saintcon2017_captures.zip
- Know the law (and company policy)
- Skills needed and skills covered

# Outline

- ~~Introduction~~
- What is Wireshark
- Where and How to sniff
- Wireshark Interface
- Network Protocols
- Advanced Uses


n9
n8
n7
n10
n11
n5
n3
n4
n12
n6
n2
wlan1
n13

# Wireshark Interface

- Data views
- Profiles
- Capture and display filters
- Columns
- Statistics

# Live Demo/Practice

- Create a new profile for Demo
- Create a new profile for HTTP
- Create a new profile for ICMP

# Wireshark Interface

- Capture filters
  - More efficient capture
  - Limit what is seen
  - Cannot recover what has been filtered
  - Use sparingly

# Wireshark Interface

- Display Filters
  - Limit packets currently displayed
  - Great for focusing
  - No efficiency boost
  - Can export packets
  - Use generously

# Display Filters

- Presets
  - Using
  - Modifying
- Freeform
- Expression Builder
- Shortcut buttons
- Apply filter
- IO Graphs

# Live Demo/Practice

- Load baseline.pcapng
- Which host is an ssh server?
- What UDP protocols are used?
- Which IP address is associated with MAC Address:  08:00:27:1e:63:2e?

# Wireshark Interface

- Coloring Rules
  - All data is still visible
  - Make certain data stand out or fade
  - Use Generously
  - Setup different configurations

# Live Demo/Practice

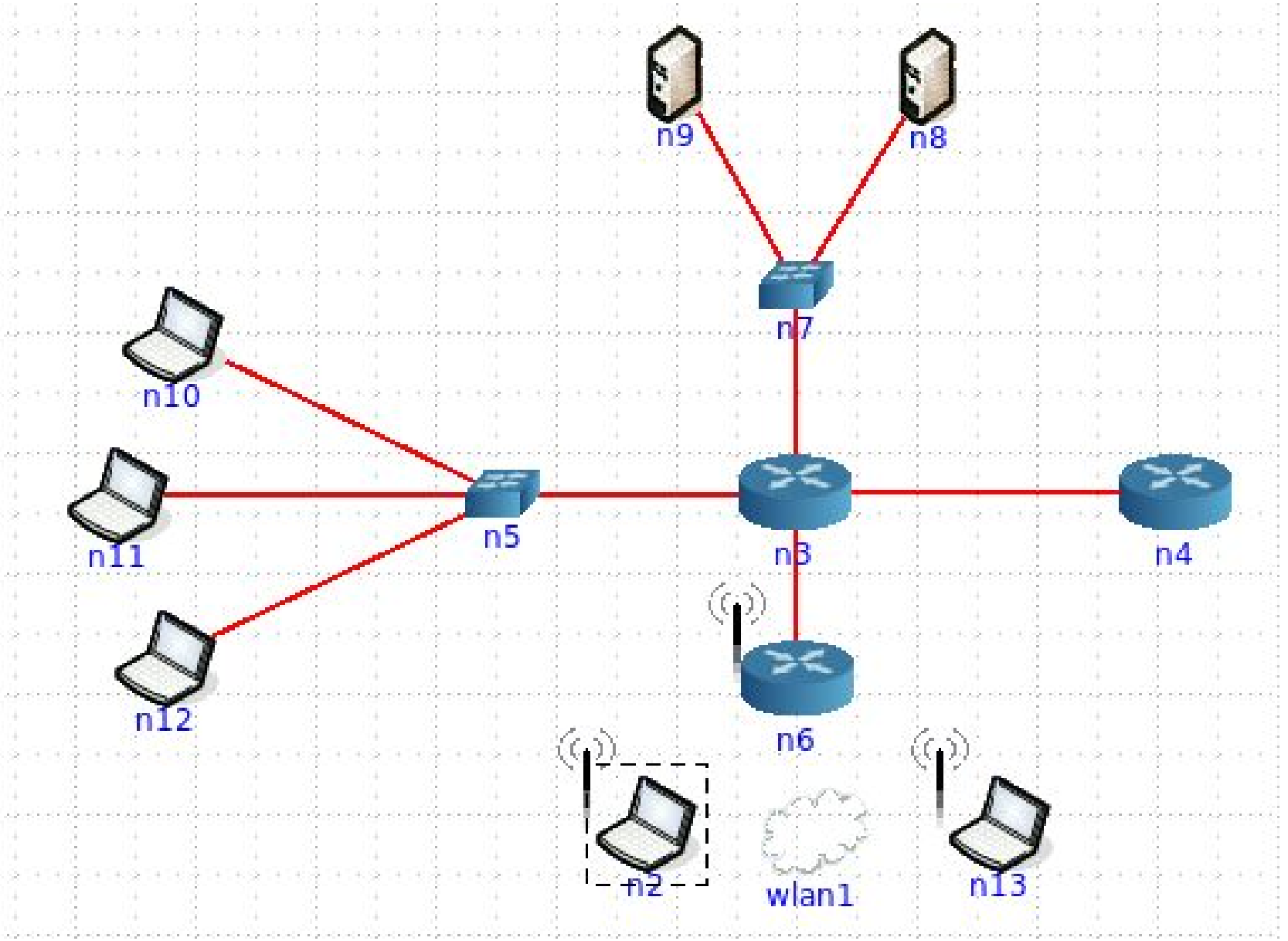
- Load baseline.pcapng
- Color all SSH traffic
- Color all traffic on port 443

# Outline

- ~~Introduction~~
- ~~What is Wireshark~~
- ~~Where and How to sniff~~
- ~~Wireshark Interface~~
- Network Protocols
- Advanced Uses

# Network Protocls

- ETHERNET
- ARP
- IP
- ICMP
- UDP
- TCP
- HTTP


n9
n8
n7
n10
n11
n5
n3
n4
n12
n6
n2
wlan1
n13

# ARP Live Demo/Practice

- Load baseline.pcapng
- Filter ARP
- Normal Request/response
- Gratuitous ARP

# IP Live Demo/Practice

- Load baseline.pcapng
- Filter IP
- Fragmentation
- TTL
- IP options

# IP - Common Protocols

- ICMP - 1
- UDP - 17
- TCP - 6
- IPv6 – 41

https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

# ICMP Live Demo/Practice

- Load baseline.pcapng
- Filter ICMP
- Echo requests/reply (ping/traceroute)
- Destination Unreachable
- Time exceeded

# ICMP - Common Types

- Echo request – 8
- Echo reply - 0
- Destination unreachable - 3
- Time Exceeded - 11

https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml

# UDP Live Demo/Practice

- Load baseline.pcapng
- Filter UDP
- DNS, DHCP, etc.

# TCP/UDP Common Ports

| Protocol | Port | | Protocol | Port |
|---|---|---|---|---|
| FTP | 21 | | DNS | 53 |
| SSH | 22 | | DHCP | 67,68 |
| Telnet | 23 | | SNMP | 161,162 |
| SMTP | 25 | | NetBIOS | 137,139 |
| HTTP | 80 | | | |
| HTTPS | 443 | | | |

https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

# TCP Live Demo/Practice

- Load baseline.pcapng
- Filter TCP
- HTTP, SSH, etc.
- Three-way handshake
- Retransmissions
- Closing connections
- Timing

# HTTP Live Demo/Practice

- Load baseline.pcapng
- HTTP Headers
  - Host
  - User-agent
  - Cookie
- Follow HTTP Stream vs TCP Stream
- Export Object
- Page “load” time

# Thank You!