Wireshark 201

Jeffrey L Carrell

Network Instructor

jeff.carrell@teachmeipv6.com

https://github.com/jeffcarrell/Wireshark-201

Wireshark 201

- Well-known ports
- IP Headers
- Wireshark key features
- Wireshark labs

Well-known ports

Protocol	TCP/UDP	Port Number
File Transfer Protocol (FTP)	TCP	20/21
Secure Shell (SSH)	TCP	22
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Domain Name System (DNS)	TCP/UDP	53
Dynamic Host Configuration Protocol (DHCP)	UDP	67/68
Trivial File Transfer Protocol (TFTP)	UDP	69
Hypertext Transfer Protocol (HTTP)	TCP	80
Post Office Protocol (POP) version 3	TCP	110
Network Time Protocol (NTP)	UDP	123
NetBIOS	TCP/UDP	137/138/139
Internet Message Access Protocol (IMAP)	TCP	143
Simple Network Management Protocol (SNMP)	TCP/UDP	161/162
Border Gateway Protocol (BGP)	TCP	179
Lightweight Directory Access Protocol (LDAP)	TCP/UDP	389
Hypertext Transfer Protocol over SSL/TLS (HTTPS)	TCP	443
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)	TCP/UDP	636
FTP over TLS/SSL	TCP	989/990

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

IP(v4) header

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Example Internet Datagram Header

https://tools.ietf.org/html/rfc791

IPv6 header

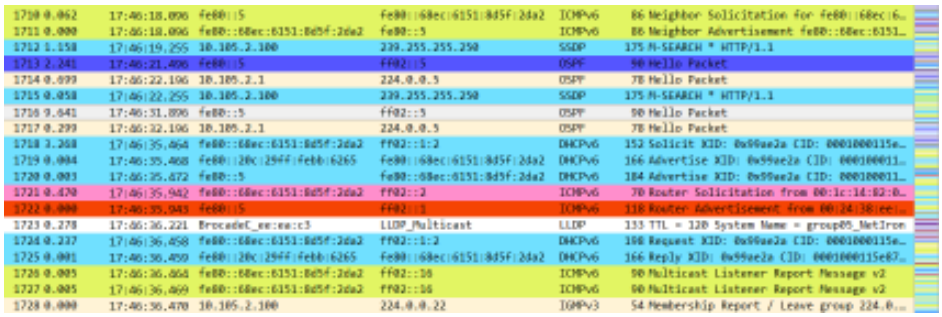
```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Traffic Class |           Flow Label                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload Length        |  Next Header  |   Hop Limit   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                         Source Address                        +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Destination Address                      +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

https://tools.ietf.org/html/rfc8200

Wireshark key features

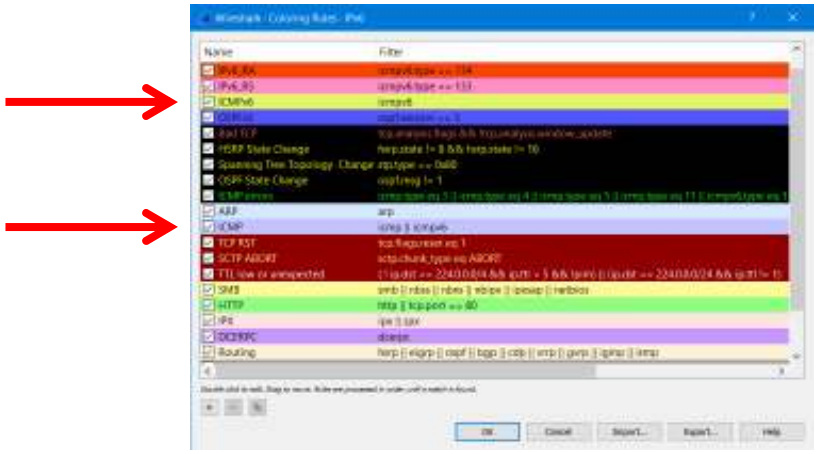
- Color rules
- Display filters
- Columns
- Configuration profiles
- Packet annotation

Coloring rules



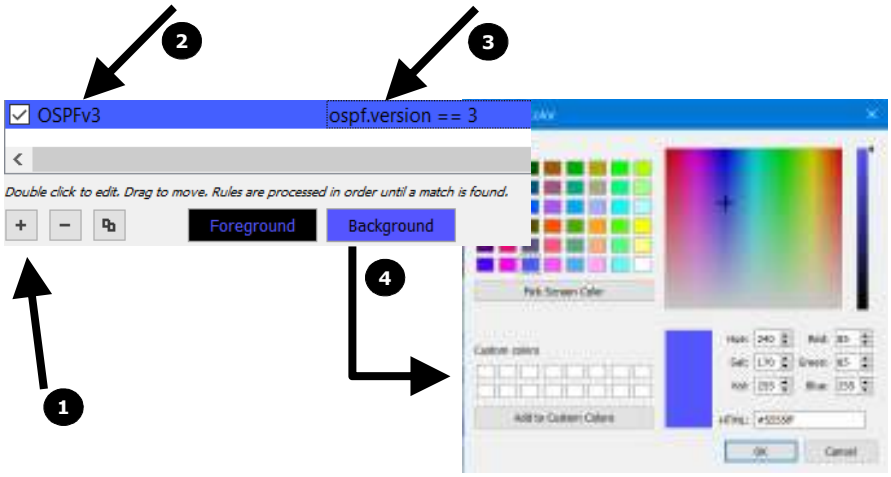
- Colors help you focus on specific address, protocols, events, and possibly find errors quickly

Color rule processing order

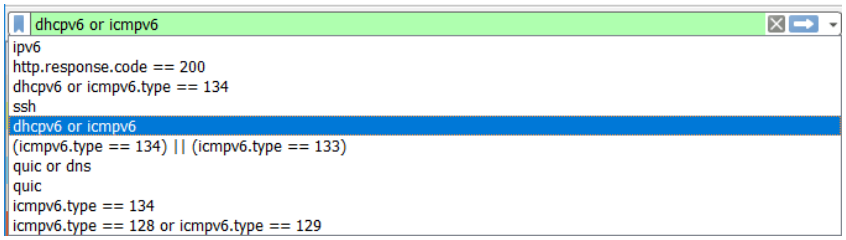


- Color rules read like a router ACL or firewall rules
  - First color rule that matches wins

Color rule creation

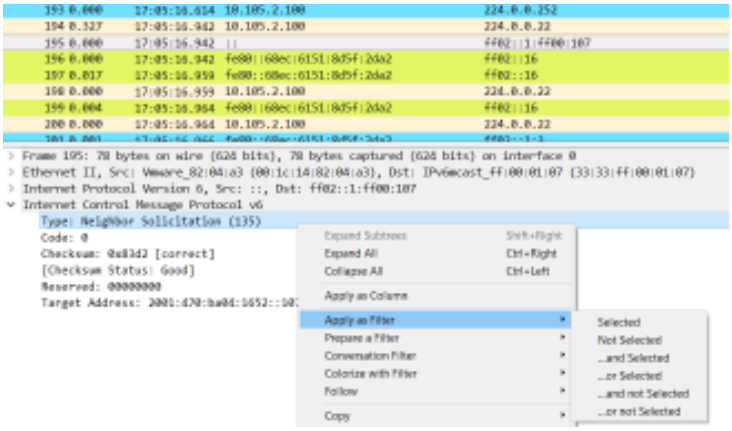


Display filters – option 1



- The Filter bar will change colors as you type to signify correct syntax for the filter
  - Green – syntax is correct
  - Red – syntax is correct
  - Yellow – syntax is suspect
- The Filter dropdown will show last 10 filters used
- You can save Filter definitions for frequent use

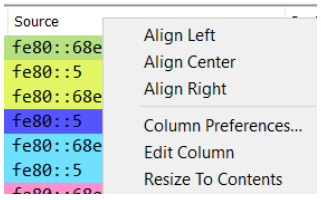
Display filters – option 2



- In the Packet Details view, right-click on a specific field to build a filter

11

Columns

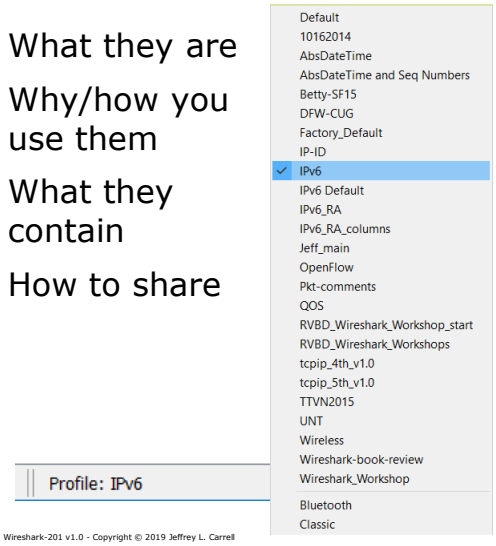


- Right-click column headings to sort, rename, align, etc
- In the Packet Details view, right-click on a specific field to Apply as Column

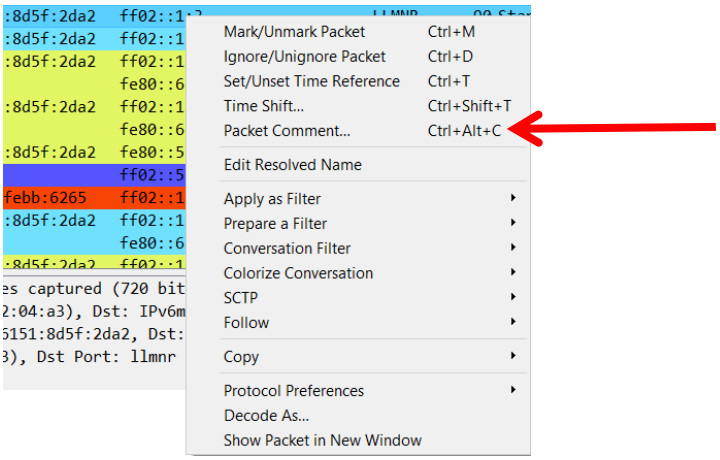
12

Configuration profiles

- What they are
- Why/how you use them
- What they contain
- How to share



Packet annotation

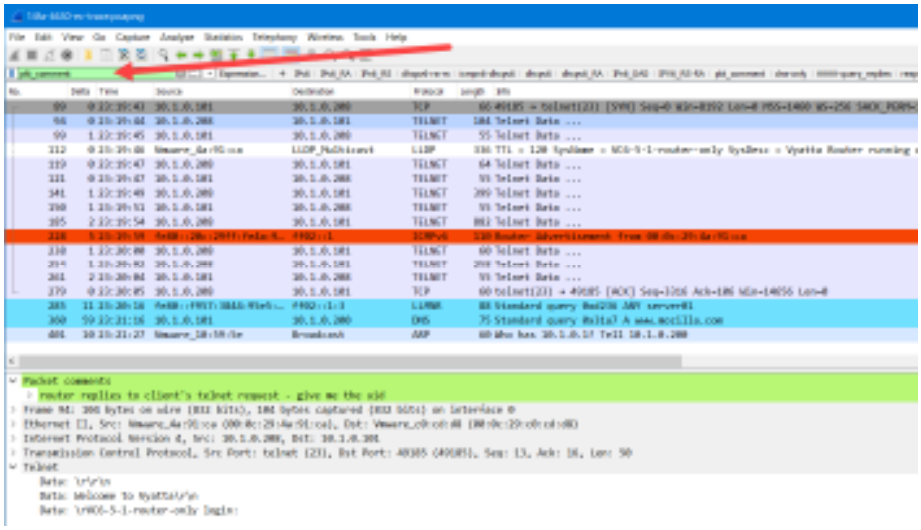


- Right click packet, select Packet Comment

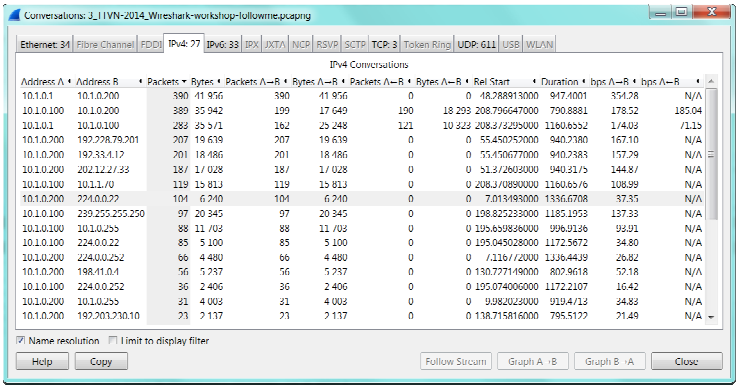
Packet annotation

```
38 4.480  17:04:07.158  fe80::20c:29ff:febb:6265  ff02::1  ICMPv6  214 Router Advertisement from 00:0c:29:bb:62:65
Packet comments
  Rogue RA, incorrect setting, has A flag "set" and M flag "not set"
    [Expert Info (Comment/Comment): Rogue RA, incorrect setting, has A flag "set" and M flag "not set"]
      [Rogue RA, incorrect setting, has A flag "set" and M flag "not set"]
      [Severity level: Comment]
      [Group: Comment]
Frame 38: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits) on interface 0
Ethernet II, Src: Vmware_bb:62:65 (00:0c:29:bb:62:65), Dst: IPv6mcast_01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::20c:29ff:febb:6265, Dst: ff02::1
Internet Control Message Protocol v6
  Type: Router Advertisement (134)
  Code: 0
```


Packet annotation display filter

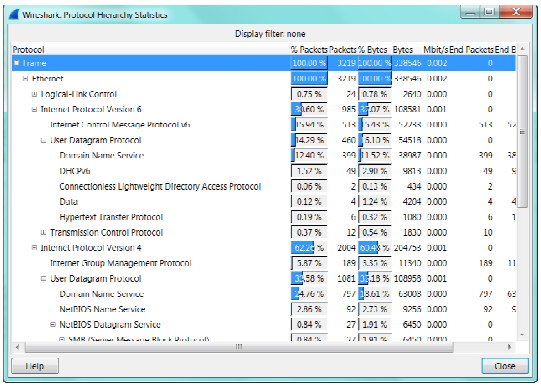


Top talkers



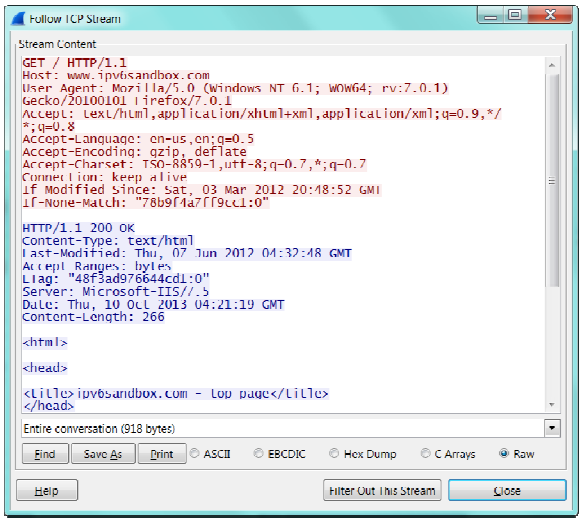
- Determine top talkers based on MAC addresses, IPv4/IPv6 addresses, port numbers, etc.
- Select: >Statistics >Conversations

Identify applications & protocols



- Identify application and protocols running on the network
- Select: >Statistics >Protocol Hierarchy

Follow streams



- Follow Streams
  - TCP
  - UDP
  - SSL
- Select packet (if known 1st in sequence)
- >Analyze > Follow TCP Stream

Wireshark lab #1

- Open "Wireshark-201-lab-file.pcapng"
- Create your own named profile
- Change time/date to time (only) and in milliseconds

Wireshark lab #2

- Still in "Wireshark-201-lab-file.pcapng"
  - We're looking at protocols:
    - Telnet
    - SSH
    - HTTP
    - DNS
    - DHCP
    - ICMP
    - TFTP
    - others

Wireshark lab #3

- Find a dns query for www.ipv6sandbox.com
  - dns.qry.name == "www.ipv6sandbox.com"
- Find a RDP session
  - Try display filter rdp
  - …gotta add tcp 3389 in the TPKT protocol filter for RDP filter name to work

Wireshark lab #4

- You will be configuring a specific display filter to view a portion of the http header to determine the host OS
  - http.user_agent
- You can further drill down to find a specific host OS/version
  - http.user_agent[24:3] == 31:30:2e:30

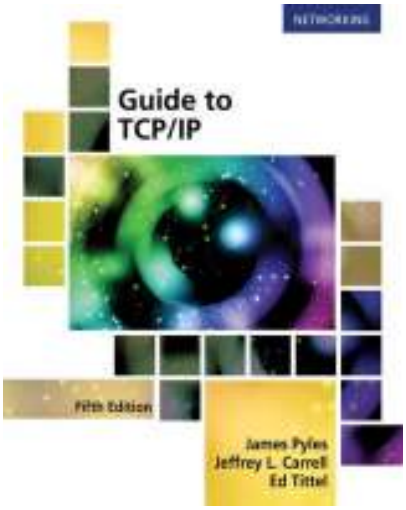
Wireshark 201

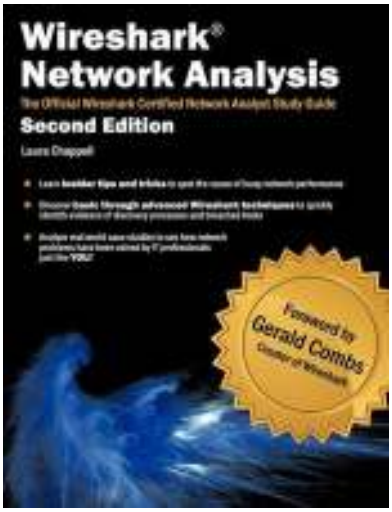
Questions ???

Resources

- https://wiki.wireshark.org/SampleCaptures
- https://www.netresec.com/?page=PcapFiles
- https://github.com/chrissanders/packets
- https://www.cellstream.com/resources/wireshark-profiles-repository

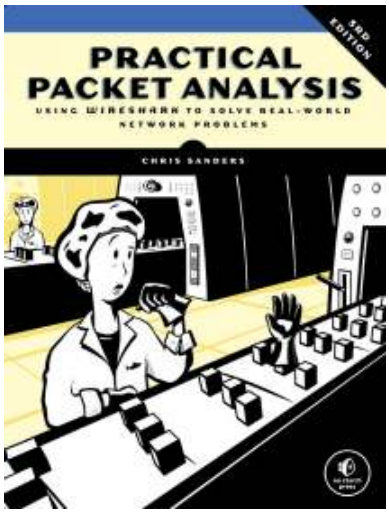
Resources





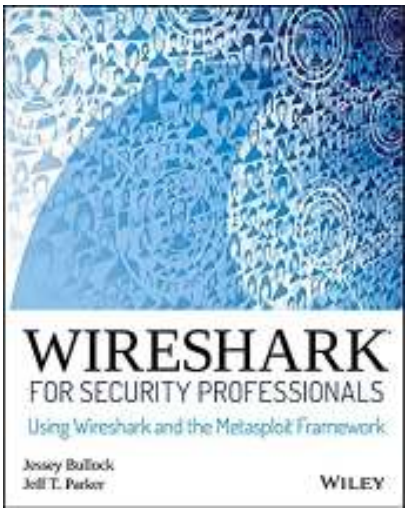
Resources

- Chapter 12: Packet Analysis for Security
  - Reconnaissance
    - SYN Scan
    - Operating System Fingerprinting
  - Traffic Manipulation
    - ARP Cache Poisoning
    - Session Hijacking
  - Malware
    - Operation Aurora
    - Remote-Access Trojan
  - Exploit Kit and Ransomware



27

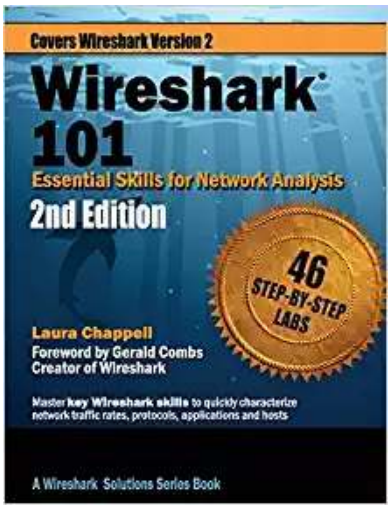
Resources

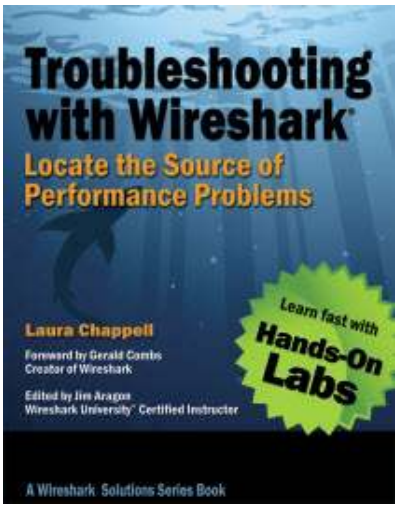


- Chapter 5: Diagnosing Attacks
  - Attack Type: Man-in-the-Middle
  - Attack Type: Denial of Service
  - Attack Type: Advanced Persistent Threat
  - Summary
  - Exercises

28

Resources





 29

Thank You for Attending!

- Jeffrey L Carrell
- Network Instructor
- jeff.carrell@teachmeipv6.com

 30