

# Wireshark 201



## Wireshark 201

---

Jeffrey L Carrell

Network Instructor

[jeff.carrell@teachmeipv6.com](mailto:jeff.carrell@teachmeipv6.com)

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

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

1



## Wireshark 201

---

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

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

2

# Wireshark 201



## 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>  
Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

3



## 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>

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

4

# Wireshark 201



## IPv6 header

```

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

```

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

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

5




## Wireshark key features

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

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

6

# Wireshark 201




## Coloring rules

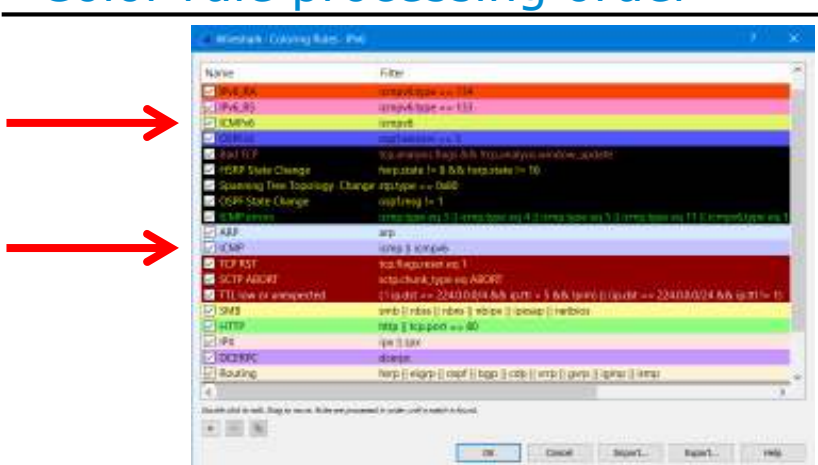
1718 0.062	17:40:10.090	fe80::5	fe80::68ec:6151:845f:2da2	ICMPv6	86 Neighbor Solicitation for fe80::68ec:6151:845f:2da2
1719 0.000	17:40:10.090	fe80::5	fe80::5	ICMPv6	86 Neighbor Advertisement fe80::68ec:6151:845f:2da2
1712 1.158	17:40:19.255	3b:105.2.100	239.255.255.250	SSDP	125 M-SEARCH * HTTP/1.1
1713 2.241	17:40:21.400	fe80::5	ff02::5	OSPF	78 Hello Packet
1714 0.099	17:40:22.196	3b:105.2.1	224.0.0.5	OSPF	78 Hello Packet
1715 0.058	17:40:22.255	3b:105.2.100	239.255.255.250	SSDP	125 M-SEARCH * HTTP/1.1
1716 0.041	17:40:31.090	fe80::5	ff02::5	OSPF	80 Hello Packet
1717 0.299	17:40:32.196	3b:105.2.1	224.0.0.5	OSPF	78 Hello Packet
1718 3.208	17:40:35.404	fe80::68ec:6151:845f:2da2	ff02::1:2	DHCPv6	153 Solicit XID: 0x88aa2a CID: 0001000115e...
1719 0.004	17:40:35.408	fe80::28c:29ff:febb:6265	fe80::68ec:6151:845f:2da2	DHCPv6	166 Advertise XID: 0x88aa2a CID: 000100011...
1720 0.003	17:40:35.472	fe80::5	fe80::68ec:6151:845f:2da2	DHCPv6	184 Advertise XID: 0x88aa2a CID: 000100011...
1721 0.470	17:40:35.942	fe80::68ec:6151:845f:2da2	ff02::2	ICMPv6	70 Router Solicitation from 00:1c:14:02:0...
1722 0.000	17:40:35.943	fe80::5	ff02::1	ICMPv6	118 Router Advertisement from 00:1c:14:02:0...
1723 0.278	17:40:36.221	BrocadeC...:c3	LLDP_Multicast	LLDP	153 TTL = 120 System Name = group0_MetIron
1724 0.237	17:40:36.458	fe80::68ec:6151:845f:2da2	ff02::1:2	DHCPv6	168 Request XID: 0x88aa2a CID: 0001000115e...
1725 0.001	17:40:36.409	fe80::28c:29ff:febb:6265	fe80::68ec:6151:845f:2da2	DHCPv6	166 Reply XID: 0x88aa2a CID: 0001000115e...
1726 0.005	17:40:36.404	fe80::68ec:6151:845f:2da2	ff02::1:0	ICMPv6	80 Multicast Listener Report Message v2
1727 0.005	17:40:36.409	fe80::68ec:6151:845f:2da2	ff02::1:0	ICMPv6	80 Multicast Listener Report Message v2
1728 0.000	17:40:36.470	3b:105.2.100	224.0.0.22	IGMPv3	54 Membership Report / Leave group 224.0...

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

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell




## Color rule processing order



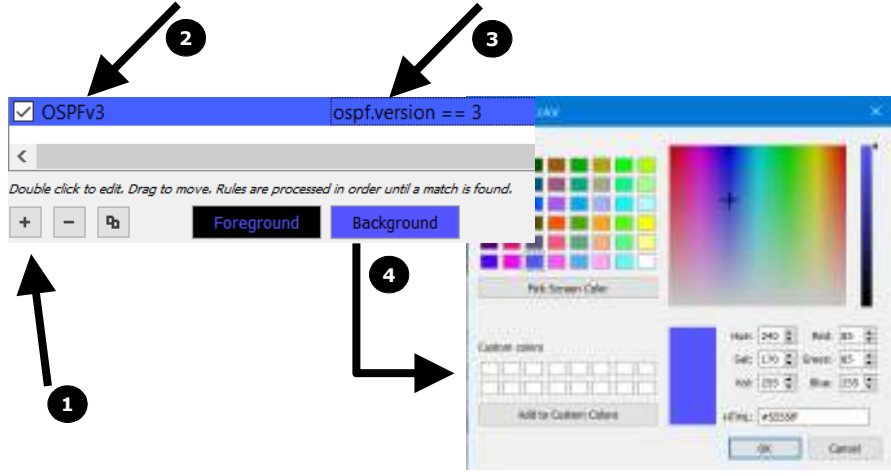
- Color rules read like a router ACL or firewall rules
  - First color rule that matches wins

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

# Wireshark 201




## Color rule creation

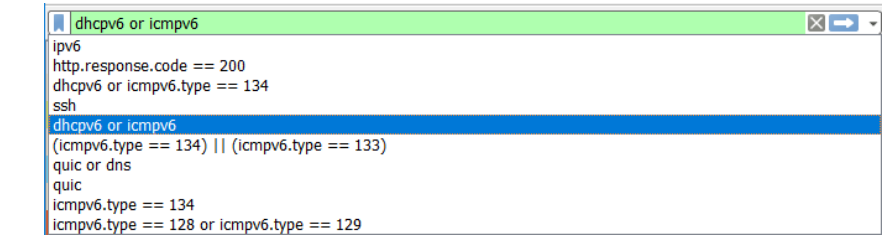


Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

9



## 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

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

10

# Wireshark 201



## Display filters – option 2

The screenshot shows the Wireshark interface. The packet list on the left shows several packets. The details pane on the right shows the 'Neighbor Solicitation' field. A right-click context menu is open over this field, with options like 'Expand Subtree', 'Expand All', 'Collapse All', 'Apply as Filter', 'Prepare a Filter', 'Conversation Filter', 'Colorize with Filter', 'Follow', and 'Copy'. The 'Apply as Filter' option is highlighted.

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

Wireshark 201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

11



## Columns

The screenshot shows the Wireshark interface. The packet list on the left shows several packets. The details pane on the right shows the 'Neighbor Advertisement' field. A right-click context menu is open over the 'Source' column heading, with options like 'Align Left', 'Align Center', 'Align Right', 'Column Preferences...', 'Edit Column', and 'Resize To Contents'.

- In the Packet Details view, right-click on a specific field to Apply as Column

Wireshark 201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

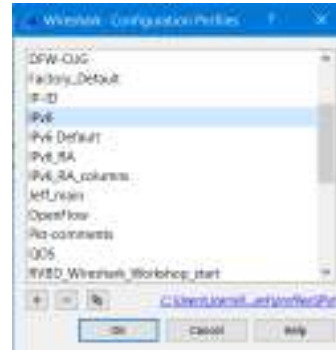
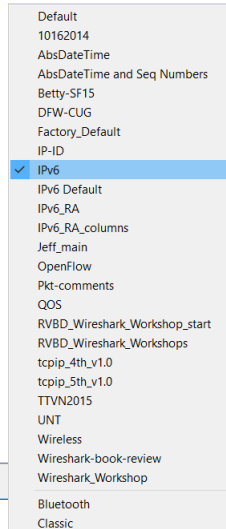
12

# Wireshark 201



## Configuration profiles

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



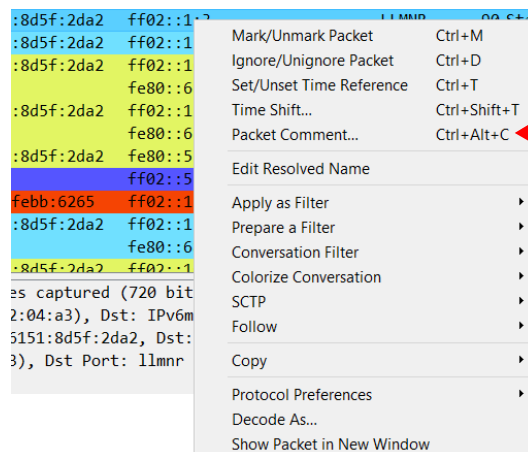
Profile: IPv6

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

13



## Packet annotation





- Right click packet, select Packet Comment

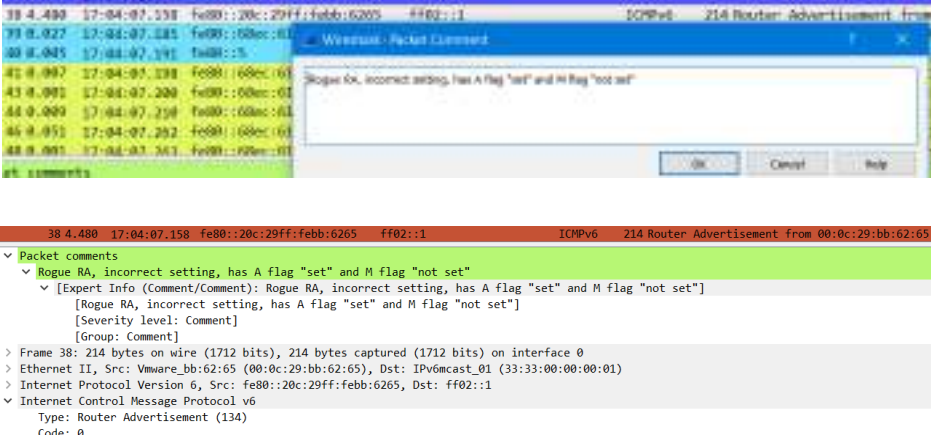
Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

14

# Wireshark 201

## 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\_b8:62:65 (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)

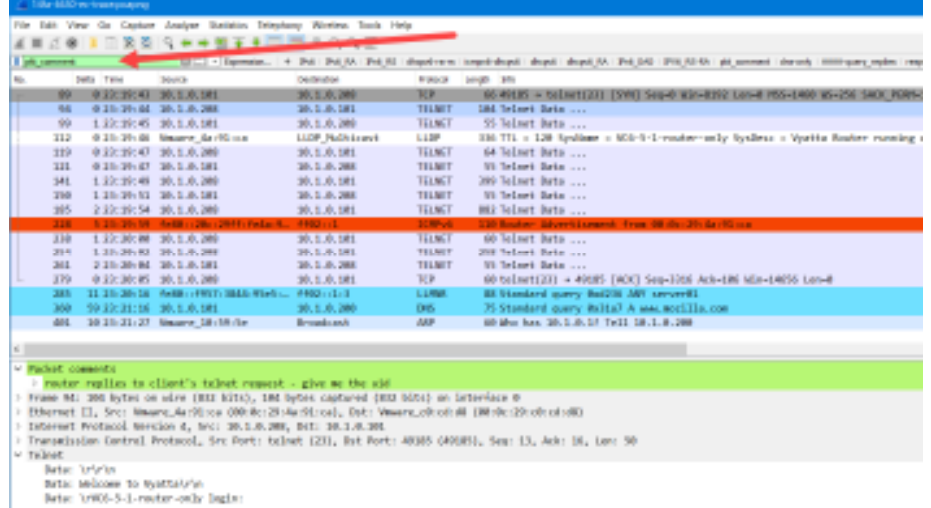
Code: 0

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

15

## Packet annotation display filter





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\_b8:62:65 (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

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

16



# Wireshark 201



## Top talkers

Conversations: J:\1\VN-2014\_Wireshark-workshop-followme.pcapng

Ethernet 34 | Fibre Channel | FDDI | IPv4: 77 | IPv6: 33 | ARP | AX.25 | NCP | RSVP | SCTP | Token Ring | UDP: 611 | USB | WLAN

IPv4 Conversations

Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets B→A	Bytes B→A	Rel. Start	Duration	bps A→B	bps B→A
10.1.0.1	10.1.0.200	380	41 956	380	41 956	0	0	48.288813000	947.4001	354.28	N/A
10.1.0.100	10.1.0.200	380	35 042	199	17 640	181	18 299	208.796647000	790.8881	178.52	185.04
10.1.0.1	10.1.0.100	283	35 571	162	25 248	121	10 523	208.474295000	1160.6552	174.03	111.15
10.1.0.200	192.228.79.201	207	19 618	207	19 618	0	0	55.450252000	940.2180	167.10	N/A
10.1.0.200	192.33.1.17	201	18 486	201	18 486	0	0	55.450677000	940.2383	157.29	N/A
10.1.0.200	202.12.27.33	187	17 028	187	17 028	0	0	51.372603000	940.3175	144.87	N/A
10.1.0.100	10.1.1.70	119	13 813	119	13 813	0	0	208.270980000	1160.6552	108.99	N/A
10.1.0.200	224.0.0.252	104	6 240	104	6 240	0	0	7.015488000	1336.6708	37.35	N/A
10.1.0.100	239.255.255.250	97	20 345	97	20 345	0	0	198.825233000	1185.1953	137.33	N/A
10.1.0.100	10.1.0.255	88	11 703	88	11 703	0	0	195.893828000	996.0136	93.01	N/A
10.1.0.100	224.0.0.22	85	5 100	85	5 100	0	0	195.045028000	1172.5672	34.80	N/A
10.1.0.200	224.0.0.252	66	4 480	66	4 480	0	0	7.116772000	1336.4439	26.82	N/A
10.1.0.200	198.41.0.4	56	5 237	56	5 237	0	0	130.777149000	807.9618	52.18	N/A
10.1.0.100	224.0.0.252	36	2 406	36	2 406	0	0	195.074006000	1172.2107	16.42	N/A
10.1.0.200	10.1.0.255	31	4 003	31	4 003	0	0	9.982023000	910.4713	34.83	N/A
10.1.0.200	192.201.210.10	21	2 117	21	2 117	0	0	118.715816000	795.5177	21.48	N/A

☒ Name resolution ☐ Limit to display filter

Help Copy Follow Sequence Graph A → B Graph B → A Close

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

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

17



## Identify applications & protocols

Wireshark: Protocol Hierarchy Statistics

Display filter: none

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s End	Packets End	Bytes End
IP (Total)	100.00%	2222	100.00%	209545	0.000	0	0
Internet	100.00%	4799	100.00%	209545	0.000	0	0
Ethernet II (Link Control)	0.35%	79	0.03%	2610	0.000	0	0
Internet Protocol Version 6	0.00%	0	0.00%	0	0.000	0	0
Internet Control Message Protocol	0.04%	115	0.05%	11544	0.000	115	11544
User Datagram Protocol	4.28%	460	5.13%	54518	0.000	0	0
Domain Name Service	12.40%	300	11.53%	39987	0.000	300	39987
DHCPv6	1.17%	49	2.80%	9815	0.000	49	9815
Connectionless Lightweight Directory Access Protocol	0.06%	2	0.12%	434	0.000	2	434
Data	0.12%	4	1.24%	4204	0.000	4	4204
Hypertext Transfer Protocol	0.19%	6	0.32%	1060	0.000	6	1060
Transmission Control Protocol	0.37%	12	0.54%	1830	0.000	10	10
Internet Protocol Version 4	0.00%	2004	0.00%	204755	0.000	0	0
Internet Group Management Protocol	5.87%	168	3.35%	11310	0.000	168	11310
User Datagram Protocol	0.50%	1081	0.45%	108959	0.000	0	0
Domain Name Service	4.16%	757	3.62%	63039	0.000	757	63039
NetBIOS Name Service	2.86%	57	2.73%	9265	0.000	57	9265
NetBIOS Datagram Service	0.84%	27	1.91%	6450	0.000	0	0
NAT Protocol Mapping Rule	0.00%	0	0.00%	0	0.000	0	0

Help Close

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

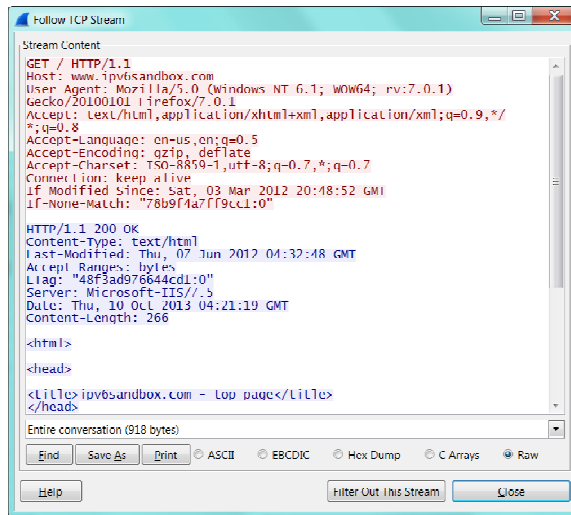
Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

18

# Wireshark 201



## Follow streams



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

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

19



## Wireshark lab #1

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

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

20

# Wireshark 201



## Wireshark lab #2

---

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

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

21



## 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-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

22

# Wireshark 201



## 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 v1.0 - Copyright © 2019 Jeffrey L. Carrell

23



# Wireshark 201

---

## Questions ???

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

24

# Wireshark 201



## Resources

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

Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

25



## Resources



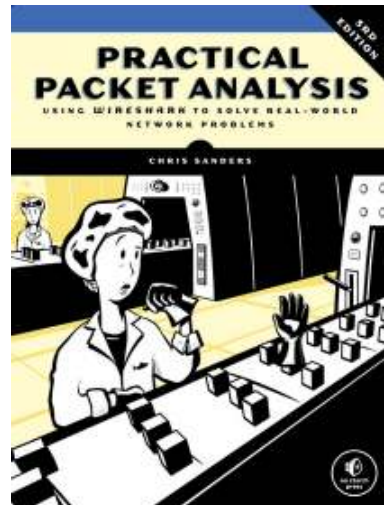
Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

26

# Wireshark 201

## Resources

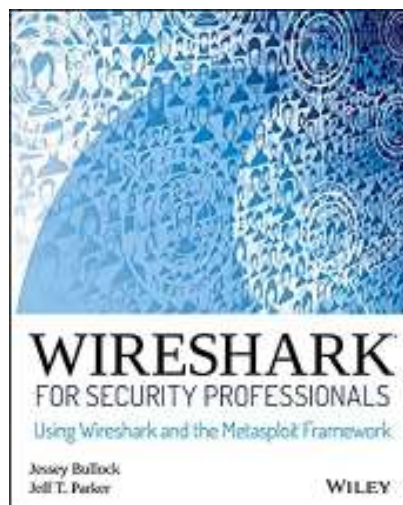
- Chapter 12: Packet Analysis for Security
  - Reconnaissance
    - SYN Scan
    - Operating System Fingerprinting
  - Traffic Manipulation
    - ARP Cache Poisoning
    - Session Hijacking
  - Malware
    - Operation Aurora
    - Remote-Access Trojan
  - Exploit Kit and Ransomware



Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

27

## Resources



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

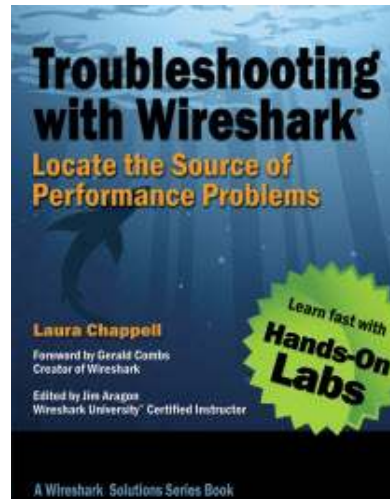
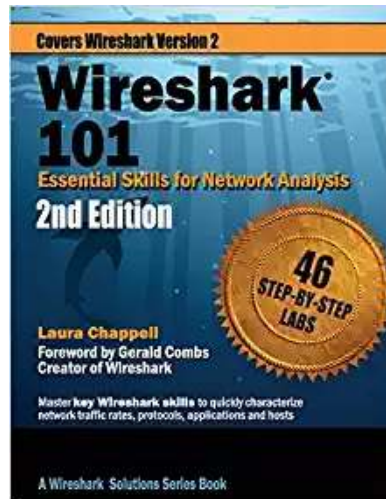
Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

28

# Wireshark 201



## Resources



Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

29



## Thank You for Attending!

- Jeffrey L Carrell
- Network Instructor
- [jeff.carrell@teachmeipv6.com](mailto:jeff.carrell@teachmeipv6.com)



Wireshark-201 v1.0 - Copyright © 2019 Jeffrey L. Carrell

30