

Cyber Security – Assignment 1

1. Lab Manual Steps followed with Screenshots.

- Wireshark screen after the traffic capture of www.wayne.edu

The screenshot displays the Wireshark interface with a traffic capture of www.wayne.edu. The packet list pane shows a series of packets, including a Host Announcement and a Temporary Redirect. The packet details pane shows the structure of a Simple Service Discovery Protocol (SSDP) packet. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
384	11.244509	192.168.0.121	13.33.183.40	TCP	54	64649 → 443 [ACK] Seq=134 Ack=365 Win=514 Len=0
385	11.260532	192.168.0.121	192.168.0.145	TCP	54	64217 → 8009 [ACK] Seq=331 Ack=331 Win=512 Len=0
386	11.265646	172.217.166.110	192.168.0.121	QUIC	67	Protected Payload (KPO)
387	11.308643	192.168.0.121	141.217.1.160	TCP	54	[TCP Retransmission] 64707 → 80 [FIN, ACK] Seq=634 Ack=1150 Win=130816 Len=0
388	11.409272	141.217.1.160	192.168.0.121	HTTP	562	[TCP Spurious Retransmission] HTTP/1.1 307 Temporary Redirect (text/html)
389	11.409327	192.168.0.121	141.217.1.160	TCP	66	[TCP Dup ACK 205#4] 64707 → 80 [ACK] Seq=635 Ack=1150 Win=130816 Len=0 SLE=1 SRE=509
390	11.468599	192.168.0.194	192.168.0.255	BROWSER	243	Host Announcement W105K6F12Z, Workstation, Server, NT Workstation
391	11.718689	192.168.0.121	23.65.109.107	TCP	55	64652 → 443 [ACK] Seq=1 Ack=1 Win=513 Len=1 [TCP segment of a reassembled PDU]
392	11.767700	23.65.109.107	192.168.0.121	TCP	66	443 → 64652 [ACK] Seq=1 Ack=2 Win=245 Len=0 SLE=1 SRE=2
393	12.001102	192.168.0.121	142.250.76.67	TCP	54	64699 → 80 [FIN, ACK] Seq=1 Ack=1 Win=514 Len=0
394	12.001337	192.168.0.121	23.67.148.153	TCP	54	64704 → 80 [FIN, ACK] Seq=1 Ack=1 Win=514 Len=0
395	12.001439	192.168.0.121	172.217.160.142	TCP	54	64701 → 80 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
396	12.001559	192.168.0.121	117.239.122.48	TCP	54	64700 → 80 [FIN, ACK] Seq=1 Ack=1 Win=512 Len=0
397	12.020348	117.239.122.48	192.168.0.121	TCP	54	80 → 64700 [FIN, ACK] Seq=1 Ack=2 Win=270 Len=0
398	12.020483	192.168.0.121	117.239.122.48	TCP	54	64700 → 80 [ACK] Seq=2 Ack=2 Win=512 Len=0
399	12.049770	23.67.148.153	192.168.0.121	TCP	54	80 → 64704 [FIN, ACK] Seq=1 Ack=2 Win=237 Len=0
400	12.049964	192.168.0.121	23.67.148.153	TCP	54	64704 → 80 [ACK] Seq=2 Ack=2 Win=514 Len=0
401	12.056533	172.217.160.142	192.168.0.121	TCP	54	80 → 64701 [FIN, ACK] Seq=1 Ack=2 Win=261 Len=0
402	12.056691	192.168.0.121	172.217.160.142	TCP	54	64701 → 80 [ACK] Seq=2 Ack=2 Win=513 Len=0
403	12.068163	142.250.76.67	192.168.0.121	TCP	54	80 → 64699 [FIN, ACK] Seq=1 Ack=2 Win=277 Len=0
404	12.068225	192.168.0.121	142.250.76.67	TCP	54	64699 → 80 [ACK] Seq=2 Ack=2 Win=514 Len=0
405	14.906647	141.217.1.160	192.168.0.121	HTTP	562	[TCP Spurious Retransmission] HTTP/1.1 307 Temporary Redirect (text/html)
406	14.906712	192.168.0.121	141.217.1.160	TCP	66	[TCP Dup ACK 205#5] 64707 → 80 [ACK] Seq=635 Ack=1150 Win=130816 Len=0 SLE=1 SRE=509
407	15.020939	192.168.0.121	141.217.1.160	TCP	54	[TCP Retransmission] 64707 → 80 [FIN, ACK] Seq=634 Ack=1150 Win=130816 Len=0

> Frame 1: 422 bytes on wire (3376 bits), 422 bytes captured (3376 bits) on interface \Device\NPF_{7D6EBCAA-ECEE-49BA-B061-3D0B46CF2482}, id 0
> Ethernet II, Src: Tp-LinkT_15:5c:ce (98:da:c4:15:5c:ce), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 53379, Dst Port: 1900
> Simple Service Discovery Protocol

0000 01 00 5e 7f ff fa 98 da c4 15 5c ce 08 00 45 00 ...E
0010 01 98 00 00 40 00 02 11 c6 b1 c0 a8 00 01 ef ff ...@
0020 ff fa d0 83 07 6c 01 84 e5 f5 4e 4f 54 49 46 59 ...l...NOTIFY
0030 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 4f 53 * HTTP/ 1.1...HOS
0040 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 2e 32 T: 239.2 55.255.2
0050 35 30 3a 31 39 30 30 0d 0a 43 41 43 48 45 2d 43 50:1900...CACHE-C
0060 4f 4e 54 52 4f 4c 3a 20 6d 61 78 2d 61 67 65 3d ONTROL: max-age=
0070 36 30 0d 0a 4c 4f 43 41 54 49 4f 4e 3a 20 68 74 60...LOCA TION: ht

- Wireshark screen after applying http filter.

Wireshark interface showing HTTP traffic. The filter bar is set to 'http'. The packet list displays several HTTP requests and responses, including GET requests for /favicon.ico and temporary redirects. The packet details pane shows the structure of a GET request for /favicon.ico.

No.	Time	Source	Destination	Protocol	Length	Info
202	8.492523	192.168.0.121	141.217.1.160	HTTP	687	GET / HTTP/1.1
204	8.510900	141.217.1.160	192.168.0.121	HTTP	1202	HTTP/1.0 200 OK (text/html)
210	8.605290	192.168.0.121	117.254.84.212	HTTP	652	GET /getjs?nadipdata=%7B%22url%22%3A%22%2F%22%2C%22referer%22%3A%22%2C%22host%22%3A%22www.wayne.edu%22%2C%22categories%22%3A%5B10...
268	8.796516	117.254.84.212	192.168.0.121	HTTP	766	HTTP/1.1 200 OK (application/x-javascript)
271	8.797435	141.217.1.160	192.168.0.121	HTTP	562	[TCP Spurious Retransmission] HTTP/1.1 307 Temporary Redirect (text/html)
275	8.813251	192.168.0.121	141.217.1.160	HTTP	637	GET /favicon.ico HTTP/1.1
281	8.854688	192.168.0.121	117.254.84.212	HTTP	898	GET /api/getnoti?tm=1604413971294&subscriberId=ZnR0aDI5NjEwMzlfZlQkGZ0dGyNubC5pbG%3D%3D&subscriberIP=59.98.27.135&nadipdata=%22%...
283	8.911511	117.254.84.212	192.168.0.121	HTTP/1.1	694	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
284	8.915698	192.168.0.121	117.254.84.212	HTTP	948	POST /api/logerror?tm=1604413971400 HTTP/1.1 (application/x-www-form-urlencoded)
293	8.962194	117.254.84.212	192.168.0.121	HTTP/1.1	530	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
297	9.121650	141.217.1.160	192.168.0.121	HTTP	584	HTTP/1.1 307 Temporary Redirect (text/html)
298	9.125103	192.168.0.121	141.217.1.160	HTTP	741	GET / HTTP/1.1
301	9.428845	141.217.1.160	192.168.0.121	HTTP	562	HTTP/1.1 307 Temporary Redirect (text/html)
305	9.663265	141.217.1.160	192.168.0.121	HTTP	562	[TCP Spurious Retransmission] HTTP/1.1 307 Temporary Redirect (text/html)
388	11.409272	141.217.1.160	192.168.0.121	HTTP	562	[TCP Spurious Retransmission] HTTP/1.1 307 Temporary Redirect (text/html)
405	14.906647	141.217.1.160	192.168.0.121	HTTP	562	[TCP Spurious Retransmission] HTTP/1.1 307 Temporary Redirect (text/html)

> Frame 202: 687 bytes on wire (5496 bits), 687 bytes captured (5496 bits) on interface \Device\NPF_{7D6EBCAA-ECEE-49BA-B061-3D0B46CF24B2}, id 0
> Ethernet II, Src: 66:08:e4:22:e7:65 (66:08:e4:22:e7:65), Dst: Tp-LinkT_15:5c:ce (98:da:c4:15:5c:ce)
> Internet Protocol Version 4, Src: 192.168.0.121, Dst: 141.217.1.160
> Transmission Control Protocol, Src Port: 64707, Dst Port: 80, Seq: 1, Ack: 1, Len: 633
> Hypertext Transfer Protocol

0000 98 da c4 15 5c ce 66 08 e4 22 e7 65 08 00 45 00 ... \f. .".e..E-
0010 02 a1 99 4d 40 00 80 06 00 00 c0 a8 00 79 8d d9 ... M@... ..y..
0020 01 a0 fc c3 00 50 00 0e d6 93 0a 49 c3 d6 50 18P... ..I..P..
0030 02 03 53 2e 00 00 47 45 54 20 2f 20 48 54 54 50 ... S...GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1..Ho st: www.
0050 77 61 79 6e 65 2e 65 64 75 0d 0a 43 6f 6e 6e 65 wayne.ed u..Conne
0060 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 ction: k eep-aliv
0070 65 0d 0a 44 4e 54 3a 20 31 0d 0a 55 70 67 72 61 e..DNT: 1..Upgra

Hypertext Transfer Protocol: Protocol

Packets: 407 · Displayed: 16 (3.9%) · Dropped: 0 (0.0%) Profile: Default

- Wireshark screen after applying filter http.host=www.wayne.edu

Wireshark interface showing HTTP traffic filtered by 'http.host=www.wayne.edu'. The packet list displays three GET requests for /favicon.ico. The packet details pane shows the structure of a GET request for /favicon.ico.

No.	Time	Source	Destination	Protocol	Length	Info
202	8.492523	192.168.0.121	141.217.1.160	HTTP	687	GET / HTTP/1.1
275	8.813251	192.168.0.121	141.217.1.160	HTTP	637	GET /favicon.ico HTTP/1.1
298	9.125103	192.168.0.121	141.217.1.160	HTTP	741	GET / HTTP/1.1

> Frame 202: 687 bytes on wire (5496 bits), 687 bytes captured (5496 bits) on interface \Device\NPF_{7D6EBCAA-ECEE-49BA-B061-3D0B46CF24B2}, id 0
> Ethernet II, Src: 66:08:e4:22:e7:65 (66:08:e4:22:e7:65), Dst: Tp-LinkT_15:5c:ce (98:da:c4:15:5c:ce)
> Internet Protocol Version 4, Src: 192.168.0.121, Dst: 141.217.1.160
> Transmission Control Protocol, Src Port: 64707, Dst Port: 80, Seq: 1, Ack: 1, Len: 633
> Hypertext Transfer Protocol

0000 98 da c4 15 5c ce 66 08 e4 22 e7 65 08 00 45 00 ... \f. .".e..E-
0010 02 a1 99 4d 40 00 80 06 00 00 c0 a8 00 79 8d d9 ... M@... ..y..
0020 01 a0 fc c3 00 50 00 0e d6 93 0a 49 c3 d6 50 18P... ..I..P..
0030 02 03 53 2e 00 00 47 45 54 20 2f 20 48 54 54 50 ... S...GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1.1..Ho st: www.
0050 77 61 79 6e 65 2e 65 64 75 0d 0a 43 6f 6e 6e 65 wayne.ed u..Conne
0060 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 ction: k eep-aliv
0070 65 0d 0a 44 4e 54 3a 20 31 0d 0a 55 70 67 72 61 e..DNT: 1..Upgra

wireshark-WH-FITWORT0.pcapng

Packets: 407 · Displayed: 3 (0.7%) · Dropped: 0 (0.0%) Profile: Default

- **Wireshark screen with dns filter**

Wireshark interface showing a DNS filter applied to the packet list. The packet list displays several DNS queries and responses. The packet details pane shows the structure of a DNS response packet.

No.	Time	Source	Destination	Protocol	Length	Info
39	6.363085	192.168.0.121	192.168.0.1	DNS	74	Standard query 0xbffd A www.google.com
40	6.377562	192.168.0.1	192.168.0.121	DNS	90	Standard query response 0xbffd A www.google.com A 172.217.160.132
44	6.436599	192.168.0.121	192.168.0.1	DNS	77	Standard query 0x79c4 A fonts.gstatic.com
46	6.451723	192.168.0.1	192.168.0.121	DNS	129	Standard query response 0x79c4 A fonts.gstatic.com CNAME.gstaticadssl1.google.com A 172.217.160.131
163	7.552998	192.168.0.121	192.168.0.1	DNS	86	Standard query 0x5552 A encrypted-tbn0.gstatic.com
164	7.569155	192.168.0.1	192.168.0.121	DNS	102	Standard query response 0x5552 A encrypted-tbn0.gstatic.com A 172.217.163.46

Frame 164: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{7D6EBCAA-ECEE-49BA-B061-3DDB46CF2482}, id 0

Ethernet II, Src: Tp-LinkT_15:5c:ce (98:da:c4:15:5c:ce), Dst: 66:08:e4:22:e7:65 (66:08:e4:22:e7:65)

Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.121

User Datagram Protocol, Src Port: 53, Dst Port: 63186

Domain Name System (response)

```

0000  66 08 e4 22 e7 65 98 da c4 15 5c ce 08 00 45 00  f...e... \...E...
0010  00 58 13 6b 40 00 f9 11 ec 5e c0 a8 00 01 c0 a8  -X.k@...A.....
0020  00 79 00 35 f6 d2 00 44 96 b5 55 52 81 00 00 01  -y5...D..UR....
0030  00 01 00 00 00 00 0e 65 6e 63 72 79 70 74 65 64  .....e ncrypted
0040  2d 74 62 6e 30 07 67 73 74 61 74 69 63 03 63 6f  -tbn0gs tatic.co
0050  6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 36  m.....-6
0060  00 04 ac d9 a3 2e                                     ....
  
```

Domain Name System: Protocol

Packets: 407 · Displayed: 6 (1.5%) · Dropped: 0 (0.0%)

Profile: Default

- **Wireshark screen after UDP follow option**

Wireshark interface showing the 'Follow UDP Stream' dialog box. The dialog box displays the stream of data for a specific UDP packet, showing the domain name 'www.google.com'.

Wireshark - Follow UDP Stream (udp.stream eq 6) - Wi-Fi

Stream 6

Find:

Find Next

Filter Out This Stream Print Save as... Back Close Help

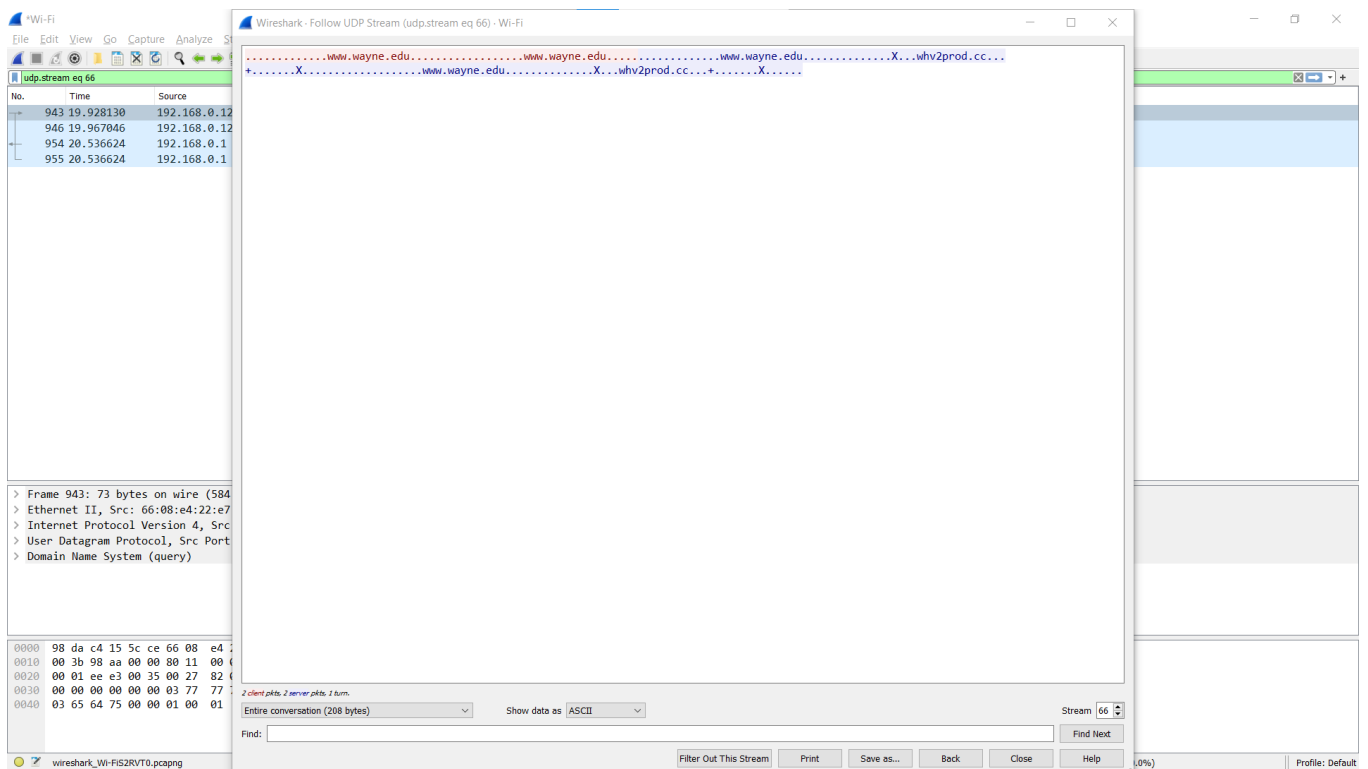
Stream 6

Find Next

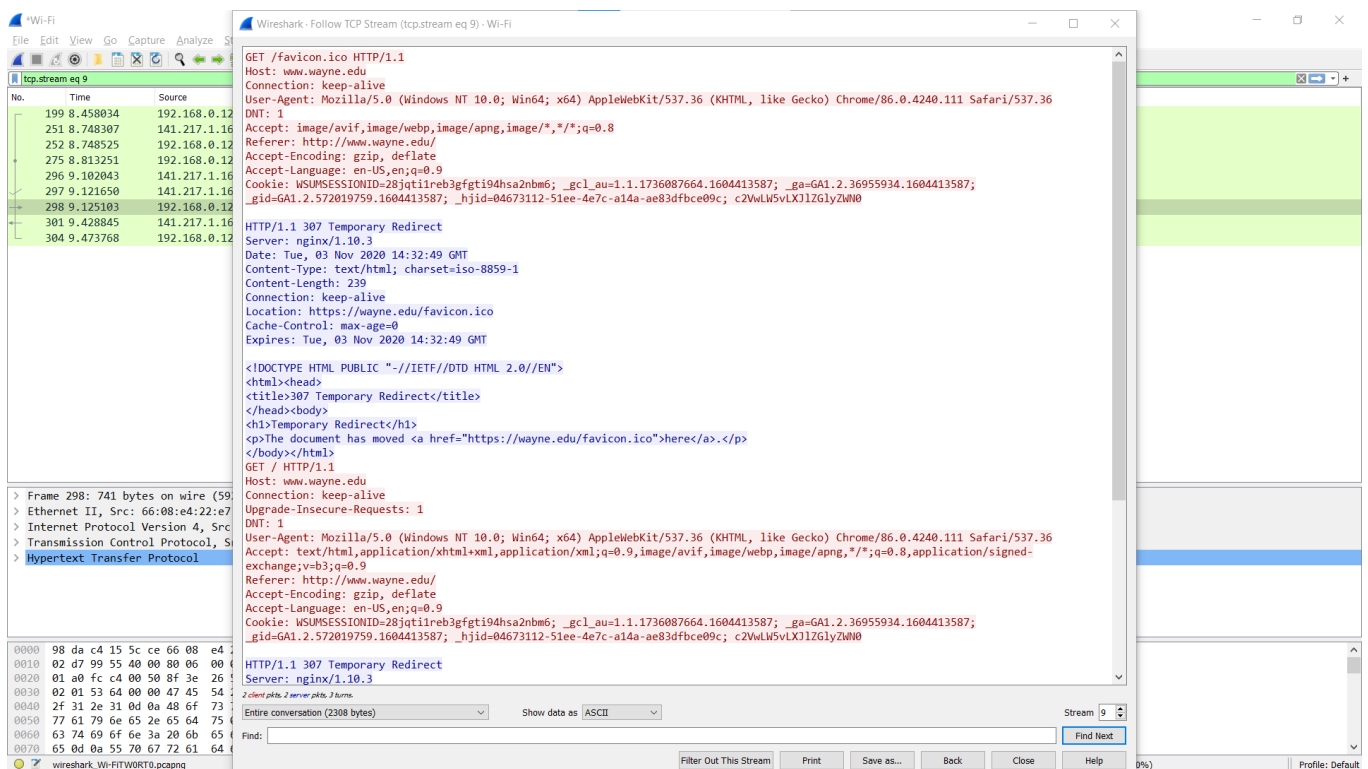
Filter Out This Stream Print Save as... Back Close Help

Profile: Default

Another example



- **Wireshark screen after TCP stream follow**



Questions from the Assignment and Answers

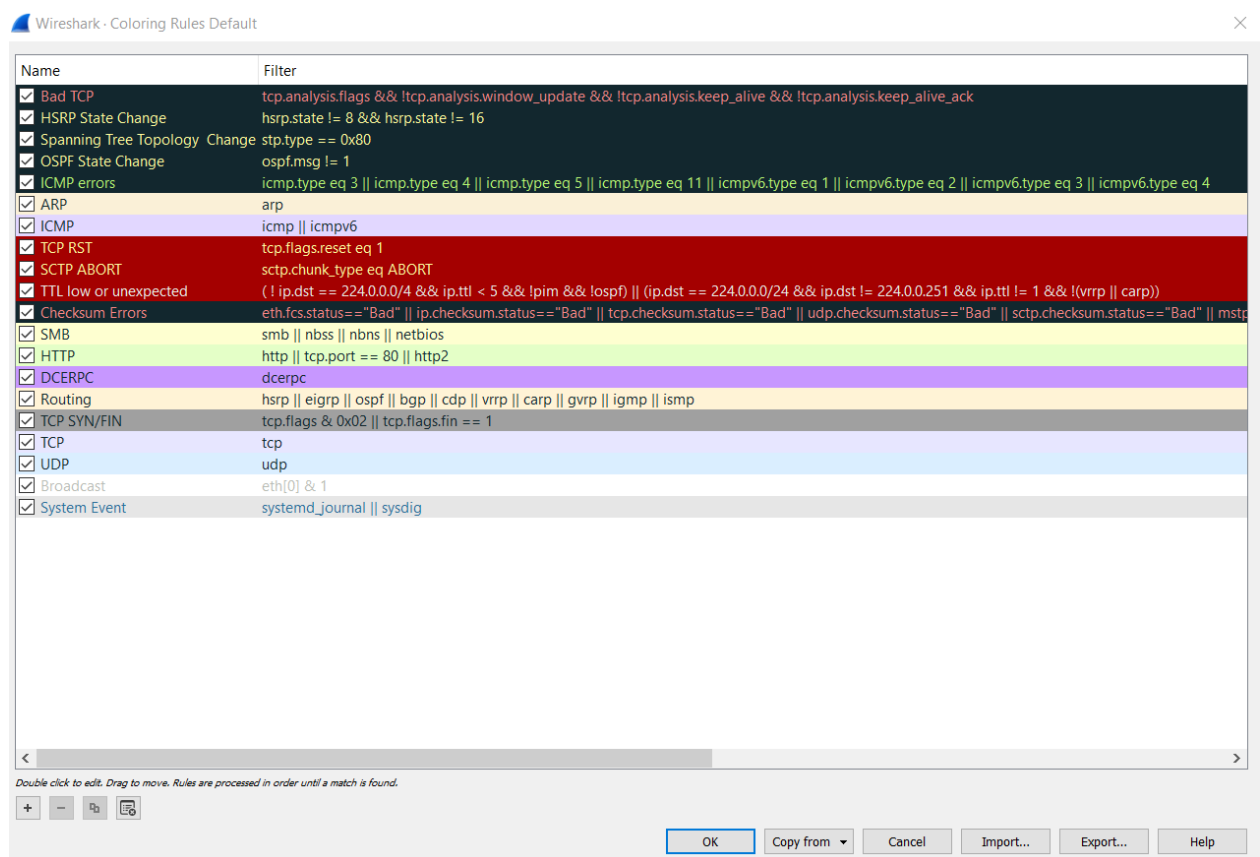
1. If a packet is highlighted by black, what does it mean for the packet?

Ans: By default the black colour code is given to packets which have some sort of problem or state change when they were received.

By default, following are the conditions for black coloured packets.

1. Bad TCP like Spurious transmission or Duplicate or out of order packet.
2. HSRP State change
3. Spanning Tree Topology change
4. OSPF State Change
5. ICMP errors

However, this colour coding can be customised by the user.



Examples are below:

4724 55.453758	192.168.0.121	192.168.0.100	TCP	66 [TCP Keep-Alive ACK] 5228 → 65093 [ACK] Seq=758 Win=67840 Len=0 SLE=758 SRE=759
4725 54.535586	74.125.24.188	192.168.0.121	TCP	66 [TCP Keep-Alive ACK] 5228 → 65093 [ACK] Seq=758 Win=67840 Len=0 SLE=758 SRE=759
4726 54.887153	192.168.0.121	157.240.192.52	TLSv1.2	85 Application Data
4727 54.938726	157.240.192.52	192.168.0.121	TCP	54 443 → 64736 [ACK] Seq=77 Ack=94 Win=349 Len=0
4728 55.102184	141.217.1.160	192.168.0.121	HTTP	562 [TCP Spurious Retransmission] HTTP/1.1 307 Temporary Redirect (text/html)
4729 55.102277	192.168.0.121	141.217.1.160	TCP	66 [TCP Dup ACK 425385] 65102 → 80 [ACK] Seq=635 Ack=1150 Win=130816 Len=0 SLE=1 SRE=509
4730 55.155959	157.240.192.52	192.168.0.121	TLSv1.2	92 Application Data
4731 55.200805	192.168.0.121	157.240.192.52	TCP	54 64736 → 443 [ACK] Seq=94 Ack=115 Win=512 Len=0
4732 55.358276	192.168.0.121	141.217.1.160	TCP	54 [TCP Retransmission] 65102 → 80 [FIN, ACK] Seq=634 Ack=1150 Win=130816 Len=0
4733 55.900611	192.168.0.121	192.168.0.145	TCP	164 65089 → 8009 [PSH, ACK] Seq=2169 Ack=7940 Win=130048 Len=110 [TCP segment of a reassembled PDU]
4734 55.905456	192.168.0.145	192.168.0.121	TCP	164 8009 → 65089 [PSH, ACK] Seq=7940 Ack=2279 Win=45568 Len=110 [TCP segment of a reassembled PDU]
4735 55.948710	192.168.0.121	192.168.0.145	TCP	54 65089 → 8009 [ACK] Seq=2279 Ack=8050 Win=130048 Len=0

2. What is the filter command for listing all outgoing http traffic?

Ans: To filter all outgoing http traffic, use this

`ip.src == <host or local ip address> && http`

or in ipv6

`ipv6.src == <host or local ipv6 address> && http`

3. Why does DNS use Follow UDP Stream while HTTP use Follow TCP Stream?

Ans: DNS uses UDP protocol on the transport layer by default. Although it can fallback to TCP protocol when packet size is large. UDP is preferred in DNS because it is fast and has low overhead. A DNS query is a single UDP request from the DNS client followed by a single UDP reply from the server.

So, to trace the Stream of UDP we use Follow UDP Stream.

HTTP uses TCP protocol on the Transport layer by default. So to trace stream we use Follow TCP Stream.

4. Using Wireshark to capture the FTP password.

Ans: Here I have used a Filezilla local FTP server hosted on my local machine and Filezilla client to connect to the server.

Step by step demo for capturing the FTP password and a possible fix to protect against password leak is shown below.

Wireshark – Capturing password of the FTP communication

Username and Password can be seen here if we apply filter as ftp.

Wireshark packet capture showing FTP traffic. The packet list shows a sequence of FTP commands and responses. Packet 50 is highlighted, showing a 'PASS password' request. The packet details pane shows the File Transfer Protocol (FTP) structure, including the current working directory. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
6	1.804592	:::1	:::1	FTP	207	Response: 220-FileZilla Server 0.9.60 beta
18	1.804809	:::1	:::1	FTP	74	Request: AUTH TLS
20	1.804934	:::1	:::1	FTP	109	Response: 502 Explicit TLS authentication not allowed
26	1.805061	:::1	:::1	FTP	74	Request: AUTH SSL
28	1.805162	:::1	:::1	FTP	109	Response: 502 Explicit TLS authentication not allowed
42	12.104434	:::1	:::1	FTP	81	Request: USER Admin_Braj
44	12.104656	:::1	:::1	FTP	102	Response: 331 Password required for admin_braj
50	12.104845	:::1	:::1	FTP	79	Request: PASS password
55	12.105112	:::1	:::1	FTP	79	Response: 230 Logged on
60	12.109102	:::1	:::1	FTP	69	Request: PWD
62	12.109409	:::1	:::1	FTP	95	Response: 257 "/" is current directory.

> Frame 50: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{...} id 0

> Null/Loopback

> Internet Protocol Version 6, Src: ::1, Dst: ::1

> Transmission Control Protocol, Src Port: 65046, Dst Port: 21, Seq: 38, Ack: 272, Len: 15

> File Transfer Protocol (FTP)

[Current working directory:]

0000 18 00 00 00 00 05 4e fb 00 23 06 80 00 00 00 00N-..#.....

0010 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00

0020 00 00 00 00 00 00 00 00 00 00 01 fe 16 00 15

0030 26 57 f7 f2 fc 1d 92 3a 50 18 27 f5 66 89 00 00 &M-.....P.'f...

0040 50 41 53 53 20 70 61 73 73 77 6f 72 64 0d 0a PASS pas sword..

Password is clearly visible here if you merely follow the TCP Stream

Wireshark packet capture showing FTP traffic. The packet list shows a sequence of FTP commands and responses. Packet 50 is highlighted, showing a 'PASS password' request. The packet details pane shows the File Transfer Protocol (FTP) structure, including the current working directory. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
31	1.804124	:::1	:::1	FTP	74	Request: AUTH TLS
41	1.804162	:::1	:::1	FTP	109	Response: 502 Explicit TLS authentication not allowed
51	1.804256	:::1	:::1	FTP	74	Request: AUTH SSL
61	1.804592	:::1	:::1	FTP	109	Response: 502 Explicit TLS authentication not allowed
91	1.804626	:::1	:::1	FTP	81	Request: USER Admin_Braj
18	1.804809	:::1	:::1	FTP	102	Response: 331 Password required for admin_braj
19	1.804863	:::1	:::1	FTP	79	Request: PASS password
20	1.804934	:::1	:::1	FTP	79	Response: 230 Logged on
21	1.804954	:::1	:::1	FTP	69	Request: PWD
26	1.805061	:::1	:::1	FTP	95	Response: 257 "/" is current directory.
27	1.805093	:::1	:::1	FTP	74	Request: AUTH TLS
28	1.805162	:::1	:::1	FTP	109	Response: 502 Explicit TLS authentication not allowed
29	1.805184	:::1	:::1	FTP	74	Request: AUTH SSL
42	12.104434	:::1	:::1	FTP	81	Request: USER Admin_Braj
43	12.104516	:::1	:::1	FTP	102	Response: 331 Password required for admin_braj
44	12.104656	:::1	:::1	FTP	79	Request: PASS password
47	12.104690	:::1	:::1	FTP	79	Response: 230 Logged on
50	12.104845	:::1	:::1	FTP	69	Request: PWD
51	12.104910	:::1	:::1	FTP	95	Response: 257 "/" is current directory.
55	12.105112	:::1	:::1	FTP	74	Request: AUTH TLS
58	12.105170	:::1	:::1	FTP	109	Response: 502 Explicit TLS authentication not allowed
60	12.109102	:::1	:::1	FTP	74	Request: AUTH TLS
61	12.109181	:::1	:::1	FTP	109	Response: 502 Explicit TLS authentication not allowed
62	12.109409	:::1	:::1	FTP	74	Request: AUTH TLS

> Frame 50: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{...} id 0

> Null/Loopback

> Internet Protocol Version 6, Src: ::1, Dst: ::1

> Transmission Control Protocol, Src Port: 65046, Dst Port: 21, Seq: 38, Ack: 272, Len: 15

> File Transfer Protocol (FTP)

[Current working directory:]

0000 18 00 00 00 00 05 4e fb 00 23 06 80 00 00 00 00N-..#.....

0010 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00

0020 00 00 00 00 00 00 00 00 00 00 01 fe 16 00 15

0030 26 57 f7 f2 fc 1d 92 3a 50 18 27 f5 66 89 00 00 &M-.....P.'f...

0040 50 41 53 53 20 70 61 73 73 77 6f 72 64 0d 0a PASS pas sword..

To protect leaking password, we should always prefer SFTP or FTP over TLS instead of FTP. Using FTP shares the username and password as clear text whereas the SFTP or FTP over TLS will encrypt the username and password as seen below.

Wireshark packet capture showing an FTP session. The packet list shows a sequence of requests and responses. Packet 124 is highlighted, showing the response to the previous request. The packet details pane shows the File Transfer Protocol (FTP) section, indicating the current working directory is empty. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Frame 84: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface \Device\NPF_{...} id 0

Null/Loopback

Internet Protocol Version 6, Src: ::1, Dst: ::1

Transmission Control Protocol, Src Port: 21, Dst Port: 65059, Seq: 1793, Ack: 726, Len: 60

File Transfer Protocol (FTP)

[Current working directory:]

Wireshark packet capture showing an FTP session. The packet list shows a sequence of requests and responses. Packet 124 is highlighted, showing the response to the previous request. The packet details pane shows the File Transfer Protocol (FTP) section, indicating the current working directory is empty. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Frame 60: 60 bytes on wire (512 bits), 60 bytes captured (512 bits) on interface \Device\NPF_{...} id 0

Null/Loopback

Internet Protocol Version 6, Src: ::1, Dst: ::1

Transmission Control Protocol, Src Port: 21, Dst Port: 65059, Seq: 1793, Ack: 726, Len: 60

File Transfer Protocol (FTP)

[Current working directory:]

Using TLS over FTP caused the user credentials to be encrypted with the public key of the server and can be decrypted only by the private key of the server on the server's end.