



Blue Team Level 1 Certification (Standard)

Introduction to BT1

Welcome to Blue Team Level 1!

4 Topics

Lab and Forum Access

SECURITY FUNDAMENTALS DOMAIN

Introduction to Security Fundamentals

1 Topic

Soft Skills

7 Topics

Security Controls

5 Topics 1 Quiz

Networking 101

6 Topics 1 Quiz

Management Principles

4 Topics 1 Quiz

PHISHING ANALYSIS DOMAIN

PA1) Introduction to Emails and Phishing

7 Topics 1 Quiz

PA2) Types of Phishing Emails

10 Topics 2 Quizzes

PA3) Tactics and Techniques Used

12 Topics 2 Quizzes

PA4) Investigating a Phishing Email

8 Topics 2 Quizzes

PA5) Analysing URLs, Attachments, and Artifacts

8 Topics 1 Quiz

PA6) Taking Defensive Actions

12 Topics 1 Quiz

PA7) Report Writing

7 Topics 1 Quiz

PA8) Phishing Response Challenge

3 Topics 1 Quiz

THREAT INTELLIGENCE DOMAIN

TI1) Introduction to Threat Intelligence

7 Topics

TI2) Threat Actors & APTs

6 Topics 2 Quizzes

TI3) Operational Threat Intelligence

7 Topics 1 Quiz

TI4) Tactical Threat Intelligence

7 Topics 1 Quiz

TI5) Strategic Threat Intelligence

5 Topics 1 Quiz

TI6) Malware and Global Campaigns

6 Topics 1 Quiz

DIGITAL FORENSICS DOMAIN

DF1) Introduction to Digital Forensics

5 Topics

DF2) Forensics Fundamentals

10 Topics 5 Quizzes

Introduction to Wireshark (Analysis)

Blue Team Level 1 Certification (Standard) > IR3 Detection and Analysis Phase > Introduction t...

IN PROGRESS



Knowing how to use Wireshark features to enhance network traffic analysis differs from having the skills to analyze network traffic. The latter can only come from real-world experience, practice and research, and a deep understanding of networks, such as the information covered at the start of this course. There is a wealth of network- analysis-related material online, and many more sample PCAP files with which you can practice.

This section will cover the former – how to take advantage of major Wireshark features to improve and assist in in-depth manual analysis. We will explore with applying display filters, using packet list columns, following protocol streams, viewing different traffic statistics.

APPLYING DISPLAY FILTERS

As described in the previous sections, the display filter controls which packets are shown in the packet list. This significantly improves the ease of traffic analysis, as important traffic can be separated from the general noise in the network. To filter by the presence of a protocol or header field in a packet, the expression should specify only the protocol or header field, e.g.

- `udp` to display only UDP packets, and
- `http.request` to display only HTTP requests

No.	Time	Source	Destination	Protocol	Length	Stream Index	Stream Index	Info
2	0.000041	192.168.1.7	162.159.133.234	TCP	54	12	60154 = 443 [ACK] Seq=313 Ack=218 Win=8182 Len=8	
7	0.714217	192.168.1.7	162.159.133.234	TCP	54	9	60154 = 443 [ACK] Seq=313 Ack=217 Win=817 Len=8	
8	0.714218	192.168.1.7	162.159.133.234	TCP	54	0	60154 = 443 [ACK] Seq=1 Ack=838 Win=8187 Len=8	
14	0.715097	192.168.1.7	162.159.133.234	TCP	54	9	60154 = 443 [ACK] Seq=1 Ack=838 Win=8187 Len=8	
15	0.715097	192.168.1.7	162.159.133.234	TCP	54	0	60154 = 443 [ACK] Seq=1 Ack=838 Win=8186 Len=8	
16	0.715097	192.168.1.7	162.159.133.234	TCP	54	0	60154 = 443 [ACK] Seq=1 Ack=838 Win=8186 Len=8	
31	1.226512	192.168.1.7	162.159.133.234	TCP	54	0	60154 = 443 [ACK] Seq=1 Ack=838 Win=8176 Len=8	
34	1.226509	192.168.1.7	162.159.133.234	TCP	54	0	60154 = 443 [ACK] Seq=1 Ack=838 Win=8176 Len=8	
46	1.352432	192.168.1.7	162.159.136.232	TCP	54	0	60154 = 443 [ACK] Seq=1 Ack=2227 Win=8187 Len=8	
61	1.598684	192.168.1.7	162.159.136.232	TCP	54	3	61996 = 443 [ACK] Seq=1 Ack=1 Win=8192 Len=8	
70	2.357754	192.168.1.7	162.159.133.234	TCP	54	0	60154 = 443 [ACK] Seq=1 Ack=3262 Win=8181 Len=8	

To filter by the values of header fields, you can specify the header field, then a comparison operator, and then the value that it should match. For example, `tcp.port == 80` displays packets that have a source or destination port of 80 (HTTP), and `tcp.window_size_value >= 8000` displays TCP packets with a window size of 8000 bytes or over.

No.	Time	Source	Destination	Protocol	Length	Stream Index	Stream Index	Info
278	28.5967	162.159.136.238	192.168.1.7	TCP	54	12	443 = 63812 [ACK] Seq=363 Ack=236 Win=8754 Len=8	
311	29.1859	162.159.136.238	192.168.1.7	TCP	54	12	443 = 63812 [ACK] Seq=363 Ack=8464 Win=8754 Len=8	
372	29.1859	162.159.136.238	192.168.1.7	TLSv1.2	583	12	Application Data	
375	29.2787	162.159.136.238	192.168.1.7	TCP	66	13	443 = 63812 [ACK] Seq=363 Ack=8784 Win=8754 Len=8	
379	29.2787	162.159.136.238	192.168.1.7	TLSv1.2	412	13	443 = 63812 [ACK] Seq=363 Ack=8784 Win=8754 Len=8	
383	29.3062	162.159.136.238	192.168.1.7	TCP	56	13	443 = 63812 [ACK] Seq=363 Ack=8784 Win=8754 Len=8	
386	29.3062	162.159.136.238	192.168.1.7	TLSv1.2	1198	13	Application Data	
386	29.7865	162.159.136.238	192.168.1.7	TLSv1.2	88	13	443 = 63812 [ACK] Seq=363 Ack=8784 Win=8754 Len=8	
388	29.7865	162.159.136.238	192.168.1.7	TLSv1.2	1224	13	Application Data	
389	29.7865	162.159.136.238	192.168.1.7	TCP	54	13	443 = 63812 [ACK] Seq=363 Ack=8784 Win=8754 Len=8	
390	29.7865	162.159.136.238	192.168.1.7	TCP	66	13	443 = 63812 [ACK] Seq=363 Ack=8784 Win=8754 Len=8	
399	29.8092	162.159.136.238	192.168.1.7	TLSv1.2	1224	13	443 = 63812 [ACK] Seq=363 Ack=8784 Win=8754 Len=8	
400	29.8092	162.159.136.238	192.168.1.7	TLSv1.2	1224	13	443 = 63812 [ACK] Seq=363 Ack=8784 Win=8754 Len=8	

Multiple filter statements can be chained by using logical operators, including `and` (`&&`) and `(or |||)`. For example, to display TCP packets addressed to 192.168.1.7, you can use `ip.dst_host == 192.168.1.7 && tcp`, and to display either NTP traffic or UDP traffic from/to port 20000, you can use `ntp or udp.port == 20000`. The `not` (!) operator excludes specific packets from being displayed, such as `not ftp` to exclude FTP packets from being displayed in the packet list. Finally, brackets can be used to group statements together.

FOLLOWING STREAMS & CUSTOMISING COLUMNS

<input type="radio"/> DF3) Digital Evidence Collection
● 8 Topics 1 Quiz
<input type="radio"/> DF4) Windows Investigations
● 3 Topics 3 Quizzes
<input type="radio"/> DF5) Linux Investigations
● 4 Topics 2 Quizzes
<input type="radio"/> DF6) Volatility
● 3 Topics 1 Quiz
<input type="radio"/> DF7) Autopsy
● 4 Topics 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

<input type="radio"/> SI1) Introduction to SIEM
● 7 Topics 1 Quiz
<input type="radio"/> SI2) Logging
● 6 Topics 2 Quizzes
<input type="radio"/> SI3) Aggregation
● 2 Topics 1 Quiz
<input type="radio"/> SI4) Correlation
● 6 Topics 1 Quiz
<input type="radio"/> SI5) Using Splunk
● 5 Topics 2 Quizzes

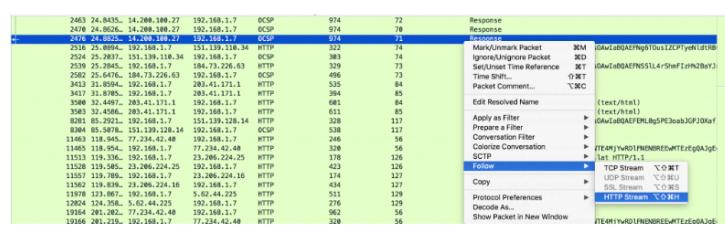
INCIDENT RESPONSE DOMAIN

<input type="radio"/> IR1) Introduction to Incident Response
● 8 Topics 1 Quiz
<input type="radio"/> IR2) Preparation Phase
● 10 Topics 2 Quizzes
<input checked="" type="radio"/> IR3) Detection and Analysis Phase
● 7 Topics 4 Quizzes
<input type="radio"/> Section Introduction, Detection & Analysis
<input type="radio"/> Common Events & Incidents
<input type="radio"/> Using Baselines & Behavior Profiles
<input type="radio"/> Introduction to Wireshark (GUI)
○ Introduction to Wireshark (Analysis)
<input type="checkbox"/> Lab Network Traffic Analysis
<input type="radio"/> YARA Rules For Detection
<input type="checkbox"/> Legacy Activity) Threat Hunting With YARA
<input type="radio"/> CMD and PowerShell For Incident Response
<input type="checkbox"/> Lab CMD and PowerShell
<input type="checkbox"/> Activity) End of Section Review, Detection & Analysis
<input type="radio"/> IR4) Containment, Eradication, and Recovery Phase
● 5 Topics 1 Quiz
<input type="radio"/> IR5) Lessons Learned and Reporting
● 7 Topics
<input type="radio"/> IR6) MITRE ATT&CK
● 13 Topics 2 Quizzes

BTL1 EXAM

<input type="radio"/> Exam Preparation
<input type="radio"/> Using RDP and SSH
<input type="radio"/> How to Start Your Exam

Imagine you want to analyze an HTTP communication between a web server and a host. You are interested in having a holistic view of the dozens of HTTP requests and responses. In this case, looking at each individual packet will not be of much profit to us – this is where Wireshark's protocol stream following feature shines.



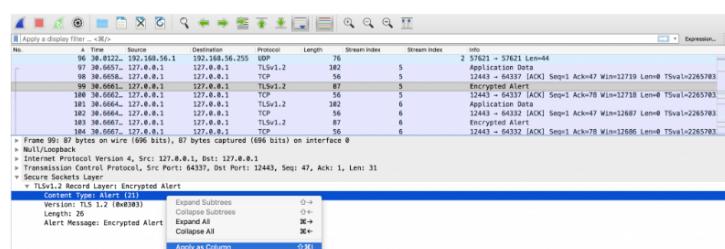
To follow a stream, right-click on a packet within the stream, and click **Follow** > **TCP Stream**/**UDP Stream**/**SSL Stream**/**HTTP Stream**. Inapplicable streams should be greyed out in the pop-up menu. Wireshark should automatically apply a display filter for the stream and open a new window displaying the contents of the packets in the stream.



As you can see from the above image of a simple HTTP file download, HTTP requests should be highlighted in red and HTTP responses in blue. You can easily see the request header and the response header and file content.

Compared to looking at the request and response packets individually, looking at the stream saves time and effort as the communication is displayed all in one window.

In addition to following streams, you can view specific packet information in the packet list by customizing the columns in the packet list.



To add a packet header value as a column, right-click the header field and select **Apply as Column**. In the above image, the SSL content type is applied as a column. The benefit of adding certain header values as a column is the ability for quick visual identification of packets having a specific value that we are interested in.

VIEWING CAPTURE STATISTICS

Wireshark collects different statistics about the traffic in the capture file – such as the percentage proportions of protocols, the number of bytes transmitted to different hosts, the IP addresses of all the hosts that has appeared in the capture. They are helpful in certain scenarios, such as finding potential exfiltration vectors and identifying the exfiltrating host based on network usage.

This section will discuss three of the statistics windows.

- Protocol Hierarchy
 - Conversations,
 - and Endpoints

PROTOCOL HIERARCHY

The Protocol Hierarchy window displays the percentages of the number of packets or bytes in a protocol conversation against the entire traffic. The protocols are organized in layers from Layer 2 to Layer 7. The below image shows:

- 99.7% of the traffic captured were IPv4 packets
 - 96.6% being TCP, and
 - 46.3% being SSL
 - It also shows that there were 2167 SSL packets, totaling around 177 KB

Language		Wingard - Protocol Header Statistics - Localhost (10)				Wingard - Connections - Localhost (10)				Wingard - Endpoints - Localhost (10)				
Protocol	Port	Percent Packets	Percent Bytes	Bytes	Bytes/s	End Packets	End Bytes	End/s	Protocol	Port	Connections	Connections/s	Protocol	Port
Frame									Frame				Frame	
Null [*]	0	46.61	0.0	1041196	1041196	0	0	0	TCP	0	0	0	TCP	0
TCP	0	100.0	45861	100.0	1724	164	0	0	TCP	0	0	0	TCP	0
Internet Protocol Version 6	0	0.3	14	0.0	560	4	0	0	TCP	0	0	0	TCP	0
Link Layer Datagram Protocol	0	0.3	14	0.0	12	0	0	0	TCP	0	0	0	TCP	0
Multicast Domain Name System	0	0.3	14	0.1	1667	14	14	1667	TCP	0	0	0	TCP	0
Internet Protocol Version 4	0	0.0	4667	0.6	93340	821	0	0	TCP	0	0	0	TCP	0
Link Layer Datagram Protocol	0	0.1	144	0.0	1667	14	14	1667	TCP	0	0	0	TCP	0
Multicast Domain Name System	0	0.9	43	0.2	3771	33	43	3771	TCP	0	0	0	TCP	0
Data	0	0.2	705	0.2	4468	39	102	4468	TCP	0	0	0	TCP	0
Transmission Control Protocol	0	0.0	4662	0.0	1040373	1040373	0	0	TCP	0	0	0	TCP	0
Secure Sockets Layer	46.3	2167	0.0	1040620	1040620	10 k	2161	10 k	TCP	0	0	0	TCP	0
HyperText Transfer Protocol	0.6	30	0.0	10767	94	15	34	30	TCP	0	0	0	TCP	0
Domain Name System Status Protocol	0.0	1	0.0	14	0	1	1	14	TCP	0	0	0	TCP	0
Line-based test data	0.0	2	0.0	1668	14	2	2059	14	TCP	0	0	0	TCP	0
JavaScript Object Notation	0.0	1	0.0	422	3	1	422	3	TCP	0	0	0	TCP	0
Data	0.0	12	0.1	2916	20	12	2931	20	TCP	0	0	0	TCP	0

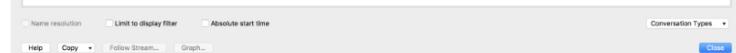
To check a specific protocol traffic in the packet list, right-click on a protocol and select **Apply as Filter > Selected/Not Selected** to have Wireshark automatically create and apply a display filter showing/excluding the specified protocol traffic.

The Protocol Hierarchy window can also identify data exfiltration through unusual or unused protocols. If you notice a very small portion of FTP traffic in a large network that doesn't use FTP, it might be worth it to check out the FTP traffic and make sure the traffic is legitimate. Quite a few of network analysis challenges in CTFs dealing with data exfiltration can be solved by identifying unusual protocols from the Protocol Hierarchy window.

CONVERSATIONS

The Conversations window also provides a wealth of information on the traffic, including which hosts communicated which hosts, on which ports, and with a total of how many bytes and packets in the conversation. This window is great for identifying the different MAC or IP addresses that a host has communicated with, and the volume of traffic between them.

Similarly to the Protocol Hierarchy window, the Conversations window can be very helpful in investigating data exfiltration attempts, as it can identify the attacker by IP address. If a host has been transmitting many packets and bytes to an unidentified IP address without receiving many packets in return, an exfiltration could have been occurring.



In the above image, as shown by the first line, host 192.168.56.17 has been connecting to 172.217.167.98's HTTPS server (this is actually Google) with port 65220 and has sent and received 9 packets. Similar to the Protocol Hierarchy window, you can right-click on a line, select **Apply as Filter > Selected/Not Selected** and choose the direction of traffic to apply a filter for the line.

ENDPOINTS

Lastly, the Endpoints window shows all of the different hosts that appear in the capture and the amount of packets/bytes they sent and received. This window is useful in sorting hosts by their network activity, by either transmission or receiving volume, or by both.

If a host has been receiving much more traffic than they have been transmitting, the host is probably downloading a large file. On the other hand, if the host has been transmitting more than they have been receiving, the host is probably uploading files or backing up to remote storage, such as the cloud.

Address	Pkts	Bytes	Tx Packets		Rx Packets		Rx Bytes	Country	City	AS Number	AS Organization
			Ethernet	IP	IP	TCP					
8.8.8.8	4	578	2	382	0	—	—	—	—	—	—
36.168.234.30	16	2013	8	828	8	1185	—	—	—	—	—
36.168.234.47	12	990	6	489	6	501	—	—	—	—	—
36.168.234.53	13	173	27	8993	28	8040	—	—	—	—	—
74.126.68.157	4	240	2	132	2	108	—	—	—	—	—
77.224.41.224	4	468	2	372	2	266	—	—	—	—	—
98.68.1.1	42	17 k	20	13 k	22	3415	—	—	—	—	—
104.17.85.4	2	110	1	95	1	54	—	—	—	—	—
104.24.1.87	21	6514	9	5330	13	1584	—	—	—	—	—
104.199.240.186	21	5660	8	1264	13	4306	—	—	—	—	—
104.244.36.20	21	5243	9	1437	12	3806	—	—	—	—	—
104.199.133.232	2	159	1	85	1	54	—	—	—	—	—
104.199.133.232	6	409	3	239	3	102	—	—	—	—	—
104.199.133.233	36	5699	18	2168	18	3031	—	—	—	—	—
104.199.133.233	172	24 k	88	18 k	88	4700	—	—	—	—	—
172.31.208.6	2	248	0	0	2	248	—	—	—	—	—
172.217.8.195	4	240	2	132	2	108	—	—	—	—	—
172.217.25.46	4	240	2	132	2	108	—	—	—	—	—
172.217.25.46	1,062	339 k	776	114 k	832	225 k	—	—	—	—	—
172.217.25.130	22	1080	11	1150	11	1536	—	—	—	—	—
172.217.167.98	4	240	2	132	2	108	—	—	—	—	—
172.217.167.98	18	1669	9	847	9	822	—	—	—	—	—
192.168.1.255	2,286	483 k	1086	311 k	1,086	182 k	—	—	—	—	—
192.168.1.255	2	172	0	0	2	172	—	—	—	—	—
192.168.43.1	2	248	0	0	2	248	—	—	—	—	—
216.58.199.34	22	2316	11	997	11	1408	—	—	—	—	—
216.58.199.68	4	240	2	132	2	108	—	—	—	—	—
216.58.203.98	100	58 k	56	8979	56	41 k	—	—	—	—	—
216.58.203.98	22	2490	11	992	11	1508	—	—	—	—	—
224.0.0.251	1	87	0	0	1	87	—	—	—	—	—
239.255.255.260	1	168	0	0	1	168	—	—	—	—	—

In the above diagram, host 192.168.1.7 has sent 1156 packets, totaling 311 KB, and has received 1080 packets, totaling 182 KB. You can switch to other protocols, such as TCP to have traffic sorted by ports and Ethernet to have traffic sorted by MAC addresses. Same with all other statistics windows, you can right-click on a host to apply it as a filter.

Quizzes

Lab) Network Traffic Analysis

◀ Previous Topic
Back to Lesson
Next Topic ▶

Privacy & Cookies Policy