

How to read a Wireshark TCP/HTTP log

In this reading, you'll learn how to read a Wireshark TCP/HTTP log for network traffic between employee website visitors and the company's web server. Most network protocol/traffic analyzer tools used to capture packets will provide this same information.

Log entry number and time

| No. | Time |
|-----|----------|
| 47 | 3.144521 |
| 48 | 3.195755 |
| 49 | 3.246989 |

This Wireshark TCP log section provided to you starts at log entry number (No.) 47, which is three seconds and .144521 milliseconds after the logging tool started recording. This indicates that approximately 47 messages were sent and received by the web server in the 3.1 seconds after starting the log. This rapid traffic speed is why the tool tracks time in milliseconds.

Source and destination IP addresses

| Source | Destination |
|---------------|---------------|
| 198.51.100.23 | 192.0.2.1 |
| 192.0.2.1 | 198.51.100.23 |
| 198.51.100.23 | 192.0.2.1 |

The source and destination columns contain the source IP address of the machine that is sending a packet and the intended destination IP address of the packet. In this log file, the IP address 192.0.2.1 belongs to the company's web server. The range of IP addresses in 198.51.100.0/24 belong to the employees' computers.

Protocol type and related information

| Protocol | Info |
|----------|------|
|----------|------|

| | |
|-----|---|
| TCP | 42584->443 [SYN] Seq=0 Win=5792 Len=120... |
| TCP | 443->42584 [SYN, ACK] Seq=0 Win=5792 Len=120... |
| TCP | 42584->443 [ACK] Seq=1 Win=5792 Len=120... |

The Protocol column indicates that the packets are being sent using the TCP protocol, which is at the transport layer of the TCP/IP model. In the given log file, you will notice that the protocol will eventually change to HTTP, at the application layer, once the connection to the web server is successfully established.

The Info column provides information about the packet. It lists the source port followed by an arrow → pointing to the destination port. In this case, port 443 belongs to the web server. Port 443 is normally used for encrypted web traffic.

The next data element given in the Info column is part of the three-way handshake process to establish a connection between two machines. In this case, employees are trying to connect to the company's web server:

- The [SYN] packet is the initial request from an employee visitor trying to connect to a web page hosted on the web server. SYN stands for "synchronize."
- The [SYN, ACK] packet is the web server's response to the visitor's request agreeing to the connection. The server will reserve system resources for the final step of the handshake. SYN, ACK stands for "synchronize acknowledge."
- The [ACK] packet is the visitor's machine acknowledging the permission to connect. This is the final step required to make a successful TCP connection. ACK stands for "acknowledge."

The next few items in the Info column provide more details about the packets. However, this data is not needed to complete this activity. If you would like to learn more about packet properties, please visit [Microsoft's Introduction to Network Trace Analysis](#).

Normal website traffic

A normal transaction between a website visitor and the web server would be like:

| No. | Time | Source | Destination | Protocol | Info |
|-----|----------|---------------|-------------|----------|--|
| 47 | 3.144521 | 198.51.100.23 | 192.0.2.1 | TCP | 42584->443 [SYN] Seq=0 Win=5792 Len=120... |

| | | | | | |
|----|----------|---------------|---------------|------|---|
| 48 | 3.195755 | 192.0.2.1 | 198.51.100.23 | TCP | 443->42584 [SYN, ACK] Seq=0 Win=5792 Len=120... |
| 49 | 3.246989 | 198.51.100.23 | 192.0.2.1 | TCP | 42584->443 [ACK] Seq=1 Win=5792 Len=120... |
| 50 | 3.298223 | 198.51.100.23 | 192.0.2.1 | HTTP | GET /sales.html HTTP/1.1 |
| 51 | 3.349457 | 192.0.2.1 | 198.51.100.23 | HTTP | HTTP/1.1 200 OK (text/html) |

Notice that the handshake process takes a few milliseconds to complete. Then, you can identify the employee's browser requesting the sales.html webpage using the HTTP protocol at the application level of the TCP/IP model. Followed by the web server responding to the request.

The Attack

As you learned previously, malicious actors can take advantage of the TCP protocol by flooding a server with SYN packet requests for the first part of the handshake. However, if the number of SYN requests is greater than the server resources available to handle the requests, then the server will become overwhelmed and unable to respond to the requests. This is a network level denial of service (DoS) attack, called a SYN flood attack, that targets network bandwidth to slow traffic. A SYN flood attack simulates a TCP connection and floods the server with SYN packets. A DoS direct attack originates from a single source. A distributed denial of service (DDoS) attack comes from multiple sources, often in different locations, making it more difficult to identify the attacker or attackers.

| | A | B | C | D | E | |
|--|-----|----------|--------------------------|-------------------------------|----------|--------------------------|
| 1 | No. | Time | Source (x = redacted) | Destination (x = redacted) | Protocol | Info |
| 2 | 47 | 3.144521 | 53.22.136.x | 100.0.111.x | TCP | 42584 |
| 3 | 48 | 3.195755 | 100.0.111.x | 53.22.136.x | TCP | 443-> |
| 4 | 49 | 3.246989 | 53.22.136.x | 100.0.111.x | TCP | 42584 |
| 5 | 50 | 3.298223 | 198.51.100.23 | 192.0.2.1 | HTTP | GET /sales.html HTTP/1.1 |
| <div> <div>+</div> <div>≡</div> <div>TCP log ▾</div> <div>Color coded TCP log ▾</div> </div> | | | | | | |

There are two tabs at the bottom of the log file. One is labeled "Color coded TCP log." If you click on that tab, you will find the server interactions with the attacker's IP address (203.0.113.0) marked with red highlighting (and the word "red" in column A).

| Color as text | No. | Time | Source (x = redacted) | Destination (x = redacted) | Protocol | Info |
|------------------|-----|------|--------------------------|-------------------------------|----------|------|
|------------------|-----|------|--------------------------|-------------------------------|----------|------|

| | | | | | | |
|-------|----|----------|---------------|---------------|------|--|
| red | 52 | 3.390692 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 53 | 3.441926 | 192.0.2.1 | 203.0.113.0 | TCP | 443->54770 [SYN, ACK] Seq=0 Win=5792 Len=120... |
| red | 54 | 3.493160 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [ACK Seq=1 Win=5792 Len=0... |
| green | 55 | 3.544394 | 198.51.100.14 | 192.0.2.1 | TCP | 14785->443 [SYN] Seq=0 Win=5792 Len=120... |
| green | 56 | 3.599628 | 192.0.2.1 | 198.51.100.14 | TCP | 443->14785 [SYN, ACK] Seq=0 Win=5792 Len=120... |
| red | 57 | 3.664863 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| green | 58 | 3.730097 | 198.51.100.14 | 192.0.2.1 | TCP | 14785->443 [ACK] Seq=1 Win=5792 Len=120... |
| red | 59 | 3.795332 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=120... |
| green | 60 | 3.860567 | 198.51.100.14 | 192.0.2.1 | HTTP | GET /sales.html HTTP/1.1 |
| red | 61 | 3.939499 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=120... |
| green | 62 | 4.018431 | 192.0.2.1 | 198.51.100.14 | HTTP | HTTP/1.1 200 OK (text/html) |

Initially, the attacker's SYN request is answered normally by the web server (log items 52-54). However, the attacker keeps sending more SYN requests, which is abnormal. At this point, the web server is still able to respond to normal visitor traffic, which is highlighted and labeled as green. An employee visitor with the IP address of 198.51.100.14 successfully completes a SYN/ACK connection handshake with the webserver (log item nos. 55, 56, 58). Then, the employee's browser requests the sales.html webpage with the GET command and the web server responds (log item no. 60 and 62).

| Color as text | No. | Time | Source | Destination | Protocol | Info |
|---------------|-----|----------|--------------|-------------|----------|--|
| green | 63 | 4.097363 | 198.51.100.5 | 192.0.2.1 | TCP | 33638->443 [SYN] Seq=0 Win=5792 Len=120... |
| red | 64 | 4.176295 | 192.0.2.1 | 203.0.113.0 | TCP | 443->54770 [SYN, ACK] Seq=0 Win=5792 Len=120... |

| | | | | | | |
|--------|----|----------|---------------|---------------|------|--|
| green | 65 | 4.255227 | 192.0.2.1 | 198.51.100.5 | TCP | 443->33638 [SYN, ACK] Seq=0 Win=5792 Len=120... |
| red | 66 | 4.256159 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| green | 67 | 5.235091 | 198.51.100.5 | 192.0.2.1 | TCP | 33638->443 [ACK] Seq=1 Win=5792 Len=120... |
| red | 68 | 5.236023 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| green | 69 | 5.236955 | 198.51.100.16 | 192.0.2.1 | TCP | 32641->443 [SYN] Seq=0 Win=5792 Len=120... |
| red | 70 | 5.237887 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| green | 71 | 6.228728 | 198.51.100.5 | 192.0.2.1 | HTTP | GET /sales.html HTTP/1.1 |
| red | 72 | 6.229638 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| yellow | 73 | 6.230548 | 192.0.2.1 | 198.51.100.16 | TCP | 443->32641 [RST, ACK] Seq=0 Win=5792 Len=120... |
| red | 74 | 6.330539 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| green | 75 | 6.330885 | 198.51.100.7 | 192.0.2.1 | TCP | 42584->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 76 | 6.331231 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| yellow | 77 | 7.330577 | 192.0.2.1 | 198.51.100.5 | TCP | HTTP/1.1 504 Gateway Time-out (text/html) |
| red | 78 | 7.331323 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| green | 79 | 7.340768 | 198.51.100.22 | 192.0.2.1 | TCP | 6345->443 [SYN] Seq=0 Win=5792 Len=0... |
| yellow | 80 | 7.340773 | 192.0.2.1 | 198.51.100.7 | TCP | 443->42584 [RST, ACK] Seq=1 Win=5792 Len=120... |
| red | 81 | 7.340778 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 82 | 7.340783 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 83 | 7.439658 | 192.0.2.1 | 203.0.113.0 | TCP | 443->54770 [RST, ACK] Seq=1 Win=5792 Len=0... |

In the next 20 rows, the log begins to reflect the struggle the web server is having to keep up with the abnormal number of SYN requests coming in at a rapid pace. The attacker is sending several SYN requests every second. The rows highlighted and labeled yellow are failed communications between legitimate employee website visitors and the web server.

The two types of errors in the logs include:

- An HTTP/1.1 504 Gateway Time-out (text/html) error message. This message is generated by a gateway server that was waiting for a response from the web server. If the web server takes too long to respond, the gateway server will send a timeout error message to the requesting browser.
- An [RST, ACK] packet, which would be sent to the requesting visitor if the [SYN, ACK] packet is not received by the web server. RST stands for reset, acknowledge. The visitor will receive a timeout error message in their browser and the connection attempt is dropped. The visitor can refresh their browser to attempt to send a new SYN request.

| Color as text | No. | Time | Source (x = redacted) | Destination (x = redacted) | Protocol | Info |
|---------------|-----|-----------|-----------------------|----------------------------|----------|---|
| red | 119 | 19.198705 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 120 | 19.521718 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| yellow | 121 | 19.844731 | 192.0.2.1 | 198.51.100.9 | TCP | 443->4631 [RST, ACK] Seq=1 Win=5792 Len=0... |
| red | 122 | 20.167744 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 123 | 20.490757 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 124 | 20.81377 | 192.0.2.1 | 203.0.113.0 | TCP | 443->54770 [RST, ACK] Seq=1 Win=5792 Len=0... |
| red | 125 | 21.136783 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 126 | 21.459796 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 127 | 21.782809 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 128 | 22.105822 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 |

| | | | | | | |
|-----|-----|-----------|-------------|-----------|-----|---|
| | | | | | | Win=5792 Len=0... |
| red | 129 | 22.428835 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 130 | 22.751848 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 131 | 23.074861 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 132 | 23.397874 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 133 | 23.720887 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 134 | 24.0439 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 135 | 24.366913 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 136 | 24.689926 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 137 | 25.012939 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 138 | 25.335952 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 139 | 25.658965 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 140 | 25.981978 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 141 | 26.304991 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 142 | 26.628004 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 143 | 26.951017 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 144 | 27.27403 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 145 | 27.597043 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 146 | 27.920056 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |

| | | | | | | |
|-----|-----|-----------|-------------|-----------|-----|---|
| red | 147 | 28.243069 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 148 | 28.566082 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 149 | 28.889095 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 150 | 29.212108 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 151 | 29.535121 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |
| red | 152 | 29.858134 | 203.0.113.0 | 192.0.2.1 | TCP | 54770->443 [SYN] Seq=0 Win=5792 Len=0... |

As you scroll through the rest of the log, you will notice the web server stops responding to legitimate employee visitor traffic. The visitors receive more error messages indicating that they cannot establish or maintain a connection to the web server. From log item number 125 on, the web server stops responding. The only items logged at that point are from the attack. As there is only one IP address attacking the web server, you can assume this is a direct DoS SYN flood attack.