Trong phần này, bạn sẽ học cách đọc **Wireshark TCP/HTTP log** cho lưu lượng mạng giữa khách truy cập website nội bộ và web server của công ty. Hầu hết các công cụ phân tích **network protocol/traffic analyzer** dùng để bắt gói tin đều cung cấp thông tin tương tự.

1. Số thứ tự log và thời gian

No.	Time
47	3.144521
48	3.195755
49	3.246989

Phần log của **Wireshark TCP** này bắt đầu tại log số 47, tức là sau 3.144521 giây kể từ khi công cụ ghi nhận bắt đầu hoạt động. Điều này cho thấy có khoảng 47 thông điệp được gửi và nhận bởi web server trong 3.1 giây đầu. Tốc độ này diễn ra rất nhanh nên công cụ phải đo bằng **milliseconds**.

2. Địa chỉ IP nguồn và đích

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

Cột **Source** và **Destination** thể hiện địa chỉ IP nguồn gửi gói tin và địa chỉ IP đích nhận gói tin. Trong file log này, **192.0.2.1** là web server của công ty, còn dải **198.51.100.0/24** thuộc về máy tính nhân viên.

3. Loại protocol và thông tin liên quan

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...

- Cột **Protocol** cho biết các gói tin đang được gửi bằng **TCP protocol** (thuộc transport layer trong mô hình **TCP/IP**). Sau khi kết nối thành công, protocol sẽ chuyển sang **HTTP** (application layer).
- Cột **Info** liệt kê port nguồn và port đích. Ở đây **port 443** là của web server, thường dùng cho web traffic mã hóa.

Ba bước bắt tay TCP (three-way handshake):

- **[SYN]**: Máy nhân viên gửi yêu cầu kết nối đến web server.
- **[SYN, ACK]**: Web server phản hồi chấp nhận yêu cầu và dự trữ tài nguyên.
- **[ACK]**: Máy nhân viên xác nhận, hoàn tất kết nối TCP.

4. Lưu lượng website bình thường

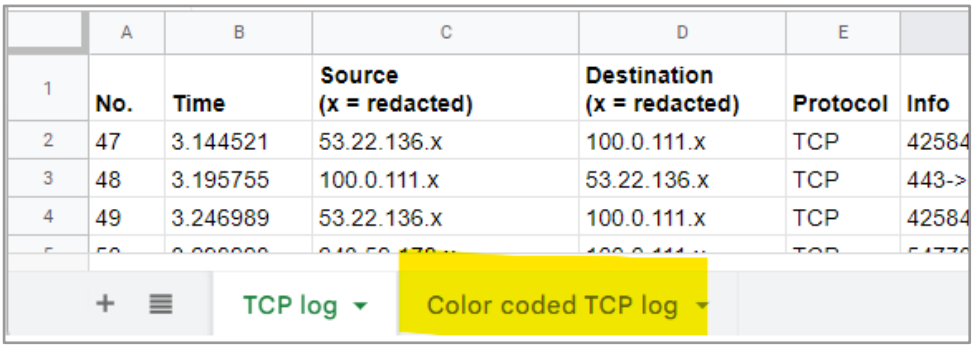
Ví dụ một giao dịch bình thường

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)

5. Cuộc tấn công

Kẻ tấn công có thể lợi dụng TCP bằng cách gửi **SYN flood** (rất nhiều gói SYN) khiến web server không còn tài nguyên để phản hồi. Đây là **DoS attack** (tấn công từ chối dịch vụ) ở mức **network layer**.

- Nếu từ một nguồn duy nhất: **DoS direct attack**.
- Nếu từ nhiều nguồn: **DDoS attack**, khó phát hiện hơn.



	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

TCP log đánh dấu màu

Trong log có hai tab:

- Một tab bình thường.
- Một tab **Color coded TCP log**: hiển thị tương tác giữa server và IP attacker **203.0.113.0** (đánh dấu màu đỏ).

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)

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...

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...

Từ log số 125 trở đi, web server không còn phản hồi traffic hợp lệ nữa, chỉ ghi nhận các gói **SYN** từ attacker. Vì chỉ có một IP tấn công, đây là **direct DoS SYN flood attack**.