

Cybersecurity Incident Report

Section 1: Analysis of the type of attack

Based on the symptoms described in the scenario, the likely type of attack causing the network interruption is a denial of service (DoS) attack, specifically a SYN flood attack. This conclusion is drawn from the observation of a large number of TCP SYN requests coming from an unfamiliar IP address, overwhelming the web server and preventing it from responding to legitimate connection requests.

Section 2: Explanation of the attack and its impact

In a SYN flood attack, the attacker floods the target server with a massive volume of SYN packets, exploiting the three-way handshake process of the TCP protocol. The three-way handshake involves sending a SYN packet from the source, receiving a SYN-ACK packet from the destination to acknowledge the connection request, and finally sending an ACK packet to establish the connection.

In this scenario, the attacker sends an overwhelming number of SYN packets, exhausting the server's resources that are reserved for establishing connections. As a result, the web server becomes unable to process legitimate connection requests from visitors, leading to connection timeouts and the website becoming inaccessible.

The consequences of this attack are significant. The website experiences service interruption, preventing employees from accessing the sales webpage and impacting the business's ability to promote and sell vacation packages. The attack disrupts normal operations, causing inconvenience to both the company and its customers.

To prevent future attacks, it is important to implement mitigation measures. One potential solution is to employ rate limiting or SYN cookies on the web server to filter and manage incoming SYN requests. Additionally, deploying a robust intrusion detection and prevention system (IDPS) can help detect and block suspicious traffic patterns associated with SYN flood attacks. Regular network monitoring and keeping security systems up to date are also essential in maintaining a secure network environment.

The figure consists of two screenshots of the Wireshark network protocol analyzer interface.

Top Screenshot: Packet 1 Analysis

- Filter:** eth.addr == 42:01:ac:15:e0:02
- Packet List:** Shows packet 1 at time 0.000000, source 172.21.224.2, destination 35.235.244.34, protocol TCP, length 196.
- Packet Details:**
 - Frame 1: 210 bytes on wire (1680 bits), 210 bytes captured (1680 bits) on interface 0.
 - Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
 - Internet Protocol Version 4, Src: 172.21.224.2, Dst: 35.235.244.34
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
 - Total Length: 196
 - Identification: 0xda77 (55927)
 - 010. = Flags: 0x2, Don't fragment
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 64
 - Protocol: TCP (6)
 - Header Checksum: 0xbb86 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 172.21.224.2
 - Destination Address: 35.235.244.34
 - Transmission Control Protocol, Src Port: 22, Dst Port: 35193, Seq: 1, Ack: 1, Len: 144
 - SSH Protocol
- Packet Bytes:** Shows the raw packet data in hexadecimal and ASCII.

Bottom Screenshot: Packet 12 Analysis

- Filter:** udp.port == 53
- Packet List:** Shows packet 12 at time 8.641978, source 169.254.169.254, destination 172.21.224.2, protocol DNS, length 177.
- Packet Details:**
 - Frame 12: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits) on interface 0.
 - Ethernet II, Src: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01), Dst: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02)
 - Internet Protocol Version 4, Src: 169.254.169.254, Dst: 172.21.224.2
 - User Datagram Protocol, Src Port: 53, Dst Port: 53
 - Domain Name System (response)
 - Transaction ID: 0xc26
- Packet Bytes:** Shows the raw packet data in hexadecimal and ASCII.

Figure 1 - Packet analyzed via Wireshark

Lab takeaways:

I gained several valuable skills and knowledge in the field of network traffic analysis using Wireshark. I learned how to open and explore packet capture files, which contain valuable information about network communications. By examining the basic Wireshark graphical user interface, I became familiar with the key properties of network packets, such as the packet index, timestamp, source and destination IP addresses, protocol, length, and payload information.

I also learned how to apply filters to efficiently sort through packet data and focus on specific criteria. By filtering traffic associated with a specific IP address, I was able to narrow down the packets of interest. Moreover, I gained the ability to inspect individual packets in detail, analyzing various protocol and data layers within them. This involved navigating through different subtrees to gather information about the overall packet, Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) data.

In addition to examining TCP packets, I explored filters to select and explore DNS packets. I learned how to identify DNS queries and responses and extract information such as the queried website name and associated IP addresses. Furthermore, I developed skills in filtering TCP packets and searching for specific text data within them, which is useful for locating packets containing relevant information.

Overall, this activity enhanced my ability to analyze network traffic effectively using Wireshark, a fundamental tool for security analysts. I gained proficiency in opening and exploring packet capture files, applying filters to select specific packets, and inspecting packet details at various protocol layers. These skills are crucial for identifying potential security threats, understanding network communications, and conducting thorough investigations in cybersecurity.

Analyzed Incident Wireshark TCP/HTTP Log:

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)
52	3.390692	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
53	3.441926	192.0.2.1	203.0.113.0	TCP	443->54770 [SYN, ACK] Seq=0 Win=5792 Len=120...
54	3.49316	203.0.113.0	192.0.2.1	TCP	54770->443 [ACK Seq=1 Win=5792 Len=0...
55	3.544394	198.51.100.14	192.0.2.1	TCP	14785->443 [SYN] Seq=0 Win=5792 Len=120...
56	3.599628	192.0.2.1	198.51.100.14	TCP	443->14785 [SYN, ACK] Seq=0 Win=5792 Len=120...
57	3.664863	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
58	3.730097	198.51.100.14	192.0.2.1	TCP	14785->443 [ACK] Seq=1 Win=5792 Len=120...
59	3.795332	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=120...
60	3.860567	198.51.100.14	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
61	3.939499	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=120...
62	4.018431	192.0.2.1	198.51.100.14	HTTP	HTTP/1.1 200 OK (text/html)
63	4.097363	198.51.100.5	192.0.2.1	TCP	33638->443 [SYN] Seq=0 Win=5792 Len=120...
64	4.176295	192.0.2.1	203.0.113.0	TCP	443->54770 [SYN, ACK] Seq=0 Win=5792 Len=120...
65	4.255227	192.0.2.1	198.51.100.5	TCP	443->33638 [SYN, ACK] Seq=0 Win=5792 Len=120...
66	4.256159	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
67	5.235091	198.51.100.5	192.0.2.1	TCP	33638->443 [ACK] Seq=1 Win=5792 Len=120...
68	5.236023	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
69	5.236955	198.51.100.16	192.0.2.1	TCP	32641->443 [SYN] Seq=0 Win=5792 Len=120...
70	5.237887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

71	6.228728	198.51.100.5	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
72	6.229638	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
73	6.230548	192.0.2.1	198.51.100.16	TCP	443->32641 [RST, ACK] Seq=0 Win=5792 Len=120...
74	6.330539	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
75	6.330885	198.51.100.7	192.0.2.1	TCP	42584->443 [SYN] Seq=0 Win=5792 Len=0...
76	6.331231	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
77	7.330577	192.0.2.1	198.51.100.5	TCP	HTTP/1.1 504 Gateway Time-out (text/html)
78	7.351323	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
79	7.360768	198.51.100.22	192.0.2.1	TCP	6345->443 [SYN] Seq=0 Win=5792 Len=0...
80	7.380773	192.0.2.1	198.51.100.7	TCP	443->42584 [RST, ACK] Seq=1 Win=5792 Len=120...
81	7.380878	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
82	7.383879	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
83	7.482754	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
84	7.581629	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
85	7.680504	192.0.2.1	198.51.100.22	TCP	443->6345 [RST, ACK] Seq=1 Win=5792 Len=0...
86	7.709377	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
87	7.738241	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
88	7.767105	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
89	13.895969	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
90	13.919832	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
91	13.943695	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
92	13.967558	192.0.2.1	198.51.100.16	TCP	443->32641 [RST, ACK] Seq=1 Win=5792 Len=120...
93	13.991421	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
94	14.015245	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
95	14.439072	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
96	14.862899	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
97	14.886727	198.51.100.9	192.0.2.1	TCP	4631->443 [SYN] Seq=0 Win=5792 Len=0...
98	15.310554	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
99	15.734381	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
100	16.158208	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
101	16.582035	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
102	17.005862	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
103	17.429678	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
104	17.452693	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
105	17.475708	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
106	17.498723	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
107	17.521738	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
108	17.544753	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
109	17.567768	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
110	17.590783	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
111	18.413795	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
112	18.436807	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
113	18.459819	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
114	18.482831	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
115	18.506655	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
116	18.529667	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

117	18.552679	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
118	18.875692	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
119	19.198705	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
120	19.521718	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
121	19.844731	192.0.2.1	198.51.100.9	TCP	443->4631 [RST, ACK] Seq=1 Win=5792 Len=0...
122	20.167744	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
123	20.490757	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
124	20.81377	192.0.2.1	203.0.113.0	TCP	443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
125	21.136783	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
126	21.459796	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
127	21.782809	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
128	22.105822	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
129	22.428835	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
130	22.751848	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
131	23.074861	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
132	23.397874	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
133	23.720887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
134	24.0439	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
135	24.366913	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
136	24.689926	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
137	25.012939	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
138	25.335952	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
139	25.658965	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
140	25.981978	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
141	26.304991	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
142	26.628004	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
143	26.951017	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
144	27.27403	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
145	27.597043	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
146	27.920056	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
147	28.243069	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
148	28.566082	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
149	28.889095	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
150	29.212108	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
151	29.535121	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
152	29.858134	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
153	30.181147	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
154	30.50416	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
155	30.827173	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
156	31.150186	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
157	31.473199	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
158	31.796212	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
159	32.119225	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
160	32.442238	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
161	32.765251	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
162	33.088264	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

163	33.411277	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
164	33.73429	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
165	34.057303	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
166	34.380316	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
167	34.703329	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
168	35.026342	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
169	35.349355	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
170	35.672368	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
171	35.995381	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
172	36.318394	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
173	36.641407	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
174	36.96442	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
175	37.287433	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
176	37.610446	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
177	37.933459	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
178	38.256472	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
179	38.579485	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
180	38.902498	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
181	39.225511	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
182	39.548524	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
183	39.871537	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
184	40.19455	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
185	40.517563	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
186	40.840576	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
187	41.163589	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
188	41.486602	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
189	41.809615	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
190	42.132628	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
191	42.455641	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
192	42.778654	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
193	43.101667	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
194	43.42468	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
195	43.747693	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
196	44.070706	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
197	44.393719	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
198	44.716732	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
199	45.039745	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
200	45.362758	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
201	45.685771	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
202	46.008784	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
203	46.331797	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
204	46.65481	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
205	46.977823	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
206	47.300836	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
207	47.623849	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
208	47.946862	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

209	48.269875	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
210	48.592888	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
211	48.915901	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
212	49.238914	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
213	49.561927	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
214	49.88494	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
214	50.207953	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
214	50.530966	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
214	50.853979	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
214	51.176992	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
214	51.500005	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
214	51.823018	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...