

Wireshark

`ftp.request` - to view FTP traffic

`http.request.method==POST` - to view credentials submitted over HTTP

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes options like 'Файл', 'Редактирование', 'Просмотр', 'Запуск', 'Захват', 'Анализ', 'Статистика', 'Телефония', 'Беспроводной', 'Инструменты', and 'Помощь'. Below the menu is a toolbar with various icons for file operations, packet navigation, and analysis. The main display area is divided into three panes. The top pane shows a list of captured packets. The middle pane displays the details of the selected packet (No. 160). The bottom pane shows the raw packet data in hexadecimal and ASCII.

The packet list pane shows a single packet (No. 160) at time 7.640966, source 192.168.0.104, destination 44.228.249.3, protocol HTTP, length 696, and info POST /login HTTP/1.1 (application/x-www-form-urlencoded).

The packet details pane shows the following structure:

- Frame 160: 696 bytes on wire (5568 bits), 696 bytes captured (5568 bits) on interface \Device\NPF_{4D49321B-65EC-4AF0-8322-37A63E}
- Ethernet II, Src: Tp-LinkT_d9:68:76 (d0:37:45:d9:68:76), Dst: Tp-LinkT_a7:f5:34 (68:ff:7b:a7:f5:34)
- Internet Protocol Version 4, Src: 192.168.0.104, Dst: 44.228.249.3
- Transmission Control Protocol, Src Port: 6634, Dst Port: 80, Seq: 1, Ack: 1, Len: 642
- Hypertext Transfer Protocol
- HTML Form URL Encoded: application/x-www-form-urlencoded
 - Form item: "username" = "USER"
 - Key: username
 - Value: USER
 - Form item: "password" = "USER"
 - Key: password
 - Value: USER

The bottom status bar shows 'HTML Form URL Encoded (urlencoded-form), 27 byte(s)' and 'Пакеты: 333 · Показаны: 1 (0.3%) · Потеряно: 0 (0.0%) | Профиль: Default'.

Apply display filter: `tcp.flags.syn==1`

No.	Time	Source	Destination	Protocol	Length	Info
151	6.938677	52.218.224.26	192.168.0.104	TCP	54	80 → 6642 [ACK] Seq=2 Ack=2 Win=251 Len=0
152	6.931859	52.218.224.26	192.168.0.104	TCP	54	80 → 6636 [ACK] Seq=2 Ack=2 Win=251 Len=0
153	6.931859	52.218.224.26	192.168.0.104	TCP	54	80 → 6656 [ACK] Seq=2 Ack=2 Win=251 Len=0
154	6.931859	52.92.195.177	192.168.0.104	TCP	54	80 → 6662 [ACK] Seq=2 Ack=2 Win=251 Len=0
155	6.937575	192.168.0.104	20.218.125.81	TCP	276	3554 → 1514 [PSH, ACK] Seq=1 Ack=1 Win=517 Len=222
156	7.007131	20.218.125.81	192.168.0.104	TCP	143	1514 → 3554 [PSH, ACK] Seq=1 Ack=223 Win=22018 Len=49
157	7.053842	192.168.0.104	20.218.125.81	TCP	54	3554 → 1514 [ACK] Seq=223 Ack=90 Win=517 Len=0
158	7.636531	192.168.0.104	8.8.4.4	UDP	102	53860 → 443 Len=60
159	7.636699	192.168.0.104	8.8.4.4	UDP	98	53860 → 443 Len=56
160	7.640966	192.168.0.104	44.228.249.3	HTTP	696	POST /login HTTP/1.1 (application/x-www-form-urlencoded)
161	7.697669	8.8.4.4	192.168.0.104	UDP	74	443 → 53860 Len=32
162	7.697669	8.8.4.4	192.168.0.104	UDP	74	443 → 53860 Len=32
163	7.702945	8.8.4.4	192.168.0.104	UDP	628	443 → 53860 Len=586
164	7.702945	8.8.4.4	192.168.0.104	UDP	68	443 → 53860 Len=26
165	7.703172	192.168.0.104	8.8.4.4	UDP	81	53860 → 443 Len=39
166	7.704139	192.168.0.104	142.251.140.74	QUIC	1292	Initial, DCID=9a4e2e4d0cfdb60b, PKT: 1, PING, PING, PING, PING, PING, CRYPTO, PING, PING, CRYPTO, PADDING, CRYPTO, PING, PADDING, PING, PADDING
167	7.711455	8.8.4.4	192.168.0.104	UDP	559	443 → 53860 Len=517
168	7.711455	8.8.4.4	192.168.0.104	UDP	68	443 → 53860 Len=26
169	7.711667	192.168.0.104	8.8.4.4	UDP	81	53860 → 443 Len=39
170	7.739680	192.168.0.104	8.8.4.4	UDP	75	53860 → 443 Len=33
171	7.708946	142.251.140.74	192.168.0.104	QUIC	1292	Initial, SCID=d4e2e4d0cfdb60b, PKT: 1, ACK, CRYPTO, PADDING
172	7.708946	8.8.4.4	192.168.0.104	UDP	68	443 → 53860 Len=26
173	7.808913	192.168.0.104	142.251.140.74	QUIC	1292	Initial, DCID=d4e2e4d0cfdb60b, PKT: 2, ACK, PADDING
174	7.803785	8.8.4.4	192.168.0.104	UDP	68	443 → 53860 Len=26
175	7.803965	192.168.0.104	8.8.4.4	UDP	76	53860 → 443 Len=34
176	7.814514	142.251.140.74	192.168.0.104	QUIC	1292	Handshake, SCID=d4e2e4d0cfdb60b
177	7.814514	142.251.140.74	192.168.0.104	QUIC	1292	Handshake, SCID=d4e2e4d0cfdb60b
178	7.814664	192.168.0.104	142.251.140.74	QUIC	83	Handshake, DCID=d4e2e4d0cfdb60b
179	7.837462	216.58.212.33	192.168.0.104	TCP	66	443 → 6617 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
180	7.894787	142.251.140.74	192.168.0.104	QUIC	1292	Handshake, SCID=d4e2e4d0cfdb60b
181	7.894787	142.251.140.74	192.168.0.104	QUIC	271	Protected Payload (KPB)
182	7.894746	44.228.249.3	192.168.0.104	TCP	60	80 → 6634 [ACK] Seq=1 Ack=643 Win=477 Len=0
183	7.894746	44.228.249.3	192.168.0.104	HTTP	561	HTTP/1.1 302 FOUND (text/html)
184	7.895390	192.168.0.104	142.251.140.74	QUIC	204	Protected Payload (KPB), DCID=d4e2e4d0cfdb60b

Frame 183: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bits) on interface \Device\NPF_{40493218-65EC-4AF0-8322-37A63E9035B0}, id 0
 Ethernet II, Src: Tp-LinkT_g7f5f34 (08:ff:7b:a7:f5f34), Dst: Tp-LinkT_d9f6876 (d0:37:45:d9:f6876)
 Internet Protocol Version 4, Src: 44.228.249.3, Dst: 192.168.0.104
 Transmission Control Protocol, Src Port: 80, Dst Port: 6634, Seq: 1, Ack: 643, Len: 507
 Hypertext Transfer Protocol
 HTTP/1.1 302 FOUND
 Server: nginx/1.19.0
 Date: Sun, 29 Jan 2023 22:47:28 GMT
 Content-Type: text/html; charset=utf-8
 Content-Length: 265
 Connection: keep-alive
 Location: http://testhtml5.vulnweb.com/
 Set-Cookie: username=USER; Path=/

`tcp.flags.syn==1` - DoS

`tcp.flags.ack==0` - DoS

Detecting SYN floods

- Look out for an immense number of TCP connection requests. The proper display filter is `tcp.flags.syn == 1` and `tcp.flags.ack == 0`
- The server, that is under attack, will respond with a smaller number of SYN/ACKs. These can be spotted with the display filter `tcp.flags.syn == 1` and `tcp.flags.ack == 1`
- Try to compare the number of SYNs with the number of SYN/ACKs. As long as the numbers are identical your firewall or server is holding up.
- Very often, the source addresses are spoofed. A good indicator of a spoofed source address is a packet with the RST bit set in response to the SYN/ACK from your server. The normal response would be a packet with just the ACK flag being set.