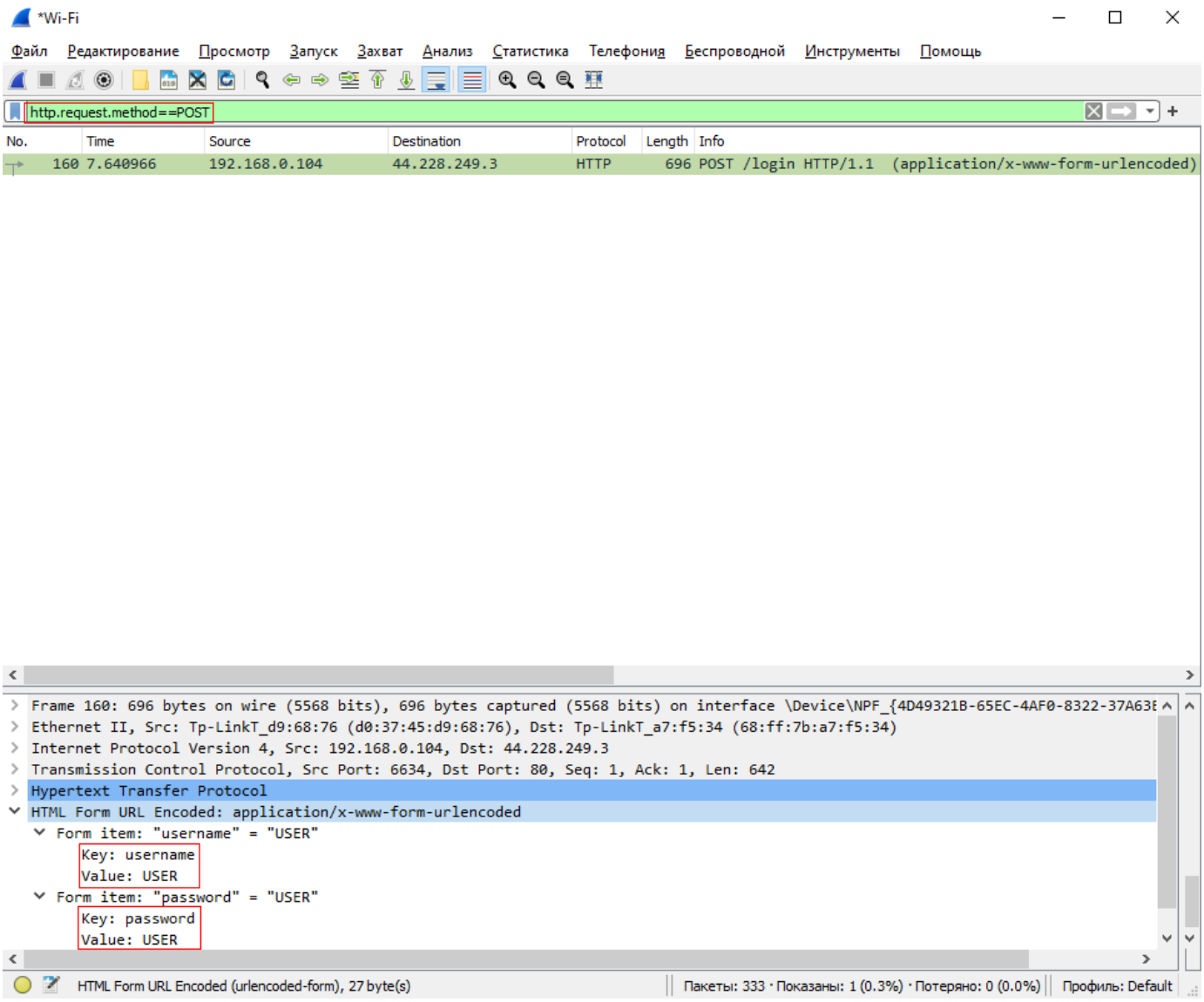
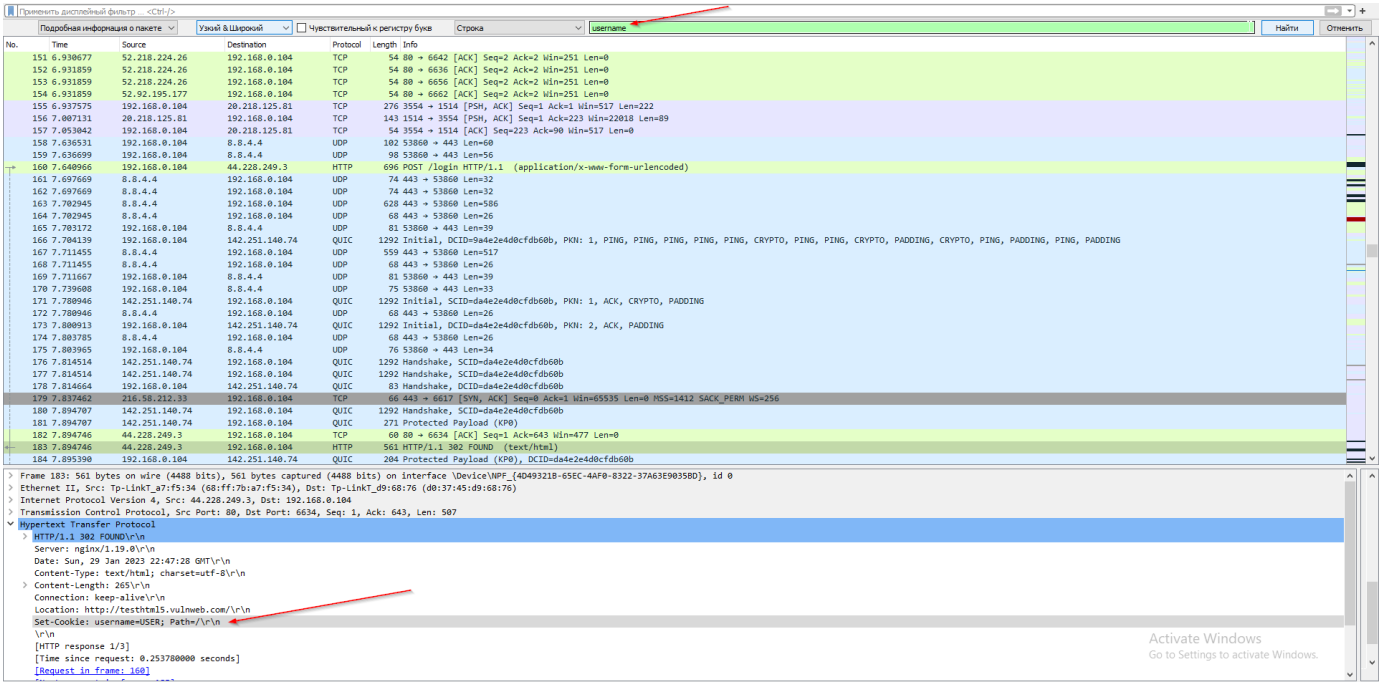
Wireshark

`ftp.request` - to view FTP traffic

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





`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.