a. Which browser is being used by the host with IP 10.0.0.69?

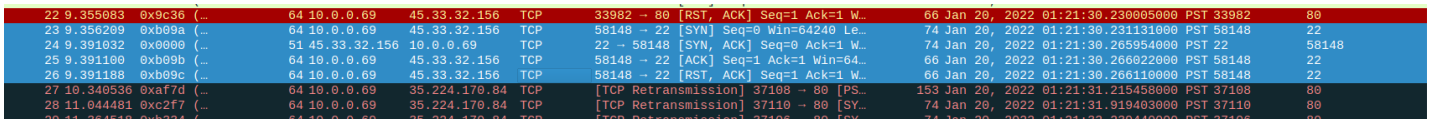
Used filter: `ip.addr==10.0.0.69 and http.user_agent`

The host is using Chrome with a Linux distribution, and seems to be on a Dell Inspiron based on the host name.

```
MX: 1\r\n
ST: urn:dial-multiscreen-org:service:dial:1\r\n
USER-AGENT: Google Chrome/97.0.4692.71 Linux\r\n
\r\n
```

```
Maximum DHCP Message Size: 65535
▾ Option: (12) Host Name
    Length: 20
    Host Name: cyborg-Inspiron-3668
▾ Option: (255) End
    Option End: 255
```

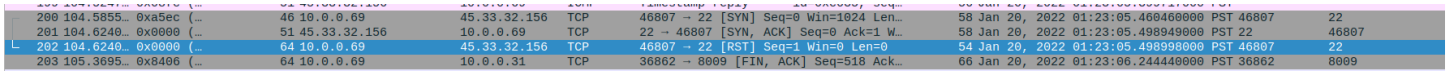
b. What can you infer about the packets exchanged between 10.0.0.69 and port 22 of 45.33.32.156 around timestamp 1:21:30?



22	9.355083	0x9c36	(…	64	10.0.0.69	45.33.32.156	TCP	33982 → 80 [RST, ACK] Seq=1 Ack=1 W…	66	Jan 20, 2022 01:21:30.230005000 PST	33982	80
23	9.356209	0xb09a	(…	64	10.0.0.69	45.33.32.156	TCP	58148 → 22 [SYN] Seq=0 Win=64240 Le…	74	Jan 20, 2022 01:21:30.231131000 PST	58148	22
24	9.391032	0x0000	(…	51	45.33.32.156	10.0.0.69	TCP	22 → 58148 [SYN, ACK] Seq=0 Ack=1 W…	74	Jan 20, 2022 01:21:30.265954000 PST	22	58148
25	9.391100	0xb09b	(…	64	10.0.0.69	45.33.32.156	TCP	58148 → 22 [ACK] Seq=1 Ack=1 Win=64…	66	Jan 20, 2022 01:21:30.266022000 PST	58148	22
26	9.391188	0xb09c	(…	64	10.0.0.69	45.33.32.156	TCP	58148 → 22 [RST, ACK] Seq=1 Ack=1 W…	66	Jan 20, 2022 01:21:30.266110000 PST	58148	22
27	10.340536	0xaf7d	(…	64	10.0.0.69	35.224.170.84	TCP	[TCP Retransmission] 37108 → 80 [PS…	153	Jan 20, 2022 01:21:31.215458000 PST	37108	80
28	11.044481	0xc2f7	(…	64	10.0.0.69	35.224.170.84	TCP	[TCP Retransmission] 37110 → 80 [SY…	74	Jan 20, 2022 01:21:31.919403000 PST	37110	80

From the looks of it in the *Info* column, the host at 10.0.0.69 initiates a tcp handshake via port 22 to the host at 45.33.32.156 by sending a [SYN] packet and then receives a [SYN,ACK] back from host 45.33.32.156. Then 10.0.0.69 sends another [ACK], and then ends and resets the tcp connection with [RST, ACK], ending the communication line.

c. What can you infer about the packets exchanged between the same hosts around timestamp 1:23:05? Characterize the differences between this and the previous question.



200	104.5855…	0xa5ec	(…	46	10.0.0.69	45.33.32.156	TCP	46807 → 22 [SYN] Seq=0 Win=1024 Len…	58	Jan 20, 2022 01:23:05.460460000 PST	46807	22
201	104.6240…	0x0000	(…	51	45.33.32.156	10.0.0.69	TCP	22 → 46807 [SYN, ACK] Seq=0 Ack=1 W…	58	Jan 20, 2022 01:23:05.498949000 PST	22	46807
202	104.6240…	0x0000	(…	64	10.0.0.69	45.33.32.156	TCP	46807 → 22 [RST] Seq=1 Win=0 Len=0	54	Jan 20, 2022 01:23:05.498998000 PST	46807	22
203	105.3695…	0x8406	(…	64	10.0.0.69	10.0.0.31	TCP	36862 → 8009 [FIN, ACK] Seq=518 Ack…	66	Jan 20, 2022 01:23:06.244440000 PST	36862	8009

Similar to the previous quiestion, but it looks like the sender, host 10.0.0.69 trys to make a tcp connection with host 45.33.32.156, but this time it seems like host 10.0.0.69 ends the communications without sending an [ACK] to the previous [SYN,ACK] and just straight up terminates the connection with a [RST].

d. I accidentally sent my password over http! Can you take advantage and compromise my account? What is my password?

Filter entries by HTTP, then look for the POST request with the plain text user name and password below: