

## 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: 000000
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.

280	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
281	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
282	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
283	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 question, but it looks like the sender, host 10.0.0.69 tries 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:

http

No.	Time	Identifier	Time to live	Source	Destination	Protocol	Info	Length	Arrival Time	Source Port	Destination Port
5	1.098787	0xaf77	(...)	64 10.0.0.69	35.224.170.84	HTTP	GET / HTTP/1.1	153	Jan 20, 2022 01:21:21.973709000	PST 37108	80
10	2.404568	0x565f	(...)	64 10.0.0.69	35.224.170.84	HTTP	GET / HTTP/1.1	153	Jan 20, 2022 01:21:23.279490000	PST 37102	80
40	48.071049	0x3d0f	(...)	64 10.0.0.69	128.59.105.24	HTTP	POST /~fdc/sample.html HTTP/1.1 (a...	248	Jan 20, 2022 01:22:09.540571000	PST 33442	80
48	52.380707	0x1a5a	(...)	234 128.59.105.24	10.0.0.69	HTTP	HTTP/1.1 301 Moved Permanently (te...	676	Jan 20, 2022 01:22:13.255709000	PST 80	33442
50	52.380872	0x21a5	(...)	234 128.59.105.24	10.0.0.69	HTTP	[TCP Spurious Retransmission] HTTP/...	676	Jan 20, 2022 01:22:13.255709000	PST 80	33442
52	52.380896	0x390a	(...)	234 128.59.105.24	10.0.0.69	HTTP	[TCP Spurious Retransmission] HTTP/...	676	Jan 20, 2022 01:22:13.255818000	PST 80	33442
70	61.435080	0xfb00	(...)	64 10.0.0.69	10.0.0.31	HTTP	GET /upnp/dev/8cf7c4fc-4206-3ec3-8e...	331	Jan 20, 2022 01:22:22.310002000	PST 38122	60000
95	60.040881	0x5b00	(...)	64 10.0.0.69	108.61.241.100	HTTP	GET /ad_abc2dc1c821d-1467021d-18h...	205	Jan 20, 2022 01:22:30.915602000	PST 45500	80

[response in frame. 40]

File Data: 20 bytes

HTML Form URL Encoded: application/x-www-form-urlencoded

Form item: "user" = "hari"

Form item: "pass" = "ssh!"

Text item (text), 10 bytes