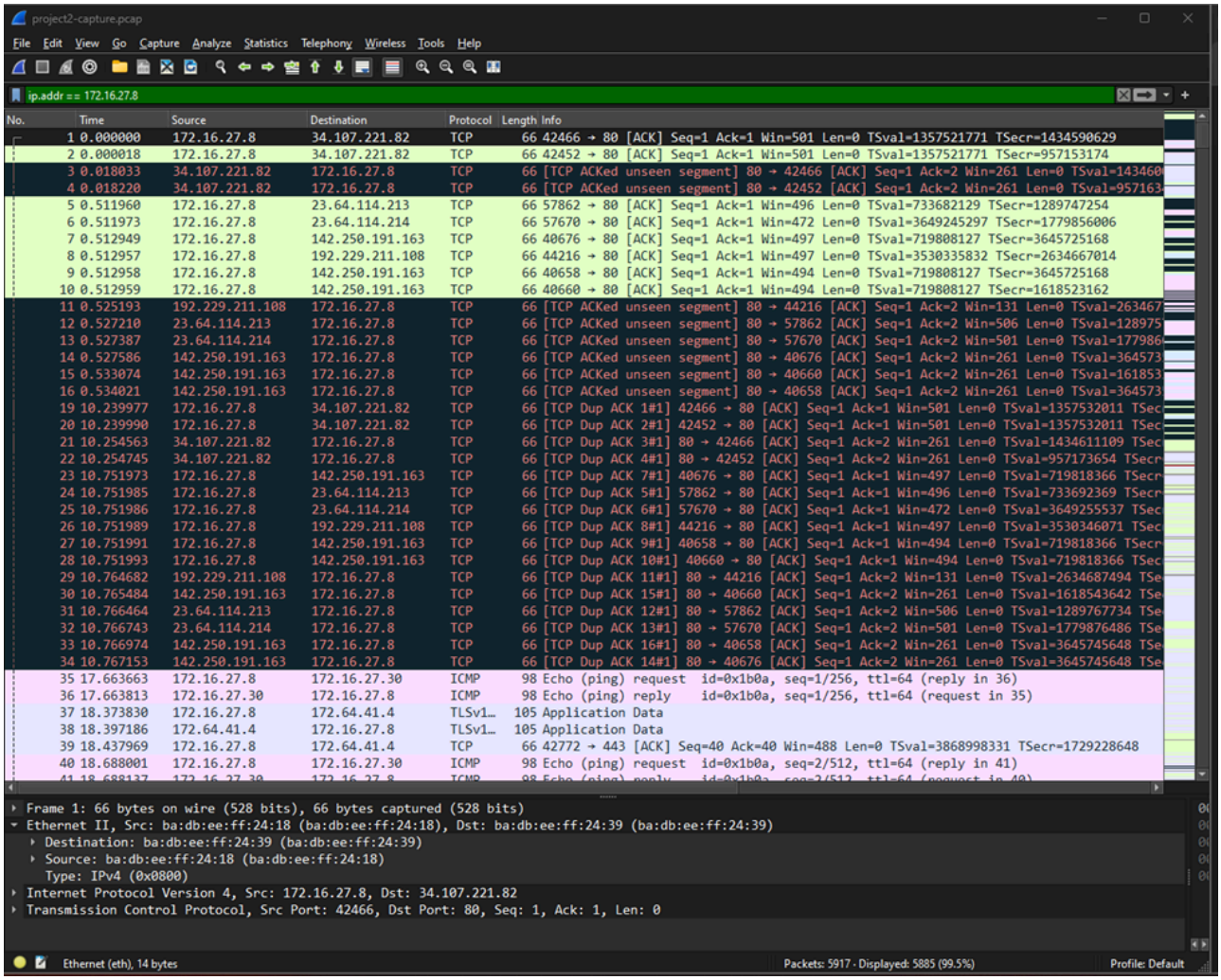
Project -2

Preparing people to lead extraordinary lives

OBAID RAZA ID: 1677274

1. What is the MAC address of the device being watched? (hex in colon-separated format)



Filter Used: ip.addr == 172.16.27.8

- **ba:db:ee:ff:24:18**

Packet Selection:

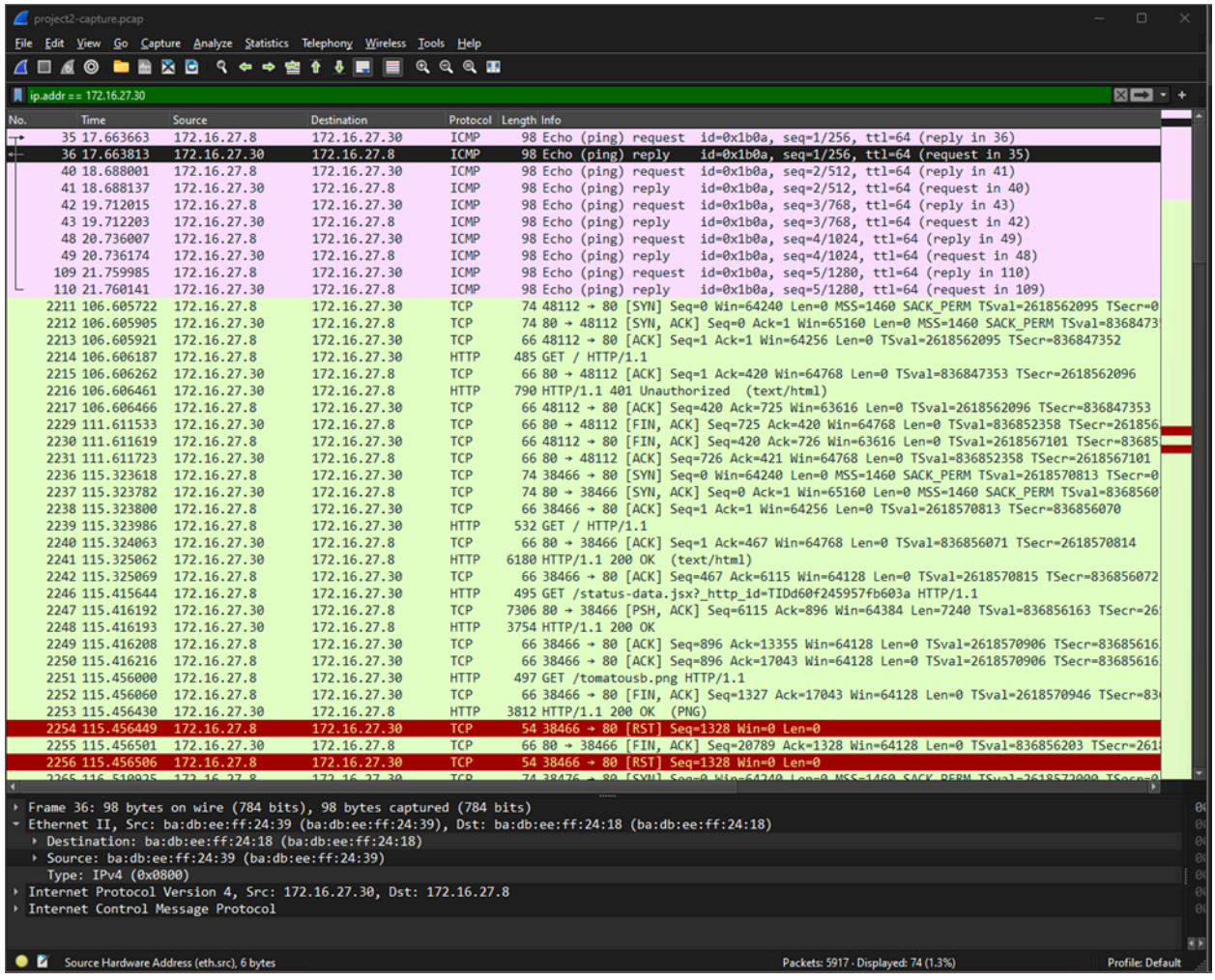
- The first packet involving the device (**172.16.27.8) is Frame 1.**
- This packet contains both the Source MAC Address and Destination MAC Address fields.

Interpretation:

- In Frame 1, under the Ethernet II header, the Source MAC Address is listed as **ba:db:ee:ff:24:18.**
- This MAC address (ba:db:ee:ff:24:18) represents the device being monitored, as it is consistently the source or destination MAC in subsequent frames related to **172.16.27.8.**

Conclusion: Based on the captured data, the MAC address of the device being watched is ba:db:ee:ff:24:18, confirmed by its role as the Source MAC Address in Frame

2. What is the MAC address of the gateway device? (hex in colon-separated format)



Answer for Gateway MAC Address:

- **Gateway Device MAC Address: ba:db:ee:ff:24:39**

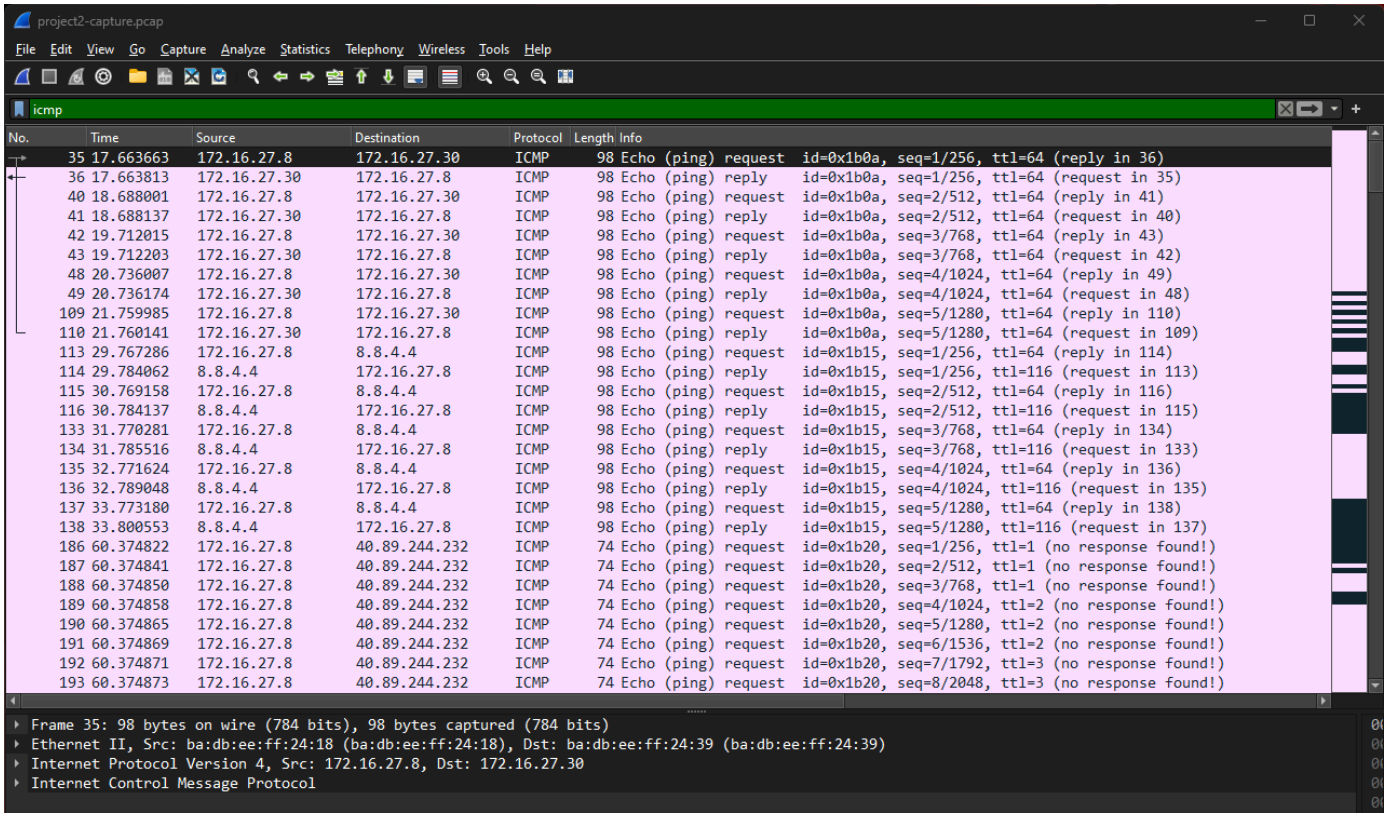
1. **Filter Used: ip.addr == 172.16.27.8**

Packet Selection:

- **In Frame 36**, we observe an ICMP (ping) reply with Source MAC Address **ba:db:ee:ff:24:39** and Destination MAC Address **ba:db:ee:ff:24:18.**
- This source MAC address **ba:db:ee:ff:24:39** is identified as the gateway since it responds to a request from the monitored device **172.16.27.8.**

2. **Interpretation:**
   - Since ba:db:ee:ff:24:39 is the source MAC address in the response to a ping request from 172.16.27.8, it indicates that this address belongs to the gateway, which is responding to the device's requests.
3. **Conclusion:**
   - The MAC address ba:db:ee:ff:24:39 is confirmed to be the gateway device, as seen in the ICMP reply packet in Frame 36.

3. What was the IP of the first device that was pinged (ICMP Echo Request)?

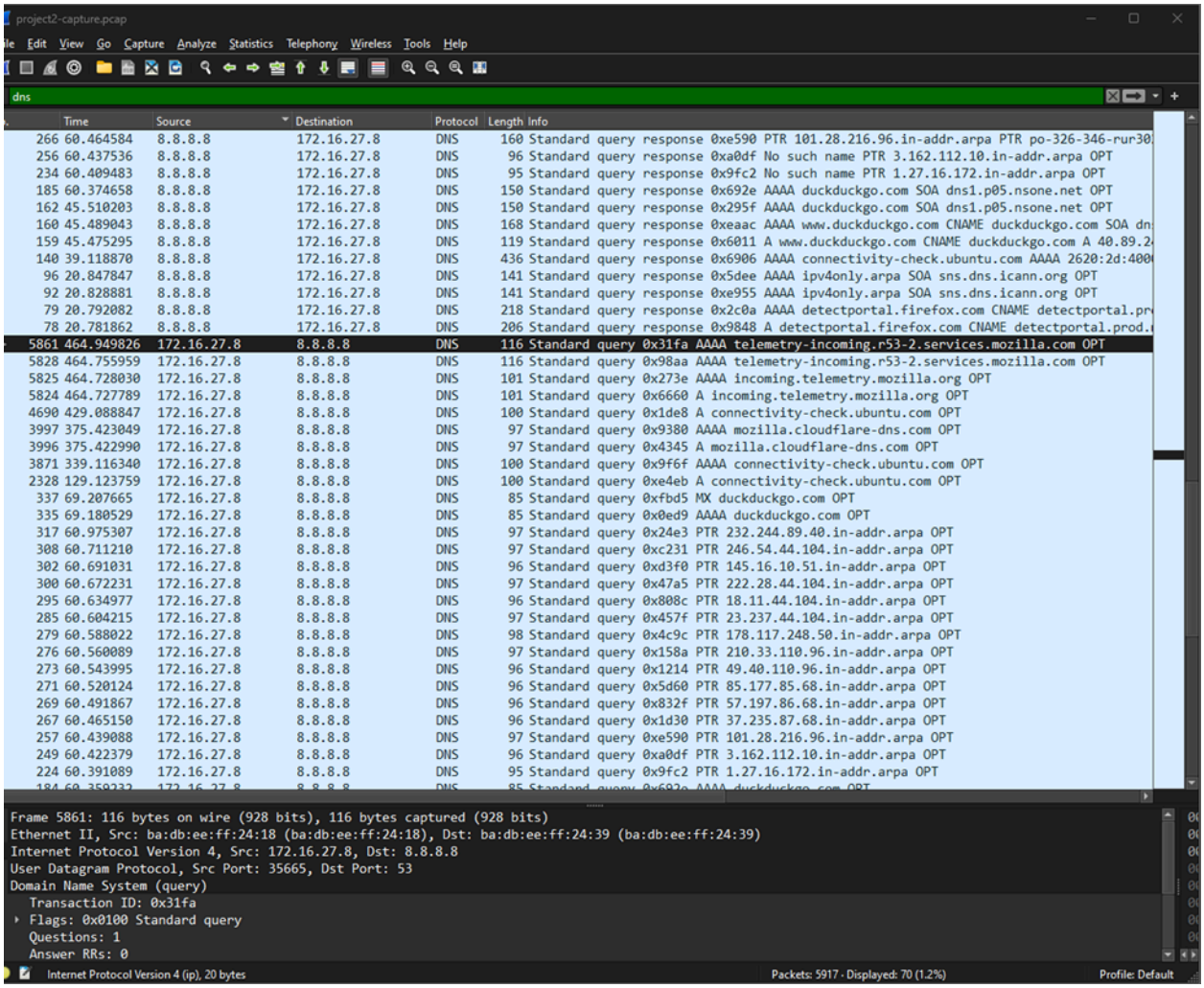


Answer:

- **First Device Pinged IP Address:172.16.27.30**

1. **Filter Used:** icmp
2. **Packet Selection: 35**
3. **Interpretation:**
    - Since this is the first ICMP Echo Request in the capture, the destination IP 40.89.244.232 is identified as the first device pinged by the monitored device.
4. **Conclusion:**
    - **The IP address of the first device that was pinged (ICMP Echo Request) by 172.16.27.30, confirmed by examining packet 35 and filter ICMP.**

4. What DNS server(s) is/are being used to resolve names to IPs?



Filter Used: dns

Answer: The monitored device is using Google's DNS server 8.8.8.8

5 SOA records:

- sns.dns.icann.org
- dns1.p05.nsone.net
- dns101.comcast.net
- ns1-06.azure-dns.com
- ns1-06.azure-dns.com

Packet Inspection:

- In Frame 5861, a DNS Standard Query is sent from the monitored device 172.16.27.8 to 8.8.8.8 with a request for telemetry-incoming.r53-2.services.mozilla.com.
- Observing other DNS query packets, we consistently see that the DNS server IP 8.8.8.8 is used as the destination for these queries.

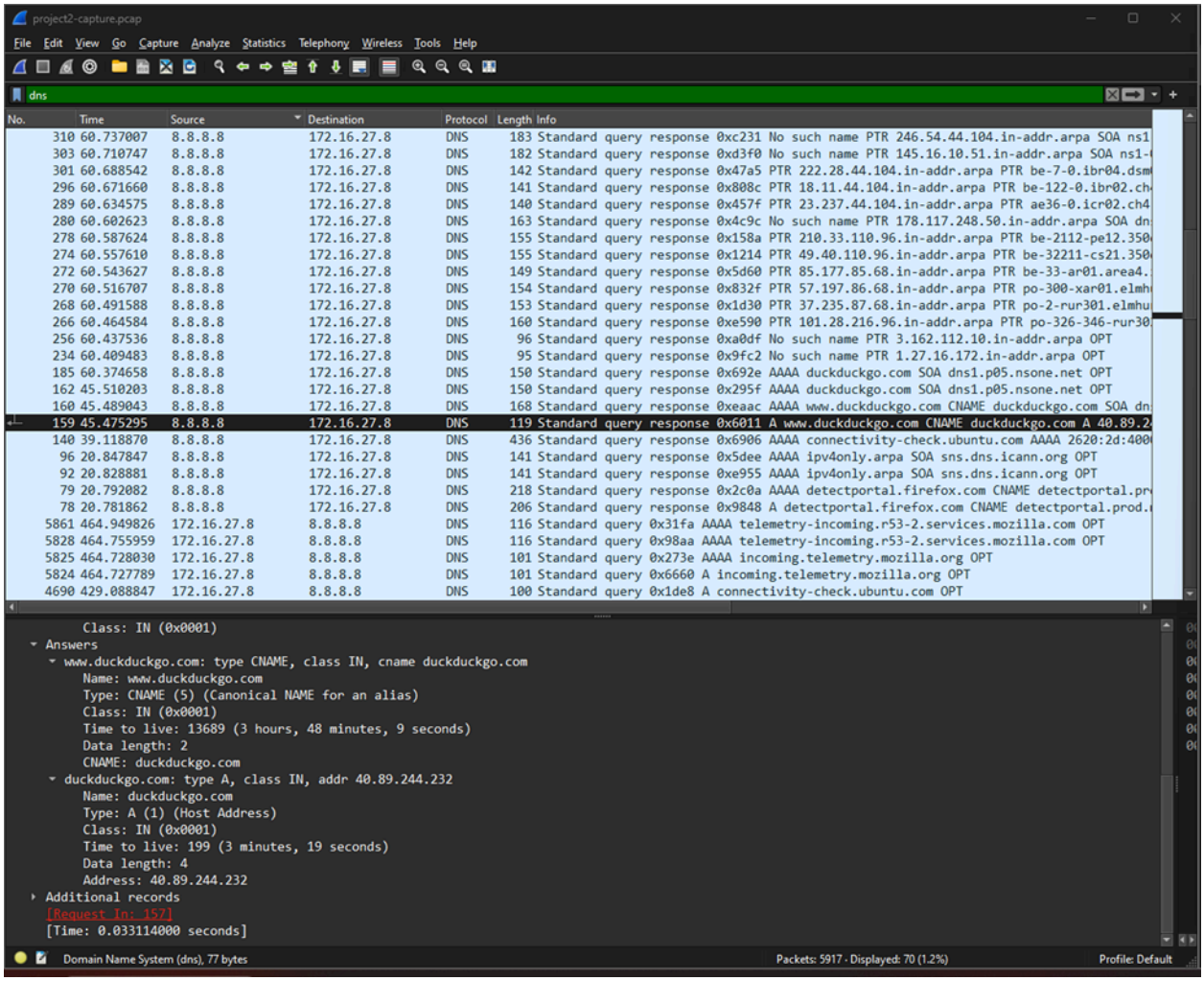
Interpretation:

- The repeated appearance of 8.8.8.8 as the destination IP for DNS queries indicates that this is the primary DNS server used by the monitored device for name resolution.

Conclusion:

- **The monitored device is using Google's DNS server 8.8.8.8 to resolve domain names to IP addresses, as evidenced by the destination address in DNS query packets, such as in Frame 5861.**

5. According to DNS in the capture, what IPv4 address hosts the duckduckgo.com website (A record)?



Answer:

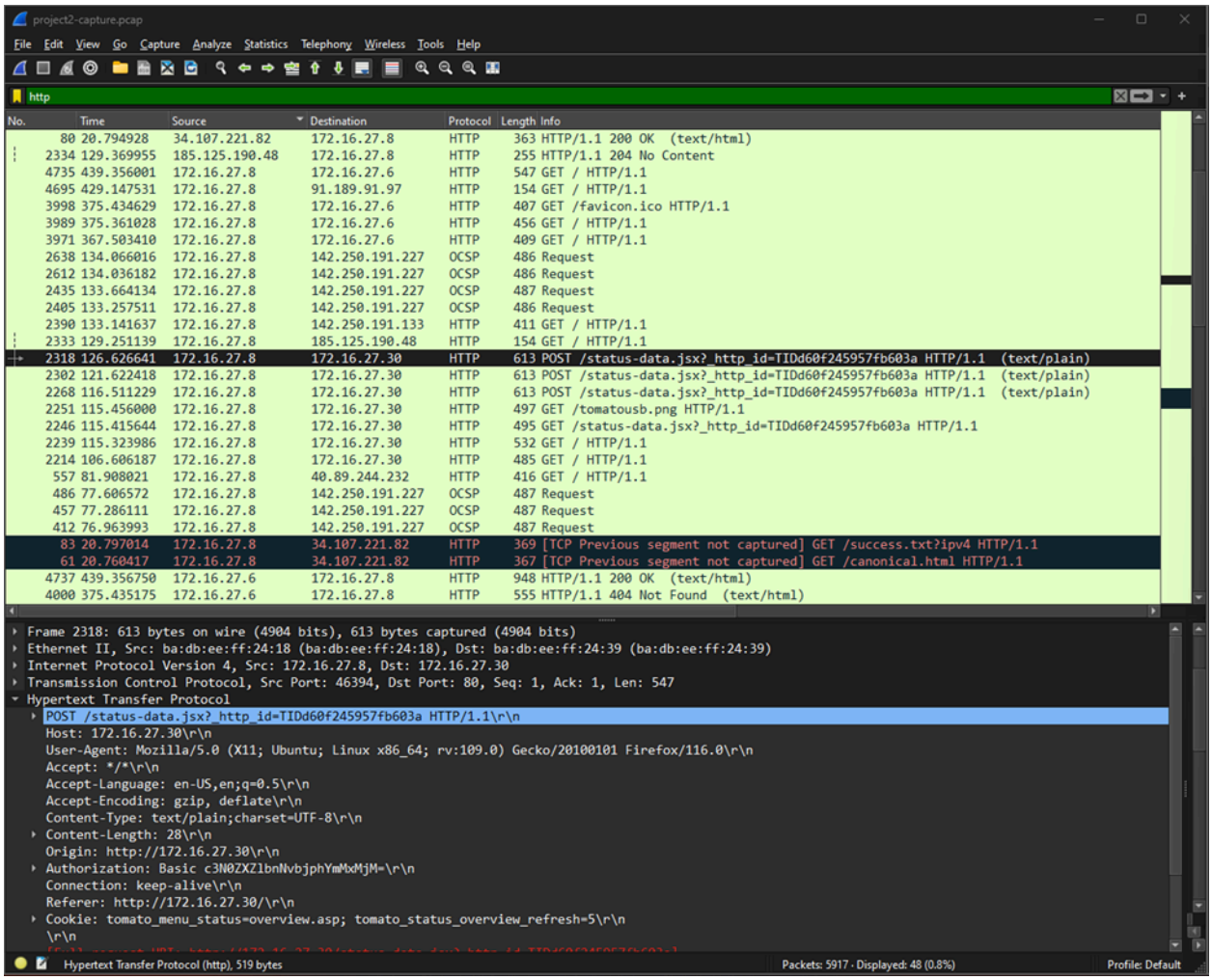
- IPv4 Address for **duckduckgo.com: 40.89.244.232**

1. **Filter Used: dns**
2. **Packet Inspection:**In Frame 159, a DNS response for the query www.duckduckgo.com contains two answers:
    - The first answer provides a CNAME (Canonical Name) record, indicating that www.duckduckgo.com is an alias for duckduckgo.com.
    - The second answer provides an A (Address) record for duckduckgo.com, giving the IPv4 address as 40.89.244.232.
3. **Interpretation:**

- Since the DNS response includes the A record for duckduckgo.com, we can conclude that 40.89.244.232 is the IP address hosting duckduckgo.com.

4. **Conclusion:**
   - The IPv4 address **40.89.244.232** is confirmed as the host IP for duckduckgo.com, as shown in Frame 159 of the DNS response.

6. What account was used to log into the router device via HTTP? (username and password)



Answer:

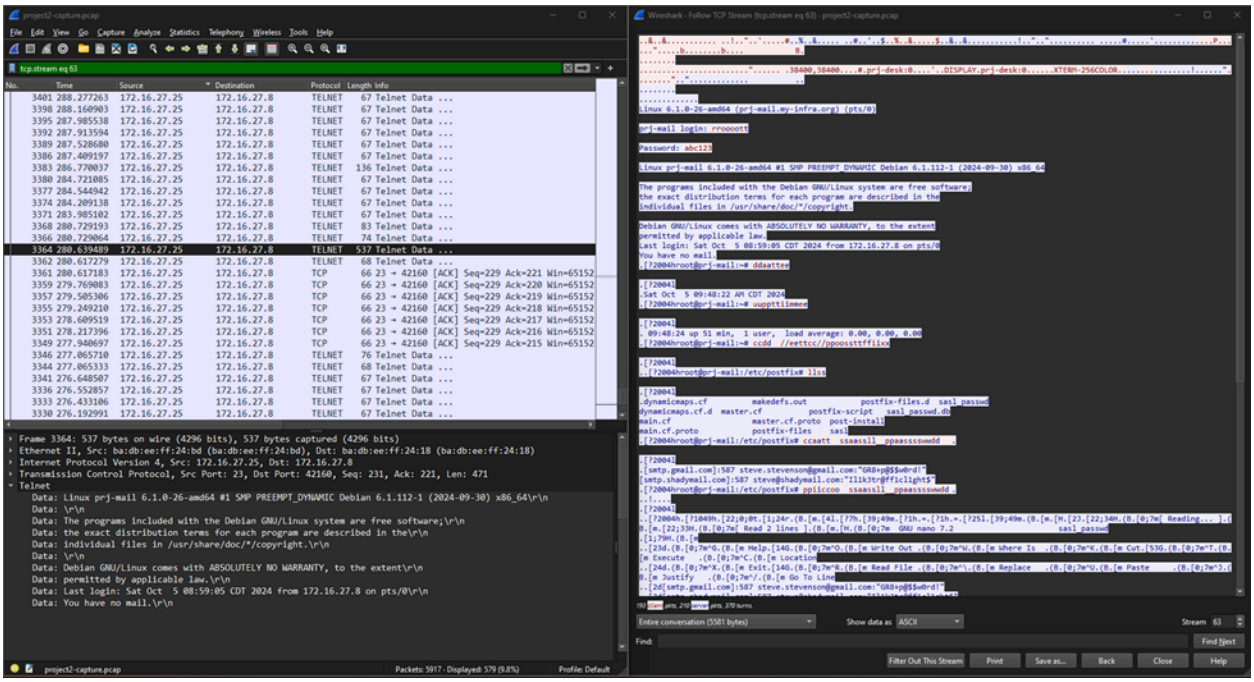
- **Username: sstevenson**
- **Password: abc123**

Packet Number: Frame 2302

Filter Used: http && ip.addr == 172.16.27.30

Explanation: In Frame 2302, the Authorization header is valid with credentials in the Basic Authorization format. The decoded string for the encoded c3N0ZXZlbnNvbjphYmMxMjM= is sstevenson:abc123. This will provide the credentials used to log into the router. It is sent in a POST to http://172.16.27.30/status-data.jsx.

7. What account was used to log into the local mail server via TELNET? (username and password)



Answer:

- Username: root
- Password: abc123

1. **Filter Used: telnet && ip.addr == 172.16.27.25**
2. **Packet Inspection:**
    - In **Frame 3364** within the TELNET session (stream 63), we can observe the login attempt.
    - The session data includes a prompt for login: where the username root is entered.
    - Shortly afterward, we see Password: followed by the password entry abc123.
3. **Interpretation:**
    - The root user logs in with the password abc123, as shown clearly in the TELNET session data.
4. **Conclusion:**
    - Username: root
    - Password: abc123

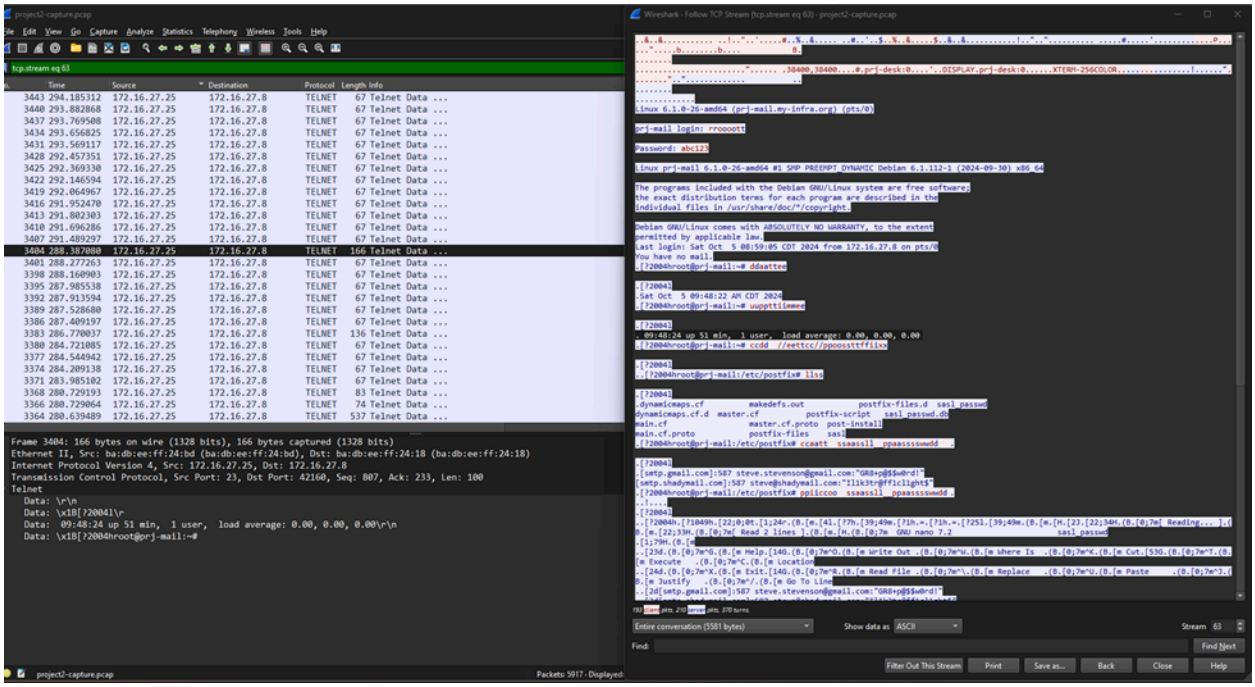
8. At the time of the capture, how long had the local mail server been up (uptime found in TELNET)?

Answer:

- Uptime: 51 minutes

1. **Filter Used: telnet && ip.addr == 172.16.27.25**
2. **Packet Inspection:**
    - In Frame 3364 within the TELNET stream (stream 63), we observe the user executing the uptime command.

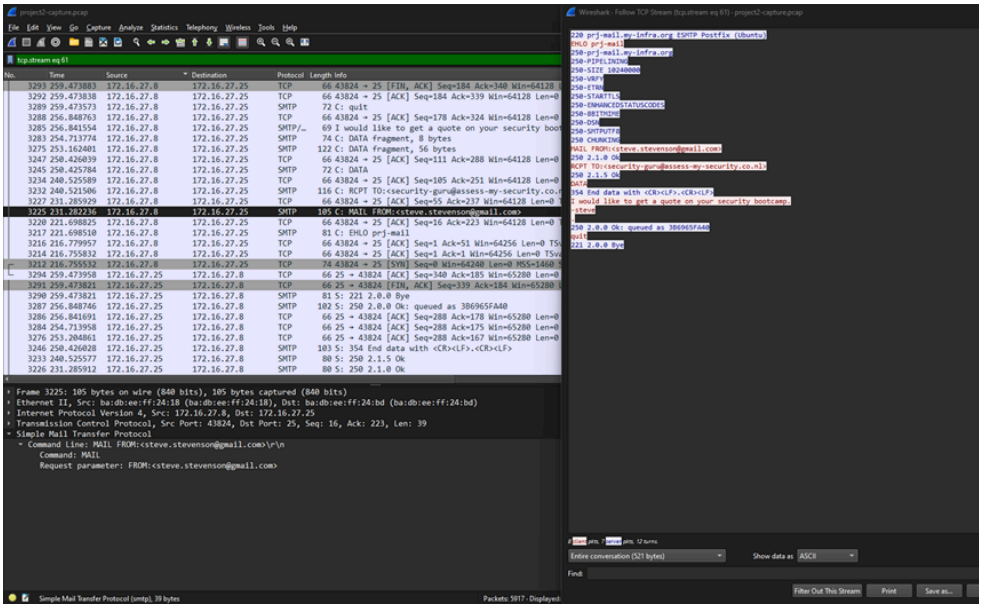
- The output in this frame indicates up 51 min, which reflects how long the server had been running at the time of capture.



9. Who did the target send e-mail as and to during the interaction via SMTP and what was the content of the message? (provide the from and to email addresses)
Answer:

- From: steve.stevenson@gmail.com
- To: security-guru@assess-my-security.co.nl
- Message Content: "I would like to get a quote on your security bootcamp. -steve"

1. **Filter Used:** smtp && ip.addr == 172.16.27.25
2. **Packet Inspection:**
    - In Frame 3299 and subsequent frames within the SMTP session (stream 61), the email transaction is visible:
        - The MAIL FROM command indicates the sender: steve.stevenson@gmail.com.
        - The RCPT TO command reveals the recipient: security-guru@assess-my-security.co.nl.
    - The DATA section of the SMTP conversation shows the message content: **I would like to get a quote on your security bootcamp. -steve**



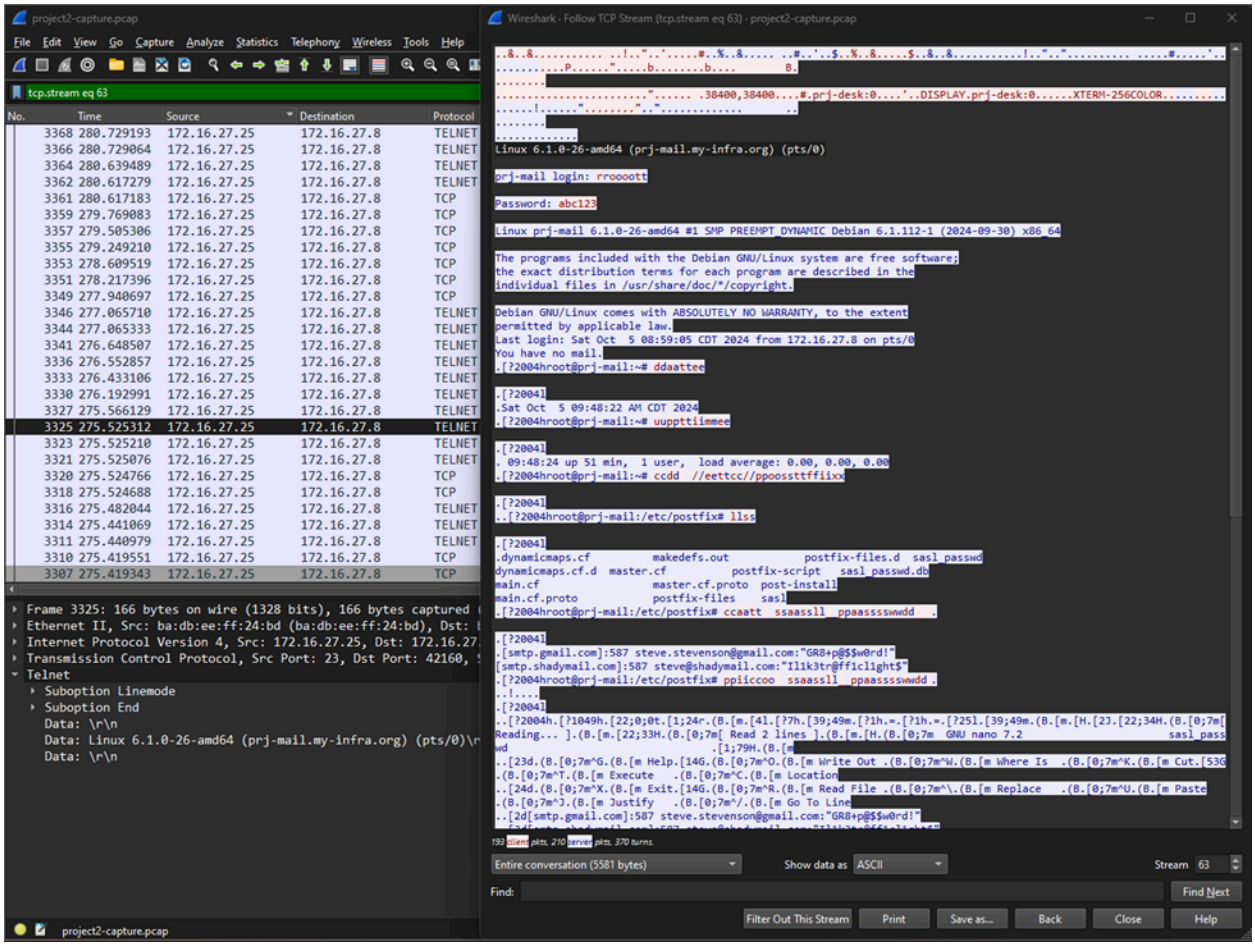
10. What version of the Linux kernel is the local mail server running, which can be found via TELNET interactions? (it is of the format "Linux 6.x.y-z-amd64"

Answer:

- **Linux Kernel Version: Linux 6.1.0-26-amd64**

1. **Filter Used: telnet && ip.addr == 172.16.27.25**
2. **Packet Inspection:**
    - In Frame 3325, the TELNET session output displays system information after login.
- The Linux kernel version is indicated in the line:
  Linux 6.1.0-26-amd64 (prj-mail.my-infra.org) (pts/0)

3. **Interpretation:**
    - This line in the TELNET session provides the exact kernel version 6.1.0-26-amd64.



11. According to the HTTP2 GET requests, embedded in the HEADERS, what was the first, complete search request sent by the user, via www.duckduckgo.com (they require the use of the ssl keys provided)?

Frame Number: 1464 and 1471

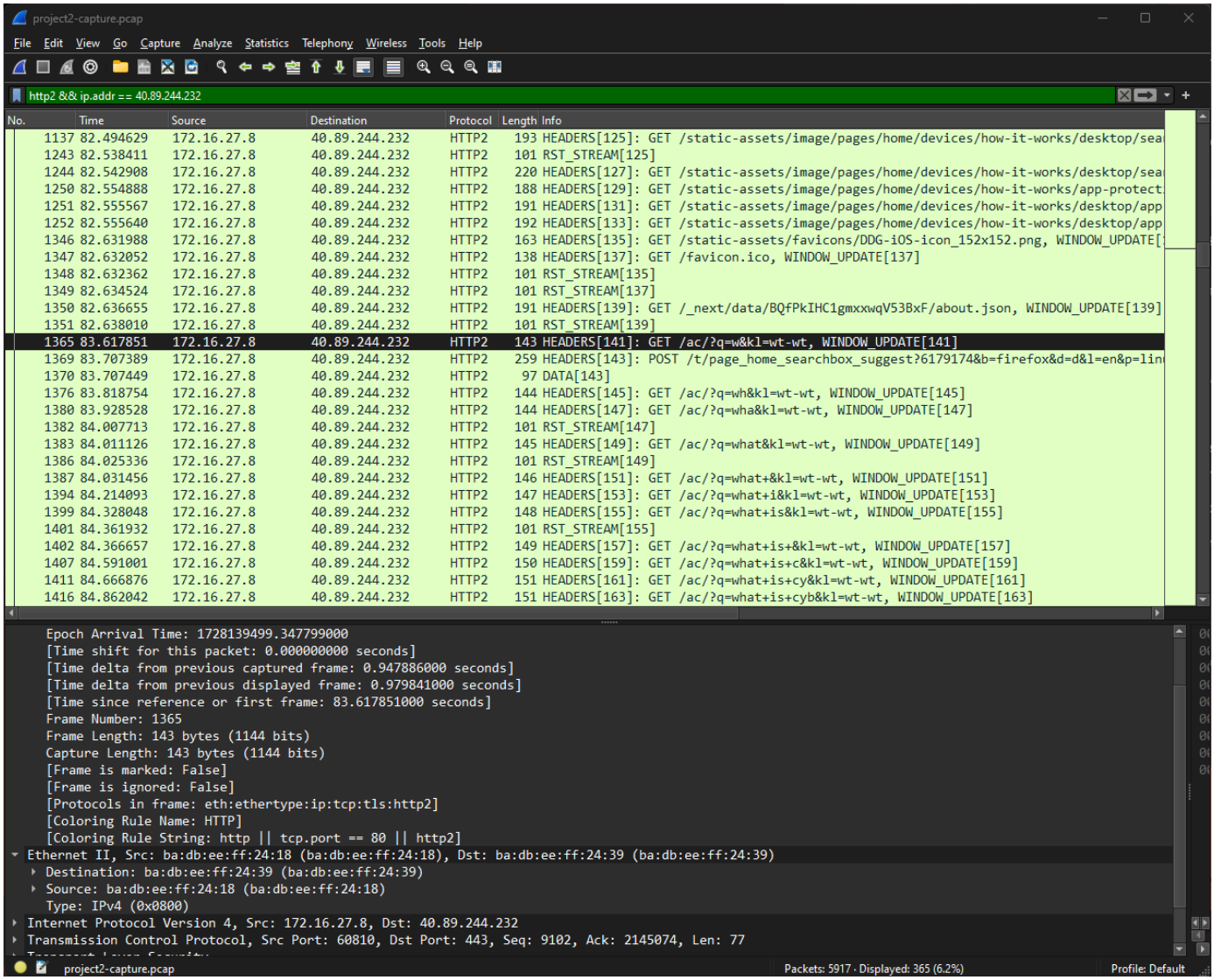
Filter Applied: http2 && ip.addr == 40.89.244.232

Search Query: q=what is cyber security

Interpretation: The HTTP2 GET request in Frame 1365 includes the search query parameter q=w in the path /ac/?q=what is cyber security &kl=wt-wt, identifying it as the first search request sent by the user to DuckDuckGo. The packet captures the full details of the request, including HTTP2 headers that specify :method: GET and :authority: duckduckgo.com. This frame is the earliest in the capture with a complete search query.

Answer:

- First Complete Search Request: q=what is cyber security
- Found in Frame: 1464 and 1471



12. According to the HTTP2 GET requests, embedded in the HEADERS what was the last, complete search request sent by the user, via www.duckduckgo.com (they require the use of the ssl keys provided)?

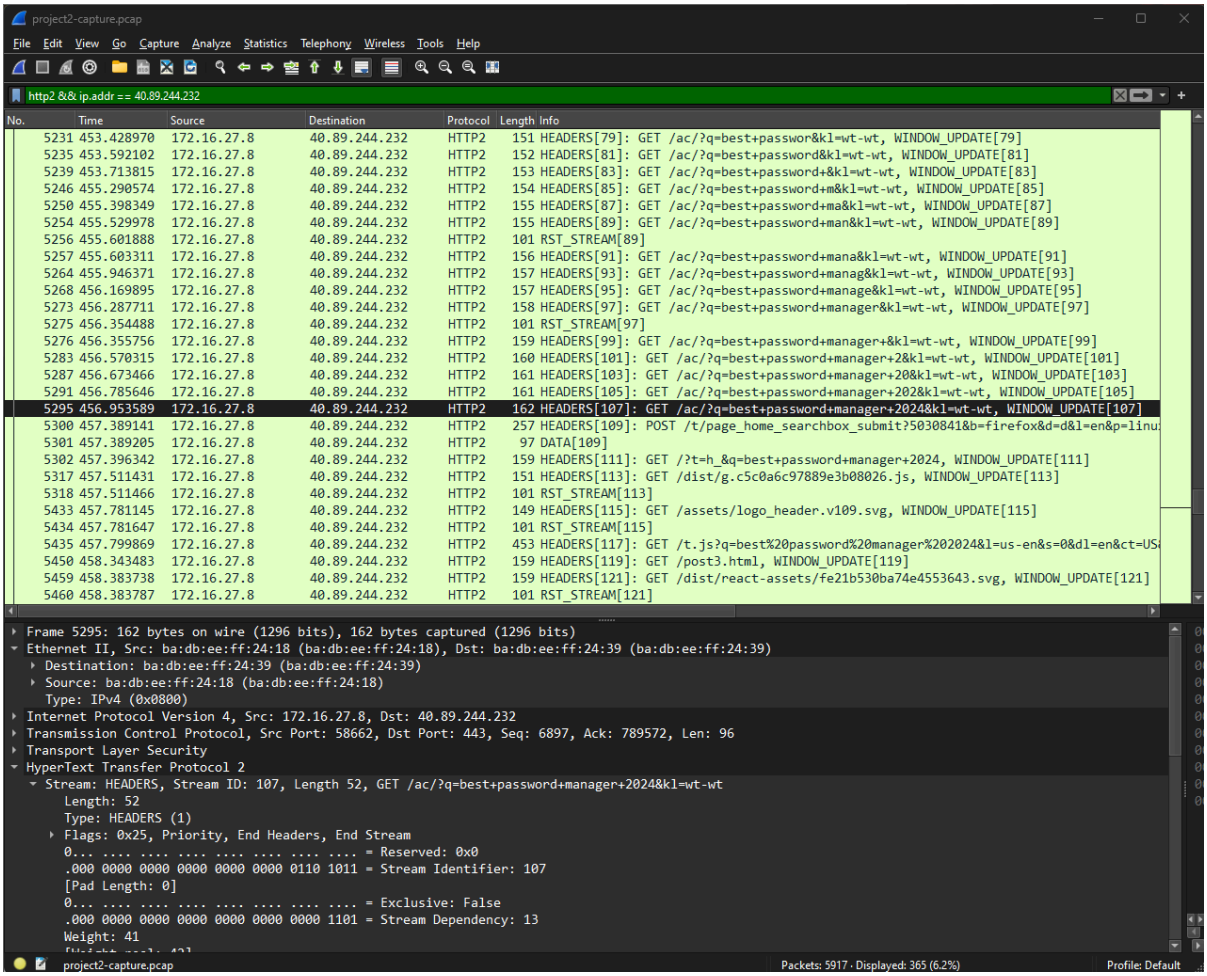
Answer:

- **Last Complete Search Request:** q=best+password+manager+2024
- Found in Frame: **5295 & 5300**
- **Filter Used: http2 && ip.addr == 40.89.244.232**

Explanation: To identify the last complete search request made by the user on DuckDuckGo, I applied the filter http2 && ip.addr == 40.89.244.232 to isolate HTTP2 traffic directed to DuckDuckGo's IP address.

Packet Inspection: In Frame 5295, the HTTP2 GET request displays the following :path header: /ac/?q=best+password+manager+2024&kl=wt-wt

- This path indicates that the search query was for "best password manager 2024".

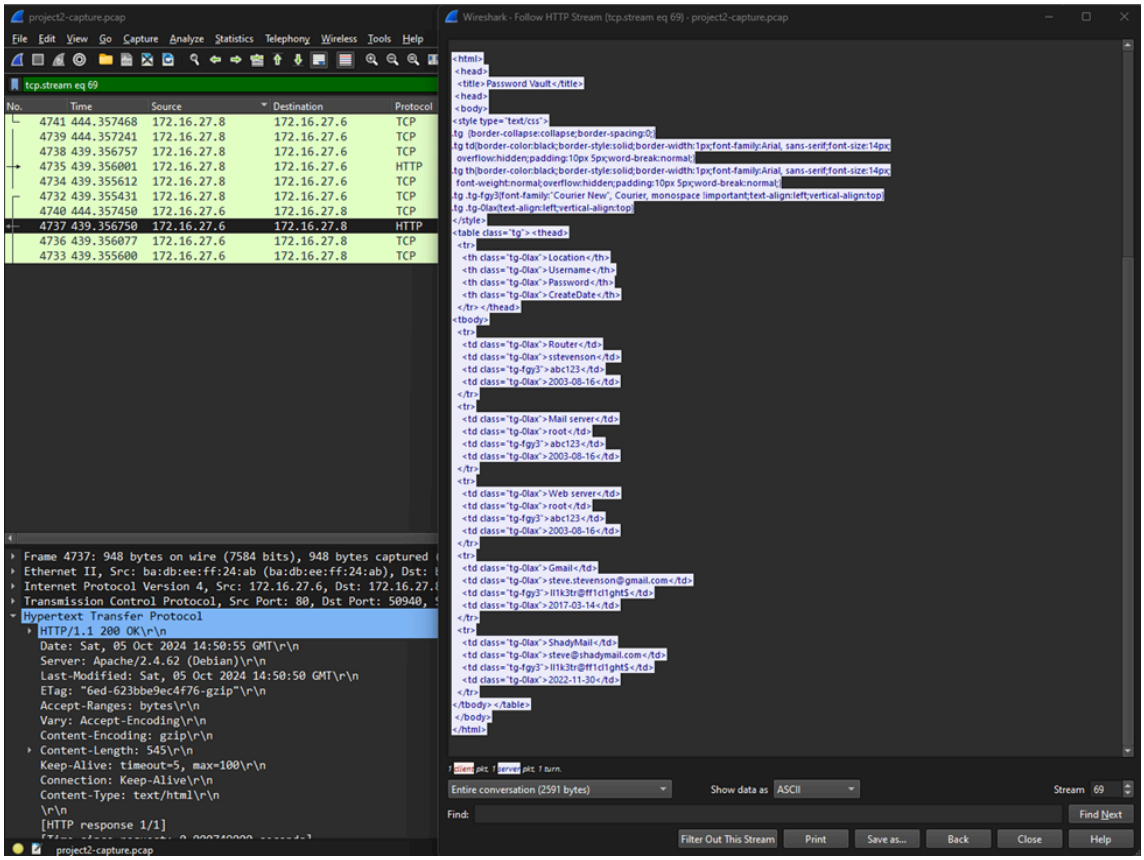


13. What information was provided on the webpage loaded from the local web server?

The data was found in **Frame 4737,** as shown in the HTTP response from the web server at Port 50940. The response was captured in **http && ip.addr == 172.16.27.6**

The webpage titled "Password Vault" on the local web server displayed sensitive information in a table format. It included:

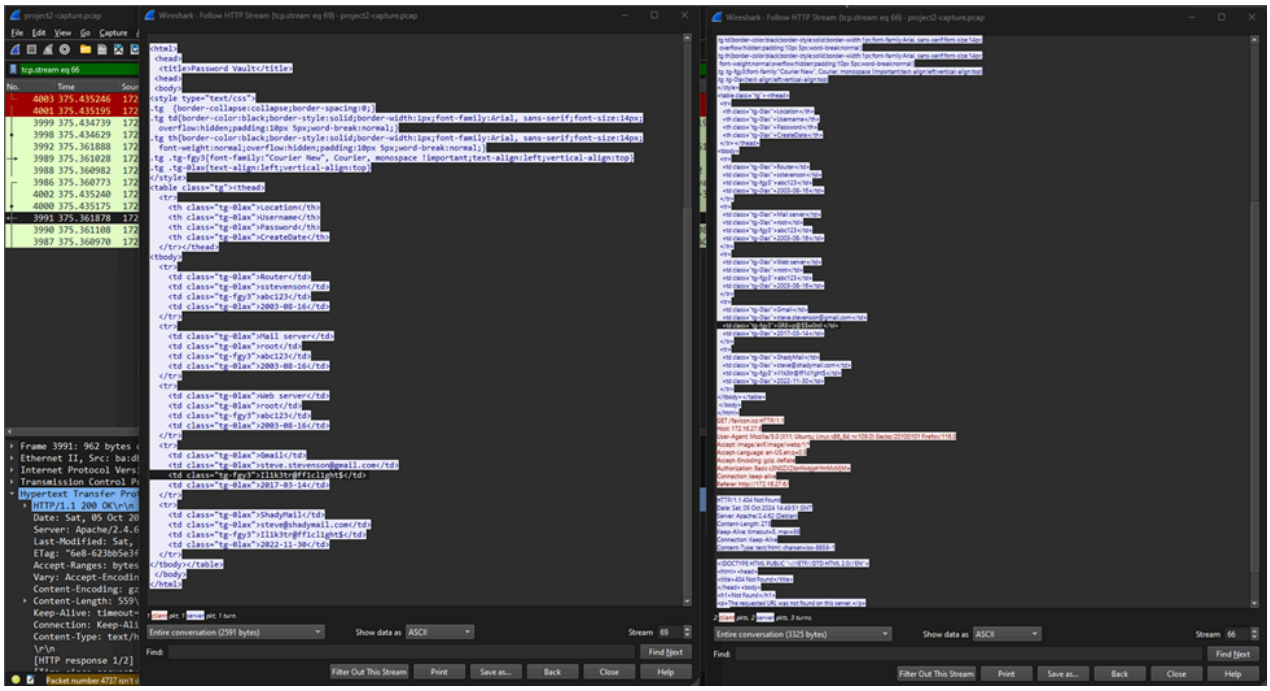
Location , Username , Password, CreateDate

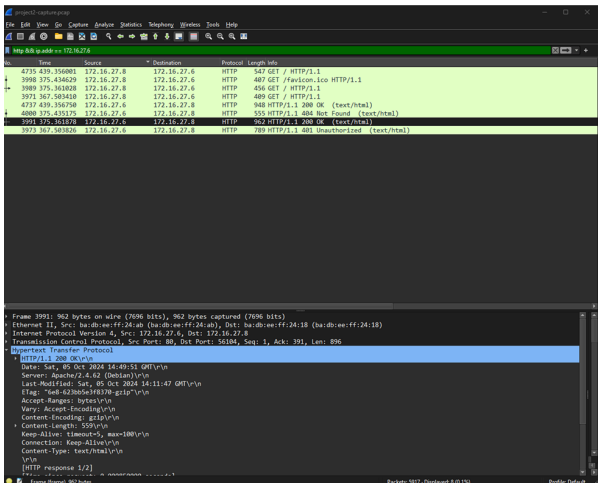


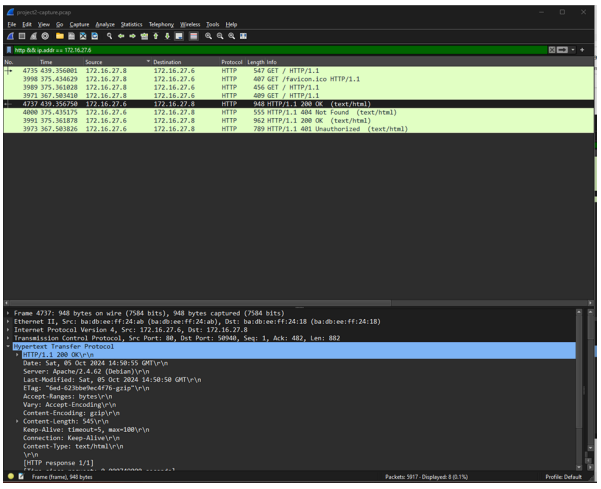
Details from the Table:

- Router
    - Username: sstevenson
    - Password: abc123
    - CreateDate: 2003-08-16
- Mail server
    - Username: root
    - Password: abc123
    - CreateDate: 2003-08-16
- Web server
    - Username: root
    - Password: abc123
    - CreateDate: 2003-08-16
- Gmail
    - Username: steve.stevenson@gmail.com
    - Password: Il1k3tr@ff1cl1ght$
    - CreateDate: 2017-03-14
- ShadyMail
    - Username: steve@shadymail.com
    - Password: Il1k3tr@ff1cl1ght$
    - CreateDate: 2022-11-30

14. What record on the local web server was changed (two requests for the same page … you will need to compare)?







The "Password Vault" webpage on the local web server showed a modification between two requests, specifically in the Gmail entry's password.

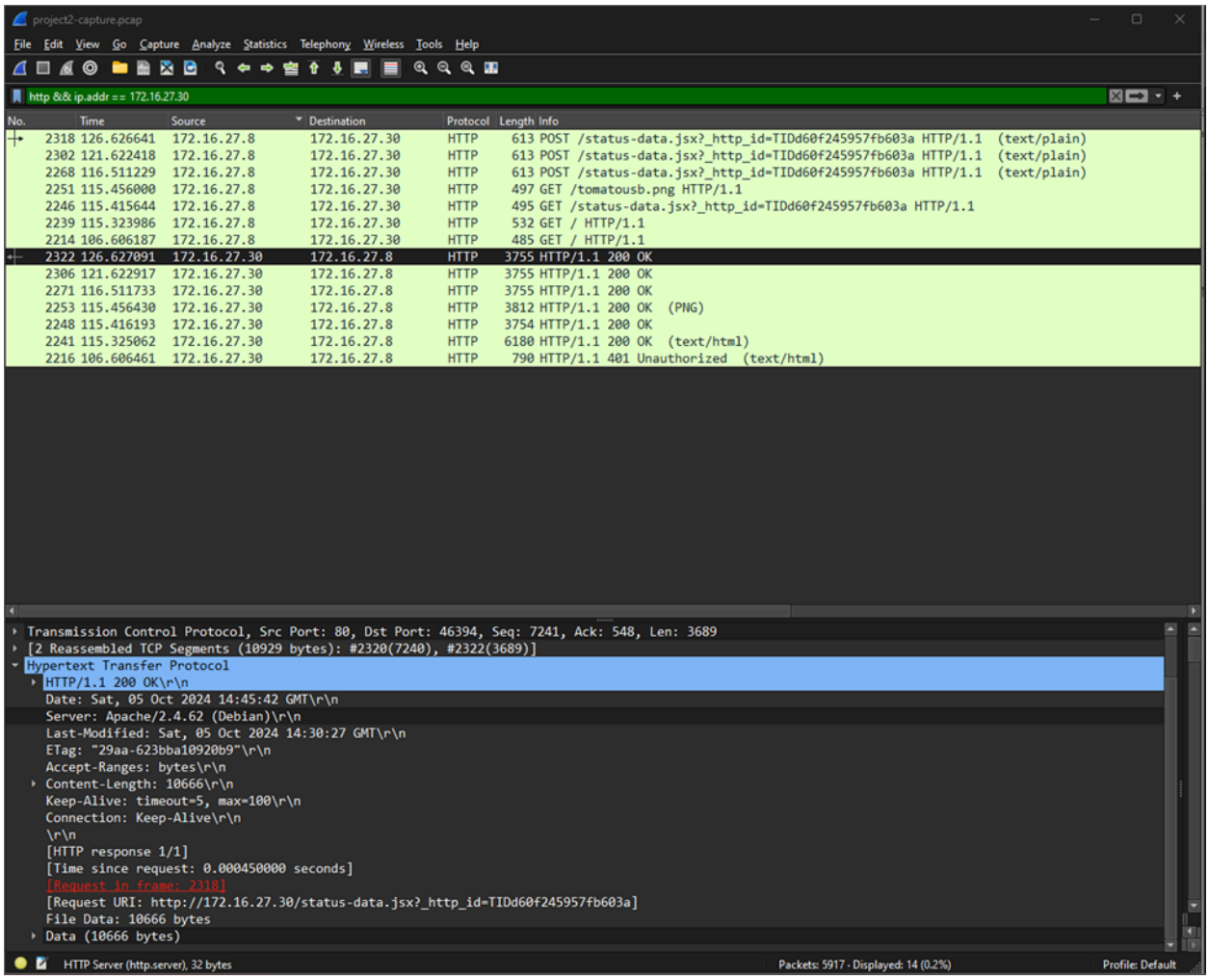
1. **Gmail Password Update:**
    - First Request: The password for Gmail was "GR8+p@$$w0rd!".
    - Second Request: The password was updated to "Il1k3tr@ff1cl1ght$".
    - Interpretation: This change indicates a recent update to the Gmail record stored on the server.
2. **ETag Modification:**
    - First Request ETag: "6e8-623bb5e3f8370-gzip"
    - Second Request ETag: "6ed-623bbe9ec4f76-gzip"

- Interpretation: The ETag change confirms that the content of the resource changed between requests, reflecting the Gmail password update.

Relevant Packet Numbers:

- First Request Packet: **Frame 3991**
- Second Request Packet: **Frame 4737**
- **Filter:http && ip.addr == 172.16.27.6**

15. What vendor made the local router and what model is it, which can be found via HTTP interactions?



In the HTTP interaction data, specifically in packet number 2322, the local router's vendor and model information can be identified. Here's how this was determined:

- **Packet Number: 2322 ,** Display Filter: **http && ip.addr == 172.16.27.30**
- **Vendor: FreshTomato**
  - **Explanation:** The router_name and wl_ssid fields in the packet data are set to "FreshTomato." FreshTomato is a custom firmware commonly used on specific router brands, indicating the device is running this firmware.
- **Model: Linksys E2500 v2**

- Explanation: The model information is directly listed under the t_model_name field in the packet, showing "Linksys E2500 v2" as the model.