**Question 1**  
A screenshot of a computer

Description automatically generated  
  
**Device MAC Address** : ba:db:ee:ff:24:18   
Located as the **Source MAC Address** in Frame 1.

2|  
A screenshot of a computer

Description automatically generated

3   
A screenshot of a computer

Description automatically generated  
4  
A screenshot of a computer

Description automatically generated  
  
5

A screenshot of a computer

Description automatically generated  
  
6 A screenshot of a computer

Description automatically generated

**Answer for Question 6:**

* **Encoded Credentials**: c3N0ZXZlbnNvbjphYmMxMjM=
* **Decoding the Credentials**:
  + The encoded string c3N0ZXZlbnNvbjphYmMxMjM= decodes to sstevenson:abc123.
  + Therefore, the **username** is sstevenson, and the **password** is abc123.

**Explanation**

* The **Authorization** header in the HTTP POST request shows Authorization: Basic c3N0ZXZlbnNvbjphYmMxMjM=.
* This indicates the use of Basic Authentication, where the credentials are encoded in Base64.
* After decoding, you obtain sstevenson:abc123, which are the login credentials for the router.

7  
A screenshot of a computer screen

Description automatically generated

**Answer for Question 7:**

* **Username**: root
* **Password**: abc123

**Explanation:**

* During the TELNET session to the mail server (prj-mail.my-infra.org), we see a login prompt:
  + prj-mail login: rroooott
  + Password: abc123
* This provides the **username** as root and the **password** as abc123, which were entered to log into the mail server.

8-   
A screenshot of a computer

Description automatically generated

**Answer for Question 8:**

* **Uptime**: The mail server has been up for **51 minutes**.

**Explanation:**

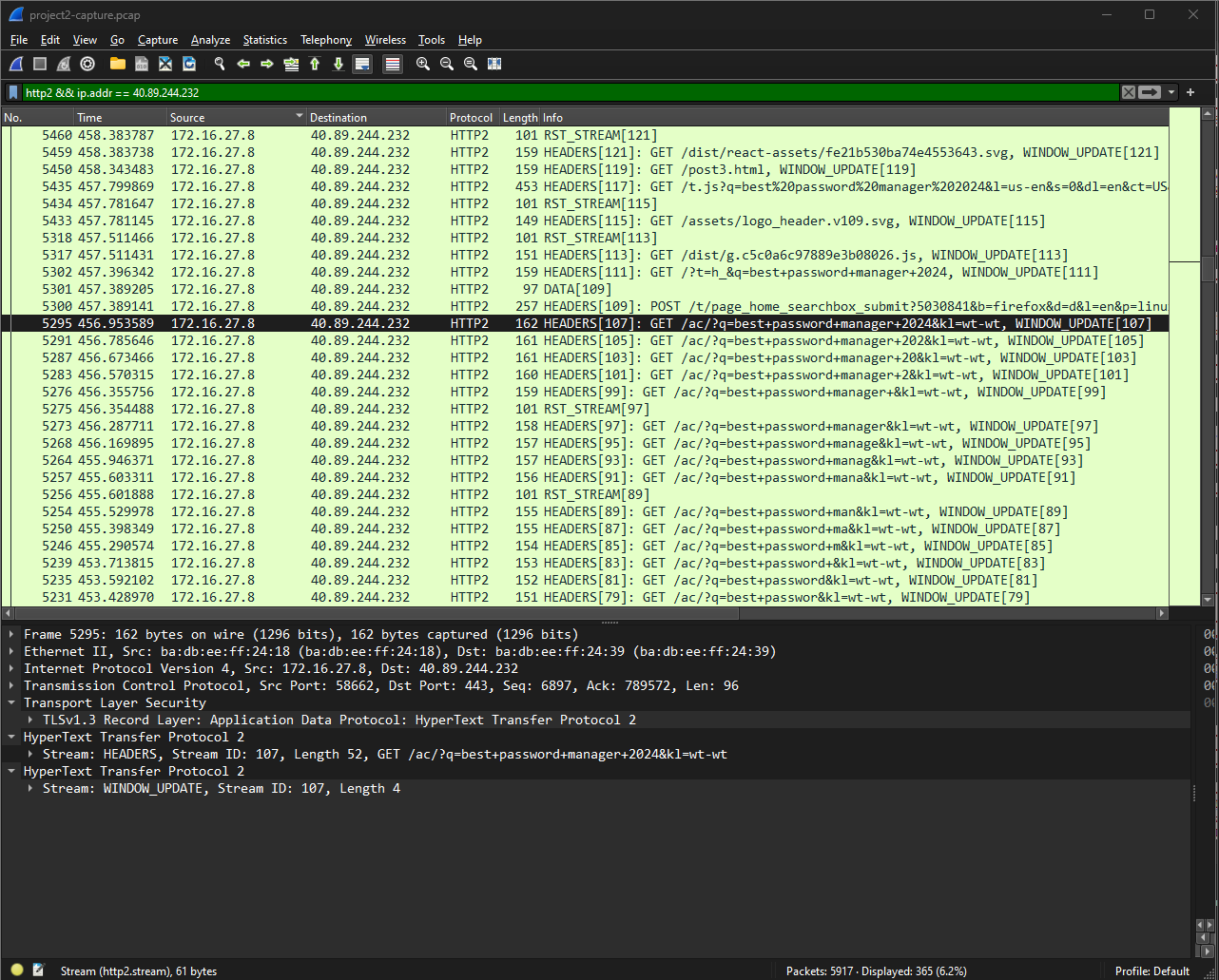
* The output of the uptime command shows that the server had been running for 51 minutes at the time this command was executed.
* This information can be found in the TELNET session after logging into the server, where system information commands like date and uptime are executed.

9

A screenshot of a computer

Description automatically generated  
  
10- A screenshot of a computer

Description automatically generated

**Linux Kernel Version**: Linux 6.1.0-26-amd64  
  
11 -

**Answer for Question 11:**

* **First Search Query**: best password manager 2024

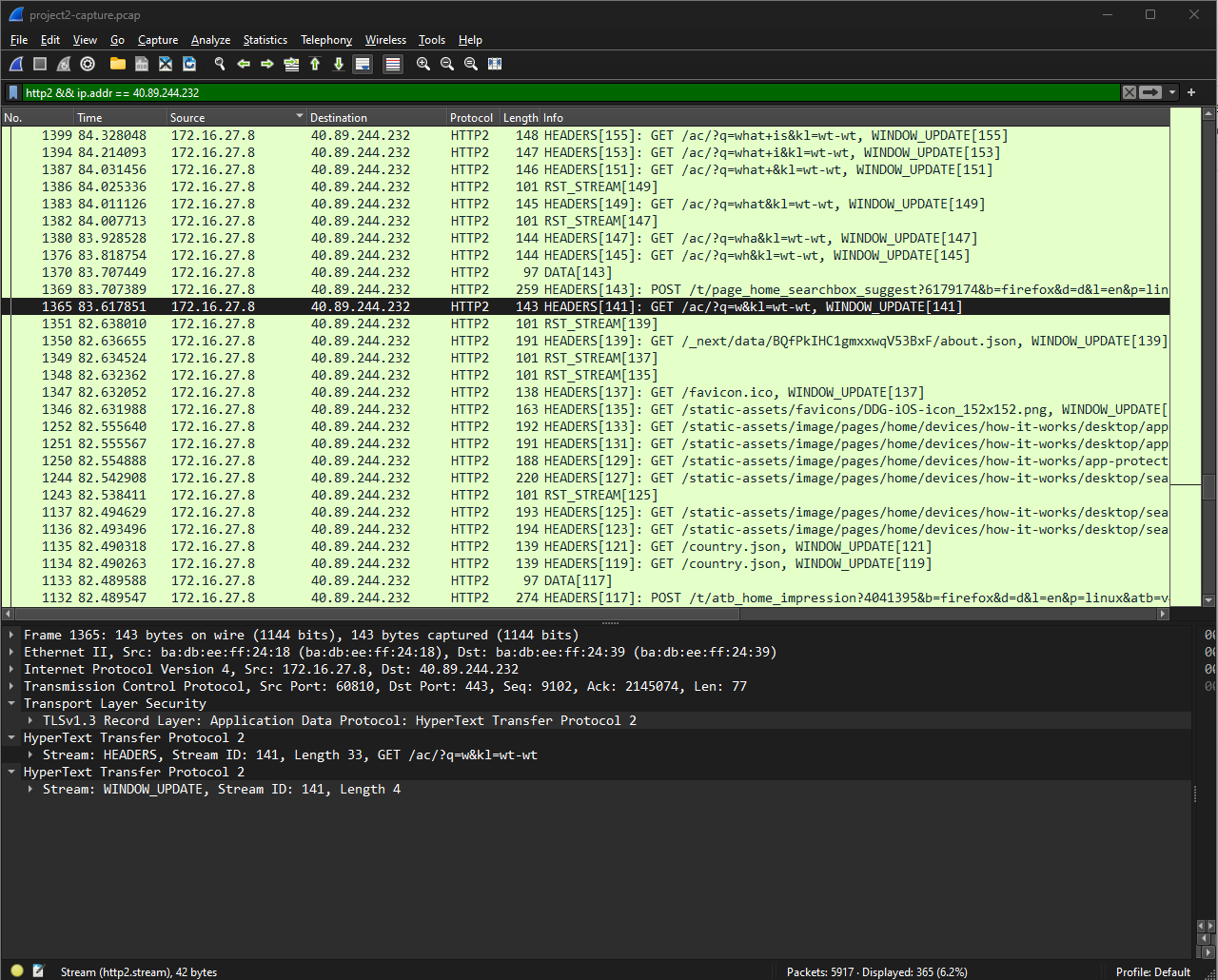
**Explanation:**

* The

field in the HTTP/2 GET request shows /ac/?q=best+password+manager+2024&kl=wt-wt.

* The parameter q=best+password+manager+2024 indicates the search query entered by the user.
* The

field shows duckduckgo.com, confirming this request was sent to DuckDuckGo.

12 -   
  
**Answer for Question 12:**

* **Last Search Query**: w

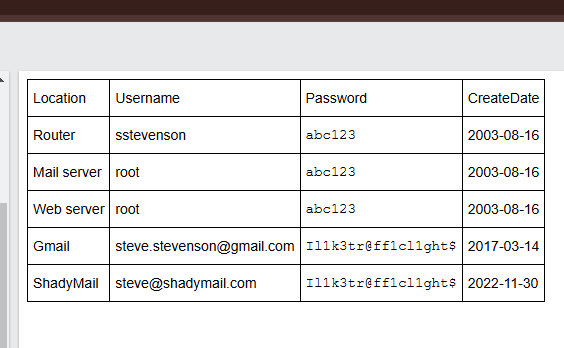
**Explanation:**

* The

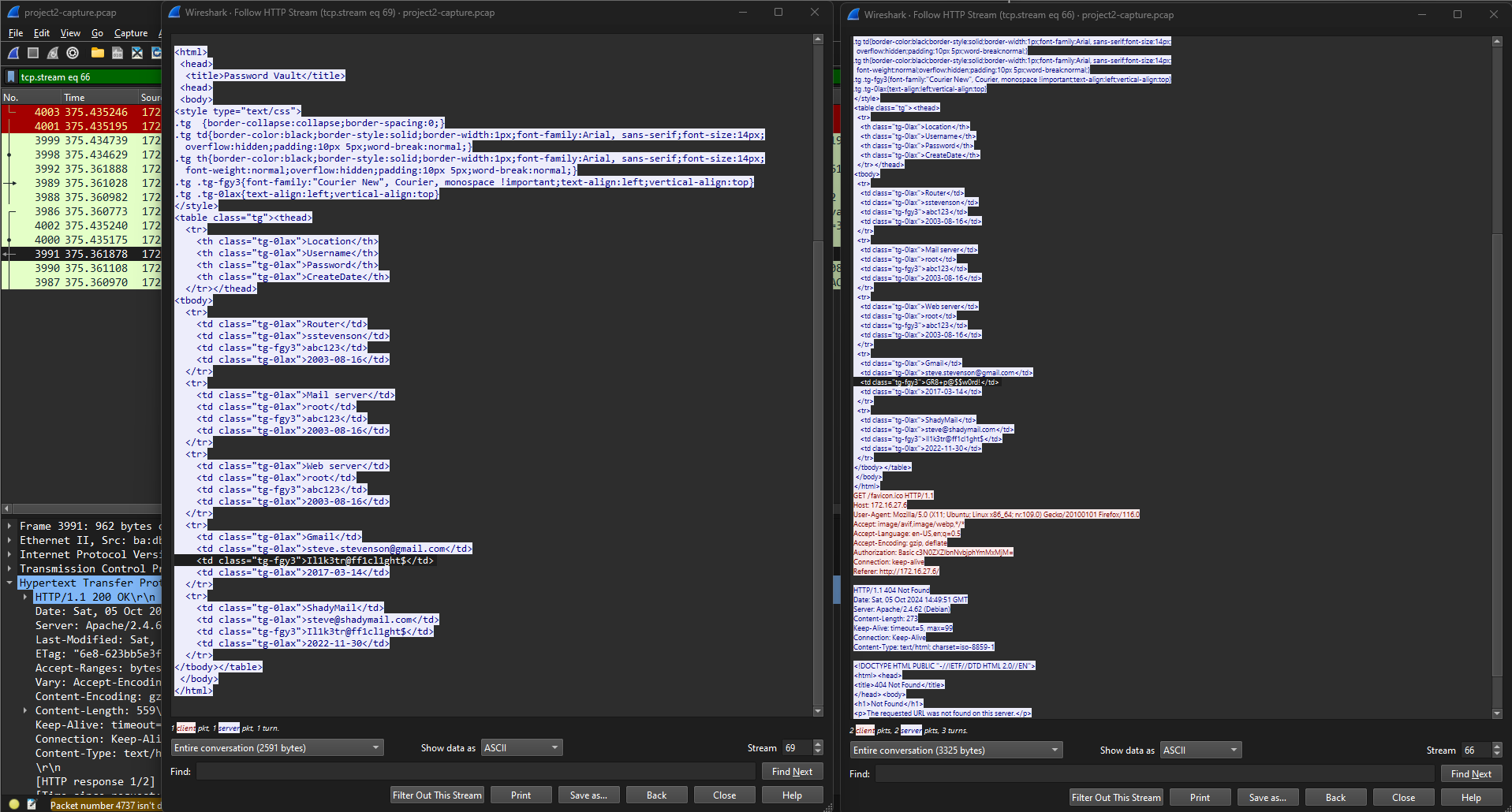
field in the HTTP/2 GET request shows /ac/?q=w&kl=wt-wt.

* The q=w parameter indicates that the user searched for the term "w."
* The

field confirms that this request was sent to duckduckgo.com.

13 - The webpage titled **"Password Vault"** displays the following information in a table format with columns for **Location**, **Username**, **Password**, and **CreateDate**  
 The webpage is titled **"Password Vault"**.

 It includes a table listing various services (Router, Mail server, Web server, Gmail, ShadyMail) along with corresponding usernames, passwords, and creation dates.  
  
A screenshot of a computer

Description automatically generated  
  
14 -   
  
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated  
  
humanize this - Analysis of Changes Between HTTP Requests to the Local Web Server

After reviewing the two HTTP GET requests to the local web server, we identified two key differences in the returned content:

1. Gmail Password Update

The password for the Gmail entry in the "Password Vault" was changed.

o First Request: GR8+p@$$w0rd!

o Second Request: Il1k3tr@ff1cl1ght$

This change indicates an update to the Gmail record stored in the web server’s database or configuration.

2. ETag Modification

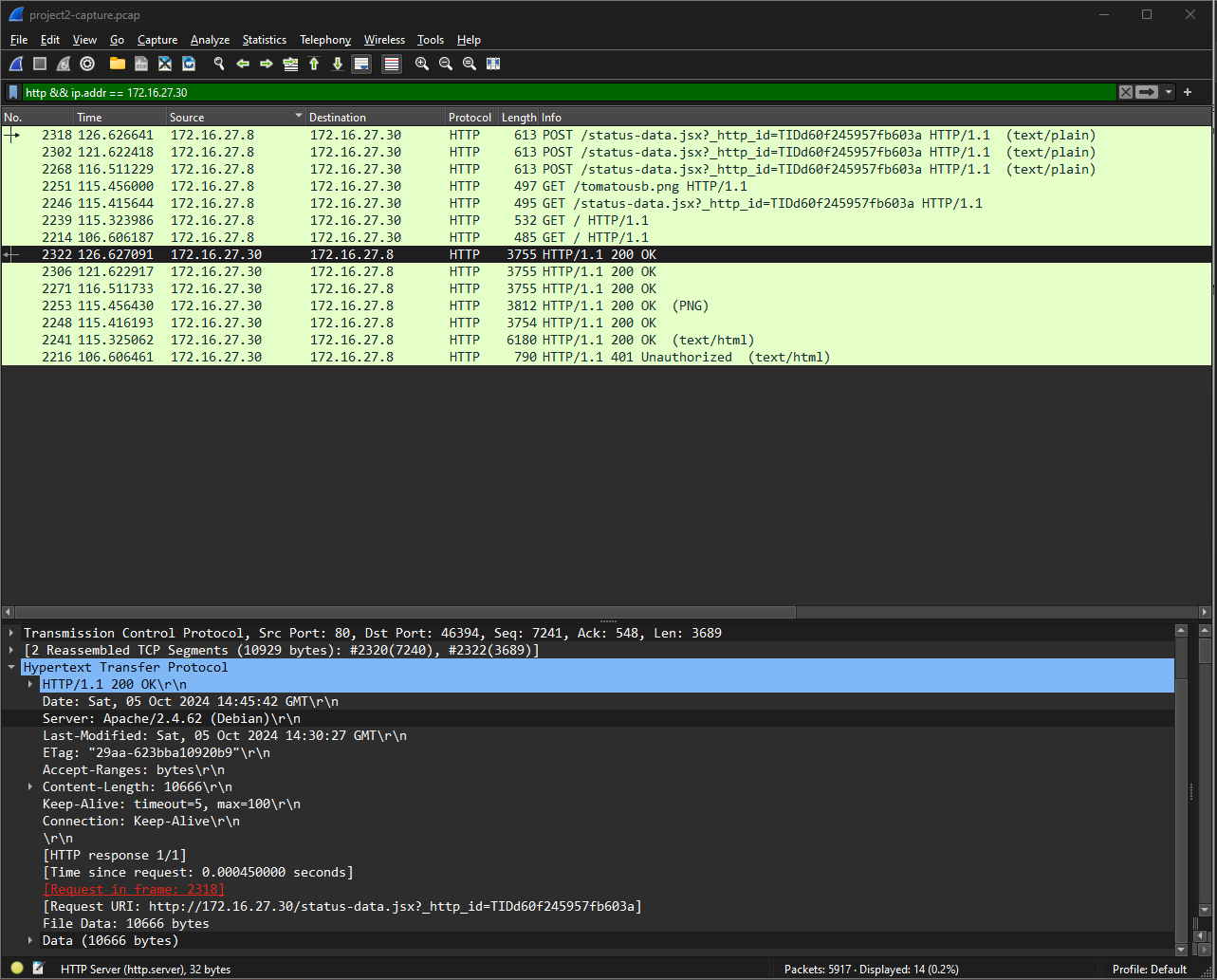
The ETag value, which acts as a version identifier for the requested resource, differed between the two responses, signaling a content update. The ETag serves as a unique identifier for the response's version, allowing caches to detect content modifications.

o First Request: "6e8-623bb5e3f8370-gzip"

o Second Request: "6ed-623bbe9ec4f76-gzip"

The modified ETag reflects the updated content following the Gmail password change.

These variations confirm that a record on the local web server, specifically the Gmail entry, was changed between the two HTTP requests.

15- 

**Answer for Question 15**

* **Vendor**: FreshTomato (This is a custom firmware based on Tomato, commonly used on certain router brands.)
* **Model**: Linksys E2500 v2

**Explanation**

* The **vendor** information is derived from the router\_name and wl\_ssid fields, both set to **FreshTomato**, which indicates the router is running the FreshTomato firmware.
* The **model** is specifically listed under t\_model\_name, which shows **Linksys E2500 v2**.