Seneca | SCHOOL OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

Lab - Email Header & Internet History Analysis

TERM	NAME – Student ID	COURSE CODE	WEIGHT
Winter 2025	Leandro Delgado	CYT215	10%

Lab Objectives

Upon completion of this lab, you will be able to perform the following:

- Examine and Analyze Email headers of Gmail webmail.
- Analyze Internet Cache of Chrome/Mozilla Browser.
- Analyze Internet History of Chrome/Mozilla Firefox Browser.

Lab Materials

- Windows Machine
- Tools and utilities:
    - MS Windows:
        - Product: **Text File reader**
        - Manufacturer: various
        - Web site: various
        - Product: **MozillaCacheView or ChromeCacheView**
        - Manufacturer: NirSoft
        - Web site: http://www.nirsoft.net/web_browser_tools.html
        - Product: **MozillaHistoryView or ChromeHistoryView**
        - Manufacturer: NirSoft
        - Web site: http://www.nirsoft.net/web_browser_tools.html
- Data files:
    - E-mail_headers.zip (password: **hands-on**)
    - Compressed_Caches.zip (password: **infected**) or your own cache and web history files

Lab Instructions

- Download and install all required software on Windows OS
- Download all required forensic images.
- Complete this lab.
- Enter your name and student ID above.
- Answer questions and add screenshots.

Part 1: Email Header Analysis

- Download the file named "**e-mail_headers.zip**" from the *Blackboard*. Extract the files from the compressed file and place them on your desktop.
- Open the file named "**Header_from_gmail_account.txt**" (Note: If you have a Gmail e-mail account, the e-mail header can be retrieved by going to your inbox with a browser, opening an e-mail, clicking on “More” on the right side of the menu and selecting "Show Original" from the pop-up menu. For this activity, this step has already been completed and the output has been saved to a text file.)

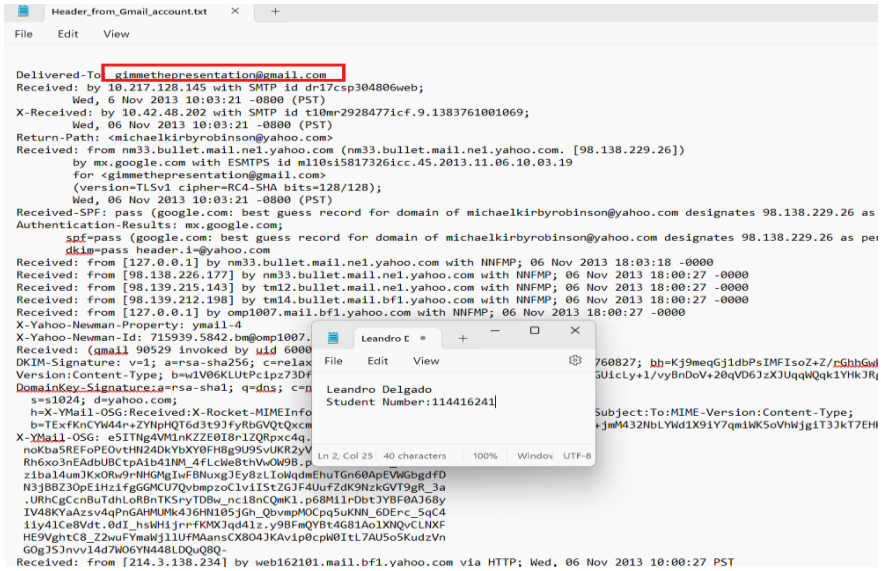


Figure 1.Image Header from Gmail

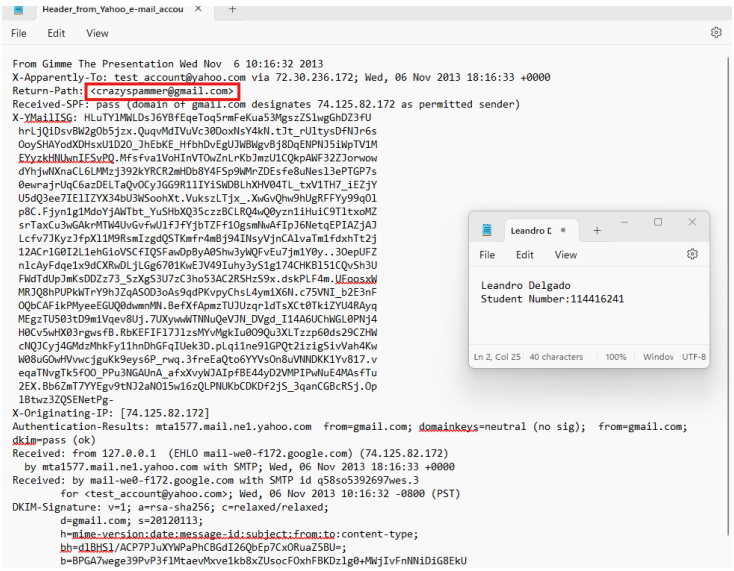


Figure 2. Image header from yahoo

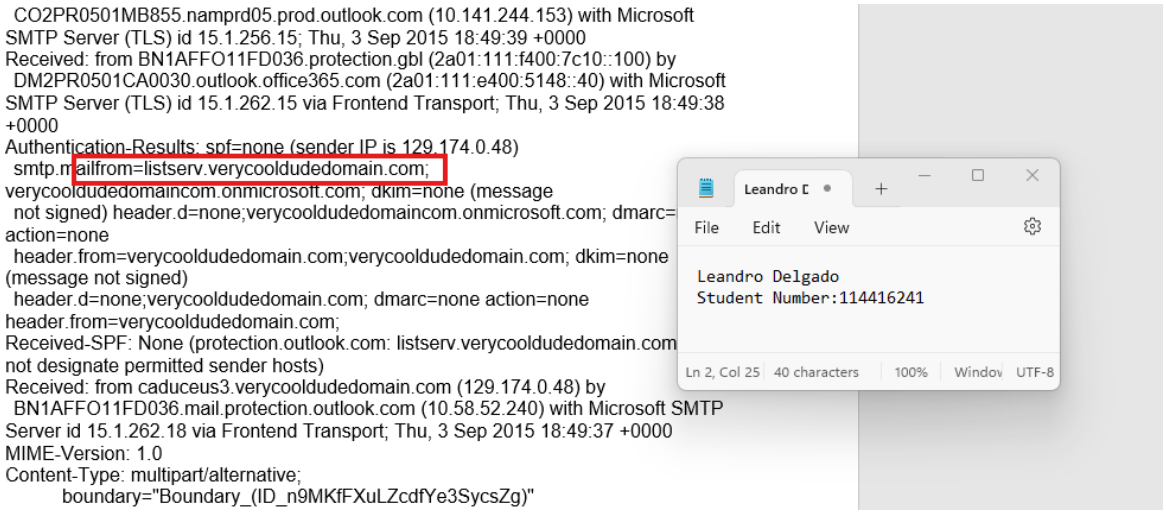
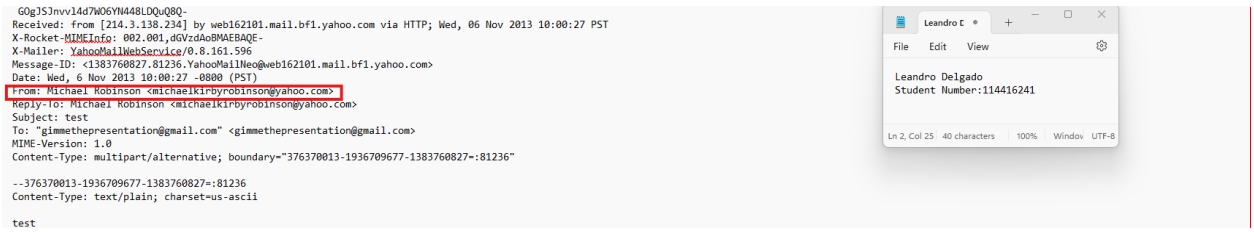


Figure 3. Header from Microsoft 365

- Answer the following questions:

From which e-mail account did it originate? [screenshot]



Gmail Email: Sent From Michael Robinson michaelkirbyrobinson@yahoo.com

Get the email sender accounts for the other available header files.

- Yahoo Email: Sent from crazyspammer@gmail.com.
- Gmail Email: gimmethepresentation@gmail.com
- Windowns 365 : listserv@verycooldudedomain.com

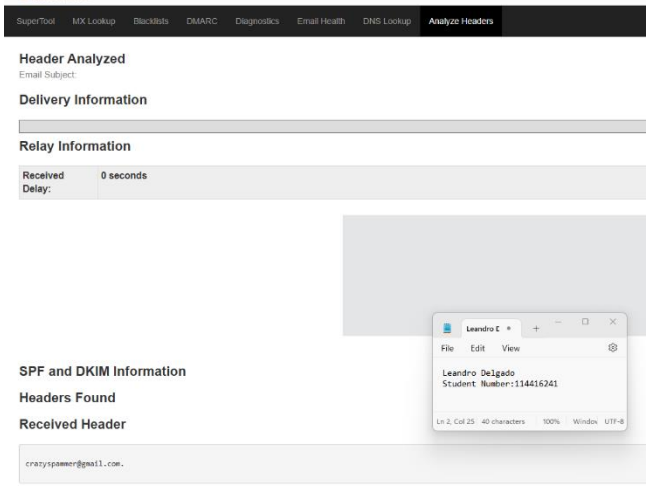
1) **What is SMTP (example below from an email header):**

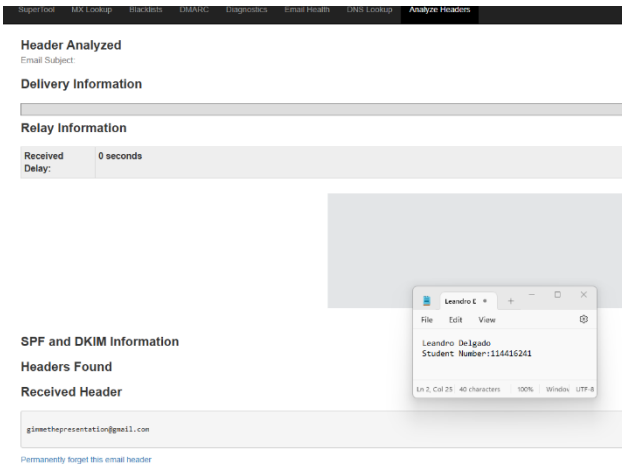
X-Received: by 10.194.88.225 with SMTP id bj1mr2994653wjb.50.1383761792331;
Wed, 06 Nov 2013 10:16:32 -0800 (PST)

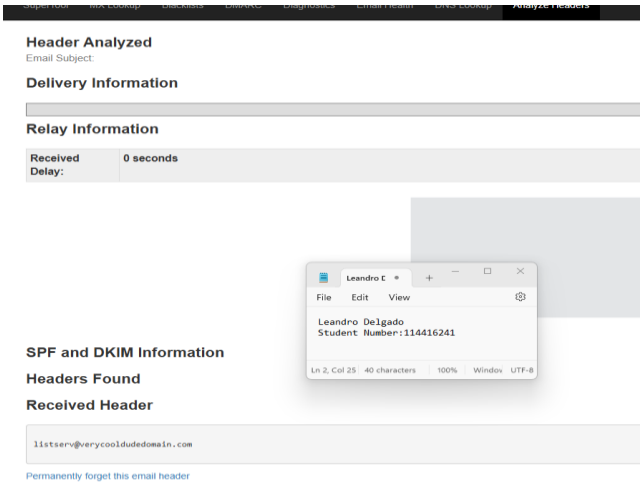
SMTP: is the communication protocol used to send emails between mail servers. It is responsible for routing and delivering outgoing emails.

2) **What is POP3/IMAP and how are these protocols different from SMTP?**
   - **POP3** pulls emails from the server to your device and deletes them, meaning you can't access them from another device.
   - **IMAP** keeps emails on the server, so you can check them from anywhere.
   - **SMTP** is different—it's only used for sending emails, not receiving them.
3) **Get a copy of the email headers for an email you received and analyze it. If you want to analyze emails easier you can copy and paste the headers in the below link:**

https://mxtoolbox.com/EmailHeaders.aspx







Part 2: Analyzing Chrome/Firefox History

- Download **MozillaHistoryView.zip** or **ChromeHistoryView.zip**.
- Run the tool and open your own Chrome/Firefox history file or use the provided files.
- Answer the below questions:

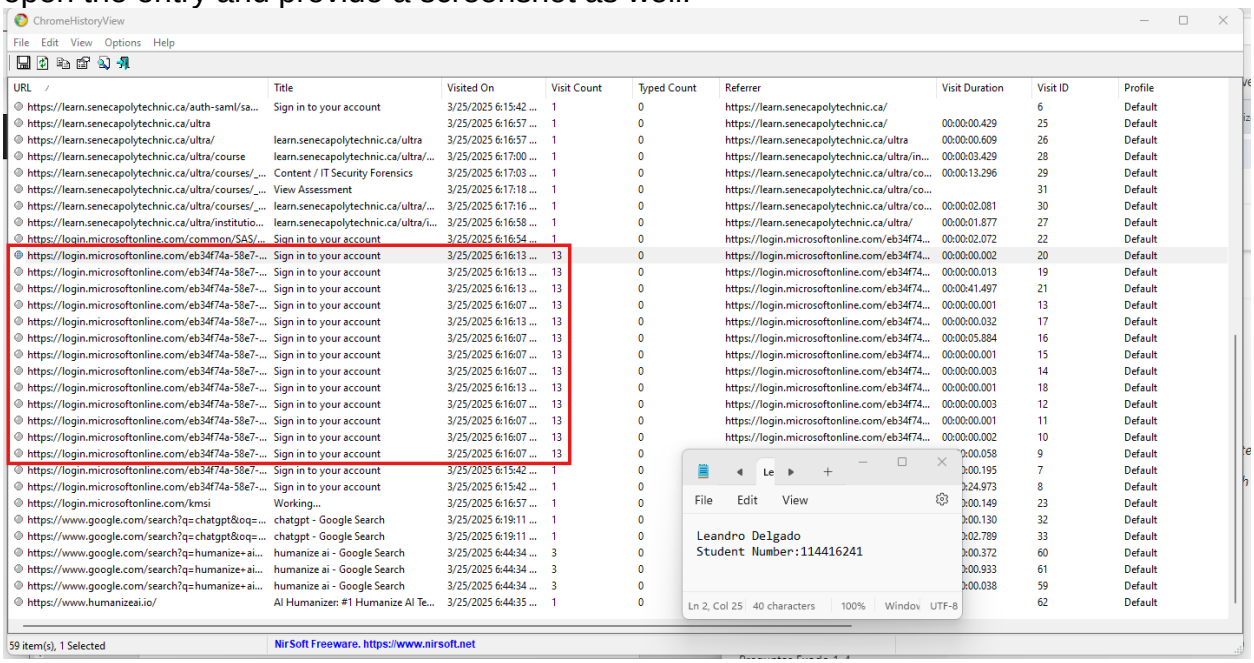
1) What is the location of your history file?
   - **Chrome:**
     C:\Users\YourUserName\AppData\Local\Google\Chrome\User Data\Default\History
   - **Firefox:**
     C:\Users\YourUserName\AppData\Roaming\Mozilla\Firefox\Profiles\yourprofile.default\places.sqlite

2) How many websites have you visited?

   2046

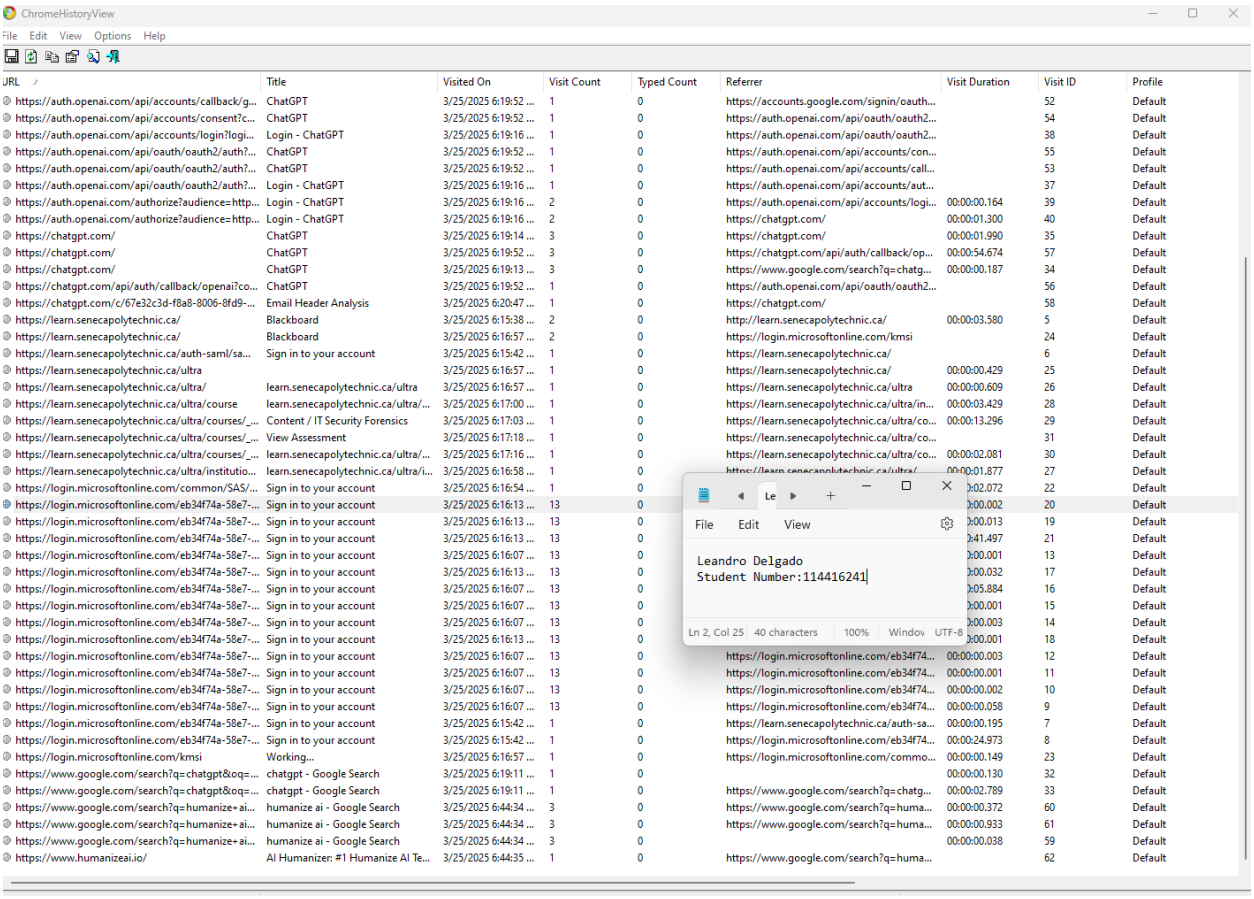
3) Select one of the most visited websites in your history and provide some information about it, e.g. was it a typed URL? What is the URL length? What

is the last visited time? When was the last time the URL was visited. You can open the entry and provide a screenshot as well.



- URL: https://login.microsoftonline.com/eb347f4a-58e7...
- Visit Count: 13 times
- Typed Count: 0 (Meaning it was not manually typed; likely accessed via a saved login, bookmark, or redirection)
- URL Length: 76 characters
- Last Visited Time: 3/25/2025 6:16:13 AM
- Referrer: https://login.microsoftonline.com/... (Indicating the visit originated from Microsoft's login system)
- Visit Duration: Extremely short (mostly 0.001–0.002 seconds, indicating quick authentication processes)

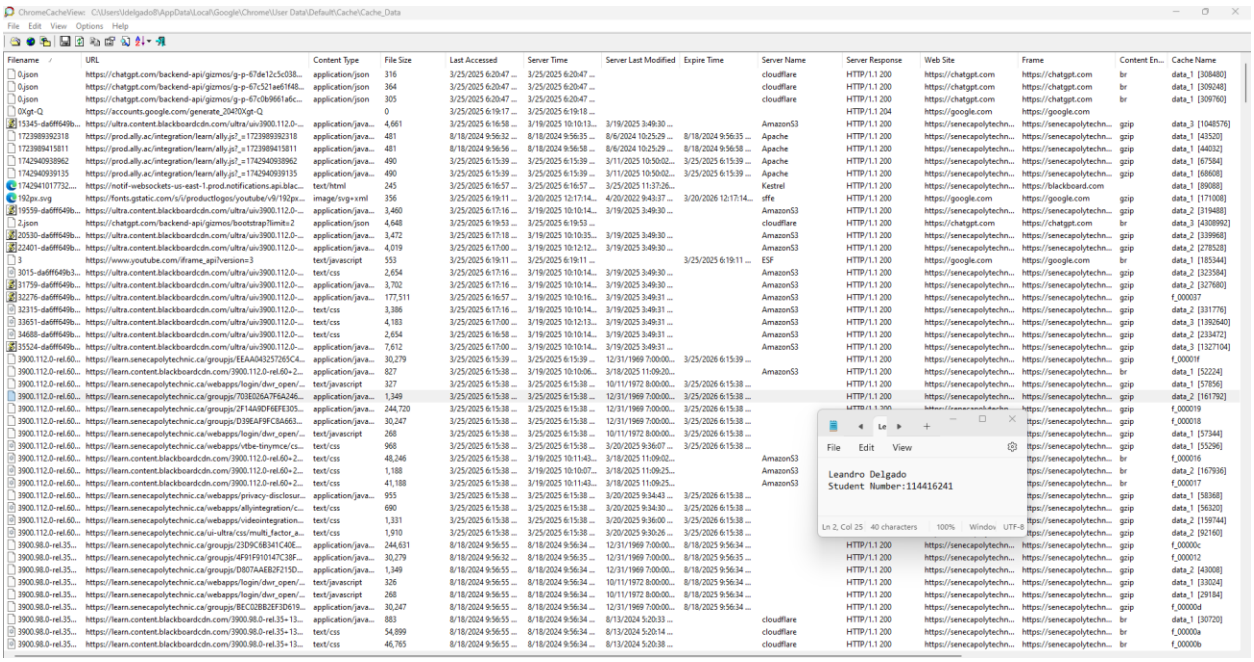
4) Is there a typed URL in your history? Provide more information about it. If you don't have a typed URL, please close the application, type a URL and re-open the tool. How many times have you typed the URL and how many times have you visited it?

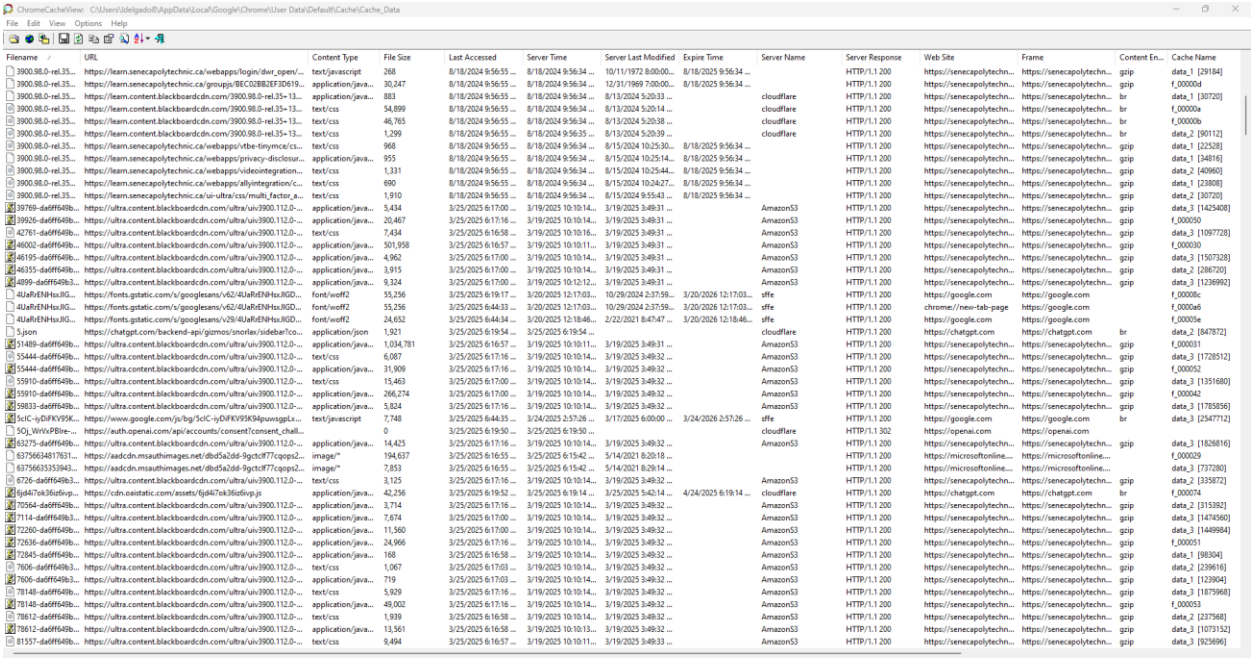


All entries in the "Typed Count" column show 0, meaning no website was manually typed into the browser's address bar.

Part 3: Analyzing Chrome/Firefox Cache

- Download **ChromeCacheView.zip** or **MozillaCacheView.zip**.
- Use your own cache files or the sample files on the blackboard.
- A sample result of MZCacheViewer is shown below:





- Answer the following questions:

1) **Do you see any URLs with HTTP status code of 301 or 206? [screenshot]**

From the screenshot, I do not see any HTTP status codes **301 (Moved Permanently)** or **206 (Partial Content)**.

2) **Explain what do these status codes mean?**

301 (Moved Permanently):

This means that the resource has been permanently moved to a new URL location.

In the future requests, the users are automatically redirected to the new URL by the browser.

For instance, whenever a website decides to change its domain, all requests redirected permanently from the old site.

206 (Partial Content):

This status is used if a client (e.g., browser, media player, downloader) requests only some portions of any resource.

This is usually used in:

- **Streaming videos**
- **Paused/resumed downloads**
- **Large transfers of files**

Example: A user may pause and resume a video, where the server will send only the missing portion.

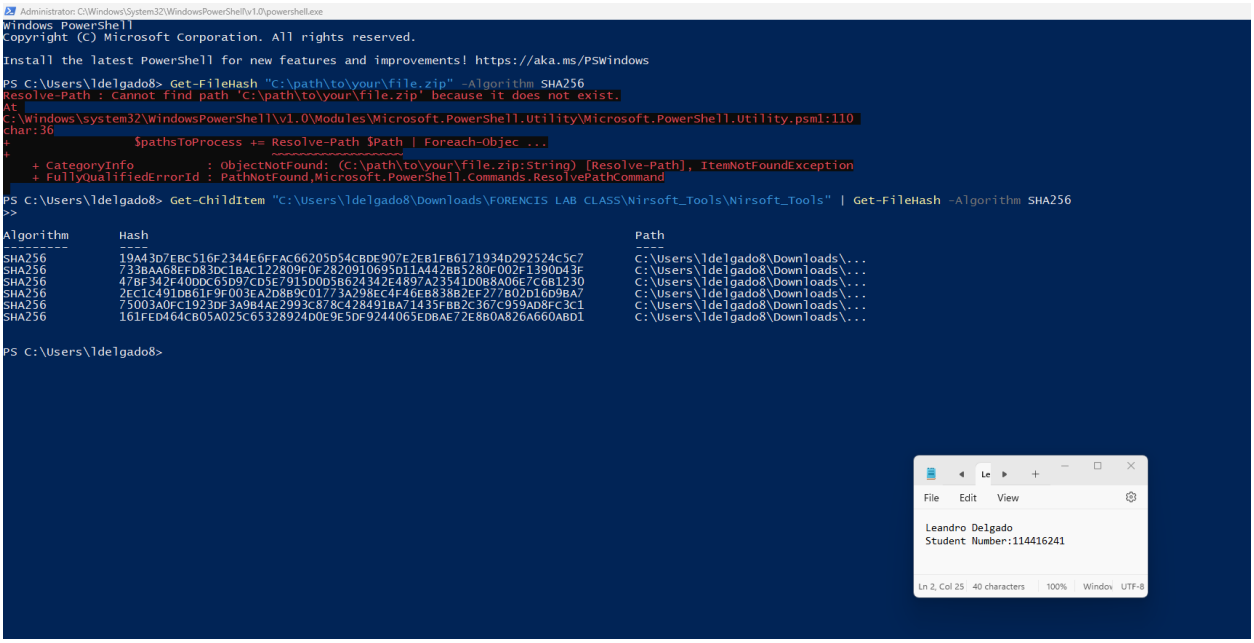
3) **Do you see any entries with the server's name as Akamai or Cloudflare? What is Akamai and how does it work?**

- Yes! The "Server Name" column shows several instances of Cloudflare.
- Akamai is not visible in this screenshot, but it may appear if the filter the data.

What is Akamai, and how does it work?

- Akamai Technologies is a Content Delivery Network (CDN) and cloud security provider.
- It helps websites load faster and more securely by:
  - Distributing content across multiple servers worldwide.
  - Reducing latency by serving content from a nearby edge server.
  - Protecting websites against DDoS attacks, bot traffic, and malware.
- Cloudflare is another major CDN provider with similar security and performance optimization services.

4) **Find a file with content type: application/javascript, export the file and send it for analysis to a sandbox of your choice. If you don't find a javascript file, select a file of your choice. You can also get the file hash and submit the hash if you can't submit the file.**



With this PowerShell command, SHA-256 file hashes of all files in the specified directory C:\Users\ldelgado8\Downloads\FORENCIS LAB CLASS\Nirsoft_Tools\Nirsoft_Tools have been generated successfully. The generated hash for each file serves as its fingerprint and can be used to detect alterations in case of integrity breaches. It thereby finds its relevance in forensic analysis, cyber-investigations, and file verification. The output shows a total of six different files along with the corresponding SHA-256 hash, confirming that their contents were not modified.