

Challenge: [Eli Lab](#)

Platform: CyberDefenders

Category: Endpoint Forensics

Difficulty: Medium

Tools Used: CLEAPP

Summary: This lab involved analysing a forensic image generated from a Chromebook using tools like CLEAPP, notepad, etc. It is a relatively easy lab; it just involves a lot of hunting around to find the answer. This was personally my first time investigating a Chromebook forensic image, so take everything I have said with a grain of salt.

Scenario: A user reported strange browser behaviour and missing files on their Chromebook. SOC analysts suspect unauthorized access and data theft. You've received a forensic image for review. Investigate user activity, application data, and browsing artifacts to uncover what happened.

ChromeOS Logs Events and Protobuf Parser (CLEAPP) is an open source tool that can parse every known ChromeOS artifact. To install this tool, execute the following commands (in my case, I used Windows 11):

- git clone <https://github.com/markmckinnon/cLeapp.git>
- pip3 install -r requirements.txt

You can then execute this tool against the Chromebook dump by issuing the following command:

```
python .\cleapp.py -t tgz -i '.\2021 CTF - Chromebook.tgz' -o .
```

The folder to store all your data in - How many files are in Eli's downloads directory?

Navigate to:

2021 CTF - Chromebook.tar\decrypted\mount\user\Downloads

In the Downloads directory, we can see a total of 6 files. This directory reflects files the user manually downloaded or saved from the internet. Such directories are useful to identify files the user has downloaded via a browser, etc.

network_diagnostics_2021-03-08.1...	Text Document
Screenshot 2021-03-04 at 3.16.31 A...	PNG File
Screenshot 2021-03-04 at 3.17.06 A...	PNG File
third_party_1613945285717.jpg	JPG File
tux.png	PNG File
Wickr-Customer-Security-Promise...	Firefox PDF Document

Answer: 6

Smile for the camera - What is the MD5 hash of the user's profile photo?

Navigate to:

2021 CTF - Chromebook\decrypted\mount\user\Accounts\Avatar Images

You will find a single file here, this is the avatar image associated with Eli's ChromeOS account. To generate the MD5 hash of this image, you can use the Get-FileHash cmdlet:

```
Get-FileHash -Algorithm MD5 .\e flatt610@gmail.com
```

Algorithm	Hash
MD5	5DDD4FE0041839DEB0A4B0252002127B

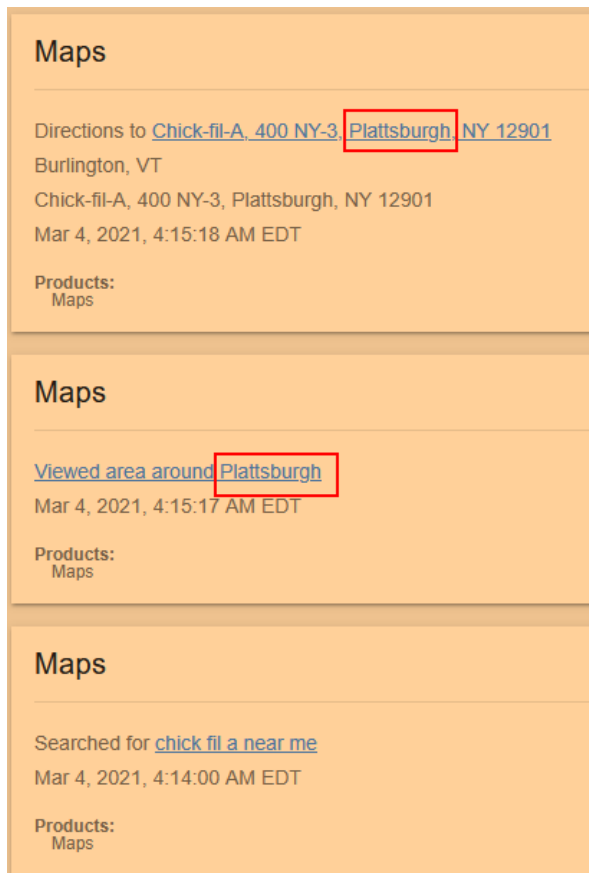
Answer: 5DDD4FE0041839DEB0A4B0252002127B

Road Trip! - What city was Eli's destination in?

Navigate to:

2021 CTF - Takeout\Takeout\My Activity\Maps\MyActivity.html

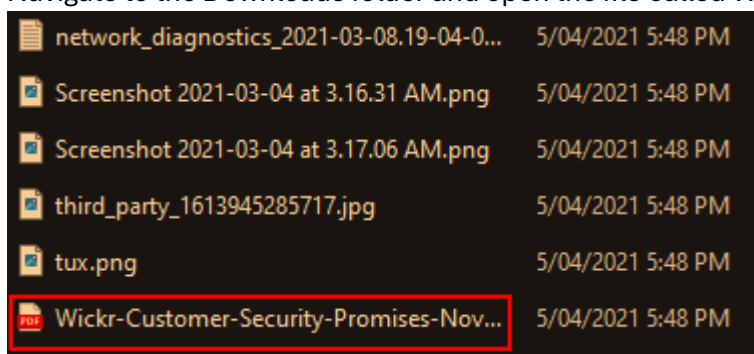
This file records Google maps activity, including searched destinations. On review, Eli appears to have searched for directions to Plattsburgh, making it the probable destination:



Answer: Plattsburgh

Promise Me - How many promises does Wickr make?

Navigate to the Downloads folder and open the file called Wickr-Customer-Security-Promises:



Within this document are 9 promises:

Wickr's Customer Security Promises	
The Wickr protocol provides end-to-end encryption and integrity protection	
The Wickr protocol enforces forward secrecy	
The Wickr protocol enforces authentication of messages	
Compromise of Wickr infrastructure does not compromise message content	
Protocol reliably informs messaging partners of ephemerality policy	
Group messaging protocol provides the same security assurances as Core protocol	
Video and audio calling provides the same security assurances as Core protocol	
Message content and supporting encryption keys are managed properly on official supported Wickr clients	
Wickr manages sensitive customer data in cloud-hosted networks in accordance with the Wickr Privacy Policy	

Answer: 9

Key-ty Cat - What are the last five characters of the key for the Tabby Cat extension?

Under the “Extensions” section on CLEAPP, you can see the extension ID for Tabby Cat:

Install Time	Extension Name	Description	Version	Extension ID
2021-02-28 06:30:39	Tabby Cat	A new friend in every tab.	2.0.0	mefhakmgclhfhbdadeojkblmeciialg

We can search for this ID within the 2021 CTF - Chromebook\decrypted\mount\user\Extensions directory. Once you find the folder for this extension, open the manifest.json file, which contains the key:

```
{
  "author": "Leslie Zacharkow",
  "chrome_url_overrides": {
    "newtab": "public/index.html"
  },
  "description": "A new friend in every tab.",
  "icons": {
    "128": "icon128.png"
  },
  "key":
  "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEajA9E1NuqHGIuDyrztUxn0nV1C
  AIxOkSvFm4Set3YRQ5994NA8Y9un1ZGhPtjFnpoLo1pEA5PP1y5/BX2y3Ci2Rb0C3wp8Nc
  +l8EdG/Ks881p8L00J3qepmhNDA/LjVWzJq5ARmIYeT3TnvR/qRGTY9UXfUvg3gcUWV2LE
  /S/9Ix1P+wItoEinTwIDAQAB",
  "manifest_version": 2,
  "name": "Tabby Cat",
  "offline_enabled": true,
  "permissions": [ "storage" ],
  "update_url": "https://clients2.google.com/service/update2/crx",
  "version": "2.0.0"
}
```

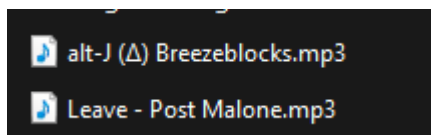
Answer: DAQAB

Time to jam out - How many songs does Eli have downloaded?

Navigate to:

2021 CTF - Chromebook\decrypted\mount\user\MyFiles\Music

Inside this folder, you will find 2 MP3 files, indicating the number of downloaded songs.



Answer: 2

Autofill, roll out - Which word was Autofilled the most?

Open the CLEAPP report and review the “Chromebook Autofill” section. This section shows saved autofill data such as names, addresses, and frequently used fields. Here, the word “email” appears three times:

Date Created	Field	Value	Date Last Used	Count
2021-02-04 00:15:25	guests	1 Guest	2021-02-04 00:15:25	1
2021-02-17 01:09:26	email	e.flatt610@gmail.com	2021-03-04 08:29:03	3
2021-03-04 08:29:24	email	e.flatt610@protonmail.com	2021-03-04 08:29:24	1

Answer: email

Dress for success - What is this bird's image's logical size in bytes?

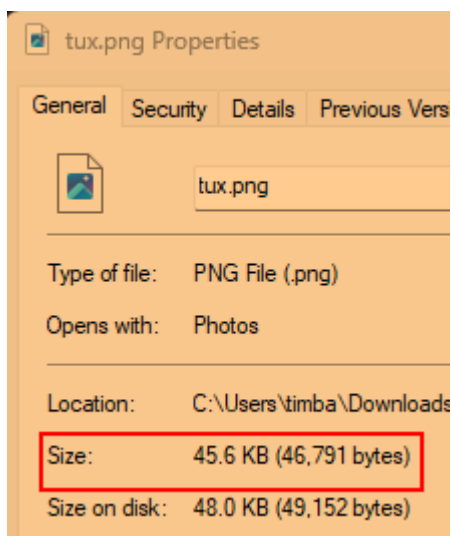
Navigate to:

2021 CTF - Chromebook\decrypted\mount\user\Downloads

Locate the image file featuring Tux, the Linux penguin mascot.



Right-click and view file properties (on Windows) to view the logical file size.



Answer: 46791

Repeat customer - What was Eli's top-visited site?

Going back to the CLEAPP report, under the “Chromebook Top Sites” section, you can find what sites Eli visited the most:

URL	Rank
https://protonmail.com/	0
https://www.amazon.com/	1
https://chrome.google.com/webstore?hl=en	2
https://www.facebook.com/	3
https://chrome.google.com/webstore/category/extensions?hl=en	4
chrome-extension://aohghmighlieiainnegkciijnfilokake/main.html	5

0 being the most visited site.

Answer: protonmail.com

Vroom Vroom, What is the name of the car-related theme?

Within the “Extensions” section of the CLEAPP report, we can find a theme called Lamborghini Cherry:

2021-02-28 06:29:27	Lamborghini Cherry	Lamborghini Cherry
------------------------	--------------------	--------------------


Answer: Lamborghini Cherry

You got mail - How many emails were received from notification@service.tiktok.com?

Navigate to:

2021 CTF - Takeout\Takeout\Mail

Here you can find a file that includes all emails stored on the device:

 All mail Including Spam and Trash.mbox

I didn't have a mail client that could import this mailbox, so I just chunked it into ChatGPT to see how many emails were received by notification@service.tiktok.com. There are tools that can view .mbox files, you can even view it using notepad or sublime, but it takes a lot of time to go through and count how many emails were received from the given address.

Answer: 6

Hungry for directions - Where did the user request directions on March 4, 2021, at 4:15:18 AM EDT?

Navigate to:

2021 CTF - Takeout\Takeout\My Activity\Maps

Within this directory, open up the MyActivity.html file. This file stores activity for Google maps. Here we can see that the user requested directions to Chick-fil-A at 4:15:18 on the 4th of March 2021:

Maps

Directions to [Chick-fil-A, 400 NY-3, Plattsburgh, NY 12901](#)
Burlington, VT
Chick-fil-A, 400 NY-3, Plattsburgh, NY 12901
Mar 4, 2021, 4:15:18 AM EDT

Answer: Chick-fil-A

Who defines essential? - What was searched on Mar 4, 2021, at 4:09:35 AM EDT?

Navigate to:

2021 CTF - Takeout\Takeout\My Activity\Search

Within this directory, open up the MyActivity.html file. After searching for the given timestamp, we can determine what was searched for:

Search

Searched for [is travelling to get chicken essential travel](#)

Mar 4, 2021, 4:09:35 AM EDT

Products:
Search

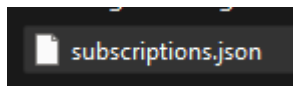
Answer: is travelling to get chicken essential travel

I got three subscribers, and counting - How many YouTube channels is the user subscribed to?

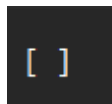
Navigate to:

2021 CTF - Takeout\Takeout\YouTube and YouTube Music\subscriptions

Within this directory, we can find a Json file called subscriptions.json:



If you view this file, you can see that it is empty, meaning the user is subscribed to no one:



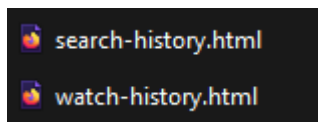
Answer: 0

Time flies when you're watching YT - What date was the first YouTube video the user watched uploaded?

Navigate to:

2021 CTF - Takeout\Takeout\YouTube and YouTube Music\history

Within this directory we can find a file called watch-history.html:



The first video this user watched was called "The BEST Clips of 2020 | Lacrosse Highlights ECD Lacrosse" on the 3rd of February, 2021 at 8:14:39 PM:

Watched [The BEST Clips of 2020 | Lacrosse Highlights](#)
[ECD Lacrosse](#)

Feb 3, 2021, 8:14:39 PM EDT

After viewing the video, it was uploaded on the 27th of January, 2021.

Answer: 2021-01-27