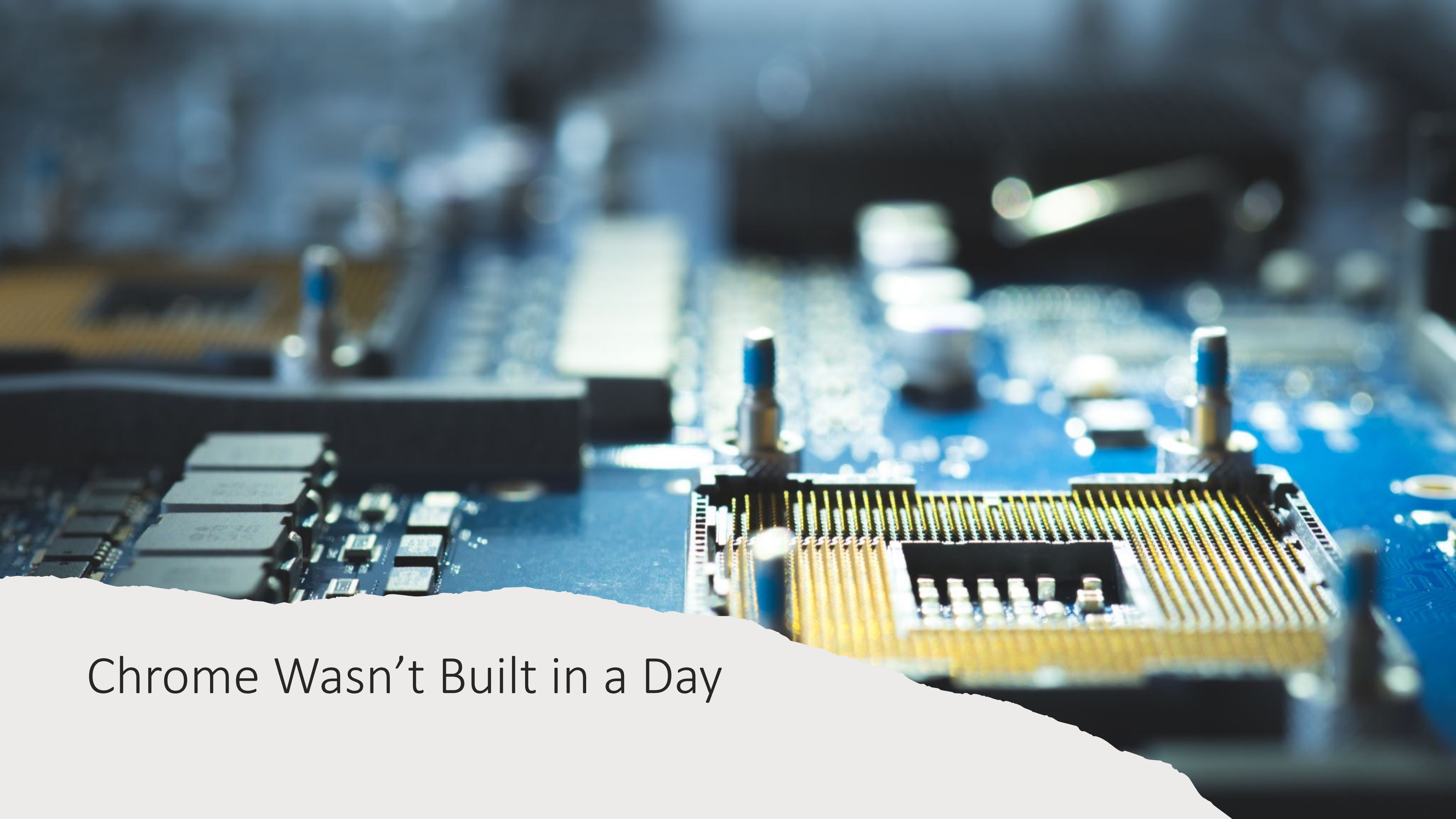


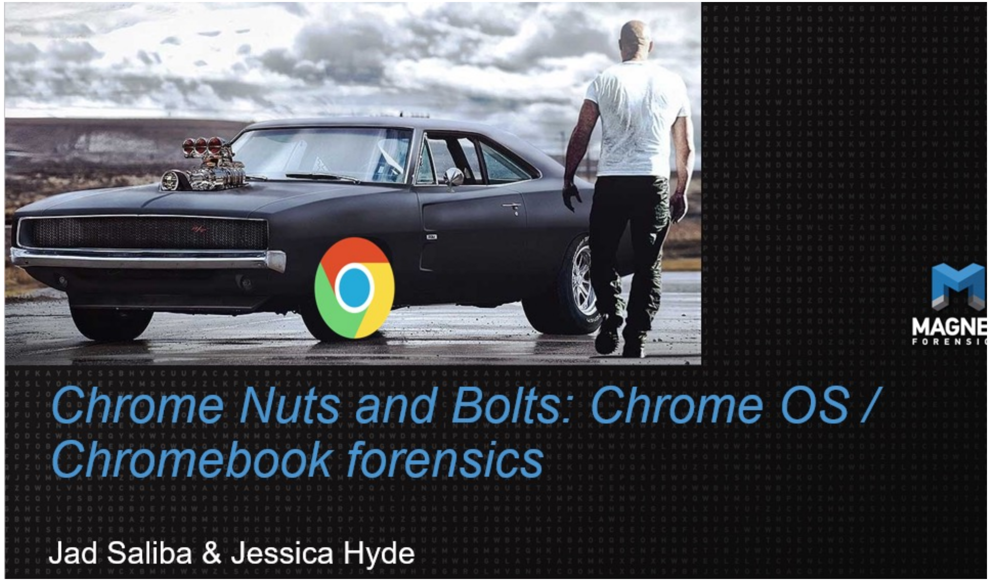
Chrome Wasn’t Built in a Day

Jessica Hyde

@B1N2H3X

- Founder & Owner, Hexordia
- Consultant, Magnet Forensics
- Adjunct Professor, George Mason Univeristy
  - Previous:
    - Director Forensics, Magnet Forensics
    - Basis Technology
    - Ernst and Young
    - American Systems
- HTCIA IEC 2nd VP

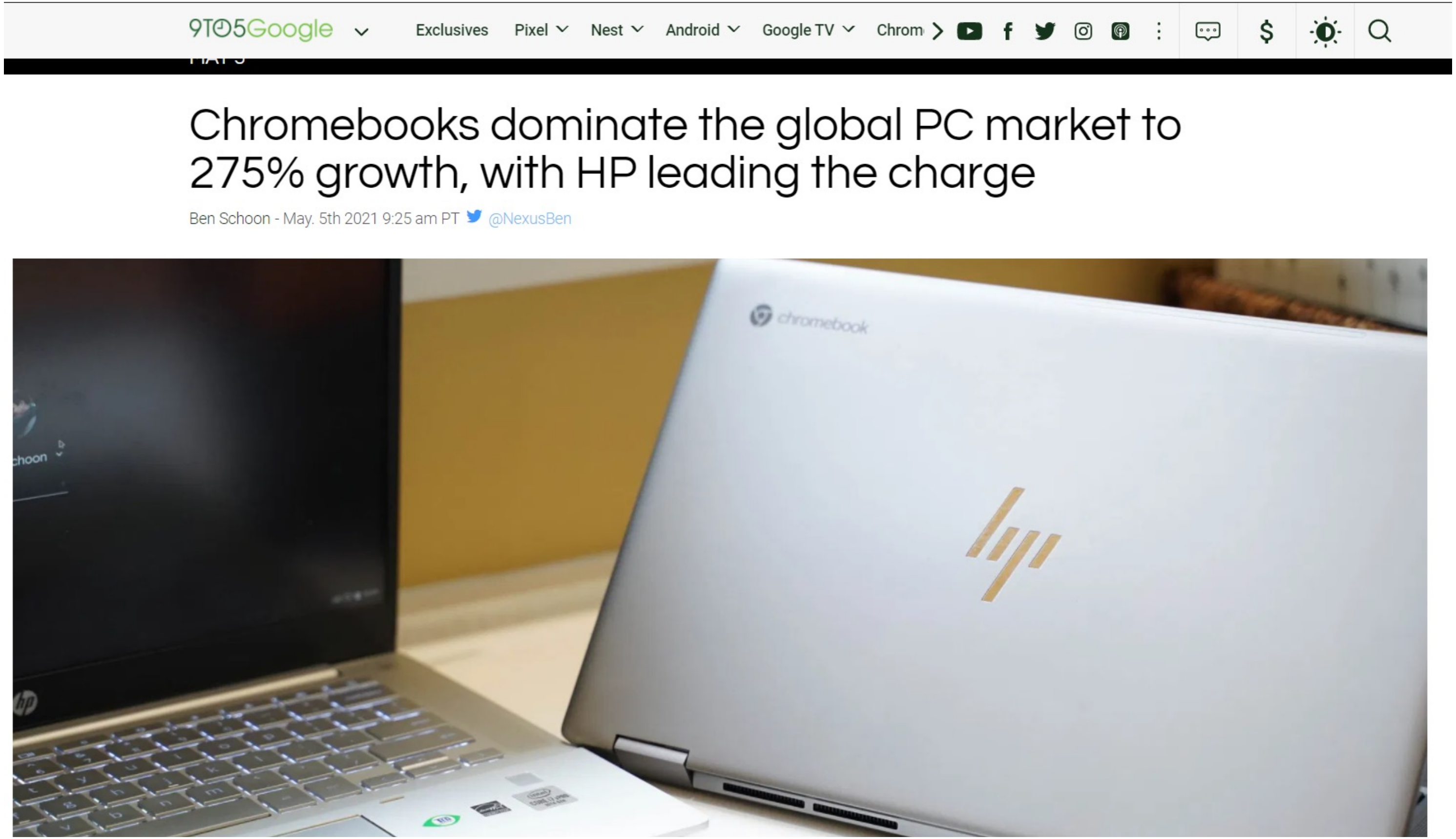
Research Evolution



Chrome Nuts and Bolts: Chrome OS / Chromebook forensics

Jad Saliba & Jessica Hyde

- 2018 Research by Jad Saliba and Jessica Hyde
- Is the data on device different/valuable compared to the cloud data storage? YES!

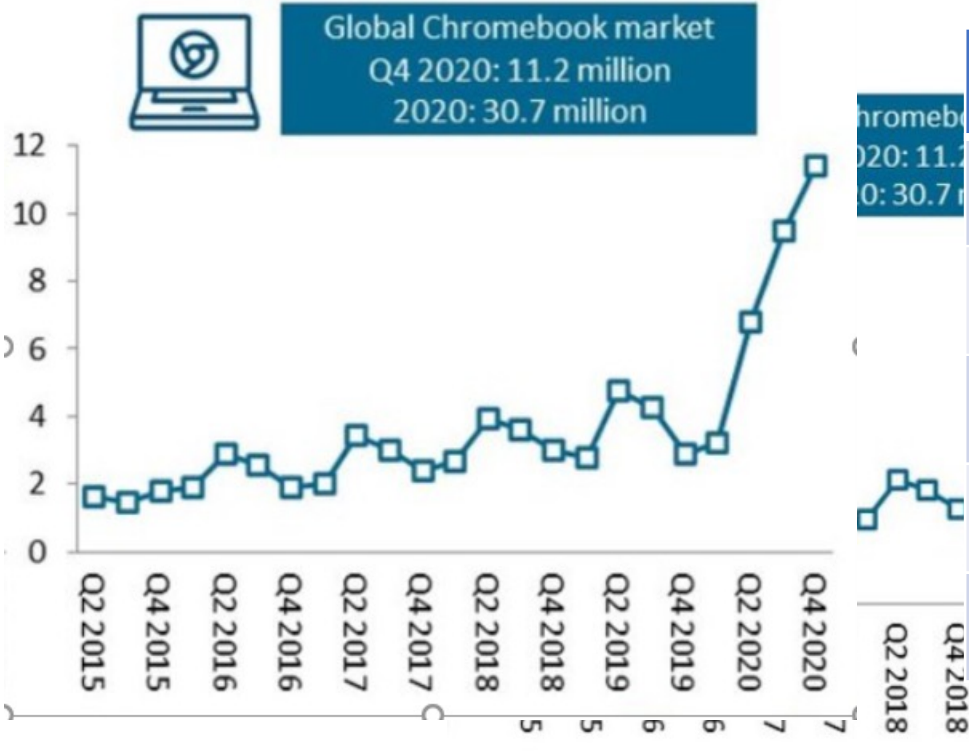


Chromebooks dominate the global PC market to 275% growth, with HP leading the charge

Ben Schoon - May. 5th 2021 9:25 am PT @NexusBen

- Source: https://9to5google.com/2021/05/05/chromebook-pc-market-growth-2021/

Chromebook Market Growth



Brand	Units Sold 2020
HP	4.3 Million
Lenovo	3.1 Million
Acer	1+ Million
Dell	1+ Million
Samsung	1+ Million

Varied Specs

Samsung Chromebook 4

- 32GB eMMC, 4GB RAM, Intel Celeron - $186

Pixelbook

- 512GB SSD, 16GB RAM, Intel Core i7 - $1700

Why do we care?

- Schools!
- Bad Guys!
- Enterprise!

Research Evolution

1 x Registration
Order total: Free

Thursday, November 14, 2019 from 9:00 AM to 4:00 PM (MST)
Add to Google · Outlook · iCal · Yahoo

- VTO Brews and Bytes event in Nov 2019
- Focused on Chromebooks

Brews & Bytes Event Focus Areas

- Acquisition
- Analysis
- Hardware Analysis
- Legal

Data Acquisition

Acquisition

COMPUTER

CLOUD

Multiple sources of data from Google Chromebooks

Device

- Decrypted Logical Backup of Chrome (username/password)
- Full physical imaging (Developer Mode, Chip-off)

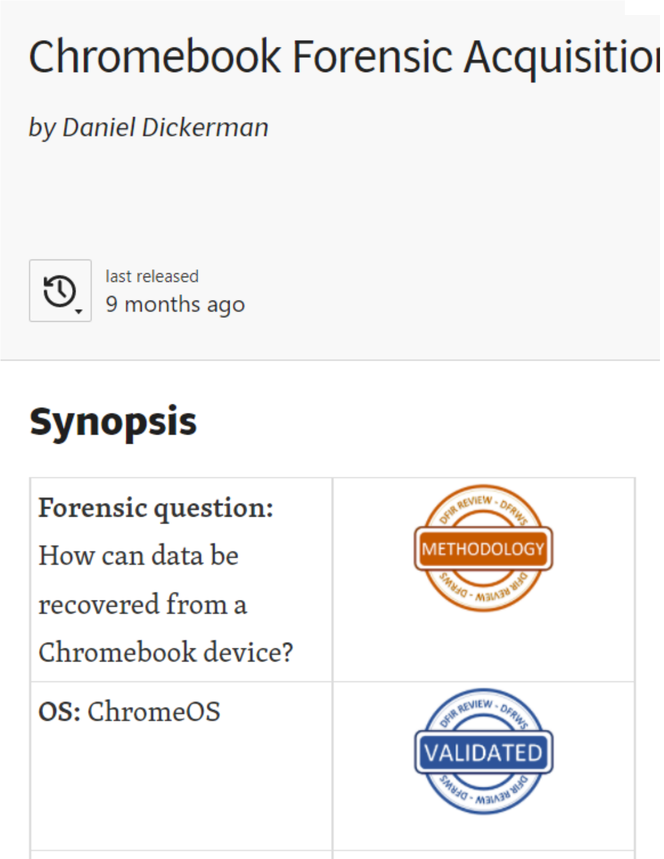
Cloud

- Takeout (consent - username/password)
- Cloud Acquisition (token, username/password)
- Warrant Return

Chromebook Acquisition

Acquisition – Chromebook Device

- Password?
  - Daniel Dickerman Method (dfir.pubpub.org)
- No Password?
  - Dev Mode
  - Placing a device in this mode will wipe the device



Chromebook Forensic Acquisitio

by Daniel Dickerman

last released
9 months ago

Synopsis

Forensic question: How can data be recovered from a Chromebook device?	DFIR REVIEW - DFRWS METHODOLOGY DFRWS - DFIR REVIEW
OS: ChromeOS	DFIR REVIEW - DFRWS VALIDATED DFRWS - DFIR REVIEW

Acquisition

- Method from Daniel Dickerman – Validated Method
- Logical decrypted partition – with username and password
- Physical Clone if device is in Developer Mode

Daniel Dickerman method

- https://dfir.pubpub.org/pub/inkjsqrh/release/1
- Decrypted Logical
- 3 USBs
  - 1) Bootable Chromium OS USB
  - 2) Encrypted Partition Recovery USB
  - 3) Physical Cloning Recovery USB

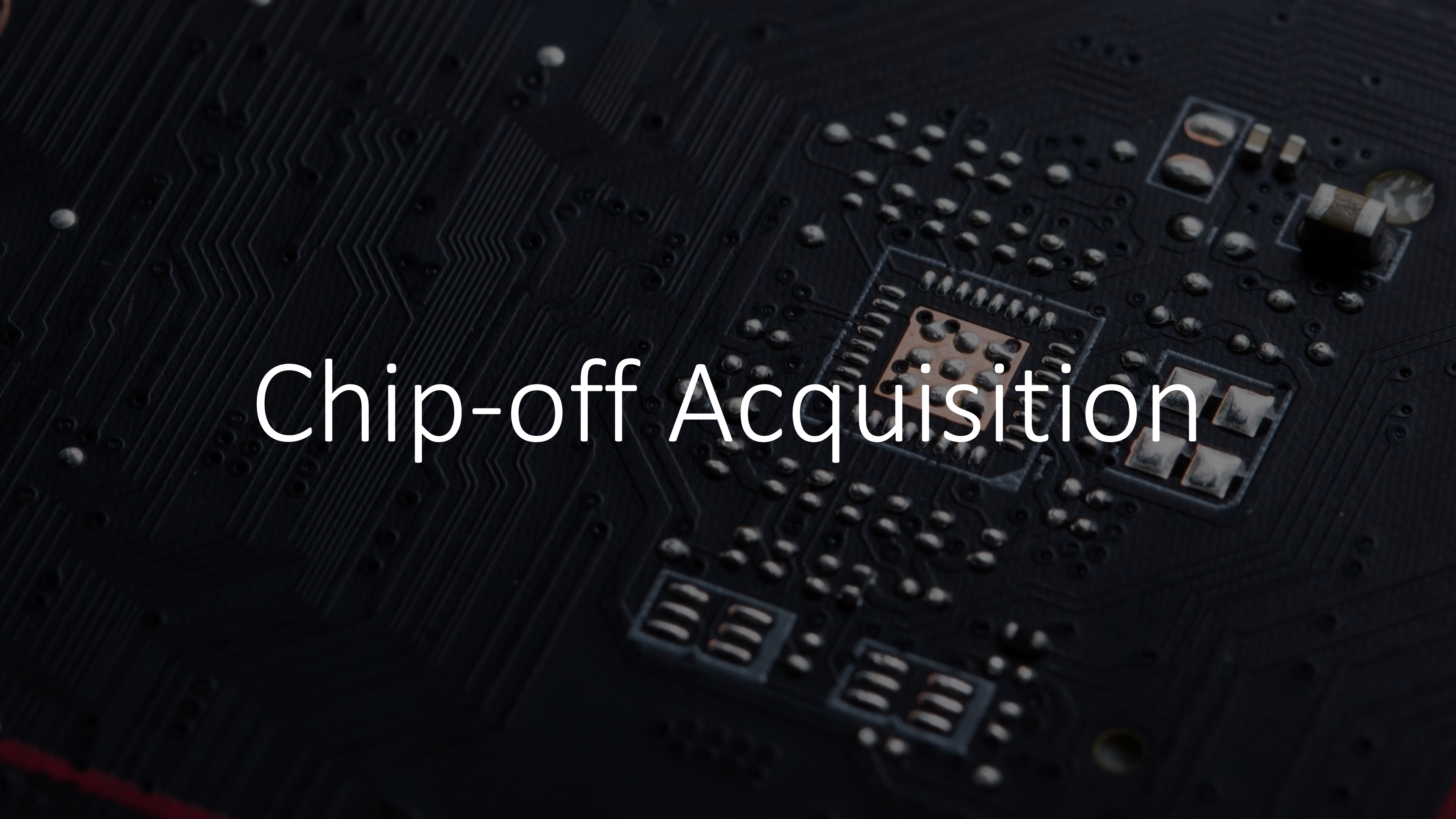
Top Tips for Acquisition!

- Yes, you need the username and passcode
- Do NOT enter any "."s in the username
- Validate language of the keyboard
- Use custom recovery version 87 recovery and below
- Like mobile not all devices have a custom recovery
- Recovery Partitions running out of space (needs to be enough free space on the device) - it will launch back to recovery screen (your partial should still be good!)
- Not all thumb drives will work for creating the recovery drive

THEY BROKE IT

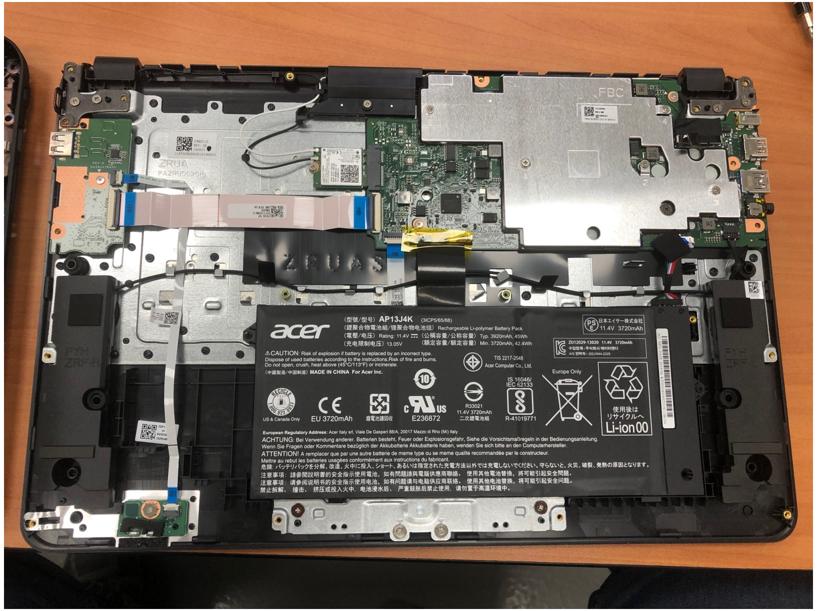
Google's update to Chrome OS version 100 breaks the Daniel Dickerman Method

Chip-off Acquisition



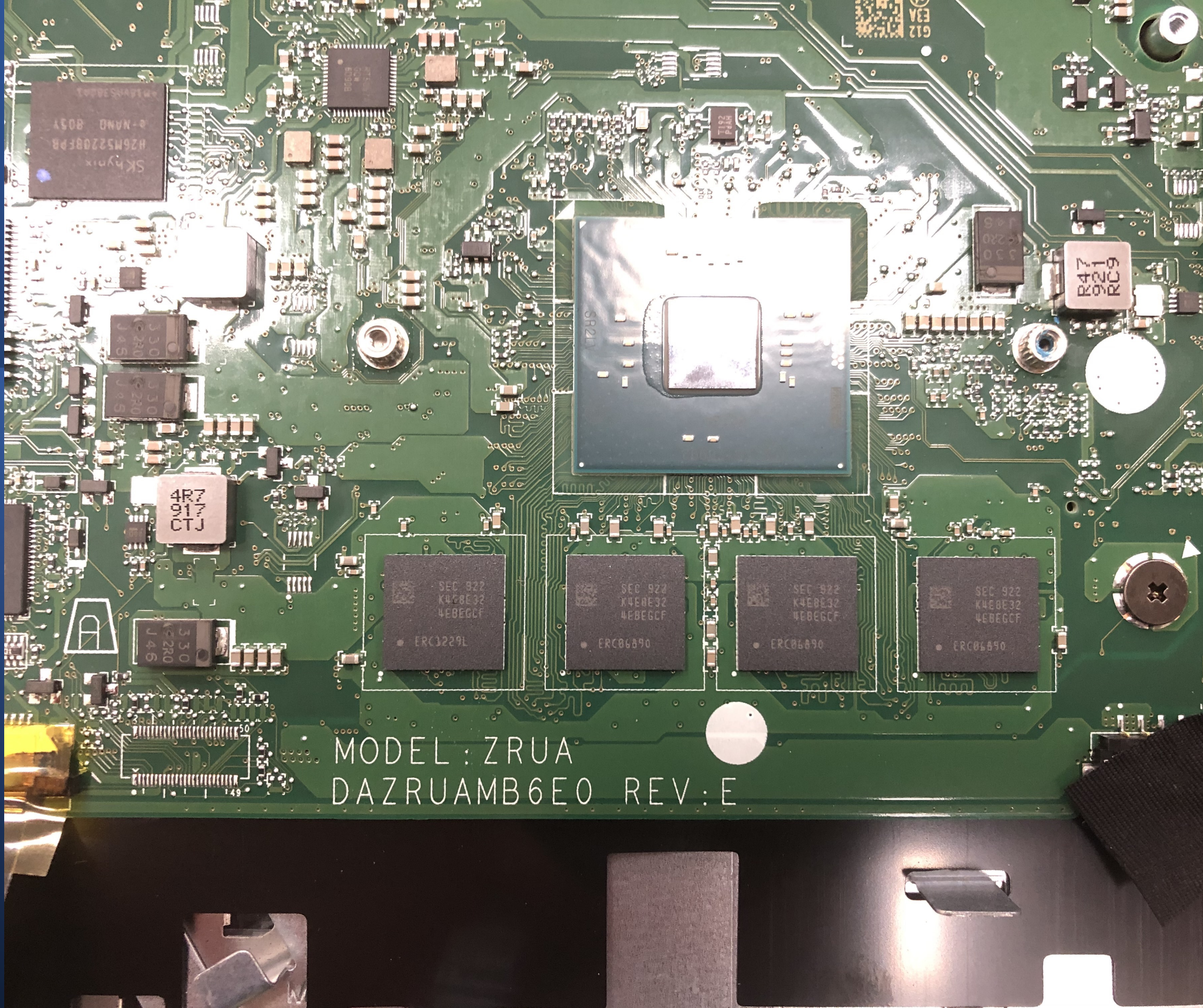
Hardware

Acer Chromebook N15Q9 - Teardown

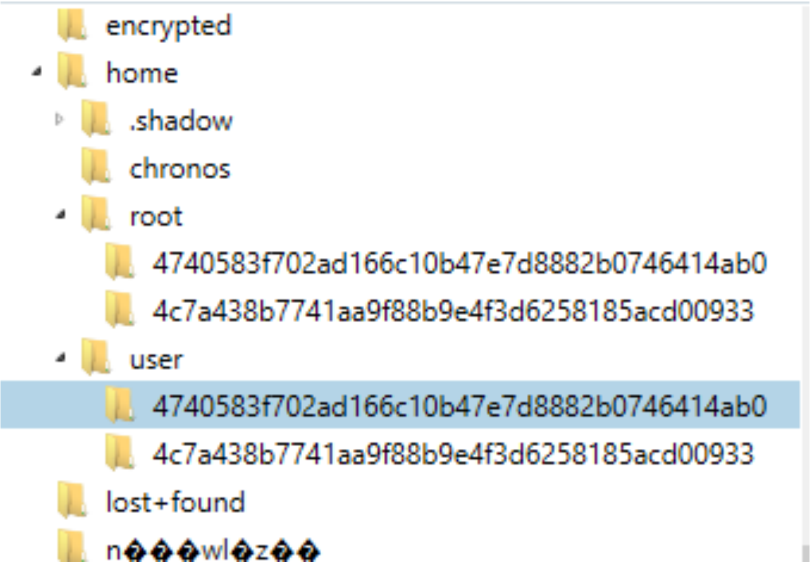


Acer Chromebook
N15Q9 - Teardown

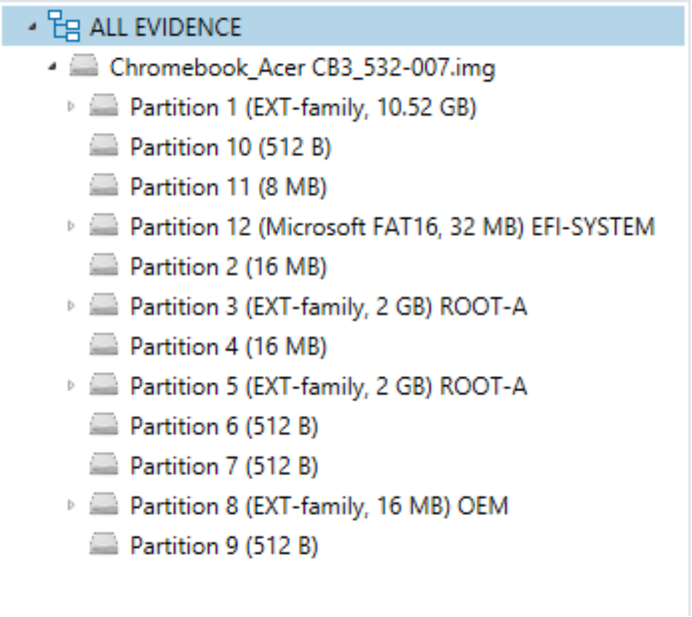
Hardware



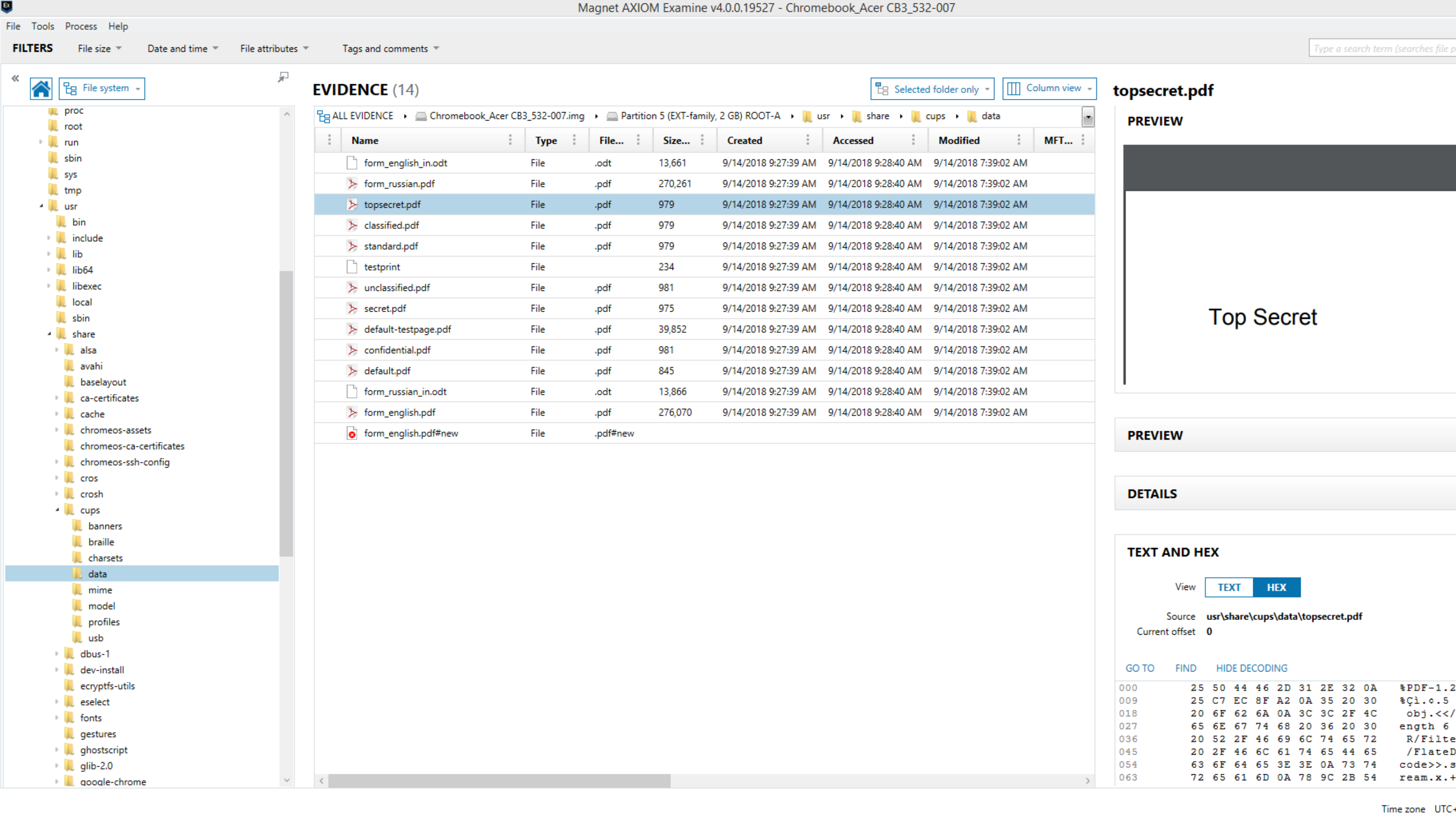
Images from chip-off



```
encrypted
home
  .shadow
  chronos
  root
    4740583f702ad166c10b47e7d8882b0746414ab0
    4c7a438b7741aa9f88b9e4f3d6258185acd00933
  user
    4740583f702ad166c10b47e7d8882b0746414ab0
    4c7a438b7741aa9f88b9e4f3d6258185acd00933
lost+found
n���wl�z��
```



```
ALL EVIDENCE
  Chromebook_Acer CB3_532-007.img
    Partition 1 (EXT-family, 10.52 GB)
    Partition 10 (512 B)
    Partition 11 (8 MB)
    Partition 12 (Microsoft FAT16, 32 MB) EFI-SYSTEM
    Partition 2 (16 MB)
    Partition 3 (EXT-family, 2 GB) ROOT-A
    Partition 4 (16 MB)
    Partition 5 (EXT-family, 2 GB) ROOT-A
    Partition 6 (512 B)
    Partition 7 (512 B)
    Partition 8 (EXT-family, 16 MB) OEM
    Partition 9 (512 B)
```



EVIDENCE (14)

ALL EVIDENCE ▸ Chromebook_Acer CB3_532-007.img ▸ Partition 5 (EXT-family, 2 GB) ROOT-A ▸ usr ▸ share ▸ cups ▸ data

Name	Type	File...	Size...	Created	Accessed	Modified	MFT...
form_english_in.odt	File	.odt	13,661	9/14/2018 9:27:39 AM	9/14/2018 9:28:40 AM	9/14/2018 7:39:02 AM	
form_russian.pdf	File	.pdf	270,261	9/14/2018 9:27:39 AM	9/14/2018 9:28:40 AM	9/14/2018 7:39:02 AM	
topsecret.pdf	File	.pdf	979	9/14/2018 9:27:39 AM	9/14/2018 9:28:40 AM	9/14/2018 7:39:02 AM	
classified.pdf	File	.pdf	979	9/14/2018 9:27:39 AM	9/14/2018 9:28:40 AM	9/14/2018 7:39:02 AM	
standard.pdf	File	.pdf	979	9/14/2018 9:27:39 AM	9/14/2018 9:28:40 AM	9/14/2018 7:39:02 AM	
testprint	File		234	9/14/2018 9:27:39 AM	9/14/2018 9:28:40 AM	9/14/2018 7:39:02 AM	
unclassified.pdf	File	.pdf	981	9/14/2018 9:27:39 AM	9/14/2018 9:28:40 AM	9/14/2018 7:39:02 AM	
secret.pdf	File	.pdf	975	9/14/2018 9:27:39 AM	9/14/2018 9:28:40 AM	9/14/2018 7:39:02 AM	
default-testpage.pdf	File	.pdf	39,852	9/14/2018 9:27:39 AM	9/14/2018 9:28:40 AM	9/14/2018 7:39:02 AM	
confidential.pdf	File	.pdf	981	9/14/2018 9:27:39 AM	9/14/2018 9:28:40 AM	9/14/2018 7:39:02 AM	
default.pdf	File	.pdf	845	9/14/2018 9:27:39 AM	9/14/2018 9:28:40 AM	9/14/2018 7:39:02 AM	
form_russian_in.odt	File	.odt	13,866	9/14/2018 9:27:39 AM	9/14/2018 9:28:40 AM	9/14/2018 7:39:02 AM	
form_english.pdf	File	.pdf	276,070	9/14/2018 9:27:39 AM	9/14/2018 9:28:40 AM	9/14/2018 7:39:02 AM	
form_english.pdf#new	File	.pdf#new					

topsecret.pdf

TEXT AND HEX

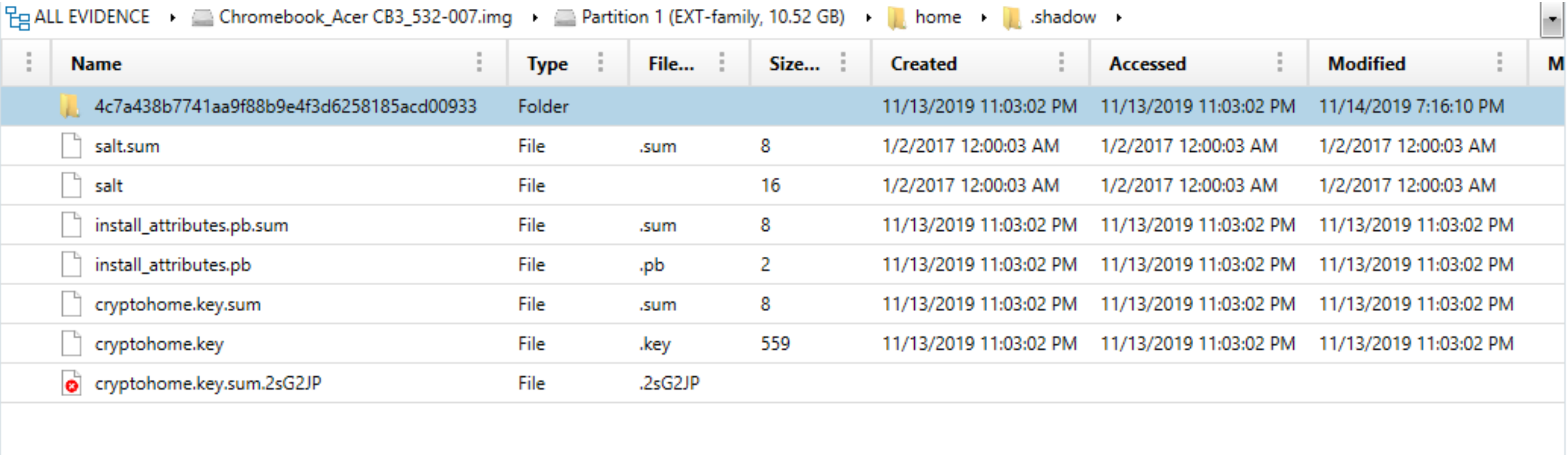
View TEXT HEX

Source usr\share\cups\data\topsecret.pdf

Current offset 0

```
000        25 50 44 46 2D 31 2E 32 0A   %PDF-1.2
009        25 C7 EC 8F A2 0A 35 20 30   %Çì.¢.5 
018        20 6F 62 6A 0A 3C 3C 2F 4C    obj.<</
027        65 6E 67 74 68 20 36 20 30   ength 6 
036        20 52 2F 46 69 6C 74 65 72    R/Filte
045        20 2F 46 6C 61 74 65 44 65    /FlateD
054        63 6F 64 65 3E 3E 0A 73 74   code>>.s
063        72 65 61 6D 0A 78 9C 2B 54   ream.x.+
```

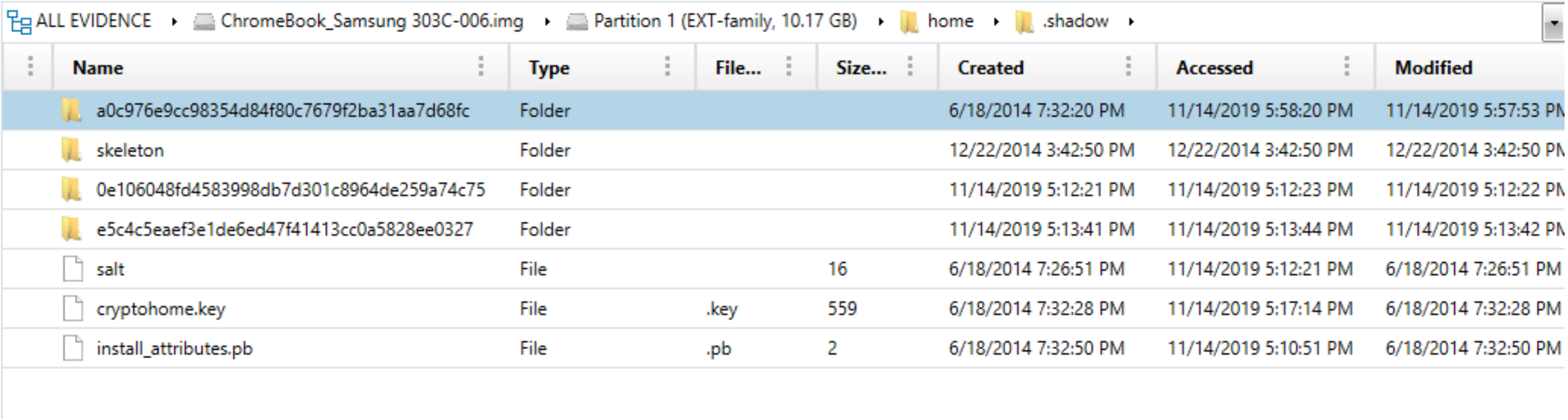
Acer CB-537



ALL EVIDENCE ▸ Chromebook_Acer CB3_532-007.img ▸ Partition 1 (EXT-family, 10.52 GB) ▸ home ▸ .shadow ▸

Name	Type	File...	Size...	Created	Accessed	Modified	M
4c7a438b7741aa9f88b9e4f3d6258185acd00933	Folder			11/13/2019 11:03:02 PM	11/13/2019 11:03:02 PM	11/14/2019 7:16:10 PM	
salt.sum	File	.sum	8	1/2/2017 12:00:03 AM	1/2/2017 12:00:03 AM	1/2/2017 12:00:03 AM	
salt	File		16	1/2/2017 12:00:03 AM	1/2/2017 12:00:03 AM	1/2/2017 12:00:03 AM	
install_attributes.pb.sum	File	.sum	8	11/13/2019 11:03:02 PM	11/13/2019 11:03:02 PM	11/13/2019 11:03:02 PM	
install_attributes.pb	File	.pb	2	11/13/2019 11:03:02 PM	11/13/2019 11:03:02 PM	11/13/2019 11:03:02 PM	
cryptohome.key.sum	File	.sum	8	11/13/2019 11:03:02 PM	11/13/2019 11:03:02 PM	11/13/2019 11:03:02 PM	
cryptohome.key	File	.key	559	11/13/2019 11:03:02 PM	11/13/2019 11:03:02 PM	11/13/2019 11:03:02 PM	
cryptohome.key.sum.2sG2JP	File	.2sG2JP					

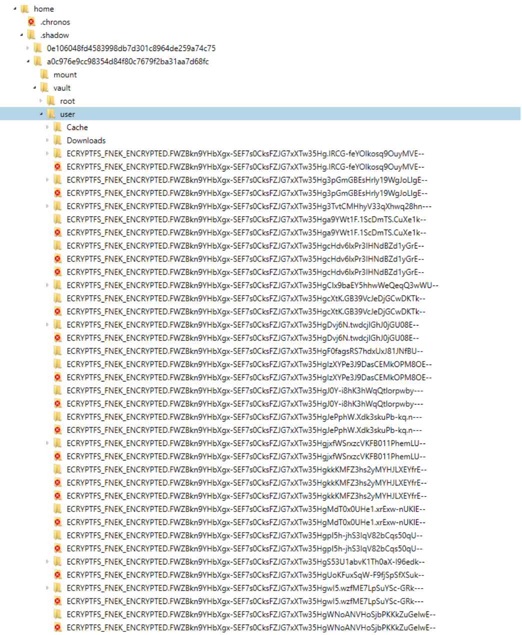
Samsung 303C



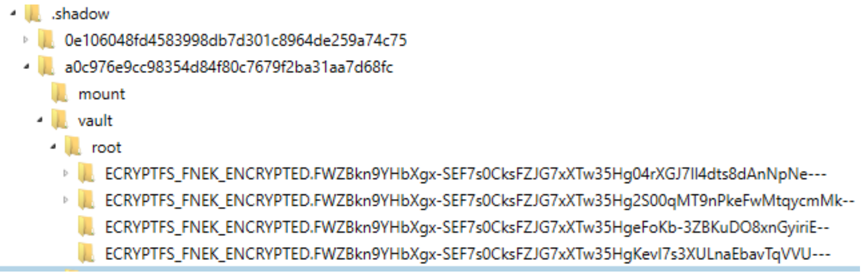
ALL EVIDENCE ▸ ChromeBook_Samsung 303C-006.img ▸ Partition 1 (EXT-family, 10.17 GB) ▸ home ▸ .shadow ▸

Name	Type	File...	Size...	Created	Accessed	Modified
a0c976e9cc98354d84f80c7679f2ba31aa7d68fc	Folder			6/18/2014 7:32:20 PM	11/14/2019 5:58:20 PM	11/14/2019 5:57:53 PM
skeleton	Folder			12/22/2014 3:42:50 PM	12/22/2014 3:42:50 PM	12/22/2014 3:42:50 PM
0e106048fd4583998db7d301c8964de259a74c75	Folder			11/14/2019 5:12:21 PM	11/14/2019 5:12:23 PM	11/14/2019 5:12:22 PM
e5c4c5eaef3e1de6ed47f41413cc0a5828ee0327	Folder			11/14/2019 5:13:41 PM	11/14/2019 5:13:44 PM	11/14/2019 5:13:42 PM
salt	File		16	6/18/2014 7:26:51 PM	11/14/2019 5:12:21 PM	6/18/2014 7:26:51 PM
cryptohome.key	File	.key	559	6/18/2014 7:32:28 PM	11/14/2019 5:17:14 PM	6/18/2014 7:32:28 PM
install_attributes.pb	File	.pb	2	6/18/2014 7:32:50 PM	11/14/2019 5:10:51 PM	6/18/2014 7:32:50 PM

Samsung 303C

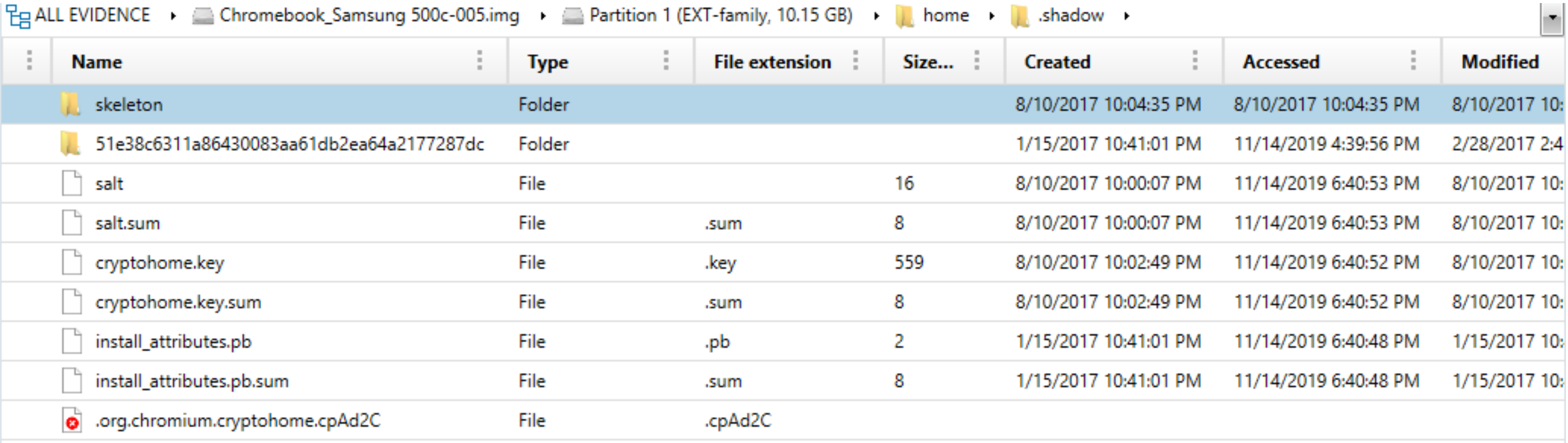


```
home
  .chronos
  .shadow
    0e106048fd4583998db7d301c8964de259a74c75
    a0c976e9cc98354d84f80c7679f2ba31aa7d68fc
      mount
      vault
        root
        user
          Cache
          Downloads
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35Hg.IRCG-feYOlkosq9OuyMVE--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35Hg.IRCG-feYOlkosq9OuyMVE--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35Hg3pGmGBEsHrly19WgJoLlgE--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35Hg3pGmGBEsHrly19WgJoLlgE--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35Hg3TvtCMHhyV33qXhwq28hn---
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35Hga9YWt1F.1ScDmTS.CuXe1k--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35Hga9YWt1F.1ScDmTS.CuXe1k--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgcHdv6lxPr3IHNdBZd1yGrE--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgcHdv6lxPr3IHNdBZd1yGrE--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgcHdv6lxPr3IHNdBZd1yGrE--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgClx9baEY5hhwWeQeqQ3wWU--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgcXtK.GB39VcJeDjGCwDKTk--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgcXtK.GB39VcJeDjGCwDKTk--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgDvj6N.twdcjlGhJ0jGU08E--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgDvj6N.twdcjlGhJ0jGU08E--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgF0fagsRS7hdxUxJ81JNfBU--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HglzXYPe3J9DasCEMkOPM8OE--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HglzXYPe3J9DasCEMkOPM8OE--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgJ0Y-i8hK3hWqQtlorpwby---
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgJ0Y-i8hK3hWqQtlorpwby---
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgJePphW.Xdk3skuPb-kq.n---
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgJePphW.Xdk3skuPb-kq.n---
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgjxfWSrxzcVKFB011PhemLU--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgjxfWSrxzcVKFB011PhemLU--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgkkKMFZ3hs2yMYHJLXEYfrE--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgkkKMFZ3hs2yMYHJLXEYfrE--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgkkKMFZ3hs2yMYHJLXEYfrE--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgMdT0x0UHe1.xrExw-nUKIE--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgMdT0x0UHe1.xrExw-nUKIE--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgpI5h-jhS3lqV82bCqs50qU--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgpI5h-jhS3lqV82bCqs50qU--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgS53U1abvK1Th0aX-l96edk--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgUoKFuxSqW-F9fjSpSfXSuk--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35Hgwl5.wzfME7LpSuYSc-GRk---
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35Hgwl5.wzfME7LpSuYSc-GRk---
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgWNoANVHoSjbPKKkZuGelwE--
          ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgWNoANVHoSjbPKKkZuGelwE--
```



```
.shadow
  0e106048fd4583998db7d301c8964de259a74c75
  a0c976e9cc98354d84f80c7679f2ba31aa7d68fc
    mount
    vault
      root
        ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35Hg04rXGJ7Il4dts8dAnNpNe---
        ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35Hg2S00qMT9nPkeFwMtqycmMk--
        ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgeFoKb-3ZBKuDO8xnGyiriE--
        ECRYPTFS_FNEK_ENCRYPTED.FWZBkn9YHbXgx-SEF7s0CksFZJG7xXTw35HgKevl7s3XULnaEbavTqVVU---
```

Samsung 500c



ALL EVIDENCE ▸ Chromebook_Samsung 500c-005.img ▸ Partition 1 (EXT-family, 10.15 GB) ▸ home ▸ .shadow ▸

Name	Type	File extension	Size...	Created	Accessed	Modified
skeleton	Folder			8/10/2017 10:04:35 PM	8/10/2017 10:04:35 PM	8/10/2017 10:
51e38c6311a86430083aa61db2ea64a2177287dc	Folder			1/15/2017 10:41:01 PM	11/14/2019 4:39:56 PM	2/28/2017 2:4
salt	File		16	8/10/2017 10:00:07 PM	11/14/2019 6:40:53 PM	8/10/2017 10:
salt.sum	File	.sum	8	8/10/2017 10:00:07 PM	11/14/2019 6:40:53 PM	8/10/2017 10:
cryptohome.key	File	.key	559	8/10/2017 10:02:49 PM	11/14/2019 6:40:52 PM	8/10/2017 10:
cryptohome.key.sum	File	.sum	8	8/10/2017 10:02:49 PM	11/14/2019 6:40:52 PM	8/10/2017 10:
install_attributes.pb	File	.pb	2	1/15/2017 10:41:01 PM	11/14/2019 6:40:48 PM	1/15/2017 10:
install_attributes.pb.sum	File	.sum	8	1/15/2017 10:41:01 PM	11/14/2019 6:40:48 PM	1/15/2017 10:
.org.chromium.cryptohome.cpAd2C	File	.cpAd2C				

Cloud Acquisition

Acquisition - Cloud

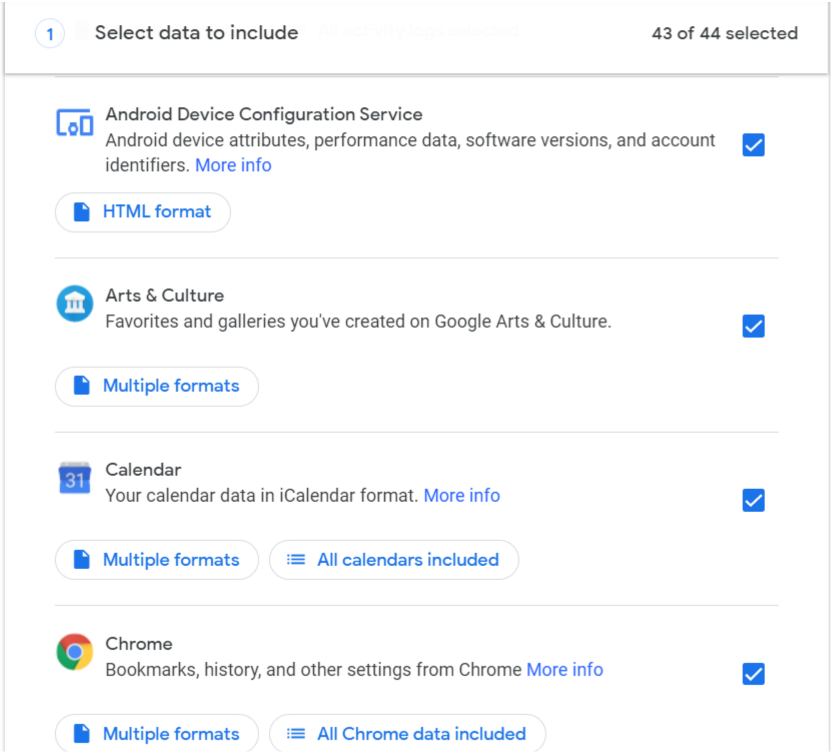
- Takeout (Credentials, Notification, Consent)
- Commercial Acquisition
- Warrant
  - https://support.google.com/transparencyreport/answer/9713961?hl=en&visit_id=637586521246082490-2603265576&rd=1
- Google Workspace via the Google Admin Data Export Tool

Takeout Acquisition

What do you need?

- Typically consent
- Username and password
- Access to 2FA
- Access to Gmail (notification when available)
- Understand notification will occur
- May want a warrant return instead

Creating a Takeout



1 Select data to include — 43 of 44 selected

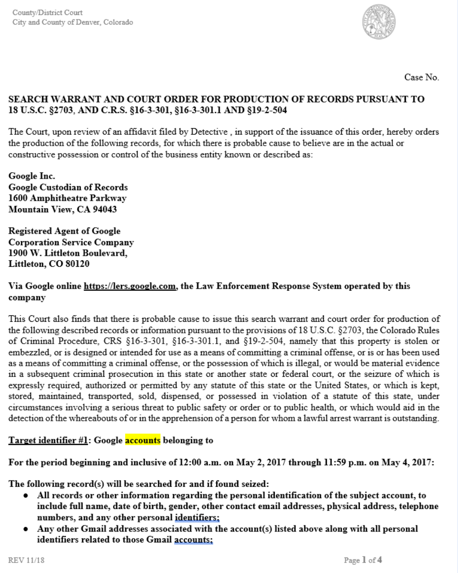
Android Device Configuration Service ☑
Android device attributes, performance data, software versions, and account identifiers. More info
HTML format

Arts & Culture ☑
Favorites and galleries you've created on Google Arts & Culture.
Multiple formats

Calendar ☑
Your calendar data in iCalendar format. More info
Multiple formats | All calendars included

Chrome ☑
Bookmarks, history, and other settings from Chrome More info
Multiple formats | All Chrome data included

Legal VTO Event



County/District Court
City and County of Denver, Colorado

Case No.

SEARCH WARRANT AND COURT ORDER FOR PRODUCTION OF RECORDS PURSUANT TO 18 U.S.C. §2703, AND C.R.S. §16-3-301, §16-3-301.1 AND §19-2-504

The Court, upon review of an affidavit filed by Detective , in support of the issuance of this order, hereby orders the production of the following records, for which there is probable cause to believe are in the actual or constructive possession or control of the business entity known or described as:

Google Inc.
Google Custodian of Records
1600 Amphitheatre Parkway
Mountain View, CA 94043

Registered Agent of Google
Corporation Service Company
1900 W. Littleton Boulevard,
Littleton, CO 80120

Via Google online https://lers.google.com, the Law Enforcement Response System operated by this company

This Court also finds that there is probable cause to issue this search warrant and court order for production of the following described records or information pursuant to the provisions of 18 U.S.C. §2703, the Colorado Rules of Criminal Procedure, CRS §16-3-301, §16-3-301.1, and §19-2-504, namely that this property is stolen or embezzled, or is designed or intended for use as a means of committing a criminal offense, or is or has been used as a means of committing a criminal offense, or the possession of which is illegal, or would be material evidence in a subsequent criminal prosecution in this state or another state or federal court, or the seizure of which is expressly required, authorized or permitted by any statute of this state or the United States, or which is kept, stored, maintained, transported, sold, dispensed, or possessed in violation of a statute of this state, under circumstances involving a serious threat to public safety or order or to public health, or which would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest warrant is outstanding.

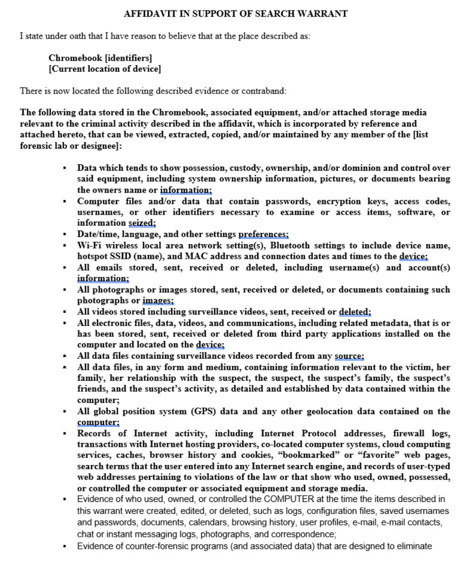
Target identifier #1: Google accounts belonging to

For the period beginning and inclusive of 12:00 a.m. on May 2, 2017 through 11:59 p.m. on May 4, 2017:

The following record(s) will be searched for and if found seized:

- **All records or other information regarding the personal identification of the subject account, to include full name, date of birth, gender, other contact email addresses, physical address, telephone numbers, and any other personal identifiers;**
- **Any other Gmail addresses associated with the account(s) listed above along with all personal identifiers related to those Gmail accounts;**

REV 11/18 Page 1 of 4



AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I state under oath that I have reason to believe that at the place described as:

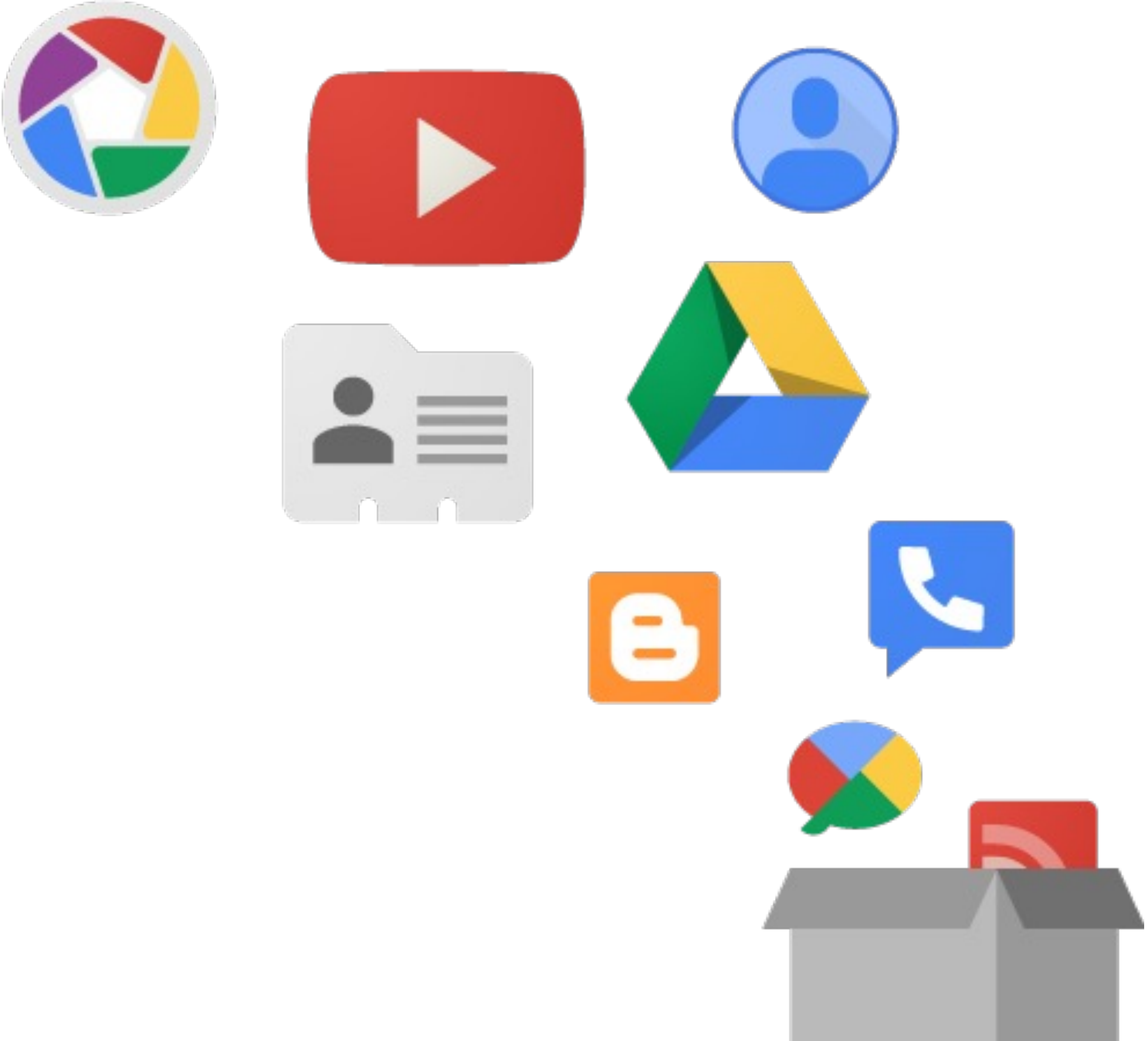
Chromebook [identifiers]
[Current location of device]

There is now located the following described evidence or contraband:

The following data stored in the Chromebook, associated equipment, and/or attached storage media relevant to the criminal activity described in the affidavit, which is incorporated by reference and attached hereto, that can be viewed, extracted, copied, and/or maintained by any member of the [list forensic lab or designee]:

- **Data which tends to show possession, custody, ownership, and/or dominion and control over said equipment, including system ownership information, pictures, or documents bearing the owners name or information;**
- **Computer files and/or data that contain passwords, encryption keys, access codes, usernames, or other identifiers necessary to examine or access items, software, or information seized;**
- **Date/time, language, and other settings preferences;**
- **Wi-Fi wireless local area network setting(s), Bluetooth settings to include device name, hotspot SSID (name), and MAC address and connection dates and times to the device;**
- **All emails stored, sent, received or deleted, including username(s) and account(s) information;**
- **All photographs or images stored, sent, received or deleted, or documents containing such photographs or images;**
- **All videos stored including surveillance videos, sent, received or deleted;**
- **All electronic files, data, videos, and communications, including related metadata, that is or has been stored, sent, received or deleted from third party applications installed on the computer and located on the device;**
- **All data files containing surveillance videos recorded from any source;**
- **All data files, in any form and medium, containing information relevant to the victim, her family, her relationship with the suspect, the suspect, the suspect's family, the suspect's friends, and the suspect's activity, as detailed and established by data contained within the computer;**
- **All global position system (GPS) data and any other geolocation data contained on the computer;**
- **Records of Internet activity, including Internet Protocol addresses, firewall logs, transactions with Internet hosting providers, co-located computer systems, cloud computing services, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses pertaining to violations of the law or that show who used, owned, possessed, or controlled the computer or associated equipment and storage media.**
- Evidence of who used, owned, or controlled the COMPUTER at the time the items described in this warrant were created, edited, or deleted, such as logs, configuration files, saved usernames and passwords, documents, calendars, browsing history, user profiles, e-mail, e-mail contacts, chat or instant messaging logs, photographs, and correspondence;
- Evidence of counter-forensic programs (and associated data) that are designed to eliminate

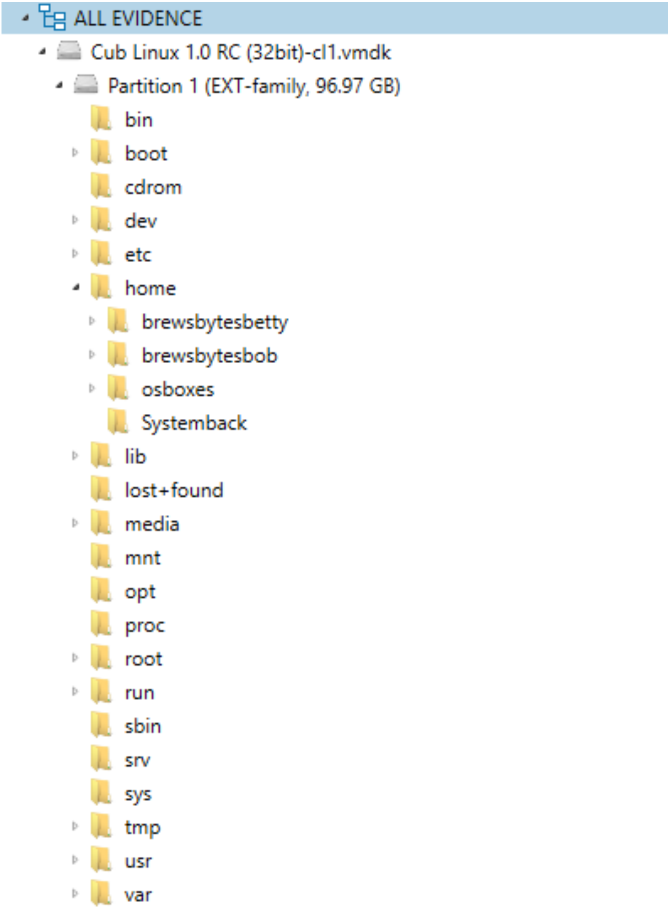
- Draft Documents
- Chromebook Device Template
- Chromebook GoBy
- Google Affidavit
- Google Warrant



Analysis

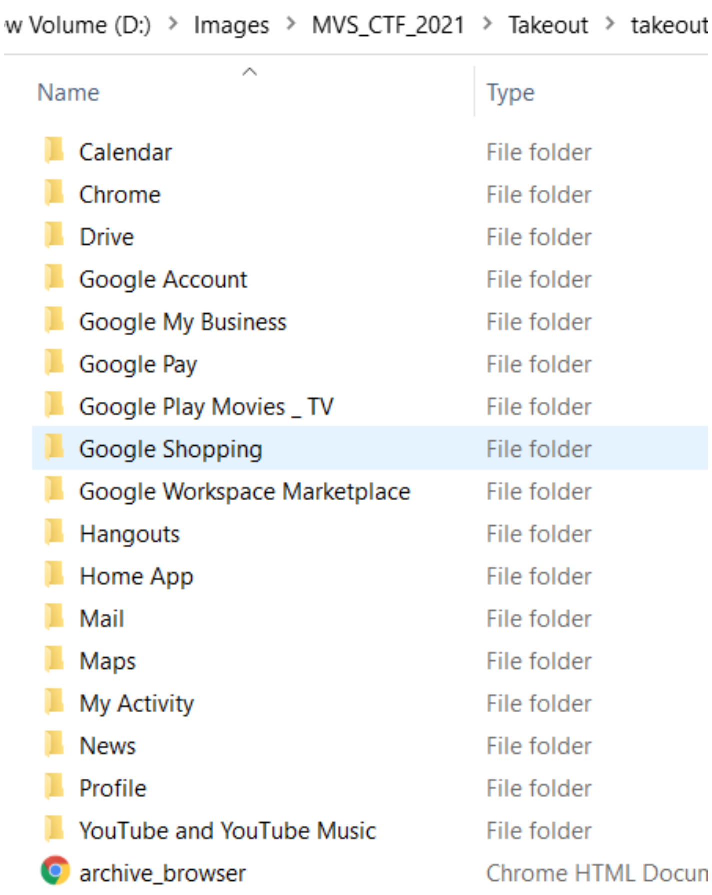
A comparative analysis of data recovered from a logical acquisition of Chromebook as compared to data from a Google Takeout

Logical Chromebook Acquisition



ALL EVIDENCE
- Cub Linux 1.0 RC (32bit)-cl1.vmdk
  - Partition 1 (EXT-family, 96.97 GB)
    - bin
    - boot
    - cdrom
    - dev
    - etc
    - home
      - brewsbytesbetty
      - brewsbytesbob
      - osboxes
      - Systemback
    - lib
    - lost+found
    - media
    - mnt
    - opt
    - proc
    - root
    - run
    - sbin
    - srv
    - sys
    - tmp
    - usr
    - var

What is in the Takeout .zip?



w Volume (D:) › Images › MVS_CTF_2021 › Takeout › takeout

Name	Type
Calendar	File folder
Chrome	File folder
Drive	File folder
Google Account	File folder
Google My Business	File folder
Google Pay	File folder
Google Play Movies _ TV	File folder
Google Shopping	File folder
Google Workspace Marketplace	File folder
Hangouts	File folder
Home App	File folder
Mail	File folder
Maps	File folder
My Activity	File folder
News	File folder
Profile	File folder
YouTube and YouTube Music	File folder
archive_browser	Chrome HTML Docun

Artifacts

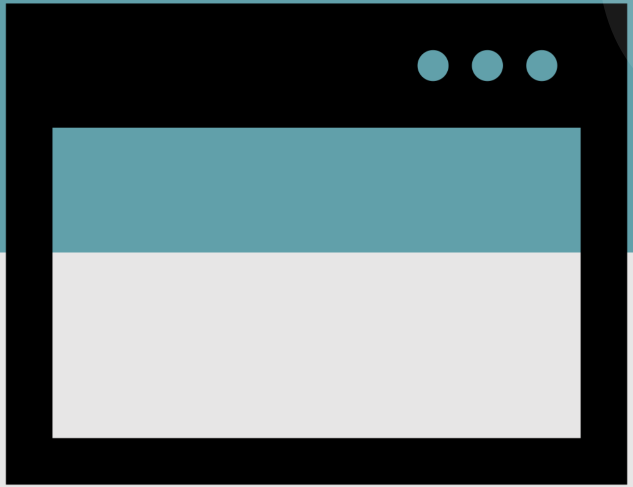
BROWSER

GEOLOCATION

MAIL

SYSTEM

Browser

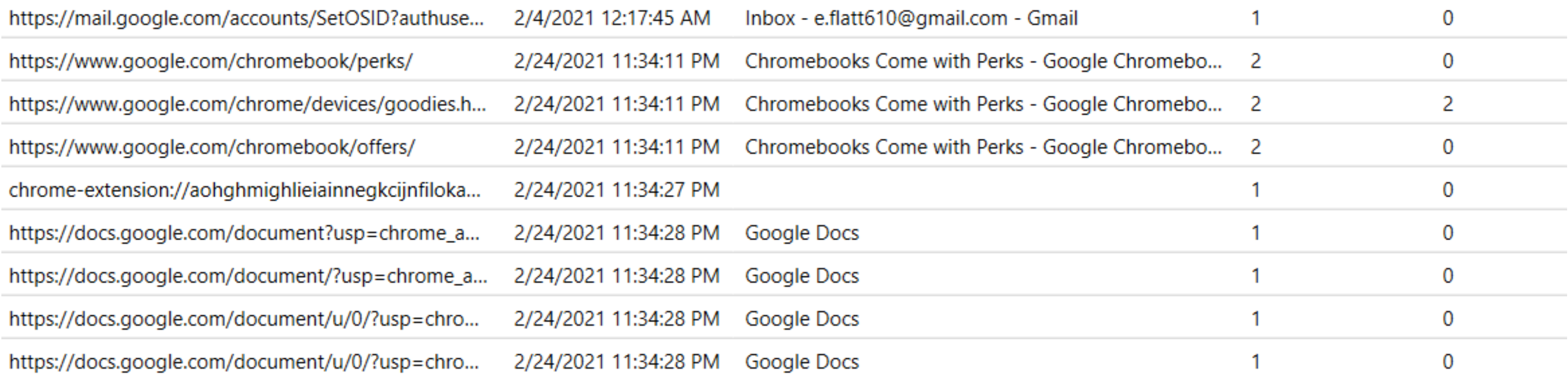


Browser History

- Each entry appears in the following paths
  - \home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\History
  - \home\chronos\user\History
  - \home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\History
  - \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\History

  OR
  - \home\brewsbytesbetty\.config\chromium\Default\History
- SQLite DB

Web History Chromebook



https://mail.google.com/accounts/SetOSID?authuse...	2/4/2021 12:17:45 AM	Inbox - e.flatt610@gmail.com - Gmail	1	0
https://www.google.com/chromebook/perks/	2/24/2021 11:34:11 PM	Chromebooks Come with Perks - Google Chromebo...	2	0
https://www.google.com/chrome/devices/goodies.h...	2/24/2021 11:34:11 PM	Chromebooks Come with Perks - Google Chromebo...	2	2
https://www.google.com/chromebook/offers/	2/24/2021 11:34:11 PM	Chromebooks Come with Perks - Google Chromebo...	2	0
chrome-extension://aohghmighlieiainnegkcijnfiloka...	2/24/2021 11:34:27 PM		1	0
https://docs.google.com/document?usp=chrome_a...	2/24/2021 11:34:28 PM	Google Docs	1	0
https://docs.google.com/document/?usp=chrome_a...	2/24/2021 11:34:28 PM	Google Docs	1	0
https://docs.google.com/document/u/0/?usp=chro...	2/24/2021 11:34:28 PM	Google Docs	1	0
https://docs.google.com/document/u/0/?usp=chro...	2/24/2021 11:34:28 PM	Google Docs	1	0

Browser Cache

- Each entry appears in the following paths
  - \home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\Cache
  - \home\chronos\user\Cache
  - \home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\Cache
  - \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Cache

  OR
  - \home\brewsbytesbetty\.cache\chromium\Default\Cache\data_1
- Contains individual files with guids for each cache

Browser History – Current Tabs

- Each entry appears in the following paths
- Can parse with your favorite chrome browser parser/carver
  - \home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\Current Tabs
  - \home\chronos\user\Current Tabs
  - \home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\Current Tabs
  - \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Current Tabs

OR

  - \home\brewsbytesbetty\.config\chromium\Default\Current Tabs

Browser History – Last Tabs

- Each entry appears in the following paths
  - \home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\Last Tabs
  - \home\chronos\user\Last Tabs
  - \home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\Last Tabs
  - \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Last Tabs

OR

  - \home\brewsbytesbetty\.config\chromium\Default\Last Tabs

Browser History – Current Sessions

- Each entry appears in the following paths
  - \home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\Current Sessions
  - \home\chronos\user\Current Sessions
  - \home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\Current Sessions
  - \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Current Sessions

  OR
  - \home\<username>\.config\Chromium\Default\CurrentSession

Browser History – Last Sessions

- Each entry appears in the following paths
  - \home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\Last Sessions
  - \home\chronos\user\Last Sessions
  - \home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\Last Sessions
  - \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Last Sessions

OR

  - \home\brewsbytesbetty\.config\chromium\Default\Last Session

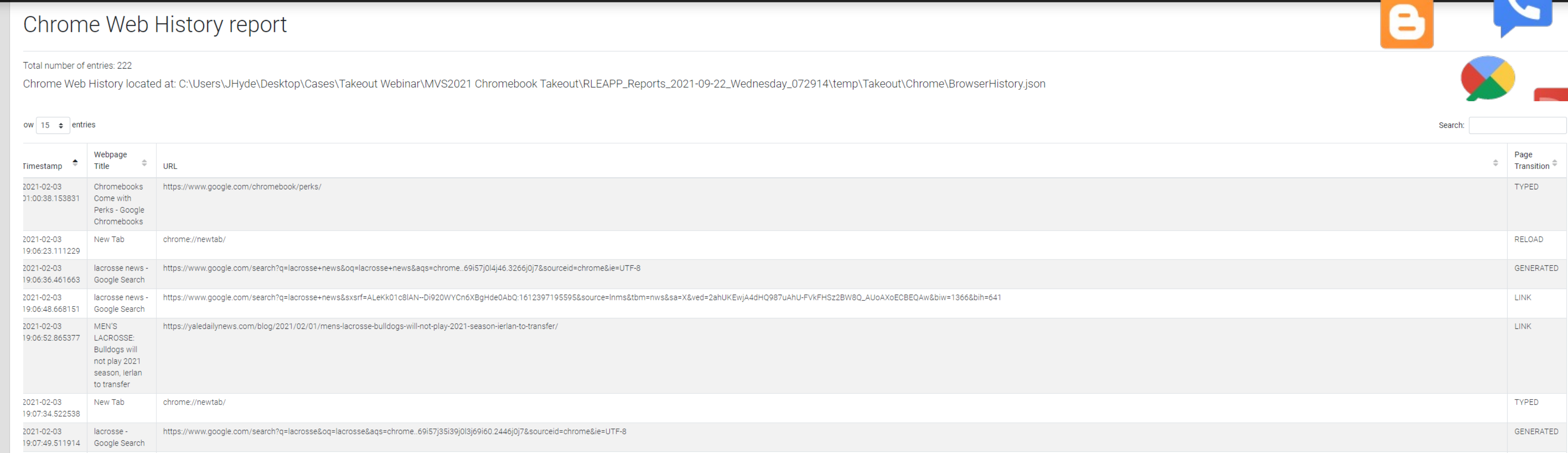
Chrome Artifacts

Takeout\Chrome\Bookmarks.html

Takeout\Chrome\BrowserHistory.json

Takeout\Chrome\SyncSettings.json

Chrome Browser History



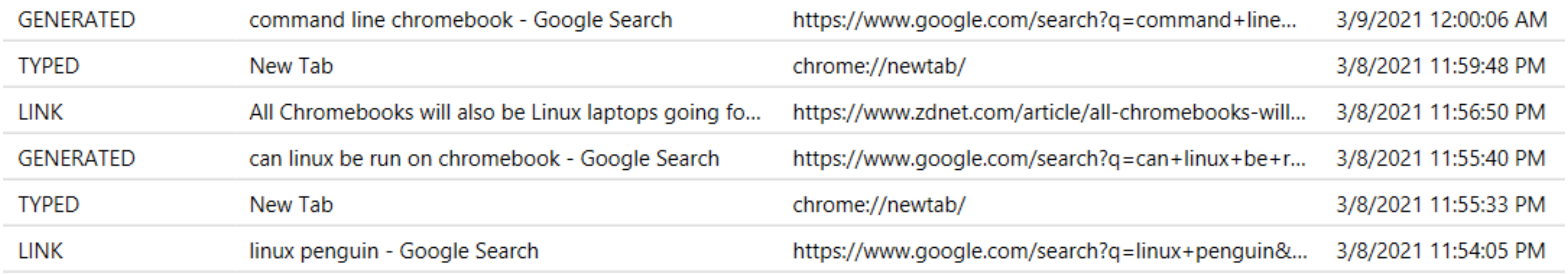
Chrome Web History report

Total number of entries: 222

Chrome Web History located at: C:\Users\JHyde\Desktop\Cases\Takeout Webinar\MVS2021 Chromebook Takeout\RLEAPP_Reports_2021-09-22_Wednesday_072914\temp\Takeout\Chrome\BrowserHistory.json

Timestamp	Webpage Title	URL	Page Transition
2021-02-03 01:00:38.153831	Chromebooks Come with Perks - Google Chromebooks	https://www.google.com/chromebook/perks/	TYPED
2021-02-03 19:06:23.111229	New Tab	chrome://newtab/	RELOAD
2021-02-03 19:06:36.461663	lacrosse news - Google Search	https://www.google.com/search?q=lacrosse+news&oq=lacrosse+news&aqs=chrome..69i57j0l4j46.3266j0j7&sourceid=chrome&ie=UTF-8	GENERATED
2021-02-03 19:06:48.668151	lacrosse news - Google Search	https://www.google.com/search?q=lacrosse+news&sxsrf=ALeKk01c8lAN--Di920WYCn6XBgHde0AbQ:1612397195595&source=lnms&tbm=nws&sa=X&ved=2ahUKEwjA4dHQ987uAhU-FVkFHSz2BW8Q_AUoAXoECBEQAw&biw=1366&bih=641	LINK
2021-02-03 19:06:52.865377	MEN'S LACROSSE: Bulldogs will not play 2021 season, Ierlan to transfer	https://yaledailynews.com/blog/2021/02/01/mens-lacrosse-bulldogs-will-not-play-2021-season-ierlan-to-transfer/	LINK
2021-02-03 19:07:34.522538	New Tab	chrome://newtab/	TYPED
2021-02-03 19:07:49.511914	lacrosse - Google Search	https://www.google.com/search?q=lacrosse&oq=lacrosse&aqs=chrome..69i57j35i39j0l3j69i60.2446j0j7&sourceid=chrome&ie=UTF-8	GENERATED

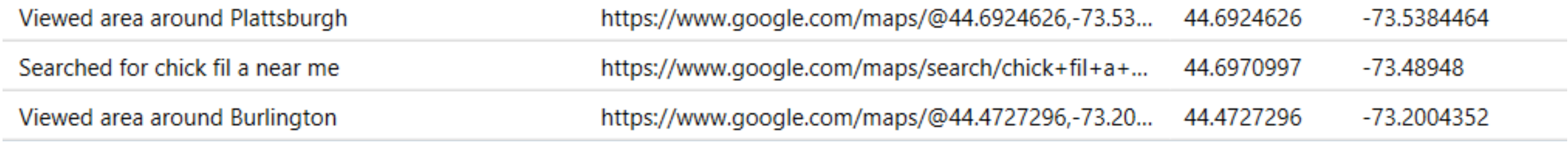
Browser History from Takeout



GENERATED	command line chromebook - Google Search	https://www.google.com/search?q=command+line...	3/9/2021 12:00:06 AM
TYPED	New Tab	chrome://newtab/	3/8/2021 11:59:48 PM
LINK	All Chromebooks will also be Linux laptops going fo...	https://www.zdnet.com/article/all-chromebooks-will...	3/8/2021 11:56:50 PM
GENERATED	can linux be run on chromebook - Google Search	https://www.google.com/search?q=can+linux+be+r...	3/8/2021 11:55:40 PM
TYPED	New Tab	chrome://newtab/	3/8/2021 11:55:33 PM
LINK	linux penguin - Google Search	https://www.google.com/search?q=linux+penguin&...	3/8/2021 11:54:05 PM

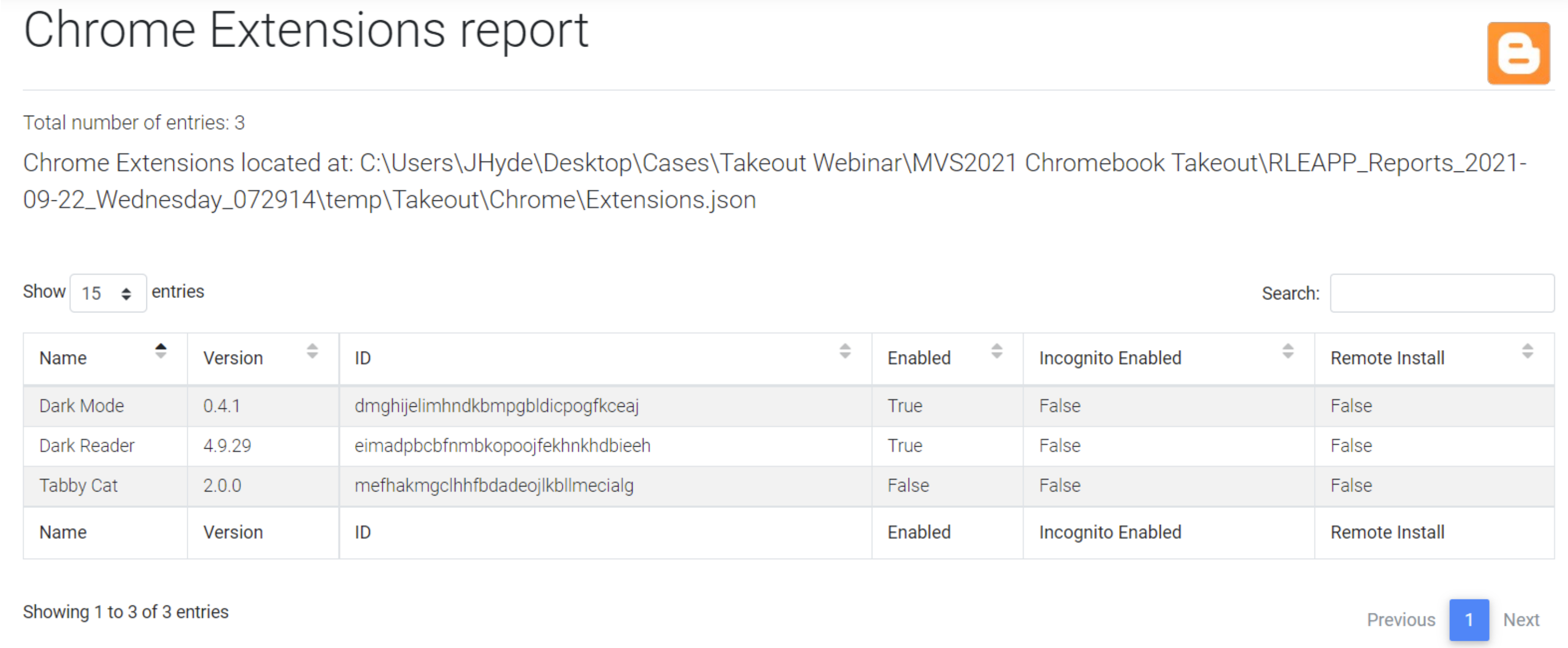
Advantage on Takeout

- Geolocations!



Viewed area around Plattsburgh	https://www.google.com/maps/@44.6924626,-73.53...	44.6924626	-73.5384464
Searched for chick fil a near me	https://www.google.com/maps/search/chick+fil+a+...	44.6970997	-73.48948
Viewed area around Burlington	https://www.google.com/maps/@44.4727296,-73.20...	44.4727296	-73.2004352

Chrome Extensions



Chrome Extensions report

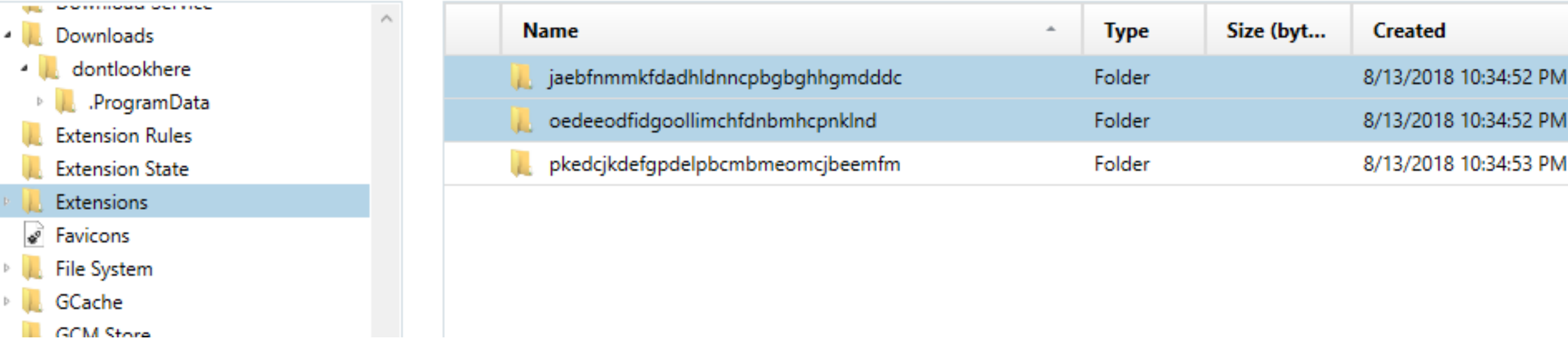
Total number of entries: 3

Chrome Extensions located at: C:\Users\JHyde\Desktop\Cases\Takeout Webinar\MVS2021 Chromebook Takeout\RLEAPP_Reports_2021-09-22_Wednesday_072914\temp\Takeout\Chrome\Extensions.json

Name	Version	ID	Enabled	Incognito Enabled	Remote Install
Dark Mode	0.4.1	dmghijelimhndkbmpgbldicpogfkceaj	True	False	False
Dark Reader	4.9.29	eimadpbcbfnmbkopoojfekhnkhdbieeh	True	False	False
Tabby Cat	2.0.0	mefhakmgclhhfbdadeojlkbllmecialg	False	False	False
Name	Version	ID	Enabled	Incognito Enabled	Remote Install

Showing 1 to 3 of 3 entries

Extensions

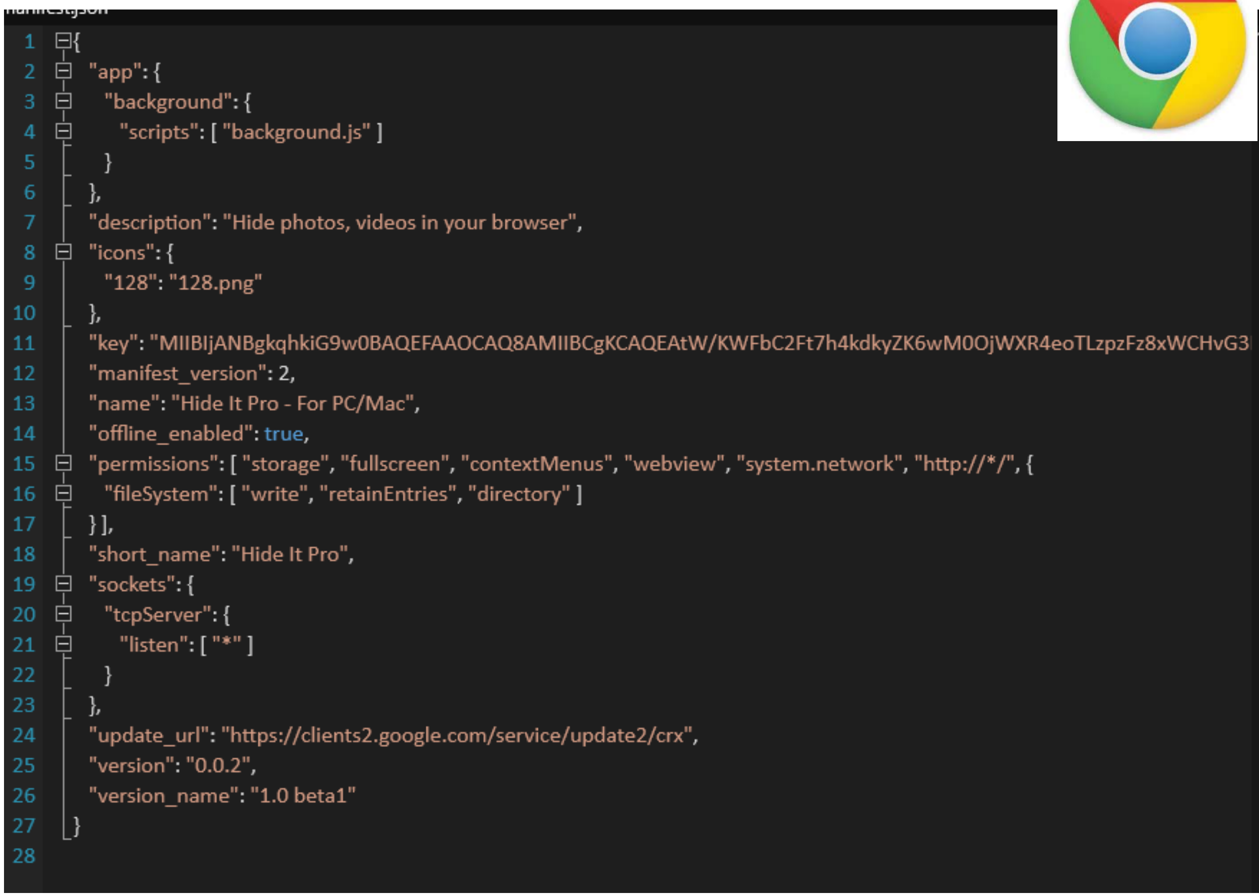


Name	Type	Size (byt...	Created
jaebfnmmkfdadhldnncpbgbghhgmdddc	Folder		8/13/2018 10:34:52 PM
oedeeodfidgoollimchfdnbmhcpnklnd	Folder		8/13/2018 10:34:52 PM
pkedcjkdefgpdelpbcmbmeomcjbeemfm	Folder		8/13/2018 10:34:53 PM

Extensions

- manifest.json contains useful info about the app

- Ex path:
- \home\chronos\user\Extensions\jaebfnmmkfdadhldnncpbgbghhgmdddc\0.0.2_0\manifest.json



```
{
  "app": {
    "background": {
      "scripts": [ "background.js" ]
    }
  },
  "description": "Hide photos, videos in your browser",
  "icons": {
    "128": "128.png"
  },
  "key": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtW/KWFbC2Ft7h4kdkyZK6wM0OjWXR4eoTLzpzFz8xWCHvG3
  "manifest_version": 2,
  "name": "Hide It Pro - For PC/Mac",
  "offline_enabled": true,
  "permissions": [ "storage", "fullscreen", "contextMenus", "webview", "system.network", "http://*/", {
    "fileSystem": [ "write", "retainEntries", "directory" ]
  } ],
  "short_name": "Hide It Pro",
  "sockets": {
    "tcpServer": {
      "listen": [ "*" ]
    }
  },
  "update_url": "https://clients2.google.com/service/update2/crx",
  "version": "0.0.2",
  "version_name": "1.0 beta1"
}
```

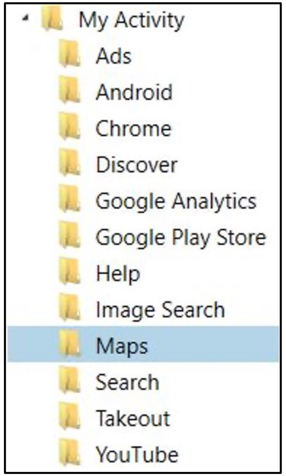
Extensions

- Sync App Settings appear in the following paths
  - \home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\Sync App Settings
  - \home\chronos\user\Sync App Settings
  - \home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\Sync App Settings
  - \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Sync App Settings
- The one in the folder with the GUID for Hide It Pro has an .ldb that contains the password for the doontlookhere folder

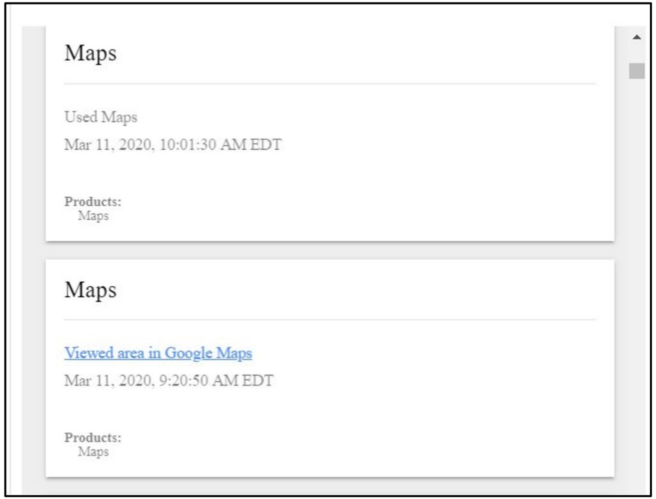
Geolocation

My Activity Maps

- Takeout\My Activity\Maps\MyActivity.html



- My Activity
  - Ads
  - Android
  - Chrome
  - Discover
  - Google Analytics
  - Google Play Store
  - Help
  - Image Search
  - Maps
  - Search
  - Takeout
  - YouTube



Maps

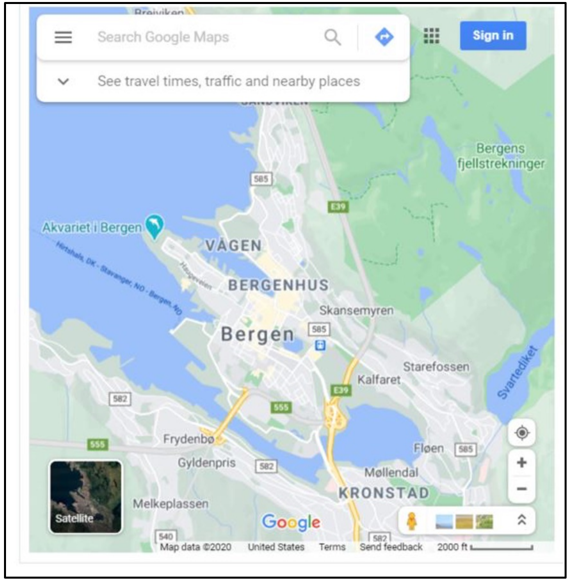
Used Maps
Mar 11, 2020, 10:01:30 AM EDT

Products:
Maps

Maps

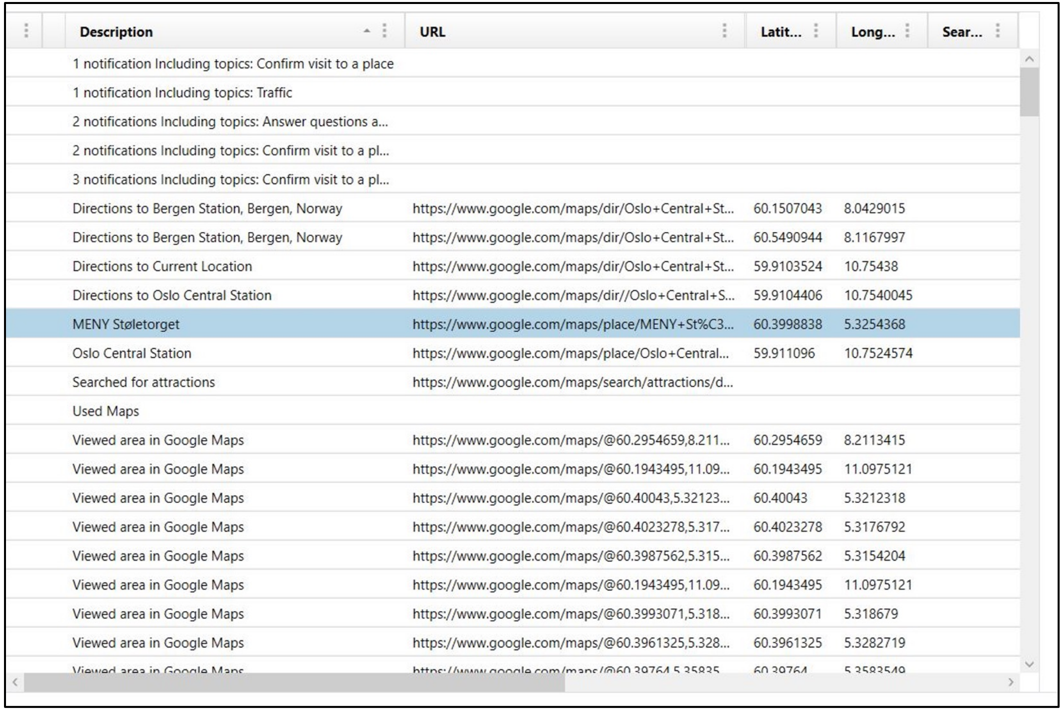
Viewed area in Google Maps
Mar 11, 2020, 9:20:50 AM EDT

Products:
Maps



My Activity Maps

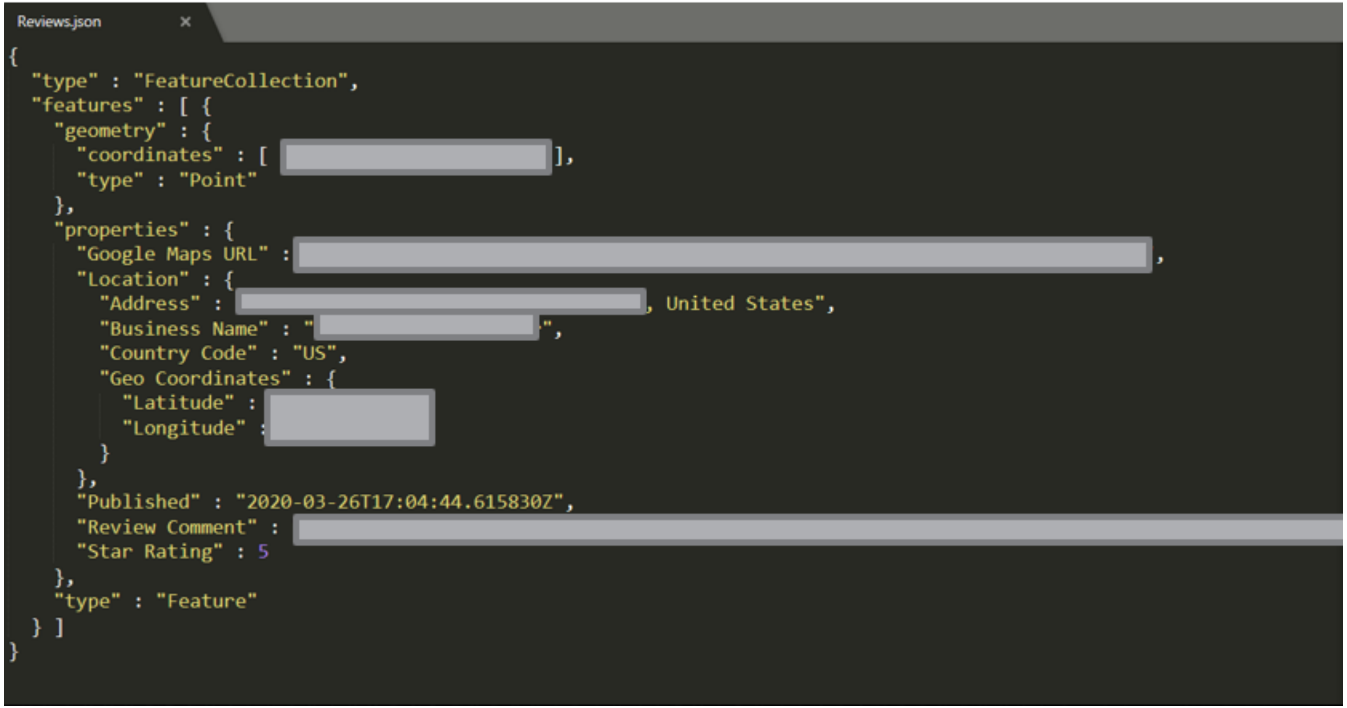
- Takeout\My Activity\Maps\MyActivity.html



Description	URL	Latit...	Long...	Sear...
1 notification Including topics: Confirm visit to a place				
1 notification Including topics: Traffic				
2 notifications Including topics: Answer questions a...				
2 notifications Including topics: Confirm visit to a pl...				
3 notifications Including topics: Confirm visit to a pl...				
Directions to Bergen Station, Bergen, Norway	https://www.google.com/maps/dir/Oslo+Central+St...	60.1507043	8.0429015	
Directions to Bergen Station, Bergen, Norway	https://www.google.com/maps/dir/Oslo+Central+St...	60.5490944	8.1167997	
Directions to Current Location	https://www.google.com/maps/dir/Oslo+Central+St...	59.9103524	10.75438	
Directions to Oslo Central Station	https://www.google.com/maps/dir//Oslo+Central+S...	59.9104406	10.7540045	
MENY Støletorget	https://www.google.com/maps/place/MENY+St%C3...	60.3998838	5.3254368	
Oslo Central Station	https://www.google.com/maps/place/Oslo+Central...	59.911096	10.7524574	
Searched for attractions	https://www.google.com/maps/search/attractions/d...			
Used Maps				
Viewed area in Google Maps	https://www.google.com/maps/@60.2954659,8.211...	60.2954659	8.2113415	
Viewed area in Google Maps	https://www.google.com/maps/@60.1943495,11.09...	60.1943495	11.0975121	
Viewed area in Google Maps	https://www.google.com/maps/@60.40043,5.32123...	60.40043	5.3212318	
Viewed area in Google Maps	https://www.google.com/maps/@60.4023278,5.317...	60.4023278	5.3176792	
Viewed area in Google Maps	https://www.google.com/maps/@60.3987562,5.315...	60.3987562	5.3154204	
Viewed area in Google Maps	https://www.google.com/maps/@60.1943495,11.09...	60.1943495	11.0975121	
Viewed area in Google Maps	https://www.google.com/maps/@60.3993071,5.318...	60.3993071	5.318679	
Viewed area in Google Maps	https://www.google.com/maps/@60.3961325,5.328...	60.3961325	5.3282719	
Viewed area in Google Maps	https://www.google.com/maps/@60.39764,5.35835...	60.39764	5.3583549	

Maps (your places)

- Takeout\Maps (your places)\Reviews.json



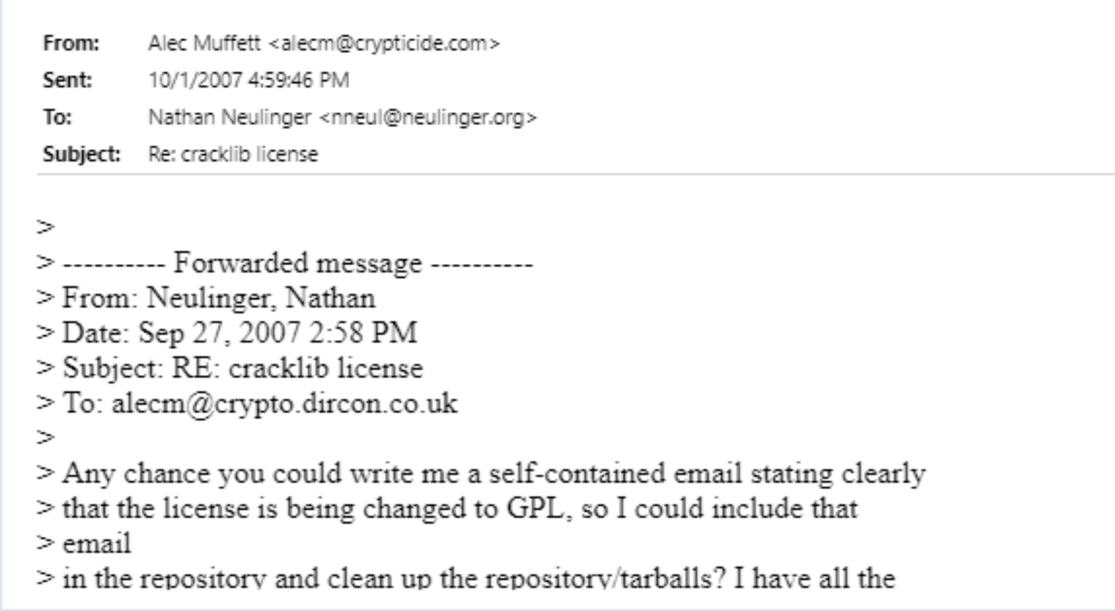
Reviews.json ×

```
{
  "type" : "FeatureCollection",
  "features" : [ {
    "geometry" : {
      "coordinates" : [ [redacted] ],
      "type" : "Point"
    },
    "properties" : {
      "Google Maps URL" : [redacted],
      "Location" : {
        "Address" : [redacted], United States",
        "Business Name" : "[redacted]",
        "Country Code" : "US",
        "Geo Coordinates" : {
          "Latitude" : [redacted]
          "Longitude" :
        }
      },
      "Published" : "2020-03-26T17:04:44.615830Z",
      "Review Comment" : [redacted]
      "Star Rating" : 5
    },
    "type" : "Feature"
  } ]
}
```

Mail

Email

Emails have been successfully carved from the ‘usr\bin



From: Alec Muffett <alecm@crypticide.com>
Sent: 10/1/2007 4:59:46 PM
To: Nathan Neulinger <nneul@neulinger.org>
Subject: Re: cracklib license

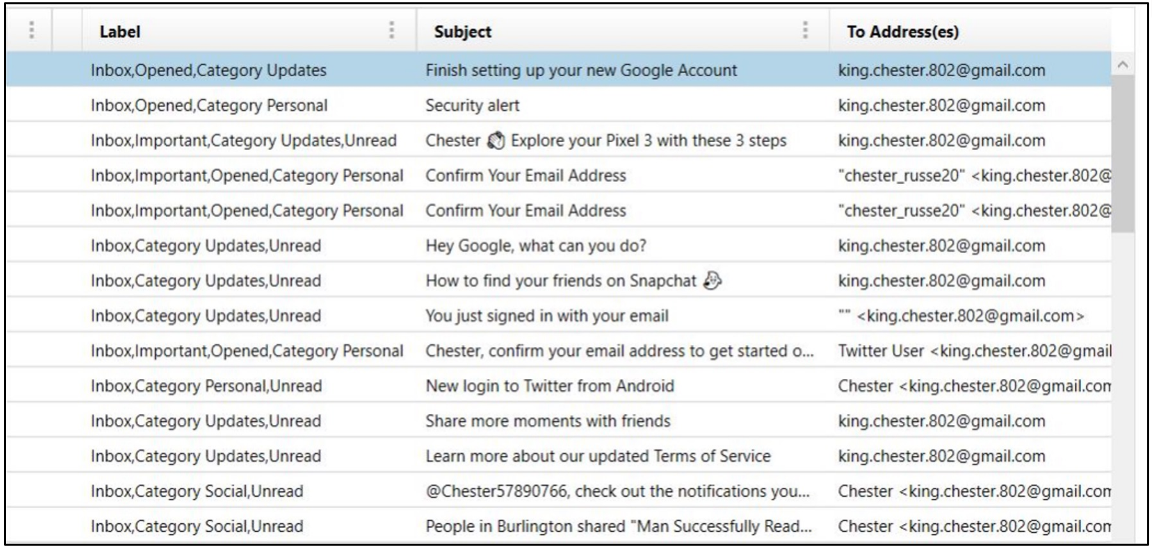
```
>
> ---------- Forwarded message ----------
> From: Neulinger, Nathan
> Date: Sep 27, 2007 2:58 PM
> Subject: RE: cracklib license
> To: alecm@crypto.dircon.co.uk
>
> Any chance you could write me a self-contained email stating clearly
> that the license is being changed to GPL, so I could include that
> email
> in the repository and clean up the repository/tarballs? I have all the
```

Takeout Mail

Takeout\Mail\All mail Including Spam and Trash.mbox

Includes:

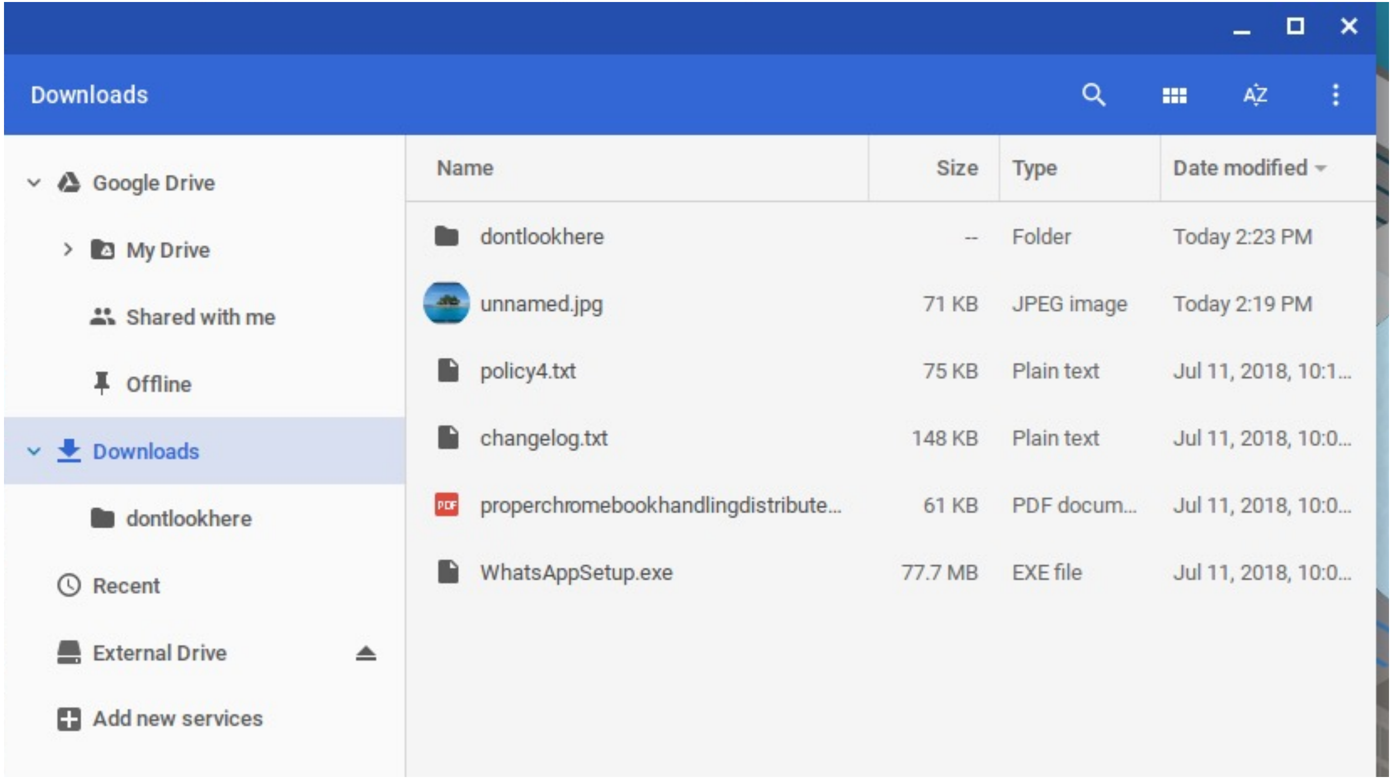
- To/From email addresses
- Labels (Inbox, Sent, Opened, Unread, Archived, etc)
- Subject
- Date/time
- Email headers
- Email body
- Attachment parsed out of mbox file!



Label	Subject	To Address(es)
Inbox,Opened,Category Updates	Finish setting up your new Google Account	king.chester.802@gmail.com
Inbox,Opened,Category Personal	Security alert	king.chester.802@gmail.com
Inbox,Important,Category Updates,Unread	Chester 👋 Explore your Pixel 3 with these 3 steps	king.chester.802@gmail.com
Inbox,Important,Opened,Category Personal	Confirm Your Email Address	"chester_russe20" <king.chester.802@
Inbox,Important,Opened,Category Personal	Confirm Your Email Address	"chester_russe20" <king.chester.802@
Inbox,Category Updates,Unread	Hey Google, what can you do?	king.chester.802@gmail.com
Inbox,Category Updates,Unread	How to find your friends on Snapchat 👻	king.chester.802@gmail.com
Inbox,Category Updates,Unread	You just signed in with your email	"" <king.chester.802@gmail.com>
Inbox,Important,Opened,Category Personal	Chester, confirm your email address to get started o...	Twitter User <king.chester.802@gmail
Inbox,Category Personal,Unread	New login to Twitter from Android	Chester <king.chester.802@gmail.con
Inbox,Category Updates,Unread	Share more moments with friends	king.chester.802@gmail.com
Inbox,Category Updates,Unread	Learn more about our updated Terms of Service	king.chester.802@gmail.com
Inbox,Category Social,Unread	@Chester57890766, check out the notifications you...	Chester <king.chester.802@gmail.con
Inbox,Category Social,Unread	People in Burlington shared "Man Successfully Read...	Chester <king.chester.802@gmail.con

System Artifacts

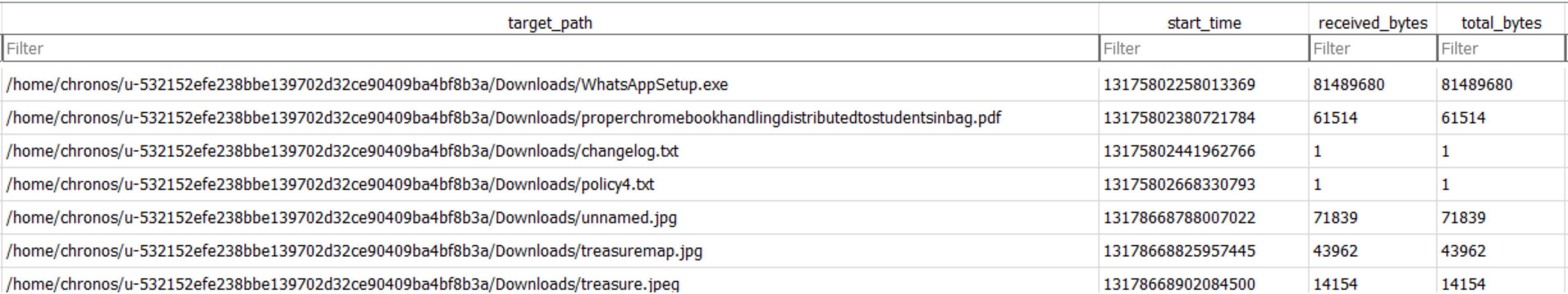
Downloads



Name	Size	Type	Date modified
dontlookhere	--	Folder	Today 2:23 PM
unnamed.jpg	71 KB	JPEG image	Today 2:19 PM
policy4.txt	75 KB	Plain text	Jul 11, 2018, 10:1...
changelog.txt	148 KB	Plain text	Jul 11, 2018, 10:0...
properchromebookhandlingdistribute...	61 KB	PDF docum...	Jul 11, 2018, 10:0...
WhatsAppSetup.exe	77.7 MB	EXE file	Jul 11, 2018, 10:0...

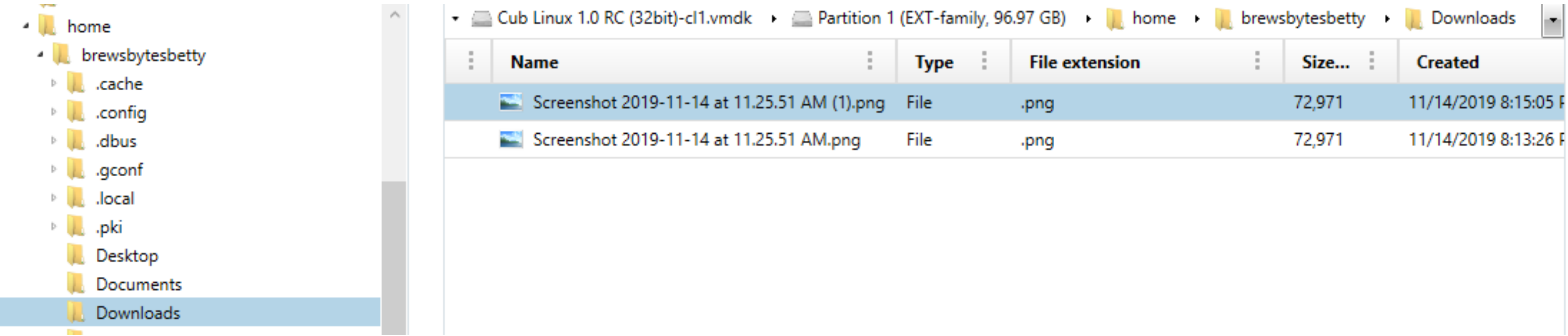
Downloads

In the downloads table:



target_path	start_time	received_bytes	total_bytes
Filter	Filter	Filter	Filter
/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/WhatsAppSetup.exe	13175802258013369	81489680	81489680
/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/properchromebookhandlingdistributedtostudentsinbag.pdf	13175802380721784	61514	61514
/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/changelog.txt	13175802441962766	1	1
/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/policy4.txt	13175802668330793	1	1
/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/unnamed.jpg	13178668788007022	71839	71839
/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/treasuremap.jpg	13178668825957445	43962	43962
/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/treasure.jpeg	13178668902084500	14154	14154

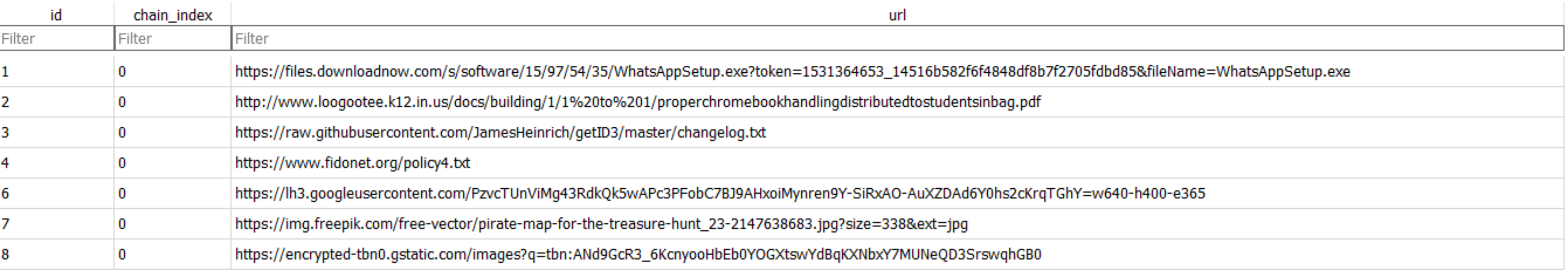
Downloads



Name	Type	File extension	Size...	Created
Screenshot 2019-11-14 at 11.25.51 AM (1).png	File	.png	72,971	11/14/2019 8:15:05
Screenshot 2019-11-14 at 11.25.51 AM.png	File	.png	72,971	11/14/2019 8:13:26

Downloads

- Which can be coordinated with the downloads_url_chains table
- Also in the Chrome Browser History

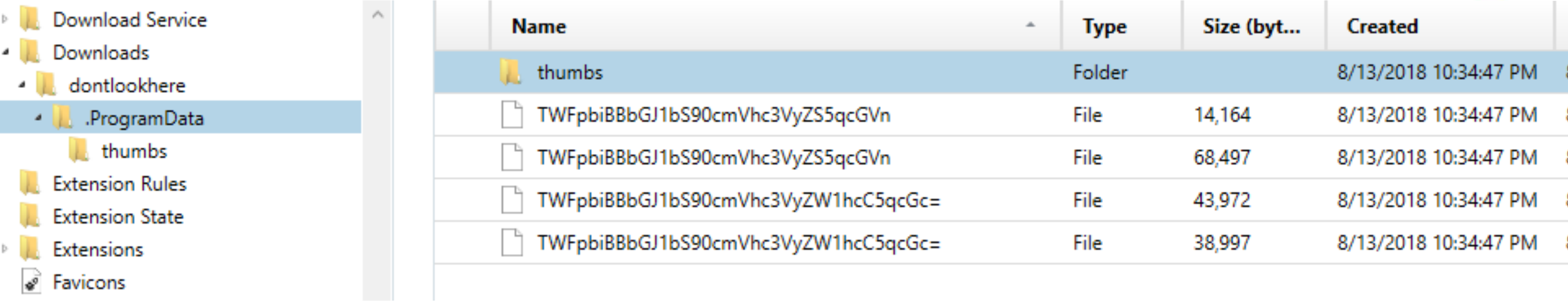


id	chain_index	url
Filter	Filter	Filter
1	0	https://files.downloadnow.com/s/software/15/97/54/35/WhatsAppSetup.exe?token=1531364653_14516b582f6f4848df8b7f2705fdbd85&fileName=WhatsAppSetup.exe
2	0	http://www.loogootee.k12.in.us/docs/building/1/1%20to%201/properchromebookhandlingdistributedtostudentsinbag.pdf
3	0	https://raw.githubusercontent.com/JamesHeinrich/getID3/master/changelog.txt
4	0	https://www.fidonet.org/policy4.txt
6	0	https://lh3.googleusercontent.com/PzvcTUnViMg43RdkQk5wAPc3PFobC7BJ9AHxoiMynren9Y-SiRxAO-AuXZDAd6Y0hs2cKrqTGhY=w640-h400-e365
7	0	https://img.freepik.com/free-vector/pirate-map-for-the-treasure-hunt_23-2147638683.jpg?size=338&ext=jpg
8	0	https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcR3_6KcnyooHbEb0YOGXtswYdBqKXNbxY7MUNeQD3SrswqhGB0

Hidden Folder

- The dontlookhere directory appears in the following paths
  - \home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\Downloads
  - \home\chronos\user\Downloads
  - \home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\Downloads
  - \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Downloads

Hidden Folder



- Download Service
- Downloads
  - dontlookhere
    - .ProgramData
      - thumbs
- Extension Rules
- Extension State
- Extensions
- Favicons

Name	Type	Size (byt...	Created
thumbs	Folder		8/13/2018 10:34:47 PM
TWFpbiBBbGJ1bS90cmVhc3VyZS5qcGVn	File	14,164	8/13/2018 10:34:47 PM
TWFpbiBBbGJ1bS90cmVhc3VyZS5qcGVn	File	68,497	8/13/2018 10:34:47 PM
TWFpbiBBbGJ1bS90cmVhc3VyZW1hcC5qcGc=	File	43,972	8/13/2018 10:34:47 PM
TWFpbiBBbGJ1bS90cmVhc3VyZW1hcC5qcGc=	File	38,997	8/13/2018 10:34:47 PM

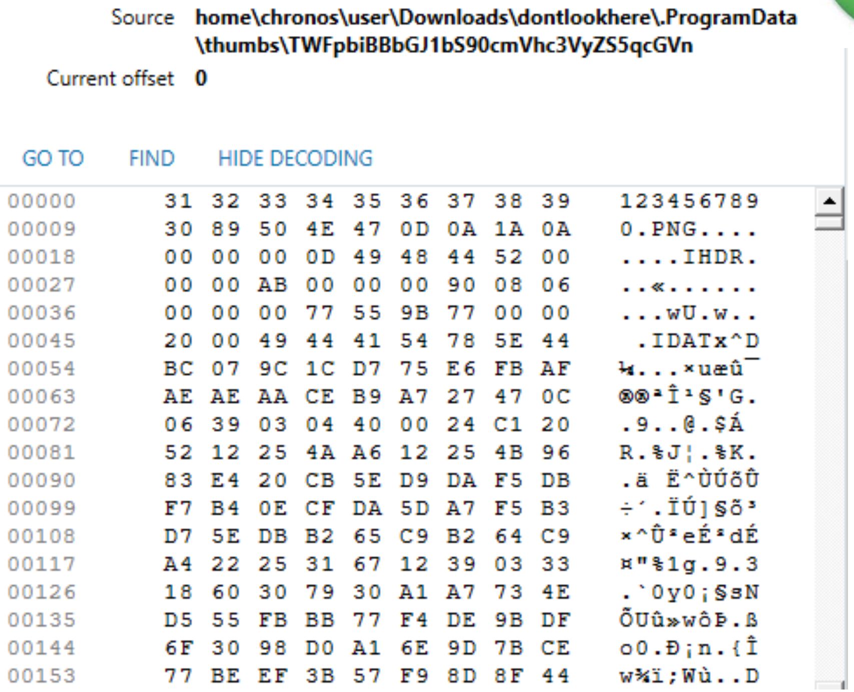
- Inside .ProgramData folder are the hidden files
- Filenames are base64 encoded
- Main Album/treasuremap.jpeg
- Main Album/treasuremap.jpg

Hidden Folder

The password is appended to the front of the file.

In this case the password = ‘1234567890’

True for the .jpg, .png, and thumbnails

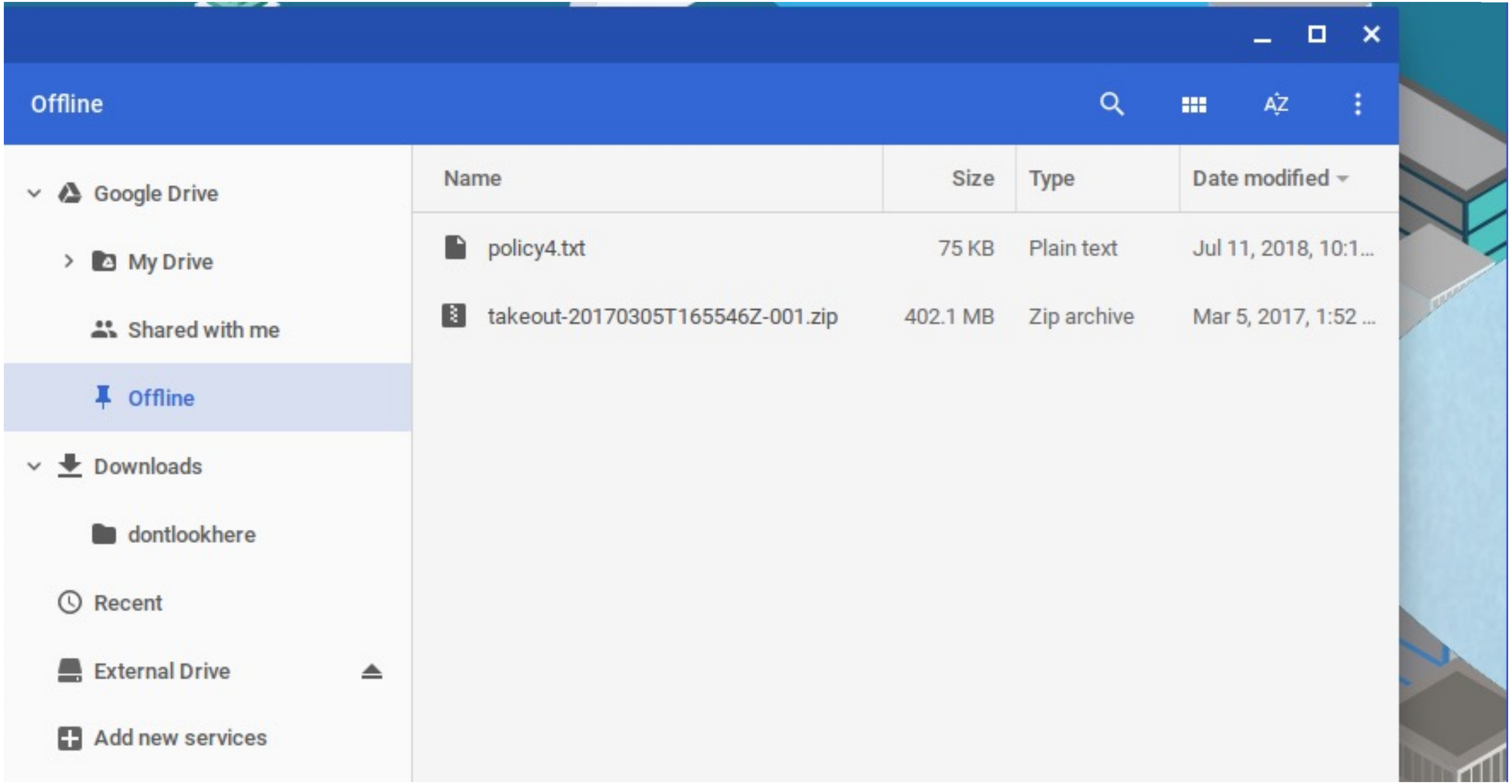


Source home\chronos\user\Downloads\dontlookhere\.ProgramData\thumbs\TWFpbiBBbGJ1bS90cmVhc3VyZS5qcGVn

Current offset 0

```
00000    31 32 33 34 35 36 37 38 39    123456789
00009    30 89 50 4E 47 0D 0A 1A 0A    0.PNG....
00018    00 00 00 0D 49 48 44 52 00    ....IHDR.
00027    00 00 AB 00 00 00 90 08 06    ..«......
00036    00 00 00 77 55 9B 77 00 00    ...wU.w..
00045    20 00 49 44 41 54 78 5E 44     .IDATx^D
00054    BC 07 9C 1C D7 75 E6 FB AF    ¼...×uæû¯
00063    AE AE AA CE B9 A7 27 47 0C    ®®ªÎ¹§'G.
00072    06 39 03 04 40 00 24 C1 20    .9..@.$Á
00081    52 12 25 4A A6 12 25 4B 96    R.%J¦.%K.
00090    83 E4 20 CB 5E D9 DA F5 DB    .ä Ë^ÙÚõÛ
00099    F7 B4 0E CF DA 5D A7 F5 B3    ÷´.ÏÚ]§õ³
00108    D7 5E DB B2 65 C9 B2 64 C9    ×^Û²eÉ²dÉ
00117    A4 22 25 31 67 12 39 03 33    ¤"%1g.9.3
00126    18 60 30 79 30 A1 A7 73 4E    .`0y0¡§sN
00135    D5 55 FB BB 77 F4 DE 9B DF    ÕUû»wôÞ.ß
00144    6F 30 98 D0 A1 6E 9D 7B CE    o0.Ð¡n.{Î
00153    77 BE EF 3B 57 F9 8D 8F 44    w¾ï;Wù..D
```

Offline Storage

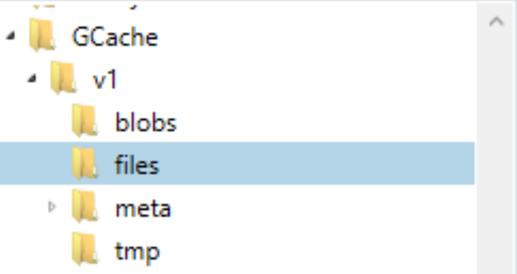


Name	Size	Type	Date modified
policy4.txt	75 KB	Plain text	Jul 11, 2018, 10:1...
takeout-20170305T165546Z-001.zip	402.1 MB	Zip archive	Mar 5, 2017, 1:52 ...

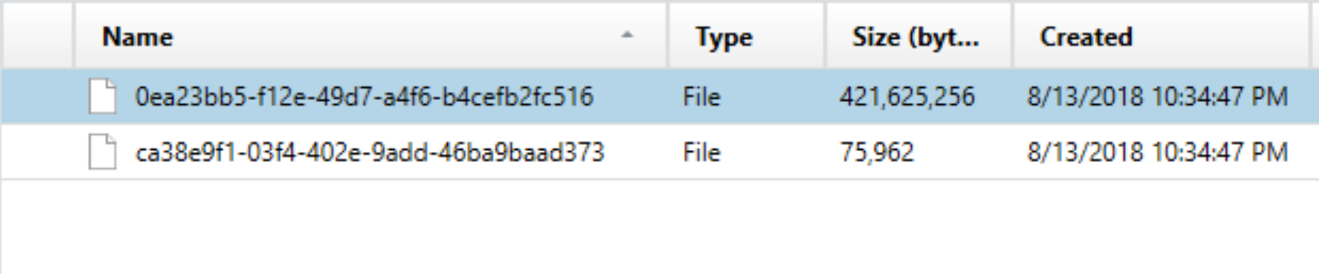
Offline Storage

- Offline Storage can be found at the following paths
  - \home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\Gcache\v1\files
  - \home\chronos\user\Gcache\v1\files
  - \home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\Gcache\v1\files
  - \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Gcache\v1\files

Offline Storage



GCache
v1
blobs
files
meta
tmp

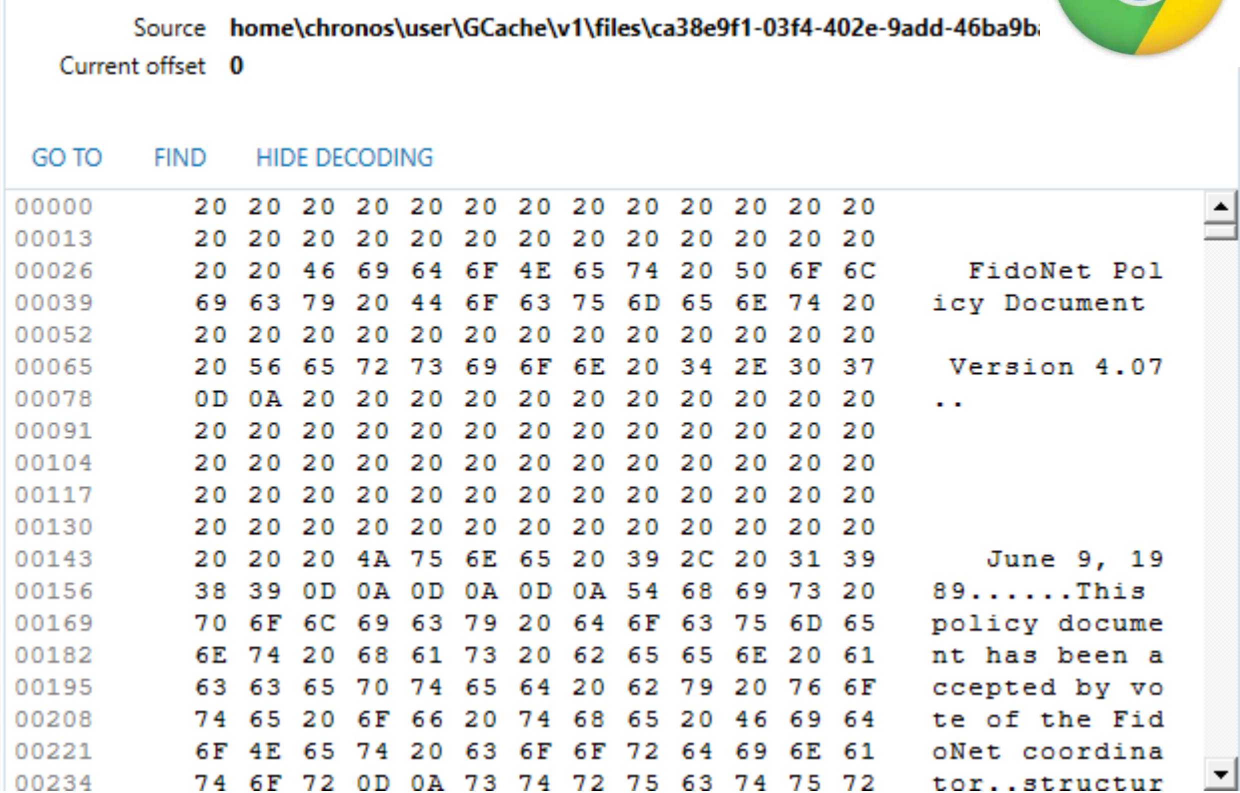


Name	Type	Size (byt...	Created
0ea23bb5-f12e-49d7-a4f6-b4cefb2fc516	File	421,625,256	8/13/2018 10:34:47 PM
ca38e9f1-03f4-402e-9add-46ba9baad373	File	75,962	8/13/2018 10:34:47 PM

Offline Storage

- Files can be saved out and exported. Just the names are changed

- Original file names and GUID can be found in an .ldb in GCache\v1\meta\

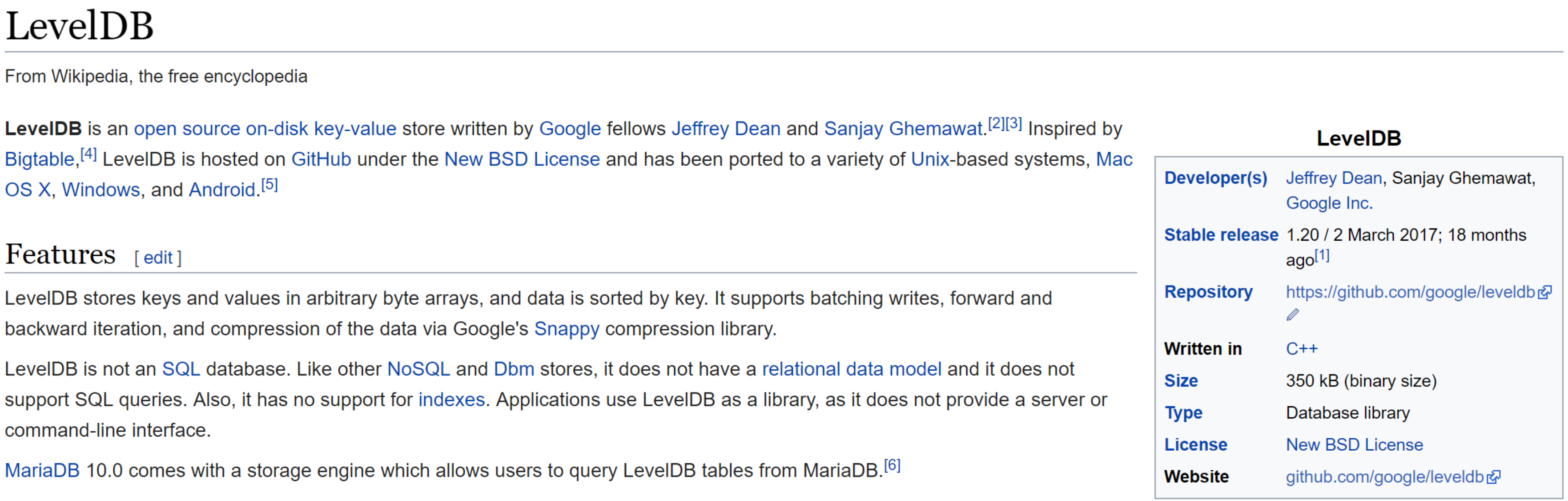


Source home\chronos\user\GCache\v1\files\ca38e9f1-03f4-402e-9add-46ba9b

Current offset 0

```
00000    20 20 20 20 20 20 20 20 20 20 20 20 20
00013    20 20 20 20 20 20 20 20 20 20 20 20 20
00026    20 20 46 69 64 6F 4E 65 74 20 50 6F 6C      FidoNet Pol
00039    69 63 79 20 44 6F 63 75 6D 65 6E 74 20    icy Document
00052    20 20 20 20 20 20 20 20 20 20 20 20 20
00065    20 56 65 72 73 69 6F 6E 20 34 2E 30 37     Version 4.07
00078    0D 0A 20 20 20 20 20 20 20 20 20 20 20    ..
00091    20 20 20 20 20 20 20 20 20 20 20 20 20
00104    20 20 20 20 20 20 20 20 20 20 20 20 20
00117    20 20 20 20 20 20 20 20 20 20 20 20 20
00130    20 20 20 20 20 20 20 20 20 20 20 20 20
00143    20 20 20 4A 75 6E 65 20 39 2C 20 31 39       June 9, 19
00156    38 39 0D 0A 0D 0A 0D 0A 54 68 69 73 20    89......This
00169    70 6F 6C 69 63 79 20 64 6F 63 75 6D 65    policy docume
00182    6E 74 20 68 61 73 20 62 65 65 6E 20 61    nt has been a
00195    63 63 65 70 74 65 64 20 62 79 20 76 6F    ccepted by vo
00208    74 65 20 6F 66 20 74 68 65 20 46 69 64    te of the Fid
00221    6F 4E 65 74 20 63 6F 6F 72 64 69 6E 61    oNet coordina
00234    74 6F 72 0D 0A 73 74 72 75 63 74 75 72    tor..structur
```

Offline Storage



LevelDB

From Wikipedia, the free encyclopedia

LevelDB is an open source on-disk key-value store written by Google fellows Jeffrey Dean and Sanjay Ghemawat.[2][3] Inspired by Bigtable,[4] LevelDB is hosted on GitHub under the New BSD License and has been ported to a variety of Unix-based systems, Mac OS X, Windows, and Android.[5]

LevelDB

Developer(s)	Jeffrey Dean, Sanjay Ghemawat, Google Inc.
Stable release	1.20 / 2 March 2017; 18 months ago[1]
Repository	https://github.com/google/leveldb
Written in	C++
Size	350 kB (binary size)
Type	Database library
License	New BSD License
Website	github.com/google/leveldb

Features [edit]

LevelDB stores keys and values in arbitrary byte arrays, and data is sorted by key. It supports batching writes, forward and backward iteration, and compression of the data via Google's Snappy compression library.

LevelDB is not an SQL database. Like other NoSQL and Dbm stores, it does not have a relational data model and it does not support SQL queries. Also, it has no support for indexes. Applications use LevelDB as a library, as it does not provide a server or command-line interface.

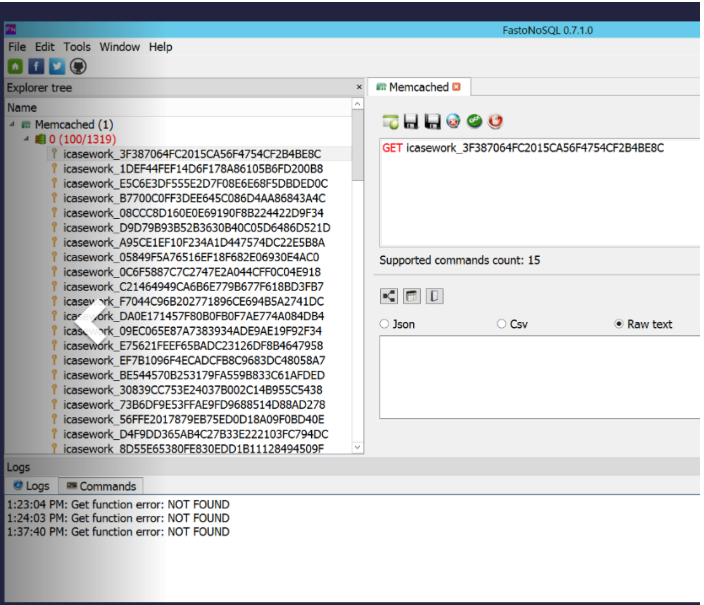
MariaDB 10.0 comes with a storage engine which allows users to query LevelDB tables from MariaDB.[6]

What is FastoNoSQL?

FastoNoSQL is the GUI platform for NoSQL databases.

Currently we support next databases:

- Redis
- Memcached
- SSDB
- LevelDB
- RocksDB
- UnQLite
- LMDB
- UpscaleDB
- ForestDB
- Pika



Memcached (1)
0 (100/1319)

```
icasework_3F387064FC2015CA56F4754CF2B4BE8C
icasework_1DEF44FEF14D6F178A86105B6FD200B8
icasework_E5C6E3DF555E2D7F08E6E68F5DBDED0C
icasework_B7700C0FF3DEE645C086D4AA86843A4C
icasework_08CCC8D160E0E69190F8B224422D9F34
icasework_D9D79B93B52B3630B40C05D6486D521D
icasework_A95CE1EF10F234A1D447574DC22E5B8A
icasework_05849F5A76516EF18F682E06930E4AC0
icasework_0C6F5887C7C2747E2A044CFF0C04E918
icasework_C21464949CA6B6E779B677F618BD3FB7
icasework_F7044C96B202771896CE694B5A2741DC
icasework_DA0E171457F80B0FB0F7AE774A084DB4
icasework_09EC065E87A7383934ADE9AE19F92F34
icasework_E75621FEEF65BADC23126DF8B4647958
icasework_EF7B1096F4ECADCFB8C9683DC48058A7
icasework_BE544570B253179FA559B833C61AFDED
icasework_30839CC753E24037B002C14B955C5438
icasework_73B6DF9E53FFAE9FD9688514D88AD278
icasework_56FFE2017879EB75ED0D18A09F0BD40E
icasework_D4F9DD365AB4C27B33E222103FC794DC
icasework_8D55E65380FE830EDD1B11128494509F
```

```
GET icasework_3F387064FC2015CA56F4754CF2B4BE8C
```

Supported commands count: 15

○ Json ○ Csv ● Raw text

```
1:23:04 PM: Get function error: NOT FOUND
1:24:03 PM: Get function error: NOT FOUND
1:37:40 PM: Get function error: NOT FOUND
```

Level DBs

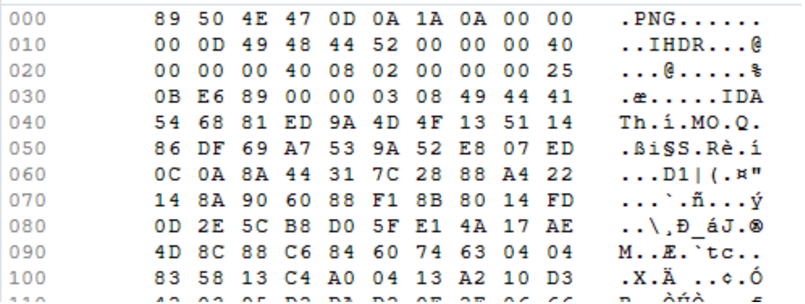
- Mark Mckinnon: https://github.com/markmckinnon/Leveldb-py
- CCL (Alex Caithness) https://github.com/cclgroupltd/ccl_chrome_indexeddb
- Kathryn Hedley: https://github.com/khyrenz/parse_leveldb
- Scalyr: https://app.scalyr.com/leveldbdashboard?teamToken=
- Hindsight from Ryan Benson also added support using Alex's libraries: https://github.com/obsidianforensics/hindsight

Shell Usage - .bash_history

- Each entry appears in the following paths
  - \home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\.bash_history
  - \home\chronos\user\.bash_history
  - \home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\.bash_history
  - \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\.bash_history

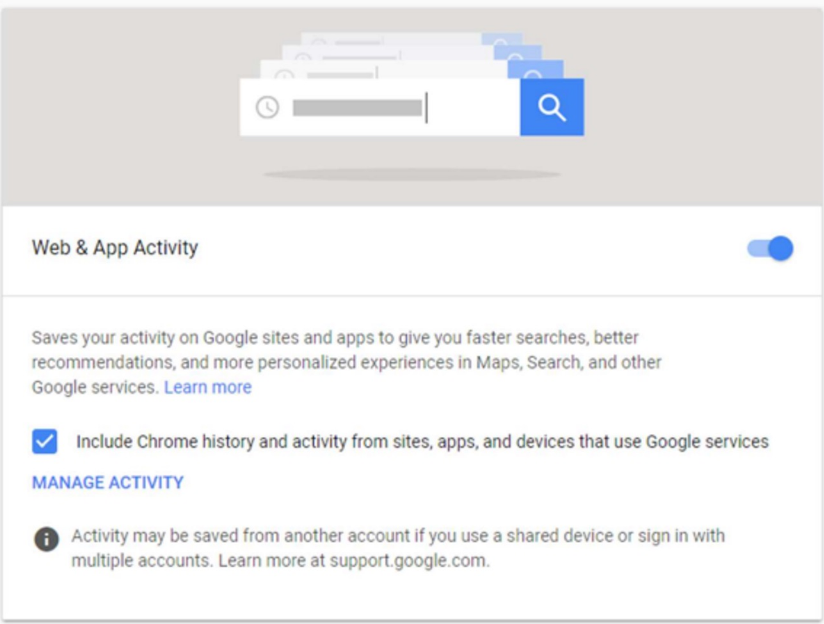
Avatar

- .png file with login email as name
  - \home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\Accounts\Avatar Images\aforensiclook@gmail.com
  - \home\chronos\user\ Accounts\Avatar Images\aforensiclook@gmail.com
  - \home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\Accounts\Avatar Images\aforensiclook@gmail.com
  - \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Accounts\Avatar Images\aforensiclook@gmail.com



```
000        89 50 4E 47 0D 0A 1A 0A 00 00    .PNG......
010        00 0D 49 48 44 52 00 00 00 40    ..IHDR...@
020        00 00 00 40 08 02 00 00 00 25    ...@.....%
030        0B E6 89 00 00 03 08 49 44 41    .æ.....IDA
040        54 68 81 ED 9A 4D 4F 13 51 14    Th.í.MO.Q.
050        86 DF 69 A7 53 9A 52 E8 07 ED    .ßi§S.Rè.í
060        0C 0A 8A 44 31 7C 28 88 A4 22    ...D1|(.¤"
070        14 8A 90 60 88 F1 8B 80 14 FD    ...`.ñ...ý
080        0D 2E 5C B8 D0 5F E1 4A 17 AE    ..\¸Ð_áJ.®
090        4D 8C 88 C6 84 60 74 63 04 04    M..Æ.`tc..
100        83 58 13 C4 A0 04 13 A2 10 D3    .X.Ä ..¢.Ó
```

My Activity



Web & App Activity

Saves your activity on Google sites and apps to give you faster searches, better recommendations, and more personalized experiences in Maps, Search, and other Google services. Learn more

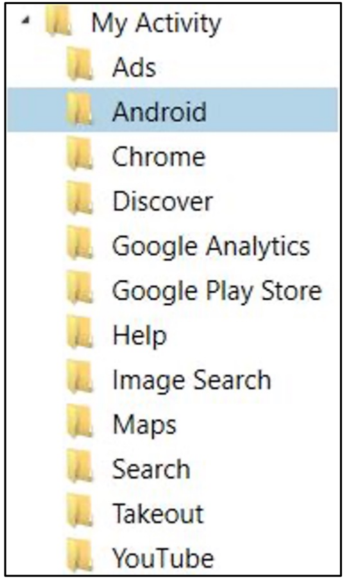
☑ Include Chrome history and activity from sites, apps, and devices that use Google services

MANAGE ACTIVITY

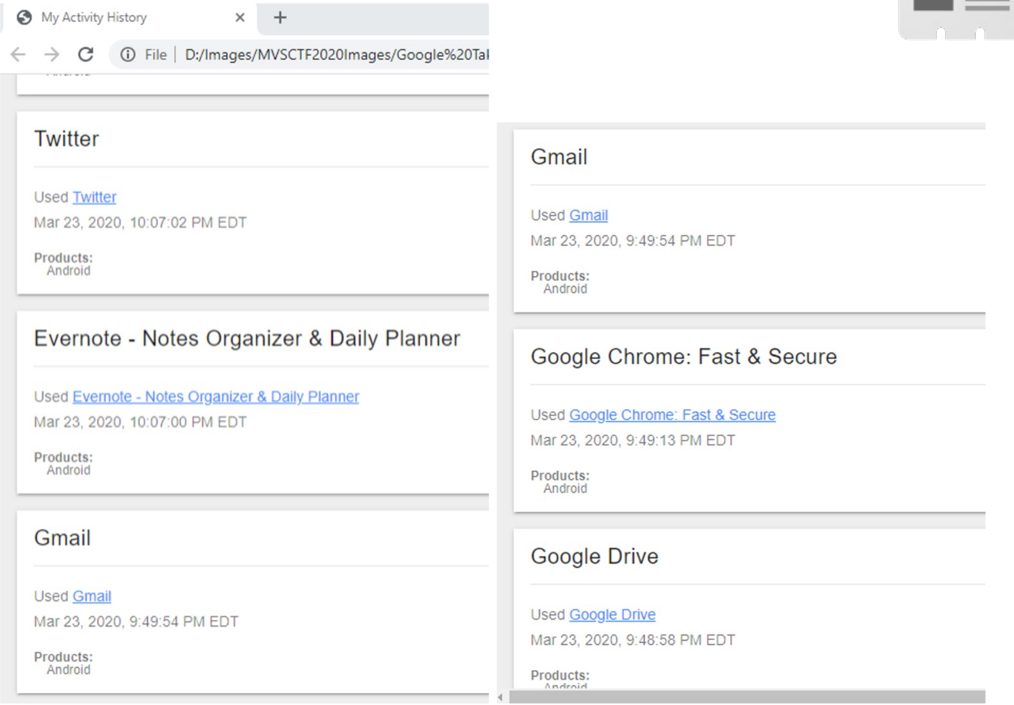
Activity may be saved from another account if you use a shared device or sign in with multiple accounts. Learn more at support.google.com.

My Activity

Takeout\My Activity\Android\MyActivity.html



- My Activity
  - Ads
  - Android
  - Chrome
  - Discover
  - Google Analytics
  - Google Play Store
  - Help
  - Image Search
  - Maps
  - Search
  - Takeout
  - YouTube



Twitter

Used Twitter
Mar 23, 2020, 10:07:02 PM EDT
Products:
Android

Evernote - Notes Organizer & Daily Planner

Used Evernote - Notes Organizer & Daily Planner
Mar 23, 2020, 10:07:00 PM EDT
Products:
Android

Gmail

Used Gmail
Mar 23, 2020, 9:49:54 PM EDT
Products:
Android

Gmail

Used Gmail
Mar 23, 2020, 9:49:54 PM EDT
Products:
Android

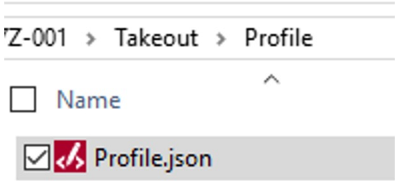
Google Chrome: Fast & Secure

Used Google Chrome: Fast & Secure
Mar 23, 2020, 9:49:13 PM EDT
Products:
Android

Google Drive

Used Google Drive
Mar 23, 2020, 9:48:58 PM EDT
Products:
Android

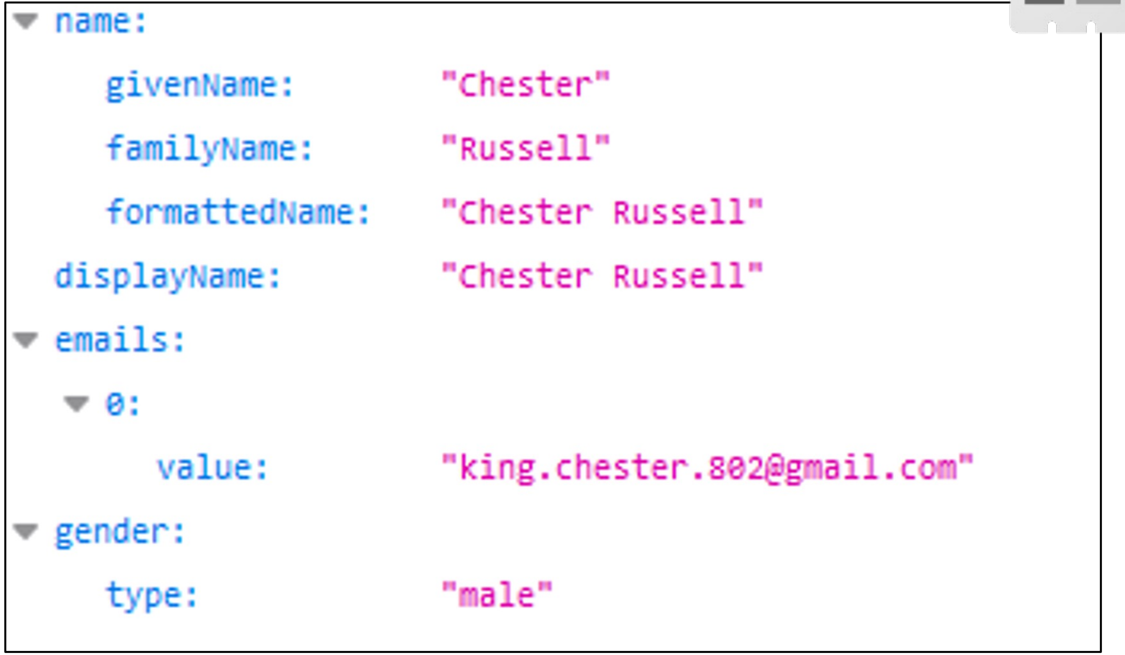
Profile.json



'Z-001 › Takeout › Profile

□ Name

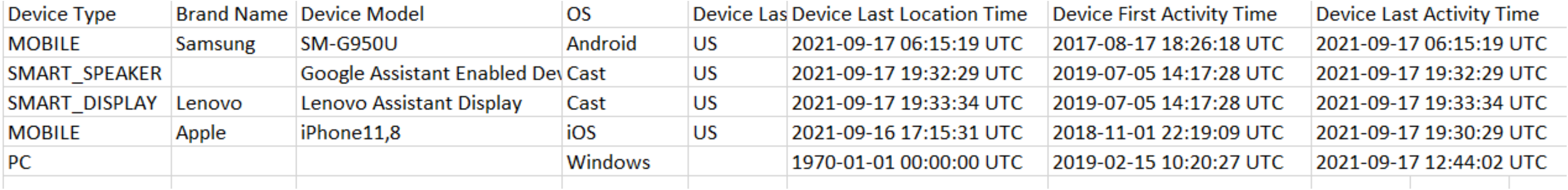
☑ Profile.json



```
▼ name:
    givenName:        "Chester"
    familyName:       "Russell"
    formattedName:    "Chester Russell"
  displayName:        "Chester Russell"
▼ emails:
  ▼ 0:
      value:          "king.chester.802@gmail.com"
▼ gender:
    type:             "male"
```

Access Log Activity - Devices

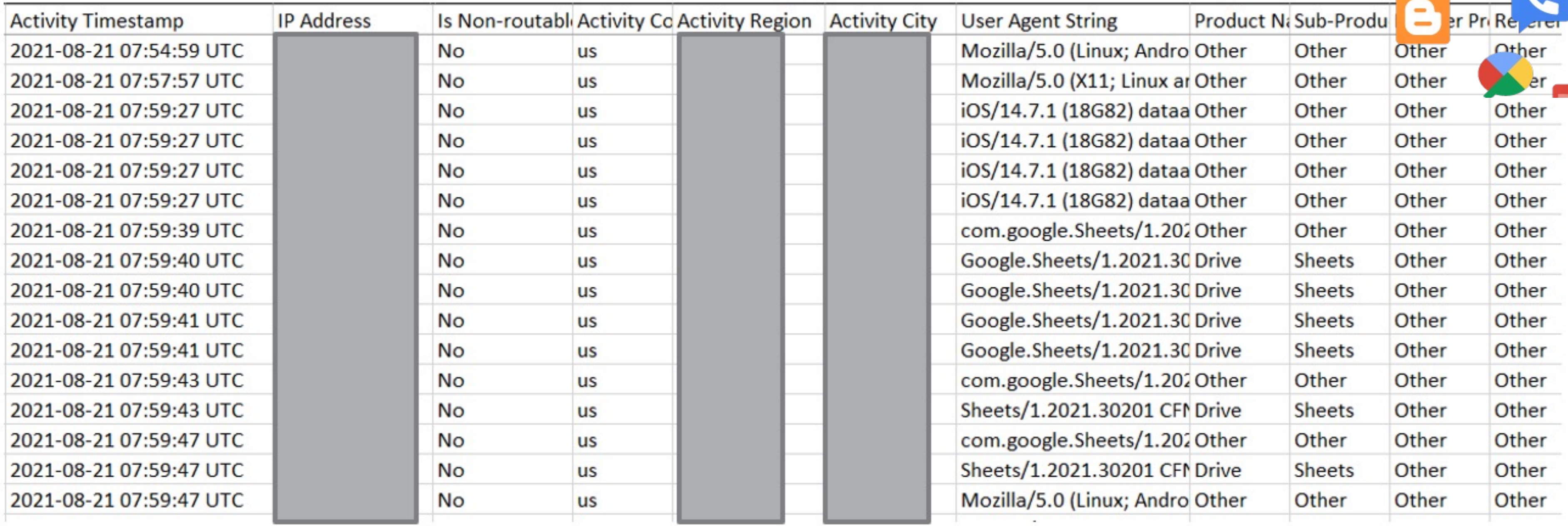
Takeout\Access Log Activity\Devices



Device Type	Brand Name	Device Model	OS	Device Las	Device Last Location Time	Device First Activity Time	Device Last Activity Time
MOBILE	Samsung	SM-G950U	Android	US	2021-09-17 06:15:19 UTC	2017-08-17 18:26:18 UTC	2021-09-17 06:15:19 UTC
SMART_SPEAKER		Google Assistant Enabled Dev	Cast	US	2021-09-17 19:32:29 UTC	2019-07-05 14:17:28 UTC	2021-09-17 19:32:29 UTC
SMART_DISPLAY	Lenovo	Lenovo Assistant Display	Cast	US	2021-09-17 19:33:34 UTC	2019-07-05 14:17:28 UTC	2021-09-17 19:33:34 UTC
MOBILE	Apple	iPhone11,8	iOS	US	2021-09-16 17:15:31 UTC	2018-11-01 22:19:09 UTC	2021-09-17 19:30:29 UTC
PC			Windows		1970-01-01 00:00:00 UTC	2019-02-15 10:20:27 UTC	2021-09-17 12:44:02 UTC

Access Log Activity - Activities

Takeout\Access Log Activity\Activities (30 days per file)



Activity Timestamp	IP Address	Is Non-routabl	Activity Co	Activity Region	Activity City	User Agent String	Product Na	Sub-Produ	er Pr	Referer
2021-08-21 07:54:59 UTC	[redacted]	No	us	[redacted]	[redacted]	Mozilla/5.0 (Linux; Andro	Other	Other	Other	Other
2021-08-21 07:57:57 UTC	[redacted]	No	us	[redacted]	[redacted]	Mozilla/5.0 (X11; Linux ar	Other	Other	Other	er
2021-08-21 07:59:27 UTC	[redacted]	No	us	[redacted]	[redacted]	iOS/14.7.1 (18G82) dataa	Other	Other	Other	Other
2021-08-21 07:59:27 UTC	[redacted]	No	us	[redacted]	[redacted]	iOS/14.7.1 (18G82) dataa	Other	Other	Other	Other
2021-08-21 07:59:27 UTC	[redacted]	No	us	[redacted]	[redacted]	iOS/14.7.1 (18G82) dataa	Other	Other	Other	Other
2021-08-21 07:59:27 UTC	[redacted]	No	us	[redacted]	[redacted]	iOS/14.7.1 (18G82) dataa	Other	Other	Other	Other
2021-08-21 07:59:39 UTC	[redacted]	No	us	[redacted]	[redacted]	com.google.Sheets/1.202	Other	Other	Other	Other
2021-08-21 07:59:40 UTC	[redacted]	No	us	[redacted]	[redacted]	Google.Sheets/1.2021.30	Drive	Sheets	Other	Other
2021-08-21 07:59:40 UTC	[redacted]	No	us	[redacted]	[redacted]	Google.Sheets/1.2021.30	Drive	Sheets	Other	Other
2021-08-21 07:59:41 UTC	[redacted]	No	us	[redacted]	[redacted]	Google.Sheets/1.2021.30	Drive	Sheets	Other	Other
2021-08-21 07:59:41 UTC	[redacted]	No	us	[redacted]	[redacted]	Google.Sheets/1.2021.30	Drive	Sheets	Other	Other
2021-08-21 07:59:43 UTC	[redacted]	No	us	[redacted]	[redacted]	com.google.Sheets/1.202	Other	Other	Other	Other
2021-08-21 07:59:43 UTC	[redacted]	No	us	[redacted]	[redacted]	Sheets/1.2021.30201 CFN	Drive	Sheets	Other	Other
2021-08-21 07:59:47 UTC	[redacted]	No	us	[redacted]	[redacted]	com.google.Sheets/1.202	Other	Other	Other	Other
2021-08-21 07:59:47 UTC	[redacted]	No	us	[redacted]	[redacted]	Sheets/1.2021.30201 CFN	Drive	Sheets	Other	Other
2021-08-21 07:59:47 UTC	[redacted]	No	us	[redacted]	[redacted]	Mozilla/5.0 (Linux; Andro	Other	Other	Other	Other

References

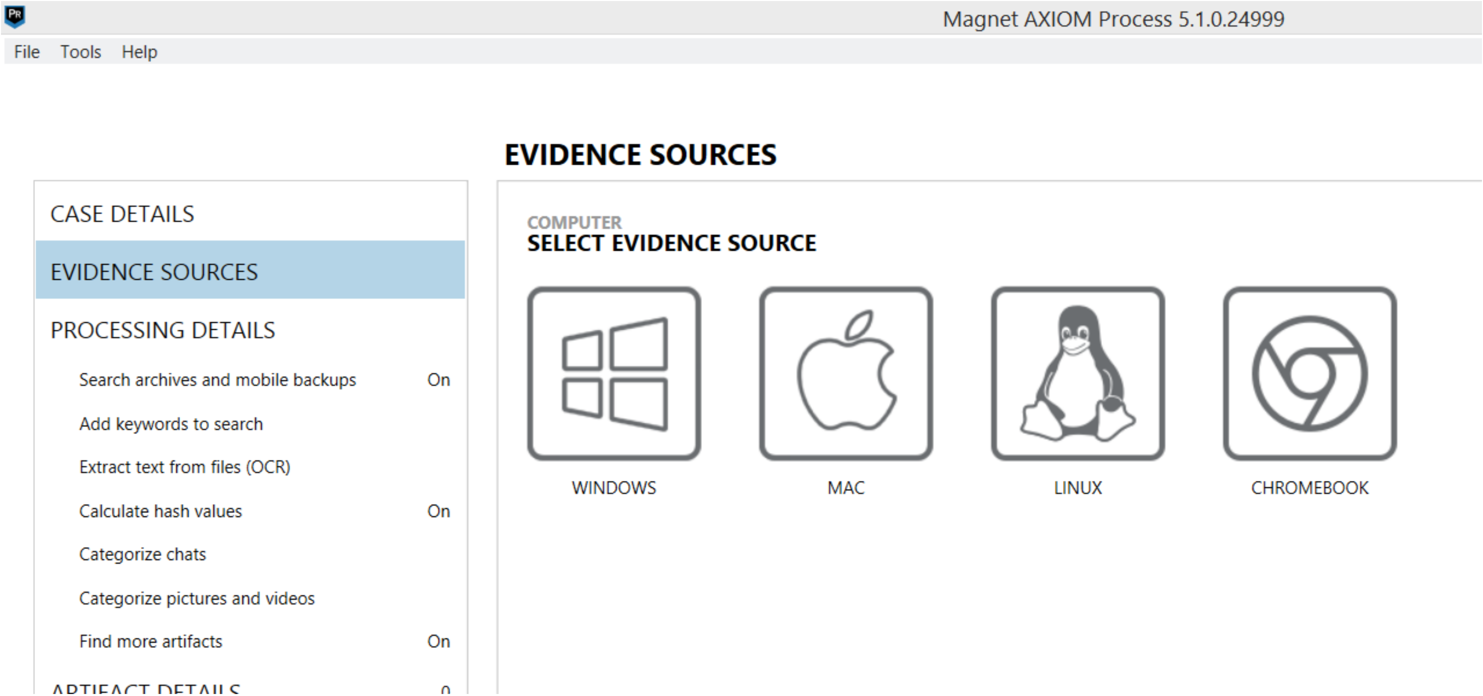
Targeted Location Quick Reference Guides

- Chromebook:
- https:///www.magnetforensics.com/blog/chromebook-data-locations/

- Takeout:
- https://www.magnetforensics.com/resources/targeted-locations-quick-reference-guide-for-android-and-google-takeouts/

Parsing Support

Direct support in AXIOM



EVIDENCE SOURCES

CASE DETAILS

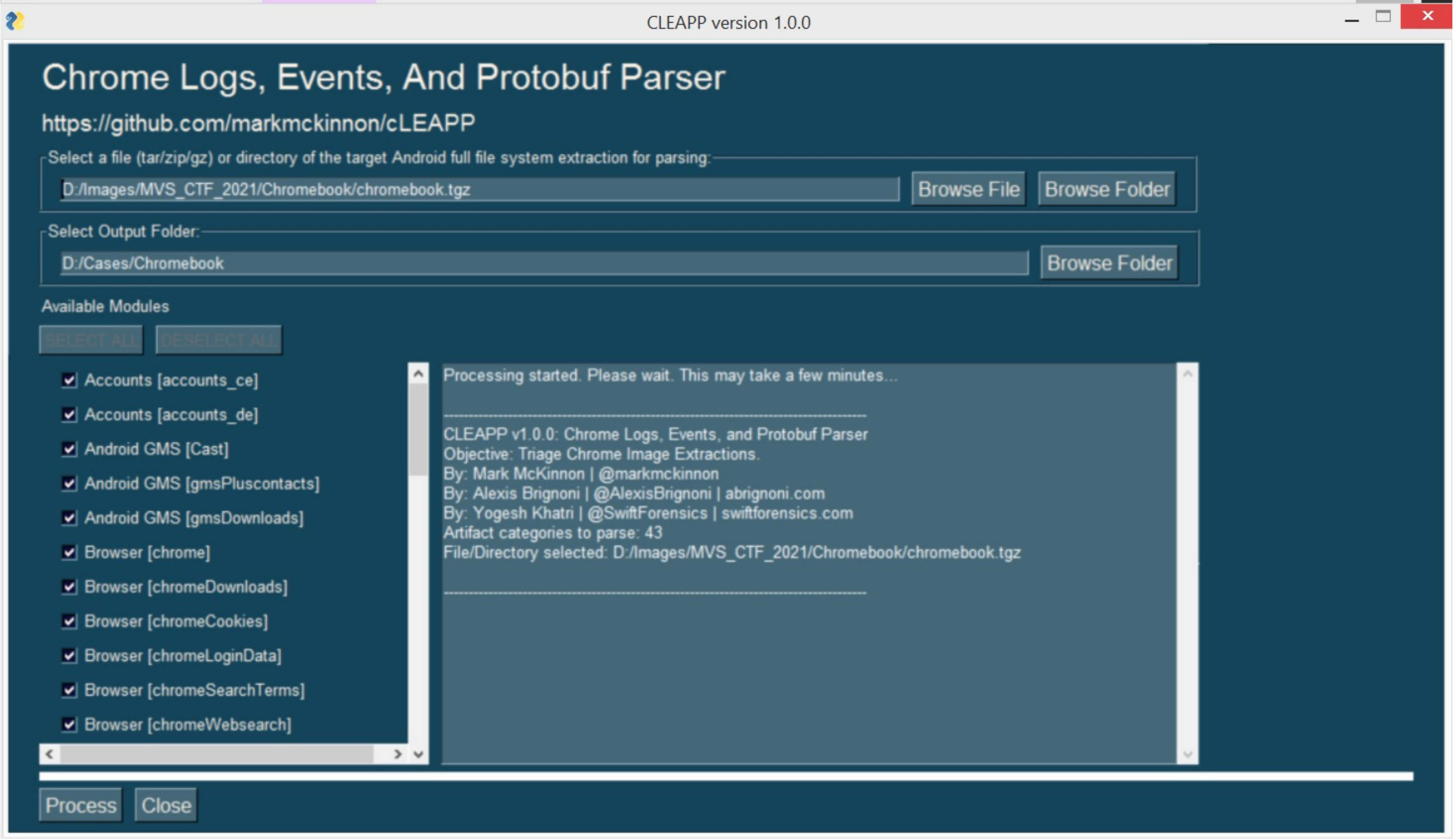
EVIDENCE SOURCES

PROCESSING DETAILS

Search archives and mobile backups	On
Add keywords to search	
Extract text from files (OCR)	
Calculate hash values	On
Categorize chats	
Categorize pictures and videos	
Find more artifacts	On

ARTIFACT DETAILS 0

COMPUTER
SELECT EVIDENCE SOURCE



Chrome Logs, Events, And Protobuf Parser

https://github.com/markmckinnon/cLEAPP

Select a file (tar/zip/gz) or directory of the target Android full file system extraction for parsing: D:/Images/MVS_CTF_2021/Chromebook/chromebook.tgz

Select Output Folder: D:/Cases/Chromebook

Available Modules

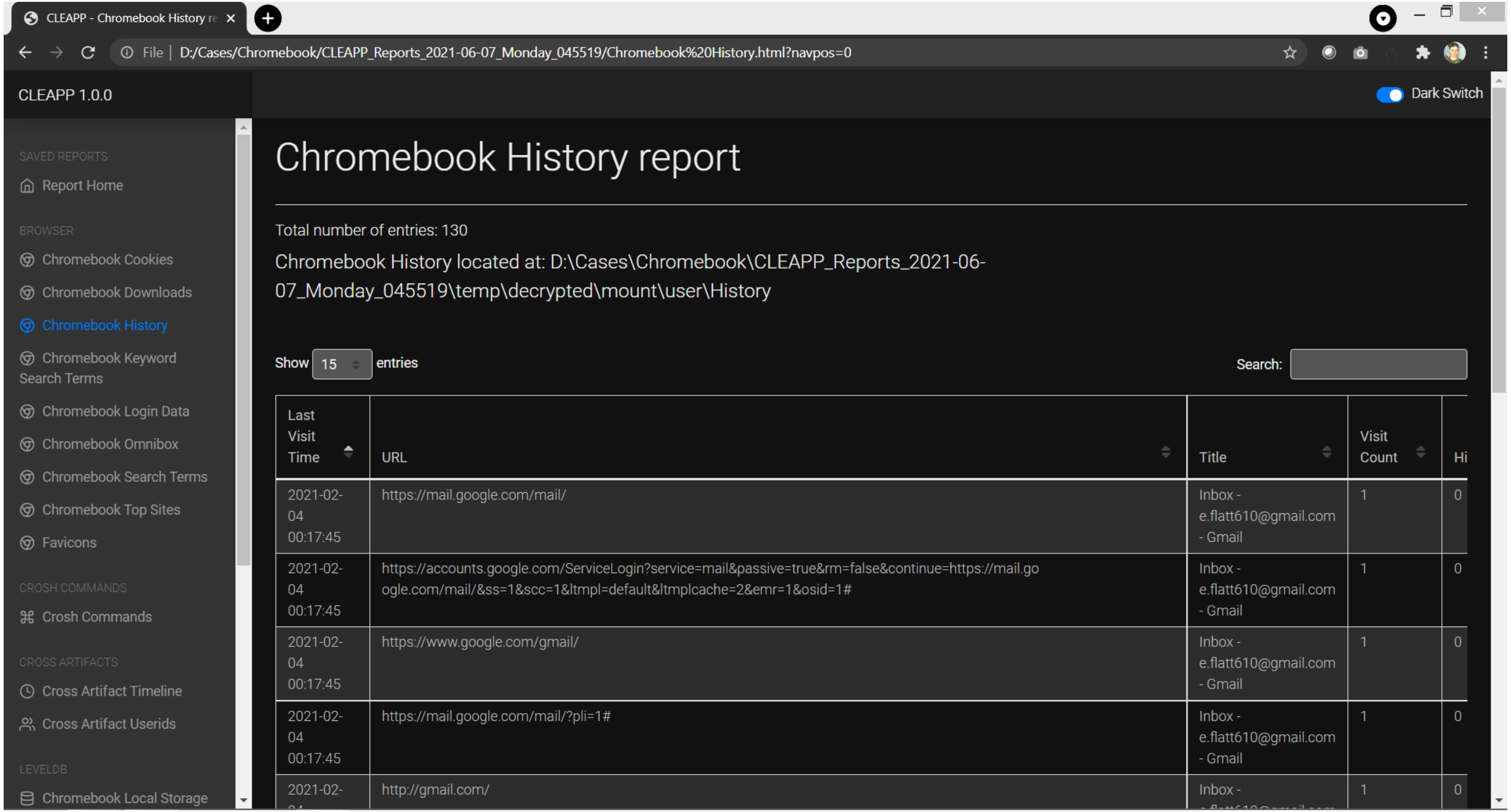
- ☑ Accounts [accounts_ce]
- ☑ Accounts [accounts_de]
- ☑ Android GMS [Cast]
- ☑ Android GMS [gmsPluscontacts]
- ☑ Android GMS [gmsDownloads]
- ☑ Browser [chrome]
- ☑ Browser [chromeDownloads]
- ☑ Browser [chromeCookies]
- ☑ Browser [chromeLoginData]
- ☑ Browser [chromeSearchTerms]
- ☑ Browser [chromeWebsearch]

```
Processing started. Please wait. This may take a few minutes...

--------------------------------------------------------------------------------
CLEAPP v1.0.0: Chrome Logs, Events, and Protobuf Parser
Objective: Triage Chrome Image Extractions.
By: Mark McKinnon | @markmckinnon
By: Alexis Brignoni | @AlexisBrignoni | abrignoni.com
By: Yogesh Khatri | @SwiftForensics | swiftforensics.com
Artifact categories to parse: 43
File/Directory selected: D:/Images/MVS_CTF_2021/Chromebook/chromebook.tgz

--------------------------------------------------------------------------------
```

- https://github.com/markmckinnon/cLeapp



Chromebook History report

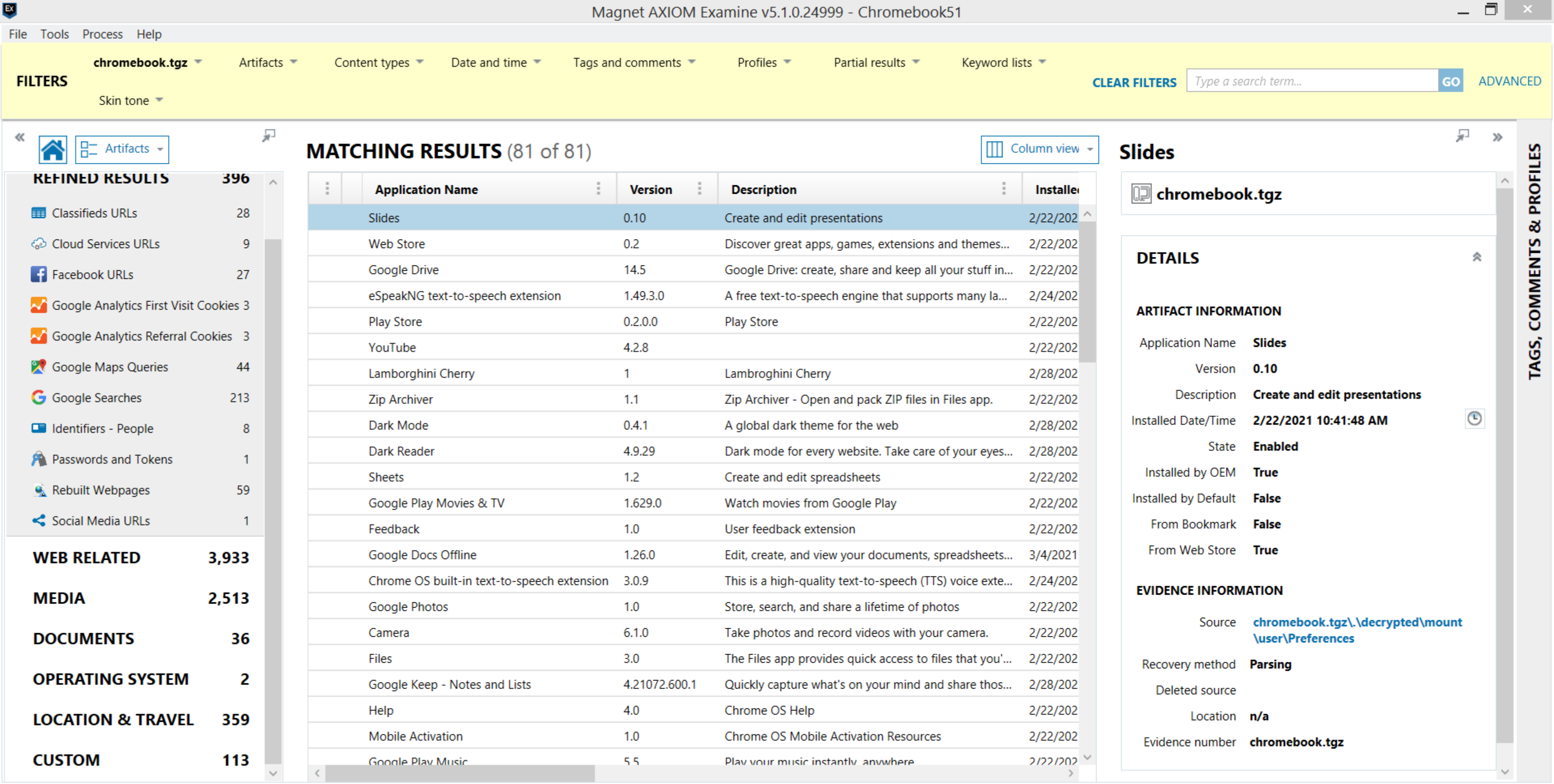
Total number of entries: 130

Chromebook History located at: D:\Cases\Chromebook\CLEAPP_Reports_2021-06-07_Monday_045519\temp\decrypted\mount\user\History

Show 15 entries

Search:

Last Visit Time	URL	Title	Visit Count	Hi
2021-02-04 00:17:45	https://mail.google.com/mail/	Inbox - e.flatt610@gmail.com - Gmail	1	0
2021-02-04 00:17:45	https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&scc=1&ltmpl=default&ltmplcache=2&emr=1&osid=1#	Inbox - e.flatt610@gmail.com - Gmail	1	0
2021-02-04 00:17:45	https://www.google.com/gmail/	Inbox - e.flatt610@gmail.com - Gmail	1	0
2021-02-04 00:17:45	https://mail.google.com/mail/?pli=1#	Inbox - e.flatt610@gmail.com - Gmail	1	0
2021-02-	http://gmail.com/	Inbox -	1	0



REFINED RESULTS	396
Classifieds URLs	28
Cloud Services URLs	9
Facebook URLs	27
Google Analytics First Visit Cookies	3
Google Analytics Referral Cookies	3
Google Maps Queries	44
Google Searches	213
Identifiers - People	8
Passwords and Tokens	1
Rebuilt Webpages	59
Social Media URLs	1
WEB RELATED	3,933
MEDIA	2,513
DOCUMENTS	36
OPERATING SYSTEM	2
LOCATION & TRAVEL	359
CUSTOM	113

MATCHING RESULTS (81 of 81)

Application Name	Version	Description	Installe
Slides	0.10	Create and edit presentations	2/22/202
Web Store	0.2	Discover great apps, games, extensions and themes...	2/22/202
Google Drive	14.5	Google Drive: create, share and keep all your stuff in...	2/22/202
eSpeakNG text-to-speech extension	1.49.3.0	A free text-to-speech engine that supports many la...	2/24/202
Play Store	0.2.0.0	Play Store	2/22/202
YouTube	4.2.8		2/22/202
Lamborghini Cherry	1	Lambroghini Cherry	2/28/202
Zip Archiver	1.1	Zip Archiver - Open and pack ZIP files in Files app.	2/22/202
Dark Mode	0.4.1	A global dark theme for the web	2/28/202
Dark Reader	4.9.29	Dark mode for every website. Take care of your eyes...	2/28/202
Sheets	1.2	Create and edit spreadsheets	2/22/202
Google Play Movies & TV	1.629.0	Watch movies from Google Play	2/22/202
Feedback	1.0	User feedback extension	2/22/202
Google Docs Offline	1.26.0	Edit, create, and view your documents, spreadsheets...	3/4/2021
Chrome OS built-in text-to-speech extension	3.0.9	This is a high-quality text-to-speech (TTS) voice exte...	2/24/202
Google Photos	1.0	Store, search, and share a lifetime of photos	2/22/202
Camera	6.1.0	Take photos and record videos with your camera.	2/22/202
Files	3.0	The Files app provides quick access to files that you'...	2/22/202
Google Keep - Notes and Lists	4.21072.600.1	Quickly capture what's on your mind and share thos...	2/28/202
Help	4.0	Chrome OS Help	2/22/202
Mobile Activation	1.0	Chrome OS Mobile Activation Resources	2/22/202
Google Play Music	5.5	Play your music instantly, anywhere	2/22/202

Slides

chromebook.tgz

DETAILS

ARTIFACT INFORMATION

Application Name	Slides
Version	0.10
Description	Create and edit presentations
Installed Date/Time	2/22/2021 10:41:48 AM
State	Enabled
Installed by OEM	True
Installed by Default	False
From Bookmark	False
From Web Store	True

EVIDENCE INFORMATION

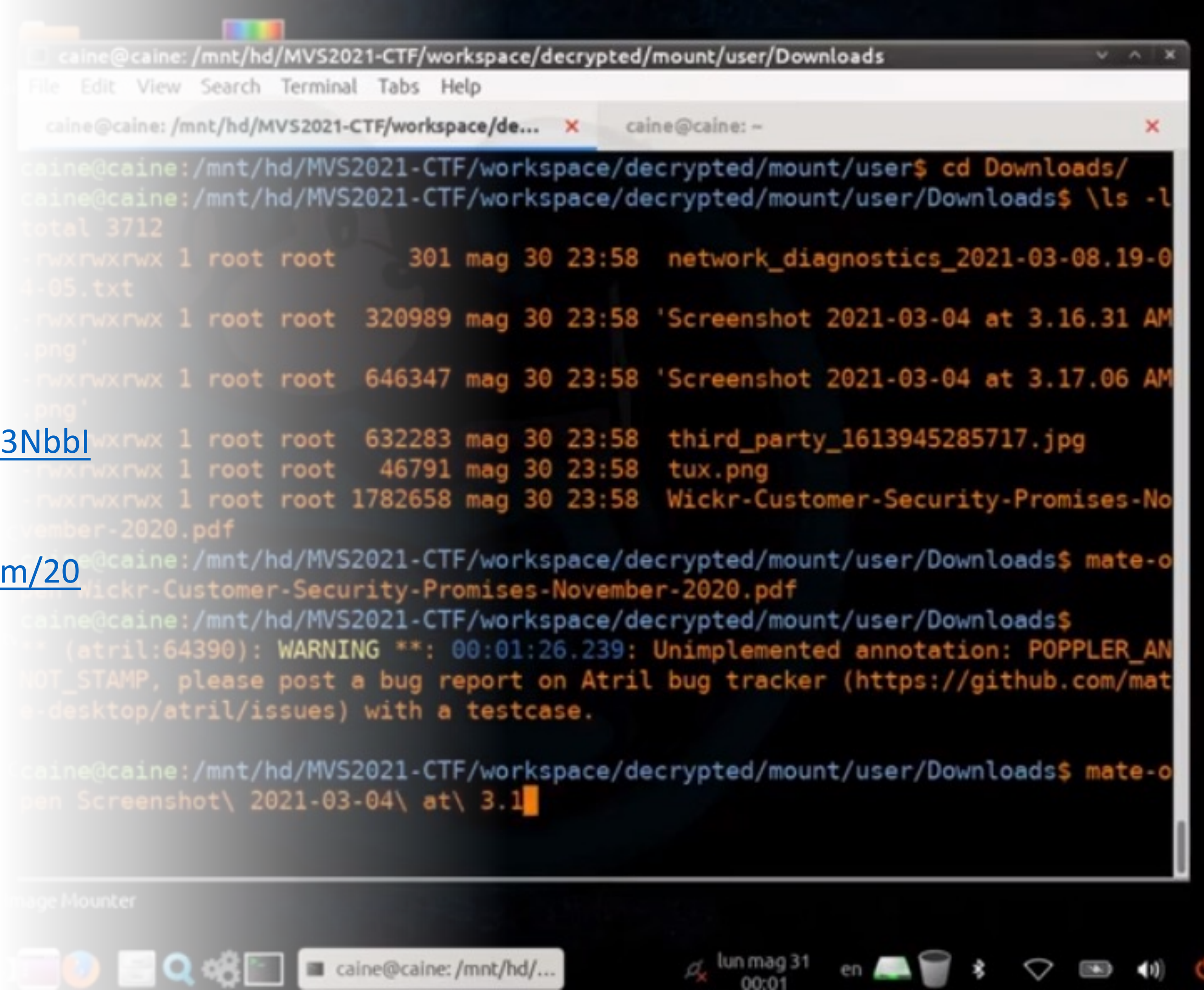
Source	chromebook.tgz\.\decrypted\mount \user\Preferences
Recovery method	Parsing
Deleted source	
Location	n/a
Evidence number	chromebook.tgz

Want to play with an image?

- Magnet 2021 CTF has a Full File System of a Chromebook and it’s associated Takeout
- https://cfreds.nist.gov/all/MagnetForensics/2021ChromebookMagnetCTF
- https://cfreds.nist.gov/all/MagnetForensics/2021TakeoutMagnetCTF

Solves - Chromebook

- BlueMonkey 4n6
- https://youtu.be/ozYdzM3NbbI
- Stark 4n6
- https://www.stark4n6.com/2021/05/mvs2021-ctf-chromebook.html



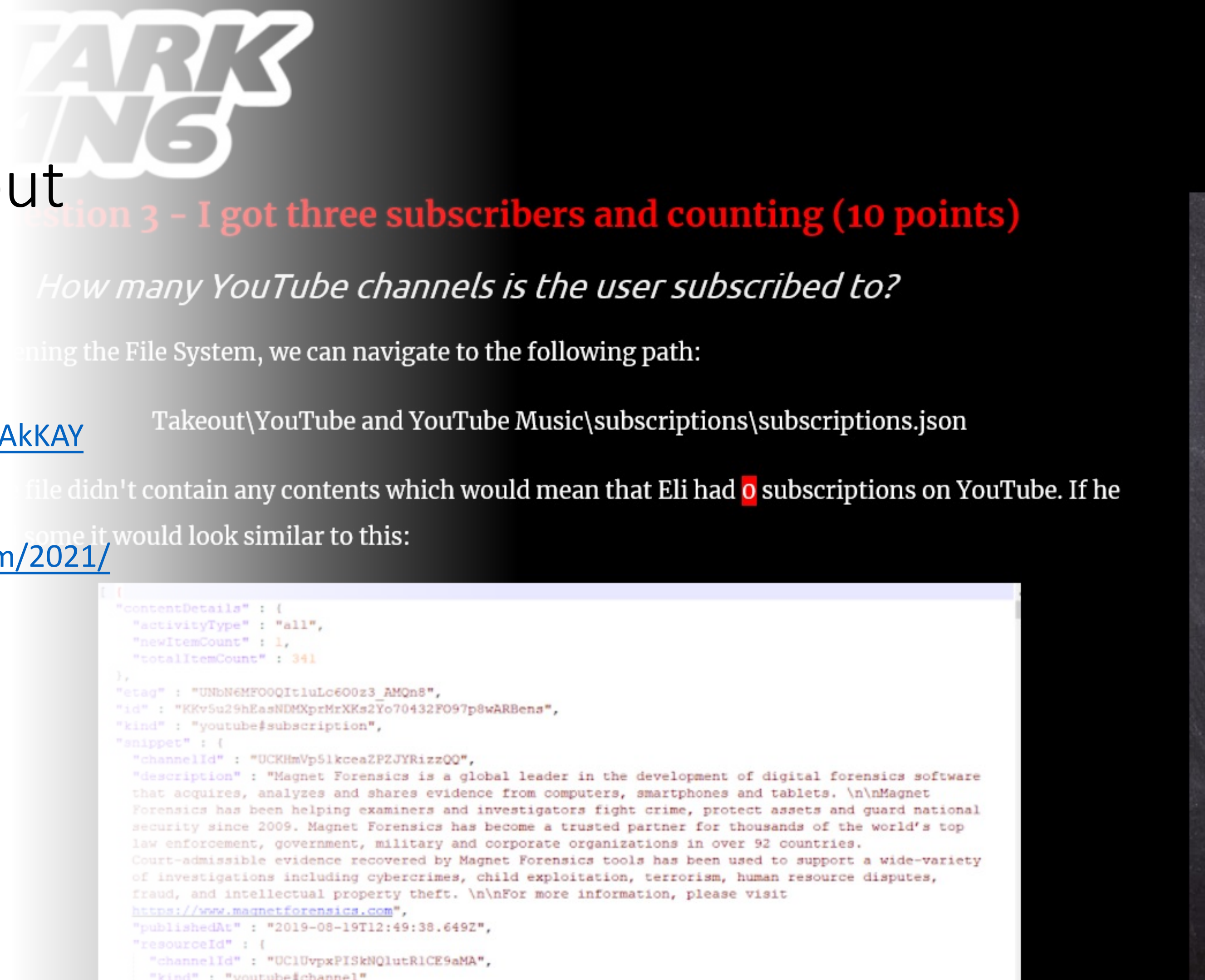
caine@caine: /mnt/hd/MVS2021-CTF/workspace/decrypted/mount/user/Downloads
File Edit View Search Terminal Tabs Help
caine@caine: /mnt/hd/MVS2021-CTF/workspace/de...
caine@caine: ~
Image Mounter
caine@caine: /mnt/hd/...
lun mag 31
00:01
en

```
caine@caine:/mnt/hd/MVS2021-CTF/workspace/decrypted/mount/user$ cd Downloads/
caine@caine:/mnt/hd/MVS2021-CTF/workspace/decrypted/mount/user/Downloads$ \ls -l
total 3712
-rwxrwxrwx 1 root root     301 mag 30 23:58  network_diagnostics_2021-03-08.19-0
4-05.txt
-rwxrwxrwx 1 root root  320989 mag 30 23:58 'Screenshot 2021-03-04 at 3.16.31 AM
.png'
-rwxrwxrwx 1 root root  646347 mag 30 23:58 'Screenshot 2021-03-04 at 3.17.06 AM
.png'
-rwxrwxrwx 1 root root  632283 mag 30 23:58  third_party_1613945285717.jpg
-rwxrwxrwx 1 root root   46791 mag 30 23:58  tux.png
-rwxrwxrwx 1 root root 1782658 mag 30 23:58  Wickr-Customer-Security-Promises-No
vember-2020.pdf
caine@caine:/mnt/hd/MVS2021-CTF/workspace/decrypted/mount/user/Downloads$ mate-o
pen Wickr-Customer-Security-Promises-November-2020.pdf
caine@caine:/mnt/hd/MVS2021-CTF/workspace/decrypted/mount/user/Downloads$
** (atril:64390): WARNING **: 00:01:26.239: Unimplemented annotation: POPPLER_AN
NOT_STAMP, please post a bug report on Atril bug tracker (https://github.com/mat
e-desktop/atril/issues) with a testcase.

caine@caine:/mnt/hd/MVS2021-CTF/workspace/decrypted/mount/user/Downloads$ mate-o
pen Screenshot\ 2021-03-04\ at\ 3.1
```

Solves - Takeout

- BlueMonkey 4n6
- https://youtu.be/v3WAsbAkKAY
- Stark 4n6
- https://www.stark4n6.com/2021/05/mvs2021-ctf-googletakeout.html



stion 3 - I got three subscribers and counting (10 points)

How many YouTube channels is the user subscribed to?

ning the File System, we can navigate to the following path:

Takeout\YouTube and YouTube Music\subscriptions\subscriptions.json

file didn't contain any contents which would mean that Eli had 0 subscriptions on YouTube. If he some it would look similar to this:

```
[ {
  "contentDetails" : {
    "activityType" : "all",
    "newItemCount" : 1,
    "totalItemCount" : 341
  },
  "etag" : "UNbN6MFOOQItluLc6O0z3_AMQn8",
  "id" : "KKv5u29hEasNDMXprMrXKs2Yo70432FO97p8wARBens",
  "kind" : "youtube#subscription",
  "snippet" : {
    "channelId" : "UCKHmVp5lkceaZPZJYRizzQQ",
    "description" : "Magnet Forensics is a global leader in the development of digital forensics software
    that acquires, analyzes and shares evidence from computers, smartphones and tablets. \n\nMagnet
    Forensics has been helping examiners and investigators fight crime, protect assets and guard national
    security since 2009. Magnet Forensics has become a trusted partner for thousands of the world's top
    law enforcement, government, military and corporate organizations in over 92 countries.
    Court-admissible evidence recovered by Magnet Forensics tools has been used to support a wide-variety
    of investigations including cybercrimes, child exploitation, terrorism, human resource disputes,
    fraud, and intellectual property theft. \n\nFor more information, please visit
    https://www.magnetforensics.com",
    "publishedAt" : "2019-08-19T12:49:38.649Z",
    "resourceId" : {
      "channelId" : "UC1UvpxPISkNQlutR1CE9aMA",
      "kind" : "youtube#channel"
```

Questions?

Jessica Hyde
@b1n2h3x

Hexordia.com