Chrome Nuts and Bolts: Chrome OS / Chromebook forensics

Jessica Hyde

Jessica's Introduction

Hello, my name is Jessica Hyde

- Hi Jessica!

Director, Forensics - Magnet Forensics

- Adjunct Professor – George Mason University
- Former forensic examiner and USMC veteran

Agenda

What is Chromebook / Chrome OS?

Why do we care?

What are the issues?

What have we learned?

What can we recover?

Summary

What is a Chromebook?

First Chromebooks were sold in 2011

Computers that run Google's Chrome OS

Designed to be used connected to the internet

Linux based

Most applications and user data lives in the cloud

Economical $150 - $999 range

Many manufacturers (HP, Google, Samsung, Asus, Acer, Lenovo, LG, etc.)

Image: Google

Chrome OS

- Integrated media player and file manager
- Supports Chrome Apps
- Android Apps available since 2016 via Google Play Store
- Linux desktop apps via “Crostini”
- Available only on hardware from Google partners
- Automatically updates to the latest version
- Can run on x86 or ARM-based processors
- Can support a hard drive

Image: Google

Chromium OS?

Open-source equivalent to Chrome

Available to be compiled from source code

Does not automatically update

Can be modified

Released 2009

Image: Google

Data Storage

Most data stored using Google Drive

- 100GB for 2 years free

However data may still be stored locally!

Image: Google

Why do we care?

Schools!

- Google for Education – 25 million students using Chromebook (Jan, 2018)

Bad Guys!

- Have received calls – Chromebook on-scene, what do I do?

Enterprise!

- Chrome Enterprise

Why do we care?

"The U.S. traditional PC market exhibited lower overall growth, contracting 3.4% in 3Q17," said Neha Mahajan, senior research analyst, Devices & Displays. "Despite the overall contraction, Chromebooks remain a source of optimism as the category gains momentum in sectors outside education, especially in retail and financial services."

Source: https://www.idc.com/getdoc.jsp?containerId=prUS43147217

What are the issues?

Imaging!

Operating System

Lack of research and methodologies

What aren’t we covering?

Imaging!

Why?

- We first want to research what data is available
- May require JTAG/Chip-off
- AND…. Decryption

So what are we covering?

Operating System and data recovered

Answer to this question:

Is it really worth even solving the encryption problem if everything is in the cloud anyway?

How did we get these images then?

Live acquisition in developer mode of VM running Chromium OS

On a Chromebook:

Older devices: physical switch under the battery compartment

Newer Devices:

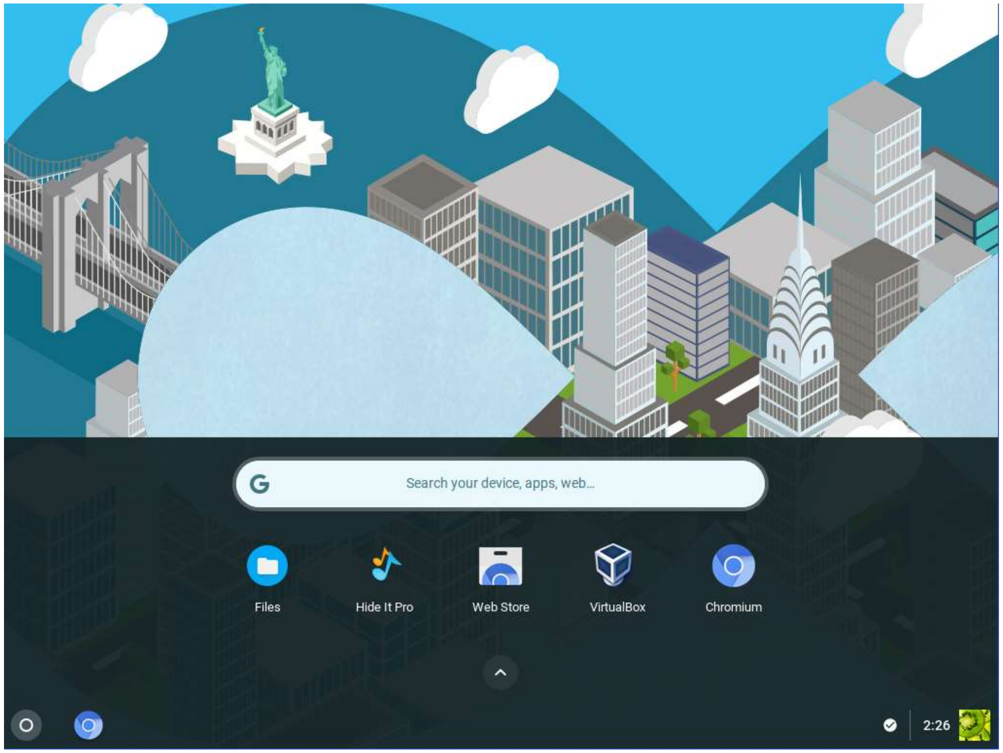
Esc/Refresh/Power together followed by Ctrl-D, and Ctrl-D

System is wiped of user data and security functions are dropped

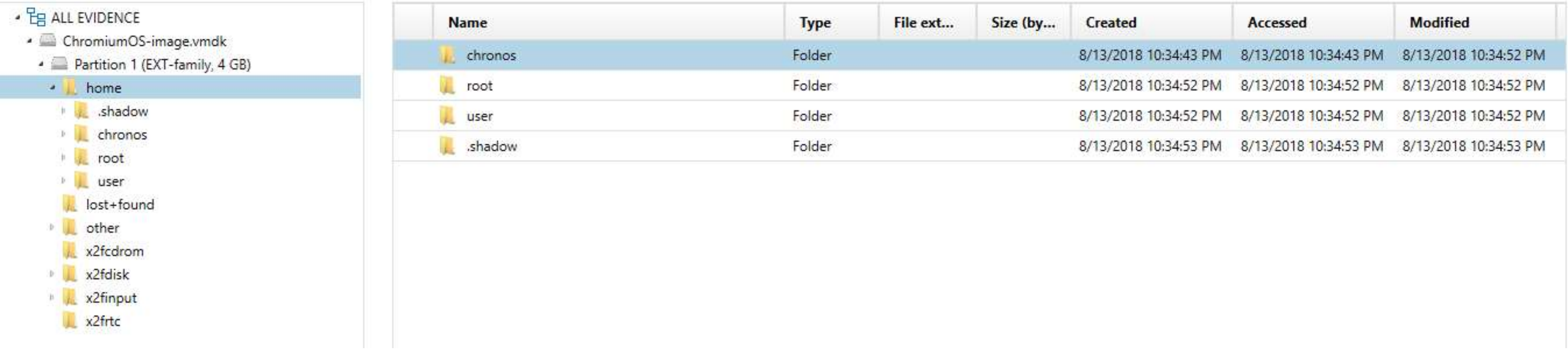
What do we know about Chromium OS?

Linux Based

Chromium does not have the same security features as Chrome OS



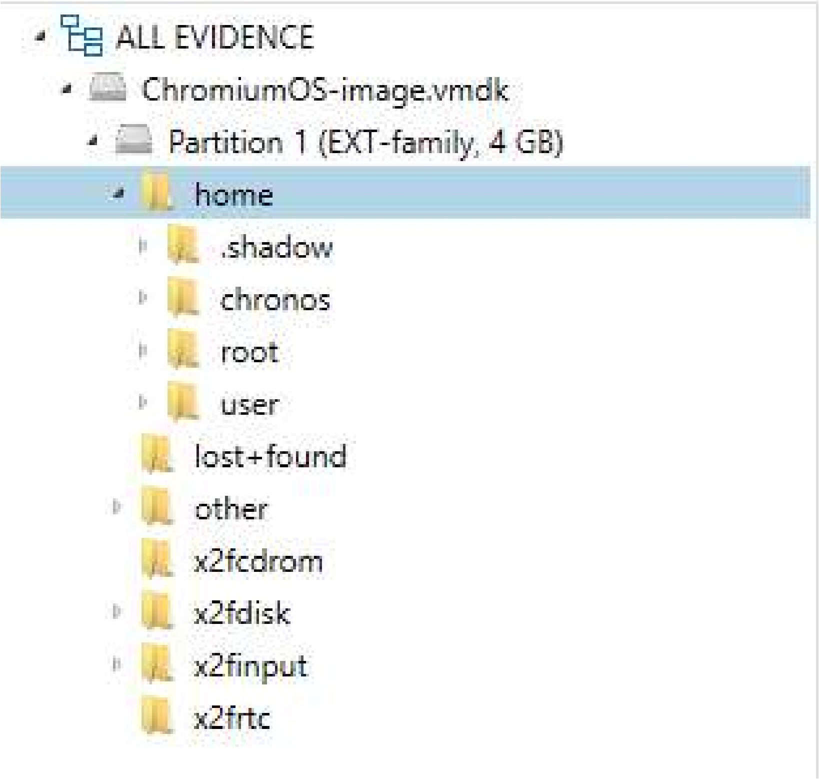
What do we know about Chromium OS?



- ALL EVIDENCE
  - ChromiumOS-image.vmdk
    - Partition 1 (EXT-family, 4 GB)
      - home
        - .shadow
        - chronos
        - root
        - user
      - lost+found
      - other
      - x2fcdrom
      - x2fdisk
      - x2finput
      - x2frtc

Name	Type	File ext...	Size (by...	Created	Accessed	Modified
chronos	Folder			8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/2018 10:34:52 PM
root	Folder			8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM
user	Folder			8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM
.shadow	Folder			8/13/2018 10:34:53 PM	8/13/2018 10:34:53 PM	8/13/2018 10:34:53 PM

What do we know about Chromium OS?



```
ALL EVIDENCE
  ChromiumOS-image.vmdk
    Partition 1 (EXT-family, 4 GB)
      home
        .shadow
        chronos
        root
        user
      lost+found
      other
      x2fcdrom
      x2fdisk
      x2finput
      x2frtc
```

.shadow

chronos

root

user

Browser History

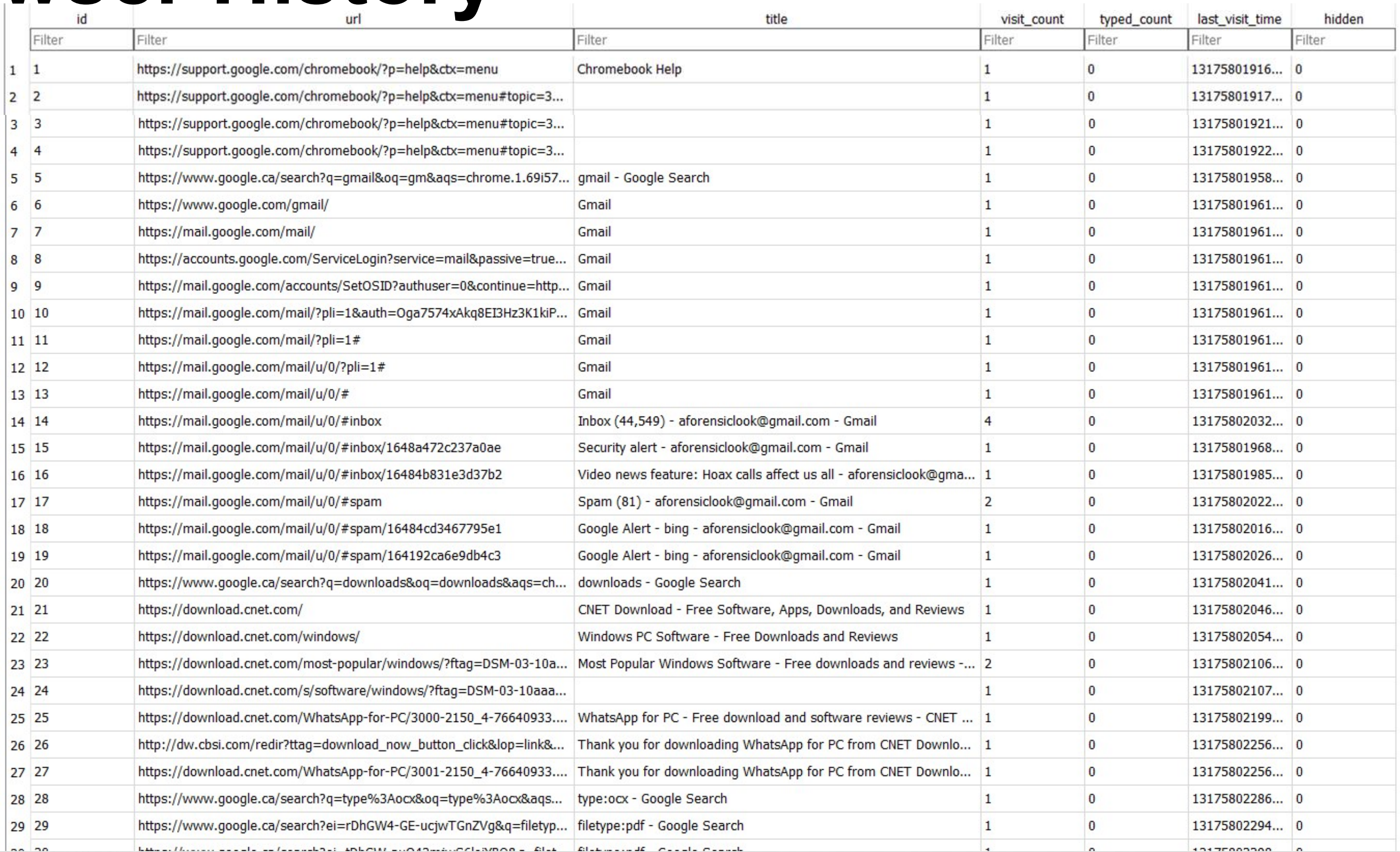
Each entry appears in the following paths

- \home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\History
- \home\chronos\user\History
- \home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\History
- \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\History

SQLite DB

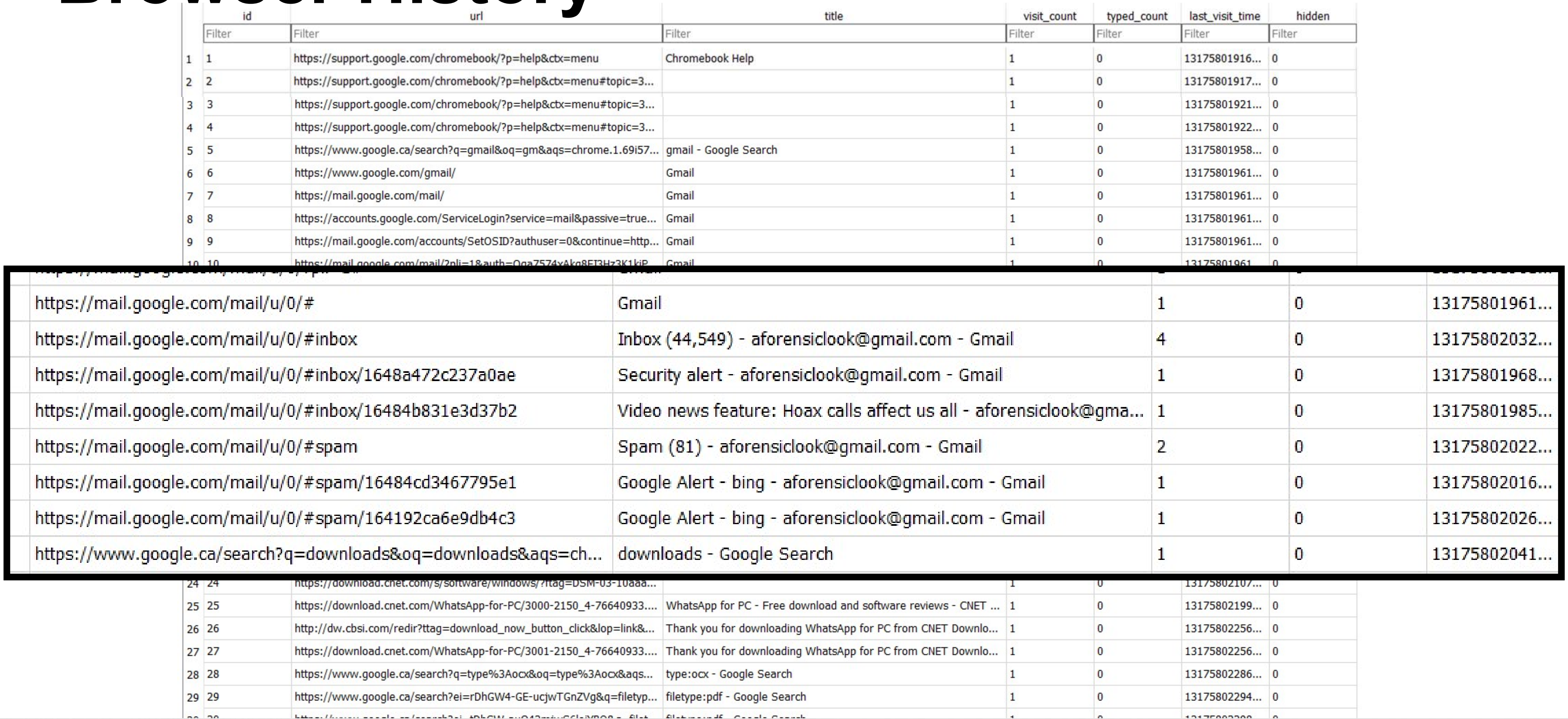
Appear to be the same file, same timestamp and each entry has the same file offset

Browser History



	id	url	title	visit_count	typed_count	last_visit_time	hidden
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	https://support.google.com/chromebook/?p=help&ctx=menu	Chromebook Help	1	0	13175801916...	0
2	2	https://support.google.com/chromebook/?p=help&ctx=menu#topic=3...		1	0	13175801917...	0
3	3	https://support.google.com/chromebook/?p=help&ctx=menu#topic=3...		1	0	13175801921...	0
4	4	https://support.google.com/chromebook/?p=help&ctx=menu#topic=3...		1	0	13175801922...	0
5	5	https://www.google.ca/search?q=gmail&oq=gm&aqs=chrome.1.69i57...	gmail - Google Search	1	0	13175801958...	0
6	6	https://www.google.com/gmail/	Gmail	1	0	13175801961...	0
7	7	https://mail.google.com/mail/	Gmail	1	0	13175801961...	0
8	8	https://accounts.google.com/ServiceLogin?service=mail&passive=true...	Gmail	1	0	13175801961...	0
9	9	https://mail.google.com/accounts/SetOSID?authuser=0&continue=http...	Gmail	1	0	13175801961...	0
10	10	https://mail.google.com/mail/?pli=1&auth=Oga7574xAkq8EI3Hz3K1kiP...	Gmail	1	0	13175801961...	0
11	11	https://mail.google.com/mail/?pli=1#	Gmail	1	0	13175801961...	0
12	12	https://mail.google.com/mail/u/0/?pli=1#	Gmail	1	0	13175801961...	0
13	13	https://mail.google.com/mail/u/0/#	Gmail	1	0	13175801961...	0
14	14	https://mail.google.com/mail/u/0/#inbox	Inbox (44,549) - aforensiclook@gmail.com - Gmail	4	0	13175802032...	0
15	15	https://mail.google.com/mail/u/0/#inbox/1648a472c237a0ae	Security alert - aforensiclook@gmail.com - Gmail	1	0	13175801968...	0
16	16	https://mail.google.com/mail/u/0/#inbox/16484b831e3d37b2	Video news feature: Hoax calls affect us all - aforensiclook@gma...	1	0	13175801985...	0
17	17	https://mail.google.com/mail/u/0/#spam	Spam (81) - aforensiclook@gmail.com - Gmail	2	0	13175802022...	0
18	18	https://mail.google.com/mail/u/0/#spam/16484cd3467795e1	Google Alert - bing - aforensiclook@gmail.com - Gmail	1	0	13175802016...	0
19	19	https://mail.google.com/mail/u/0/#spam/164192ca6e9db4c3	Google Alert - bing - aforensiclook@gmail.com - Gmail	1	0	13175802026...	0
20	20	https://www.google.ca/search?q=downloads&oq=downloads&aqs=ch...	downloads - Google Search	1	0	13175802041...	0
21	21	https://download.cnet.com/	CNET Download - Free Software, Apps, Downloads, and Reviews	1	0	13175802046...	0
22	22	https://download.cnet.com/windows/	Windows PC Software - Free Downloads and Reviews	1	0	13175802054...	0
23	23	https://download.cnet.com/most-popular/windows/?ftag=DSM-03-10a...	Most Popular Windows Software - Free downloads and reviews -...	2	0	13175802106...	0
24	24	https://download.cnet.com/s/software/windows/?ftag=DSM-03-10aaa...		1	0	13175802107...	0
25	25	https://download.cnet.com/WhatsApp-for-PC/3000-2150_4-76640933....	WhatsApp for PC - Free download and software reviews - CNET ...	1	0	13175802199...	0
26	26	http://dw.cbsi.com/redir?ttag=download_now_button_click&lop=link&...	Thank you for downloading WhatsApp for PC from CNET Downlo...	1	0	13175802256...	0
27	27	https://download.cnet.com/WhatsApp-for-PC/3001-2150_4-76640933....	Thank you for downloading WhatsApp for PC from CNET Downlo...	1	0	13175802256...	0
28	28	https://www.google.ca/search?q=type%3Aocx&oq=type%3Aocx&aqs...	type:ocx - Google Search	1	0	13175802286...	0
29	29	https://www.google.ca/search?ei=rDhGW4-GE-ucjwTGnZVg&q=filetyp...	filetype:pdf - Google Search	1	0	13175802294...	0

Browser History



	id	url	title	visit_count	typed_count	last_visit_time	hidden
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	https://support.google.com/chromebook/?p=help&ctx=menu	Chromebook Help	1	0	13175801916...	0
2	2	https://support.google.com/chromebook/?p=help&ctx=menu#topic=3...		1	0	13175801917...	0
3	3	https://support.google.com/chromebook/?p=help&ctx=menu#topic=3...		1	0	13175801921...	0
4	4	https://support.google.com/chromebook/?p=help&ctx=menu#topic=3...		1	0	13175801922...	0
5	5	https://www.google.ca/search?q=gmail&oq=gm&aqs=chrome.1.69i57...	gmail - Google Search	1	0	13175801958...	0
6	6	https://www.google.com/gmail/	Gmail	1	0	13175801961...	0
7	7	https://mail.google.com/mail/	Gmail	1	0	13175801961...	0
8	8	https://accounts.google.com/ServiceLogin?service=mail&passive=true...	Gmail	1	0	13175801961...	0
9	9	https://mail.google.com/accounts/SetOSID?authuser=0&continue=http...	Gmail	1	0	13175801961...	0
10	10	https://mail.google.com/mail/?pli=1&auth=Oga7574xAkq8EI3Hz3K1kiP...	Gmail	1	0	13175801961...	0

https://mail.google.com/mail/u/0/#	Gmail	1	0	13175801961...
https://mail.google.com/mail/u/0/#inbox	Inbox (44,549) - aforensiclook@gmail.com - Gmail	4	0	13175802032...
https://mail.google.com/mail/u/0/#inbox/1648a472c237a0ae	Security alert - aforensiclook@gmail.com - Gmail	1	0	13175801968...
https://mail.google.com/mail/u/0/#inbox/16484b831e3d37b2	Video news feature: Hoax calls affect us all - aforensiclook@gma...	1	0	13175801985...
https://mail.google.com/mail/u/0/#spam	Spam (81) - aforensiclook@gmail.com - Gmail	2	0	13175802022...
https://mail.google.com/mail/u/0/#spam/16484cd3467795e1	Google Alert - bing - aforensiclook@gmail.com - Gmail	1	0	13175802016...
https://mail.google.com/mail/u/0/#spam/164192ca6e9db4c3	Google Alert - bing - aforensiclook@gmail.com - Gmail	1	0	13175802026...
https://www.google.ca/search?q=downloads&oq=downloads&aqs=ch...	downloads - Google Search	1	0	13175802041...

24	24	https://download.cnet.com/s/software/windows/?ttag=DSM-03-10aaa...		1	0	13175802107...	0
25	25	https://download.cnet.com/WhatsApp-for-PC/3000-2150_4-76640933....	WhatsApp for PC - Free download and software reviews - CNET ...	1	0	13175802199...	0
26	26	http://dw.cbsi.com/redir?ttag=download_now_button_click&lop=link&...	Thank you for downloading WhatsApp for PC from CNET Downlo...	1	0	13175802256...	0
27	27	https://download.cnet.com/WhatsApp-for-PC/3001-2150_4-76640933....	Thank you for downloading WhatsApp for PC from CNET Downlo...	1	0	13175802256...	0
28	28	https://www.google.ca/search?q=type%3Aocx&oq=type%3Aocx&aqs...	type:ocx - Google Search	1	0	13175802286...	0
29	29	https://www.google.ca/search?ei=rDhGW4-GE-ucjwTGnZVg&q=filetyp...	filetype:pdf - Google Search	1	0	13175802294...	0

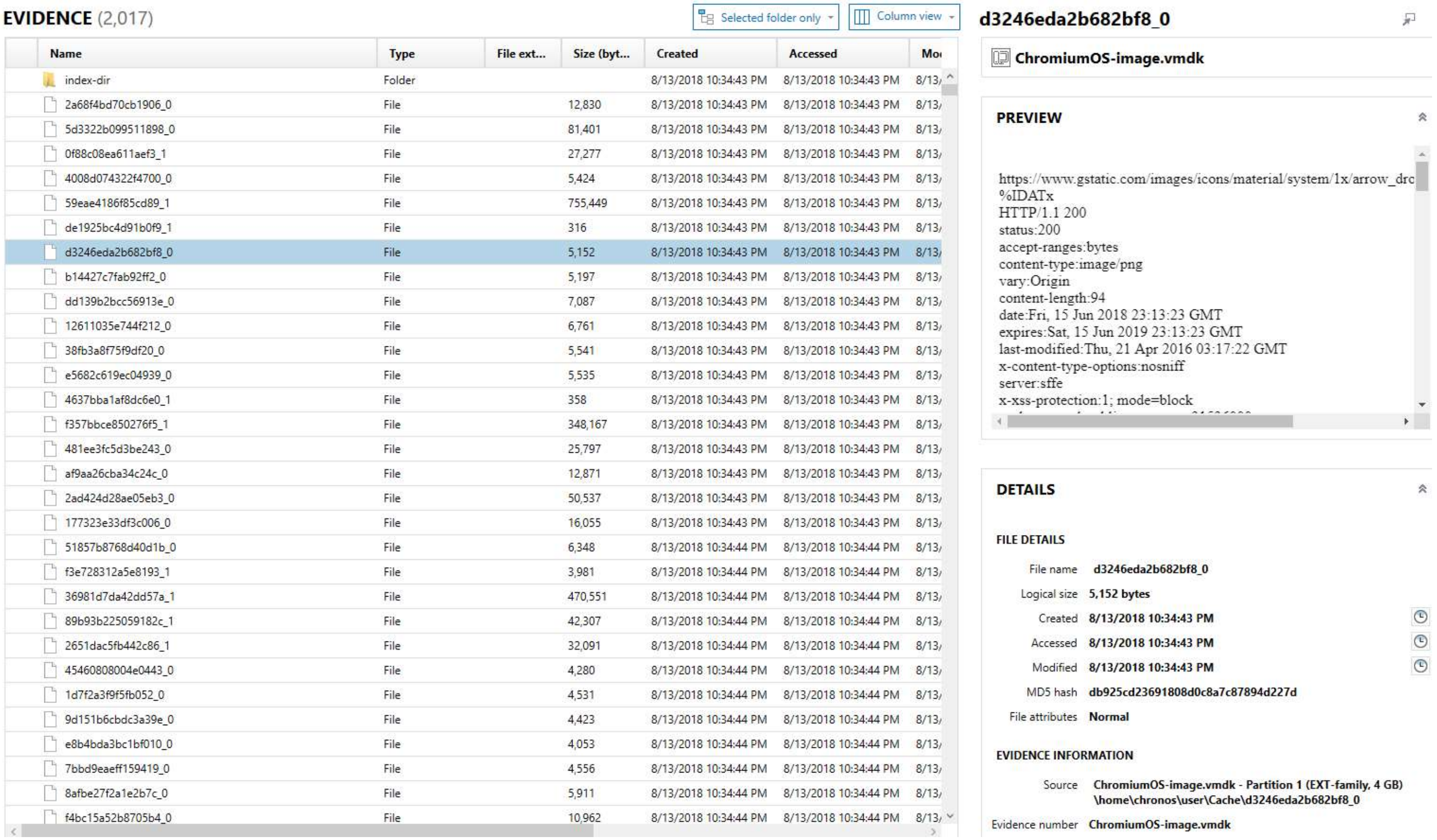
Browser Cache

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

Contains individual files with guids for each cache

Browser Cache



EVIDENCE (2,017)

Name	Type	File ext...	Size (byt...	Created	Accessed	Mo
index-dir	Folder			8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
2a68f4bd70cb1906_0	File		12,830	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
5d3322b099511898_0	File		81,401	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
0f88c08ea611aef3_1	File		27,277	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
4008d074322f4700_0	File		5,424	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
59eae4186f85cd89_1	File		755,449	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
de1925bc4d91b0f9_1	File		316	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
d3246eda2b682bf8_0	File		5,152	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
b14427c7fab92ff2_0	File		5,197	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
dd139b2bcc56913e_0	File		7,087	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
12611035e744f212_0	File		6,761	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
38fb3a8f75f9df20_0	File		5,541	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
e5682c619ec04939_0	File		5,535	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
4637bba1af8dc6e0_1	File		358	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
f357bbce850276f5_1	File		348,167	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
481ee3fc5d3be243_0	File		25,797	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
af9aa26cba34c24c_0	File		12,871	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
2ad424d28ae05eb3_0	File		50,537	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
177323e33df3c006_0	File		16,055	8/13/2018 10:34:43 PM	8/13/2018 10:34:43 PM	8/13/
51857b8768d40d1b_0	File		6,348	8/13/2018 10:34:44 PM	8/13/2018 10:34:44 PM	8/13/
f3e728312a5e8193_1	File		3,981	8/13/2018 10:34:44 PM	8/13/2018 10:34:44 PM	8/13/
36981d7da42dd57a_1	File		470,551	8/13/2018 10:34:44 PM	8/13/2018 10:34:44 PM	8/13/
89b93b225059182c_1	File		42,307	8/13/2018 10:34:44 PM	8/13/2018 10:34:44 PM	8/13/
2651dac5fb442c86_1	File		32,091	8/13/2018 10:34:44 PM	8/13/2018 10:34:44 PM	8/13/
45460808004e0443_0	File		4,280	8/13/2018 10:34:44 PM	8/13/2018 10:34:44 PM	8/13/
1d7f2a3f9f5fb052_0	File		4,531	8/13/2018 10:34:44 PM	8/13/2018 10:34:44 PM	8/13/
9d151b6cbdc3a39e_0	File		4,423	8/13/2018 10:34:44 PM	8/13/2018 10:34:44 PM	8/13/
e8b4bda3bc1bf010_0	File		4,053	8/13/2018 10:34:44 PM	8/13/2018 10:34:44 PM	8/13/
7bbd9eaeff159419_0	File		4,556	8/13/2018 10:34:44 PM	8/13/2018 10:34:44 PM	8/13/
8afbe27f2a1e2b7c_0	File		5,911	8/13/2018 10:34:44 PM	8/13/2018 10:34:44 PM	8/13/
f4bc15a52b8705b4_0	File		10,962	8/13/2018 10:34:44 PM	8/13/2018 10:34:44 PM	8/13/

d3246eda2b682bf8_0

ChromiumOS-image.vmdk

PREVIEW

```
https://www.gstatic.com/images/icons/material/system/1x/arrow_drc
%IDATx
HTTP/1.1 200
status:200
accept-ranges:bytes
content-type:image/png
vary:Origin
content-length:94
date:Fri, 15 Jun 2018 23:13:23 GMT
expires:Sat, 15 Jun 2019 23:13:23 GMT
last-modified:Thu, 21 Apr 2016 03:17:22 GMT
x-content-type-options:nosniff
server:sffe
x-xss-protection:1; mode=block
```

DETAILS

FILE DETAILS

File name d3246eda2b682bf8_0

Logical size 5,152 bytes

Created 8/13/2018 10:34:43 PM

Accessed 8/13/2018 10:34:43 PM

Modified 8/13/2018 10:34:43 PM

MD5 hash db925cd23691808d0c8a7c87894d227d

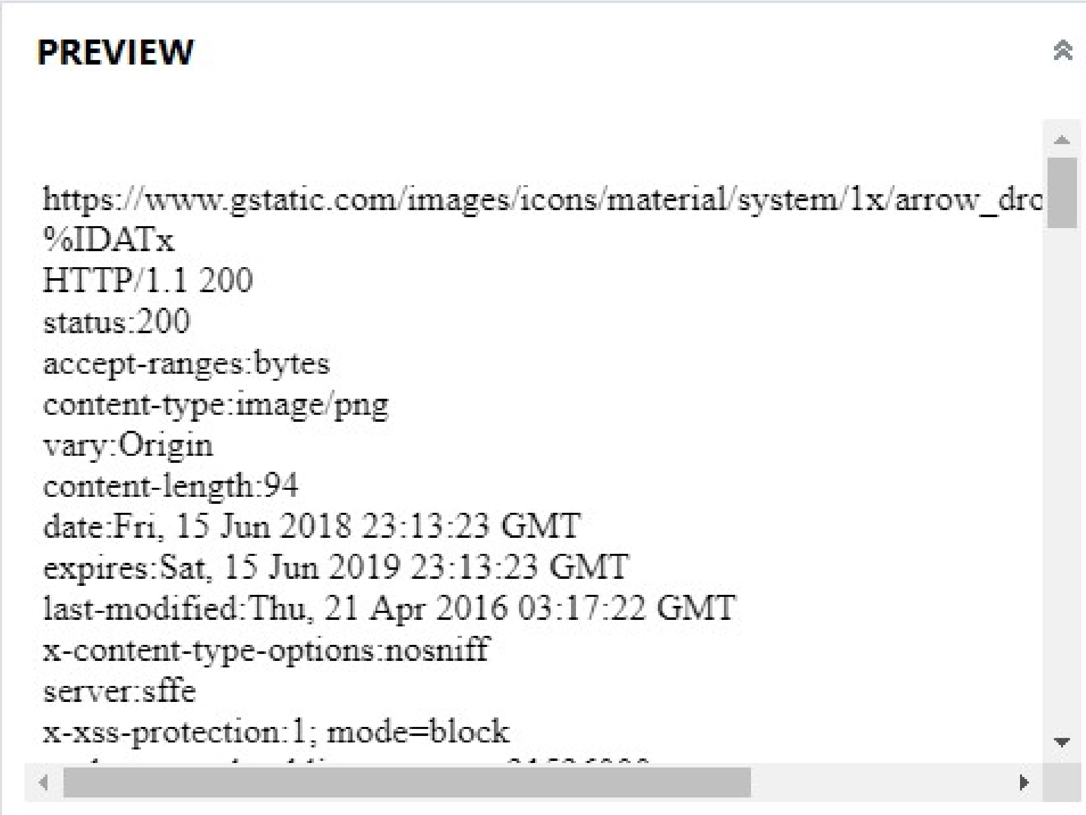
File attributes Normal

EVIDENCE INFORMATION

Source ChromiumOS-image.vmdk - Partition 1 (EXT-family, 4 GB)
\home\chronos\user\Cache\d3246eda2b682bf8_0

Evidence number ChromiumOS-image.vmdk

Browser Cache



```
https://www.gstatic.com/images/icons/material/system/1x/arrow_drc
%IDATx
HTTP/1.1 200
status:200
accept-ranges:bytes
content-type:image/png
vary:Origin
content-length:94
date:Fri, 15 Jun 2018 23:13:23 GMT
expires:Sat, 15 Jun 2019 23:13:23 GMT
last-modified:Thu, 21 Apr 2016 03:17:22 GMT
x-content-type-options:nosniff
server:sffe
x-xss-protection:1; mode=block
```

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

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

Browser History – Current Sessions

Each entry appears in the following paths

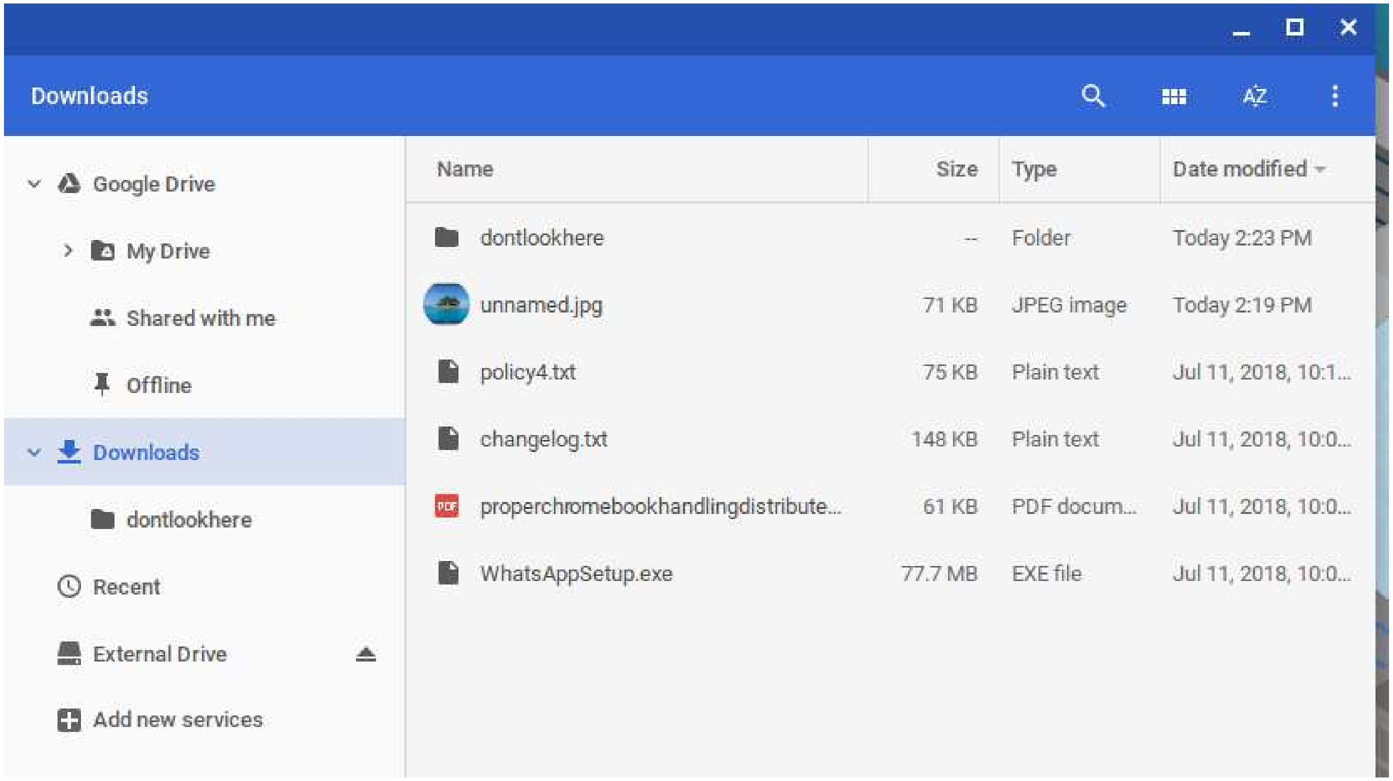
- \home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\Current Sessions
- \home\chronos\user\Current Sessions
- \home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\Current Sessions
- \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Current Sessions

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

Downloads

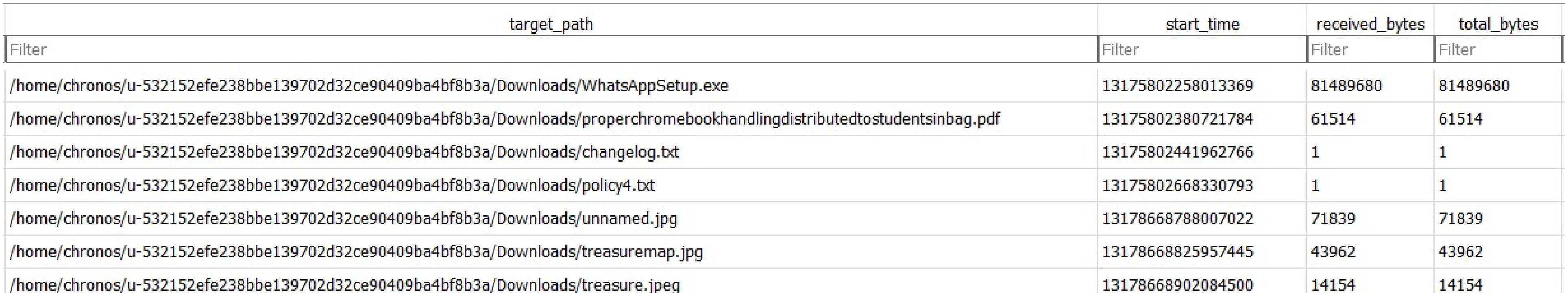


Name	Size	Type	Date modified
dontlookhere	--	Folder	Today 2:23 PM
unnamed.jpg	71 KB	JPEG image	Today 2:19 PM
policy4.txt	75 KB	Plain text	Jul 11, 2018, 10:1...
changelog.txt	148 KB	Plain text	Jul 11, 2018, 10:0...
properchromebookhandlingdistribute...	61 KB	PDF docum...	Jul 11, 2018, 10:0...
WhatsAppSetup.exe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

Downloads

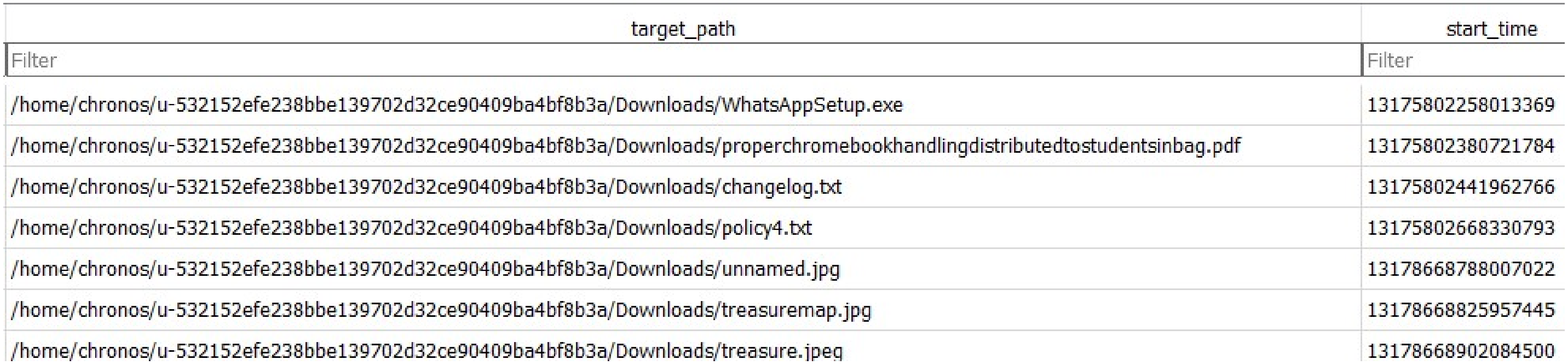
Can be found in Chrome Browser History (all 4 locations)

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

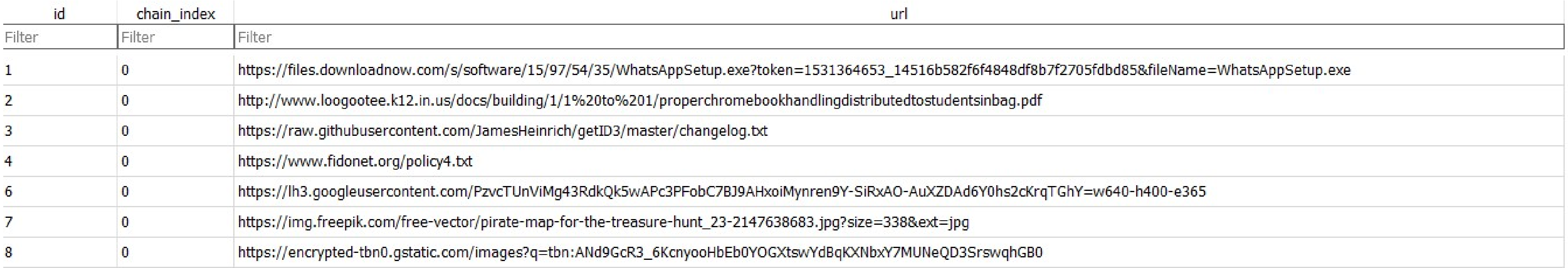


target_path	start_time
Filter	Filter
/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/WhatsAppSetup.exe	13175802258013369
/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/properchromebookhandlingdistributedtostudentsinbag.pdf	13175802380721784
/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/changelog.txt	13175802441962766
/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/policy4.txt	13175802668330793
/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/unnamed.jpg	13178668788007022
/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/treasuremap.jpg	13178668825957445
/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/treasure.jpeg	13178668902084500

Downloads

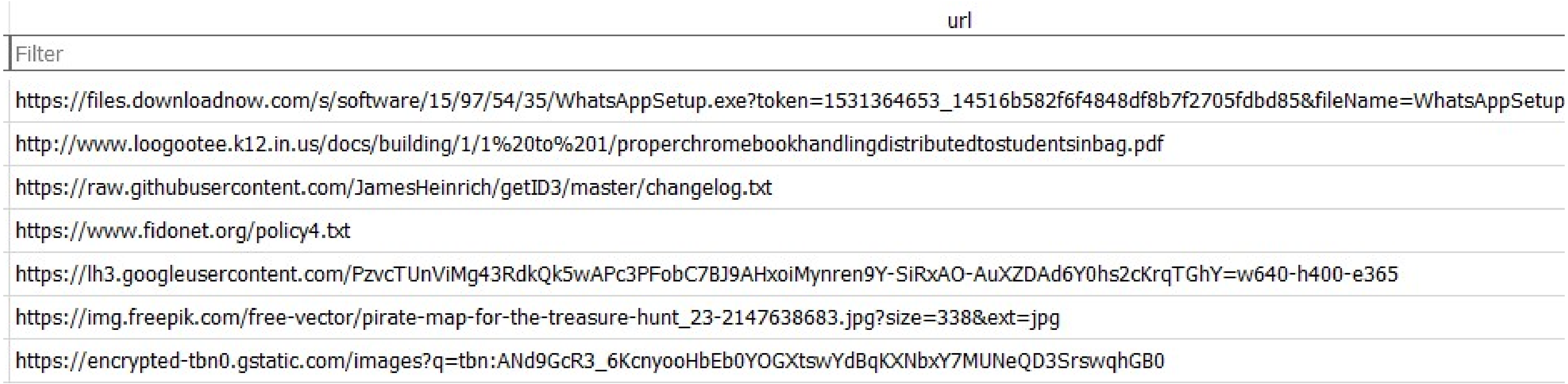
Which can be coordinated with the downloads_url_chains table

Also in the Chrome Browser History



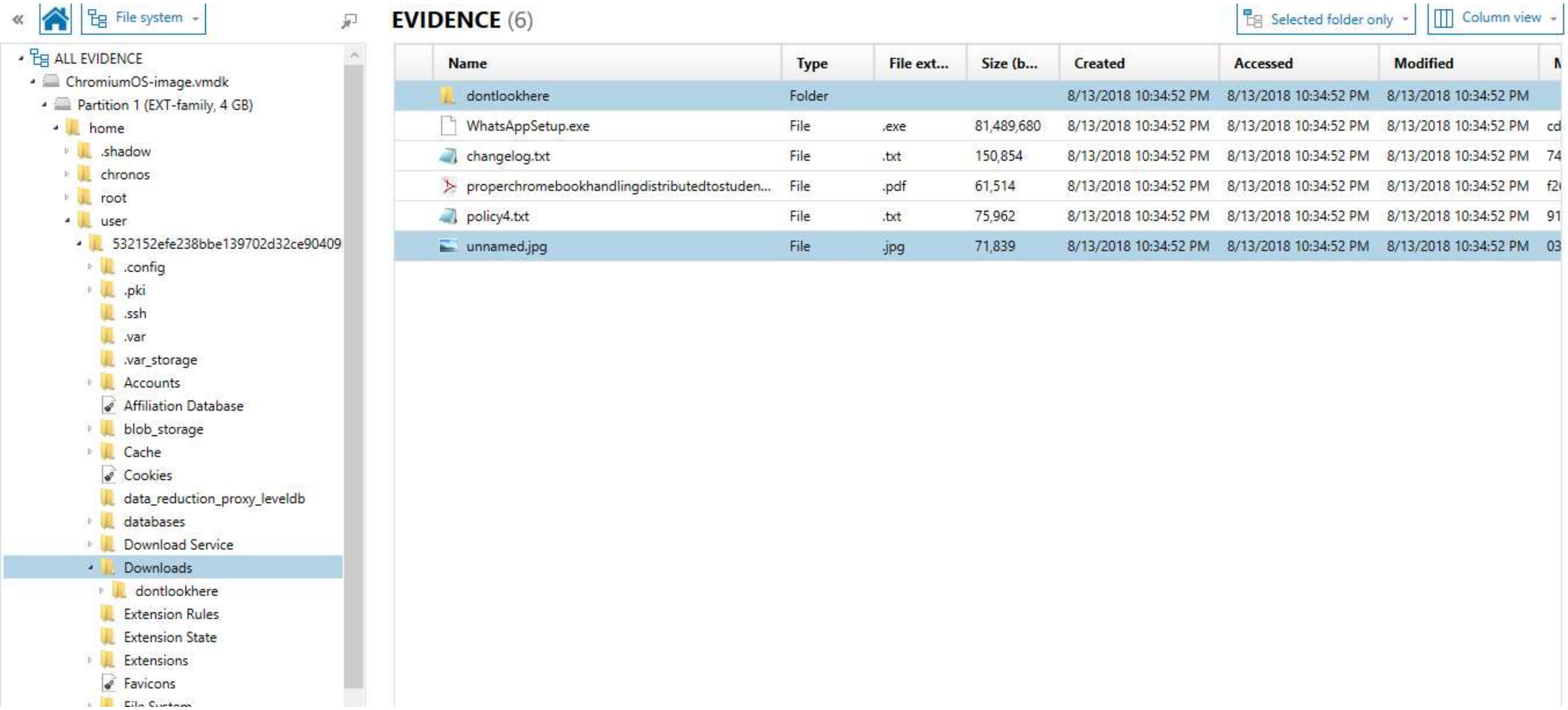
id	chain_index	url
Filter	Filter	Filter
1	0	https://files.downloadnow.com/s/software/15/97/54/35/WhatsAppSetup.exe?token=1531364653_14516b582f6f4848df8b7f2705fdbd85&fileName=WhatsAppSetup.exe
2	0	http://www.loogootee.k12.in.us/docs/building/1/1%20to%201/properchromebookhandlingdistributedtostudentsinbag.pdf
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

Downloads



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

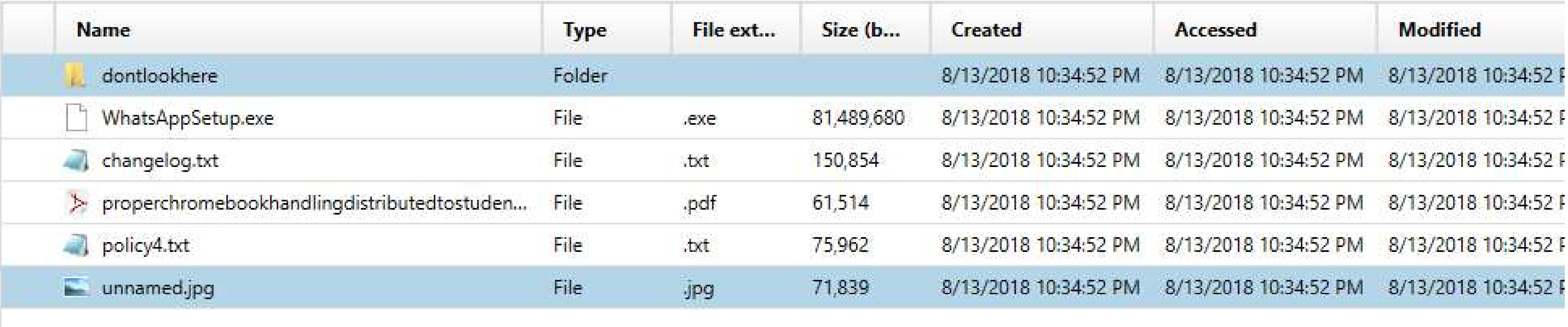
Downloads



- ALL EVIDENCE
  - ChromiumOS-image.vmdk
    - Partition 1 (EXT-family, 4 GB)
      - home
        - .shadow
        - chronos
        - root
        - user
          - 532152efe238bbe139702d32ce90409
            - .config
            - .pki
            - .ssh
            - .var
            - .var_storage
            - Accounts
            - Affiliation Database
            - blob_storage
            - Cache
            - Cookies
            - data_reduction_proxy_leveldb
            - databases
            - Download Service
            - Downloads
              - dontlookhere
            - Extension Rules
            - Extension State
            - Extensions
            - Favicons
            - File System

Name	Type	File ext...	Size (b...	Created	Accessed	Modified	M
dontlookhere	Folder			8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	
WhatsAppSetup.exe	File	.exe	81,489,680	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	cd
changelog.txt	File	.txt	150,854	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	74
properchromebookhandlingdistributedtostuden...	File	.pdf	61,514	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	f2
policy4.txt	File	.txt	75,962	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	91
unnamed.jpg	File	.jpg	71,839	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	03

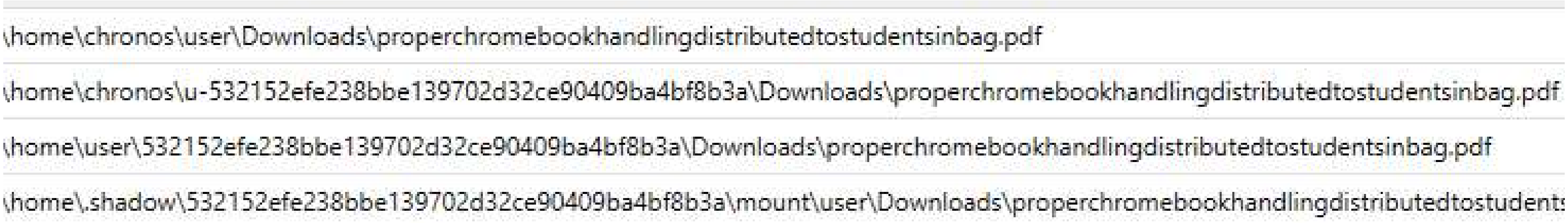
Downloads



Name	Type	File ext...	Size (b...	Created	Accessed	Modified
dontlookhere	Folder			8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 P
WhatsAppSetup.exe	File	.exe	81,489,680	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 P
changelog.txt	File	.txt	150,854	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 P
properchromebookhandlingdistributedtostuden...	File	.pdf	61,514	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 P
policy4.txt	File	.txt	75,962	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 P
unnamed.jpg	File	.jpg	71,839	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 PM	8/13/2018 10:34:52 P

Downloads

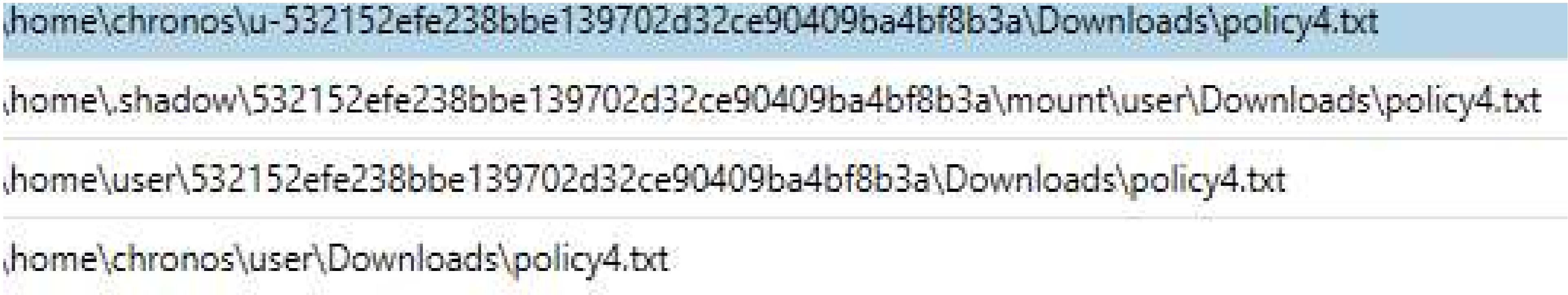
Just as before found in 4 locations



```
\home\chronos\user\Downloads\properchromebookhandlingdistributedtostudentsinbag.pdf
\home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\Downloads\properchromebookhandlingdistributedtostudentsinbag.pdf
\home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Downloads\properchromebookhandlingdistributedtostudentsinbag.pdf
\home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\Downloads\properchromebookhandlingdistributedtostudent
```

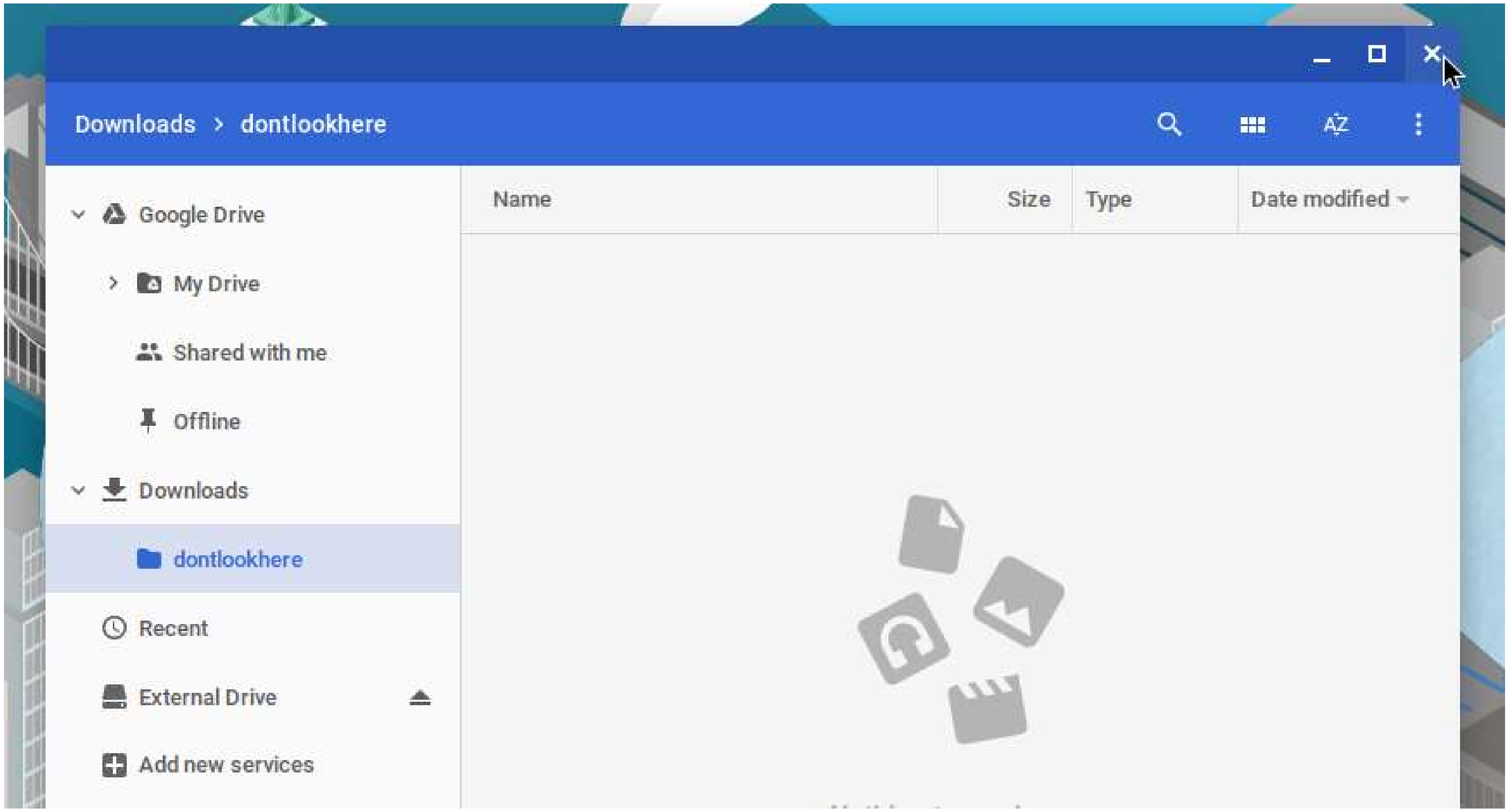
Downloads

Example: Policy4.txt



```
\home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\Downloads\policy4.txt
\home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\Downloads\policy4.txt
\home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Downloads\policy4.txt
\home\chronos\user\Downloads\policy4.txt
```

Hidden Folder

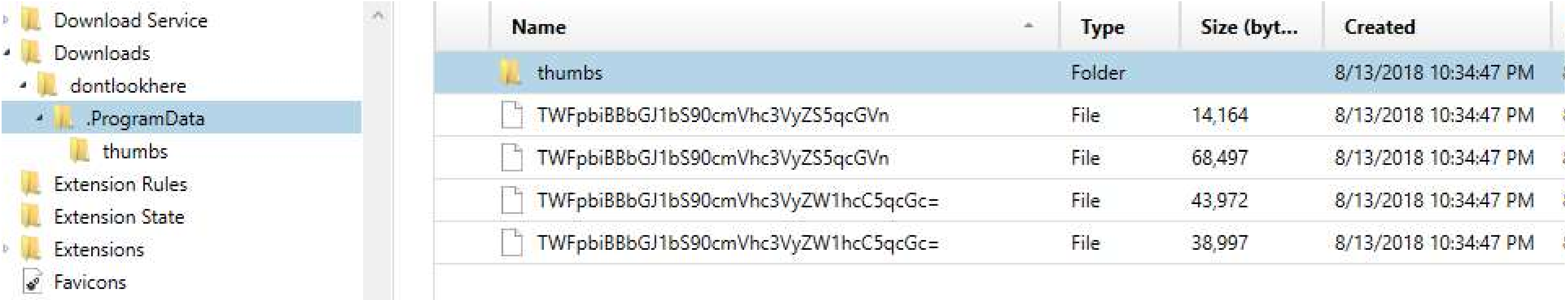


Hidden Folder

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

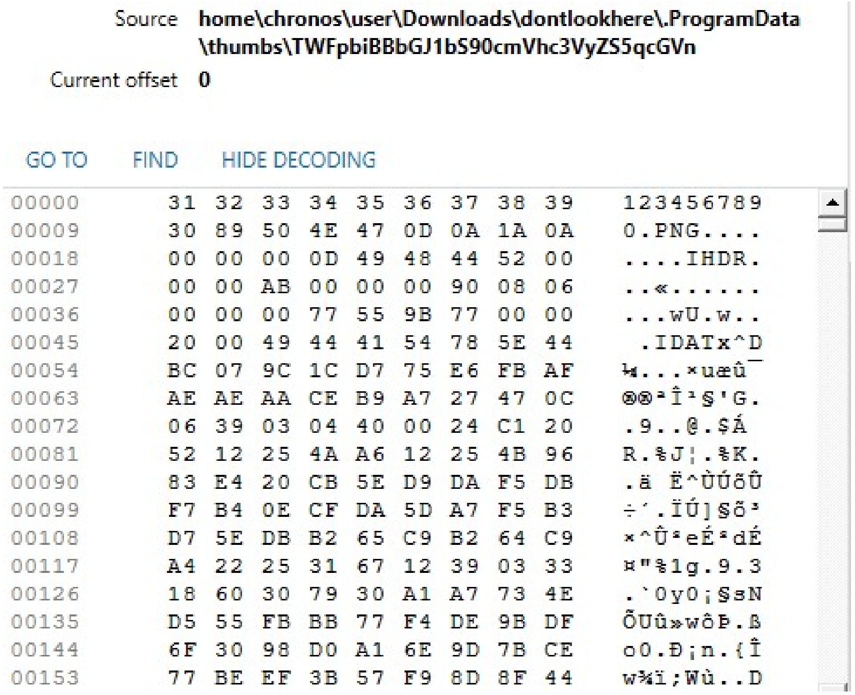
Hidden Folder

The password is appended to the front of the file.

In this case the password =

‘1234567890’

True for the .jpg, .png, and thumbnails

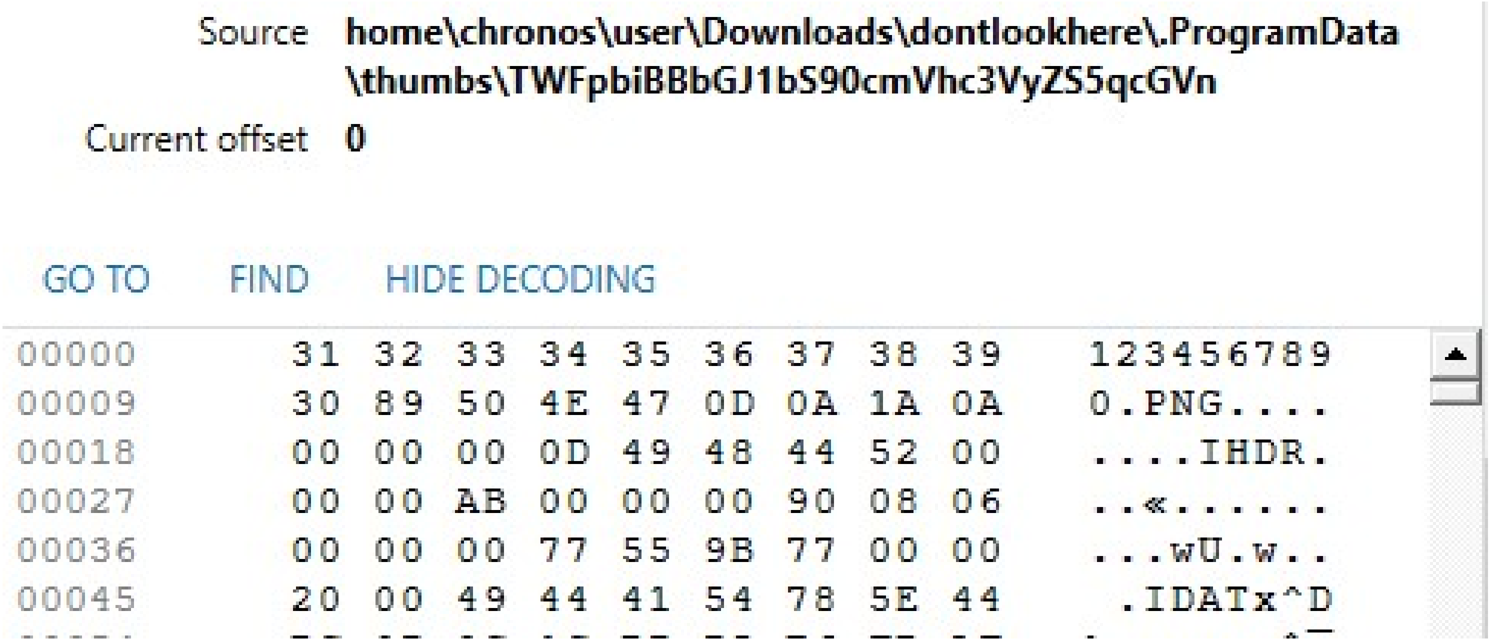


Source home\chronos\user\Downloads\dontlookhere\.ProgramData\thumbs\TWFpbiBBbGJ1bS90cmVhc3VyZS5qcGVn

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
```

Hidden Folder



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

Current offset 0

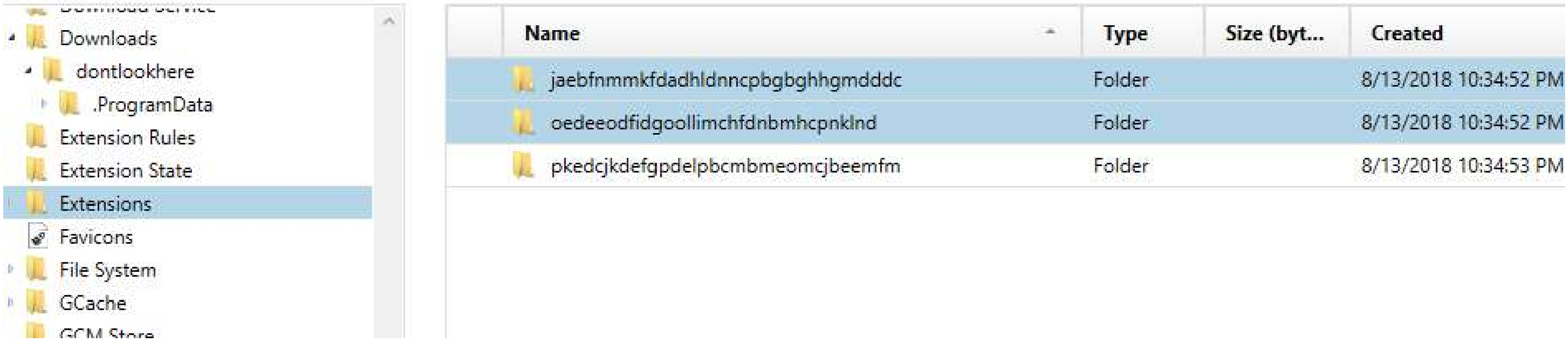
```
00000      31 32 33 34 35 36 37 38 39    123456789
00009      30 89 50 4E 47 0D 0A 1A 0A    0.PNG....
00018      00 00 00 0D 49 48 44 52 00    ....IHDR.
00027      00 00 AB 00 00 00 90 08 06    ..«......
00036      00 00 00 77 55 9B 77 00 00    ...wU.w..
00045      20 00 49 44 41 54 78 5E 44     .IDATx^D
```

Extensions

Extensions appear in the following paths

- \home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\Extensions
- \home\chronos\user\Extensions
- \home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\Extensions
- \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Extensions

Extensions



Download Service
Downloads
dontlookhere
.ProgramData
Extension Rules
Extension State
Extensions
Favicons
File System
GCache
GCM Store

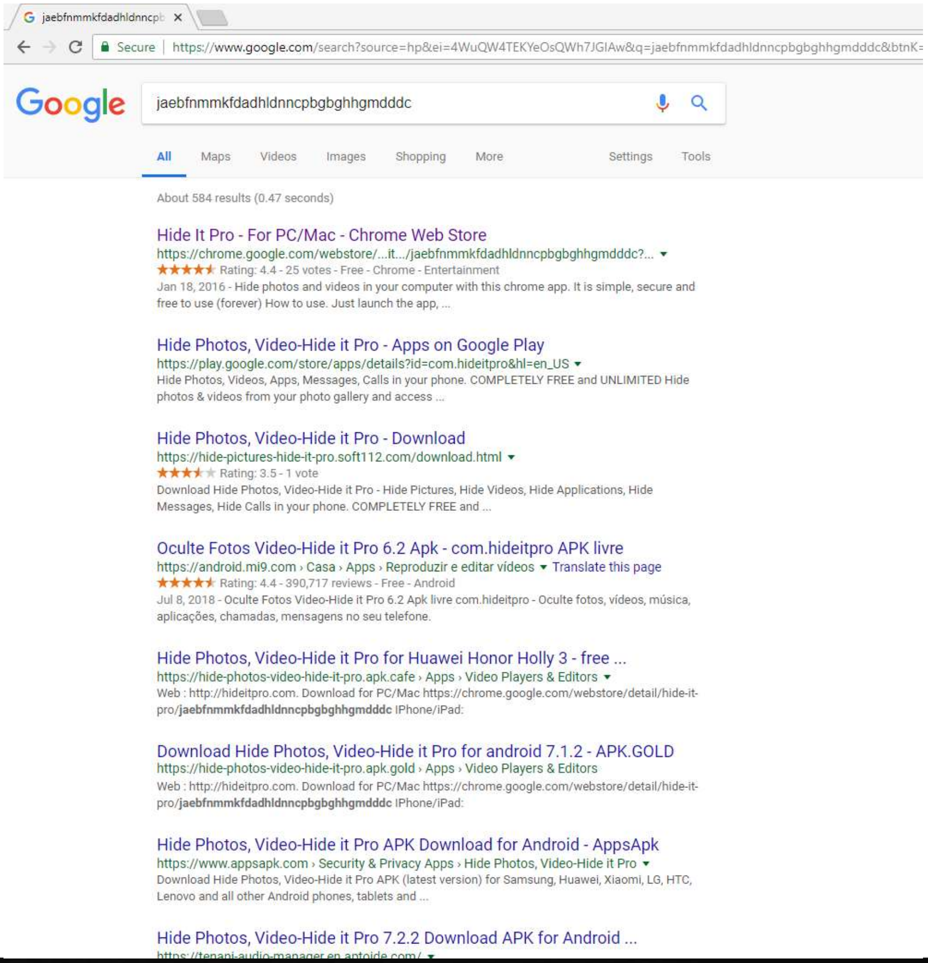
Name	Type	Size (byt...	Created
jaebfnmmkfdadhldnncpbgbghhgmdddc	Folder		8/13/2018 10:34:52 PM
oedeeodfidgoollimchfdnbmhcpnklnd	Folder		8/13/2018 10:34:52 PM
pkedcjkdefgpdelpbcmbmeomcjbeemfm	Folder		8/13/2018 10:34:53 PM

Extensions

Want to find out what app that guid is for?

Google it!

Part of the URL for Play Store and Chrome Store



https://www.google.com/search?source=hp&ei=4WuQW4TEKYeOsQWh7JGIAw&q=jaebfnmmkfdadhldnncpbgbghhgmdddc&btnK=

jaebfnmmkfdadhldnncpbgbghhgmdddc

About 584 results (0.47 seconds)

Hide It Pro - For PC/Mac - Chrome Web Store
https://chrome.google.com/webstore/...it.../jaebfnmmkfdadhldnncpbgbghhgmdddc?...
★★★★★ Rating: 4.4 - 25 votes - Free - Chrome - Entertainment
Jan 18, 2016 - Hide photos and videos in your computer with this chrome app. It is simple, secure and free to use (forever) How to use. Just launch the app, ...

Hide Photos, Video-Hide it Pro - Apps on Google Play
https://play.google.com/store/apps/details?id=com.hideitpro&hl=en_US
Hide Photos, Videos, Apps, Messages, Calls in your phone. COMPLETELY FREE and UNLIMITED Hide photos & videos from your photo gallery and access ...

Hide Photos, Video-Hide it Pro - Download
https://hide-pictures-hide-it-pro.soft112.com/download.html
★★★★☆ Rating: 3.5 - 1 vote
Download Hide Photos, Video-Hide it Pro - Hide Pictures, Hide Videos, Hide Applications, Hide Messages, Hide Calls in your phone. COMPLETELY FREE and ...

Oculte Fotos Video-Hide it Pro 6.2 Apk - com.hideitpro APK livre
https://android.mi9.com › Casa › Apps › Reproduzir e editar vídeos Translate this page
★★★★★ Rating: 4.4 - 390,717 reviews - Free - Android
Jul 8, 2018 - Oculte Fotos Video-Hide it Pro 6.2 Apk livre com.hideitpro - Oculte fotos, vídeos, música, aplicações, chamadas, mensagens no seu telefone.

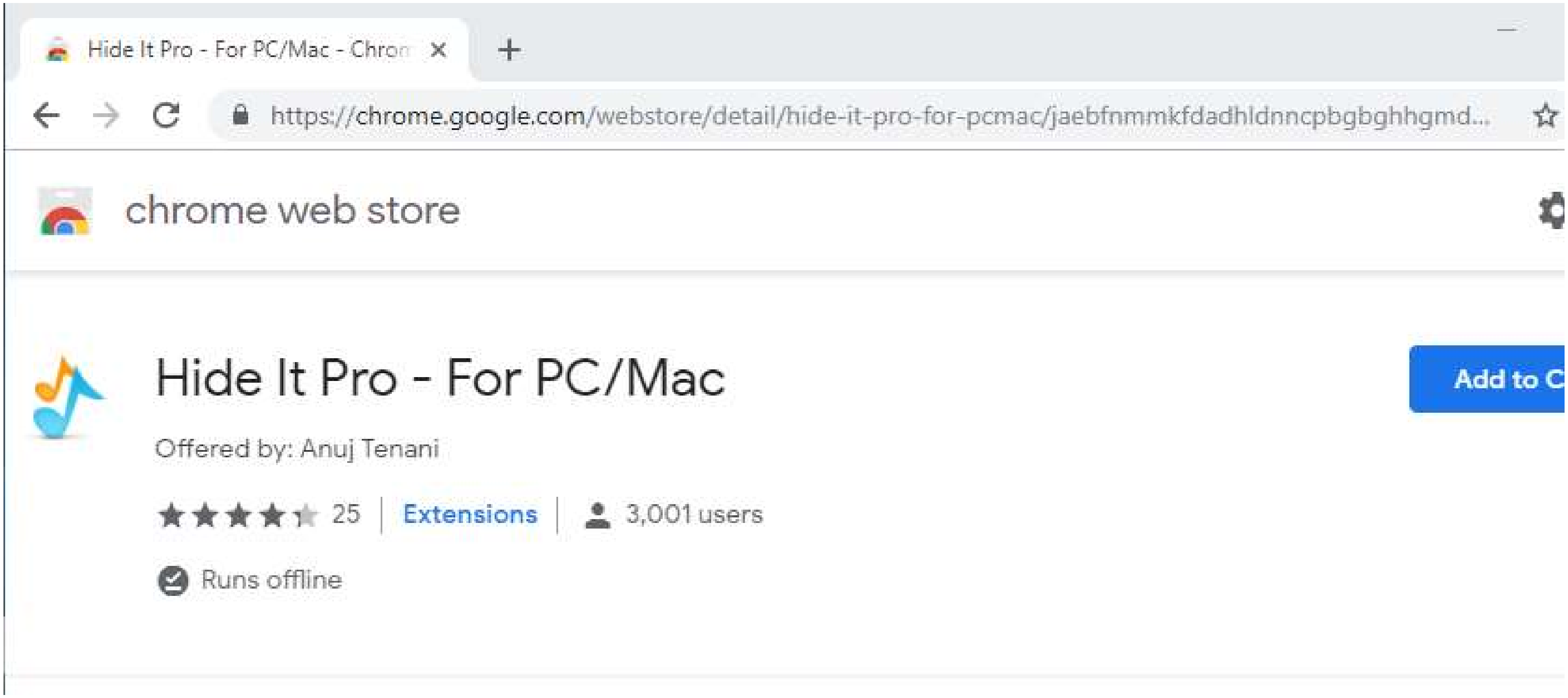
Hide Photos, Video-Hide it Pro for Huawei Honor Holly 3 - free ...
https://hide-photos-video-hide-it-pro.apk.cafe › Apps › Video Players & Editors
Web : http://hideitpro.com. Download for PC/Mac https://chrome.google.com/webstore/detail/hide-it-pro/**jaebfnmmkfdadhldnncpbgbghhgmdddc** IPhone/iPad:

Download Hide Photos, Video-Hide it Pro for android 7.1.2 - APK.GOLD
https://hide-photos-video-hide-it-pro.apk.gold › Apps › Video Players & Editors
Web : http://hideitpro.com. Download for PC/Mac https://chrome.google.com/webstore/detail/hide-it-pro/**jaebfnmmkfdadhldnncpbgbghhgmdddc** IPhone/iPad:

Hide Photos, Video-Hide it Pro APK Download for Android - AppsApk
https://www.appsapk.com › Security & Privacy Apps › Hide Photos, Video-Hide it Pro
Download Hide Photos, Video-Hide it Pro APK (latest version) for Samsung, Huawei, Xiaomi, LG, HTC, Lenovo and all other Android phones, tablets and ...

Hide Photos, Video-Hide it Pro 7.2.2 Download APK for Android ...
https://tenapi-audio-manager.en.aptoide.com/

Extensions



Hide It Pro - For PC/Mac - Chron

https://chrome.google.com/webstore/detail/hide-it-pro-for-pcmac/jaebfnmmkfdadhldnncpbgbghhgmd...

chrome web store

Hide It Pro - For PC/Mac

Add to C

Offered by: Anuj Tenani

★★★★☆ 25 | Extensions | 3,001 users

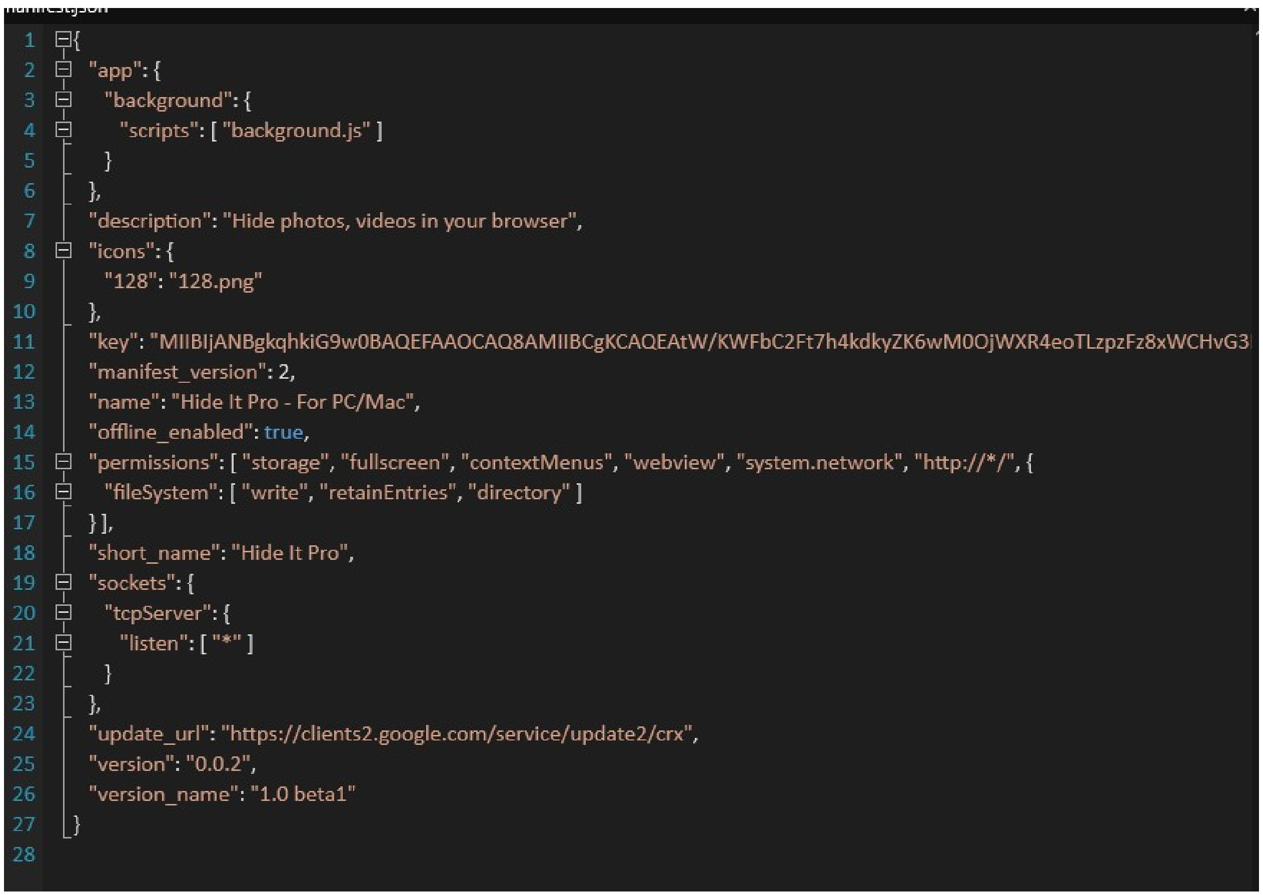
Runs offline

Extensions

manifest.json contains useful info about the app

Ex path:

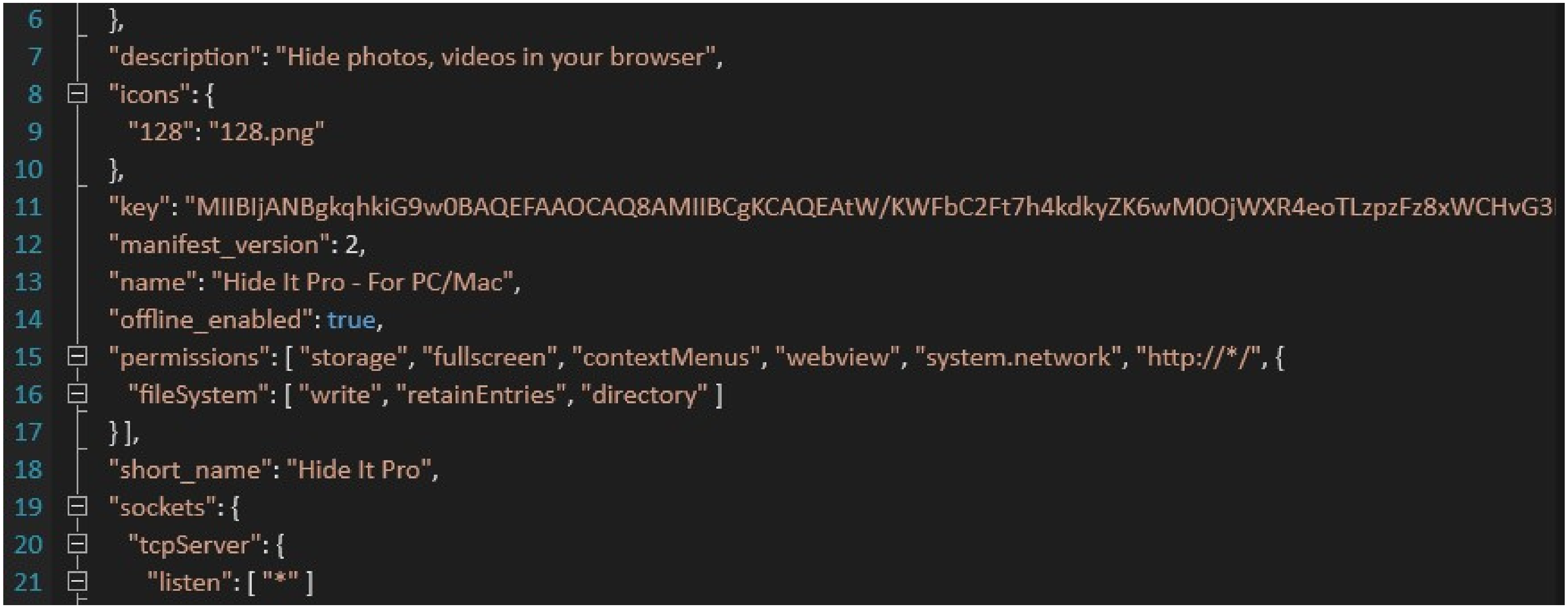
\home\chronos\user\Extensions\jaebfnmmkfdadhldnncpbgbghhgmdddc\0.0.2_0\manifest.json



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



```
},
"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": [ "*" ]
```

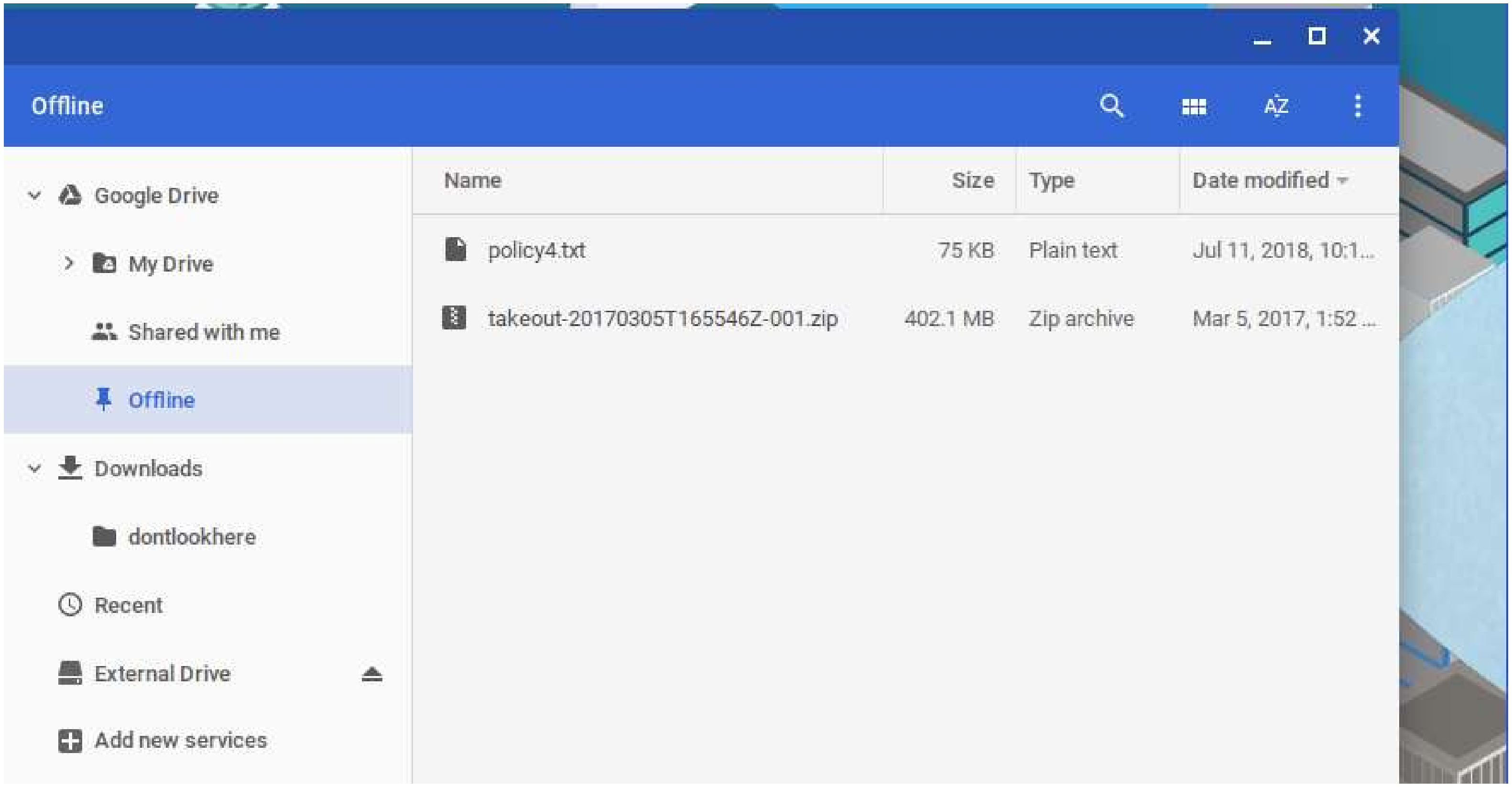
Extensions

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

Offline Storage



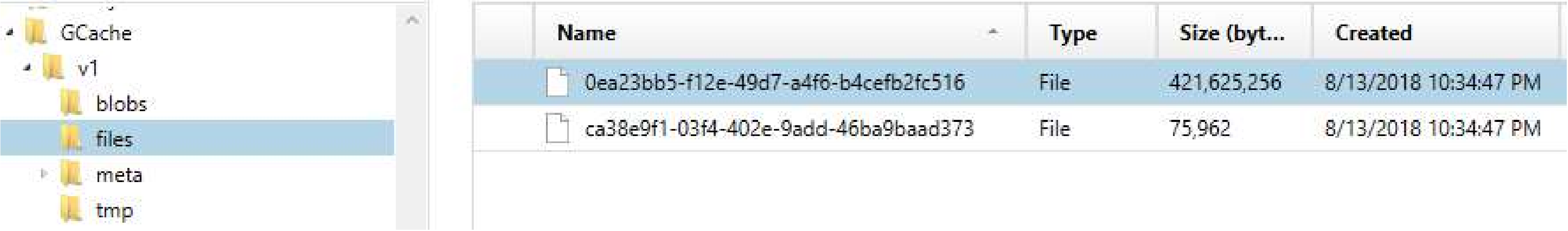
Name	Size	Type	Date modified
policy4.txt	75 KB	Plain text	Jul 11, 2018, 10:1...
takeout-20170305T165546Z-001.zip	402.1 MB	Zip archive	Mar 5, 2017, 1:52 ...

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



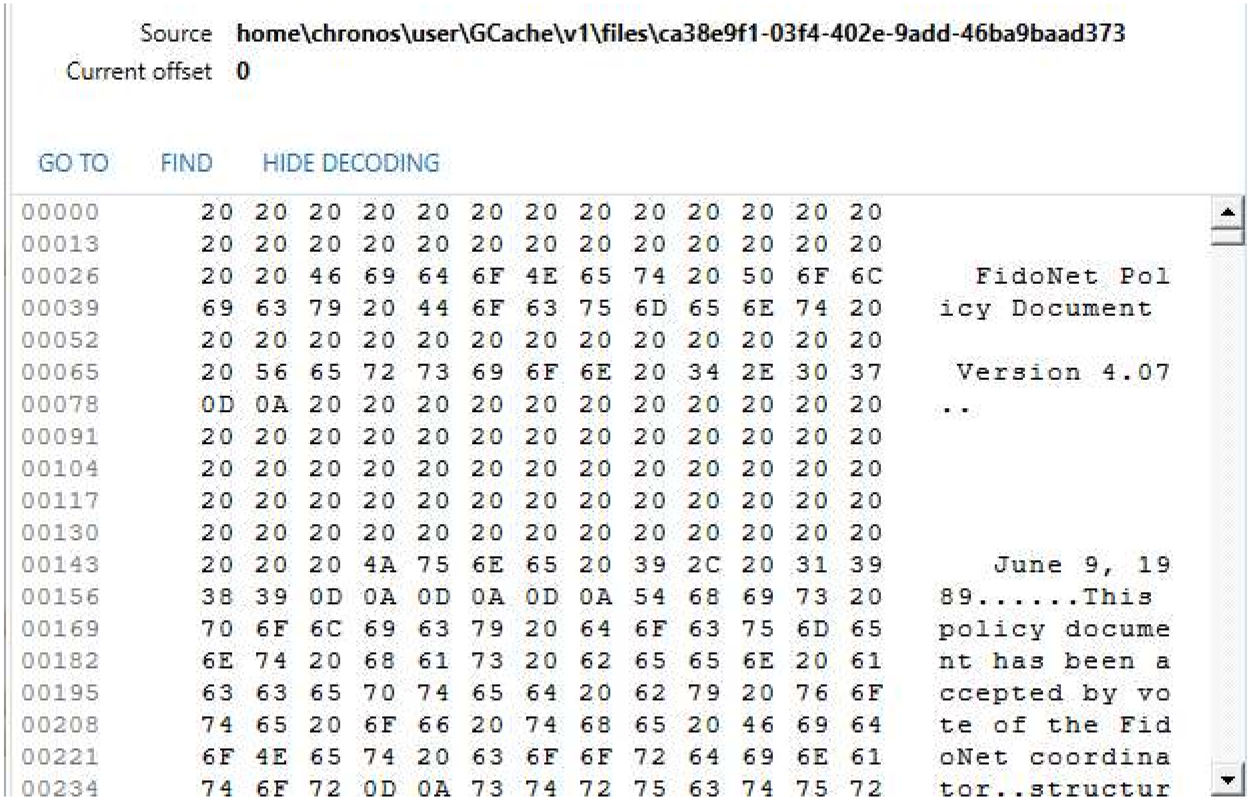
- GCache
  - v1
    - blobs
    - files
    - meta
    - tmp

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\

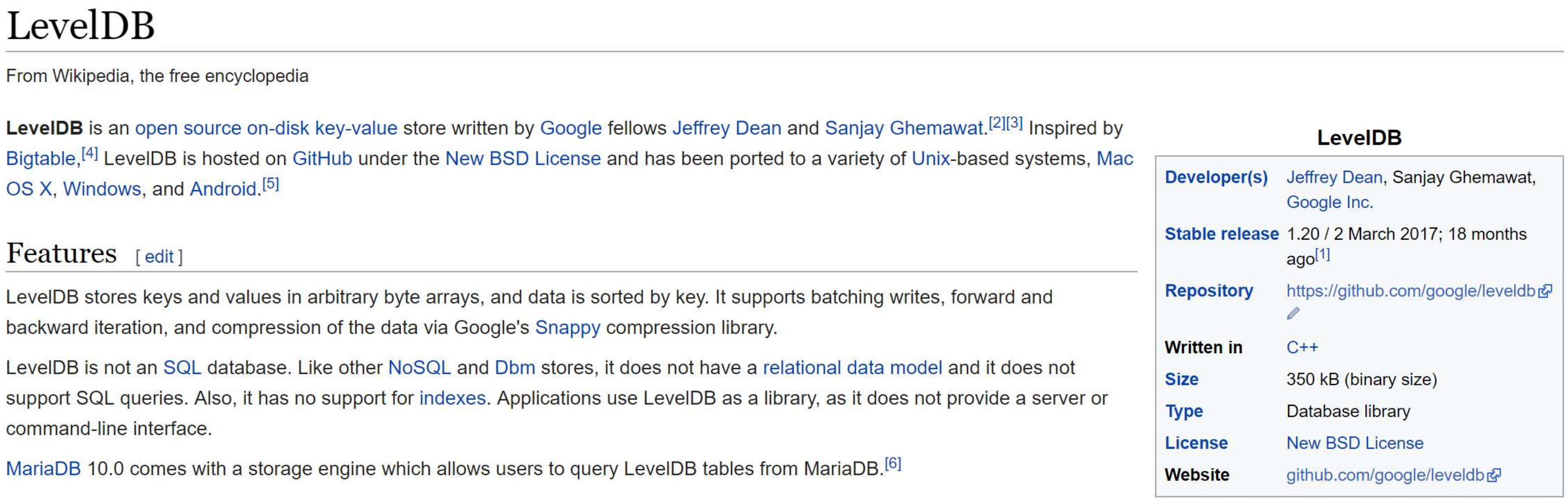


Source home\chronos\user\GCache\v1\files\ca38e9f1-03f4-402e-9add-46ba9baad373

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]

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]

LevelDB

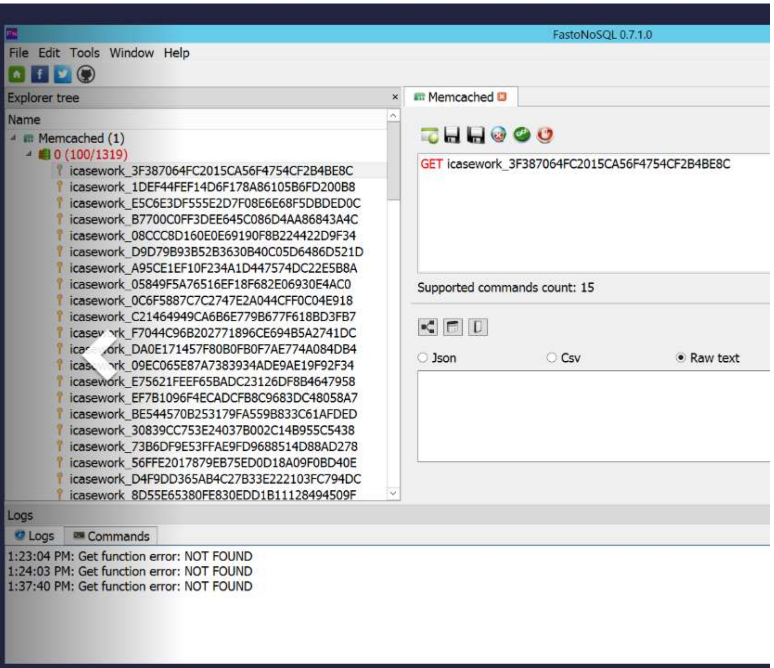
Developer(s)	Jeffrey Dean, Sanjay Ghemawat, Google Inc.
Stable release	1.20 / 2 March 2017; 18 months ago[1]
Repository	https://github.com/google/leveldb
Written in	C++
Size	350 kB (binary size)
Type	Database library
License	New BSD License
Website	github.com/google/leveldb

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
```

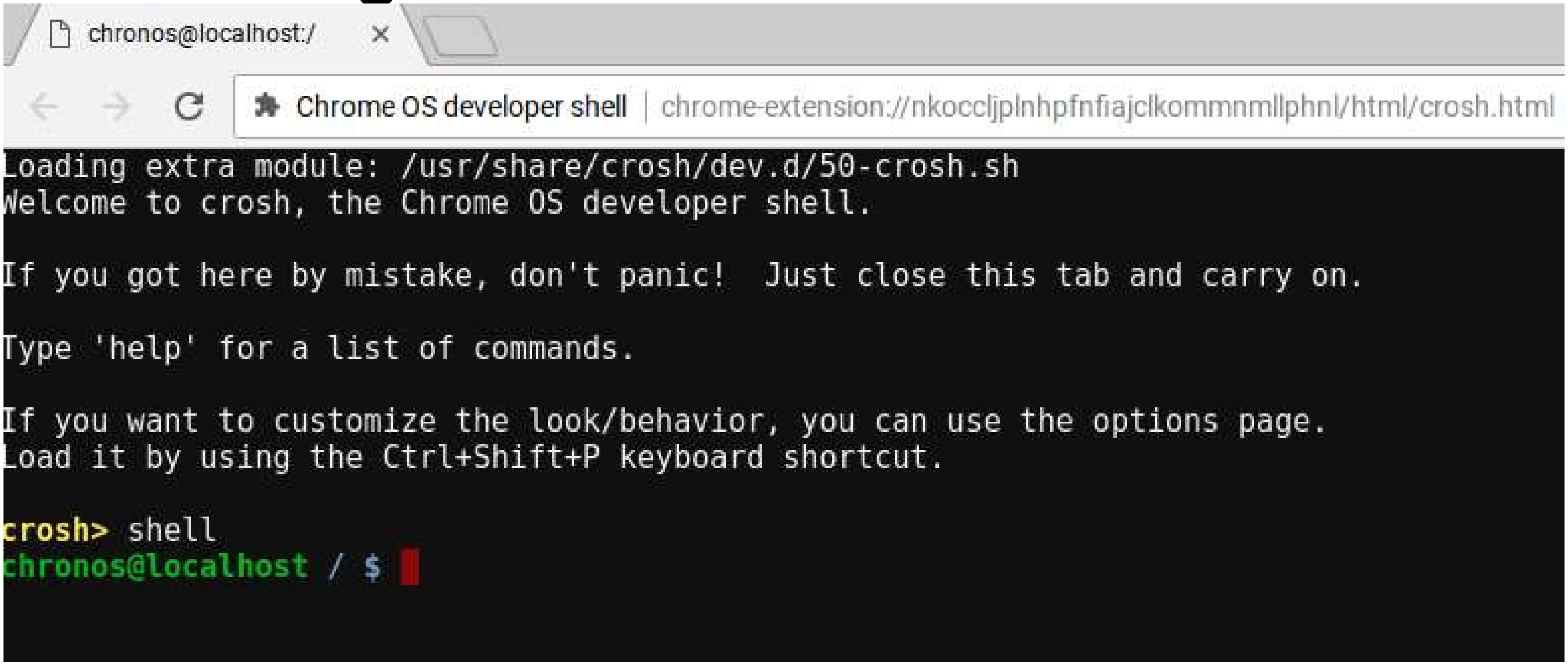
```
GET icasework_3F387064FC2015CA56F4754CF2B4BE8C
```

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
```

Shell Usage



chronos@localhost:/
Chrome OS developer shell | chrome-extension://nkoccljplnhpfnfiajclkommnmllphnl/html/crosh.html

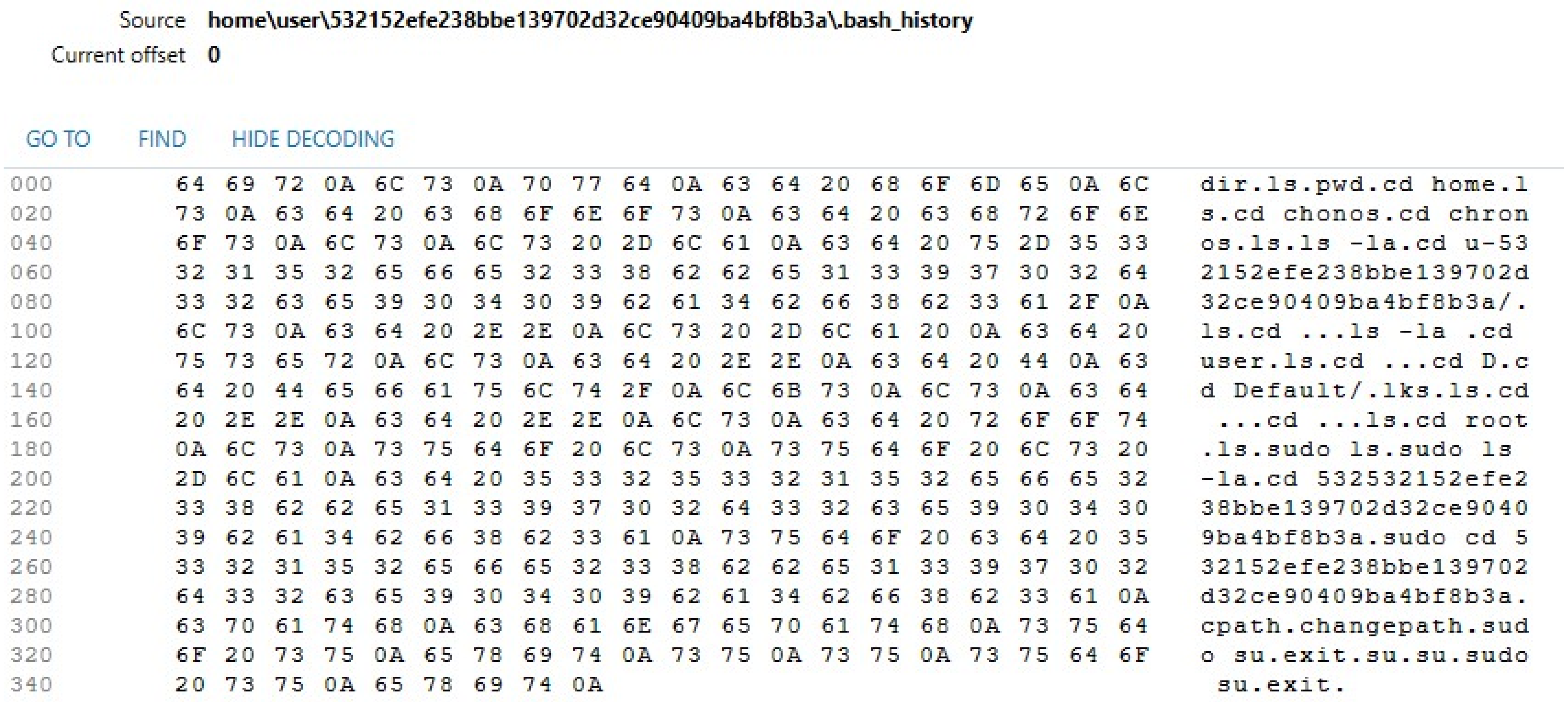
```
Loading extra module: /usr/share/crosh/dev.d/50-crosh.sh
Welcome to crosh, the Chrome OS developer shell.

If you got here by mistake, don't panic!  Just close this tab and carry on.

Type 'help' for a list of commands.

If you want to customize the look/behavior, you can use the options page.
Load it by using the Ctrl+Shift+P keyboard shortcut.

crosh> shell
chronos@localhost / $
```

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

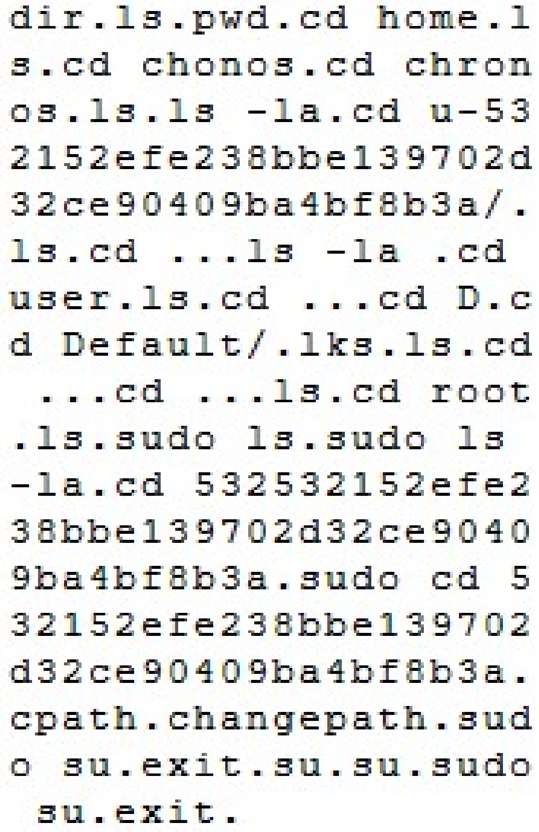
Shell Usage - .bash_history



Source home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\.bash_history
Current offset 0

```
000        64 69 72 0A 6C 73 0A 70 77 64 0A 63 64 20 68 6F 6D 65 0A 6C   dir.ls.pwd.cd home.l
020        73 0A 63 64 20 63 68 6F 6E 6F 73 0A 63 64 20 63 68 72 6F 6E   s.cd chonos.cd chron
040        6F 73 0A 6C 73 0A 6C 73 20 2D 6C 61 0A 63 64 20 75 2D 35 33   os.ls.ls -la.cd u-53
060        32 31 35 32 65 66 65 32 33 38 62 62 65 31 33 39 37 30 32 64   2152efe238bbe139702d
080        33 32 63 65 39 30 34 30 39 62 61 34 62 66 38 62 33 61 2F 0A   32ce90409ba4bf8b3a/.
100        6C 73 0A 63 64 20 2E 2E 0A 6C 73 20 2D 6C 61 20 0A 63 64 20   ls.cd ...ls -la .cd 
120        75 73 65 72 0A 6C 73 0A 63 64 20 2E 2E 0A 63 64 20 44 0A 63   user.ls.cd ...cd D.c
140        64 20 44 65 66 61 75 6C 74 2F 0A 6C 6B 73 0A 6C 73 0A 63 64   d Default/.lks.ls.cd
160        20 2E 2E 0A 63 64 20 2E 2E 0A 6C 73 0A 63 64 20 72 6F 6F 74    ...cd ...ls.cd root
180        0A 6C 73 0A 73 75 64 6F 20 6C 73 0A 73 75 64 6F 20 6C 73 20   .ls.sudo ls.sudo ls 
200        2D 6C 61 0A 63 64 20 35 33 32 35 33 32 31 35 32 65 66 65 32   -la.cd 532532152efe2
220        33 38 62 62 65 31 33 39 37 30 32 64 33 32 63 65 39 30 34 30   38bbe139702d32ce9040
240        39 62 61 34 62 66 38 62 33 61 0A 73 75 64 6F 20 63 64 20 35   9ba4bf8b3a.sudo cd 5
260        33 32 31 35 32 65 66 65 32 33 38 62 62 65 31 33 39 37 30 32   32152efe238bbe139702
280        64 33 32 63 65 39 30 34 30 39 62 61 34 62 66 38 62 33 61 0A   d32ce90409ba4bf8b3a.
300        63 70 61 74 68 0A 63 68 61 6E 67 65 70 61 74 68 0A 73 75 64   cpath.changepath.sud
320        6F 20 73 75 0A 65 78 69 74 0A 73 75 0A 73 75 0A 73 75 64 6F   o su.exit.su.su.sudo
340        20 73 75 0A 65 78 69 74 0A                                      su.exit.
```

Shell Usage - .bash_history



```
dir.ls.pwd.cd home.l
s.cd chonos.cd chron
os.ls.ls -la.cd u-53
2152efe238bbe139702d
32ce90409ba4bf8b3a/.
ls.cd ...ls -la .cd
user.ls.cd ...cd D.c
d Default/.lks.ls.cd
 ...cd ...ls.cd root
.ls.sudo ls.sudo ls
-la.cd 532532152efe2
38bbe139702d32ce9040
9ba4bf8b3a.sudo cd 5
32152efe238bbe139702
d32ce90409ba4bf8b3a.
cpath.changepath.sud
o su.exit.su.su.sudo
 su.exit.
```

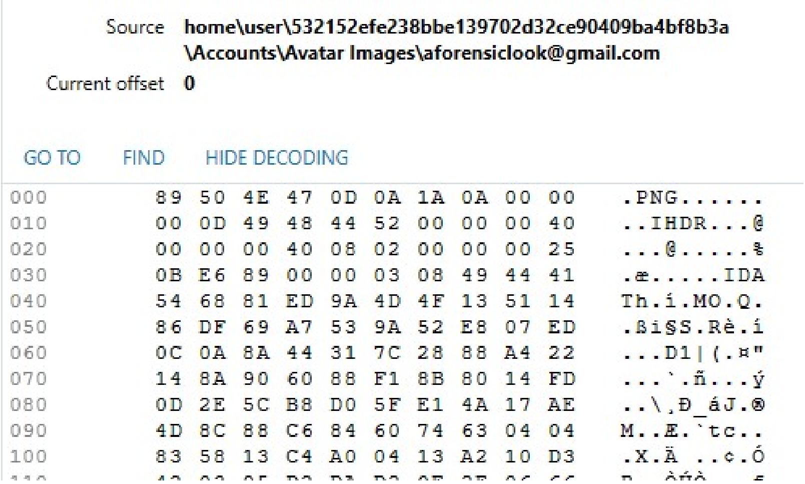
Shell Usage - .bash_history

```
dir
ls
pwd
cd home
ls
cd chonos
cd chronos
ls
ls -la
cd u-532152efe238bbe139702d32ce90409ba4bf8b3a/
```

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

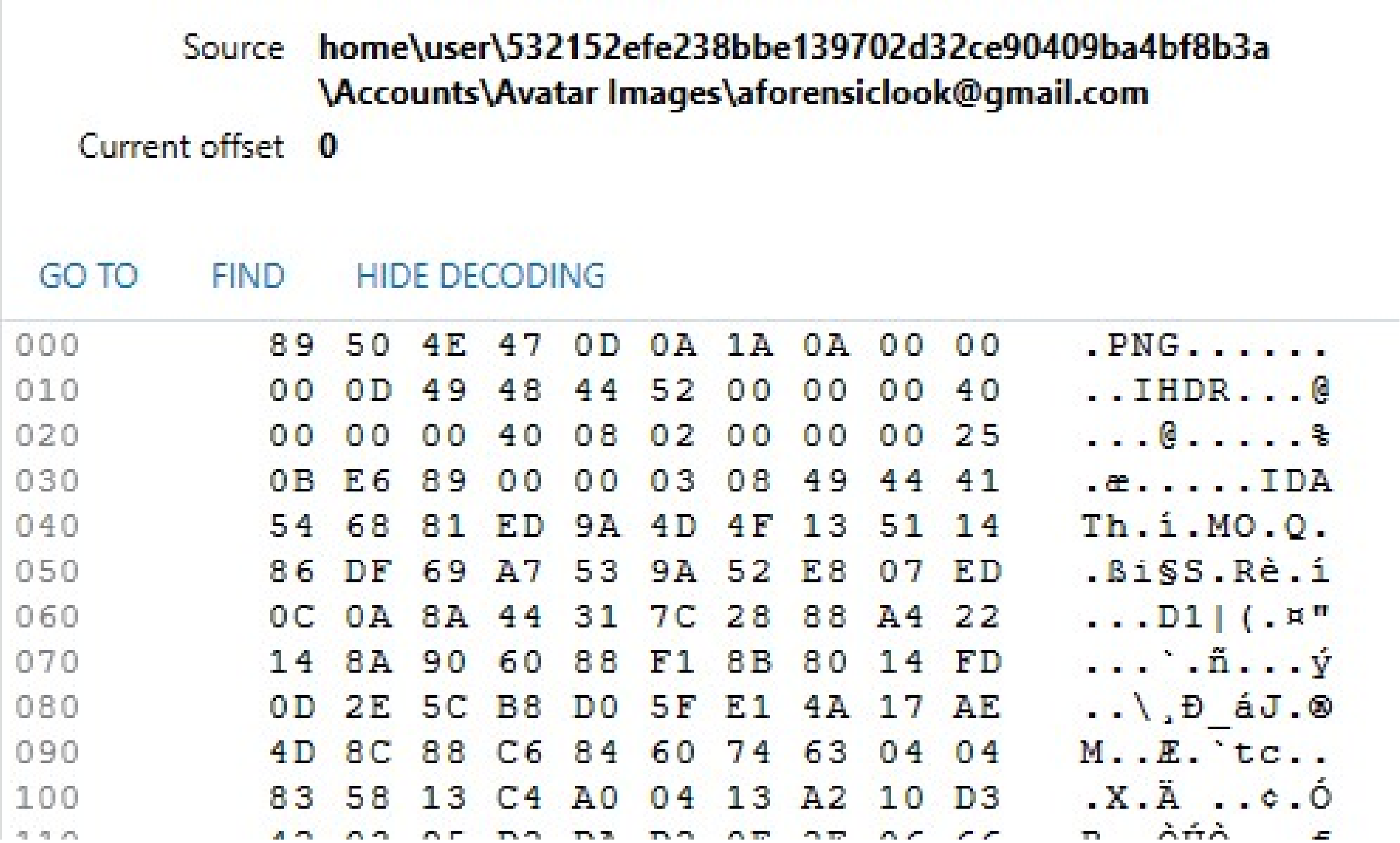


Source home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Accounts\Avatar Images\aforensiclook@gmail.com

Current offset 0

```
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
```

Avatar



Source home\user\532152efe238bbe139702d32ce90409ba4bf8b3a \Accounts\Avatar Images\aforensiclook@gmail.com

Current offset 0

```
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
```

Cloud/Takeouts/Chromium

What is the difference if I look at Chromium vs a Cloud or Takeout acquisition of the user account?

Cloud/Takeouts/Chromium

Artifact	Chromium	Takeout
Browser History	✓	✓
Browser Cache	✓	✗
Browser Current Tabs	✓	?
Browser Last Tabs	✓	?
Browser Current Sessions	✓	?
Browser Last Sessions	✓	?
Downloads	✓	✗

Cloud/Takeouts/Chromium

Artifact	Chromium	Takeout
Hidden Folder	✓	✗
Extensions	✓	✓
Offline Storage	✓	✗ *
Shell Usage	✓	✗
Avatar	✓	?
Pictures	✓ *	✓*
Task Lists	✗	✓

Open Source Support

Support for Chrome OS paths has been added to Hindsight.

Thank you, Ryan Benson!

Further Research

Now that we know that there is definitely data of value on Chromium…

- Method to image Chromebooks
- Method to decrypt Chromebooks

Summary

Chromebooks and Chromium OS are becoming more common and you may see these in an investigation

Need methods to acquire

Need to understand the data that is stored and what you can gain from looking at it.

Google Cloud acquisitions may be your friend

Questions?

jessica.hyde@magnetforensics.com

@B1N2H3X