Chrome Nuts and Bolts: Chrome OS / Chromebook forensics

Jad Saliba and Jessica Hyde
Jad’s Introduction

Hello, my name is Jad Saliba

• Hi Jad!

Founder and CTO - Magnet Forensics

• Former Digital Investigator for Waterloo Regional Police Service

FUN FACT
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

FUN FACT
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.)
Chrome OS

Integrated media player and file manager
Supports Chrome Apps
Android Apps available since 2014 via Google Play Store
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

- Coupon for 100GB Google Drive Storage for two years

However data may still be stored locally!
Why do we care?

Gartner estimates:
2015: 6.8 million Chromebooks shipped
2016: 9.4 million Chromebooks shipped

"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
Why do we care?

Schools!
  - Google for Education

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

Enterprise!
  - Chrome Enterprise – introduced in August
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

Want to understand what can be recovered…

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?
What do we know about Chromium OS?

- .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
<table>
<thead>
<tr>
<th>id</th>
<th>url</th>
<th>title</th>
<th>visit_count</th>
<th>typed_count</th>
<th>last_visit_time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><a href="https://support.google.com/chromebook/answer/93544?hl=en&amp;menu=chromebooks&amp;topic=help">https://support.google.com/chromebook/answer/93544?hl=en&amp;menu=chromebooks&amp;topic=help</a></td>
<td>Chromebook Help</td>
<td>1</td>
<td>0</td>
<td>1375801916... 0</td>
</tr>
<tr>
<td>2</td>
<td><a href="https://support.google.com/chromebook/answer/93544?hl=en&amp;menu=chromebooks&amp;topic=help">https://support.google.com/chromebook/answer/93544?hl=en&amp;menu=chromebooks&amp;topic=help</a></td>
<td>Chromebook Help</td>
<td>1</td>
<td>0</td>
<td>1375801917... 0</td>
</tr>
<tr>
<td>3</td>
<td><a href="https://support.google.com/chromebook/answer/93544?hl=en&amp;menu=chromebooks&amp;topic=help">https://support.google.com/chromebook/answer/93544?hl=en&amp;menu=chromebooks&amp;topic=help</a></td>
<td>Chromebook Help</td>
<td>1</td>
<td>0</td>
<td>1375801921... 0</td>
</tr>
<tr>
<td>4</td>
<td><a href="https://support.google.com/chromebook/answer/93544?hl=en&amp;menu=chromebooks&amp;topic=help">https://support.google.com/chromebook/answer/93544?hl=en&amp;menu=chromebooks&amp;topic=help</a></td>
<td>Chromebook Help</td>
<td>1</td>
<td>0</td>
<td>1375801922... 0</td>
</tr>
<tr>
<td>5</td>
<td><a href="https://www.google.ca/search?q=gmail&amp;ie=utf-8&amp;client=chrome-1.6957">https://www.google.ca/search?q=gmail&amp;ie=utf-8&amp;client=chrome-1.6957</a>... 0</td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>1375801858... 0</td>
</tr>
<tr>
<td>6</td>
<td><a href="https://www.google.com/gmail/">https://www.google.com/gmail/</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>1375801861... 0</td>
</tr>
<tr>
<td>7</td>
<td><a href="https://mail.google.com/mail/">https://mail.google.com/mail/</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>1375801861... 0</td>
</tr>
<tr>
<td>8</td>
<td><a href="https://mail.google.com/mail/">https://mail.google.com/mail/</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>1375801861... 0</td>
</tr>
<tr>
<td>9</td>
<td><a href="https://mail.google.com/mail/">https://mail.google.com/mail/</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>1375801861... 0</td>
</tr>
<tr>
<td>10</td>
<td><a href="https://mail.google.com/mail/">https://mail.google.com/mail/</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>1375801861... 0</td>
</tr>
<tr>
<td>11</td>
<td><a href="https://mail.google.com/mail/">https://mail.google.com/mail/</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>1375801861... 0</td>
</tr>
<tr>
<td>12</td>
<td><a href="https://mail.google.com/mail/u/1/#inbox">https://mail.google.com/mail/u/1/#inbox</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>1375801861... 0</td>
</tr>
<tr>
<td>13</td>
<td><a href="https://mail.google.com/mail/u/1/#inbox">https://mail.google.com/mail/u/1/#inbox</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>1375801861... 0</td>
</tr>
<tr>
<td>14</td>
<td><a href="https://mail.google.com/mail/u/1/#inbox">https://mail.google.com/mail/u/1/#inbox</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>1375801861... 0</td>
</tr>
<tr>
<td>15</td>
<td><a href="https://mail.google.com/mail/u/1/#inbox">https://mail.google.com/mail/u/1/#inbox</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>1375801861... 0</td>
</tr>
<tr>
<td>16</td>
<td><a href="https://mail.google.com/mail/u/1/#inbox">https://mail.google.com/mail/u/1/#inbox</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>1375801861... 0</td>
</tr>
<tr>
<td>17</td>
<td><a href="https://mail.google.com/mail/u/1/#inbox">https://mail.google.com/mail/u/1/#inbox</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>1375801861... 0</td>
</tr>
<tr>
<td>18</td>
<td><a href="https://mail.google.com/mail/u/1/#spam">https://mail.google.com/mail/u/1/#spam</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>1375801861... 0</td>
</tr>
<tr>
<td>19</td>
<td><a href="https://mail.google.com/mail/u/1/#spam">https://mail.google.com/mail/u/1/#spam</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>1375801861... 0</td>
</tr>
<tr>
<td>20</td>
<td><a href="https://mail.google.com/mail/u/1/#spam">https://mail.google.com/mail/u/1/#spam</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>1375801861... 0</td>
</tr>
<tr>
<td>21</td>
<td><a href="https://download.cnet.com/">https://download.cnet.com/</a></td>
<td>CNET Download</td>
<td>1</td>
<td>0</td>
<td>1375802046... 0</td>
</tr>
<tr>
<td>22</td>
<td><a href="https://download.cnet.com/">https://download.cnet.com/</a></td>
<td>Windows PC Software</td>
<td>1</td>
<td>0</td>
<td>1375802054... 0</td>
</tr>
<tr>
<td>23</td>
<td><a href="https://download.cnet.com/">https://download.cnet.com/</a></td>
<td>Most Popular Windows Software</td>
<td>1</td>
<td>0</td>
<td>1375802156... 0</td>
</tr>
<tr>
<td>24</td>
<td><a href="https://download.cnet.com/">https://download.cnet.com/</a></td>
<td>Most Popular Software</td>
<td>1</td>
<td>0</td>
<td>1375802027... 0</td>
</tr>
<tr>
<td>25</td>
<td><a href="https://download.cnet.com/whatsapp-app-for-pc-2019-4_7664933">https://download.cnet.com/whatsapp-app-for-pc-2019-4_7664933</a>... 0</td>
<td>WhatsApp for PC</td>
<td>1</td>
<td>0</td>
<td>1375802199... 0</td>
</tr>
<tr>
<td>26</td>
<td><a href="https://download.cnet.com/whatsapp-app-for-pc-2019-4_7664933">https://download.cnet.com/whatsapp-app-for-pc-2019-4_7664933</a>... 0</td>
<td>WhatsApp for PC</td>
<td>1</td>
<td>0</td>
<td>1375802236... 0</td>
</tr>
<tr>
<td>27</td>
<td><a href="https://download.cnet.com/whatsapp-app-for-pc-2019-4_7664933">https://download.cnet.com/whatsapp-app-for-pc-2019-4_7664933</a>... 0</td>
<td>WhatsApp for PC</td>
<td>1</td>
<td>0</td>
<td>1375802199... 0</td>
</tr>
<tr>
<td>28</td>
<td><a href="https://www.google.ca/search?q=type%3A%2F%2Flink%26tbs%3Asite:type%3A%2F%2Flink%26tbs%3Asite">https://www.google.ca/search?q=type%3A%2F%2Flink%26tbs%3Asite:type%3A%2F%2Flink%26tbs%3Asite</a>:</td>
<td>Google Search</td>
<td>1</td>
<td>0</td>
<td>1375802289... 0</td>
</tr>
<tr>
<td>29</td>
<td><a href="https://www.google.ca/search?q=type%3A%2F%2Flink%26tbs%3Asite:type%3A%2F%2Flink%26tbs%3Asite">https://www.google.ca/search?q=type%3A%2F%2Flink%26tbs%3Asite:type%3A%2F%2Flink%26tbs%3Asite</a>:</td>
<td>Google Search</td>
<td>1</td>
<td>0</td>
<td>1375802294... 0</td>
</tr>
</tbody>
</table>
## Browser History

<table>
<thead>
<tr>
<th>id</th>
<th>url</th>
<th>title</th>
<th>visit_count</th>
<th>typed_count</th>
<th>last_visit_time</th>
<th>hidden</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><a href="https://support.google.com/chromebook/?p=help&amp;ctb=menu">https://support.google.com/chromebook/?p=help&amp;ctb=menu</a></td>
<td>Chromebook Help</td>
<td>1</td>
<td>0</td>
<td>13175801916...</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td><a href="https://support.google.com/chromebook/?p=help&amp;ctb=menu?topic=3">https://support.google.com/chromebook/?p=help&amp;ctb=menu?topic=3</a>...</td>
<td></td>
<td>1</td>
<td>0</td>
<td>13175801917...</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td><a href="https://support.google.com/chromebook/?p=help&amp;ctb=menu?topic=3">https://support.google.com/chromebook/?p=help&amp;ctb=menu?topic=3</a>...</td>
<td></td>
<td>1</td>
<td>0</td>
<td>13175801921...</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td><a href="https://support.google.com/chromebook/?p=help&amp;ctb=menu?topic=3">https://support.google.com/chromebook/?p=help&amp;ctb=menu?topic=3</a>...</td>
<td></td>
<td>1</td>
<td>0</td>
<td>13175801922...</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td><a href="https://www.google.ca/search?q=gmail&amp;gq=gm&amp;q=chrome.1.69577">https://www.google.ca/search?q=gmail&amp;gq=gm&amp;q=chrome.1.69577</a>...</td>
<td>gmail · Google Search</td>
<td>1</td>
<td>0</td>
<td>13175801958...</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td><a href="https://www.google.com/gmail/">https://www.google.com/gmail/</a></td>
<td></td>
<td>1</td>
<td>0</td>
<td>13175801961...</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td><a href="https://mail.google.com/mail/">https://mail.google.com/mail/</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>13175801961...</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td><a href="https://mail.google.com/mail/">https://mail.google.com/mail/</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>13175801961...</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td><a href="https://mail.google.com/mail/">https://mail.google.com/mail/</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>13175801961...</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td><a href="https://mail.google.com/mail/">https://mail.google.com/mail/</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>13175801961...</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td><a href="https://mail.google.com/mail/u/6/#">https://mail.google.com/mail/u/6/#</a></td>
<td>Gmail</td>
<td>1</td>
<td>0</td>
<td>13175801961...</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td><a href="https://mail.google.com/mail/u/6/#">https://mail.google.com/mail/u/6/#</a></td>
<td>Inbox (44,546) · <a href="mailto:aforesniclook@gmail.com">aforesniclook@gmail.com</a> · Gmail</td>
<td>1</td>
<td>0</td>
<td>13175802002...</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td><a href="https://mail.google.com/mail/u/6/#">https://mail.google.com/mail/u/6/#</a></td>
<td>Inbox [1648a472c237a6 Ske</td>
<td>1</td>
<td>0</td>
<td>13175801968...</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td><a href="https://mail.google.com/mail/u/6/#">https://mail.google.com/mail/u/6/#</a></td>
<td>Security alert · <a href="mailto:aforesniclook@gmail.com">aforesniclook@gmail.com</a> · Gmail</td>
<td>1</td>
<td>0</td>
<td>13175801985...</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td><a href="https://mail.google.com/mail/u/6/#">https://mail.google.com/mail/u/6/#</a></td>
<td>Video news feature · Hexx calls affect us all · <a href="mailto:aforesniclook@gmail.com">aforesniclook@gmail.com</a></td>
<td>1</td>
<td>0</td>
<td>13175801985...</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td><a href="https://mail.google.com/mail/u/6/#">https://mail.google.com/mail/u/6/#</a></td>
<td>Spam [22] · <a href="mailto:aforesniclook@gmail.com">aforesniclook@gmail.com</a> · Gmail</td>
<td>1</td>
<td>0</td>
<td>13175802016...</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td><a href="https://mail.google.com/mail/u/6/#">https://mail.google.com/mail/u/6/#</a></td>
<td>Google Alert · Bing · <a href="mailto:aforesniclook@gmail.com">aforesniclook@gmail.com</a> · Gmail</td>
<td>1</td>
<td>0</td>
<td>13175802026...</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td><a href="https://mail.google.com/mail/u/6/#">https://mail.google.com/mail/u/6/#</a></td>
<td>Google Alert · Bing · <a href="mailto:aforesniclook@gmail.com">aforesniclook@gmail.com</a> · Gmail</td>
<td>1</td>
<td>0</td>
<td>13175802041...</td>
<td>0</td>
</tr>
</tbody>
</table>
Browser Cache

Each entry appears in the following paths

- `\home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mount\user\Cache`
- `\home\chronos\user\Cache`
- `\home\chronos\user-\532152efe238bbe139702d32ce90409ba4bf8b3a\Cache`
- `\home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Cache`

Contains individual files with guids for each cache
Browser Cache

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>File size</th>
<th>Created</th>
<th>Accessed</th>
<th>Modifed</th>
</tr>
</thead>
<tbody>
<tr>
<td>d345eda2b682bf8_0</td>
<td>File</td>
<td>5.152 KB</td>
<td>8/13/2018 10:34:43 PM</td>
<td>8/13/2018 10:34:43 PM</td>
<td>8/13/2018</td>
</tr>
<tr>
<td>d456fda2b682bf8_0</td>
<td>File</td>
<td>5.151 KB</td>
<td>8/13/2018 10:34:43 PM</td>
<td>8/13/2018 10:34:43 PM</td>
<td>8/13/2018</td>
</tr>
<tr>
<td>e567gda2b682bf8_0</td>
<td>File</td>
<td>5.150 KB</td>
<td>8/13/2018 10:34:43 PM</td>
<td>8/13/2018 10:34:43 PM</td>
<td>8/13/2018</td>
</tr>
<tr>
<td>f678hda2b682bf8_0</td>
<td>File</td>
<td>5.149 KB</td>
<td>8/13/2018 10:34:43 PM</td>
<td>8/13/2018 10:34:43 PM</td>
<td>8/13/2018</td>
</tr>
</tbody>
</table>

**PREVIEW**

https://www.geronic.com/images/icons/material/system%3Axarrow_down%40%2D%2048px.png

HTTP/1.1 200
status: 200
accept: image/png
content-type: image/png
vary: Origin
content-length: 94

date: Fri, 15 Jun 2018 23:33:25 GMT
last-modified: Thu, 21 Apr 2016 09:17:22 GMT
server: nginx
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block

**DETAILS**

**FILE DETAILS**

- File name: d345eda2b682bf8_0
- 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: da8256f736f818889b827a2f999692bf
- File attributes: Normal

**EVIDENCE INFORMATION**

- Source: ChromiumOS-image.vmdk - Partition 1 (EXT family, 4 GB)
- Source: chromiumOSuser/Cachef/d345eda2b682bf8_0
- Evidence number: ChromiumOS-image.vmdk
Browser Cache

PREVIEW

https://www.gstatic.com/images/branding/material/system Tx: loose doc

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
last-modified: Thu, 21 Apr 2016 09:17:22 GMT
content-type-options: nosave
server: ghttp
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\user\-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\user-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\user-532152efe238bbe139702d32ce90409ba4bf8b3a\Last Sessions
- \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Last Sessions
Downloads
# Downloads

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

In the downloads table:

<table>
<thead>
<tr>
<th>target_path</th>
<th>start_time</th>
<th>received_bytes</th>
<th>total_bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/WhatsAppSetup.exe</td>
<td>13175802258013369</td>
<td>81489680</td>
<td>81489680</td>
</tr>
<tr>
<td>/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/properchromebookhandlingdistributedtostudentsinbag.pdf</td>
<td>13175802380721784</td>
<td>61514</td>
<td>61514</td>
</tr>
<tr>
<td>/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/changelog.txt</td>
<td>13175802441962766</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/policy4.txt</td>
<td>13175802668330793</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/unnamed.jpg</td>
<td>1317866878007022</td>
<td>71839</td>
<td>71839</td>
</tr>
<tr>
<td>/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/treasuremap.jpg</td>
<td>13178668825957445</td>
<td>43962</td>
<td>43962</td>
</tr>
<tr>
<td>/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/treasure.jpg</td>
<td>13178668902084500</td>
<td>14154</td>
<td>14154</td>
</tr>
</tbody>
</table>
## Downloads

<table>
<thead>
<tr>
<th>target_path</th>
<th>start_time</th>
</tr>
</thead>
<tbody>
<tr>
<td>/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/WhatsAppSetup.exe</td>
<td>13175802258013369</td>
</tr>
<tr>
<td>/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/properchromebookhandlingdistributedtostudentsinbag.pdf</td>
<td>13175802380721784</td>
</tr>
<tr>
<td>/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/changelog.txt</td>
<td>13175802441962766</td>
</tr>
<tr>
<td>/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/policy4.txt</td>
<td>13175802668330793</td>
</tr>
<tr>
<td>/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/unnamed.jpg</td>
<td>13178668788007022</td>
</tr>
<tr>
<td>/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/treasuremap.jpg</td>
<td>13178668825957445</td>
</tr>
<tr>
<td>/home/chronos/u-532152efe238bbe139702d32ce90409ba4bf8b3a/Downloads/treasure.jpg</td>
<td>13178668902084500</td>
</tr>
</tbody>
</table>
Downloads

Which can be coordinated with the downloads_url_chains table

Also in the Chrome Browser History

<table>
<thead>
<tr>
<th>id</th>
<th>chain_index</th>
<th>url</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td><a href="https://files.downloadnow.com/s/software/15/97/54/35/WhatsAppSetup.exe?token=1531364653_14516b582f6f4848d8b7f2705fd6d85&amp;fileName=WhatsAppSetup.exe">https://files.downloadnow.com/s/software/15/97/54/35/WhatsAppSetup.exe?token=1531364653_14516b582f6f4848d8b7f2705fd6d85&amp;fileName=WhatsAppSetup.exe</a></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td><a href="http://www.loogootee.k12.in.us/docs/building/1/1%20to%201/properchromebookhandlingdistributetostudentsinbag.pdf">http://www.loogootee.k12.in.us/docs/building/1/1%20to%201/properchromebookhandlingdistributetostudentsinbag.pdf</a></td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td><a href="https://raw.githubusercontent.com/JamesHeinrich/getID3/master/changelog.txt">https://raw.githubusercontent.com/JamesHeinrich/getID3/master/changelog.txt</a></td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td><a href="https://www.fidonet.org/policy4.txt">https://www.fidonet.org/policy4.txt</a></td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td><a href="https://lh3.googleusercontent.com/PzvcTUnVMg43RdjQ5wAPc3FQkOBc7BJ9AHxolMynren9Y-SiRxAO-AuXZADd6Yhs2cKrqTGJY=w640-h400-e365">https://lh3.googleusercontent.com/PzvcTUnVMg43RdjQ5wAPc3FQkOBc7BJ9AHxolMynren9Y-SiRxAO-AuXZADd6Yhs2cKrqTGJY=w640-h400-e365</a></td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td><a href="https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcR3_6Kcnv0oH6Eb0YOGXtswYd8qONbxY7MUNeQD3swGwqG80">https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcR3_6Kcnv0oH6Eb0YOGXtswYd8qONbxY7MUNeQD3swGwqG80</a></td>
</tr>
<tr>
<td>url</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://files.downloadnow.com/s/software/15/97/54/35/WhatsAppSetup.exe?token=1531364653_145166582f6f4848df8b7f2705f4db85&amp;fileName=WhatsAppSetup.exe">https://files.downloadnow.com/s/software/15/97/54/35/WhatsAppSetup.exe?token=1531364653_145166582f6f4848df8b7f2705f4db85&amp;fileName=WhatsAppSetup.exe</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.linuxarena.com/docs/building/1/120to%201/properchromebookhandlingdistributedtostudentsinbag.pdf">http://www.linuxarena.com/docs/building/1/120to%201/properchromebookhandlingdistributedtostudentsinbag.pdf</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://www.fidonet.org/policy4.txt">https://www.fidonet.org/policy4.txt</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://lh3.googleusercontent.com/PzvcTUmVIMg43RbdQkJ3wAPc3PFobC7BJ9AHxolMynren9Y-SiRxAO-AwXZDAd6Y0hs2cKrqTqhY=w640-h400-e365">https://lh3.googleusercontent.com/PzvcTUmVIMg43RbdQkJ3wAPc3PFobC7BJ9AHxolMynren9Y-SiRxAO-AwXZDAd6Y0hs2cKrqTqhY=w640-h400-e365</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcR3_6Kcny00HbEo0YOGXtwYD8o8XNbxY77MUNeQD3SrsqwGb0">https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcR3_6Kcny00HbEo0YOGXtwYD8o8XNbxY77MUNeQD3SrsqwGb0</a></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Downloads
## Downloads

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>File ext.</th>
<th>Size (B)</th>
<th>Created</th>
<th>Accessed</th>
<th>Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>doclockhere</td>
<td>Folder</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Downloads

Just as before found in 4 locations
Downloads

Example: Policy4.txt
Hidden Folder

The `dontlookhere` directory appears in the following paths:

- `\home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mnt\user\Downloads`
- `\home\chronos\user\Downloads`
- `\home\chronos\user\-532152efe238bbe139702d32ce90409ba4bf8b3a\Downloads`
- `\home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Downloads`
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
**Hidden Folder**

Source: `home\chronos\user\Downloads\dontlookhere\ProgramData\thumbs\TWFpblBBbGJ1b590cmVhc3VyZS5qcGVn`

Current offset: 0

<table>
<thead>
<tr>
<th>GO TO</th>
<th>FIND</th>
<th>HIDE DECODING</th>
</tr>
</thead>
<tbody>
<tr>
<td>00000</td>
<td>31</td>
<td>32 33 34 35 36 37 38 39</td>
</tr>
<tr>
<td>00009</td>
<td>30</td>
<td>89 50 4E 47 0D 0A 1A 0A</td>
</tr>
<tr>
<td>00010</td>
<td>00</td>
<td>00 00 00 0D 49 48 44 52 00</td>
</tr>
<tr>
<td>00027</td>
<td>00</td>
<td>00 AB 00 00 00 90 08 06</td>
</tr>
<tr>
<td>00036</td>
<td>00</td>
<td>00 00 77 55 9B 77 00 00</td>
</tr>
<tr>
<td>00045</td>
<td>20</td>
<td>00 49 44 41 54 78 5E 44</td>
</tr>
</tbody>
</table>
Extensions

Extensions appear in the following paths

- `\home\.shadow\532152efe238bbe139702d32ce90409ba4bf8b3a\mnt\user\Extensions`
- `\home\chronos\user\Extensions`
- `\home\chronos\user-\532152efe238bbe139702d32ce90409ba4bf8b3a\Extensions`
- `\home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Extensions`
Extensions
Extensions

Want to find out what app that guid is for?
Google it!
Part of the URL for Play Store and Chrome Store
Extensions

Hide It Pro - For PC/Mac

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`
```json
{
  "description": "Hide photos, videos in your browser",
  "icons": {
    "128": "128.png"
  },
  "key": "MII8bljAI88gkqhiG9w0BAQFBAOAQCAQAMIIIBCgKCAQEAtW/KWFbC2Ft7h4kdkyZK6wM0OjWXR4ehTLzpzFz8xWCHvG3",
  "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

- Google Drive
  - My Drive
  - Shared with me
- Offline
- Downloads
  - dontlookhere
- Recent
- External Drive
- Add new services

- policy4.txt
  - Size: 75 KB
  - Type: Plain text
  - Date modified: Jul 11, 2018, 10:12...
- takeout-20170305T165545Z-001.zip
  - Size: 402.1 MB
  - Type: Zip archive
  - Date modified: 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\user\-532152efe238bbe139702d32ce90409ba4bf8b3a\Gcache\v1\files`
- `\home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Gcache\v1\files`
Offline Storage

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Size (byte)</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>0ea23bb5-f12e-49d7-a4f6-b4cefb2fc516</td>
<td>File</td>
<td>421,625,256</td>
<td>8/13/2018 10:34:47 PM</td>
</tr>
<tr>
<td>ca38e9f1-03f4-402e-9add-46ba9baad373</td>
<td>File</td>
<td>75,962</td>
<td>8/13/2018 10:34:47 PM</td>
</tr>
</tbody>
</table>
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\.
**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, MacOS X, Windows, and Android.[8]

**Features**

- 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 Dbim 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.[9]

**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
Shell Usage

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\mnt\user\bash_history
- \home\chronos\user\bash_history
- \home\chronos\u-532152efe238bbe139702d32ce90409ba4bf8b3a\bash_history
- \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\bash_history
# Shell Usage - .bash_history

<table>
<thead>
<tr>
<th>GO TO</th>
<th>FIND</th>
<th>HIDE DECODING</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>64</td>
<td>dir.ls.pwd.cd home.1</td>
</tr>
<tr>
<td>020</td>
<td>73</td>
<td>s.cd chronos.cd chron</td>
</tr>
<tr>
<td>040</td>
<td>6F</td>
<td>os.ls.1s -ls.cd u-33</td>
</tr>
<tr>
<td>060</td>
<td>32</td>
<td>2152efe238bbe139702d</td>
</tr>
<tr>
<td>080</td>
<td>33</td>
<td>32ce90409ba4bf8b3a/</td>
</tr>
<tr>
<td>100</td>
<td>6C</td>
<td>ls.cd ...ls -la .cd</td>
</tr>
<tr>
<td>120</td>
<td>75</td>
<td>user.ls.cd ...cd D.c</td>
</tr>
<tr>
<td>140</td>
<td>64</td>
<td>d Default/.lks.1s.cd</td>
</tr>
<tr>
<td>160</td>
<td>20</td>
<td>...cd ...ls.cd root</td>
</tr>
<tr>
<td>180</td>
<td>0A</td>
<td>.ls.sudo ls.sudo ls</td>
</tr>
<tr>
<td>200</td>
<td>2D</td>
<td>-la.cd 532532152efe2</td>
</tr>
<tr>
<td>220</td>
<td>33</td>
<td>38bbe139702d32ce9040</td>
</tr>
<tr>
<td>240</td>
<td>39</td>
<td>9ba4bf8b3a.sudo cd 5</td>
</tr>
<tr>
<td>260</td>
<td>32</td>
<td>32ce90409ba4bf8b3a.</td>
</tr>
<tr>
<td>280</td>
<td>64</td>
<td>cpath.changepath.sud</td>
</tr>
<tr>
<td>300</td>
<td>65</td>
<td>o su.exit.su.su.sudo</td>
</tr>
<tr>
<td>320</td>
<td>20</td>
<td>su.exit.</td>
</tr>
<tr>
<td>340</td>
<td>73</td>
<td>75 0A 65 78 69 74 0A</td>
</tr>
</tbody>
</table>
Shell Usage - .bash_history

dir ls pwd cd home.l
s cd chronos.cd chron
os ls ls -la cd u-33
2152efe238bbe139702d
32ce90409ba4bf8b3a/.
ls cd ...ls -la .cd
user ls cd ...cd D.c
d Default/..ls.ls.cd
...cd ...ls.cd root
.ls sudo ls sudo ls
-1a.cd 532532152efe2
38bbe139702d32ce9040
9ba4bf8b3a.sudo cd 5
32152efe238bbe139702
d32ce90409ba4bf8b3a.
cpath.changepath.sud
o su.exit su 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\AvatarImages\aforensiclook@gmail.com
- \home\chronos\user\Accounts\AvatarImages\aforensiclook@gmail.com
- \home\chronos\user-532152efe238bbe139702d32ce90409ba4bf8b3a\Accounts\AvatarImages\aforensiclook@gmail.com
- \home\user\532152efe238bbe139702d32ce90409ba4bf8b3a\Accounts\AvatarImages\aforensiclook@gmail.com
What is the difference if I look at Chromium vs a Cloud or Takeout acquisition of the user account?
## Cloud/Takeouts/Chromium

<table>
<thead>
<tr>
<th>Artifact</th>
<th>Chromium</th>
<th>Takeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser History</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Browser Cache</td>
<td>✔️</td>
<td>✗️</td>
</tr>
<tr>
<td>Browser Current Tabs</td>
<td>✔️</td>
<td>❓️</td>
</tr>
<tr>
<td>Browser Last Tabs</td>
<td>✔️</td>
<td>❓️</td>
</tr>
<tr>
<td>Browser Current Sessions</td>
<td>✔️</td>
<td>❓️</td>
</tr>
<tr>
<td>Browser Last Sessions</td>
<td>✔️</td>
<td>❓️</td>
</tr>
<tr>
<td>Downloads</td>
<td>✔️</td>
<td>✗️</td>
</tr>
</tbody>
</table>
## Cloud/Takeouts/Chromium

<table>
<thead>
<tr>
<th>Artifact</th>
<th>Chromium</th>
<th>Takeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hidden Folder</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Extensions</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Offline Storage</td>
<td>✔️</td>
<td>✗*</td>
</tr>
<tr>
<td>Shell Usage</td>
<td>✔️</td>
<td>✗</td>
</tr>
<tr>
<td>Avatar</td>
<td>✔️</td>
<td>✉️</td>
</tr>
<tr>
<td>Pictures</td>
<td>✔️*</td>
<td>✔️*</td>
</tr>
<tr>
<td>Task Lists</td>
<td>✗️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Further Research

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

- Method to image Chromebooks
- Method to decrypt Chromebooks
- Parsers
  - Will have some by OSDFCOn in a few weeks!
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?

jad@magnetforensics.com
@JadAtMagnet

jessica.hyde@magnetforensics.com
@B1N2H3X