dbling: Identifying Extensions Installed on Encrypted Web Thin Clients

DFRWS 2016 | Seattle, WA | August 8, 2016

Mike Mabey, Adam Doupé, Ziming Zhao, Gail-Joon Ahn
Arizona State University

Chromebooks In the News

Apple loses more ground to Google's Chromebook in education market

Jon Swartz, U

(Photo: Laraine Weschle
(Waterbury, Conn.) Republican-
American via AP)

according to a recent re
Futuresource Consultin
fundamental shift in hov
buying tech in bulk and assessing students online, placing
easy-to-manage machines.

THE VERGE

TRENDING NOW
Police are filing warrants for Android's vast store of location data

42 NEW ARTICLES

LOG IN | SIGN UP LONGFORM REVIEWS VIDEO TECH CIRCUIT BREAKER SCIENCE ENTERTAINMENT CARS TL;DR FORUMS

GOOGLE TECH REPORT

174 COMMENTS

Chromebooks outsold Macs for the first time in the U

By Tom Warren on May 19, 2016 07:50 am

THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

TECH | CONSUMER TECHNOLOGY

Google Bringing Android Apps to Chromebooks

codeweavers

CrossOver What Runs Porting About Us

CROSSOVER FOR ANDROID RUNS ON CHROMEBOOKS!

James Ramey / July 14th, 2016 / CrossOver for Android RUNS on ChromeBooks!

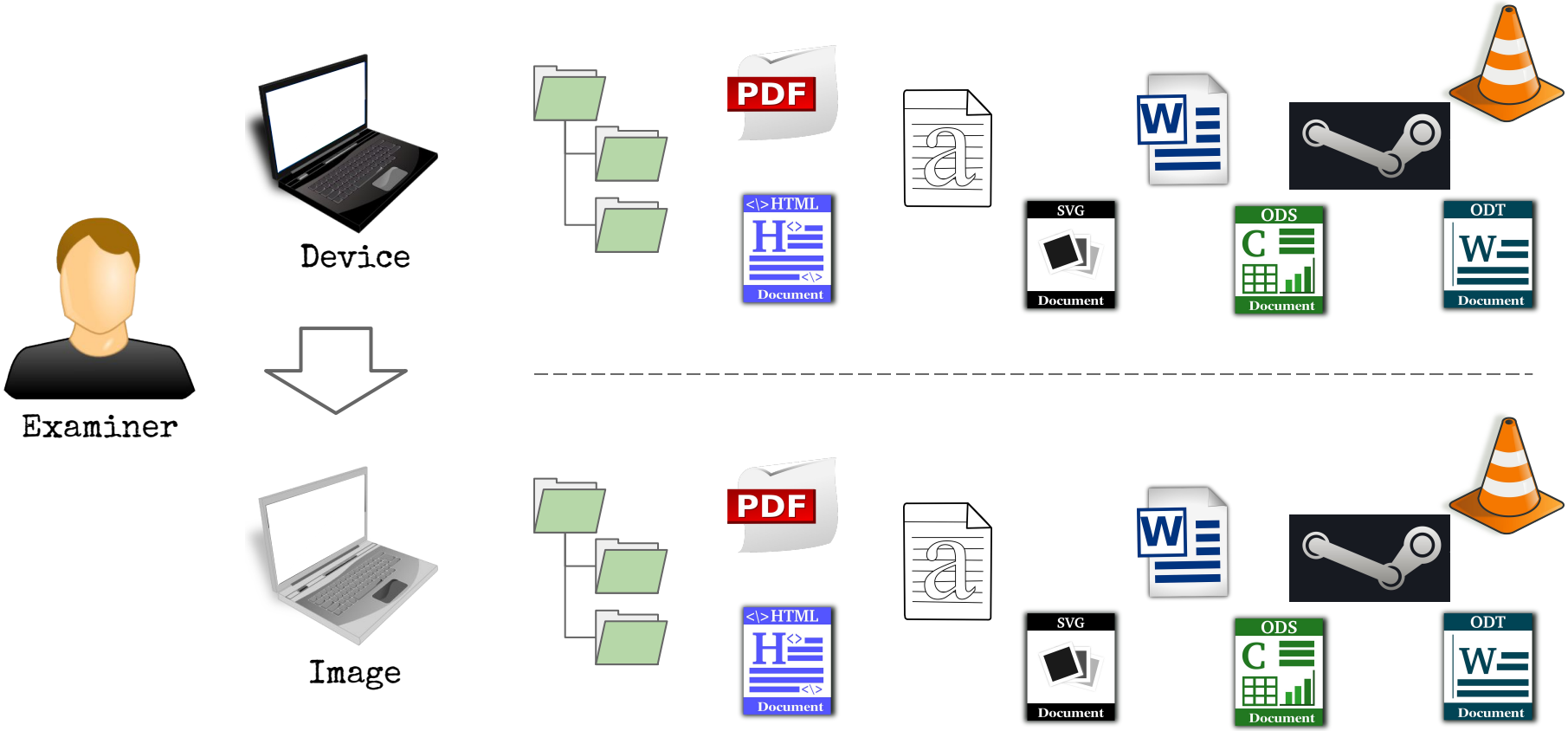
Sources:

http://www.usatoday.com/story/tech/news/2016/01/11/apple-loses-more-ground-googles-chromebook-education-market/78323158/
http://www.theverge.com/2016/5/19/11711714/chromebooks-outsold-macs-us-idc-figures
http://www.wsj.com/articles/google-bringing-android-apps-to-chromebooks-1463689585
https://www.codeweavers.com/about/blogs/jramey/2016/7/14/crossover-for-android-runs-on-chromebooks

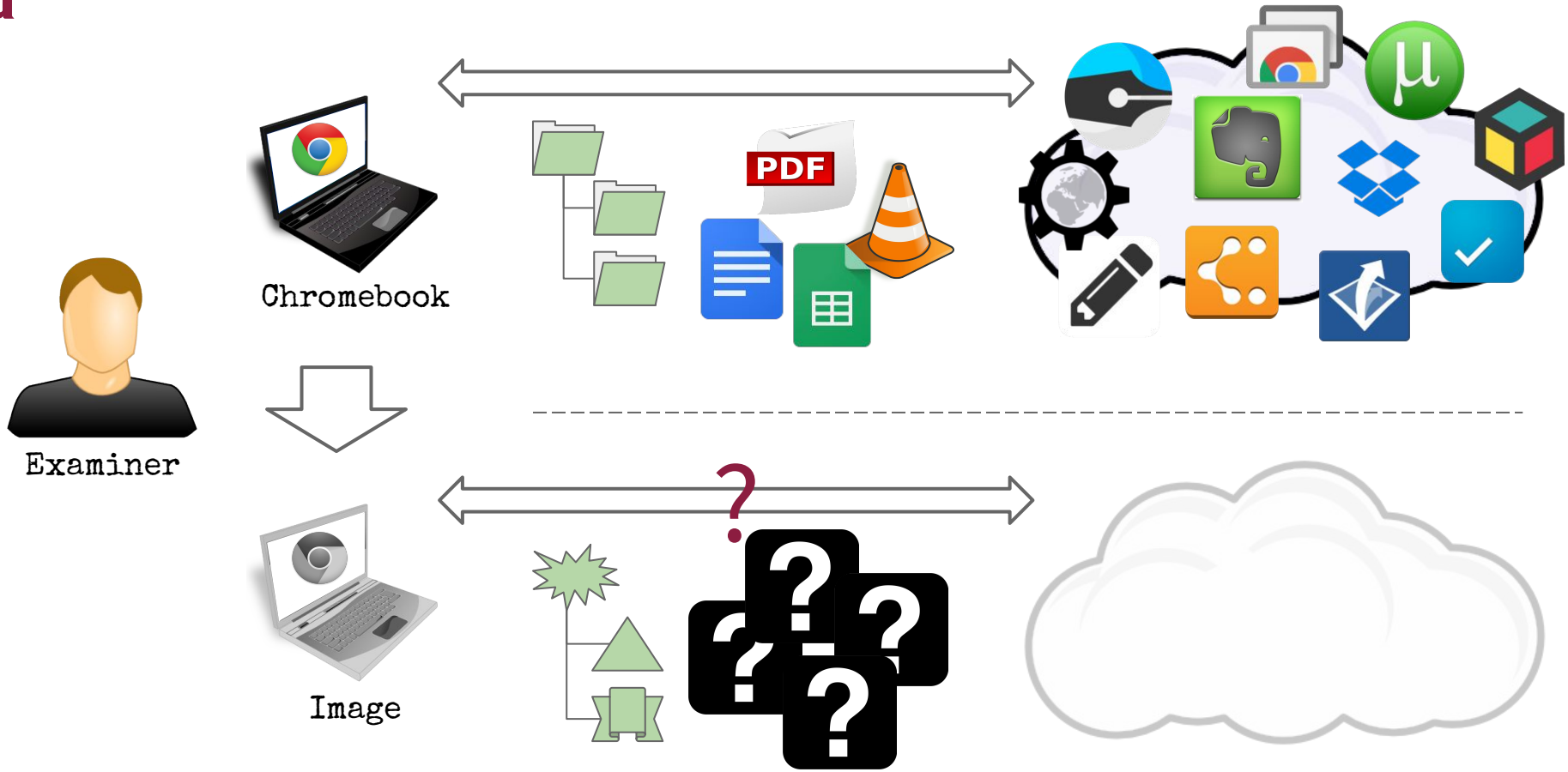
Forensics?

?

iOS



"Traditional" Acquisition

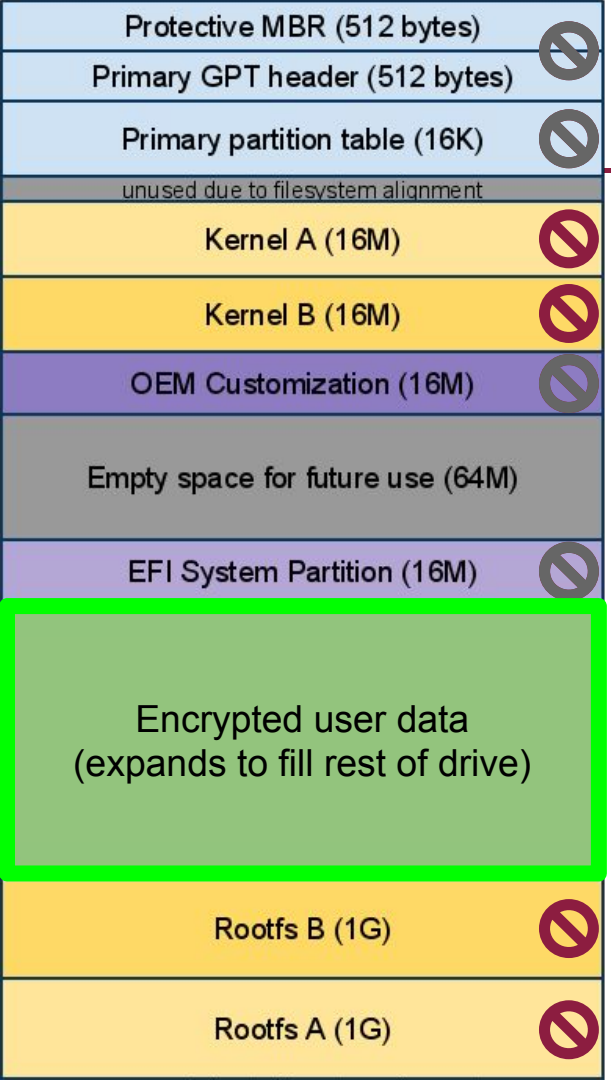


Acquisition on a Chromebook

Some Chrome OS Features

- Linux kernel
- TPM and Secure Boot
- Encrypted user data (eCryptfs)
- Limited local storage
- Extensions

Disk Structure

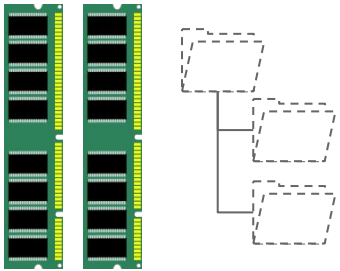


- The Kernel and Rootfs partitions are:
  - Effectively read-only
  - Have verified contents
- User data “stateful partition”
  - Contains `/home` directory
  - Encrypted per-user by eCryptfs

Image source: http://www.chromium.org/chromium-os/chromiumos-design-docs/disk-format

sefcom

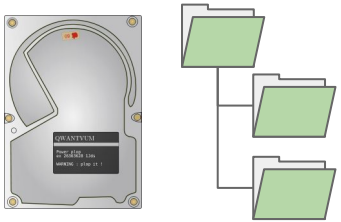
Filesystem Structure



Upper Filesystem

- Lives in memory
- Decrypted version of user data
- Directory of most interest for forensics:
  `/home/user/<user ID>/`

Users can't control this

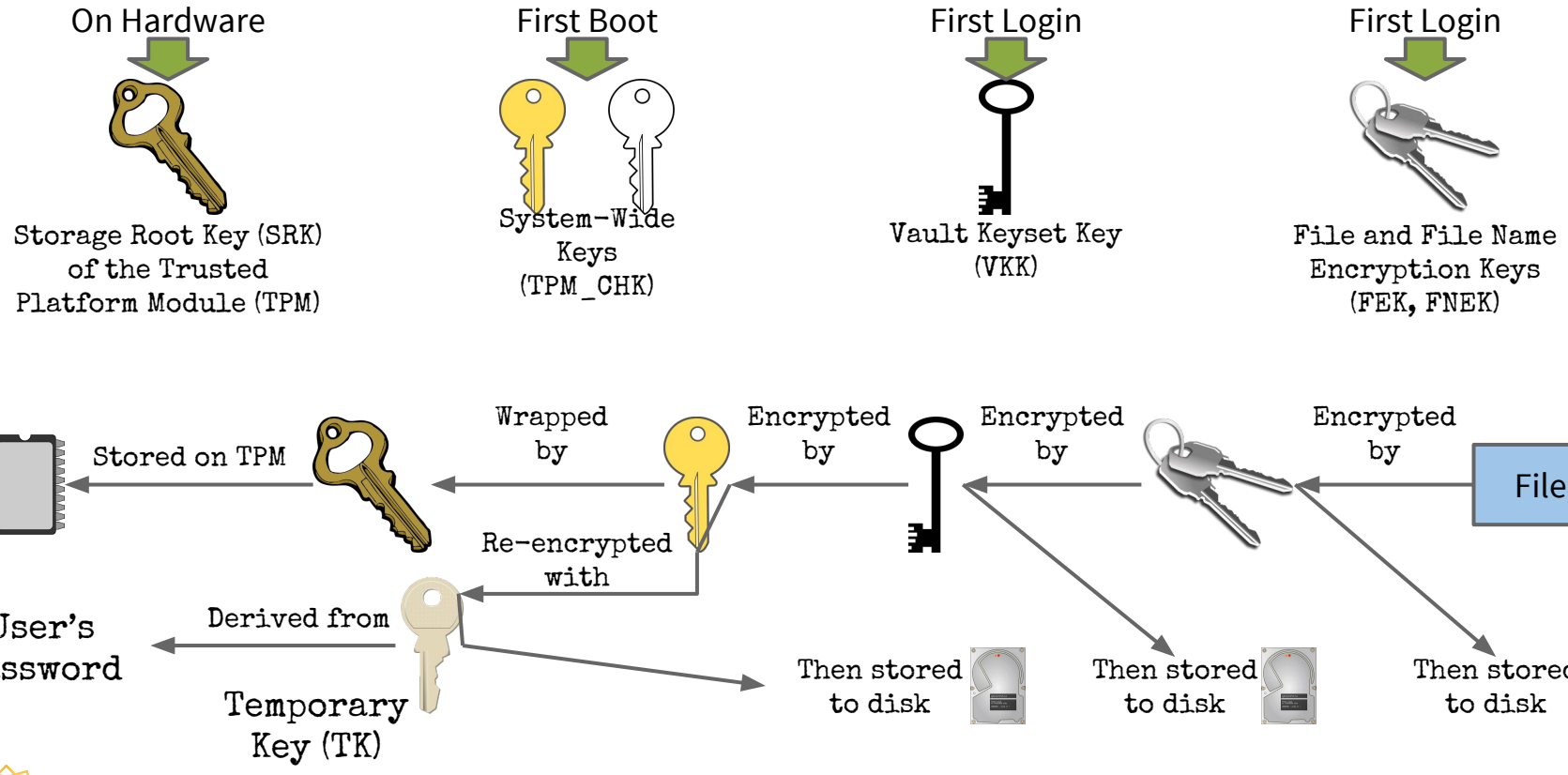


Lower Filesystem

- Data at-rest on the drive
- Encrypted version of user data
- Path of directory listed above:
  `/home/.shadow/<user ID>/vault/user/`
- Metadata remains mostly intact

Important

Encryption Summary



Assumptions

- Cannot analyze files directly from hard drive image
  - Can't break the encryption → some keys are 8192 bits long
  - Can't extract the keys → TPM is tamper-resistant
  - Might be able to brute-force the user's password if weak
    - TPM rate-limits guesses
  - Local storage has some *unknown subset* of users' files
    - Doesn't satisfy the Completeness rule of evidence

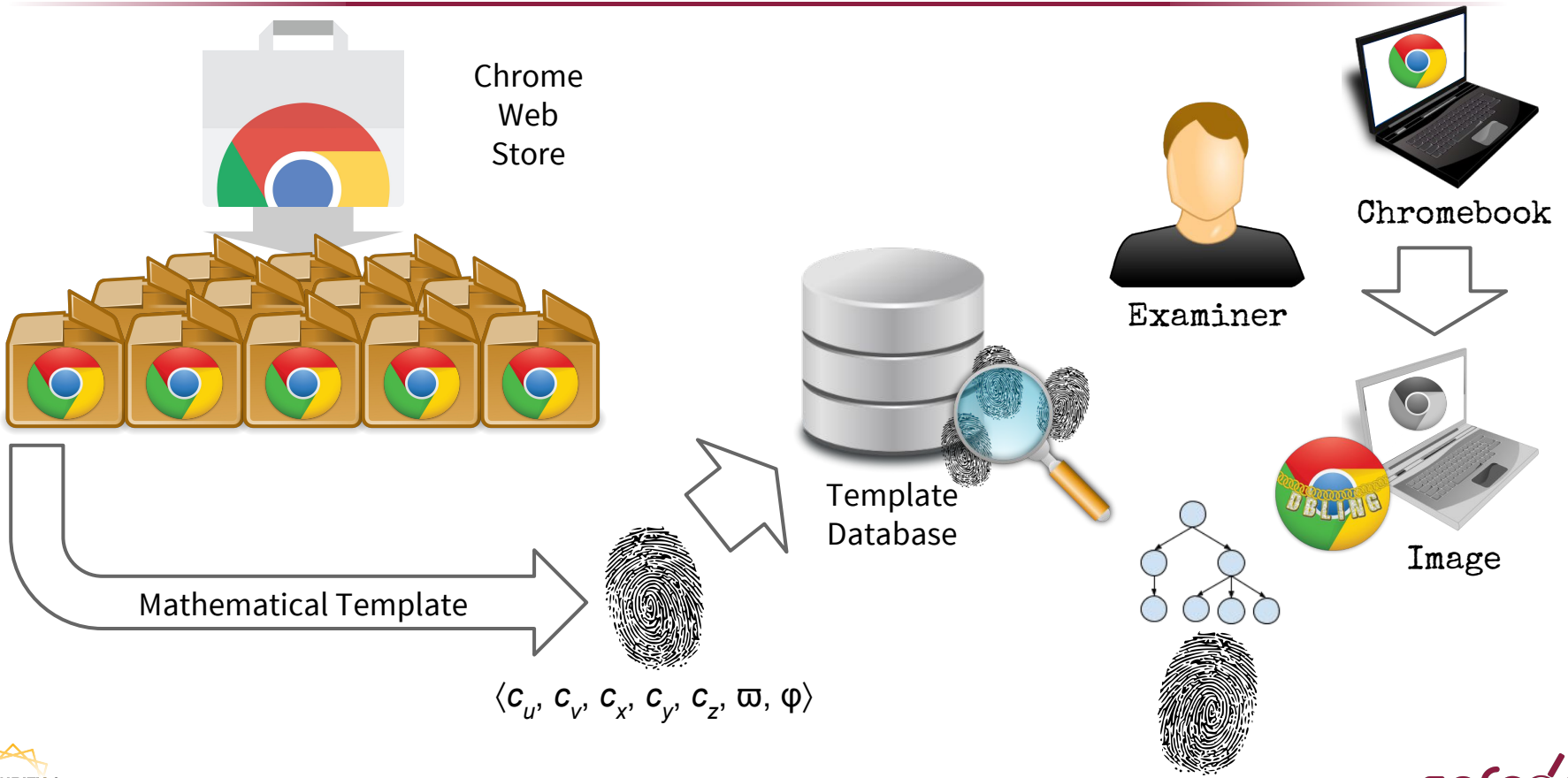
- Cannot boot to custom forensics OS
  - Requires putting the device in developer mode which resets the TPM

Approach

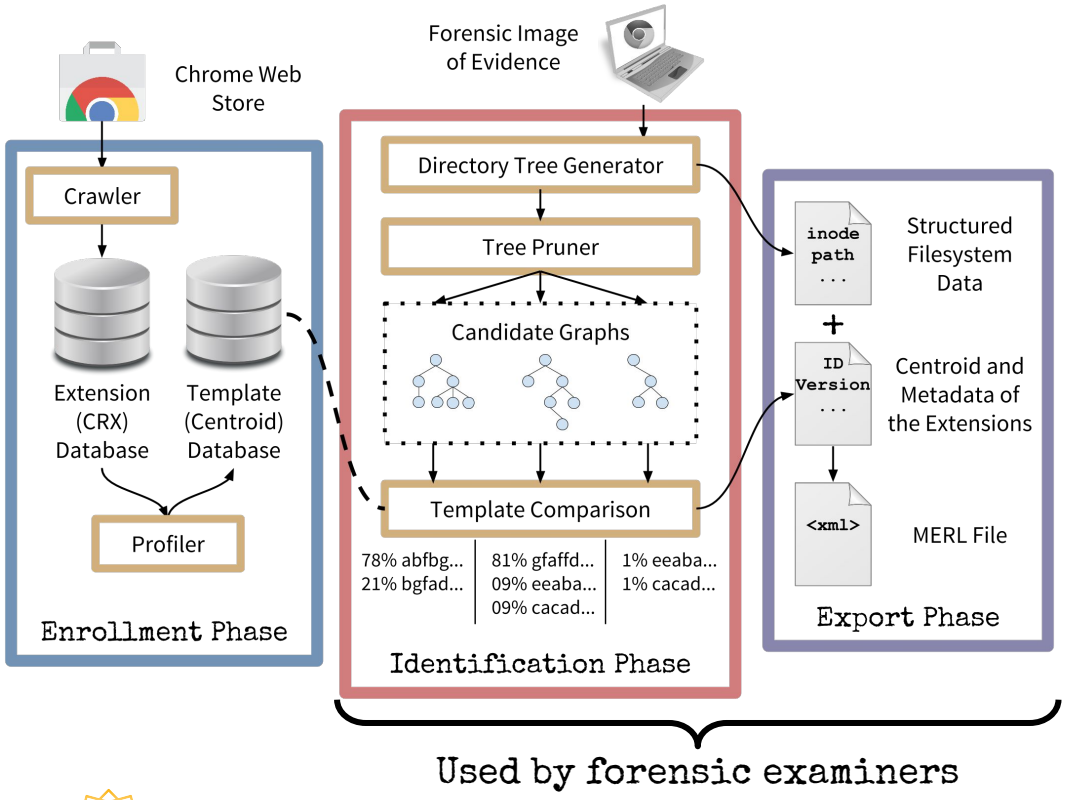
dbling: Goals

- Extract residual evidence stored by Chrome OS
- Do not rely on:
  - Accessing users' data stored online
  - Breaking or extracting encryption keys
  - Circumventing secure boot features
- Determine which extensions and apps users installed

dbling: Overview



dbling: Three Phases

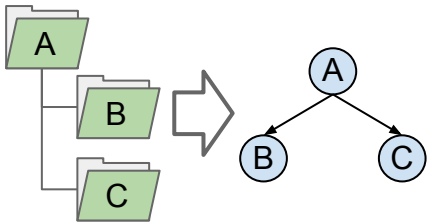


1. Enrollment
   - Download, extract CRX, create profile
2. Identification
   - Candidate selection
   - Compare against template database
3. Export
   - Store comparison results in structured format

dbling: Enrollment

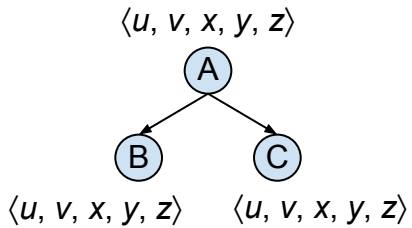
Create graph from directory tree 5D-FileTree

- 5D-FT = (V, A)
- Arcs denote membership in a directory



Give each vertex a 5D-Coordinate

- u: Num child directories
- v: Num child files
- x: Mode (permissions)
- y: Depth from root
- z: File type number



Calculate the template

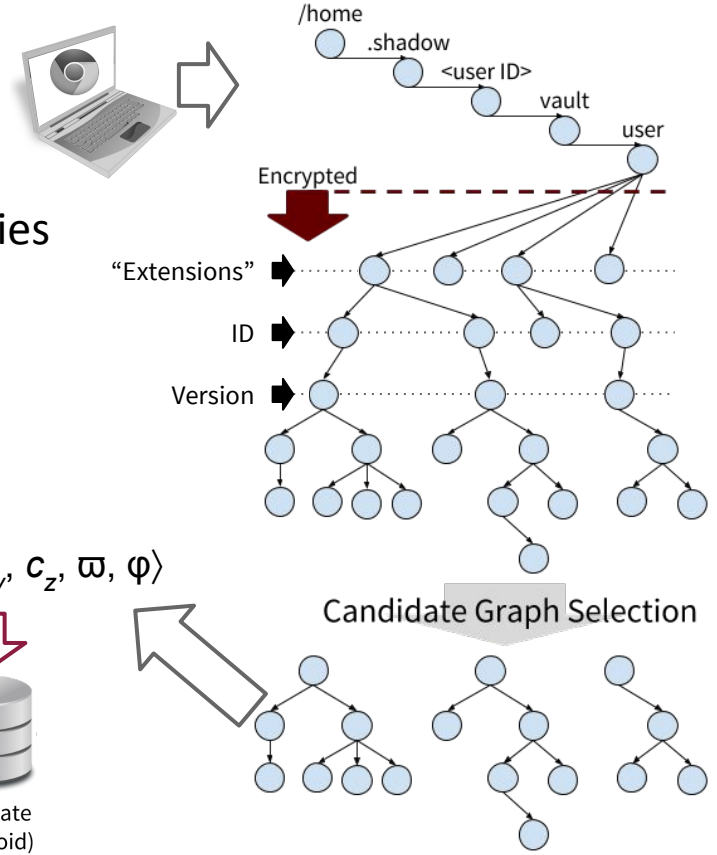
- 7-dimensional vector
- ϖ: Size of files
- φ: $|V|$

$$\langle c_u, c_v, c_x, c_y, c_z, \varpi, \varphi \rangle$$

$$c_i = \frac{\sum_{a(p,q) \in A} (\varpi_p i_p + \varpi_q i_q)}{\varpi}$$

dbling: Identification

1. Import raw image of device
2. Make graph from directory tree
3. Isolate (potential) extension version directories
4. Calculate template for each candidate graph
5. Search the database for match
   i. Filter by φ
   ii. Sort (rank) by distance
6. Export results

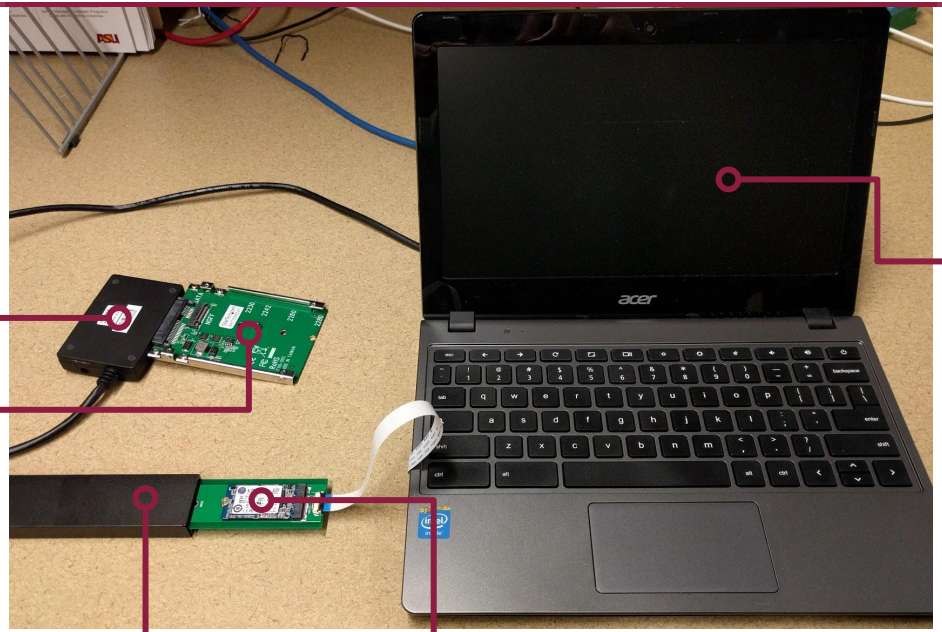


dbling: Export

- Matching Extension Ranking List (MERL)
- XML document
- Identifies:
  - Original image
  - Source program
  - Environment
  - Matching inode
  - Potential matches

```
<merl>
  <source>
    <image_filename>chromebook_test01.img</
        image_filename>
    <mount_point>/mnt/dbling/</mount_point>
  </source>
  <creator>
    <program>dbling_merl</program>
    <version>0.0.1</version>
    <execution_environment>
      <command_line>sudo dbling_merl -v -m /mnt/dbling/<
          /command_line>
    </execution_environment>
  </creator>
  <match>
    <inode>259696</inode>
    <candidate>
      <ext_id>abfbgiabldngkapfilcncjplidclalae</ext_id>
      <ext_ver>1.0.3</ext_ver>
      <ext_name>Mangekyou1999</ext_name>
      <ext_vendor>Mangekyou1999</ext_vendor>
      <confidence>0.78</confidence>
    </candidate>
  </match>
</merl>
```

dbling: Case Study Setup



SATA to USB 3.0 Adapter

NGFF to SATA Adapter

NGFF External Adapter

Original 16 GB SSD (NGFF 2242)

Acer C720 Chromebook in Developer Mode

dbling: Case Study Results (1)

Name	Version	Offline	# Users*	φ	τ	Rank
Lucidchart Diagrams — Desktop	1.116	Y	389,087	3,507	3	1-3
Marxico	1.6.1	Y	29,379	711	7	1-7
Piconion Photo Editor	1.9.0.0	Y	24,684	370	12	2
Reditr — The Best Reddit Client	0.3.3.1	Y	53,687	134	71	1
Google Hangouts	2016.120.1336.1	N	5,468,622	150	78	1-19
Advanced REST client	4.6.0	N	1,040,107	131	102	8-12
Evernote Web	1.0.8	N	3,638,599	41	580	308

*Number of users is based on what was posted on the Chrome Web Store as of the original publication submission

φ = # of files

τ = # of extensions with same φ

dbling: Case Study Results (2)

Name	Version	Offline	# Users*	φ	τ	Rank
TweetDeck by Twitter	3.10	N	1,584,975	15	2,808	894; 1,904
Any.do	3.1.1	Y	260,355	13	3,894	3,217
ShiftEdit	1.43	Y	159,170	6	5,766	2,175
Outlook.com	1.0.2	N	1,485,767	7	9,259	4,318; 4,520
Google Play	3.1	N	3,624,424	5	11,768	6,919; 6,989
Netflix	1.0.0.4	N	1,769,793	5	11,768	9,630
Little Alchemy	1.4.0	Y	1,518,447	5	11,768	10,328

*Number of users is based on what was posted on the Chrome Web Store as of the original publication submission

φ = # of files

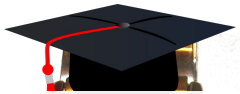
τ = # of extensions with same φ

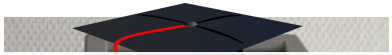
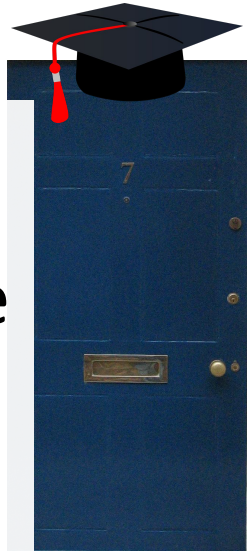
dbling: Future Work

- Enrollment improvements:
  - Unpacking CRXs in manner more like Chrome OS
  - Accounting for eCryptfs overhead space
- Evaluation:
  - Large-scale evaluation of all CRXs
  - Obtain previously inaccessible extensions
- Other residual evidence:
  - Timeline reconstruction
  - …

dbling: Contributions

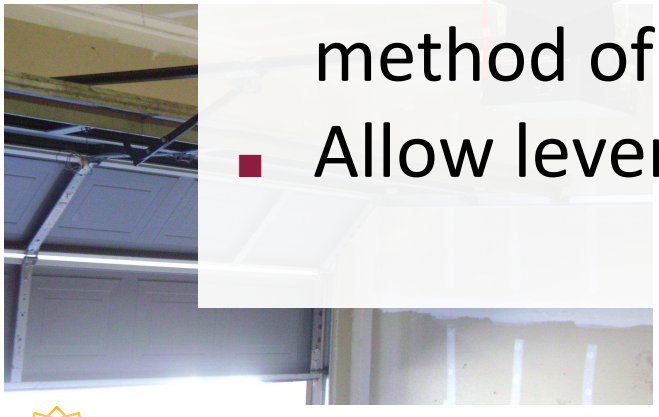
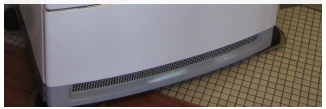
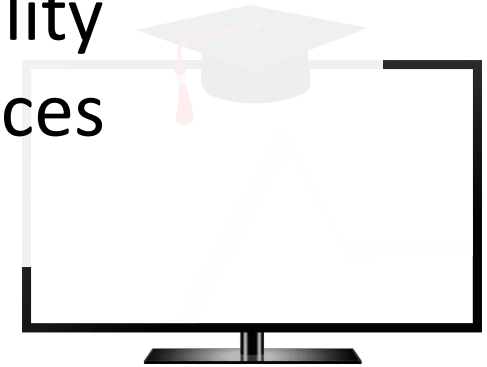
- Make sense of metadata on an encrypted device
  - No breaking the encryption
  - No loading custom OS
- Narrow down scope of the forensic analysis
  - 6/14 extensions had correct match in the top 10
  - 100K extensions to 10K in worst case
- First step toward comprehensive web thin client forensics

Web Thin Client Operating Systems:

- Lightweight OS with minimal hardware requirements
- Extensions provide a sandboxed method of adding functionality
- Allow leveraging cloud services

Sources: https://commons.wikimedia.org/wiki/File:Mandeville_Maxens_refrigerator.JPG, https://commons.wikimedia.org/wiki/File:Pylon_ds.jpg, https://commons.wikimedia.org/wiki/File:Monitor_(medical).jpg, https://commons.wikimedia.org/wiki/File:24-hour_watch_by_Zureks.jpg, https://commons.wikimedia.org/wiki/File:Modern_TV.png, https://commons.wikimedia.org/wiki/File:Garage_door_opener.jpg, https://commons.wikimedia.org/wiki/File:Blue_Door.jpg, https://commons.wikimedia.org/wiki/File:Old_car_at_Newport_Quay_2.JPG

Acknowledgements

- Alex Nelson
- Anonymous reviewers
- U.S. Department of Defense Information Assurance Scholarship Program (IASP)
- Center for Cybersecurity and Digital Forensics (CDF) at Arizona State University

Thank You!
Questions?

Mike Mabey

mmabey@asu.edu

mikemabey.com

@mkmabey