

THE GOOGLE CHROME OPERATING SYSTEM FORENSIC ARTIFACTS

By

George Corbin

A Capstone Project Submitted to the Faculty of

Utica College

December 2014

In Partial Fulfillment of the Requirements for the Degree of

Master of Science in  
Cybersecurity

UMI Number: 1571599

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



UMI 1571599

Published by ProQuest LLC (2014). Copyright in the Dissertation held by the Author.

Microform Edition © ProQuest LLC.

All rights reserved. This work is protected against unauthorized copying under Title 17, United States Code



ProQuest LLC.  
789 East Eisenhower Parkway  
P.O. Box 1346  
Ann Arbor, MI 48106 - 1346

© Copyright 2014 by George Corbin

All Rights Reserved

## **Abstract**

The increased popularity of Google Chromebooks due to their ease of use, security features and low price have contributed to explosive growth in terms of their market share in the personal computing marketplace. This growing market share will result in Chromebooks becoming part of new and ongoing forensic investigations. It is important for forensic investigators to have a strong understanding of the forensic artifacts found on a Google Chromebook. The investigators need to know what these artifacts mean and how to acquire them. A Google Chromebook uses the Google Chrome Operating System for its operating system. The purpose for the research was to begin developing the necessary art in support of forensic examiners tasked with investigating Google Chromebooks and the data they use. Keywords: Cybersecurity Intelligence and Forensics, Professor Cynthia Gonnella, ChromeBook, forensic artifacts, virtual machine.

## **Acknowledgements**

Many people helped me along the way to completing this dual major Master's program. I would like to start with my lovely Bride Tonya for her patience, love and support. I want to issue my thanks to my three wonderful children Brianna, Aiden and Brendan whom are the reason for everything I do. The past few years have had their challenges, and I love you each very much and considering the daddy time you have sacrificed so I can complete this program you have given more than others have.

I would also like to acknowledge the hard work my first and second readers have put into my efforts, Professor Cynthia Gonnella and Detective Duc Nguyen. Professor Gonnella has gone beyond the call of duty in her efforts to get me to the end. Thank you very much Professor Gonnella. I would also like to thank Assistant Professor Lopez for pinch-hitting for Professor Gonnella. Without each of you, I would not have finished and may not have ever started since you helped me to acquire a topic technical enough to keep my attention.

Finally, I want to offer my sincerest gratitude to my parents. My father taught me that everyone brings value into my life and showed me how to see it. My passion for volunteer work and helping others to be their best version of themselves comes from his influence. My mother deserves most of the credit for how I have come to love and value myself. She has been and will always be my biggest fan. She taught me how important it is to love your family and friends, even when you sometimes do not like them. My mother taught me to value education over popularity. She taught me to love and value myself no less than I do others. The blessings my parents gave me make me the man I am today. I have no regrets.

## Table of Contents

List of Illustrative Materials.....	vi
The Google Chrome Operating System Forensic Artifacts .....	1
The Relevance of Google Chrome Operating System Artifacts.....	2
Literature Review.....	6
Methodology.....	13
Setup .....	18
Hardware.....	18
ZTC 2-in-1 Thunder Board M.2 (NGFF) Board Adapter.....	19
Patuoxun USB 2.0 to SATA Converter Adapter Cable.....	19
Acer c720 Chromebook.....	19
Dell Inspiron 15 7000 Series Model 7537 Touchscreen.....	19
Software.....	20
Microsoft Word Professional 2010.....	20
VMWare Workstation 10.0.3 – build 1895310.....	20
Microsoft Windows XP Professional SP 3.....	20
Google Chrome browser version 38.0.2125.111 m.....	20
Google Chrome Operating System v38.....	21
AccessData FTK Imager 3.1.0.1514.....	21
AccessData Forensic Toolkit 1.81.6.....	21
ChromeAnalysis Plus 1.4.1 Trial for Windows.....	21
Google Gmail Account.....	21
Evaluation Foundation.....	21
Analysis.....	22
Commence .....	22
Preparation .....	23
Evidence Source Identification and Preservation .....	23
Collection.....	23
Examination and Analysis .....	24
Artifacts of Google Chrome Operating System from SSD Image Capture.....	24
Artifacts of Google Chrome Browser in Windows XP VM While Logged In.....	28
Artifacts of Google Chrome Operating System in Developer Mode.....	33
Crosch Tools Available in <i>Shell</i> .....	40
Crosch Running Ubuntu Unity Release.....	43
Using Linux Tools on Chrome Operating System for Forensic Toolkits.....	47
Logical Copy of Chromebook User Directory and Analysis Using FTK.....	47
Discussion of Findings.....	52
Future Research Recommendatios.....	55
Google Chromebook Forensic Tools Run from a USB Flash drive.....	55
Establish a Legal Relationship with Google.....	555
Chromebook Browser Artifact Extraction in Mainstream Tools.....	56
Conclusion .....	56
References.....	58

## List of Illustrative Materials

<i>Figure 1.</i> FTK Object table of captured image after carving .....	25
<i>Figure 2.</i> Thirteen areas carved from SSD space .....	25
<i>Figure 3.</i> EFI-SYSTEM object group from data carve .....	26
<i>Figure 4.</i> Grub in boot sector.....	26
<i>Figure 5.</i> FTK showing User work of SSD Image named STATE .....	27
<i>Figure 6.</i> Start of User space .....	28
<i>Figure 7.</i> User directory containing Chrome files .....	29
<i>Figure 8.</i> Website History from Google account.....	29
<i>Figure 9.</i> Bookmarks stored in Google account .....	30
<i>Figure 10.</i> Cookies from Google account.....	30
<i>Figure 11.</i> Empty download history from Google Account .....	31
<i>Figure 12.</i> Empty Search history .....	31
<i>Figure 13.</i> Empty Login History for remote accounts.....	31
<i>Figure 14.</i> Most visited website list.....	31
<i>Figure 15.</i> Icons from websites in favorites (bookmarks) .....	32
<i>Figure 16.</i> Archived webpages unused.....	32
<i>Figure 17.</i> First 25 from cache .....	33
<i>Figure 18.</i> Listing of User directory in Crosh .....	34
<i>Figure 19.</i> Chromebook browser History .....	35
<i>Figure 20.</i> Chromebook browser Bookmarks .....	35
<i>Figure 21.</i> Chromebook browser Cookies.....	36
<i>Figure 22.</i> Chromebook browser Downloads directory .....	37
<i>Figure 23.</i> Chromebook browser Search History .....	37
<i>Figure 24.</i> Chromebook browser Login History .....	38
<i>Figure 25.</i> Chromebook browser Most Visited Sites .....	39
<i>Figure 26.</i> Chromebook browser Cache.....	39
<i>Figure 27.</i> Chromebook browser Google Drive Contents.....	40
<i>Figure 28.</i> Path to USB drive .....	41
<i>Table 1:</i> Linux-based programs available in Crosh Shell within Chrome Operating System.....	41
<i>Figure 29.</i> Issuing Crosh command "sudo startunity" .....	43
<i>Figure 30.</i> Ubuntu Unity release desktop .....	44
<i>Figure 31.</i> Ubuntu Terminal <i>ls</i> of local user dir Downloads .....	45
<i>Figure 32.</i> Crosh shell after logoff Ubuntu screen 1 .....	46
<i>Figure 33.</i> Crosh shell after logoff Ubuntu screen 2 .....	46
<i>Figure 34.</i> Snapshot of FTK files from <i>user</i> dir .....	49
<i>Figure 35.</i> Web History unavailable.....	49
<i>Figure 36.</i> Bookmarks .....	49
<i>Figure 37.</i> Cookies.....	50
<i>Figure 38.</i> Empty Download Directory .....	50
<i>Figure 39.</i> Empty Search Terms .....	50
<i>Figure 40.</i> Empty Logins .....	51
<i>Figure 41.</i> Most Visited Sites .....	51
<i>Figure 42.</i> Favicons revisited .....	51
<i>Figure 43.</i> Empty Archive .....	51
<i>Figure 44.</i> Empty Cache .....	52

## **The Google Chrome Operating System Forensic Artifacts**

The Google Chrome Operating System is a robust and powerful operating system designed to run on inexpensive laptops. The growing popularity and affordable price-point of Chromebooks make it a certainty that forensic examiners not already tasked with investigating the digital contents of these popular devices, eventually will. One reason for choosing this research topic was to assist forensic examiners with their future tasks of examining the Chromebook studied in this paper, and any other devices running the Google Chrome Operating System. The purpose of this research was to explore the forensic artifacts recoverable during investigations involving the Google Chrome Operating System.

When investigating the artifacts within the Google Chrome Operating System, several questions arise. What artifacts are available from a cold capture of data from a Google Chromebook's storage device? What additional data is available directly from the suspect Google account logging in with Google Chrome Browser? What artifacts are available on a Chromebook in Developer Mode that may aid or hinder a forensic examination? What additional artifacts are available with Ubuntu installed within the Crosh shell? What artifacts are discoverable from a logical image of the user data from Google Chromebook?

This research explains the relevance of Google Chrome Operating System artifacts for today's electronic investigations, describes techniques for examiners to become familiar with Google Chrome Operating System and its files. Further, it offers insight into the many artifacts that can be located for the various installations and usage of Google Chrome Operating System as well as the Google Chrome browser for a more comprehensive comparison. This research will enable others to investigate Google Chrome Operating System artifacts and conduct future research. In order to support forensic examiner's efforts to collect, preserve, and analyze artifacts



from Google Chrome Operating System based devices, it was important to identify and share the actual artifacts available. Due to the tight integration of Cloud computing in Google accounts, the data found was diverse, varied, and complex.

### **The Relevance of Google Chrome Operating System Artifacts**

Today's Information Technology industry innovates rapidly by developing and releasing new products that require testing and research to understand the artifact. The expectation is that forensic examiners keep themselves up-to-date in the latest technologies. Chromebooks based upon the Google Chrome Operating System are one such innovation, which is an attractive new technology. Just a year ago (2013), at the Intel Developer Forum, Jason Mick reported that Intel was beginning to distance themselves from Microsoft (MS) over problems they have been having with Windows 8 adoption and moving to grow their presence in the Chromebook sub-sector of personal computers. At the time, Intel announced the approaching availability of more power efficient processors in low cost personal computing devices such as Google Chromebooks and other Google Chrome Operating System based devices (Mick, 2013). As reported by Frederic Lardinois of TechCrunch.com, Google and its partners sold 1 million Chromebooks in the fiscal quarter of April through June 2014 (Lardinois, 2014). With this high level of consumer adoption, it is inevitable that a device using the Google Chrome Operating System will find its way into an investigation requiring a forensic investigator to collect artifacts during the course of their work. For the examiners who would have had no formal training or experience with the Google Chrome Operating System, this paper identified and explained the various artifacts. Criminals use what tools they have access to and the low price point of around \$200 USD for a Chromebook makes the devices attractive as a communication tool used for the Internet (Lardinois, 2014). Packed with features to address modern Information Technology security

problems, combined with a very competitive price-point for new and low-income users, Chromebooks are quickly becoming a prolific presence in consumer households (Fang, Hanus, & Zheng, 2011). These features include encryption of network traffic, encryption of data on the device and stored in the Cloud, constant checks for updates, verified boot that detects system changes when it launches the operating system, and provides a secure way to backup and restore the system.

Chromebooks have been available since June 15, 2011, when Acer and Samsung began shipping their first models (Efrati & Sherr, 2011). Schools buy them for just \$20 per device per month using the Chromebooks for Education program offered by Google (Chromebooks for Education, 2013). Further enhancing their popularity, Chromebooks provide a personal computer experience without requiring installation and maintenance of software. This is possible since the applications connect to the user's Chromebook ID and executes the applications within the Chrome web browser. This function is very similar to how MS Windows Remote Desktop operates. Google refers to this as Chrome Remote Desktop.

However, not all users are the same. Some will use Chromebooks in ways unintended by their designers producing unusual challenges to forensic examiners and will use Chromebooks in support of illicit endeavors. Cyber criminals are likely to utilize Chromebooks due to the encryption features, low price, and since it is still relatively new, they leverage the limited Chrome Operating System forensic experience of Law Enforcement to support, conceal, and execute their illegal activities. While the use of Chromebooks is spreading quickly, a thorough Internet search has produced no papers or articles specifically covering the forensic artifacts of the Google Chrome Operating System (Lardinois, 2014). Scholarly research and forensic manuals only include materials to handle the data stored inside of the Cloud such as Google

Drive, which is the Cloud service Chrome Operating System uses to store user files (Ackerman, 2013). This lack of useful research is wholly inadequate in light of the popularity of Chromebooks and their fast growing market share of low-end personal computers. Without this kind of research, forensic examiners would have to expend additional time doing this research themselves. Extra time used by the examiner prolongs the investigation and possibly results in a failure to prosecute in a timely manner. While the Google Chrome Operating System is technically a Linux based operating system, it is divergent enough from other distributions that an examiner needs to treat it as a completely new device. As a new device, an examiner would be required to discover artifacts present, understand them scientifically, and identify their origin and value to the overall operating system. Research which identifies these artifacts, how to collect them, how to analyze them, and finally how to incorporate them into an investigation is of tremendous value to the forensic community. This paper initiates production of this body of research and includes suggestions for additional complimentary research and development.

Cold capture is the first effort an examiner uses since typically evidence arrives on their examination table as powered down electronic devices. It is very likely that a powered down Chromebook or the Solid State Drive (SSD) will require data captured and analyzed (Rogers, Goldman, Mislán, Wedge, & Debrotá, 2006). While cold capture readily enables an investigator to capture data and analyze digital copies of the data, it introduces a weakness to the investigation. A running computer may have applications running which have valuable data inside of memory that the application is using. Active memory can reveal useful data in an investigation. While a computer is running, applications in memory maintain the data in memory unencrypted, even when encrypted on the remote system. Furthermore, if there are any running applications connected to a remote system, credentials required to access those remote sources

are available in an open and readable format for collection. These credentials may include userids, passwords, and keys for encryption and decryption. For instance, when a user connects to a Cloud service, such as Google Drive, the data resides in memory unencrypted and encrypted when stored in the remote Google Drive directory. Being able to capture this live memory can provide unencrypted data and re-usable credentials to further the investigation. A computer which is shut down does not have programs running in memory and the only useful data will be that which is stored onto local storage media such as a Hard Disk Drive (HDD), Universal Serial Bus (USB) flash drives, or optical storage media such as CD's and DVD's. In terms of Google Chrome Operating System based devices, encryption is heavily used and when the computer is shutdown, the encrypted user data is beyond reach of an investigator via typical cold capture (Fang et al., 2011; Panchal, 2013).

Due to the heavy use of Cloud technologies in Google services, the user data maintained by Google within the Gmail account is an important part of properly understanding the forensic artifacts associated with the Google Chrome Operating System installation (Fournier, 2014). For this reason, the Chrome Browser artifacts were included in this research for comparison and depth of understanding to the analysis. In order to understand the data that is available from the Chrome Browser, this investigation included processing Chrome Browser artifacts on a Windows XP Virtual Machine (VM) which has been logged into the Google Gmail account used for the other parts of this investigation.

Investigators are required to process computer systems used by suspected computer hackers who were attracted to the advanced encryption features of the Google Chrome Operating System (Fang et al., 2011). Understanding advanced features of the Google Chrome Operating System, and the impact user features have on the artifacts discoverable is important to a forensic

investigator. This research delved into a ChromeBook configured into Developer Mode, and examined Ubuntu Linux installed using an emulator virtualization program (Cipriani, 2014; Bhartiya, 2014). An investigator should know the additional artifacts available as well as the applications that may be of use to their investigation. The Crosh shell and the Ubuntu Linux distribution provide many of these additional artifacts and the applications available in the installation and usefulness to an investigation identified in this research. The purpose of these particular methods were to offset a lack of any forensic related tools known to be available specifically for running on Google Chrome Operating System.

### **Literature Review**

The purpose of this research was to explore the forensic artifacts recoverable during investigations involving the Google Chrome Operating System. In support of this effort, prior art must be considered to add strength to the effort. Researching prior art in the topic of the Google Chrome Operating System and Chromebook forensics, uncovered only a couple notable papers complimentary to the research completed for this paper. Katherine Fang, Deborah Hanus, and Yuzhi Zheng of the Massachusetts Institute of Technology (MIT) in Cambridge Massachusetts wrote the first, “Security of Google Chromebook” (Fang et al., 2011). Another of interest was “Technical Challenges of Forensic Investigations in Cloud Computing Environments” written by Dominik Birk (Birk, 2011). In “Computer Forensics Field Triage Process Model,” Rogers, Goldman, Mislan, Wedge and Debrotta provided an “on the scene” triage approach for handling digital data that included Google Chromebooks along with other digital devices of forensic interest to the investigator (2006). Finally, this literature review included a guide titled “Forensic Examination of Digital Evidence: A Guide for Law Enforcement” that was provided by the U.S.

Department of Justice to aid law enforcement with examination of digital evidence (Hart, Ashcroft, & Daniels, 2004).

In the paper “Security of Google Chromebook”, the authors Fang et al. identified two different adversaries that the Google Chrome Operating System is designed to protect against (2011). The first adversary they identified was the “opportunistic” adversary who used phishing, web site hacks, and other malicious hooks to catch the unwary Internet user. According to the authors, the opportunistic adversary casts a broad net and plans to catch a small percentage of users. Once compromised, the adversary uses the newly introduced exploit to escalate privileges on the users system to anchor their presence for later exploitation. The second adversary identified by the authors was a more dedicated adversary that may start with an opportunistic approach, but had chosen the user specifically, and was willing to bring to bear stronger efforts to compromise the user such as trying to trick them into using corrupt USB flash drives and DVDs. This dedicated adversary might even arrange to have secretive physical access to the user’s devices in order to use hardware hacks to break into the users system (Fang et al., 2011).

The authors noted that the Google Chrome Operating System really did not provide anything directly to prevent opportunistic hacks such as phishing and polymorphic viruses planted on compromised websites. However, they explained that the Google Chrome Operating System carefully blocked the functions those attacks depend on to provide access to a user’s computer. According to their results, the Google Chrome Operating System comes set up in User mode, which only allows a user to run the embedded Chrome Browser and not run any other applications on the system. Most phishing links and other attacks by an opportunistic hacker are not possible since they require an administrator level of access on the user system. Administrator

level is required to escalate the privileges it is running under, ultimately to take control and deliver a payload on the computer system (Fang et al., 2011).

The more dedicated hacker has a few extra challenges to deal with in addition to the difficulty they would have using an opportunistic hacker's approach (Fang et al., 2011). According to the authors, having physical access is certainly an option for the dedicated hacker, thus Google designed a solid Operating System in the Google Chrome Operating System by providing several secure features. The firmware for the device, which is what the hardware uses to begin functioning prior to the loading of an operating system for the user to use to perform their computer tasks, is read-only and verifies itself at boot (Fang et al., 2011). The authors also documented the firmware uses a verification process that keeps a working backup of a last known good firmware. If during boot it detects a corrupt firmware, such as that loaded on the system by a hacker, it then runs the backup and checks with Google's servers to see if there happens to be a newer version to download and install at the next boot. This verification uses some very powerful encryption processes to test the firmware before it is used and includes RSA encryption of 1024-8192 bit keys combined with hashing verification using SHA-1/256/512 message digests to ensure the firmware contents match the last time downloaded and the last time booted. The Google Chrome Operating System combined this with a read-writeable firmware for the current active one separately and if the firmware about to load is determined to be good, it then moves forward and boots up to the operating system (Fang et al., 2011).

According to Fang et al., another function provided is the operating system kernel verification performed by the firmware before booting. To support this function, the system maintains three partitions for kernel use. The first is a read-only kernel that is last known good and kept in reserve in the event the current active kernel is determined to be corrupt and

unusable. The second is the current active kernel. The third partition is for when a new kernel downloads to the computer and switches to be the active kernel at the next boot (Fang et al., 2011).

Fang et al. explained that a Google Chrome Operating System based device does an auto-update check at boot in order to verify the system has the most current firmware, kernel, and operating system. The devices use a SSD and perform all data updates very swiftly (Fang et al., 2011). To further enhance this security the system uses the same basic approach in each of the three areas; the current writeable software is verified (if not verified, the backup read-only version is used). Then once that level finishes loading, the operating system checks the Google servers for updates and downloads any necessary updates for use after the next reboot. This careful separation of data not only happens in the system partitions, it carries into the user spaces with the same high level of security in mind. The Google Chrome Operating System uses a completely separate physical storage space on the SSD for every user who logs into the device. While one user account logged in, all others suspended, so there is never a software thread or process running on the system from another user. This prevents a compromise of the current user's data by another user's data through the active Random Access Memory (RAM) (Fang et al., 2011).

The authors also asserted that the Google Chrome Operating System is a very secure system and can become even more solid with some simple changes to how the system operates. They claimed the opportunities that a hacker may have typically exist while the system is running and that the verify and update process the core operating system functions use would be more powerful if the system was rebooted more frequently. Fang et al. stated that if compromised while running, the system could do nothing about it until it runs its verification at



the next reboot. They also explained the default function of the system keeps the user logged in when closing the lid of the device such as in the case of laptops. By not logging the user out or at least locking the session and requiring a re-login when opened the next time, it leaves it open for a hacker to access it without effort when it is left unattended (Fang et al., 2011). Finally, they cited that the Developer Mode provides far too much power and leaves the system very vulnerable to hackers (Fang et al., 2011).

According to Birk's paper (2011), due to the large variety of technical implementations of Cloud computing services and the large variety of the services themselves, there are complex technical challenges for forensic examination. This complexity, he claimed, required a much larger toolset for forensic examiners to handle the high variation in the network layer, large selection of client applications, and the robust and highly varied technologies each Cloud service is based upon. Birk also explained that the core of Cloud computing solutions are VM based and the data does not necessarily reside on a specifically identifiable piece of hardware that has an address, human owner or operator, nor is it necessarily easy to access for collection and archival use (2011). This is of significance to this research since the user data the Google Chrome Operating System is handling is stored and passed through the Cloud that Google created and maintains for its users (Birk, 2011).

Darren Quick, Ben Martini, and Raymond Choo, authors of *Cloud Storage Forensics*, proposed what they named the Cloud Storage Forensic Framework (2014). They designed the framework to support the research they performed for their book. The framework consisted of seven steps:

1. *Commence*: identify the scope of the investigation and layout the requirements and limitations that constrain the investigation

2. *Preparation*: assemble the tools and team of experts to process the evidence
3. *Evidence source identification and preservation*: prepare for data collection
4. *Collection*: collect data and preserve, make clones of data to begin examination
5. *Examination and analysis*: Process clone of data to collect artifacts and document discoveries and analysis steps
6. *Presentation*: Prepare and present pertinent evidence discovered in support of investigation objectives
7. *Complete*: Review the results of investigation. (Quick, Martini, & Choo, 2014, p. 14)

They followed this process, including repeating steps two through five iteratively as necessary while performing their own extensive research in support of the book. The key ingredient offered in addition to usual forensic procedures, is number three, *Evidence source identification and preservation*. This is an important feature to the process as it is where the examiner considers where the data resides which they need to collect and thus Cloud based data is included since it needs special handling, according to the authors (Quick et al., 2014).

In the paper “Computer Forensics Field Triage Model” published in the *Journal of Digital Forensics, Security and Law*, the authors Marcus K. Rogers, James Goldman, Rick Mislán, Timothy Wedge, and Steve Debrotá suggested that an abridged forensics triage model is required in investigations. They based this model on the large volume of digital artifacts that need to be processed and a much shorter window of opportunity law enforcement has within which to act and execute on knowledge gathered from digital evidence (2006). They claimed that while there was an established “forensics field triage model” in use by law enforcement for tens of decades, it has only been the past decade or so that the model needed to be updated to allow

for the new challenges of digital evidence. When there is one piece of data in a single file on a HDD containing over a million files, an examiner would have to search through all the files to find the one they need, time may be very short to meet the urgency of an ongoing investigation (Rogers et al., 2006).

The authors proposed a few modifications to the traditional forensic triage model in an effort to make them more effective and allow the field agents a methodology to prioritize the evidence they collected. Thus, their methodology changes may streamline the effort enabling the investigators to get to the evidence they need most, sooner. Below is the bulleted list they provide listing the points the model changes:

1. Find evidence most applicable to investigation and of greatest utility
2. Identifies victims at most acute risk and under the greatest threat
3. Provide guidance and influence the investigation
4. Recognize legal charges that may be brought to bear in the developing case
5. Quickly and carefully, identify the suspect's threat level to society. (Rogers et al., 2006, p. 22)

The authors delved into the steps of the model and considerations for each step in light of the list of priorities to focus the investigation.

A Department of Justice paper titled "Forensic Examination of Digital Evidence: A Guide for Law Enforcement" provided a simple high-level framework that all investigations follow (Hart et al., 2004, p.2). The four common steps outlined in the guide included: Assessment, Acquisition, Examination, and Documenting and Reporting. The guide inserts an optional step ahead of these, Policy and Procedure Development. The guide placed it in the front in case there are law enforcement agencies that have not yet created policies and procedures

specifically for handling digital evidence. This reminds us that digital forensics is a constantly changing profession and in need of constant updates to keep abreast of technological advancements and changes in criminal activity.

### **Methodology**

Despite Google Chrome Operating System being three years old, there was virtually no research found that explores the forensic artifacts of the operating system running on Google Chrome based devices. Several books and papers looked at the artifacts stored in Cloud storage such as Google Drive, used by the Google Chrome Operating System to store user files. Like any other operating system, there are several types of data artifacts within the Google Chrome Operating System of interest to an investigator. Operating systems use file systems, roadmaps for an operating system to utilize files based upon how the files are stored on the HDD (Nelson, Phillips, & Stuart, 2010). Within a file system are many files, each with their own types and purpose. MS Windows operating systems use flat files and binary files. Flat files generally contain no special binary formatting and contain only text characters recognizable to the human reader like the letters and numbers in this paper (ComputerHope.com, 2014).

Binary files are specialized files made up of data that when viewed in a flat file editor, such as MS Windows Notepad, would make absolutely no sense to most users, as the characters displayed by the editor do not relate to actual use of data in the file itself (The Microsoft Windows Team, 2003). According to The Microsoft Windows Team, the MS Windows operating system files have many purposes (2003):

- Log files showing some computer activity
- Error trace files displaying data for troubleshooting computer problems

- Application executables for both the operating system and third party installed programs
- Configuration files for both applications and various parts of the operating system
- Application and operating system data files
- User files

Other operating systems such as Linux and Google Chrome Operating System are also composed of file systems containing flat files and binary files.

Dominik Birk provided in his paper some excellent points that a forensic examiner needs to be aware of in order to appreciate the challenges that Cloud computing based devices bring to the table in terms of evidentiary collection, analysis and some legal implications (2011).

Experienced examiners will note it aligns well with known forensic processing methodologies used by law enforcement in handling digital evidence in preparation for a prosecutor's casework (Hart et al., 2004, p. 3-4).

An investigator has many concerns when processing digital evidence. The primary concern they have above all else is that an unbroken chain of custody is maintained for the evidence collected (Sammons, 2012, p. 52). As part of maintaining chain of custody, examiners use clones of digital evidence for processing. The original evidence is safely stored to ensure it remains intact (Sammons, 2012, p. 52). The cloning process requires two parts according to John Sammons, author of the book *The Basics of Digital Forensics* (Sammons, 2012, p. 52). The first step is to use forensically clean media to store the clone. The second step is to make sure that even the clone created for processing remained unchanged by the processing to the extent possible. However, there are some technological limitations of concern to an investigation. Digital files, unlike physical paper files, contain additional data of use in an investigation called

metadata. Metadata can possess extra info like date and time of the file creation, software used to create it, and in the case of an image file created by a smart phone it may contain the GPS coordinates where they took the picture (Peterson, 2011). In some ways, a digital file is superior to physical paper files because of the larger forensic picture it enables an investigator to rebuild from the data (Bell & Boddington, 2010).

With flash storage, a category of storage to which SSDs belong, there are known limits to how many times a specific byte of data can be written to before it fails, which numbers in the tens of thousands of re-writes (Morgan, 2013). The firmware carefully designed to extend the SSD life, tries to use all available storage bytes equally in order to address this problem relating to the effective lifetime of an SSD (Morgan, 2013). These firmware enhancements include aggressive garbage collection that does not even require an operating system command to “trim” the space of data marked as deleted by the operating system. This garbage collection can occur simply by powering up the device by plugging it into a USB adapter to allow a forensic image capture of the drive space (Morgan, 2013). There are an increasing number of computers using SSD for storage like in Chromebooks, Apple Mac laptops and other tablet devices. Examiners have many tools to recover evidence from computer disks, even some data after deletion and or after reformatting the storage media, yet the SSDs introduce new challenges to the collection phase of an investigation.

An analyst may encounter three different types of storage spaces when working with devices (Altheide & Carvey, 2011, p. 45). The first is data space with usable data files. The second is slack space, which is space set aside logically within the file system for existing files and is unused by the files contents (Hoog 2008, Slack Space). Computers allocate storage in blocks of 512 bytes (Hoog, 2008, Slack Space). When a file created which is 873 bytes in size,

the operating system reserves 1024 bytes in the storage device in total leaving 151 bytes unused by the file. The 151 unused bytes is slack space for the file allocated from space that may have previously been storage for older data. These 151 bytes may actually contain data from that previous file. AccessData's Forensic Toolkit is one of many tools that can carve out the data from file slack space. The third portion of the storage device space not used by existing files and their slack space is unallocated storage (Hoog, 2008, Unallocated Space). The process in a nutshell: space reserved for files deleted by the operating system is freed up, noted by the operating as unallocated space, and used for new data storage. Slack space and unallocated space may still have the data on it from the files that the operating system had deleted (Altheide & Carvey, 2011, p. 56). In reality the data is usually left in place and the operating system merely remove a reservation for the space so it is available for new data later (Altheide & Carvey, 2011, p. 56).

With SSDs, as soon as something is deleted from a drive, the unallocated space is at risk of being overwritten and anything that was in that space becoming forensically useless is very high (Howell, 2011). An examiner often finds the most incriminating evidence carved out of slack and unallocated space and restored for examination using the specialized tools in the examiners toolbox (Spenneberg, 2008). Do to the aggressiveness of SSD firmware in reclaiming unallocated storage, the bulk of evidence that is useful to an examiner will ultimately be the remaining files on the storage drive. Since nearly all devices, which use Google Chrome Operating System, also have inexpensive and small SSDs inside of them, this is a critical risk factor in the research completed for this paper. Data on a live computer system that remains in active memory can contain crucial evidence such as unencrypted remote data and credentials for accessing other devices services in the Cloud, which will be unavailable on the storage devices

when the system is cold. Special care is required to collect live data if a reliable method is available for the device.

Encryption is the tallest technical hurdle to any forensic analyst tasked with evaluating a Chromebook. According to Fang et al., Google Chrome Operating System uses encryption in over 10 different functions of the system in order to maintain the integrity of the operating system and user data. Google Chromebook, according to Fang et al. uses encryption to protect the firmware by verifying the system at boot time to verify it has not become corrupt since last boot. The system notifies the user if the firmware fails, then the system restores to a locally stored, encrypted, and read-only version. Furthermore, the Operating System verification process occurs as it boots to ensure that any updates to the Operating System are valid and if not, the last known good copy of the operating system is booted. In their conclusion, they state trivial changes to this very secure operating system to make it even more so with limited usability changes. It is clear from their analysis that “the basic design is secure” as they claim.

Sean Gallagher of Ars Technica made the argument that because so much of the data generated by a user of Chromebooks stores in the Cloud, that the National Security Agency (NSA) and other government agencies would love the rollout of more Chromebooks into consumer hands (Gallagher, 2013). While data kept on a local HDD requires physical access to the HDD, data stored in the Cloud can be accessible from anywhere and is subject to forensic tools run remotely. This is a factor in the understanding of the artifacts under examination in this paper.

Increasingly, computer users prefer cloud storage to store their data in one place on the Internet so they can access it from many devices (Fournier, 2014). An example would be a student working on a paper for their college course saves the MS Word file in their Google Drive



account, along with other materials used in the writing process. Using this method, they may access the materials from their home desktop computer, the college computer lab, from the tablet computer they used for taking notes in class, and even from their Android based cell phone so they can proofread it while waiting in line at the grocery store. Devices using Google Chrome Operating System connect to Google Drive by default and provide this convenience easily and effectively.

For the purposes of Law Enforcement and to align with best practices, forensic examiners should follow all legally recognized means to access, acquire, store and analyze all forensic evidence retrieved from remote (Cloud) systems. One paper to reference is “Computer Forensics Field Triage Process Model” (Rogers et al., 2006). Two key aspects of the Computer Forensics Field Triage Process Model (CFFTPM) is that it considers the volatility of the data into the processing while being careful to maintain the chain of custody of all collected and analyzed data. This research methodology followed the suggested framework from *Cloud Storage Forensics* (Quick et al., 2014).

## **Setup**

The lab space for this investigation required specific hardware and software be set up. According to the National Institute of Justice, it is important to document not only the software but also the hardware an investigator uses to collect, store, and analyze forensic evidence during an investigation (Hart et al., 2004).

## **Hardware**

Several pieces of hardware were required to perform this examination into Google Chrome Operating System artifacts. In some cases, the hardware may be crucial as some hardware have special handling requirements forensically and may in fact later be determined to

have weaknesses in design that impacts any investigations which may have been performed on or with the devices.

**ZTC 2-in-1 Thunder Board M.2 (NGFF) Board Adapter.** The ZTC 2-in-1 board was required in order to be able to connect the Chromebook's SSD to the examination laptop to collect an image using Forensic Toolkit (FTK) Imager. This board essentially makes the small SSD drive fit into a typical SATA III socket.

**Patouxun USB 2.0 to SATA Converter Adapter Cable.** This connected the ZTC 2-in-1 Thunder board into a USB slot on the examination laptop. When connecting the SSD removed from the Chromebook, the SSD appeared to Windows 7 to be an external USB HDD allowing the content capture by forensics imaging software.

**Acer c720 Chromebook.** An Acer c720 Chromebook was the test-bed examined. The c720 technical specifications are below (Acer.com, 2013).

- Intel Celeron 2955U 1.4 GHz (2MB Cache) CPU
- Chrome Operating System update 30
- 2 GB DDR3L SDRAM memory
- 32 GB SSD (Serial ATA)
- 12-inch screen, Intel HD graphics, HDMI output
- Built-in 802.11bgn wireless adapter

**Dell Inspiron 15 7000 Series Model 7537 Touchscreen.** The Inspiron laptop is the examination laptop used to process all data and compose this paper. The basic technical specifications are below (Dell.com, 2014).

- 15" Touchscreen laptop
- Intel i7 1.9GHz CPU (4M cache)

- 16 GB DDR3L 1600 MHz memory
- Built-in 802.11 ac dual band wireless + Bluetooth
- Windows 8.1

## **Software**

As with any other forensics effort, there are hundreds of software choices in order to perform the requisite steps of acquiring, analyzing and presenting the results of a forensics investigation. Function and cost determined the software used for this investigation, with free software winning out over software with a license whenever possible.

**Microsoft Word Professional 2010.** The examiner already owned a license of MS Office 2010, installed for related coursework, and Word used to compose this paper (Microsoft Word, 2013).

**VMWare Workstation 10.0.3 – build 1895310.** For the section below using VMs, VMWare workstation was used as it was already available on the examination laptop from previous efforts and provided free of charge for educational purposes by Utica College to students for the term of their degree of study at Utica College (VMware Workstation 10.0, 2014).

**Microsoft Windows XP Professional SP 3.** This is the version of Windows installed into the VM used for acquiring and processing the data on the SSD as well as to log into the Google Gmail account using the installed Google Chrome Browser (Windows XP, 2014).

**Google Chrome browser version 38.0.2125.111 m.** This is the Google Chrome browser installed into the Windows XP VM and used to connect to the Gmail account under examination for browser artifacts later in this paper (Google Chrome Browser, 2014).

**Google Chrome Operating System v38.** This is the version of the Google Chrome Operating System running on the Acer c720 Chromebook used in this examination (Chromebook Help Center, 2014).

**AccessData FTK Imager 3.1.0.1514.** This is the software used to acquire the image of the SSD removed from the Chromebook (FTK Imager, 2014).

**AccessData Forensic Toolkit 1.81.6.** This is the Forensic Toolkit used to carve out the contents of the image file captured from the SSD and later to process logical copy of user files copied off Chromebook in Crosh shell onto external HDD (FTK, 2014).

**ChromeAnalysis Plus 1.4.1 Trial for Windows.** This tool was used within the Windows XP VM to process the Chrome browser to identify the artifacts of the Chrome Browser running on Windows provides when it is logged into the test subjects Gmail account. (Foxton Software, 2014)

**Google Gmail Account.** In order to perform the investigation, a Google Gmail account was required to seed an account in order to analyze it and identify the artifacts found in the Chromebook data files.

## **Evaluation Foundation**

The Acer c720 is in Developer Mode and a Gmail account created for the fictitious email *jacobmarley199@gmail.com*. Some data was generated, files downloaded to Google Drive and bookmarks created along with a brief browsing and search history. In preparation for analysis: a drive image was captured from the Acer c720 SSD, a Windows XP VM was created and Chrome Browser installed, user files were logically copied from Crosh to an external USB HDD and *dd* was run to capture the SSD contents from Crosh onto the external USB HDD.

## **Analysis**

In the course of performing an analysis, the forensic examiner chooses from a variety of options to process the collected devices and data. The devices are varying states, which include but are not limited to a shutdown state, Standby or Hibernate mode, or powered up and running. When considering what has been revealed about the heavy use of encryption and Cloud centric use of data for Chromebooks, this paper introduced analysis from least revealing to most revealing as discovered during processing of an Acer Chromebook C720 (16 GB). The examination started with an Image of the SSD captured and processed using the AccessData Forensic Toolkit, then a VM was used to login to the Gmail account. An installed Chrome browser and ChromeAnalysis Plus Trial were used as processing tools to cull out browser artifacts of interest to an investigation. Finally, the Chromebook was explored in Developer Mode to discover artifacts with full access provided to the device. A logical copy of a full disk using both *rsync* and *cp* resulted in a failed process and files copied to the storage drive with problems the host operating system was unable to handle. The final step was the logical copy of the contents in the chrome *user* directory to the storage drive for analysis using AccessData Forensic Toolkit and ChromeAnalysis Plus Trial.

## **Commence**

The examiner started by pulling the SSD from the Ace C720 16GB Chromebook, connected it to a USB adapter mounted with USB set to Read Only via Windows registry settings. The drive was imaged using AccessData FTK Imager 3.1.0.1514 to capture the contents of the SSD and was processed with the AccessData Forensic Toolkit version 1.81.6 to carve any recognizable artifacts within the Image file. The second part used a Windows XP VM with Chrome browser installed and the Gmail account logged into in order to run browser analysis on

the data that is synched by Chrome browser. Finally, the Chromebook itself was logged into using the ID and password from the previous section and the drive contents were manually explored to identify any additional artifacts present while a user logged into a Chromebook connected to an active Gmail account.

## **Preparation**

In order to begin, create a Windows XP VM and the latest Chrome browser installed along with FTK Imager and the Forensic Toolkit. An empty 16GB USB drive will hold screen captures from the Chromebook device and used to show discovered data in the last phase of this exploration of Chrome Operating System and its artifacts. The Chromebook itself was also prepared by placing it in Developer Mode to enhance the available functions on the device during the final manual phase of the examination and Ubuntu installed using Crouton.

## **Evidence Source Identification and Preservation**

Google Chrome Operating System utilizes the Google provided Cloud via its Google Drive function. This indicates an early need to capture Cloud data as quickly as possible during any forensics investigation considered most volatile; then capture an image from the SSD.

## **Collection**

After carefully removing the SSD from the Acer C720 Chromebook, it was connected to a Thunderboard manufactured by ZTC designed to receive SSDs such as this one and plug into a SATA port replicator. To make all USB drives read-only, this *RegEdit* instruction was entered in the registry of the VM's operating system:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies]
```

```
"WriteProtect"=dword:00000001
```

AccessData FTK Imager was run from the VM to collect an image from the SSD drive. The image was imported into AccessData Forensic Toolkit to process and carve out recognizable artifacts from the image. After a snapshot was taken of the VM, the installed Chrome browser was executed and the user ID and password were used to login to the Gmail account. The Google Drive directory was copied into a directory on the VM alongside the SSD image file. The ChromeAnalysis application was run to process the Chrome browser installation and all associated files and embedded data. Finally, the examiner carefully replaced the SSD in the Acer C720 Chromebook and booted up the device. Using the same user ID and password from the Chrome browser login to access the Chromebook, the examiner connected the blank 16GB USB drive to hold any screen captures generated during manual examination of the device.

### **Examination and Analysis**

Seven different approaches to the data collection were used. Each of the approaches covered accessing the data from a different direction to examine similarities and differences of importance to a forensic examiner.

### **Artifacts of Google Chrome Operating System from SSD Image Capture**

AccessData Forensic Toolkit provided an in depth view into the contents of the data stored onto the SSD. It included space for the Unified Extensible Firmware Interface used to replace BIOS in newer systems that handles basic device control to enable booting up an operating system. The Forensic Toolkit carved out 647 data objects in the image as exhibited in Figure 1.

Evidence Items		File Status		File Category	
Evidence Items:	13	KFF Alert Files:	0	Documents:	0
<b>File Items</b>		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	647	Bad Extension:	2	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	0
Unchecked Items:	647	From E-mail:	0	Multimedia:	0
Flagged Thumbnails:	0	Deleted Files:	1	E-mail Messages:	0
Other Thumbnails:	0	From Recycle Bin:	0	Executables:	2
Filtered In:	647	Duplicate Items:	6	Archives:	0
Filtered Out:	0	OLE Subitems:	0	Folders:	4
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	630
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	0
		Data Carved Files:	0	Unknown Type:	11

Figure 1. FTK Object table of captured image after carving.

Note the processing carved out 13 areas from the drive space with each consisting of varying contents. Figure 2 shows the labels provided by the file-carving tool culled from the file system objects, and offered a tree view structure of what each of those spaces contained.

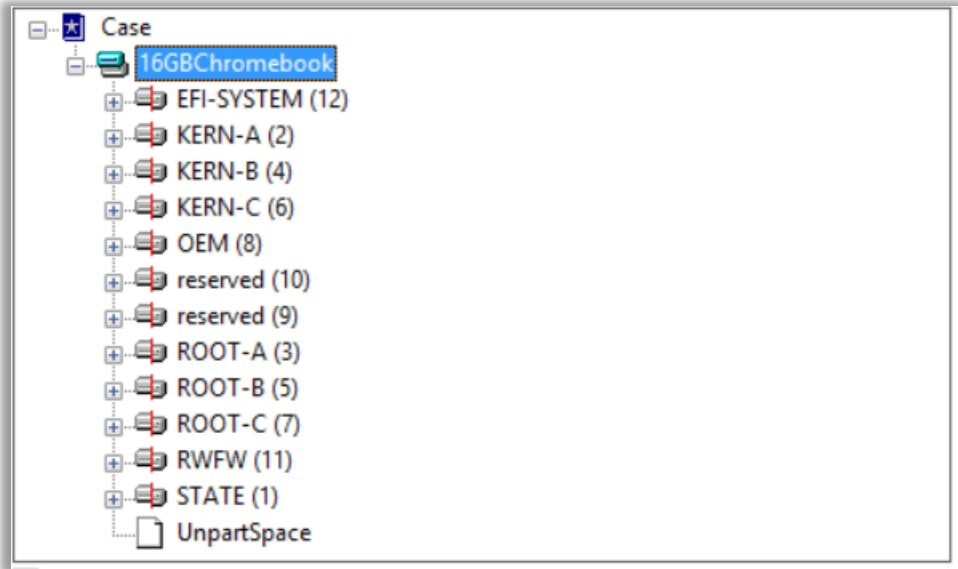


Figure 2. Thirteen areas carved from SSD space

Referring to the paper by Fang et al., the three KERN (Kernels), three ROOT (roots A, B and C), RFW (Read/Write Firmware), and EFI-SYSTEM (UEFI and boot loader) are objects



expected in this discovery. Within the EFI-SYSTEM object group, there were 12 contained artifacts. FTK displayed them in tree as shown in Figure 3.

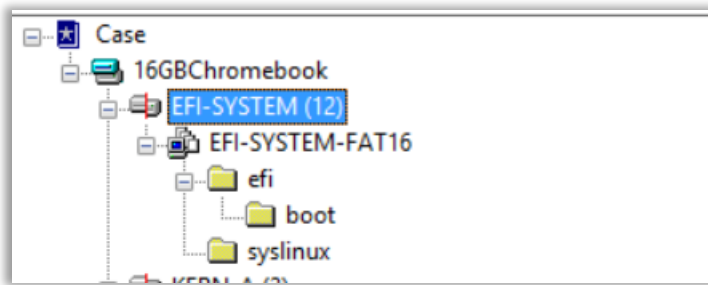


Figure 3. EFI-SYSTEM object group from data carve.

AccessData's Forensic Toolkit revealed the UEFI sector was a FAT16 file system, using *Syslinux* and *Grub* for its boot loader as shown in Figure 4.

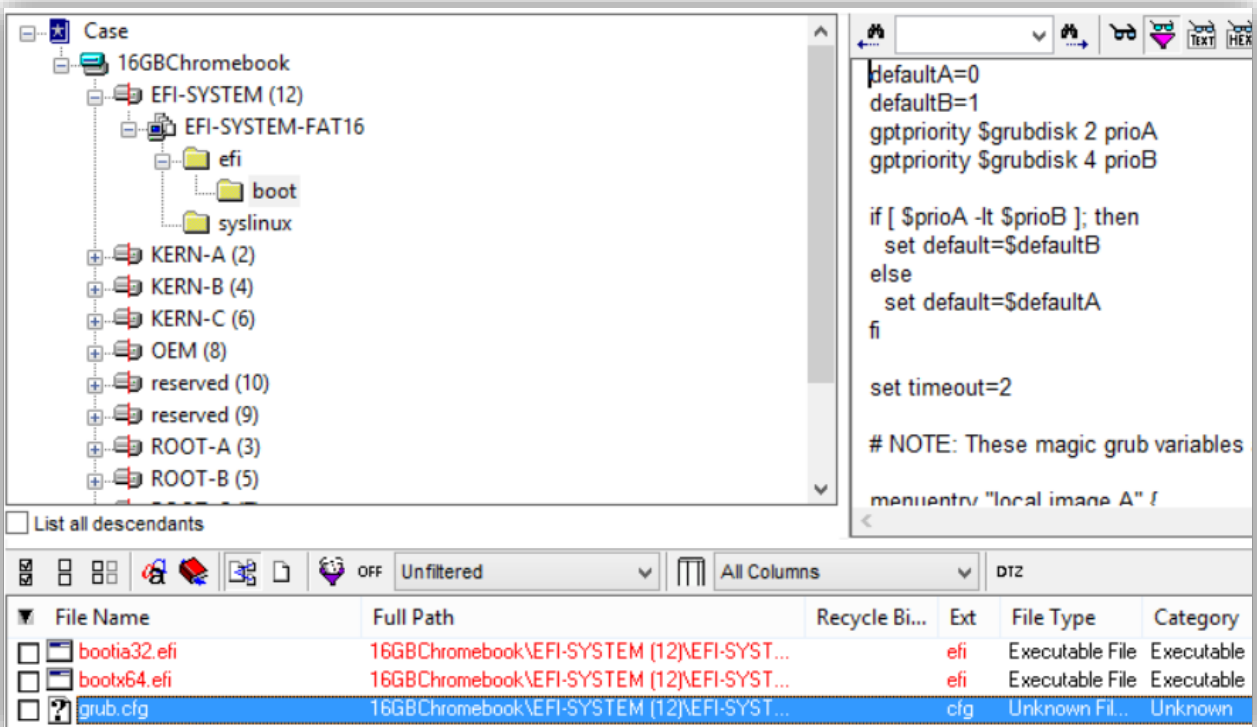


Figure 4. Grub in boot sector.

Browsing the Hex contents of each of the other twelve carved object groups in FTK revealed that KERN-C, OEM, reserved (10) and reserved (9), ROOT-C, and RFW each filled

with all 00 values. While the others had portions of mixed Hex values revealing binary executables and files that used compression and encryption, these sections were very clearly just unused storage space at the time of the Image capture. These were sections allocated for use, but did not provide useful artifacts. Fang et al. explained how two versions of the operating system were maintained on the system as part of ensuring the system could boot even in the event of a failed operating system upgrade. The objects carved out from the image support that design. Considering further the paper, it is clear that the User area of the Chromebook SSD artifacts found inside the object group named STATE in Figure 5.

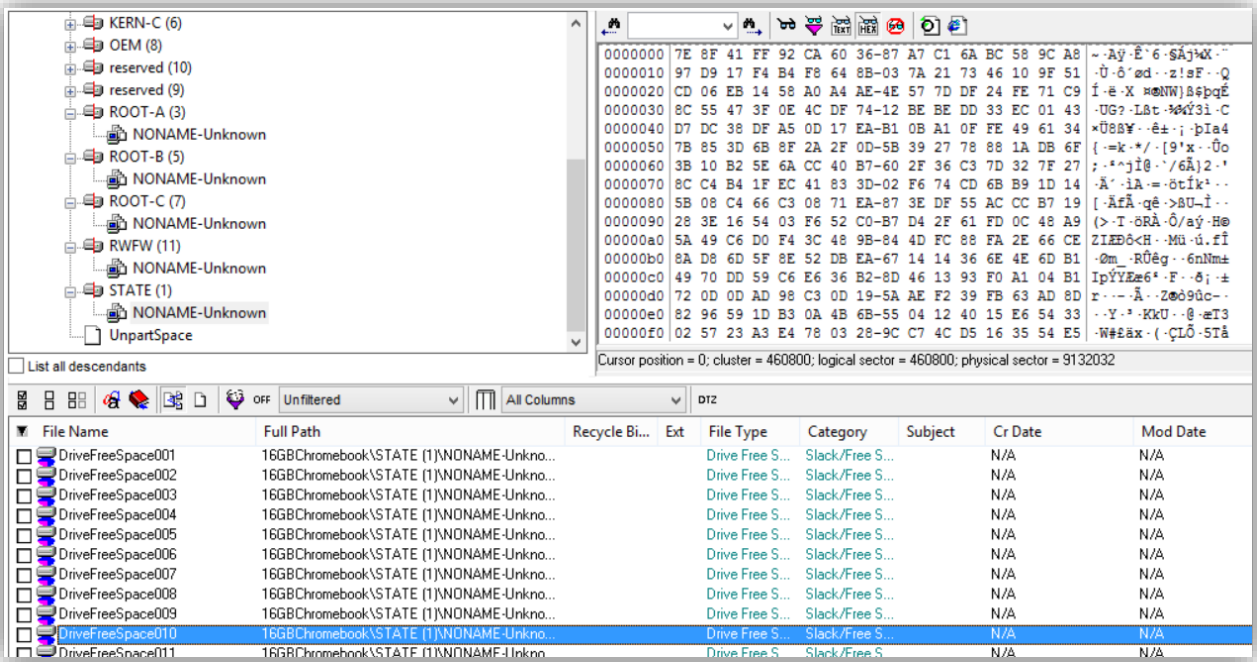


Figure 5. FTK showing User work of SSD Image named STATE

In the early space of this block of the SSD, was some plain text content supporting the view that the STATE part of the drive is the User space as shown in Figure 6.

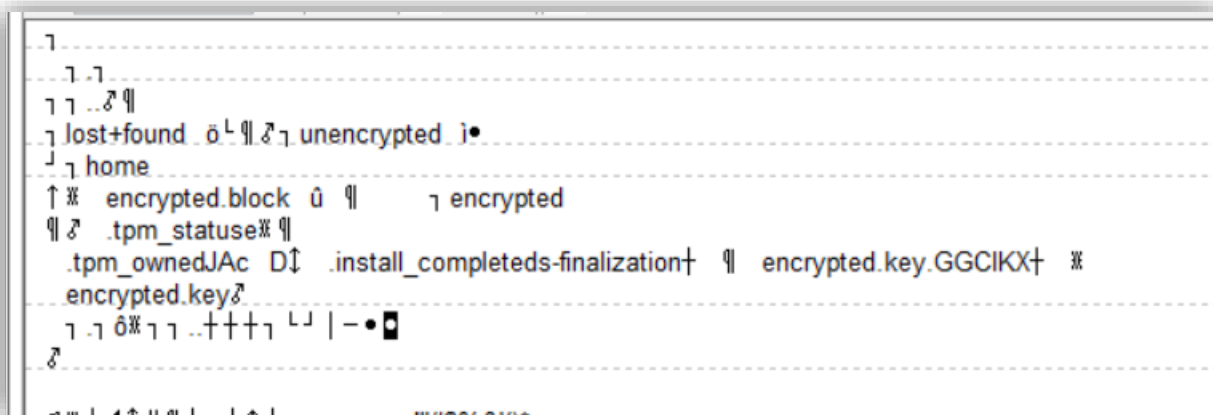
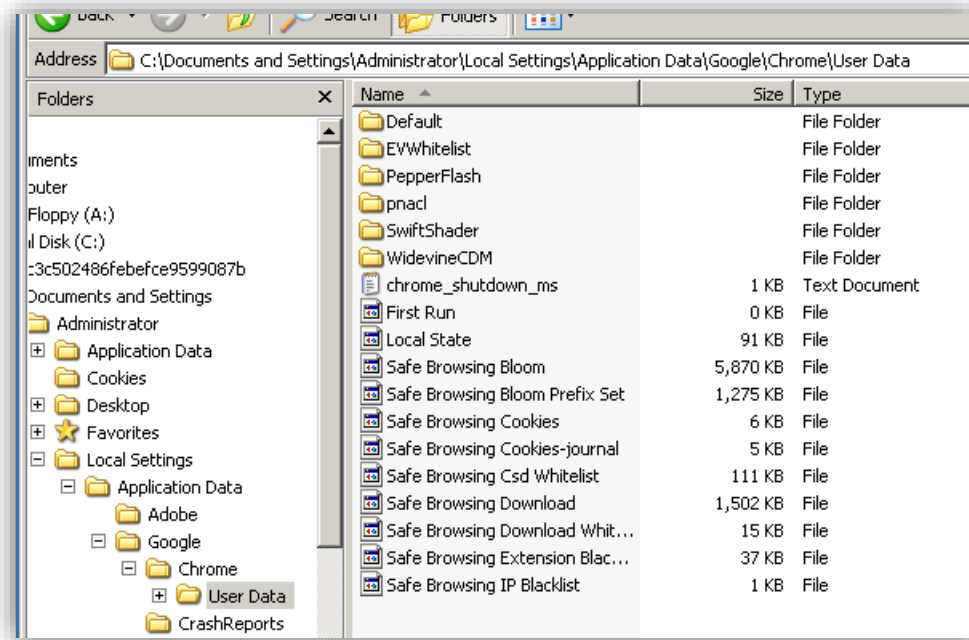


Figure 6. Start of User space.

After completing the manual viewing through all the carved out portions of the Chromebook SSD image, the examiner found no further useful artifacts.

### Artifacts of Google Chrome Browser in Windows XP VM While Logged In

The examiner used up a Windows XP VM with the latest version of the Google Chrome browser installed on it. The approach was to use the VM to log in to the Gmail account and run software to scan for user data to determine what artifacts may exist while logged in. This shall reveal any data produced while a Chromebook connected to an active Gmail account is subsequently stored in Google's Cloud. It was also to determine artifacts when logged into the account from other devices. This is the first portion of the examination that actually revealed real user data compared later with the manual walkthrough on the Chromebook itself. The examiner used ChromeAnalysis Plus Trial to parse the Chrome artifacts inside the Windows XP VM. Figure 7 and 8 present the user's Chrome directory contents and the activity using Google Chrome browser functions respectively.



**Figure 7.** User directory containing Chrome files.

ID	From Visit	Date Visited (UTC -5, DST Enabled)	URL	Total Visit Count	ChromeAnalysis Total Visit Count	Title
6	5	11/9/2014 2:19:27 PM	https://www.google.com/intl/en-US/chrome/blank.html?source=0%3...	1	1	
5	4	11/9/2014 2:19:27 PM	https://accounts.youtube.com/accounts/SetSID?ssdc=1&ssid=ALWU...	1	1	
4	3	11/9/2014 2:19:27 PM	https://accounts.google.com/CheckCookie?hl=en-US&srp=1&check...	1	1	
3	0	11/9/2014 2:19:27 PM	https://accounts.google.com/ServiceLoginAuth	1	1	
2	1	11/9/2014 2:19:00 PM	https://www.google.com/intl/en/chrome/browser/welcome.html	1	1	Getting Started
1	0	11/9/2014 2:19:00 PM	http://tools.google.com/chrome/intl/en/welcome.html	1	1	Getting Started
15	0	11/9/2014 1:16:49 PM	https://www.google.com/	4	4	Google
11	0	11/9/2014 1:15:59 PM	http://www.amazon.com/	1	1	Amazon.com: Online Shopping for Electronics, ...
14	0	11/2/2014 9:48:57 PM	https://www.google.com/	4	4	Google
8	0	11/2/2014 9:48:31 PM	http://baiff.py/	2	2	
7	0	11/2/2014 9:48:19 PM	http://baiff.py/	2	2	
13	0	11/2/2014 9:20:23 PM	https://www.google.com/	4	4	Google
10	0	10/13/2014 3:38:19 PM	http://www.omgchrome.com/meet-the-new-chrome-os-recovery-utility	2	2	Hands On With The New Chrome OS Recover...
16	0	10/13/2014 3:18:00 PM	http://maps.google.com/	1	1	Google Maps
12	0	10/13/2014 3:16:57 PM	https://www.google.com/	4	4	Google
9	0	10/13/2014 2:47:04 PM	http://www.omgchrome.com/meet-the-new-chrome-os-recovery-utility	2	2	Hands On With The New Chrome OS Recover...

**Figure 8.** Website History from Google account.

Google Chrome browser provides the user history so they can quickly find a website they may have forgotten to create a bookmark for returning or else did not make it before realizing they probably should have for later revisit. Note Google Maps, a page of Chromebook backup utility instructions and some YouTube links are included in the listing. As shown in Figure 9, only a handful of bookmarks were discovered. These bookmarks may be significant to the

investigation, as they are clearly sites the user wishes to be able to return to in the future since the user bookmarked them.

ID	Date Added (UTC -5, DST Enabled)	URL	Title	Type
5	11/9/2014 1:16:36 PM	http://www.amazon.com/10Pcs-Memory-Storage-Swivel-Design/dp/B00DZ2KY...	Amazon.com: MECO(TM) 10Pcs 8GB 8G USB 2.0 Fl...	url
6	11/9/2014 1:17:17 PM	http://lifehacker.com/5935863/five-best-vpn-service-providers	Five Best VPN Service Providers	url
7	11/9/2014 1:17:33 PM	https://www.privateinternetaccess.com/	Anonymous VPN Service From The Leaders   Privat...	url
8	11/9/2014 1:23:16 PM	http://www.cnet.com/how-to/how-to-run-both-chrome-os-and-ubuntu-on-a-chrom...	How to run both Chrome OS and Ubuntu on a Chro...	url
9	11/9/2014 1:18:10 PM	chrome-extension://nkocclplnhpfrfajcilkommmlplhnl/html/crosh.html	chronos@localhost:~/Downloads	url
10	11/9/2014 1:14:39 PM	http://www.backyardchickens.com/atype/2/Coops	Coop Designs	url

Figure 9. Bookmarks stored in Google account.

While cookies are less interesting than the Uniform Resource Locator (URL) of websites, advertisements create many kinds of cookies. Some may be useful as they may be part of websites that the user logs into regularly and provide additional information for investigators to collect additional artifacts in support of a forensic investigation. Figure 10 displays many of the cookies preserved in the Google account used by all browsers logged into the user account.

Host	Path	Created (UTC -5, DST Enabled)	Last Accessed (UTC -5, DST Enabled)	Name	Expiry (UTC -5, DST Enabled)	Is Secure	Is HTTP Only	Value
.doubleclick.net	/	11/9/2014 2:19:41 PM	11/9/2014 2:19:41 PM	test_cookie	11/9/2014 2:34:41 PM	No	No	
.doubleclick.net	/	11/9/2014 2:19:41 PM	11/9/2014 2:19:41 PM	__dt__	11/10/2014 2:19:41 PM	No	Yes	
accounts.google.com	/	11/9/2014 2:19:40 PM	11/9/2014 2:19:40 PM	LSID	11/8/2016 2:19:40 PM	Yes	Yes	
accounts.google.com	/	11/9/2014 2:19:40 PM	11/9/2014 2:19:40 PM	GAPS	11/8/2016 2:19:40 PM	Yes	Yes	
.google.com	/	11/9/2014 2:19:33 PM	11/9/2014 2:19:33 PM	PREF	11/8/2016 2:19:33 PM	No	No	
.google.com	/	11/9/2014 2:19:32 PM	11/9/2014 2:19:32 PM	NID	5/11/2015 3:19:32 PM	No	Yes	
accounts.google.com	/	11/9/2014 2:19:32 PM	11/9/2014 2:19:32 PM	ACCOUNT_CHOOSER	11/8/2016 2:19:32 PM	Yes	Yes	
.google.com	/	11/9/2014 2:19:32 PM	11/9/2014 2:19:32 PM	SAPISID	11/8/2016 2:19:32 PM	Yes	No	
.google.com	/	11/9/2014 2:19:32 PM	11/9/2014 2:19:32 PM	APISID	11/8/2016 2:19:32 PM	No	No	
.google.com	/	11/9/2014 2:19:32 PM	11/9/2014 2:19:32 PM	SSID	11/8/2016 2:19:32 PM	Yes	Yes	
.google.com	/	11/9/2014 2:19:32 PM	11/9/2014 2:19:32 PM	HSID	11/8/2016 2:19:32 PM	No	Yes	
.google.com	/	11/9/2014 2:19:32 PM	11/9/2014 2:19:32 PM	SID	11/8/2016 2:19:32 PM	No	No	
.google.com	/intl/en/chrome/...	11/9/2014 2:19:06 PM	11/9/2014 2:19:06 PM	__utmz	5/11/2015 3:19:06 AM	No	No	
.google.com	/intl/en/chrome/...	11/9/2014 2:19:06 PM	11/9/2014 2:19:06 PM	__utmb	11/9/2014 2:49:06 PM	No	No	
.google.com	/intl/en/chrome/...	11/9/2014 2:19:06 PM	11/9/2014 2:19:06 PM	__utma	11/8/2016 2:19:06 PM	No	No	
.google.com	/intl/en/chrome/...	11/9/2014 2:19:06 PM	11/9/2014 2:19:06 PM	__utmt	11/9/2014 2:29:06 PM	No	No	
.youtube.com	/	11/9/2014 2:19:02 PM	11/9/2014 2:19:02 PM	VISITOR_INFO_LIVE	7/11/2015 3:12:02 AM	No	No	

Figure 10. Cookies from Google account.

Figure 11 shows the download history associated with the local Chrome browser and reveals nothing from the Google account logged into by the examiner. This will be a notable place to look during the manual walkthrough in the next section.

ID	URL	Full Path	Start Time (UTC -5, DST Enabled)	State	Bytes Downloaded	Total Bytes

Figure 11. Empty download history from Google Account.

Search history is also associated with the local browser install and is thus empty as Figure 12 shows. Note that in the History section, there were Google website searches included. This is also a place to look closely at during the manual walkthrough in the next section.

Term	URL	Last Visit Time (UTC -5, DST Enabled)

Figure 12. Empty Search history.

The login history panel is for use of the local browser to reveal a user logging in remotely to server accounts and is empty as shown in Figure 13. This will be looked closer in the manual walkthrough in the next section.

Origin URL	Action URL	Username Field	Password Field	Username	Sign On Realm	Date Created (UTC -5, DST Enabled)

Figure 13. Empty Login History for remote accounts.

The Google Chrome browser notes websites visited frequently and provides some possible insight as to user tendencies. Figure 14 shows the two most visited websites by the user of this Gmail account.

URL Rank	URL	Title	Redirects	Last Updated (UTC -5, DST Enabled)
0	<a href="http://www.google.com/chrome/intl/en/welcome.html">http://www.google.com/chrome/intl/en/welcome.html</a>	Welcome to Google Chrome	<a href="http://www.google.com/chrome/n...">http://www.google.com/chrome/n...</a>	11/9/2014 2:18:52 PM
1	<a href="https://chrome.google.com/webstore?hl=en">https://chrome.google.com/webstore?hl=en</a>	Chrome Web Store	<a href="https://chrome.google.com/websto...">https://chrome.google.com/websto...</a>	11/9/2014 2:18:53 PM

Figure 14. Most visited website list.

These was a listing of the web-icons used for the websites bookmarked in the browser.

The data in Figure 15 is notable as a function of the tool used, yet it is of limited forensic value in this investigation.

ID	Image	URL	Page URL	Last Updated (UTC -5, DST Enabled)
8		https://www.google.com/favicon.ico	https://www.google.com/_/chrome/newtab?espy=2&ie=UTF-8	11/9/2014 2:19:37 PM
6		http://www.cnet.com/favicon.ico	http://www.cnet.com/how-to/how-to-run-both-chrome-os-and-ubuntu...	11/9/2014 2:19:35 PM
7		http://www.backyardchickens.com/custom/huddle/backyardchicken...	http://www.backyardchickens.com/atype/2/Coops	11/9/2014 2:19:35 PM
5		https://www.privateinternetaccess.com/favicon.ico	https://www.privateinternetaccess.com/	11/9/2014 2:19:35 PM
4		http://i.kinja-img.com/gawker-media/image/upload/s-rqDhe7s2-/c_fil...	http://lifehacker.com/5935863/five-best-vpn-service-providers	11/9/2014 2:19:35 PM
3		http://www.amazon.com/favicon.ico	http://www.amazon.com/10Pcs-Memory-Storage-Swivel-Design/dp/B...	11/9/2014 2:19:35 PM
1		https://www.google.com/images/icons/product/chrome-32.png	http://tools.google.com/chrome/intl/en/welcome.html	11/9/2014 2:19:11 PM
2		https://www.google.com/images/icons/product/chrome-32.png	https://www.google.com/intl/en/chrome/browser/welcome.html	11/9/2014 2:19:11 PM

Figure 15. Icons from websites in favorites (bookmarks).

The user had not locally used the archive function of the Google Chrome browser and Figure 16 shows it empty.

ID	From Visit	Date Visited (UTC -5, DST Enabled)	URL	Total Visit Count	ChromeAnalysis Total Visit Count	Title

Figure 16. Archived webpages unused.

Figure 17 lists some of the files in the browser cache. This listing is perhaps the most interesting artifacts from the browser. It is also the most densely populated of the types of data that the ChromeAnalysis tool carved out of the local install of the Google Chrome browser. The local directory of the browser cache in this case was:

*C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\User Data\Default\Cache*

Filename	Content Type	URL	File Size (Bytes)	Last Fetched (UTC-5, DST Enabled)
si?p=CAE&ut=AFAXlQAAAAVF_Bzz4ZK7zk;ISCjtVwdjKh...		https://googleads.g.doubleclick.net/pagead/dt/si?p=CAE...	43	11/9/2014 2:19:41 PM
si%3Fp%3DCAE%26u%3DAFAKxIQAAAAVF_Bzz4ZK7zki...		https://accounts.google.com/ServiceLogin?service=doritos...	0	11/9/2014 2:19:40 PM
ui?ogt=1		https://www.google.com/pagead/dt/ui?ogt=1	0	11/9/2014 2:19:39 PM
en-us-3-0.bdic?cms_redirect=yes&expire=1415575176&ip=6...	application/octet-stream	http://t5--sn-vgqs7n7k.c.pack.google.com/edged/chrome...	440949	11/9/2014 2:19:39 PM
ne?di=%5B%2220140509-01%22%2Cnull%2C0%5D		https://clients5.google.com/pagead/dt/ne?di=%5B%2220...	82	11/9/2014 2:19:39 PM
dn.js		https://clients5.google.com/pagead/dt/dn/dn.js	11445	11/9/2014 2:19:38 PM
https://clients5.google.com/pagead/dt/dn/		https://clients5.google.com/pagead/dt/dn/	132	11/9/2014 2:19:37 PM
cb=gapi.loaded_0		https://apis.google.com/_/scs/abc-static/_/is/k=gapi.gapi...	48911	11/9/2014 2:19:37 PM
favicon.ico		https://www.google.com/favicon.ico	982	11/9/2014 2:19:37 PM
gen_204?v=3&s=newtab&atyp=csi&e=3300102,3300133,33...		https://www.google.com/gen_204?v=3&s=newtab&atyp=c...	0	11/9/2014 2:19:36 PM
light-sprite.png		https://www.google.com/logos/2014/simplevideo/light-sprit...	5257	11/9/2014 2:19:36 PM
25th-anniversary-of-the-fall-of-the-berlin-wall-508461979166...		https://www.google.com/logos/doodles/2014/25th-anniver...	34256	11/9/2014 2:19:36 PM
simplevideo14.2.js		https://www.google.com/logos/2014/simplevideo/simplelevi...	12506	11/9/2014 2:19:36 PM
25th-anniversary-of-the-fall-of-the-berlin-wall-508461979166...		https://www.google.com/logos/doodles/2014/25th-anniver...	1770	11/9/2014 2:19:36 PM
rs=AllRSTPsh2aivyEVcV60bQjav6n7GauUQ		https://www.gstatic.com/og/_/is/k=og.og.en_US.tHgmGA...	58678	11/9/2014 2:19:36 PM
en-us-3-0.bdic	text/html	http://cache.pack.google.com/edged/chrome/dict/en-us-...	0	11/9/2014 2:19:36 PM
v1_fd3cfc85.png		https://ssl.gstatic.com/gb/images/v1_fd3cfc85.png	53091	11/9/2014 2:19:36 PM
manifest?espv=2&ie=UTF-8		https://www.google.com/_/chrome/newtab/manifest?espv...	222	11/9/2014 2:19:35 PM
classic_plus_sprite.png		https://www.google.com/images/srpi/classic_plus_sprite.png	42803	11/9/2014 2:19:35 PM
newtab?espv=2&ie=UTF-8		https://www.google.com/_/chrome/newtab?espv=2&ie=U...	12126	11/9/2014 2:19:35 PM
newtab?async=xid:1_fmjson&espv=2&yv=1		https://www.google.com/async/newtab?async=xid:1_fmjt...	71261	11/9/2014 2:19:35 PM
gen_204?v=3&s=newtab&ei=Rb5VPjFJcepyATf7YClCQ&e...		https://www.google.com/gen_204?v=3&s=newtab&ei=Rb5...	0	11/9/2014 2:19:35 PM
gen_204?v=3&s=newtab&atyp=csi&e=3300102,3300133,33...		https://www.google.com/gen_204?v=3&s=newtab&atyp=c...	0	11/9/2014 2:19:35 PM
rs=ACT90fC1IH6VJBraqqYUEpoKDa1gm8xbA		https://www.google.com/xjs/_/js/k=xjs.ntp.en_US.hv_hzd...	49825	11/9/2014 2:19:34 PM
rs=ACT90fC1IH6VJBraqqYUEpoKDa1gm8xbA		https://www.google.com/xjs/_/js/k=xjs.ntp.en_US.hv_hzd...	13395	11/9/2014 2:19:34 PM

Figure 17. First 25 from cache.

## Artifacts of Google Chrome Operating System in Developer Mode

During a forensic investigation sometimes an examiner needs to log into the suspects device and try to capture whatever data they can manually as the device may not provide another means to capture it without logging into it. This section covers a manual walkthrough to reveal discovered forensic artifacts on the Acer c720 Chromebook. These next Figures reveal what is on the Chromebook using the Chrome browser running on it. Figure 18 displays the directory contents for the logged in user's home directory. The data displayed in the browser in the following Figures of this section comes from this directory of the Chromebook synchronized with Google when the account logged into the Google Gmail server.



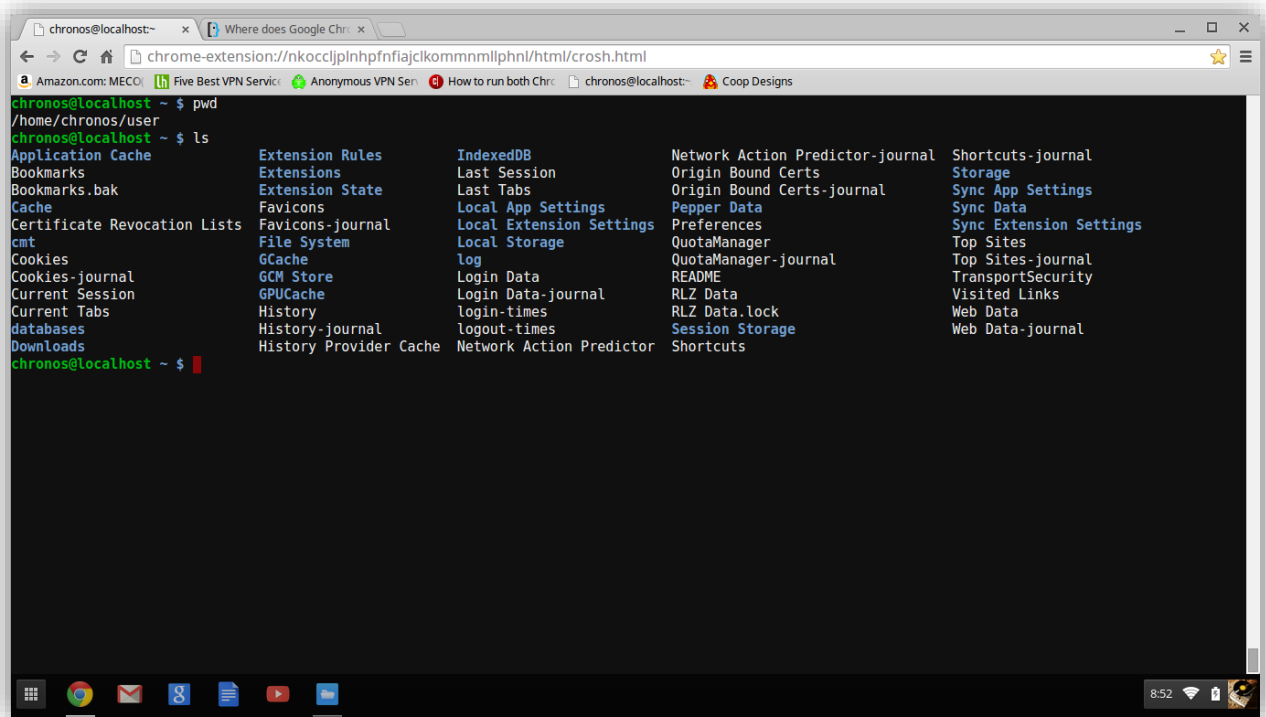


Figure 18. Listing of User directory in Crosh.

When using the Chrome browser on any computer, the browser history is viewable by directing the browser to the URL *chrome://history/*. Figure 19 shows what the Chrome browser on the Chromebook when directed to load that URL provides.

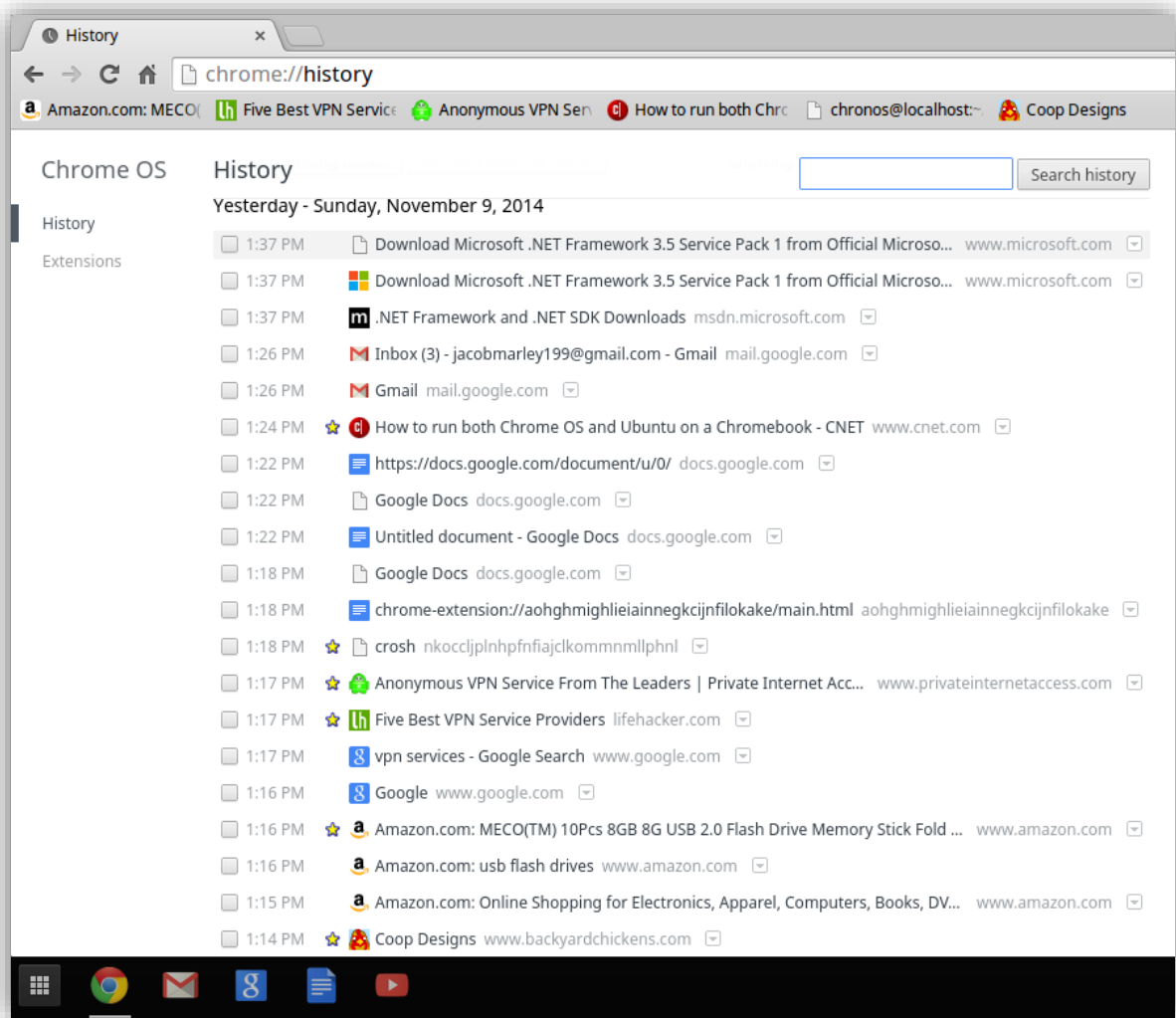


Figure 19. Chromebook browser History.

When opening the Bookmark Manager in the Chrome browser on the Chromebook, the contents shown in Figure 20. This is consistent with what the tool in the previous section showed.

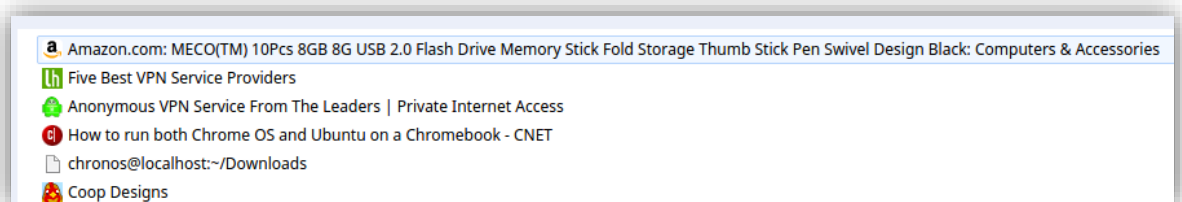
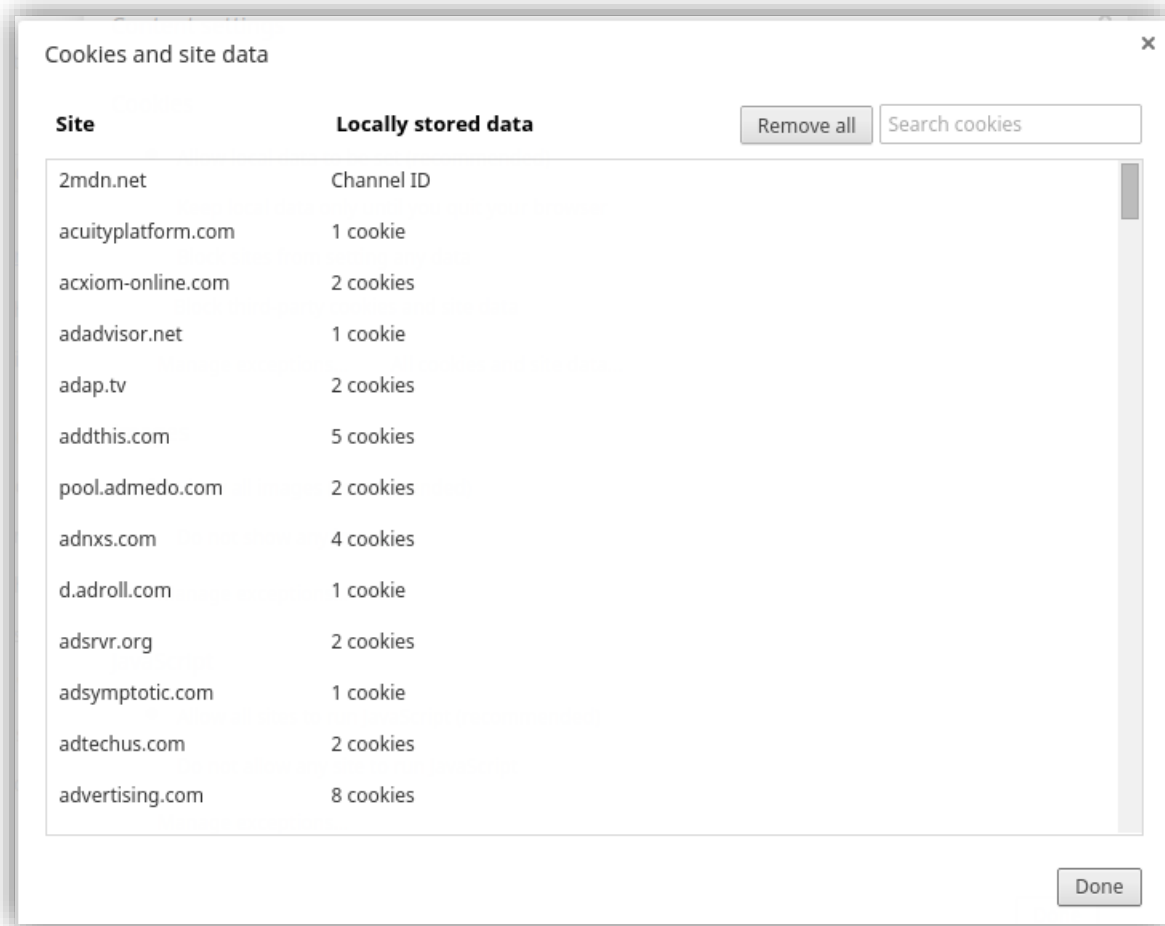


Figure 20. Chromebook browser Bookmarks

Figure 21 shows the cookie listing that is available from the browser through the Settings interface.



*Figure 21.* Chromebook browser Cookies

Figure 22 shows the contents of the local directory where the Chrome browser places downloaded files. This listing shows a file named “Crouton” which is used in Developer Mode to download and install a Linux operating system covered later in analysis.

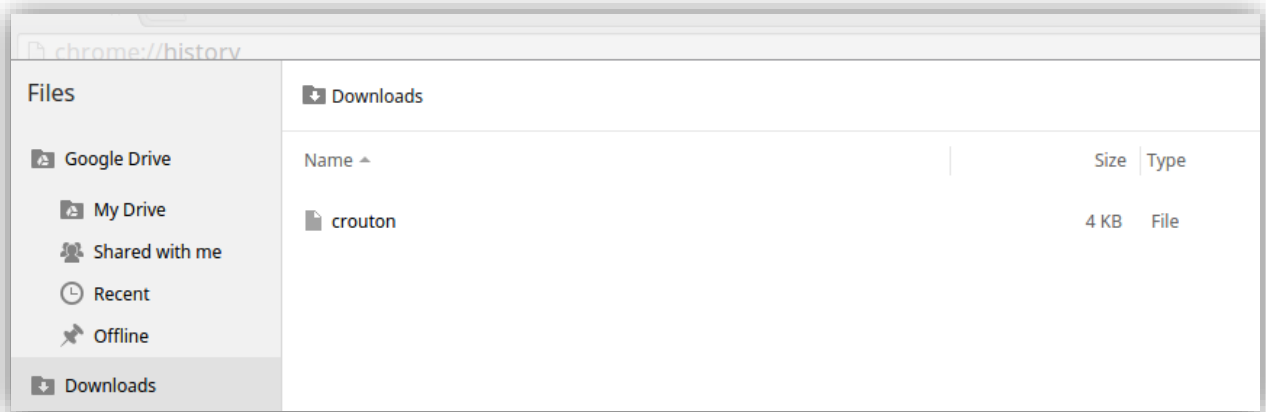


Figure 22. Chromebook browser Downloads directory

Figure 23 displays Browser history when you point the browser to the URL <http://history.google.com/history/>.

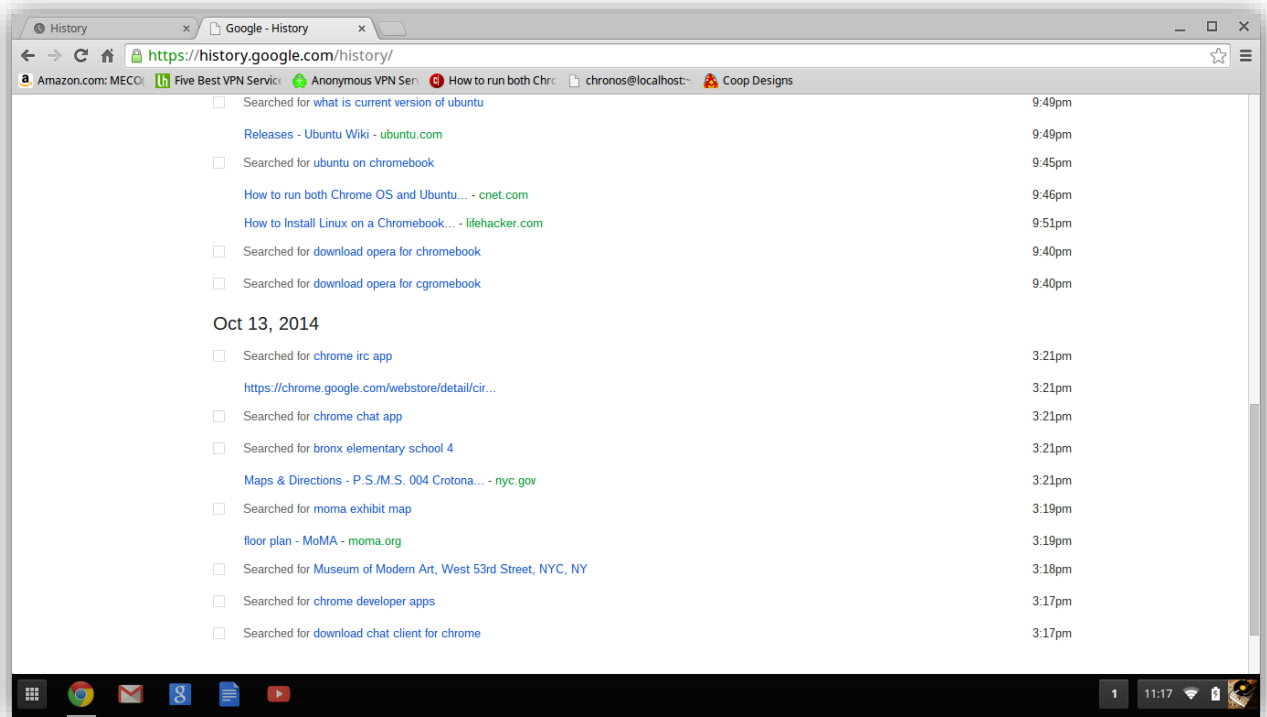


Figure 23: Chromebook browser Search History

Figure 24 displays the Login history for the google Gmail account used to login into the Chromebook. Login occurs every time the Chromebook is opened and the account logged into from any other browser at any time.

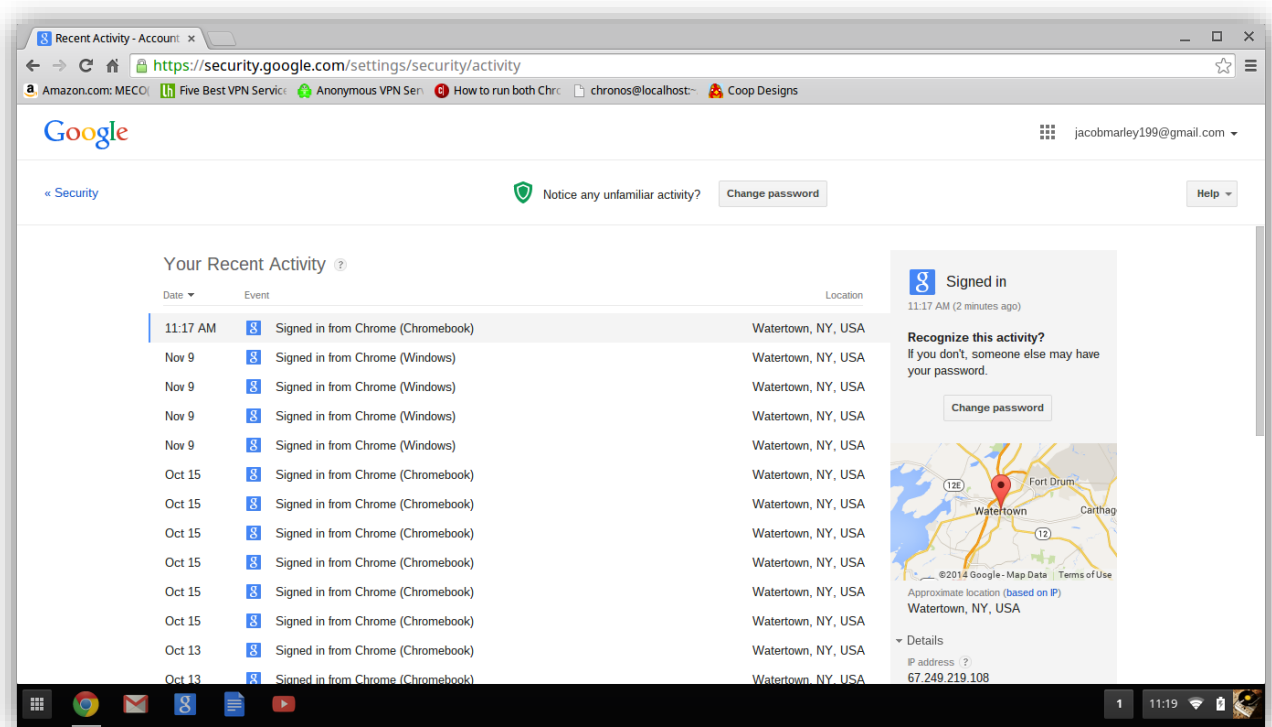


Figure 24: Chromebook browser Login History

Figure 25 it is displayed the most visited sites displayed whenever a new tab in the Chrome browser is open. The data revealed in this view changes as the user surfing habits change.

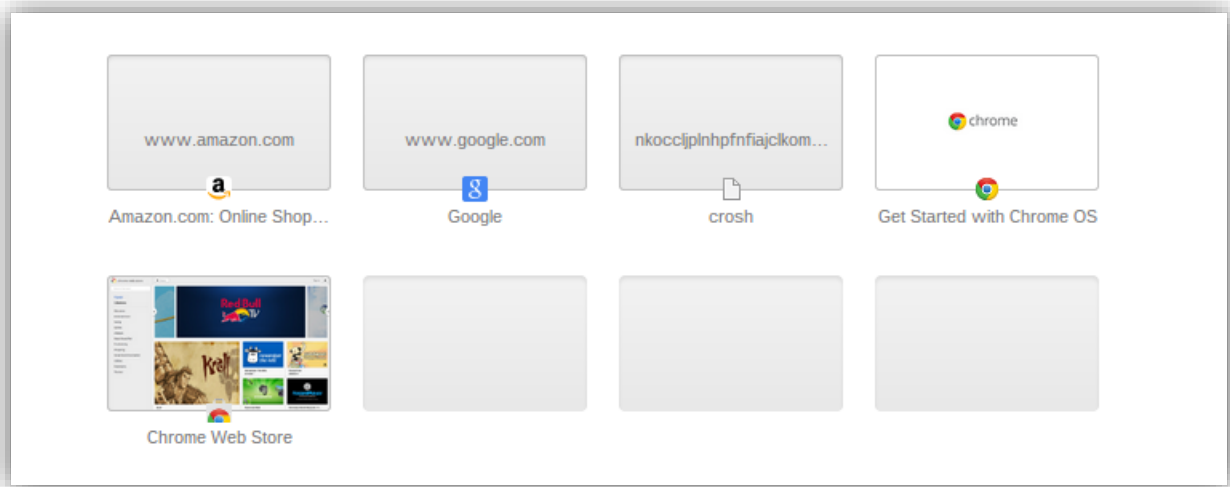


Figure 25: Chromebook browser Most Visited Sites

Figure 26 shows the browser cache listing. This listing is viewable from any Chrome browser logged into the user account and pointed at the URL *chrome://cache/*.

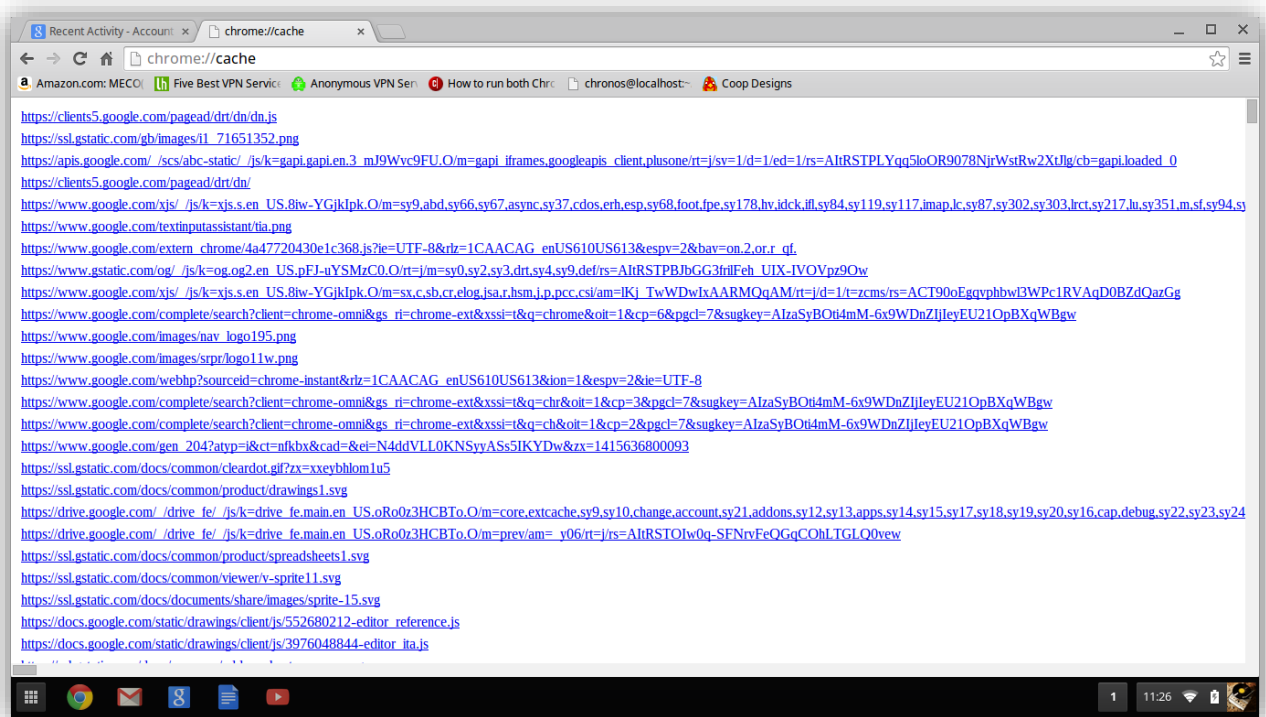
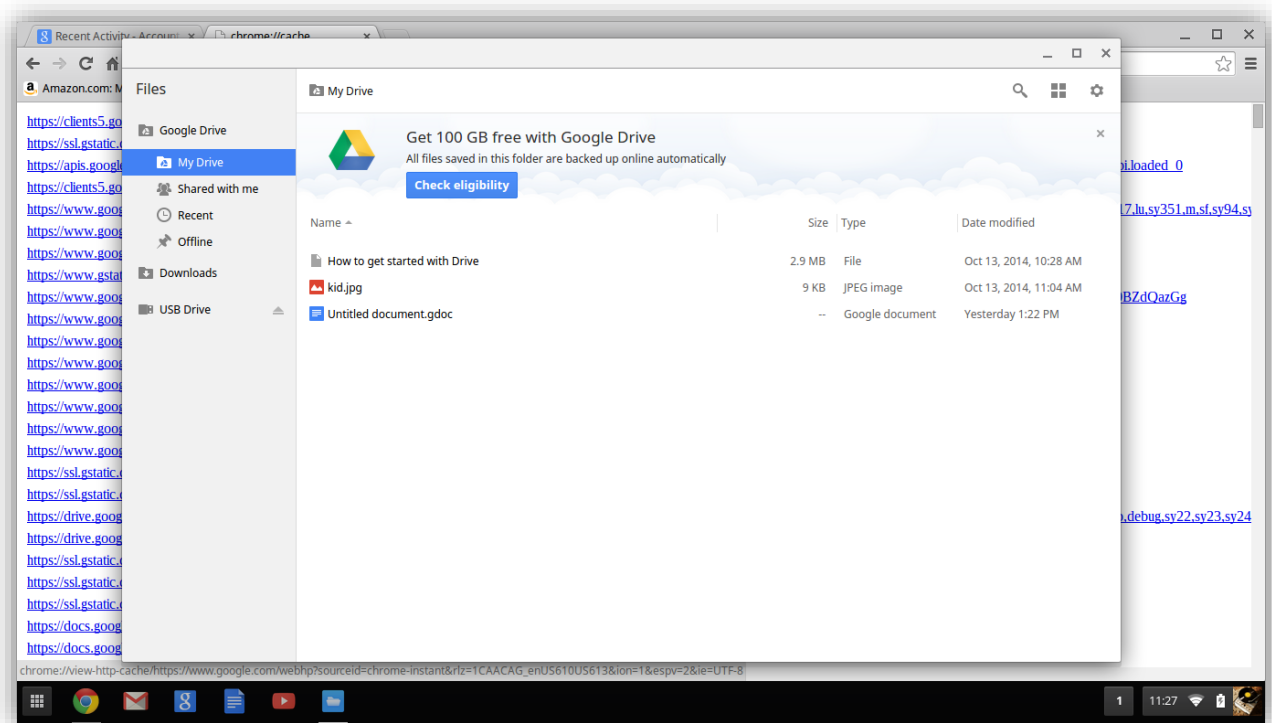


Figure 26: Chromebook browser Cache

Figure 27 show the contents of the Google Drive folder as viewed on the Chromebook computer. These files are also available from any other computer logged into the user account.



**Figure 27:** Chromebook browser Google Drive Contents

### **Crosh Tools Available in *Shell***

Forensic examiners have a host of tools available during the process of collecting and analyzing evidence. Within the Chrome Operating System using the Crosh shell there are several tools of note that are useful for analyzing a Linux-based operating system like Chrome Operating System. Plugging an examiner prepared USB Flash drive automatically mounts into the system. It provides trusted apps to execute and acts as a storage device for captured items during the gathering of forensic artifacts within the Crosh shell. The path to this USB drive may be something like shown in Figure 28.

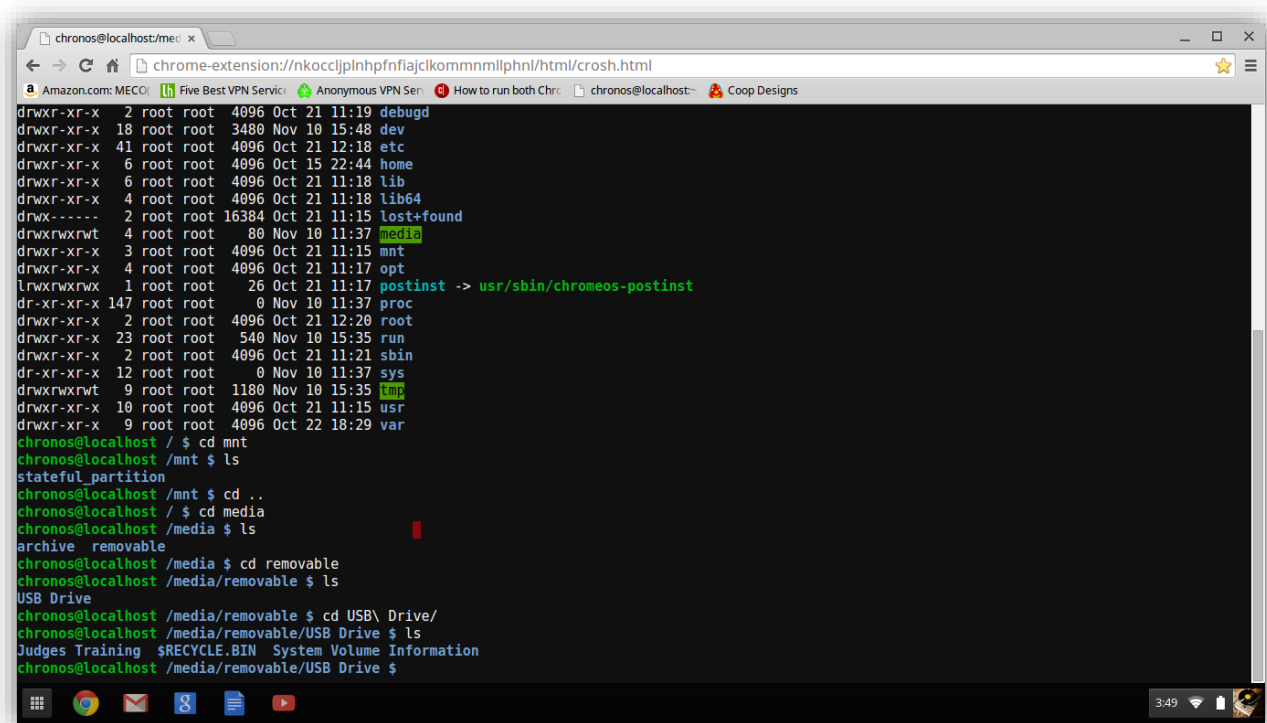


Figure 28: Path to USB drive

Table 1 lists the Linux applications provided with the Chrome Operating System accessed from the Crash shell.

Table 1

*A selection of Linux-based programs available in Crash Shell within Chrome Operating System providing forensic function in an investigation*

Program	Forensic Function Provided
dd	Create disk images similar to FTK DiskImager
grep	Scan text files for specific strings
w	Listing of current and prior logged in users
ls	Listing of current directory contents
ps	List currently running processes
lsof	List of open files (to compare to running processes)



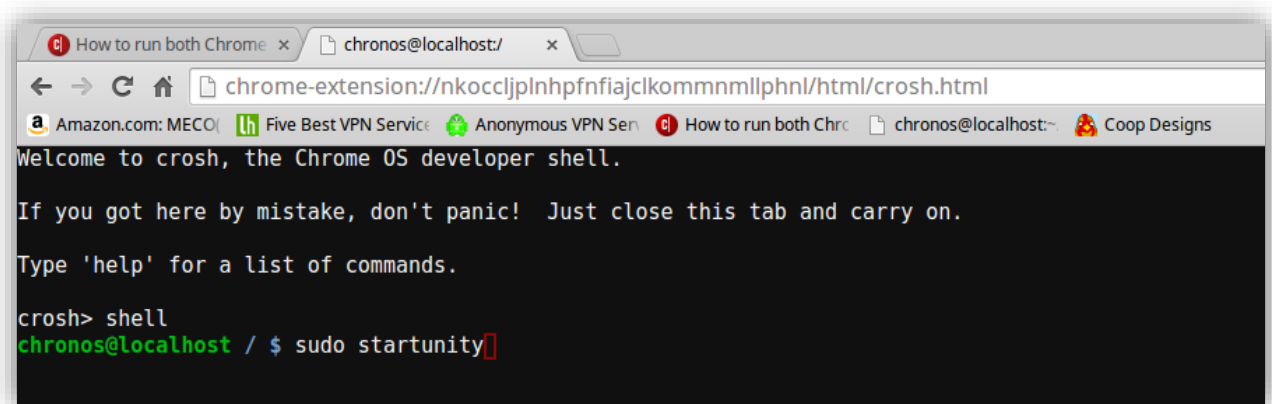
find	To search specified directories for a specific filename which may include wildcards
tar	Create an archive file containing specified files. Useful for capturing logs, trace and message files as well as other files of interest
date	Capture the current date/time on the running system (useful if you have scripts you run that use it for naming files copied/generated)
sh & bash	Useful shells to use for running custom Unix scripts
md5sum	Can be used to generate MD5SUM value for files
cp	Copy files between directories
mount and umount	Used to mount and un-mount file systems. Useful for changing a file system to read-only during forensic investigation
cat	List out contents of a file to the command line

---

Forensic examiners with experience know how to use these tools to find, archive, and analyze the output from these commands. The *dd* application is perhaps the most familiar of UNIX tools available. By issuing *sudo dd if=/dev/sda of=/media/removable/USB\ Drive/chromebookhd.img conv=sync,noerror bs=64K* the chromebook will create a bit by bit copy of the Chromebook SSD copying it into the file *chromebookhd.img* placed upon the USB HDD that had been plugged into the device. Before issuing it, examiners should issue the command *ls /media/removable/* to display the name of the directory mounted to the USB device. Once this *img* file is on the USB Drive, forensic tools can process it and carve out the contents of IMG files such as these.

## Crosh Running Ubuntu Unity Release

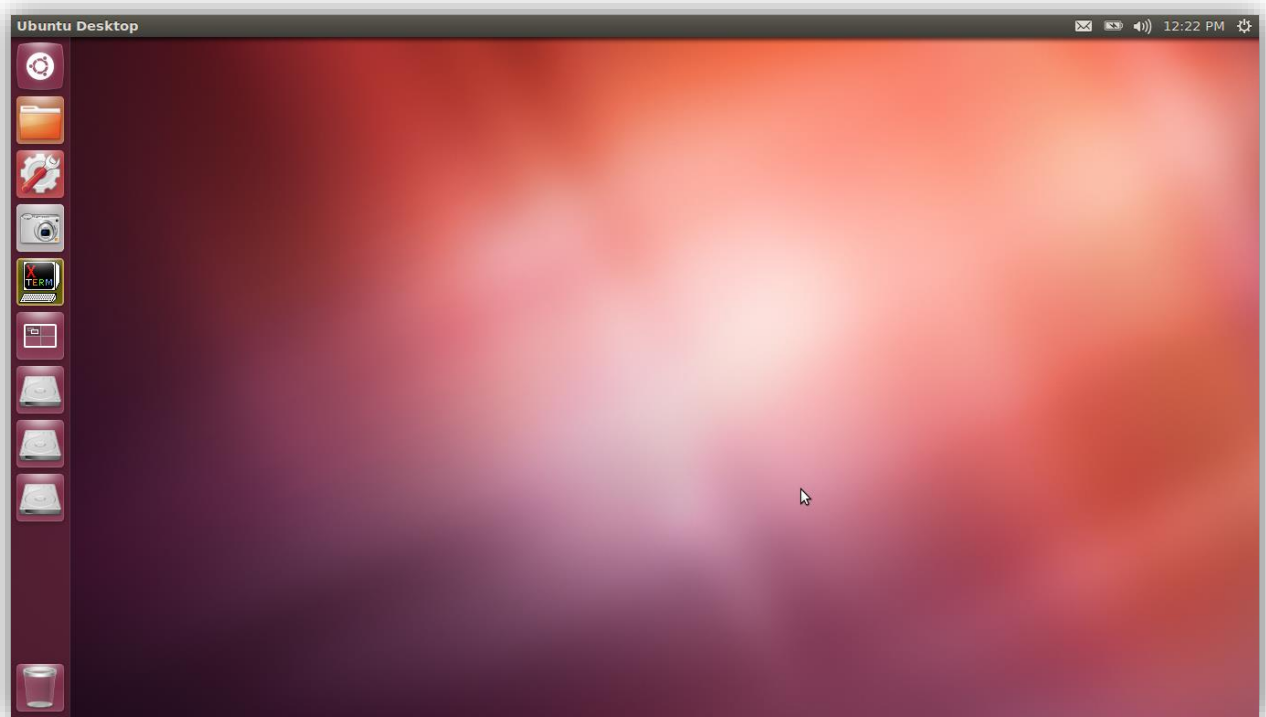
Noting earlier that there was a file named “Crouton” in the Download directory revealed that the user likely installed a Linux Operating System to run inside Chrome Operating System. Performing a Google search for “Chromebook Crouton” revealed the most often found Operating System to install is the “Ubuntu unity” release (Ubuntu Unity, 2014). In order to open the shell command-line in Chromebook Operating System, the device must already be in Developer Mode and issue keystrokes *Ctrl-Alt-t*. Figure 29 shows the Chrome Browser already has a bookmark to the terminal window. Clicking this bookmark opens up the Crosh shell. To enter the Linux terminal shell from Crosh, the user enters *shell* as displayed in Figure 29. In order to start Ubuntu, the shell command required is *sudo startunity*. Figure 29 shows this command issued.



```
chrome-extension://nkocljplnhpfnfajclkommmmlphnl/html/crosh.html
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.
crosh> shell
chronos@localhost / $ sudo startunity
```

Figure 29: Issuing Crosh command "sudo startunity"

Figure 30 shows success loading the Ubuntu Operating System inside the Chromebook.



*Figure 30:* Ubuntu Unity release desktop

Noting the Disk Drive shortcuts on the left-hand side of the desktop, the three are unreadable Linux drives from the Chrome Operating System itself. The examiner browsed their contents by clicking and screen capturing the results (See Figure 31).

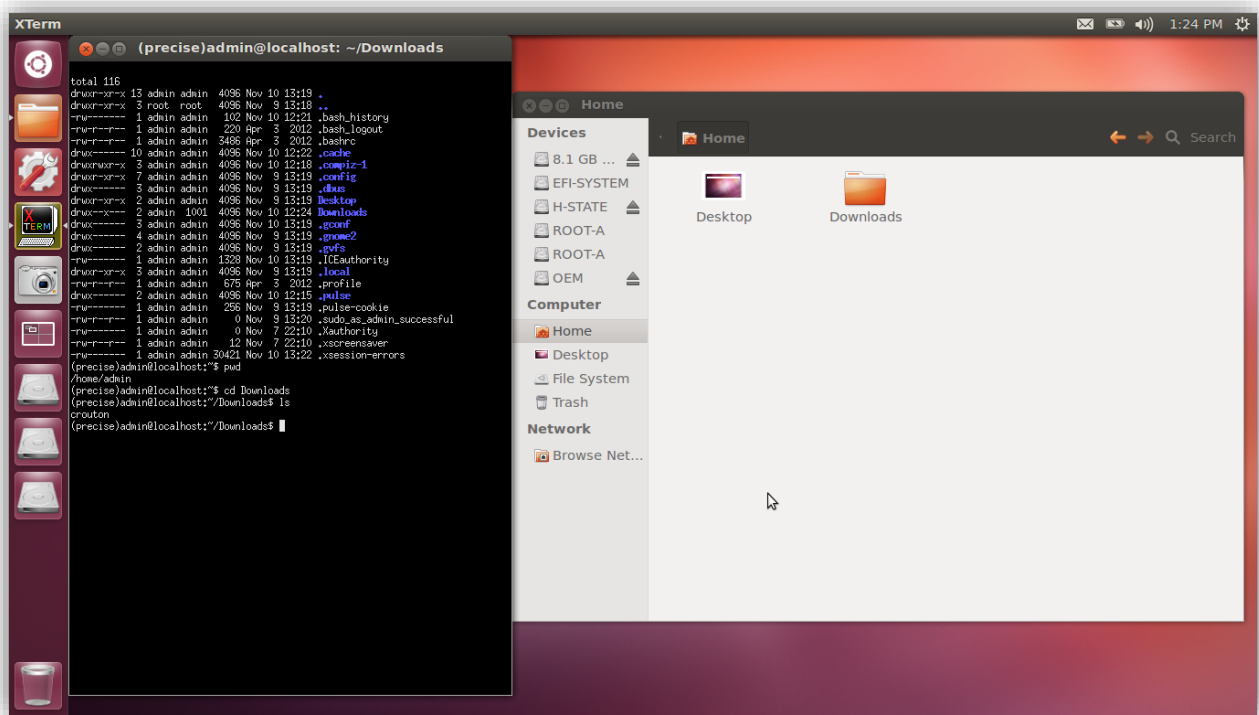


Figure 31: Overlay of Ubuntu Terminal `ls` of local user dir Downloads compared to GUI view in Ubuntu Unity Desktop.

Opening a terminal window in Ubuntu and requesting a listing of the current user Downloads directory shows that the Ubuntu uses the same directory structure as Chrome Operating System for the user when it lists the file “Crouton.” The implication is that the other directories may in fact be the same user accessible directories as made available in Crosh shell. Figure 32 and Figure 33 reveal the Crosh shell messages after selecting *shutdown* in the Ubuntu VM. These two figures reveal many of the shell messages written to the console during both boot and shutdown of the VM.

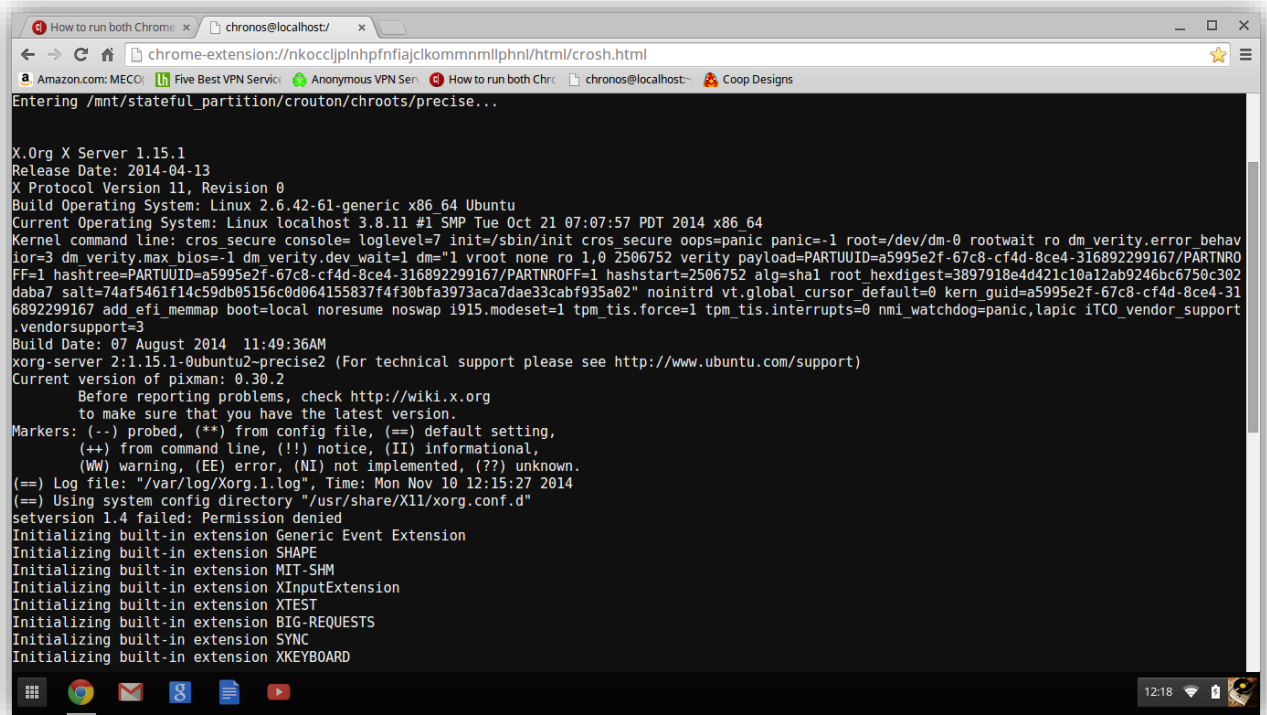


Figure 32: Crash shell after logoff Ubuntu (continued in Figure 33).

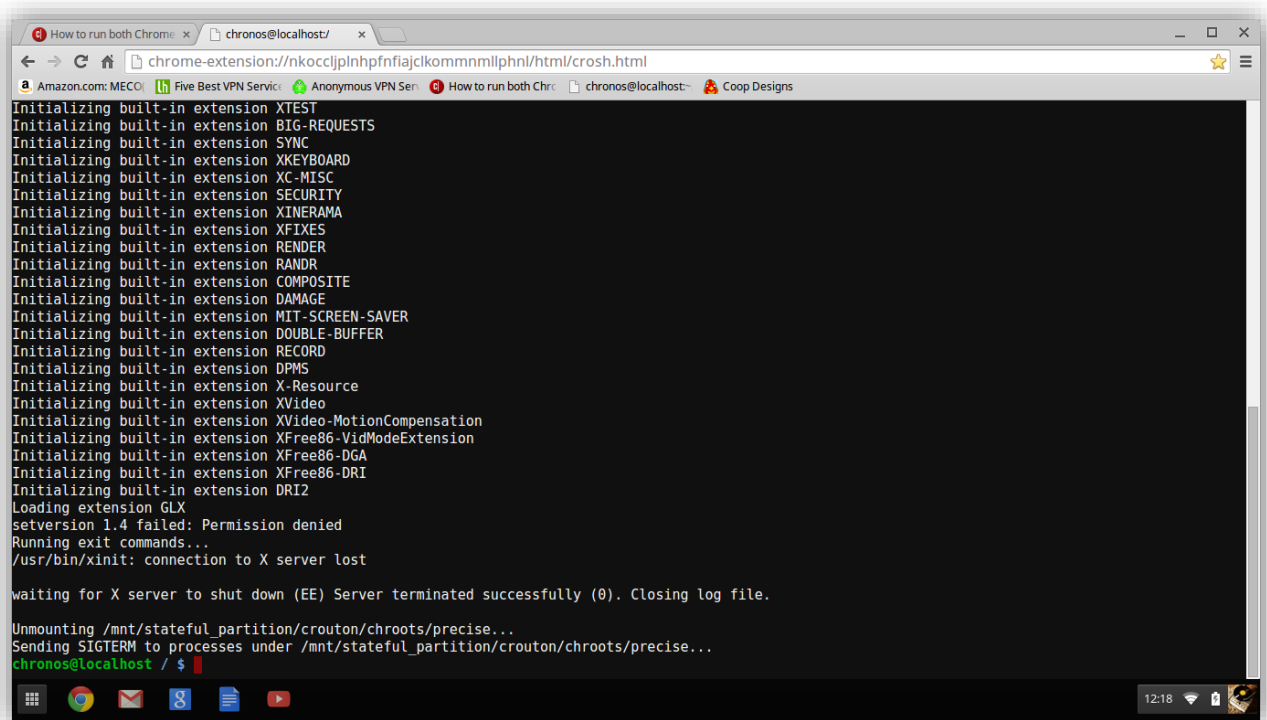


Figure 33: Crash shell after logoff Ubuntu cont'd.

## **Using Linux Tools on Chrome Operating System for Forensic Toolkits**

The tools available in Crosh listed in the previous section are also available from within Ubuntu. An examiner would be interested to know if any tools available on other operating systems can be compiled and run on a Chromebook. There are of course things to understand about Linux applications and compiling programs for them. The first is the chipset. Each chipset, currently Intel x86 and ARM used in Chromebooks requires the application compiled separately. The trouble of identifying which applications to compile for use on Chrome Operating System is no small task and is easier than actually collecting the source code for those apps and compiling them for all the potential Chrome Operating System based devices.

The first requirement is for a Linux Operating System installed like Ubuntu with Crouton. As this was done already for this investigation, that is the approach used for this section. The scripting language Python (version 2.7.3) installed with the Ubuntu installation via Crouton enables scripting. This scripting provides the capacity to use most of the Python code provided with Harlan Carvey and Cory Altheide's book *Digital Forensics with Open Source Tools*, all of which may be placed on a USB Flash drive that can be plugged into the Chromebook to execute and write results to the USB Flash drive (2011, p. 56). The first desire of an investigator is to copy the device data processed externally to reduce the risk of anything being inadvertently modified or missed during the investigation (Sammons, 2012).

### **Logical Copy of Chromebook User Directory and Analysis Using FTK**

Connecting the external USB HDD used previously, the examiner copied the contents of the user directory `/home/chronos/user` to the external USB HDD. This directory contained the user data available to the logged in user via both the Chrome browser and when in Developer Mode from the command line shell *Crosh*. As it is possible that the user of the Google

Chromebook could have modified the *cp* application used on the system, an MD5SUM was taken of the executable and compared to the MD5SUM of a known good version for that version of the operating system meant for those devices. If possible, a copy of that alternate trusted *cp* application would be on the external USB HDD to execute to reduce the possibility of the data copied deliberately corrupted during the copying (Greetham, 2013). The less standard the tool, the harder it would be for a hacker to anticipate the copying tool to corrupt its execution. This is precisely the reason forensic examiners prefer to use cold captured data since they can control the applications used as well as the applications which are running in memory of the computer used for analysis.

As performed for an earlier section, FTK executed and the directory imported as evidence analyzed for forensic artifacts. From a forensic examiners perspective, this is likely the best case of artifact collection available under the current configuration of a Google Chromebook. Having access to the userid and password provides access to the most possible data and with it configured in Developer Mode, the command line can provide a means to copy the relevant files from the Chromebook onto external storage to be isolated, archived and analyzed for incorporation into the overall investigation.

The processing of the user directory by FTK revealed approximately 4550 files, which will vary from one user to another. Note the user data included the Crouton file and the Ubuntu installation as well significantly swelled the count. In an effort to keep the content of useful artifacts down in number, removing the Crouton app as well as the Ubuntu installation as they provided little additional forensic value outside of possibly revealing the user is a sophisticated computer user to have configured the Chromebook to that extent. Furthermore, removing the Crouton and Ubuntu installation reduced the file count to a little more than 2400 artifacts. Many

of the artifacts previously identified, shown in Figure 34, are included in the FTK analysis of the *user* directory.

File Name	Full Path
data_0	C:\Users\george\Desktop\ud\Application Cache\Cache\data_0
data_1	C:\Users\george\Desktop\ud\Application Cache\Cache\data_1
data_2	C:\Users\george\Desktop\ud\Application Cache\Cache\data_2
data_3	C:\Users\george\Desktop\ud\Application Cache\Cache\data_3
f_000001	C:\Users\george\Desktop\ud\Application Cache\Cache\f_000001
f_000002	C:\Users\george\Desktop\ud\Application Cache\Cache\f_000002
f_000003	C:\Users\george\Desktop\ud\Application Cache\Cache\f_000003
index	C:\Users\george\Desktop\ud\Application Cache\Cache\index
Index	C:\Users\george\Desktop\ud\Application Cache\Index
Bookmarks	C:\Users\george\Desktop\ud\Bookmarks
data_0	C:\Users\george\Desktop\ud\Cache\data_0
data_1	C:\Users\george\Desktop\ud\Cache\data_1

Figure 34: Snapshot of FTK files from *user* directory.

The advantage of having these artifacts is to be able to separate them out as needed for individual presentation in support of other evidence when presenting the case in court. Since the contents are made of files that are mostly not human readable files, the examiner used the ChromeAnalysis Plus application again to reveal what is in the contents of this *user* directory. Website History failed due to date translation errors as shown in Figure 35.

ID	From Visit	Date Visited (UTC -5, DST Enabled)	URL	Total Visit Count	ChromeAnalysis Total Visit Count	Title
[Content obscured]						

Figure 35: Web History unavailable

Figure 36 shows the Bookmarks from earlier analysis found in the *user* files.

ID	Date Added (UTC -5, DST Enabled)	URL	Title	Type
5	11/9/2014 1:16:36 PM	http://www.amazon.com/10Pcs-Memory-Storage-Swivel-Design/dp/B00DXZKY...	Amazon.com: MECO(TM) 10Pcs 8GB 8G USB 2.0 P...	url
6	11/9/2014 1:17:17 PM	http://fihacker.com/5935863/five-best-vpn-service-providers	Five Best VPN Service Providers	url
7	11/9/2014 1:17:33 PM	https://www.privateintemetaccess.com/	Anonymous VPN Service From The Leaders   Privat...	url
8	11/9/2014 1:23:16 PM	http://www.cnet.com/how-to/how-to-run-both-chrome-os-and-ubuntu-on-a-chrom...	How to run both Chrome OS and Ubuntu on a Chro...	url
9	11/9/2014 1:18:10 PM	chrome-extension://rkokcplnhpfrfajckommmlphnl/html/crash.html	chronos@localhost:~/Downloads	url
10	11/9/2014 1:14:39 PM	http://www.backyardchickens.com/atype/2/Coops	Coop Designs	url

Figure 36: Bookmarks



Figure 37 lists cookies from several advertisers and many from Google.

Host	Path	Created (UTC -5, DST Enabled)	Last Accessed (UTC -5, DST Enabled)	Name	Expiry (UTC -5, DST Enabled)	Is Secure	Is HTTP Only	Value
doubleclick.net	/	11/16/2014 6:39:29 PM	11/16/2014 6:39:29 PM	test_cookie	11/16/2014 6:54:29 PM	No	No	
.doubleclick.net	/	11/16/2014 6:39:29 PM	11/16/2014 6:39:29 PM	__dt__	11/17/2014 6:39:29 PM	No	Yes	
accounts.google.com	/	11/16/2014 6:39:29 PM	11/16/2014 6:39:29 PM	LSID	Invalid Date	Yes	Yes	
accounts.google.com	/	11/16/2014 6:39:29 PM	11/16/2014 6:39:29 PM	GAPS	11/15/2016 6:39:29 PM	Yes	Yes	
accounts.google.com	/	11/16/2014 6:38:24 PM	11/16/2014 6:39:29 PM	GoogleAccountsLocale_ses...	Invalid Date	Yes	Yes	
accounts.google.com	/	11/16/2014 6:38:24 PM	11/16/2014 6:39:29 PM	GALX	Invalid Date	Yes	No	
google.com	/	11/16/2014 6:39:27 PM	11/16/2014 6:39:27 PM	PREF	11/15/2016 6:39:27 PM	No	No	
youtube.com	/	11/16/2014 6:38:47 PM	11/16/2014 6:38:47 PM	SAPISID	Invalid Date	Yes	No	
youtube.com	/	11/16/2014 6:38:47 PM	11/16/2014 6:38:47 PM	APISID	Invalid Date	No	No	
youtube.com	/	11/16/2014 6:38:47 PM	11/16/2014 6:38:47 PM	SSID	Invalid Date	Yes	Yes	
youtube.com	/	11/16/2014 6:38:47 PM	11/16/2014 6:38:47 PM	HSID	Invalid Date	No	Yes	
youtube.com	/	11/16/2014 6:38:47 PM	11/16/2014 6:38:47 PM	SID	Invalid Date	No	No	
google.com	/	11/16/2014 6:38:46 PM	11/16/2014 6:38:46 PM	SAPISID	Invalid Date	Yes	No	
google.com	/	11/16/2014 6:38:46 PM	11/16/2014 6:38:46 PM	APISID	Invalid Date	No	No	
google.com	/	11/16/2014 6:38:46 PM	11/16/2014 6:38:46 PM	SSID	Invalid Date	Yes	Yes	
google.com	/	11/16/2014 6:38:46 PM	11/16/2014 6:38:46 PM	HSID	Invalid Date	No	Yes	
google.com	/	11/16/2014 6:38:46 PM	11/16/2014 6:38:46 PM	SID	Invalid Date	No	No	
google.com	/	11/16/2014 6:38:43 PM	11/16/2014 6:38:43 PM	NID	5/18/2015 7:38:43 PM	No	Yes	

Figure 37: Cookies

As expected, the download directory was empty since the examiner had removed the Crouton application to reduce the files to process for this section of analysis. Figure 38 displays the empty table.

ID	URL	Full Path	Start Time (UTC -5, DST Enabled)	State	Bytes Downloaded	Total Bytes

Figure 38: Empty Download Directory

Search Terms and Logins were empty in this step, as shown in Figure 39 and 40.

Term	URL

Figure 39: Empty Search Terms

Origin URL	Action URL	Username Field	Password Field	Username	Sign On Realm	Date Created (UTC -5, DST Enabled)

Figure 40: Empty Logins

Since the last analysis on this browser data, the browser's Most Visited Sites reduced to merely the more recent ones. Figure 41 shows this short list of websites.

URL Rank	URL	Title	Redirects	Last Updated (UTC -5, DST Enabled)
0	chrome-extension://nkocdplnhpfnfajclkommmllphrl/html/crosh.html	crosh	chrome-extension://nkocdplnhpfnf...	11/16/2014 6:40:00 PM
1	http://www.google.com/chrome/intl/en/welcome.html	Get Started with Chrome OS	http://www.google.com/chrome/in...	11/16/2014 6:38:45 PM
2	https://chrome.google.com/webstore?hl=en	Chrome Web Store	https://chrome.google.com/websto...	11/16/2014 6:38:45 PM

Figure 41: Most Visited Sites

Favicons, displayed in Figure 42, is the same list as revealed much earlier in this investigation.








ID	Image	URL	Page URL	Last Updated (UTC -5, DST Enabled)
6		https://www.google.com/favicon.ico	https://www.google.com/_/chrome/newtab?ftz=1CAACAG_enUS614...	11/16/2014 6:39:28 PM
6		https://www.google.com/favicon.ico	https://www.google.com/_/chrome/newtab?ftz=1CAACAG_enUS614...	11/16/2014 6:39:28 PM
5		http://www.backyardchickens.com/custom/huddle/backyardchicken...	http://www.backyardchickens.com/atype/2/Coops	11/16/2014 6:38:49 PM
4		http://www.cnet.com/favicon.ico	http://www.cnet.com/how-to/how-to-run-both-chrome-os-and-ubuntu-...	11/16/2014 6:38:49 PM
3		https://www.privateinternetaccess.com/favicon.ico	https://www.privateinternetaccess.com/	11/16/2014 6:38:49 PM
2		http://i.kinja-img.com/gawker-media/image/upload/s-rqDhe7s2-/c_fil...	http://lifehacker.com/5935863/five-best-vpn-service-providers	11/16/2014 6:38:49 PM
1		http://www.amazon.com/favicon.ico	http://www.amazon.com/10Pcs-Memory-Storage-Swivel-Design/dp/B...	11/16/2014 6:38:49 PM

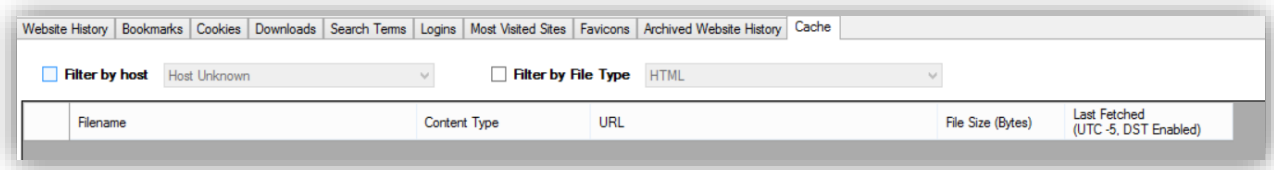
Figure 42: Favicons revisited

The Archive and Cache are clean after the reset to remove Crouton and Ubuntu shown in Figure 43.

ID	From Visit	Date Visited (UTC -5, DST Enabled)	URL	Total Visit Count	ChromeAnalysis Total Visit Count	Title

Figure 43: Empty Archive

The data artifacts which were revealed from the copied content of the *user* directory were indeed mostly duplicates of what the examination already found attempting to retrieve them a different way. Figure 44 shows the empty cache.



*Figure 44:* Empty Cache

### **Discussion of Findings**

Reviewing the data revealed in the Analysis phase of this investigation, there is an effective approach to acquire data from a device using the Google Chrome Operating System. During the usual cold capture of data from the contents of an HDD, or in this case an SSD, the user data remained out of reach without additional decryption technology. This technology of course was not available at the time of this investigation, or else the investigator was unable to find it to use. The analysis revealed much of what Feng et al. predicted in their paper about the file systems, kernels, and UEFI portions of the device firmware and operating system. While what is discoverable in this method, with decryption software it is not of material value to the investigation, as it reveals nothing specific to any users of the device.

The next step of accessing the data objects stored within the cloud using only a Google Chrome Browser running inside a Windows XP VM yielded some data that could possibly be of use to forensic examiners depending on the investigation. While it requires the userid and password for the suspect's Gmail account, this may be available via consent or a properly crafted legally acquired search warrant and thus is a valid path for an examiner to take to acquire the data.

The operating system file path to these files the Google Chrome Browser data resides in is *C:\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\User Data*. The data available includes emails still stored in the account, files stored in the Cloud, google search history, Chrome Extensions that provide extra function to the browser, userid, and passwords, stored for re-use by the browser with the users permission. This approach also provides the bookmarks stored by the user, cookies from websites they have visited while logged into the Gmail account, and the most recent compilation of Most Visited Websites showing sites. Perhaps most useful after emails is website history showing the websites the user has visited with date and time stamps as well providing the browser cache which may contain data put into form fields, and other specific data related to individual sessions the user had with websites listed in the history. These latter two allow an investigator to place the user activity into a timeline with specific data (Altheide & Carvey, 2011).

The artifacts available to an investigator logged in directly to the Google Chrome Operating System device in Developer Mode includes all the data, which is available above via the Google Chrome Browser running in a Windows XP VM logged into the Gmail account. Furthermore, the device under investigation may have a local folder for storing data by the user and additional user directories that may contain user created files. While in the Crosh shell, an investigator has all those convenient Linux-based applications listed in Table 1 to use in order to explore the user data files and other directories within the Crosh shell. All of the same data found in the Windows VM running the Google Chrome Browser were available in this approach. The key difference is in where the data was since the normal Linux file locations used on the Chromebook instead of the file locations for Windows. In the Google Chrome Operating System, the file system path to the user files is */home/chronos/user*.

The next approach was to examine the Google Chromebook in Developer Mode, which had the Crouton tool run to install a version of Ubuntu into the system. A useful difference is Ubuntu based programs run from the Ubuntu VM against the local files for the current user. The requirements for this setup are quite high considering the relatively high technical computing skills required to make it work. The device needs to be in Development Mode, Crouton downloaded and Ubuntu installed to reach this complex configuration. This method revealed that the only additional artifacts of interest would be applications installed into Ubuntu by the user which are not already available within the Crosh shell while all the same user files from the Crosh shell are also rendered into user space within the Ubuntu file system while running. This lead to the next section that discusses the factors involved in a user acquiring applications that can run in this Ubuntu installation.

Finally, it is clear that the best approach to capturing data from a Google Chrome Operating System based device configured in Developer Mode is to create a logical copy from the Crosh shell onto an external USB HDD. This is the method used for live capture of Google Chrome Operating System based device on the scene. If done on the scene any network connections currently made to remote systems, such as *ftp*, *ssh* and *rlogin*, will be available to the investigator to include in artifact collection. As mentioned in Analysis, an examiner should have an application on the external USB HDD as the application that copies from the Google Chrome Operating System device onto the HDD. In the future, investigators may have access to tools like Volatility to capture the active memory of these live systems, further improving the depth and quality of the data collected during the investigation.

While there were many approaches attempted, the analysis revealed the live capture provided access to the best data despite the risks of the running system modifying items while

the live capture occurred and the possibility that the user may have an application running on the system that could interfere with the live capture. Alternatively, if a Google Chrome Operating System based device is User Mode instead of Developer Mode, the best approach is using the legally obtained Gmail account info and logging into a Google Chrome Browser running inside a VM. Inside the VM, an investigator may have access to full forensic software suites in order to process the data mirrored in the Google Cloud and the challenges of SSDs and hacked operating system files are not a risk of concern.

### **Future Research Recommendations**

#### **Google Chromebook Forensic Tools Run from a USB Flash drive**

There is a need to develop and distribute trusted tools that can be run from a USB flash drive to find and collect artifacts from Google Chromebooks. These tools need testing on each of the various Chromebooks available to consumers. What are some trusted tools that perform the necessary functions of finding and extraction data from a Google Chromebook when run from a USB flash drive mounted on the Google Chromebook?

#### **Establish a Legal Relationship with Google**

Law enforcement forensic examiners should establish a legal relationship with Google to understand the proper legal procedures regarding search warrants and court orders to acquire privileged access to the Google Gmail accounts. There will be times when legal process is necessary to obtain the ID and password required to log into and collect forensic evidence. What is the most expedient legal process to obtain user name and ID for a Google account from Google? What specific language obtains the most appropriate data for the given investigation?

## **Chromebook Browser Artifact Extraction in Mainstream Tools**

Forensic tools such as AccessData's Forensic Toolkit and Guidance Software's Encase should incorporate specific Chromebook browser artifacts processing similar to the functions developed in the tool ChromeAnalysis Plus by Foxtan Software Limited. How can mainstream forensic suites benefit from incorporating Google Chromebook Browser Artifacts?

### **Conclusion**

Google Chrome Operating System has many very well designed features. Other investigators looked into the many layers of encryption and careful security measures put into place in order to protect the users both in User mode and in Developer Mode (Fang et al., 2011). Separating out the three ways in which Google Users' data presented, provided a few views that examiners should be aware of in order to better prepare them for examining a Google Chromebook. For this investigation, the contents of the SSD were imaged and processed within AccessData Forensic Toolkit, revealing the contents are encrypted by the operating system. Next, the Google Gmail account was logged into from a Chrome browser to see what kinds of data persists in Google Cloud between sessions, across multiple devices, for a user. Finally, the Chromebook examination revealed the same data discovered in the previous step.

In the process of investigating the Chromebook itself in Developer Mode several useful Linux applications were identified of use to examiners who have an ID and password for a Chromebook system placed in Developer Mode. Most notable of the Linux applications is the *dd* application used for generating image files of a disk drive. With a *dd* created image file, an investigator can do the normal processing of Linux images. The data of most use to an investigator will come after acquiring the password for a suspect ID. The means of gathering the data varies based on a couple factors: if the Chromebook is in User or Developer Mode; if they

user installed an Operating System into the system while it was in Developer Mode; and what precisely is the data the investigator is most interested in discovering through examination.

Considering the investigator needs access to the user account, it is likely that investigating the Cloud data while legally logged in to the account with the Chrome browser will yield the most useful artifacts for an investigation.

Other forensic examiners may expect to find most of the data that is available using the VM method legally logging into the Gmail account and analyzing the Chrome browser artifacts. It has the advantage of not needing the Chromebook to be in Developer Mode while leveraging the access to the account ID and password that allows them to get past the effective encryption technology used in Google Chrome Operating Systems to protect user data. In order to keep the forensic examination of the Google Chrome Operating System in a context useful to law enforcement, an important reference to follow-up with is a journal article from the Journal of Digital Forensics, Security and Law, Vol. 1 (2).



## References

- Acer.com. (2013). *c720*. Retrieved September 13, 2014, from Acer.com:  
<http://us.acer.com/ac/en/US/content/series/c720>
- Ackerman, D. (2013, April 29). *Living with Chromebook: Can you use it to actually get work done?* Retrieved September 5, 2014, from CNET.com: Living with Chromebook: Can you use it to actually get work done? - CNET. (n.d.). Retrieved from  
<http://www.cnet.com/news/living-with-chromebook-can-you-use-it-to-actually-get-work-done/>
- Altheide, C., & Carvey, H. (2011). *Digital Forensics with Open Source Tools*. Waltham, MA: Syngress.
- Bell, G. B., & Boddington, R. (2010). Solid state drives: the beginning of the end for current practice in digital forensic recovery? *Journal of Digital Forensics, Security and Law*, 5(3), 1-20.
- Bhartiya, S. (2014, November 17). *How to Easily Install Ubuntu on Chromebook with Crouton*. Retrieved September 1, 2014, from Linux.com:  
<http://www.linux.com/learn/tutorials/795730-how-to-easily-install-ubuntu-on-chromebook-with-cROUTON>
- Birk, D. (2011). *Technical Challenges of Forensic Investigations in Cloud*. n.d.: Workshop on Cryptography and Security in Clouds.
- Chromebook Help Center*. (2014). Retrieved from Google:  
<https://support.google.com/chromebook/?hl=en#topic=3399709>

- Chromebooks for Education*. (2013). Retrieved October 4, 2014, from Google:  
[https://static.googleusercontent.com/media/www.google.com/en/us/intl/en/chrome/assets/common/files/chromebook\\_overview.pdf](https://static.googleusercontent.com/media/www.google.com/en/us/intl/en/chrome/assets/common/files/chromebook_overview.pdf)
- Cipriani, J. (2014, August 29). *How to enable developer mode on a Chromebook*. Retrieved October 13, 2014, from CNET.com: <http://www.cnet.com/how-to/how-to-enable-developer-mode-on-a-chromebook/>
- ComputerHope.com. (2014). *Flat File*. Retrieved October 14, 2014, from Computer Hope:  
<http://www.computerhope.com/jargon/f/flatfile.htm>
- Dell.com. (2014). *Inspiron 15 7000 series laptop*. Retrieved September 4, 2014, from Dell.com:  
<http://www.dell.com/us/p/inspiron-15-7547-laptop/pd>
- Efrati, A., & Sherr, I. (2011, May 11). *Google Sets Laptop Foray*. Retrieved September 13, 2014, from The Wall Street Journal:  
<http://online.wsj.com/articles/SB10001424052748703730804576317361801753874>
- Fang, K., Hanus, D., & Zheng, Y. (2011, December 16). *Security of Google Chromebook*. Retrieved October 10, 2014, from Deborah Hanus:  
<http://dhanus.mit.edu/docs/ChromeOSSecurity.pdf>
- FTK. (2014). Retrieved from AccessData: <http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk>
- Fournier, E. R. (2014, March 27). *Why Cloud Storage is Growing in Use and Popularity*. Retrieved October 10, 2014, from BPlans.com: <http://articles.bplans.com/why-cloud-storage-is-growing-in-use-and-popularity/>
- Foxton Software. (2014). *ChromeAnalysis Plus*. Retrieved October 3, 2014, from Foxton Software: <http://forensic-software.co.uk/chromeanalysis.aspx>

- FTK Imager*. (2014). Retrieved from AccessData: <http://accessdata.com/product-download/digital-forensics/ftk-imager-version-3.2.0>
- Gallagher, S. (2013, September 11). *Why the NSA loves Google's Chromebook*. Retrieved October 3, 2014, from Ars Technica: <http://arstechnica.com/information-technology/2013/09/why-the-nsa-loves-googles-chromebook/>
- Google Chrome Browser*. (2014). Retrieved from Google: <https://www.google.com/chrome/browser/desktop/index.html>
- Greetham, D. (2013, January 16). *Live Data Acquisition: The New Default Standard for Capturing ESI?* Retrieved from Riscoh Legal USA.
- Hart, S. V., Ashcroft, J., & Daniels, D. J. (2004). *Forensic examination of digital evidence: a guide for law enforcement*. National Institute of Justice. Washington DC: National Institute of Justice NIJ-US, Washington DC, USA, Tech. Rep. NCJ, 199408. Retrieved from <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>
- Hoog, A. (2008, October 17). *Slack Space*. Retrieved October 23, 2014, from Viaforensics Computer Forensics Glossary: <https://viaforensics.com/computer-forensic-ediscovery-glossary/what-is-slack-space.html>
- Hoog, A. (2008, November 11). *Unallocated Space*. Retrieved October 23, 2014, from Viaforensics Computer Forensics Glossary: <https://viaforensics.com/computer-forensic-ediscovery-glossary/what-is-unallocated-space.html>
- Howell, G. (2011, March 9). *Solid State Drives And Forensic Troubles*. Retrieved September 7, 2014, from Wiredpig.us: <http://tech.wiredpig.us/post/12292126487/solid-state-drives-and-forensic-troubles>

- Lardinois, F. (2014, 07 19). *With 1M Sold In The Last Quarter, Google's Chromebooks Are A Hit With Schools*. Retrieved September 12, 2014, from TechCrunch.com:  
<http://techcrunch.com/2014/07/19/with-1m-sold-in-the-last-quarter-googles-chromebooks-are-a-hit-with-schools/>
- Mick, J. (2013, September 12). *IDF 2013: Intel Distances Itself From Windows 8, Microsoft*. Retrieved 10 12, 2014, from Daily Tech:  
<http://www.dailytech.com/IDF+2013+Intel+Distances+Itself+From+Windows+8+Microsoft/article33363.htm>
- Microsoft Word*. (2013). Retrieved from Microsoft Store:  
[http://www.microsoftstore.com/store/msusa/en\\_US/pdp/Word-2013/productID.259323500](http://www.microsoftstore.com/store/msusa/en_US/pdp/Word-2013/productID.259323500)
- Morgan, C. (2013, August 28). *Data storage lifespans: How long will media really last?* Retrieved from StorageCraft: <http://www.storagecraft.com/blog/data-storage-lifespan/>
- Nelson, B., Phillips, A., & Steuart, C. (2010). *Guide to Computer Forensics and Investigations, Fourth Edition*. Boston, MA: Course Technology Cengage Learning.
- Panchal, E. P. (2013). Extraction of Persistence and Volatile Forensics Evidences from Computer System. *International Journal of Computer Trends and Technology (IJCTT) - volume4 Issue5*, 964-968. Retrieved October 23, 2014
- Peterson, D. (2011, June 14). *How do you find the GPS coordinates of your photos?* Retrieved from Digital Photo Secrets: <http://www.digital-photo-secrets.com/tip/1401/how-do-you-find-the-gps-coordinates-of-your-photos/>
- Quick, D., Martini, B., & Choo, K. R. (2014). *Cloud Storage Forensics*. Waltham, MA: Syngress.

- Rogers, M. K., Goldman, J., Mislán, R., Wedge, T., & Debrotá, S. (2006). Computer Forensics Field Triage Process Model. *Journal of Digital Forensics, Security and Law*, 19-37. Retrieved October 12, 2014
- Sammons, J. (2012). *The Basics of Digital Forensics*. Waltham, MA: Syngress. Retrieved October 10, 2014
- Spenneberg, R. (2008, February 9). *Carving tools help you recover deleted files*. Retrieved from Linux Magazine: <http://www.linux-magazine.com/Issues/2008/93/Recovering-Deleted-Files>
- The Microsoft Windows Team. (2003). File Systems. In *Microsoft® Windows® XP Professional Resource Kit, Second Edition* (pp. 547-621). Redmond, WA: Microsoft Press. Retrieved October 23, 2014
- Ubuntu Unity*. (2014). Retrieved from Ubuntu: <https://unity.ubuntu.com/>
- VMware Workstation 10.0*. (2014). Retrieved from VMWare: [https://my.vmware.com/web/vmware/info/slug/desktop\\_end\\_user\\_computing/vmware\\_workstation/10\\_0](https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/10_0)
- Welcome to Gmail*. (2014). Retrieved from Google: <https://www.gmail.com/intl/en/mail/help/about.html>
- Whatis.com. (2014). *Binary File*. Retrieved October 23, 2014, from Whatis.com: <http://whatis.techtarget.com/definition/binary-file>
- Windows XP*. (2014). Retrieved from Microsoft: <http://windows.microsoft.com/en-us/windows/end-support-help>