

## Windows and Android Forensics CCIC Training

Chapter 0: Preamble

Cassidy Elwell and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 0

## **Preparing for the CCIC 2019**

The 2019 California Cyber Innovation Challenge (CCIC) will be hosted by the California Cybersecurity Institute (CCI) on June 21-23. Training is provided for the DFC at <u>https://cci.calpoly.edu/events/ccic/2019-df-downloads</u>.

As part of the DFC, teams will be presented with a case where digital AND physical evidence will have to be collected, verified, analyzed, and a criminal case will have to be assembled on a timeline and presented to a judge. Digital forensics, critical thinking, teamwork and communication skills will all be tested as part of this event.

In preparation of the DFC, it is highly recommended that the DFC training is completed by all team members. The Windows and Android Forensics CCIC Trainings are designed to take an inexperienced high school student about 22-27 hours to complete. However, the trainings can be split amongst team members to be specialized within areas of Windows and Android Forensics resulting in about 6-8 hours per student.

The DFC training serves as a primer - which covers the necessary skills for teams to compete in the challenge. However, there will be portions of the DFC that will NOT be covered by the DFC training, and your team's ability to handle these unexpected challenges will be a part of your team's overall success.

#### What is Digital Forensics and how will it be used in the CCIC 2019?

Digital Forensics is a subset of the field of forensics science and has evolved out of computer forensics as digital devices now not only include computers, but other digital devices. Nearly all modern day crimes now have a digital element. However, there is a large divide between the number of law enforcement officers with formal training in Digital Forensics and the number of crimes with a digital element. The DFC is designed to highlight some of these challenges and we believe serves as an example of how "human" cyber problems can be.

Digital Forensics can be broken down into multiple stages, which include:

- 1. Seizure Focusing on the preservation of evidence to be legally permissible in court
- 2. Acquisition Ensuring evidence is forensically sound (authentic and not tampered with)
- 3. Analysis Identifying the evidence and establishing a timeline for the crime
- 4. Reporting Putting together a concrete case, often for a non-technical audience

#### Seizure

After an introduction of the DFC on June 24th, teams will be issued a blanket warrant for searching allocated space(s) to search and seize digital evidence. Please refer to the Windows and Android Forensics CCIC Trainings on the proper seizure of evidence

#### Acquisition

The acquisition stage of the DFC will be aided by "forensics technicians." Teams that seize a piece of digital evidence will be turning these devices to a "forensic technician" in exchange for a USB drive with a forensics image (creating a forensics image may take several hours). Drive hashes should still be verified upon receipt of the forensics image and once again at the end of the Analysis phase. The Windows and Android Forensics CCIC Trainings will help prepare teams in this regard, but the DFC will provide forensics images to all competitors to avoid long imaging durations.

#### Analysis

Due to the complexity of the field of Digital Forensics, the DFC's evidence will focus mostly on Windows and Android-based forensics and serves as the bulk of the training. Note that there will be some physical evidence and other digital elements as part of the DFC which will require teams to be able to integrate evidence from multiple sources.

#### Reporting

After the Analysis phase, teams will have to make an oral presentation (aided by a presentation slide deck, if desired) to a series of judge advocates. The report should focus on the "Who, What, Where, When, and How" will/did this crime take place, and provide evidence supporting these findings. Additionally, teams will be asked to provide recommendations for remediation - what should be done at the outcome of their findings.

#### **Open-Source Tools for Trainings**

All tools utilized in these training manuals are open-source and therefore available for download through the links provided.

Prior to starting the trainings, you will want to install/have access to the following tools on your PC:

#### Windows Forensics

- 1. <u>Autopsy</u> and/or Sleuthkit
- 2. <u>Registry Explorer</u>
- 3. Ophcrack v 3.7 and Vista Free Table
- 4. Autopsy's Multi Content Viewer 3rd Party Plugin
- 5. <u>DCode v 4.2</u>
- 6. JumpLister v 1.1.0
- 7. <u>USB Historian v 1.3</u>
- 8. <u>SkypeLogView v 1.55</u>
- 9. <u>7Zip v 16.04</u>
- 10. USB Deview

#### **Android Forensics**

- 1. QuickHash GUI
- 2. Google Map Creation
- 3. <u>Thunderbird Mail</u>

Additionally, you may want to download the Windows and Android Forensics CCIC Training manuals and training images located at: <u>http://cci.calpoly.edu/ccic</u>.

**Note:** UFED Reader is a free program provided with the creation of an extraction report and therefore is not an executable which can be downloaded online.

#### **Recommended Training Schedule**

It is recommended that all team members complete all training materials. The following is a recommended training schedule, assuming that team training session are each about 1-2 hours long:

#### Windows Forensics

- Chapters 1-4 Introduction, Starting a Case, Drive Geometry, Image Verification, Registry
- Chapter 5 Windows File Overview
- Chapter 6 Recent Files
- Chapters 7-8 Recycle Bin, External Storage Devices
- Chapter 9 Email
- Chapters 10-11 Internet History, Chat Logs
- Chapter 12 Hidden Data
- Chapter 13 Installed Programs
- Chapter 14 Legality, Reporting
- Appendices, as time allows

#### **Android Forensics**

- Chapters 1-3 Introduction, Secure the Device, Data Extraction with UFED
- Chapters 4-6 Image Verification, UFED Reader Basics, Lock/Home Screens, Personal Files
- Chapters 7-9 Installed Applications, Contacts, Phone, Messaging, Location Data
- Chapter 10-11 Calendar, To-do Lists, Notes, Email, Internet History
- Appendices, as time allows

**Note:** Android Forensics Chapter 3 on Data Extraction with UFED is for your team's knowledge of understanding the mobile forensics process. You will exchange any mobile phone(s) for a USB drive containing a physical data extraction during the competition.

The training manuals will be available to all teams during the competition, but familiarity with the topics in the training manuals will greatly impact your team's performance. It is therefore also recommended immediately prior to the CCIC that individual team members are assigned to "own and review" one or more of Chapters 6-14 of Windows Forensics and Chapters 4-11 of Android Forensics.

#### Questions

If you have any questions about the CCIC, or the CCI in general, please do not hesitate to email us at <u>cci@calpoly.edu</u>.



### **Windows Forensics CCIC Training**

#### Chapter 1: Introduction

Lauren Pixley, Cassidy Elwell, and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 1

## Introduction

During this CCIC Event, there will be a computer forensics challenge where you will have to analyze digital evidence. The documentation provided will help ease you into how to conduct analysis on digital evidence and how to triage a case. You will be provided evidence files with specific case scenarios to work through. The first evidence file this documentation will walk you through is the Craig Tucker case. The following is the scenario for the Craig Tucker case:

#### **Tucker Case Summary**

As part of a normal business practice, Walmart security receives Counterfeit Coupon Alerts from the Coupon Information Corporation. Within the past month, Walmart security has received specific information regarding fraudulent coupons being passed at their store. Using the information they received, they conducted an internal investigation using video surveillance footage in an effort to identify the customers who are engaged in this activity.

One of the suspects was an unknown white, male adult, approximately 28 years old, brown hair, 5' 9", 200 pounds, no facial hair, and no visible tattoos. A photograph of this suspect was circulated to the employees in the store.

On December 22, 2013, Craig Tucker was detained by Walmart security as he matched the description and he had just passed 2 fraudulent coupons for Monster energy drink and Arizona Ice Tea beverages while paying for other items.

Walmart security contacted the Santa Monica Police Department to arrest and prosecute Tucker for theft.

Santa Monica PD Officer Smith interviewed Tucker and he denied knowing the coupons were fraudulent. He claimed to have received the coupons after completing an online survey for students at Santa Monica Community College.

Although Tucker gave consent to the search of his personal computer, a search warrant was obtained to search his computer for evidence as it may be an instrument to committing a crime.

You have been given a forensic image of his hard drive. Based on your review of the search warrant, you are authorized to search for any information or communication associated with the creation, downloading, distribution, and possession of fraudulent consumer coupons.

Craig was caught with the following coupons:



After working through the documentation and the Craig Tucker case, you will be given some questions on the evidence and your findings. As you provide your answers, you will be given feedback as to whether or not you had the correct results and where you can look to find the correct results.

Once you complete the Tucker evidence file, you will be provided two additional evidence files you can use for practice. The Kip and Rico cases have their own case scenarios and you will analyze the evidence the same way you did the Tucker evidence. You will also be given questions on your findings for these practice evidence files and feedback based on your answers.

#### **Documentation Phased Approach**

This documentation is designed for a new forensic examiner to start the analysis of digital evidence using a phased approach. Often new examiners will start with an "everything and the kitchen sink" method, which will lead to a lot of distractions, frustration, and unproductive use of time. This documentation will walk you through how to conduct an investigation, where evidence can potentially be stored, and it will prepare you for the computer forensics challenge during the actual CCIC event.

The phased approach methodology that this documentation follows is based on years of case triage experience. It is designed to keep your analysis focused at a high level and then drill down into targeted areas as needed.

Phase 1 is about setting up the foundation of your case analysis and is broken down into the following sections:

- 1) Create your case
- 2) Verify the forensic image
- 3) Check the drive geometry
- 4) Determine the operating system
- 5) Establish the time zone
- 6) Identify the computers users

Phase 2 is where you will begin to delve deeper into specific areas and it is made up of the following sections:

- 1) Look for the user's personal data
- 2) Examine LNK files and jump lists
- 3) Inspect the recycle bin
- 4) Check for external storage devices
- 5) Review the user's email
- 6) Examine Internet history
- 7) Check for chat logs
- 8) Look for hidden or encrypted data
- 9) Carve data from unallocated space (if necessary)
- 10) Determine installed programs
- 11) Scan for malware



### **Computer Forensics CCIC Training**

#### Chapter 2: Starting Phase 1

Lauren Pixley, Cassidy Elwell, and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

## 2

## **Starting Phase 1**

#### Introduction

When you are first given a forensic image to conduct analysis on, you need to use forensic software and create a case. For this training, you will use Autopsy and other third-party tools. Creating your case while using forensic software like Autopsy is the very first step, and it involves adding your forensic images, setting the case information, and adjusting the time zone for your case. While you search through the evidence in the software, your work will be saved. This allows you to reopen the case later to look through the evidence again if necessary. Therefore, the following are steps you MUST do if you are doing analysis of a **Windows** system. This training does not cover analysis of other systems.

#### **Creating Your Case**

This section assumes you have already properly installed Autopsy on your forensic computer. Start Autopsy and click on Create New Case.



Figure 2-1 – Create New Case

A New Case Information window will open and you need to set the Case Name. Set it to Craig Tucker since that is the first case you are going to work on. Set the Base Directory to where you want your case saved on the computer and then click Next (see Figure 2-2).

Steps	Case Info
<ol> <li>Case Info</li> <li>Additional Information</li> </ol>	Enter New Case Information:
	Case Name: Craig Tucker
	Base Directory: G:\Cases\Tucker Browse
	Case Type:  Single-user Multi-user Case data will be stored in the following directory:
	G:\Cases\Tucker\Craig Tucker

Figure 2-2 – Set Case Name and Base Directory

On the next "New Case Information" window, set a case number and your name. Click Finish.

teps	Additional Info	ormation
. Case Info . Additional Information	Optional: Se	et Case Number and Examiner
	Case Number:	001
	Examiner:	Pixley
		1

Figure 2-3 – Set Case Number and Name

An Add Data Source window will open and you need to select Disk Image or VM File as the data source type. Click on the Browse button and then navigate to the Tucker.E01 file you have downloaded and click Open. For now, set the time zone to (GMT + 0.00) GMT. We will later cover how to determine the time zone that the computer was set to. Leave "Ignore orphan files in FAT file systems" unchecked and then click Finish (see Figure 2-4).

Steps	Select Data Source
Select Data     Source     Configure Ingest     Modules     Add Data Source	Select data source type: Disk Image or VM File
3. Add Data Source	G:\CDER\Final Craig Image\Updated\Tucker.E01 Browse
	Please select the input timezone: (GMT+0:00) GMT
	Ignore orphan files in FAT file systems
	(faster results, although some data will not be searched)
	1

Figure 2-4 – Set Data Source to Disk Image and Navigate to Tucker.E01

On the next Add Data Source window, click the Deselect All button and leave Process Unallocated Space checked. When you are working on a live case, you may not have time to wait for all of these modules to process, and they may not always be helpful with the evidence you are trying to look for. You can always run these modules later during your investigation if necessary as well. Click Next.

Steps	Configure Ingest Modules	
<ol> <li>Select Data Source</li> <li>Configure Ingest Modules</li> <li>Add Data Source</li> </ol>	Recent Activity           Hash Lookup           File Type Identification           Embedded File Extractor           Exif Parser           Keyword Search           Email Parser           Extension Mismatch Detector           E01 Verifier           Android Analyzer           Interesting Files Identifier           PhotoRec Carver           Virtual Machine Extractor	The selected module has no per-ru
	Select All Deselect All	Extracts recent user activity, suc
	View Ingest History View Ingest History Process Unallocated Space	Global Settings

Figure 2-5 – Click Deselect All Button and Click Next

On the last Add Data Source window just click Finish and then wait for Autopsy to finish processing the evidence.



## **Computer Forensics CCIC Training**

Chapter 3: Verification

Lauren Pixley, Cassidy Elwell, and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

## 3

## Verification

#### Introduction

Before you even begin your analysis, you always want to first establish a solid foundation. You generally want to make sure that the forensic image verifies by checking its hash value. A hash value is basically a fingerprint for a file. The chance of two MD5 hash values being the same is  $1/2^{128}$ . By checking the hash value of the forensic image and comparing it to the hash value when it was imaged, you are confirming that the evidence has not been corrupted or tampered with. This becomes a vital piece of information later when you are being questioned on the integrity of the image and if you missed any partitions or data. The hash value should be checked once again after investigation is complete to ensure that you haven't unintentionally changed your evidence.

**Note:** In some simulated images that are created for you, the MD5 hash will not compute. This is due to some technical difficulties in the Virtual Machine that prevent an export with an MD5 computable hash as a .E01 File. This is ok when doing challenges like the CCIC or trainings, but in a real investigation you should always be able to, and should run the MD5 hash verifier. This ensures that your evidence is admissible in court and that the image itself was not tampered with.

#### Verify the Image

After creating a case and having Autopsy open the evidence, you want to have Autopsy verify the forensic image. To verify the image, you need to run the E01 Verifier module. This was one of the modules that you could have run when you first created the case. However, since you did not run any modules at the beginning, you can always click Tools ► Run Ingest Modules ► Tucker.E01. This will allow you to run or rerun any of the modules that were available at the beginning (see Figure 3-1).



Figure 3-1 – Run Ingest Modules

When the Run Ingest Modules window opens, check the E01 Verifier module and then click Start.

Recent Activity Hash Lookup File Type Identification	The selected module has no per-run
Embedded File Extractor Exif Parser Keyword Search Email Parser	
Extension Mismatch Detector	
Android Analyzer Interesting Files Identifier PhotoRec Carver Virtual Machine Extractor	۰ ا
Select All Deselect All	Validates the integrity of E01 files.
View Ingest History	Global Settings

Figure 3-2 – Check E01 Verifier and Click Start

Autopsy will take a few minutes to verify the evidence file. Once it is processed, you can mouse over the drop-down arrow in the top bar and then click on the Ingest Messages button (see Figure 3-3).

Case View Tools Window Help					
🕂 Add Data Source 📠 View Images/Videos 🗮 Timelin	ie 膨 Generate Report 🍙 Close Case 🛛 🕴	👁 - Keywo	rd Lists 🔍 🔍 K	eyword S	
♦ ⇒ Show Rejected Result	s Directory Listing	a			
Data Sources		est Messag	Messages 3 Result		
🖶 🔳 Tucker.E01	Table Thumbnail	ID	CI 11 C 1		
Views	Name	ID	Starting Sector	Length in Se	
Results	vol1 (Unallocated: 0-2047)	1	0	2048	
Extracted Content	wol2 (NTFS / exFAT (0x07): 2048-1258	<b>2707</b> 2	2048	125825024	
Single Literal Keyword Search (0)	wol3 (Unallocated: 125827072-1258291	.19) 3	125827072	2048	
Single Regular Expression Search (0)      Aasheet Hits      E-Mail Messages      ★ Interesting Items	٠ ا			,	
★ Hashset Hits		d Text Me	dia		
<ul> <li>➡ Hashset Hits</li> <li>➡ Set Hits</li> <li>➡ Set Hits</li> <li>➡ Interesting Items</li> </ul>	✓     III       Hex     Strings       File     Metadata       Results     Indexe       Pa     1       of     3932032       P     €	d Text Med Go to Pa		) Jump to Offs	

Figure 3-3 – Mouse over Drop-Down Arrow and Click Ingest Messages

There should be two entries in the Module list. One will say Starting Tucker.E01 and the other will say Tucker.E01 Verified. Click on Tucker.E01 verified in the Ingest Messages list, and Autopsy will show you the results that the Tucker.E01 verified and its calculated hash value matches the stored hash value. This means that the forensic image you have is the same and has not been corrupted or changed since it was first imaged.



Figure 3-4 – Tucker.E01 Verified



### **Computer Forensics CCIC Training** Chapter 4: Understanding the Registry

Lauren Pixley, Cassidy Elwell, and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

## 4

## **Understanding the Registry**

#### Introduction

As you are going through your investigation, you will need to know basic information about the forensic image you are searching. To find out more about the image you are analyzing, you will need to look through the Windows Registry. The Windows Registry is basically a database that stores thousands of records with information, such as the operating system, time zone, user settings, user accounts, external storage devices, and some program data.

When you look through the Windows Registry in the next section with REGEDIT, it may appear as though the registry is one large storage location. However, there are several files where the information is being stored throughout the computer. REGEDIT simply takes these files and records stored in different locations and displays them for you. There are many records in the Windows Registry that will have no forensic value to you as an examiner, but there are some pieces of information that you will find useful. This chapter will walk you through the basic structure of the registry and where you need to look to find information that is valuable to your investigation.

#### REGEDIT

In this section, you will start with the Windows registry utility known as REGEDIT.exe. You can open this by pressing the Windows key+R and then typing in "REGEDIT". You can also click on the Start menu and type "REGEDIT" in the Search box.

**Note**: REGEDIT.exe displays your computer's registry. You should not make any adjustments to your registry unless you know what the change will do to your computer.

When conducting a forensic examination of a target hard drive, you will not see the same subtrees displayed in REGEDIT. However, most information you come across on the Internet will be notated in a format that assumes you are using REGEDIT. For example, you may find information showing you the location for a user's home page setting for Internet Explorer written as:

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

However, if you received information from another examiner, he may have written it as:

SYSTEM Hive: [CurrentControlSet]\Control\TimeZoneInformation

Both of these locations are exactly the same; it just depends on how you are viewing them.

It is a good idea to start using proper terminology so there is no confusion when you are documenting your findings. The first terms you need to become familiar with are subtree, key, subkey, hive, and value.

Type REG_SZ REG_DWORD	Data (value not set)
REG_DWORD REG_DWORD mGood REG_DWORD	0x00000001 (1)
	value
v:	y: Select

Figure 4-1 – Windows Registry Terms

#### Subtrees, Keys, and Subkeys

There are 5 *subtrees* that make up the Windows registry. The following list contains each subtree, the standard abbreviation, and the type of information found within each subtree:

Subtree	Abbreviation	Description
HKEY_CLASSES_ROOT	HKCR	Contains information about file extension associations and the Object Linking and Embedding (OLE) database.
HKEY_CURRENT_USER	HKCU	Contains user information, preferences, and settings for the user that is currently logged on (in this case, you will see your settings).
HKEY_LOCAL_MACHINE	HKLM	Contains computer-specific information, such as software, hardware, and security.
HKEY_USERS	HKU	Contains user information from the user currently logged in, the default profile, and system accounts.
HKEY_CURRENT_CONFIG	НКСС	Created during the boot process and contains information associated with the hardware configuration.

Below the HKEY\_LOCAL\_MACHINE *subtree*, there are five *keys*, which are also called *hives*. Below each *key*, such as SYSTEM, there are *subkeys*, such as Select.

#### Hives

The Windows registry has several system files called hives, with each hive being mapped to a single file. The HKEY\_LOCAL\_MACHINE (HKLM) subtree contains settings that apply to the local computer's configuration and affect each user that logs on. There are four main hives that are associated with HKLM, and the list below displays the name of each hive and the actual filename associated with that hive:

Hives	Location of Hives
HKEY_LOCAL_MACHINE\SYSTEM	C:\Windows\system32\config\SYSTEM
HKEY_LOCAL_MACHINE\SOFTWARE	$C:\Windows\system 32\config\SOFTWARE$
HKEY_LOCAL_MACHINE\SECURITY	C:\Windows\system32\config\SECURITY
HKEY_LOCAL_MACHINE\SAM	C:\Windows\system32\config\SAM

**Note:** Backups of the hives are located in C:\Windows\system32\config\regback. Look at the Modified dates of those files to determine if they may contain old information that could be useful to your investigation.

With REGEDIT, you will see a key called HARDWARE. However, there is not a system file that matches this key. The key is volatile in memory, so you will not be able to see it during your analysis. It contains information about the hardware devices that were detected during the boot process.

#### Values

You need to be familiar with the terms *value name*, *value data*, and *value type*. Each subkey in the registry contains at least one or more values. In Figure 4-1, there is a *value name* of LastKnownGood and its *value data* is 2. The registry also contains different types of data, which is referred to as a *value type*. Here is a list of values types:

Value Type	Description
REG_NONE	No defined value type.
REG_SZ	Null-terminated string that will be either ANSI or Unicode.
REG_EXPAND_SZ	Null-terminated string that contains references to environment variables.
REG_BINARY	This is binary data and it's displayed in hexadecimal notation.
REG_DWORD	A 32-bit number. The values stored are sometimes used as Boolean flags ( $00 = disabled$ ; $01 = enabled$ ).
REG_DWORD_BIG_ENDIAN	This is a double-word value stored as big endian (most significant byte first).
REG_MULTI_SZ	Array of null-terminated strings, terminated by two null characters.
REG_QWORD	A 64-bit number.

As you look at values stored in the registry, remember that an application can store data in different ways and the interpretation is up to the program. Never assume a value means something unless you have confirmed the setting. For example, you may see a value of 0 and assume that means disabled; however, the programmer might have used the value of 0 to mean not disabled (therefore it is enabled).

#### **User Profiles**

On Windows 7 and 8 computers, the user profile is stored in a separate folder for each user under C:\Users\[username]. Each user profile folder contains a profile hive, which is a system file called NTUSER.DAT.

When a user is logged in, the user's NTUSER.DAT file is mapped to the following two subtrees:

HKEY\_CURRENT\_USER

HKEY\_USERS

Under the HKEY\_USERS subtree, there are some additional profile hives, which are listed below:

HKU\S-1-5-18	Local System (same as .DEFAULT)
HKU\S-1-5-19	LocalService NTUSER.DAT
HKU\S-1-5-20	NetworkService NTUSER.DAT



Figure 4-2 – User Profiles in Registry

#### Security Identifiers (SID)

Under HKEY\_USERS, you will see *Security Identifiers* (SID), which is part of Windows security. Windows uses a concept referred to as a *security principle*, which would include items such as computer accounts, user accounts, user groups, and other security-related objects.

On a local computer, the *Local Security Authority* (LSA) generates a SID for local security principles and then stores them in the local security database.

In Figure 4-3, you can see a SID of S-1-5-21-674973493-240844686-639060511-1002, which can be broken down into the following components:

[S]-[version]-[identifier authority]-[domain identifier]-[relative identifier]

The first 3 characters of a SID consist of:

- S: A SID always begins with S
- 1: SID version
- 5: Identifier authority (5 is NT authority)

The following string of numbers (21-674973493-240844686-639060511) is the domain identifier.

The last 4 bytes of the SID is a *relative identifier* (RID), which is the account or group. Some of the common RIDs are:

500 Administrator

501 Guest

1000+ User Accounts

Microsoft lists well-known security identifiers on their website:

http://support.microsoft.com/kb/q243330

#### **Operating System**

Now that you have a good understanding of Windows time stamps and the registry, you can check the suspect's operating system. This is an important step before you begin your analysis, because you need to know what type of artifacts you are going to find and where they are located. Where are the user's documents or recent folder located? How is data being stored? If the suspect deleted something, can it be recovered? All of these questions and many others start to become easier to answer once you know what operating system the suspect was using.

The operating system information is stored in the SOFTWARE hive. This is located in:

```
C:\Windows\System32\config
```

**Note:** This current version of Autopsy (4.3) has issues opening the System32 folder since there is a large amount of data in it.

To view the time zone information stored in the SOFTWARE hive, you need to run another built-in module. Click Tools ► Run Ingest Modules ► Tucker.E01. When the Run Ingest Modules window opens, check Recent Activity and then click Start.



Figure 4-3 – Check Recent Activity Module and Click Start

The Recent Activity module will pull web browser history data and important registry information so you do not have to manually find the data. However, it is still important to know where this information is being pulled from so you could manually find and verify the results if necessary. We will further cover where this data is stored in the registry as we view the results.

Once the Recent Activity module finishes running, you can click on Results ► Extracted Content ► Operating System Information. The last entry in the table pane shows that the operating system is Windows 8.1 Pro. It also shows that the owner of the computer is simply just Windows User (see Figure 4-4). This information has been extracted from the SOFTWARE hive and is stored under the following subkey:

```
Microsoft\Windows NT\Current Version
```

		-			·				
🕂 Add Data Source 📠 Images/Videos 📓 Commu	inicatio	ins 🧮 Tim	eline 🎖			O ▼ Keyword List	ts Q <sub>e</sub> Ke	yword Search	h
€ →	¢	Listing							
🛄 🗄 🖳 Windows (106)	•		stem Informatio	n				2 Re	esults
vol4 (Unallocated: 41940992-41943039)		Table Thu	umbnail						
···· · Views		Source File			P	rogram Name	Date/Time		Pat
E Results		SYSTE	м						
🖶 🔄 Extracted Content			VARE			indows 10 Education	2019-04-25 06:2	26:38 PDT	C://
Devices Attached (15)									
Operating System Information (2)									
- 🦂 Operating System User Account (4)									
Recent Documents (24)									
Web Bookmarks (1)	÷.	<							>
Web Bookmarks (1) Web Cookies (253)	l	< Hex	Strir	nas	Appl	cation	Indexed	Text	>
Web Bookmarks (1) Web Cookies (253) Web Downloads (5)	l	_	Strir	ngs letadata	Appl Results	cation Annotations		Text ccurrences	>
	l	Hex	E File N	letadata		Annotations		ccurrences	>
	l	Hex Message	e File N of 53	letadata	Results	Annotations	Other O	ccurrences ion	
Web Bookmarks (1) Web Cookies (253) Web Downloads (5) Web History (255) Web Search (166) Keyword Hits	l	Hex Message	E File N	letadata	Results	Annotations	Other O	ccurrences	
Web Bookmarks (1)     Web Cookies (253)     Web Downloads (5)     Web Bostrory (255)     Web Bistory (255)     Web Search (166)     Keyword Hits     ⊕-    Single Literal Keyword Search (0)		Hex Message Result: 1 Type	e File N of 53	letadata Result	Results	Annotations	Other O	ccurrences ion	
Web Bookmarks (1) Web Cookies (253) Web Downloads (5) Web History (255) Web Search (166) Keyword Hits		Hex Message Result: 1 Type Program N	of 53 Value	Result	Results	Annotations	Other O	courrences ion Source(s)	ti A
Web Bookmarks (1)           Web Cookies (253)           Web Downloads (5)           Web Boardh (15)           Web Bearch (166)           Keyword Hits           B-         Single Literal Keyword Search (0)           B-         Single Regular Expression Search (0)		Hex Message Result: 1 Type Program N	of 53 Value Windows 10 Edu	Result	Results	Annotations	Other O	courrences ion Source(s) RecentAct	ti A
Web Bookmarks (1)     Web Cookies (253)     Web Downloads (5)     Web History (255)     Web Search (166)     Keyword Hits     Single Literal Keyword Search (0)     Single Regular Expression Search (0)     Hashset Hits		Hex Messag Result: 1 Type Program N Date/Time Path	File N           of 53           Value           Windows 10 Edu           2019-04-25 06:	Result cation 26:38	Results	Annotations	Other O	Source(s) RecentAct	ti A
Web Bookmarks (1)     Web Cookies (253)     Web Downloads (5)     Web History (255)     Web Search (166)     Keyword Hits     Single Literal Keyword Search (0)     Single Regular Expression Search (0)     Hashset Hits     E-Mail Messages		Hex Messagy Result: 1 Type Program N Date/Time Path Product ID	Value Value Windows 10 Edu 2019-04-25 06: C:\Windows	Result cation 26:38	Results	Annotations	Other O	Source(s) RecentAct RecentAct RecentAct	ti A
Web Bookmarks (1)     Web Cookies (253)     Web Downloads (5)     Web History (255)     Web Search (166)     Single Literal Keyword Search (0)     Single Regular Expression Search (0)     Hashset Hits     E-Mail Messages     Interesting Items		Hex Messagy Result: 1 Type Program N Date/Time Path Product ID	File N           of 53           Value           Windows 10 Edu           2019-04-25 06::           C:\Windows           00328-00259-56	Result cation 26:38	Results	Annotations	Other O	Source(s) RecentAct RecentAct RecentAct	

Figure 4-4 – Operating System Information Extracted from SOFTWARE Hive

**Note:** There is another SOFTWARE entry in the table pane because there are backups for each registry hive.

#### **Registry Explorer**

The information that Autopys extracts from the SYSTEM hive is useful, but it is very limited. If you want to further explore the user's registry and find more information, you will need to use another tool. For this case, we are going to use the tool called Registry Explorer. You can download it from:

```
https://ericzimmerman.github.io/
```

To use the tool, you will need to extract the registry hives from Autopsy. First, you need to right-click SOFTWARE in the table pane and select



Figure 4-5 – Right-Click SOFTWARE Hive in Table Pane and Select View Source File in Directory

This will take you to the config folder where the registry hives are stored. You will want to export out the SOFTWARE, SYSTEM, and SAM hive from the config folder. To do this, click the first hive then press the Control key while clicking on the other hives. This will highlight all three files. Right-click one of the hives in the table pane and select Extract File(s) (see Figure 4-6).

	Tools Window Help	eline 🕞 Conord	h ti A i a tri tutt	0 4 1 1 0
	ita Source 📠 View Images/Videos 🗮 Tim	enne 📠 Genera	• Keyword Lists	Q- Keyword S
- →	Show Rejected Resu	ts Directory L		
	System32 (6919)		r.E01,vol_vol2/Windows/System3	32/config 56 Resu
	- 3 0409 (2)	Table Thu	mbnail	
	- AdvancedInstallers (10)	Name		Created Time
	- 🤑 AppLocker (2)	SAM		2013-08-22 13:2
	- 🥦 ar-SA (19)	SAM.LO	DG1	2013-08-22 13:2
	→ → bg-BG (14)	SAM.LC	DG2	2013-08-22 13:2
	- Bthprops (4)		ITY	2013-08-22 13:2
	$\blacksquare$ $\blacksquare$ catroot (4)	SECUR	ITY.LOG	2013-08-22 13:2
	⊕ 🔋 catroot2 (26)	SECUR	ITY.LOG1	2013-08-22 13:2
	- 🔑 CodeIntegrity (6)	SECUR	ITY.LOG2	2013-08-22 13:2
	⊕	SOFTW	ARE	2013-08-22 13:2
	□ □ □ config (56) □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	SOFTW	/ARE.LOG	2013-08-22 13:2
	RegBack (17)	SOFTW	/ARE.LOG1	2013-08-22 13:2
		SOFTW	/ARE.LOG2	2013-08-22 13:2
		SYSTE	M	2013-08-22 13:2
	Configuration (5)	SYSTE	M Properties	013-08-22 13:2
	🔑 cs-CZ (20) 退 da-DK (20)	۰ III	Extract File(s)	•
	- B de-DE (19)	Hex String		t Media
			Tag Files	•
	- 📜 downlevel (192)		Add files to hash databa	
	🕀 🔑 drivers (627)	•	Add mes to hash databa	se r

Figure 4-6 – Highlight SAM, SOFTWARE, and SYSTEM, Right-Click One and Select Extract File(s)

A Save window will open, and you need to create a folder to export the registry hives to. Once you have an export folder, click Save.

**Note:** Sometimes when Autopsy exports these registry hives, they attach a number to the name. Some tools may not recognize or open these renamed files. If Autopsy does attach a number to the SAM, SYSTEM, or SOFTWARE hive name in the export folder, you will need to navigate to your case export folder and then right-click on each hive and select Rename. Rename each one to their exact name without the numbers.

Once you have the registry hives exported, open the Registry Explorer tool and click File►Load Offline Hive.

🎁 Re	egistry Ex	cplorer v0.8	.1.0							•	•	x
File	Tools	Options	Bookn	hark	s (0/0)	Vie	w H	elp				
	Load o	ffline <mark>h</mark> ive	Alt+1	-	arks ((	)/0)			Values	;		
B	Export	'Registry h	nives'	F	ues		L	D	rag a	colum	n heade	er her
-	Exit				-				٧	V	Data	Va
-				_				۴				
	Key:	None				Valu	ne:	Nor	ne	Collap	ose all	hives

Figure 4-7 – Load Offline Hive in Registry Explorer

Navigate to where you exported the registry hives and select SOFTWARE hive to open. Once the tool opens the SOFTWARE hive, you need to go to the following subkey:

```
Microsoft\Windows NT\Current Version
```

Registry hiv	res (1) Available bookmarks (10	6/0)			Values				
Key name		Last write timestamp		D	rag a column header he	ere to group by that colum	1		
			*		Value Name	Data			
- E	WIMMount	2013-08-22 15:37:08							
Þ 🚞	Windows	2013-08-22 15:37:08			Custom Datat	Culture dance	-	_	-
D 🚞	Windows Defender	2013-12-30 03:56:29			SystemRoot	C:\Windows		•••	
=	Windows Desktop Search	2013-08-22 15:37:09			SoftwareType	System		••	
Þ	Windows Embedded	2013-08-22 19:11:29			RegisteredOwner	Windows User			
D 🚞	Windows Mail	2013-08-22 15:37:09			InstallDate	1387303892			
Þ	Windows Media Device Manager	2013-08-22 15:37:08			CurrentVersion	6.3			
D 🚞	Windows Media Foundation	2013-08-22 15:37:08			CurrentBuild	9600		•••	
D 🚞	Windows Media Player NSS	2013-08-22 15:37:08			RegisteredOrganiza				
Þ 🧰	Windows Messaging Subsystem	2013-08-22 15:37:08			CurrentType	Multiprocessor Free			
4 🚞	Windows NT	2013-08-22 13:25:43			InstallationType	Client			
Þ	CurrentVersion	2013-12-30 03:56:46			EditionID	Professional			
D 🚞	Windows Photo Viewer	2013-08-22 15:37:08		,	ProductName	Windows 8.1 Pro			
D 🧮	Windows Portable Devices	2013-08-22 15:37:09			ProductId	00260-00151-37227			
D 🚞	Windows Script Host	2013-08-22 15:37:09		-	DigitalProductId	A4-00-00-00-03-00-0			
۵ 🗖	Windows Search	2013-12-17 18:17:40	. •	L		A4-00-00-00-03-00-0			-
Key:	Microsoft\Windows NT\Curr	ant/arcing			Value: Pr	oductName Collapse	-11		

Figure 4-8 – Operating System in SOFTWARE

#### **Time Zone**

While Autopsy already pulled the operating system information with its module, there is some information in the registry that it does not pull. To find the time zone information in the registry, you will need to look at the SYSTEM hive. Open up the SYSTEM hive with Registry Explorer.

File	Tools Optic	ons Bookmarks (26/0) Vie	w Help		
Reg	gistry hives (2)	Available bookmarks (42/0)			
Ke	ey na <mark>m</mark> e			•	
٩					
4	E:\Cases\Ci	raig Tucker\Craig Tucker\E	cport\SOFTWARE		
	🛚 🚞 CsiTool-Cre	eateHive-{00000000-0000-0000-	-0000-0000000000		
	Second Associated	deleted records			
	🛚 🚾 Unassociate	ed deleted records			
-	E:\Cases\C	raig Tucker\Craig Tucker\E>	(port\SYSTEM		
	🛚 🚞 CsiTool-Cre	eateHive-{00000000-0000-0000	-0000-0000000000		
	🖻 🙀 Associated	deleted records			
	Da Unassociate	d deleted records			

Figure 4-9 – Open SYSTEM Hive in Registry Explorer

**Note:** When navigating through Registry Explorer and the subkeys, always look under the top key "CsiTool-CreateHive". From there, navigate to the subkey path you are directed to.

Once you have the SYSTEM hive opened, navigate to the following subkey:

[CurrentControlSet]\Control\TimeZoneInformation

You will notice a subkey called ControlSet001. In other images, you may see two or more subkeys with the name ControlSet, such as ControlSet002 and ControlSet003.

If there are multiple control sets in SYSTEM, then you need to know which one is current. You can navigate to the Select subkey and it will show you a value for the current control set. In this case, it is showing 1 as the current control set.

File Tools Options Bookmarks (26/0) View Help							
Registry hives (2) Available bookmarks (42/0)			1	/alues			
Key name	•	•	Dr	ag a column head	ler here	to group b	y that co
9				Value Name	Data		Val
E:\Cases\Craig Tucker\Craig Tucker\Export\SOFTWARE	e),		ę				
▷ 📻 CsiTool-CreateHive-{00000000-0000-0000-0000-000000000	•	•	,	Current	1	_	Re
Associated deleted records		•	1000	Default	1		Re
Unassociated deleted records		•	-	Failed	0		Re
E:\Cases\Craig Tucker\Craig Tucker\Export\SYSTEM	•			LastKnownGood			Re
▲ CsiTool-CreateHive-{0000000-0000-0000-0000-000000000		•	-	Lastkilowildoou	1		Re
ControlSet001		•					
▷		•					
E HardwareConfig MountedDevices		-					
RNG	•						
Select							
▶ ► Setup	•						
▶ = WPA							
▷ Associated deleted records							
Unassociated deleted records		•					
		_		Law Law		n	
Kev: Select				Value: Cu	irrent	Collapse	all hive

Figure 4-10 - Current Control Set in SYSTEM

Now that you know the current control set, navigate to:

ControlSet001\Control\TimeZoneInformation

Under TimeZoneInformation there are two important values to look at. The first value is the TimeZoneKeyName, and Registry Explorer decodes the value data to plain text. The other value is ActiveTimeBias, and it shows how many minutes the system is off from UTC. For this computer, it's 480 minutes off from UTC. If you divide that by 60, you get 8 hours, which is the Pacific Standard Time Zone (see Figure 4-11).

Key name       Image	Registry hives (	2) Available bookmarks	(42/0	)	Values			
Image       Image <td< td=""><td>Key name</td><td></td><td></td><td></td><td>)rag a column header here to gro</td><td>oup by that column</td><td></td><td>-</td></td<>	Key name				)rag a column header here to gro	oup by that column		-
Image       Image <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>								
SrpExtensionConfig .   StillImage .   StillImage .   Storage .   StorageManagement .   StorPort .   StorPort .   StorPort .   TabletPC .   Terminal Server .   Ubpm .   Usbflags .   VAN .	Þ 💳 S	Srp				Dutu		•••
Stillinage   Storage   StorageManagement   StorPort   StorPort   StorPort   StorPort   StorPort   StorPort   StorBetPC   TabletPC   TabletPC   Terminal Server   Ubpm   Ubpm   Ubpm   StorPort   StorAgeManagement   StandardStart   DoubleCouplightStart   DoubleCouplightTimeDisabled   O   ActiveTimeBias   480	<b>=</b> 9	SrpExtensionConfig				100 10 500 5	+	-
Storage          StorageManagement          StorPort          Bias       480         DaylightStart       00-00-03-00-02-00-02-00-0         TimeZoneKeyName       Pacific Standard Time          DynamicDaylightTimeDisabled       0         ActiveTimeBias       480	Þ 🚞 9	StillImage					•	•••
StorageManagement .   StorageManagement .   StorageManagement .   StorPort .   StorPort .   SystemResources .   TabletPC .   Terminal Server .   Terminal Server .   Ubpm .   VAN .	Þ 💳 9	Storage						•••
Support       -         SystemResources       -         TabletPC       -         Terminal Server       -         TimeZoneInformation       -         TimeZoneInformation       -         Support       -         Ubpm       -         Support       -         StandardName       @tzres.dll,-212         Bias       480         DaylightStart       00-00-03-00-02-00-02-00-0         TimeZoneKeyName       Pacific Standard Time          DynamicDaylightTimeDisabled       0         ActiveTimeBias       480	2 💳 د	StorageManagement			StandardStart	00-00-0B-00-01-00-02-00-0		
Bias 480   Construction Construction   Construction	<b>=</b> 9	StorPort			StandardBias	0		
Image: Server       Image: Server<	Þ 💳 S	SystemResources			StandardName	@tzres.dll,-212		
TimeZoneInformation       -         Webpm       -         Webpm<	D 🚞 T	TabletPC			Bias	480		
Ubpm       -         Image: State of the st	D 🚞 1	Ferminal Server			DaylightStart	00-00-03-00-02-00-02-00-0		
Image: Strained of Strain	6	TimeZoneInformation		-	TimeZoneKeyName	Pacific Standard Time 🛛 🕇 🗕	٦.	
Active ninebias 400 .	🚞 l	Jbpm			DynamicDaylightTimeDisabled	0		
Image: Constraint of the second se	Þ 🧮 (	ısb		. E	ActiveTimeBias	480		
	۵ 🚞 ۱	usbflags						
	۵ 🚞 ۱	usbstor	•					
Video -	Þ 🚞 V	/AN						
	Þ 🧰	/ideo		. •				

Figure 4-11 - TimeZoneInformation Subkey in SYSTEM

#### **Identify Computer Users**

The next section you will want to focus on when looking at registry data is identifying the computer users.

Understanding who was using the computer is a key part of your analysis. If your suspect was the only one that had access to the computer, then it makes it much easier to tie that person back to any activity on the computer. However, if other people were using it, you need to know who had access to what and which user account you need to focus on.

To view the user account information, select on Results ► Extracted Content ► Operating System User Account. There are several users listed, but if you remember from the User Profiles section, most of these are default accounts and default security identifiers (SIDs). In this case, there is only one user account, which is Craig. This user account has a SID of "S-1-5-21-1049150138-4017234595-3791460656-1001" and the RID is "1001" (see Figure 4-12).

Case <u>V</u> iew <u>T</u> ools <u>W</u> indow <u>H</u> elp			i . @:					
🕂 Add Data Source 🜆 View Images/Videos 🗧	Timeline 📗 Ger	erate Report ×	🛕 🖲 🗣 Keyword Lists	থ <del>ন</del> Keyword S				
♦ → Show Rejected Results	Directory Listing Operating System	User Account		8 Resul				
B Data Sources	Table Thumbna	1						
E esults	Source File	Username	User ID					
Extracted Content	<b>SOFTWARE</b>	systemprofile	S-1-5-18					
Devices Attached (28)	SOFTWARE		S-1-5-19					
Installed Programs (64)	SOFTWARE	NetworkService	S-1-5-20					
<ul> <li>Operating System Information (4)</li> <li>Operating System User Account (8)</li> </ul>	SOFTWARE	Craig	S-1-5-21-1049150138-40172345	95-3791460656-100				
<ul> <li>Recent Documents (48)</li> </ul>	SOFTWARE	systemprofile	S-1-5-18					
Web Bookmarks (1)	SOFTWARE	LocalService	S-1-5-19					
- 🚳 Web Cookies (321)	SOFTWARE	NetworkService	S-1-5-20					
Web Downloads (8)	SOFTWARE	Craig	S-1-5-21-1049150138-40172345	95-3791460656-10				
<ul> <li>— <sup>™</sup> Web History (194)</li> <li>— <sup>™</sup> Web Search (17)</li> </ul>	4	Ш						
	Hex Strings File	Metadata Result	s Indexed Text Media					
- 🛬 Hashset Hits	Name		01 vol vol2/Windows/System32/config/S					
E-Mail Messages	Туре	File System	onvor_voiz/vvindows/systemsz/coring/s	SOFTWARE				
-* Interesting Items Accounts	MIME Type	null						
	Size	43778048						
Reports	File Name Allocation Allocated							
	Metadata Allocatio	n Allocated						
	Modified	2013-12-30 04	:04:14 GMT					

Figure 4-12 – User Account Information Extracted from SOFTWARE Hive

Note: There are duplicate entries for the user accounts because there are backups for each registry hive.

To find more information that Autopsy does not extract from the registry on users, look at the SOFTWARE hive in Registry Explorer. You need to navigate to the following subkey:

Microsoft\Windows NT\CurrentVersion\ProfileList

Under the ProfileList, there are four subkeys. The names of these four subkeys are the SIDs. The first three SIDs are defaults, and the last one is the user (see Figure 4-13).
ile <u>T</u> ools <u>O</u> p	tions Bookmarks (16,	/0) <u>V</u> iew <u>H</u> elp			
Registry hives (2)	Available bookmarks	(42/0)			
Key name			L		
۹					
D 🧰 1	PeerDist		2	0	
D 🚞 I	PeerNet		2	0	
D 🚞 I	Perflib		2	5	
Þ 🚞 I	PerHwIdStorage		2	0	
	Ports		2	11	
	Prefetcher		2	3	
Þ	Print		2	1	
• 4 🔚	ProfileList		2	4	
	S-1-5-18 Local Syste	em	2	5	
	S-1-5-19 Local Servi	ce	2	3	
	S-1-5-20 Network Se	ervice	2	3	
6	S-1-5-21-1049150138-4	4017234595-3791460656-1001	2	10	100
	ProfileLoader	X	2	0	E
Þ 🧮	ProfileNotification	User	2	6	
	elated.desc		2	1	
<b>1</b>	RemoteRegistry		2	1	-

Figure 4-13 - User Profiles in SOFTWARE

In this case, there is only one user account with a SID of "S-1-5-21-1049150138-4017234595-3791460656-1001" and the RID is "1001". You can easily identify this profile to the user account called Craig by looking at the ProfileImagePath value.

File Tools Options Bookmarks (16/0) View	Help					×
Registry hives (2) Available bookmarks (42/0)				Values		
Key name			D	rag a column heade	r here to group by tha	t colu
۹		*		Value Name	Data	
PeerDist			9	Value Hume	Dutu	
PeerNet			-	D. Clater Dall	Chillen I Contra d	1
🖻 🚞 Perflib			'	ProfileImagePath	C:\Users\Craig 🔫	<b>.</b>
PerHwIdStorage			H	Flags	0	
E Ports				State	0	
Prefetcher				Sid	01-05-00-00-00-0	
Print				ProfileAttempte	0	
⊿ 🚍 ProfileList				ProfileAttempte	0	
😑 S-1-5-18				ProfileLoadTim	0	
😑 S-1-5-19				ProfileLoadTim	0	
😑 S-1-5-20				RefCount	0	
> S-1-5-21-1049150138-4017234	595-3791460656-1001		F	RunLogonScript	0	
ProfileLoader		E				
ProfileNotification			Ŀ			
🚞 related.desc			Ŀ			
C RemoteRegistry		•				
Key: Microsoft\Windows NT\CurrentVersi	on\ProfileList\S-1-5-21-104915	1	/alu	e: ProfileImage	Path Collapse all	hives
Last write: 2013-12-30 04:04:08 +00:00 10 c	of 10 values shown (100.00 %)	Lo	ad	complete	Hidden keys: 0 51	

Figure 4-14 - User Craig's SID

The next place you can look at user accounts is the SAM hive. This hive is the Security Account Manager (SAM). You already exported this hive from Autopsy, so go ahead and open the hive in Registry Explorer. Go to the following subkey of the SAM hive:

```
SAM\Domains\Account\Users
```

Under the Users subkey, there are 3 subkeys listed. These subkeys are the hex values of the user's relative identifier (RID). If you were to convert these hex values to decimal, they would decode as the following:

000001F4 = 500000001F5 = 501

000003E9 = 1001



Figure 4-15 - User Profiles in SAM Hive

Since you already know that the actual user account, Craig, has a RID of 1001, select the 000003E9 subkey. This subkey stores a lot of information about the user account Craig. Information such as if the user account is disabled, how many times they logged in, and if the account has a password is mostly embedded within the values named F and V

### **Login Password**

When a user sets a login password in Windows, the password is not stored in clear text. A hash value of the password is stored within the SAM hive in the V value.

From a security standpoint, Microsoft did not just store a hash value of the user's password. As an added security measure to secure the NTLM hashes, the hash values are protected with Syskey. Syskey is basically an encryption key that is scattered throughout the SYSTEM hive, which is unique to a given system AND user.



Figure 4-16 - Password Hash Value is Encrypted with Syskey

When a user types his password at the login prompt, the password is then hashed and compared against the stored hash in V. If the hash values match, then the user will successfully login to the operating system.

You can attempt to break the user's password by using a freeware tool called Ophcrack. This tool will also help determine which user accounts are password protected. The newest version of this tool (3.7) can be downloaded from:

```
http://ophcrack.sourceforge.net
```

To use Ophcrack and attempt to break the user's login password, you need to first export out the SAM and SYSTEM hives. Ophcrack uses the encrypted NTLMv2 hash value from the SAM hive and Syskey from the SYSTEM hive to reveal the actual NTLMv2 hash value. Once you have an actual hash value, Ophcrack will compare it to a rainbow table to find the password.

**Note:** A rainbow table is a pre-calculated dictionary full of hash values. Each hash value matches a password combination. Ophcrack uses the tables to compare the hash value stored in SAM, and tells you the password that matches the hash value.

You will also need to download the Vista free rainbow table from Ophcrack's website under the Tables tab (see Figure 4-17).





Open the Ophcrack tool and click Load ► Encrypted SAM.

ophcrack						
Load, Dele	ete Save-	-	💸 🕜 rack Help	Exit		OS About
Single ha PWDUM		25				
Session f	ile	sh	LM Pwd 1	LM Pwd 2	NT Pwd	
Encrypte	d SAM 🔫	_				
Local SA	M with samd	ump2				
Table	Status	Preload		Prog	gress	

Figure 4-18 – Click Load Encrypted SAM in Ophcrack

Ophcrack will open a window for you to navigate to your case export folder. Highlight the Export folder and click Select Folder (see Figure 4-19).

**Note:** Make sure you took out the numbers in the SYSTEM and SAM hive and renamed them to just SYSTEM and SAM. Ophcrack will not recognize the files if they have numbers in the name.

Select the directory contain	ning the encrypted SAM and SYSTEM	files.(Usually under C:\WINDOWS\syste	×
Correction Cases Cases C	raig Tucker 🕨 Craig Tucker 🕨	🔻 🍫 🛛 Search Craig Tuck	er P
Organize • New folde	er		?
🜛 Music 🔺	Name	Date modified	Тур
Pictures Videos	📙 Cache	4/10/2017 3:34 PM	File
- VIGCOS	🝌 Export	4/10/2017 5:01 PM	File
🔩 Homegroup	Log	4/10/2017 4:10 PM	File
Nonegroup	👃 ModuleOutput	4/10/2017 3:40 PM	File
	📙 Reports	4/10/2017 3:34 PM	File
Computer     Local Disk (C:)     ✓ STORAGE-512 (D:     ✓ SCRATCH-240 (E:)	🗼 Temp	4/10/2017 4:10 PM	File
@ LAP (G:)			
*	•		۲
Folder	Export		
		Select Folder Cancel	

Figure 4-19 – Highlight Export Folder and Click Select Folder

After it loads, Ophcrack will show three users. The first two are the disabled Administrator and Guest user accounts. The third user account is Craig, and his decrypted hash value is shown as "85786ac88f59806d085ff414553fae6e." Before you crack Craig's login password, you need to install the Vista Free rainbow table. Click Tables in the top bar of Ophcrack. A Table Selection window will open and you need to highlight the Vista Free and then click Install.

Table Directory	Status	Preload	-
<ul> <li>XP free fast</li> </ul>	not installed	on disk	
<ul> <li>XP free small</li> </ul>	not installed	on disk	
<ul> <li>XP special</li> </ul>	not installed	on disk	E
• XP german v1	not installed	on disk	F
• XP german v2	not installed	on disk	
<ul> <li>Vista special</li> </ul>	not installed	on disk	
Vista free	not installed	on disk	
<ul> <li>Vista nine</li> </ul>	not installed	on disk	
<ul> <li>Vista eight</li> </ul>	not installed	on disk	
<ul> <li>Vista num</li> </ul>	not installed	on disk	
<ul> <li>Vista seven</li> </ul>	not installed	on disk	

Figure 4-20 – Highlight Vista Free Table and Click Install

After clicking Install, navigate to where you downloaded the Vista free table from Ophcrack. You want to then click Select folder on the folder that you extracted from the downloaded zip from Ophcrack (see Figure 4-21).

Select the directory which co		🗸 🍫 Search Downloa	ds P
Organize • New folder			2
	Name	Date modified	Туре
Libraries Documents	👃 Attachments_20151017	10/17/2015 7:11	File fol
Jusic	📕 HP Downloads	8/22/2015 3:16 PM	File fol
Pictures	bophcrack-3.7.0-bin	4/10/2017 4:51 PM	File fol
~	b tables_vista_free	4/10/2017 5:16 PM	File fol
Judeos	b usb-over-ethernet-client	9/20/2015 5:09 PM	File fo
Komegroup	=		
🔍 Computer			
bcal Disk (C:)			
	<del>•</del> • • •		Þ
Folder:	tables_vista_free		
		Select Folder Cance	h.

Figure 4-21 – Select Extracted Folder from Downloaded ZIP File and Click Select Folder

On the Table Selection window in Ophcrack, click OK. On the main Ophcrack window, you should see Vista free under Tables now. Click the Crack button in the top bar to crack Craig's login password.

Load Delete Progress Stati		-	Crack Help	Exit			Abo
User		LM Hash		NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
*disabled* Adm	inistrator		31d6cfe0d16	ae931b73c59d7e0c089	:0		empty
			21d6cfo0d16	ae931b73c59d7e0c089	-0		empty
*disabled* Gues	t		STUDCIEDUTO	uc5516/5c55u/c0c005			chipty
*disabled* Gues Craig	[			9806d085ff414553fae6			empty
	Status	Prelo	85786ac88f5	9806d085ff414553fae6			
Craig	-		85786ac88f5	9806d085ff414553fae6	9		

Figure 4-22 – Click Crack

If Ophcrack successfully finds a match, it will report back that hash value's matching password. In this case, Craig's password is hungry123. Knowing this password may help you break other password-protected files.

Progress	Statistics	Preference		NT Hash	IM Pwd 1	LM Pwd 2	NT Pwd
*disabled* /				e0d16ae931b73c59d7e0c089c0			empty
*disabled* (			31d6cfe	e0d16ae931b73c59d7e0c089c0	)		empty
Craig			85786a	c88f59806d085ff414553fae6e			hungry123
Table	Stat	tus F	reload	F	rogress		
▷ ● Vista fr	ee inac	tive 100	% in RAM				

Figure 4-23 - Craig's Login Password Cracked

**Note:** Craig's login password "hungry123" is a very simple password and that is why you are able to break it with a smaller rainbow table. If the password had upper case letters, symbols, and was longer, you would need a much larger rainbow table to break the password, and it would take much more time to crack.



## **Computer Forensics CCIC Training**

### Chapter 5: Starting Phase 2

Lauren Pixley, Cassidy Elwell, and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 5

# **Starting Phase 2**

### Introduction

During the Phase 2 Analysis, you will start to take a deeper dive into the forensic image to find specific evidence based on your case. The following steps are common areas of analysis done with Windows systems, but these steps may not be useful in every case. First, you will typically want to start by looking at where the user stored their personal data, what files they recently opened, and if there are any deleted files. You will also look to see if the user stored any personal data on external storage. After that, you will go through the suspect's email, Internet history, and chat logs. This phase will finish with a quick look for any evidence of data hiding and you will determine what programs the user installed. This more in depth phase will also cover how you can create a simple timeline and report your findings.

This chapter will focus on the first part, which is personal data. Users can save their pictures, documents, and videos in almost any location on the computer. However, you always want to first check the Windows default Desktop, Documents, Pictures, and Videos folder since a large majority of users store data in these folders. You also want to look at the Downloads folder and any cloud storage user folders. These folders will sometimes show what personal data the user downloaded or uploaded.

### **Personal Documents and Photos**

Go to the Users folder. Under this folder there are five user folders. However, as you remember from the SAM and SYSTEM hives, there is only one true and active user profile, and that is Craig. The other folders are default account folders.

Under the Craig user profile folder, there is a file called NTUSER.DAT. If you remember from the registry section, the NTUSER.DAT file is the profile registry hive. Every user account has one, and it contains information specific to that user, such as their start page in Internet Explorer, desktop wallpaper, and information about programs they installed. You will go through Craig's NTUSER.DAT file later.

Since Craig is the only active user account for this computer, you can focus your attention on that user account. Navigate to Craig's Documents folder, which is located in:

```
C:\Users\Craig\Documents
```

This is a default location where many users store their documents. This does not mean that every user will put their documents there, but it is a good place to look.

😹 Craig Tucker - Autopsy 4.3.0			
Case <u>V</u> iew <u>T</u> ools <u>W</u> indow <u>H</u> elp			
🕂 Add Data Source 📠 View Images/Videos 🗮 Timeline	🔓 Generate F 🛕 🕠	👁 - Keyword Lists 🛛 🔍 Key	word S
Show Rejected Results	Directory Listing /img_Tucker.E01 <mark>/vol_vc</mark>	ol2/Users/Craig/Documents	9 Results
□ □ □ Users (8)	Table Thumbnail		
$\square$ $\square$ $\square$ Craig (35)	Name	Modified Time	Change
🕀 📜 .gimp-2.8 (48)	🔑 Guides	2013-12-20 21:27:33 GMT	2013-1: 🔺
thumbnails (3)     thumbnails (3)	🚨 My Music	2013-12-17 18:11:35 GMT	2013-1:
⊕	My Pictures	2013-12-17 18:11:35 GMT	2013-1
Contacts (3)	My Stuff	2013-12-21 19:19:58 GMT	2013-1: 🗏
Cookies (2)	My Videos	2013-12-17 18:11:35 GMT	2013-1:
	😺 Papers	2013-12-18 23:18:54 GMT	2013-1: 🔻
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	<ul> <li>■</li> </ul>		•
Wy Music (2)	Hex Strings File Metad	data Results Indexed Text Med	lia
	Pa 1 of 1	P ← → Go to Page:	ງເ
—      —      My Stuff (90)     —      —      My Videos (2)     —      Papers (14)     —      Downloads (21)     ⊕ Favorites (5)     _      Links (7)     _      Local Settings (2)     _      Music (3)     _      My Documents (2)     _      NetHood (2)	0x00000000: 30 00 00 00 0x0000010: 10 00 00 00 0x0000002: 00 00 00 00 0x0000002: 00 00 00 00 0x00000030: 00 00 00 00		

Figure 5-1 – Craig's Documents Folder

As you can see, Craig has several subfolders under his Documents folder. In the Guides subfolder, he has documents describing how to make and use coupons.

### Tag

When you have files of interest in your case, you may want to tag them so you can easily find and review them later. You can tag these files by clicking a file at the top of the list in the table pane and then press the Shift key while left clicking the last file in the table pane. This will highlight all the files in between the two you clicked. Once you have all four files of interest highlighted in the Guide subfolder, right-click one and select Tag Files ► Tag and Comment.

😽 Craig Tucker - Autopsy 4.3.0		- • ×
Case View Tools Window Help		
🕂 Add Data Source 📠 View Images/Videos 🗮 Timeline	🗽 Generate F 🛕 🛛 👁 - Keyword Lists	Q- Keyword S
Show Rejected Results	Directory Listing /img_Tucker.E01/vol_vol2/Users/Craig/Docume Table Thumbnail	nts/Guides 6 Results
🖃 📙 Craig (35)	Name	Modified Time
.gimp-2.8 (48)	[current folder]	2013-12-20 21:27:
	[parent folder]	2013-12-18 19:41:
Application Data (2)	6CommandmentsofCouponMaking.docx	2013-12-20 21:27:
Contacts (3)	Guide1.png	2013-12-18 02:29:
Cookies (2)	Guide2.png	2013-12-18 02:29:
→ Desktop (10) → Documents (9)	HowtoMakeCoupons.jpg	2013-12-20 21:26:
Guides (10)	Properties	•
- J My Music (2) - J My Pictures (2)	He Extract File(s)	ext Media
Wy Stuff (90)	Tag Files Qu	uick Tag
- B My Videos (2) - B Papers (14)	Add files to hash database	g and Comment
Ownloads (21)     Favorites (5)     Outries (7)     Uinks (7)     Oucal Settings (2)     Wusic (3)     Wy Documents (2)     Outries (2)     WetHood (2)	1	

Figure 5-2 – Highlight Files in Guide Subfolder, Right-Click and Select Tag and Comment

A Create Tag window will open and you can use Autopsy's default Tag, which is Bookmark. You can also create your own preferred tag name by clicking the New Tag Name button. You can also type a quick comment if you'd like to help you remember later why you tagged a file. Click OK.

Tag:	Coupon Guides	
Comm <mark>en</mark> t:	These are guides on how to make and use fraud	ulent coupons

Figure 5-3 – Set Tag Name and Comment and Click OK

When you want to view your tagged files later, simply scroll down to Tags in the left pane. This is a quick and easy way to mark files that relate to your investigation, and it helps you remember and report all of your findings at the end of your investigation (see Figure 5-4).

Case view Tools	Window Help			
🕂 Add Data Sour	ce 顑 View Images/Videos 🗮 Timelin	e ×	👍 💿 🕶 Keyword Lists	Q <del>.</del> Keyword S
€ >	Show Rejected Results	Directory Listi	ing	
Data Sources		Coupon Guide Table Thum		4 Result
📄 🗐 Tucker.E01	allocated: 0-2047)	File		Comment
	FS / exFAT (0x07): 2048-125827071)	🕭 HowtoMal	keCoupons.jpg	These are guides on ho
8	allocated: 125827072-125829119)	Suide1.pr	ng	These are guides on ho
Views     Results		🕭 Guide2.pr	ng	These are guides on he
Extracted C	ontent	🕭 6Commar	ndmentsofCouponMaking.docx	These are guides on h
E-Mail Mess     Kenner     Coupon Gu     Go Result T     S Reports	ides (4)	Name Type MIME Type Size File Name	File Metadata Results Indexen /img_Tucker.E01 vol_vol2/Use File System null 2089397 Allocated	
Kinteresting     Accounts     Son Tags     Son Coupon Gu     Son File Tags     Son Result T	ides (4)	Hex Strings Name Type MIME Type Size File Name Allocation Metadata	/img_Tucker.E01 <mark>vol_vol2/Use</mark> File System null	
Kinteresting     Accounts     Son Tags     Son Coupon Gu     Son File Tags     Son Result T	ides (4)	Hex Strings Name Type MIME Type Size File Name Allocation	/img_Tucker.E01 <mark>vol_vol2/Use</mark> File System null 2089397 Allocated	

Figure 5-4 – View Tagged Files in Tags

Take a look at Craig's other subfolder under Documents called My Stuff. There are several pictures of coupons in this folder. Go ahead and add these files to your same Tag or a new one.

😹 Craig Tucker - Autopsy 4.3.0		- <b>•</b> ×
Case View Tools Window Help		
🕂 Add Data Source 📠 View Images/Videos 🗮 Timeline	× 🛕 👁 • Keyw	ord Lists Q <del>.</del> Keyword S
← →	Directory Listing	Craig/Documents/My Stuff 47 Resu
□ □ □ Users (8)	Table Thumbnail	raig/Documents/My Stun 47 Kesu
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	Name	Modified Time
⊞ 🖟 .gimp-2.8 (48)	1304400692832.png	2011-05-03 08:36:40 GMT
⊕	🖹 1304643149337.png	2011-05-06 05:20:18 GMT
H → AppData (5) - → Application Data (2)	1304643663005.png	2011-05-06 05:22:20 GMT
Contacts (3)	📓 1304643804769.png	2011-05-06 05:23:04 GMT
- 🖟 Cookies (2)	■ 1304644031008.png	2011-05-06 05:25:18 GMT
- 😺 Desktop (10)	📓 1304644210039.png	2011-05-06 05:25:22 GMT +
	• III	•
Generation (1)     Generation (2)     Generation (2)	Save \$19 Dray 1 pool 24 Par This per transformed transformed transformed that per transformed transformed transformed transformed transformed to per transformed to per transformed transformed to per transformed to per	TURER'S COUPON E

Figure 5-5 – Tag Coupon Files in Craig's My Stuff Folder

### Zone ID

In the My Stuff folder, you will notice that one graphic file, Whopper.jpg, is different than the other files. Autopsy shows in the table pane that this file also has another entry called Whopper.jpg:Zone.Identifier. Highlight this file and you will see in the Hex view pane or the Strings view pane that it contains the text "[ZoneTransfer] ZoneId=3".



Figure 5-6 - Zone ID=3 in Whopper.jpg:Zone Identifier

Starting with Windows XP SP2, Microsoft added an Alternate Data Stream (ADS) to a file that was downloaded from the Internet to a NTFS volume. Think of this as a security flag used to determine the source of a file. The ZoneId value of 3 means that the file was downloaded from the Internet and it is potentially unsafe. The values could be from other zones, such as the following:

MyComputer	0
Intranet	Ι
Trusted	2
Internet	3
Untrusted	4

From an analysis perspective, a file that has an ADS called Zone.Identifier with ZoneID=3, you know that the file originated from the Internet and is direct evidence of downloading a file.

**Note:** Any files that are extracted from a downloaded ZIP will have an ADS added to the file with a Zone ID of 3.

### **Personal Documents and Photos (Continued)**

The next place to look for personal data is the Pictures folder. Navigate to:

```
C:\Users\Craig\Pictures
```



Figure 5-7 – Craig's Pictures Folder

As you can see, the only data in the folder is personal pictures, and they are unrelated to your case.

Next, navigate to Craig's desktop (see Figure 5-8). This is under:

```
C:\Users\Craig\Desktop
```

Add Data Source 📠 View Images/Vide	eos	🗄 Timeline 🗧 🔥 🕢 🔿 - Keyw	ord Lists Qr Keyword S	5
Show Rejected Resu		Directory Listing		
Users (8)		/img_Tucker.E01 vol_vol2/Users/Craig/Desktop Table Thumbnail	7	Result
$\square$		Name	Modified Time	Cha
.gimp-2.8 (48)		[current folder]	2013-12-21 19:08:18 GMT	201
		[parent folder]	2013-12-21 00:58:42 GMT	20:
		AWESOME COUPONS.docx	2013-12-20 21:43:05 GMT	20
		AWESOME COUPONS.docx:Zone.Identifier	2013-12-20 21:43:05 GMT	20
		N desktop.ini	2013-12-17 23:11:25 GMT	20
Desktop (10)		MyCoupons.zip	2013-12-21 19:08:18 GMT	20
🕀 🔑 Documents (9)		Pricing Sheet.rtf	2013-12-21 18:53:52 GMT	20
Downloads (21)			2010 12 21 10.00.02 0(1)	20
🕀 🔑 Favorites (5)		< III		P
Links (7)		Hex Strings File Metadata Results Indexed T	Description of the second s	
		Pa 1 of 1 P ← → Go to Pa	ige: Jump to C	Offset
My Documents (2)     Wy Documents (2)     WetHood (2)     Pictures (12)     Santa Monica (10)     School (8)     PintHood (2)     Recent (2)     Saved Games (3)	I	0x00000000: 7B 5C 72 74 66 31 5C 61 6E 73 69 0 0x00000010: 63 70 67 31 32 35 32 5C 61 6E 73 69 0 0x000002010: 75 69 63 67 6D 70 61 74 5C 64 65 66 0x00000020: 31 30 33 33 7B 5C 66 6F 6E 74 74 0x000000050: 30 5C 66 6E 69 6C 5C 66 63 68 61 0x000000050: 20 41 72 69 61 6C 38 7D 75 5C 66 0x00000000: 6C 5C 66 36 86 12 73 65 74 30 0x00000000: 62 72 69 3B 7D 7B 5C 66 32 5C 66 0x00000000: 63 68 61 72 73 65 74 30 20 4D 53 0x000000000: 63 68 61 72 73 65 74 00 20 4D 53 0x000000000: 63 68 61 72 73 65 74 00 20 4D 53 0x000000000: 63 68 61 72 73 65 74 00 20 4D 53 0x000000000: 20 53 65 72 69 66 3B 7D 70 40 0A 54 0x000000000: 20 53 65 72 69 66 3B 7D 70 40 0A 54 0x000000000: 20 53 65 72 69 66 3B 7D 70 40 0A 54 0x000000000: 20 53 65 72 69 66 3B 7D 70 40 0A 54 0x0000000000: 20 53 65 72 69 66 3B 7D 70 40 0A 54 0x000000000000: 20 53 65 72 69 66 3B 7D 70 40 0A 54 0x00000000000000000000000000000000000	<pre>56 30 SC 62 67 cpg1252/det 65 CC 61 65 7 uicompat/dd 52 6C 7B 5C 66 1038{\form 12 73 65 74 30 0\fn1\form 13 C 66 62 69 Arial;}{\translat},{\trans</pre>	ff0\no aflang cbl{\f arset0 f1\fni D Cali fnil\f S Sans .{\*\g

Figure 5-8 – Craig's Desktop

Craig only has a few documents on his desktop. If you want to view document or some email type files within Autopsy, you will need to download the Multi Content Viewer 3<sup>rd</sup> party module. This can be downloaded from:

https://github.com/lfcnassif/MultiContentViewer/releases/tag/v1.0-beta

After you download the .nbm file for the Multi Content Viewer module, you need to install it. To install a  $3^{rd}$  party module, you need to click Tools  $\triangleright$  Plugins.



Figure 5-9 – Click Plugins under Tools

When the Plugins window opens, click the Downloaded tab at the top of the window. Click the Add Plugins button (see Figure 5-10).

pdates Ava	ailable Plugins	Downloaded	Installed (13)	Settings
------------	-----------------	------------	----------------	----------

Figure 5-10 – Click Add Plugins under Downloaded Tab

An Add Plugins window will open, and you need to navigate to where you downloaded the .nbm file. Select the .nbm file and click Open.

😹 Add Plug	gins		×
Look in:	Downloads	🖻 💣 🔝 -	
Recent I	Attachments_20151017 HP Downloads MultiContentViewer-master		
Desktop	<ul> <li>ophcrack-3.7.0-bin</li> <li>tables_vista_free</li> <li>usb-over-ethernet-client</li> <li>usp64.v.0.46.win</li> </ul>		
My Doc Computer	■ dpf-sp-gpinf-indexer-search-viewer.nbm		Ļ
( Network	File name:     dpf-sp-gpinf-indexer-search-viewer.nbm       Files of type:     Plugin distribution files (*.nbm)		Open Cancel

Figure 5-11 – Select nbm File and Click Open

The Multi Content Viewer plugin will now show up in the list. Click the Install button in the bottom left corner.



Figure 5-12 – Click Install on MultiContentViewer Plugin

Go through the steps to install the plugin. The last Plugin Installer window will prompt you to restart Autopsy. Select Restart Now and then click Finish (see Figure 5-13).

estart application to constant application to finish p	
he Plugin Installer has suc	ccessfully installed the following plugins:
MultiContentViewer	
Restart Now	
	1

Figure 5-13 – Select Restart Now After Installing Plugin and Click Finish

Open up Autopsy again and navigate to Craig's Desktop folder. You can now view certain file types within Autopsy, such as the .rtf file on Craig's Desktop.

There are still some other files on Craig's Desktop of interest, such as the AWESOME COUPONS.docx and MyCoupons.zip files. First, let's try to open the AWESOME COUPONS.docx file. You are unable to view this file within Autopsy perhaps because it is password protected. To view this file, you need external software that can open and view docx files, such as Microsoft Word or Open Office. Right-click the AWESOME COUPONS.docx file and click Open in External Viewer.

e View Tools Window Help Add Data Source <u>द</u> View Images/Vide	os	ี Timeline 脑 Generate Re 🛕		_
Show Rejected Resul	te	Directory Listing	4.20	
Show Rejected Resul \$Unalloc (5) Boot (47)	×	/img_Tucker.E01/vol_vol2/Users/Cra Table Thumbnail	ig/Desktop 7 Res	sul
Documents and Settings (2)		Name	Modified Time	Ch
		[current folder]	2013-12-21 19:08:18 GMT	20
🕀 🔑 Program Files (21)		[parent folder]	2013-12-21 00:58:42 GMT	20
	_	AWESOME COUPONS.docx	2013-12-20 21:43:05 GMT	20
ProgramData (10)     Recovery (3)     System Volume Information (9     Users (8)		AWESOME COUPONS.docx:2 desktop.ini	Properties View in New Window Open in External Viewer	
→      ↓ Users (8)     →      ↓ All Users (2)     →      ↓ Craig (35)     ⊕      ↓ .gimp-2.8 (48)     ⊕      ↓ thumbnails (3)     ⊕      ↓ AppData (5)		Pricing Sheet.rtf     III     Hex Strings File Metadata Resi	View File in Timeline Extract File(s) Search for files with the same MD5 ha	as
AppData (5)		Pa 1 of 39 P	Tag File	
Application Data (2)     Contacts (3)     Contacts (2)     Desktop (10)     Documents (9)     Documents (9)     Downloads (21)     Favorites (5)     Cuiks (7)     Cuiks (7)     Cuiks (7)     Cuiks (2)	Ш	0x0000000: D0 CF 11 E0 Al B1 1A           0x00000010: 00 00 00 00 00 00 00           0x00000010: 00 00 00 00 00 00           0x00000010: 00 00 00 00 00 00           0x00000000: 06 00 00 00 00 00 00           0x00000000: 01 00 00 00 00 00 00           0x00000000: 01 00 00 00 00 00 00           0x00000000: 01 00 00 00 00 00 00 00           0x00000000: 05 00 00 00 00 00 00 00 00           0x00000000: 07 00 00 00 00 00 00 00           0x00000000: 07 00 00 00 10 00 00           0x00000000: 13 00 00 14 00 00 00           0x00000000: FF           0x00000000: FF	Add file to hash database	

Figure 5-14 – Right-Click AWESOME COUPONS.docx and Select Open in External Viewer

Your default document viewer should attempt to open the file and you will be prompted with a Password window. We will come back to this password protected document later.

Enter password to open file E:\\Craig Tucker\Temp\AWESOME COUPONS.docx	Password		? 🗙
E:\\Craig Tucker\Temp\AWESOME COUPONS.docx	and the second second	and the constant in the design of the second	
	E:\\Craig	Tucker\Temp\AWESON	ME COUPONS.docx

Figure 5-15 – Password Needed for AWESOME COUPONS.docx

Let's next try to open the MyCoupons.zip file. To open and view the contents of container files, such as zip and rar files, you need to run the Embedded File Extractor module. Click on Tools ► Run Ingest Modules ► Tucker.E01. When the Run Ingest Modules window opens, check Embedded File Extractor and then click Start.

😹 Run Ingest Modules	×
<ul> <li>▲ Recent Activity         <ul> <li>Hash Lookup</li> <li>File Type Identification</li> <li>✓ Embedded File Extractor</li> <li>Exif Parser</li> <li>Keyword Search</li> <li>Email Parser</li> <li>Extension Mismatch Detector</li> <li>▲ E01 Verifier</li> <li>Android Analyzer</li> <li>Interesting Files Identifier</li> <li>PhotoRec Carver</li> <li>Virtual Machine Extractor</li> </ul> </li> </ul>	The selected module has no per-run settings.
Select All Deselect All View Ingest History	Extracts embedded files (doc, docx, ppt, pp Global Settings
Process Unallocated Space	Start Close

Figure 5-16 – Check Embedded File Extractor and Click Start

If you click on the Ingest Messages button in the top bar of Autopsy, you will see that the Embedded File Extractor module has detected an encrypted file (see Figure 5-17).

Craig Tucker - Autopsy 4.3.0		- <b>•</b> ×
Case View Tools Window Help	imeline 🚡 Generate R 🚺 💿 - Keyword	Lists Qr Keyword S
🖨 📮 Users (8) 🔹 🔺	Directory Listing /img_Tucker.E01/vol_vol2/Users/Craig/Desktop Table Thumbnail	p 7 Results
→ → All Users (2) → → → Craig (35)	Name	Modified Time
in jung (55)	[current folder]	2013-12-21 19:08:18 GMT
🖽 🔑 .thumbnails (3)	[parent folder]	2013-12-21 00:58:42 GMT
🕀 🔑 AppData (5)	AWESOME COUPONS.docx	2013-12-20 21:43:05 GMT
	AWESOME COUPONS.docx:Zone.Identifie	r 2013-12-20 21:43:05 GMT
Contacts (3)	🖲 desktop.ini	2013-12-17 23:11:25 GMT
Besktop (10)	MyCoupons.zip	2013-12-21 19:08:18 GMT
🕀 🔑 Documents (9)	Pricing Sheet.rtf	2013-12-21 18:53:52 GMT
Downloads     Downloads		X
	Num New? Subject	Timestamp
<ul> <li>→ Music (3)</li> <li>→ My Docume</li> <li>→ NetHood (2</li> <li>→ Pictures (12</li> <li>→ PrintHood (</li> </ul>	Encrypted files in archive detected.	19:13:16
Recent (2) Sort by: Time V	Total: 1 Uniq	gue: 1
- U Saved Gam		
- SendTo (2)	•	111
	Analyzing files from Tucker.E01	19% 🛛 🥥

Figure 5-17 – Click Ingest Messages Button to View Encrypted Files Detected

If you click on this message in the module list, it will show that the MyCoupons.zip has encrypted files. We will come back to this file and the other encrypted docx file later.

Next, take a look at Craig's SkyDrive, now known as Microsoft OneDrive, (see Figure 5-18). This is located at:

```
C:\Users\Craig\SkyDrive
```

Add Data S	Gource 📠 View Images/Videos 🗮	Timeline 膨 Generate Re	👍 💿 - Keyword Lists	৭ <mark>-</mark> Keyword S
≥	Show Rejected Results	Directory Listing		
			ol2/Users/Craig/SkyDrive	5 Resul
	All Users (2)	Table Thumbnail		
	Craig (35)	Name	Modified Time	Change Time
	🔋 .gimp-2.8 (48)	[current folder]	2013-12-30 03:56:50 GMT	2013-12-30 03:56:
3 3 3 3 3 3 3 3 3 3	👃 .thumbnails (3)	[parent folder]	2013-12-21 00:58:42 GMT	2013-12-21 00:58:
	AppData (5)	Documents	2013-12-21 19:05:38 GMT	2013-12-21 19:05:
	Application Data (2)	🖲 desktop.ini	2013-12-30 03:56:50 GMT	2013-12-30 03:56:
	Contacts (3) Cookies (2)	x fsHelper.tmp	0000-00-00 00:00:00	0000-00-00 00:00:
	<ul> <li>Downloads (21)</li> <li>Favorites (5)</li> <li>Links (7)</li> <li>Local Settings (2)</li> <li>Music (3)</li> <li>My Documents (2)</li> <li>NetHood (2)</li> <li>Pictures (12)</li> <li>PrintHood (2)</li> <li>Recent (2)</li> <li>Saved Games (3)</li> <li>Searches (7)</li> </ul>	Hex Strings File Meta	data Results Indexed Text Med	lia
	SendTo (2)			

Figure 5-18 – Craig's Skydrive

When this drive was imaged, Microsoft still had Skydrive incorporated into the user's environment. Skydrive is now known as Onedrive, but its basic function is the same. When something is saved to Skydrive (Onedrive), it syncs to the Cloud and users can then access these files from other computers, tablets, or their phone. Users might not always save data to this location, but it's a good place to check.

Craig's Skydrive contains several coupons. Each coupon also has a Zone ID of 3, which means they have been downloaded from the Internet. You can tag these files for now to easily come back and review them later.

Now, navigate to Craig's Download folder (see Figure 5-19), which is located at:

```
C:\Users\Craig\Downloads
```

Users can change where they want their default download folder, so there might not always be data here. However, it is still a good place to check.



Figure 5-19 – Craig's Downloads Folder

You will notice that all six of the actual files listed in the Downloads folder have an ADS with Zone ID=3, which means they were also downloaded from the Internet.

In Craig's Downloads folder, he has a RAR file, two ZIP files, and three programs. You already ran the Embedded File Extractor module for the other zip file on his desktop, so you can now open and view the data in these compressed files. As you can see, these ZIP and RAR files contain several coupons. You can tag these files for now since we will come back to them later to determine where Craig downloaded them from.



# Computer Forensics CCIC Training

## Chapter 6: Recent Files

Lauren Pixley, Cassidy Elwell, and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 6

# **Recent Files**

### Introduction

From an investigative standpoint, you usually want to determine what files a user recently accessed. It gives you a perspective on how the user used the computer, and it also associates file activity back to the suspect. This will help demonstrate their knowledge about the existence of the files and show that they opened and viewed it. In this chapter, we will focus on link files and jump lists. Both of these artifacts will show you what files the user opened.

### **Link Files**

You are going to first look in Craig's Recent folder. This is located in the following path for versions 7-10 of Windows:

ld Data Source 📠 View Images/Videos 🗮	Time	ine 📗 Generate Report 🗧 🔺		• Keyword Lists	Q. Keyword	S		
Show Rejected Re	sults	Directory Listing /img_Tucker.E01 vol_vol2/Users/Co	raig/A	ppData/Roaming/Micr		/Recent		
	^	Table Thumbnail						
⊕ Jimp-2.8 (48) ⊕ J .thumbnails (3)		Name		Modified Tim	e	Chan		
😑 🔑 AppData (5)		Obesity.Ink		2013-12-18 2	3:13:16 GMT	2013-		
		Papers.Ink		2013-12-21 1	8:35:39 GMT	2013-		
Cocation (4)  Cocation (4)  Cocation (5)  Cocation (3)  Cocation (12)  Cocation (3)  Cocation (12)  Cocation (3)  Cocation (12)  Cocation (1	Park.Ink		2013-12-20 2	1:16:53 GMT	2013			
	Pictures.Ink		2013-12-21 1		2013			
	Pier.lnk		2013-12-20 2		2013			
	Pricing Sheet.Ink		2013-12-21 1		2013			
	Russian Videos.Ink		2013-12-21 1		2013			
	Santa Monica.Ink		2013-12-20 2	1:16:57 GMT	2013			
⊕		Hex Strings File Metadata Results Indexed Text Media						
🕀 🔑 Protect (5)		Res 1 of 1 Re ← →						
	Ш	Recent Documents						
🖃 🔑 Windows (11)		Path C:\Users\Craig\AppData\L	.ocal\P	ackages\microsoft.windo	vscommunication	isapps		
AccountPictures (3)		Path ID 41041						
<ul> <li>– Libraries (11)</li> <li>– Network Shortcuts (2)</li> </ul>		Date/Time 2013-12-18 20:03:53						
- B Printer Shortcuts (2)		Source /img_Tucker.E01/vol_vol2	/Users	/Craig/AppData/Roaming	/Microsoft/Windo	ws/Re		
E Recent (88)		4 10						

C:\Users\Craig\AppData\Roaming\Microsoft\Windows\Recent

Figure 6-1 – Craig's Link Files in Recent Folder

This folder contains the user's link files. A link file, or LNK, is a Windows shortcut that points back to an original file. A link file is generally created when a file is first opened. Link files are important during analysis, because they show where files were located, when they were opened, and they contain date and time stamps associated with the file. If you look at Windows Explorer and go to the Recent folder, you can see your own link files.

		·				
C:\Users\Demo\AppDa	та∖ко	aming\wicrosoft\wi	naows\kecen	IJ		
File Edit View Tools Help						
Organize 🔻						• • •
🐌 Vault	*	Name	Туре	Date created	Date modified	Date accessed
Undows		Desert.jpg	Shortcut	5/2/2014 11:04 AM	5/2/2014 11:04 AM	5/2/2014 11:04 AM
L Cookies		Penguins.jpg	Shortcut	5/2/2014 11:00 AM	5/2/2014 11:00 AM	5/2/2014 11:04 AM
DNTException		Tulips.jpg	Shortcut	5/2/2014 11:00 AM	5/2/2014 11:00 AM	5/2/2014 11:00 AM
📜 IECompatCache		Laubsiba	Shortcut	5/2/2014 11.04 AIVI	5/2/2014 11.04 AM	5/2/2014 11.04 AW
📗 IECompatUACache						
📗 IEDownloadHistory						
Libraries						
I Network Shortcuts						
I Printer Shortcuts						
🐌 PrivacIE	Ξ					
la Recent Items						
📜 SendTo						
🐌 Start Menu						
📜 Templates						
) Themes						
U Word	-					

Figure 6-2 – Link Files in Windows Explorer

Note: To view the AppData folder since it is hidden, open Windows Explorer and click Organize ► Folder and Search Options. Check Show Hidden Files, Folders, and Drives under the View tab. If you are on a Windows 8 or 10 machine, click the View tab on Windows Explorer and check Hidden Items.

If you right-click one of the link files and select properties, you can see the information about the link file (see Figure 6-3).

Penguins.jpg	Properties
General Shorto	ut Security Details Previous Versions
	Penguins.jpg
Type of file:	Shortcut (.lnk)
Opens with:	Windows Photo Viewer Change
Location:	C:\Users\Demo\AppData\Roaming\Microsoft\Windows'
Size:	1.22 KB (1,257 bytes)
Size on disk:	4.00 KB (4,096 bytes)
Created:	Today, May 02, 2014, 9 minutes ago
Modified:	Today, May 02, 2014, 11:09:44 AM
Accessed:	Today, May 02, 2014, 11:09:44 AM
Attributes:	Read-only Hidden Advanced
	OK Cancel Apply

Figure 6-3 – Link File Properties

This link file is merely a pointer back to the actual file. It contains date and time stamps, the size of the file, and if you look at the Shortcut tab, you can even see where the file was located when it was opened.

Penguins.jpg Properties													
General Shortcut	Security Details Previous Versions												
Pe	Penguins.jpg												
Target type:	Target type: JPEG image												
Target location: Sample Pictures													
Target	Target: "C:\Users\Public\Pictures\Sample Pictures\Penguins.												
Start in:	Start in: "C:\Users\Public\Pictures\Sample Pictures"												
Shortcut key:	None												
Run:	Normal window 🔹												
Comment													
Open File Lo	cation Change Icon Advanced												
	OK Cancel Apply												

Figure 6-4 - Link File Pointing to Actual File's Location

### **Example 1 (File Opened Once)**

Back in Autopsy, look at the link file called Pier.lnk and click on the Results view. Autopsy will show you the path of where Pier.jpg was stored when it was opened.

Hex Strings	File Metadata Results Indexed Text Media
Res 1	of 1 Re ← →
lecent Docume	nts
Path	C:\Users\Craig\Pictures\Santa Monica\Pier.jpg
Path ID	46925
Date/Time	2013-12-20 21:16:57
Source File Path	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Roaming/Microsoft/Windows/Recent/Pier.Inl
raui	

Figure 6-5 – Link File Shows Path of Pier.jpg

If you view Pier.lnk in Hex view, you can see that inside this link there is embedded data that points back to the original file that was opened.

Name				Modified Time							
Obesity	/.lnk			2013-12-18 23	:13:16 GMT	2013-3					
Papers.	.lnk			2013-12-21 18	:35:39 GMT	2013-					
Park.In	k			2013-12-20 21	:16:53 GMT	2013-					
Picture	s.lnk		1	2013-12-21 19	:32:45 GMT	2013-					
Pier.Inl				2013-12-20 21	:16:57 GMT	2013-					
Pricing	Sheet.Ink	:53:52 GMT	2013-								
Russiar	Nideos.lnk			2013-12-21 19	2013-						
•	111										
Hex String	Eilo Motor	data Results	Indoved Tay	t-Modia							
Pa 1	of 1	P ← →		The second s	Jump to O	feet					
1 4 1	0 1		GO to Pay	le: 1	Jump to O	iset 0					
	C 00 00 00	01 14 02 00	00 00 00 00	CO 00 00 00	L						
0x00000010:	00 00 00 46	9B 00 20 00	20 00 00 00	56 61 89 AA	F	Va					
0x00000010: 0x00000020:	00 00 00 46 C8 FD CE 01	9B 00 20 00 56 61 89 AA	20 00 00 00 C8 FD CE 01	56 61 89 AA 00 2D 24 C6	F	Va \$.					
0x00000010: 0x00000020: 0x000000030:	00 00 00 46 C8 FD CE 01 C4 FD CE 01	9B 00 20 00 56 61 89 AA FF 79 05 00	20 00 00 00 C8 FD CE 01 00 00 00 00	56 61 89 AA 00 2D 24 C6 01 00 00 00	F	Va \$.					
0x00000010: 0x00000020: 0x00000030: 0x00000040:	00 00 00 46 C8 FD CE 01 C4 FD CE 01 00 00 00 00	9B 00 20 00 56 61 89 AA	20 00 00 00 C8 FD CE 01	56 61 89 AA 00 2D 24 C6	F Vа у.	Va					
0x00000010: 0x00000020: 0x00000030: 0x00000040: 0x00000050:	00 00 00 46 C8 FD CE 01 C4 FD CE 01 00 00 00 00 1F 54 25 48	9B 00 20 00 56 61 89 AA FF 79 05 00 00 00 00 00	20 00 00 00 C8 FD CE 01 00 00 00 00 00 00 00 00	56 61 89 AA 00 2D 24 C6 01 00 00 00 1A 0B 14 00	F	Va \$. 					
0x00000010: 0x00000020: 0x00000030: 0x00000040: 0x00000050: 0x00000060: 0x00000060:	00 00 00 46 C8 FD CE 01 C4 FD CE 01 00 00 00 00 1F 54 25 48 8D D5 20 00 9F AE 90 A9	9B 00 20 00 56 61 89 AA FF 79 05 00 00 00 00 00 1E 03 94 7B	20 00 00 00 C8 FD CE 01 00 00 00 00 00 00 00 00 C3 4D B1 31	56 61 89 AA 00 2D 24 C6 01 00 00 00 1A 0B 14 00 E9 46 B4 4C	F	Va \$. .F.L .PA.					
0x00000010: 0x00000020: 0x00000030: 0x00000040: 0x00000050: 0x00000050: 0x00000060: 0x00000070:	00 00 00 46 C8 FD CE 01 C4 FD CE 01 00 00 00 00 1F 54 25 48 8D D5 20 00 9F AE 90 A9 00 00 73 02	9B 00 20 00 56 61 89 AA FF 79 05 00 00 00 00 00 1E 03 94 7B 00 00 1A 00	20 00 00 00 C8 FD CE 01 00 00 00 00 C3 4D 81 31 EE BB FE 23 94 BC 99 12 81 19 14 10	56 61 89 AA 00 2D 24 C6 01 00 00 00 1A 0B 14 00 E9 46 B4 4C 00 00 10 00	F	Va \$. .F.L .PA.					
0x00000010 0x00000020 0x00000030 0x0000040 0x0000050 0x0000060 0x0000070 0x0000070 0x00000080 0x00000080	00         00         00         46           C8         FD         CE         01           C4         FD         CE         01           00         00         00         00           1F         54         25         48           BD         D5         20         00           9F         AE         90         A9           00         00         73         02           00         00         00         60	9B         00         20         00           56         61         89         AA           FF         79         05         00           00         00         00         00           1E         03         94         7B           00         00         1A         00           3B         AO         80         4E           00         00         6D         02           00         00         00         00	20 00 00 00 C8 FD CE 01 00 00 00 00 00 00 00 00 C3 4D B1 31 EE BB FE 23 94 BC 99 12 81 19 14 10 00 00 00 00	56 61 89 AA 00 2D 24 C6 01 00 00 00 1A 0B 14 00 E9 46 B4 4C 00 00 10 00 D7 50 41 04 43 02 20 00 00 00 00 00	F	Va \$. .F.L .PA. C.					
0x00000010 0x00000020 0x00000030 0x0000040 0x0000050 0x0000060 0x0000070 0x0000070 0x00000080 0x00000080	00 00 00 46 C8 FD CE 01 C4 FD CE 01 00 00 00 00 1F 54 25 48 8D D5 20 00 9F AE 90 A9 00 00 73 02 00 00 00 00	9B 00 20 00 56 61 89 AA FF 79 05 00 00 00 00 00 1E 03 94 7B 00 00 1A 00 3B A0 80 4E 00 00 6D 02	20 00 00 00 C8 FD CE 01 00 00 00 00 C3 4D 81 31 EE BB FE 23 94 BC 99 12 81 19 14 10	56 61 89 AA 00 2D 24 C6 01 00 00 00 1A 0B 14 00 E9 46 B4 4C 00 00 10 00 D7 50 41 04 43 02 20 00	FVa	Va \$. .F.L .PA. C.					

Figure 6-6 – Embedded Data in Pier.lnk

There are three date and time stamps EMBEDDED within the link file. The time stamps you see in the Hex view refer back to the file "Pier.jpg".

Embedded Time Stamps	Description				
Creation Time (Yellow)	This is the time that the file (Pier.jpg) was created in that local path. If the file had been copied to that location, then the Creation date/time is when it was copied.				
Last Access Time (Green)	Last access times have been disabled since Windows Vista. It keeps the same date as the Creation time (UTC), but there are some variables that can change or update it.				
Last Write Time (Blue)	This is the time that the file (Pier.jpg) was last modified. This is not necessarily the last time it was opened.				
Hex Strings File	Metadata Results Indexed Text Media				

Hex	Strin	gs	File	e M	eta	data	F	Resi	ults	Ind	exe	ed T	Text	M	edi	а		
Pa.	·· 1	(	of	1		P		ę	- >	C	Go t	to F	Page	:	1			Jump to Offset 0
0x000	00000:	4C	00	00	00	01	14	02	00	00	00	00	00	CO	00	00	00	L
0x000	00010:	00	00	00	46	9B	00	20	00	20	00	00	00	56	61	89	AA	FVa
0x000	00020:	C8	FD	CE	01	56	61	89	AA	CB	FD	CE	01	00	2D	24	C6	Va\$.
0x000	00030:	C4	FD	CE	01	FF	79	05	00	00	00	00	00	01	00	00	00	y
0x000	00040:	00	00	00	00	00	00	00	00	00	00	00	00	1A	0B	14	00	
0x000	00050:	1F	54	25	48	1E	03	94	7B	C3	4D	B1	31	E9	46	B4	4C	.T%H{.M.1.F.L
0x000	00060:	8D	D5	20	00	00	00	1A	00	EE	BB	FE	23	00	00	10	00	#
0x000	00070:	9F	AE	90	A9	3B	AO	80	4E	94	BC	99	12	D7	50	41	04	;PA.
0x000	00080:	00	00	73	02	00	00	6D	02	81	19	14	10	43	02	20	00	smC
0x000	00090:	00	00	00	60	00	00	00	00	00	00	00	00	00	00	00	00	····*
0x000	000a0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0x000	000b0:	10	01	00	00	31	53	50	53	A6	6A	63	28	ЗD	95	D2	11	1SPS.jc(=
0x000	000c0:	B5	D6	00	CO	4F	D9	18	DO	25	00	00	00	0B	00	00	00	

Figure 6-7 – Embedded Creation, Last Access, and Last Write Times of Pier.jpg

To decode these time stamps, you are going to use the tool called DCode (Version 4.02a). You can download this tool at:

http://www.digital-detective.net/digital-forensic-software/free-tools/

Once you have DCode up and running, you need to copy the time stamps out Pier.lnk in hex view and paste them into Notepad.



Figure 6-8 – Copy and Paste Embedded Time Stamps of Pier.lnk

In DCode, set the Decode Format to Windows: 64 bit Hex Value – Little Endian. Next, past the first time stamp (creation time of pier.jpg) into the Value to Decode. Hit the Decode button in the bottom right corner and you should see the decoded embedded creation time stamp (see Figure 6-9).

🙆 DCode v4.02a (Build: 9306)	<b>×</b>
DCODE	$\bigcirc$
Convert Data to Date / Time Values	
Add Bias: UTC 00:00 Decode Format: Windows: 64 bit He Example: FF03D2315FE1C	
Value to Decode: <mark>566189AAC8FDCE0</mark> Date & Time: <b>Fri, 20 Decembe</b> r	
www.digital-detective.co.uk	Cancel Clear Decode

Figure 6-9 – Embedded Creation Time Stamp Decoded

Repeat this for the other two time stamps, and you should have the following date and time stamps:

Embedded Creation Time (UTC): Fri, 20 December 2013 21:15:53 UTC

Embedded Access Time (UTC): Fri, 20 December 2013 21:15:53 UTC

Embedded Last Write Time (UTC): Fri, 20 December 2013 20:48:02 UTC

Next, you need to look at the date and time stamps of the link file itself.

Name	Created Time	Modified Time	Access Time
Pictures.Ink	2013-12-21 19:32:38 GMT	2013-12-21 19:32:45 GMT	2013-12-21 19:32:45 GMT
🧧 Pier.Ink	2013-12-20 21:16:57 GMT	2013-12-20 21:16:57 GMT	2013-12-20 21:16:57 GMT
Pricing Sheet.Ink	2013-12-21 18:53:52 GMT	2013-12-21 18:53:52 GMT	2013-12-21 18:53:52 GMT
Russian Videos.Ink	2013-12-21 19:42:16 GMT	2013-12-21 19:42:16 GMT	2013-12-21 19:42:16 GMT
Santa Monica.Ink	2013-12-20 21:16:53 GMT	2013-12-20 21:16:57 GMT	2013-12-20 21:16:57 GMT
School.Ink	2013-12-20 21:16:19 GMT	2013-12-20 21:16:19 GMT	2013-12-20 21:16:19 GMT

Figure 6-10 - Date and Time Stamps of the Link File

The time stamps in the table pane are about the link file itself and are separate from the time stamps embedded within the link file.

Link File Time Stamps	Description
Created Time	When a file is first opened, it creates a link file. The link file's Created time stamp is when the file (Pier.jpg) was FIRST opened.
Modified Time	This is the time when the file (Pier.jpg) was LAST opened. If this is the same as the Created time stamp, then you know that the file was only opened once.
Access Time	Once again, the accessed time is disabled in Windows Vista, 7, and 8. Accessed will be the same date and time as Modified.

As you can see in Figure 6-10, the Created and Modified time of the link file are the same. This means that the file (Pier.jpg) was only opened once.

Here is a timeline of the file Pier.jpg (All UTC):



Figure 6-11 - Timeline of Pier.jpg Based on Link File

Since the last time this picture was modified is BEFORE the time it was created in that folder, it is likely that this file was copied to the Pictures folder.

### **Example 2 (Files Opened More than Once)**

Take a look at the file called Cheetos.lnk and click on the Results view. Autopsy will show that this link file is pointing to a "Cheetos.jpg" in E:\Coupons. This is important to note, because this could mean that Craig had plugged in and used an external drive since it is found on something other than the C: drive.

Hex Strin	gs File Metadata Results Indexed Text Media
Res 1	of 1 Re < 🔿
Recent Docur	nents
Path	E:\Coupons\Cheetos.jpg
Path ID	-1
Date/Time	2013-12-18 19:42:32
Source	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Roaming/Microsoft/Windows/Recent/Cheetos.Ink
File Path	

Figure 6-12 - Link File Shows Path of Cheetos.jpg

Next, take a look at the embedded date and time stamps in the Cheetos.Ink file.

Hex	Stri	ings	5	File	e M	eta	data	F	Resi	Ilts	Ind	exe	ed T	Text	L M	edi	а		
Pa	•	1	C	f	1	111	P		<	- >	C	io t	o F	age	e:	1			Jump to Offset
0x000	0000	0: 4	1C	00	00	00	01	14	02	00	00	00	00	00	CO	00	00	00	L
0x000	0001	0: 0	00	00	00	46	93	00	20	00	20	00	00	00	AO	19	83	6E	Fn
0x000	0002	0: 2	28	FC	CE	01	00	00	21	7B	59	FD	CE	01	00	A1	90	6C	(!{Y1
0x0000	0003	0: 1	78	F1	CD	01	2A	96	01	00	00	00	00	00	01	00	00	00	
0x0000	0004	0: 0	00	00	00	00	00	00	00	00	00	00	00	00	E7	00	14	00	
0x000	0005	0: 1	LF	50	EO	4F	DO	20	EA	3A	69	10	A2	D8	08	00	2B	30	.P.O:i+0
0x0000	0006	0: 3	80	9D	19	00	2F	45	3A	SC	00	00	00	00	00	00	00	00	0/E:\
0x000	0007	0:0	00	00	00	00	00	00	00	00	00	00	00	56	00	31	00	00	V.1
0x0000	0008	0: 0	00	00	00	92	43	88	90	10	00	43	4F	55	50	4F	4E	53	CCOUPONS
0x0000	0009	0:0	00	40	00	09	00	04	00	EF	BE	92	43	88	9C	92	43	00	.@CC.
0x0000	000a	0: 4	10	2E	00	00	00	60	85	6E	00	00	00	00	00	00	00	00	@`.n
0x0000	000b	0:0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	43	C
0x0000	000c	0: 0	00	6F	00	75	00	70	00	6F	00	6E	00	73	00	00	00	16	.o.u.p.o.n.s

Figure 6-13 - Embedded Creation, Last Access, and Last Write Times of Cheetos.jpg

Use the DCode tool to decode the embedded time stamps. You should have the following time stamps:

Embedded Creation Time (UTC): Wed, 18 December 2013 19:36:22 UTC

Embedded Access Time (UTC): Fri, 20 December 2013 08:00:00 UTC

Embedded Last Write Time (UTC): Mon, 14 January 2013 01:42:34 UTC

**Note:** You can tell a device is FAT32 based on the Last Access Time embedded in the link file. FAT32 does not track the time of the last accessed activity, only the date. In, DCode is reporting a last accessed date of 12/20/2013 and the time is 8:00 AM (UTC). DCode is attempting to report UTC by adding 8 hours to a field that by default reports 12:00 AM.

Next, take a look at the time stamps of the link file itself.

Name	Created Time	Modified Time	Access Time
ALL COUPONS.Ink	2013-12-18 20:07:21 GMT	2013-12-18 20:07:21 GMT	2013-12-18 20:07:21 GMT
AWESOME COUPO	N: 2013-12-20 21:43:07 GMT	2013-12-20 21:43:32 GMT	2013-12-20 21:43:32 GMT
Biology and Aggres	si 2013-12-18 23:15:30 GMT	2013-12-18 23:17:33 GMT	2013-12-18 23:17:33 GMT
Cheetos.Ink	2013-12-18 19:42:32 GMT	2013-12-20 21:17:12 GMT	2013-12-20 21:17:12 GMT
Coca- Cola.Ink	2013-12-20 21:17:27 GMT	2013-12-20 21:17:27 GMT	2013-12-20 21:17:27 GMT
Coupons (2).Ink	2013-12-18 19:42:16 GMT	2013-12-21 01:09:58 GMT	2013-12-21 01:09:58 GMT

Figure 6-14 - Date and Time Stamps of the Link File

The link file's Modified date and time is different from the Created date and time. This means that Craig opened the file more than once.

Here is a timeline for the file "Cheetos.jpg" (All UTC):



Figure 6-15 - Timeline of Cheetos.jpg Based on Link File

If a file has been opened more than two times, you will only know the FIRST time it was opened (Link Created) and the LAST time it was opened (Link Modified). Without other information, you will not know what the date and time stamps were when it was opened in between. The computer does not track the times in between,

### Example 3 (No Embedded Date/Time)

Another example you will want to look at is the MileyCyrus\_tongue.lnk. If you look at the link file in Hex view, you will see that there aren't any date and time stamps embedded in the link file.

Name	Created Time	Modified Time	Access Time
httpmail.live.comlnk	2013-12-17 23:42:05 GMT	2013-12-17 23:42:05 GMT	2013-12-17 23:42:05
Pad - Edited 2013.lnk	2013-12-21 01:01:41 GMT	2013-12-21 01:09:52 GMT	2013-12-21 01:09:52
Leaf Transmutation.Ink	2013-12-18 19:42:59 GMT	2013-12-18 19:42:59 GMT	2013-12-18 19:42:59
MileyCyrus_tongue.lnk	2013-12-27 07:41:31 GMT	2013-12-27 07:41:31 GMT	2013-12-27 07:41:31
Monster Drink Coupon.Ink	2013-12-17 23:32:34 GMT	2013-12-17 23:32:34 GMT	2013-12-17 23:32:34
Multiple Intelligences Theor	2013-12-18 19:45:00 GMT	2013-12-21 18:35:39 GMT	2013-12-21 18:35:39
My Stuff.Ink	2013-12-17 23:35:04 GMT	2013-12-18 00:48:30 GMT	2013-12-18 00:48:30
• 111			•
Hex Strings File Metadata Re	sults Indexed Text Media		
Pa 1 of 1 P	← → Go to Page: 1	Jump to Offset 0	
0x00000020: 00 00 00 00 00 00 00 0x00000030: 00 00 00 00 00 00 00 0x00000040: 00 00 00 00 00 00 00 0x00000050: 1F 54 25 48 1E 03 5	10         00<	10 10 10 10 10 10 10 10 10 10	

Figure 6-16 - No Embedded Time Stamps in Link File for MileyCyrus\_tongue.jpg

There are a few situations that can cause this to occur. If the user uses the function "Save as" on a picture when viewing a site using Internet Explorer, a link file will be created with no embedded date and time stamps. Once the user opens the file, embedded date and time stamps will be added in the link file. A link file is also created when a user does a "Save Image as" in Mozilla Firefox and Google Chrome. If the file isn't opened after it has been saved, there won't be any embedded date and time stamps as well.

With certain applications, if the user creates a file in an application and saves it, but never opens it, there won't be any embedded date and time stamps. Once they do open the file, embedded date and time stamps will be added to the link file.

If a user saves an email attachment but does not open it, there will be a link file with no embedded date and time stamps. This only applies to certain email client software programs, such as Windows Live Mail. Once the user actually opens the file, embedded date and time stamps will be added.

The Created time stamp of the link file shows when the picture was saved or created in an application. The Modified time stamp matches the Created time stamp because it was never opened.

If the file had been opened after it was saved, it would create date and time stamps embedded within the link file. The link file's Modified time stamp would show when the file was LAST opened.

So, if a link file has no embedded date and time stamps it means the user could have:

- 1) Used Save as on a picture in a website, but never opened the file
- 2) Created the file in an application, but never opened it
- 3) Saved an attachment through an email client software, but never opened the file

A link file with no embedded date and time stamps merely gives you an idea of where the file might have come from. Later, you will go through the user's email and Internet history. If you see the file as an email attachment or in their download history, you will know exactly where it came from.

#### Example 4 (File is Moved, Link File is Updated)

Now that you have an understanding of link files, let's take a look at how these can help in an investigation. Look at the link file called Underage\_lolita\_r@ygold\_001.lnk and click on the Results view.



Figure 6-17 – Path of Underage\_lolita\_r@ygold\_001.jpg

This link file shows that when the picture was opened, it was located in:

```
C:\Users\Craig\Pictures
```

If you go to that location, you will see that the picture is no longer there. Go back to the link file and look at the date and time stamps embedded in the link file.

Hex	Str	ring	S	File	e M	etad	data	R	lesi	Ilts	Ind	exe	ed 1	Text	M	ledi	а		
Pa 1	1	C	of	1		Ρ.		<	$\langle - \rangle$	Go to	o F	Page	:	1			Jump to Offset		
0x0000	0000	00:	4C	00	00	00	01	14	02	00	00	00	00	00	CO	00	00	00	L
0x0000	0001	L0:	00	00	00	46	9B	00	20	00	20	00	00	00	72	01	DA	73	F
0x0000	0002	20:	83	FE	CE	01	72	01	DA	73	83	FE	CE	01	00	90	EA	85	rg
0x0000	0003	30:	10	FE	CE	01	B5	93	08	00	00	00	00	00	01	00	00	00	
0x0000	0004	10:	00	00	00	00	00	00	00	00	00	00	00	00	4E	07	14	00	N
0x0000	0005	50:	1F	54	25	48	1E	03	94	7B	C3	4D	B1	31	E9	46	B4	4C	.T%H{.M.1.F.L
0x0000	0006	50:	8D	D5	20	00	00	00	1A	00	EE	BB	FE	23	00	00	10	00	
0x000x0	0007	70:	9F	AE	90	A9	3B	AO	80	4E	94	BC	99	12	D7	50	41	04	;NPA.
0x000x0	0008	80:	00	00	73	02	00	00	6D	02	81	19	14	10	43	02	20	00	<mark>s</mark> mC
0x0000	0005	:06	00	00	00	60	00	00	00	00	00	00	00	00	00	00	00	00	
0x0000	000a	a0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0x0000	DOOL	: 00	10	01	00	00	31	53	50	53	A6	6A	63	28	ЗD	95	D2	11	1SPS.jc(=
0x0000	0000	:0:	B5	D6	00	CO	4F	D9	18	DO	25	00	00	00	0B	00	00	00	

Figure 6-18 - Embedded Creation, Last Access, and Last Write Times of Underage\_lolita\_r@ygold\_001.jpg

Use the DCode tool to decode the embedded time stamps. You should have the following time stamps:

Embedded Creation Time (UTC): Sat, 21 December 2013 19:32:57 UTC

Embedded Access Time (UTC): Sat, 21 December 2013 19:32:57 UTC

Embedded Last Write Time (UTC): Sat, 21 December 2013 05:50:16 UTC

Next, take a look at the date and time stamps of the link file itself.

Table Thumbnail									
Name	Created Time	Modified Time	Access Time						
SonyPSP.Ink	2013-12-21 01:02:46 GMT	2013-12-21 01:14:07 GMT	2013-12-21 01:14:07 GMT						
The Evolutionary Steps of Fish.Ink	2013-12-18 19:45:47 GMT	2013-12-18 19:45:47 GMT	2013-12-18 19:45:47 GMT						
underage daughter R@ygold.lnk	2013-12-21 19:42:16 GMT	2013-12-21 19:43:21 GMT	2013-12-21 19:43:21 GMT						
Underage_lolita_r@ygold_001.lnk	2013-12-21 19:32:38 GMT	2013-12-21 19:33:05 GMT	2013-12-21 19:33:05 GMT						
Underage_lolita_r@ygold_002.lnk	2013-12-21 19:32:45 GMT	2013-12-21 19:33:10 GMT	2013-12-21 19:33:10 GMT						

Figure 6-19 - Date and Time Stamps of the Link File

The link file's Modified date and time is different from the Created date and time. This means that Craig opened the file more than once.



Here is a timeline for the file "Underage\_lolita\_r@ygold\_001.jpg" (All UTC):

Figure 6-20 - Timeline of Underage\_lolita\_r@ygold\_001.jpg Based on Link File

The embedded Last Write Time tells us that the file was last modified BEFORE the creation time. This indicates that the embedded Creation Time was when the picture was copied, not when it was actually created.

The link file was FIRST opened several seconds before the embedded Creation Time, which means it could have been opened on external media or in another folder before it was copied over.

When a file is opened in one location, it creates a link file. This is important to note that if a suspect then copies that same file to a different location and opens it there, a new link file is not created. The original link file is merely updated.

In this case, a link file was first created for the underage picture when it was opened in another location. When it was copied and opened in the Pictures folder, that same link file's embedded data was updated. The local path displays where it was last opened, and its embedded Creation Time is updated to when the file was copied to the Pictures folder.

You were able to determine the picture was opened somewhere else because the FIRST time it was opened was before the embedded Creation Time. In the next section, you will learn how jump lists can sometimes show other locations a file was opened in.

**Note:** This type of file naming is an indicator of child pornography. Searching for child pornography on this suspect's computer would be out of the scope of your original search warrant, which was just to search for coupons. In a normal investigation, you should obtain another search warrant to further investigate and see if the suspect had child pornography.
#### **Jump Lists**

Jump Lists were a new feature added to Windows 7. They are similar to the Windows shortcuts (link files) because they are designed to take a user directly to a specific file or directory used frequently or recently.



Figure 6-21 - Jump List for Microsoft Word

Jump lists are important to look at because they may contain information of file activity that is no longer present in the link files. However, you may also find file activity in link files but not in a jump list. It is important to note that these are two separate artifacts and will not always match up.

There are two sets of jump lists, which are called Destination files:

automaticDestinations, which are created and maintained by the operating system.

customDestinations, which are maintained by the specific application.

A jump list is basically a catalog of one or more link files associated with a specific application. This catalog stores the data in compound file binary (CFB) format. The jump lists are located in the following subdirectories for all versions of Windows:

C:\[username]\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

C:\[username]\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

There are various tools that you can use to review the contents of these files:

JumpLister from WoanWare: https://github.com/woanware/JumpLister

Windows Jump List Parser from TZWorks: http://www.tzworks.net

For this case, use JumpLister from WoanWare. To use this tool you need to first export the jump lists. Navigate to the folder in the Tucker image that contains them.

Each jump list file name starts with a hex value prefix. This prefix is the Application ID. A resource for looking up AppID's is located at:

```
http://forensicswiki.org/wiki/List of Jump List IDs
```

Go ahead and highlight all the jump list files in the AutomaticDestinations folder, right-click one, and select Extract File(s) (see Figure 6-22).



Figure 6-22 – Highlight Jump Lists in AutomaticDestinations, Right-Click and Select Extract File(s)

Extract these files to your case Export folder. Open up the JumpLister tool where you downloaded it, and then select File►Load.

File Tool	s Help	×
Export Exit	cation	
•		•

Figure 6-23 - Click Load in JumpLister

Navigate to your export folder that contains the jump list files. Highlight and select each jump list file and click Open.

If you click the jump list 46507-c9533998e1308d73.automaticDestinations-ms in JumpLister, you can see what pictures have been opened (see Figure 6-24).

File Tools Help			
File Name		Application	
46499-28c8b86deab5	49a1.automaticDestinations-ms		
46501-469e4a7982ce	a4d4.automaticDestinations-ms		
46502-46f433176bc0	b3d2.automaticDestinations-ms		
46504-4cb9c5750d51	c07f.automaticDestinations-ms		
46506-7e4dca802468	63e3.automaticDestinations-ms		L
46507-c9533998e130	8d73.automaticDestinations-ms	<b>←</b>	
46509-db53b23fd1ed	lbd46.automaticDestinations-ms		
🖃 Root 🔷	Name	Value	
- 1F: 2311 bytes	Local Base Path	E:\Pictures\Underage_lolita_r@ygold_001.jpg	ן
-1E: 2311 bytes	Working Path	<u></u>	٦
-1D: 617 bytes	Arguments		
-1C: 617 bytes	Flags	VolumeIDAndLocalBasePath	ľ
-1B: 1884 bytes	Attributes	Archive	
- 19: 550 bytes	Show Command	Normal	
-1A: 585 bytes	Created Timestamp	Saturday, December 21, 2013 5:57:35 AM	
- 18: 550 bytes	Accessed Timestamp	Saturday, December 21, 2013 8:00:00 AM	
-17: 558 bytes	Modified Timestamp	Saturday, December 21, 2013 5:50:16 AM	
- 16: 3316 bytes - 15: 1913 bytes	Drive Type	Removable	
15 1913 bytec	Serial No.	-1737476168	
-14: 561 bytes			- 1

Figure 6-24 - Individual Entries in Photos App Jump List

**Note:** This version of Jumplister does not display what application goes with the jump list c9533998e1308d73. This application is the Windows 8 "Photos" app and it is the default photo viewer in Windows 8. This application is also present in Windows 10.

In the bottom left pane, there are entries for individual files that have been opened. These entries are equivalent to a link file because they show where the file was located and it has the embedded date and time stamps.

The bottom left pane also has an entry called DestList (Destination List). This list is a summary of each entry (see Figure 6-25). There are three key fields that you want to focus your attention:

Number:	This number will be associated with the entry number in the bottom left pane
Date/Time:	This is the last time the file was accessed with the program
Data:	This is the file location and filename

<u>File Tools Help</u>		
🖻   🔌		
File Name		Application
46499-28c8b86deab54	19a1.aut	omaticDestinations-ms
16501-469e4a7982cea	4d4.auto	omaticDestinations-ms
46502-46f433176bc0b	3d2.aut	omaticDestinations-ms
46504-4cb9c5750d51c	07f.auto	omaticDestinations-ms
6506-7e4dca8024686	3e3.auto	omaticDestinations-ms
6507-c9533998e1308	3d73.aut	omaticDestinations-ms
16509-db53b23fd1edl	od46.aut	tomaticDestinations-ms
E: 1904 bytes		Data
B: 606 bytes		E:\Coupons\SonyPSP.JPG
- A: 1881 bytes		E:\Coupons\iPad - Edited 2013.png
-9: 1881 bytes		C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8
-8: 3278 bytes		E:\Pictures\Underage_lolita_r@ygold_001.jpg
- <mark>7: 1</mark> 889 bytes		E:\Pictures\Underage_lolita_r@ygold_002.jpg
- 6: 1892 bytes		C:\Users\Craig\Pictures\Underage_lolita_r@ygold_001.jpg
- 5: 1892 bytes		C:\Users\Craig\Pictures\Underage_lolita_r@ygold_002.jpg
-4: 3368 bytes		C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8
- 3: 1925 bytes	=	C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8
-2: 1916 bytes		C:\Users\Craig\Documents\My Stuff\Bagel Bites Coupon.jpg
- 1: 1919 bytes		C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8
DestList (9304 byt	es) 🔔	

Figure 6-25 - DestList in Jumplister

As you can see in Figure 6-25, the jump list shows the underage pictures that were opened on the E: drive. You did not have this information in the link files because the link files were updated.

You can see in the column Date/Time that the pictures Underage\_lolita\_r@ygold\_001.jpg and Underage\_lolita\_r@ygold\_002.jpg were opened on the E:\ drive and in the Pictures folder on the following dates:

Underage_lolita_r@ygold_001.jpg (E: Drive):	12/21/13 7:32:38 PM (UTC)
Underage_lolita_r@ygold_002.jpg (E: Drive):	12/21/13 7:32:45 PM (UTC)
Underage_lolita_r@ygold_001.jpg (Pictures Folder):	12/21/13 7:33:05 PM (UTC)
Underage_lolita_r@ygold_002.jpg (Pictures Folder):	12/21/13 7:33:10 PM (UTC)

**Note:** There are two other timestamps called Timestamp (New) and Timestamp (Birth). These are related to Object IDs, which is a more advanced topic. For now, just use the Date/Time stamp to determine when the file was first opened.

You can export out this jump list information to a CSV file by clicking File►Export

File Tools Help	
Load	
	Application
Export deab549a	1.automaticDestinations-ms
Exit	LautomaticDestinations-ms
	2.automaticDestinations-ms
5504-4cb9c5750d51c07f	automaticDestinations-ms
	B.automaticDestinations-ms
	3.automaticDestinations-ms
	6.automaticDestinations-ms
E: 1904 bytes	Data
- B: 606 bytes	E:\Coupons\iPad - Edited 2013.png
- A: 1881 bytes	C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps 8wekyb3d8
-9: 1881 bytes	E:\Pictures\Underage lolita r@ygold 001.jpg
-8: 3278 bytes	E:\Pictures\Underage lolita r@ygold_002.jpg
-7: 1889 bytes	C:\Users\Craig\Pictures\Underage lolita r@ygold 001.jpg
-6: 1892 bytes	C:\Users\Craig\Pictures\Underage_lolita_r@ygold_002.jpg
-5: 1892 bytes	C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8
-4: 3368 bytes	C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps_overlybsde
- 3: 1925 bytes	
- 2: 1916 bytes	C:\Users\Craig\Documents\My Sturt\Bagel Bites Coupon.jpg C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8
- 1: 1919 bytes	C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps_owekyb3d8
DestList (9304 bytes)	

Figure 6-26 - Export Jump List Information to CSV File

Export the files to your case's Export Folder. Now, open up Excel and go to the Data tab. Click "From Text" under "Get External Data".

🖾 🖬 🔊 - (° -   <del>-</del>	Booki	L - Microsoft	Excel	_ (	
File Home Insert	Page Layout	Formulas	Data Review	View 🛆 🕜	- # X3
Get External Data ~ All ~ C	Sort Filter	Clear Reapply Advanced	Columns Dupli	ove Outline	e
Connections	Sort & Fil	ter	Data To	DOIS	
A1 •	(* <i>f</i> x				¥
		D	E	F G	⊢ F ▲
From From From From Access Web Text Source Get External D	ces • Connectio				=
4					
5					
6					
7					
8					
9					-
H + + H Sheet1 She	et2 / Sheet3	/92/		III	
Ready			100%	Θ	

Figure 6-27 - Get External Data from Text to Open CSV File

Navigate to your Tucker Export\Jumplist folder and open the file DestList.csv. A window will open and prompt you to choose your text import options. Pick Delimited and click Next (see Figure 6-28).

Text Import Wizard - Step 1 of 3
The Text Wizard has determined that your data is Delimited.
If this is correct, choose Next, or choose the data type that best describes your data.
Original data type
Choose the file type that best describes your data:
Delimited - Characters such as commas or tabs separate each field.
Fixed width - Fields are aligned in columns with spaces between each field.
Start import at row: 1 File origin: Windows (ANSI)
Preview of file C:\Users\Demo\Desktop\DestList.csv.
1 File Name, Application, Stream No., NetBIOS Name, Date/Time, MAC (New), Timestamp (New), 2 c9533998e1308d73.automaticDestinations-ms, 1, win-bk3j6tfmhll, 12/17/2013 11:31:02 F
3c9533998e1308d73.automaticDestinations-ms,,10,win-bk3j6tfmhl1,12/20/2013 9:16:06 F
4 c9533998e1308d73.automaticDestinations-ms,,11,win-bk3j6tfmhll,12/20/2013 9:16:19 F 5 c9533998e1308d73.automaticDestinations-ms,,12,win-bk3j6tfmhll,12/20/2013 9:16:53 F
6 c9533998e1308d73.automaticDestinations-ms.,12,Win-bb396thm11,12/20/2013 9.16:57 F
< <u> </u>
Cancel < Back <u>N</u> ext > <u>F</u> inish

Figure 6-28 - Import DestList.csv as Delimited

Text Import Wizard - Step 2 of 3	? 🗙
This screen lets you set the delimiters your data contains.	You can see how your text is affected in the preview below.
Delimiters          Iab         Semicolon         Comma         Text gualifier:         Space         Other:	as one
File Name	Application Stream No. NetBIOS Name Dat 🔺
c9533998e1308d73.automaticDestinations-ms c9533998e1308d73.automaticDestinations-ms	
c9533998e1308d73.automaticDestinations-ms	
c9533998e1308d73.automaticDestinations-ma	
c9533998e1308d73.automaticDestinations-ms	
< □	1
Can	el < <u>B</u> ack <u>N</u> ext > <u>F</u> inish

Figure 6-29 - Set Comma as Delimiter

This will give you a clean report of the jump list information (see Figure 6-30).

File Name	Date/Time	Data
c9533998e1308d73.automaticDestinations-ms	12/17/2013 23:31	C:\Users\Craig\AppData\Local\Packages\microsoft.windowscom
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:16	C:\Users\Craig\Pictures\desk_setup.jpg
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:16	C:\Users\Craig\Pictures\School\SMC_Library.jpg
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:16	C:\Users\Craig\Pictures\Santa Monica\Park.jpg
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:16	C:\Users\Craig\Pictures\Santa Monica\Pier.jpg
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:17	E:\Coupons\Coca- Cola.jpg
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:26	C:\Users\Craig\AppData\Local\Packages\microsoft.windowscom
c9533998e1308d73.automaticDestinations-ms	12/20/2013 21:28	C:\Users\Craig\Documents\Guides\HowtoMakeCoupons.jpg
c9533998e1308d73.automaticDestinations-ms	12/21/2013 0:55	E:\Coupons\GiftCards.jpg

Figure 6-30 - CSV of Jump List Information

If you click on one of the cells in the top row and then click the Filter button under the Data tab, you can easily filter for specific text or sort the columns.

X	J 19 -	(" -   ∓			Book1 -	Microsoft	Excel			_ 0	1 🛛
F	ile H	ome Insert	Page	Layout	Formulas	Data	Review	v View		○ ? -	er XX
Get E	External Re	Conr fresh Connection	erties Links	Â↓ Â Z↓ So	_	K Clear Reap Advar	· ·	Text to Rem columns Dupli Data Te	cates 🖙 🔹	<ul> <li>⇒ Group +</li> <li>↓ Ungroup +</li> <li>Subtotal</li> <li>Outline</li> </ul>	egi egi Es
	J1	•	(*	$f_x$	Data						¥
				J				K	L	Μ	
1	Data							· ]			
2	-				-	rosoft.wi	ndows	communic	ationsapp	s_8wekyb3d8	bbwe
3	C:\Users	Craig\Pictu	ures\des	k_setup	o.jpg						
4		Craig\Pictu									
5		Craig\Pictu				-					
6	C:\Users	Craig\Pictu	ures\San	ta Mon	ica\Pier.jp	g					
7		ons\Coca- C									
8									ationsapp	s_8wekyb3d8	bbwe
9		Craig\Doci		Guides	HowtoMa	keCoupo	ns.jpg				
10	10 E:\Coupons\GiftCards.jpg										
11	11 E:\Coupons\Shavers.png										
12		ons\SonyPS									
13	E:\Coup	ons\iPad - E	dited 20	13.png							-
	( ) ) S	heet1 She	et2 / Sł	neet3 /	to/``		i   4				
Rea	dy								100% —	0	-+:

Figure 6-31 - Filter Function in Excel under Data Tab

By clicking the arrow at the end of each column header, you can select filters such as Text Filters ► Begins With. These are helpful if you want to only view files on external media or just on the C: drive.

Custom AutoFilter	? 🗙
Show rows where: Data	
begins with E:\	•
	×
Use ? to represent any single character Use * to represent any series of characters	
	OK Cancel

Figure 6-32 - Text Filter Begins with E:\



## **Computer Forensics CCIC Training**

### Chapter 7: Recycle Bin

Lauren Pixley, Cassidy Elwell, and James Poirier May 2019 (Version 1)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

## 7

## **Recycle Bin**

#### Introduction

Since the file "Underage\_lolita\_r@ygold\_001.jpg is no longer in the Pictures folder and you don't have Craig's E: drive, you should see if it was deleted. Most computer users believe that when a file is deleted and the recycling bin is emptied, that the file cannot be accessed. However, deleting a file can still leave data behind for recovery. This is because when a file is deleted, the data is only marked as deleted by the computer and allows that area of the disk to be available for storing new data. It's not until the user overwrites this area of the disk that the data is actually deleted. Even part of the original file may still be recoverable if the user only overwrote a portion of the disk space. Therefore, this data can be recovered by investigators. This process is known as "file carving."

#### **\$R and \$I Files**

The first time a user deletes a file, the file is not actually deleted. A new folder is created in the Recycle Bin, and the deleted files are moved to it. The folder that is created is named after the security identifier (SID) and the relative ID (RID) of the associated user. You can use this information to determine which user account deleted the file. You are going to look at Craig's Recycle Bin (see Figure 7-1), which is located in:

C:\\$Recycle.Bin\S-1-5-21-1049150138-4017234595-3791460656-1001

ults Directory Listing /img_Tucker.E01_vol_vol2/\$F Table Thumbnail Name Ucurrent folder]	Recycle.Bin/S-1-5-21-1049150138-40 Created Time 2013-12-17 23:12:05 GMT	Modified Time 2013-12-27 08:45:34 GMT
Table Thumbnail     Name     [current folder]	Created Time 2013-12-17 23:12:05 GMT	Modified Time
[current folder]	2013-12-17 23:12:05 GMT	
		2013-12-27 08:45:34 GMT
[parent folder]		
	2013-08-22 15:36:31 GMT	2013-12-17 23:12:05 GM
s18MHF6S.jpg	2013-12-27 07:27:06 GMT	2013-12-27 07:27:06 GM
sIGQWXSI.jpg	2013-12-27 07:27:09 GMT	2013-12-27 07:27:09 GM
sIVWUORQ.wmv	2013-12-27 08:45:34 GMT	2013-12-27 08:45:34 GM
SR8MHF6S.jpg	2013-12-21 19:32:57 GMT	2013-12-21 05:50:16 GM
≡ SRGQWXSI.jpg	2013-12-21 19:32:57 GMT	2013-12-21 05:56:30 GM
sRVWUORQ.wmv	2013-12-21 19:43:02 GMT	2013-12-02 05:00:54 GM
🕒 desktop.ini	2013-12-17 23:12:05 GMT	2013-12-17 23:12:05 GM
	<ul> <li>\$IGQWXSI.jpg</li> <li>\$IVWUORQ.wmv</li> <li>\$R8MHF6S.jpg</li> <li>\$R8QWXSI.jpg</li> <li>\$RQWXSI.jpg</li> <li>\$RVWUORQ.wmv</li> </ul>	Image: Start

Figure 7-1 - Craig's Recycle Bin

**Note:** If a user deletes a file using the command prompt or does Shift+Del, the file bypasses the Recycle Bin and it is deleted right away.

Both file names contain 6 identical, random characters and its original extension, preceded by either \$I or \$R. The I file contains information about the deleted file including the file's size, deleted time, path, etc. The R file contains the actual deleted file itself.

Table Thumbnail					
Name	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]	2013-12-27 00:45:34	2013-12-27 00:45:34	2013-12-27 00:45:34	2013-12-17 15:12:05	56
[parent folder]	2013-12-17 15:12:05	2013-12-17 15:12:05	2013-12-17 15:12:05	2013-08-22 08:36:31	328
\$I8MHF6S.jpg	2012 12 26 22:27:06	2012 12 26 22 27 26	2013-12-26 23:27:06	2013-12-26 23:27:06	544
■\$IGQWXSI.jpg 🗲	20 EMBEDDED	) Information	2013-12-26 23:27:09	2013-12-26 23:27:09	544
\$IVWUORQ.wmv	2015 12 27 00.15.51	2013 12 27 00.13.31	2013-12-27 00:45:34	2013-12-27 00:45:34	544
\$R8MHF6S.jpg	2012 12 20 21 50 16	2013-12-26 23:27:06	2013-12-21 11:32:57	2013-12-21 11:32:57	562101
🛎 \$RGQWXSI.jpg 🗲	20 Original File	e .3-12-26 23:27:09	2013-12-21 11:32:57	2013-12-21 11:32:57	626337
\$RVWUORQ.wmv	2013-12-01 21.00.34	2013-12-27 00:45:34	2013-12-21 11:43:02	2013-12-21 11:43:02	807672
desktop.ini	2013-12-17 15:12:05	2013-12-17 15:12:05	2013-12-17 15:12:05	2013-12-17 15:12:05	129

Figure 7-2 - \$I and \$R Files

In Autopsy, look at the \$I file called \$IGQWXSI.jpg and click the Strings view. You will see the path of where \$IGQWXSI.jpg was originally stored on the computer before the user deleted the file.

Name	Created Time	Modified Time
[current folder]	2013-12-17 23:12:05 GMT	2013-12-27 08:45:34 GM
[parent folder]	2013-08-22 15:36:31 GMT	2013-12-17 23:12:05 GM
s18MHF6S.jpg	2013-12-27 07:27:06 GMT	2013-12-27 07:27:06 GM
🗟 \$IGQWXSI.jpg 🔫 🗕	2013-12-27 07:27:09 GMT	2013-12-27 07:27:09 GM
SIVWUORQ.wmv	2013-12-27 08:45:34 GMT	2013-12-27 08:45:34 GM
sR8MHF6S.jpg	2013-12-21 19:32:57 GMT	2013-12-21 05:50:16 GM
📓 \$RGQWXSI.jpg	2013-12-21 19:32:57 GMT	2013-12-21 05:56:30 GM
sRVWUORQ.wmv	2013-12-21 19:43:02 GMT	2013-12-02 05:00:54 GM
🖲 desktop.ini	2013-12-17 23:12:05 GMT	2013-12-17 23:12:05 GM
•		
Hex Strings File Metadata	Results Indexed Text Media Previe	W
Pa 1 of 1 P	← → Go to Page:	Script: Latin - Basic

Figure 7-3 - \$IGQWXSI File Shows Location and Name of File Before Deletion

Next, if you view \$IGQWXSI.jpg in Hex view, you can see there is EMBEDDED data regarding the file before it was deleted. There are three pieces of critical information: the Windows version, file size, and time and date.

Name	Modified Time	Change Time	Access Time	Created Time	Size
[current folder]	2013-12-27 00:45:34	2013-12-27 00:45:34	2013-12-27 00:45:34 .	2013-12-17 15:12:05	56
[parent folder]	2013-12-17 15:12:05	2013-12-17 15:12:05	2013-12-17 15:12:05 .	2013-08-22 08:36:31	328
si8MHF6S.jpg	2013-12-26 23:27:06	2013-12-26 23:27:06	2013-12-26 23:27:06 .	2013-12-26 23:27:06	544
🛚 \$IGQWXSI.jpg 🗲	2013-12-26 23:27:09	2013-12-26 23:27:09	2013-12-26 23:27:09 .	2013-12-26 23:27:09	544
#\$IVWUORQ.wmv	2013-12-27 00:45:34	2013-12-27 00:45:34	2013-12-27 00:45:34 .	2013-12-27 00:45:34	544
sR8MHF6S.jpg	2013-12-20 21:50:16	2013-12-26 23:27:06	2013-12-21 11:32:57 .	2013-12-21 11:32:57	562101
sRGQWXSI.jpg	2013-12-20 21:56:30	2013-12-26 23:27:09	2013-12-21 11:32:57 .	2013-12-21 11:32:57	626337
\$RVWUORQ.wmv	2013-12-01 21:00:54	2013-12-27 00:45:34	2013-12-21 11:43:02 .	2013-12-21 11:43:02	8076724
desktop.ini	2013-12-17 15:12:05	2013-12-17 15:12:05	2013-12-17 15:12:05 .	. 2013-12-17 15:12:05	129
Ļ					
Hex Strings File Metad	data Results Indexed Tex				
1 of 1	So to Page:	Jump to Offset 0	20.00		3
	Go to Page:				3
1 of 1 0x00000000: 01 00 0x00000010: 60 92 0x00000020: 73 00	Go to Page: 00 00 00 00 00 00 7A 0D D5 02 CF 01 65 00 72 00 73 00	Jump to Offset         0           A1         8E         09         00	55 00 `.zC.:.\ 51 00 s.e.r.s.\.C.r	.a.	;
1 of 1 0x00000000: 01 00 0x00000010: 60 92 0x00000020: 73 00 0x00000030: 69 00	Go to Page:           00         00         00         00           7A         0D         D5         02         CF         01           65         00         72         00         73         00           67         00         5C         00         50         00	Jump to Offset         0           A1 8E 09 00         00 00 00           43 00 3A 00 5C 00         5C 00 4           5C 00 43 00 72 00         69 00 63 00 74 00	55 00 `.zC.:.\ 51 00 s.e.r.s.\.C.r 75 00 i.g.\.P.i.c.t	.a. .u.	;
1 of 1 0x00000000: 01 00 0x00000020: 73 00 0x00000030: 69 00 0x00000040: 72 00	Go to Page:           00         00         00         00         00           7A         0D         D5         02         CF         01           65         00         72         00         73         00           65         00         73         00         50         00           65         00         73         00         50         00	Jump to Offset         0           A1         8E         09         00         00         00           43         00         3A         00         5C         00         5C           5C         00         43         00         72         00         6           69         00         63         00         74         00         75           55         00         6E         00         64         00         64	55 00     `.zC.:.\       51 00     s.e.r.s.\.C.r       75 00     i.g.\.P.i.c.t       55 00     r.e.s.\.U.n.c	a. u. i.e.	
1 of 1 0x00000000: 01 00 0x00000010: 60 92 0x00000020: 73 00 0x00000030: 69 00 0x00000040: 72 00 0x00000050: 72 00	Go to Page:           00         00         00         00         00           7A         0D         D5         02         CF         01           65         00         72         00         73         00           65         00         72         00         73         00           65         00         73         00         65         00           65         00         73         00         65         00	Jump to Offset         0           A1 BE 09 00         00 00           43 00         3A 00         5C 00           5C 00         43 00         72 00           69 00         63 00         74 00           55 00         62 00         64 00           55 00         6C 00         67 00	55 00       `.zC.:.`         51 00       s.e.r.s.\.C.r         75 00       i.g.\.P.i.c.t         55 00       r.e.s.\.U.n.c         55 00       r.a.g.el.c.t	a. u. l.e. 0.1.	
1 of 1 0x00000000: 01 00 0x00000000: 60 92 0x000000000: 73 00 0x00000000: 69 00 0x00000000: 72 00 0x00000000: 72 00 0x00000000: 69 00	Co to Page:           00 00 00 00 00 00           7A 0D D5 02 CF 01           65 00 72 00 73 00           65 00 73 00 50 00           65 00 73 00 50 00           65 00 73 00 55 00           74 00 61 00 55 00	Jump to Offset         0           A1         82         09         00         00         00           43         00         3A         00         5C         00         5           5C         00         43         00         72         00         6           69         00         63         00         74         00         7           55         00         62         00         64         00         65         00           57         00         62         00         67         00         67         00           72         00         40         00         79         00         67         00	35     00     `.zC.:.`       51     00     s.e.r.s.\.C.:       75     00     i.g.\.P.i.c.:       55     00     r.e.s.\.U.n.c.       56     00     r.e.s.\.U.n.c.       56     00     r.a.g.el.c.       57     00     i.t.ar.e.g.s	  i.e. 0.1. 7.g.	
1 of 1 0x0000000: 01 00 0x00000010: 60 92 0x00000020: 73 00 0x00000000: 69 00 0x00000050: 72 00 0x00000050: 72 00 0x00000050: 69 00 0x0000070: 65 00	Co to Page:           00         00         00         00         00           7A         0D         D5         02         CF         01           65         00         72         00         50         00         60           70         05         C0         50         00         61         00         61         00         61         00         74         00         65         00         74         00         57         00         55 <t< td=""><td>Jump to Offset         0           Å1         82         09         00         00         00           43         00         3A         00         5C         00         43           5C         00         43         00         7C         00         69         00         65         00         65         00         65         00         65         00         65         00         65         00         65         00         67         00         60         30         00</td><td>35     00     `.zC.:.`       51     00     s.e.r.s.\.C.r       75     00     i.g.\.P.i.c.t       55     00     r.e.s.\.U.n.c       56     00     r.a.g.el.c.t       57     00     i.t.ar.@.j       22     00     o.l.d0.0.2</td><td></td><td>2</td></t<>	Jump to Offset         0           Å1         82         09         00         00         00           43         00         3A         00         5C         00         43           5C         00         43         00         7C         00         69         00         65         00         65         00         65         00         65         00         65         00         65         00         65         00         67         00         60         30         00	35     00     `.zC.:.`       51     00     s.e.r.s.\.C.r       75     00     i.g.\.P.i.c.t       55     00     r.e.s.\.U.n.c       56     00     r.a.g.el.c.t       57     00     i.t.ar.@.j       22     00     o.l.d0.0.2		2
1 of 1 0x00000000: 01 00 0x00000000: 60 92 0x000000000: 73 00 0x00000000: 69 00 0x00000000: 72 00 0x00000000: 72 00 0x00000000: 69 00	So to Page:           00         00         00         00         00           7A         0D         D5         02         CF         01           65         00         72         00         73         00         60         00           70         05         C         05         00         73         00         60         00           65         00         73         00         52         00         61         00         67         00         60         00         74         00         61         00         70         00         70         65         00         74         00         61         00         57         00         74         00         61         00         57         00         74         00         61         00         55         00         70         00         70         00         70         00         70         00         70         00         70         00         70         00         70         70         70         70         70         70         70         70         70         70         70         70         70         70	Jump to Offset         0           A1         82         09         00         00         00           43         00         3A         00         5C         00         5           5C         00         43         00         72         00         6           69         00         63         00         74         00         7           55         00         62         00         64         00         65         00           57         00         62         00         67         00         67         00           72         00         40         00         79         00         67         00	55 00       '.zC.:\'         51 00       s.e.r.s.\C.:         75 00       i.g.\.P.i.c.:         55 00       r.e.s.\U.n.c         56 00       r.a.g.el.c         57 00       i.t.ar.e.s         57 00       i.t.ar.e.s         58 00       r.a.g.el.c         50 0       r.a.g.el.c         50 0       r.a.g.el.c         50 0       i.t.ar.e.s         50 0       j.p.g		2

Figure 7-4 – Embedded Data in \$IGQWXSI File

The first 8 bytes of the \$I file tell you the Windows version the file was created on. If the first byte is "01" then the user's computer was running Windows 8 and "02" if the user was running Windows 10. The second set of 8 bytes (starting at offset 8) represent the size of the original file.

	1 of	1			< )	G	o to	Pag	e:		10	mp	to (	Offset	0				
								, ag			Ju	mp		511500					
x000	0000	0:	01	00	00	00	00	00	00	00	A1	8E	09	00	00	00	00	00	
x000	0001	0:	60	92	7A	0D	D5	02	CF	01	43	00	ЗA	00	5C	00	55	00	`.zC.:.\.U.
x000	0002	0:	73	00	65	00	72	00	73	00	5C	00	43	00	72	00	61	00	s.e.r.s.\.C.r.a.
x000	0003	0:	69	00	67	00	5C	00	50	00	69	00	63	00	74	00	75	00	i.g.\.P.i.c.t.u.
x000	0004	0:	72	00	65	00	73	00	5C	00	55	00	6E	00	64	00	65	00	r.e.s.\.U.n.dve.
x000								þ	65	00	5F	00	6C	00	6F	00	6C	00	r.a.g.
x000		'n	ao	ws	V V	ersi	on	þ	5F	00	72	00	40	00	79	00	67	00	i.t.a. File Size
x000		υ.	02		00	00		60	5F	00	30	00	30	00	32	00	2E	00	0.1.d
x000	0008	0:	6A	00	70	00	67	00	00	00	00	00	00	00	00	00	00	00	j.p.g
x000	0009	0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
x000	000a	0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
x000	000b	0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
x000	000c	0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
x000	000d	0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
x000	000e	0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
x000	000f	0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Figure 7-5 – Embedded Information on Windows Version and Size of File

The hex value of the file size is represented in "Little Endian" format which means the little end is read first. To convert this into human-readable information you must read the hex value with the larger order first (read the sets of two digits from right to left). Therefore, you would convert from "Little Endian" as follows:

I Untitled - Notepad	-		$\times$
File Edit Format View Help			
HEX OFFSET 0x8 OF A1 8E 09> 09		I.JPG	^
			~
<			> .

Figure 7-6 – Convert Little Endian Format by Reading Data Right to Left

Then convert this hex value to a decimal to get the file size in bytes by using a conversion calculator. To do so, you are going to use the following website:

http://www.rapidtables.com/convert/number/hex-to-decimal.htm

Once you have this calculator open, type your converted human-readable hex value into the "Enter hex number" box and then click "Convert".

Hex to Decimal converter	
Enter hex number: 098EA1	16
C Convert * Reset t Swap	
Decimal number:	
626337	10
Decimal from signed 8/16/32 bit:	
	10
Binary number:	
10011000111010100001	2

Figure 7-7 – Type in Converted File Size Hex Value from \$\$IGQWXSI.jpg and Click Convert

The value displayed in the "Decimal number" box in the conversion calculator is the size of the file before it was deleted by the user in bytes.

Next, encoded in the hex value of \$IGQWXSI.jpg is the date and time stamp of when the file was deleted.

	1	of	1		< -)	G	o to	Pag	e:		Ju	mp	to (	Offset	0				
		000:	01	00	00	00	00	00	00	00	A1	07	09	00	00	00	00	00	
		010:								01			3A			00			
		020:							73				43		72				
		030:							50		69			00	74				
	000	040:	72	00	65	00	773	00	SC	00	55	00	6E	00	64	00	65	00	
¢٥٥					_		<u> </u>			~.			6C	00	6F	00	6C	00	r.a.g.e1.o.1.
:00		DEI	.E I	ΕD	Da	ate	ð.	IIn	ne	Star	np		40	00	79	00	67	00	i.t.ar.@.y.g.
:00						0.0				0.0			30	00	32	00	2E	00	o.l.d0.0.2
:000	00	080:	6A	00	70	00	67	00	00	00	00	00	00	00	00	00	00	00	j.p.g
:000	00	090:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
:000	00	0a0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
:000	00	0ъ0:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
-000	0.0	0c0:	0.0	0.0	0.0	0.0	0.0	0.0	00	0.0	0.0	00	00	0.0	0.0	00	0.0	0.0	
		0d0:							00				00			00			
		0e0:							00		00		00			00			
		oeu:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
		0£0:							00		00			00		00			

Figure 7-8 – Embedded Deleted Time Stamp in \$IGQWXSI.jpg

To decode the timestamp, you are going to once again use the DCode (Version 4.02a) tool. Once you have DCode open, you need to copy the time stamp from the Hex tab of the selected \$I file which begins at offset 16 and is 8 bytes in length. Then, set the Decode Format to Windows: 64 bit Hex Value - Little Endian. Click the Decode button to see the decoded Date and Time. You should have Fri, 27 December 2013 07:27:06 UTC for when the file Underage\_lolita\_r@ygold\_002.jpg was deleted from the user's Pictures folder (see Figure 7-9).

2 DCode v4.02a (Build: 9306)	×
Convert Data to Date / Time Values Add Bias: UTC 00:00 Decode Format: Windows: 64 bit He Example: FF03D2315FE1C	
Value to Decode: 0006A00BD502CF0 Date & Time: Fri, 27 Decembe	
www.digital-detective.co.uk	Cancel Clear Decode

Figure 7-9 – Copy Deleted Time Stamp, Set Format to Little Endian, and Click Decode

**Note:** This encoded date is important to decode since Autopsy does not automatically provide the Deleted time in its platform. This often helps with creating timelines in analysis.

Now, look at the file called \$RGQWXSI.jpg and click on Media view. You will see a preview of the file that was deleted by the user. In this case, you should see a .jpg picture.

Table Thumbnail		
Name	Created Time	Modified Time
🔄 \$R8MHF6S.jpg	2013-12-21 19:32:57 GMT	2013-12-21 05:50:16 GMT
🖺 \$RGQWXSI.jpg 🔫—	2013-12-21 19:32:57 GMT	2013-12-21 05:56:30 GMT
🗐 \$RVWUORQ.wmv	2013-12-21 19:43:02 GMT	2013-12-02 05:00:54 GMT
🖲 desktop.ini	2013-12-17 23:12:05 GMT	2013-12-17 23:12:05 GMT
۰ III		
Hex Strings File Metadata	esults Indexed Text Media Previe	W
	CRIME SCENE - DO NOT CROSS	

Figure 7-10 – Preview \$RGQWXSI.jpg with Media View

**Note:** Throughout these practice and test images, you may see pictures with crime scene tape. These are the simulated child pornography images, and you should tag any of these images since they are important to your investigation.



### **Computer Forensics CCIC Training** Chapter 8: External Storage Devices

Lauren Pixley, Cassidy Elwell, and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

## 8

## **External Storage Devices**

#### Introduction

When you looked at Craig's link files and jump lists, some of the data was pointing to an E: drive, which was a removable disk. These link files pointed back to potential fraudulent coupons and CP. Now that you are aware of the suspect's external E: drive, you need to know more about it. It is also important for you to learn more about USB devices and what information is stored when they are plugged into a computer.

USB devices are designed under USB Bus specifications, which describe the design and technical details for manufacturing them. From a forensics viewpoint, there are a couple of technical details under the Standard USB Descriptors Definitions that help to identify a specific USB device. Each USB device contains information that is embedded at the time of manufacturing.

You can use a freeware tool, such as Microsoft's Universal Serial Bus Viewer (USBView) to read the information. USBView can list USB host controllers, USB hubs, and attached USB devices. The following information for a SanDisk, U3 Cruzer Micro, 2GB thumb drive was extracted using USBView:

```
===>Device Descriptor<===
bLength:
                           0x12
                           0x01
bDescriptorType:
bcdUSB:
                           0x0200
bDeviceClass:
                           0x00->This is an Interface Class Defined Device
                           0x00
bDeviceSubClass:
bDeviceProtocol:
                           0x00
bMaxPacketSize0:
                           0x40 = (64) Bytes
idVendor:
                           0x0781 = SanDisk Corporation
idProduct:
                           0x5406
bcdDevice:
                           0x0200
iManufacturer:
                           0x01
English (United States)
                          "SanDisk"
iProduct:
                           0x02
                           "U3 Cruzer Micro"
English (United States)
iSerialNumber: 0x03
English (United States)
                           "43174013F2C14667"
bNumConfigurations:
                           0x01
```

The key fields of information that can be relevant to a forensic investigation are:

Vendor ID (idVendor) Product ID (idProduct) Manufacturer (iManufacturer) Product (iProduct) Serial Number (iSerialNumber)

Since I physically possessed the device, I could confirm the accuracy of the information listed by USBView. I could see that the device was in fact a SanDisk U3 Cruzer Micro. However, the serial number was not stamped on the exterior of the device. You should also be aware that while some devices may have a serial number that is visible, it may not match the serial number that is embedded in the USB circuit board.

No matter what serial number is stamped on the exterior, you will always want to check the internal serial number, which is also called the iSerialNumber.

The Vendor ID, which is 2 bytes in length, is assigned by the USB Implementers Forum, Inc. Each vendor is assigned a unique ID.

The Product ID is also 2 bytes in length, but it is randomly assigned by the manufacturer. A good reference for Vendor and Product ID's can be found at the following website:

http://www.linux-usb.org/usb.ids

Although the information on this website shouldn't be considered authoritative, since it's submitted by individuals, it is a good starting point to look up information that may match the Product ID.

Another freeware tool that can be used to read a USB device is USBDeview, which can be downloaded from:

http://www.nirsoft.net

🛱 USBDeview						×				
File Edit View Options Help										
×⊚ ● ● ● [	] () () () () () () () () () () () () ()									
Device Name	Description	Serial Number	VendorID	ProductID	Drive Letter					
CodeMeter-Stick	WIBU - CodeMeter-Stick USB Device	0001188755	064f	03e9	I:	Ξ				
Backup+ BK     BK     Backup+ BK     BK     Backup+ BK     BK     Backup+	Seagate Backup+ BK USB Device	NA53T044	0bc2	a003	G:					
Backup+ BK     BK     Backup+ BK     BK     Backup+ BK     BK     Backup+	Seagate Backup+ BK USB Device	NA53Z37E	0bc2	a013	J:	Ŧ				
III.					4					
76 item(s), 1 Selected	NirSoft Freeware.	http://www.nirsoft.n	et usb.ids	is not loade	ed					

Figure 8-1 – USBDeview

#### Windows Plug and Play

Now that you know what information is embedded in a USB device, you need to understand what happens when a USB device is plugged into a Windows-based computer.

The plug and play manager extracts information from the USB device when it is first plugged into a Windows computer. As you can see in Figure 8-2, it records that information in several locations.



Figure 8-2 - Information Recorded when USB is Connected

#### **Autopsy Devices Attached**

When you ran modules earlier on Autopsy, it pulled different information from the registry, including devices connected.

ase View Tools	Name and Annual Annu					
🛉 Add Data Sour	rce 📠 View Images/Videos 🗮 Timeline	e *		• Keyword	Lists	Q <del>.</del> Keyword S
- >	Show Rejected Results	Directory List				
		Devices Attach				28 Res
Data Sources Data Sources		Table Thum	bnail			
	nallocated: 0-2047)	Source File	Devic	e Model		
	FFS / exFAT (0x07): 2048-125827071)	SYSTEM	ROOT	HEB		
	nallocated: 125827072-125829119)	SYSTEM		HUB20		
Views		SYSTEM		HUB30		
Results		SYSTEM		_	102 Elack	n Drive / HEMA Flas
Extracted C		SYSTEM		l USB Hub	1021105	T DATIVE / T ILLMAY T Tab
	Attached (28)	SYSTEM		I USB Hub		
	on Detected (2) Programs (64)	that				
	ng System Information (4)	SYSTEM		l Mouse		
	ng System User Account (8)	SYSTEM		l Mouse		
	Documents (48)	SYSTEM		l Mouse		
🖌 🖉 Web Boo	okmarks (1)	SYSTEM	Produ	ct: 0007		
- 🚳 Web Co	okies (321)	SYSTEM	Produ	ct: 0007		
- 💽 Web Do		۱ I	Π			•
Web His		Hex Strings	File Me	tadata Results 1	ndexed 1	ext Media
₩eb Sea Web Sea			of 15	Re 🗲 🔶		Contract International
Hashset Hi				<u></u>	-	
E-Mail Mes	eb .	Devices Attached				
* Interesting						
Accounts		4			111	

Figure 8-3 – Devices Attached Information Autopsy Retrieved After Running Module

While this information can be useful at face value, it does not really give much detail on the devices actually connected. There are also entries that are not related to external drives that were physically connected, which is not useful to the investigation at the moment. You are going to extract the four key files that store USB information (SYSTEM, SOFTWARE, NTUSER.DAT, and setupapi.dev.log) and then use another tool to find more detailed information.

#### **SYSTEM Hive**

Throughout these next sections, you can use the Windows 8 USB Worksheet in the Appendix to follow along with the useful information you want to find for connected USBs.

When a USB device is first connected, it stores the following information in the SYSTEM hive:

Vendor Product Version VID and PID iSerialNumber GUID Drive letter of the USB

Open the SYSTEM hive in Registry Explorer and navigate to the following subkey:

[CurrentControlSet]\Enum\USBSTOR

**Note:** As you may remember from earlier, the Select subkey showed you that the current control set was 1. In this case, it is also the only control set in this SYSTEM hive.

File Tools	Options Bookmarks (26/0) View Help		
Registry hives	(1) Available bookmarks (26/0)		
Key name		•	
,			*
Þ	HID		
Þ	HTREE		
D	LPTENUM		
Þ	PCI		
Þ	PCIIDE		
Þ	ROOT		
Þ	SCSI		
Þ	STORAGE		н
Þ	SW		
Þ	SWD		
Þ	USB	•	
۵ <mark></mark>	USBSTOR 🔫 —		
4	Disk&Ven_Kingston&Prod_DT_100_G2&Rev_PMAP		
	000FEAFB938CECC027E200F6&0		
Þ 🚞 H	lardware Profiles		
🚞 F	Policies		-

Figure 8-4 - USBSTOR Subkey in SYSTEM Hive

You will see a subkey under USBSTOR which has a name with the following information:

Vendor (Ven):	Kingston
Product (Prod):	DT_100_G2
Version (Rev):	PMAP

**Checkpoint:** Write Vendor, Product, and Version in Section 1 on your USB worksheet.

Below this subkey is another subkey named after the iSerialNumber "000FEAFB938CECC027E200F6&0", which Microsoft calls the Instance ID. By omitting the suffix (&#), you can see the iSerialNumber.

Note: The (&#) suffix shows what port the USB device was connected to.

**Checkpoint:** Write the iSerialNumber in Section 2 on your USB worksheet.

Open up the iSerialNumber subkey and go to the following location:

```
Properties \{83da6326-97a6-4088-9453-a1923f573b29}
```

As you can see in Figure 8-5, this subkey contains six subkeys. Four of the subkeys, 0064, 0065, 0066, and 0067, have important time stamps. The subkey 0064 shows the date and time when the device's driver was first installed. The subkey 0065 shows when the device's driver was installed. 0064 and 0065 will typically be the same date and time.

The subkeys 0066 and 0067 are new to Windows 8. 0066 shows when the device was last connected and 0067 shows when the device was last removed.

<u>File Tools Opti</u>	ons Bookmarks (26/0) <u>V</u> iew <u>H</u> elp			
Registry hives (1)	Available bookmarks (26/0)			
Key name	Ÿ		•	
۴				
⊿ 🚞 USB	STOR			
⊿ 🧰 Di	sk&Ven_Kingston&Prod_DT_100_G2&Rev_PMAP			
۵ 🚞	000FEAFB938CECC027E200F6&0			
Þ	Device Parameters			
4	Properties			
D	{3464f7a4-2444-40b1-980a-e0903cb6d912}			
C	{540b947e-8b40-45bc-a8a2-6a0b894cbda2}			
D	{80497100-8c73-48b9-aad9-ce387e19c56e}	•		
• 4	{83da6326-97a6-4088-9453-a1923f573b29}	•		
	C0003			
	CO0A		•	
	□ 0064	•	•	-
	□ 0065			
	Connected (Win 8)			
	🚞 0067 🔫 Device Last Removed (Win 8)		•	

Figure 8-5 - Date and Time Stamps for USB Device

Checkpoint: Write the first time connected, last time connected, and last time removed in Sections 3, 4, and 5 on your USB worksheet.

Registry hives (1) Available bookmarks (	0) Vie 26/0)	w Help				Val	ues			
Key name			2.	2		Drag	a column	header here to (	arou	n h
•					•	-	alue Name	Value Type		
⊳ 🥅 SW						• V	alue Marrie	value Type		
▷ 🚞 SWD						5 N C		D (	H	-
⊳ 🚞 USB				4		2012	eviceDesc	RegSz	••	••
⊿ 🚞 USBSTOR							apabilities	RegDword		_
Disk&Ven_Kingston&Prod_	DT_100	_G2&Rev_PMAP					ontainerID	RegSz		
	7E200F	6&0		• _	_	H	ardwareID	RegMultiSz		
Device Parameters	Ke	y: 000FEAFB938CEC	C027	/E2(	DOF	50	atible	-		
⊿ Properties	_						UID	RegSz	•••	••
▷ 🚞 {3464f7a4-2444-40	200	Add bookmark				F4			1	
▷ 🚞 {540b947e-8b40-45	-	Hide key					• ewer	Slack viewer		
▷ 🚞 {80497100-8c73-48		Export					ne	DeviceDesc		
⊿ 🚞 {83da6326-97a6-40	88-	Export						-		-
<b>0003</b>	5	Сору					۲ 🤰	Key name <	-	
🚞 000A	420	Expand subkeys		Alt	+De		2	Key path		
0064	0.59						100			
0065		Collape subkeys			Alt	⊦Up	4	Last write tim	e	
Key: ControlSet001\Enum\USB:	TC 🕲	Technical details				F5	viceDe	sc Collapse	all	biv

Figure 8-6 – Right-Click iSerialNumber Subkey and Select Copy Key Name

Press Control+F or click on Tools Find to conduct a search. When the Find window opens, paste the iSerialNumber into the Search For field. Delete the &0 at the end of the iSerialNumber. Check Key Name, Value Data, and Value Name. Leave Value Slack unchecked and then click Search.

地 Find	
Options Help	
Standard	
Search for 000FEAFB938CECC027E200F6	- Search in
	🗹 Key name 🛛 🗹 Value name
	🗷 Value data 🛛 🔲 Value slack
	Search type
	<ul> <li>Simple</li> <li>Regular expression</li> </ul>
History	Literal     Search

Figure 8-7 – Paste iSerialNumber, Check Key Name/Value Name/Value Data, Click Search

Down in the results pane, you want to look in the Key Path column for a hit under the USB subkey and the Mounted Devices subkey.

ey Path	
ountedDevices	
ountedDevices	
riverDatabase\DeviceIds\USB\VID_046E&PID_6782&MI_01\##?#USBSTOR#Disk&Ven_Kingston&F	Prod_DT_100_G2&Rev_PMAP
riverDatabase\DeviceIds\USB\VID_046E&PID_6782&MI_01\##?#USBSTOR#Disk&Ven_Kingston&F	Prod_DT_100_G2&Rev_PMAP
ontrolSet001\Services\rdyboost\AttachState	
ontrolSet001\Enum\USBSTOR\Disk&Ven_Kingston&Prod_DT_100_G2&Rev_PMAP\000FEAFB938CE	CC027E200F6&0
ontrolSet001\Enum\USB\VID_0930&PID_6545\000FEAFB938CECC027E200F6\Device Parameters	
ontrolSet001\Enum\USB\VID_0930&PID_6545\000FEAFB938CECC027E200F6	

Figure 8-8 – Search Result in MountedDevices and USB Subkeys

First, the iSerialNumber for the connected Kingston device is under the USB subkey. The iSerialNumber has a parent subkey named with the Vendor ID (VID) and the Product ID (PID), which in this case is "VID 0930&PID 6545".

**Checkpoint:** Write the VID and PID in Section 6 on your USB worksheet.

Close out of the Find window and navigate to the MountedDevices subkey. Take a look at the different values in the MountedDevices subkey. There are two types of values here. There are some values with names of GUIDs and some values with drive letter names. The value named "Volume{16d5eeec-681c-11e3-824f-000c29d6ef92}" contains information on the Kingston USB. A GUID is a 16-byte value that is randomly generated. Since the value consists of 128 bits, it is unlikely that a randomly generated GUID will match another GUID.

Registry hives (1) Available book	Values							
Key name  Key name  E:\Cases\Craig Tucker\Craig T  CoiTool-CreateHive-{0000000-00  ControlSet001  ControlSet001  E DriverDatabase  HardwareConfig	\??\Volume	16d5eeec-681 3f8a630c-674 3f8a6315-674	c-11e3-824f-0 6-11e3-824b-8 6-11e3-824b-8	00c29d6ef92} 306e6f6e6963} 306e6f6e6963}		  		
MountedDevices	\??\Volume	3f8a6316-674	6-11e3-824b-8	806e6f6e6963}			•	1
E RNG	Type viewer	Slack viewer						
Select		00 01 02	03 04 0	5 06 07			_	
<ul> <li>▷ Setup</li> <li>▷ WPA</li> </ul>	00000028	5F 00 4E	3 00 69 0 3 00 74 0	U UL UU	<mark>K.i.</mark> r g.s.t.o			
Associated deleted records	0000038	6E 00 26	00 50 0	0 72 00	n. & P. r	٢.		-
Unassociated deleted records	00000040 00000048 00000050	6F 00 64 54 00 5F 30 00 5F	00 31 0 00 47 0	0 30 00	o. d [ T 1. ( O G. 2	D. 2.		,
•	Current offse	t: 42 (0x2/	A) Bytes se	lected: 15	(0xF)			
Key: MountedDevice Value:	\??16	d5000-681	-11_03_82//f_(	00c29d6ef97	2} Collaps		lbi	VO

Figure 8-9 – Kingston UBS Information in GUID Value

**Checkpoint:** Write the GUID in Sections 7 on your USB worksheet.

Next take a look at the drive letter values. If you look at the value "DosDevices\E:", you will see Kingston USB information in it. This device's drive letter is E. If the drive letter had been assigned to another drive that was attached at a later date, the drive letter information would be overwritten with the new device's serial number.

ile Tools Options Bookmarks (26/0	· ·												
Registry hives (1) Available book	Values												
Key name	Drag a column	heade	er her	e to g	group	by t	hat co	olumi	1				
	Value Name										•		
E:\Cases\Craig Tucker\Craig T	÷												
▲ CsiTool-CreateHive-{0000000-00.	\DosDevices	\C:											-
ControlSet001     DriverDatabase	\DosDevices	\D:											
DriverDatabase HardwareConfig	<ul> <li>\DosDevices</li> </ul>	\E: •	-	2									
												i	ł
E RNG	Type viewer	Clay	c <mark>k vi</mark> e	Mor	1								
🚞 Select	Type viewei			0.2	03	0.4	0.5	0.0	07				-
🖻 🚞 Setup	0000028	00 5 E	01	4B	00	04 69	00	06 6F	00	. <mark>K. i</mark>			
D 🔤 WPA	00000028	67	00	73	00	74	00	6F	00	a. s. t			
Associated deleted records	00000038	6 E	00	26	00	50	00	72	00	n. & P			
Unassociated deleted records	00000040	6F	00	64	00	5 F	00	44	00	o. d	. D.		
	00000048	54	00	5F	00	31	00	30	00	T 1			
	00000050	30	00	5F	00	47	00	32	00	00			
III b	Current offse	et:	42 (0	x2A)	E	Bytes	sele	cted:	15	(0xF)			
Key: MountedDevices					Va	lue:	\D	osDe	evices\l	E: Colla	pse	all h	niv

Figure 8-10 – Kingston USB Information in E: Drive Letter Value

**Checkpoint:** Write the Drive Letter in Section 8 on your USB worksheet.

#### **SOFTWARE Hive**

When a USB device is connected, it stores similar information in the SOFTWARE hive. However, one important piece of information that is only in the SOFTWARE hive is the Volume Label. Open the SOFTWARE hive with Registry Explorer and navigate to the following subkey:

```
Microsoft\Windows Portable Devices\Devices
```

There is only one subkey below Devices, since only one device was connected. The subkey name will contain the same information you found in the SYSTEM hive, except it doesn't have the GUID and drive letter. The subkey will also have a value name called "FriendlyName". The value data of FriendlyName contains the Volume Label, which is "Stuff".

Registry hiv	ves (1) Available bookmarks (16/0)				Values	
4 4 4 4 5 6	Windows Mail Windows Media Device Manager Windows Media Foundation Windows Media Player NSS Windows Messaging Subsystem Windows NT Windows Photo Viewer	La 20 20 20 20 20 20 20 20	5 1 0 0 1 0		Value Name	
	Windows Portable Devices Contract Device	20 20 20	0		Value name	FriendlyName RegSz
D D D	FormatMap Windows Script Host Windows Search WindowsRuntime Wisp	20 20 20 20	0 9 2		Value	STUFF
⊳ <mark>=</mark> □ Key:	WlanSvc Microsoft\Windows Portable Devices\Devices	20 # ?	0 Value	•	FriendlyName	Collapse all hiv

Figure 8-11 - Volume Label in SOFTWARE Hive

**Checkpoint:** Write the Volume Label in Section 9 on your USB worksheet.

If you remember from the Recent Files section, a link file stores the volume label and volume serial number where the file was located.

The volume serial number is created when the device is formatted. The way it is calculated is based on the date and time of when the device was formatted, which means that the chance of two devices having the same volume serial number is very unlikely.

A device's volume label can be changed at any time, but the volume serial number can only be changed if the device is reformatted.

#### **NTUSER.DAT**

If the computer contained multiple user accounts, you would want to know which user plugged in the device. The user profile hive (NTUSER.DAT) will show you if that user account was specifically associated with that USB device. It will also show you the last time the device was plugged in by that user.

Open Craig's NTUSER.DAT file in Registry Explorer and conduct a search in the NTUSER.DAT file for the first part of the device's GUID (16d5eeec) that you obtained earlier. Only have Key Name checked and then click Search.

**Note:** Make sure you remove other hives from Registry Explorer before conducting a search so your results will only come from the NTUSER.DAT file.

🔥 Find	
Options Help	
Standard	
Search for 16d5eeec	Search in <ul> <li>Key name</li> <li>Value name</li> <li>Value data</li> <li>Value slack</li> </ul>
	Search type
	<ul> <li>Simple</li> <li>Regular expression</li> </ul>
History	Literal

Figure 8-12 – Search for First Part of GUID in Craig's NTUSER.DAT File and Click Search

You should see a result in the following subkey:

Key Path

Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\{16d5eeec-681c-11e3-824f-000c29d6ef92}

Figure 8-13 – Search Result of Kingston USB GUID

Since the device's GUID is located in Craig's NTUSER.DAT under the MountPoints2 subkey, you know that he was the user that plugged in the device.

**Checkpoint:** Write the user that connected the device in Section 10 on your USB worksheet.

**Note:** Since you do not have the subkeys 0066 and 0067 in the SYSTEM hive for Windows 7 machines, you could look at these Key Properties to determine the last time the device was connected. However, you would not know the last time the device was removed.

#### Setupapi.dev.log

When a USB device is first connected, it also stores information in the "setupapi.dev.log" file. You already know the first time the device was connected from the SYSTEM hive, but this is another file that will show you the first time the USB device was connected. It is located in:





Figure 8-14 – Setupapi.dev.log File

If you click through the pages of the setupapi.dev.log file, you will find an entry for the Kingston USB with the following text:

```
>>> [Device Install (Hardware initiated) -
SWD\WPDBUSENUM\_??_USBSTOR#Disk&Ven_Kingston&Prod_DT_100_G2&Rev_PMAP#000FE
AFB938CECC027E200F6&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
>>> Section start 2013/12/18 11:41:02.723
```

The last line that starts with ">>> Section start" contains the date and time when the device was first connected. This log records information in local time. That means that the first time the device was plugged in was December 18, 2013 at 11:41 AM (PST).

You are going to need this file for the USB tool, so go ahead and extract the setupapi.dev.log file by rightclicking it and selecting Extract File(s) (see Figure 8-15).



Figure 8-15 – Extract setupapi.dev.log to Export Folder

Navigate to the setupapi.dev.log file to the case Export folder and click Save.

#### **USB** Historian

Now that you know what information is stored when a USB device is connected, and where it is stored, you can use tools to quickly create a USB report. You are going to use a tool called USB Historian from 4Discovery, which you can download for free from their website:

```
https://4discovery.com/usb-historian/
```

Open the USB Historian tool, and in the top left corner you need to click the button Open File(s). A Wizard window will open, and you need to choose Select Individual Hives/Files. Click Next.

Wizard	
Chose which method you would like to parse data fro	<sup>m</sup> 44
Select a Drive Letter	
Select Windows and Users Folder	
Select Individual Hives/Files	
	<b>↓</b>
< B	lack Next > Cancel

Figure 8-16 – Choose Select Individual Hives/Files and Click Next

When the next window opens, you need to add the SYSTEM hive, the SOFTWARE hive, the NTUSER.DAT registry hive, and the setupapi.dev.log file you exported. Navigate to your case's Export folder and add each corresponding hive or file and then click Finish (see Figure 8-17).

Vizard	
Modify or Confirm Individual Registry Hives and Logs	4.4
Software Hive	
E:\Cases\Craig Tucker\Craig Tucker\Export\SOFTWARE	
System Hive	
E:\Cases\Craig Tucker\Craig Tucker\Export\SYSTEM	
User Hives (Right Click to Add)	
E:\Cases\Craig Tucker\Craig Tucker\Export\NTUSER.DAT	
Setup API Logs (Right Click to Add)	
E:\Cases\Craig Tucker\Craig Tucker\Export\setupapi.dev.log	2
< Back	Finish Cancel

Figure 8-17 – Add Exported SOFTWARE, SYSTEM, NTUSER.DAT, setupapi.dev.log and Click Finish

Friendly Name	Serial No		S_ M	ount Point 2	Drive Le	tter Volume	Name	Ready Boost Volume Name		
Kingston DT 100 G2 USB Device	000FEAFB9380	CECC027E200F6	[C	raig: 12/21/2013 9:23:15	PM] E:			STUFF		
Friendly Name:		The name of	of th	e device. (Four	nd in SYS	STEM hiv	e)			
Serial No:		The iSerial	Nun	nber of the dev	ice. (Fou	nd in SYS	TEM	hive)		
Mount Point 2: The user				user that plugged in the device and the last time (UTC) that the						
		device was	plug	gged in by that	user. (Fo	ound in N7	USE	R.DAT)		
Vol:		The device	's dı	rive letter. (Fou	ind in SY	STEM hiv	/e)			
<b>Ready Boost Volume Name:</b> Volume label of the device. (Found in SOFTWARE hive)										
Usb Stor DateTime Usb S	tor DateTime64	Usb Stor DateTir	ne65	Vendor Pr	oduct	Version	Vid	Pid		
12/18/2013 7:41:02 PM				Ven_Kingston Pr	od_DT_100_	Rev_PMAP	VID_	0930 PID_6545		
Usb Stor DateTime		The date/ti	ne t	hat the device	driver wa	s installed	(Fou	nd in SVSTEM		
		hive)				is motured	(			
Vendor, Product, Vo	ersion:	hive)	, pro	oduct, and vers			,			
Vendor, Product, Vo Vid and Pid:	ersion:	hive) The vendor			ion. (Fou	ind in SYS	TEM	hive)		
, , ,	ersion:	hive) The vendor The Vender Guid	r ID	oduct, and vers	ion. (Fou D. (Found	ind in SYS	TEM	hive)		



### Computer Forensics CCIC Training Chapter 9: Email

Lauren Pixley, Cassidy Elwell, and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 9

## **Email Review**

#### Introduction

Email can become a vital part of your investigation. In this case, you are looking for fraudulent coupons and now there are issues with CP. It is important to check email, because you need to know who your suspect was communicating with and if they were trading any data. You know that there were fraudulent coupons and CP associated with a USB device, but could the suspect have also received this type of data from other people?

Suspects can use webmail or software such as Thunderbird or Outlook to view their mail. It can be difficult to sometimes recover any email if the user was just using webmail, since most of it is not stored on the computer itself. However, if the suspect uses software to view their mail, then you can typically see what emails or attachments they sent and received.

#### Windows 8 Mail App

In Autopsy, click on E-Mail Messages under Results in the left pane. As you can see, Autopsy is reporting that there are zero email messages.



Figure 9-1 – Autopsy Shows Zero E-Mail Messages

Just because Autopsy shows zero email under this tab, that does not necessarily mean the suspect didn't have any email. They could have been using mail through their web browser or they could have been using a mail app that Autopsy does not recognize. You know that for this image, the suspect's operating system is Windows 8. That means the suspect could have been using the built-in Windows 8 Mail app, which is a program that Autopsy does not pull or recognize as email. To see if Craig used the Windows 8 Mail app, navigate to the following subfolder:

C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps\_ 8wekyb3d8bbwe\LocalState\Indexed\LiveComm\ba871ed4e8a350e0\120712-0049\Mail\1

In a Windows 10 image, the path is slightly different to get to all the emails and the way they are stored is not the same as it was in Windows 8 and earlier. Now, they are stored as .dat files which can be opened through a web browser. This adds a level of security in Windows 10 for consumers, but makes your job as a forensic examiner more difficult. To see if Craig had used the Windows 10 Mail app, you would navigate to the following subfolder:

```
C:\Users\Craig\AppData\Local\Comms\Unistore\data/1/a
```



Figure 9-2 – Subfolders for Windows 8 Mail App

Below the Mail\1 subfolders, there are six subfolders. These subfolders that are named 1d00000# represent a mail folder, such as Inbox, Sent, Deleted. Take a look at the first eml file in the 1d000001 subfolder that has the subject "Free Coupons".



Figure 9-3 – Free Coupons Email in 1d000001 Subfolder

This email is from someone named Stan Marsh and they sent 3 attachments. Since this relates to your investigation, go ahead and tag the eml file with any tag name you prefer (see Figure 9-4).



Figure 9-4 – Tag Free Coupons Email

#### Attachments

With Windows 8 mail, all of these emails are being stored in eml files. If you look at the line in the email called "Attachments", you will see the names of three jpgs attached to the email. With Windows 8 mail, the user has to download the attachments. Even when the attachments are downloaded, they are not encoded and stored in the same eml file as the email. If the user downloaded the attachment from mail, it is stored in an attachment folder called Att.

First, take a look at the eml file that this email is being stored in. One thing you should check before looking at the attachments folder is the first part of the eml name. This number is the Message ID and will match the email's attachment folder. Make note that the Free Coupons email attachment folder will be named 20000262. The attachment folder is located in:

```
C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps_
8wekyb3d8bbwe\LocalState\LiveComm\ba871ed4e8a350e0\120712-0049\Att
```

There are several subfolders below the Att folder, and their name matches up to an eml file name. Look for the subfolder 20000262. This contains the Free Coupons email attachments (see Figure 9-5).


Figure 9-5 - Email Stored under Mail Subfolder and Attachments Stored in Corresponding Att Subfolder

The three jpg files in the Att subfolder match the names of the attachments you saw in the email.

😹 Craig Tucker - Auto	psy 4.3.0				
Case <u>View</u> <u>Tools</u> <u>Winc</u>	dow <u>H</u> elp			12	
🕂 Add Data Source 🧃	🛿 View Images/Videos 🧮 Timeline 🗧		🛕 🛛 👁 - Keyword Li	ts Q <del>.</del> Keyw	vord S
€ >	Show Rejected Result	s	Directory Listing		
	□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	•	/img_Tucker.E01/vol_vol2/Users/Co Table Thumbnail	aig/AppData/Loc	al/Packages
	= $=$ $=$ 120712-0049 (7)		Name	Created Time	e
	→ ↓ Att (24)		[current folder]	2013-12-30 0	03:59:30 GM
			[parent folder]	2013-12-17	23:30:33 GM
	2000008 (2)		📄 Bagel Bites Coupon.jpg	2013-12-30 (	03:59:30 GM
	20000012 (2) 20000018 (2)		🔄 Monster Drink Coupon.png	2013-12-30 (	03:59:34 GM
	20000018 (2)		Snack Food Coupon.jpg	2013-12-30 0	03:59:31 GN
	20000069 (2)		1		111
	<ul> <li>200000cc (2)</li> <li>2000134 (2)</li> <li>2000135 (2)</li> <li>2000196 (2)</li> <li>200025f (3)</li> <li>2000265 (8)</li> <li>20000270 (8)</li> <li>20000270 (8)</li> <li>20000274 (6)</li> <li>20000274 (6)</li> <li>20000275 (4)</li> <li>20000274 (3)</li> <li>20000274 (4)</li> <li>20000276 (4)</li> </ul>	III	Hex Strings File Metadata Result	RAVE 50.50	Media Prev

Figure 9-6 - Free Coupons Email Attachments

The Monster Drink coupon was one of the coupons Craig was caught with. Go ahead and tag these three picture attachments.

### Windows 10 Mail App

In Autopsy, click on E-Mail Messages under Results in the left pane. As you can see, Autopsy is reporting that there are zero email messages again.



Figure 9-7 – Autopsy Shows Zero E-Mail Messages

Windows 10 Mail stores the emails in the following subfolder:

C:\Users\Craig\AppData\Local\Comms\Unistore\data\1\a

Once you have navigated to the data folder, there will be numbered folders with corresponding lettered folders containing the emails. The emails are web based in Windows 10 Mail, which means that you cannot simply export them as a .eml file. The files save by default as .dat files now, which for your purposes is a way to save HTML source code and view the email.

The easiest way to convert these to a readable format unless you are comfortable reading html source code is to simply change the file extension to a .html. This will allow you to open the .dat file in a web browser of your choice and see what the formatted message looks like. To do this, open the .dat file in notepad or some other text editor and click the "Save As" button. This will give you the option to change the extension and open it in a web browser. When it is saved, you should have an icon that looks like the web browser that you chose (In this example, Google Chrome was used)

**Note:** You MUST open the .dat file in notepad or another text editor before changing the file extension. If you don't it will put null characters between all of your letters and make it unreadable by the browser. We recommend that you use notepad (not notepad++) because it is a good basic text editor that comes pre-installed on all windows machines.



Figure 9-8 – Saving the email as a .html

The new email file will appear wherever you saved it last, so it is recommended to use either the export folder or create an emails folder to place all of the newly converted .html files for easy access. Note that you should include in your report that you had to export and change the extensions, since that is technically modifying evidence and without reason can cause your discovered data to be dismissed.



Figure 9-9 – New email\_example file that can be opened in a web browser to view

### MD5 Hash

There are several coupons in Craig's email attachment folder. If you want to know if Craig has these files saved anywhere else on his computer, you can conduct a search for the coupon based on its MD5 hash value.

A hash value is basically a fingerprint for a file. The chance of two MD5 hash values being the same is  $2^{128}$ . You can use hash values to exclude known files, such as Windows operating system files. There are also "hash libraries", which are large files that contain hash values of alert files, such as CP or hacking software. You can then run these alert hash libraries against the hash values in the image to quickly see if the user has any of these "bad" files.

To find the hash value for files, you will need to run the Hash Lookup plugin. Click Tools ► Run Ingest Modules ► Tucker.E01. When the Run Ingest Modules window opens, check Hash Lookup and then click Start.



Figure 9-10 – Check Hash Lookup and Click Start

Once Autopsy finishes processing the hash values, take a look at the file 1353033721971.png in the 20000270 attachment subfolder (see Figure 9-8).



Figure 9-11- Coupon in 20000270 Attachment Subfolder

These attachments come from the 20000270 eml file in the 1d000001 mail subfolder.

d Data Source 📠 View Imag	ges/Videos 🗮 Timeline 脑 Ge	enerate Report 🍙 Close Case 🏾 🛛	🔔 👁 - Keyword Lists 🔍 🔍	Keyword S
	Show Rejected Results	Directory Listing		
	🖶 📕 Mail (3)	/img_Tucker.E01/vol_vol2/Users/Craig Table Thumbnail	g/AppData/Local/Packages/microsoft.v	vindowscommur
	□ □ 1 (8) □ □ 1 (000001 (55)	Name	Created Time	Modified Time
	1d000002 (2)	2000026e 5823b3dbd72210.eml	2013-12-27 07:50:24 GMT	2013-12-27 0
	- J 1d000003 (2)	x 2000026f 145efdb97b43e.eml	0000-00-00 00:00:00	0000-00-00 00
- 1 d000004 (26) - 1 d000005 (2) - 1 d000008 (2) - 1 d00008 (2) - 1 d0008 (2) - 1 d00008 (2) - 1 d0008 (2) - 1 d00008 (2) - 1 d0008 (2) - 1 d00008 (2) - 1 d0008 (2) - 1 d008		2000026f 5e7a78519b17b6.eml	2013-12-27 07:50:24 GMT	
	20000270 92c3b9bf3bfec.eml <	2013-12-27 07:50:24 GMT	2013-12-27 0	
		20000271 96a32a9db1a281.eml	2013-12-27 07:50:24 GMT	2013-12-27 0
	x 20000271 f2bf626f53367e.eml	0000-00-00:00:00	0000-00-00 00	
		20000272_2a6c5c84990623.eml	2013-12-27 07:50:24 GMT	2013-12-27 0
	120712-0049 (7)	20000273 a2718b0c1ffca7.eml	2013-12-27 07:50:24 GMT	2013-12-27 0
		20000274 af42a44db9ef97.eml	2013-12-27 07:50:24 GMT	2013-12-27 0
	20000001 (4)	4	111	
	- 2000008 (2) - 2000012 (2) - 2000018 (2) - 2000067 (2) ≡ - 2000069 (8) - 20000134 (2) - 20000135 (2) - 20000135 (2) - 2000025f (3) - 2000025f (8) - 20000265 (8) - 20000269 (6) - 20000270 (8)	Hex Strings File Metadata Results Subject: RE: College Paperl HELP From: Kenny McCormick -kenny mcCormit To: Craig Tucker <coupon-king@outlook co<br="">Date: 18/12/2013 12:02-16 Attachments: (4) [Noname], 13530337215 THXI U r a lifesaver and yea I got ur back v From: coupon-king@outlook.com To: kenny.mccormick28@outlook.com Subject: Re: College Paperl HELP Date: Wed, 18 Dec 2013 19:46:58 +0000</coupon-king@outlook>	ck28@outlook.com> om> 971.png, 1353034157726.jpg, 1353034600	

Figure 9-12 – Email with Coupon Attachments

If you want to see if these coupons are saved anywhere else on the computer, right-click the first coupon in the 20000270 attachment subfolder and click Search for Files with the Same MD5 Hash.

Scraig Tucker - Autopsy 4.3.0		
Case View Tools Window Help	A O • Keywa	ord Lists Q+ Keyword S
Add Data Source View Images/Videos Timeline *  Add Data Source View Images/Videos Timeline *  Add Data Source Mail (3)  Mail (	Table       Thumbnail         Name       [current folder]         [parent folder]       [a]         [a]       1353033721971.nnn         [a]       13         Properties       [a]         [a]       View in New W         Open in Extern       View File in Tin         Extract File(s)       [s]	Jsers/Craig/AppData/Local/Package Created Time 2013-12-30 03:58:30 GMT 2013-12-17 23:30:33 GMT 2013-12-30 03:58:30 GMT Vindow hal Viewer heline s with the same MD5 hash Pre
		2 C

Figure 9-13 – Right-Click Coupon in 20000270 Attachment Subfolder and Search for Hash

There are three matches based on the MD5 hash value. One of the matches is in Craig's My Stuff folder and the other two matches are located in downloaded ZIP files. In the next chapter, you will look into where these downloaded ZIP files came from.

Name	Location
🖹 1353033721971.png	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunications
🖹 1353033721971.png	/img_Tucker.E01/vol_vol2/Users/Craig/Documents/My Stuff/1353033721971.png
📓 1353033721971.png	/img_Tucker.E01/vol_vol2/Users/Craig/Downloads/Coupons.zip/Coupons/1353033721971.png
📓 1353033721971.png	/img_Tucker.E01/vol_vol2/Users/Craig/Downloads/Coupons.zip/Coupons/1353033721971.png

Figure 9-14 - MD5 Hash Match Locations

### **Email (Continued)**

You should continue to look over and tag any emails or attachments of interest to your investigation. One email in particular you should check is the "Re: More Hot Pics", which is under the 20000286 eml in the 1d000004 mail subfolder.

If you remember from earlier, you found link files that pointed to CP. You then found two pictures and a video in the recycle bin. This email mentions "underage pictures", but there aren't any attachments since the original email, "More Hot Pics" is gone. You will go over this later, but tag the email for now.



Figure 9-15 – Potential CP Email

**Note:** The way these emails and attachments are being stored is specific to Windows 8 mail. See Appendix E for information on Windows Live Mail and Mozilla Thunderbird.

### **Contacts and Keyword Search**

With Windows 8 mail, you can see the user's contacts under the People folder, which is located at:

```
C:\Users\Craig\AppData\Local\Packages\microsoft.windowscommunicationsapps_
8wekyb3d8bbwe\LocalState\Indexed\LiveComm\ba871ed4e8a350e0\120712-0049
\People\AddressBook
```

Each file in the AddressBook folder will show a contact name and email address. Craig only has one actual contact: Kenny McCormick.



Figure 9-16 - Craig's Email Contact

Look at the subfolder called Implicit under the People folder (see Figure 9-14). Each file in this list shows a name and email address that Craig either sent emails to or received emails from. This information is stored here so when a user begins typing in who the email is "To:", a drop down menu will appear and allow you to auto complete a name or email address.



Figure 9-17 - People Craig Sent Email To or Received Email From

Between the AddressBook and Implicit subfolders, you can tell that Craig sent emails to and received email from:

Kyle Broflovski

Stan Marsh

Kenny McCormick

Since Craig was discussing coupons with these three people, go ahead and conduct a Keyword Search for them to see if their names show up anywhere else. To run a Keyword search, you need to first run the Keyword Search plugin. Click Tools ► Run Ingest Modules ► Tucker.E01. When the Run Ingest Modules window opens, check Keyword Search and click Start.



Figure 9-18 – Check Keyword Search Plugin and Click Start

Once Autopsy finishes processing, click the Keyword Search button in the top right corner. Type in Craig's first contact, "Kenny McCormick", and then click the Search button.



Figure 9-19 – Conduct Keyword Search for Kenny McCormick

You should see several results in the table pane. One keyword search result of particular interest is the main.db file. This file is a database for Skype.

Table Thumbnail	
Name	Location
🗋 20000275_d3734e1d1aa77.eml	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps
🖹 20000280_4003b9ba1d2c9a.eml	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps
1e000066_aee915a8efc74b.appcontent-ms	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps
🖺 main.db	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/Microsoft.SkypeApp_kzf8qxf38zg5c/Loc
🗋 pagefile.sys	/img_Tucker.E01/vol_vol2/pagefile.sys
🗎 main.db-journal	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/Microsoft.SkypeApp_kzf8qxf38zg5c/Loc
🖺 \$LogFile	/img_Tucker.E01/vol_vol2/\$LogFile
📄 livecomm.edb	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps
Microsoft-Windows-PushNotification-Platform	//img_Tucker.E01/vol_vol2/Windows/System32/winevt/Logs/Microsoft-Windows-PushNotification-Platfor
2000026f_5e7a78519b17b6.eml	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps
🗋 edb00009.log	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps
🗎 edbtmp.log	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps
26000001_d4636c334a0172.appcontent-ms	/img_Tucker.E01/vol_vol2/Users/Craig/AppData/Local/Packages/microsoft.windowscommunicationsapps

Figure 9-20 – Keyword Search Results for Kenny McCormick

Since there are search hits in the Skype database for Kenny McCormick, this indicates that Craig may have been using Skype to communicate with him. Make note of this, because later you will look into chat programs that Craig may have used.



## **Computer Forensics CCIC Training**

### Chapter 10: Internet History

Lauren Pixley, Cassidy Elwell, and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 10

## **Internet History**

### Introduction

Internet history is an important aspect in many cases. You can find out what sites your suspect visited, what they were searching for, and if they downloaded any data. Earlier in the Craig Tucker case, you found files in his Downloads folder. There was a RAR file and two ZIP files that contained several coupons. Where did the suspect download these files from? Some of Craig's email messages also mentioned a "4chan site". What is the 4chan site, and why did Craig visit it? By the end of this section, you will be able to answer these questions and you will have a better understanding of Internet history.

### Cookies

Cookies are small pieces of text which is sent to your browser by a website the user visits. The information a cookie stores helps the visited website remember any settings or preferences you specified so that returning to the website will be easier. While companies use cookies to remember your preferences, count visitors, and make relevant ads, investigators can use such information as one way to track the user's browser activity. The following data is stored in the browser's cookies:

Name	The name of the cookie
Content/Value	The value of the cookie <b>Note:</b> This is often a string which often represents a session id used by the visited website to recover your session from a larger session state.
Domain	The domain of the cookie
Accessible to script	Yes if Https, No if HttpOnly
Created	The date/time the cookie was created
Expires	The date/time the cookie will expire (typically 1 year from Created) <b>Note:</b> If a date/time is not specified then this cookie will remain in the browser until the user deletes it.

Site	Locally stored data	Rem	ove all	Search cookies	
1rx.io	3 cookies	i_fp			
	Name:	_rxuuid			
	Content:	%7B%22rx_uuid%22%3A%22R) 006613d385d0%22%2C%22nxt yncall%22%3A14907488454579	rdr%22%		
	Domain:	.1rx.io			×
	Path:	/			
	Send for:	Any kind of connection			
	Accessible to script:	No (HttpOnly)			
	Created:	Tuesday, March 28, 2017 at 5:54	4:06 PM		
	Expires:	Thursday, March 28, 2019 at 5:	54:06 PM		

When looking at cookies within a browser, the user sees a view similar to this:

Figure 10-1 – Browser View of Cookies

### History

The History SQLite database stores a user's past activity which can be divided into Downloads, History, and Searches.

History	URL	Full URL that was visited by the user
	Date Accessed	Date/time the URL was last visited
	Title	The title of the website visited (ie. Welcome to Facebook)
Downloads	Path	Location of file when downloaded <b>Note:</b> This provides you with the downloaded file's name and possible location within the image.
	URL	Full url that was visited by the user to accomplish download
	Date Accessed	Date/time of the download
Searches	Domain	URL where the search was made (ie. google.com, bing.com)
	Text	Text exactly as searched by the user
	Date Accessed	Date/time of the web search

### Chrome

Chrome is one of the most commonly used open source web browsers. The browser automatically saves all user activity in all versions of Windows at:

Add Data Source 🖪 View Images/Videos 🧮 Tir	meline 🕨 Generate Report 🌘 Close C	ase -			÷ ⊗·Keywo	ord Lists	◦ Keyw
Recovery (3)	Show Rejected Results	Directory Listing /img_Craig Tucker Desktop.E Table Thumbnail	01/vol_vol2/Users/Craig/	AppData/Local/Google/0	Chrome/User Data/Default		43 Res
System Volume Information (9) Users (8)		Name	Modified Time	Change Time	Access Time	Created T	ïme
<ul> <li>All Users (2)</li> <li>Craig (35)</li> <li>.gimp-2.8 (48)</li> <li>.thumbnails (3)</li> <li>AppData (5)</li> </ul>		Cache	2013-12-21 11:03:53	2013-12-21 11:03:53	2013-12-21 11:03:53	2013-12-1	17 18:27:0
		Extension Rules	2013-12-26 23:41:45	2013-12-26 23:41:45	2013-12-26 23:41:45	2013-12-1	17 18:27:0
		Extensions			2013-12-17 18:28:10		
		JumpListIcons	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-0	0:00:00
=== Local (19)		JumpListIcons	2013-12-26 23:43:00	. 2013-12-26 23:43:00	2013-12-26 23:43:00	2013-12-2	26 23:43:0
Application Data (2)		JumpListIconsOld	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-0	0:00:00
fontconfig (3) gegl-0.2 (3)		JumpListIconsOld	2013-12-26 23:42:00	2013-12-26 23:43:00	2013-12-26 23:42:00	2013-12-2	26 23:42:0
Google (4)		Local Storage	2013-12-26 23:43:00	. 2013-12-26 23:43:00	2013-12-26 23:43:00	2013-12-1	17 18:27:
Chrome (3)		Pepper Data	2013-12-17 18:27:21	. 2013-12-17 18:27:21	2013-12-17 18:27:21	2013-12-1	17 18:27:
□ User Data (33)		Session Storage	2013-12-26 23:41:48	. 2013-12-26 23:41:48	2013-12-26 23:41:48	2013-12-1	17 18:27:
Đ Default (56)		User StyleSheets	2013-12-17 18:27:08	2013-12-17 18:27:08	2013-12-17 18:27:08	2013-12-1	17 18:27:
PepperFlash (2)		Archived History	2013-12-17 18:27:09	. 2013-12-17 18:27:09	2013-12-17 18:27:09	2013-12-1	17 18:27:0
⊕■ pnacl (3) ⊕■ SwiftShader (3)		Archived History-journal	2013-12-17 18:27:09	. 2013-12-17 18:27:09	2013-12-17 18:27:09	2013-12-1	17 18:27:
WidevineCDM (3)		Cookies +	2013-12-26 23:43:00	. 2013-12-26 23:43:00	2013-12-17 18:27:09	2013-12-1	17 18:27:
CrashReports (2)		Cookies-journal	2013-12-26 23:43:00	. 2013-12-26 23:43:00	2013-12-17 18:27:09	2013-12-1	17 18:27:0
→ gtk-2.0 (3)		Current Session	2013-12-26 23:43:00	. 2013-12-26 23:43:00	2013-12-26 23:41:47	2013-12-1	17 18:27:
History (2)		Current Tabs	2013-12-26 23:43:00	. 2013-12-26 23:43:00	2013-12-26 23:43:00	2013-12-1	17 18:27:
	*	Favicons	2013-12-26 23:42:55	2013-12-26 23:42:55	2013-12-17 18:27:09	2013-12-1	17 18:27:0
		Favicons-journal	2013-12-26 23:42:55	. 2013-12-26 23:42:55	2013-12-17 18:27:09	2013-12-1	17 18:27:0
		Google Profile.ico	2013-12-17 18:27:39	. 2013-12-17 18:27:39	2013-12-17 18:27:39	2013-12-1	17 18:27:0
		History 🔶	2013-12-26 23:43:00	. 2013-12-26 23:43:00	2013-12-17 18:27:09	2013-12-1	17 18:27:0
		History Provider Cache	2013-12-26 23:43:00	. 2013-12-26 23:43:00	2013-12-26 23:41:45	2013-12-1	17 18:27:0
		History-journal	2013-12-26 23:43:00	. 2013-12-26 23:43:00	2013-12-17 18:27:09	2013-12-1	17 18:27:0
		Last Session	2013-12-21 11:04:00	. 2013-12-26 23:41:47	2013-12-21 11:02:11	2013-12-1	17 18:27:1
		Last Tabs	2013-12-21 11:04:00	. 2013-12-26 23:43:00	2013-12-21 11:04:00	2013-12-1	17 18:27:3
		Login Data	2013-12-17 18:27:16	. 2013-12-17 18:27:16	2013-12-17 18:27:16	2013-12-1	17 18:27:1
		Login Data-journal	2013-12-17 18:27:16	. 2013-12-17 18:27:16	2013-12-17 18:27:16	2013-12-1	17 18:27:1
					2013-12-17 18:27:09	2013-12-1	17 18:27:0
		Naturk Action Dradictor	2013-12-26 23:42:03	2012-12-26 23-42-03	2012-12-17 18-27-00	2012-12-1	17 19.27.0

C:\Users\[*username*]\AppData\Local\Google\Chrome\User Data\Default

Figure 10-2 – Chrome Cookies and History Database

### **Internet Explorer**

Internet Explorer is another popular web browser and is also the automatic default for Windows computers before Version 10. Being a Windows default, the browser's data is stored within:

C:\Users\[*username*]\AppData\Local\Microsoft\Windows

Show Rejected	Results	Directory Listing /img_Craig Tucker Desktop	.E01/vol_vol2/Users/Craid	a/AppData/Local/Microsof	t/Windows
Windows (43)	^	Table Thumbnail		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	· · · · · · · · · · · · · · · · · · ·
		Name	Modified Time	Change Time	Access Time
⊞≢ Burn (3)		[current folder]	2013-12-29 19:58:33	2013-12-29 19:58:33	2013-12-29 19:5
- Caches (16)		<pre>[parent folder]</pre>	2013-12-21 11:51:45	2013-12-21 11:51:45	2013-12-21 11:5
<ul> <li>ConnectedSearch (4)</li> <li>DNTException (4)</li> </ul>		₽1033	2013-12-17 15:11:26	2013-12-17 15:11:26	2013-12-17 15:1
Explorer (37)		Application Shortcuts	2013-12-17 15:11:25	2013-12-17 15:11:25	2013-12-17 10:1
		Burn	2013-12-17 15:11:29	2013-12-17 15:11:29	2013-12-17 15:1
GameExplorer (2)		Caches	2013-12-29 20:04:08	2013-12-29 20:04:08	2013-12-29 20:0
History (5)		ConnectedSearch	2013-12-26 23:27:30	2013-12-26 23:27:30	2013-12-26 23:
<ul> <li>IECompatCache (4)</li> <li>IECompatUACache (4)</li> </ul>		DNTException	2013-12-17 15:42:05	2013-12-17 15:42:05	2013-12-17 15:4
<ul> <li>IECompatoAcache (4)</li> <li>IEDownloadHistory (3)</li> </ul>		Explorer	2013-12-21 11:39:58	2013-12-21 11:39:58	2013-12-21 11:
INetCache (9)		FileHistory	2013-12-21 13:30:24	2013-12-21 13:30:24	2013-12-21 13:
		GameExplorer	2013-08-22 08:36:30	2013-12-17 10:11:34	2013-12-17 10:
Notifications (6)		History	2013-12-17 15:31:02	2013-12-17 15:31:02	2013-12-17 15:
<ul> <li>PicturePassword (2)</li> <li>PRICache (2)</li> </ul>		IECompatCache	2013-12-17 15:42:05	2013-12-17 15:42:05	2013-12-17 15:
		IECompatUACache	2013-12-17 15:42:05	2013-12-17 15:42:05	2013-12-17 15:
Ringtones (2)		IEDownloadHistory	2013-12-17 15:42:05	2013-12-17 15:42:05	2013-12-17 15:
RoamingTiles (2)		INetCache	2013-12-20 13:38:38	2013-12-20 13:38:38	2013-12-20 13:
E SettingSync (6)		INetCookies	2013-12-26 23:37:11	2013-12-26 23:37:11	2013-12-26 23:
■ SkyDrive (4)	*	Notifications	2013-12-29 19:56:43	2013-12-29 19:56:43	2013-12-29 19:
		PicturePassword	2013-12-17 15:25:51	2013-12-17 15:25:51	2013-12-17 15:
		PRICache	2013-12-17 10-11-50	2013-12-17 10-11-50	2013-12-17 10-

Figure 10-3 – Internet Explorer History and Cookies

#### **SQLite View Example**

Next, we will look at the SQLite information you can use to analyze a user's browser activity and how Autopsy makes investigations even easier with the "Extracted Content" window.

In Autopsy, you can view the data stored in SQLite databases by opening the Results view and using the arrows to move between entries. In bold text, at the top of each entry, you will see the word "Web" followed by either "Cookies", "History", "Downloads", or "Search". This tells you of which category the data is considered under (see Figure 10-4).

**Note:** The same procedure is followed for both Chrome and Internet Explorer browsers. However, this version of Autopsy is not pulling the Internet Explorer history into the Results view. You should always make sure to validate your software and see if it is pulling all the browser history information and determine if the user is using multiple browsers.

😹 Craig Tucker - Autopsy 4.3.0			- • ×
Case View Tools Window Help	line 🕞 Cenerate Depart v		
Time Add Data Source 🏨 View Images/Videos 🚬 Time	eline 🔚 Generate Report 🌣	🔔 💿 - Keyword L	
♦ ⇒ Show Rejected Results	Directory Listing		la (Churren e // Laner Data /Dafault
	Table Thumbnail	Users/Craig/AppData/Local/Goog	
E Recovery (3)	Name	Created Time	Modified Time
System Volume Information (9)	Google Profile.ico	2013-12-18 02:27:08 GMT	2013-12-18 02:27:39 GMT
→      ↓     Users (8)     →     ↓     All Users (2)	🗌 History 🔫 🗕	2013-12-18 02:27:09 GMT	2013-12-27 07:43:00 GMT
$\square$	History Provider Cache	2013-12-18 02:27:09 GMT	2013-12-27 07:43:00 GMT
	History-journal	2013-12-18 02:27:09 GMT	2013-12-27 07:43:00 GMT
⊕ ] .thumbnails (3)	Last Session	2013-12-18 02:27:11 GMT	2013-12-21 19:04:00 GMT
🖨 🤑 AppData (5)	Last Tabs	2013-12-18 02:27:33 GMT	2013-12-21 19:04:00 GMT
🖨 🔑 Local (19)	•		
- Application Data (2)	Hex Strings File Metadata	Results Indexed Text Media	Preview
⊕	Res of 222	Re 🗧 🔶 🔫 🗕	
□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	Web Downloads		
📄 🖟 Chrome (3)	The boundary		
🖨 🔑 User Data (33)	Path C:\Users\Cr	aig\Downloads\Coupons.zip	
🕀 🖟 Default (56)	Path ID 46837		
PepperFlash (2)	URL http://downl	oad1346.mediafire.com/hn7hme361	m4g/5ndip96wteag14g/Coupons.z
⊕	Date Accessed 2013-12-18		
	Domain download13	346.mediafire.com	
	Program Name Chrome		
- ] gtk-2.0 (3)		r.E01/vol_vol2/Users/Craig/AppData	/Local/Google/Chrome/User
			•

Figure 10-4 – Use Arrows in Results View for Chrome History

The Date/Time shown by Autopsy represents the Created date and time for Cookies as seen below. The Expired data and time are not stored along with whether the Cookie is Accessible to script.

Name		Created Time	Modified Time
🔋 User StyleSh	eets	2013-12-18 02:27:08 GMT	2013-12-18 02:27:08 GMT
Archived His	tory	2013-12-18 02:27:09 GMT	2013-12-18 02:27:09 GMT
Archived His	tory-journal	2013-12-18 02:27:09 GMT	2013-12-18 02:27:09 GMT
📄 Cookies 🤜	-	2013-12-18 02:27:09 GMT	2013-12-27 07:43:00 GMT
Cookies-jour	nal	2013-12-18 02:27:09 GMT	2013-12-27 07:43:00 GMT
Current Sess	ion	2013-12-18 02:27:11 GMT	2013-12-27 07:43:00 GMT
Res 1 of Web Cookies	270 Re		
URL	.youtube.com		
Date/Time	2013-12-2 <mark>1</mark> 01	:18:28	
Name	VISITOR_INFO	1_LIVE	
	ri0V0D9OBHc		
Value	no robo o bino		
100	Chrome		
Program Name			

Figure 10-5 – Use Arrows in Results View for Chrome Cookies

### **Extracted Content View Example**

Another way to view the SQLite data in Autopsy is through the Results\Extracted Content window, provided by the program. This window separates each entry into its own "Source File" and then places it within its category of "Web Cookies", "Web Downloads", "Web History", or "Web Search".

Add Data Source 🚇 Vi	ew Images/Videos 🗮 Timeline 🖹 G				ž O·	Keyword Lists	⊶ Keyw
>	Show Rejected Results	Directory Lis Web Cookies	ting				321 Resu
Views	^	Table Thum	bnail				JZI Kesu
Results <b></b> Extracted Content	_	Source File	Name	Value	Domain	Date/Time	
Devices Attached	•						
EXIF Metadata (45)		Cookies	VISITOR_INFO1_LIVE	ri0V0D9OBHc	youtube.com	2013-12-20 17	
-> Encryption Detect		Cookies	utma	173272373.215461852.1387333640.1387333640.13873	5.5	2013-12-17 18	:27:20
-  Extension Mismate	ch Detected (21)	Cookies	utmz	173272373.1387333640.1.1.utmcsr=(direct) utmccn=(di	google.com	2013-12-17 18	:27:20
Installed Program		Cookies	PREF	ID=93a9f9bf94e371de:U=80131685b4f4d0a1:FF=0:TM	google.com	2013-12-26 23	:42:46
Operating System		Cookies	NID	67=RvX3fGEVDnhnKYgQE8QgtLnCTUIXlBcG-40AQBegBo	google.com	2013-12-26 23	:42:46
Operating System		Cookies	GAPS	1:C9ZeHEkEKb-Nkv-CJlsjefCya134Eg:ATHt6OtpA3ysd2de	accounts.google.com	2013-12-26 23	:42:49
Recent Document Web Bookmarks (		Cookies	cfduid	dcb19ae39d4257ace9e35064233f1dfd81387333966783	4chan.org	2013-12-18 12	:05:30
Web Cookies (321		Cookies	MSPShared	1	login.live.com	2013-12-17 18	:39:15
- Web Downloads (		Cookies	SDIDC	Ct!FlipSmUWbmBk1Px4B1pTlOpuOje7Z1MUknKEQ2uccO	login.live.com	2013-12-17 18	:39:15
Web History (194)		Cookies	cfduid	d9d5ae40c9f5353a8748c64c1eee816bc1387335716510	4chan-ads.org	2013-12-18 12	:05:30
Web Search (17)		Cookies	ukey	gog8pc8c7zn33g3d312db8u8dbo4ho8u	mediafire.com	2013-12-18 12	:05:55
Keyword Hits	_	Cookies	cfduid	db5751b1d1ac72c22a8f70332df646e2f1387335757254	ohmcasting.com	2013-12-18 12	:05:56
Single Literal Keyv		Cookies	gads	ID=5ad626cf0f019ca9:T=1387335757:S=ALNI_Mb-bTx	mediafire.com	2013-12-18 12	:06:56
Single Regular Exp Escape Email Addresses (		Cookies	quest id	v1%3A138733575807927060	twitter.com	2013-12-18 12	:05:55
Hashset Hits	1920)	Cookies	pubtime 37524	ТМС	pubmatic.com	2013-12-18 12	:05:57
E-Mail Messages		Cookies	KADUSERCOOKIE	6D74076E-45CD-49FC-BC5D-9F6F9687B2AF	pubmatic.com	2013-12-18 12	:05:57
Interesting Items		Cookies	id	22ef80357d02004b][t=1387335759]et=730]cs=002213f	doubleclick.net	2013-12-26 23	:42:46
Accounts	~	Cookies	KRTBCOOKIE 80	4031-CAESEKea3mOwhNuy62bgbixoABs	pubmatic.com	2013-12-18 12	:05:57
		<ul> <li>Cookies</li> </ul>	DotomiUser	873902096961313689\$3\$42\$\$1	dotomi.com	2013-12-18 12	
		Cookies	demdex	27594390183790675893997109833429147655	demdex net	2013-12-18 11	

Figure 10-6 – Extracted Content View for Web Cookies, Downloads, History, and Search

**Note:** Under web history, you will see several entries for the website 4chan. People go to this site to post data anonymously to different boards. There are many boards where people will post inappropriate data, but also many fake coupons. People will post their fake coupons to this site so more people will use them and it will be harder to track down who created the coupons and all the people that use the coupons.



### **Computer Forensics CCIC Training** Chapter 11: Chat Logs

Lauren Pixley, Cassidy Elwell, and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 11

## **Chat Logs**

### Introduction

When you ran a keyword search earlier for Kenny McCormick, you found that a search result in the Skype main.db file. The Skype main.db file is used to store chat and contact information for the chat application Skype. It is always important to check chat artifacts because they show who the suspect was communicating with. Many chat programs also support file sharing, so you can see if the suspect shared or received any files through chat.

### SkypeLogView

To view Craig's Skype chat logs, you are going to use a tool called SkypeLogView from Nirsoft. It can be downloaded from:

http://www.nirsoft.net/utils/skype\_log\_view.html

To use SkypeLogView, you need to export Craig's main.db file (see Figure 11-1). This is located in:

```
C:\Users\Craig\AppData\Local\Packages\Microsoft.SkypeApp_kzf8qxf38zg5c\
LocalState\live#3acoupon-king_1\main.db
```

**Note:** This location for the Skype database is specific to Windows 8. In Windows Vista and 7, it was located in:

C:\Users\[User Name]\AppData\Roaming\Skype\[Skype Name]



Figure 11-1 – Right-Click Craig's main.db File and Select Extract File(s)

Extract Craig's main.db file to your case Export folder. Open up the SkypeLogView tool. Either type in the location of your case Export folder or use the [...] button to browse to your case Export folder. Click OK.

Select :	Skype Logs Fol	der / Fi	ilename					×
E:\Cases	\Craig Tucker\Cr	aig Tuc	ker\Export					
Load o	only log records i	n the fo	llowing date/	ti <mark>me rang</mark> e:	:			
From:	4/17/2017	▼ 7	:30:12 P	To:	4/18/2017	٣	7:30:12 P	
					-	-	ОК	Cancel

Figure 11-2 – Add Case Export Folder and Click OK

SkypeLogView will parse out all the Skype messages. It will also show who sent the chat message and when it was sent (see Figure 11-3).

File Edit View Option	ons Help			
🗅 🖬 🙆 🖪 🖆 🖏 📲				
Action Time	User Name	Display Name	Chat Message	1
12/20/2013 8:53:28	live:coupon-king_1	Craig Tucker	hey kenny, whats up? u finally on winter break 4 school?	
12/20/2013 8:55:12	live:kenny.mccormick28	Kenny McCormick	yea 2day was my last day, altho i heard sum teachers r ma	
12/20/2013 8:56:49	live:coupon-king_1	Craig Tucker	thats cray manwell i was gonna hit sum stores this weeke	
12/20/2013 8:59:10	live:kenny.mccormick28	Kenny McCormick	sweet, yea im in. im checking sum of my coupons 2 c if the	
12/20/2013 9:01:11	live:coupon-king_1	Craig Tucker	alrite well i'Il ttyl, im gonna play call of duty 4 a bit	
12/20/2013 9:02:33	live:kenny.mccormick28	Kenny McCormick	cool, coolttyl <ss type="highfive">(highfive)</ss>	111
12/21/2013 10:31:0	live:kenny.mccormick28	Kenny McCormick	hey dude, if we r going 2 wallmart 2day can u set me up w	
12/21/2013 10:56:3	live:coupon-king_1	Craig Tucker	arizona iced tea? what r u a girl? LOL while we r at wallma	
12/21/2013 10:58:2	live:kenny.mccormick28	Kenny McCormick	shut up u newb its a good drink! so r u going 2 bring a co	
12/21/2013 10:59:2	live:coupon-king_1	Craig Tucker	yea i will set 1 up 4 ubut rly?? iced tea? cant u just be nor	
12/21/2013 11:10:1	live:kenny.mccormick28	Kenny McCormick	well u know what? i'll be drinking my iced tea over u	
12/21/2013 11:11:3	live:coupon-king_1	Craig Tucker	whatever dude <ss type="facepalm">(facepalm)</ss>	-
•		III	•	

Figure 11-3 - Parsed Skype Messages in SkypeLogView

If you click Edit  $\triangleright$  Select All and then File  $\triangleright$  Save Selected Items, you can save these messages to an html, csv, or txt report. As you can see through these logs, Kenny had asked Craig to get him the Arizona Iced Tea coupon.



## **Computer Forensics CCIC Training** Chapter 12: Hidden Data

Lauren Pixley, Cassidy Elwell, and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

## 12

## **Hidden Data**

### Introduction

There are several ways suspects will try to hide their data. A very common way suspects will usually hide their data is through encryption and passwords. However, they might also try to change file extensions or create hidden files and folders. Not every suspect will try to hide their data through these methods, but it is still important for you to be aware of the different data hiding methods. Once you know how some suspects might try to hide their data, you can learn how to better detect and handle passwords or renamed file extensions.

### **Passwords and Encryption**

Towards the beginning of your analysis, you came across a password protected word document and ZIP file on Craig's desktop. Both file names had the word coupon in it, which means that these files could contain data relevant to your case. You are going to attempt to decrypt these files.

A good method to use when attempting to break a file's password is to follow a phased approach (see Figure 12-1). With a phased approach, you first try the easiest method, which is usually trying any known passwords, such as the user's login password. You can also try to run an English dictionary attack. If those both fail, you can index the suspect's drive and create a word list from the indexed words. The word list can then be used as a dictionary attack. Many criminals are lazy and will save passwords in places on their computer, reuse passwords for multiple accounts, and have physical versions like sticky notes and papers with passwords written on them. Be sure to check all of these sources when doing a real investigation before resorting to the brute force method. If the password is still not broken after all of these attempts, you can try a brute force attack.

The brute force attack method is usually a last resort. It goes through every possible combination of uppercase letters, lowercase letters, numbers, and symbols. A brute force attack will work eventually, but it takes a great deal of time and resources.



Figure 12-1 - Phased Approach to Breaking Passwords

First, you are going to try to use Craig's login password on the MyCoupons.zip and AWESOME COUPONS.docx. Export both these files out of Autopsy and save them into your Export folder.



Figure 12-2 – Extract MyCoupons.zip and AWESOME COUPONS.docx in Craig's Desktop Folder

Once MyCoupons.zip is in your case Export folder, you are going to need a tool to open it with, such as 7-Zip or WinRAR. You can download 7-Zip at:

```
http://www.7-zip.org/download.html
```

Once you have the 7-Zip tool, right-click MyCoupons.zip and click 7-Zip►Open Archive (see Figure 12-3).



Figure 12-3 – Right-Click MyCoupons.zip and Select Open Archive under 7-Zip

When 7-Zip opens, highlight all the files and click the Extract button in the top bar.

🛛 7-Zip File Manager		- 0 🗙
File Edit View Favorites	Fools Help	
Add Extract Test Copy	Move Delete	<mark>រ</mark> ្មី Info
E:\Cases\Craig Tucker	r\Craig Tucker\E	xport\MyCoup
Name	Size	Packed Size
🔚 Gatorade.jpg	1 403 292	1 270 273
Misc Many Drinks.png	1 980 <mark>8</mark> 82	1 929 206
🌆 Mountain Dew.png	975 225	833 965
🜆 Pizza.png	1 063 307	976 524
🜆 Poptarts.png	1 755 500	1 593 163
Magentary Twinkies.png	1 539 107	1 453 355
•		Þ
6 object(s) selectec 8 717 313	3 1 539 107	2012-11-15 21:08

Figure 12-4 – Highlight All Files and Click Extract Button

7-Zip will prompt you with a Copy window. Create a subfolder under your case Export folder and then click OK (see Figure 12-5).



Figure 12-5 – Create Subfolder under Case Export Folder and Click OK

Next, you need to type in Craig's login password "hungry123" and then click OK.

Inter password	
Enter password:	
hungry123	
Show password	
Show password	

Figure 12-6 – Type in Craig's Login Password and Click OK

Now you can view the decrypted password protected zip files.



Figure 12-7 – Password Protected Zip Files Decrypted

Now you should try to open Craig's AWESOME COUPONS.docx file with the same login password. When you open the file, you should be prompted with a Password window. Type in hungry123 and click OK.

Enter password to	open file	
E:\\Craig Tucker\	Export\AWESO	ME COUPONS.doo
•••••		
_	OK	Cancel

Figure 12-8 – Type hungry123 for AWESOME COUPONS.docx

The program should tell you that the password is incorrect. If you were to try and find the password for this Word document, you would then want to look if the suspect wrote any passwords down or had sent any in emails or chat. You could also then follow the phased approach and next try an English Dictionary Attack with password breaking software.

### Signature Analysis

Sometimes users have suspicious data they do not want deleted, but rather hidden. Users can accomplish storing data yet hiding its true nature by simply changing the file's name and/or extension. For example, a user could change naughty\_photo.jpg to water\_bill.txt in order to revert attention to the file. The change in file extension, however, is detectable through signature analysis. Each file has a signature embedded in itself which can then be compared to what the file claims to be. When these two pieces of information do not match, the investigators know a more detailed analysis of the file is required. The following are the "magic numbers" for common file types:

File Type	Extension	Magic Number / Hex Value
JPEG Graphic	.jpg	FF D8
PNG Graphic	.png	89 50 4E 47 0D 0A 1A 0A
MP3 Audio	.mp3	49 44 33
AVI Video	.avi	52 49 46 46
MOV Video	.mov	6D 6F 6F 76
Windows Video File	.wmv	30 26 B2 75 8E 66 CF
PDF	.pdf	25 50 44 46
Rich Text Document	.rtf	7B 5C 72 74 66 31
Word / Excel / PowerPoint Document	.doc / .xls / .ppt	D0 CF 11 E0 A1 B1 1A E1

These specific hex values (also known as "magic numbers") are at the beginning of each file and identify the file's type based on its content, not its file extension.

For additional signatures, you can use a File Extension Seeker or File Signature Table such as:

```
http://file-extension.net/seeker/
https://en.wikipedia.org/wiki/List of file signatures
```

Windows uses a file's extension to determine what program to use to open or execute a file. For example, if there is a picture called Stuff.jpg, it will be opened with Windows Photo Viewer or another picture viewing program by default. However, if the file is renamed to Stuff.txt, it will be opened with Notepad or Word by default and it will look like Figure 12-9.

Stuff.txt - Notepad	- • ×	3
File Edit Format View Help		
yöyä + JFIF       yöl + jrif         yöyä + jFIF       yöl + jrif         yöyä + jFIF       yöl + jrif         yöyä + jrif       yöl + jrif         yöyä + jrif       yöl + jrif         yöja + jrif       yöla + jrif	2';I <b>0</b> #B †‡ ÀA :QNB';±A ;YMB';±A ;YMB';±A ; yMB';±A ;Y i+A ;Y (ÈQč:Ĕø *ÿ ÅWNÿ f?	•

Figure 12-9 - Picture Renamed to Text File, Windows Opens Picture in Notepad by Default

#### **Extension Mismatch Detector**

One way to view the files that are suspicious and possible candidates of a user-modified file extension is to use Autopsy's Extension Mismatch Detector plugin. Click on Tools ► Run Ingest Modules ► Tucker.E01. When the Run Ingest Modules window opens, check Extension Mismatch Detector and then click Start.

😹 Run Ingest Modules	
Recent Activity     Hash Lookup     File Type Identification     Embedded File Extractor     Exif Parser     Keyword Search     Email Parser     Intersting Files Identifier     PhotoRec Carver     Virtual Machine Extractor	<ul> <li>Check all file types</li> <li>Check all file types except text files</li> <li>Check only multimedia and executable files</li> <li>Skip files without extensions</li> <li>Skip known files</li> </ul>
Select All Deselect All View Ingest History	Flags files that have a non-standard extension Global Settings
Process Unallocated Space	→ Start Close

Figure 12-10 – Check Extension Mismatch Detector and Click Start

When Autopsy finishes running, you can view the results in Results\Extracted Content\Extension Mismatch Detected window. This window is where Autopsy places any files that it finds during analysis whose signature possibly does not match its defined extension (see Figure 12-11).

Add Data Source	🖷 View Images/Videos 🗮 Timeline 🖭	Generate Report Close Case * * • • Keyword Lists	♀ Key	/w
*	Show Rejected Results	Directory Listing		(+ +)
Data Sources		Extension Mismatch Detected	21	Result
Views		Table Thumbnail		
Results 🔶		*Source File	Exten	sior 🔍
Extracted Cont Devices Attac		≤ underage_r@ygold_013.txt	txt	^
= EXIF Metadat		underage r@ygold_012.txt	txt	
Encryption D		= underage_r@ygold_011.txt	txt	
	smatch Detected (21)	= underage_r@ygold_010.txt	txt	
Installed Prog		≊4-http::∯ ∯wscont2.apps.microsoft.com∯winstore ∯1x∯ca628e7f-7a3e-4176-ac5d-83b644f48040∯Icon.243565.png.dat	dat	
	stem Information (4)	=4-http:::∯	dat	
<ul> <li>Operating Sy</li> <li>Recent Docur</li> </ul>	stem User Account (8)	=4-http:::∯ ∯wscont2.apps.microsoft.com ∯winstore ∯1x∯38ad5c98-9a11-4e93-8c52-13a43974643d ∯AppTile.1.281245.282407.jpg.dat	dat	
<ul> <li>Web Bookma</li> </ul>		=4-http::#∯wscont2.apps.microsoft.com∯winstore∯1x∯360c3180-ba83-4e28-b407-33fc37832e13∯AppTile.1.261594.262587.png.dat	dat	
Web Cookies		■ 4-http:: ∯ ∯ wscont2.apps.microsoft.com ∯ winstore ∯ 1x ∯ 1c2b1e0f-ea6b-4d35-99a7-d0c02faf7caf ∯ Icon.28291.png.dat	dat	
Web Downloa		≊ 4-http::∯∯wscont2.apps.microsoft.com∯winstore∯1x∯1c2b1e0f-ea6b-4d35-99a7-d0c02faf7caf∯AppTile.1.28291.232799.png.dat	dat	
Web History		≊ 4-http::∯∯wscont1.apps.microsoft.com∯winstore∯1x∯fe352f28-96ae-474b-b604-4d5a88086216∯Icon.273089.png.dat	dat	
<ul> <li>Web Search</li> </ul>	(17)	= 4-http::∯∯wscont1.apps.microsoft.com∯winstore∯1x∯fe352f28-96ae-474b-b604-4d5a88086216∯AppTile.1.273089.274182.png.dat	dat	
Keyword Hits	Keyword Search (0)	≊ 4-http::∯∯wscont1.apps.microsoft.com∯winstore∯1x∯f937b170-b8d1-4608-90e9-a570ff935fa7∯Icon.257176.png.dat	dat	
	ar Expression Search (0)	≈4-http:::∯∯wscont1.apps.microsoft.com∯winstore∯1x∯f937b170-b8d1-4608-90e9-a570ff935fa7∯AppTile.1.257176.258316.png.dat	dat	
<ul> <li>Hashset Hits</li> </ul>		≈4-http::##wscont1.apps.microsoft.com#winstore#1x#f3413050-a0ff-4c2a-9074-a074ea78f0fa#AppTile.1.270420.275779.png.dat	dat	
E-Mail Message	es	■ 4-http::##wscont1.apps.microsoft.com#winstore#1x#db355874-40fc-45d6-a0e9-ce52b05e3498#Icon.99877.png.dat	dat	
* Interesting Ite	ms	= 4-http:+∯∯wscont1.apps.microsoft.com∯winstore∯1x∯b607a83d-55d5-4984-a892-93450a18d63e∯Icon.139533.png.dat	dat	
Accounts	~	= 4-http:: # # wscont1.apps.microsoft.com # winstore # 1x#8d4e7174-5d0e-43ad-b5f0-c79b82baf607 # AppTile.1.275374.276368.png.dat	dat	
		= 4-httn::: # #wecont1 anne microsoft com #winetore #1v#6f45a8d8_80c3-4a8c-h050_17088h08h106#icon 63085 nng dat	dat	~
				>

Figure 12-11 – Results for Extension Mismatch Detector Plugin

Click the Extension column in the Table pane, and scroll down to the entries with txt. As you can see there are four text files of interest all with the names underage\_r@ygold. Autopsy has determined based on the hex header of these files that they are actually jpeg images and not text files.



Figure 12-12 – Sort by Extension Column and View Text Files that are Images

**Note:** The problem with this category is that it comes back with many results that are not useful. It's true that these files' extensions don't match their headers, but that does not mean the suspect intentionally renamed the extensions. There are several Windows system files and programs files that have mismatched headers and extensions.

### Hex View Example

In Autopsy, navigate to the location of the file that you deem as suspicious and open it in Hex view. Open the file "underage\_r@ygold\_011.txt" to check its contents, as it seems suspicious.

<ul> <li>Data Sources</li> <li>Views</li> <li>Results</li> <li>Extracted Content</li> <li>Extracted Content</li> <li>Encryption Detected (28)</li> <li>Encryption Detected (20)</li> <li>Extension Mismatch Detected (1339)</li> <li>Installed Programs (64)</li> <li>Operating System Information (4)</li> <li>Operating System User Account (8)</li> </ul>	rectory Listing ension Mismatch Detected able Thumbnail urce File Microsoft.Common.Tasks wop7627.tmp underage_r@ygold_013.txt underage_r@ygold_012.txt u Properties		MIME Type text/plain application/x-msoffice image/jpeg image/jpeg	esul
Data Sources     Views     Results     Extracted Content     Devices Attached (28)     Encryption Detected (2)     Extension Mismatch Detected (1339)     J Installed Programs (64)     Operating System Information (4)     Operating System User Account (8)	able Thumbnail urce File Microsoft.Common.Tasks wop7627.tmp underage_r@ygold_013.txt underage_r@ygold_012.txt u Properties	tasks tmp txt	MIME Type text/plain application/x-msoffice image/jpeg	
<ul> <li>Results</li> <li>Extracted Content</li> <li>Devices Attached (28)</li> <li>Encryption Detected (2)</li> <li>Extension Mismatch Detected (1339)</li> <li>Installed Programs (64)</li> <li>Operating System Information (4)</li> <li>Operating System User Account (8)</li> </ul>	Microsoft.Common.Tasks wop7627.tmp underage_r@ygold_013.txt underage_r@ygold_012.txt u Properties	tasks tmp txt	text/plain application/x-msoffice image/jpeg	-
Devices Attached (28)     Encryption Detected (2)     Extension Mismatch Detected (1339)     Jinstalled Programs (64)     Operating System Information (4)     Operating System User Account (8)	wop7627.tmp underage_r@ygold_013.txt underage_r@ygold_012.txt u Properties	tmp txt	application/x-msoffice image/jpeg	3
Encryption Detected (2)     Extension Mismatch Detected (1339)     ✓ Installed Programs (64)     Operating System Information (4)     Operating System User Account (8)	underage_r@ygold_013.txt underage_r@ygold_012.txt u Properties	bit	image/jpeg	3
Extension Mismatch Detected (1339)     ✓ Installed Programs (64)     Operating System Information (4)     ✓ Operating System User Account (8)	underage_r@ygold_012.txt u Properties			
→       Installed Programs (64)         ■       Operating System Information (4)         -       ↑         Operating System User Account (8)	u Properties	txt	image/ineg	
- Operating System Information (4) - Coperating System User Account (8)			mage/peg	
<ul> <li>Recent Documents (48)</li> <li>Web Bookmarks (1)</li> <li>Web Cookies (321)</li> <li>Web Downloads (8)</li> <li>Web History (194)</li> <li>Web Search (17)</li> <li>Keyword Hits</li> <li>Single Literal Keyword Search (120)</li> <li>Single Regular Expression Search (0)</li> <li>Hashset Hits</li> <li>E-Mail Messages</li> <li>F-Mail Messages</li> <li>Kersen (190)</li> </ul>	view in New Windo	Directory w ewer the same MD5 s matching MIN	•	

Figure 12-13 – Right-Click One of the Text Files and Click View Source File in Directory

Autopsy will take you to the folder where these pictures are being stored, which is the following path (see Figure 12-14):

```
C:\Windows\System32\system files
```

se View Tools Window H	elp			
Add Data Source I View	Images/Videos 🗮	Timeline × 🛕 🛚 👁 - Keyw	ord Lists Q <del>.</del> Keyword S.	
⇒ Shov	Rejected Results	Directory Listing	( )	-
		/img_Tucker.E01/vol_vol2/Windows/System32/s	system files 10 Re	esu
$\oplus$ sl-SI (10) $\oplus$ slmgr (3)	^	Table Thumbnail		_
⊕ J SMI (5)		Name	Created Time	-
🕀 🐌 Speech (5)		underage_r@ygold_010.txt	2013-12-27 07:51:10 GMT	
🕀 📜 spool (8)		underage_r@ygold_010.txt:Zone.Identifier	2013-12-27 07:51:10 GMT	
🕀 🔑 spp (5)		underage_r@ygold_011.txt	2013-12-27 07:51:17 GMT	
- 📕 sppui (4)		underage_r@ygold_011.txt:Zone.Identifier	2013-12-27 07:51:17 GMT	
😺 sr-Latn-CS (1 🔑 sr-Latn-RS (1		📓 underage_r@ygold_012.txt 🔫	2013-12-27 07:51:21 GMT	
- 3 sru (11)	(1-	underage_r@ygold_012.txt:Zone.Identifier	2013-12-27 07:51:21 GMT	
- <b>b</b> sv-SE (20)		underage_r@ygold_013.txt	2013-12-27 07:51:26 GMT	
🕀 📜 Sysprep (9)		underage r@ygold 013.txt:Zone.Identifier	2013-12-27 07:51:26 GMT	
– 📜 system files (		4	•	
🕀 🔑 SystemResetl	Platform (22)			-
⊕ 🖟 Tasks (9)		Hex         Strings         File         Metadata         Results         Indexed T           Pa         1         of         6         P         ←         →         Go to Pa		ffee
🔑 th-TH (16) 📜 tr-TR (19)				iise
- <b>u</b> uk-UA (16)		0x00000000: FF D8 FF E0 00 10 4A 46 49 46 00 0x00000010: 00 48 00 00 FF D8 00 43 00 03 02		
		0x00000020: 03 03 03 04 03 03 04 05 08 05 05	04 04 05 0A 07	
⊞ 🔋 WCN (3)		0x00000030: 07 06 08 0C 0A 0C 0C 0B 0A 0B 0B 0x00000040: 0E 11 0E 0B 0B 10 16 10 11 13 14	15 15 15 0C 0F	
🕀 📜 wdi (12)		0x00000050: 17 18 16 14 18 12 14 15 14 FF DB 0x00000060: 04 05 04 05 09 05 05 09 14 0D 0B		.c.
- 🔑 wfp (3)	(2)	0x00000070: 14 14 14 14 14 14 14 14 14 14 14 14 14		
→ 🤑 WinBioDatab 🕀 🔑 WinBioPlugIr				

Figure 12-14 – Renamed Picture Files Stored in system files Subfolder

View one of these picture files in hex view and look at the header. As you can see it has a header of a JPEG Graphic file.

lump to Offset	Preview	a	1edia		Indexed Text				Results			File Metadata				JS	Hex Strings		
	J				age	o P	io t	G	>	¢		Ρ.		6	of	C	• 1	Pa	
JFIF	48	00	01	01	01	00	46	49	46	4A	10	00	EO	FF	D8	FF	0000:	0x0000	
HC	03 .H	02	02	03	02	02	03	00	43	00	DB	FF	00	00	48	00	00010:	0x0000	
	07	OA	05	04	04	05	05	08	05	04	03	03	04	03	03	03	00020:	0x000x	
	0D	10	12	0E	OD	OB	OB	OA	OB	0C	0C	0A	OC	08	06	07	00030:	0x0000	
	OF	OC	15	15	15	14	13	11	10	16	10	OB	0B	OE	11	0E	00040:	0x0000	
C	04	03	01	43	00	DB	FF	14	15	14	12	18	14	16	18	17	00050:	0x0000	
	14	14	14	14	OD	0B	OD	14	09	05	05	09	05	04	05	04	00060:	0x0000	
	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	00070:	0x0000	
	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	00080:	0x0000	

Figure 12-15 – JPEG Graphic File Header on Renamed Text File

When you compare the extension of "underage\_r@ygold\_011" with the file type found from the signature, you should have a mismatch. The signature matches a JPEG Graphic file with "FF D8", rather than that of a Plain Text File (.txt). Therefore, you as an investigator should do more analysis on the file since the user was attempting to keep its contents hidden.



## **Computer Forensics CCIC Training**

### Chapter 13: Installed Programs

Lauren Pixley, Cassidy Elwell, and James Poirier May 2019 (Version 2)


This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 13

# **Installed Programs**

#### Introduction

Looking at what programs your suspect had installed can start to give you a better idea of how they used their computer. If he had pictures, how did he view or edit them? If he had ZIP and RAR files, how did he open them and extract data? If he had digital movies, how did he play them?

In this section, you will be looking at three specific programs. Programs are almost never the same, so information about how they were used will be stored differently. You can often find information about a program from its website. You can also try downloading the program on a virtual machine with the same OS as your suspect to see what it does and how it is storing evidence on your suspect's computer.

Take a look at what programs are installed on Craig's computer. You can find installed programs under:

```
C:\Program Files
C:\Program Files (x86)
```

The first program you are going to look at is GIMP 2.

+ Add Data Source	ce 📠 View Images/Videos 🗮 Time	line × 🔒	👁 - Keyword Lists 🛛 🔍	Keyword S		
€ >	Show Rejected Results	Directory Listing /img_Tucker.E01_vol_v	vol2/Program Files/GIMP 2	10 Result		
🖬 Data Sources	-	Table Thumbnail				
Tucker.E01	allocated: 0-2047)	Name	Created Time	Modified Tim		
	FS / exFAT (0x07): 2048-1258270	[current folder]	2013-12-20 21:37:20 GMT	2013-12-20 2		
🖶 退 \$Extend (9)	[parent folder]	2013-08-22 13:36:15 GMT	2013-12-21 1			
- 😺 \$Orph		32	2013-12-20 21:37:29 GMT	2013-12-20 2		
	3 bin	2013-12-20 21:37:31 GMT	2013-12-20			
	Boot (47)     Documents and Settings (2)     PerLogs (2)     Program Files (21)	🔋 etc	2013-12-20 21:37:20 GMT	2013-12-20		
		🔋 lib	2013-12-20 21:37:20 GMT	2013-12-20		
				libexec	2013-12-20 21:37:41 GMT	2013-12-20
		Python	2013-12-20 21:37:41 GMT	2013-12-20		
Common Files (5)     File Association Helper (10)	🔉 share	2013-12-20 21:37:20 GMT	2013-12-20			
		🔋 uninst	2013-12-20 21:37:20 GMT	2013-12-20		
⊕ <b>0</b> 3		4 111		,		
		Hex Strings File Met	adata Results Indexed Text Me	dia Preview		

Figure 13-1 – GIMP 2 in Program Files

#### GIMP

GIMP is a freeware graphic manipulation tool. You can alter pictures and add layers to a photo with it. If you look at Craig's email, there is one called "Re: Coupon Making" from Stan Marsh. Craig had asked him how to make his own coupons, and then Stan attached two guides and told him to download GIMP.



Figure 13-2 – Email Mentioning GIMP

#### Go to Craig's downloads folder in:

C:\Users\Craig\Downloads

	ools Window Help a Source 📠 View Images/Vi	deos 🧧	Timeline ×	🔥 👁 - Keywor	d Lists 🛛 🔍 Keyw	ord S	
€ ⇒	Show Rejected R	esults	Directory Listing			4 » v	
🖨 🕅	Users (8) All Users (2)	^	/img_Tucker.E01.vol Table Thumbnail	_vol2/Users/Craig/Downlo	ads	15 Resu	
			Name		Created Time		
	🕂 📜 .gimp-2.8 (48)		Coupons1.zip:Zo	one Identifier	2013-12-18 19:50:55 GM		
			desktop.ini		2013-12-17 23:11:25 GMT		
			gimp-2.8.10-set	2013-12-20 21:29:13 GMT			
				up.exe:Zone.Identifier	2013-12-20 21:29:13 GMT		
			winrar-x64-501.		2013-12-18 20:06:	46 GMT	
6			winrar-x64-501.	exe:Zone.Identifier	2013-12-18 20:06:-	46 GMT	
			WinZip180.exe		2013-12-21 19:02:4	43 GMT	
			WinZip180.exe:	Zone.Identifier	2013-12-21 19:02:-	43 GMT	
			III ►			F	
	- Local Settings (2)		Hex Strings File Me	etadata Results Indexed 1	Foot Madia Draviaw		
	– 🔋 Music (3)						
	My Documents (2)		Name	/img_Tucker.E01/vol_vol2/U	sers/Craig/Downloads/gii	np-2.8.10	
	→ IVIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		Туре	File System			
	PrintHood (2)		MIME Type Size	application/x-dosexec 90396104			
			File Name Allocation	Allocated			
	- Saved Games (3)		Metadata Allocation	Allocated			
	- 😺 Searches (7)		Metadata Allocation	2013-12-20 21:31:09 GMT			

Figure 13-3 – GIMP Installer in Downloads Folder

As you can see, Craig downloaded the installer for GIMP and then installed it.

Something that is unique to GIMP is that it has a "document history." This document history feature is so users can easily find and open their recently used files.

1	GNU Im	age Mar	nipulati	ion Prog	ram					
<u>F</u> ile	e <u>E</u> dit	<u>S</u> elect	<u>V</u> iew	<u>I</u> mage	Layer	<u>C</u> olors	Tools	Filte <u>r</u> s	Windows	<u>H</u> elp
	<u>N</u> ew				Ctrl+N					
	Crea <u>t</u> e				•					
	<u>O</u> pen				Ctrl+O					
•	Op <u>e</u> n a	s Layers		Ctrl+	Alt+O					
	Open L	ocation.								
	Open R	ecent			•	🔚 Te	st3.jpg		Ctrl+	1
	<u>S</u> ave				Ctrl+S	🗆 Te	st2.jpg		Ctrl+	+2
	Save A	s		Shift+	Ctrl+S	III Te	st1.jpa		Ctrl+	2
	Save a	Cop <u>y</u>				i ie	stripg		Curt	
	Re <u>v</u> ert					⊗ Do	ocument	: Histor <u>y</u>	-	-   -

Figure 13-4 – GIMP Document History

The document history is being stored in:

```
C:\Users\Craig\AppData\Local
```

In the Local folder, there is a file called recently-used.xbel. This is an XML-formatted file that contains information about the pictures that Craig had opened with GIMP.

😹 Craig Tucker - Autopsy 4.3.0		- • ×
Case <u>V</u> iew <u>T</u> ools <u>W</u> indow <u>H</u> elp		
🕂 🕂 Add Data Source 📠 View Images/Videos 🗮 Timeli	ne 🗧 🔥 🔹 Keyi	word Lists Qr Keyword S
Show Rejected Results	Directory Listing /img_Tucker.E01_vol_vol2/Users/Cra Table Thumbnail	aig/AppData/Local 17 Results
$\square$	Name	Created Time
	🔋 Packages	2013-12-17 18:11:42 GMT
AppData (5)	Programs	2013-12-20 21:37:18 GMT
🖨 🚨 Local (19)	Ju Temp	2013-12-17 18:11:34 GMT
→ → Application Data (2)	Temporary Internet Files	2013-12-17 18:11:35 GMT 2013-12-17 18:14:04 GMT
	WinZip	2013-12-17 18:14:04 GMT
🕀 🔑 Google (4)	S Winzip	2013-12-21 19:03:30 GMT
	recently-used.xbel	2013-12-21 19:32:04 GMT -
→ History (2) ⊞ → Microsoft (18)		
	Line Chinese File Material Description	Indexed Text Media Preview
🕀 🖟 Programs (3) 📃	Hex Strings File Metadata Results Matches on page: - of -	Match C > Page: 1 of 1
<ul> <li>Temp (28)</li> <li>Temporary Internet Files (2)</li> <li>VirtualStore (2)</li> <li>WinZip (4)</li> <li>CocalLow (4)</li> <li>Roaming (6)</li> <li>Application Data (2)</li> <li>Contacts (3)</li> </ul>	<pre><?xml version="1.0" encoding="UTF-8" <xbel version="1.0" xmlns:bookmark="http://www.fre xmlns:mime="http://www.freedes"</pre></pre>	<pre>2&gt; edesktop.org/standards/desktop-bookma ktop.org/standards/shared-mime-info" /iPad.png" added="2013-12-21700:58:50 02"&gt; sktop.org"&gt;</pre>

Figure 13-5 - GIMP Document History Stored in XML File

If you look in the XML file in Indexed Text or Strings view, there are several entries that appear to be coupons. He opened these on his drive and from his external drive. The XML file even gives you the date and time when each file was opened (see Figure 13-6).



Figure 13-6 - Entries in GIMP Document History

You don't have Craig's E: drive, so you can't look at most of the picture files that he opened with GIMP. However, you can look for "1304644031008.png" and "Iced tea – edited.png" in his My Stuff folder.

Double-click the Created time column to sort the files by created time. If you look at the bottom of the list, you will see a file called "1304644031008.png" and "Iced tea - edited.png".

Look at the first Arizona Iced Tea coupon named 1304644031008.png. It has a file Created time of 12/21/2013 at 19:14:07 GMT.



Figure 13-7 - Iced Tea Coupons in Craig's My Stuff Folder, Sorted by Created Time

To know if these files were created on Craig's computer at that time or if they were copied from another source, you can look at the Created time for the other files. Nine of the other coupons have a Created time of 12/21/2013 at 19:14:07 GMT.

Now, look at the Modified times of these 10 files. These times predate the Created time. Based on these time stamps, this activity is consistent with these files being copied to the My Stuff folder from another source, such as his external E: drive.

Name	△Created Time	Modified Time
, anno		
1304377546277.jpg	2013-12-21 19:14:06 GMT	2011-05-03 05:59:12 GMT
1304377950804.png	2013-12-21 19:14:06 GMT	2011-05-03 05:59:52 GMT
1304393958244.png	2013-12-21 19:14:06 GMT	2011-05-03 08:24:16 GMT
<b>1304394230314.jpg</b>	2013-12-21 19:14:06 GMT	2011-05-03 08:23:44 GMT
🖹 1304644210039.png	2013-12-21 19:14:06 GMT	2011-05-06 05:25:22 GMT
1304400692832.png	2013-12-21 19:14:07 GMT	2011-05-03 08:36:40 GMT
🔄 1304643149337.png	2013-12-21 19:14:07 GMT	2011-05-06 05:20:18 GMT
1304643663005.png	2013-12-21 19:14:07 GMT	2011-05-06 05:22:20 GMT
1304643804769.png	2013-12-21 19:14:07 GMT	2011-05-06 05:23:04 GMT
■ 1304644031008.png	2013-12-21 19:14:07 GMT	2011-05-06 05:25:18 GMT
Iced tea - edited.png	2013-12-21 19:19:58 GMT	2013-12-21 19:19:58 GMT

Figure 13-8 – Timeline of Coupons

The edited version of the Arizona Iced Tea coupon (Iced tea – edited.png) was created approximately 5 minutes later on 12/21/2013 at 19:19:58 GMT. The Modified time of Iced tea- edited.png matches the Created time, which is consistent with this file being created on this computer.

#### WinZIP

The next program you are going to look at is called WinZIP. WinZIP allows you to zip and unzip files. You can also use it to create password protected ZIP files. Earlier, you found that Craig downloaded ZIP files that contained several coupons.

WinZIP keeps some information stored in the user's NTUSER.DAT file. Open up Craig's NTUSER.DAT file with Registry Explorer, and navigate to:

Software\Nico Mak	Computing\WinZip	
	Registry Explorer v0.8.1.0	
	File Tools Options Bookmark	s (17/0) View Help
	Registry hives (1) Available bookr	marks (17/0)
	Key name	Last write timestamp
	<b>9</b>	Lust mile unestamp
	🖡 🖉 WinZip 🔶	2013-12-21 19:08:26
	aution	2013-12-21 19:03:27
	🚞 directories	2013-12-21 19:08:26
	💳 Filters	2013-12-21 19:03:27
	📻 fm	2013-12-21 19:03:27
	E ListView	2013-12-21 19:08:26
	Þ 🚞 mru	2013-12-21 19:03:27
	🚞 programs	2013-12-21 19:03:27
	Þ 🚞 rrs	2013-12-21 19:08:17
	🚞 Splitter	2013-12-21 19:03:27
	Statistics	2013-12-21 19:03:27
	Check Check	2013-12-21 19:03:27
	🚞 WinIni	2013-12-21 19:08:26
	🚞 WinZip	2013-12-21 19:08:26
	D 🚞 WXF	2013-12-21 19:03:54
	🚞 wzshlext	2013-12-21 19:03:27 •

Figure 13-9 - WinZip Key in Craig's NTUSER.DAT

Under the WinZip subkey, there are several other subkeys. The "directories" subkey contains value names of "AddDir" and "ZipTemp" (see Figure 13-10).

Reg	istry hive	es (	1) Available bookmark	s (17/0)					1	/alues		
Ke	y name		k.	Last	write t	im			Dr	ag a column h	eader here to group by that column	
								*		Value N •	Data	
	4 🚞	Nic	o Mak Computing	2013	8-12-2	1 1			÷	value m	Duta	
	Þ	0	Common	2013	8-12-2	1 1			-			
	E	F	ile Association Helper	2013	8-12-2	1 1				AddDir	C:\Users\Craig\SkyDrive\Documents	
	4 📑	V	VinZip	2013	3-12-2	1 1				CheckOutB		
		-	caution	2013	8-12-2	1 1				gzAddDir	0	
		-	directories 🔫 ー	2013	8-12-2	1 1				gzExtractTo	2	
		-	Filters	2013	3-12-2	1 1				ZipTemp	C:\Users\Craig\AppData\Local\Temp	
		-	fm	2013	3-12-2	1 1				ZipTempR	1	
		-	ListView	2013	3-12-2	1 1		Е				-
	D	-	mru	2013	3-12-2	1 1			17	ype viewer		
		e	programs	2013	8-12-2	1 1			Va	lue name	AddDir	
	D	-	rrs	2013	3-12-2	1 1						_
		-	Splitter	2013	3-12-2	1 1			Va	lue type	RegSz	
		E	Statistics	2013	3-12-2	1 1			Va	lue	C:\Users\Craig\SkyDrive\Documents	-
		F	UpdateCheck	2013	3-12-2	1 1					- (	
		-	WinIni	2013	8-12-2	1 1		-				
	Key:	S	oftware\Nico Mak Com	puting\V	VinZip	\dire	ecto	ories			Value: AddDir Collapse all h	nin

Figure 13-10 - AddDir and ZipTemp Values in Directories Subkey

The ZipTemp value shows you the location for temporary files. When a user opens a file in a ZIP using WinZIP, it will store the opened file in this temporary folder. The temporary folder location for this user is:

```
C:\Users\Craig\AppData\Local\Temp
```

However, if you look at this location in Autopsy, there aren't any files from WinZIP. You won't always find data in the temporary folder, because it's usually overwritten quickly. It's still a good idea to check it though.

The AddDir value shows you the last location a ZIP file was extracted to. In this case, it is:

```
C:\Users\Craig\SkyDrive\Documents
```

If you look at Craig's Skydrive, there are several coupons stored there. Now that you know this was the last location for a ZIP file to be extracted to, these coupons could have potentially been from the downloaded ZIP files. You also know that these coupons were downloaded from the Internet, because they have an ADS of 3.

Another piece of information in the NTUSER.DAT file is under the "mru\archives" subkey (see Figure 13-11).

Note: The abbreviation mru stands for "most recently used."

Registry hives (1) Av	ailable bookmarks	s (17/0)		Values	
Key name		Last write tim		Drag a column	header here to group by that column
				Value +	Data
🔺 🚞 Nico Mak Co	omputing	2013-12-21 1		•	
🖻 🚞 Common		2013-12-21 1			
😑 File Assoc	iation Helper	2013-12-21 1		• 0	C:\Users\Craig\Desktop\MyCoupons.zip
⊿ 🚞 WinZip		2013-12-21 1		MRUList	00-00
😑 caution		2013-12-21 1			
🚞 director	ies	2013-12-21 1			
🚞 Filters		2013-12-21 1			
🚞 fm		2013-12-21 1			
🚞 ListViev	I	2013-12-21 1			
a 🚞 mru		2013-12-21 1		Type viewer	Slack viewer
🚞 archiv	ves 🔶	2013-12-21 1		Value name	0
🚞 jobs		2013-12-21 1			
🚞 prograr	ns	2013-12-21 1		Value type	RegSz
Þ 🚞 rrs		2013-12-21 1		Value	C:\Users\Craig\Desktop\MyCoupons.zip
🚞 Splitter		2013-12-21 1		, and c	,
🚞 Statistic	s	2013-12-21 1		Slack	
Key: Software	Nico Mak Com	puting\WinZip\mru	() arc	nives	Value: 0 Collapse all hiv

Figure 13-11 - ZIP File Created Using WinZIP

The values within this subkey will show what ZIP files were created using WinZIP. As you can see, there was only one ZIP file that Craig created using WinZIP, and it is the encrypted MyCoupons.zip on his desktop.

If you look at MyCoupons.zip on Craig's desktop, you will also notice that the Created and Modified times are the same. This is consistent with the ZIP file being created on Craig's computer.

#### WinRAR

WinRAR is another program used to compress and decompress ZIP and RAR files. Craig has a file called ALL COUPONS.rar located in his Downloads folder. Take a look at the following subkey in Craig's NTUSER.DAT file:

Registry hives (1) Available bookmarks (17		(s (17/0)	.7/0)							
Key name		Last write tim			Drag a column	header here to c	roup by that column			
				•	• Data	1				
Nico Mak Computing		2013-12-21 1	Τ.							
🛛 🧰 Policie	s	2013-12-17 1	2013-12-17 1			*				
🚞 Regist	eredApplications	2013-12-17 2			• 0 C:\Use	rs\Craig\Downlo	ads\ALL COUPONS.rar			
⊿ 🚞 WinR/	AR	2013-12-18 2								
🚞 Arc	History 🔫	2013-12-18 2								
⊳ 🚞 File	ist	2013-12-18 2								
⊳ 🚞 Fori	nats	2013-12-18 2								
🛛 🚞 Gen	eral	2013-12-18 2	•							
🛛 🚞 Inte	rface	2013-12-18 2				1				
🖻 🚞 Prot	iles	2013-12-18 2			Type viewer	Slack viewer				
🖻 🚞 Setu	ip	2013-12-18 2		2	Value name	0				
🚞 WinR/	AR SFX	2013-12-18 2		E	Malura Arma	De -C-				
🚞 WinZi	o Computing	2013-12-21 1			Value type	RegSz				
⊳ 🚞 Wow6	432Node	2013-12-17 2	•		Value	C:\Users\Craig	) Downloads ALL			
🛛 🚞 System		2013-12-17 1			Slack	COUPONS.rar				
Associated	deleted records			-	SIDUK					
Key: Soft	ware\WinRAR\ArcHi					Valu	e: 0 Collapse all hiv			

Figure 13-12 – ArcHistory Subkey Shows Files Opened with WinRAR

As you can see, WinRAR stores what files were opened in WinRAR under this subkey. If you wanted to see when the file was opened, you could look at Craig's Recent folder for any link files (see Figure 13-13).



Figure 13-13 – Link File for ALL COUPONS.rar

As you can see, the Created time and the Modified time are the same on the link file, so ALL COUPONS.rar was only opened once on 12-18-2013 20:07:21 GMT.

Table Thumbnail			
Name	Created Time	Modified Time	Access Time
20000196.lnk	2013-12-21 01:14:07 GMT	2013-12-21 01:14:07 GMT	2013-12-21 01:14:07 GMT
6CommandmentsofCouponMaking.Ink	2013-12-20 21:26:41 GMT	2013-12-20 21:27:33 GMT	2013-12-20 21:27:33 GMT
ALL COUPONS.Ink	2013-12-18 20:07:21 GMT	2013-12-18 20:07:21 GMT	2013-12-18 20:07:21 GMT
AWESOME COUPONS.Ink	2013-12-20 21:43:07 GMT	2013-12-20 21:43:32 GMT	2013-12-20 21:43:32 GMT
Biology and Aggression.lnk	2013-12-18 23:15:30 GMT	2013-12-18 23:17:33 GMT	2013-12-18 23:17:33 GMT

Figure 13-14 – ALL COUPONS.rar Opened Once



# Computer Forensics CCIC Training

### Chapter 14: Legal

Bruce Pixley May 2017 (Version 1)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 14

# Legal

#### Introduction

Once you start conducting forensic examinations of data, your role starts to fall into the category of an expert witness. As such, you need to be prepared to testify about your procedures and findings.

Whether you are simply preserving and collecting digital evidence or conducting the steps through analysis and reporting, you need to always do your job in a forensically-sound manner. If you do not, either you or another examiner may likely spend more time trying to explain to the court what you did and how that did not tamper or alter the original evidence.

If your case goes to trial, the court will have to determine if you are qualified to be an expert witness. The defense may try to challenge your designation as an expert by simply asking if you have a Ph.D. in computer science. However, an expert is not required to have a degree or major credentials. The court will determine if you are qualified based on your special knowledge, skills, training, or experience to provide testimony to aid the factfinder in matters that exceed common knowledge of ordinary people.

As you continue down the path of this field, keep track of your training and try to obtain credentials or certifications if you can. All of this will lead toward your qualifications to be designated by the court as an expert witness.

In federal court, the Daubert standard provides rules of evidence regarding the admissibility of expert testimony including scientific data. Digital evidence collected and analyzed using forensic software by an expert can be challenged.

What does this mean to you? The court will have to consider the admissibility of the digital evidence.

If the opposing side files a motion to suppress the evidence or challenge your skills based on the technology you used, the court will evaluate "whether the testimony's underlying reasoning or methodology is scientifically valid and properly can be applied to the facts at issue."

The court will consider factors such as:

- Whether the technique in question can be or has been tested;
- Whether it has been subjected to peer review and publication;
- The technique is known to have potential errors and there are maintenance standards controlling its operation;
- It is a widely accepted practice in the relevant scientific community.

As you go forward, you need to keep all of this in perspective as it affects how you do your job.

An excellent resource for legal issues related to digital evidence can be found on the U.S. Justice Department's website and is titled Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.

#### **Expectation of Privacy**

A search is considered to be constitutional if it does not violate a person's reasonable expectation of privacy.

A computer, storage media, and cell phone should be considered a "closed container" such as a briefcase or file cabinet. The Fourth Amendment generally prohibits law enforcement from accessing and viewing information stored on a computer if it would be prohibited from opening a closed container and examining its contents in the same situation.

#### **Private Searches**

Individuals who retain a reasonable expectation of privacy in the data stored on their computer may lose Fourth Amendment protections when they give their computer to a third party, such as a repair shop or a friend.

The Fourth Amendment is not violated when a search is conducted by a private individual acting on his own (not acting as an agent of the Government or with the participation or knowledge of any governmental official) and makes the results available to law enforcement.

Law enforcement can reenact the original private search without violating any reasonable expectation of privacy. However, law enforcement cannot exceed the scope of the original search. It is better for law enforcement to use the information learned from the private search as probable cause to get a warrant that will allow for a complete search.

#### **Search Authority**

Before you jump into any collection or search, you need to determine if you have the authority to do that.

If you are a government agent, then the Fourth Amendment applies to your actions. If a person is acting as an individual or on behalf of their company and not under the direction of the government, then the Fourth Amendment does not apply.

So what are the exceptions to a search warrant when it comes to digital evidence?

#### Consent

Law enforcement does not need a search warrant or even probable cause if the person with authority has voluntarily consented to the search. When using consent as an exception, you should consider the following factors:

- In the future, will you need to prove consent was given? How will you do that?
- When does a search exceed the scope of the consent?
- Who is the proper party to consent to a search?
- The consent may be revoked

Ideally, use a written consent form that states the scope of consent includes the consent to search computers and "other electronic storage devices."

When a third party gives consent to search a computer that consent may have some issues. For example, two people share a computer that is not password-protected. However, what if one person password-protected some files and the consenter does not know the password? You hit a crossroad, what should you do?

Parents can consent to searches of their children's computers when the children are under 18 years old. If the children are 18 or older, the parents may not have the authority to consent.

Computer searches by repairman prior to contact with law enforcement are private searches and do not violate the Fourth Amendment. Again, it is best practice for law enforcement to use the information revealed through a repairman's private search as a basis to secure a warrant for a full search of the computer.

#### **Exigent Circumstances**

When considering the use of exigent circumstances as an exception to the search warrant requirements, you need to consider the following:

- The degree of urgency
- The amount of time necessary to obtain a warrant
- Whether the evidence is about to be removed or destroyed
- The possibility of danger at the site
- Whether those in possession of the contraband know the police are on the trail
- The ready destructibility of the contraband

Just remember that the existence of exigent circumstances is tied to the facts of that particular case.

- 1. Can someone remotely issue a kill command to a cell phone? Yes. Could you seize a smartphone for the purpose of placing it in airplane mode? Probably, but conducting a search is another issue.
- 2. If an unlocked iPhone is allowed to enter a "locked screen" mode, will that prevent the investigator from accessing the data on the phone?
- 3. Can someone effectively lock their data on a computer that is using Microsoft Bitlocker?

#### **Plain View**

You are conducting a search of a computer for evidence of fraudulent documents and identification pursuant to a valid search warrant. During the examination, you see child pornography in "plain view." Do you continue to search for more child pornography or do you stop and seek a new search warrant?

At that point, stop your search for additional child pornography and obtain a new search warrant authorizing the search for that content.

The "plain view doctrine" does not authorize law enforcement to open and view the contents of a container that they are not otherwise authorized to open and review.

#### **Probation and Parole**

Individuals on probation, parole, or supervised release have a diminished expectation of privacy and may be subject to warrantless searches based on reasonable suspicion, or, potentially, without any particularized suspicion.

#### Search Incident to an Arrest

Pursuant to a lawful arrest, officers may conduct a "full search" of the arrested person, and a more limited search of his surrounding area, without a warrant. When it comes to computers, cell phones, or storage devices seized incident to an arrest, a complete forensic search often requires the data to be extracted and then searched using forensic software. While the devices may be seized, a search warrant needs to be obtained to conduct the search.

#### **California Electronic Communications Privacy Act**

Based on the passage of SB 178, four new Penal Code sections (1546, 1546.1, 1546.2 and 1546.4) became effective January 1, 2016, which is known as the California Electronic Communications Privacy Act (CalECPA).

The Act restricts government access to information contained in electronic form and mandates procedures for law enforcement to follow in order to obtain electronic evidence.

PC §1546 defines 12 terms used in the Act.



### **Computer Forensics CCIC Training** Chapter 15: Reporting and Timeline

Lauren Pixley, Cassidy Elwell, and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# 15

# **Reporting and Timeline**

#### Introduction

After you complete your analysis of the forensic image, you will need to create a timeline and a report. Since this is still an introduction to digital forensics, your report will be simple and you will only stick to the key points of Who, What, When, Where, Why, and How. You will also want to create a very simple timeline of only the important events that happened on the computer, such as an incriminating email being sent or a file of interest being opened. This chapter will use the Craig Tucker case as an example.

#### Report

For the CCIC Event, you are expected to create a presentation (PowerPoint, Prezi, etc) that discusses Who, What, When, Where, and How. When you answer these questions, you will want to support your answer with as much evidence as possible. You can back up your answer with emails, Internet searches, files opened, or anything else of interest that relates to your response. For your presentation, you will want to have your title slide with the case name and each team member name.



Figure 15-1 – Title Slide with Case Name and Team Member Names

Your next slides should focus on the Who part of the report. When writing your answers on who the suspect is and who they were communicating with, you can easily go beyond just the simple points made below for the Craig Tucker case. Some cases you might find pictures of the suspect, personal documents with their information, or see them logging into personal accounts online.

#### Who was the suspect?

- 1. You know based on the scenario given at the beginning that the main suspect was Craig Tucker.
- 2. After searching through the Windows Registry, you determined the only user account was named Craig.
- 3. After going through the Windows 8 Mail App, you found emails that were sent and received by Craig Tucker under the email address "coupon-king@outlook.com".
- 4. After looking at the Google Chrome history and Windows 8 mail, you found Facebook accounts for Craig Tucker.
- 5. After reviewing the Skype chat logs, you saw chats to and from Craig Tucker.

Reporting on who was using the computer is important, because later you want to be able to prove that the suspect was the actual one behind the keyboard. You will also want to report who the suspect was talking to, because you may need to make recommendations to go after other accomplices. Your second slide after your title slide should focus on who the suspect was.

The Suspect
<ul> <li>Only user account was named Craig</li> <li>Found in SOFTWARE hive under <u>ProfileList</u> Subkey</li> </ul>
• Emails sent and received by Craig Tucker o Coupon-king@outlook.com
Internet history and emails showed Facebook account for Craig Tucker
Skype chat to and from Craig Tucker

Figure 15-2 – Slide on Suspect

After the second slide, you will want to include a slide on who the suspect was communicating with. This can include people he simply talked to or actual accomplices to a crime. Make sure to support your findings and show how the suspect knows the person if possible. You will also want to report who the suspect was talking to, because you may need to make recommendations to go after other accomplices.

#### Who did the suspect talk to or work with?

- 1. Craig sent and received emails from Stan Marsh, Kyle Broflovski, and Kenny McCormick about creating coupons. They also traded email attachments of coupons and guides on how to make them.
- 2. Craig talked to Kenny McCormick through Skype chat about coupons.
- 3. Craig sent and received emails from Stan Marsh about underage pictures.



Figure 15-3 – Slide on Witnesses and Accomplices

Next, focus on the What section of your report. For this section, you want to include what crimes the suspect committed or what they were planning on doing. You can support this through emails, documents, guides, chat, or anything else that shows they intentionally did something or planned something (see Figure 15-4). The What section can be put into one slide or multiple ones if necessary.

#### What did the suspect do? What was the suspect planning on doing?

- 1. Craig had accessed fraudulent coupons stored in his documents subfolders.
- 2. Craig had some images depicting child pornography in the recycle bin, but had other child pornography images stored in other locations.
- 3. Craig potentially has other child pornography and fraudulent coupons stored on external storage devices.
- 4. Craig sent and received fraudulent retail coupons.
- 5. Craig intentionally searched for and downloaded fraudulent retail coupons from the Internet.
- 6. Craig modified and produced fraudulent retail coupons, which were subsequently used to commit theft against a retail store.
- 7. Craig sent and received images depicting child pornography.
- 8. Craig talked with others about creating and using fraudulent coupons at a retail store.

# Crimes Committed/Crimes Planned • Accessed fraudulent retail coupons stored on his computer • Jump lists and link files show he accessed coupons in Documents /My Stuff folder and email attachment folder

- Has CP images stored on his computer
   Pictures and movies in his recycle bin and in Windows/System 32/system files folder
- Potentially has CP and fraudulent coupons on other devices
- Link files and jump lists show files in Coupons folder and underage pictures in Pictures folder on E: drive. The E: drive is a Kingston device Craig plugged in.
- Sent and received fraudulent coupons
   Email Subject: Free Coupons; 4chan Coupons, RE: College Paper! HELP; Re: Coupon Making; Awesome Coupons; Re: 4chan
- Intentionally searched for and downloaded fraudulent coupons
- Web history and web searches show Craig searched "coupons" and "how to make coupons"
  Modified and produced fraudulent retail coupons
- Recently-used shell file in AppData/Local folder shows Craig modified files using GIMP
- Talked with others about using fraudulent retail coupons
- Skype chat logs from main.db.file in App.Data\Local\Packages\Microsoft.SkypeApp\_kz/8qx/38zg5c\ LocalState\live#3acoupon-king\_1 folder

Figure 15-4 – Slide on Crimes Committed or Crimes Planned

After covering the What section, you will want to cover the How section. This ties together with the What part because you need to not only answer what the suspect did or planned on doing, but also how they did something or planned on doing something. You can include what software they used to accomplish something, how they used external drives to store and access data, or documents and chat that shows how they were going to commit a crime.

#### How did the suspect do the crime? How was the suspect planning on committing a crime?

- 1. Craig plugged in an external drive to access potential CP and fraudulent coupons.
- 2. Craig used the Windows 8 Mail App to send and receive emails with CP and fraudulent coupon attachments.
- 3. Craig used Google Chrome to search for and download fraudulent coupons.
- 4. Craig used GIMP to modify and create fraudulent coupons.
- 5. Craig used Skype chat to plan with Kenny on using fraudulent coupons at Walmart.



Figure 15-5 - Slide on How Crime was Committed or How Crime was Planned

The next part of the report is Where. The Tucker case does not really have that much location information. You know that he was caught at Walmart using fraudulent coupons. He also chatted with Kenny McCormick about going to Walmart to use fraudulent coupons.



Figure 15-6 Slide on Location of Crime or Planned Location of Crime

Some other cases you may be able to show more information on where the suspect did something or where they were planning on doing something. You can support your answer by providing time stamps, emails, chats, Internet history, or any other activity related to locations.

One slide you could potentially include is based on Why. You are not the suspect, so you cannot truly know why the person might have done what they did or planned to do something. However, you can speculate based on the evidence you found, such as needing money, wanting revenge, etc. In the Tucker case, there really is not a reason for why Tucker used fraudulent coupons, other than possibly wanting to save money, so I am not going to include a why section for this case.

#### Timeline

After working on the Who, What, How, and Where sections, you will probably want to include a section on When for your report. You will want to show when the suspect did certain things or when they planned on doing something. The best way to achieve this is by creating a timeline. Timeline analysis can usually become very complicated when you actually go into all the details about what was happening on the computer. Since this is still an introduction to digital forensics, you are only going to create a very simple timeline.

For this project, you will want to use the Office Timeline tool. You can download the 14-day free trial at the following website:

```
https://www.officetimeline.com/14-days-trial
```

**Note:** You only need to enter an email address to get the 14-day free trial. Once they send you the Plus Edition product key to the email address, simply open PowerPoint and click the Activate button under the Office Timeline Free tab. From there, you just need to paste the product key and click the Activate button.

Once you have Office Timeline downloaded and installed, open Office Timeline and click the New button.



Figure 15-7 – Click New Button on Office Timeline

When the Create New Timeline window opens, select the Metro timeline. Then, click the Next arrow in the bottom right corner.



Figure 15-8 – Select Metro and Click Next Arrow

×

On the next window, you will be prompted to enter the events and dates. You will also need to the click the Clock button in the top right corner to add time stamps to each event. Use the Plus button in the top right corner to add more events. You can set different colors and shapes based on the types of events. You may also want to check the Below box for certain events so the event text stays within the bounds of the PowerPoint slide.

Ultimately it is up to you what events you want to include in your timeline. You may want to show when certain Internet, file, email, or USB activity occurred. When creating your timeline, you may want to either create a separate slide for each day or keep your timeline to only specific simple events. This will help prevent the timeline from looking cluttered or confusing. For the Tucker case, I split the events that occurred on the 18<sup>th</sup> to just one slide. Once you add all the events you want, click the Finish button in the bottom right corner.

> Title	Date	Shape Below
Downloaded zip file with fraudulent coupons	<b>12/18/2013</b> 03:02	arr 🔻 🔲
Received email from Kenny with fraudulent coupons	<b>12/18/2013</b> 12:02	prr 🕨 🔲
Kingston device plugged in	<b>12/18/2013</b> 07:41	pm 🔶 🔲
Downloaded zip file with fraudulent coupons	<b>12/18/2013</b> 07:50	prr 🔻 🗌
Conducted search for coupons on 4chan website	<b>12/18/2013</b> 08:05	pr 🔻 🗌
Downloaded rar file with fraudulent coupons	12/18/2013 08:05	pr 🔻 🕅

#### Figure 15-9 – Add Events, Dates, and Times and Click Finish

Since most of your events are broken down by the hour, you will want to change the timeline scale. To do this, click on the Style Pane button under the Office Timeline+ tab. Then, click on the Timeline scale in the main slide. The right pane of PowerPoint will show a button called Timeline Scale. Click on it and then select Hours/Minutes (see Figure 15-10).



Figure 15-10 – Click Style Pane Button, Select Timeline Scale in Slide, and Choose Hours/Minutes under Timeline Scale

**Note:** You can also change where the timeline scale is by clicking the drop-down menu in the top bar called Timeline Position. The Middle position may work the best because you can then choose to have some events displayed above the timeline and some below.

After creating a timeline for one set of events, you can create another timeline on a different slide. This may help separate the days and keep your timeline from getting cluttered. However, it is ultimately up to you to choose what events you want to show in your timeline and how you want to report and present it.

s     12/20/2013     01:25 prr     ▶     ♥       12/20/2013     05:15 prr     ▶     ♥     ♥       12/20/2013     09:10 prr     ▼     ♥       12/20/2013     09:11 prr     ▼     ■
12/20/2013 09:10 pm 🔻 🔽
12/20/2013 09:11 pm
••• 12/20/2013 09:26 pm 🔺 🥅 🗙
12/20/2013 09:29 pm
12/20/2013 09:37 pm
12/20/2013 11:59 pm
12/21/2013 11:31 am
12/21/2013 07:19 pm 🔶 🔽
12/21/2013 07:32 pm 🔺 🔽

Figure 15-11 – Timeline with More Events on Second Slide

×

Depending on what case you are working on, you may want to show specific events that help support your Who, What, When, Where, and How points you previously made in your slides. For example, on the Tucker crime slide I showed a bullet point on how Tucker used GIMP to modify and produce fraudulent retail coupons. I then included in my timeline when Tucker downloaded and installed GIMP, when he accessed guides on how to make coupons, and when he modified a fraudulent coupon with GIMP.

If the case you are working on has a suspect planning to do something on a certain date, you may want to include that in your timeline as well. Again, it is up to you to decide how to best show your work and support your argument.



Figure 15-12 – Timeline of Events

After creating your timeline slides, you can also do a slide that just lists some events that you want to discuss further. For example, if the suspect planned on doing something, you may want to include a separate slide that discusses your findings further. It is up to you how you want to present all your findings.

One last slide you should include is a recommendation slide for the event. As an examiner, you may not always be asked to make recommendations, but for this event you will need to come up with recommendations based on your findings. Some possible recommendations include other accomplices that need to be looked into or where a suspect might be if they are on the run. For the Tucker case, the only real recommendation you could make is to look into Stan, Kyle, and Kenny because they traded coupons and underage pictures with Craig (see Figure 5-13).

### Recommendations

- Look into Kyle Broflovski for also using and creating fraudulent coupons
- Look into Kenny McCormick for also using and creating fraudulent coupons
- Look into Stan Marsh for fraudulent coupons and child pornography

Figure 15-13 Slide with Recommendations Based on Findings



# Windows Forensics CCIC Training Appendix A - G

Lauren Pixley, Cassidy Elwell, and James Poirier May 2019 (Version 2)



This work by <u>California Cybersecurity Institute</u> is licensed under a <u>Attribution-NonCommercial-NoDerivatives 4.0 International License</u>.

# Appendix A

#### **Review of Phases**

This is NOT a checklist to use when you are doing your analysis. Every case is different, and your analysis methods will change based on what you are looking for. Each step in Phase 1 is important to at least set the foundation of your analysis. Phase 2 then takes you through the key places to look when doing analysis. These different locations also depend on what you have the authority to search for.

#### Phase 1

- 1) Create your case and set the case options
- 2) Add your evidence
- 3) Verify the evidence file and check drive geometry
- 4) Check the computer's time zone and operating system
- 5) Identify the computer's users

#### Phase 2

- 1) Look for personal documents and pictures
- 2) Examine link files and jump lists for date/time stamps and data stored in other locations
- 3) Check recycle bin for any deleted data
- 4) Determine if there are any external storage devices
- 5) Review the user's email
- 6) Check Internet history and determine the user's web browser(s)
- 7) Look for any chat logs
- 8) Determine if there are any password protected files
- 9) Search for renamed files or hidden files and folders
- 10) Attempt to carve data (if it is necessary)
- 11) Identify the programs that are installed and what information they leave behind
- 12) Scan for malware

# **Appendix B**

#### **Common Areas (File System)**

There are several locations where data is stored on a computer. This appendix shows the most common areas for personal data, Internet history, email, and recent files for Windows XP, Vista, 7, and 8.

#### Windows Vista, 7, and 8

#### Desktop:

C:\Users\[User Name]\Desktop

#### Documents:

C:\Users\[User Name]\Documents

#### SkyDrive or OneDrive (Windows 8):

C:\Users\[User Name]\SkyDrive

C:\Users\[User Name]\OneDrive

#### Pictures:

C:\Users\[User Name]\Pictures

#### Videos:

C:\Users\[User Name]\Videos

#### Downloads:

C:\Users\[User Name]\Downloads

#### Recent (LNK Files):

 $C: \label{eq:lister_l$ 

#### Jump Lists:

 $C: \label{eq:lister_l$ 

C:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

#### Recycle Bin:

C:\\$Recycle.bin

#### History (Prior to Internet Explorer 10):

 $C: \label{eq:listers} C: \label{eq:listers$ 

#### Internet Explorer Cookies (Prior to Internet Explorer 10):

C:\Users\[User Name]\AppData\Roaming\Microsoft\Windows\Cookies

#### Internet Explorer Temporary Internet Files (Prior to Internet Explorer 10): C:\Users\[*User Name*]\AppData\Local\Microsoft\Windows\Temporary Internet Files

Internet Explorer History (Internet Explorer 10 or 11):

 $C:\Users\[User Name]\AppData\Local\Microsoft\Windows\WebCache$ 

Internet Explorer Cookies (Internet Explorer 10 or 11): C:\Users\[User Name]\AppData\Local\Microsoft\Windows\WebCache
Google Chrome History: C:\Users\[User Name]\AppData\Local\Google\Chrome\User Data\Default\History
Mozilla Firefox History: C:\Users\[ <i>User Name</i> ]\AppData\Roaming\Mozilla\Firefox\Profiles\[ <i>random</i> ].default\places.sqlite
Skype (Windows Vista and 7): C:\Users\[User Name]\AppData\Roaming\Skype\[Skype Name]
Skype (Windows 8): C:\Users\[ <i>UserName</i> ]\AppData\Local\Packages\Microsoft.SkypeApp_kzf8qxf38zg5c\LocalState\ [ <i>Skype Name</i> ]\main.db
Thunderbird Email: C:\Users\[User Name]\AppData\Roaming\Thunderbird\Profiles\[Profile Name]
Outlook Email: C:\Users\[User Name]\AppData\Local\Microsoft\Outlook
*Windows 8 Mail: C:\Users\[ <i>User Name</i> ]\AppData\Local\Packages\microsoft.windowscommunicationsapps_ 8wekyb3d8bbwe\LocalState\Indexed\LiveComm\[xxxxx]\[xxxxx-xxxx]\Mail\1
*Windows 8 Attachments: C:\Users\[ <i>User Name</i> ]\AppData\Local\Packages\[microsoft.windowscommunicationsapps_ 8wekyb3d8bbwe]\LocalState\LiveComm\[xxxxx]\[xxxxx-xxxx]\Att
NTUSER.DAT: C:\Users\[User Name]
USRClass.DAT: C:\Users\[User Name]\AppData\Local\Microsoft\Windows
Registry Hives (SYSTEM, SOFTWARE, SAM, SECURITY): C:\Windows\System32\config
*Note: The [ <i>xxxxx</i> ] is the user's live account number and the [ <i>xxxxx-xxxx</i> ] is the version of the app.

#### Windows XP

Desktop: C:\Documents and Settings\[User Name]\Desktop
Documents: C:\Documents and Settings\[User Name]\My Documents
Pictures: C:\Documents and Settings\[User Name]\My Documents\My Pictures
Videos: C:\Documents and Settings\[User Name]\My Documents\My Videos
Recent (LNK Files): C:\Documents and Settings\[User Name]\Recent
Recycle Bin: C:\RECYCLER
History: C:\Documents and Settings\[User Name]\Local Settings\History\History.IE5
Internet Explorer Temporary Internet Files: C:\Documents and Settings\[User Name]\Local Settings\Temporary Internet Files
Internet Explorer Cookies: C:\Documents and Settings\[User Name]\Cookies
Google Chrome History: C:\Documents and Settings\[ <i>User Name</i> ]\Local Settings\Application Data\Google\Chrome
$\label{eq:model} Mozilla \ Firefox \ History: \\ C:\Documents \ and \ Settings\[User \ Name]\ ApplicationData\ Mozilla\ Firefox\ Profiles\[random]. default\ places. sqlite$
Skype: C:\Documents and Settings\[User Name]\Application Data\Skype\[Skype Name]
Thunderbird Email: C:\Documents and Settings\[User Name]\Application Data\Thunderbird\Profiles\[Profile Name]
Outlook Email: C:\Documents and Settings\[User Name]\Local Settings\Application Data\Microsoft\Outlook
NTUSER.DAT: C:\Documents and Settings\[User Name]
Registry Hives (SYSTEM, SOFTWARE, SAM, SECURITY): C:\Windows\System32\config

# Appendix C

#### Common Areas (Registry)

As you learned in this class, the registry contains a great deal of information. Some of it will be useful during your investigation, so this appendix will show you the most common areas in the registry and where to find specific information.

#### **SYSTEM Hive**

The first thing you will want to do is determine the Current Control Set. Once you know the value of Current, then you focus on ControlSet*nnn*, such as ControlSet001.

	Subkey:	\Select		
	Value:	Current		
Tii	ne Zone:			
111				
	Subkey:	[ControlSetnnn]\Control\TimeZoneInformation		
	Value:	TimeZoneKeyName	(Name of time zone)	
		ActiveTimeBias	(Number of minutes off from UTC)	
Co	mputer Name:			
	Subkey:	[ControlSetnnn]\Control\ComputerName\ComputerName		
	Value:	ComputerName		
Sh	utdown Time:			
	Subkey:	[ControlSetnnn]\Control\Windows		
	Value:	Shutdown Time	(8 byte time stamp)	
IP	Address:			
	Subkey:	[ControlSetnnn]\Services\Tcpip\Parameters\Interfaces\{GUID}		
	Values:	DhcpServer	(IP Address of DHCP server)	
		DhcpNameServer	(IP Address of DHCP Name Server)	
		DhcpDefaultGateway	(IP Address of Gateway)	
		IPAddress	(Static IP Address, only if one is set)	
Pr	inters:			
	Subkey:	[ControlSet <i>nnn</i> ]\Control\Print\Environments\Windows NT x86\Drivers\[Version-#] [ControlSet <i>nnn</i> ]\Control\Print\Environments\Windows x64\Drivers\[Version-#]		
#### Share Points:

Subkey:	[ControlSetnnn]\S	[ControlSetnnn]\Services\LanmanServer\Shares	
Value:	[share name]	[ <i>share name</i> ] (contains share information)	
USB iSerialNum	ber, Vendor, Product, a	nd Version:	
Subkey:	[ControlSetnnn]\E	[ControlSetnnn]\Enum\USBSTOR\	
USB VID and PI	D:		
Subkey:	[ControlSetnnn]\E	num\USB\	

#### **USB Drive Letter and GUID:**

Subkey: \Mounted Devices

### **SOFTWARE Hive**

#### Windows Version:

Subkey:	Microsoft\Windows NT\Current Version		
Values:	ProductName	(Operating System)	
InstallDate (4-byte tim		(4-byte time stamp)	
	RegisteredOwner		
	RegisteredOrganization		
	CSDVersion (Service Pack)		

#### User Profiles, SIDs, and RIDs:

Subkey:	Microsoft\Windows NT\Currer	ntVersion\ProfileList[User SID]	
Value:	ProfileImagePath	(User Name)	
USB Volume Label:			
Subkey:	Microsoft\Windows Portable Devices\Devices		
Value:	FriendlyName		

### SAM

#### **User Account Names:**

Subkey: SAM\Domains\Account\Users\Names

#### User Account Information (Logon Count, Disabled Accounts, Last Logon Time):

Subkey: SAM\Domains\Account\Users

## NTUSER.DAT

Desktop Wallpaper:		
Subkey:	Software\Microsoft\Internet Explorer\Desktop\General	
Value:	Wallpaper	
Recent files in Wind	ows Start Menu:	
Subkey:	$Software \ Microsoft \ Windows \ Current \ Version \ Explorer \ Recent \ Docs$	
Commands typed in	Windows Run Box:	
Subkey:	$Software \ Microsoft \ Windows \ Current \ Version \ Explorer \ RunMRU$	
Programs that run w	when the user logs in:	
Subkey:	$Software \ Microsoft \ Windows \ Current Version \ Run$	
Typed URLS:		
Subkey:	Software\Microsoft\Internet Explorer\TypedURLs	
Typed URLS Time (	Windows 8):	
Subkey:	Software\Microsoft\Internet Explorer\TypedURLsTime	
Internet Explorer St	art Page:	
Subkey:	Software\Microsoft\Internet Explorer\Main	
Value:	Start Page	
Drives connected by	user:	
Subkey:	Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2	

## Appendix D

## Tools

Throughout this class, you used several different tools. The main tool was Autopsy, but there are many others that work just as well, if not better. These tools are useful, but it is always important to understand how they work, where they are pulling their information from, and to verify that they work.

The USB Historian tool is a perfect example. You first went through the NTUSER.DAT user profile hive, the SYSTEM hive, the SOFTWARE hive, and the setupapi.dev.log file to find information on the connected USBs. After knowing what information was extracted from the USB when it was connected and where the information was stored, you were able to use USB Historian and get a clean report without much effort.

The following is a list of the tools used in this class:

- 1) Autopsy v4.3
   https://www.sleuthkit.org/autopsy/
- Regedit Windows Default Program
- 3) Registry Explorer v0.8.1.0 https://ericzimmerman.github.io/PRTK
- 4) Ophcrack v3.7 and Vista Free Table http://ophcrack.sourceforge.net
- 5) Multi Content Viewer 3rd Party Plugin https://github.com/lfcnassif/MultiContentViewer/releases/tag/v1.0-beta
- 6) DCode v4.02a http://www.digital-detective.net/digital-forensic-software/free-tools/
- 7) JumpLister v1.1.0
  https://github.com/woanware/JumpLister
- 8) Jump List Parser https://tzworks.net/download\_links.php
- 9) Microsoft Excel (software capable of parsing .CSV files)
- 10) USB View

https://msdn.microsoft.com/enus/library/windows/hardware/ff560019(v=vs.85).aspx

- 11) USBDeview
  http://www.nirsoft.net
- 12) USB Historian v 1.3 http://www.4discovery.com/our-tools/
- 13) SkypeLogView v 1.55
  http://www.nirsoft.net/utils/skype\_log\_view.html

- 14) 7Zip v 16.04 http://www.7-zip.org/download.html
- 15) GIMP
  https://www.gimp.org/downloads/
- 16) Hex Decimal Converter
   http://www.rapidtables.com/convert/number/hex-to-decimal.htm

#### 17) File Extension/Signature Tables

http://file-extension.net/seeker/

https://en.wikipedia.org/wiki/List\_of\_file\_signatures

The following is a list of other useful tools that were not used in class:

- Aid4Mail (www.aid4mail.com) Use to collect, filter, search, convert, and extract email.
- Blackbag Macquisition (www.blackbagtech.com) Use for data acquisitions, targeted data collection, and forensic imaging for Mac computers.
- Bulk\_extractor (digitalcorpora.org) Use to scan a disk image, a file, or a directory of files. It then extracts useful information without parsing the file system or file system structures. Use to create word lists for password breaking.
- Directory Lister Pro (www.krksoft.com) Use to create file lists and view document metadata.
- Discovery Attender (www.sherpasoftware.com) Use to automate the search and collection of electronically stored information across a variety of platforms.
- 6) EDB Viewer (www.nucleustechnologies.com/exchange-edb-viewer.html) Use to open and view Outlook EDB files.
- Emailchemy (www.weirdkid.com)
   Use to convert, export, and import email between Outlook, Entourage, Apple Mail, Thunderbird, Outlook Express, Eudora, AOL, CompuServe, QuickMail Pro, Claris Emailer, and other email.
- 8) EnCase Forensic Imager (www1.guidancesoftware.com/Order-Forensic-Imager.aspx) Use to create EnCase evidence files and EnCase logical evidence files.
- Encrypted Disk Detector (info.magnetforensics.com/encrypted-disk-detector) Use to check local physical drives on a system for TrueCrypt, PGP, or Bitlocker encrypted volumes.
- 10) EWF Metadata Editor (www.4discovery.com/our-tools/)Use to edit EWF (E01) meta data and remove passwords (EnCase v6 and earlier).
- 11) FAT32 Format (www.ridgecrop.demon.co.uk/index.htm?fat32format.htm) Enables large capacity disks to be formatted as FAT32.
- 12) FirstPage 2000 (www.evrsoft.com)HTML editor and website builder that lets you create websites quickly.
- 13) Forensic Acquisition of Websites (www.fawproject.com/en/default.aspx) Use to forensically capture web pages.
- 14) F-Response (www.f-response.com)Utility that enables an investigator to conduct live forensic analysis, data recovery, and eDiscovery over an IP network using their tool(s) of choice.
- 15) Hashmyfiles (www.nirsoft.net)Use to calculate the MD5 and SHA-1 hashes of one or more files.

- 16) HotSwap (mt-naka.com/hotswap/index\_enu.htm) Safely remove SATA disks similar to the "Safely Remove Hardware" icon in the notification area.
- 17) Hypersnap (www.hyperionics.com)Use to take screen captures from Windows screen.
- 18) Irfanview (www.irfanview.com)Photo viewing tool for several different formats and will display EXIF data.
- 19) IE PassView (www.nirsoft.net)Small password management utility that reveals the passwords stored by Internet Explorer.
- 20) ISO Buster (www.isobuster.com) Use to recover data from optical media, hard drives, flash drives, and media cards.
- 21) LiveView (liveview.sourceforge.net)

Java-based graphical forensics tool that creates a VMware virtual machine out of a raw (dd-style) disk image or physical disk. This allows the forensic examiner to "boot up" the image or disk and gain an interactive, user-level perspective of the environment without modifying the image or disk.

22) Log Parser Lizard (www.lizard-labs.net)

Software tool that provides universal query access to text-based data, such as log files, XML files, and CSV files, as well as key data sources on the Microsoft Windows operating system, such as the event log, IIS log, the registry, the file system, and the Active Directory services.

- 23) MacDrive (www.mediafour.com) Use to get access of files on almost any Mac-formatted disk from Windows.
- 24) Mail Viewer (www.mitec.cz/mailview.html) Viewer for Outlook Express, Windows Mail, Windows Live Mail, Mozilla Thunderbird, and single EML files.
- 25) MD5 Summer (www.md5summer.org) Application for Microsoft Windows 9x, NT, ME, 2000 and XP which generates and verifies MD5 checksums.
- 26) MFT PictureBox (www.mikesforensictools.co.uk) Use to view digital photographs' EXIF data.
- 27) Mount Image Pro (www.mountimage.com)Use to mount E01, L01, AD1, DD, AFF, SMART, ISO, VMWare, Safeback v2, ProDiscover, Microsoft VHD, and Apple DMG images.
- 28) MyEventViewer (www.nirsoft.net) Alternative to the standard event viewer of Windows. Allows you to watch multiple event logs in one list and the event description and data are displayed in the main window.
- 29) Navroad (www.faico.net/navroad)Use as an off-line HTML browser for viewing HTML and web image files.

- 30) NetAnalysis (www.digital-detective.co.uk) Use for Internet history analysis.
- 31) Notepad++ (notepad-plus-plus.org) Notepad replacement.
- 32) Offline Explorer Enterprise (www.metaproducts.com) Use to download web sites to your disk and browse them any time; download Web, HTTPS, FTP, RTSP, PNM and MMS streaming media downloads. Offline Explorer Enterprise can create static offline copy of SharePoint and ASP/ASPX sites.
- 33) OSFClone (www.osforensics.com/tools/create-disk-images.html) Boot utility for CD/DVD or USB flash drives to create dd or AFF images/clones.
- 34) OSFMount (www.osforensics.com/tools/mount-disk-images.html) Mounts a wide range of disk images. Also allows creation of RAM disks.
- 35) OST Viewer (www.nucleustechnologies.com/ost-viewer.html) Use to open and view Outlook OST files.
- 36) PST Password (www.nirsoft.net)Use to recover lost password of Outlook .PST (Personal Folders) file.
- 37) PST Viewer (www.nucleustechnologies.com/pst-viewer.html)Use to open and view Outlook PST files.
- Reconnoitre (sandersonforensics.com)
   Parse data from Volume Shadow Copies.
- 39) Recover my Files (www.recovermyfiles.com) Use to recover deleted files.
- 40) RegexBuddy (www.regular-expressions.info) Use to build regular expressions.
- 18) RegRipper (regripper.wordpress.com) Use for registry analysis.
- 41) Robocopy (technet.microsoft.com/en-us/library/cc733145(v=ws.10).aspx)Command line file copy program that is a part of Windows 7. GUI versions are available.
- 42) SANS SIFT Workstation (computer-forensics.sans.org/community/downloads) The SIFT Workstation is a VMware appliance, pre-configured with tools to perform forensic examination. It is compatible with E01, AFF, and raw (dd) evidence formats.
- 43) Screenprint32 (screenprint32.en.softonic.com)Use to print and capture the desktop, active window, predefined area, or selected area of the screen.
- 44) Shadow Explorer (www.shadowexplorer.com)Use to browse the Shadow Copies created by the Windows Vista/7 Volume Shadow Copy Service.

45) SQLite Database Browser (sqlitebrowser.sourceforge.net/)

Use to create, design and edit database files compatible with SQLite. It is meant for users and developers that want to create, edit and search data without learning complicated SQL commands.

- 46) Tableau Imager (www.tableau.com) Imaging tool to use with Tableau imaging products.
- 47) The Sleuth Kit (www.sleuthkit.org) Tools that run on Windows, Linux, OS X, and other Unix systems. They can be used to analyze disk images and perform in-depth analysis of file systems (such as NTFS, FAT, HFS+, Ext3, and UFS) and several volume system types.
- 48) UltraEdit (www.ultraedit.com) Use as a text, hex, and HTML editor.
- 49) usp (www.tzworks.net)Use to create a report of each USB device connected to the computer.
- 50) VHD Tool (archive.msdn.microsoft.com/vhdtool) Use to convert raw disk images to VHD format, which are mountable in Windows Disk Management.
- 51) VideoLAN (www.videolan.org) Media player that plays files, discs, webcams, devices, and streams. Plays most codecs with no codec packs needed: MPEG-2, DivX, H.264, MKV, WebM, WMV, MP3.
- 52) Virtual Clone Drive (www.slysoft.com) Use to mount ISO images and treat them as actual CDs or DVDs.
- 53) Virtual Forensic Computing (www.virtualforensiccomputing.com) Use to boot a forensic image of a suspects computer or boot a physical write blocked hard drive. A Virtual machine can be created from a forensic image, a write blocked physical disk or a raw DD file image. Bypass any Windows user account password and rewind a machine by utilizing restore points.
- 54) Windows File Analyzer (www.mitec.cz/wfa.html) Use to decode and analyze special files used by Windows OS, such as thumbnails, prefetch, shortcuts, index.dat, and recycle bin.
- 55) Windows Jump List Parser (www.tzworks.net) Use to parse jump lists.
- 56) Win Prefetch (www.nirsoft.net)Utility that reads the Prefetch files and display the information stored in them.
- 57) XML to CSV Conversion Tool (xmltocsv.codeplex.com) Use to convert XML files to CSV files.

# Appendix E

## Email

During your analysis of the Tucker image, you found that he was using the Windows 8 app called Mail. There are several other email client software programs out there you should be aware of, and this appendix will walk you through two very common ones called Windows Live Mail and Mozilla Thunderbird.

### Windows Live Mail

Windows Live Mail is a free email client software program. Autopsy does not specifically support Windows Live Mail, because it's email module does not pull the email into the Results\E-Mail Messages. However, you can still see if the suspect is using Windows Live Mail by looking at the following path:

C:\Users\[User Name]\AppData\Local\Microsoft\Windows Live Mail\

Add Data Source 📠 View Images/Videos 🗮 Timeli	na 💽 Canarata Banart y		
Show Rejected Results	Directory Listing	✓ ✓ Keyword L	4.5 💌
AppData (5)		_ / // // //	
ianti anticianti antication (16) iantication (2) → Barbara (2)	Name	Created Time	Modified Time
	[current folder]	2014-05-01 18:36:35 GMT	2014-05-01 18:40:00 GM
- 📜 History (2)	[parent folder]	2014-02-14 22:22:34 GMT	2014-07-03 18:43:04 GM
□ □ □ Microsoft (16)	Backup	2014-05-01 18:36:41 GMT	2014-05-01 18:36:42 GM
→ Credentials (4)	Calendars	2014-05-01 18:36:35 GMT	2014-05-01 18:36:35 GN
E Feeds (7)	🗦 Gmail (Kyle 105	2014-05-01 18:38:16 GMT	2014-05-01 18:38:50 GM
⊕ Internet Explorer (13)	🔋 🗦 Outbox	2014-05-01 18:36:42 GMT	2014-05-01 18:36:42 GM
🕀 🔑 Media Player (6)	Sentinel	2014-05-01 18:36:43 GMT	2014-05-01 18:36:43 GM
Messenger (4)	Storage Folders	2014-05-01 18:36:42 GMT	2014-05-01 18:36:42 GN
→ NetTraces (2) ⊕	Your Feeds	2014-05-01 18:36:42 GMT	2014-05-01 18:36:47 GN
H Windows (20)	<ul> <li>III</li> </ul>		
Windows Live Mail (28)	Hex Strings File Metada	ta Results Indexed Text Media	Preview
→       Backup (3)       =         →       Calendars (3)         →       Gmail (Kyle 105 (5)         →       Outbox (2)         →       Sentinel (4)         →       Storage Folders (5)         →       Your Feeds (5)         →       Windows Mail (18)			

Figure E-1 – Windows Live Mail Path

The subfolder "Gmail (kyle 105\Inbox]\" is specific to this user and email account. If the user had an Outlook account, the path would be the:

```
C:\Users\[User Name]\AppData\Local\Microsoft\Windows Live Mail\[Outlook]
```

With Windows Live Mail, each email is being stored in plain text in a single .eml file. If an email has attachments, they are stored within the same eml file as the email.

If you want to view the attachment stored in the eml file, simply click the attachment name in the Preview pane.



Figure E-2 - Click on Attachment Name in Preview Pane to View Attachments

### Mozilla Thunderbird

Mozilla Thunderbird is another common email client software program. You can easily recognize Mozilla Thunderbird by the path:

C:\Users\[User Name]\AppData\Roaming\Thunderbird\Profiles\[xxxxxxx].default\

Note: The [xxxxxxx] will be randomly generated numbers and letters.

e <u>V</u> iew <u>T</u> ools <u>M</u> Add Data Source	e 📠 View Images/Videos 🗮 Timelin	ne 📕 Generate Report 🖇	▲ • Keyword	Lists Q- Keyword S
	Show Rejected Resul	ts Directory Listing	mdk.vol_vol2/Users/Stan/AppData/	() () () () () () () () () () () () () (
😺 All U 🕀 😺 Defa		Name	Created Time	Modified Time
	ult User (2)	[current folder]	2014-02-14 02:45:25 GMT	2014-02-14 19:08:07 GM
🖽 🔑 Publ		[parent folder]	2014-02-14 02:45:25 GMT	2014-02-14 02:45:25 GM
🗎 📜 Stan		🗦 ImapMail	2014-02-14 04:14:50 GMT	2014-02-14 04:14:51 GM
	ppData (5) Local (13)	📜 Mail	2014-02-14 04:14:51 GMT	2014-02-14 04:14:51 GM
	LocalLow (3)	minidumps	2014-02-14 02:45:25 GMT	2014-02-14 02:45:25 GM
	Roaming (8)	abook.mab	2014-02-14 04:15:12 GMT	2014-02-14 04:15:12 GM
	Identities (3)	addons.sqlite	2014-02-14 02:49:25 GMT	2014-02-14 02:49:25 GM
	Media Center Programs (2)	blist.sqlite	2014-02-14 02:45:26 GMT	2014-02-14 02:45:26 GM
	Microsoft (9) Mozilla (3)	blocklist.xml	2014-02-14 02:51:26 GMT	2014-02-14 02:51:26 GM
	Thunderbird (5)	cert8.db	2014-02-14 02:45:25 GMT	2014-02-14 19:08:07 GM
	Crash Reports (3)	۱۱۱ (III)		
Profiles (3)     Profiles (3)     Profiles (3)     Profiles (3)     Profiles (44)     Profiles (		Hex Strings File Metada	ta Results Indexed Text Media F	Preview
	🔋 Trillian (5)			
	pplication Data (2) ontacts (5)	4	111	

Figure E–3 – Mozilla Thunderbird Path

The subfolders "ImapMail\imap.mail.yahoo.com" is specific to that user and email client. For example, if the user was using POP3 instead of IMAP, the subfolder would be called "pop.mail.yahoo.com". If the email account was Gmail, the subfolder would be "imap.googlemail.com".

Each mail folder is stored in two files. One file has no extension, such as INBOX, and the second file has an extension of .msf, such as INBOX.msf. The INBOX file is the actual mail folder, while the INBOX.msf is an index file. The index file keeps track of the email sender, recipient, and subject line. It even contains a Unix 4-byte time stamp of when the email was sent and received.

Autopsy technically supports MBOX format with its Email Parser module. However, this version of Autopsy sometimes has errors when parsing each message and it does not display the email attachments. For these reasons, let's use another tool called Mailbag Assistant. This can be downloaded at:

```
http://www.tucows.com/preview/194096
```

To use Mailbag Assistant, you need to export the subfolder that contains the INBOX and other mail files. Right-click the subfolder in the left pane and then click Extract File(s) (see Figure E-4).

ase View Tools Window Help 🕂 Add Data Source 📠 View Images/Videos 🗮 Time					
🛉 Add Data Source 🌆 View Images/Videos 🚬 Time		1			
	line ¥	🔔 💿 - Key	word Lists	Q <del>.</del> Keyword S	•
← → Show Rejected	l Results	Directory Listing		( ) (	
→ □ Derauit User (2) → □ Public (12)	*	/img_Stan Thunderbird.vr Table Thumbnail	ndk/vol_vol2/l	Jsers/Stan/AppDat	a/Ro
🖨 🔑 Stan (32)		Name	Created 1	Time	Mo
AppData (5)		[current folder]	2014-02-	14 04:14:51 GMT	20
⊕		[parent folder]	2014-02-	14 04:14:50 GMT	20
Boaming (8)		Archives.msf	2014-02-	14 04:15:11 GMT	20
⊕      □ Identities (3)		Bulk Mail.msf	2014-02-	14 04:14:57 GMT	20
- December 20 -		Draft.msf	2014-02-	14 04:14:57 GMT	20
Hicrosoft (9)		Drafts.msf	2014-02-	14 04:14:51 GMT	20
⊕ Dozilla (3) → Dozilla (3)		INBOX	2014-02-	14 04:15:12 GMT	20
- Crash Reports (3)		INBOX.msf	2014-02-	14 04:14:51 GMT	20
□ D Profiles (3)		msgFilterRules.dat	2014-02-	14 04:14:56 GMT	20
🖶 🔑 tvjez0kw.default (44)		Sent-1	2014-02-	14 04:15:31 GMT	20
E ImapMail (5)	(25)	4	111		
umap.mail.yahoo.com □ □ □ □ Mail (3)		J File	Results In	dexed Text Media	Pre
Local Folders (8)	Tag	j i lie	[	Go to Page:	1
🔋 🖟 🖟 🖓 🖓 🖓 🖓	Ad	d file to hash database			
⊕ J Trillian (5)	Ext	ract File(s) 🔫	3D 22 31 2	C 6D 64 62 3A 6D 6 E 34 22 2F 3E 20 2	D 2D
<ul> <li>— J Application Data (2)</li> <li>— J Contacts (5)</li> </ul>		n Ingest Modules	6F 2D 38 3	D 63 29 3E 20 2F 2 B <mark>35 39 2D 31 29 0</mark>	D OA
Contacts (3)	2000	llapse All	3D 6E 73 3	A 6D 73 67 3A 64 6	2 3A

Figure E-4 – Extract Subfolder that Contains Mail Files

Extract the subfolder to your case's Export folder. It will export the subfolder and all the files within it. Once the files are exported, open Mailbag Assistant. You should be prompted with an E-Mail Wizard window after you close the Tip window. Highlight Mozilla Thunderbird as the type of mailbox and then click Next.



Figure E–5 – Highlight Mozilla Thunderbird and Click Next

On the second E-Mail Wizard window, navigate to your case's Export folder and highlight the mailbox subfolder you exported. Click Finish (see Figure E-6).

E-Mail Wizard			×
<ol> <li>Select the location that contains you can pick individual folders/mai</li> </ol>	a second a second s		a filment water and a second a filment of
Kip Kyle Nelson Stan Stan Marsh			•
Stan Marsh Stan Marsh Cache Export Log ModuleOutput Reports	il.yahoo.com		
Open all mailboxes		Include <u>s</u> ubfolders	
< <u>Back</u> <u>N</u> ext >	Einish	Cancel	Help

Figure E-6 – Highlight Exported Mail Subfolder and Click Finish

You can now view all the Thunderbird messages and see who sent the message, when it was sent, and if it had an attachment. If an email has an attachment, you can right-click the message in the grid and click Extract Attachments.

	orites Tools Help					
			1			
Grid View - Main Grid View -	Subset Message He	ader Message Body Raw E-Mail				
UTC D. Who	E-Mail Address	1.7.7.7.7.7.7.1.1.1.1.1.1.1.1.1.1.1.1.1	Status	Attachment /	Priority	Size I
2013/12/2 * Stan Marsh	stan.marsh27@y	Re. Coupon Making	2	•		894 🔺
2013/12/1 * Craig Tucker	coupon-king@out	Ne. Hundh	3	0		111
2013/12/2 * Craig Tucker	coupon-king@out	Re. Coupon Making	2	0		198
2013/12/2 * Craig Tucker	coupon-king@out	Hot Pics	3	0		126
2013/12/2 🤲 Stan Marsh	stan.marsh27@y	More Hot Pics	3	30		925
2013/12/2 ** Stan Marsh	stan.marsh27@y	MOLE HOLFICS	3	View		
2013/12/2 * Stan Marsh	stan.marsh27@y	MOLE HOLPICS	3	Copy To		
2013/12/2 ** Stan Marsh	stan.marsh27@y	More Hot Pics	2	Transfer		
•	m					
			_	Clear Subset (	Dirici	
Date: Sun, 22 Dec 20		0800		Close Selected	d Files	
Subject: More Hot Pi				Close All		
		upon-King@outlook.com>		Extract Attach	ments	-
From: Stan Marsh <st< th=""><td>-</td><td></td><td></td><td>Reply/Resend</td><td></td><td></td></st<>	-			Reply/Resend		
Reply To: Stan Marsh			_	Reply/Reserve	INIESSay	je
		1.jpg]; [underage_r@yg rage r@ygold 010.jpg]	01.	Invert Selection	n	
[underage_reygoid_0]	rs.jpg]; [unde	rage_reygora_oro.jpg]		Unselect		
Hey craig, i got u s	um more pics 2	2 add 2 ur russian col.	lec	Select All		
them away tho, dont b stupid and put them on the desktop o						
onon anal ono, aono	delete this email.			Groups Properties		
and the state of t						

Figure E–7 – Right-Click Email with Attachment and Click Extract Attachments

You will be prompted with a Browse For Folder window. Create a subfolder under your case's Export folder called Extracted Attachments. Select this folder and click OK (see Figure E-8).

	older: C:\Users\Lauren\AppData\Roam Trial\Attachments	ing\ <mark>Mailbag</mark>
4	Stan Marsh	~
4	📕 Stan Marsh	
	📙 Cache	
1	🚛 Export	
	👃 10256-imap.mail.yahoo.con	n 🗏
	膨 Extracted Attachments	
	Log	-
•	III /	Þ
	lew Folder OK	Cancel

Figure E-8 – Create Subfolder called Extracted Attachments and Click OK

You can now view the attachments from the email message that you extracted under the Extracted Attachments folder.



Figure E–9 – View Extracted Attachments

# Appendix F

## **Digital Photography EXIF Data**

Exif data, which stands for exchangeable image file format, is information stored in a digital photograph. A lot of the information, such as shutter speed, exposure, and flash usage, will have no forensic value. However, there is some useful information you want to focus on.

If you find digital photographs on your suspect's computer, it may be relevant to know the make and model of the camera that was used to take the photos. If your suspect possesses that camera, it becomes easier to confirm that he was the one taking the photos. It is also a good idea to know when the photos were taken.

In Autopsy, you can view this information by highlighting a digital photograph and then selecting the Strings view. There are a few entries of value in the Strings view. The first entry shows make of the camera used to take the picture. The second entry shows the model of the camera used to take the picture. The third entry shows when the picture was taken. As you can see in this example, the picture was taken on 2/12/14 at 18:58:04 GMT.

🗕 Add Data Source 📠 View Images,	/Videos 🧮 Timeline 🏻	🛕 💿 - Keyword Lists	থ <mark>ন্</mark> Keyword S
Show Rejected	d Results Directory Listing		<
	/img_Kyle Pictures	.vmdk/vol_vol2/Users/Kyle/Pictures	11 Resu
➡ Users (8) ■ Users (2)	Table Thumbnail		
	Name	Created Time	Modified Time
Default User (2)	↓ [parent folder]	2014-02-14 22:22:34 GMT	2014-02-14 22:23:
$\square$ $\square$ Kyle (31)	Stuff	2014-07-25 20:02:43 GMT	
🕀 🖟 AppData (5)	🕒 desktop.ini	2014-02-14 22:23:13 GMT	22220201000000000000000000000000000000
	DSC03225.JP		2014-02-13 02:58:
	DSC03226.JP		2014-02-13 02:58:-
	■ DSC03220.3P		
Desktop (3)			
Documents (6) Downloads (7)	DSC03228.JP	G 2014-02-14 23:08:23 GMT	2014-02-13 02:59:
⊕ Downloads (7)			
Links (7)		Metadata Results Indexed Text Me	dia Preview
Local Settings (2)	Pa 1 of 1	159 P ← → Go to Page:	Script
- <b>Wusic (3)</b>	Exif		
My Documents (2)	SONY		
	DSC-T9 2014:02:12 18:58:04	4	
🕀 🔑 Pictures (18)	PrintIM 0300	_	
PrintHood (2)	0220		
Recent (2)	0100 2014:02:12 18:58:04	4	
Saved Games (3)	2014:02:12 18:58:04 SONY DSC	4	
		III	

Figure F-1 – EXIF Make, Model, Date and Time Picture was Taken

If you want to have Autopsy pull all the files with EXIF data, you can run the Exif Parser plugin. Click Tools►Run Ingest Modules►[*Name of Evidence*]. When the Run Ingest Modules window opens, check Exif Parser and click Start (see Figure F-2).

😹 Run Ingest Modules	×
Recent Activity         Hash Lookup         File Type Identification         Embedded File Extractor         ✓         Exit Parser         Example         Email Parser         Extension Mismatch Detector         E01 Verifier         Android Analyzer         Interesting Files Identifier         PhotoRec Carver	The selected module has no per-run settings.
Virtual Machine Extractor Select All Deselect All View Ingest History Process Unallocated Space	Ingests JPEG files and retrieves their EXIF metadata. Global Settings Start Close

Figure F–2 – Check Exif Parser and Click Start

When Autopsy finishes processing the exif data, you can view it under Results\Extracted Content\EXIF Metadata. You can highlight the files in this list, right-click one of them and select Tag Results ► Tag and Comment.



Figure F-3 – Highlight and Right-Click EXIF Metadata Results and Click Tag and Comment

Create a new tag for the results. Once all the results are tagged, click Tools ► Generate Report (see Figure F-4).

Case View To	ools Window Help
🕂 Add Da	View Images/Videos Timeline
<b>€</b> →	Generate Report 🔫 ー
Data S	File Search by Attributes Run Ingest Modules
E S Views	Plugins Python Plugins
Result	Options
	Open Output Folder

Figure F-4 – Click Generate Report under Tools

When the Generate Report window opens, select Results - Excel. Click Next.

eport Modules: Results - HTML Results - Excel Add Tagged Hashes Files - Text Google Earth/KML STIX TSK Body File	A report about results and tagged items in Excel (XLS) format. This report will be configured on the next screen.
---	---

Figure F–5 – Select Results – Excel and Click Next

On the next window, select Tagged Results. Check the tag name you created for your EXIF Metadata results. Click Finish.

😹 Generate Report	×
Configure Artifact Reports	
Select which data to report on:	
C All Results	
Tagged Results	
EXIF Data	Select All
	Deselect All
	Data Types
< Back Next > Finish C	Cancel Help

Figure F–6 – Select Tagged Results, Check Tag Name, and Click Finish

Autopsy will generate an Excel spreadsheet under your case's Report folder (see Figure F-7).

	/le\Kvl	e\Reports\Kvle 04-	23-2017-13-24-57	
Organize • 📲 O			mail New folder	······································
Judeos	*	Name	Date modified	Туре
🤞 Homegroup		Excel.xlsx	4/23/2017 1:24 PM	Microsoft Excel Worksheet
<ul> <li>Computer</li> <li>Local Disk (C:)</li> <li>STORAGE-512 (D</li> <li>SCRATCH-240 (E:</li> <li>LAP (G:)</li> </ul>	-	/		
🕵 Network		(	m	4
Excel.xlsx Microsoft E	xcel W		Add a title	

Figure F-7 - Open Report in Case's Report Folder

You can view the results in a clean Excel spreadsheet report format. Click the EXIF Metadata tab at the bottom of Excel to view the EXIF Metadata. This function of Autopsy is useful if you need to give a report of the information you found to someone.

	<b>⋽ 5</b> - ∂	- 1 -				Excel.xl	sx - Excel		Lauren Pixle	ey 🗹	-		×
F	ile Home	Insert	Page Layout	Formulas	Data F	Review	View	🖓 Tell me what you	want to do			R	Share
Pas	te 💉 B		• 10 • A A • 🖄 • A • nt 5			\$	eneral ▼ ▼ % 9 0 →.0 umber □	Conditional Form Format as Table Cell Styles • Styles	•	■ Insert → → Delete → ↓ Format → Cells	$\sum_{x} \cdot \frac{2}{2} \cdot \frac{1}{2}$ $\downarrow \cdot \cdot$		^
128	3 -	: ×	√ fx										~
		A		В		С				D			
1	Date Taken	50.00 01		nufacturer		Model	Source		1 12 (1)	(W L (D) -	100000	225 100	
2	2014-02-12 18 2014-02-12 18				DSC-TS DSC-TS			yle Pictures.vmdk/v yle Pictures.vmdk/v		111	-		
4	2014-02-12 18		and a second second second		DSC-TS			yle Pictures.vmdk/v		and the second se	Guraalitar		
5	2014-02-12 18				DSC-TS			yle Pictures.vmdk/v					
6	2014-02-12 18	:59:59 GN	IT SONY		DSC-TS	Ð		yle Pictures.vmdk/v					
7	2014-02-12 19	:00:12 GN	IT SONY		DSC-TS	)	/img_K	yle Pictures.vmdk/v	ol_vol2/User	s/Kyle/Picto	ures/DSC03	230.JPC	j.
8	2014-02-12 19	:00:21 GN	IT SONY		DSC-TS	Ð	/img_K	yle Pictures.vmdk/v	ol_vol2/User	s/Kyle/Pict	ures/DSC03	3231.JPG	i
9													
10		-		-									-
.4	Sur	mmary	EXIF Metadata	Tagged	Files   T	agged F	Results	+ : •					•
Read	ły									ـ		-+ :	L00%

Figure F-8 – Report of EXIF Metadata Results

# Appendix G

## Windows 8 USB Worksheet

Section1					
Vendor:	Hive: SYSTEM				
Product:	Subkey: [CurrentControlSet]\Enum\USBSTOR				
Version:					
Section 2					
iSerialNumber:	Hive: SYSTEM				
	Subkey: [CurrentControlSet]\Enum\USBSTOR\[Device]				
	Section 3				
First time connected:	Hive: SYSTEM				
	<b>Subkey:</b> [CurrentControlSet]\Enum\USBSTOR\[Device]\[iSerialNumber]				
	\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0064				
	Section 4				
Last time connected:	Hive: SYSTEM				
	<b>Subkey:</b> [CurrentControlSet]\Enum\USBSTOR\[Device]\[iSerialNumber]\				
	Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0066				
	Section 5				
Last time removed:	Hive: SYSTEM				
	<b>Subkey:</b> [CurrentControlSet]\Enum\USBSTOR\[Device]\[iSerialNumber]\				
	Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0067				
	Section 6				
VID:	Hive: SYSTEM				
	Subkey: [CurrentControlSet]\Enum\USB				
PID:	Note: Conduct a search in USB subkey for the iSerialNumber.				
	Section 7				
GUID:	Hive: SYSTEM				
	Subkey: MountedDevices				
	Note: Conduct a search in MountedDevices subkey for the iSerialNumber.				
Section 8					
Drive Letter:	Hive: SYSTEM				
	Subkey: MountedDevices				
	Note: Conduct a search in MountedDevices subkey for the iSerialNumber				
	Section 9				
Volume Label:	Hive: SOFTWARE				
	Subkey: Microsoft\Windows Portable Devices\Devices				
	Section 10				
User that connected the device:	Hive: NTUSER.DAT				
	Subkey: Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2				
	Note: Conduct a search in NTUSER.DAT for device GUID.				

## Windows 7 USB Worksheet

Section 1						
Vendor:	Hive: SYSTEM					
Product:	Subkey: [CurrentControlSet]\Enum\USBSTOR					
Version:						
	Section 2					
iSerialNumber:	Hive: SYSTEM					
	<b>Subkey:</b> [CurrentControlSet]\Enum\USBSTOR\[Device]					
	Section 3					
First time connected:	Hive: SYSTEM					
	<b>Subkey:</b> [CurrentControlSet]\Enum\USBSTOR\[Device]\[iSerialNumber]\					
	Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0064					
	Section 4					
VID:	Hive: SYSTEM					
	Subkey: [CurrentControlSet]\Enum\USB					
PID:	Note: Conduct a search in USB subkey for the iSerialNumber.					
	Section 5					
GUID:	Hive: SYSTEM					
	Subkey: MountedDevices					
	Note: Conduct a search in MountedDevices subkey for the iSerialNumber.					
	Section 6					
Drive Letter:	Hive: SYSTEM					
	Subkey: MountedDevices					
	Note: Conduct a search in MountedDevices subkey for the iSerialNumber					
	Section 7					
Volume Label:	Hive: SOFTWARE					
	Subkey: Microsoft\Windows Portable Devices\Devices					
Section 8						
User that connected the device:	Hive: NTUSER.DAT					
	Subkey: Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2					
	Note: Conduct a search in NTUSER.DAT for device GUID.					
	Section 9					
Last time connected:	Hive: NTUSER.DAT					
	${\small Subkey: Software \\ Microsoft \\ Windows \\ Current \\ Version \\ Explorer \\ MountPoints \\ 2$					
	Note: Conduct a search in NTUSER.DAT for device GUID.					