CAL POLY

California Cybersecurity Institute

Computer Forensics CCIC Training

Chapter 4: Understanding the Registry

Lauren Pixley, Cassidy Elwell, and James Poirier

May 2019 (Version 2)

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.

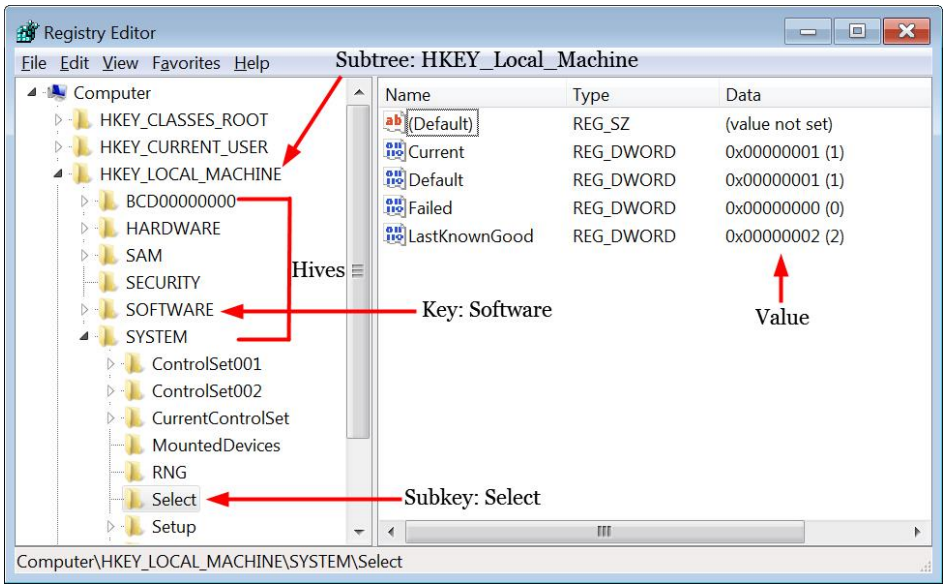

Figure 4-1 – Windows Registry Terms

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	HKCC	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\system32\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

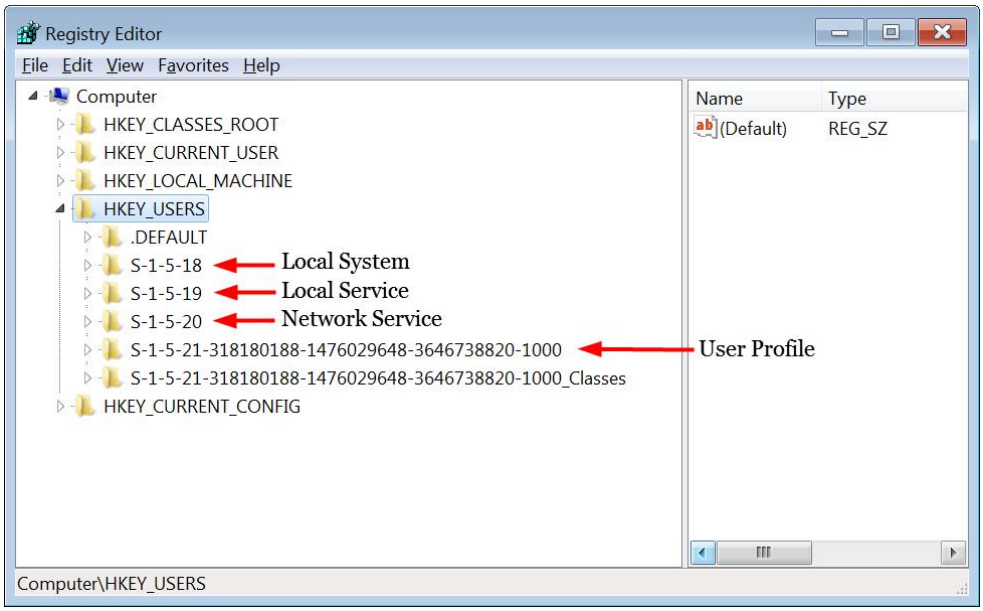

Figure 4-2 – User Profiles in Registry

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.

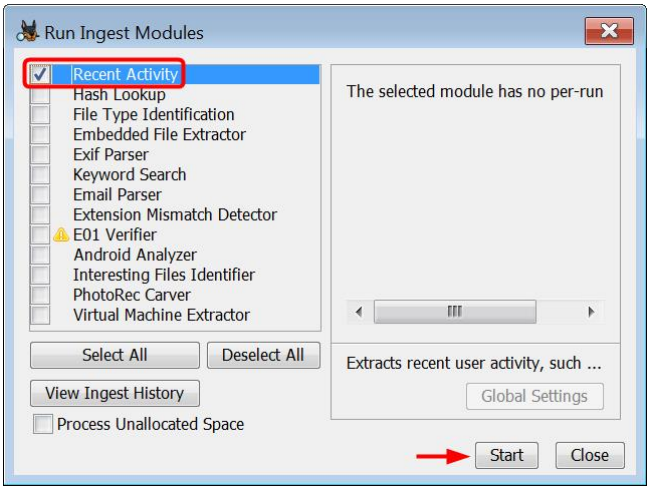

Figure 4-3 – Check Recent Activity Module and Click Start

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
```


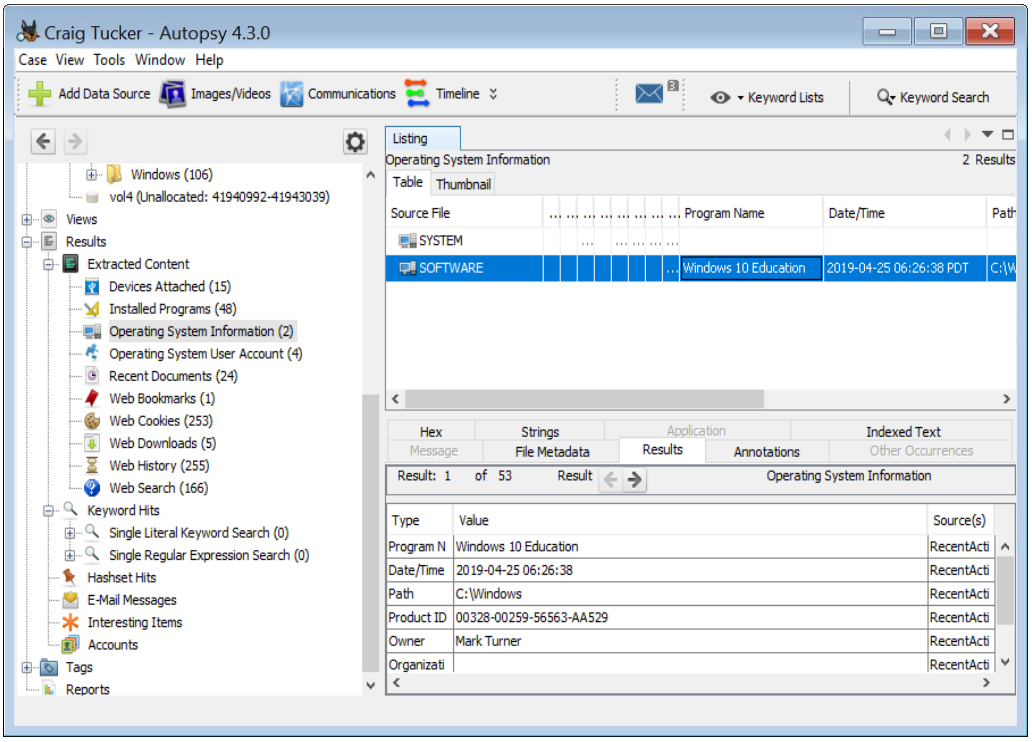

Figure 4-4 – Operating System Information Extracted from SOFTWARE Hive

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

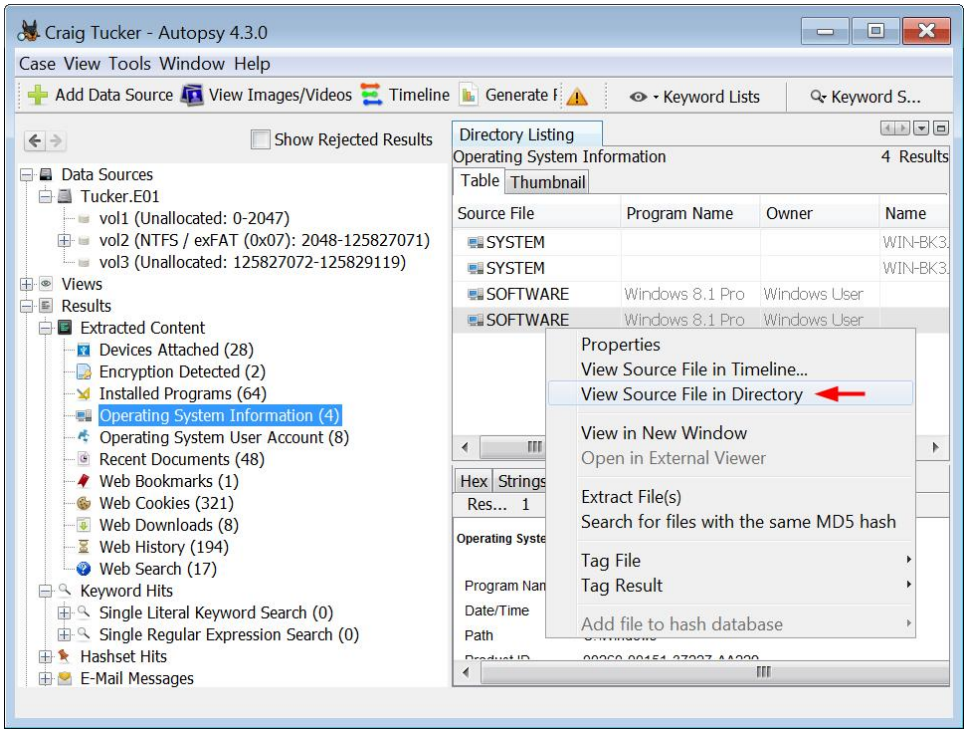

Figure 4-5 – Right-Click SOFTWARE Hive in Table Pane and Select View Source File in Directory

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).

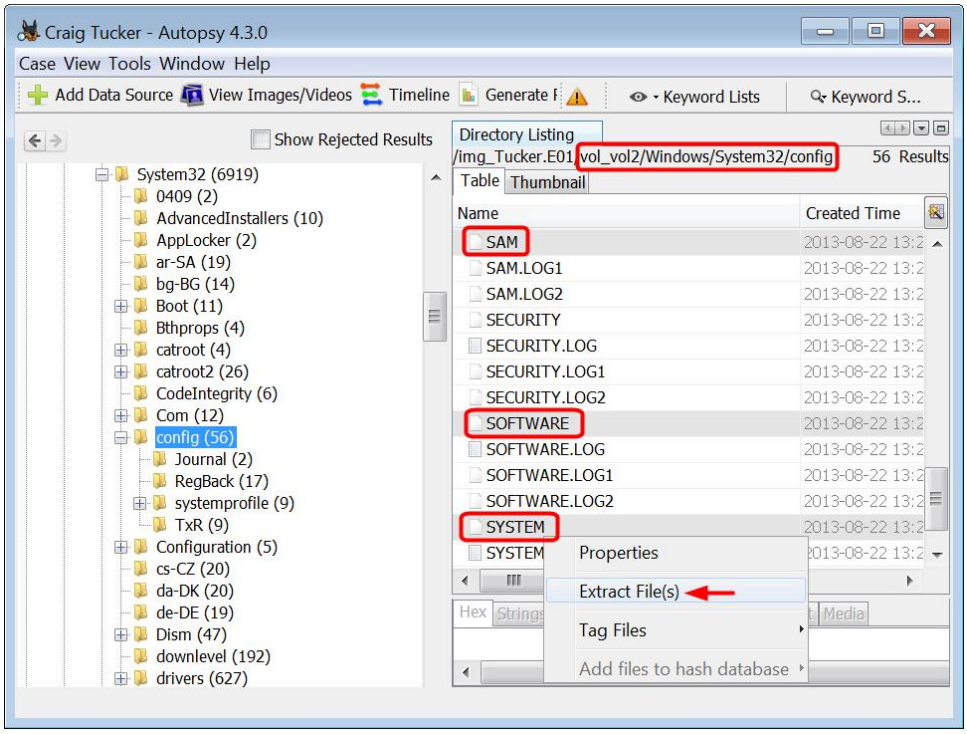

Figure 4-6 – Highlight SAM, SOFTWARE, and SYSTEM, Right-Click One and Select Extract File(s)

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.

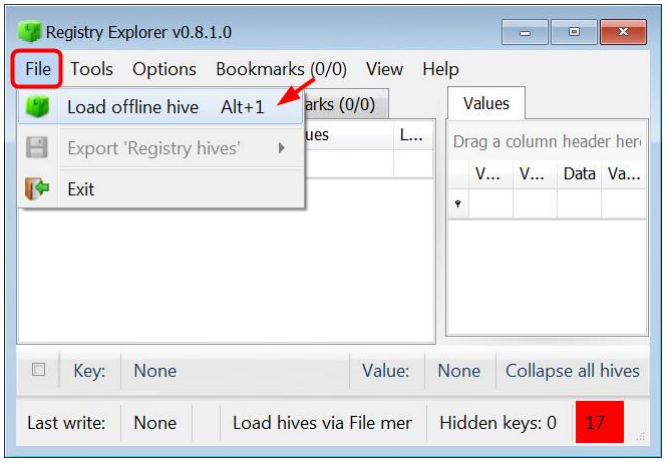

Figure 4-7 – Load Offline Hive in Registry Explorer

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
```

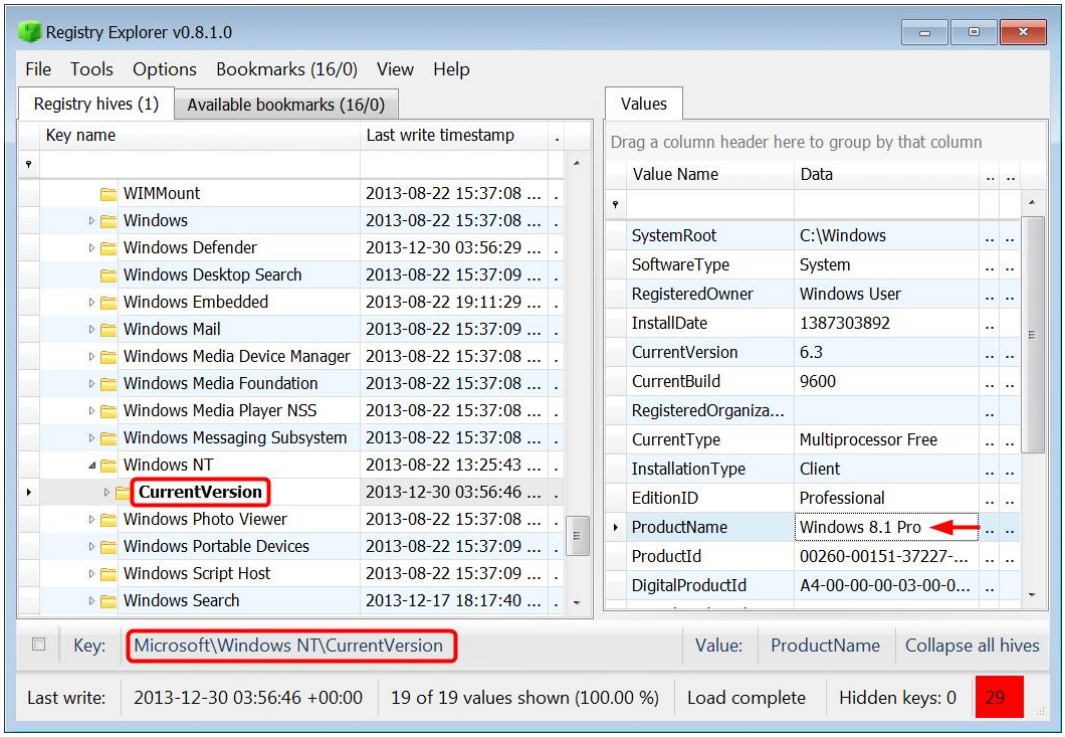

Figure 4-8 – Operating System in SOFTWARE

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.

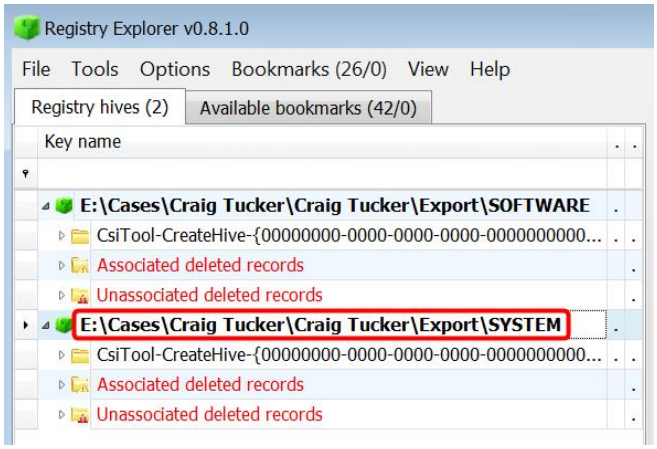

Figure 4-9 – Open SYSTEM Hive in Registry Explorer

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.

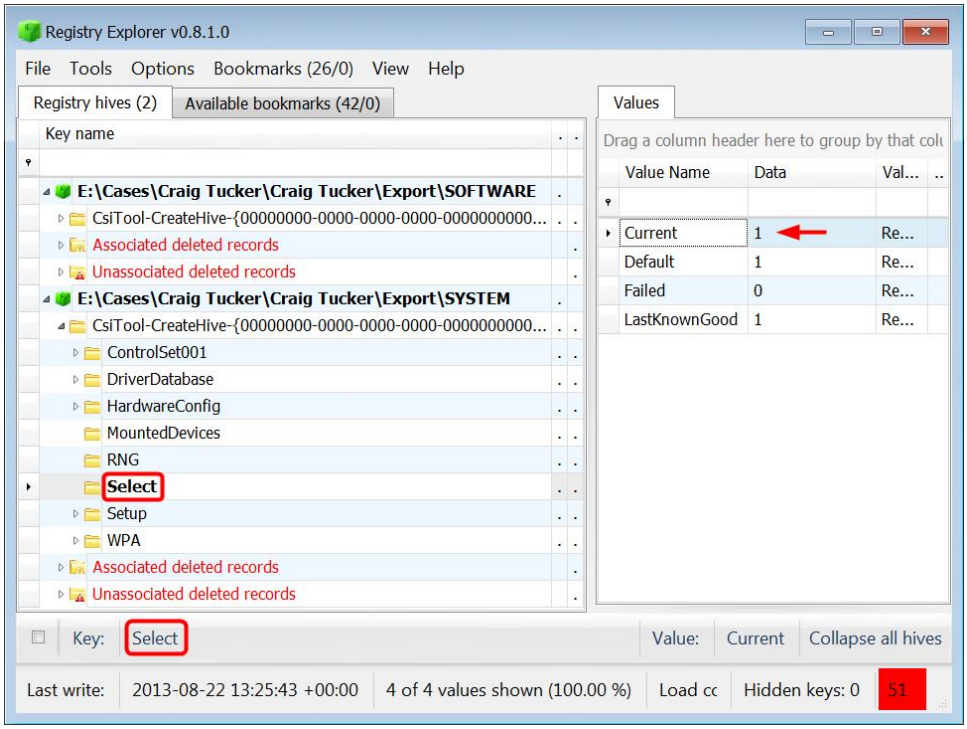

Figure 4-10 - Current Control Set in SYSTEM

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).

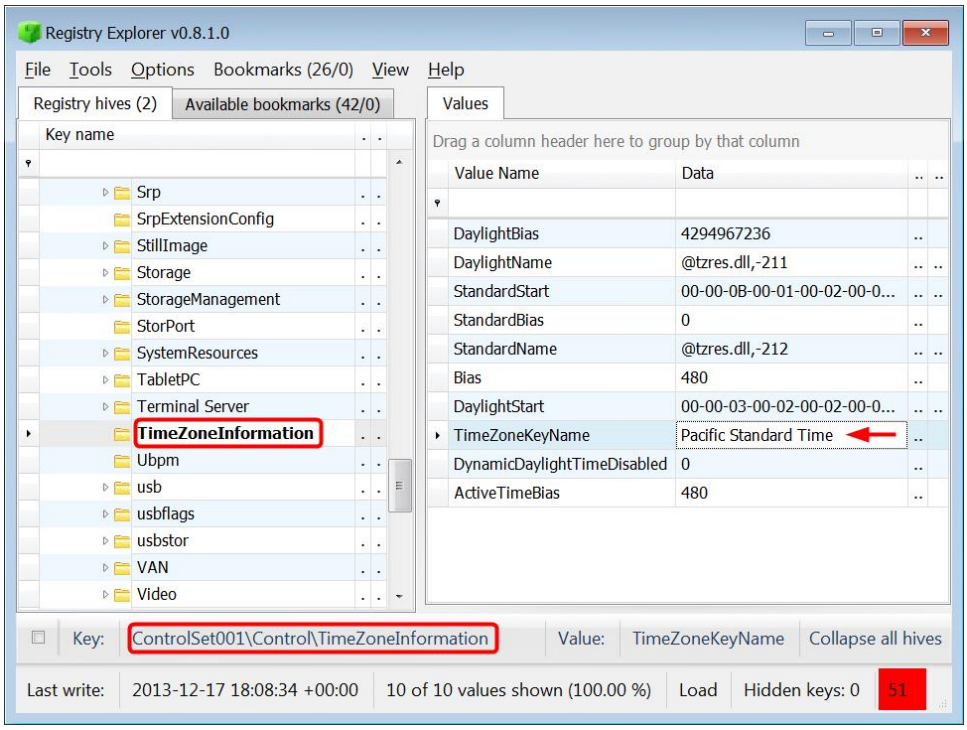

Figure 4-11 - TimeZoneInformation Subkey in SYSTEM

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).

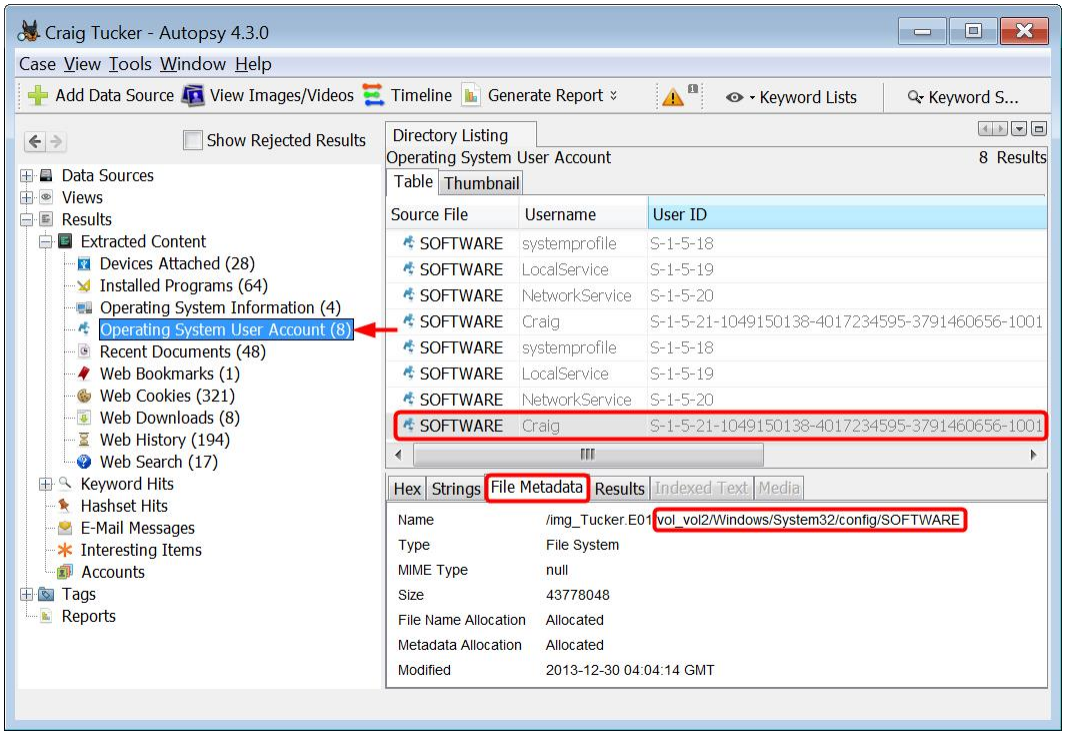

Figure 4-12 – User Account Information Extracted from SOFTWARE Hive

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).

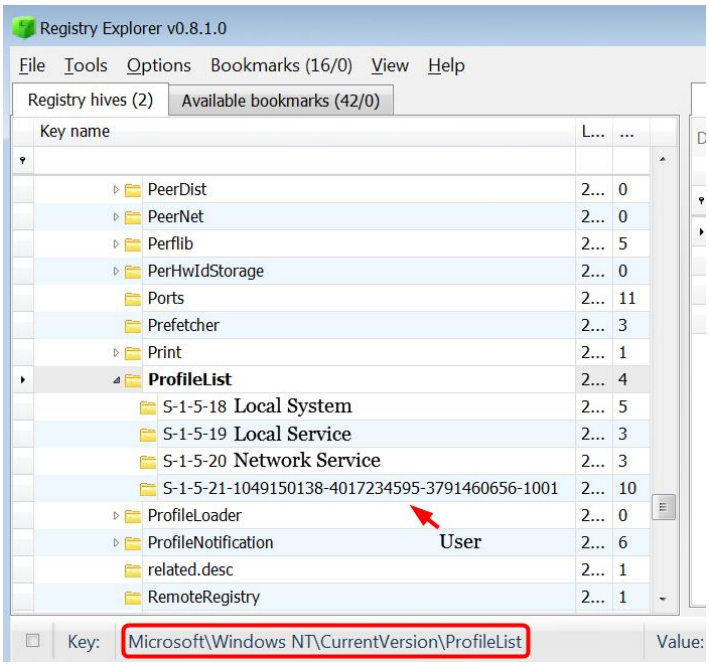

Figure 4-13 - User Profiles in SOFTWARE

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.

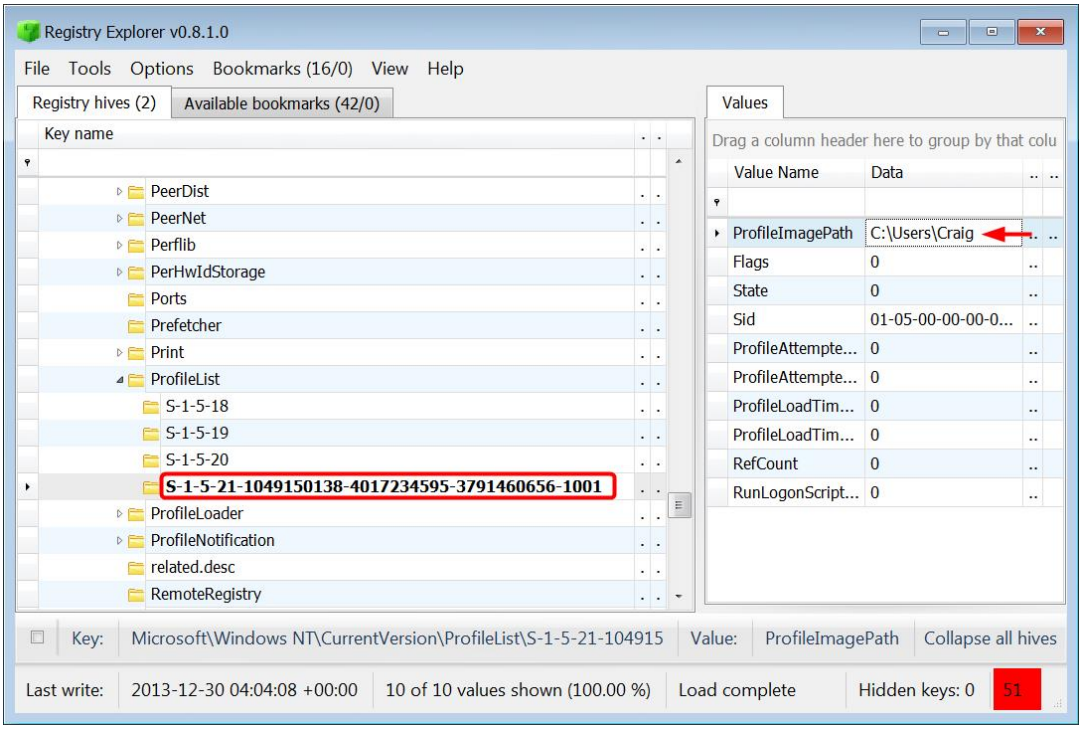

Figure 4-14 - User Craig's SID

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 = 500

000001F5 = 501

000003E9 = 1001

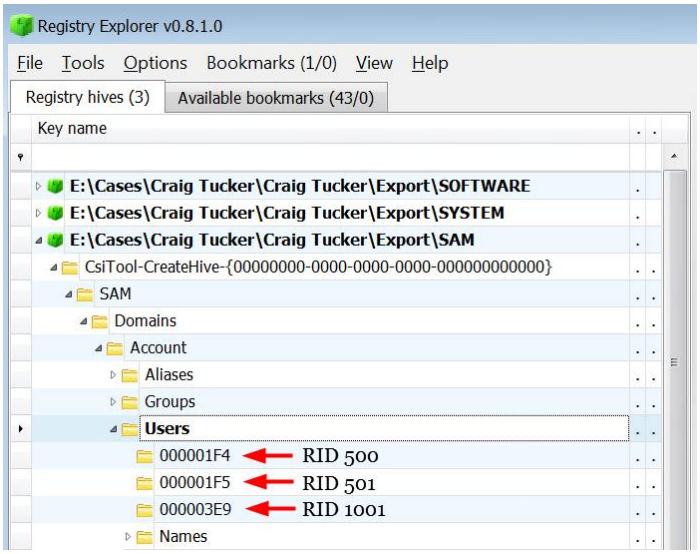

Figure 4-15 - User Profiles in SAM Hive

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.

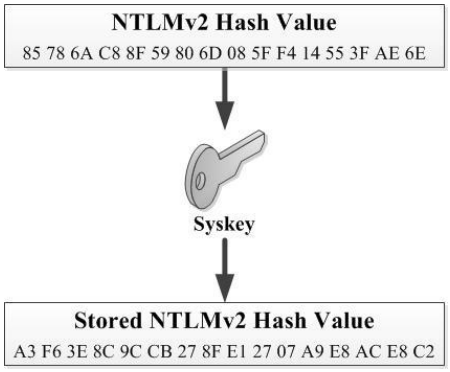

Figure 4-16 - Password Hash Value is Encrypted with Syskey

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).

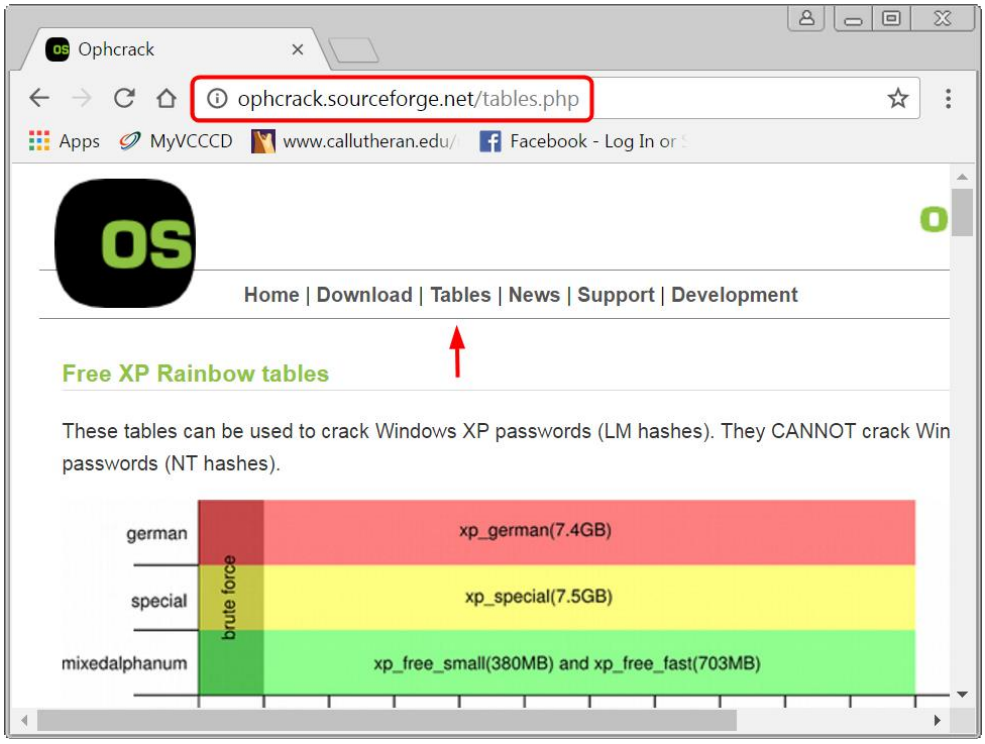

Figure 4-17 – Install Vista Free Table From Ophcrack's Website under Tables Tab

Open the Ophcrack tool and click Load►Encrypted SAM.

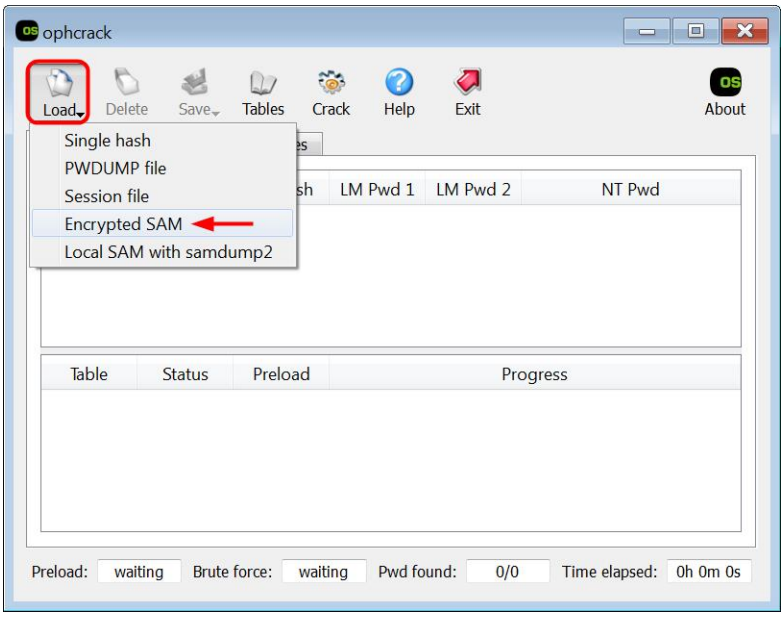

Figure 4-18 – Click Load Encrypted SAM in Ophcrack

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.

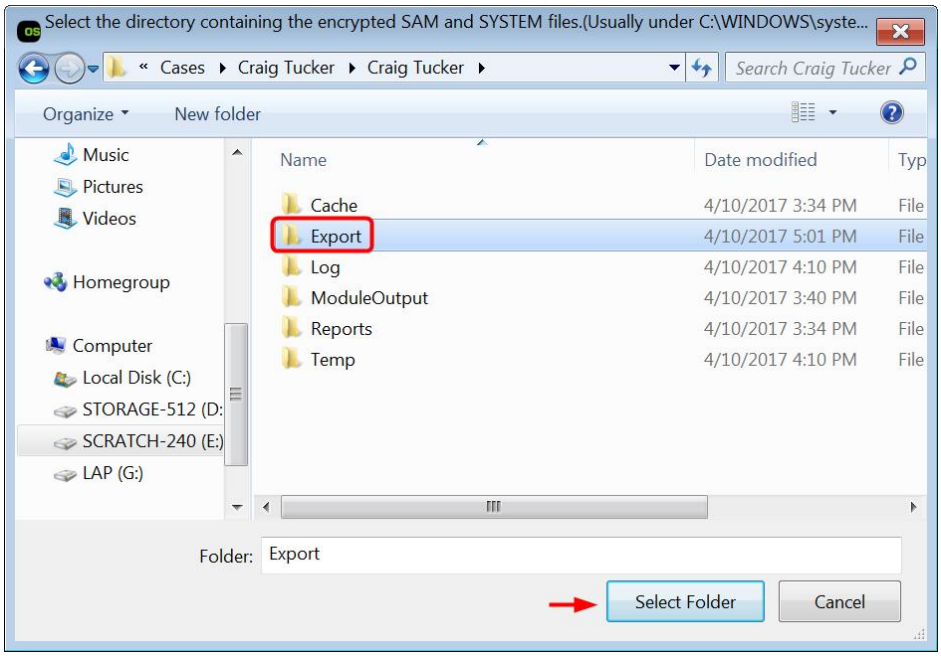

Figure 4-19 – Highlight Export Folder and Click Select Folder

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.

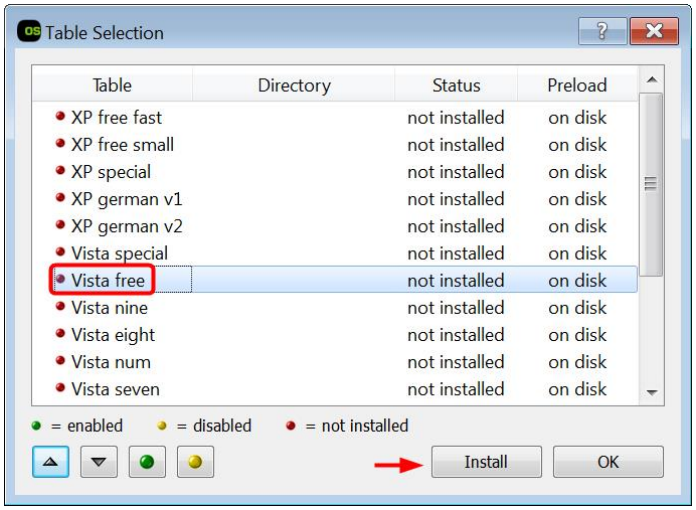

Figure 4-20 – Highlight Vista Free Table and Click Install

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).

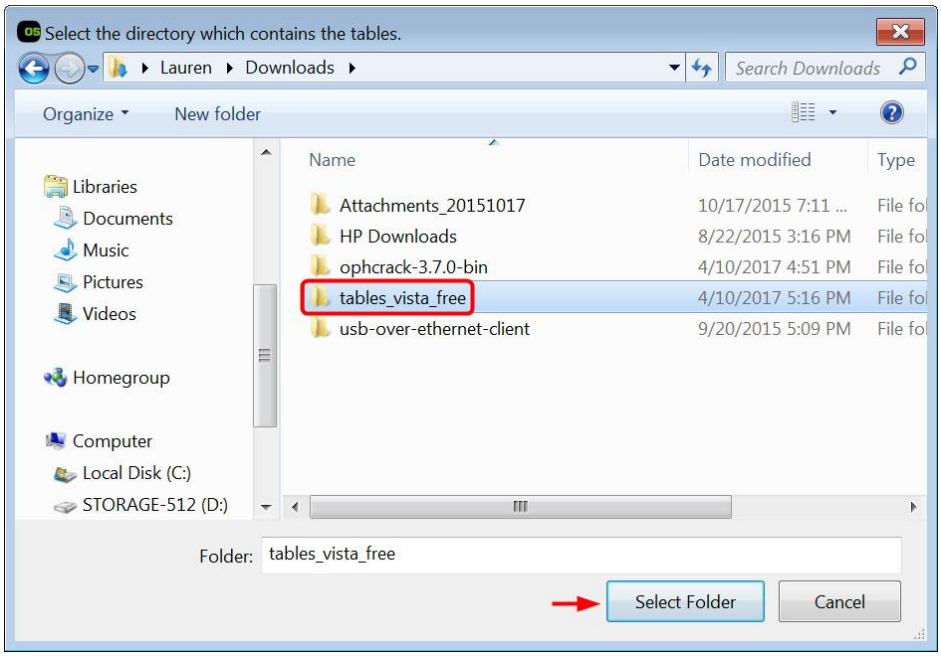

Figure 4-21 – Select Extracted Folder from Downloaded ZIP File and Click Select Folder

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.

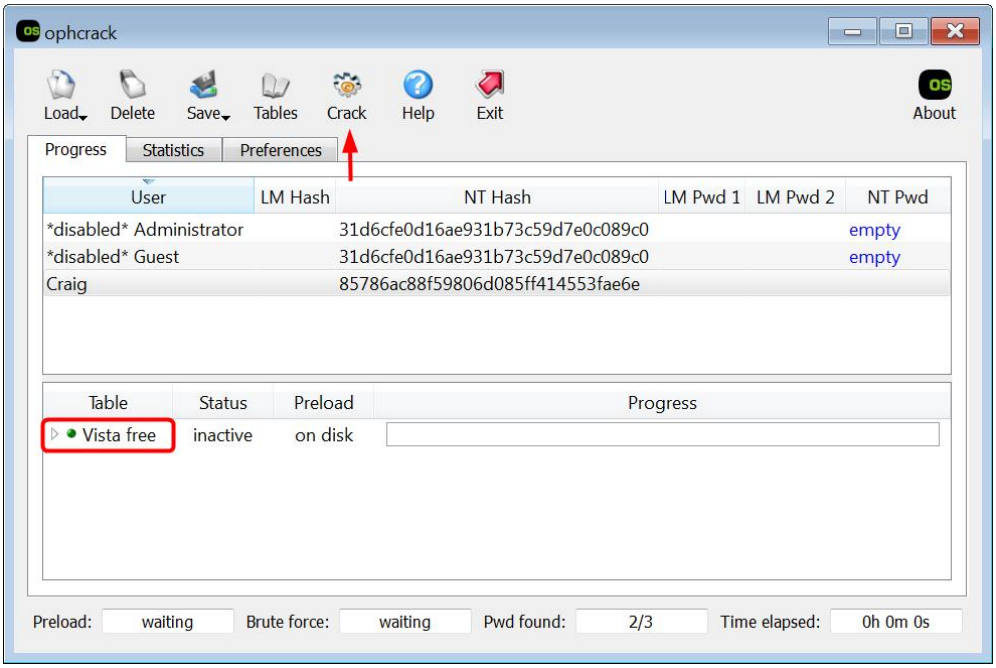

Figure 4-22 – Click Crack

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.

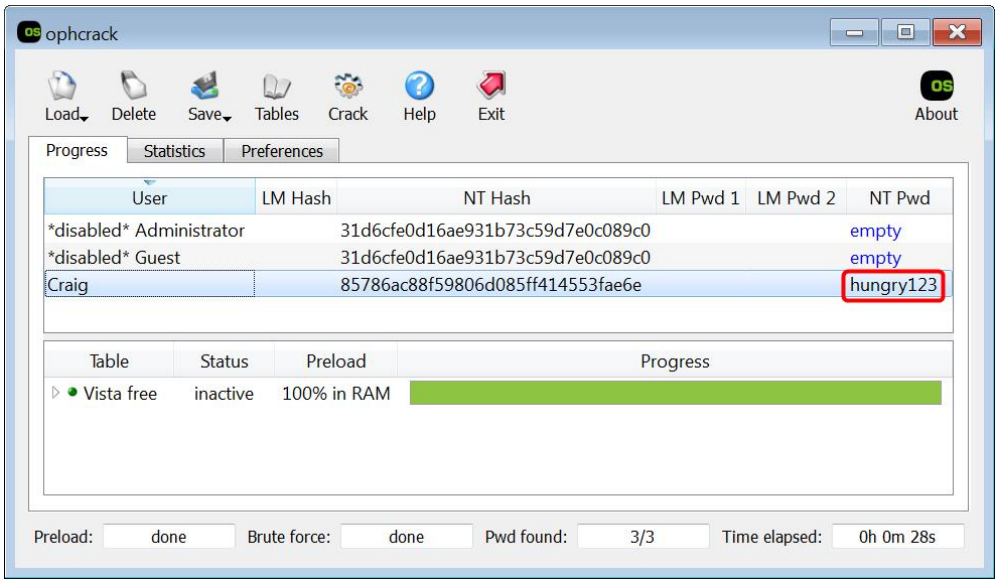

Figure 4-23 - Craig's Login Password Cracked

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.

