

CAL POLY

California Cybersecurity
Institute

Computer Forensics CCIC Training

Chapter 13: Installed Programs

Lauren Pixley, Cassidy Elwell, and James Poirier

May 2019 (Version 2)



This work by [California Cybersecurity Institute](#) is licensed under a [Attribution-NonCommercial-NoDerivatives 4.0 International License](#).

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.

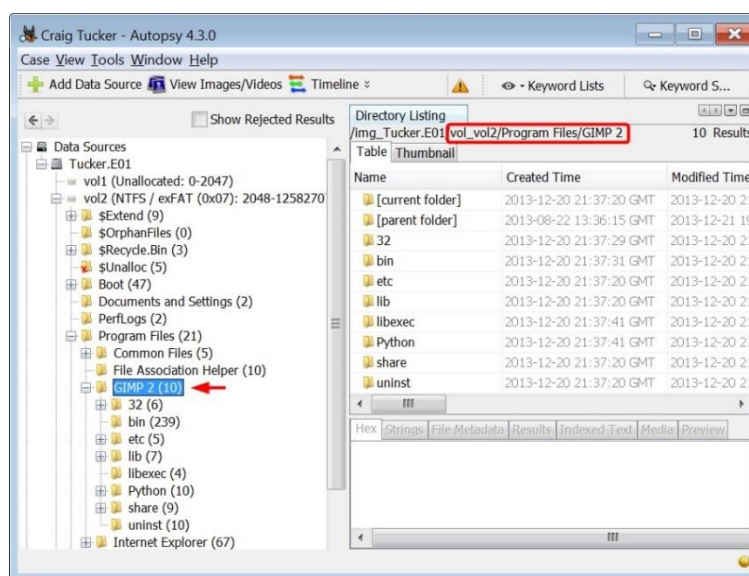


Figure 13-1 – GIMP 2 in Program Files

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.

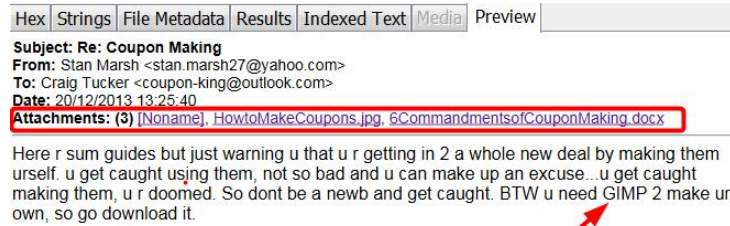


Figure 13-2 – Email Mentioning GIMP

Go to Craig's downloads folder in:

C:\Users\Craig\Downloads

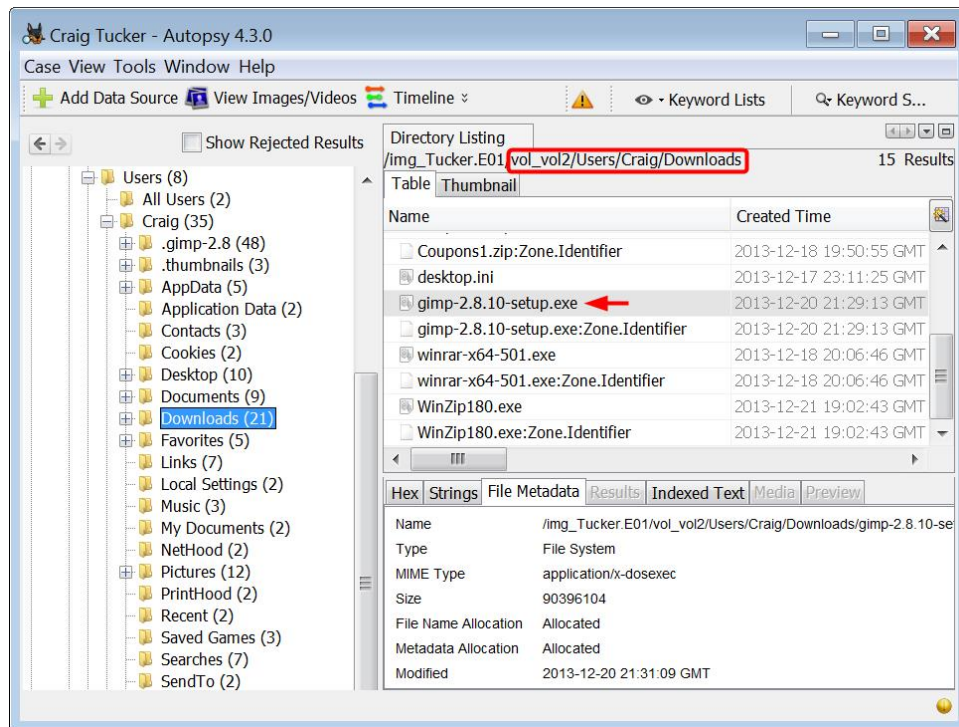


Figure 13-3 – GIMP Installer in Downloads Folder

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.

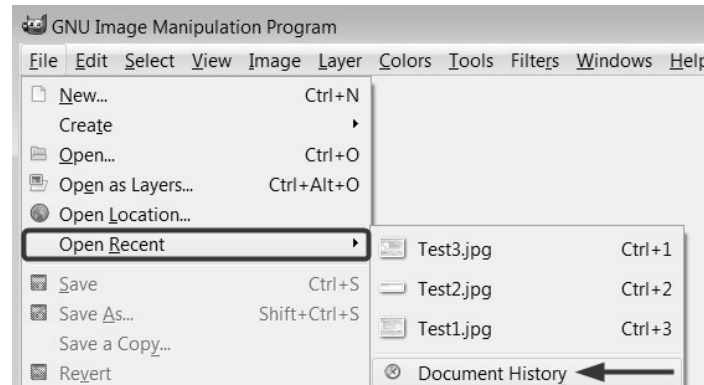


Figure 13-4 – GIMP Document History

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.

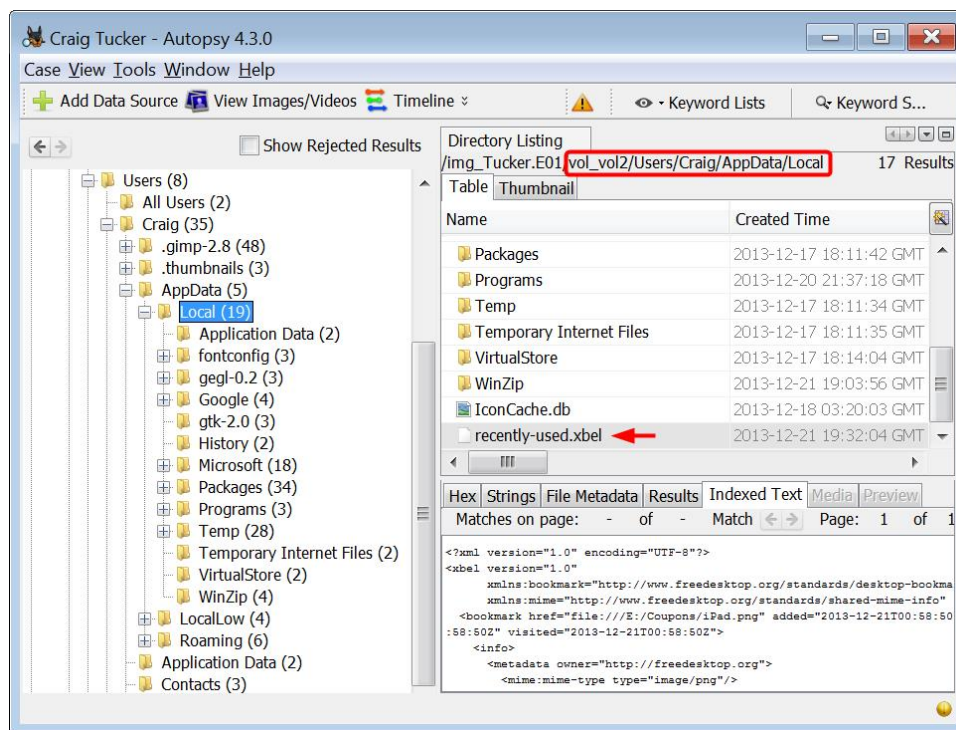


Figure 13-5 - GIMP Document History Stored in XML File

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).

```

Hex Strings File Metadata Results Indexed Text Media Preview
Matches on page: - of - Match Page: 1 of 1 Page
<bookmark href="file:///E:/Coupons/4.jpg" added="2013-12-21T19:17:45Z" modified="2013-12-21T19:17:45Z" visited="2013-12-21T19:17:45Z">
<info>
<metadata owner="http://freedesktop.org">
<mime:mime-type type="image/jpeg"/>
<bookmark:groups>
<bookmark:group>Graphics</bookmark:group>
</bookmark:groups>
<bookmark:applications>
<bookmark:application name="GNU Image Manipulation Program" exec="sapos:gimp-2.8 %sapos;
" modified="2013-12-21T19:17:45Z" count="2"/>
</bookmark:applications>
</metadata>
</info>
</bookmark>
<bookmark href="file:///C:/Users/Craig/Documents/My Stuff/Iced tea - edited.png" added="2013-12-21T19:19:58Z" modified="2013-12-21T19:19:58Z" visited="2013-12-21T19:19:58Z">
<info>
<metadata owner="http://freedesktop.org">
<mime:mime-type type="image/png"/>
<bookmark:groups>
<bookmark:group>Graphics</bookmark:group>
</bookmark:groups>
<bookmark:applications>
<bookmark:application name="GNU Image Manipulation Program" exec="sapos:gimp-2.8 %sapos;
" modified="2013-12-21T19:19:58Z" count="2"/>
</bookmark:applications>
</metadata>
</info>
</bookmark>

```

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.

Craig Tucker - Autopsy 4.3.0

Case View Tools Window Help

+ Add Data Source View Images/Videos Timeline Keyword Lists Keyword S...

Directory Listing

/img_tucker.E01 vol_vol2/Users/Craig/Documents/My Stuff 47 Results

Name	Created Time	Modified Time
1304643804769.png	2013-12-21 19:14:07 GMT	2011-05-06 05:23:04
1304644031008.png	2013-12-21 19:14:07 GMT	2011-05-06 05:25:18
Iced tea - edited.png	2013-12-21 19:19:58 GMT	2013-12-21 19:19:58

MANUFACTURER'S COUPON Expires:10/31/2011

Save \$3.00
on any one(1) 128oz container of AriZona® Iced Tea

RETAILER: We will pay you the face value plus 6¢ if all terms are met.
CONSUMER: Redeem only one coupon per product(s) and receipt indicated.
TERMS: Coupon must be redeemed in accordance with AriZona Beverage Co. coupon redemption policy (copies available upon request). Any other use constitutes fraud and may be prosecuted. Coupon good only in USA on specified product(s). Limit one coupon (any kind) per purchase. Coupon void if by you or agency authorized by us, you do not show on required product invoice(s) for all redeemed coupons.
Mail to: AriZona Beverage Co, CMS Dept. #762581, 1 Fawcett Dr. Del Rio, TX 78840, Cash Value 120¢, ©2009 AriZona Beverage Co.

Pin Number 87645581
Offer ID # 6843
POWERED BY SMARTSOURCE® 51 07336 00087 7

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.












Table Thumbnail		
Name	Created Time	Modified Time
 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
 1304394230314.jpg	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
```

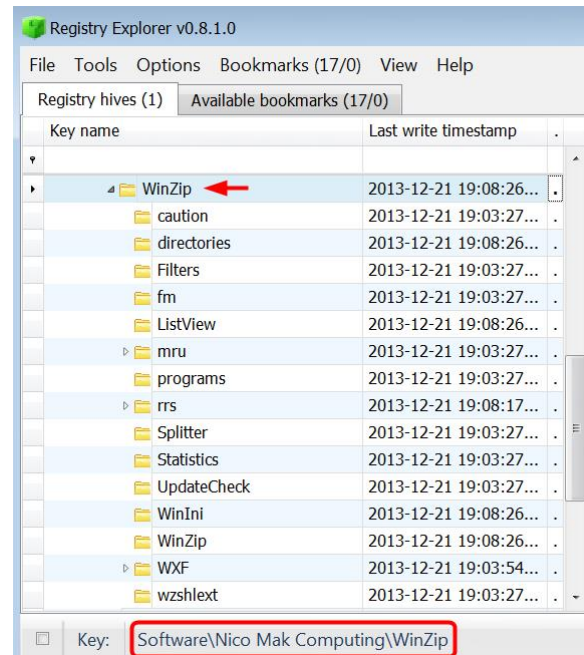


Figure 13-9 - WinZip Key in Craig's NTUSER.DAT

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

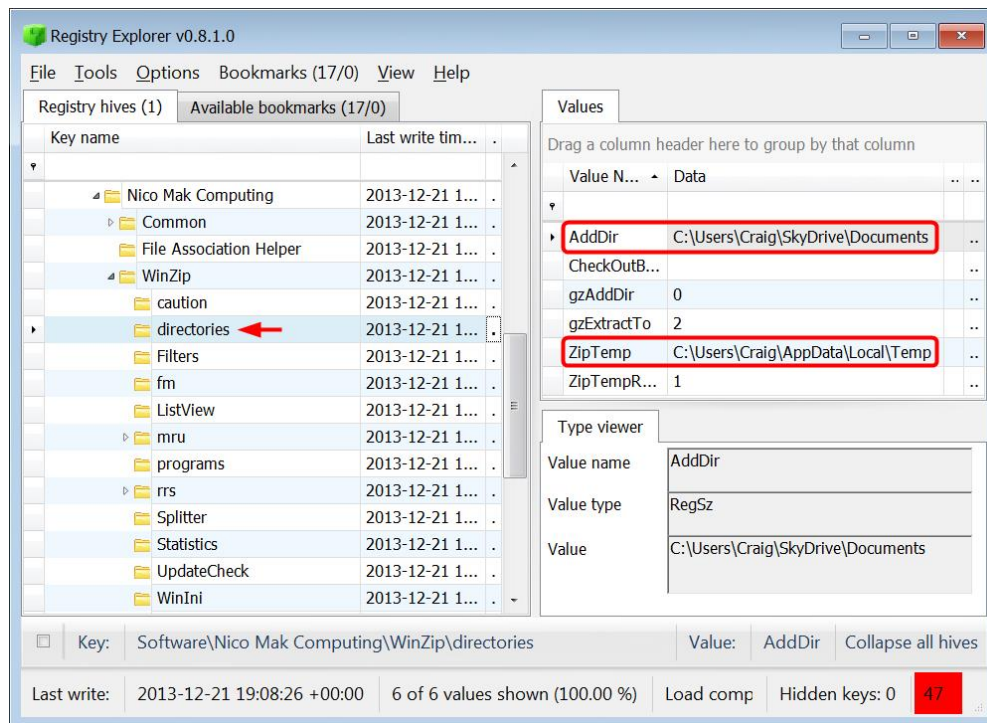


Figure 13-10 - AddDir and ZipTemp Values in Directories Subkey

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."

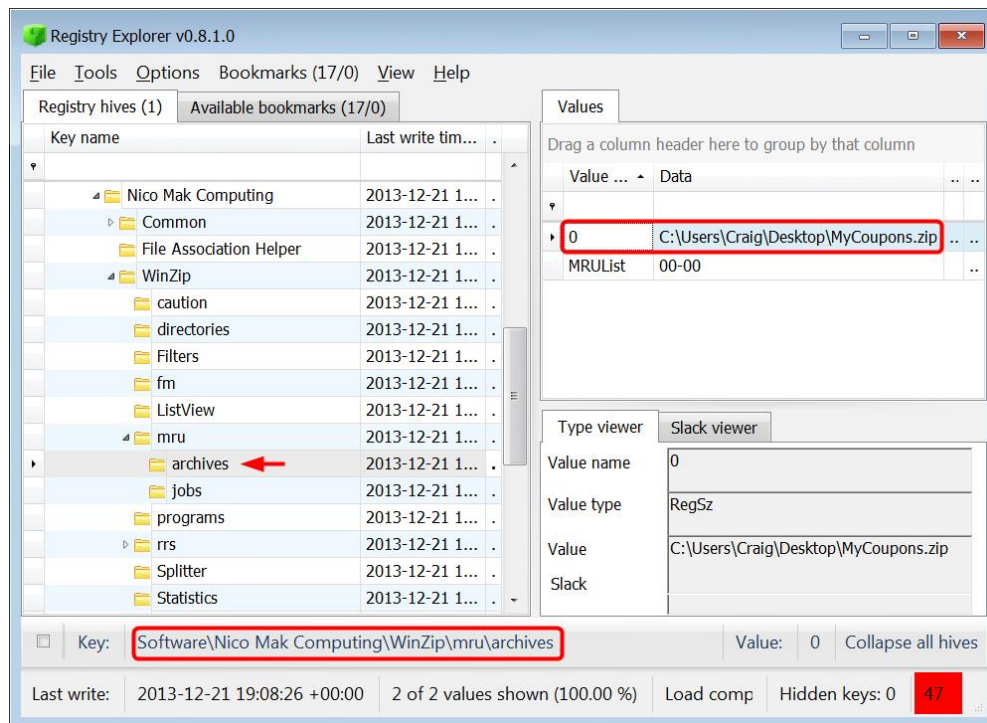


Figure 13-11 - ZIP File Created Using WinZIP

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:

Software\WinRAR\ArcHistory

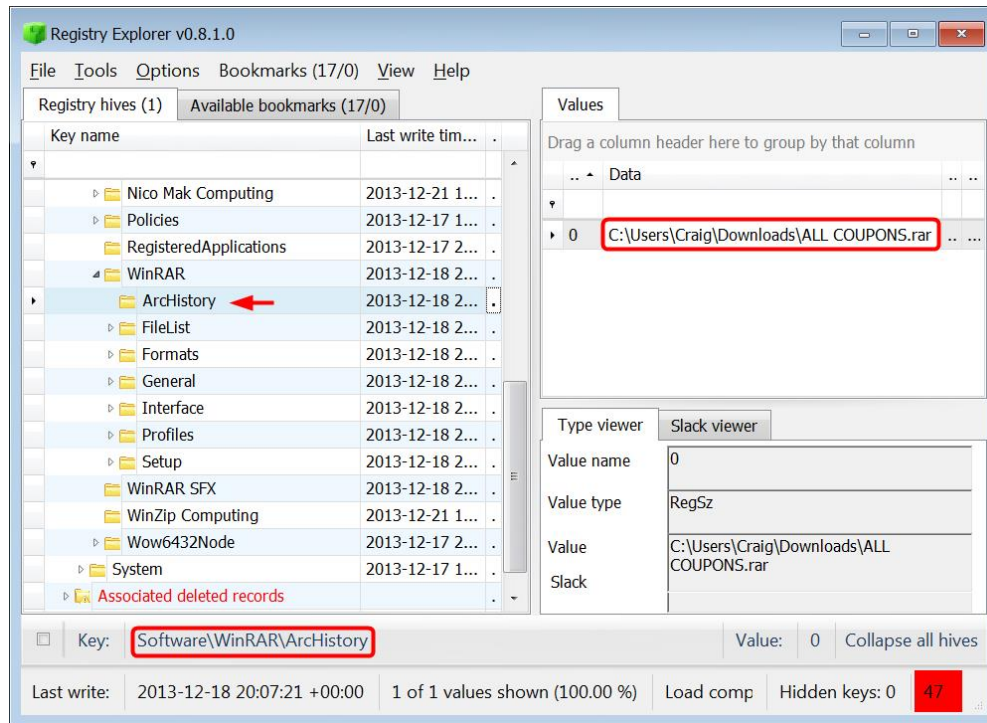


Figure 13-12 – ArcHistory Subkey Shows Files Opened with WinRAR

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).

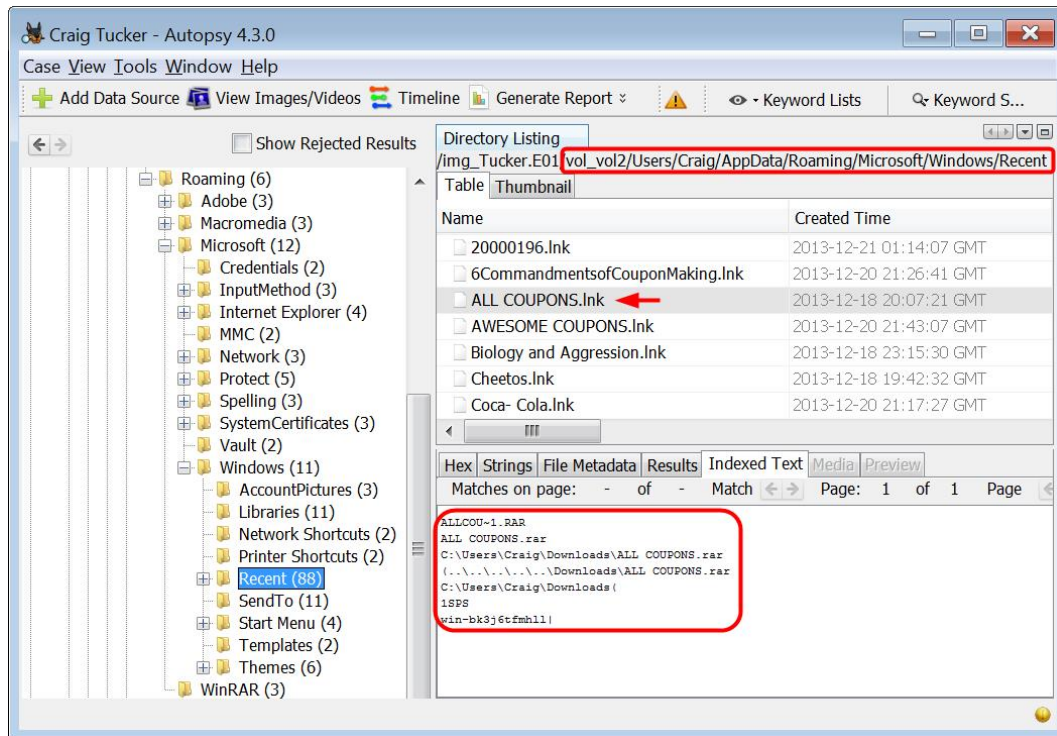


Figure 13-13 – Link File for ALL COUPONS.rar

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.

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.lnk	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