Forensics of a USB Drive

Chris P David

November 17, 2016

CSC 317

Professor MacDonald

Contents

1 Introduction

In this section I will try to, at best with my limited knowledge with these tools, explain what steps are required for this project as well as explain the steps for the following tasks:

Acquire a bit-stream copy from the pen drive: - For this step its essentially the first step of any criminal investigation as you need to copy the device. This is essentially done for the chain of custody rule as any work done on the drive without doing this first step will result in the entire evidence to do thrown out the window. Now for zip drives you can use some programs that will completely clone that drive and allow you to work around with the copy, this ensures the original is never touched and altered. We would place the device into the reader or if it dictates into the devices used for cloning drives. Then get the clone.

Recover deleted files:- This step is unique, usually speaking one would go to the trash bin to see if the files are truly deleted. Otherwise look at the MFT (Master File Table) and then look for the special character indicating a deleted file. You can also use programs like Recuva that would allow you to recover those files. Not only that but in extreme cases you can even use file recovery if the document is in word, but this works rarely. We use the program to view any of the deleted files then recover them.

Analyze all files:- This can be done simply with any hex editor/viewer like Winhex as we are using for this project. Simply put you use WinHex and look at the file type in the analyzer. We would look for a IMAGE_FILE type of structure. By using the tools within WinHex we would get sector information along with any data pertaining to file type association.

Try to identify image files concealing information:- We would use the stenography tool provided for this portion of the process, and would look for any irregularities within. We would use the program to let us know if any such occurrence happens.

Look for the pass phrase for steghide stored in the devices slack space:- This one is cool in the fact that the person hide their password into the slack space of a file. I haven't used the tool before but I assume that it will allow us to see the full details of the file. One thing that kinda irks me is that if a person hid a password into their file would they say it's a password of even encrypt that?

Recover information with steghide:- Finally use steghide to get information, and this would be done after doing all previous steps.

2 Winhex

2.1 What are you really?

Well at first what I did was to look at the budget.xls and saw that it had the header values 4A, 46, 49, 46, 00 which indicated that it was a jpeg so I renamed it.Upon opening in Winhex and looking at the contents I saw a link and went to it,www.corbisimages.com, and saw what seems to be images. Could this of been used as a image to place a hidden password?! Openign the jpg gave me a wave with a surfer

I then checked the Book.pdf and saw that it too is a jpeg and then renamed it to image02.jpeg. Looking into the file I'm seeing some weird things as the text indicates Global lighting angle and some other txt I also see a U n t i t l e d section. The photo gave me a sunset.

Brochure also is a jpeg it has almost the same data as Book did but with a Photoshop text, indicating Photoshop was used. This time the photo is a bunch of lilies.

The command.bat after being renamed to an jpg gave me almost the same information that the first one did. another JFIF header with the corbisimages.com text. The photo is of a skier.

Directions.doc is yet another jpg, I wonder how many this person did. upon renaming I got the same information as I did from command.bat. At this point I'm certain the corbisimages.com just refers to the fact this image was pulled from the site.

Guest list is another jpeg, that has the same information as Brochure.

License is another image from the corbis site and it is of a woman in the dessert.

Signature is a photo of a yellow tang! What's interesting is how the images are just images taken from the web yet serve another purpose.

Essentially all the files are jpgs!

The pass phase is steganography.