COMP6445 Digital Forensics

Week 2 Activity

Objective

As a digital forensic practitioner, you are obliged to take reasonable steps to ensure the outcome of your own work is reliable and sufficient. That means ensuring the techniques and tools you choose to use perform reliably and their performance is comparable to other tools commonly used by your peers for the same purpose.

The objective of this activity is to perform simple data carving using different tools and compare the results. Apart from familiarising you with common data carving tools, you should experience that relying on a single tool alone, without some checking (i.e. validation) may lead to incomplete or incorrect results.

Parts 1-7 of this week's activity are to be done during the tutorial/lab. The optional Part 8 is to be done at home.

Scenario

See the scenario provided with the Week 1 activity.

Instructions for week 2 activity

Instructions

You are instructed to examine the external hard disk drive provided by Ms Moneypenny and determine what pictures are currently on it and what pictures were on it i.e. what pictures can be recovered.

You are further instructed that Mr Bond claims that the Land Rover depicted could be anyone's car. Ms Moneypenny recalls that one of the two pictures of the Land Rover clearly showed Mr Bond's number plate.

For the purpose of this activity, you can assume that the pictures are in the JPEG format. You can also assume that you have already made a forensic copy (which you did as part of the Week 1 activity).

Tools

Forensic Workstation #1: A Kali Linux workstation
Forensic Workstation #2: A Windows 10 workstation.

An image of the USB key is installed in the Documents folder on each workstation and is called USBkey.img.

Process using Kali Linux

Step 1 – View the image

Mount the image and view the pictures.

How many pictures are currently there?

Step 2 – Hash the current pictures

Step 3 – Unmount the image

Step 4 – Recover pictures using Scalpel

These carving tools will extract pictures from the image file, some of which are still there and some of which the user deleted (or so they thought).

Create a directory for the output and then run scalpel.

Did you recover the picture of the sports car?

Step 5 – Recover pictures using Photorec

Run photorec.

Do you see recovered pictures?

Step 6 – Recover pictures using Recoverjpeg

Create a directory for the output and then run recoverjpeg.

Did you recover the picture of the sports car?

Step 7 – locate the requested pictures

For each tool (i.e. scalpel, photorec and recoverjpeg):

- Use md5sum to create hashes of the pictures and locate the identical pictures.
- Visually locate the pictures of the sports car and the Land Rover, noting features that demonstrate it is the same car.

Construct a table comparing the performance (i.e. number of files recovered) for each tool. An example is given in the Appendix.

Step 8 – repeat the activity using one or more other tools

Research data carving or data recovery tools on the Internet. Conduct the activity using a selection of these tools and add them to the table comparing performance. If you run out of time in the tutorial/lab, you might want to do this at home.

Assessment (to be submitted prior to week 3 tutorial)

The assessment for this activity will be as follows (out of 2.5%):

- up to 1.5% = construct comparison table for scalpel, photorec and recoverjpeg;
- up to 0.5% = construct comparison table for 1 x other tool;
- up to 0.5% = construct comparison table for multiple other tools.

The assessment for this week's activity is a comparison table to be submitted online using WebCMS.

Appendix – example comparison table

Tool	Photos on test image	Photos successfully recovered		Unusable files recovered (false positives)	
		Number	%	Number	%
Scalpel (for each tool, note down the switches used)					
Photorec					
Recoverjpeg					