

Lab: File Analysis

A Using findstr on a disk

With **findstr** program can use simple regular expressions to find strings within files. First start up your virtual machine, and open a command window. Next go into the **c:\forensics** folder, and run the command:

```
findstr /N /i /s "[a-zA-Z0-9._%+-].@[a-zA-Z0-9._%+-]" *.html
```

Outline four email addresses you have found:

Using **findstr /i /s "hello"**, find the **text files** which have the word "hello" in them:

Now find the documents with "goodbye" in them:

B Examining Files from Live System

Open **Autopsy**, and create a new a **New Case**. Next select:

Select source type of add: **Logical Files**

Now add the folder **c:\forensics**

Now wait for Autopsy to archive. Once complete, from Views-> File Types, determine the number of:

Images:	Videos:	Archives:
HTML:	Office:	PDF:
Plain text:	Rich Text:	Executable:

Outline the magic numbers used for the image, video, archive and PDF files:

Now, using Keyword Search with a Regular Expression. Find all the email addresses, using:

```
[a-zA-Z0-9._%+-]+@[a-zA-Z0-9._%+-]
```

Outline four of the email addresses:

Now try:

```
[a-z0-9%+_-]+(?:\\. [a-z0-9%+_-]+)*@(?:[a-z0-9](?:[a-z0-9-]*[a-z0-9])?\\.)+[a-z]{2,4}
```

Outline four of the email addresses:

Now find domain names in the files with:

```
[a-zA-Z0-9\\-\\.]+\\. (com|org|net|mil|edu|COM|ORG|NET|MIL|EDU|UK)
```

Outline four domains contained on the image:

C Examining files from disk archives

You should find **nps-2010-emails.E01** on the top level of the c: drive.

Using OSFMount, now mount the EnCase drive as an E: drive and examine the contents (select Auto for the disk type). Outline a few of the files contained:

With Autopsy, open up a new case, and investigate it (using . Once complete, from Views-> File Types, determine the number of:

Images:	Videos:	Archives:
HTML:	Office:	PDF:
Plain text:	Rich Text:	Executable:

Outline four email addresses in the disk image and the documents that they are contained in:

Now investigate nps-2013-canon1.E01.

What are the contents of the disk:

Which camera was used to take the photograph(s):

Extract all the images of your disk, and view them. What are they an image of:

D Examining the Master Boot Record

Demo: <http://youtu.be/4n8WvNFyjuo>

From your desktop, download and extract the following file:

<https://dl.dropboxusercontent.com/u/40355863/nps-2009-canon2-gen1.zip>

With WinHex, now examine the file.

At which byte number is 55 AA:

Using <http://asecuritysite.com/forensics/mbr>

Determine the details of the partitions:

E Extracting images from partitions

Download the following file:

<https://dl.dropboxusercontent.com/u/40355863/nps-2009-canon2-gen1.zip>

The image is a DOS file system type.

Open Autopsy, and determine the files on the disk.

Which file(s) have been deleted:

Which camera has been used:

Now we will use Sleuthkit to examine the disk.

First examine the command line options for the partition viewer (mmls). Replace **OPTION** with the required value (use **mmls -t** list to see options):

```
> mmls -t OPTION nps-2009-canon2-gen1.raw
```

What is the option used:

What is the size of the sectors (in bytes):

Outline the start, end and length of the sectors for each partition:

What is the first sector for the FAT 16 partition.

Now we will view the i-Nodes of the FAT-16 partition using the ils command. Use the help option to determine the i-Nodes

```
> ils -o START -f OPTION -i raw nps-2009-canon2-gen1.raw
```

Now outline the i-Nodes present.

Now use **istat** to list the details of the nodes:

What is the details of i-Node 2:

What is the details of i-Node 3:

What is the details of i-Node 4:

What are the details of i-Node 1029:

What are the details of i-Node 1030:

Now we will examine the file names on the disk with **fls**:

```
> fls -o 51 -f fat16 -i raw -r nps-2009-canon2-gen1.raw
```

Outline the volume label and the directories in the disk image and some of the files on it:

Next we'll examine the machine ready format for the activity on the file with:

```
> fls -o 51 -f fat16 -i raw -m / -r nps-2009-canon2-gen1.raw > bodyfile.txt
```

Examine this file. What can you determine from it:

You can then parse this into a CSV file with (if you are using Windows, download and install Perl and add the command Perl at the start of the command):

```
> mactime.pl -b bodyfile.txt -d > macout.csv
```

Examine this file. What can you determine from it:

Now let's extract the deleted image (replace STARTSECTOR with the starting sector of the first deleted image):

```
> icat -o START nps-2009-canon2-gen1.raw STARTSECTOR > img_0001.jpg
```

Go ahead and undelete the first 10 images. What do they contain:

F Extracting images

Now download the following file and repeat the procedure above, and extract all the content from the image:

<https://dl.dropboxusercontent.com/u/40355863/nps-2013-canon1.zip>

Document your results here for the contents:

G File Carving

Determine the magic file number for the following file types
(<http://www.asecuritysite.com/forensics/magic>):

JPEG:

GIF:

DOCX:

PDF:

Photoshop:

PK Zip:

RAR:

Postscript file:

Go into the c:\scalpel folder, and examine the scalpel.conf file. What is the start and end identifiers used to identify GIF, PDF and JPEG files.

JPEG:

GIF:

PDF:

Now download the following dd image of a disk:

<https://dl.dropboxusercontent.com/u/40355863/11-carve-fat.zip>

Using WinHex, examine the raw image. Can you spot any file types on the disk:

Now run Scalpel, and determine the following:

Which files are contained on the disk image?

Sample a few different file types. What do they contain:

Are there any errors in the file extract?

Now analyse:

<https://dl.dropboxusercontent.com/u/40355863/12-carve-ext2.rar>

Using WinHex, examine the raw image. Can you spot any file types on the disk:

Now run Scalpel, and determine the following:

Which files are contained on the disk image?

Sample a few different file types. What do they contain:

Are there any errors in the file extract?

Why might errors occur in the extract?