Hard Drive Analysis

Cyber Discovery 2.0

Investigative Session Day 2

Hard Drive Analysis

- Hard drive investigation or hard drive analysis is one aspect of a larger field of work called digital forensics
- Digital forensics is forensics applied to information stored or transported on digital devices
  - These include computers, cell phones, MP3 players, etc

Three Phases

- Digital forensics has three main phases
  - System preservation
  - Evidence searching
    - Also called evidence recognition
  - Event reconstruction

System Preservation

- System preservation is just as it sounds, we are preserving the system
  - Reduce or limit the amount of evidence that may be overwritten
  - We make a copy or an image of the storage media of the digital device (i.e. hard drive)
    - This image is an exact bit-by-bit copy of the original data
    - A special device called a write blocker is used
      - This ensures that the original data is not disturbed

System Preservation

- This raises a question.
- Why can't we just copy and paste?
- When you access a file, as in copying it, the operating system takes note of that and modifies the metadata (data about data) for that file

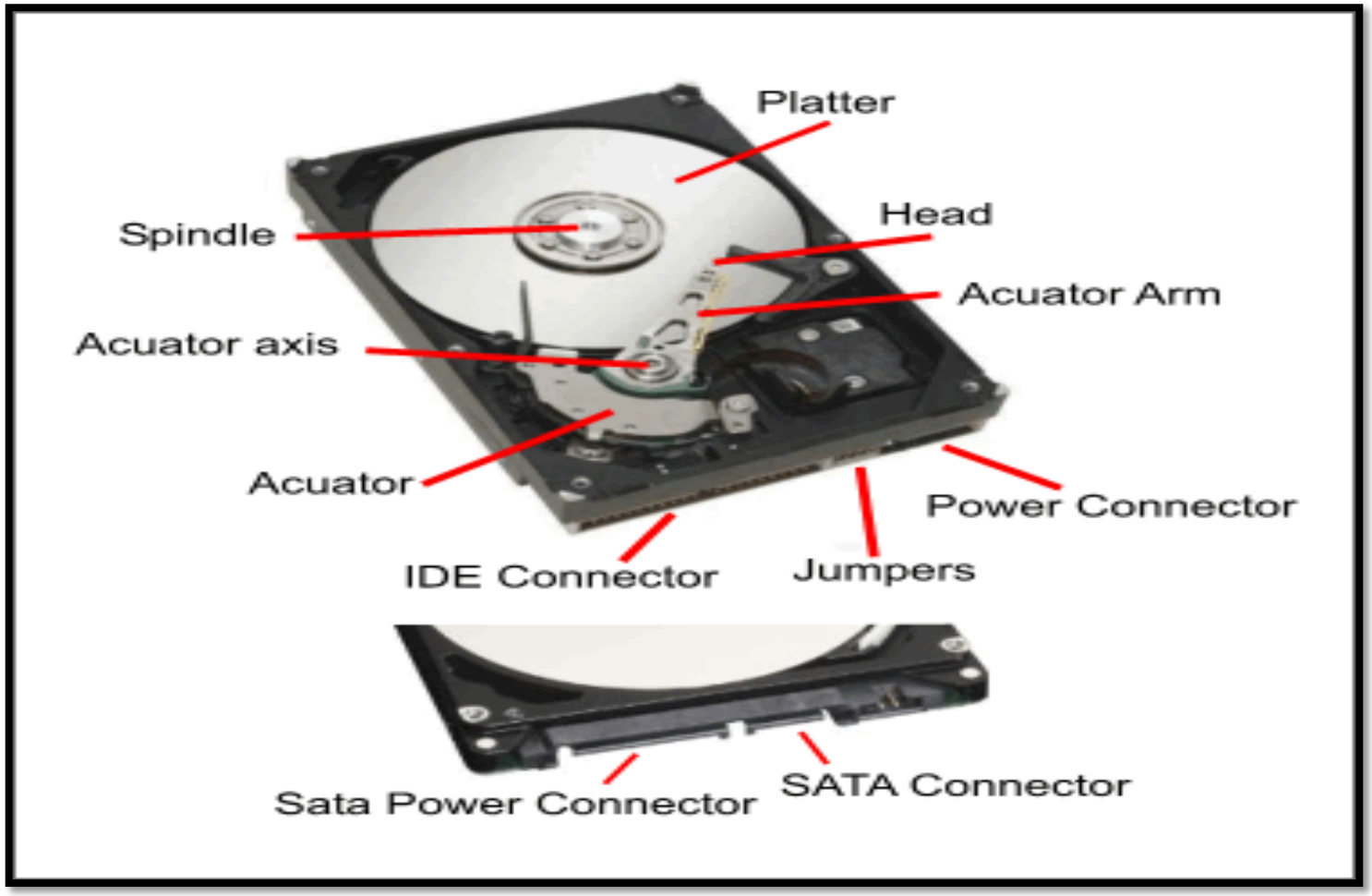
Evidence Recognition and Event Reconstruction

- Evidence recognition and event reconstruction are cyclic in nature
  - Like putting a puzzle together
  - First you have to find the correct pieces in a sea of puzzle pieces

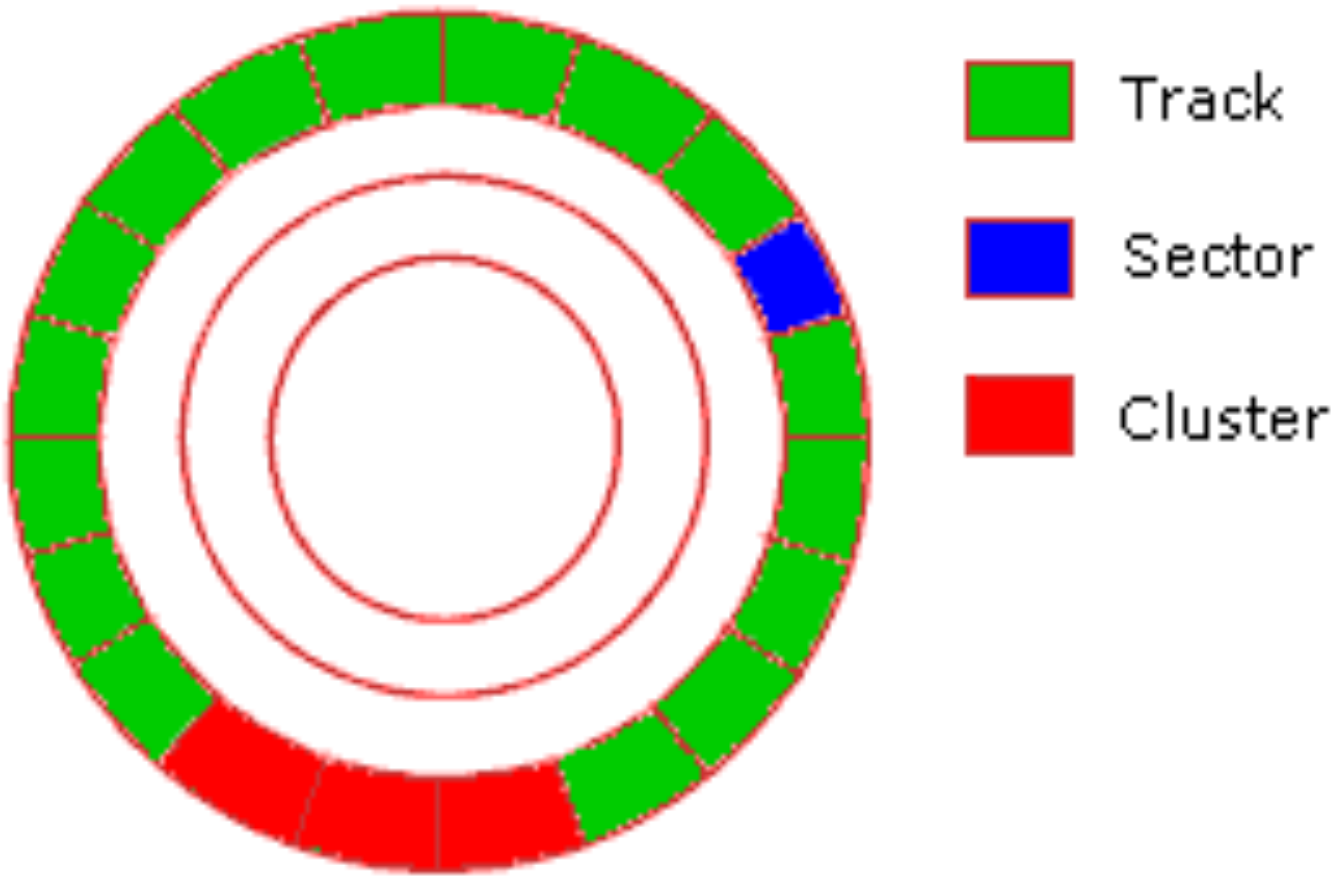
Hard Drives

- How are files stored on a hard drive?
  - Physical make-up of a hard drive
    - Disk has several platters in it
      - The platters are where the information is written
      - Platters are divided up into tracks and further into sectors
        - » Sectors are usually 512 bytes in size
    - Combine several sectors together and you get a cluster
      - Cluster is the minimum file allocation unit

Hard Drive


Platter
Spindle
Head
Acuator Arm
Acuator axis
Acuator
Power Connector
IDE Connector
Jumpers
Sata Power Connector
SATA Connector

Hard Drive



Hard Drive

- How are files stored on a hard drive?
  - Now let's discuss how an operating system, like Windows, handles files
    - When you create a file and save it to your hard drive
      - Windows finds enough clusters to store the file and writes it
      - Windows also creates an entry in a lookup table
        - » Called the File Allocation Table or Master File Table
          - Depending on the version of Windows
        - » This lookup table contains information about your file
          - This is known as metadata
            - Name, size, cluster location, etc

- Tying this back in with ‘why we can’t just copy and paste’
  - We could miss valuable information

Hands-on

- Let's take a look at the files listed in a given disk image
- We will be using tools within a toolset called SluethKit

List Files and Directories

cyber@cyber-laptop: ~/Desktop/cd2/wednesday

File Edit View Terminal Help

```
cyber@cyber-laptop:~/Desktop/cd2/wednesday$ filelist


      File List Tool

Please specify the image file:
hdimage
Save output to file? [y/n]
n
r/r 3:  PAGEFILE.SYS
d/d 4:  WINDOWS
+ d/d 1310853:  system32
++ d/d 1310981: config
+++ r/r * 1311109:      _YS$$$$$.DEL
+++ r/r * 1311110:      _OF$$$$$.DEL
+++ r/r * 1311111:      _EF$$$$$.DEL
+++ r/r 1311112:        userdiff
+++ r/r 1311113:        system.LOG
+++ r/r 1311114:        software.LOG
+++ r/r 1311115:        default.LOG
+++ r/r 1311116:        userdiff.LOG
+++ r/r * 1311118:      TempKey
+++ r/r 1311120:        TempKey.LOG
+++ r/r * 1311122:      TempKey
```

List Files and Directories

cyber@cyber-laptop: ~/Desktop/cd2/wednesday

File Edit View Terminal Help

```
cyber@cyber-laptop:~/Desktop/cd2/wednesday$ filelist


      File List Tool

Please specify the image file:
hdimage
Save output to file? [y/n]
y
Please specify the name of the file to be created:
listing.txt
cyber@cyber-laptop:~/Desktop/cd2/wednesday$
```

Hard Drive Analysis

- What information can we gain about a file in our image?

- Example:
  - Let's look for a picture named `bulldog2.jpg`
  - Searching for `bulldog2.jpg` in our `listing.txt` we find the following line

```
++++ r/r 50467467: bulldog2.jpg
```

  - The + signs provide for the depth in the directory structure
  - The `r/r` provides the file type
    - `r/r` means that this is a file
    - `d/d` means that this is a directory
  - The number is the metadata address or `inode` number

Search Listing

listing.txt (~/Desktop/cd2/wednesday) - gedit

File Edit View Search Tools Documents Help

Open Save Undo

listing.txt

```
+++ r/r 15163528:        bulldog2.lnk
+++ r/r 15163531:        My Pictures.lnk
++ d/d 14753302:         PrintHood
++ d/d 14753304:         My Documents
+++ r/r 15163781:        desktop.ini
+++ d/d 15163783:        My Pictures
++++ r/r 50467462:       Desktop.ini
++++ r/r 50467465:       Sample Pictures.lnk
++++ r/r * 50467466:     _ulldog2.jpg
++++ r/r 50467467:       bulldog2.jpg
+++ d/d 15163785:        My Music
++++ r/r 50467846:       Desktop.ini
++++ r/r 50467849:       Sample Music.lnk
+++ r/r * 15163786:      _MP4352$.TMP
++ d/d 14753306:         NetHood
++ d/d 14753308:         Favorites
+++ r/r * 15164037:      _MP4352$.TMP
+++ d/d 15164039:        Links
++++ r/r 14827143:       Windows Marketplace.url
++++ r/r 14827146:       Customize Links.url
```

Plain Text | Tab Width: 8 | Ln 10467, Col 25 | INS

Examine the Metadata

cyber@cyber-laptop: ~/Desktop/cd2/wednesday

File Edit View Terminal Help

```
cyber@cyber-laptop:~/Desktop/cd2/wednesday$ inodestats


      Inode Stats Tool

Please specify the image file:
hdimage
Please specify the inode number:
50467467
Directory Entry: 50467467
Allocated
File Attributes: File, Archive
Size: 189372
Name: bulldog2.jpg

Directory Entry Times:
Written:        Fri Jun 15 00:24:50 2012
Accessed:       Fri Jun 15 00:00:00 2012
Created:        Fri Jun 15 00:25:16 2012

Sectors:
3224824 3224825 3224826 3224827 3224828 3224829 3224830 3224831
3224832 3224833 3224834 3224835 3224836 3224837 3224838 3224839
3224840 3224841 3224842 3224843 3224844 3224845 3224846 3224847
```

Extract File

cyber@cyber-laptop: ~/Desktop/cd2/wednesday

File Edit View Terminal Help

```
cyber@cyber-laptop:~/Desktop/cd2/wednesday$ fileextract


      File Extraction Tool

Please specify the image file:
hdimage
Please specify the inode of the file to be extracted:
50467467
Save output to file? [y/n]
y
Please specify the name of the file to be created (new extracted file):
bulldog2.jpg
cyber@cyber-laptop:~/Desktop/cd2/wednesday$
```

Hard Drive Analysis

- Now what about recovering a deleted file
- In this format deleted files are denoted by an '*' and sometimes the first character of the file name '_'

- Following the same process as above
  - Search for `_ulldog.jpg` in `listing.txt`
  - We find the following entry

```
+++ r/r * 15164165:    _ulldog.jpg
```

Deleted Files

listing.txt (~/Desktop/cd2/wednesday) - gedit

File Edit View Search Tools Documents Help

Open Save Undo

listing.txt

```
++++ r/r 14827143:      Windows Marketplace.url
++++ r/r 14827146:      Customize Links.url
++++ r/r 14827149:      Free Hotmail.url
++++ r/r 14827151:      Windows.url
++++ r/r 14827154:      Windows Media.url
+++ r/r 15164041:       Desktop.ini
+++ r/r 15164043:       MSN.com.url
+++ r/r 15164046:       Radio Station Guide.url
++ d/d 14753310:        Desktop
+++ r/r * 15164165:     _ulldog.jpg
+++ r/r * 15164166:     _ulldog.jpg
++ d/d 14753312:        Cookies
+++ r/r 15164293:       index.dat
+++ r/r 15164297:       raymond martin@microsoft[1].txt
+++ r/r 15164301:       raymond martin@blogger[2].txt
+++ r/r 15164307:       raymond martin@www-blogger-
opensocial.googleusercontent[1].txt
+++ r/r 15164311:       raymond martin@www.msn[1].txt
+++ r/r 15164314:       raymond martin@msn[2].txt
+++ r/r 15164318:       raymond martin@adnxs[1].txt
```

Plain Text | Tab Width: 8 | Ln 10485, Col 25 | INS

Deleted Files

```
cyber@cyber-laptop: ~/Desktop/cd2/wednesday
File  Edit  View  Terminal  Help
cyber@cyber-laptop:~/Desktop/cd2/wednesday$ inodestats


      Inode Stats Tool

Please specify the image file:
hdimage
Please specify the inode number:
15164165
Directory Entry: 15164165
Not Allocated
File Attributes: File, Archive
Size: 0
Name: _ulldog.jpg

Directory Entry Times:
Written:        Fri Jun 15 00:23:08 2012
Accessed:       Fri Jun 15 00:00:00 2012
Created:        Fri Jun 15 00:23:07 2012

Sectors:
12264

Press [Enter] to exit the tool...
```

Deleted Files

listing.txt (~/Desktop/cd2/wednesday) - gedit

File Edit View Search Tools Documents Help

Open Save Undo

listing.txt

```
+++ r/r * 28884870:     _ET615.tmp
+++ r/r 28884873:       Moon flower.jpg
+++ r/r * 28884874:     _ET616.tmp
+++ r/r * 28884875:     _ET616.tmp
+++ r/r 28884878:       Red moon desert.jpg
+++ r/r * 28884879:     _ET617.tmp
+++ r/r * 28884880:     _ET617.tmp
+++ r/r 28884883:       Vortec space.jpg
+++ r/r * 28884884:     _ET618.tmp
+++ r/r * 28884885:     _ET618.tmp
+++ r/r * 28884887:     Ascent.jpg
+++ r/r * 28884888:     _ET619.tmp
+++ r/r * 28884889:     _ET619.tmp
+++ r/r 28884891:       Autumn.jpg
+++ r/r * 28884892:     _ET61A.tmp
+++ r/r * 28884893:     _ET61A.tmp
+++ r/r 28884895:       Friend.jpg
+++ r/r * 28884896:     _ET61B.tmp
+++ r/r * 28884897:     _ET61B.tmp
+++ r/r 28884899:       Home.jpg
```

Plain Text | Tab Width: 8 | Ln 6770, Col 25 | INS

Deleted Files

cyber@cyber-laptop: ~/Desktop/cd2/wednesday

File Edit View Terminal Help

```
cyber@cyber-laptop:~/Desktop/cd2/wednesday$ inodestats


      Inode Stats Tool

Please specify the image file:
hdimage
Please specify the inode number:
28884887
Directory Entry: 28884887
Not Allocated
File Attributes: File, Archive
Size: 63244
Name: _SCENT.JPG

Directory Entry Times:
Written:        Mon Apr 14 07:00:00 2008
Accessed:       Sun Jul 22 00:00:00 2012
Created:        Thu Jun 14 20:45:13 2012

Sectors:
1818032 1818033 1818034 1818035 1818036 1818037 1818038 1818039
1818040 1818041 1818042 1818043 1818044 1818045 1818046 1818047
1818048 1818049 1818050 1818051 1818052 1818053 1818054 1818055
```

Extract Deleted Files

cyber@cyber-laptop: ~/Desktop/cd2/wednesday

File Edit View Terminal Help

```
cyber@cyber-laptop:~/Desktop/cd2/wednesday$ fileextract


      File Extraction Tool

Please specify the image file:
hdimage
Please specify the inode of the file to be extracted:
28884887
Save output to file? [y/n]
y
Please specify the name of the file to be created (new extracted file):
Ascent.jpg
cyber@cyber-laptop:~/Desktop/cd2/wednesday$
```

Browser History

- Let's look at Web Browser History
- Where is the browser history stored
  - Internet Explorer – `index.dat`
  - Firefox – `history.dat` (older versions) or `places.sqlite` (version 3 and above)
  - Chrome – `history.sqlite`
- Internet Explorer
  - Lots of `index.dat` files
  - Look for ones associated with a `MSHist`*`date`* directory
  - Example:

```
+++++ d/d 15160972:  MSHist012012071720120718
++++++ r/r 50764421: index.dat
```

Browser History

listing.txt (~/Desktop/cd2/wednesday) - gedit

File Edit View Search Tools Documents Help

Open Save Undo

listing.txt

```
++++ d/d * 15160828:    _R_E6540.tmp
++++ d/d * 15160831:    scoped_dir2537
++++ r/r * 15160832:    _.tmp
++++ r/r * 15160833:    _.tmp
++++ r/r * 15160834:    _.tmp
+++ d/d 15160584:       History
++++ d/d 15160838:      History.IE5
+++++ r/r 15160965:     desktop.ini
+++++ r/r 15160966:     index.dat
+++++ d/d * 15160969:   MSHist012012061520120616
+++++ d/d 15160972:     MSHist012012071720120718
++++++ r/r 50764421:    index.dat
+++++ d/d 15160975:     MSHist012012072220120723
++++++ r/r 75720837:    index.dat
++++ r/r * 15160839:    _esktop.ini
++++ r/r 15160840:      desktop.ini
+++ d/d 15160587:       Temporary Internet Files
++++ d/d 15161094:      Content.IE5
+++++ d/d 15161221:     EL4BMP2R
++++++ r/r 15161349:    desktop.ini
```

Plain Text | Tab Width: 8 | Ln 9215, Col 25 | INS

Browser History

cyber@cyber-laptop: ~/Desktop/cd2/wednesday

File Edit View Terminal Help

```
cyber@cyber-laptop:~/Desktop/cd2/wednesday$ fileextract


      File Extraction Tool

Please specify the image file:
hdimage
Please specify the inode of the file to be extracted:
50764421
Save output to file? [y/n]
y
Please specify the name of the file to be created (new extracted file):
index.dat
cyber@cyber-laptop:~/Desktop/cd2/wednesday$
```

Browser History

cyber@cyber-laptop: ~/Desktop/cd2/wednesday

File Edit View Terminal Help

```
cyber@cyber-laptop:~/Desktop/cd2/wednesday$ pascotool


      PASCO MS IE cache extraction tool

Please specify the history file:
index.dat
Please specify the resulting .csv filename to store the history:
index.csv
cyber@cyber-laptop:~/Desktop/cd2/wednesday$
```

Browser History

index.csv - OpenOffice.org Calc

File Edit View Insert Format Tools Data Window Help

Liberation Sans 10

A1 History

	A	B	
1	History	File:	index.dat
2			
3	TYPEURLMODIFIED	TIMEACCESS	TIMEFILENAMEDIRECTORYHTTP
4	URL:2012071720120718:	Raymond	Martin@http://www.msn.com 07/17/2012
5	URL:2012071720120718:	Raymond	Martin@:Host:
6	URL:2012071720120718:	Raymond	Martin@http://www.irongeek.com/i.php?page=security/windows-forensics-registry-and-file-system-spots 07/17/2012
7	URL:2012071720120718:	Raymond	Martin@:Host:
8	URL:2012071720120718:	Raymond	Martin@http://www.google.com/search?hl=en&source=hp&q=how+to+hide+files+on+windows&gbv=2&og=how+to+hide+fil
9	URL:2012071720120718:	Raymond	Martin@http://www.online-tech-tips.com/computer-tips/how-to-hide-files-and-folders-in-windows-xp-the-easy-way 07/17/201
10	URL:2012071720120718:	Raymond	Martin@:Host:
11	URL:2012071720120718:	Raymond	Martin@http://www.microsoft.com/en-us/default.aspx 07/17/2012
12	URL:2012071720120718:	Raymond	Martin@:Host:
13	URL:2012071720120718:	Raymond	Martin@http://www.apple.com 07/17/2012
14	URL:2012071720120718:	Raymond	Martin@:Host:
15	URL:2012071720120718:	Raymond	Martin@http://www.apple.com/iphone 07/17/2012
16	URL:2012071720120718:	Raymond	Martin@http://www.forensicswiki.org/wiki/Internet_Explorer_History_File_Format 07/17/2012
17	URL:2012071720120718:	Raymond	Martin@:Host:
18	URL:2012071720120718:	Raymond	Martin@http://www.google.com 07/17/2012
19	URL:2012071720120718:	Raymond	Martin@http://www.google.com/search?hl=en&source=hp&q=internet+explorer+history+files+location&gbv=2&og=internet+
20	URL:2012071720120718:	Raymond	Martin@:Host:
21			
22			
23			
24			
25			
26			
27			
28			

Sheet1

Sheet 1 / 1 | Default | STD | Sum=0 | 100%

Hard Drive Analysis

- Now it's your turn
  - See if you can find the following files and see if you can extract them
  - Or you can begin your own investigation of the sample disk image and see what you can find

```
clock.avi
ding.wav
triangle.wav
ratchet.wav
Dogs.doc
```

Investigating a Crime Scene

- Investigating a scene
  - Be very observant of the surroundings
  - Listen to see if the computer is on
    - If the monitor is on, note what is on the screen
    - Look for indications of suspect trying to cover up activities
    - Look for a web cam and see if active
    - Look for evidence of ongoing communication
      - Look for wireless access points
  - Look around and identify all digital devices

Investigating a Crime Scene

- Investigating a scene
  - Take pictures of how everything is set up
  - Look at papers on desk
    - Is there anything there that may provide any clues?
      - Passwords written on post-it notes
        - » These could be under the keyboard or on the monitor
      - Notepads with information written on them
  - Document everything before anything is touched
  - Roam around the room look at everything from multiple angles
    - You never what may be hidden on first glance