MP5 Forensics

Leslie Hwang
University of Illinois
CS461 / ECE422 Spring 2016

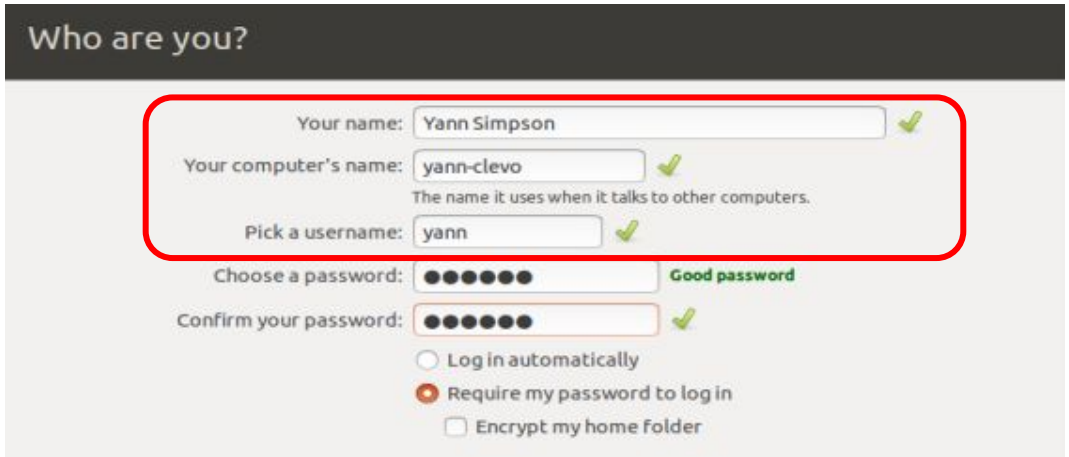
Outline

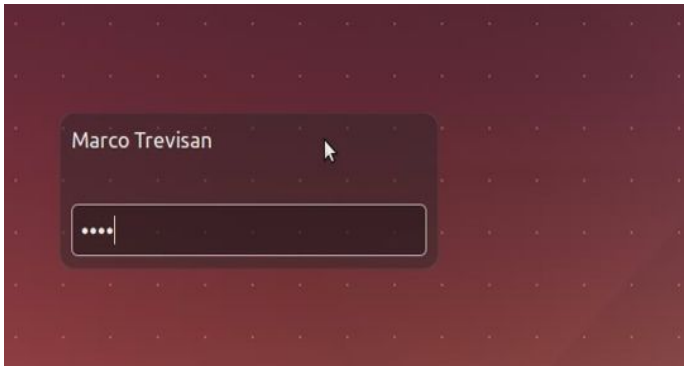
- Forensic analysis
- Unix file system
- Tool setup and demo
- File metadata and GPS coordinate conversion
- Password cracking
- File recovery

Forensic Analysis

- ***Live*** Analysis
  - Investigator examines “**running**” copy of the target
  - User account password will be required to log in
  - MP tool: VirtualBox
- ***Dead*** Analysis
  - Investigator examines data artifacts from target “***without* running**” the system
  - User account password is not required for analysis
  - MP tool: Autopsy

Username vs. Display name?





<Login page examples>

Unix File System

- Linux Ubuntu
  - **Ext2**
    - Default filesystem in several Linux distributions (e.g. Debian and Red Hat Linux)
    - Every file or directory is represented by an inode, "index node". The inode includes data about the size, permission, ownership, and location on disk of the file or directory.
    - Marks inode blocks as unused in the block bitmaps
    - When file is deleted, it marks the inode as "deleted" and leaves the block pointers alone
  - **Ext3**
    - Journaled file system, the default file system for many popular Linux distributions.
    - Journaling improves reliability and eliminates the need to check the file system after an unclean shutdown
    - To safely resume an unlink after a crash, it zeros out the block pointers in the inode
  - **Ext4**
    - Journaling file system for Linux
- Windows: FAT32 and NTFS

Unix/Linux System Administration

- Reference: Unix System Administration Handbook (https://subversion.ews.illinois.edu/svn/sp16-ece422/_shared/mp5)
  - Chapter 4: Access control and rootly powers
  - Chapter 11: Syslog and log files
  - Chapter 22: Security

Disk Partition

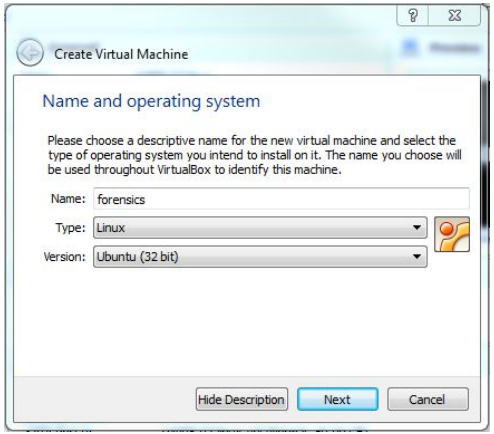
- Division of a computer hard disk
- Multiple partitions allows OS to manager information in each region separately.
- The disk stores the information about the partitions' locations and sizes in an area known as the partition table that the operating system reads before any other part of the disk.
- Each partition appears in the operating system as a distinct "logical" disk that uses part of the actual disk.
- https://en.wikipedia.org/wiki/Disk_partitioning

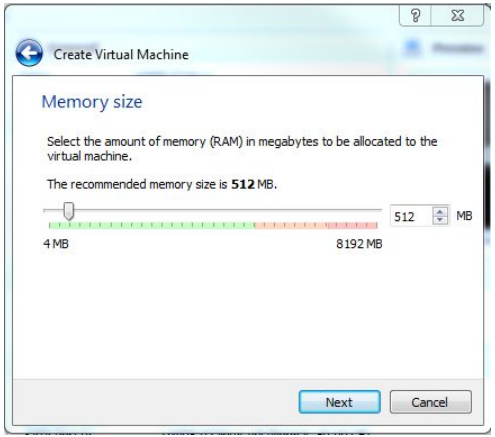
Live Analysis Setup

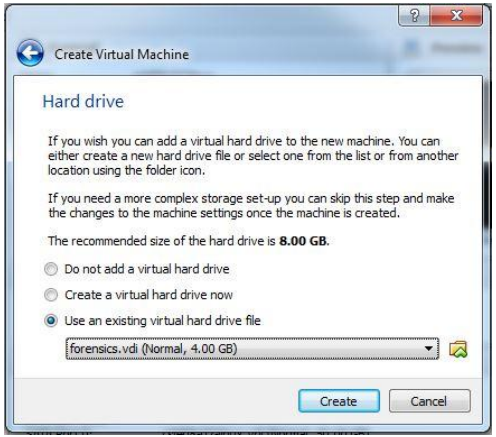
- Use your **own** machine
  - Decompressed disk image (.raw) file: >8GB ← Dead Analysis
  - VirtualBox disk image (.vdi) file: >3GB ← Live Analysis
  - EWS quota: 10GB
  - VirtualBox **not** supported on EWS
  - VirtualBox download link: https://www.virtualbox.org/wiki/Downloads
  - Convert raw to vdi

```
%VBoxManage convertdd forensics_sp16_victim.raw
forensics_sp16_victim.vdi -format VDI
```

Live Analysis: Windows OS VirtualBox Demo (1)





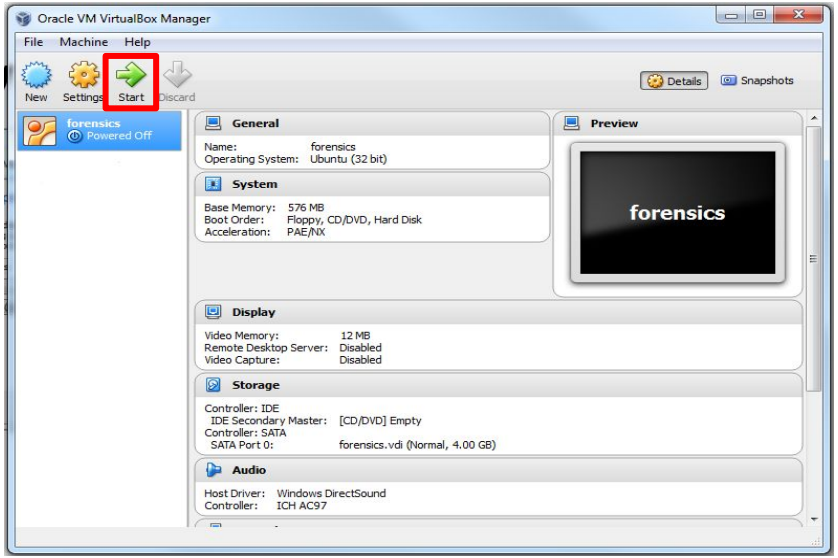


Step 1. Choose OS type

Step 2. Select memory size

Step 3. Browse existing .vdi file

Live Analysis: Windows OS VirtualBox Demo (2)



Step 4. Start the VB

Live Analysis: Troubleshooting

- VirtualBox: Convert to VDI
  - http://serverfault.com/questions/365423/how-to-run-vboxmanage-exe
  - Manual: https://www.virtualbox.org/manual/ch08.html
- Fail to load live VM
  - **READ the error message**
  - Press “ESC” button at the very beginning of boot
    (message will pop up when to use)

Dead Analysis Setup

- You MUST use your **own** machine
  - Autopsy installed on EWS Linux is the outdated version
- Tool Installation
  - The Sleuth Kit (TSK): http://www.sleuthkit.org/sleuthkit/download.php
  - Autopsy (version 3 or higher): http://www.sleuthkit.org/autopsy/
- Linux Autopsy tutorial: https://digital-forensics.sans.org/blog/2009/05/11/a-step-by-step-introduction-to-using-the-autopsy-forensic-browser/

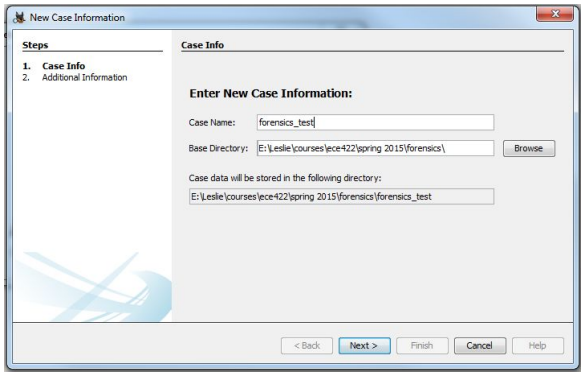
Dead Analysis: Autopsy

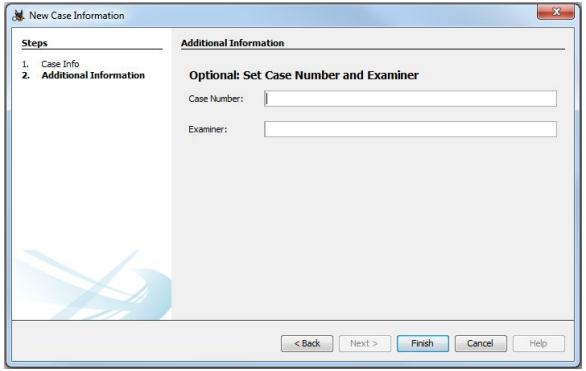
- Tips
  - Attacker mindset
  - Trace history
  - Examine ***system logs***
  - Check for ***deleted*** or ***encrypted*** files
  - Search for ***strings / keywords*** that may be relevant
  - File name, date and time, file extension, size, metadata … etc.
- References
  - http://www.sleuthkit.org/autopsy/help/general.html
  - http://www.sleuthkit.org/autopsy/v2/
- File recovery
  - http://sleuthkit.org/autopsy/docs/user-docs/3.1/photorec_carver_page.html

Dead Analysis: Autopsy

- Modified time vs. Changed time
  - **Accessed**: When the file data was last accessed. This time can be modified using the utimes() function.
  - **Modified**: When the file data was last modified. This time can be modified using the utimes() function.
  - **Changed**: When the file status (inode data) was last changed. This time can not be set using the utimes() function in UNIX (but it will be set when utimes() is used to modify other values).
  - http://www.sleuthkit.org/autopsy/help/file_mode.html
- Allocated file vs. Unallocated file
  - **Allocated**: Files that are seen when doing an '`ls`' or '`dir`' in a directory.
  - **Unallocated**: Files that have been deleted, but that TSK can still access. Files in this category include orphan files, which are files that no longer have a name, but whose metadata still exists. If a deleted file name points to an allocated metadata structure, then the name will say "realloc" next to it.

Dead Analysis: Windows OS Autopsy Demo (1)



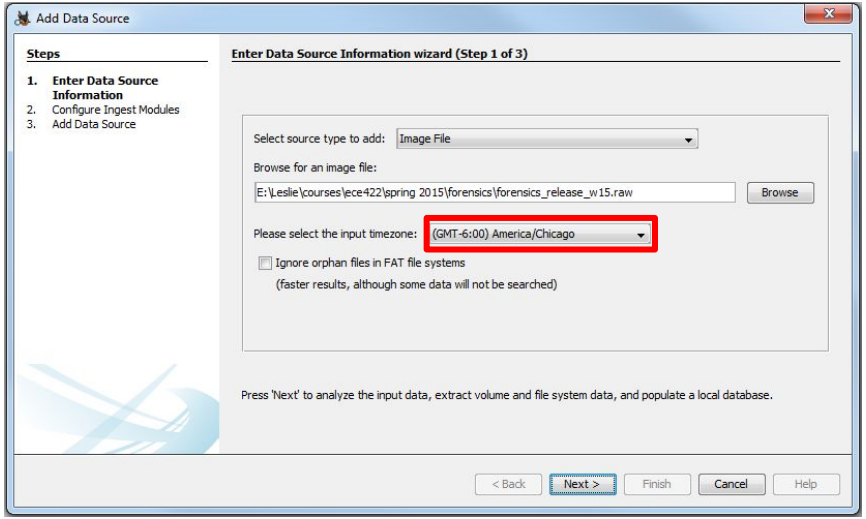


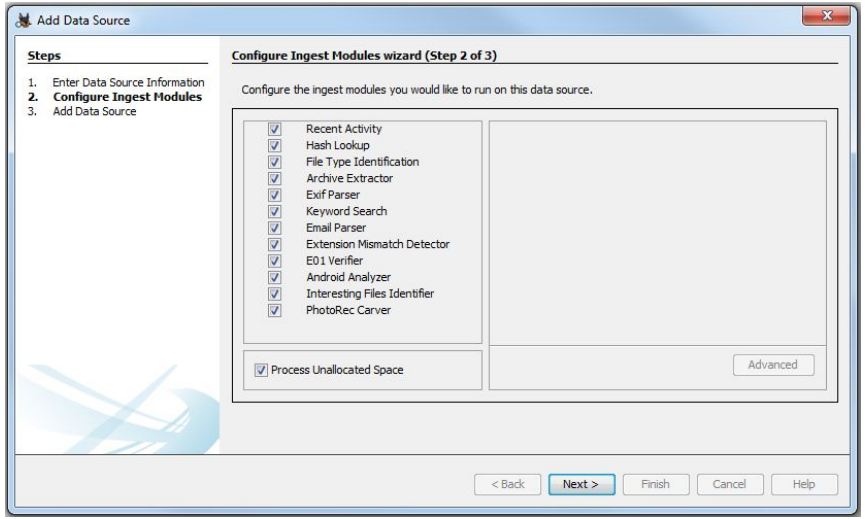
Step 1. Create new case

Step 2. Choose directory

Step 3. Optional: leave it blank

Dead Analysis: Windows OS Autopsy Demo (2)

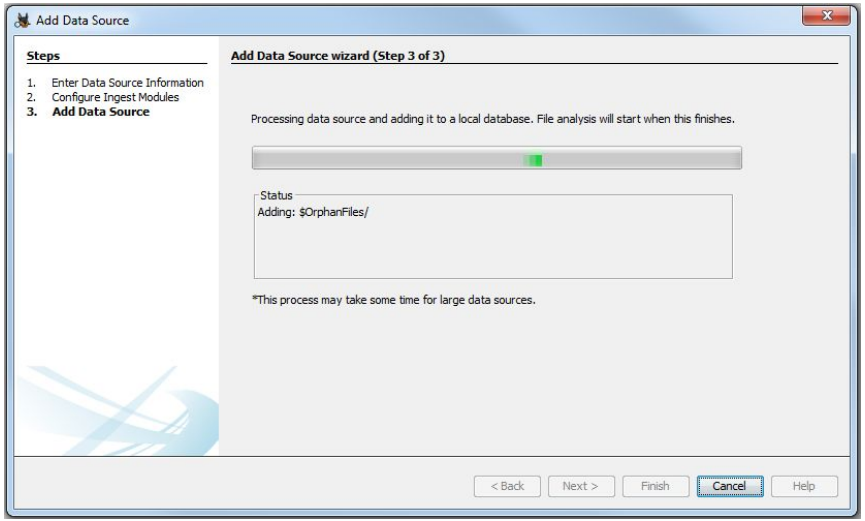


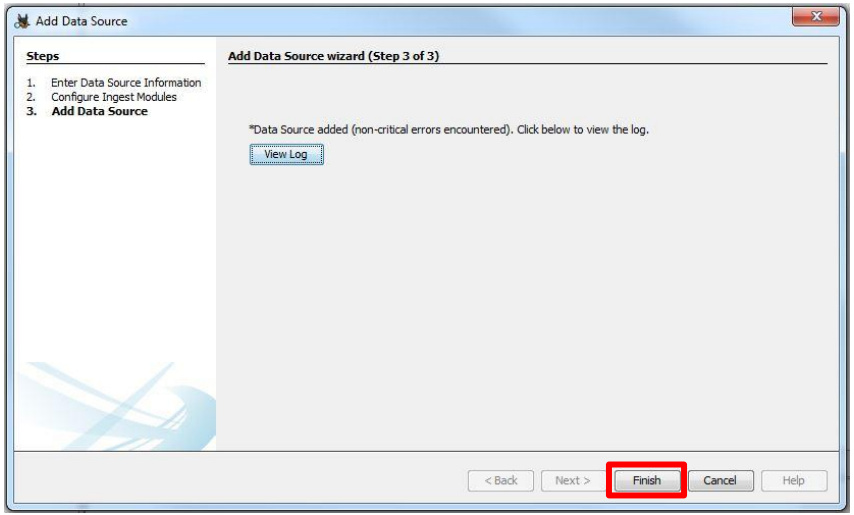


Step 4. Browse raw disk image

Step 5. Leave as default

Autopsy: Windows OS Demo (3)

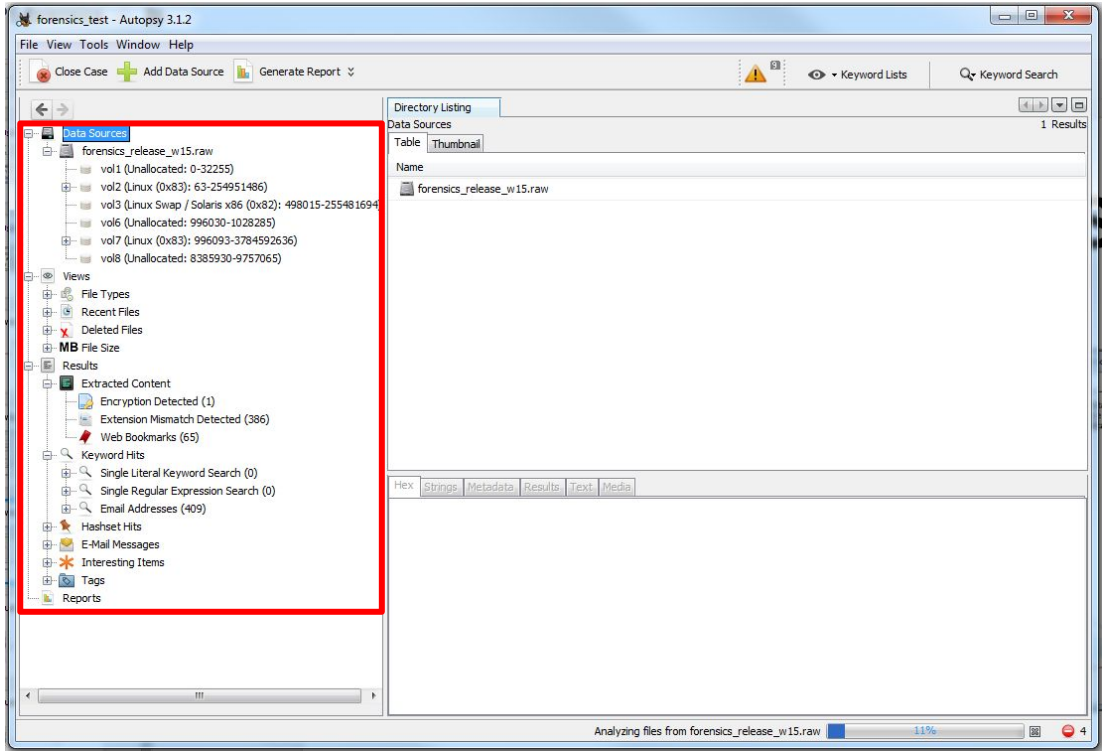




Step 6. Setup wizard

Step 7. Finish creating case

Autopsy: Windows OS Demo (4)



Step 8. Start investigation

File Metadata

- Metadata is “data about data”
- Two types
  - **Structural** metadata is data about the containers of data
  - **Descriptive** metadata uses individual instances of application data or the data content
- Used to describe digital data, describing the contents and context of data files increases their usefulness
- Facilitate in the discovery of relevant information, classified as resource discovery
- Helps organize electronic resources, provide digital identification, support archiving and preservation of the resource

Geotag Degree Conversion

- Decimal coordinate signs
  - Latitude: **North** → positive (+), **South** → negative (-)
  - Longitude: **East** → positive (+), **West** → negative (-)
- EXIF Tool
  - Obtain metadata from image file
  - Download link: http://owl.phy.queensu.ca/~phil/exiftool/
  - Manual: http://owl.phy.queensu.ca/~phil/exiftool/exiftool_pod.html
    - Decimal format: `exiftool -c "%.3f" [imagefile.jpg]`
  - Verify the location result on the map
- GPS coordinates converter
  - http://www.gps-coordinates.net/gps-coordinates-converter

http://www.gps-coordinates.net/gps-coordinates-converter

Address: New York, NY

Get GPS Coordinates

DD (decimal degrees)*

Latitude: 40.7127837

Longitude: -74.0059413

Get Address

DMS (degrees, minutes, secondes)*

Latitude: N S 40 ° 42 ' 46.021 "

Longitude: E W 74 ° 0 ' 21.388 "

* World Geodetic System 84 (WGS 84)

Password Cracking

- Use your **own** machine
  - Currently, EWS is not set up for this support
  - It is never a good idea to run cracking tools on public computer
- Tools
  - John the Ripper: UNIX password cracker
  - Hydra: Remote login password cracker (brute-force)
  - Fcrackzip: ZIP password cracker
  - PDFcrack: PDF password cracker

Password Cracking: Demo

- References
  - http://oldhome.schmorp.de/marc/fcrackzip.html
  - http://linuxers.org/article/how-crack-zip-file-passwords-linux-using-fcrackzip
- Options
  - -b: brute-force
  - -c: character-set (e.g. lower case, upper case, digits etc.)
  - -D: dictionary
  - -l: length
  - -p: initial password string
  - -u: unzips the file (this option doesn't work on Windows OS)
- Unix / Mac OS: fcrackzip demo

```
%./fcrackzip -b -c a -p aaaaaa -u filename.zip
```

6-character long: all alphabets

File Recovery

- Recover vs. Extract vs. Export?
- Photorec
  - Run photorec: photorec.exe diskimage.raw
  - Select Drive/Select partition/no partition (whole)
  - *(before pressing enter)* right arrow to file ops
  - Select file extensions to recover
  - Choose file system
  - Choose directory to save recovered files
  - Start searching
- Other tools: scalpel, extundelete (w/ kpartx), ext3grep and etc.
- References
  - http://www.cgsecurity.org/wiki/PhotoRec_Step_By_Step
  - http://www.bootmed.com/bootmed/tutorials-11/how-to-recover-deleted-files-with-photorec/
  - http://extundelete.sourceforge.net/