MP5 Forensics

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

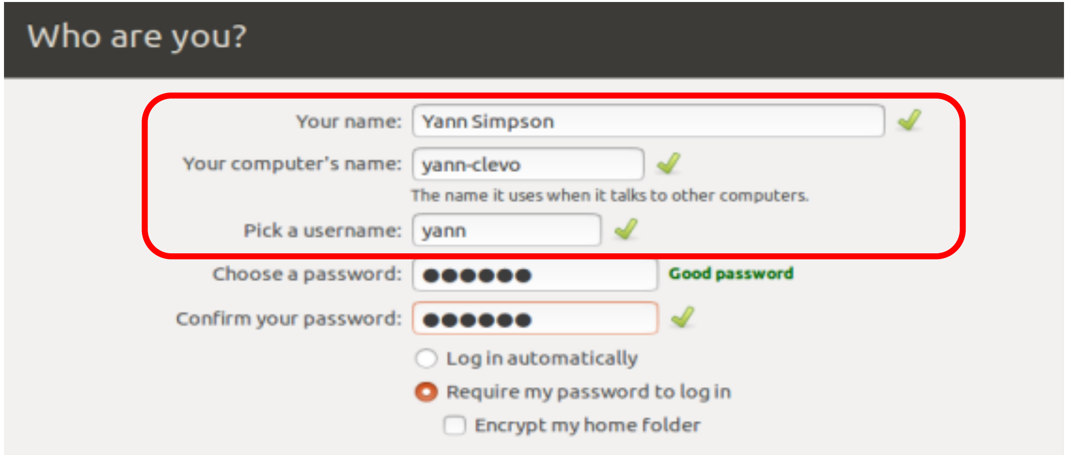
Dead Analysis

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?



Who are you?

Your name: Yann Simpson ✓

Your computer's name: yann-clevo ✓
The name it uses when it talks to other computers.

Pick a username: yann ✓

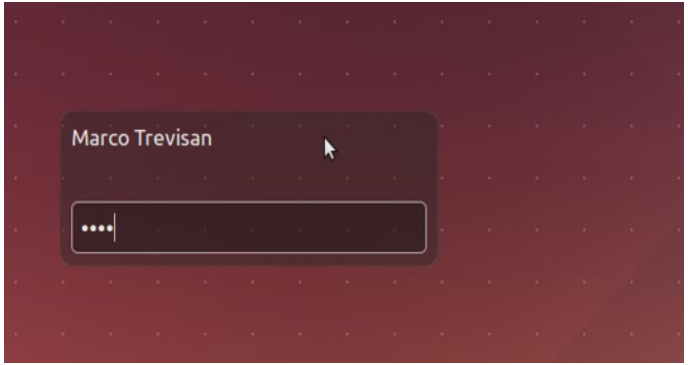
Choose a password: ●●●●●● Good password

Confirm your password: ●●●●●● ✓

○ Log in automatically

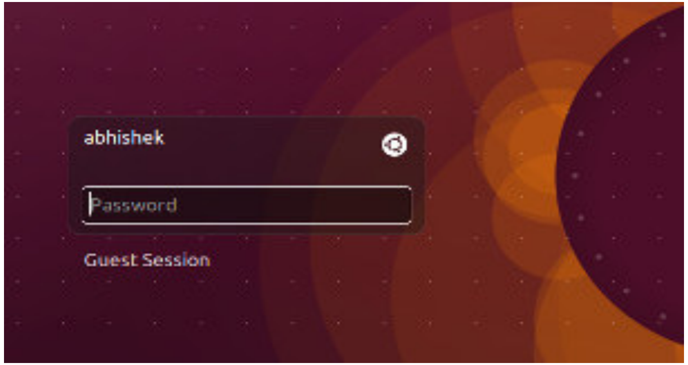
● Require my password to log in

□ Encrypt my home folder



Marco Trevisan

••••



abhishek

Password

Guest Session

<Login page examples>

Unix/Linux System Administration

Reference: Unix System Administration Handbook

(https://subversion.ews.illinois.edu/svn/fa16-ece422/_shared/mp5)

Chapter 4: Access control and rootly powers

Chapter 11: Syslog and log files

Chapter 22: Security

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

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

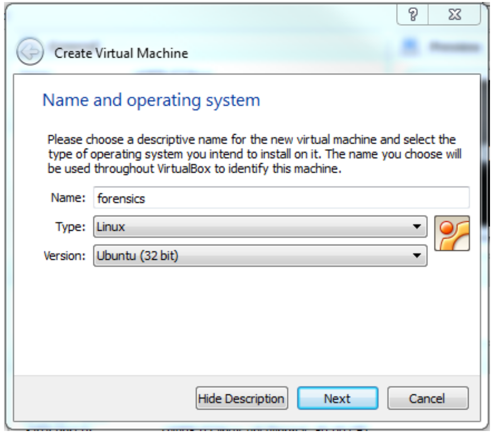
VirtualBox **not** supported on EWS

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)



Name and operating system

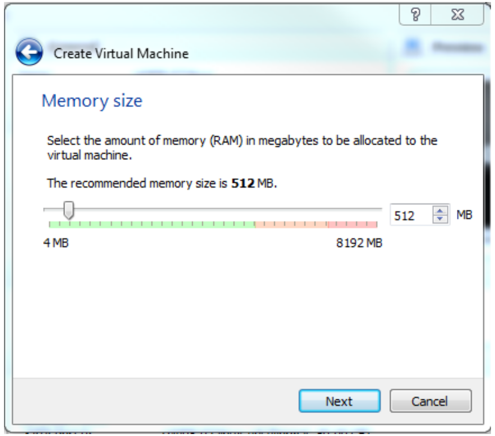
Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: forensics

Type: Linux

Version: Ubuntu (32 bit)

Step 1. Choose OS type



Memory size

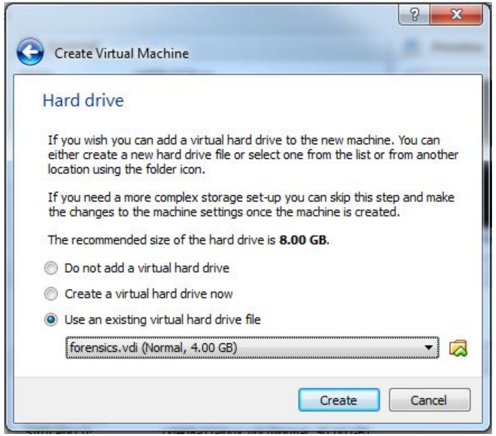
Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **512** MB.

512 MB

4 MB — 8192 MB

Step 2. Select memory size



Hard drive

If you wish you can add a virtual hard drive to the new machine. You can either create a new hard drive file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard drive is **8.00 GB**.

○ Do not add a virtual hard drive

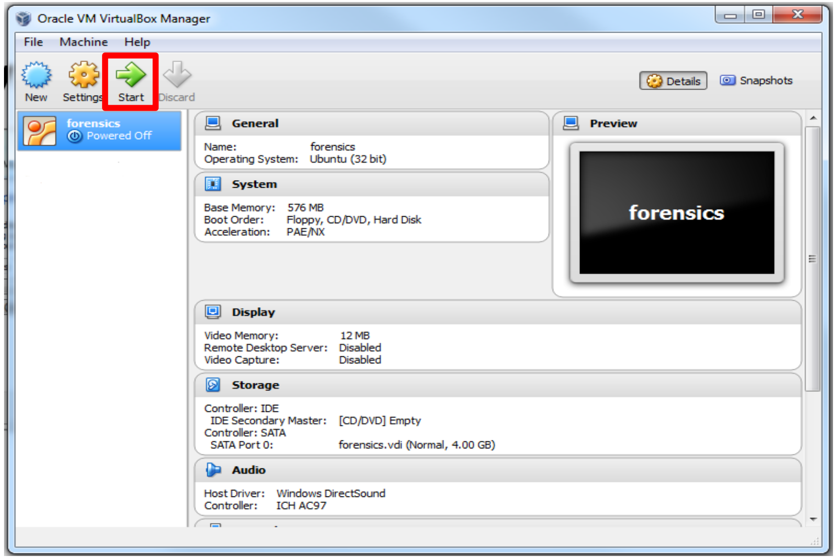
○ Create a virtual hard drive now

● Use an existing virtual hard drive file

forensics.vdi (Normal, 4.00 GB)

Step 3. Browse existing .vdi file

Live Analysis: Windows OS VirtualBox Demo (2)



General

Name: forensics
Operating System: Ubuntu (32 bit)

System

Base Memory: 576 MB
Boot Order: Floppy, CD/DVD, Hard Disk
Acceleration: PAE/NX

Display

Video Memory: 12 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage

Controller: IDE
IDE Secondary Master: [CD/DVD] Empty
Controller: SATA
SATA Port 0: forensics.vdi (Normal, 4.00 GB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Step 4. Start the VB

Dead Analysis Setup

You MUST use your **own** machine

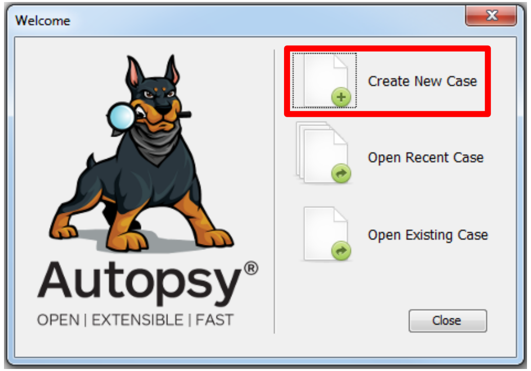
- Autopsy installed on EWS Linux is the outdated version

Tool Installation

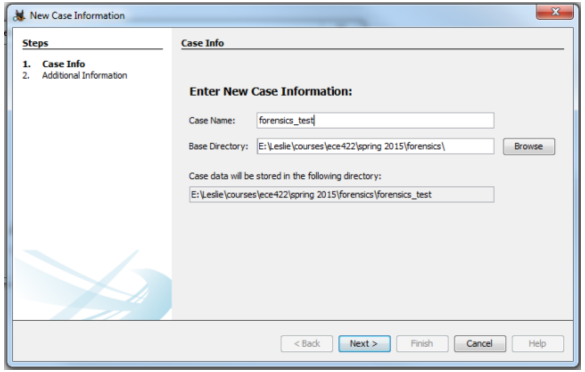
- The Sleuth Kit (TSK): http://www.sleuthkit.org/sleuthkit/download.php
- Autopsy (version 3 or higher): http://www.sleuthkit.org/autopsy/

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: Windows OS Autopsy Demo (1)



Step 1. Create new case



Enter New Case Information:

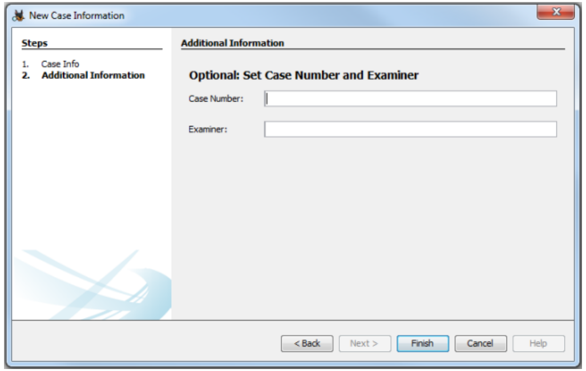
Case Name: forensics_test

Base Directory: E:\Leslie\courses\ece422\spring 2015\forensics\

Case data will be stored in the following directory:

E:\Leslie\courses\ece422\spring 2015\forensics\forensics_test

Step 2. Choose directory



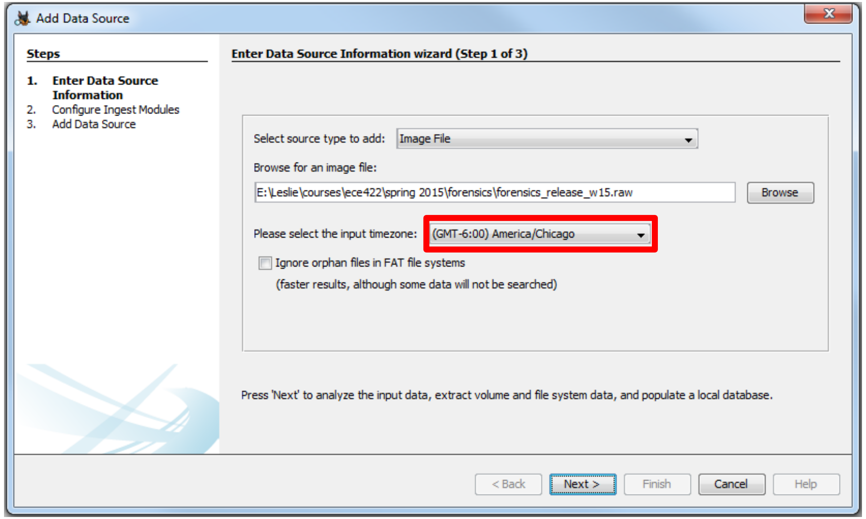
Optional: Set Case Number and Examiner

Case Number:

Examiner:

Step 3. Optional: leave it blank

Dead Analysis: Windows OS Autopsy Demo (2)



Steps

1. **Enter Data Source Information**
2. Configure Ingest Modules
3. Add Data Source

Enter Data Source Information wizard (Step 1 of 3)

Select source type to add: Image File

Browse for an image file:

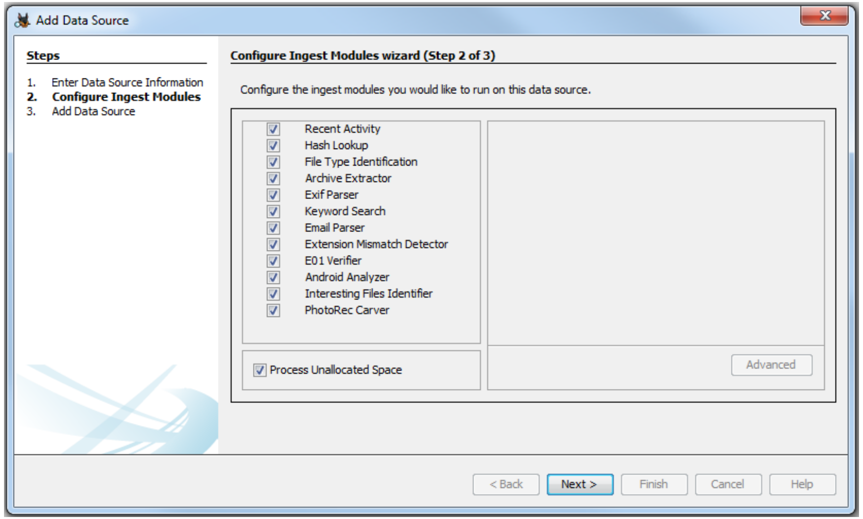
E:\Leslie\courses\ece422\spring 2015\forensics\forensics_release_w15.raw

Browse

Please select the input timezone: (GMT-6:00) America/Chicago

☐ Ignore orphan files in FAT file systems
(faster results, although some data will not be searched)

Press 'Next' to analyze the input data, extract volume and file system data, and populate a local database.



Steps

1. Enter Data Source Information
2. **Configure Ingest Modules**
3. Add Data Source

Configure Ingest Modules wizard (Step 2 of 3)

Configure the ingest modules you would like to run on this data source.

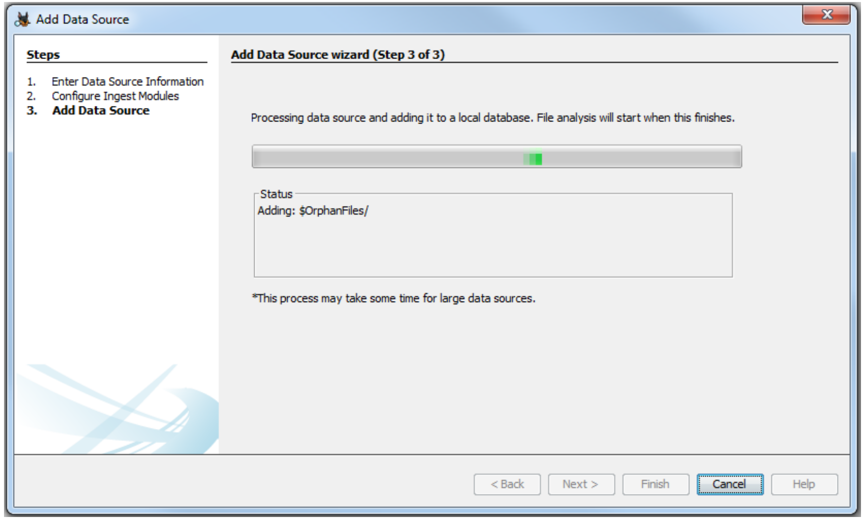
☑ Recent Activity
☑ Hash Lookup
☑ File Type Identification
☑ Archive Extractor
☑ Exif Parser
☑ Keyword Search
☑ Email Parser
☑ Extension Mismatch Detector
☑ E01 Verifier
☑ Android Analyzer
☑ Interesting Files Identifier
☑ PhotoRec Carver

☑ Process Unallocated Space

Step 4. Browse raw disk image

Step 5. Leave as default

Autopsy: Windows OS Demo (3)



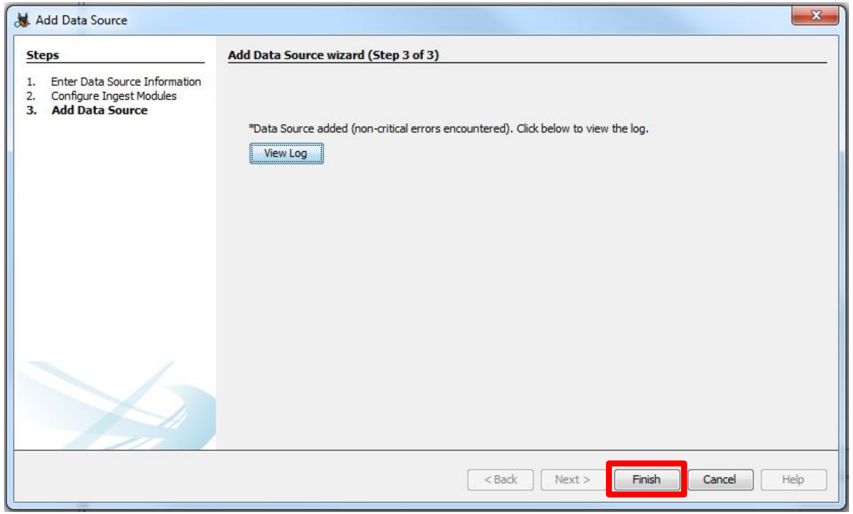
Add Data Source wizard (Step 3 of 3)

Processing data source and adding it to a local database. File analysis will start when this finishes.

Status
Adding: $OrphanFiles/

*This process may take some time for large data sources.

Step 6. Setup wizard

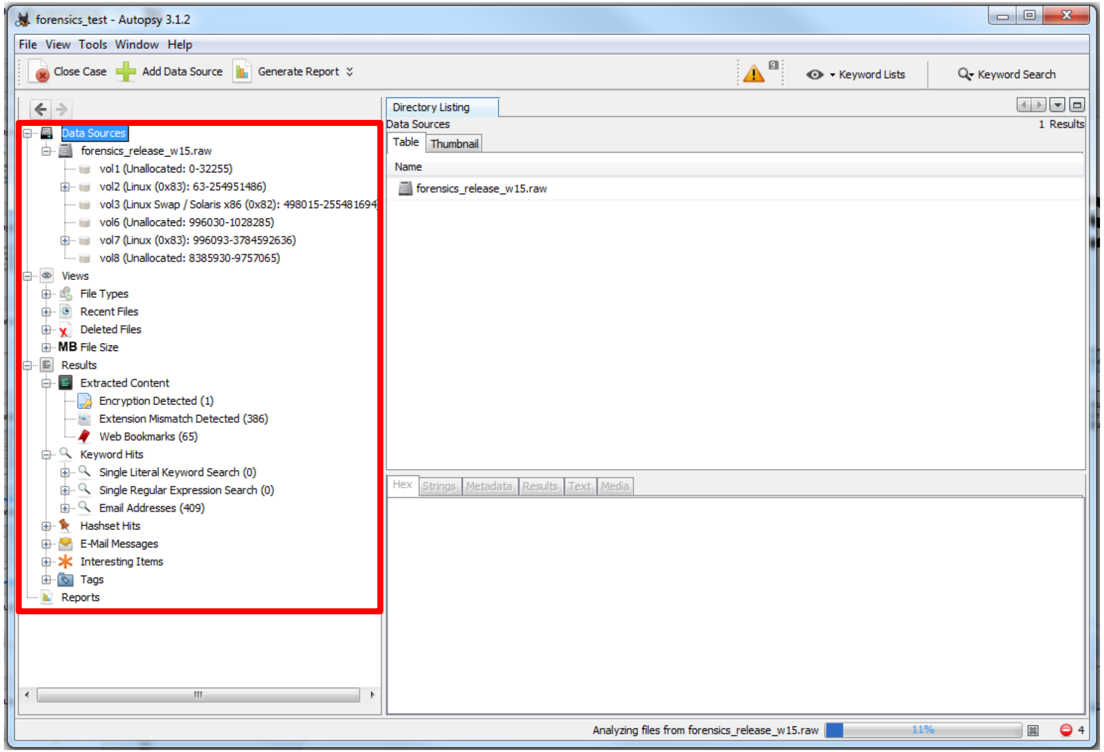


Add Data Source wizard (Step 3 of 3)

*Data Source added (non-critical errors encountered). Click below to view the log.

Step 7. Finish creating case

Autopsy: Windows OS Demo (4)



- Data Sources
  - forensics_release_w15.raw
    - vol1 (Unallocated: 0-32255)
    - vol2 (Linux (0x83): 63-254951486)
    - vol3 (Linux Swap / Solaris x86 (0x82): 498015-255481694
    - vol6 (Unallocated: 996030-1028285)
    - vol7 (Linux (0x83): 996093-3784592636)
    - vol8 (Unallocated: 8385930-9757065)
- Views
  - File Types
  - Recent Files
  - Deleted Files
  - File Size
- Results
  - Extracted Content
    - Encryption Detected (1)
    - Extension Mismatch Detected (386)
    - Web Bookmarks (65)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
    - Email Addresses (409)
  - Hashset Hits
  - E-Mail Messages
  - Interesting Items
  - Tags
- Reports

Data Sources — 1 Results

forensics_release_w15.raw

Analyzing files from forensics_release_w15.raw 11%

Step 8. Start investigation

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.

File Metadata

Metadata is “data about data”

Two types

- **Structural** - Data about the containers of data – internal structure – camera, iso, exposure, file format
- **Descriptive** - Data about the content of the file – name, creator, subject, description

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 (-)

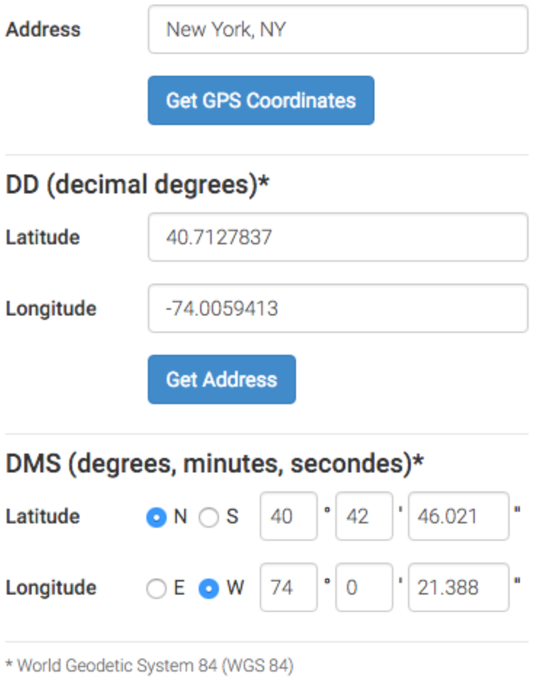
EXIF Tool

- 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

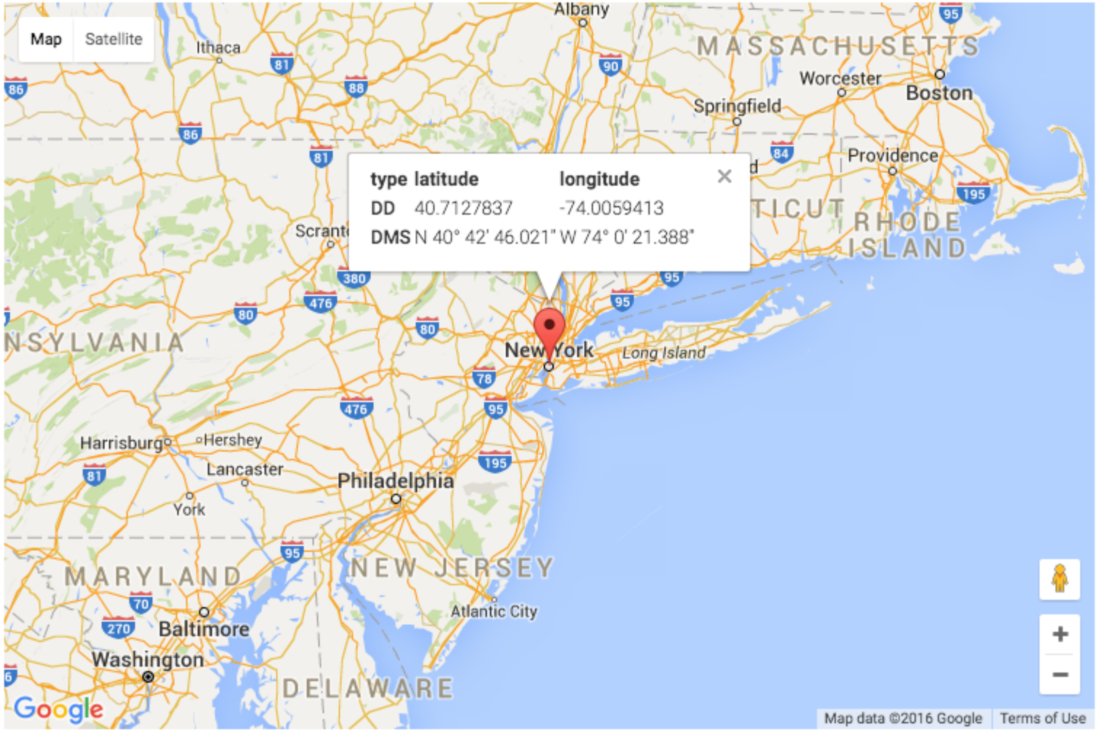
DD (decimal degrees)*

Latitude	40.7127837
Longitude	-74.0059413

DMS (degrees, minutes, secondes)*

Latitude	● N ○ S	40 °	42 '	46.021 "
Longitude	○ E ● W	74 °	0 '	21.388 "

* World Geodetic System 84 (WGS 84)



type	latitude	longitude
DD	40.7127837	-74.0059413
DMS	N 40° 42' 46.021"	W 74° 0' 21.388"

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)
- PDFcrack: PDF password cracker

Password Cracking: John The Ripper

References

http://www.openwall.com/john/doc/

http://pentestmonkey.net/cheat-sheet/john-the-ripper-hash-formats

Options

-- single – Single crack mode – password candidates from user account

-- wordlist – A Sample word list

-- incremental – All possible character combinations

--show – outputs the cracked password in a human-readable format

Community Enhanced Edition – Extra features

Unix / Mac OS: Sample John command

```
./john --wordlist=password_list --show hash_file
```

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.

http://extundelete.sourceforge.net/
https://www.cgsecurity.org/wiki/PhotoRec_Step_By_Step