**AUTOPSY LABS**

<https://training.autopsy.com/courses/take/autopsy-basics-8-hours>

**DOWNLOADS**

Let’s start downloading the data we'll need for the later labs.  We won't need them for a few sections, so you can start them now and let them download in the background.

Autopsy: We focus on the Windows version of Autopsy.  You may encounter problems with the course if you use it on Linux or macOS since not all features are supported.

64-bit Autopsy: <http://www.autopsy.com/download>

Disk images.  Given the popularity of the free COVID-19 training, we have had trouble hosting these images with reasonable speeds.  If one of these is past its quota, try the other.

* + [Mirror #1](https://drive.google.com/drive/folders/1YJ0v9izpUZUfB2U3IAQ8ke3T9dUe57Jb?usp=sharing)
  + **OR**
  + [Mirror #2](https://drive.google.com/drive/folders/15b8_gKQmj7Nz6wo2n34CSD9LBu5TKgHX?usp=sharing)
  + **OR**
  + [Mirror #3](https://file.ac/YVZWKZFVanc/)  
      
    Hashes for the files:  
    MD5 (device1\_laptop.e01) = dc176d653c5613e305e831525e874090  
    MD5 (device2\_mediacard.e01) = c8343d3976eec2985e7580a2b6321591
* NIST NSRL Hash Set: <https://sourceforge.net/projects/autopsy/files/NSRL/NSRL-266m-computer-Autopsy.zip/download>
* Video Triage Module: Fill out the form and download the ZIP file.  [https://www.autopsy.com/add-on-modules/video-triage/](https://www.autopsy.com/add-on-modules/video-triage/))

**PLATFORM NOTE**

Added April 21, 2020

Autopsy is primarily developed for Microsoft Windows, but there is minimal support for running on Linux and macOS. There are feature limitations on Linux and macOS. This course was originally written under the assumption that the student was running Windows.

If you do not have access to a Windows system, you may experience problems with some of the labs.

**LAB: INSTALLATION**

We will now install Autopsy on your computer so that we can later do hands-on activities.

1. You should have downloaded the ".msi" installer in Section 1.
2. Install it using the default options.
3. Launch Autopsy and enable the Central Repository using a SQLite database in the default AppData location.

**LAB: CASES AND DATA SOURCES**

Before we begin the lab, make sure you downloaded the images that were listed back in Section 1. If you want to confirm that you had no corruption, these are the MD5 values of the files:

* MD5 (device1\_laptop.e01) = dc176d653c5613e305e831525e874090
* MD5 (device2\_mediacard.e01) = c8343d3976eec2985e7580a2b6321591

We will now begin the analysis of the hard drive that was found in the dognappers car.  At this point in the scenario, we haven’t searched the house yet and therefore will not have access to the media card device.  So, make sure you do not add that yet.

1. Launch Autopsy
2. Choose “Create New Case”
3. Make a case with the following information:
   1. Case Name: case1
   2. Base Directory: c:\  (or where ever you'd like to store the case)
   3. Skip case number and examiner
4. Add device1\_laptop.e01 image as data source.    
   \*\*\*\*\* NOTE: Do NOT add device2\_mediacard.e01 yet \*\*\*\*\*
5. Deselect ALL ingest modules.    
   - As a reminder, this is not what you’d typically do.  But, we are doing it this way for the course.
6. Finish Adding Image.
7. Open the “Data Sources” part of the left-hand tree (we’ll cover this tree more in the next section).
   1. Question: How many volumes does the disk image have?
   2. Question: What is the name of the unallocated space file in vol1?
   3. Question: Right click on vol7 and choose “File System Details”.  What file system is in vol7?
8. In Windows, open “C:\case1” in a file explorer and observe its contents.
   1. Question: What is the database called?
   2. Question: Roughly how big is the database (in megabytes)?

**LAB: UI BASICS**

1. Keep the same case open that you created in the last section.  Let’s look at the data in the tree.
   1. Question: By extension, how many databases are there?
   2. Question: What is the size of the largest database?
   3. Question: Are there any databases by MIME type yet?
   4. Question: What are the names of the files between 200MB and 1GB in size?

**LAB: ANALYZING DATA AND HASH LOOKUP MODULE**

We are now going to begin analyzing the laptop.  We are starting off the case with some clues. Most notably, we have pictures that were sent with the ransom emails to Basis Technology

1. Keep same case open from previous lab, or reopen the case ("case1").
2. Right click on device1\_laptop.e01 image in tree and choose “Run Ingest Modules”
3. Disable all modules except the following (we will pre-load some for the next lap):
   1. Hash Lookup
   2. File Type Identification
   3. Extension Mismatch Detector
   4. Embedded File Extractor
   5. Exif Parser
   6. Email Parser
   7. Correlation Engine
4. Configure the Hash Lookup module with two hash sets:
   1. Import the NSRL File (NSRLComplete.txt-md5.idx) that you previously downloaded in Section 1.
      1. You may need to unzip the file you downloaded.
      2. You can use the default values (i.e. Type: Known).
   2. Create a New Hash Set:
   * Destination: Local
   * Name: Ransom Case
   * Hash Set Path: [Any folder on your computer]
   * Type: Notable
   1. Use "Add Hashes to Hash Set" button to copy and paste the following MD5 value into the "Ransom Case" hash set.  This is the hash of the ransom note.  
      07c94320f4e41291f855d450f68c8c5b
5. Start the Ingest Modules.
6. Observe:
   1. Use Ingest Inbox as an indicator when ‘Known Bad’ hash hits are found.
   2. Use “Go To Result” to go to tree area of hash hits.
   3. View the hash hit.
   4. Question: Let ingest get at least 15% through the drive.  How many total hits are found under the “Hashset Hits” results after running the Hash Lookup Ingest Module?
   5. Question: What are the filenames of the hash hits?
   6. One of the hits is in a folder named “Pictures”.  Right click on the file to “View” there.
   7. Question: How many total ".jpg" files are in the folder “Pictures” where the notable hash hit was found?
   8. While reviewing the images in that folder, it is noticed that “IMG\_20191024\_155744.jpg” shows health violations by bringing the dog into a restaurant.  We want to tag this as Notable:
      1. Right click on it
      2. Select “Add File Tag” and choose “Notable Item”

**LAB: VARIOUS SMALL MODULES (FILE TYPE, EXIF, ETC.)**

NOTE: We already ran the modules in the last lab.

1. Question: Under the “Exif Metadata results, how many photos were taken with the following devices?
   1. iPhone 7 Plus?
   2. Samsung Galaxy S8?
   3. BLU R1 HD?
2. From the “Views” area, find the archive file that is named “Archive.zip”.
   1. Go to original directory (Right click -> View File In Directory).
   2. Double click on it to go into it.
   3. Question: What is the MIME type listed for the file “D3D11\_Default.shader-db.bin”?
   4. Question: What is the file size for the file “D3D11\_Default.shader-db.bin”?”
3. Question: Are there extension mismatch results?
4. Question: What are some common file types with unexpected extensions?
5. Run ingest again with only the Interesting Files module enabled.
   1. Create an Interesting File Set named “Encryption”.  With two rules that match files named “veracrypt.exe” or “truecrypt.exe”.
   2. Question: Was VeraCrypt found on the system?
   3. Question: Was TrueCrypt found on the system?

**LAB: RECENT ACTIVITY**

Run ingest with only “Recent Activity” enabled.

1. Question: How many Web Bookmarks were found?
2. Question: What URL is a suspicious bookmark given the dognapping?
3. Question: What day are the cookies associated with the domain “youtube.com” from?
4. Question: What is the Value associated with the Name “identification” under Web Form Autofill?
5. Question: Under Web History, what day were the following Google Searches performed?
   1. “how to treat a dog bite”
   2. “how to make a ransom note”
6. Question: How many non-VM USB devices were attached to the system?
   1. NOTE: April 21, 2020: Some Linux systems are not getting a correct answer for this with Autopsy 4.14 because RegRipper cannot run.  This problem was fixed in 4.15.
   2. We are hearing about some Windows systems where the UI does not show the device IDs ( but they are saved into the case database). You can then re-open the case and see the results. We are investigating why this happens.
7. Question: How many file(s) is/are currently in the Recycle Bin?
   1. What was likely the original name of the file(s)?
8. Question: Under Accounts, what is the username associated with the Twitter account found on the device?

**LAB: KEYWORD SEARCH**

We will now run ingest and prepopulate with keywords that we already know about the case.

1. Run ingest with “Keyword Search” enabled.
   1. Create a keyword list with the following words:
      1. Exact Match Keywords:
         1. renzik
      2. Configure to update every 1 minute (so that you don’t have to wait too long - change it back after).
2. Start Ingest.
3. After it runs for a few percent of the files, you should see some hits.   They honestly aren’t that exciting, but they are good enough for this lab.  There are more relevant ones if you let it run until 15% or so.
4. Question: There are references to a document with renzik.  What is the name of the file?
5. Question: How many hits are there for “Renzik” in NTUSER.DAT?
6. Don’t forget to change your keyword search periodic timer back to 5 minutes.

**LAB: CORRELATION ENGINE**

At this point in the scenario, the police have searched the house and, with the help of Siri the electronic sniffing K9, found a media card.  We will add that to our case and find some correlations.

1. Add device2\_mediacard.e01 as a new data source (NOTE: We already added the device1\_laptop.e01 data source to the Central Repository during the Hash Lookup Lab)
2. Right click on device2\_mediacard.e01 and run Ingest Modules, with the following enabled:
   1. Hash Lookup
   2. Exif Parser
   3. Correlation Engine
3. Question: Was an Interesting Item created because a file on the media card was previously marked as notable?
4. Question: The picture on the laptop had a created date of 2019-11-01. What is the created date (in YYYY-MM-DD format) on the mediacard?
5. Question: How many total .jpg files are in the same folder as the Notable file?
6. Question: Look at the Other Occurrences tab for that file to see if it showed up anywhere else in this case with a different name. If it was, what is the other name?

<The following sections did not have labs - Android Analyzer, Timeline Interface, Image Gallery, Communications Interface, and Tagging, Commenting, and Reporting>

**LAB: 3RD PARTY MODULES**

1. You downloaded the Video Triage module from the [autopsy.com](https://www.autopsy.com/add-on-modules/video-triage/) site in Section 1.
2. Install it using Tools -> Plugins.
3. Try it on one of the videos from the case. The dognappers did not do much with videos, but you can sort them by size to pick a "big" one and see the various frames.

**CONCLUSION**

Congratulations!

During the labs, you analyzed the media associated with the dognapping of Renzik by the Anti-Renzik Group.  
  
Your analysis led to the dismantling of the Anti-Renzik Group and, most importantly, allowed the recovery of Renzik. who has been returned safely to his home at Basis Technology!