FOR518 | MAC AND IOS FORENSIC ANALYSIS AND INCIDENT RESPONSE
GIAC iOS and macOS Examiner (GIME)

Workbook

SANS | GIAC CERTIFICATIONS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

All reference links are operational in the browser-based delivery of the electronic workbook.

Welcome to the FOR518 Workbook

Workbook Overview

This workbook contains all lab materials for SANS FOR518. Each lab is designed to address a hands-on application of concepts covered in the corresponding courseware and help students achieve the learning objectives the course and lab authors have established.

This workbook comes in both PDF/printed format and in HTML format. The HTML-based "electronic workbook" includes the following features:

- Workbook site navigation is displayed on the left and intra-page navigation is on the right
- Integrated keyword searching across the entire site at the top of each page
- Convenient copy-to-clipboard buttons at the right side of code blocks
- Inline drop-down solutions, command lines, and results for easy validation and reference
- High-resolution images can be clicked to enlarge when necessary
- Authors can update the HTML content to implement minor typo and clarification fixes

Because of these advantages, we highly recommend students use the HTML-based electronic workbook as their main way to work on the labs. The printed workbook can be helpful for writing down notes, and as a reference to use on the GIAC exam. Otherwise, we believe the electronic workbook offers a better student experience.

Lab 1.0: Lab Setup (In-Class)

Objectives

1. Introduction to FOR518 ISO Files
2. Unarchive and copy files to analysis system.

Lab Preparation

1. **Software Preparation**: The following tools may be used in this Lab:
    - The Unarchiver.app
        a. Locate "The Unarchiver.app" from `/Applications/` ; if you have not installed this yet, you may find it in the Tools directory on your FOR518-A ISO.

Lab

1. **Create a FOR518 directory**
    - The labs for this class will reference an FOR518 folder in the user's home directory to dump various files for use in other labs (`~/FOR518`).
    - Please create a directory named FOR518. You do not have to create it in your home directory but be sure to remember where it is. The workbook used in class will reference this directory in your home directory.
    - The command below shows how to create this folder in your home directory. You may also use the GUI interface to do this.
    - To make this directory more accessible, you can drag and drop it to your Finder sidebar. Using the "open" command, you can open it from Terminal into Finder.
        a. Select the folder icon for the FOR518 directory and drop it into the Finder sidebar in "Favorites."

```
mkdir ~/FOR518

open ~
```

2. **Introduction to the [FOR518 - A] ISO**
    a. Open and mount the **FOR518 - A** ISO. This can be done by double-clicking the file.
    b. View the mounted ISO using the Finder application.
    c. The ISO has the following directory structure:
        i. **Lab Files**: This directory contains files and software that you will need for the class Labs, listed for each Lab.
        ii. **Lab Images**: This directory contains the forensic images that you will be working with on the Labs. You will need to unarchive these files for this class.

iii. **FOR518 APFS Cheat Sheet and Command-line Reference PDF (FOR518_APFS_CheatSheet_######.pdf)**: This file contains a command line cheat sheet as well as a reference for APFS for the class.

iv. **Tools**: This directory contains many of the tools you have already installed plus some extras that can be installed later in the class.

v. **VERSION-FOR518-##-##.txt**: This file contains the MD5 hashes for the 7zip archives as well as for the image files used in this class.

3. **Unarchive**

   a. Unarchive the following items to your host system (or external hard drive) from the Lab_Images directory. You should have installed "The Unarchiver.app" application prior to coming to class in Lab 0. If you have not yet installed it, please do so now. This zip file containing this application can be found in the Tools directory on the FOR518 - A ISO. The iPhone and Mac images are needed first, you will not be using the Memory file until Day 5 if you want to wait to unarchive these files. The Time Machine image is part of a bonus lab and is not required to unarchive at this time.

      i. DavidLightman_physical_logical_dump.dmg.7z (Unarchived Size: 13.98GB)

      ii. galaga.E01.7z (Unarchived Size: 14.71GB)

      iii. galaga_memory.raw.7z (Unarchived Size: 19.05GB)

      iv. galaga_timemachine.E01.7z (Unarchived Size: 55.64GB)

4. **Copy out the Lab Files**

   a. Copy the Lab_Files directories to your ~/FOR518 directory.

5. **Install Cellebrite Inspector**

   a. In the Tools directory, find the `Cellebrite_Inspector_macos_10.5.pkg` installer.

   b. Double-click the file and follow the default prompts to install.

6. **Add license to Inspector**

   a. Open Inspector from your `/Applications/Inspector/Inspector #### Release #/` directory. You should be presented with a window allowing you to "`Enter Demo Key...`", your instructor will provide you with a license name and key. Please enter this information where appropriate.

      i. For OnDemand students, the Inspector license info will be located in the MyLabs section of your SANS portal, or you can get there directly by going to https://connect.labs.sans.org while logged into your portal account.

7. **Install Cellebrite Epoch Converter**

   a. Open the `epoch_converter.app_.zip` file in the Tools directory on your FOR518 ISO.

   b. Copy this app to the `/Applications` directory.

8. **Additional Setting Changes for 10.14+ Users**

   - Users who are using macOS 10.14 and higher will need to configure additional items to allow full disk access for mounted images for labs and the final challenge for this course. The final settings should look like the example below. You may now close the System Preferences application. You may choose to revert these actions at the end of class.
   - Change Privacy Settings:

      a. Open "System Preferences" from the Dock or the Apple Menu at the top-left of the menu bar.

      b. Select the "Security & Privacy" Preferences Panel

c. Select the "Privacy" tab.

d. Click the lock icon at the bottom-left of the window, provide the pop-up window Administrator credentials. Select "Unlock"

e. On the left, select "Full Disk Access"

f. In the right panel, select the "+" icon to add two Applications. (Adding these Applications may require those applications to be exited, please allow them to be closed.)

   - `/Applications/Utilities/Terminal.app`
   - `/Applications/Xcode.app`
   - `/Applications/Inspector/Inspector #.#/Inspector`

Lab 1.1: Inspector Case Setup and Image Mounting

Objectives

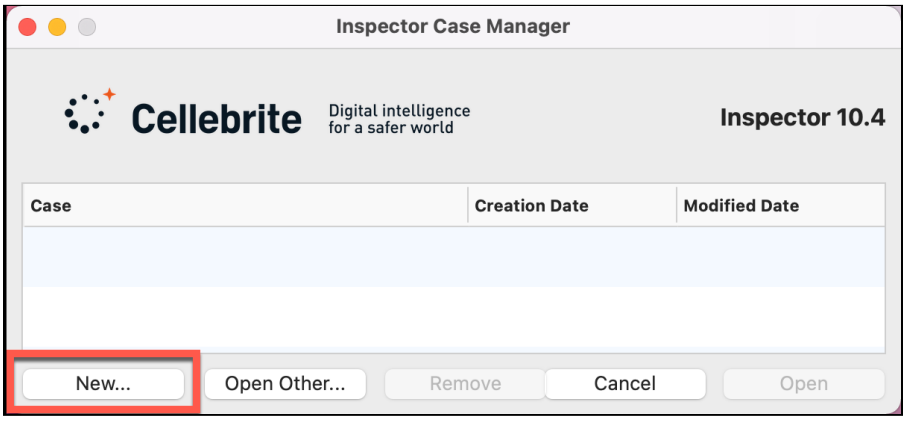
- Import exercise images to Inspector
- Practice mounting lab images on the command line
- Introduction to Inspector

Lab Preparation

1. Locate the `galaga.E01` file that was extracted from your FOR518-A ISO file from the `Lab_Images/Mac/` directory.
2. **Software Preparation:** The following tools will be used in this exercise:
   - Inspector.app
     a. Locate and open `/Applications/Inspector/Inspector Release #/Inspector.app`
   - Inspector Key: Your instructor should provide this to you.
   - Terminal.app
     a. Locate and open the native macOS Terminal.app from `/Applications/Utilities/`

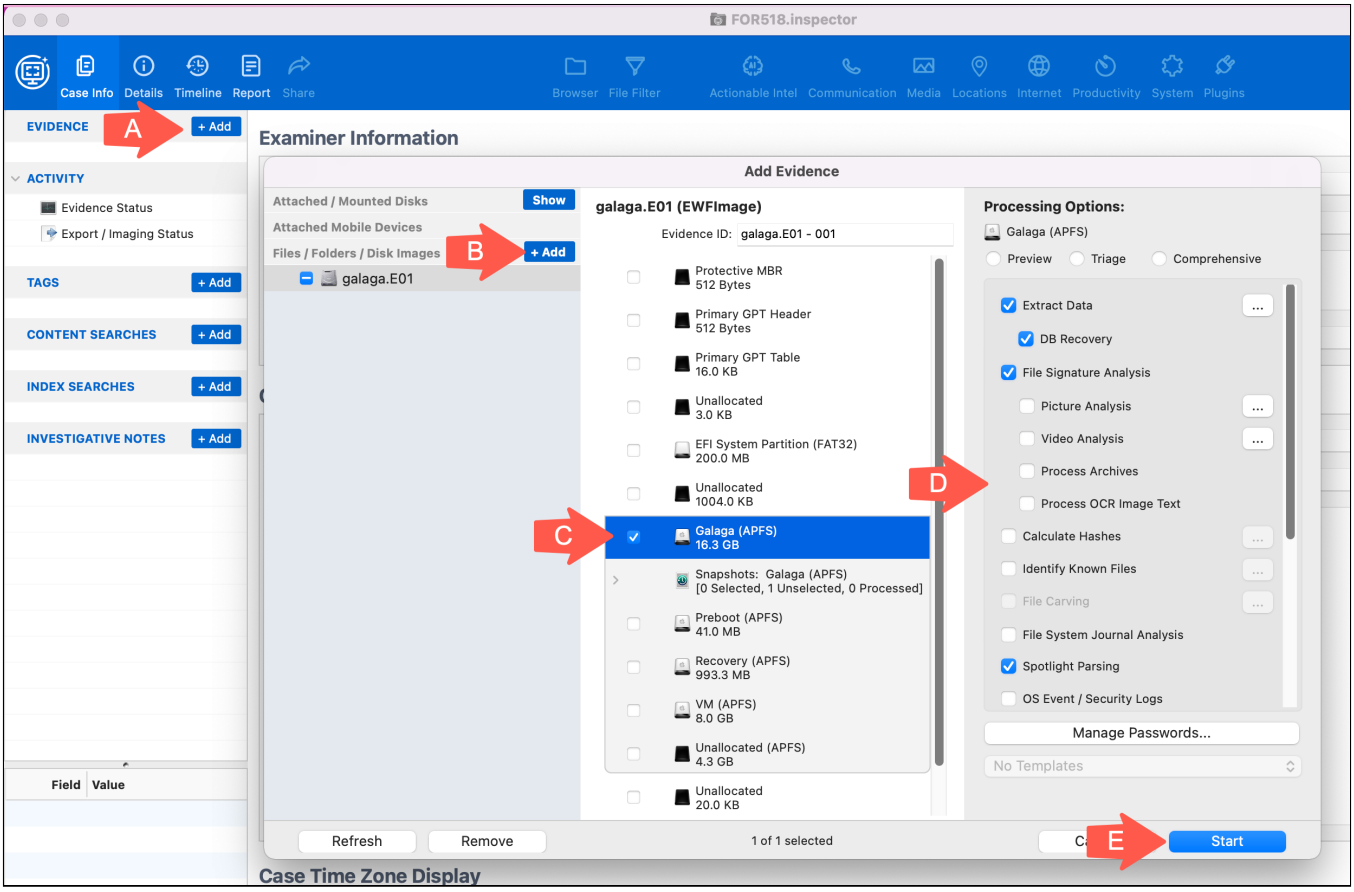
Lab

1. **Load Lab Image in Inspector**
   a. The first window presented to a user is the Case Manager window. This window will show all your recent cases and allow you to create new ones.
      i. Create a new case. Select the "New..." button at the bottom-left of the window.
      ii. Save the case in a directory of your choice. You may want to create a `FOR518` directory for this class, as we will be saving a variety of files for analysis.
      iii. Save the case file as `FOR518.inspector` in your `FOR518` directory.



b. This should open up the Inspector Case Info window.
    i. The Case Info tab of Inspector allows an analyst to input case specifics and change the time zone display. The defaults are fine.

c. Open the Disk Image:
    i. In the upper-left corner near “EVIDENCE,” you should see a small “Add“ button. Select this button.
    ii. In the “Add Evidence” window, select the “Add” button to select the image file. Locate the `Lab_Images` directory where you extracted your files, select the `galaga.E01` image and click Open.
    iii. This will open the Evidence Selection window. Please de-select the following disks so that only the "Galaga (APFS)" disk is checked (shown below).
        i. EFI System Partition (FAT32)
        ii. Preboot (APFS)
        iii. Recovery (APFS)
        iv. VM (APFS)
    iv. Select the following options:
        i. Extract Data
        ii. DB Recovery
        iii. File Signature Analysis
        iv. Spotlight Parsing
    v. Select "Start." This will start the image processing; this may take a few minutes. The Evidence Status window will show the disk processing progression.



d. While Inspector is processing, please move on to mounting the image via the command line below.

   i. Once processing has finished, feel free to browse the disk at your leisure!

2. **Practice Mounting David Lightman's Mac forensic image (`galaga.E01`)**

   a. Using Terminal.app, perform the commands to mount the `galaga.E01` macOS image.

   - Use the `mkdir` command to create a mount point for the `xmount` output. In this class, the directory name `galaga_image` is used because it will host the converted image file. `sudo` is required to perform this action as the mount point `/Volumes` chas limited permissions, thus it may ask you for your administrator password when executed.
   - Use the `mkdir` command to create a mount point for the mounted image. The directory `galaga_mounted` is used in this class to represent the mounted disk image. `sudo` is required to perform this action as the mount point `/Volumes` has limited permissions, thus it may ask you for your administrator password when executed.
   - Use `xmount` to mount the `galaga.E01` image (where you have your image located, the example shows `~/FOR518/Lab_Images/Mac/`) as a DMG file. This command requires you to use the `sudo` command, thus it may ask you for your administrator password when executed.
     - `--in` - Tells `xmount` what input file type to expect; our images are in a compressed EWF format.
     - `--out` - Tells `xmount` what output format you want; we want a DMG file so we can mount it in Finder.
     - `Input File` - Where the image file is located on your system.
     - `Mount Point` - Newly created mount point `/Volumes/galaga_image` specifically for this image.

```
sudo mkdir /Volumes/galaga_image/

sudo mkdir /Volumes/galaga_mounted/

sudo xmount --in ewf ~/FOR518/Lab_Images/Mac/galaga.E01 --out dmg /Volumes/
galaga_image/
```

- Use the `hdiutil` command with the "`attach`" verb to make the newly created DMG volume available. Use the `-nomount` argument to suppress mounting (for now). The output from this command will display several `/dev/disk#`; use the appropriate disk device in the next command.
    - APFS disks will show many `/dev/disk*` options in the `hdiutil` output. The one we want to mount is the user's macOS volume. We can use the command "`diskutil list /dev/disk4`" on the synthesized disk to determine which is likely the user's macOS volume. David Lightman's volume is named "`Galaga`", highlighted in the example below. We will use `/dev/disk4s1` in the next command. **Be aware that yours may be mounted on a different disk number!**

```
Sarahs-MBP:~ oompa$ hdiutil attach -nomount /Volumes/galaga_image/galaga.dmg
/dev/disk3              GUID_partition_scheme
/dev/disk3s1            EFI
/dev/disk3s2            Apple_APFS
/dev/disk4              EF57347C-0000-11AA-AA11-0030654
/dev/disk4s1            41504653-0000-11AA-AA11-0030654
/dev/disk4s2            41504653-0000-11AA-AA11-0030654
/dev/disk4s3            41504653-0000-11AA-AA11-0030654
/dev/disk4s4            41504653-0000-11AA-AA11-0030654
Sarahs-MBP:~ oompa$ diskutil list /dev/disk4
/dev/disk4 (synthesized):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      APFS Container Scheme -                      +31.8 GB    disk4
                                 Physical Store disk3s2
   1:                APFS Volume Galaga                  17.5 GB    disk4s1
   2:                APFS Volume Preboot                 43.0 MB    disk4s2
   3:                APFS Volume Recovery                1.0 GB     disk4s3
   4:                APFS Volume VM                      8.6 GB     disk4s4
```

- Use the `mount_apfs` command with the following parameters to mount the `/dev/disk#s#` (from the previous command) to the `/Volumes/galaga_mounted/` mount point. This command requires you to use the sudo command, thus it may ask you for your administrator password when executed. This drive will now be available in the Finder or Terminal applications.
    - `-o` - Options:
        - `rdonly` - Mount in read-only mode.
        - `noexec` - Do not allow execution of binaries on the mounted system.
        - `noowners` - Ignore ownership on the mounted volume.

```
hdiutil attach -nomount /Volumes/galaga_image/galaga.dmg

sudo mount_apfs -o rdonly,noexec,noowners /dev/disk#s# /Volumes/galaga_mounted/
```

3. **Sanity Check**
    - You can access this newly created mounted drive on `/Volumes/galaga_mounted/`, thus all command-line references in the workbook will be using this path. Using the Finder or the Terminal, access your newly created mounted volume.
    - Use the `ls -l` command to view the contents in the Terminal to (hopefully) view the macOS directory structure. You should see an account for "`dlightman`" in the Users directory, hopefully not yours!

```
ls -l /Volumes/galaga_mounted/Users/
```

4. **Unmount and Eject the Exercise Image**
    - Use the `diskutil list` command to view the list of mounted disks. Find the disk that you want to eject. This one will be the one labeled "(`disk image`)" versus the one labeled "(`synthesized`)". In my example, it would be `/dev/disk3`.
    - Use the `diskutil eject` command on the disk you would like to eject.
    - Use the `mount` command to view the list of mounted disks. Find the disk that you want to unmount (likely `/Volumes/galaga_image/` if you are following the naming scheme from the examples).
    - Use the `umount` command with the mount point to unmount the disk. You will have to use the `sudo` command.

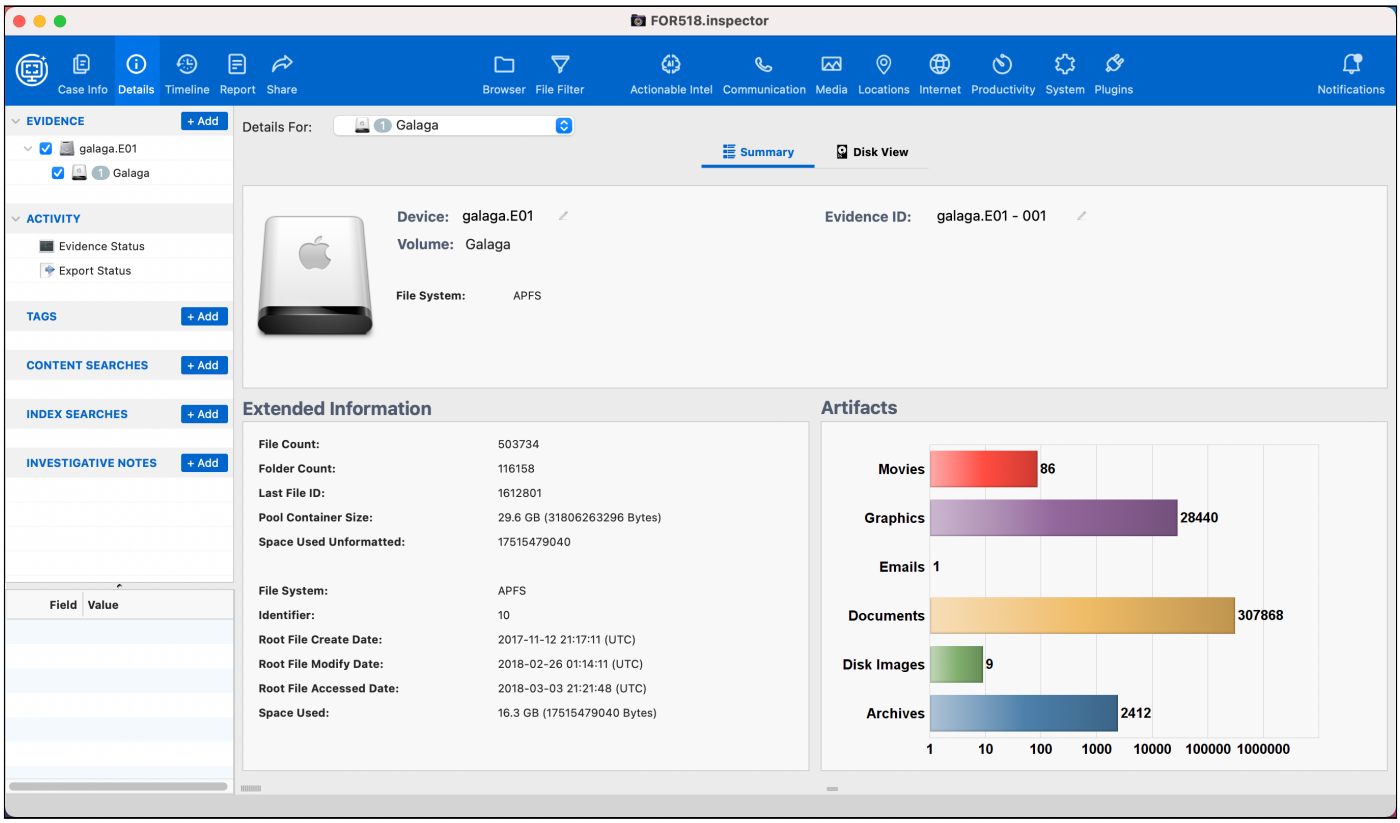
> **Warning**
>
> **If you are in the mounted image in Terminal, or have a program using the mounted disk, you will get an error that it cannot be ejected or unmounted.**

```
diskutil list

diskutil eject /dev/disk#

mount

sudo umount /Volumes/galaga_image
```

OPTIONAL

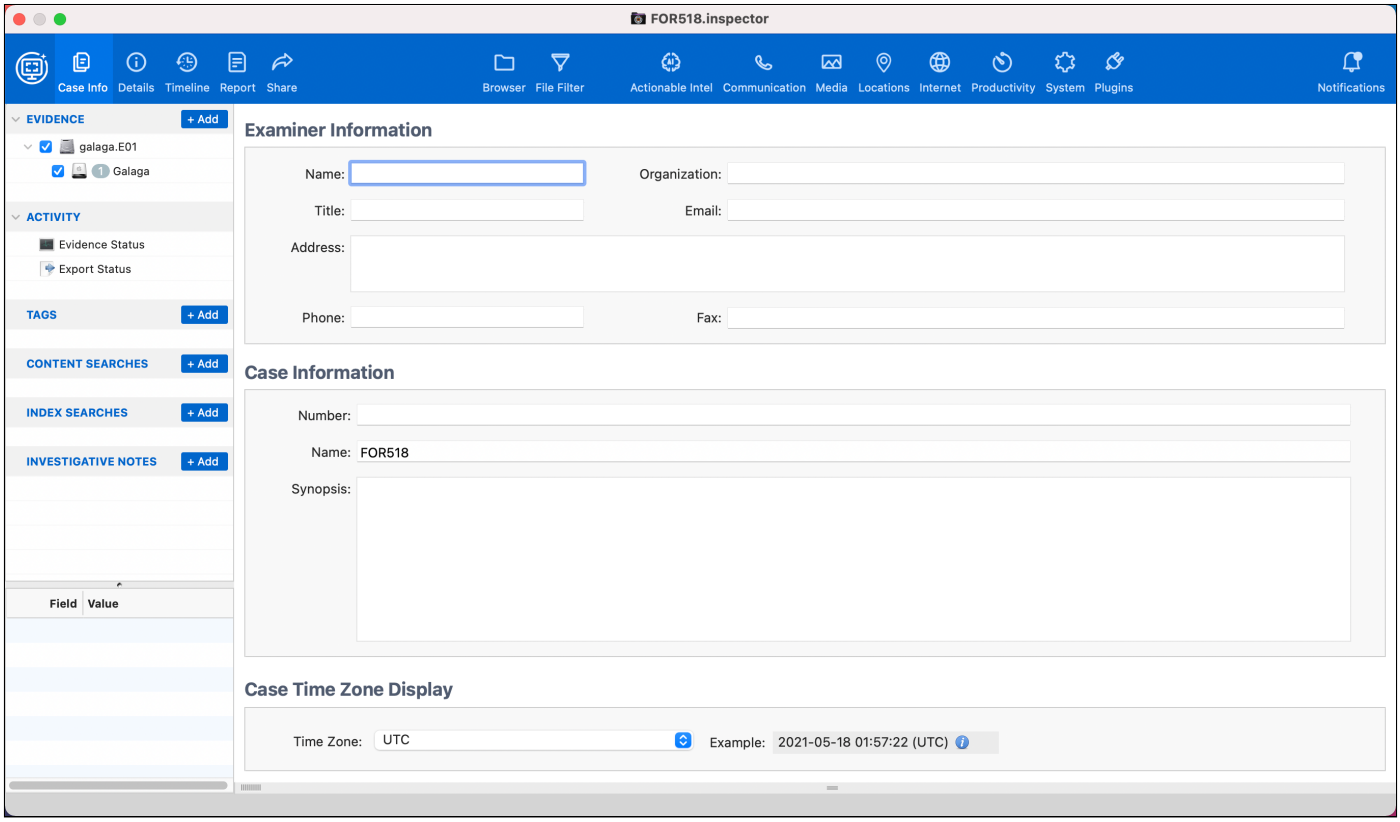
1. **Inspector 101**
    a. If you have never used Inspector before, this section of the lab will give you a beginner overview of the tool.
    b. Using the Inspector Case file you just created in the beginning of this lab, let's take a look at some of the features of Inspector.
2. **Details Tab**
    a. Check the box next to the `galaga.E01` drive under the EVIDENCE section on the left and select the Details tab at the top. This view will show basic triage information for the disk and the Galaga volume.

b. Use the dropdown to switch between the drive and the volume to view different details.



3. **Case Info Tab**

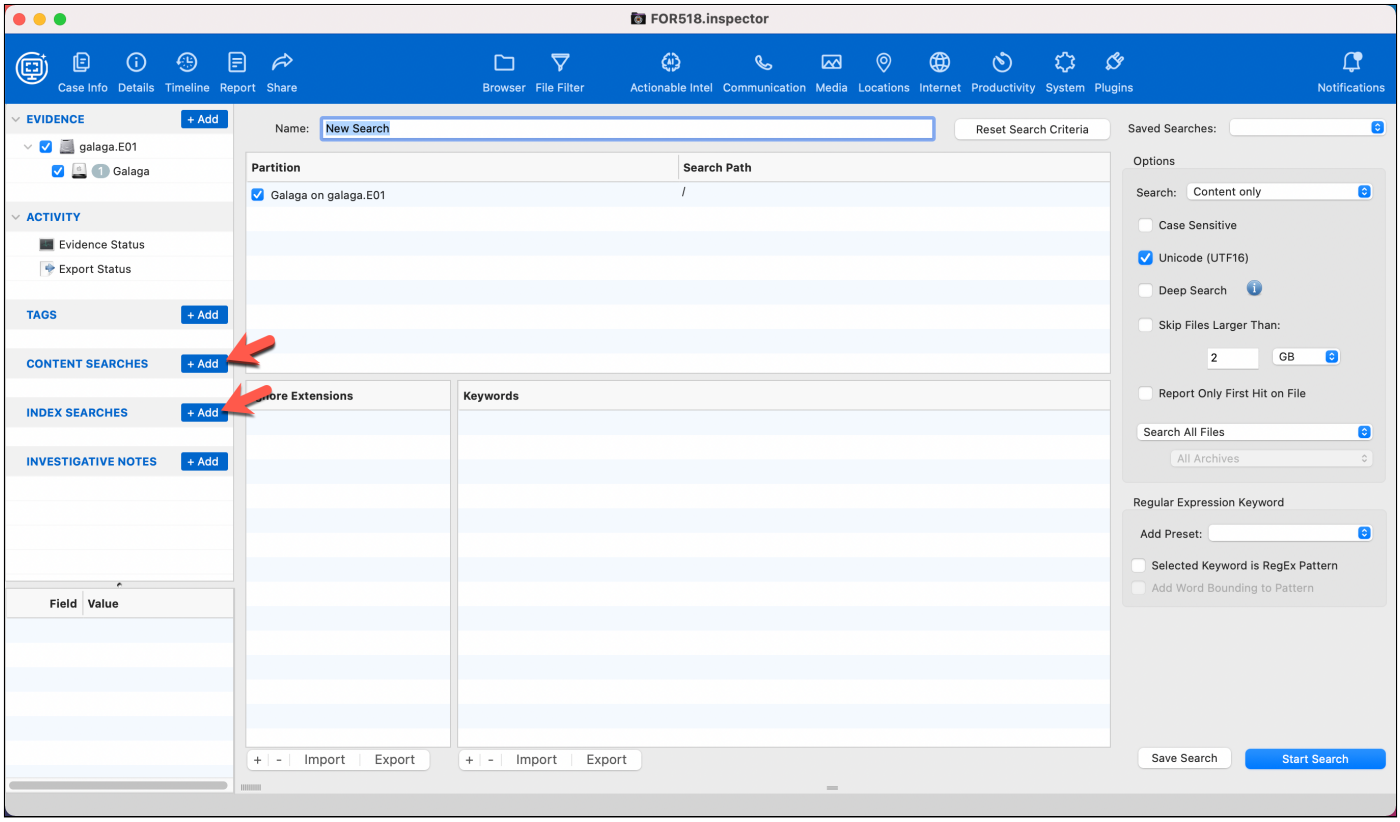
a. Select the Case Info tab, this shows an area where you may fill in case-specific information and change the time zone.



4. **Search Tab**

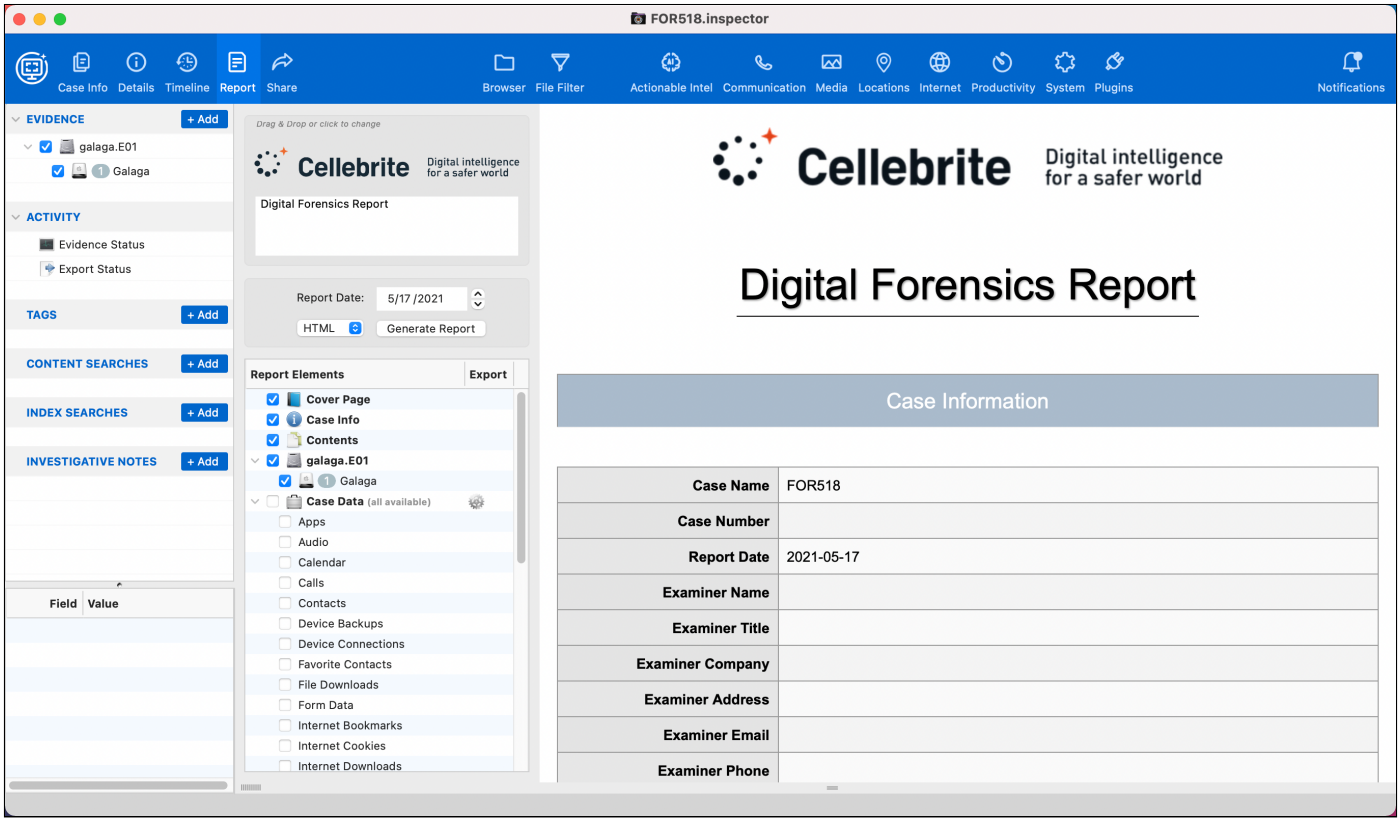
   a. Select the CONTENT SEARCHES on the sidebar. This view allows an investigator to perform keyword searches. Each keyword list has a Name as filled in the Name text box. The keywords may be typed in the Keywords pane. File extensions may be ignored by typing them into the Ignore Extensions pane. Other keyword configurations may be selected in the pane on the right side. Select “Start Search” when ready to search. Results can be filtered in various ways using the filter button on the left side.

   b. Index Searches can also be done by using the INDEX SEARCHES option on the sidebar, however the index must be built first in the Evidence Status area.



5. **Report Tab**

   a. The Report tab shows default report information for the selected hard drive.

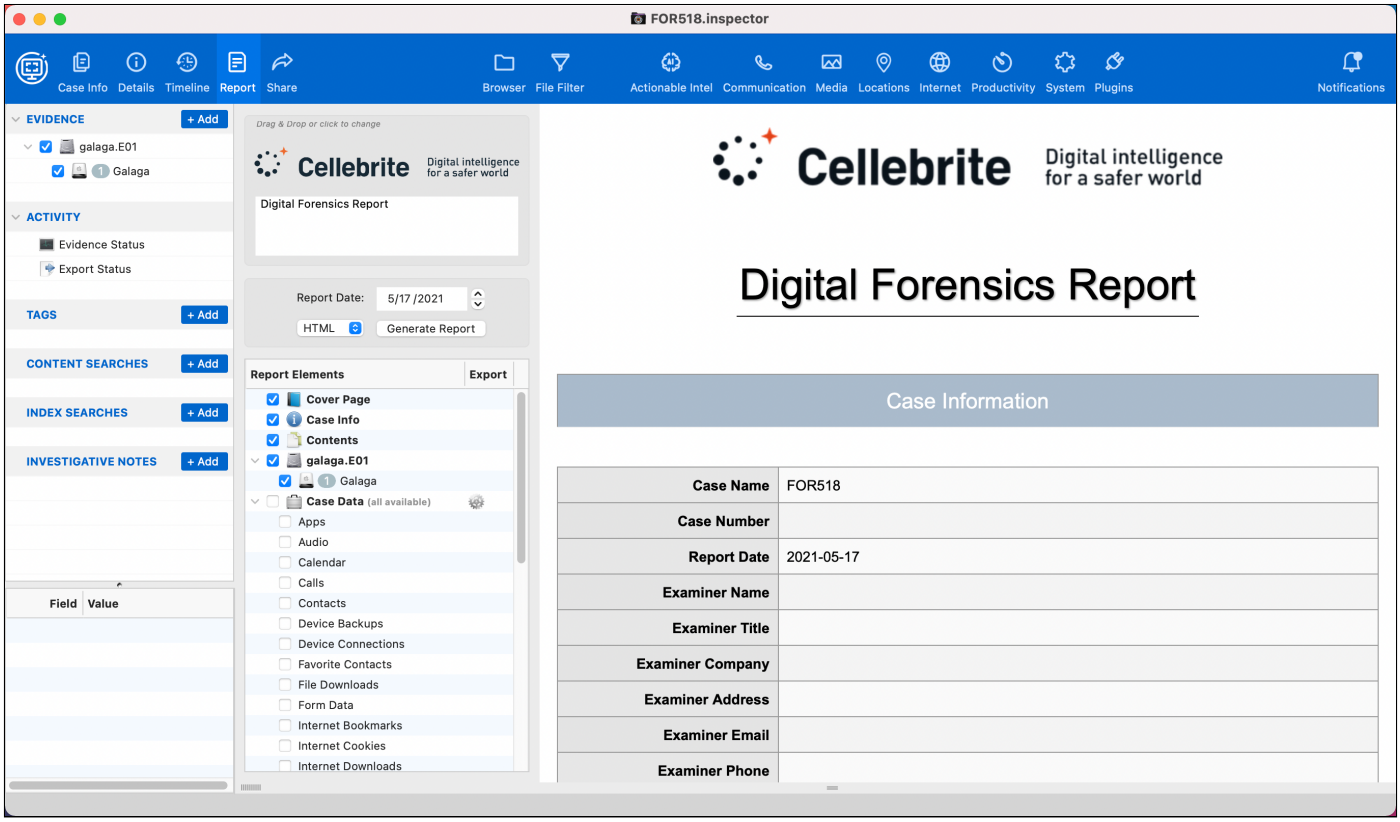


6. **Browser Tab**

   a. The Browser tab shows the file system as an investigator is most likely used to seeing it. This view shows the file system in a tree format with hidden files shown in gray, and other file metadata including timestamps and file size.

   b. The lower pane (the bar may have to be moved up from the bottom of the window) shows the file. The views available include Hex, Strings, Preview, Metadata, Location, and Record. An analyst may also select the “eye”-shaped button to do a “Quick Look” on the file. The Data and Resource fork may also be chosen. In the Hex view, the data-type window on the right will be shown for the analyst to select various data types, if conversion is needed.

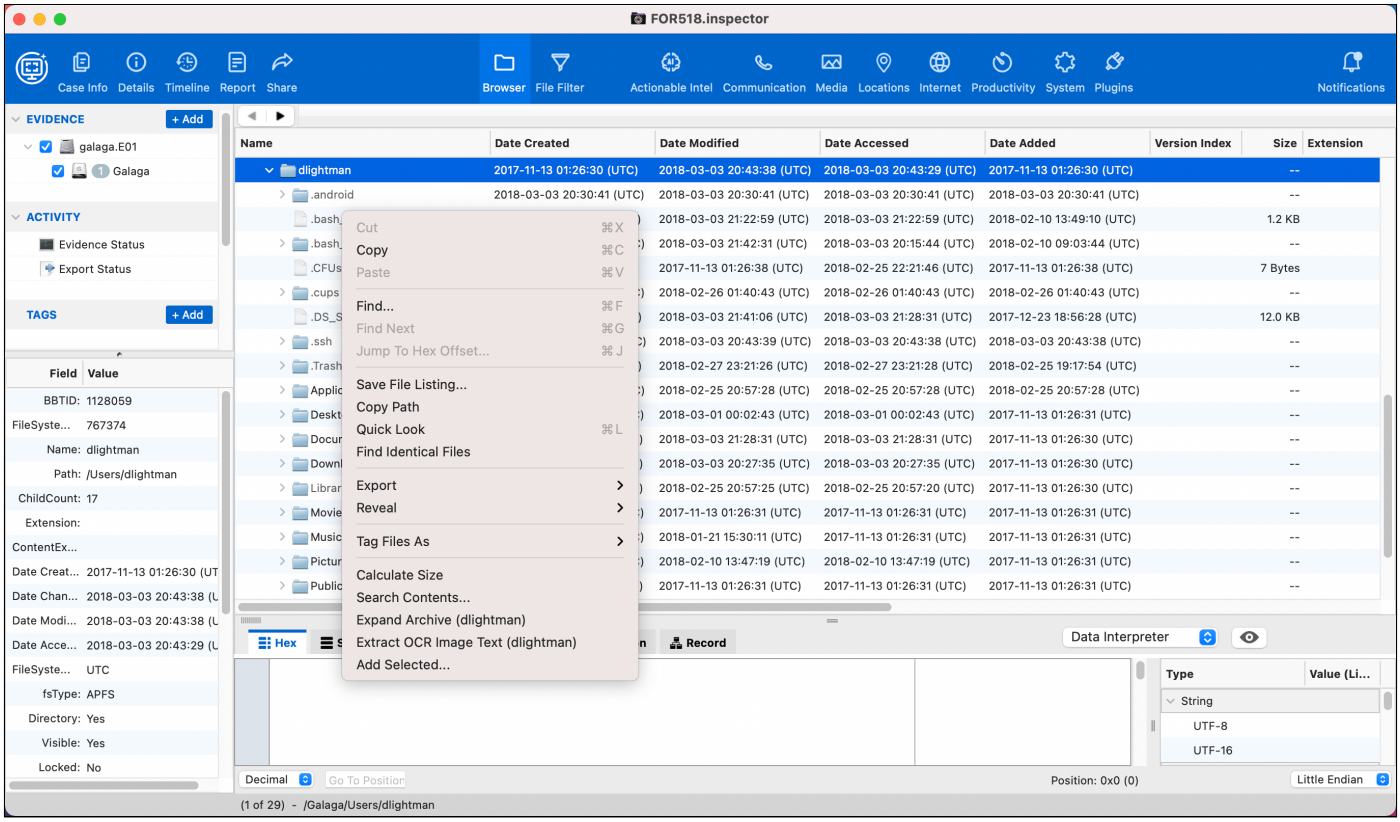
   c. In the lower-left pane, the file metadata and extended attributes are shown. Everything from file size, filename, timestamps, Finder data, and disk location, to extended attributes are available in this window. Lots of good information may be found here!



7. **Context Menu**

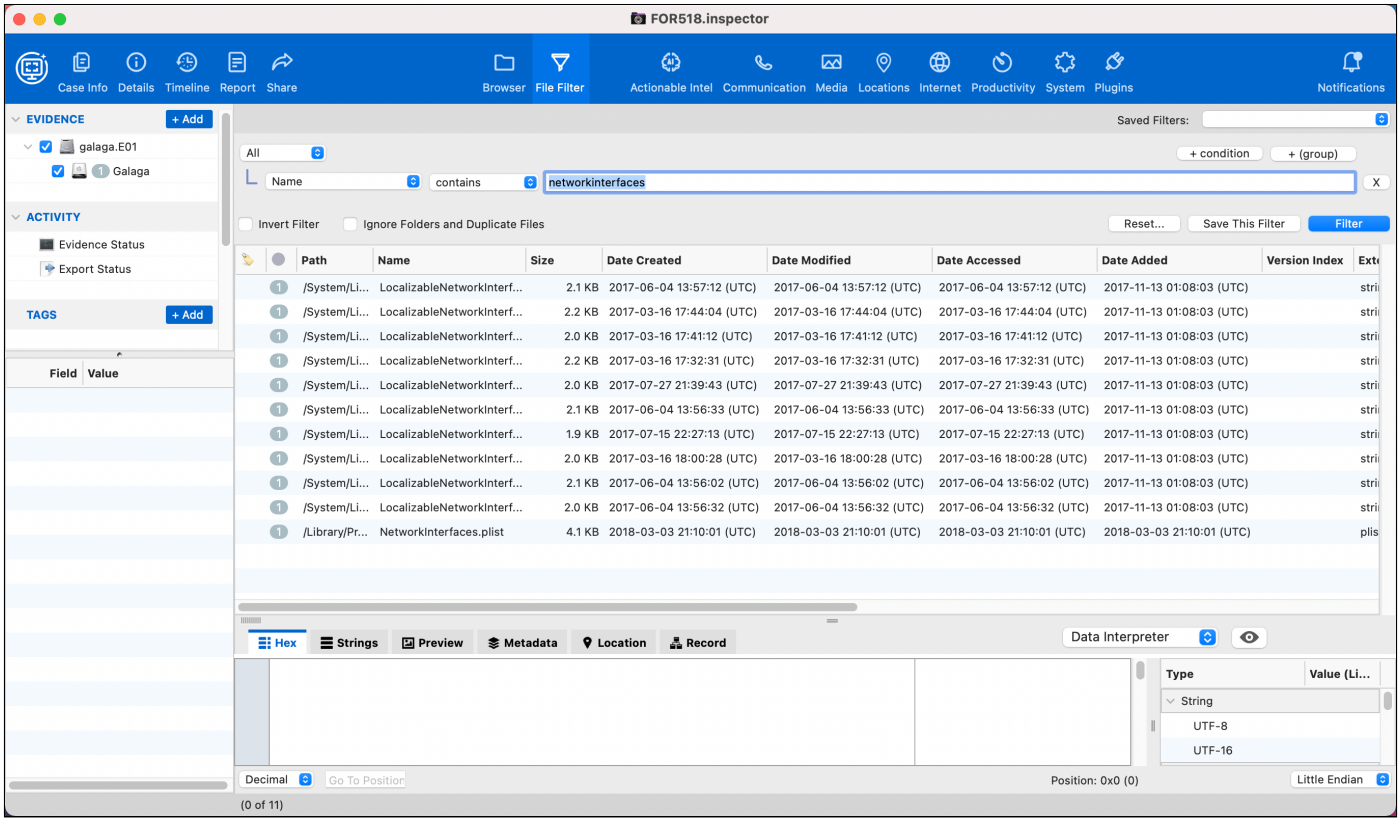
   a. A “right-click” (or two-finger click on a track pad, or control-click) will bring up a context menu as shown below. This menu allows the analyst to perform certain actions such as export information, jump to a file location, or tag a file.

   b. File tagging is similar to bookmarking as seen in other forensic suites. These tags will show up in the left pane under “TAGS”.



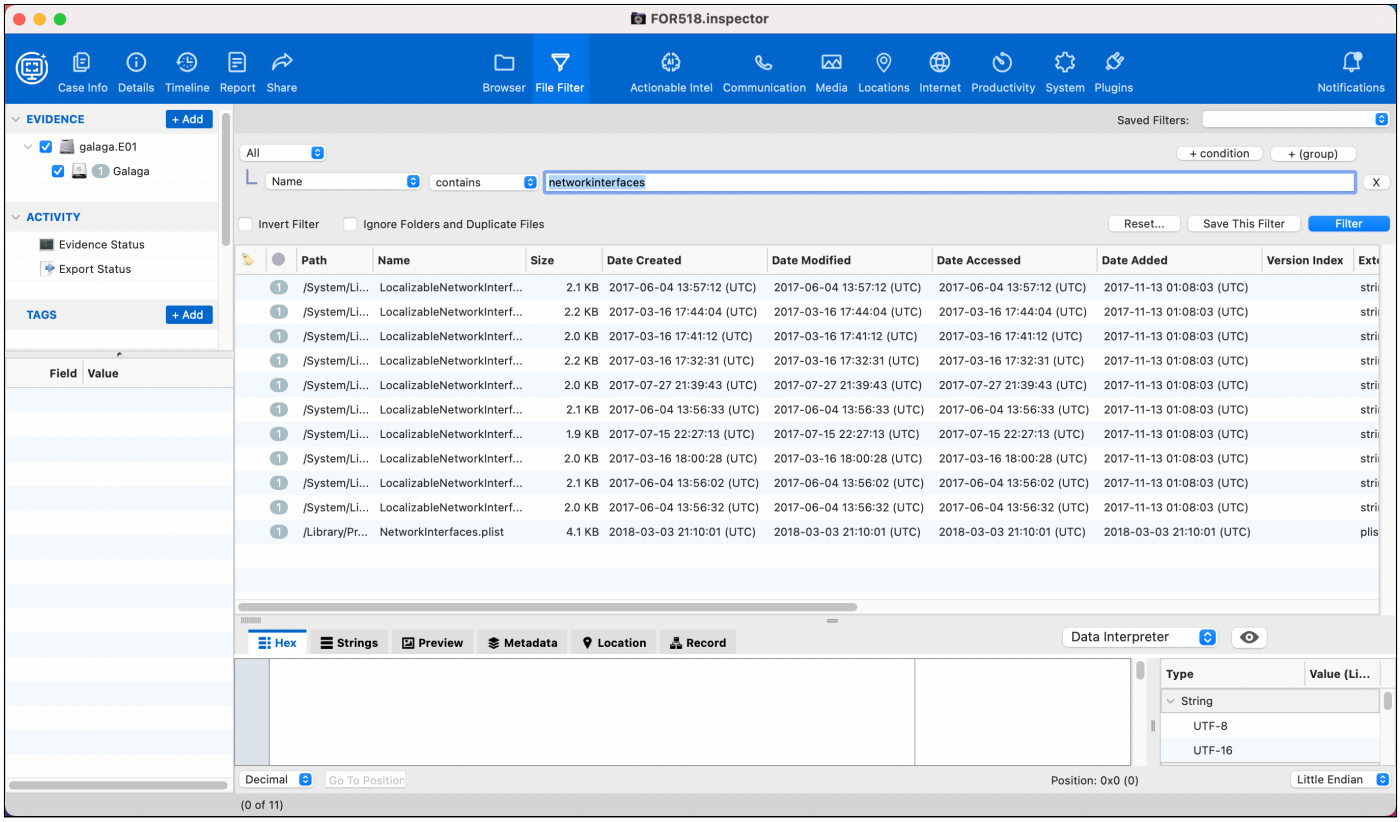
8. **File Filter Tab**

   a. The File Filter tab allows an investigator to select certain files based on some type of data, whether it is size, file type, or by creation date. Many different combinations can be played with. The course author highly recommends spending some time with this feature. It can help you pinpoint specific files quickly.



9. **Artifact Tabs**

   a. Inspector also does some pre-processing when it comes to various popular artifacts. We will be reviewing some of these more in depth during the course labs, but you may start reviewing the contents when you get a free moment.


FOR518.inspector
Case Info
Details
Timeline
Report
Share
Browser
File Filter
Actionable Intel
Communication
Media
Locations
Internet
Productivity
System
Plugins
Notifications
EVIDENCE
+ Add
galaga.E01
Galaga
ACTIVITY
Evidence Status
Export Status
TAGS
+ Add
Field
Value
Saved Filters:
All
+ condition
+ (group)
Name
contains
networkinterfaces
X
Invert Filter
Ignore Folders and Duplicate Files
Reset...
Save This Filter
Filter
Path
Name
Size
Date Created
Date Modified
Date Accessed
Date Added
Version Index
/System/Li... LocalizableNetworkInterf... 2.1 KB 2017-06-04 13:57:12 (UTC) 2017-06-04 13:57:12 (UTC) 2017-06-04 13:57:12 (UTC) 2017-11-13 01:08:03 (UTC)
/System/Li... LocalizableNetworkInterf... 2.2 KB 2017-03-16 17:44:04 (UTC) 2017-03-16 17:44:04 (UTC) 2017-03-16 17:44:04 (UTC) 2017-11-13 01:08:03 (UTC)
/System/Li... LocalizableNetworkInterf... 2.0 KB 2017-03-16 17:41:12 (UTC) 2017-03-16 17:41:12 (UTC) 2017-03-16 17:41:12 (UTC) 2017-11-13 01:08:03 (UTC)
/System/Li... LocalizableNetworkInterf... 2.2 KB 2017-03-16 17:32:31 (UTC) 2017-03-16 17:32:31 (UTC) 2017-03-16 17:32:31 (UTC) 2017-11-13 01:08:03 (UTC)
/System/Li... LocalizableNetworkInterf... 2.0 KB 2017-07-27 21:39:43 (UTC) 2017-07-27 21:39:43 (UTC) 2017-07-27 21:39:43 (UTC) 2017-11-13 01:08:03 (UTC)
/System/Li... LocalizableNetworkInterf... 2.1 KB 2017-06-04 13:56:33 (UTC) 2017-06-04 13:56:33 (UTC) 2017-06-04 13:56:33 (UTC) 2017-11-13 01:08:03 (UTC)
/System/Li... LocalizableNetworkInterf... 1.9 KB 2017-07-15 22:27:13 (UTC) 2017-07-15 22:27:13 (UTC) 2017-07-15 22:27:13 (UTC) 2017-11-13 01:08:03 (UTC)
/System/Li... LocalizableNetworkInterf... 2.0 KB 2017-03-16 18:00:28 (UTC) 2017-03-16 18:00:28 (UTC) 2017-03-16 18:00:28 (UTC) 2017-11-13 01:08:03 (UTC)
/System/Li... LocalizableNetworkInterf... 2.1 KB 2017-06-04 13:56:02 (UTC) 2017-06-04 13:56:02 (UTC) 2017-06-04 13:56:02 (UTC) 2017-11-13 01:08:03 (UTC)
/System/Li... LocalizableNetworkInterf... 2.0 KB 2017-06-04 13:56:32 (UTC) 2017-06-04 13:56:32 (UTC) 2017-06-04 13:56:32 (UTC) 2017-11-13 01:08:03 (UTC)
/Library/Pr... NetworkInterfaces.plist 4.1 KB 2018-03-03 21:10:01 (UTC) 2018-03-03 21:10:01 (UTC) 2018-03-03 21:10:01 (UTC) 2018-03-03 21:10:01 (UTC)
Hex
Strings
Preview
Metadata
Location
Record
Data Interpreter
Type
Value (Li...
String
UTF-8
UTF-16
Decimal
Go To Position
Position: 0x0 (0)
Little Endian
(0 of 11)

Lab 1.2: Exploring iOS Acquisitions

Objectives

- Review the different types of iOS acquisitions, including backups and physical/logical acquisition
- Perform an initial triage analysis

Lab Preparation

1. **Software Preparation:** The following tools will be used in this exercise:
    - Terminal.app
        a. You will be using the native macOS Terminal application for this lab.
        b. Locate and open the Terminal.app from /Applications/Utilities/
    - Inspector.app
        a. Locate and open `/Applications/Inspector/Inspector Release #/Inspector.app`
2. **Exercise File Preparation:**
    - Locate the files located in the `Lab_Images/iPhone/` directory on your FOR518-A ISO file.
3. **Mount David Lightman's Mac Forensic Image** (`galaga.E01`)
    - Mounting Instructions

Lab Questions

Review iOS Files from David's macOS Disk Image

In David's Mac mounted image, navigate to and open the file `/Volumes/galaga_mounted/Users/dlightman/Library/Preferences/com.apple.iPod.plist` and answer the following questions. Note the identifiers: IMEI and Serial Number.

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Preferences/

open com.apple.iPod.plist
```

1. How many times was an iPhone connected to this system while using the "dlightman" user account?

    _____

    Solution

    "Use Count" Key: 14 times

2. When was this iPhone last connected (UTC)?

_____

Solution

"Connected" Key: 03/03/2018 21:10:00 UTC

3. What was the iOS version of the iPhone when it was last connected?

_____

Solution

"Firmware Version String": iOS 11.0.3

4. What is the "human-conversion" make and model of the iPhone (i.e., iPhone X, iPhone 6S+)?

_____

Solution

a. "Product Type": iPhone9,3 = iPhone 7

b. Search for it; this website is good: https://www.theiphonewiki.com/wiki/Models

Navigate to the MobileSync backup directory on David's Mac, located here: `/Volumes/galaga_mounted/Users/dlightman/Library/Application\ Support/MobileSync/Backup/.`

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Application\ Support/MobileSync/Backup/

ls -la
```

5. What are the first few characters of the Universal Device Identifier (UDID) for this backup?

_____

Solution

Each backup is stored in a directory named with its UDID: 01bdc468ee1e1f0bc186d7992314dbe7fdb168ac

Navigate into this iOS backup, review the backup structure, and open the plist metadata files.

```
cd 01bdc468ee1e1f0bc186d7992314dbe7fdb168ac

ls -la

open *.plist
```

- Review the contents of the `Status.plist` file.
- Review the contents of the `Info.plist` file.

6. What is the date of this backup (UTC)?

_____

Solution

"Last Backup Date" Key: 03/03/2018 20:28:06 UTC

7. What is the name of this iPhone?

_____

Solution

"Device Name" or "Display Name": David's iPhone

8. What was the phone number of this device when it was backed up?

_____

Solution

"Phone Number": +44 7848 916073

- Review the contents of `Manifest.plist`

9. Was there a passcode set on the device at the time of backup?

_____

Solution

"WasPasscodeSet" Key: Yes, it had a passcode.

10. Is this backup encrypted or not?

_____

Solution

"IsEncrypted" Key: Yes, this backup is encrypted.

- Navigate to the lockdown directory for this system, `/Volumes/galaga_mounted/private/var/db/lockdown/`. Open the lockdown file/pairing certificate for the connected iPhone.

```
cd /Volumes/galaga_mounted/private/var/db/lockdown/

ls -la

open 01bdc468ee1e1f0bc186d7992314dbe7fdb168ac.plist
```

11. What is the Wi-Fi MAC Address for the connected iPhone?

_____

Solution

"WiFiMACAddress" Key: b8:53:ac:09:cc:86

Extract and Analyze iOS Backup Files from David's macOS Disk Image

Navigate to David Lightman's `Documents` directory. David was smart enough to back up his backups before he jailbroke his iPhone. He created an encrypted and unencrypted version of his iPhone and stored them in the `iPhone_Backups` directory (`/Volumes/galaga_mounted/Users/dlightman/Documents/iPhone_Backups/`).

In the unencrypted backup (`/Volumes/galaga_mounted/Users/dlightman/Documents/iPhone_Backups/unencrypted_iPhone_backup_01bdc468ee1e1f0bc186d7992314dbe7fdb168ac`), copy the `Manifest.db` file to your `~/FOR518` directory and review the contents of the `Manifest.db` file. If you look for this file in the encrypted backups, you'll find that it is… encrypted!

We are copying out this file because `sqlite3` (via command line) and DB Browser for SQLite application cannot open the file on a read-only volume. This is something you will have to do quite often to access the SQLite databases outside of another application like Inspector.

Use whichever tool you prefer to open the `Manifest.db` database and review its contents.

```
cd /Volumes/galaga_mounted/Users/dlightman/Documents/iPhone_Backups
unencrypted_iPhone_backup_01bdc468ee1e1f0bc186d7992314dbe7fdb168ac/

cp Manifest.db ~/FOR518
```

1. In the "Files" table, what is the `fileID` hash of the `sms.db` database?

   _____

   Solution

   a. 3d0d7e5fb2ce288813306e4d4636395e047a3d28

   b. You can run a query on the database such as:

   ```
   select * from Files where relativePath like "%sms.db%"
   ```

   c. In DB Browser for SQLite, you can filter for "sms.db" in the `relativePath` column area.

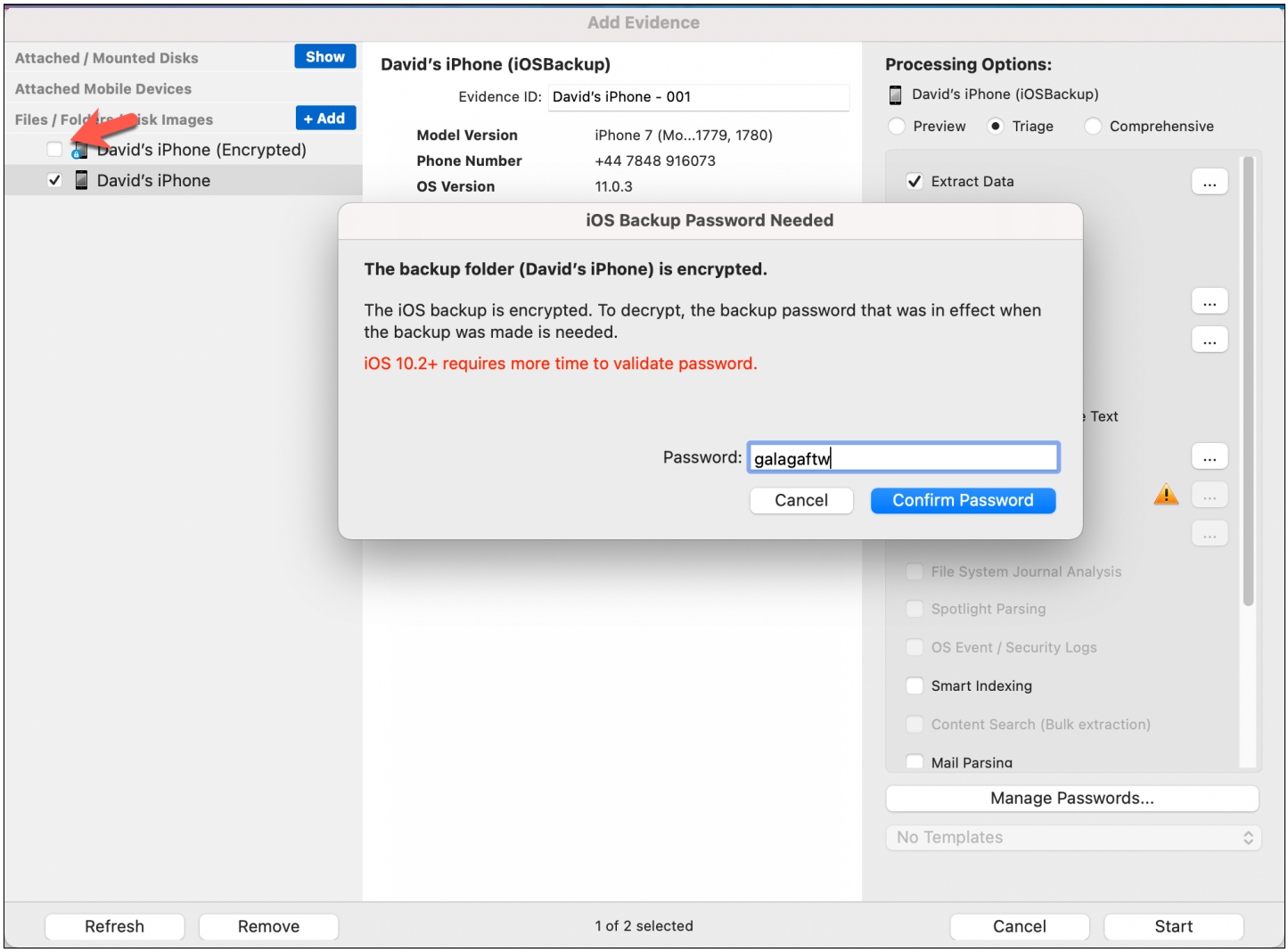
Extract both backups to your `~/FOR518` directory.

```
cd /Volumes/galaga_mounted/Users/dlightman/Documents/

cp -R iPhone_Backups/ ~/FOR518
```

Import these backups into your FOR518 Inspector Case File.

- Select the "Add" Evidence button.
- Select the "Add" button under "Files/Folders/Disk Images".
- Navigate to where you saved the backups (~/FOR518).

- Select each backup directory (separately). For the backup labeled “encrypted,” you’ll have to input the backup password by clicking the checkbox. The backup password is " `galagaftw` ". Please be patient; as stated in the pop-up window, this will take a bit of time.
- Once each backup is imported into the "Add Evidence" window, select both backups, keep the default "Ingestion Options" and select "Start" to add them to the Case File.



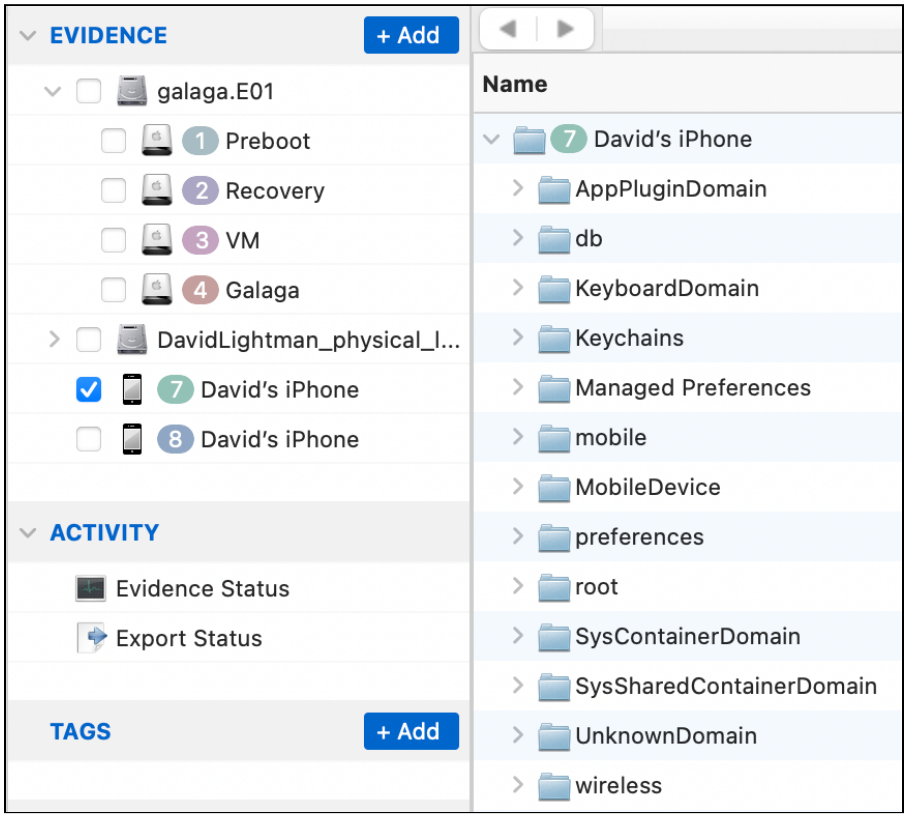
Once imported, both backups will be labeled "David’s iPhone"; let's figure out which one is encrypted and take note which evidence number is the encrypted and unencrypted backup.

Select any backup and go to the "File Filter" section of Inspector. Look for the `healthdb.sqlite` database file (FYI: This file keeps track of all the health-related data for the user; however, it is only backed up when the user performs an encrypted backup).

- In the "File Filter," select the "List all Files" dropdown and select "Name".
- In the next dropdown, select "contains".
- In the text field, type " `healthdb.sqlite` ".
- Select "Filter". If the database exists, that is the encrypted backup. If it does not, it is the unencrypted backup.

• Make a note of which evidence item is the encrypted backup versus the unencrypted backup.

Going back to the "Browser" view for each backup, review how the backup files have been "normalized" from what you saw when you looked at the backup in its "raw" format.



Analyze the "Logical Physical" iOS Acquisition

In your FOR518 /Lab_Images/iPhone/ directory, there is a "Physical/Logical" dump of David's jailbroken iPhone (`DavidLightman_physical_logical_dump.dmg`).

This dump was created from the jailbroken iPhone, using the SSH/TAR combination to acquire all the physical files in an "unlocked" state. This TAR bundle was then uncompressed and stored in a DMG file, using the Disk Utility.app application for easy transport and mounting.

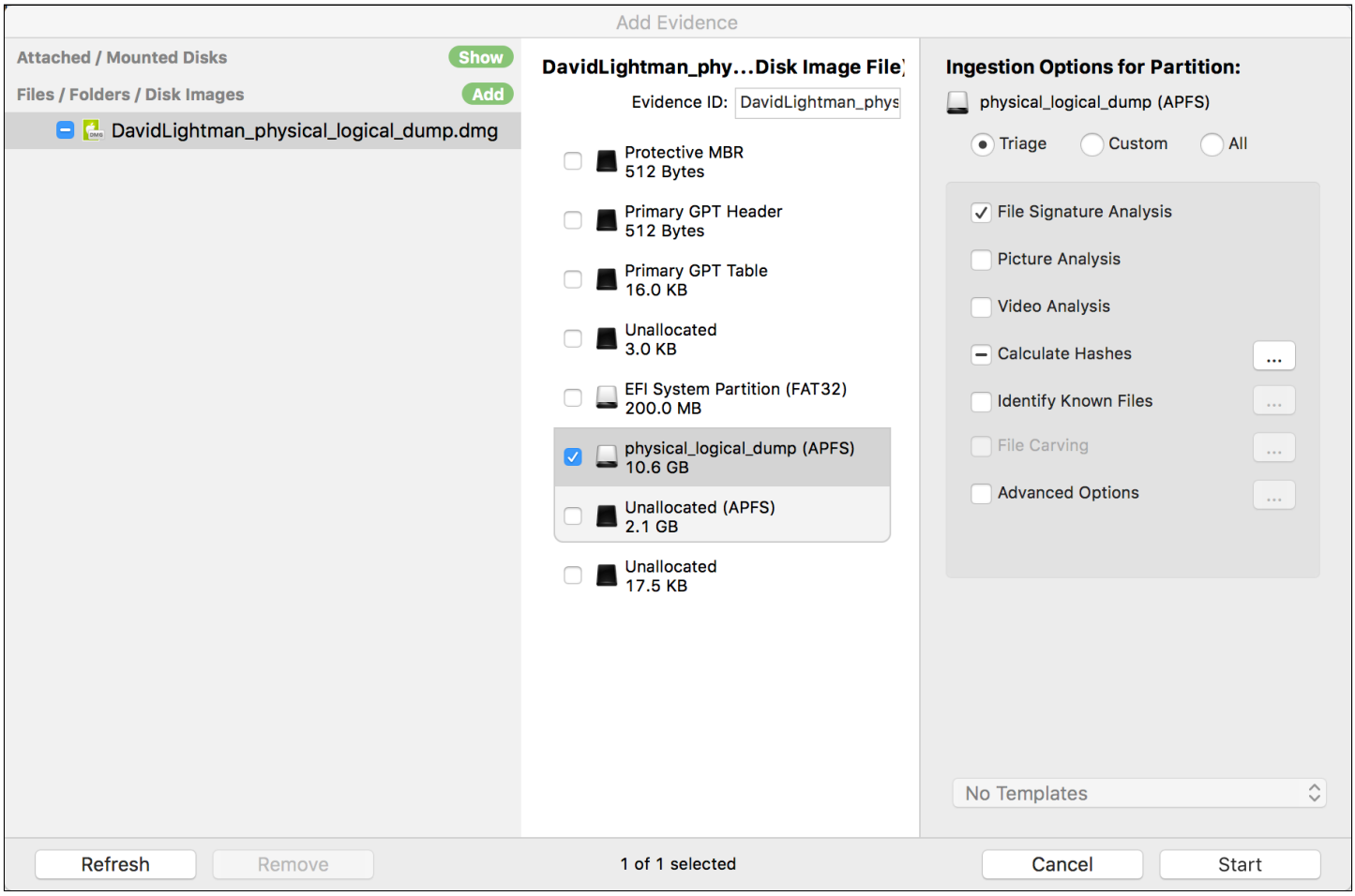
You may choose to import this DMG into Inspector, using or mounting it within the Terminal (or both, your choice!). Follow the instructions for at least one method below:

Terminal Mount: Follow nearly the same procedure as the disks mounted previously. Select the partition labeled "41504653-0000-11AA-AA11-0030654" for the `mount_apfs` command. If you perform a `diskutil list`, it will show up as an APFS volume named "`physical_logical_dump`".

```
sudo mkdir /Volumes/davids_iphone/

hdiutil attach -nomount DavidLightman_physical_logical_dump.dmg
```

```
sudo mount_apfs -o rdonly,noexec,noowners /dev/disk#s# /Volumes/davids_iphone/
```

Import into Inspector: Follow the steps above when importing the iOS backup directories. For the DMG, de-select "`EFI System Partition (FAT32)`". We will only be looking at the volume labeled "`physical_logical_dump`". Default "Ingestion Options" are ok to keep.



Take a moment to peruse the structure of this "Physical/Logical Acquisition".

- Note the contents of `/jb/` on the root of the file system, this is one of the artifacts left behind for the LiberiOS jailbreak.

Take a look at the matching Lockdown records located in `/private/var/root/Library/Lockdown/`

1. What was the name of the computer that last backed up this device (data_ark.plist)?

   _____

   Solution

   "com.apple.iTunes.backup-LastBackupComputerName" Key: "David's MacBook Pro"

2. What type of system was it? (Mac or Windows?)

Solution

"com.apple.iTunes.backup-LastBackupComputerType" Key: Surprise! It was a Mac! (Couldn't see that one coming!)

Review the following files and their locations in all the different iOS acquisitions

Note

Some files are there; some aren't!

- **Health Database**
  a. Physical Logical: `/private/var/mobile/Library/Health/healthdb.sqlite`
  b. Encrypted Backup: `/mobile/Library/Health/healthdb.sqlite`
  c. Unencrypted Backup: Does not exist!
- **Keychain**
  a. Physical Logical: `/private/var/Keychains/`
  b. iOS Backups: `/Keychains/`
- **Location Data**
  a. Physical Logical: `/private/var/root/Library/Caches/locationd/cache_encrypted*`
  b. iOS Backups: `/root/Library/Caches/locationd/`

Lab: Key Takeaways

- **Notice the differences between each type of iOS acquisition.**
- **Get comfortable with the key areas in which to find initial triage data for the device being analyzed.**

Lab 1.3: Disks and Partitions

Objectives

- Review the disks and partitions on your analysis system.

Lab Preparation

> **Note**
>
> Some of this might already be accomplished via earlier labs, but this is the state that we hope your system is in prior to the start of this lab. Just in case your system rebooted, we are including a guide to help you get back to the proper analysis starting point prior to the beginning of this lab.

1. **Software Preparation:** The following tools will be used in this lab:
    - Terminal.app
        a. Locate and open the native macOS Terminal.app from /Applications/Utilities/.
2. **FOR518 Reference Sheet:** Locate the FOR518 Reference Sheet provided to you in your class material and books. The PDF format of this sheet is available on your FOR518-A ISO file.

Lab: Questions

1. **Run the `diskutil list` command**
    - Use the `diskutil list` command to view the disks and partitions on your analysis system.

```
diskutil list
```

2. **Run the diskutil info command on a couple of disks**

```
diskutil info disk#
```

3. **Run the diskutil info command on a couple of partition slices**

```
diskutil info disk#s#
```

4. **Run the diskutil ap list command**

```
diskutil ap list
```

Lab: Key Takeaways

- **There are many command-line utilities on macOS to view disks and partitions.**

Lab 2.1: Mac and iOS Triage

Objectives

- Review files that can provide triage information.
- Get familiar with the MacOS command line and Inspector.

Lab Preparation

Note

Some of this might already be accomplished via earlier exercises, but this is the state that we hope your system is in prior to the start of this exercise. Just in case your system rebooted, we are including a guide to help you get back to the proper analysis starting point prior to the beginning of this exercise.

1. **Software Preparation**: The following tools will be used in this exercise:
    - Terminal.app
        a. Locate and open the native macOS Terminal.app from /Applications/Utilities/.
    - Xcode.app
        a. Locate and open the Xcode.app from /Applications/.
    - SQLite Database Browser
        a. You will be using the SQLite Database Browser (Applications/sqlitebrowser.app)
        b. This tool is available on your FOR518-A ISO file in the Tools directory.
        c. The SQLite Manager is available at http://sqlitebrowser.org/
    - Inspector.app
        a. Locate and open the Inspector.app from /Applications/Inspector Release #/Inspector.app
        b. This tool is available on your FOR518-A ISO file in the Tools directory.
2. **FOR518 Reference Sheet**: Locate the FOR518 Reference Sheet provided to you in your class material and books. The PDF format of this sheet is available on your FOR518-A ISO file.
3. **Open the FOR518.inspector Inspector Case file.**
4. **Mount David Lightman's Mac forensic image** (`galaga.E01`).
    - Mounting Instructions
5. **Mount David Lightman's Physical Logical iPhone DMG** (`DavidLightman_physical_logical_dump.dmg`)
    - Mounting Instructions

Lab: Questions

Mac Triage

Perform the following in David's mounted image on the command line:

Mac Version Information

Use the `cd` command to navigate to the `CoreServices` directory.

Use the `open` command to open the `SystemVersion.plist` file.

```
cd /Volumes/galaga_mounted/System/Library/CoreServices

open SystemVersion.plist
```

1. What version of macOS is this system running?

_____

Solution

`ProductVersion` Key = 10.13.1

System Installation Date

Use the `cd` command to navigate to the `/private/var/db` directory

Use the `ls -la` command to view all the files in this directory

```
cd /Volumes/galaga_mounted/private/var/db/

ls -la
```

1. What is the likely date of system installation?

_____

Solution

- November 13, 2017 (UTC)
  a. Use the `stat -x` command to determine MAC times for .AppleSetupDone and `.AppleInstallType.plist` files.
  b. To view the UTC/Unix Epoch timestamps, use `-r` instead of `-x` .
  c. Change your terminal time zone to UTC temporarily using this command: `export "TZ=UTC"`

System Time Zone and Language Settings

Use the `cd` command to navigate to the `/etc` directory.

Use the `ls -l` command to view all the files in this directory. Note the contents of this directory.

Use the `ls -l` command on the `localtime` file.

```
cd /Volumes/galaga_mounted/etc/

ls -l

ls -l localtime
```

1. What time zone is in use on this system?

   _____

   Solution

   America/New_York

Review the user property list for user `dlightman`

Get a root shell (`sudo -s`).

Change directory to view the user property lists on the system.

- `/Volumes/galaga_mounted/private/var/db/dslocal/nodes/Default/users`

Using the `cp` command, copy the `dlightman.plist` property list to a directory of your choice.

Use the `chown` command to change the ownership to your user account name.

VERY IMPORTANT: Exit the root shell.

Use the open command to open and view the `dlightman.plist` property list in Xcode.

```
sudo -s

cd /Volumes/galaga_mounted/private/var/db/dslocal/nodes/Default/users

cp dlightman.plist ~/FOR518

chown <your username> ~/FOR518/dlightman.plist

exit

open -a Xcode ~/FOR518/dlightman.plist
```

Review the `dlightman` 's user property list.

1. What is the user's "Real Name"?

   _____

Solution

`realname` Key = David Lightman

2. What is the path to the user's home directory?

_____

Solution

`/Users/dlightman`

3. What is the user's UID (User ID)?

_____

Solution

`uid` Key = 501

4. What is the user's linked iCloud identity?

_____

Solution

- d.l1ghtm4n@gmail.com
- Extract the contents of the `LinkedIdentity` Key into a text viewer. Review the contents of the "full name" key of this embedded XML plist file.

5. When was this user account created (Hint: `accountPolicyData` Key)?

_____

Solution

- 2017-11-13 01:26:28 Mon UTC
- Extract the contents of the `accountPolicyData` Key, input into a hex editor, and save as a .plist file. Open the plist file in Xcode.
- 10.15 users can use the PlistBuddy instead in a couple different ways.
  a. XML Output: `/usr/libexec/PlistBuddy -c Print: accountPolicyData dlightman.plist`
  b. Plutil Output:
  `/usr/libexec/PlistBuddy -c Print: accountPolicyData:0 dlightman.plist | plutil -p -`
- The `creationTime` key holds the time the account was created: copy the first 10 digits (1510536388, remove the commas), and convert it in the Terminal with `date -r 1510536388`.

Review the time zone and language settings for `dlightman`

Use the `cd` command to navigate to the system preferences directory.

- `/Volumes/galaga_mounted/Library/Preferences`

Use the `ls -la` command to view all files in this directory. Note the contents of this directory.

Use the `open` command to open the `.GlobalPreferences.plist` file.

```
cd /Volumes/galaga_mounted/Library/Preferences

ls -la

open .GlobalPreferences.plist
```

1. What city is used to determine the time zone used?

   _____

   Solution

   Arlington

   - `com.apple.TimeZonePref.Last_Selected_City` Key

2. What are the location coordinates? Do they match up with the city listed?

   _____

   Solution

   Yes, they do. 38.89076, -77.08475 = Arlington, VA

3. What is the primary language setting used?

   _____

   Solution

   en_US: US English

   - `AppleLocale` or `AppleLanguages` Keys

Network Settings

Use the `cd` command to navigate to the `SystemConfiguration` directory.

Use the `ls -la` command to view all files in this directory. Note the contents of the directory.

Use the `open` command to open all the plist files in this directory.

```
cd SystemConfiguration/

ls -la

open *.plist
```

Review the `NetworkInterfaces.plist` file.

1. What model system is this?

   _____

Solution

MacBookPro11,1

2. What is the MAC address for the Wi-Fi interface?

_____

Solution

- `<b8e85637 ec06> = b8:e8:56:37:ec:06`
- `Item 0 | IOMACAddress` Key for the interface labeled `en0, IEEE80211` and/or `Wi-Fi`.

Review the `com.apple.airport.preferences.plist` file.

1. How many "remembered" Wi-Fi networks are there?

_____

Solution

- Three
- Number of items under `KnownNetworks` Key

2. Provided all Wi-Fi networks are available, which is the name of the first access point to be connected to via user configuration?

_____

Solution

- `CrystalPalace`
- The `PreferredOrder` key contains the order in which each will be connected. Item 0 is the most preferred.
- Take the key "`wifi.ssid.<43727973 74616c50 616c6163 65>`" and match it with the entry under `KnownNetworks` to find `CrystalPalce` in the key `SSIDString`.

3. What is the name of the network that was last accessed on January 21, 2018 (UTC)?

_____

Solution

- `schmoocon`
- Look for the `LastConnected` Key timestamp under each access point.

4. Which access point has WPA2 Personal security implemented?

_____

Solution

- `CrystalPalace`
- `SecurityType` key contains WPA2 Personal (versus Open)

Determine what IP Address this system had at the time of collection. Navigate to the `leases` directory.

```
cd /Volumes/galaga_mounted/private/var/db/dhcpclient/leases/

ls -la

plutil -p en0-1\,b8\:e8\:56\:37\:ec\:6
```

1. When this system was last connected to `CrystalPalace`, what was its IP address?

   _____

   Solution

   - 192.168.101.138
   - `IPAddress` Key

iOS Triage

- **Perform the following in David's iPhone images in Inspector:**

iOS Device Information

In David's iPhone, select the "physical_logical" acquisition.

Review the `general.log` file located in either of the following paths: `/private/var/logs/AppleSupport/general.log` / `private/var/mobile/Library/Logs/AppleSupport/general.log`

1. What version of iOS is this phone running?

   _____

   Solution

   11.0.3

2. What is the serial number of this phone (last four digits)?

   _____

   Solution

   C6KSC32BHG7L Last 4 digits: **HG7L**

3. Model of the Phone: translate "comma'ed" make/model into a commercially known model.

   _____

   Solution

   iPhone9,3 = iPhone 7

Review the file at `/private/var/containers/Data/System/BB422B72-4829-4993-ABC7-3D6E54E01FBE/Library/activation_records/activation_record.plist`

1. What are the last four digits of the IMEI?

   _____

   Solution

   359204070808925 Last 4 digits: **8295** (extract the `AccountToken` Key)

Now select any of David's iPhone acquisitions.

Review the file at [`private/var`] `/wireless/Library/Preferences/com.apple.commcenter.plist` file.

1. What was the phone number of this device when it was imaged?

   _____

   Solution

   `NetworkPhoneNumber` Key = `+447848916073`

2. What is the ICCID number for the device (last four digits)?

   _____

   Solution

   `ICCID` Key = `8944200116623054965`

3. Who was the provider of the device at the time of acquisition?

   _____

   Solution

   `CarrierBundleName` Key = 23420 (MCC = 234, MNC = 20) = The "3" Network. Look this up on https://www.mcc-mnc.com/

Now select any of David's iPhone acquisitions.

Review the file at [`private/var`] `/mobile/Library/Preferences/com.apple.purplebuddy.plist`

1. On what day was this device likely setup?

   _____

   Solution

   November 12, 2017 (Review the `GuessedCountry` "at" time, or `SetupLastExit` Key.)

Network Settings

Select any of David's iPhone acquisitions.

Review the [`private/var`] `/preferences/SystemConfiguration/com.apple.wifi.plist` file

1. How many "known" Wi-Fi networks are there?

   _____

   Solution

   - 18
   - " `List of known networks` " Keys

2. On what day was " `Fly Dulles` " last potentially used (local system time)?

   _____

   Solution

   February 11, 2018 (Check the `lastJoined` and `LastAutoJoined` keys.)

Exercise: Key Takeaways

- **Determine where triage information is stored for Mac and iOS devices.**
- **Get comfortable with some MacOS command lines.**
- **Get comfortable with the Inspector application interface and nuances.**

Lab 2.2: File System Fun!

Objectives

- Learn how the file system metadata can be found in different files and databases.
- Find various ways to look for forensic artifacts that may be useful in an investigation that are not common to other systems other than Mac and iOS.

Lab Preparation

> **Note**
>
> Some of this might already be accomplished via earlier Labs, but this is the state that we hope your system is in prior to the start of this Lab. Just in case your system rebooted, we are including a guide to help you get back to the proper analysis starting point prior to the beginning of this exercise.

1. **Software Preparation**: The following tools will be used in this Lab:
    - Terminal.app
        a. Locate and open the native macOS Terminal.app from /Applications/Utilities/.
    - Xcode.app
        a. Locate and open the Xcode.app from /Applications/.
2. **FOR518 Reference Sheet**: Locate the FOR518 Reference Sheet provided to you in your class material and books. The PDF format of this sheet is available on your FOR518-A ISO file.
3. **Mount David Lightman's Mac forensic image** (`galaga.E01`).
    - Mounting Instructions

Lab Questions

Perform the following in David's mounted image on the command line

Extended Attributes

Review the `dlightman's` Downloads directory for Extended Attributes

Use the `cd` command to change the directory to the `dlightman` 's Downloads directory.

```
cd /Volumes/galaga_mounted/Users/dlightman/Downloads/

ls -l
```

1. When was the file "`Firefox 58.0.2.dmg`" downloaded? (UTC)?

_____

Solution

a. Use "`xattr -xl" on the files to get the extended attributes.

b. The timestamps are located in the following attributes:

   i. `com.apple.metadata:kMDItemDownloadedDate` in the binary `plist` file

   ii. `com.apple.quarantine` (type `date -r 0x5a931512` in the Terminal to see the result of 2018-02-25 19:57:06 Sun UTC)

c. It is far easier to get the date from `com.apple.quarantine` than it is to extract the binary `plist` from an extended attribute—but it's good to have other options when needed.

2. What browser application downloaded the file "`Firefox 58.0.2.dmg`"?

_____

Solution

`com.apple.quarantine` attribute: Safari

3. Which file was transferred to the system via a Messages File Transfer?

_____

Solution

a. `ms-nAphDJ.gif`

b. Using "`xattr -xl *`" on all the files, look for the following attributes:

   i. `com.apple.metadata:kMDItemWhereFroms` - This contains a binary plist that shows the file was transferred from 1337jmack@gmail.com via Messages file transfer.

   ii. `com.apple.quarantine` - This contains the application that downloaded the file Messages.app.

4. Which DMG file in the Downloads directory was the only one NOT double-clicked and opened?

_____

Solution

a. Using "`xattr -xl *.dmg`", look for the attributes `com.apple.diskimages.fsck` and `com.apple.diskimages.recentcksum`, which indicate that a DMG was opened.

   i. The only DMG file that was not opened was `Firefox 58.0.2.dmg`. `Impactor_0.9.44.dmg` and `googlechrome.dmg` were both opened.

File System Events Store Database (FSEvents)

Review the `dlightman's` File System Events Store Database.

Use the `cd` command to change directory to the `dlightmans`'s . `fseventsd` directory.

List the Files with the `ls` command.

Determine the file types with the `file` command.

```
cd /Volumes/galaga_mounted/.fseventsd

ls -l

file *
```

Locate the FSEParser python script in your lab files for this Lab. Use it to parse these files. **Be sure to check your file paths; the location of the FSEParser script will likely be different depending on where you unarchived your lab files. Note: There is no space before ".fsevents".**

- "-t" is for what type of evidence, we will be using 'folder' here.
- "-s" is for the source directory (the directory you are currently in).
- "-o" is for the output directory, your FOR518 directory.

Move into the ~/FOR518 directory and review the file output from the script. The files are in a directory named `FSE_Reports/`. Find the one starting with the file name, "FSEvents.sqlite". You should see a text file, a TSV file, and one SQLite database.

Open the database for analysis using a SQLite viewer. The SQLite database browser is being used as an example below.

```
python ~/FOR518/Lab_Files/Lab\ 2.2\ -\ File\ System\Fun/FSEventsParser-master/
FSEParser_v4.0.py -t folder -s /Volumes/galaga_mounted/.fseventsd -o ~/FOR518/

cd ~/FOR518/FSE_Reports/

ls -l ~/FOR518/

open -a "DB Browser for SQLite" FSEvents.sqlite
```

Use the filters in SQLite Browser to search for mounted volumes. In the "Browse Data" tab, type in " `/Volumes` " in the " `fullpath` " column. Review the mounted Volumes.

Now search for DMG files on the system; focus on `dlightman`'s Desktop directory.

1. What two DMG files were located on `dlightman`'s Desktop (not inside of a sub-directory of the Desktop)?

   _____

Solution

a. Filter on "`/dlightman/Desktop/`" in the "`fullpath`" column. You can filter on file extension by typing "`dmg`" in the "`filename`" column.

b. `kl.dmg` and `kl2.dmg`

2. Are these two separate files or one file that was renamed (hint: look at the CNID in "`node_id`" column)?

Solution

a. The CNIDs for these files are different; therefore, they are two separate DMG files that are similarly named.

i. `kl.dmg` = 1529172

ii. `kl2.dmg` = 1529237

Search for the file IMG_0030.JPG using an SQLite query in the "Execute SQL" tab.

```
select * from fsevents where fullpath like '%IMG_0030.JPG%'
```

1. How do you think this file ended up on `dlightman`'s system (staring in February 2018)?

Solution

a. Looking at entry #2349120, it shows that it was "shared" via the `sharingd` process.

b. This file was shared via AirDrop from Jen Mack's iPhone; take a look at the extended attributes for this file, "`xattr -xl /Volumes/galaga_mounted/Users/dlightman/Documents/IMG_0030.jpeg`".

c. This file was originally downloaded into the user's Downloads directory, then opened with Preview App (a couple of times), edited, and finally moved/saved into the users Documents directory.

2. This picture was later edited by David Lightman; what software did he use to edit it?

Solution

a. There are multiple entries that suggest that this file was edited by "Preview.app".

b. "`(A Document Being Saved By Preview)`"

i. 2434304

ii. 2435655

iii. 2436512

iv. 2437481

v. 2438373

vi. 2438398

Search activity for a file using the iNode/CNID 1417428.

```
select * from fsevents where node_id == 1417428
```

1. What browser downloaded this file?

Solution

Safari: Looking at entry # 1093597, it shows that it was "`(A Document Being Saved By Safari)`"; this can be validated by extended attributes.

2. This file was downloaded to the default downloads directory (`~/Downloads`); where did it move later?

Solution

`/Users/dlightman/Documents/games/asteroids_1b.pdf` , Entry #2881049

Search for a file `ms-nAphDJ.gif` .

```
select * from fsevents where filename == "ms-nAphDJ.gif" order by id
```

1. Where did this file come from?

Solution

a. It was an attachment in Messages; it was sent in a chat. It was later downloaded to the default downloads directory.

b. See records:

i. 2344842

ii. 2882654

iii. 2882668

Spotlight

Review dlightman's Spotlight Directory

Use the `cd` command to enter the Spotlight directory.

Use the `ls -la` command to view the contents of this directory. Review the contents of this directory. Go ahead and browse through the other directories to see all the files associated with Spotlight

```
cd /Volumes/galaga_mounted/.Spotlight-V100

ls -la
```

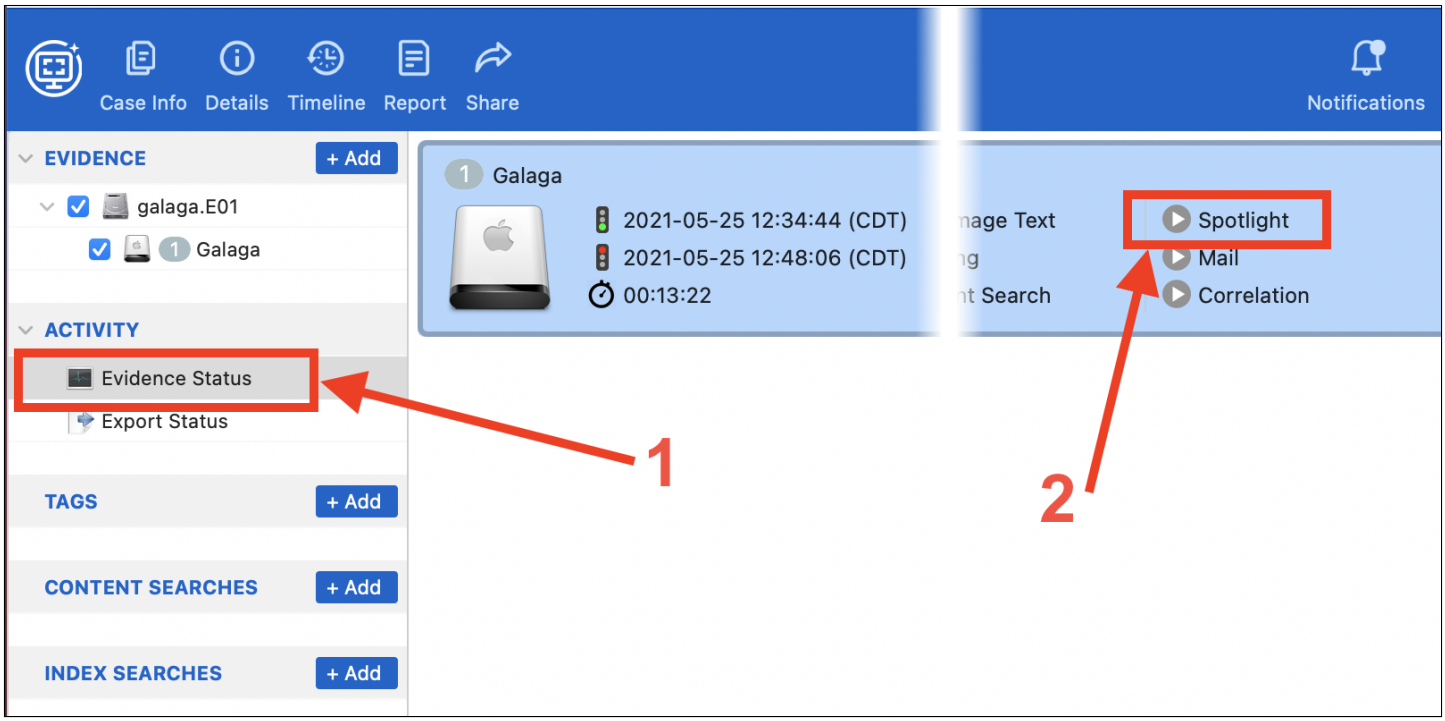
Spotlight: Review the Spotlight Metadata

Use the `cd` command to explore the `dlightman` 's `~/Downloads` directory.

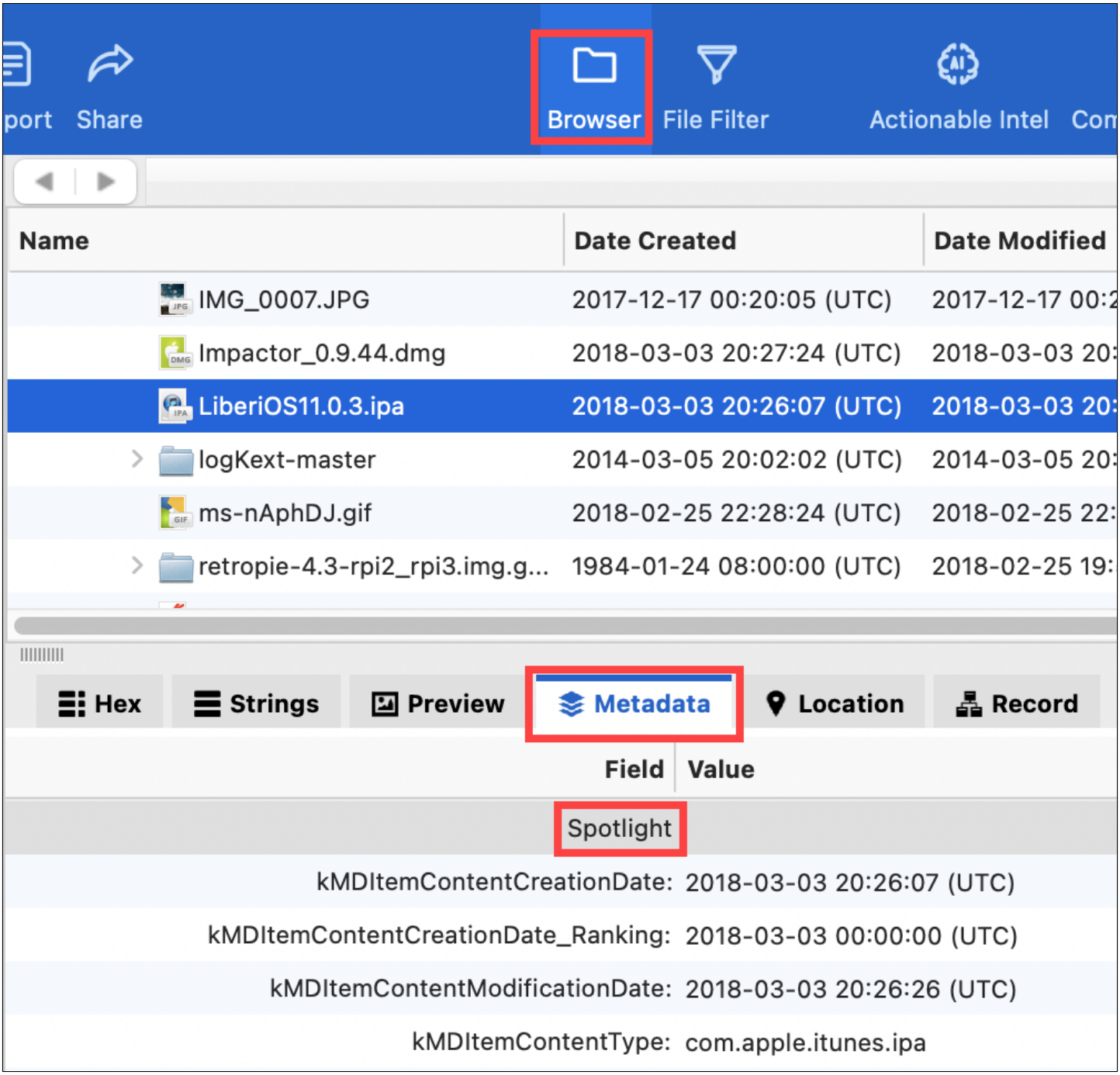
Use the `mdls` command to view the files in this directory. Answer the following questions(some students may need to use "`sudo`" with the `mdls` command).

Students on macOS 11 (Big Sur) or newer will not be able to answer these questions using this method. For students using macOS 11+, please use the instructions below:

- Open your existing case file in Inspector. Click on **Evidence Status** (1) and then, on the **Galaga** image. Click on the grey play button next to Spotlight (2) to start indexing Spotlight data. This will take several minutes to complete. You may have already done this in Lab 1.1.



- Once the Spotlight data has been indexed, go to the **Browser** in Inspector. As you highlight specific files, the Spotlight data can be seen in the **Metadata** tab in the lower pane (you will need to scroll down to find it).




```
cd /Volumes/galaga_mounted/Users/dlightman/Downloads/

mdls LiberiOS11.0.3.ipa     # <--Repeat as necessary for each file
```

1. Where was the file `LiberiOS11.0.3.ipa` downloaded from?

_____

Solution

a. `kMDItemWhereFroms` = http://newosxbook.com/liberios/

b. The same information is found in the Quarantine Extended Attribute.

2. On what day did the file `Impactor_0.9.44.dmg` get used last?

_____

Solution

a. `kMDItemUsedDates` (more general) = 03/03/2018

b. `kMDItemLastUsedDate` (more specific) = 2018-03-03 20:27:35 +0000

3. Please answer the following on the file `IMG_0007.JPG` :

a. How did the file get transferred to this system?

_____

Solution

`kMDItemUserSharedReceivedTransport` = AirDrop

b. From whom?

_____

Solution

i. `kMDItemUserSharedReceivedSender` = Jen Mack

ii. `kMDItemUserSharedReceivedSenderHandle` = 1337jmack@gmail.com

iii. `kMDItemWhereFroms` = Jen Mack's iPhone

c. When?

_____

Solution

`kMDItemUserSharedReceivedDate` = 2018-02-25 22:31:57 +0000

d. What is the Make/Model of the phone?

_____

Solution

i. `kMDItemAcquisitionMake` = Apple

ii. `kMDItemAcquisitionModel` = iPhone 6

e. What version of iOS was it running?

Solution

`kMDItemCreator` = 11.0.1

f. Does this photo have location coordinates?

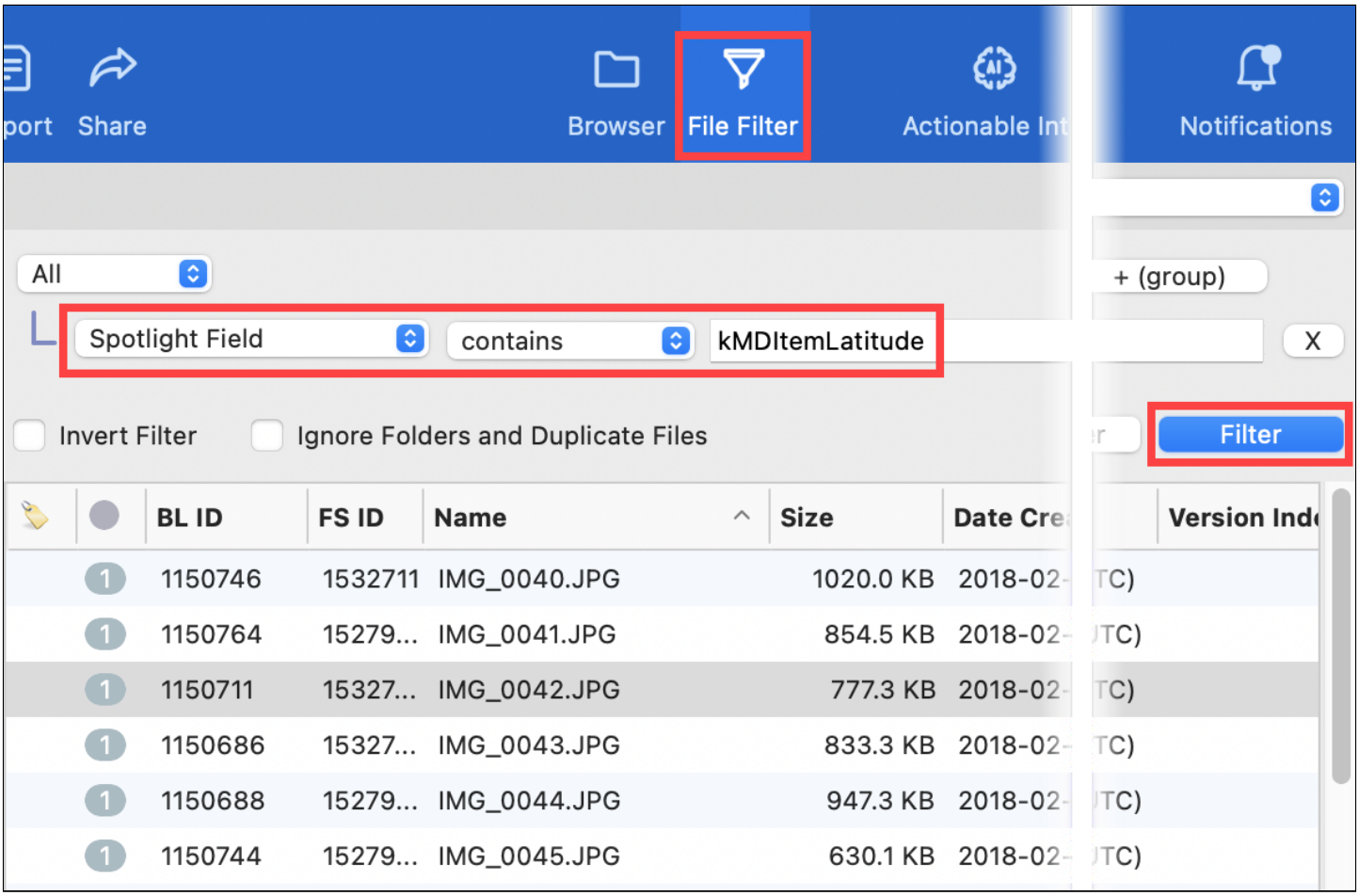
Solution

No.

Find photos that have locational data in them.

Use the `"mdfind"` command to search `“-onlyin”` in the mounted volume for David Lightman.

- Students on macOS 11 (Big Sur) or newer will not be able to perform this command on the mounted Galaga volume, but Inspector can be used to the same effect as long as you have followed the steps above to index the Spotlight data.
- Go to the **File Filter** in Inspector. Change the default filter to **Spotlight Field -> contains -> kMDItemLatitude** and then click on the blue **Filter** button. The results will be displayed in the bottom pane.



Search for items containing the metadata item for latitude.

Find the path for the photo `IMG_0042.JPG` and perform an `mdls` on it (some students may need to use "`sudo`" with the `mdls` command).

- Students on macOS 11 (Big Sur) or newer will need to reference the indexed Spotlight metadata in Inspector as explained earlier in the exercise.

```
mdfind -onlyin /Volumes/galaga_mounted/ -name "kMDItemLatitude == *"

mdls "/Volumes/galaga_mounted/Users/dlightman/Library/Containers/com.apple.cloudphotosd/Data/
Library/Application Support/com.apple.cloudphotosd/services/
com.apple.photo.icloud.sharedstreams/assets/66B292A9-9F24-4889-913C-1A90395F2338/
E17A868C-9AF1-4DED-802A-A9F7655F4065/IMG_0042.JPG"
```

1. What are the coordinates for IMG_0042.JPG?

   _____

   Solution

   a. Latitude: `kMDItemLatitude` = 51.51343

   b. Longitude: `kMDItemLongitude` = -0.099358

2. In what major landmark was this photo taken?

   _____

   Solution

   a. St. Paul's Cathedral

   b. Plug these coordinates into Google Maps, Apple Maps, etc. or…

   c. Open the photo in the Preview application and open the Inspector [Tools | Show Inspector]

      i. Select the GPS tab and zoom in.

Trash

Review the dlightman's Trash.

Use the `cd` command to change directory to the `dlightman's .Trash` directory.

Use the `ls -la` command to view the contents of this directory.

```
cd /Volumes/galaga_mounted/Users/dlightman/.Trash

ls -la
```

1. What three files are in the trash?

   _____

_____

_____

Solution

a. `ApplePi-Baker.zip`

b. `Spectacle+1.2.zip`

c. `logKext-master 2`

2. Where did some of these files once exist?

_____

Solution

a. `/Users/dlightman/Downloads` directory

b. View the `.DS_store` file in a Hex Editor or use `xxd` on the command line.

   i. `xxd .DS_Store | less`

c. Note that the file `Spectacle+1.2.zip` did not exist in the `.DS_Store` file—it's not a perfect system.

Lab: Key Takeaways

- **Review the contents of files and databases that contain data that use the file system.**
- **Find that different files may contain metadata that may not be easy to find at first glance, but that you may have to go digging for it.**

Lab 2.3: Parsing APFS (Optional)

Objectives

• Parse out important APFS structures; Container Super Block, Volume Super Block, and a file entry.

Lab Preparation

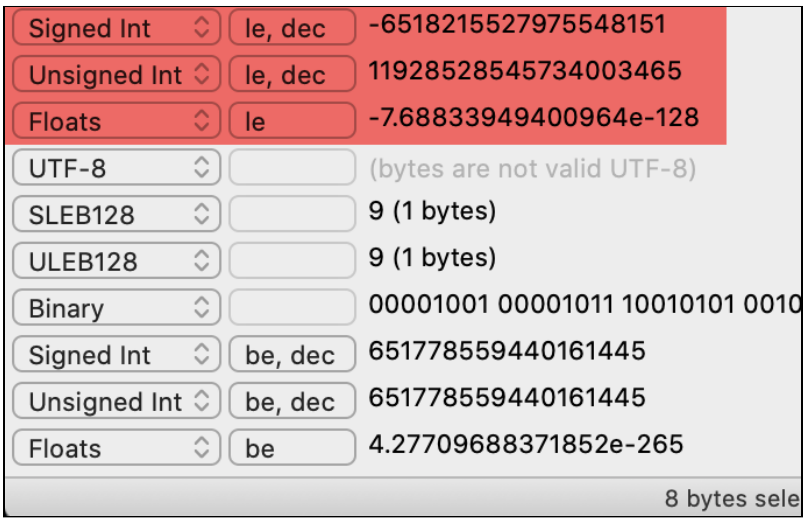
Note

Some of this might already be accomplished via earlier Labs, but this is the state that we hope your system is in prior to the start of this Lab. Just in case your system rebooted, we are including a guide to help you get back to the proper analysis starting point prior to the beginning of this Lab.

1. **Software Preparation:** The following tools will be used in this Lab:
    • Terminal.app
        a. Locate and open the native macOS Terminal.app from /Applications/Utilities/.
    • Hex Editor
        a. Locate and open the Hex Editor of your choice.
        b. I like this one:
            i. Hex Fiend: http://ridiculousfish.com/hexfiend/
                i. /Applications/Hex Fiend.app
2. **Lab File Preparation:** Locate the `APFS.dmg` file located in the `Lab Files/Lab 2.3 - Parsing APFS` directory on your FOR518-A ISO file. This file should have the MD5: `f1234a31feb2ddd4a57a61dc540cacc5`. This can be checked by executing the command: `md5 APFS.dmg`.
3. **FOR518 APFS Reference Sheet:** Locate the FOR518 APFS Reference Sheet provided to you in your class material and books. The PDF format of this sheet is available on your FOR518-A ISO file. This reference is **HIGHLY** recommended for this Lab.

Lab Questions

1. **Determine how to view little endian values in your hex editor.**
    • In Hex Fiend, for example, ensure you have at least the highlighted entries shown.



2. **Extract structures to parse from the APFS DMG image.**

   a. Use `dd` to extract each APFS structure. Each block is 4096 bytes. The offsets were provided to you as, these have the most recent transaction ID (XID) values for each object structure. The input block size is set to 1 (`ibs=1`) so these values can be seen in the command line (The default block size for dd is 512).

   b. **Container Super Block - 4096 bytes at offset 53248**

```
dd if=APFS.dmg ibs=1 skip=53248 count=4096 > ~/FOR518/container_super_block
```

   c. **Volume Super Block - 4096 bytes at offset 921600**

```
dd if=APFS.dmg ibs=1 skip=921600 count=4096 > ~/FOR518/volume_super_block
```

   d. **B-Tree Node - 4096 bytes at offset 905216**

```
dd if=APFS.dmg ibs=1 skip=905216 count=4096 > ~/FOR518/btree_node
```

3. **Parse the Container Super Block**

   a. Open the `container_super_block` file you just created in the hex editor of your choice. Fill in the blanks.

Object Header (obj_phys_t) [32 bytes, offset 0]

B-tree Offset	Size (in bytes)	Field	Value & Notes
0	8	o_cksum	
8	8	o_oid	
16	8	o_xid	
24	2	o_type.type	Type
	2	o_type.flags	Flags 0x0080 = Non-persistent
28	4	o_subtype	0x00000000 = None

Solution

B-tree Offset	Size (in bytes)	Field	Value & Notes
0	8	o_cksum	**0x4E90821780CF1BFA**
8	8	o_oid	**0x0100000000000000 = 1**
16	8	o_xid	**0x0C00000000000000 = 12**
24	2	o_type.type	**Type** **0x0100 = Container Super Block**
	2	o_type.flags	Flags 0x0080 = Non-persistent
28	4	o_subtype	0x00000000 = None

Container Super Block Object (nx_superblock) [4064 bytes, Offset 32]

B-tree Offset	Size (in bytes)	Field	Value & Notes
32	4	nx_magic	_____
36	4	nx_block_size	_____
40	8	nx_block_count	_____
48	8	nx_features	0x00000000 00000000
56	8	nx_read_only_ compatible_features	0x00000000 00000000
64	8	nx_incompatible_features	0x02000000 00000000 = NX_INCOMPAT_VERSION2
72	16	nx_uuid	0x65EC907FCF8C4869AD342F2E02C59E02 = 65EC907F-CF8C-4869-AD34-2F2E02C59E02 (verify with `diskutil info /dev/disk#` [Container])
88	8	nx_next_oid	0x0804000000000000 = 1032
96	8	nx_next_xid	0x0D00000000000000 = 13
104	4	nx_xp_desc_blocks	0x08000000 = 8
108	4	nx_xp_data_blocks	0x34000000 = 52
112	8	nx_xp_desc_base	0x01000000 00000000 = 1
120	8	nx_xp_data_base	0x9D000000 00000000 = 9
128	4	nx_xp_desc_next	0x00000000 = 0
132	4	nx_xp_data_next	0x2E000000 = 46
136	4	nx_xp_desc_index	0x06000000 = 6
140	4	nx_xp_desc_len	0x02000000 = 2
144	4	nx_xp_data_index	0x2A000000 = 42
148	4	nx_xp_data_len	0x04000000 = 4
152	8	nx_spaceman_oid	0x00040000 00000000 = 1024
160	8	nx_omap_oid	0xDD00000000000000 = 221
168	8	nx_reaper_oid	0x01040000 00000000 = 1025
176	4	nx_test_type	0x00000000
180	4	nx_max_file_systems	_____
184	8	nx_fs_oid[0]	0x02040000 00000000 = 1026 (oid for LetsParseAPFS Volume)

Solution

B-tree Offset	Size (in bytes)	Field	Value & Notes
32	4	nx_magic "NXSB"	**0x4E585342 = "NXSB"**
36	4	nx_block_size	**0x00100000 = 4096**
40	8	nx_block_count	**0x330A000000000000 = 2611 (verify with `diskutil info /dev/disk#` [Container]) 2611*4096 = 10694656 Bytes**
48	8	nx_features	0x00000000 00000000
56	8	nx_read_only_ compatible_features	0x00000000 00000000
64	8	nx_incompatible_features	0x02000000 00000000 = NX_INCOMPAT_VERSION2
72	16	nx_uuid	0x65EC907FCF8C4869AD342F2E02C59E02 = 65EC907F-CF8C-4869-AD34-2F2E02C59E02 (verify with `diskutil info /dev/disk#` [Container])
88	8	nx_next_oid	0x0804000000000000 = 1032
96	8	nx_next_xid	0x0D00000000000000 = 13
104	4	nx_xp_desc_blocks	0x08000000 = 8
108	4	nx_xp_data_blocks	0x34000000 = 52
112	8	nx_xp_desc_base	0x01000000 00000000 = 1
120	8	nx_xp_data_base	0x9D000000 00000000 = 9
128	4	nx_xp_desc_next	0x00000000 = 0
132	4	nx_xp_data_next	0x2E000000 = 46
136	4	nx_xp_desc_index	0x06000000 = 6
140	4	nx_xp_desc_len	0x02000000 = 2
144	4	nx_xp_data_index	0x2A000000 = 42
148	4	nx_xp_data_len	0x04000000 = 4
152	8	nx_spaceman_oid	0x00040000 00000000 = 1024
160	8	nx_omap_oid	0xDD00000000000000 = 221
168	8	nx_reaper_oid	0x01040000 00000000 = 1025
176	4	nx_test_type	0x00000000
180	4	nx_max_file_systems	0x01000000 = 1
184	8	nx_fs_oid[0]	0x02040000 00000000 = 1026 (oid for LetsParseAPFS Volume)

4. **Parse the Volume Super Block**

   a. Open the **`volume_super_block`** file you just created in the hex editor of your choice. Fill in the blanks.

Object Header (obj_phys_t) [32 bytes, offset 0]

Offset	Size (in bytes)	Field	Value & Notes
0	8	o_cksum	0xE0345B935464182B
8	8	o_oid	_____
16	8	o_xid	_____
24	2	o_type.type	Type _____
	2	o_type.flags	Flags 0x0000 = None
28	4	o_subtype	0x00000000 = None

Solution

Offset	Size (in bytes)	Field	Value & Notes
0	8	o_cksum	0xE0345B935464182B
8	8	o_oid	**0x0204000000000000 = 1026**
16	8	o_xid	**0x0C00000000000000 = 12**
24	2	o_type.type	**Type** **0x0D00 = Volume Super Block**
	2	o_type.flags	Flags 0x0000 = None
28	4	o_subtype	0x00000000 = None

Volume Super Block Object (apfs_superblock) [4064 bytes, Offset 32]

Offset	Size (in bytes)	Field	Value/Notes
32	4	apfs_magic	
36	4	apfs_fs_index	0x00000000 = 0 (First volume…only one volume)
40	8	apfs_features	0x02000000 00000000 = APFS_FEATURE_HARDLINK_MAP_RECORDS
48	8	apfs_readonly_compatible_features	0x00000000 00000000
56	8	apfs_incompatible_features	0x01000000 00000000 = APFS_INCOMPAT_CASE_INSENSITIVE
64	8	apfs_unmount_time	
72	8	apfs_fs_reserve_block_count	0x00000000 00000000 = 0
80	8	apfs_fs_quota_block_count	0x00000000 00000000 = 0
88	8	apfs_fs_alloc_count	0x3800000000000000 = 56
96	2	wrapped_crypto_state_t. wrapped_crypto_state.major_version	0x0500
98	2	wrapped_crypto_state_t. wrapped_crypto_state.minor_version	0x0000
100	4	wrapped_crypto_state_t. wrapped_crypto_state.cpflags	0x00000000
104	4	wrapped_crypto_state_t. wrapped_crypto_state.persistent_class	0x06000000
108	4	wrapped_crypto_state_t. wrapped_crypto_state.key_os_version	0x39004313 19 C 57 – 19C57 – Catalina 10.15.2
112	2	wrapped_crypto_state_t. wrapped_crypto_state.key_revision	0x0100
114	2	wrapped_crypto_state_t. wrapped_crypto_state.key_len	0x0000

N/A	0	wrapped_crypto_state_t. wrapped_crypto_state.persistent_key	Null – No Key, see key_len above
116	4	apfs_root_tree_oid_type	0x02000000 = B-Tree
120	4	apfs_extentref_tree_oid_type	0x02000040 = B-Tree, Physical
124	4	apfs_snap_meta_tree_oid_type	0x02000040 = B-Tree, Physical
128	8	apfs_omap_oid	0xD900000000000000 = 217
136	8	apfs_root_tree_oid	0x0404000000000000 = 1028
144	8	apfs_extentref_tree_oid	0xD400000000000000 = 212
152	8	apfs_snap_meta_tree_oid	0x5800000000000000 = 88
160	8	apfs_revert_to_xid	0x0000000000000000 = 0
168	8	apfs_revert_to_sblock_oid	0x0000000000000000 = 0
176	8	apfs_next_obj_id	0x1A00000000000000 = 26
184	8	apfs_num_files	_____
192	8	apfs_num_directories	_____
200	8	apfs_num_symlinks	0x00000000 00000000 = 0
208	8	apfs_num_other_fsobjects	0x00000000 00000000 = 0
216	8	apfs_num_snapshots	0x00000000 00000000 = 0
224	8	apfs_total_blocks_alloced	0x4100000000000000 = 65
232	8	apfs_total_blocks_freed	0x1000000000000000 = 16
240	16	apfs_vol_uuid	0xED919A5F81114AA5B88A5D34316C7EE9 = ED919A5F-8111-4AA5-B88A-5D34316C7EE9 (verify with `diskutil info /dev/disk#s#` [Volume])
256	8	apfs_last_mod_time	_____ _____
264	8	apfs_fs_flags	0x0100000000000000
272	32	apfs_modified_by_t.formatted_by.id[]	_____
304	8	apfs_modified_by_t.formatted_by. timestamp	_____ _____
312	8	apfs_modified_by_t.formatted_by. last_xid	0x0200000000000000
320	32	apfs_modified_by_t.modified_by.id[]	_____

352	8	apfs_modified_by_t.modified_by. timestamp	
360	8	apfs_modified_by_t.modified_by. last_xid	0x0900000000000000
368	336	apfs_modified_by_t.modified_by[1-7]	apfs_modified_by_t[8] 48x8 = 384
704	256	apfs_volname	
960	4	apfs_next_doc_id	0x03000000 = 3
964	2	apfs_role	0x0000 = None
966	2	apfs_reserved	0x0000
976	8	apfs_root_to_xid	0x00000000 00000000 = 0
984	8	apfs_er_state_oid	0x00000000 00000000 = 0

Solution

Offset	Size (in bytes)	Field	Value/Notes
32	4	apfs_magic "APSB"	**0x41505342 = "APSB"**
36	4	apfs_fs_index	0x00000000 = 0 (First volume…only one volume)
40	8	apfs_features	0x02000000 00000000 = APFS_FEATURE_HARDLINK_MAP_RECORDS
48	8	apfs_readonly_compatible_features	0x00000000 00000000
56	8	apfs_incompatible_features	0x01000000 00000000 = APFS_INCOMPAT_CASE_INSENSITIVE
64	8	apfs_unmount_time	**0xCF29D2975443ED15 = 1579993074880358863 = 2020-01-25 22:57:54.880359 UTC**
72	8	apfs_fs_reserve_block_count	0x00000000 00000000 = 0
80	8	apfs_fs_quota_block_count	0x00000000 00000000 = 0
88	8	apfs_fs_alloc_count	0x3800000000000000 = 56
96	2	wrapped_crypto_state_t. wrapped_crypto_state.major_version	0x0500
98	2	wrapped_crypto_state_t. wrapped_crypto_state.minor_version	0x0000
100	4	wrapped_crypto_state_t. wrapped_crypto_state.cpflags	0x00000000
104	4	wrapped_crypto_state_t. wrapped_crypto_state.persistent_class	0x06000000
108	4	wrapped_crypto_state_t. wrapped_crypto_state.key_os_version	0x39004313 19 C 57 – 19C57 – Catalina 10.15.2
112	2	wrapped_crypto_state_t. wrapped_crypto_state.key_revision	0x0100
114	2	wrapped_crypto_state_t. wrapped_crypto_state.key_len	0x0000

N/A	0	wrapped_crypto_state_t. wrapped_crypto_state.persistent_key	Null – No Key, see key_len above
116	4	apfs_root_tree_oid_type	0x02000000 = B-Tree
120	4	apfs_extentref_tree_oid_type	0x02000040 = B-Tree, Physical
124	4	apfs_snap_meta_tree_oid_type	0x02000040 = B-Tree, Physical
128	8	apfs_omap_oid	0xD900000000000000 = 217
136	8	apfs_root_tree_oid	0x0404000000000000 = 1028
144	8	apfs_extentref_tree_oid	0xD400000000000000 = 212
152	8	apfs_snap_meta_tree_oid	0x5800000000000000 = 88
160	8	apfs_revert_to_xid	0x0000000000000000 = 0
168	8	apfs_revert_to_sblock_oid	0x0000000000000000 = 0
176	8	apfs_next_obj_id	0x1A00000000000000 = 26
184	8	apfs_num_files	**0x0700000000000000 = 7**
192	8	apfs_num_directories	**0x0300000000000000 = 3**
200	8	apfs_num_symlinks	0x00000000 00000000 = 0
208	8	apfs_num_other_fsobjects	0x00000000 00000000 = 0
216	8	apfs_num_snapshots	0x00000000 00000000 = 0
224	8	apfs_total_blocks_alloced	0x4100000000000000 = 65
232	8	apfs_total_blocks_freed	0x1000000000000000 = 16
240	16	apfs_vol_uuid	0xED919A5F81114AA5B88A5D34316C7EE9 = ED919A5F-8111-4AA5-B88A-5D34316C7EE9 (verify with `diskutil info /dev/disk#s#` [Volume])
256	8	apfs_last_mod_time	**0xA933888C6943ED15 = 1579993164885275561 = 2020-01-25 22:59:24.885276 UTC**
264	8	apfs_fs_flags	0x0100000000000000
272	32	apfs_modified_by_t.formatted_by.id[]	**0x6E657766735F6170667320283134313232E36312E31290000000000000000000 = "newfs_apfs (1412.61.1)"**
304	8	apfs_modified_by_t.formatted_by. timestamp	**0xD8B96C2C3743ED15 = 1579992948524497368 2020-01-25 22:55:48.524498 UTC**
312	8	apfs_modified_by_t.formatted_by. last_xid	0x0200000000000000
320	32	apfs_modified_by_t.modified_by.id[]	**0x617066735F6B6578742028313431322E36312E31290000000000000000000000 = apfs_kext (1412.61.1)**

352	8	apfs_modified_by_t.modified_by. timestamp	**0x5919D2975443ED15 = 1579993074880354649 = 2020-01-25 22:57:54.880355 UTC**
360	8	apfs_modified_by_t.modified_by. last_xid	0x0900000000000000
368	336	apfs_modified_by_t.modified_by[1-7]	apfs_modified_by_t[8] 48x8 = 384
704	256	apfs_volname	**0x4C6574735061727365415046534 = LetsParseAPFS**
960	4	apfs_next_doc_id	0x03000000 = 3
964	2	apfs_role	0x0000 = None
966	2	apfs_reserved	0x0000
976	8	apfs_root_to_xid	0x00000000 00000000 = 0
984	8	apfs_er_state_oid	0x00000000 00000000 = 0

5. **Parse a B-Tree Node**

   a. Open the `btree_node` file you just created in the hex editor of your choice. Fill in the blanks.

Object Header (obj_phys_t) [32 bytes, offset 0]

Btree Offset	Size (in bytes)	Field	Value & Notes
0	8	o_cksum	0x77B4DE6C812048DE
8	8	o_oid	_____
16	8	o_xid	_____
24	2	o_type.type	Type _____
	2	o_type.flags	Flags 0x0000 = None
28	4	o_subtype	_____

Solution

Btree Offset	Size (in bytes)	Field	Value & Notes
0	8	o_cksum	0x77B4DE6C812048DE
8	8	o_oid	**0x0704000000000000 = 1031**
16	8	o_xid	**0x0C0000000000000 = 12**
24	2	o_type.type	**Type 0x0300 = B-Tree Node**
	2	o_type.flags	Flags 0x0000 = None
28	4	o_subtype	**0x0E000000 = File System Tree**

B-Tree Node (btree_node_phys_t) [24 bytes, offset 32]

Btree Offset	Size (in bytes)	Field	Value & Notes
32	2	btn_flags	0x0200 – Leaf Node
34	2	btn_level	0x0000
36	4	btn_nkeys	_____ (keys stored in this node)
40	2	btn_table_space.off	_____ (TOC)
42	2	btn_table_space.len	_____
44	2	btn_freespace.off	0xA303 = 931 (Free Space)
46	2	btn_freespace.len	0x2300 = 35
48	2	btn_key_free_list.off	0x9303 = 915 (Free Key Space)
50	2	btn_key_free_list.len	0x1000 = 16
52	2	btn_val_free_list.off	0xCA09 = 2506 (Free Value Space)
54	2	btn_val_free_list.len	0x3000 = 48

Solution

Btree Offset	Size (in bytes)	Field	Value & Notes
32	2	btn_flags	0x0200 – Leaf Node
34	2	btn_level	0x0000
36	4	btn_nkeys	**0x2F000000 = 47 (keys stored in this node)**
40	2	btn_table_space.off	**0x0000 = 0 (TOC)**
42	2	btn_table_space.len	**0x8001 = 384**
44	2	btn_freespace.off	0xA303 = 931 (Free Space)
46	2	btn_freespace.len	0x2300 = 35
48	2	btn_key_free_list.off	0x9303 = 915 (Free Key Space)
50	2	btn_key_free_list.len	0x1000 = 16
52	2	btn_val_free_list.off	0xCA09 = 2506 (Free Value Space)
54	2	btn_val_free_list.len	0x3000 = 48

Table of Contents - Fill in the missing pieces of the TOC fields. [376 bytes (47 entries * 8 bytes), offset 56]

B-tree Offset	TOC Entry	key_offset (2 bytes)	key_length (2 bytes)	value_offset (2 bytes)	value_length (2 bytes)	Object ID (Inode # in Hex)
56	1	0x0000 = 0	0x1800 = 24	0x1200 = 18	0x1200 = 18	01 private-dir
64	2	0x1800 = 24	0x1100 = 17	0x2400 = 36	0x1200 = 18	01 root
72	3	0x2900 = 41	0x0800 = 8	0x9000 = 144	0x6C00 = 108	02
80	4	49	22	162	18	02
88	5	71	22	180	18	02
96	6	93	23	198	18	02
104	7	116	22	216	18	02
112	8	138	8	332	116	03
120	9	146	8	2666	160	10
128	10	154	31	368	36	10
136	11	185	8	372	4	10
144	12	193	16	396	24	10
152	13	209	8	512	116	11
160	14	217	28	542	30	11
168	15	245	36	560	18	11
176	**16**	**281**	**8**	**728**	**168**	**12**
184	**17**	**289**	**36**	**748**	**20**	**12**
192	**18**	**325**	**47**	**936**	**188**	**12**
200	**19**	**372**	**31**	**997**	**61**	**12**
208	**20**	_____	_____	_____	_____	**12**
216	**21**	_____	_____	_____	_____	**12**

224	**22**	_____	_____	_____	_____	**12**
232	23	455	8	1171	116	13
240	24	463	28	1201	30	13
248	25	491	35	1219	18	13
256	26	526	29	1237	18	13
264	27	555	8	1405	168	14
272	28	563	36	1425	20	14
280	29	599	31	1486	61	14
288	30	630	28	1516	30	14
296	31	658	8	1520	4	14
304	32	666	16	1544	24	14
312	33	682	8	1660	116	15
320	34	690	27	1678	18	15
328	35	717	29	1696	18	15
336	36	746	29	1714	18	15
344	37	775	8	1874	160	16
352	38	783	8	1878	4	16
360	39	791	16	1902	24	16
368	40	807	8	2070	168	17
376	41	815	8	2074	4	17
384	42	823	16	2098	24	17
392	43	839	8	2266	168	18
400	44	847	8	2270	4	18
408	45	855	16	2294	24	18
416	46	871	8	2462	168	19
424	47	879	36	2482	20	19
432	8	Extra 8 bytes, table space value is 384 while TOC contents is 376 bytes				

Solution

B-tree Offset	TOC Entry	key_offset (2 bytes)	key_length (2 bytes)	value_offset (2 bytes)	value_length (2 bytes)	Object ID (Inode # in Hex)
56	1	0x0000 = 0	0x1800 = 24	0x1200 = 18	0x1200 = 18	01 private-dir
64	2	0x1800 = 24	0x1100 = 17	0x2400 = 36	0x1200 = 18	01 root
72	3	0x2900 = 41	0x0800 = 8	0x9000 = 144	0x6C00 = 108	02
80	4	49	22	162	18	02
88	5	71	22	180	18	02
96	6	93	23	198	18	02
104	7	116	22	216	18	02
112	8	138	8	332	116	03
120	9	146	8	2666	160	10
128	10	154	31	368	36	10
136	11	185	8	372	4	10
144	12	193	16	396	24	10
152	13	209	8	512	116	11
160	14	217	28	542	30	11
168	15	245	36	560	18	11
176	16	281	8	728	168	**12**
184	17	289	36	748	20	**12**
192	18	325	47	936	188	**12**
200	19	372	31	997	61	**12**
208	20	**403**	**28**	**1027**	**30**	**12**
216	21	**431**	**8**	**1031**	**4**	**12**

224	22	**439**	**16**	**1055**	**24**	**12**
232	23	455	8	1171	116	13
240	24	463	28	1201	30	13
248	25	491	35	1219	18	13
256	26	526	29	1237	18	13
264	27	555	8	1405	168	14
272	28	563	36	1425	20	14
280	29	599	31	1486	61	14
288	30	630	28	1516	30	14
296	31	658	8	1520	4	14
304	32	666	16	1544	24	14
312	33	682	8	1660	116	15
320	34	690	27	1678	18	15
328	35	717	29	1696	18	15
336	36	746	29	1714	18	15
344	37	775	8	1874	160	16
352	38	783	8	1878	4	16
360	39	791	16	1902	24	16
368	40	807	8	2070	168	17
376	41	815	8	2074	4	17
384	42	823	16	2098	24	17
392	43	839	8	2266	168	18
400	44	847	8	2270	4	18
408	45	855	16	2294	24	18
416	46	871	8	2462	168	19
424	47	879	36	2482	20	19
432	8	Extra 8 bytes, table space value is 384 while TOC contents is 376 bytes				

File System Keys - Fill in the missing pieces of for TOC Entries 16 - 22. These are the File System Keys for the `smudge_transformer.jpeg` file. File System Keys in B-tree File: Bytes 440 - 915 (475 total bytes).

File System Keys - Inode Keys for `smudge_transformer.jpeg` file

B-tree Offset	Entry	Offset	Size (in bytes)	Object ID (Inode #)	Entry Kind [Highest byte in first 8 bytes]	Entry Type	Value & Notes
721	16	281	**8**	0x12000 0000000 00 = 12	0x30	Inode	N/A
729	17	289	**36**	0x12000 0000000 00 = 12	0x40	Xattr	com.apple.lastuseddate#PS [2 byte size before, 1 byte padding after]
765	18	325	**47**	0x12000 0000000 00 = 12	0x40	Xattr	_____ _____ [2 byte size before, 1 byte padding after]
812	19	372	**31**	0x12000 0000000 00 = 12	0x40	Xattr	_____ _____ [2 byte size before, 1 byte padding after]
843	20	_____	_____	0x12000 0000000 00 = 12	_____	_____	com.dropbox.attrs [2 byte size before, 1 byte padding after]
871	21	_____	_____	0x12000 0000000 00 = 12	_____	_____	N/A
879	22	_____	_____	0x12000 0000000 00 = 12	_____	_____	0x0000000000000000

Solution

B-tree Offset	Entry	Offset	Size (in bytes)	Object ID (Inode #)	Entry Kind [Highest byte in first 8 bytes]	Entry Type	Value & Notes
721	16	281	8	0x12000000000000 = 12	0x30	Inode	N/A
729	17	289	36	0x12000000000000 = 12	0x40	Xattr	com.apple.lastuseddate#PS [2 byte size before, 1 byte padding after]
765	18	325	47	0x12000000000000 = 12	0x40	Xattr	com.apple.metadata:kMDItemWhereFroms **[2 byte size before, 1 byte padding after]**
812	19	372	31	0x12000000000000 = 12	0x40	Xattr	com.apple.quarantine **[2 byte size before, 1 byte padding after]**
843	20	**403**	**28**	0x12000000000000 = 12	**0x40**	**Xattr**	com.dropbox.attrs [2 byte size before, 1 byte padding after]
871	21	**431**	**8**	0x12000000000000 = 12	**0x60**	**Data Stream**	N/A
879	22	**439**	**16**	0x12000000000000 = 12	**0x80**	**File Extent**	0x0000000000000000

File System Values - Fill in the missing pieces of for TOC Entries 16 - 22. These are the File System Values for the `smudge_transformer.jpeg` file. File System Values in B-tree File: Bytes 1614 - 4096 (2482 total bytes).

File System Values - Inode Values for `smudge_transformer.jpeg` File

B-tree Offset	Entry	Offset	Size (in bytes)	Entry Type	Value & Notes
3368	16	728	**168**	Inode	File Metadata for smudge_transformer.jpeg **[See below]** 0x1100000000000000120000000000000000C8B8E50243ED1500C8B8E50243ED1570D76C933743ED15002E5F812D43ED150080000000000000001000000000000020000000000000F501000014000000A4810000000000000000000020040000402180008202800736D756467655F7472616E73666F726D65722E6A70656700A0890000000000000090000000000000000000000000A0890000000000000000000000000000
3348	17	748	**20**	Xattr	0x0200100028C72C5E00000000AED5671300000000 = com.dropbox.attrs
3160	18	936	**188**	Xattr	**Question: Where was this photo downloaded from?** _____
3099	19	997	**61**	Xattr	**Question: How was this photo downloaded?** _____
3069	20	1027	**30**	Xattr	0x02001A000A120A1059C45688BCFCFFB4000000000007C9FD1099BD92B608 = com.dropbox.attrs
3065	21	1031	**4**	Data Stream	0x01000000 = Number of References
3041	22	1055	**24**	File Extent	File Size: _____ Physical Block Location: Physical Block Number from start of container (add 5 (20,480) blocks for start of disk) (# * 4096) + 20,480 = start of file location in bytes: _____ crypto_id: 0x0000000000000000 – No Key

Solution

B-tree Offset	Entry	Offset	Size (in bytes)	Entry Type	Value & Notes
3368	16	728	**168**	Inode	File Metadata for smudge_transformer.jpeg **[See below]** 0x1100000000000000120000000000000000C8B8E50243ED1500C8B8E50243ED1570D76C933743ED15002E5F812D43ED150080000000000000001000000000000020000000000000F501000014000000A4810000000000000000000020040000402180008202800736D756467655F7472616E73666F726D65722E6A70656700A0890000000000000090000000000000000000000000000000A0890000000000000000000000000000
3348	17	748	**20**	Xattr	0x0200100028C72C5E00000000AED5671300000000 = com.dropbox.attrs
3160	18	936	**188**	Xattr	**Answer: Twitter** **0x0200B80062706C6973743030A201025F10436874747073A2F2F7062732E7477696D672E636F6D2F6D656469612F454F716C726963565541556538374A3F666F726D61743D6A7067266E616D653D393030783930305F10416874747073A2F2F747769747465722E636F6D2F536F6E6F66476967616E2F7374617475732F313231383936383832303237363035313936382F70686F746F2F31080B5100000000000001010000000000000030000000000000000000000000000095 = Binary Plist containing Spotlight WhereFroms Data** **"bplist00¢_Chttps://pbs.twimg.com/media/EOqlricVUAUe87J?format=jpg&name=900x900_Ahttps://twitter.com/SonofGigan/status/1218968820276051968/photo/1"**
3099	19	997	**61**	Xattr	**Answer: Chrome** **0x020039003030383333B3565326336366133 3B4368726F6D653B323131393531453 32D313741432D344333362D383545302D383935353333383344434539 = File Quarantine Attribute Data** **0083;5e2cc6a3;Chrome;211951E3-17AC-4C36-85E0-89553383DCE9**
3069	20	1027	**30**	Xattr	0x02001A000A120A1059C45688BCFCFFB4000000000007C9FD1099BD92B608 = com.dropbox.attrs

<table>
<tr><td>3065</td><td>21</td><td>1031</td><td>4</td><td>Data Stream</td><td>0x01000000 = Number of References</td></tr>
<tr><td>3041</td><td>22</td><td>1055</td><td>24</td><td>File Extent</td><td>0x0090000000000006000000000000000000000000000000

<table><tr><td>File Size</td><td>0x0090000000000000 = 36864</td></tr><tr><td>Physical Block Location:
Physical Block Number from start of container (add 5 (20,480) blocks for start of disk)
(# * 4096) + 20,480 = start of file location in bytes</td><td>0x6000000000000000 = 96 = Physical Block Number

(96 * 4096) + 20,480 = 413696 bytes</td></tr><tr><td>crypto_id</td><td>0x0000000000000000 – No Key</td></tr></table></td></tr>
</table>

Inode Entry/File Metadata for `smudge_transformer.jpeg`

B-tree Offset	Inode Entry Offset	Size (in bytes)	Field	Value & Notes
3368	0	8	parent_id	_____
3376	8	8	private_id	_____
3384	16	8	create_time	0x00C8B8E50243ED15 = 1579992724000000000 = 2020-01-25 22:52:04 UTC
3392	24	8	mod_time	0x00C8B8E50243ED15 = 1579992724000000000 = 2020-01-25 22:52:04 UTC
3400	32	8	change_time	0x70D76C933743ED15 = 1579992950252558192 = 2020-01-25 22:55:50.252558 UTC
3408	40	8	access_time	0x002E5F812D43ED15 = 1579992907000000000 = 2020-01-25 22:55:07 UTC
3416	48	8	internal_flags	0x0080000000000000
3424	56	4	nchildren or nlink	0x01000000 = 1
3428	60	4	default_protection_class	0x00000000
3432	64	4	write_generation_counter	0x02000000
3426	68	4	bsd_flags	0x00000000
3440	72	4	owner	_____
3444	76	4	group	_____
3448	80	2	mode	1000 = 8 (Regular File) 000 = SetUID, SetGID, Sticky bits ___ = ___ User Permissions ___ = ___ Group Permissions ___ = ___ Other Permissions
3450	82	2	pad1	0x0000
3452	84	8	pad2	0x0000000000000000
3460	92	2	xf_num_exts	Number of Extended Fields = 0x0200 = 2
3462	94	2	xf_used_data	Extended Fields Data Used = 0x4000 = 64 bytes
3464	96	x_field_t 8	x_type [1 byte]: 0x04 = String Name; 0x08 = Data Stream x_flags [1 byte]: 0x02 = Do not copy; 0x20 = System Field x_size [2 byte]: 0x1800 = 24; 0x2800 = 40	
3472	104	{24}	File Name	_____ (w/1 padding bytes 0x00), 24 total bytes
3496	120	{40}	Data Stream (Size: First 8 bytes)	File Size: _____ Allocated: 0090000000000000 = 36864

Solution

B-tree Offset	Inode Entry Offset	Size (in bytes)	Field	Value & Notes
3368	0	8	parent_id	**0x1100000000000000 = 17**
3376	8	8	private_id	**0x12000000 00000000 = 18**
3384	16	8	create_time	0x00C8B8E50243ED15 = 1579992724000000000 = 2020-01-25 22:52:04 UTC
3392	24	8	mod_time	0x00C8B8E50243ED15 = 1579992724000000000 = 2020-01-25 22:52:04 UTC
3400	32	8	change_time	0x70D76C933743ED15 = 1579992950252558192 = 2020-01-25 22:55:50.252558 UTC
3408	40	8	access_time	0x002E5F812D43ED15 = 1579992907000000000 = 2020-01-25 22:55:07 UTC
3416	48	8	internal_flags	0x0080000000000000
3424	56	4	nchildren or nlink	0x01000000 = 1
3428	60	4	default_protection_class	0x00000000
3432	64	4	write_generation_counter	0x02000000
3426	68	4	bsd_flags	0x00000000
3440	72	4	owner	**0xF5010000 = 501**
3444	76	4	group	**0x14000000 = 20**
3448	80	2	mode	0xA481 = 1010010010000001 Byte Flip = 1000 000 110 100 100 1000 = 8 (Regular File) 000 = SetUID, SetGID, Sticky bits **110 = 6 (rw-) User Permissions** **100 = 4 (r--) Group Permissions** **100 = 4 (r--) Other Permissions** (See tables 15.11-15.13 in File System Forensic Analysis by Brian Carrier)
3450	82	2	pad1	0x0000
3452	84	8	pad2	0x0000000000000000
3460	92	2	xf_num_exts	Number of Extended Fields = 0x0200 = 2
3462	94	2	xf_used_data	Extended Fields Data Used = 0x4000 = 64 bytes
3464	96	x_field_t 8	x_type [1 byte] 0x04 = String Name 0x08 = Data Stream	x_flags [1 byte] 0x02 = Do not copy 0x20 = System Field	x_size [2 byte] 0x1800 = 24 0x2800 = 40

3472	104	{24}	File Name	**0x736D756467655F7472616E73666F726D65722E6A70656700 = smudge_transformer.jpeg (w/1 padding bytes 0x00), 24 total bytes**
3496	120	{40}	Data Stream (Size: First 8 bytes)	**0x0A0890000000000000900000000000000000000000000000A0890000000000000000000000 File Size: 0xA0890000000000 = 35232 bytes Allocated: 0090000000000000 = 36864**

Use `dd` to extract the picture:

- From File Extent Data:
  - skip= (From File System Values - Inode Values)
  - count= (From Inode Entry/File Metadata)

```
dd if=APFS.dmg ibs=1 skip=________ count=________ > ~/FOR518/
smudge_transformer_extracted.jpeg
```

Solution

```
dd if=APFS.dmg ibs=1 skip=413696 count=35232 > ~/FOR518/smudge_transformer_extracted.jpeg
```

Lab: Key Takeaways

- **Review and manually parse the contents of the file system.**

Lab 3.1: Log Parsing and Analysis

Objectives

- Know where the key log files are stored and how to parse the Apple System Logs, Basic Security Module Audit logs, and Unified logs.
- Get familiar with the macOS command line.

Lab Preparation

> **Note**
>
> Some of this might already be accomplished via earlier labs, but this is the state that we hope your system is in prior to the start of this lab. Just in case your system rebooted, we are including a guide to help you get back to the proper analysis starting point prior to the beginning of this lab.

1. **Software Preparation**: The following tools will be used in this exercise:
    - Terminal.app
        a. Locate and open the native macOS Terminal.app from /Applications/Utilities/.
    - Console.app
        a. Locate and open the native macOS Console.app from /Applications/Utilities.
2. **FOR518 Reference Sheet**: Locate the FOR518 Reference Sheet provided to you in your class material and books. The PDF format of this sheet is available on your FOR518-A ISO file.
3. **Mount David Lightman's Mac forensic image** (`galaga.E01`).
    - Mounting Instructions

Lab Questions

Introduction to the Console Application

Locate and open the native `macOS Console.app` from `/Applications/Utilities/` .

This will show you the log contents of your host system.

System Log Directory and Bzip2 Compression

Use the `cd` command to navigate to the System Log directory.

Use the `ls -l` command to view all files in this directory. Note the contents of this directory.

Use the `file` command to view the file types listed for these files. Note the files labeled as "`bzip2 compressed data`".

```
cd /Volumes/galaga_mounted/private/var/log/

ls -l

file *
```

1. What set of log files has been archived using Bzip2 compression?

   _____

   Solution

   `wifi.log.bz2*`

2. What set of log files has been archived using Gzip compression?

   _____

   Solution

   `system.log.gz*`

Use the `gzcat` and `cat` commands to decompress and create a comprehensive log file of the `system.log`. Output this log file to your FOR518 directory as `system_all.log`.

```
gzcat system.log.{5..0}.gz > ~/FOR518/system_all.log

cat system.log >> ~/FOR518/system_all.log
```

1. Use the `wc -l` command to determine how many records are now in the `system_all.log` file.

   _____

   Solution

   18,254 records (`wc -l ~/FOR518/system_all.log`)

Apple System Log (ASL) Directory

Use the `cd` command to navigate to the Apple System Log directory.

Use the `ls -la` command to view all files in this directory. Note the contents of this directory.

```
cd /Volumes/galaga_mounted/private/var/log/asl/

ls -la
```

1. What is the date of the oldest ASL log file (not including "best before" ASL files)?

_____

> **Solution**
>
> 02/25/2018

2. How many days in the past are events recorded, as shown by the ASL filenames (not including “best before” ASL files)?

_____

> **Solution**
>
> Seven (2/25/2018-3/3/2018)

ASL Log Conversion Using the `syslog` Command

- View the man page for the `syslog` command using the man command.
  - **Briefly**, review its contents.
  - Use the `spacebar` to page down.
  - Press "`q`" when ready to quit the viewer.

```
man syslog
```

Use the `syslog` command to view the contents of any ASL log file.

Note the contents and format of this output.

```
syslog -F 2018.02.28.U501.asl
```

Use the `syslog` command to view the contents of the same ASL log file in RAW format.

Note the differences in the log output.

```
syslog -F raw -f 2018.02.28.U501.asl
```

- Use the `syslog` command to output all the ASL logs in this directory using the UTC timestamp in RAW format.
  - Your terminal should be set with the UTC time zone; if not, use the "`export TZ=UTC`".
  - Redirect the output to a file `ASL.log` in your FOR518 directory.
  - You can check the time zone of the terminal window by using the `date` command and looking at the time zone.

Open the `ASL.log` log in `Console.app` using the open command.

Review this output.

```
export TZ=UTC

syslog -F raw -T utc -d . > ~/FOR518/ASL.log
```

```
open -a Console ~/FOR518/ASL.log
```

1. How many records are there? (Hint: Use `wc -l` command.)

   _____

   Solution

   14,006 Records

2. What is the date (UTC) of the first message?

   _____

   Solution

   2017-11-13 01:18:25Z

3. When does the first message expire?

   _____

   Solution

   a. 1542158305 = 2018-11-14 01:18:25 Wed UTC

      i. `ASLExpireTime` Field

4. How long until the last message (2018-03-03 21:43:59Z) expires?

   _____

   Solution

   a. Seven days

   b. If no `ASLExpireTime` field is present, default expire time is seven days from the date of the message.

Basic Security Module Audit Logs

Ensure the time zone of your Terminal window is UTC using the `export TZ=UTC` command.

Use the `cd` command to navigate to the Audit Log Directory.

Use the `ls -la` command to view all files in this directory. Note the contents of this directory.

```
export TZ=UTC

cd /Volumes/galaga_mounted/private/var/audit/

ls -la
```

1. What is the start timestamp of the oldest audit log file?

Solution

20171113011901 = November 13, 2017 01:19:01

Use the `praudit` command to output the contents of any single audit log file.

- Use the `less` command to control the output.

Review the output of this command.

```
praudit 20171113011901.crash_recovery | less
```

Use the praudit command to output the contents of the audit log in XML format.

- Use the `less` command to control the output.

Review the output of this command. Note how the data pieces are now labeled.

```
praudit -x 20171113011901.crash_recovery | less
```

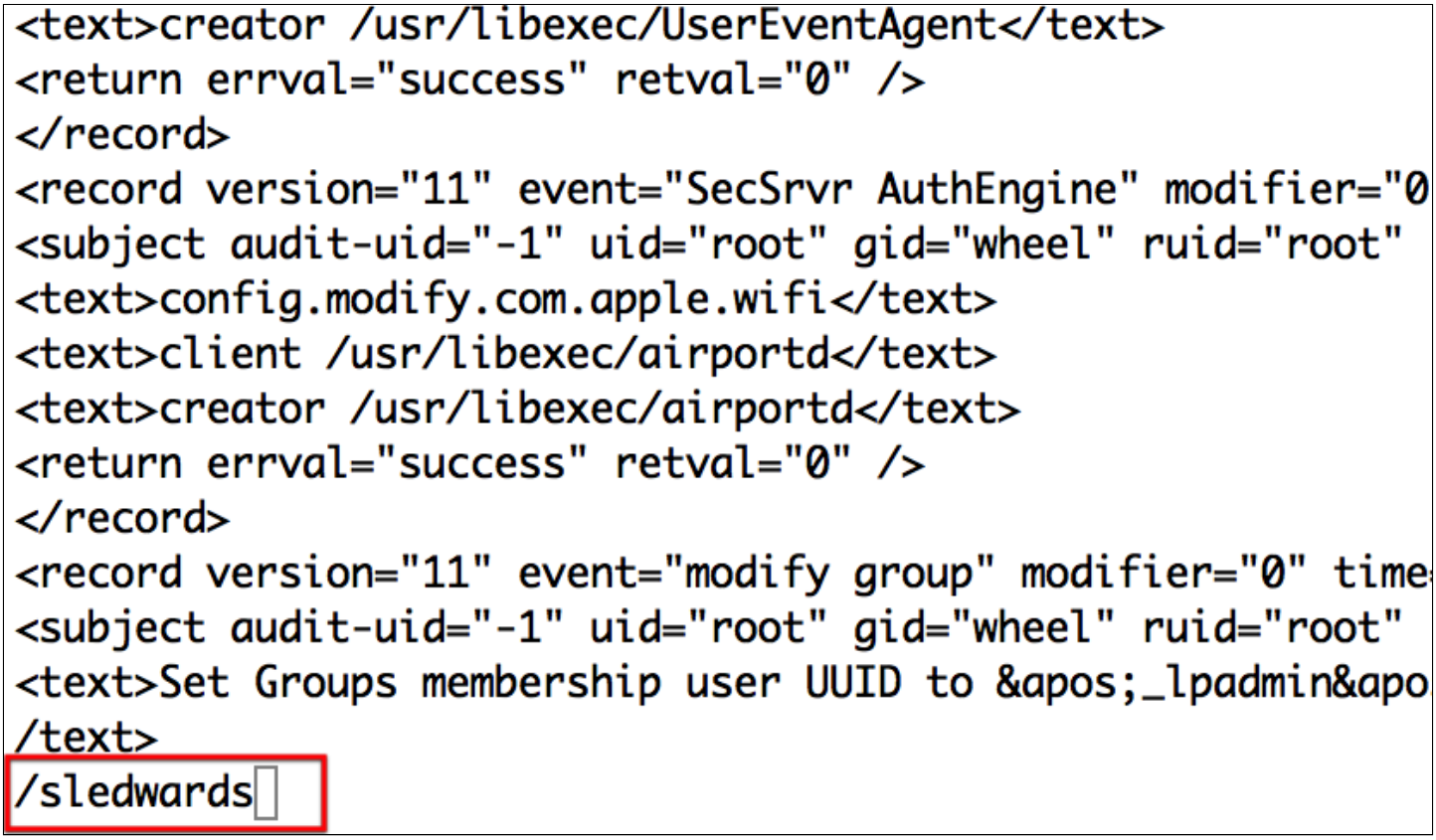
Perform a search for a username.

- While in the `less` output from the previous command, type a "/", then type the username for user 501 on your system. (i.e., /sledwards). Hit [return]. This will search the output for this username.
- **A username on your system** should not be showing up in someone else's logs!

Hint

This will only work if you have a user 501; some systems that are network-logon-based may not have one. If you are not user 501 on your system, please skip this demo.

- The `praudit` command is translating the current users of the system into the output of these logs - **not good for forensics!**



Use the "`-n`" option to stop the UID and the GID translation.

Perform the same search-does your username show up now?

```
praudit -xn 20171113011901.crash_recovery | less
```

Use the `praudit` command to output the contents of the audit logs in this directory to a file in your FOR518 directory named `audit.log`.

- The "." notation is used so as not to include the "`current`" link. (This file is already included, and the link is pointing to your own file system.)

Review the contents in Console.app.

```
praudit -xn *.* > ~/FOR518/audit.log

open -a Console ~/FOR518/audit.log
```

To search, press `Command` + `F` — this will allow you to search the contents while still viewing all the contents.

The search box located in the top-right of the application will filter contents based on a search string. While convenient for records using one line, this causes issues when records are multi-line, much like these XML-based records.

1. When was the user `dlightman` created? (Search "`create user`".)

_____

Solution

Mon Nov 13 01:26:28 2017

2. Find the “user authentication” event recorded Mon Nov 13 01:26:35 2017. What user authenticated to the system?

_____

Solution

`dlightman`

3. Did the default `Guest` user ever log in successfully?

_____

Solution

Sure did, on Sat Feb 10 13:54:19 2018

Unified Logs

Navigate to `/var/db/uuidtext/` and use `ls -laR` to view the contents of this directory recursively.

Feel free to select a file and review the contents of it using the `xxd` command.

```
cd /Volumes/galaga_mounted/private/var/db/uuidtext

ls -laR
```

Navigate to `/var/db/diagnostics/` and use `ls -laR` to view the contents of this directory recursively.

```
cd /Volumes/galaga_mounted/private/var/db/diagnostics

ls -laR
```

View the man page for the `log` command using the `man` command.

- **Briefly**, review its contents.
- Use the `spacebar` to page down.
- Press " `q` " when ready to quit the viewer.

```
man log
```

Navigate up one directory to `/var/db/` .

Use `mkdir` to make a log archive for this system named `galaga.logarchive` .

Use `cp` to copy the `uuidtext` and `diagnostics` directories to this log archive.

- Those using ZSH and/or are using 10.15+ (default shell is ZSH) make sure those forward slashes appear after the `uuidtext` and `diagnostics` directories.

```
cd ../

mkdir ~/FOR518/galaga.logarchive

cp -R diagnostics/ uuidtext/ ~/FOR518/galaga.logarchive
```

Run this command to force it into the proper Logarchive format: `/usr/libexec/PlistBuddy -c "Add :OSArchiveVersion integer 4" ~/FOR518/galaga.logarchive/Info.plist`

Run the `log show` command and pipe it to `less`.

Expect to get some errors, although the log file appears to be ok.

Note the "Skipping info and debug messages" message; let's get the `info` messages too!

Re-run with `--info`; let's also change the time zone to UTC with `--timezone`

Briefly browse the content and format of this output.

```
/usr/libexec/PlistBuddy -c "Add :OSArchiveVersion integer 4" ~/FOR518/galaga.logarchive/
Info.plist

log show ~/FOR518/galaga.logarchive | less

log show --info --timezone utc ~/FOR518/galaga.logarchive | less
```

1. What is the timestamp of the first record?

   _____

> **Solution**
>
> a. 2018-02-07 08:49:50.000000+0000
>
> b. Note the time zone and the microseconds

Give the `log stats` command a try. This may take a few moments to run. Review the output.

```
log stats --overview --archive ~/FOR518/galaga.logarchive/
```

Exercise: Key Takeaways

- **Know how to parse these log files by hand; most tools do not parse these automatically.**
- **Get comfortable with some macOS command-line utilities.**

Lab 3.2: Log Analysis

Objectives

- Get familiar with correlating events using log analysis and data correlation of key macOS data files.
- Get familiar with property lists using Xcode.
- Get more comfortable with the macOS command line using Terminal by getting creative with command line utilities built into the Mac.

Lab Preparation

> **Note**
>
> Some of this might already be accomplished via earlier labs, but this is the state that we hope your system is in prior to the start of this lab. Just in case your system rebooted, we are including a guide to help you get back to the proper analysis starting point prior to the beginning of this lab.

1. **Software Preparation**: The following tools will be used in this exercise:
    - Terminal.app
        a. Locate and open the native macOS Terminal.app from /Applications/Utilities/.
    - Xcode.app
        a. Locate and open the Xcode.app from /Applications/.
    - Inspector.app
        a. Locate and open the Inspector.app from /Applications/Inspector Release #/Inspector.app
2. **FOR518 Reference Sheet**: Locate the FOR518 Reference Sheet provided to you in your class material and books. The PDF format of this sheet is available on your FOR518-A ISO file.
3. **Open the FOR518.inspector Inspector Case file.**
4. **Mount David Lightman's Mac forensic image** (`galaga.E01`).
    - Mounting Instructions

Choose Your Own Adventure Log Analysis

- **Choose one of two choices:**
    - **Choice A: Use Console.app.**
    - **Choice B: Use the command line.**

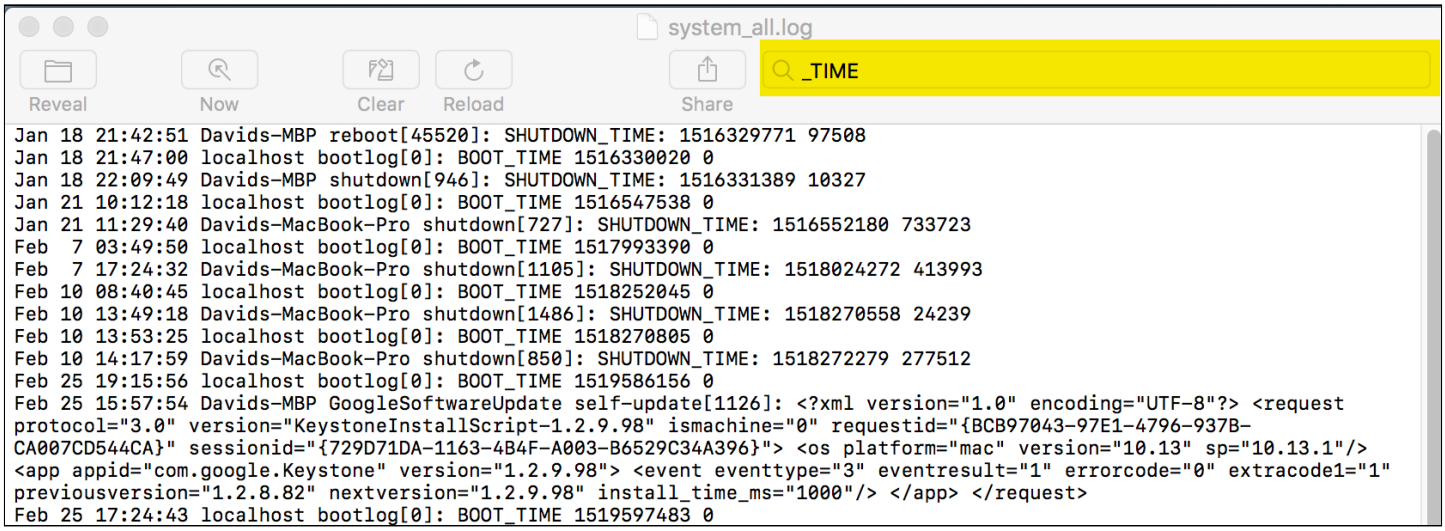
Choice A: Console.app.

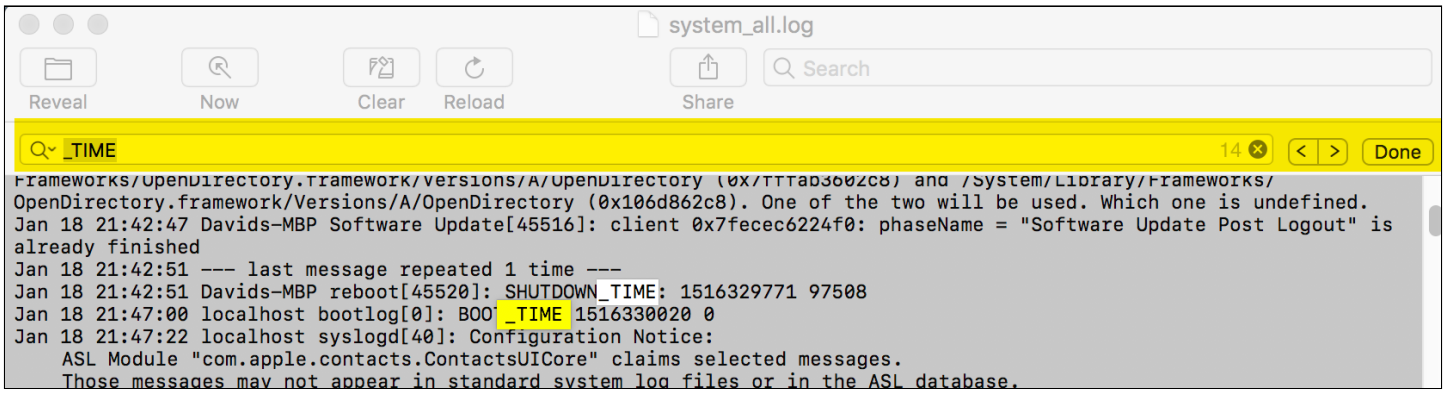
Use the `open` command to open the log file of interest in Console.app . You do not necessarily have to open a specific log file; remove the .log section and you will open your logs in Console.

```
open -a Console <example>.log
```

Use the search functions:

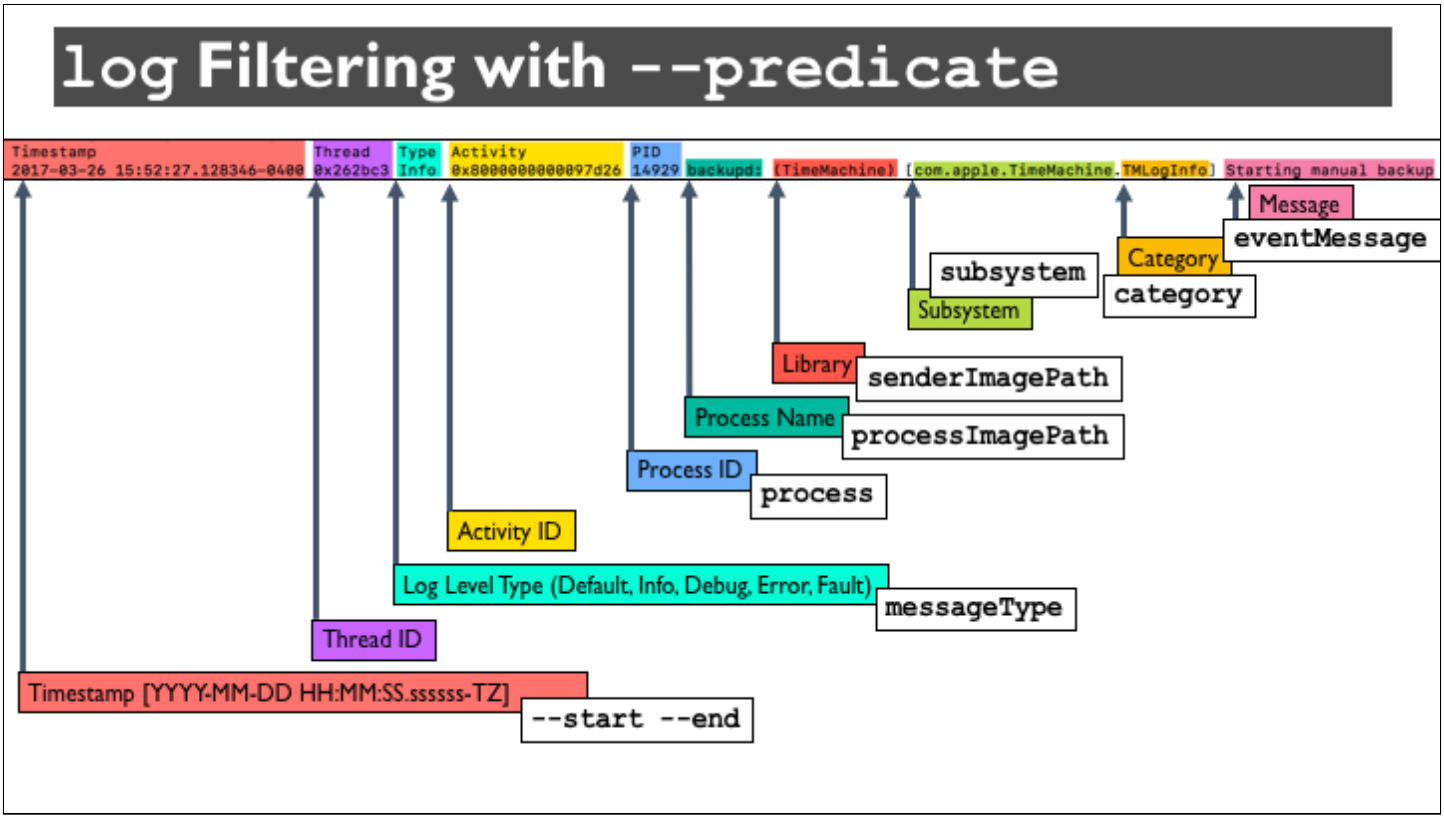
1. Filter text box at the top right
2. “Find” Function - Edit | Find (Command+F)





Choice B: Via the command line using `grep` and/or `log` commands

Use the `log` command with `--predicate` filtering.



Use the `grep` command to search for items of interest.

1. Recommended for students with previous `grep` experience.
2. Use the `man grep` command for options to this utility.

```
grep "some string" <example>.log
```

Exercise: Questions

Volume Analysis

Review these files

Unified logs (`galaga.logarchive` , created in Lab 3.1)

1. What is the USBMSC identifier for the actual USB device mounted most often in the Unified Logs?

_____

Solution

a. AA011024121553093678

b. Use `log show galaga.logarchive/ --timezone UTC --info --predicate 'eventMessage contains "USBMSC"'| awk '{print $13}' | sort | uniq -c`

i. This command filters the USBMSC entries using `log` and pipes the results to an `awk` command to print out only the 13th column (the ID). This output gets piped to `sort` to sort them so it can finally be piped to `uniq -c` to uniquely count each entry.

c. Count the different USBMSC entries for each one. Remember the entries "`000000000820 0x5ac 0x8406 0x820`" are the internal SD card reader and do not count.

2. Looking at the Vendor ID, what company makes the device inserted into the system on March 3, 2018, at 16:11 (UTC)?

_____

Solution

a. Maxtor: `0x00000000 0xd49 0x7250 0x1`

b. To find the Vendor ID, use `log show galaga.logarchive/ --timezone UTC --info --predicate 'eventMessage contains "USBMSC"'`

c. Look up the Vendor ID "`0x0d49`" at http://usb-ids.gowdy.us/read/UD/

3. What is the model of the device associated with ID 070843790D1DDF61?

_____

Solution

a. `FlashBlu 30`

b. Export all the Unified Logs to a text file using the command `log show galaga.logarchive/ --timezone UTC --info > galaga_logs.txt`

c. Search within the context of "`070843790D1DDF61`"; you should be able to find it a few lines below in "`icdd`" messages.

4. When was the volume named SEKRET encrypted (UTC)?

_____

Solution

a. `2018-02-26 01:49:08.663634+0000`

b. Grep or search for the keyword SEKRET - `log show galaga.logarchive/ --timezone UTC --info --predicate 'eventMessage contains "SEKRET"'`

c. Find the entry that shows the "-S <passphrase>".

d. `diskmanagementd: diskmanagement: execve(2) pid=1276 /System/Library/Filesystems/apfs.fs/Contents/Resources/newfs_apfs -A -i -E -S frogger13 -v SEKRET disk5`

5. What file system is this volume using?

_____

Solution

a. APFS (note the use of `newfs_apfs` command).

System Information and State

Review these files

1. Unified Logs (`galaga.logarchive` , created in Lab 3.1)
2. `/Volumes/galaga_mounted/private/var/log/system.log` (remember you should have the full log created in Lab 3.1)
3. `/Volumes/galaga_mounted/private/var/log/daily.out`

1. When was the last time this system booted (UTC)?

_____

Solution

a. Sun Feb 25 22:24:43 UTC 2018

b. Grep or search for BOOT_TIME in the system.log.

c. Even though the Feb 25 19:15:56 timestamped entry is later, in reality, the record timestamp was recorded in local system time, using the Unix epoch timestamp; the last entry is the last startup time, as shown below with the date command.

```
[Sarahs-MBP:FOR518 oompa$ grep BOOT_TIME system_all.log
Jan 18 21:47:00 localhost bootlog[0]: BOOT_TIME 1516330020 0
Jan 21 10:12:18 localhost bootlog[0]: BOOT_TIME 1516547538 0
Feb  7 03:49:50 localhost bootlog[0]: BOOT_TIME 1517993390 0
Feb 10 08:40:45 localhost bootlog[0]: BOOT_TIME 1518252045 0
Feb 10 13:53:25 localhost bootlog[0]: BOOT_TIME 1518270805 0
Feb 25 19:15:56 localhost bootlog[0]: BOOT_TIME 1519586156 0
Feb 25 17:24:43 localhost bootlog[0]: BOOT_TIME 1519597483 0
[Sarahs-MBP:FOR518 oompa$ date -ur 1519586156
Sun Feb 25 19:15:56 UTC 2018
[Sarahs-MBP:FOR518 oompa$ date -ur 1519597483
Sun Feb 25 22:24:43 UTC 2018
```

2. Was this system ever hard powered down?

_____

Solution

a. Yes, on `2018-02-07 08:49:50.789676+0000`

b. Search for "`shutdown cause`" in the Unified Logs. look for entries with a "3".

c. `log show galaga.logarchive/ --timezone UTC --info --predicate 'eventMessage contains[c] "shutdown cause"'`

3. On February 10, 2018 (local system time), what time zone was this system in?

_____

Solution

a. GMT

b. Do a search for the timestamps in `daily.out` with "`2018`"; look for Feb 10.

c. Sat Feb 10 08:49:08 GMT 2018

4. What percentage of the boot drive was allocated on February 7, 2018 (local system time)?

_____

Solution

a. 75%

b. `daily.out log`: Search for the day then look in the Disk Status area for the percentage for root disk "/".

Application Bundles & Extensions

Use the `cd` command to navigate to the kernel extensions directory.

Use `ls -la` to view the contents of this directory; note the timestamp on `logKext.kext`.

Use `ls -laR` on `logKext.kext` to view the recursive contents of this kernel extension.

Use the `plutil -p` command to open the Info.plist file for this extension.

Use `xxd` to view the file signature on the `logKext` binary. (Use "`q`" to quit out of the `less` command.)

```
cd /Volumes/galaga_mounted/System/Library/Extensions/

ls -la

ls -laR logKext.kext

plutil -p logKext.kext/Contents/Info.plist

xxd logKext.kext/Contents/MacOS/logKext | less
```

```
file logKext.kext/Contents/MacOS/logKext
```

1. What is the file signature on the `logKext` binary?

   _____

   Solution

   a. `cffa edfe`

   b. The first four bytes of the file.

2. What type of file is this (via `file` command)?

   _____

   Solution

   `Mach-O 64-bit kext bundle x86_64`

Software Updates

Use the `cd` command to navigate to the system preferences directory.

Use the `open` command to open the `com.apple.SoftwareUpdate.plist` file.

```
cd /Volumes/galaga_mounted/Library/Preferences/

open com.apple.SoftwareUpdate.plist
```

1. What is the name of the recommended update that has yet to install?

   _____

   Solution

   a. `macOS High Sierra 10.13.3 Update Combo`

   b. Use the "`Display Name`" Key.

Use the `cd` command to navigate to the software receipts directory.

Use the `ls -l` command to view all files in this directory. Note the contents of this directory.

Use the `open` command to open the `InstallHistory.plist` file.

```
cd /Volumes/galaga_mounted/Library/Receipts/

ls -l
```

```
open InstallHistory.plist
```

1. How many updates are shown in the `InstallHistory.plist` file?

_____

> **Solution**
>
> a. 14 items
>
> b. Look at the `Root` Key.

2. What native application was updated on February 10, 2018?

_____

> **Solution**
>
> a. iTunes
>
> b. `Item 9`

3. How many times was `logKext` installed, take note of the timestamps?

_____

> **Solution**
>
> a. Twice
>
> b. `Item 11` and `12`
>
> c. `2018-02-25T21:31:26Z` and `2018-02-25T21:35:11Z`

Use the `cd` command to navigate to the `/private/var/log` directory to view the `install.log` file.

Use `grep` to search around the first timestamp that logKext was installed, `2018-02-25 21:31`. Recall that these logs tend to store their timestamps in local system time therefore we need to do some timezone math to compensate by removing 5 hours.

Review the output of this `grep` command and answer the following question.

1. Were administrator credentials provided successfully to install `logKext`?

_____

> **Solution**
>
> a. Yes!
>
> b. Look for the string `2018-02-25 16:30:14-05 Davids-MBP Installer[1354]: Administrator authorization granted.`

```
cd /Volumes/galaga_mounted/var/log

grep "2018-02-25 16:" install.log
```

Use the `cd` command to navigate to the software receipts directory where the receipts are stored.

Use the `ls -lt` command to view all files in this directory. The "`t`" option allows us to sort by last modified time. Note how each receipt *`.plist` and *`.bom` file modified time matches those found in the `InstallHistory.plist` file.

Use the `open` command to open a plist file. Note the similar data found in the `InstallHistory.plist` file.

Use the `lsbom -s` command to view the files for the Text Wrangler application.

```
cd /Volumes/galaga_mounted/var/db/receipts/

ls -lt

open <anyfile>.plist

lsbom -s com.barebones.textwrangler.bom
```

Exercise: Key Takeaways

- **Start getting comfortable with log analysis while also looking at configuration files**
- **Determine how best to review log files for your personal analysis preferences.**

Lab 3.3: User Data & System Configuration - Part I

Objectives

- Get familiar with the macOS user preferences and system configuration data files.
- Get familiar with property lists using Xcode.
- Get more comfortable with the macOS command line using Terminal.
- Use log analysis to help answer some investigative questions.

Lab Preparation

> **Note**
>
> Some of this might already be accomplished via earlier labs, but this is the state that we hope your system is in prior to the start of this lab. Just in case your system rebooted, we are including a guide to help you get back to the proper analysis starting point prior to the beginning of this lab.

1. **Software Preparation**: The following tools will be used in this exercise:
    - Terminal.app
        a. Locate and open the native macOS Terminal.app from /Applications/Utilities/.
    - Xcode.app
        a. Locate and open the Xcode.app from /Applications/.
    - Inspector.app
        a. Locate and open the Inspector.app from /Applications/Inspector Release #/Inspector.app
2. **FOR518 Reference Sheet**: Locate the FOR518 Reference Sheet provided to you in your class material and books. The PDF format of this sheet is available on your FOR518-A ISO file.
3. **Open the FOR518.inspector Inspector Case file.**
4. **Mount David Lightman's Mac forensic image** (`galaga.E01`).
    - Mounting Instructions

Lab: Questions

iOS GUI Artifacts

iOS Keyboard Dynamic Text

Select the " `physical_logical` " acquisition.

Review the contents of the `dynamic-lexicon.dat` file.

iOS Icon Settings

Pick any iOS acquisition.

Review the contents of the `IconState.plist` file.

1. What is the top left application on David's iPhone on the second screen?

_____

> **Solution**
>
> a. FaceTime
>
> b. `Item 1` is the second screen; `com.apple.facetime` is the bundle ID shown first (it goes top to bottom, left to right)

macOS Saved Application State

Use the `cd` command to change the directory to the `dlightman's` Saved Application State directory.

Use the `ls -la` command to list the files in this directory; note how some are symbolic links to `Container` directories.

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Saved\ Application\ State

ls -la

cd com.apple.Safari.savedState

ls -la

open windows.plist
```

1. What website was open in Safari?

_____

> **Solution**
>
> a. `Wikipedia (Spider Monkey)`
>
> b. Look for the `NSTitle` keys.

Bluetooth

Pick any iOS acquisition.

Review the contents of the `com.apple.MobileBluetooth.ledevices.paired.db` file.

1. Was there an Apple Watch associated with this iPhone?

_____

Solution

Yes, David's Apple Watch (`Paired Devices` key)

Briefly take a look at Bluetooth entries in the galaga.logarchive you created in Lab 3.1.

```
log show ~/FOR518/galaga.logarchive --predicate 'process = "bluetoothd"'
```

Network Analysis

Review these files

1. `/Volumes/galaga_mounted/private/var/log/system.log` (remember you should have the full log created in Lab 3.1)
2. `/Volumes/galaga_mounted/Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist`

1. What four Wi-Fi networks did this system associate to?

_____

Solution

a. CrystalPalace (Unified/Airport plist)

b. De Vere Grand Connaught Rooms (Unified/Airport plist)

c. shmoocon (Airport plist)

d. acetomato (Unified only—it was removed by the user in the preferences panel, therefore it was not in the plist file.)

e. `log show galaga.logarchive/ --timezone UTC --info --predicate 'eventMessage contains "BSSID"' | grep configd`

2. Create a timeline of travel activity (UTC)?

Time Frame	Wi-Fi SSID(s)	Possible IP(s)	Possible Location/Country
Feb 07–Feb 10, 2018			
Feb 25–March 3, 2018			

Solution

Time Frame	Wi-Fi SSID(s) Search "SSID" in Unified Logs	Possible IP(s) Search "network changed" in Unified Logs	Possible Location/Country
Feb 07–Feb 10 2018	De Vere Grand Connaught Rooms	10.5.48.38 10.5.49.169	De Vere Grand Connaught Rooms in United Kingdom (GMT)
Feb 25–March 3 2018	CrystalPalace acetomato	192.168.101.138 (Crystal Palace) 192.168.8.133 (acetomato)	Home (Crystal Palace) in US

Lab: Key Takeaways

- Review the contents of user data and system configuration files.
- Determine how the system was used.

Lab 3.4: User Data & System Configuration - Part II

Objectives

- Get familiar with the macOS user preferences and system configuration data files.
- Get familiar with property lists using Xcode.
- Get more comfortable with the macOS command line using Terminal.
- Use log analysis to help answer some investigative questions.

Lab Preparation

> **Note**
>
> Some of this might already be accomplished via earlier labs, but this is the state that we hope your system is in prior to the start of this lab. Just in case your system rebooted, we are including a guide to help you get back to the proper analysis starting point prior to the beginning of this lab.

1. **Software Preparation**: The following tools will be used in this exercise:
    - Terminal.app
        a. Locate and open the native macOS Terminal.app from /Applications/Utilities/.
    - Console.app
        a. Locate and open the native macOS Console.app from /Applications/Utilities.
    - Inspector.app
        a. Locate and open the Inspector.app from /Applications/Inspector Release #/Inspector.app
2. **FOR518 Reference Sheet**: Locate the FOR518 Reference Sheet provided to you in your class material and books. The PDF format of this sheet is available on your FOR518-A ISO file.
3. **Mount David Lightman's Mac forensic image** (`galaga.E01`).
    - Mounting Instructions

Lab Questions

Printing

Use the `cd` command to navigate to the system preferences directory.

Use the `open` command to open the `org.cups.printers.plist` file.

```
cd /Volumes/galaga_mounted/Library/Preferences/

open org.cups.printers.plist
```

1. What kind of printer was used with this system?

   _____

   Solution

   "Brother HL-L2380DW series" (`printer-make-and-model` Key)

2. How was this printer accessed?

   _____

   Solution

   Via the network (`device-uri` Key)

Use the `cd` command to navigate to the Printer Spool directory.

Use the `ls -la` command to view all files in this directory. Note the contents of this directory.

Use strings to view the contents of the third print job, `c00003`.

```
cd /Volumes/galaga_mounted/private/var/spool/cups/

ls -la

strings c00003
```

- Provide the following information for this print job.

   a. What `user` printed this?

      _____

      Solution

      i. David Lightman

      ii. Search around the term "`com.apple.print.JobInfo.PMJobOwner`"

   b. What application did they print from?

      _____

      Solution

      i. Safari

      ii. Search around the term "`com.apple.print.JobInfo.PMApplicationName`"

c. What is the name of the print job?

_____

Solution

i. Red panda - Wikipedia

ii. Search around the term "`job-name`" or "`com.apple.print.JobInfo.PMJobName`"

Use the `file` command on the printer data files.

Use the `open` command to view the PDF printer data files using the Preview application.

```
file d0000*

open -a Preview d0000*
```

1. What did the user print at 3/3/18 4:31 (their system time)?

_____

Solution

The first page of the Wikipedia article for Spider Monkey (`d00004-001`)

Terminal History

Use the `cd` command to change directory to the `dlightman's` home directory.

Use the `cat` command to view the contents of the `.bash_history` file.

```
cd /Volumes/galaga_mounted/Users/dlightman/

cat .bash_history
```

1. What command/s were run to check the `dlightman's` network status?

_____

Solution

a. `ifconfig`

b. `ping google.com`

2. What command software did the `dlightman` install via the brew command?

_____

Solution

`libimobiledevice` (`brew install libimobiledevice`)

Review the contents of the `.bash_sessions` files.

```
cd .bash_sessions

ls -la
```

1. When was the `libimobiledevice` potentially installed (hint: use `grep -r` ?

   _____

   Solution

   a. March 3, 2018 (UTC)

   b. Use a grep to recursively search the files for "brew install" - `grep -r "brew install" *`. This will locate the file: `B7341ECB-98BB-4863-8220-A965CF7DB9C3.history`

   c. Use `stat -x` command on that file to review MAC timestamps.

Autoruns

Use the `cd` command to navigate to one of the launch daemons directories.

Use the `plutil -p` command to open each launch daemon in this directory.

```
cd /Volumes/galaga_mounted/Library/LaunchDaemons/

plutil -p keylogger.plist

plutil -p logKext.plist
```

1. What path and binary are run for the keylogger named "keylogger"?

   _____

   Solution

   a. `/usr/local/bin/keylogger`

   b. `ProgramArguments` Key

2. What is the bundle ID for `logKext` ?

   _____

   Solution

   `com.fsb.logKext` (`Label` Key)

User Access

Review these files

1. `/Volumes/galaga_mounted/private/var/log/system.log` (remember you should have the full log created in Lab 3.1)
2. `/Volumes/galaga_mounted/private/var/log/asl` (remember you should have the full log created in Lab 3.1)
3. `/Volumes/galaga_mounted/private/var/audit` (remember you should have the full log created in Lab 3.1)

1. What two methods did users use to log on to this system?

_____

Solution

a. Login Window

b. Terminal

c. Search "_PROCESS:" in system.log (use the full log created).

2. What are the start time and end time of the logon session associated with PID 612 (local system time)?

_____

Solution

a. Feb 25 17:53:12 -> Mar 3 15:27:39 (2018)

b. `Feb 25 17:53:12 Davids-MBP login[612]: USER_PROCESS: 612 ttys000`

c. `Mar  3 15:27:39 Davids-MBP login[612]: DEAD_PROCESS: 612 ttys000`

3. What user account logged on at this time?

_____

Solution

a. dlightman (Search for “612” or timestamps in ASL.log or audit.log)

b. Audit File:

```
<record version="11" event="logout - local" modifier="0" time="Sat Mar
3 20:27:39 2018" msec=" + 633 msec" >
<subject audit-uid="501" uid="0" gid="20" ruid="501" rgid="20"
pid="612" sid="612" tid="2684354560.0.0.0" />
<return errval="success" retval="0" />
</record>
```

c. ASL File:

```
[ASLMessageID 24869] [Time 2018-02-25 22:53:12Z] [TimeNanoSec
433279000] [Level 5] [PID 612] [UID 0] [GID 20] [ReadGID 80] [Host
Davids-MBP] [Sender login] [Facility com.apple.system.lastlog]
[Message USER_PROCESS: 612 ttys000] [ut_user dlightman] [ut_id s000]
[ut_line ttys000] [ut_pid 612] [ut_type 7] [ut_tv.tv_sec 1519599192]
[ut_tv.tv_usec 433191] [SenderMachUUID 9015BFF2-0D5C-34E3-BE7E-
15DA6FC115C6] [ASLExpireTime 1551221592]
```

Keychain

Use the `cd` command to change directory to the `dlightman's` Keychain directory.

Use the `file` command to view the file type for the files in this directory.

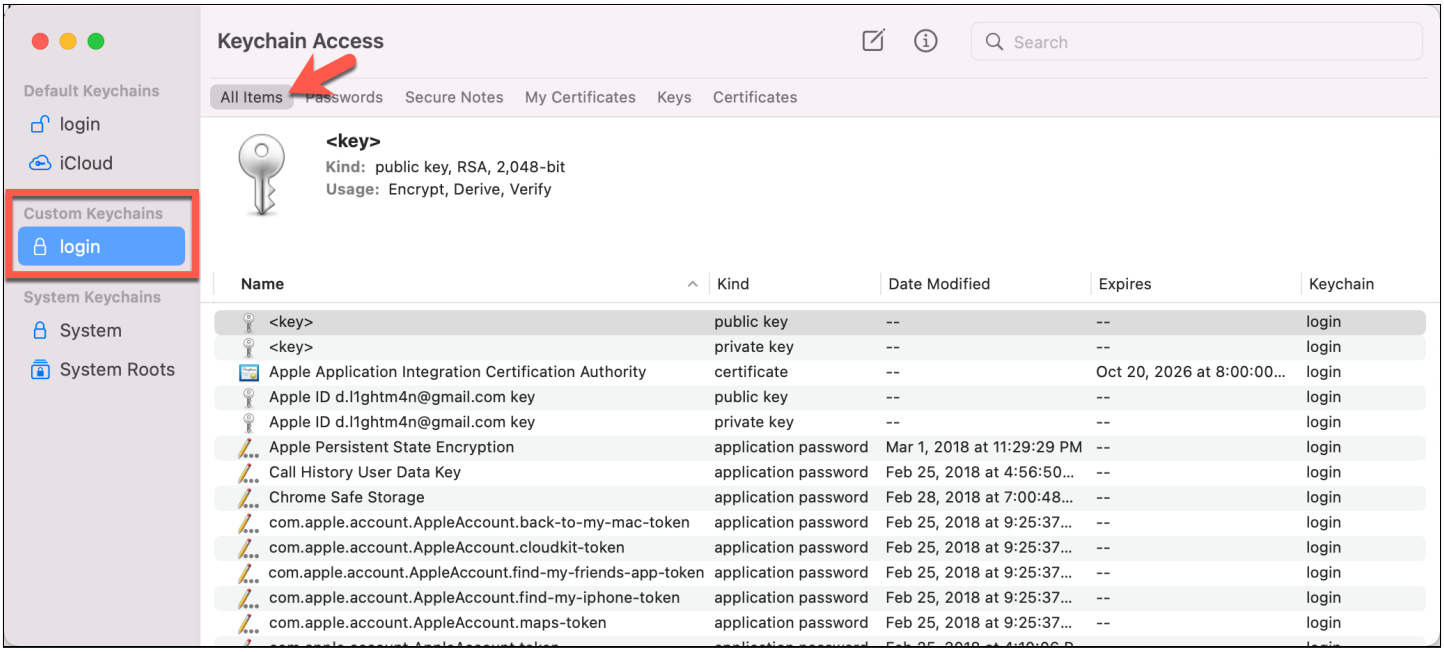
Use `strings` on the `login.keychain-db` to get an idea of what is contained in the file.

Use the open command to view the contents of the `login.keychain-db` using `Keychain Access.app`

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Keychains

file *

strings login.keychain-db | less

open login.keychain-db
```

Once `Keychain Access.app` has been opened, view the `login.keychain-db`. On the left-hand side choose the correct login keychain under “`Keychains`”. The `login` under ‘Default Keychains’ is your keychain—choose login keychain under ‘Custom Keychains’.

In the “`Category`” section, choose “`All Items`”. This will display all keychain items in the main viewing pane.



1. What email address appears to be used for many of the credentials?

_____

Solution

`d.l1ghtm4n@gmail.com`

2. If one of these entries is double-clicked, and the “Show password” checkbox is checked, are you able to see the password?

_____

Solution

No, a password entry box is opened. You’ll need the user’s password (by default) to see these passwords.

3. Does this keychain hold the credentials for an iTunes backup?

_____

Solution

Yes, the entry labeled “ `iOS Backup` ” holds these credentials.

4. What DMG file's password is stored in this keychain?

_____

Solution

`k12.dmg`

Note

You may remove David's Keychain by right-clicking and selecting "Delete Keychain". Select "Delete References".

Extra Credit

- **Keep reviewing log files. Get comfortable with the different types of events in each type.**
- **Review these files in the Inspector application.**

Lab: Key Takeaways

- Review the contents of user data and system configuration files.
- Determine how the system was used.

Lab 4.1: iOS Snapshots, App Permissions, & MRUs

Objectives

- Look at the iOS KTX Snapshots
- Review the App Permissions database (TCC)
- Parse macOS MRUs

Lab Preparation

Note

Some of this might already be accomplished via earlier labs, but this is the state that we hope your system is in prior to the start of this lab. Just in case your system rebooted, we are including a guide to help you get back to the proper analysis starting point prior to the beginning of this lab.

1. **Software Preparation**: The following tools will be used in this exercise:
    - Terminal.app
        a. Locate and open the native macOS Terminal.app from /Applications/Utilities/.
    - Xcode.app
        a. Locate and open the Xcode.app from /Applications/.
    - SQLite Database Browser
        a. You will be using the SQLite Database Browser (Applications/sqlitebrowser.app)
        b. This tool is available on your FOR518-A ISO file in the Tools directory.
        c. The SQLite Manager is available at http://sqlitebrowser.org/
    - Inspector.app
        a. Locate and open the Inspector.app from /Applications/Inspector Release #/Inspector.app
        b. This tool is available on your FOR518-A ISO file in the Tools directory.
2. **FOR518 Reference Sheet**: Locate the FOR518 Reference Sheet provided to you in your class material and books. The PDF format of this sheet is available on your FOR518-A ISO file.
3. **Open the FOR518.inspector Inspector Case file.**
4. **Mount David Lightman's Mac forensic image** (`galaga.E01`).
    - Mounting Instructions
5. **Mount David Lightman's Physical Logical iPhone DMG** (`DavidLightman_physical_logical_dump.dmg`)
    - Mounting Instructions

Lab Questions

iOS App Snapshots

1. **Review iOS Application Snapshots**
    - Open the FOR518.Inspector case file in Inspector.
    - Select the "`physical_logical_dump`" evidence disk. (These files will not be found in the backup acquisitions.)
    - Go to the "File Filter" tab at the top. In the dropdown where it says, "List All Files", select "Path".
    - In the text box, type "/Snapshots/". This should filter all files and directories that contain the term "/Snapshots/".
    - Select the "+" sign on the right to create another filter for "Extension" "contains" and put in "ktx" in the text box.
    - Note the different apps that have snapshots available.
    - Inspector does not have the capability to show them, so they would have to be extracted and reviewed using the Preview.app application. If you prefer to use the mounted DMG, please use the second method below.
    - Extract the Snapshots for the Safari app only. Change the "Path" filter to include the bundle ID for Mobile Safari (/Snapshots/com.apple.mobilesafari).
    - Extract these files (you may choose to put these in a specific "Safari Snapshots" directory) and review them using Preview.app. (Yes, some of them will be "blank"; this is normal.)
2. Run the commands below to mount the DMG. Select the partition labeled "41504653-0000-11AA-AA11-0030654" for the `mount_apfs` command. If you perform a `diskutil list`, it will show up as an APFS volume named "`physical_logical_dump`".

```
sudo mkdir /Volumes/davids_iphone/

hdiutil attach -nomount DavidLightman_physical_logical_dump.dmg

sudo mount_apfs -o rdonly,noexec,noowners /dev/disk#s# /Volumes/davids_iphone/
```

3. Use the `find` command to perform a similar search for KTX files as the Inspector File Filter above.
    - Create a directory for the extracted KTX files.
    - Find and copy the KTX files out to the directory.
        - This command searches the mounted DMG for paths containing "`snapshots`" and files with the filename ending in "`.ktx`". The "`-exec`" copies the found files into the `~/FOR518/extracted_ktx` directory.
    - Finally, open the extracted files directory and review the files.
        - Once opened with finder, select the first image, and press the spacebar to use Quicklook. To review other images, use the arrows to navigate.

```
mkdir ~/FOR518/extracted_ktx

sudo find /Volumes/davids_iphone -ipath "*snapshots*" -iname "*.ktx" -exec cp {} ~/FOR518/
extracted_ktx \;
```

```
open ~/FOR518/extracted_ktx
```

a. What game was being played in the web browser?

_____

Solution

i. Tetris

ii. `4F78A4E9-2A76-4EF8-BC26-FFA211080116@2x.ktx`

iii. `BB592D88-C52C-4D23-B1A3-F2CD60A638F2@2x.ktx`

App Permissions

1. **Review iOS Application Permissions**

   • For David's iPhone, review the TCC database ([`/private/var]/mobile/Library/TCC/TCC.db`). You may choose any acquisition type you want.

   a. What is the application that the user did not allow to use the microphone permission?

   _____

   Solution

   i. WhatsApp: net.whatsapp.WhatsApp

   ii. The "allowed" column in the "access" table is "0" for the bundle ID: net.whatsapp.WhatsApp. This bundle ID belongs to the WhatsApp application.

MRUs

1. **MRUs: Open and Review the contents of the dlightman's /Library/Preferences directory.**

   • Use the `cd` command to change the directory to `dlightman's` /Library/Preferences/ directory.

   • Open the Finder plist file in Xcode. While default settings should open it in Xcode, to explicitly open it in Xcode, use the command `open -a Xcode com.apple.finder.plist`.

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Preferences/

open -a Xcode com.apple.finder.plist
```

2. **Review the Recent Folders.**

   Review the contents of the `com.apple.finder.plist` file.

   a. Under the `FXRecentFolders` key, where did the folder "`iPhone`" exist? (10.15 users will need to extract the BLOB using another tool, try PlistBuddy.)

   _____

Solution

i. `/Volumes/WDPassport/MyBackups/iPhone`

ii. Extract the `file-bookmark` data for the folder `iPhone` and view it in a hex editor. If you are on 10.15, use `PlistBuddy` and `xxd`.

- `/usr/libexec/PlistBuddy -c Print:FXRecentFolders:0:file-bookmark com.apple.finder.plist | xxd`

- Review the newer SFL MRU files (`/Users/dlightman/Library/Application\ Support/com.apple.sharedfilelist`).
- Attempt to open the `com.apple.LSSharedFileList.RecentApplications.sfl2` plist with Xcode. These will fail because of the file extension.
- Use `plutil` to make a readable copy of this plist file and save it as `recentapps.txt`.

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Application\ Support/
com.apple.sharedfilelist

open com.apple.LSSharedFileList.RecentApplications.sfl2

open -a Xcode com.apple.LSSharedFileList.RecentApplications.sfl2

plutil -p com.apple.LSSharedFileList.RecentApplications.sfl2 > ~/FOR518/recentapps.txt

open ~/FOR518/recentapps.txt
```

- Determine the most recent application in the "list" manually; follow the steps from the slides.

b. What is the name of the most recent app used (the first app in the list)?

_____

Solution

Home Printer

3. **Try running the MacMRU python script.**

- Find the script in the exercise folder for this exercise. **Be sure to check your file paths; the location of the MacMRU script will likely be different depending on where you unarchived your files. Make sure the file `ccl_bplist.py` is also in the directory.**
- Run it on the `dlightman's` directory mounted image and output it to a file called `galaga_mrus.txt`.
- Run it again, using the "`–blob_parse_human`" option and save it to a text file called `galaga_mrus_blobs.txt`.
- Review each file using the `open` command.
- For `com.apple.LSSharedFileList.RecentApplications.sfl2` and `com.apple.textedit.sfl2`, answer the following:

a. From what location was the Home Printer application run?

_____

Solution

`/Users/dlightman/Library/Printers/Home Printer.app`

b. What is the filename and path of the document that was most recently opened with the TextEdit application?

_____

Solution

`/Users/dlightman/Desktop/out_logfile.txt`

```
python macMRU.py /Volumes/galaga_mounted/Users/dlightman/ > ~/FOR518/galaga_mrus.txt

python macMRU.py --blob_parse_human /Volumes/galaga_mounted/Users/dlightman > ~/FOR518/
galaga_mrus_blobs.txt

open ~/FOR518/galaga_mrus*
```

Extra Credit

- **Explore the nuances with these files in Inspector.**
- **Try running the macMRU script on your own system.**
- **Review your own TCC.db databases.**

Lab: Key Takeaways

- **Know what applications are requesting permissions and how to determine if they are allowed or not.**
- **Know what applications have recently been used by the user.**
- **See what details can be found in iOS snapshots.**

Lab 4.2: Safari and Mail

Objectives

- Introduce the key data files associated with the Safari web browser and Apple Mail (with some extras thrown in!).
- Parse these data files using native, free, and commercial toolsets.
- Recognize differences in tool output versus raw data.

Lab Preparation

Note

Some of this might already be accomplished via earlier labs, but this is the state that we hope your system is in prior to the start of this lab. Just in case your system rebooted, we are including a guide to help you get back to the proper analysis starting point prior to the beginning of this lab.

1. **Software Preparation**: The following tools will be used in this exercise:
    - Terminal.app
        a. Locate and open the native macOS Terminal.app from /Applications/Utilities/.
    - Xcode.app
        a. Locate and open the Xcode.app from /Applications/.
    - SQLite Database Browser
        a. You will be using the SQLite Database Browser (Applications/sqlitebrowser.app)
        b. This tool is available on your FOR518-A ISO file in the Tools directory.
        c. The SQLite Manager is available at http://sqlitebrowser.org/
    - Inspector.app
        a. Locate and open the Inspector.app from /Applications/Inspector Release #/Inspector.app
        b. This tool is available on your FOR518-A ISO file in the Tools directory.
2. **FOR518 Reference Sheet**: Locate the FOR518 Reference Sheet provided to you in your class material and books. The PDF format of this sheet is available on your FOR518-A ISO file.
3. **Open the FOR518.inspector Inspector Case file.**
4. **Mount David Lightman's Mac forensic image** (`galaga.E01`).
    - Mounting Instructions
5. **Mount David Lightman's Physical Logical iPhone DMG** (`DavidLightman_physical_logical_dump.dmg`)
    - Mounting Instructions

Lab: Questions

Safari Browser

1. **Review the Mac Safari Preferences**
   - Use the `cd` command to change the directory to `dlightman's /Library/Preferences/` directory.
   - Use the `open` command to open the `com.apple.Safari.plist` property list file in Xcode.

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Preferences/

open -a Xcode com.apple.Safari.plist
```

   a. What was the most recent item searched for? (Hint: Item 0 is the newest item.)

   _____

   Solution

   "image jailbroken iphone" (`RecentWebSearches` key)

2. **Review the Mac Web Browser Files**
   - Use the `cd` command to change the directory to `dlightman's /Library/Safari/` directory.
   - Use the `open` command to open all the *.plist files in this directory using Xcode.

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Safari/

open -a Xcode *.plist
```

3. **Review the Mac Safari Bookmarks (this plist might have opened in a separate Xcode window)**
   - Review the `Bookmarks.plist` file.
4. **Review the Mac Safari Downloads**
   - Review the `Downloads.plist` file.

   a. How many items are listed in the Safari download list?

   _____

   Solution

   Two (Note: This is just the current list; more items were downloaded, but they were cleared from the list after 24 hours.)

   b. How many bytes in size is the `LiberiOS11.0.3.ipa` file?

   _____

   Solution

   6,830,024 bytes (you can verify this by looking at the file in the ~/Downloads directory).

c. What domain was the file `Impactor_0.9.44.dmg` downloaded from?

_____

Solution

`cache.saurik.com`

5. **Review the Mac Safari Recently Closed Tabs and Last Session**
   - Review the `RecentlyClosedTabs.plist` file.
   - Review the `LastSession.plist` file.
6. **Review the Mac Safari Internet History**
   - Open this directory to review the files and databases within Finder.
   - Review the `History.db` file.
   - Using the `cp` command, copy out the `History.db` files to your FOR518 directory.
   - Open the main database file in SQLite Database Browser by either opening it using the `File | Open` menu or dragging and dropping History.db to the SQLite Database Browser icon (either in `/Applications` or on the Dock if you put it there).

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Safari/

cp History.db* ~/FOR518
```

   - Briefly review the contents in the `history_visits` and `history_items` tables. We will use the SQL query below to correlate the records in these two tables. You can do this in the "Browse Data" tab.
   - Either type out the following SQL query or copy it from the class notebook (for518.com/notebook) and execute it in the "Execute SQL" tab. Select the “play” button near the top to execute the SQL query.
   - Take a moment to understand what each piece of the query is doing.
     a. Renaming columns using the “AS” feature.
     b. Timestamp conversion using the “DATETIME” function.
     c. Table Joins using “LEFT OUTER JOIN”.
     d. Sorting records using “ORDER BY”.
     e. If you have questions, please call your instructor over.

```
SELECT
HISTORY_VISITS.ID AS "HISTORY ITEM ID",
DATETIME(HISTORY_VISITS.VISIT_TIME+978307200,'UNIXEPOCH') AS "VISIT TIME",
HISTORY_ITEMS.URL,
HISTORY_ITEMS.VISIT_COUNT,
HISTORY_VISITS.TITLE,
HISTORY_VISITS.ORIGIN,
HISTORY_VISITS.LOAD_SUCCESSFUL,
HISTORY_VISITS.REDIRECT_SOURCE,
HISTORY_VISITS.REDIRECT_DESTINATION
```

```
FROM HISTORY_ITEMS
LEFT OUTER JOIN HISTORY_VISITS ON HISTORY_ITEMS.ID == HISTORY_VISITS.HISTORY_ITEM
ORDER BY "VISIT TIME"
```

a. When was the Wikipedia article on “Room 40” visited? (Hint: Add a “WHERE” statement in the query.)

_____

Solution

i. 2017-12-30 21:13:37UTC

ii. You can scroll until you find it, or you can add the following line to the query before the “ORDER BY” function.

- WHERE TITLE LIKE "%ROOM 40%"

b. The first indications where "jailbreak" was searched for—were these searches performed on the Mac system or an iCloud connected device?

_____

Solution

i. On an iCloud connected device. The "origin" column shows the first searches as a "1" (versus a "0").

ii. 2018-02-27 00:49:18 UTC, History Item 1219

iii. Try using: WHERE TITLE LIKE "%jailbreak%".

c. What page was visited the most (even though it failed to load a few times)? (Hint: Change the “ORDER BY” statement.)

_____

Solution

i. `http://shmoocon.org/schedule/#sunday`, 7 times.

ii. ORDER BY "VISIT_COUNT" DESC

7. **Review the iOS Safari Internet Thumbnails**

- Review the KTX files in the Safari `Thumbnails` directory. (You may choose to put these in a specific “Safari Thumbnails” directory. You can view them individually by pressing the space bar, or use the ‘View in External Application’ option under the Preview tab.)
- Change the File Filter path from above to “ `/Thumbnails/` ”.
- Review these thumbnails; these were the current contents of each tab on the iOS device when it was acquired.

8. **Review the iOS Safari CloudTabs Database**

- Navigate to the `/private/var/mobile/Library/Safari/` directory.
- Review the `CloudTabs.db` database within Inspector. This database is not located in the iOS backup acquisitions; however, it is available on the Mac system image if you choose to look at it from the Mac side later.

a. How many devices are syncing to David’s iCloud?

_____

Solution

i. Two, David's MacBookPro and David's iPhone

ii. Review the `cloud_tab_devices` table

b. What two websites did the MacBook Pro have opened when it was last synced?

_____

Solution

i. Google Search for Ars Technica

ii. CNN Money

iii. Review the `cloud_tabs` table for the MacBook Pro Device GUID: ED3C80D9-9F03-4440-A903-3794C384A4CD.

Apple Mail

1. **Mail Accounts**

- Use the cd command to change the directory to the `dlightman's` Apple Accounts directory `/Users/dlightman/Library/Accounts/`.
- Copy the `Accounts4.sqlite` database files to your FOR518 directory and open the database with SQLite Database Browser.

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Accounts/

cp Accounts4.sqlite* ~/FOR518/
```

- In the "Browse Data" tab, view the "ZACCOUNTTYPE" table.

a. Which account type "number" (Z_PK) is associated with "IMAP"? (Hint: ZACCOUNTTYPEDESCRIPTION)

_____

Solution

i. 38

ii. Filter for "IMAP" in the ZACCOUNTTYPEDESCRIPTION column.

- Review the contents of the "ZACCOUNT" table.

b. How many accounts have the type "IMAP" (38) associated with them? (Hint: ZACCOUNTTYPE)

_____

Solution

i. Two

ii. Filter for "38" in the ZACCOUNTTYPE column.

c. What is the number (Z_PK) associated with the account with the GUID 8E359999-5616-4625-B74F-46E812760213?

_____

Solution

i. 5

ii. Look for it in the Z_PK column.

- Review the contents of the "ZACCOUNTPROPERTY" table.

d. Looking for entries associated with a "5" from the previous question in the "ZOWNER" column, what name and email is used for this account? (Hint: EmailAliases)

_____

Solution

i. David Lightman, `d.l1ghtm4n@gmail.com`

ii. Filter for "5" in the "ZOWNER" column, then view the BLOBs associated with these entries—focus on the EmailAliases record. This contains a binary plist file containing this information. If you look closely, you can determine this without extracting the plist data, but that could be done as well.

2. **Apple Mail Directory**

- Moving back to David's system image, use the cd command to change the directory to the `dlightman's` Apple Mail directory `/Users/dlightman/Library/Mail/V5/`.
- Use the "`ls -l`" command to view the files in this directory.
- Browse into the GUID labeled "`8E359999-5616-4625-B74F-46E812760213`."
- Perform a recursive listing on this directory using "`ls -laR`". Note the nested structure of the email directories.

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Mail/V5/

ls -l

cd 8E359999-5616-4625-B74F-46E812760213/

ls -laR
```

- Navigate to the MailData directory to review the "Envelope Index" email database.
- Copy out and review the "Envelope Index" database using SQLite Database Browser.

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Mail/V5/MailData/

cp Envelope\ Index* ~/FOR518/
```

- Type or copy from the FOR518 Notebook (for518.com/notebook) the following SQL query and execute it.

```
SELECT MESSAGES.ROWID, READ, FLAGGED, DELETED,
DATETIME(DATE_SENT,'UNIXEPOCH') AS DATE_SENT,
DATETIME(DATE_RECEIVED,'UNIXEPOCH') AS DATE_RECEIVED,
DATETIME(DATE_CREATED,'UNIXEPOCH') AS DATE_CREATED,
DATETIME(DATE_LAST_VIEWED,'UNIXEPOCH') AS DATE_LAST_VIEWED,
MAILBOXES.URL, ADDRESSES.ADDRESS, SUBJECTS.SUBJECT,
```

```
SNIPPET FROM MESSAGES
LEFT JOIN ADDRESSES ON MESSAGES.SENDER == ADDRESSES.ROWID
LEFT JOIN SUBJECTS ON MESSAGES.SUBJECT == SUBJECTS.ROWID
LEFT JOIN MAILBOXES ON MESSAGES.MAILBOX == MAILBOXES.ROWID
```

a. Find the message with the subject “C Is For Cookie”; what email sent this message?

_____

Solution

i. `no-reply@yelp.com`

ii. Either scroll through the subject column manually or add “WHERE SUBJECTS.SUBJECT LIKE '%COOKIE%'” to the query at the very end.

b. What is the original epoch time of the DATE_LAST_VIEWED for this message?

_____

Solution

i. 2017-12-23 02:41:28 = 1513996888

ii. Remove the section of the query that does the conversion.

i. “DATETIME(DATE_LAST_VIEWED, 'UNIXEPOCH', 'LOCALTIME') AS”

iii. Or look for the original content in the "messages" table in the `date_last_viewed` column with ROWID = 29.

- Find the original email message in the file system.
- Look at the URL in the database output.
  i. “imap://8E359999-5616-4625-B74F-46E812760213/%5BGmail%5D/All%20Mail”
- View the contents of this message using the cat command.
  i. Note the metadata plist contents at the end of the message.
- Open the email message `29.partial.emlx` in TextEdit, using the "`open`" command. This should open this email in the Mail application.
  i. It is a bit easier to read; however, you will need to play around with the Mail interface to read headers and metadata.

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Mail/V5/8E359999-5616-4625-B74F-46E812760213/[Gmail].mbox/All\ Mail.mbox/66BF2B07-39F7-4E41-8A65-FA44E73B388D/Data/Messages

cat 29.partial.emlx

open 29.partial.emlx
```

3. **iOS Email**

- Review the contents of the `/mobile/Library/Mail/` directories in either of the backup files of David’s iPhone (encrypted or unencrypted).
- Now go to the same directory in the Logical/Physical acquisition and review its contents.

- This is a good example of how much more email data is available in a physical acquisition as opposed to a logical/backup acquisition.

4. **EXTRA CREDIT: Mac and iOS Safari and macOS Email Analysis with Inspector**
    - Review these same files under the “Internet” and “Communication” tabs.
    - You may have to run the “Advanced” functions in the Evidence Status section.

Extra Credit

- **Keep exploring the property lists and SQLite databases associated with the Safari browser.**
- **Explore the nuances with these files in Inspector.**
- **Get comfortable using the Inspector interface—browse other email messages.**
- **Review the Envelope Index to find more information pertaining to various email messages.**

Lab: Key Takeaways

- **Know the key files associated with the Safari web browser and Apple Mail and where to find them in the file system.**
- **Know which files are available with different types of iOS acquisitions.**
- **Know what your tools are parsing and what they are showing (or not showing) you.**
- **Get comfortable using the Inspector application.**

Lab 4.3: Applications: Part I

Objectives

- Introduce the key data files associated with various applications.
- Parse these data files using native, free, and commercial toolsets.
- Recognize differences in tool output versus raw data.

Lab Preparation

> **Note**
>
> Some of this might already be accomplished via earlier labs, but this is the state that we hope your system is in prior to the start of this lab. Just in case your system rebooted, we are including a guide to help you get back to the proper analysis starting point prior to the beginning of this lab.

1. **Software Preparation**: The following tools will be used in this exercise:
    - Terminal.app
        a. Locate and open the native macOS Terminal.app from /Applications/Utilities/.
    - Xcode.app
        a. Locate and open the Xcode.app from /Applications/.
    - SQLite Database Browser
        a. You will be using the SQLite Database Browser (Applications/sqlitebrowser.app)
        b. This tool is available on your FOR518-A ISO file in the Tools directory.
        c. The SQLite Manager is available at http://sqlitebrowser.org/
    - Inspector.app
        a. Locate and open the Inspector.app from /Applications/Inspector Release #/Inspector.app
        b. This tool is available on your FOR518-A ISO file in the Tools directory.
2. **FOR518 Reference Sheet**: Locate the FOR518 Reference Sheet provided to you in your class material and books. The PDF format of this sheet is available on your FOR518-A ISO file.
3. **Open the FOR518.inspector Inspector Case file.**
4. **Mount David Lightman's Mac forensic image** (`galaga.E01`).
    - Mounting Instructions
5. **Mount David Lightman's Physical Logical iPhone DMG** (`DavidLightman_physical_logical_dump.dmg`)
    - Mounting Instructions

Lab: Questions

Mac Instant Messaging

Use the `cd` command to go to `dlightman's` Preferences directory.

Use the `open` command to open all the property list files in this directory.

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Preferences/

open *.plist
```

Filter for all `plist` files with the keyword "iChat" in them (use the lower left filter box).

Review the contents of these files.

Review the contents of the `com.apple.iChat.Jabber.plist` file.

1. What email is David chatting from via Jabber?

   _____

   Solution

   a. `d.lightman@gmail.com`

   b. There is also a `d.l1ghtm4n@gmail.com` account, however that is not an "Active" account in the "ActiveAccounts" key. Look at the GUIDs assigned to each account.

   Use the `cd` command to go to `dlightman's` Messages Archive, `/Volumes/galaga_mounted/Users/dlightman/Library/Messages/` directory.

   Use the `ls` command to list the contents of this directory; review the contents.

   Navigate to the Archive directory.

   Use the `ls` command to list the contents of this directory; review the contents.

   Navigate to the chats on 2018-02-27.

   Using "`plutil -p`", look at the plist contents of this chat.

   - It is an ugly NSKeyedArchive binary plist, not much fun to parse by hand!

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Messages/

ls -l

cd Archive/

ls -l

cd 2018-02-27
```

```
plutil -p Jen\ Mack\ on\ 2018-02-27\ at\ 18.28.53.ichat
```

2. What video game is the file transfer associated with?

_____

Solution

Galaga (Galaga Nos. 508 514 510 Part Operating Manual Form No. 0508003000000 Midway-2.pdf)

Review the `chat.db` database. Navigate back to the Messages directory.

Copy out the `chat.db` files to your FOR518 directory.

Open these files in the SQLite Database Browser.

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Messages/

cp chat.db* ~/FOR518
```

Review the contents of this database; start with the "message" table.

3. Review entry ROWID = 38 in the text field—what is the message?

_____

Solution

a. Emoji (Soup/Pho/Ramen)

b. 0x f09f8d9c

c. Luckily, SQLite Database Browser has some support for emojis!

4. What about entry ROWID = 32—is this a message, just an attachment, or both?

_____

Solution

It is both. The message is “What!?” but if you look at the hex it has a few extra bytes that happen to be indicative of an attachment. You can also look for the “1” in the "cache_has_attachments" column.

5. Find entry 32 in the "message_attachments_join" table. What attachment ID does entry 32 associate with?

_____

Solution

3 (attachment_id column)

6. In the "attachment" table, find attachment “3”; find the on-disk location of the attachment. What is the attachment a picture of?

_____

Solution

National Squirrel Agency squirrel talking about classified nuts!

iOS Call History

On David's iPhone (any acquisition).

Navigate to the `CallHistory.storedata` file in the [`/private/var]/mobile/Library/CallHistoryDB/` directory.

1. How many calls are in the database?

   _____

   Solution

   a. 15

   b. ZCALLRECORD Table

2. How many FaceTime calls are in the database?

   _____

   Solution

   a. 1

   b. Look for com.apple.FaceTime under ZSERVICE_PROVIDER.

3. Who was the contact for this FaceTime call?

   _____

   Solution

   a. `1337jmack@gmail.com`

   b. ZADDRESS column

Mac Calendar

Use the `cd` command to go to dlightman's Calendars directory.

Use the `ls -l` command to list the contents of the directory.

Copy out and view the Calendar Cache database in SQLite Database Browser.

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Calendars/

ls -l

cp Calendar\ Cache* ~/FOR518/
```

Type or copy (for518.com/notebook) the following query on the database.

```
SELECT
DATETIME(ZCREATIONDATE+978307200,'UNIXEPOCH','LOCALTIME') AS "CREATED",
DATETIME(ZDATESTAMP+978307200,'UNIXEPOCH','LOCALTIME') AS "LAST MODIFIED",
DATETIME(ZSTARTDATE+978307200,'UNIXEPOCH','LOCALTIME') AS "EVENT START",
DATETIME(ZENDDATE+978307200,'UNIXEPOCH','LOCALTIME') AS "EVENT END",
ZTIMEZONE,
ZCALENDARITEM.ZTITLE AS "EVENT", ZNODE.ZTITLE AS "CALENDAR/LIST" ,
ZCOMPLETEDDATE, ZSTATUS
FROM ZCALENDARITEM
LEFT JOIN ZNODE ON ZCALENDARITEM.ZCALENDAR = ZNODE.Z_PK
```

1. What application put the event “The Schrödinger Lecture 2018: Professor Ben L. Feringa” into the Calendar?

_____

Solution

Eventbrite

2. Is the calendar titled "London" a Calendar or a Reminder List?

_____

Solution

Reminder List, the events do not have a start/finish and some entries have a ZSTATUS message.

3. Which two time zones do you see in these events?

_____

Solution

a. America/New_York

b. Europe/London

c. Review the ZTIMEZONE column

Use the `cd` command to go to one of the calendars.

Use the `ls -l` command to list the contents of this directory.

Use the `open` command to open the `Info.plist` file for this calendar.

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Calendars/BB4D60EF-A39B-4867-9E93-
B85162E9BF2E.caldav

ls -l

open Info.plist
```

4. What kind of calendar is this?

_____

Solution

CalDAV (`Type` Key)

5. What is the title for this calendar?

_____

Solution

iCloud (`Title` Key)

6. What is the login for this calendar?

_____

Solution

`d.l1ghtm4n@gmail.com` (`Login` Key)

Use the `cd` command to go to one of the calendars in this calendar directory (`1A86889D-DD11-4EF6-A265-4D8B4E7B7604.calendar`).

Use the `ls -l` command to list the contents of this directory.

Use the `open` command to open the Info.plist file for this calendar.

```
cd 1A86889D-DD11-4EF6-A265-4D8B4E7B7604.calendar

ls -l

open Info.plist
```

7. What is the title for this calendar?

_____

Solution

Work (`Title` Key)

8. What is the time zone of this calendar?

_____

Solution

America/New_York (`TimeZone` Key)

Use the `cd` command to go to the default calendar /Events directory.

Use the `1s -l` command to list the contents of this directory.

```
cd Events/

ls -l
```

9. How many events are in this calendar (*.ics files)?

   _____

   Solution

   Three

   Use the `cat` command to view the contents of the `C4D9487F-1A0F-42E7-93A3-9847D8784B58.ics` file.

   ```
   cat C4D9487F-1A0F-42E7-93A3-9847D8784B58.ics
   ```

10. When was this calendar item created?

    _____

    Solution

    20180210T103051Z, February 10, 2018, 10:30:51 UTC (CREATED)

11. When did this calendar item occur?

    _____

    Solution

    20180210T183000 = February 10, 2018, at 18:30:00 UTC (DTSTART)

12. Where is this event likely to occur?

    _____

    Solution

    a. At the Shard building in London.

    b. X-APPLE-STRUCTURED-LOCATION or LOCATION

Contacts (Address Book)

Use the `cd` command to go to `dlightman's` Address Book directory.

Use the `ls -l` command to list the contents of this directory. Note the contents.

Use the `cd` command to enter the directory for the default source for the Address Book using the GUID noted above.

Use the `ls -l` command to list the contents of this directory. Note the contents.

Use the `cd` command to enter the Metadata/ directory.

Use the `ls -l` command to list the contents of this directory.

```
cd /Volumes/galaga_mounted/Users/dlightman/Library/Application\ Support/AddressBook/

ls -l

cd Sources/2B3A0FE4-7594-4474-B9D9-3C2B21A637E1

ls -l

cd Metadata/
```

1. How many groups are in this Address Book?

   _____

   Solution

   a. One

      i. `C27B3CC2-1E92-4AFB-9EA8-44C88C31A1EB:ABGroup.abcdg`

2. How many persons are in this Address Book?

   _____

   Solution

   Six, all that end with `*.abcdp`

   Use the `plutil -p` command to view the `DF2CDB39-EAE9-462B-B030-FA7E87FF8C83:ABPerson.abcdp` file, piping the output to the `less` utility. (Use "`q`" to exit `less`.)

   ```
   $ plutil -p DF2CDB39-EAE9-462B-B030-FA7E87FF8C83:ABPerson.abcdp | less
   ```

3. What is the full name of this contact?

   _____

   Solution

   Jen Mack (`First` and `Last` Keys)

4. What is her email address?

   _____

   Solution

   `1337jmack@gmail.com` (`Email` Key)

5. What is her phone number?

_____

> **Solution**
>
> +15714578083 (**Phone** Keys)

6. When was this contact created?

_____

> **Solution**
>
> 2017-12-23 00:54:01 +0000 (**Creation** Key)

Using the **cd** command, traverse back to the previous directory and into the **Images** directory.

List the contents of this folder using the **ls -l** command.

Using the **open** command, open all the files in this directory.

```
cd ../Images/

ls -l

open *
```

7. What picture does David have set for the Jen Mack contact?

_____

> **Solution**
>
> a. Queen Elizabeth in Lego form
>
> b. The GUID of the images matches the contact GUID previously seen.

Lab: Key Takeaways

- **Know the key files associated with certain applications and where to find them in the file system.**
- **Know which files are available with different types of iOS acquisitions.**
- **Know what your tools are parsing and what they are showing (or not showing) you.**
- **Get comfortable using the Inspector application.**

Lab 4.4: Applications: Part II

Objectives

- Introduce the key data files associated with various applications.
- Parse these data files using native, free, and commercial toolsets.
- Recognize differences in tool output versus raw data.

Lab Preparation

> **Note**
>
> Some of this might already be accomplished via earlier labs, but this is the state that we hope your system is in prior to the start of this lab. Just in case your system rebooted, we are including a guide to help you get back to the proper analysis starting point prior to the beginning of this lab.

1. **Software Preparation**: The following tools will be used in this exercise:
    - Terminal.app
        a. Locate and open the native macOS Terminal.app from /Applications/Utilities/.
    - Xcode.app
        a. Locate and open the Xcode.app from /Applications/.
    - SQLite Database Browser
        a. You will be using the SQLite Database Browser (Applications/sqlitebrowser.app)
        b. This tool is available on your FOR518-A ISO file in the Tools directory.
        c. The SQLite Manager is available at http://sqlitebrowser.org/
    - Inspector.app
        a. Locate and open the Inspector.app from /Applications/Inspector Release #/Inspector.app
        b. This tool is available on your FOR518-A ISO file in the Tools directory.
2. **FOR518 Reference Sheet**: Locate the FOR518 Reference Sheet provided to you in your class material and books. The PDF format of this sheet is available on your FOR518-A ISO file.
3. **Open the FOR518.inspector Inspector Case file.**
4. **Mount David Lightman's Mac forensic image** (`galaga.E01`).
    - Mounting Instructions
5. **Mount David Lightman's Physical Logical iPhone DMG** (`DavidLightman_physical_logical_dump.dmg`)
    - Mounting Instructions

Lab: Questions

Notes

In David's iPhone in the FOR518.Inspector case file

Find and extract the NoteStore.sqlite database to your FOR518 directory. (You may choose whichever acquisition you want. If you choose the Physical/Logical acquisition, be sure to extract the *.shm and the *.wal files as well.)

View the database in the SQLite Database Browser.

Open the "ZICCLOUDSYNCINGOBJECT" table.

Filter the Z_ENT column by "11"—These are the "Note Folders."

1. How many Note Folders are there?

_____

Solution

a. 3

b. Z_PK = 1, 2, 15

2. What is the Z_PK for the Folder titled "London"?

_____

Solution

a. 15

b. ZTITLE2 or ZNESTEDTITLEFORSORTING

• Clear the previous filter. Filter the ZFOLDER column by "15"—These are the Notes in the "London" folder.

3. How many notes are there in the "London" Folder and what are their Z_PK #'s?

_____

Solution

5 = 12, 13, 14, 17, 19

• Review the record data for Note "14," titled "Visit The National Museum of Computing | The National Museum of Computing."

4. What value is associated ZNOTEDATA for note "14"?

_____

Solution

a. 4

b. ZNOTEDATA

• Remove the filter from ZFOLDER, and filter on ZNOTE for "14".

5. What URL does this note contain?

_____

Solution

a. `http://www.tnmoc.org/visit`

b. ZURLSTRING

Move to the ZICNOTEDATA table, and filter on ZNOTE = "14" **or** Z_PK = "4".

Double-click and review the binary BLOB data in the ZDATA column.

Extract this BLOB data using the "Export" button.

Save it as note_extract.gz to your FOR518 directory; you have to select the "All Files" option in the Save window.

Navigate to this file, double-click to unarchive, and review its contents in a hex viewer.

Apple Pay/Wallet/Passes

In David's iPhone, find the `/mobile/Library/Passes/` directory. Do this first on the Backup Acquisitions.

1. There is only one "card" available. What kind of card is it?

_____

Solution

a. Starbucks Card

b. You can find this by looking at the logo pictures, the pass.json file, or the signature file.

2. What is the last four digits of this card?

_____

Solution

a. 0930

b. View the `pass.json` file—Look for "`auxiliaryFields`".

3. How much money is left on this card?

_____

Solution

a. $2.62

b. View the `pass.json` file—Look for "BALANCE".

Photos

Use the `cd` command to go to `dlightman's` Photos Library directory.

Use the `ls -la` command to list the contents of this directory. Note the contents.

Navigate to the database directory.

Use the `ls -la` command to list the contents of this directory. Note the contents.

Copy out the Photos database to your FOR518 directory.

Open this database in SQLite Database Browser.

```
cd /Volumes/galaga_mounted/Users/dlightman/Pictures/Photos Library.photoslibrary

ls -la

cd database/

ls -la

cp photos.db* ~/FOR518/
```

Review the contents of the "RKAlbum" Table. Note the different Album names and associated metadata.

1. Which Album was likely created because of a third-party application that was installed on David's iPhone?

   _____

   Solution

   a. Instagram: This is not one of the "default" Photos albums.

   b. "`name`" column

   • Review the contents of the "RKPlace" Table.

2. What two countries have photos been taken in?

   _____

   Solution

   a. United States and Great Britain

   b. `defaultName` or `countryCode` columns

   • Review the contents of the "RKMaster" Table.

3. Find image "IMG_0087.HEIC" using the file on the filename column. What is the creation timestamp of this photo (UTC)?

   _____

Solution

a. 539983657.029676 = 2018-02-10 19:27:37 Sat UTC

b. Find the timestamp in fileCreationDate column; use `date -r 539983657` in the Terminal to change to human-readable time (be sure to use only the digits before the decimal point).

- Review the imagePath column for this photo; find this in the "Masters" directory on your mounted file system.
- Open this file using the Preview.app (usually the default it you open it in Finder and double-click it).

4. What city was this photo taken in?

_____

Solution

a. London, GB

b. Use the Preview.app “Inspector” (Tools | Inspector)

Maps

Go to the Maps directory on David’s iPhone Backups: `/mobile/Applications/com.apple.Maps/Library/Maps/`

- Note the lack of files that are backed up for the Maps application!

Go to the Maps directory on the Physical/Logical acquisition: `/private/var/mobile/Containers/Data/Application/C5CD18E2-6440-4E23-B31E-E78FFC755B65/Library/Maps/`

- We have a few more files to do analysis on here!

Review the `GeoHistory.mapsdata` plist file to see the Maps history data.

Look at the entry labeled 27B425CD-9991-4EB0-B931-59A070CC5FD2

1. What was searched for in this entry?

_____

Solution

a. Ramen in Arlington

b. View the "contents" key

Find the file named `27B425CD-9991-4EB0-B931-59A070CC5FD2` in the path `/private/var/mobile/Containers/Data/Application/C5CD18E2-6440-4E23-B31E-E78FFC755B65/Library/Maps/ReportAProblem/Search/`

Note the contents of this file.

Perform a File Filter for the path "/Snapshots/com.apple.Maps/".

Export these KTX snapshot files to their own directory in your FOR518 directory. (You can view them individually by pressing the space bar, or use the ‘View in External Application’ option under the Preview tab.)

1. Can you say definitely that this device was in a certain location? Where is the approximate location?

_____

Solution

Yes, the file `CB6D4077-BAA5-4896-B20B-4780B5A97982@2x.ktx` shows this device was close to a Starbucks in downtown London. This can be determined by searching for some of the locations listed or the street names.

iOS Third-Party Apps

1. Select any iOS acquisition. Can you find the PIN code to the Photo Vault App (com.enchantedcloud.photovault)?

_____

Solution

a. 4242

b. Look in `/mobile/Applications/com.enchantedcloud.photovault/Library/Preferences/com.enchantedcloud.photovault.plist` for the PIN key.

2. What was the last city that was searched in for the Eventbrite application?

_____

Solution

a. London, United Kingdom

b. `/mobile/Applications/com.eventbrite.attendee/Library/Preferences/com.eventbrite.attendee.plist` - "current user city" Key

3. Who was being chatted with in WhatsApp?

_____

Solution

a. JMack

b. `/mobile/Applications/group.net.whatsapp.WhatsApp.shared/ChatStorage.sqlite`

c. Look in the ZWAMESSAGE table.

Lab: Key Takeaways

- **Know the key files associated with certain applications and where to find them in the file system.**
- **Know which files are available with different types of iOS acquisitions.**
- **Know what your tools are parsing and what they are showing (or not showing) you.**
- **Get comfortable using the Inspector application.**

Lab 5.1: Patterns of Life

Objectives

- Get familiar with various iOS and macOS pattern-of-life databases.

Lab Preparation

> **Note**
>
> Some of this might already be accomplished via earlier labs, but this is the state that we hope your system is in prior to the start of this lab. Just in case your system rebooted, we are including a guide to help you get back to the proper analysis starting point prior to the beginning of this lab.

1. **Software Preparation**: The following tool will be used in this exercise:
    - Terminal.app
        a. Locate and open the native macOS Terminal.app from /Applications/Utilities/.
2. **FOR518 Reference Sheet**: Locate the FOR518 Reference Sheet provided to you in your class material and books. The PDF format of this sheet is available on your FOR518-A ISO file.
3. **Mount David Lightman's Mac forensic image** (`galaga.E01`).
    - Mounting Instructions

Lab: Questions

macOS

Review the macOS knowledgeC.db Database for Application Usage

Navigate to the `Knowledge` directory below in your mounted macOS image.

Use `cp` to copy out the `knowledgeC.db` database files to your `FOR518` directory.

Use the `open` command to view these files in DB Browser for SQLite.

Browse the contents in the tables.

```
cd /Volumes/galaga_mounted/private/var/db/CoreDuet/Knowledge/

cp knowledgeC.db* ~/FOR518

open ~/FOR518/knowledgeC.db
```

Copy from the FOR518 notebook the following query and execute it on the `knowledgeC.db` database.

```
SELECT
datetime(ZOBJECT.ZCREATIONDATE+978307200,'UNIXEPOCH') as "ENTRY CREATION",
ZOBJECT.ZVALUESTRING AS "BUNDLE ID",
CASE ZOBJECT.ZSTARTDAYOFWEEK
    WHEN "1" THEN "Sunday"
    WHEN "2" THEN "Monday"
    WHEN "3" THEN "Tuesday"
    WHEN "4" THEN "Wednesday"
    WHEN "5" THEN "Thursday"
    WHEN "6" THEN "Friday"
    WHEN "7" THEN "Saturday"
END "DAY OF WEEK",
ZOBJECT.ZSECONDSFROMGMT/3600 AS "GMT OFFSET",
datetime(ZOBJECT.ZSTARTDATE+978307200,'UNIXEPOCH') as "START",
datetime(ZOBJECT.ZENDDATE+978307200,'UNIXEPOCH') as "END",
(ZOBJECT.ZENDDATE-ZOBJECT.ZSTARTDATE) as "USAGE IN SECONDS"
FROM ZOBJECT
WHERE ZSTREAMNAME IS "/app/inFocus"
ORDER BY "START"
```

1. How many time zones was this device likely in using the active records in this database?

   _____

   Solution

   a. Two, GMT (0) and -5 (East Coast of US)

   b. Look at the 'GMT offset' column.

2. On what days was Google Chrome used (Bundle ID: com.google.Chrome)?

   _____

   _____

   Solution

   a. 2018-02-25

   b. 2018-03-01

   c. 2018-03-03

   d. Add "and "bundle id" like '%chrome%'" to the end of the WHERE clause.

3. What was the most used "application" in a single session?

_____

Solution

a. `com.apple.loginwindow` - The laptop was sitting at the login screen for a good amount of time.

b. Change the "ORDER BY" line from "START" to "USAGE IN SECONDS"

Review the macOS knowledgeC.db Database for Application Activities

Copy from the FOR518 notebook the following query and execute it on the `knowledgeC.db` database.

```
SELECT
DATETIME(ZOBJECT.ZCREATIONDATE + 978307200, 'UNIXEPOCH') AS "ENTRY CREATION",
CASE ZOBJECT.ZSTARTDAYOFWEEK
    WHEN "1" THEN "Sunday"
    WHEN "2" THEN "Monday"
    WHEN "3" THEN "Tuesday"
    WHEN "4" THEN "Wednesday"
    WHEN "5" THEN "Thursday"
    WHEN "6" THEN "Friday"
    WHEN "7" THEN "Saturday"
    END "DAY OF WEEK",
ZOBJECT.ZVALUESTRING AS "BUNDLE ID",
ZSTRUCTUREDMETADATA.Z_DKAPPLICATIONACTIVITYMETADATAKEY__ACTIVITYTYPE
AS "ACTIVITY TYPE",
ZSTRUCTUREDMETADATA.Z_DKAPPLICATIONACTIVITYMETADATAKEY__TITLE
AS "TITLE",
DATETIME(ZSTRUCTUREDMETADATA.Z_DKAPPLICATIONACTIVITYMETADATAKEY__EXPIRATIONDATE + 978307200,
'UNIXEPOCH') AS "EXPIRATION DATE",
ZSTRUCTUREDMETADATA.Z_DKAPPLICATIONACTIVITYMETADATAKEY__ITEMRELATEDCONTENTURL AS "CONTENT URL",
ZOBJECT.ZSTREAMNAME AS "STREAM NAME",
ZOBJECT.Z_PK AS "ZOBJECT TABLE ID"
FROM
    ZOBJECT
    LEFT JOIN
        ZSTRUCTUREDMETADATA
        ON ZOBJECT.ZSTRUCTUREDMETADATA = ZSTRUCTUREDMETADATA.Z_PK
    LEFT JOIN
        ZSOURCE
        ON ZOBJECT.ZSOURCE = ZSOURCE.Z_PK
WHERE
    ZSTREAMNAME IS "/app/activity"
ORDER BY "ENTRY CREATION"
```

1. What two applications have activities recorded in this database?

_____

Solution

a. `com.apple.Maps` = Apple Maps

b. `com.apple.Mail` = Apple Mail

c. Look at the 'BUNDLE ID' column.

Review the macOS knowledgeC.db Database for Safari Browsing

Copy from the FOR518 notebook the following query and execute it on the `knowledgeC.db` database.

```
SELECT
DATETIME(ZOBJECT.ZCREATIONDATE + 978307200, 'UNIXEPOCH') AS "ENTRY CREATION",
CASE ZOBJECT.ZSTARTDAYOFWEEK
WHEN "1" THEN "Sunday"
WHEN "2" THEN "Monday"
WHEN "3" THEN "Tuesday"
WHEN "4" THEN "Wednesday"
WHEN "5" THEN "Thursday"
WHEN "6" THEN "Friday"
WHEN "7" THEN "Saturday"
END "DAY OF WEEK",
ZOBJECT.ZVALUESTRING AS "URL",
ZSOURCE.ZBUNDLEID AS "BUNDLE ID",
ZOBJECT.ZSTREAMNAME AS "STREAM NAME",
ZOBJECT.Z_PK AS "ZOBJECT TABLE ID"
FROM
    ZOBJECT
    LEFT JOIN
        ZSTRUCTUREDMETADATA
        ON ZOBJECT.ZSTRUCTUREDMETADATA = ZSTRUCTUREDMETADATA.Z_PK
    LEFT JOIN
        ZSOURCE
        ON ZOBJECT.ZSOURCE = ZSOURCE.Z_PK
WHERE
    ZSTREAMNAME IS "/safari/history"
    ORDER BY "ENTRY CREATION"
```

1. What was searched for in Safari on February 27th?

_____

Solution

a. A Google search was performed for "ars technica"

b. "https://www.google.com/search?client=safari&rls=en&q=ars+technica&ie=UTF-8&oe=UTF-8"

iOS

Review the iOS knowledgeC.db Database for Application Usage

Navigate to the `Knowledge` directory below in your mounted Physical/Logical iPhone image.

Use `cp` to copy out the `knowledgeC.db` database files to your `FOR518` directory.

> **Note**
>
> These will overwrite your macOS database files from the previous part of the lab.

Use the open command to view these files in DB Browser for SQLite.

Browse the contents in the tables.

```
cd /Volumes/davids_iphone/private/var/mobile/Library/CoreDuet/Knowledge/

cp knowledgeC.db* ~/FOR518

open ~/FOR518/knowledgeC.db
```

Copy from the FOR518 notebook the following query and execute it on the `knowledgeC.db` database.

```
SELECT
datetime(ZOBJECT.ZCREATIONDATE+978307200,'UNIXEPOCH') as "ENTRY CREATION",
ZOBJECT.ZVALUESTRING AS "BUNDLE ID",
CASE ZOBJECT.ZSTARTDAYOFWEEK
    WHEN "1" THEN "Sunday"
    WHEN "2" THEN "Monday"
    WHEN "3" THEN "Tuesday"
    WHEN "4" THEN "Wednesday"
    WHEN "5" THEN "Thursday"
    WHEN "6" THEN "Friday"
    WHEN "7" THEN "Saturday"
END "DAY OF WEEK",
ZOBJECT.ZSECONDSFROMGMT/3600 AS "GMT OFFSET",
datetime(ZOBJECT.ZSTARTDATE+978307200,'UNIXEPOCH') as "START",
datetime(ZOBJECT.ZENDDATE+978307200,'UNIXEPOCH') as "END",
(ZOBJECT.ZENDDATE-ZOBJECT.ZSTARTDATE) as "USAGE IN SECONDS"
FROM ZOBJECT
WHERE ZSTREAMNAME IS "/app/inFocus"
ORDER BY "START"
```

1. When was WhatsApp used the longest?

   _____

Solution

a. 2018-02-25 20:56:56, for 68 seconds.

b. Add “AND "BUNDLE ID" LIKE '%WHATSAPP%'” to the WHERE clause to search for the WhatsApp bundle ID (`net.whatsapp.WhatsApp`).

2. In what time zone was the Starbucks app used?

_____

Solution

a. GMT

b. Add “AND "BUNDLE ID" LIKE '%starbucks%'” to the WHERE clause to search for the Starbucks bundle ID (`com.starbucks.mystarbucks`).

3. What was the most used "application" in a single session?

_____

Solution

a. `com.apple.mobileslideshow` - The “Photos” App, 940 seconds

b. Change the “ORDER BY” line from “START” to “USAGE IN SECONDS”

Review the iOS knowledgeC.db Database for Application Activities

Copy from the FOR518 notebook the following query and execute it on the `knowledgeC.db` database.

```
SELECT
DATETIME(ZOBJECT.ZCREATIONDATE + 978307200, 'UNIXEPOCH') AS "ENTRY CREATION",
CASE ZOBJECT.ZSTARTDAYOFWEEK
WHEN "1" THEN "Sunday"
WHEN "2" THEN "Monday"
WHEN "3" THEN "Tuesday"
WHEN "4" THEN "Wednesday"
WHEN "5" THEN "Thursday"
WHEN "6" THEN "Friday"
WHEN "7" THEN "Saturday"
END "DAY OF WEEK",
ZOBJECT.ZVALUESTRING AS "BUNDLE ID",
ZSTRUCTUREDMETADATA.Z_DKAPPLICATIONACTIVITYMETADATAKEY__ACTIVITYTYPE AS "ACTIVITY TYPE",
ZSTRUCTUREDMETADATA.Z_DKAPPLICATIONACTIVITYMETADATAKEY__TITLE AS "TITLE",
DATETIME(ZSTRUCTUREDMETADATA.Z_DKAPPLICATIONACTIVITYMETADATAKEY__EXPIRATIONDATE + 978307200,
'UNIXEPOCH') AS "EXPIRATION DATE",
ZSTRUCTUREDMETADATA.Z_DKAPPLICATIONACTIVITYMETADATAKEY__ITEMRELATEDCONTENTURL AS "CONTENT URL",
ZOBJECT.ZSTREAMNAME AS "STREAM NAME",
ZOBJECT.Z_PK AS "ZOBJECT TABLE ID"
FROM
    ZOBJECT
    LEFT JOIN
        ZSTRUCTUREDMETADATA
        ON ZOBJECT.ZSTRUCTUREDMETADATA = ZSTRUCTUREDMETADATA.Z_PK
    LEFT JOIN
```

```
        ZSOURCE
        ON ZOBJECT.ZSOURCE = ZSOURCE.Z_PK
WHERE
    ZSTREAMNAME IS "/app/activity"
ORDER BY "ENTRY CREATION"
```

1. What "tour" was looked at in the Viator App (com.viator)?

   _____

   Solution

   a. Jack the Ripper Tour with 'Ripper-Vision' in London

   b. Look for entries with the bundle ID of com.viator. The activity type is '`com.viator.viatorApp.product`'

2. What two locations were likely researched using Apple Maps (com.apple.Maps) on February 26, 2018?

   _____

   Solution

   a. Central Library in Arlington

   b. Gaijin Ramen Shop in Arlington

Review the iOS CurrentPowerlog.PLSQL Database for Battery Level

Get into a root shell.

Navigate to the `BatteryLife` directory below in your mounted Physical/Logical iPhone image.

Use `cp` to copy out the `CurrentPowerlog.PLSQL` database files to your FOR518 directory.

Exit the root shell.

Using `chown` and your username change the ownership of these files.

Use the `open` command to view these files in DB Browser for SQLite.

```
sudo -s

cd /Volumes/davids_iphone/private/var/containers/Shared/SystemGroup/
A6BC0D08-2B73-431D-872B-71C6DDE3B162/Library/BatteryLife/

cp CurrentPowerlog.PLSQL* ~/FOR518

exit

sudo chown yourusername ~/FOR518/CurrentPowerlog.PLSQL*

open -a "DB Browser for SQLite" ~/FOR518/CurrentPowerlog.PLSQL
```

Copy from the FOR518 notebook the following query and execute it on the `CurrentPowerlog.PLSQL` database.

```
SELECT
    DATETIME(TIMESTAMP, 'unixepoch') AS TIMESTAMP,
    LEVEL,
    ID AS "PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI TABLE ID"
FROM
    PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI
```

1. When was the battery level at its lowest point?

   _____

> **Solution**
>
> a. 2018-02-26 01:41:15, for level 59.
>
> b. Add "ORDER BY 'Level'" at the end of the query.

Review the iOS healthdb_secure.sqlite for Step Count

Navigate to the Health directory below in your mounted Physical/Logical iPhone image.

Use `cp` to copy out the `healthdb_secure.sqlite` database files to your FOR518 directory.

Use the `open` command to view these files in DB Browser for SQLite.

```
$cd /Volumes/davids_iphone/private/var/mobile/Library/Health/

cp healthdb_secure.sqlite* ~/FOR518

open -a "DB Browser for SQLite" ~/FOR518/healthdb_secure.sqlite
```

Copy from the FOR518 notebook the following query and execute it on the `healthdb_secure.sqlite` database.

```
SELECT
DATETIME(SAMPLES.START_DATE + 978307200, 'unixepoch') AS "START DATE",
DATETIME(SAMPLES.END_DATE + 978307200, 'unixepoch') AS "END DATE",
SAMPLES.DATA_TYPE AS "DATA TYPE",
QUANTITY AS "STEPS",
SAMPLES.DATA_ID AS "SAMPLES TABLE ID"
FROM
    SAMPLES
    LEFT OUTER JOIN
        QUANTITY_SAMPLES
        ON SAMPLES.DATA_ID = QUANTITY_SAMPLES.DATA_ID
    LEFT OUTER JOIN
        UNIT_STRINGS
        ON QUANTITY_SAMPLES.ORIGINAL_UNIT = UNIT_STRINGS.ROWID
    LEFT OUTER JOIN
        CORRELATIONS
        ON SAMPLES.DATA_ID = CORRELATIONS.OBJECT
    LEFT OUTER JOIN
```

```
        METADATA_VALUES
        ON METADATA_VALUES.OBJECT_ID = SAMPLES.DATA_ID
    LEFT OUTER JOIN
        METADATA_KEYS
        ON METADATA_KEYS.ROWID = METADATA_VALUES.KEY_ID
WHERE
    SAMPLES.DATA_TYPE = 7
    AND KEY IS NULL
    ORDER BY "START DATE"
```

1. What is the date range of the recorded steps?

   _____

   Solution

   2017-11-12 - 2018-03-03

2. Were there any steps recorded on February 12, 2018?

   _____

   Solution

   a. None; on the day before and after yes.

   b. The watch was not being worn and likely the phone was not being used, thus not recording steps.

iOS Cellular/Wi-Fi Locations

On the Physical/Logical image, navigate to the `/private/var/root/Library/Caches/locationd/` directory.

Extract the `cache_encryptedB.db` files (all of them: *-shm and *-wal) to a "location" directory in your FOR518 directory.

Open this database using SQLite Database Browser.

Browse the contents of the following tables:

- CellLocation
- LteCellLocation
- WifiLocation

iOS Routined/Significant Locations

On the Physical/Logical image, navigate to the `/private/var/mobile/Library/Caches/com.apple.routined/` directory.

Extract all the database files (including: *-shm and *-wal) to the same "location" directory in your FOR518 directory.

Open these database files using SQLite Database Browser.

Browse the contents of the following tables:

- Cloud.sqlite
  - ZRTLearnedPlaceMO

    - ZRTLearnedTransitionMO
    - ZRTLearnedVisitMO
- Cache.sqlite
    - ZRTCLLocationMO
    - ZRTHintMO
- Local.sqlite
    - ZRTLearnedLocationOfInterestMO
        - Specifically, ZPLACEMAPITEMGEOMAPTITEMHANDLE BLOB data
    - ZRTLearnedLocationOfInterestTransitionMO
    - ZRTLearnedLocationOfInterestVisitMO
    - ZRTPredictionItemMO
    - ZRTVehicleEventHistoryMO
    - ZRTVehicleEventMO

Lab: Key Takeaways

- **Review some of the pattern-of-life artifacts in databases from macOS and iOS.**

Lab 5.2: Document Versions

Objectives

• Get familiar with Document Versions storage data and databases.

Lab Preparation

Note

Some of this might already be accomplished via earlier labs, but this is the state that we hope your system is in prior to the start of this lab. Just in case your system rebooted, we are including a guide to help you get back to the proper analysis starting point prior to the beginning of this lab.

1. **Software Preparation**: The following tool will be used in this exercise:
    • Terminal.app
        a. Locate and open the native macOS Terminal.app from /Applications/Utilities/.
2. **FOR518 Reference Sheet**: Locate the FOR518 Reference Sheet provided to you in your class material and books. The PDF format of this sheet is available on your FOR518-A ISO file.
3. **Mount David Lightman's Mac forensic image** (`galaga.E01`).
    • Mounting Instructions

Lab: Questions

Review the Document Versions Directory

Use the `sudo -s` command to get a privileged shell.

Use the `cd` command to explore the system's Document Versions directory.

Use the `ls -la` command to view the contents of this directory.

Use the `ls -laR` command to recursively view the contents of the `PerUID` directory. Note the contents of these directories.

Use the `cd` command to explore the `PerUID/501/c/com.apple.documentVersions` directory.

Use the `ls -litr` command to view the contents of this directory reverse sorted by time. It will also print the inode numbers for these files. Note the contents of this directory.

```
sudo -s
```

```
cd /Volumes/galaga_mounted/.DocumentRevisions-V100

ls -la

ls -laR PerUID

cd PerUID/501/c/com.apple.documentVersions/

ls -litr
```

1. Did this file grow or shrink in size over time?

   _____

   Solution

   a. It grew, 178b -> 421b -> 502b -> 546b

   b. Look at the file size column.

2. What are the inode numbers for these files?

   _____

   _____

   Solution

   a. 1529625 = com~apple~TextEdit_93AC3DEB-4D6A-4AB9-8293-EAAA824334E5_6.rtf

   b. 1422797 = F54F8520-A9BB-4E7F-9C23-0B41C11DC720.rtf

   c. 1532140 = com~apple~TextEdit_93AC3DEB-4D6A-4AB9-8293-EAAA824334E5_w.rtf

   d. 1531497 = CE93CFC8-A53F-40C9-8A22-A932BBB9DFF5.rtf

   - Use `xattr -xl` to review the contents of the extended attributes of these files. Feel free to run it all at once (`xattr -xl *`) or on a per- file basis (`xattr -xl <file>`).

3. What was the original filename and the final filename? Also take note of the filenames of the first and last file generation (generally, just the first section of the GUID and the last few characters of the filename will work).

   _____

   Solution

   a. Original = Untitled.rtf

      i. (com~apple~TextEdit_93AC3DEB-4D6A-4AB9-8293-EAAA824334E5_6.rtf)

   b. Final = games.rtf

      i. (CE93CFC8-A53F-40C9-8A22-A932BBB9DFF5.rtf)

   c. com.apple.genstore.origposixname

Review the Document Versions Database

Use the `cd` command to explore the systems' Document Versions database directory.

Copy out the `db.sqlite` files to your FOR518 directory and open these files in SQLite Database Browser.

```
cd /Volumes/galaga_mounted/.DocumentRevisions-V100/db-V1/

cp db.sqlite* ~/FOR518/
```

Review the generations table.

Find the "`generations_name`" column. That looks familiar—you should see the files we just saw.

1. Generation IDs = 3, 11, 13, 18
2. Also note the `generation_size` column.

Review the files table.

Find our "`games.rtf`" file; review the information in this tuple.

Review the Versions Chunk Store Database

Use the `cd` command to explore the systems' Versions Chunk Store database directory.

Use the `ls -la` command to view the contents of this directory.

Copy the ChunkStoreDatabase to your FOR518 directory and open the database with SQLite Database Browser.

```
cd /Volumes/galaga_mounted/.DocumentRevisions-V100/.cs/

ls -la

cp ChunkStoreDatabase* ~/FOR518/
```

Review the `CSStorageChunkListTable`; note the items for `clt_rowid` and `clt_inode` listed in the table below:

Review the `CSChunkTable` table.

Note

Note the number in the column `ft_rowid` = 5; this is the ChunkStorage file we will look at.

Fill in the table below with the offset and data length for items 3 and 13 in the `CSChunkTable`. The other generations do not appear to store metadata in this table, perhaps because they are iCloud documents.

clt_rowid	clt_inode	offset	dataLen
3	1422797		
11	1529625	N/A	N/A
13	1531497		
18	1532140	N/A	N/A

Solution

clt_rowid	clt_inode	offset	dataLen
3	1422797	3193764	446
11	1529625	N/A	N/A
13	1531497	3417208	527
18	1532140	N/A	N/A

Keeping the `ChunkStoreDatabase` open for reference, change directories to the Chunk Storage file - “5”.

Using the `open` command, open this file in your favorite hex editor (e.g., Hex Fiend).

Exit the root shell.

```
cd /Volumes/galaga_mounted/.DocumentRevisions-V100/.cs/ChunkStorage/0/0/0/

open -a "Hex Fiend" 5

exit
```

If you get an error while using the "`open`" command, please copy ("`cp`") the file to your ~/FOR518 directory, change ownership of the file ("`chown`"), and open it directly in any hex editor.

Using the offsets and data lengths above, find the two generations of the `games.rtf` file.

Use the Chunk Storage Record Format below to review the contents of these chunks.

Chunk Storage Record Format	
4 bytes	Size of chunk record
21 bytes	Chunk ID
Remaining	Chunk Contents

1. What changed between these two document versions?

   _____

Solution

a. Added two games (Centipede and Frogger)

b. Added a link for SEGA games and retropie.

c. This can be seen in the RTF files. To make it easier, you can extract the RTF files starting with the curly bracket "{" and ending with the opposite curly bracket "}", saving these chunks into two separate files and opening them.

Lab: Key Takeaways

- **Understand how Chunk Storage is implemented in Document Versions.**

Lab 5.3: Malware and Live Response

Objectives

- Review the contents of security-related files and databases.
- Get familiar with the macOS command-line utilities.
- Gather and analyze live response data.

Lab Preparation

> **Note**
>
> Some of this might already be accomplished via earlier labs, but this is the state that we hope your system is in prior to the start of this lab. Just in case your system rebooted, we are including a guide to help you get back to the proper analysis starting point prior to the beginning of this lab.

1. **Software Preparation**: The following tool will be used in this exercise:
    - Terminal.app
        a. Locate and open the native macOS Terminal.app from /Applications/Utilities/.
2. **FOR518 Reference Sheet**: Locate the FOR518 Reference Sheet provided to you in your class material and books. The PDF format of this sheet is available on your FOR518-A ISO file.
3. **Mount David Lightman's Mac forensic image** (`galaga.E01`).
    - Mounting Instructions

Lab: Questions

Review the File Quarantine Database

- Copy and review the David's `com.apple.LaunchServices.QuarantineEventsV2` database using SQLite Database Browser.

```
cp /Volumes/galaga_mounted/Users/dlightman/Library/Preferences/
com.apple.LaunchServices.QuarantineEventsV2 ~/FOR518/
```

a. Who sent the files via the "sharing" process?

_____

Solution

i. Jen Mack

ii. LSQuarantineSenderName column

b. What action might have caused this sharing?

_____

Solution

i. These files were AirDrop'ed.

ii. It does not specifically say AirDrop; however, looking at the extended attributes for these files, we can make the inference (`xattr -xl <file>`).

c. How many items were downloaded with Safari as it pertains to this database?

_____

Solution

i. Two

ii. Look for Safari in the LSQuarantineAgentName column.

- Run the following `xattr` command on David's Downloads directory. Were there really only two downloads? It's not a perfect system. This is why it is good to look at multiple sources for the same information.

```
xattr -xlp com.apple.quarantine /Volumes/galaga_mounted/Users/dlightman/Downloads/*
```

Review the XProtect Signatures

- Navigate to the XProtect files in CoreServices.
- Use the `ls -la` command to view the contents of this directory.
- Use the `less` command to take a peek at the YARA rules. (Use " `q` " to quit `less` .)
- Use `plutil -p` to review the contents of `XProtect.meta.plist` .
- Use `open` to view the contents of `XProtect.plist` . Take a moment to review it.

```
cd /Volumes/galaga_mounted/System/Library/CoreServices/XProtect.bundle/Contents/Resources/

ls -la

less XProtect.yara

plutil -p XProtect.meta.plist

open XProtect.plist
```

Gather Information From Your Analysis System

Gather the System Information

- Run and review the following commands as if you were responding to your analysis system.
- Run the `date` command.
  a. What time zone is your system set to?

  _____

  b. Is your time current?

  _____
- Run the `hostname` command.
- Run the uname -a command.
  a. What is your kernel version?

  _____
- Run the `sw_vers` command.
  a. What macOS version and build are you running?

  _____

```
date

hostname

uname -a

sw_vers
```

What Are the Active Network Connections?

- Run and review the following commands as if you were responding to your analysis system.
  - Run the `netstat -an` command.

> **Note**
>
> The option " `-f inet` " or " `-f inet6` " may be used to limit the output to just IPv4 or IPv6 addresses.

  - Try the same command without the " `-n` ".
  - Try performing a " `whois` " on some of these IP addresses.

> **Note**
>
> The option " `-b` " shows the number of bytes transferred/received for each IP address.

```
netstat -an
```

What Are the Active Network Connections, by Process?

- Run and review the following commands as if you were responding to your analysis system.

  a. Run the `lsof -i` command.

```
lsof -i
```

Review the Network Configuration Data

- Run and review the following commands as if you were responding to your analysis system.
- Run the `ifconfig` command.

  a. What is the IP of your system?

  _____

```
ifconfig
```

What Are the Open Files?

- Run and review the following commands as if you were responding to your analysis system.
- Run the `lsof` command.
- Review the Command, Process ID, User, and Name fields.

> **Note**
>
> Pipe the output to the less command "`lsof | less`" for easier viewing. (Use "`q`" to exit less.)
>
> ```
> lsof
> ```

What Users Are Logged On?

- Run and review the following commands as if you were responding to your analysis system.
- Run the `who -a` and `w` commands.
- Run the `last` command to get a historical overview of logins, system shutdowns, and reboots.

```
who -a

w

last
```

What Are the Running Processes?

- Run and review the following commands as if you were responding to your analysis system.
- Run the `ps aux` command.

> **Note**
>
> The "`ps -ef`" command gives a different output that you may find preferable.
>
> ```
> ps aux
> ```

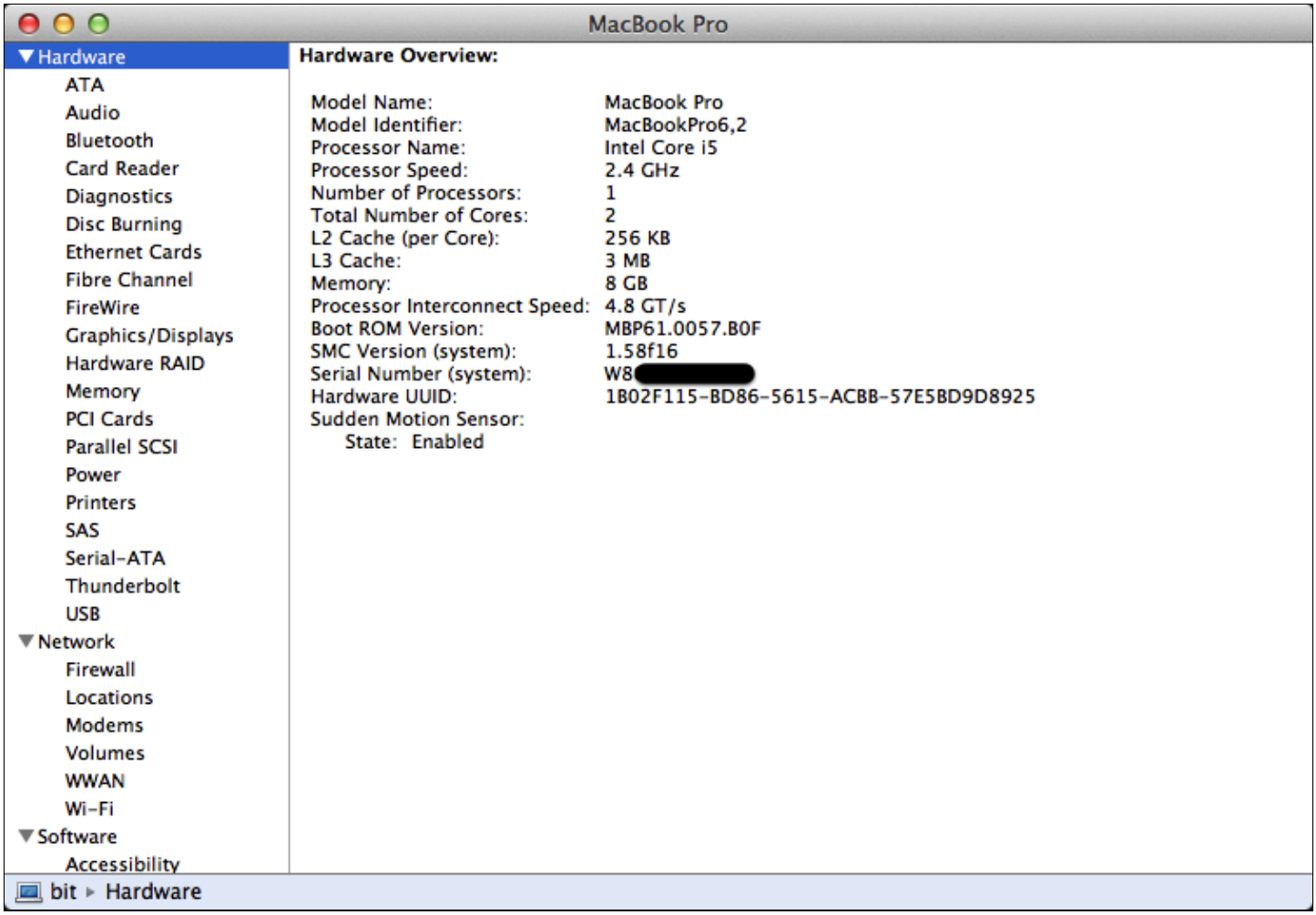
Extract Your System Information Using the `system_profiler` Command-Line Utility

- Run the `system_profiler` command; output to a file named `system-profiler-data.spx` in your FOR518 directory.

```
system_profiler -xml -detailLevel full > ~/FOR518/system-profiler-data.spx

open ~/FOR518/system-profiler-data.spx
```

Review the Output of the system_profiler Command Using System Information.app

- Open the file `system-profiler-data.spx` file you just created in the System Information.app. This application is located in /Applications/Utilities/.
- Use the `open` command to open the file you have just created.
- Review the various data components.



Lab: Key Takeaways

- **Review some of the security-related files and databases.**
- **Get comfortable with some Mac OS X command-line utilities.**
- **Many of the same commands you may have used with other systems may be different on Mac OS X, such as the ps aux command.**

Lab 5.4: Memory Analysis, Password Cracking, and Encrypted Containers

Objectives

- Understand the capability of Volatility, how it is used, and what you can expect to extract from Mac memory.
- Create a dictionary file using the memory image.
- Use John the Ripper to crack (or attempt to crack) passwords for a keychain file, an encrypted DMG, and a user account.

Lab Preparation

> **Note**
>
> Some of this might already be accomplished via earlier labs, but this is the state that we hope your system is in prior to the start of this lab. Just in case your system rebooted, we are including a guide to help you get back to the proper analysis starting point prior to the beginning of this lab.

1. **Software Preparation**: The following tools will be used in this exercise:
    - Terminal.app
        a. You will be using the native macOS Terminal application for this lab.
        b. Locate and open the Terminal.app from /Applications/Utilities/
    - John the Ripper
        a. Ensure you have John the Ripper (john-jumbo) installed via Homebrew (see Lab 0).
    - Keychain Access.app
        a. You will be opening David Lightman's keychain file.
        b. Locate and open the `Keychain Access.app` from /Applications/Utilities/
2. **Lab File Preparation:** Locate the `Lab Files/Lab 5.4 - Memory Analysis, Password Cracking & Encrypted Containers` directory.
3. **FOR518 Reference Sheet**: Locate the FOR518 Reference Sheet provided to you in your class material and books. The PDF format of this sheet is available on your FOR518-A ISO file.
4. **Memory Image:** Copy the `galaga_memory.raw` memory image to your local host system to make some of the memory commands run faster. Remember where you put this file; you need to point to that file and path in this lab. While the icon for this file

may look like an archive to “The Unarchiver”, this file **DOES NOT** need to be unarchived. This file should have been unarchived from the 7-Zip archive on Day 1 from the original file on FOR518-A ISO file : `galaga_memory.raw.7z`

- This memory dump was created with OSXPMem. The default output for OSXPMem is AFF format, which is compressed but not compatible with Volatility. We will also be creating a dictionary file to use with John the Ripper, so we need the RAW format. The following commands were used to convert this memory image from AFF format to RAW format. The first command is used to determine which data stream to output (/dev/pmem). The second command is used for the format conversion.
- `-V` - View AFF Metadata
- `-e` - Export a data stream (/dev/pmem)
- `-o` - Output file (RAW memory image)
- `./osxpmem -V galaga_memory.aff`
- `./osxpmem -e /dev/pmem -o galaga_memory.raw galaga_memory.aff`

5. **Mount David Lightman’s Mac forensic image** (`galaga.E01`).
    - Mounting Instructions

Lab: Questions

macOS Memory Analysis with Volatility

Documentation

- In your Lab 5.4 directory, change directory to the `volatility` directory.
- Run the `vol.py` with the `--info` parameter to view the tool documentation.

```
cd volatility/

python vol.py --info | less
```

- Review the “Plugins” Section. Note the plugins named with the “ `mac_*` ”. We will be using some of these in this lab.

```
mac_arp                 - Prints the arp table
mac_check_syscalls      - Checks to see if system call table entries are hooked
mac_check_sysctl        - Checks for unknown sysctl handlers
mac_check_trap_table    - Checks to see if mach trap table entries are hooked
mac_dead_procs          - Prints terminated/de-allocated processes
mac_dmesg               - Prints the kernel debug buffer
mac_dump_maps           - Dumps memory ranges of processes
mac_find_aslr_shift     - Find the ASLR shift value for 10.8+ images
mac_ifconfig            - Lists network interface information for all devices
mac_ip_filters          - Reports any hooked IP filters
mac_list_sessions       - Enumerates sessions
mac_list_zones          - Prints active zones
mac_lsmod               - Lists loaded kernel modules
mac_lsof                - Lists per-process opened files
mac_machine_info        - Prints machine information about the sample
mac_mount               - Prints mounted device information
mac_netstat             - Lists active per-process network connections
mac_notifiers           - Detects rootkits that add hooks into I/O Kit (e.g. LogKext)
mac_pgrp_hash_table     - Walks the process group hash table
mac_pid_hash_table      - Walks the pid hash table
mac_print_boot_cmdline  - Prints kernel boot arguments
mac_proc_maps           - Gets memory maps of processes
mac_psaux               - Prints processes with arguments in user land (**argv)
mac_pslist              - List Running Processes
mac_pstree              - Show parent/child relationship of processes
mac_psxview             - Find hidden processes with various process listings
mac_route               - Prints the routing table
mac_tasks               - List Active Tasks
mac_trustedbsd          - Lists malicious trustedbsd policies
mac_version             - Prints the Mac version
mac_volshell            - Shell in the memory image
mac_yarascan            - Scan memory for yara signatures
machoinfo               - Dump Mach-O file format information
```

- You may notice some “errors” at the beginning of the output. These are normal as some dependencies have not been installed. You may choose to suppress these by adding ‘ **`| grep -v Failed`** ’ when you call vol.py in the commands within this exercise.

```
oompa@MBP-M1 volatility % vol.py --info
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apihooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getsids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apihooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.amcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcscan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssdt (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registryapi (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apihooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.envars (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
```

```
oompa@MBP-M1 volatility % vol.py --info | grep -v Failed
Volatility Foundation Volatility Framework 2.6.1


Address Spaces
--------------
AMD64PagedMemory                - Standard AMD 64-bit address space.
ArmAddressSpace                 - Address space for ARM processors
FileAddressSpace                - This is a direct file AS.
```

- Review the "**Profiles**" Section.
- The profile *HighSierra_10.13.1_17B35a.zip* was copied to the Volatility profile directory (**/volatility/plugins/overlays/mac/**). By default, there are no Mac profiles loaded with Volatility, they must be copied into this directory to be used. Note that the profile is named '**MacHighSierra_10_13_1_17B35ax64**' and thus will be used in future commands with '**--profile=**'.
- Run the **vol.py** with the **-h** parameter to view the tool usage documentation. (Type '**q**' to quit out of the less command.)

```
python vol.py -h | less
```

```
Usage: Volatility - A memory forensics analysis platform.

Options:
  -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
                        (/etc/volatilityrc)
  --conf-file=/Users/sledwards/.volatilityrc
                        User based configuration file
  -d, --debug           Debug volatility
  --plugins=PLUGINS     Additional plugin directories to use (colon separated)
  --info                Print information about all registered objects
  --cache-directory=/Users/sledwards/.cache/volatility
                        Directory where cache files are stored
  --cache               Use caching
  --tz=TZ               Sets the timezone for displaying timestamps
  -f FILENAME, --filename=FILENAME
                        Filename to use when opening an image
  --profile=WinXPSP2x86
                        Name of the profile to load
  -l LOCATION, --location=LOCATION
                        A URN location from which to load an address space
  -w, --write           Enable write support
  --dtb=DTB             DTB Address
  --output=text         Output in this format (format support is module
                        specific)
  --output-file=OUTPUT_FILE
                        write output in this file
  -v, --verbose         Verbose information
  --shift=SHIFT         Mac KASLR shift address
  -g KDBG, --kdbg=KDBG  Specify a specific KDBG virtual address
  -k KPCR, --kpcr=KPCR  Specify a specific KPCR address
```

System Information

- Run the **vol.py** with the **-f** (filename) parameter on the **galaga_memory.raw** image.

- Use the `mac_version` parameter to view the system kernel information.

> **Note**
>
> These Volatility command lines can be long. These commands are meant to be executed as a single line, even if they appear as two lines in this lab.

```
python vol.py -f galaga_memory.raw --profile=MacHighSierra_10_13_1_17B35ax64 mac_version
```

1. What kernel version does this system use?

   _____

   > **Solution**
   >
   > a. 17.2.0
   >
   > b. "Darwin Kernel Version **17.2.0:** Fri Sep 29 18:27:05 PDT 2017; root:xnu-4570.20.62~3/RELEASE_X86_64"

   - Run the `vol.py` with the `mac_mount` parameter to view mounted volumes on this system.

   ```
   python vol.py -f galaga_memory.raw --profile=MacHighSierra_10_13_1_17B35ax64 mac_mount
   ```

2. What external disk is mounted on this system?

   _____

   > **Solution**
   >
   > `/Volumes/WDPassport`

3. What format is `/dev/disk5s2` ?

   _____

   > **Solution**
   >
   > HFS+

Network Information

- Run the `vol.py` with the `mac_ifconfig` parameter to view the system network configuration.

```
python vol.py -f galaga_memory.raw --profile=MacHighSierra_10_13_1_17B35ax64 mac_ifconfig
```

1. What IPv4 did this system have at the time of acquisition?

   _____

Solution

192.168.101.38

- Run the `vol.py` with the `mac_netstat` parameter to view network connections.

```
python vol.py -f galaga_memory.raw --profile=MacHighSierra_10_13_1_17B35ax64 mac_netstat
```

2. Whose email servers are the Mail applications calling out to (use `whois`)?

_____

Solution

a. 173.194.206.109 = Google

b. 17.36.205.4 = Apple

c. Look for entries in the output that have “Mail/1093” in the Process column.

d. Perform a `whois` on these IP addresses to find out the company associated with the IP address (`whois <IP Address>`).

Processes

- Run the `vol.py` with the `mac_pslist` parameter to view system processes by walking the process list.

```
python vol.py -f galaga_memory.raw --profile=MacHighSierra_10_13_1_17B35ax64 mac_pslist
```

1. What are the process names for PID 0 and 1?

_____

Solution

`Kernel_task` (0), `launchd` (1)

2. Find the "keylogger" process - who owns this process?

_____

Solution

UID/GID is 0 = root

3. What is the process ID for the "`logKextDaemon`" process?

_____

Solution

96

- Run the `vol.py` with the `mac_pstree` parameter to view system processes in a tree formation.

```
python vol.py -f galaga_memory.raw --profile=MacHighSierra_10_13_1_17B35ax64 mac_pstree
```

4. What process was performed using the `sudo` command?

_____

Solution

`osxpmem` (Capturing this memory image)

- Run the `vol.py` with the `mac_lsof` parameter to view the open file handles for each process.
- The output from this command can be quite verbose; you can choose to redirect the output to a file for easier analysis.

```
python vol.py -f galaga_memory.raw --profile=MacHighSierra_10_13_1_17B35ax64 mac_lsof > ~/FOR518/mac_lsof.txt

open ~/FOR518/mac_lsof.txt
```

5. What file (that would be of Investigative value) does " `logKextDaemon` " have open?

_____

Solution

a. `/Galaga/Library/Preferences/com.fsb.logKext`

b. Look for items opened by process 96 that we found in a previous question.

Kernel Extensions

- Run the `vol.py` with the `mac_lsmod` parameter to view kernel extensions.

```
python vol.py -f galaga_memory.raw --profile=MacHighSierra_10_13_1_17B35ax64 mac_lsmod
```

1. What two kernel extensions are loaded that are not from Apple?

_____

Solution

a. `com.google.MacPmem`

b. `com.fsb.kext.logKext`

c. Look for items that do not have the “com.apple.*” naming scheme. Yes, someone could name their malware as `com.apple.somethingevil` and hide as an Apple kernel extension.

Password Cracking

Create a Dictionary File for Password Cracking

- Use the `strings` command below to create a dictionary file from the memory image to crack some passwords.
  a. The `-n` flag specifies the minimum string length of 8 characters.
  b. This output will be piped to the " `sort -u` " command to filter out only unique strings.

c. This output will then be piped to two `awk` commands.

i. The first `awk` command will filter for strings that contain only lower and uppercase characters (no special characters).

ii. The second `awk` command will filter for string lengths of less than 12 characters.

d. Finally, the output of these commands will be outputted to a file named `galaga_dictionary.txt` in your FOR518 directory.

e. This should output a dictionary that is of reasonable size (416k) for relatively quick brute force password cracking. This should take just over a minute or so.

```
strings -n 8 galaga_memory.raw | sort -u | awk '$0 ~ /^[a-zA-Z]{1,}$/'| awk 'length($0)<12' >
~/FOR518/galaga_dictionary.txt
```

Determine the Path to john's Password Hash Extraction Scripts

- Run the following brew info command to determine where brew installed the john-jumbo files.
- This path will be used for the next few commands to extract the password hashes from a variety of files using different utilities.

```
brew info john-jumbo
```

- You may find your path different than the one below, it may be the following instead:

a. `/usr/local/Cellar/john-jumbo/1.9.0`

```
oompa@MBP-M1 ~ % brew info john-jumbo
john-jumbo: stable 1.9.0 (bottled)
Enhanced version of john, a UNIX password cracker
https://www.openwall.com/john/
Conflicts with:
  john (because both install the same binaries)
/opt/homebrew/Cellar/john-jumbo/1.9.0 (446 files, 76.0MB) *
  Poured from bottle on 2021-10-29 at 17:38:08
From: https://github.com/Homebrew/homebrew-core/blob/HEAD/Formula/john-jumbo.rb
License: GPL-2.0-or-later
==> Dependencies
Build: pkg-config ✔
Required: gmp ✔, openssl@1.1 ✔
==> Caveats
zsh completions have been installed to:
  /opt/homebrew/share/zsh/site-functions
==> Analytics
install: 565 (30 days), 1,391 (90 days), 5,032 (365 days)
install-on-request: 567 (30 days), 1,394 (90 days), 5,032 (365 days)
build-error: 0 (30 days)
```

Crack a Keychain File with John the Ripper

- Extract the `login.keychain-db` file for `dlightman` to your FOR518 directory.

a. `/Volumes/galaga_mounted/Users/dlightman/Library/Keychains/`

- Extract the password hash from the `login.keychain-db` file using the `keychain2john.py` Python3 script. (Use the path you found using the `brew info john-jumbo` command previously.)

- Ensure you extracted the password hash by using `cat` to view the contents of the newly created file.
- Using the `john` utility and the created dictionary file, crack the keychain password.
  a. The `--wordlist` parameter allows the program to intake a dictionary file for use in cracking the password.
  b. Press the "Enter" key a few times to see the status.
  c. This should not take too long (~40 seconds depending on your Mac hardware—example time was performed on a 2016 MacBook Pro, 2.9Ghz, Core i5)
  d. Once you get the password, use Control+C to quit John.
- Open the `login.keychain` file using "Keychain Access.app"; you may need to switch back and forth from your login keychain to `dlightman`'s keychain file to get it to read correctly.

Note

If you would like to re-run this hash crack again, remove the `john.pot` file from your home directory using the command "`rm ~/.john/john.pot`".

```
cp login.keychain-db ~/FOR518/

python3 <path_to_john-jumbo>/share/john/keychain2john.py ~/FOR518/login.keychain-db > ~/FOR518/
dlightman_keychain.txt

cat ~/FOR518/dlightman_keychain.txt

john --wordlist=~/FOR518/galaga_dictionary.txt ~/FOR518/dlightman_keychain.txt
```

1. What kind of password hash is detected in the keychain?

_____

Solution

(`keychain, Mac OS X Keychain [PBKDF2-SHA1 3DES 8x SSE2]`)

2. Approximately how many passwords per second is john brute forcing (sixth column from the left with the numbers labeled p/s)?

_____

Solution

~900-1,000 (2016 MacBook Pro, 2.9Ghz, Core i5)

3. What is `dlightman`'s keychain password?

_____

Solution

`galagarocks`

4. Open the `login.keychain-db` file using Keychain Access.app. What is the password for the iOS Backup?

_____

> **Solution**
>
> `galagaftw`

Crack a Login Password with John the Ripper

- Using the already extracted (Lab 2.1) user plist for dlightman, extract the password hash from the `dlightman.plist` file using the `mac2john.py` Python3 script. (Use the path you found using the `brew info john-jumbo` command previously.)
  a. `/Volumes/galaga_mounted/private/var/db/dslocal/nodes/Default/users/dlightman.plist`
- Ensure you extracted the password hash by using cat to view the contents of the newly created file.
- Using the `john` utility and the created dictionary file, crack the login password.
  a. The `--wordlist` parameter allows the program to intake a dictionary file for use in cracking the password.
  b. Press the "Enter" key a few times to see the status.
  c. **YOU WILL NOT CONTINUE TO CRACK THIS PASSWORD; use Control+C to quit John.**
    i. This took approximately 90 minutes on a 2016 MacBook Pro, 2.9Ghz, Core i5.

```
python3 <path_to_john-jumbo>/share/john/mac2john.py ~/FOR518/dlightman.plist > ~/FOR518/
dlightman_loginpassword.txt

cat ~/FOR518/dlightman_loginpassword.txt

john --wordlist=~/FOR518/galaga_dictionary.txt ~/FOR518/dlightman_loginpassword.txt
```

1. What kind of password hash is detected in the login password?

_____

> **Solution**
>
> PBKDF2-HMAC-SHA512

2. Approximately how many passwords per second is john brute forcing (sixth column from the left with the numbers labeled p/s)?

_____

> **Solution**
>
> ~29 (2016 MacBook Pro, 2.9Ghz, Core i5)

3. If you had to take a guess, what is the user's login password?

_____

> **Solution**
>
> Same as keychain file, galagarocks.

Crack a DMG Password with John the Ripper

- Extract the `kl2.dmg` file from `dlightman`'s system to your FOR518 directory.
- Extract the password hash from the `kl2.dmg` file using the `dmg2john` script. (Use the path you found using the `brew info john-jumbo` command previously.)
- Ensure you extracted the password hash by using `cat` to view the contents of the newly created file.
- Using the `john` utility and the created dictionary file, crack the DMG password.
  a. The `--wordlist` parameter allows the program to intake a dictionary file for use in cracking the password.
  b. Press the "Enter" key a few times to see the status.
  c. **YOU WILL NOT CONTINUE TO CRACK THIS PASSWORD; use Control+C to quit John.**
- Password cracking using a dictionary file is not perfect, as it turns out the password is not in the dictionary file we created, because it is six characters in length. Even if we filtered for passwords that were shorter, our dictionary file would have strings that included the password text but not as a string itself. Sometimes you win, sometimes you do not. A better dictionary file could have been created, but that takes a bit more work to do.

```
cp /Volumes/galaga_mounted/Users/dlightman/Documents/Stuff/kl2.dmg ~/FOR518/

<path_to_john-jumbo>/share/john/dmg2john ~/FOR518/kl2.dmg > ~/FOR518/dlightman_dmg.txt

cat ~/FOR518/dlightman_dmg.txt

john --wordlist=~/FOR518/galaga_dictionary.txt ~/FOR518/dlightman_dmg.txt
```

1. What kind of password hash is detected in the encrypted DMG file?

   _____

   Solution

   (dmg, Apple DMG [PBKDF2-SHA1 3DES/AES 8x SSE2])

2. Approximately how many passwords per second is john brute forcing (sixth column from the left with the numbers labeled p/s)?

   _____

   Solution

   ~3-4 (2016 MacBook Pro, 2.9Ghz, Core i5)

3. Using the keychain password, what is the password for this DMG file?

   _____

   Solution

   `tetris`

Lab: Key Takeaways

- **Get comfortable with the Volatility command-line utilities for Mac memory analysis.**
- **Get familiar with John the Ripper's password cracking utilities.**
- **Understand the speed differences when using a dictionary file as well as speed differences of different encryption methods.**

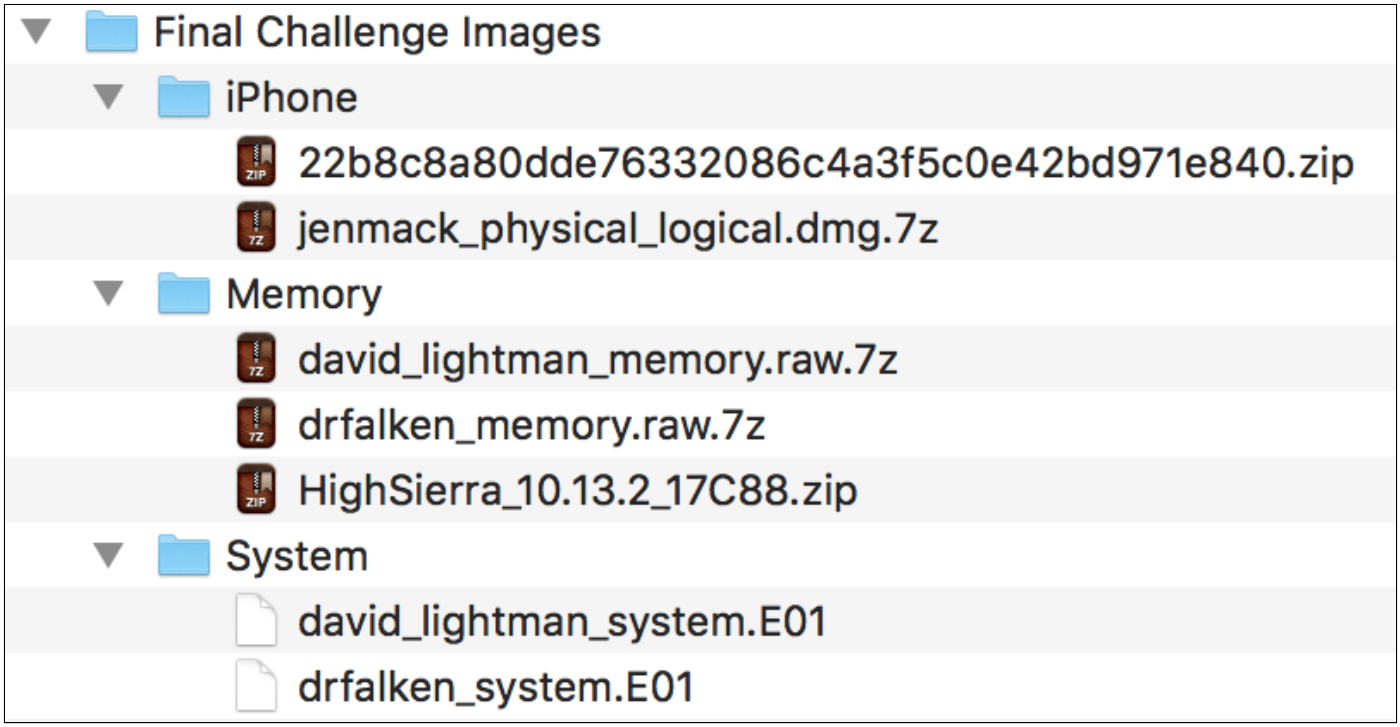
Mac Forensic Analysis Challenge Preparation

Objectives

- Create and organize your group.
- Decompress the images and data used for the Mac Forensic Challenge.
- Start preparing your data.
- Get ready to put your new Mac and iOS forensic analysis skills to the test!

Challenge Preparation

1. Challenge Rules
    - This exercise is intended to help you **PREP ONLY**, please do not start conduct analysis.
        - If a group decides to start analysis before the start of Day 6 the group will be penalized.
        - You may strategize with your group, but **DO NOT** start analyzing the images.
    - You will receive an additional lab handout with specific tasks for you to accomplish at the beginning of Day 6.
    - You **may** ask the instructor about the tools and techniques you learned this week.
    - You **may not** ask the instructor for answers.
    - Your team is expected to draft a presentation; your instructor will let you know what time the challenge will end.
        a. The most complete, innovative, and accurate presentation will win the challenge and the class coin!
        b. Voting: Each team member will vote for another team (not themselves).
            i. In the case of a tie, the instructor will be the tiebreaker.
2. Form a group of four.
    - Students leaving early should be on one team.
    - If there are an odd number of students, one team may have a larger group.
    - Depending on the class size this group may be smaller or larger; your instructor will advise you if this is the case.
3. Determine who in your group is going to work on what evidentiary items:
    - You may want to break this up by person (i.e., David Lightman, Jen Mack, or Dr. Falken), but any combination of data distribution is welcome. You may ask for instructor for advice.
    - The images and data are stored on the FOR518 – B ISO, as shown in the screenshot.



Note

General unarchived sizes are listed in square brackets.

- **David Lightman**
  a. `david_lightman_system.E01` – macOS System Image [15GB]
     - Not archived.
     - This image is a newer image than the one provided for the labs during the week. You do not need the galaga.E01 image for this challenge.
  b. `david_lightman_memory.raw.7z` – RAW output format of a memory dump, 7zip archive. [19GB]
     - **This file should be unarchived.**
     - The Volatility profile provided to you in your Lab Files on USB FOR518-A will work for this memory dump.
- **Dr. Falken**
  a. `drfalken_system.E01` – macOS System Image [19GB]
     - **Not archived.**
  b. `drfalken_memory.raw.7z` – RAW output format of a memory dump, 7zip archive. [10.5GB]
     - **This file should be unarchived.**
     - A Volatility profile has been provided to you on this USB drive. (HighSierra_10.13.2_17C88.zip, installation is required). **This file does not need to be unarchived.**

- **Jen Mack**
  - These are dumps of the same phone, one logical and one physical.
  - `22b8c8a80dde76332086c4a3f5c0e42bd971e840.zip` – iOS Backup [300MB]
    - **This file should be unarchived.**
    - **The backup password is 'password'.**
  - `jenmack_physical_logical.dmg.7z` – DMG file containing a "physical/logical" tar bundle dump of Jen Mack's iPhone. [15GB]
  - **This file should be unarchived.**

4. Unarchive evidence archives.
   - On your FOR518 - B flash drive, locate the appropriate images/data that you will be analyzing.
   - If you un-archive everything, this may take a while and will take up to ~80GB of disk space.
   - Be patient, this will take a while.
5. Create a method of communication and finding documentation for your team:
   - Online documentation (Google Docs) and chat applications have been used successfully in the past to silently communicate your findings to the rest of your team.
   - Find a conference room or other private space where you can speak freely with your team.
   - Be sure to document your findings, you will need to present these to the class.
6. Software & Case File Preparation – Please prepare and install any tools you think may help you in your analysis. Please feel free to use tools, scripts, etc., NOT used in this class. Creativity is a plus!
   - If you choose to create an Inspector Case file with your evidentiary items please do so, any processing options are fair game!
7. You may also choose to mount them using the same techniques you used in class.

> **Note**
>
> Be sure to name your mount points unique to the volume you are reviewing. For example:
>
> a. `/Volumes/davidlightman_image`, `/Volumes/davidlightman_mounted`
>
> b. `/Volumes/drfalken_image`, `/Volumes/drfalken_mounted`

8. Mount the forensic image; remember to create unique mount points for each image!
   - Using Terminal.app, perform the commands to mount the `galaga.E01` MacOS image.
   - Use the mkdir command to create a mount point for the `xmount` output. In this class, the directory name `galaga_image` is used because it will host the converted image file. sudo is required to perform this action as the mount point /Volumes has limited permissions, thus it may ask you for your administrator password when executed.
   - Use the mkdir command to create a mount point for the mounted image. The directory `galaga_mounted` is used in this class to represent the mounted disk image. sudo is required to perform this action as the mount point /Volumes has limited permissions, thus it may ask you for your administrator password when executed.

- Use `xmount` to mount the `galaga.E01` image (where you have your image located, the example shows `~/FOR518/Lab_Images/Mac/`) as a DMG file. This command requires you to use the sudo command, thus it may ask you for your administrator password when executed.
  a. `--in` – Tells `xmount` what input file type to expect, our images are in a compressed EWF format.
  b. `--out` – Tells `xmount` what output format you want, we want a DMG file so we can mount it in Finder.
  c. `Input File` – Where the image file is located on your system.
  d. `Mount Point` – Newly created mount point `/Volumes/galaga_image` specifically for this image.

```
sudo mkdir /Volumes/galaga_image/

sudo mkdir /Volumes/galaga_mounted/

sudo xmount --in ewf ~/FOR518/Lab_Images/Mac/galaga.E01 --out dmg /Volumes/galaga_image/
```

- Uses the `hdiutil` command with the "`attach`" verb to make the newly created DMG volume available. Use the `-nomount` argument to suppress mounting (for now). The output from this command will display several `/dev/disk#`, use the appropriate disk device in the next command.
  - APFS disks will show many `/dev/disk*` options in the `hdiutil` output. The one we want to mount is the user's MacOS volume. We can use the command '`diskutil list /dev/disk4`' on the synthesized disk to determine which is likely the user's MacOS volume. David Lightman's volume is named '`Galaga`', highlighted in the example below. We will use `/dev/disk4s1` in the next command. **Be aware that yours may be mounted on a different disk number!**

```
Sarahs-MBP:~ oompa$ hdiutil attach -nomount /Volumes/galaga_image/galaga.dmg
/dev/disk3              GUID_partition_scheme
/dev/disk3s1            EFI
/dev/disk3s2            Apple_APFS
/dev/disk4              EF57347C-0000-11AA-AA11-0030654
/dev/disk4s1            41504653-0000-11AA-AA11-0030654
/dev/disk4s2            41504653-0000-11AA-AA11-0030654
/dev/disk4s3            41504653-0000-11AA-AA11-0030654
/dev/disk4s4            41504653-0000-11AA-AA11-0030654
Sarahs-MBP:~ oompa$ diskutil list /dev/disk4
/dev/disk4 (synthesized):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      APFS Container Scheme -                      +31.8 GB    disk4
                                 Physical Store disk3s2
   1:                APFS Volume Galaga                  17.5 GB    disk4s1
   2:                APFS Volume Preboot                 43.0 MB    disk4s2
   3:                APFS Volume Recovery                1.0 GB     disk4s3
   4:                APFS Volume VM                      8.6 GB     disk4s4
```

- Use the `mount_apfs` command with the following parameters to mount the `/dev/disk#s#` (from the previous command) to the `/Volumes/galaga_mounted/` mount point. This command requires you to use the sudo command, thus it may ask you for your administrator password when executed. This drive will now be available in the Finder or Terminal applications.
  - `-o` – Options:
    - `rdonly` – Mount in read-only mode.

- `noexec` – Do not allow execution of binaries on mounted system.
- `noowners` – Ignore ownership on the mounted volume.

```
hdiutil attach -nomount /Volumes/galaga_image/galaga.dmg

sudo mount_apfs -o rdonly,noexec,noowners /dev/disk#s# /Volumes/galaga_mounted/
```

9. **Sanity Check**
    - You can access this newly created mounted drive on `/Volumes/galaga_mounted/`, thus all command line references in the workbook will be using this path. Using the Finder or the Terminal, access your newly created mounted volume.
    - Use the `ls -l` command to view the contents in the terminal to (hopefully) view the macOS directory structure. You should see an account for '`dlightman`' in the Users directory, hopefully not yours!

```
$ ls -l /Volumes/galaga_mounted/Users/
```

10. **When Needed - Image Unmount Instructions**
    - Use the `diskutil list` command to view the list of mounted disks. Find the disk that you want to eject. This one will be the one labeled '(disk image)' versus the one labeled '(synthesized)'. In my example it would be /dev/disk3.
    - Use the `diskutil eject` command on the disk you would like to eject.
    - Use the `mount` command to view the list of mounted disks. Find the disk that you want to `unmount` (likely `/Volumes/galaga_image/`, if you are following the naming scheme from the examples.)
    - Use the `umount` command with the mount point to unmount the disk. You will have to use the `sudo` command.)

> **Warning**
>
> If you are in the mounted image in Terminal, or have a program using the mounted disk, you will get an error that it cannot be ejected or unmounted.

```
diskutil list

diskutil eject /dev/disk#

mount

sudo umount /Volumes/galaga_image
```

SANS Courseware License Agreement

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With this CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, USER AGREES TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, USER AGREES THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If User does not agree, User may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP® and PMBOK® are registered trademarks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

All reference links are operational in the browser-based delivery of the electronic workbook.

Mounting Instructions

Mount David Lightman's Mac forensic image (`galaga.E01`).

- Using Terminal.app, perform the commands to mount the **`galaga.E01`** MacOS image.
- Use the **`mkdir`** command to create a mount point for the **`xmount`** output. In this class, the directory name **`galaga_image`** is used because it will host the converted image file. sudo is required to perform this action, as the mount point **`/Volumes`** has limited permissions, thus it may ask you for your administrator password when executed.
- Use the **`mkdir`** command to create a mount point for the mounted image. The directory **`galaga_mounted`** is used in this class to represent the mounted disk image. **`sudo`** is required to perform this action as the mount point **`/Volumes`** has limited permissions, thus it may ask you for your administrator password when executed.
- Use **`xmount`** to mount the **`galaga.E01`** image (where you have your image located, the example shows **`~/FOR518/Lab_Images/Mac/`**) as a DMG file. This command requires you to use the **`sudo`** command, thus it may ask you for your administrator password when executed.
  - **`--in`** - Tells **`xmount`** what input file type to expect; our images are in a compressed EWF format.
  - **`--out`** - Tells **`xmount`** what output format you want; we want a DMG file so we can mount it in Finder.
  - **`Input File`** - Where the image file is located on your system.
  - **`Mount Point`** - Newly created mount point **`/Volumes/galaga_image`** specifically for this image.

```
sudo mkdir /Volumes/galaga_image/

sudo mkdir /Volumes/galaga_mounted/

sudo xmount --in ewf ~/FOR518/Lab_Images/Mac/galaga.E01 --out dmg /Volumes/galaga_image/
```

- Use the **`hdiutil`** command with the "**`attach`**" verb to make the newly created DMG volume available. Use the **`-nomount`** argument to suppress mounting (for now). The output from this command will display several **`/dev/disk#`**; use the appropriate disk device in the next command.
  - APFS disks will show many **`/dev/disk*`** options in the **`hdiutil`** output. The one we want to mount is the user's MacOS volume. We can use the command "**`diskutil list /dev/disk4`**" on the synthesized disk to determine which is likely the user's MacOS volume. David Lightman's volume is named "**`Galaga`**", highlighted in the example below. We will use **`/dev/disk4s1`** in the next command. **Be aware that yours may be mounted on a different disk number!**

```
Sarahs-MBP:~ oompa$ hdiutil attach -nomount /Volumes/galaga_image/galaga.dmg
/dev/disk3                  GUID_partition_scheme
/dev/disk3s1                EFI
/dev/disk3s2                Apple_APFS
/dev/disk4                  EF57347C-0000-11AA-AA11-0030654
/dev/disk4s1                41504653-0000-11AA-AA11-0030654
/dev/disk4s2                41504653-0000-11AA-AA11-0030654
/dev/disk4s3                41504653-0000-11AA-AA11-0030654
/dev/disk4s4                41504653-0000-11AA-AA11-0030654
Sarahs-MBP:~ oompa$ diskutil list /dev/disk4
/dev/disk4 (synthesized):
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      APFS Container Scheme -                      +31.8 GB    disk4
                                 Physical Store disk3s2
   1:                APFS Volume Galaga                  17.5 GB    disk4s1
   2:                APFS Volume Preboot                 43.0 MB    disk4s2
   3:                APFS Volume Recovery                1.0 GB     disk4s3
   4:                APFS Volume VM                      8.6 GB     disk4s4
```

- Use the `mount_apfs` command with the following parameters to mount the `/dev/disk#s#` (from the previous command) to the `/Volumes/galaga_mounted/` mount point. This command requires you to use the `sudo` command, thus it may ask you for your administrator password when executed. This drive will now be available in the Finder or Terminal applications.
  - `-o` - Options:
    - `rdonly` : Mount in read-only mode.
    - `noexec` : Do not allow execution of binaries on mounted system.
    - `noowners` : Ignore ownership on the mounted volume.

```
hdiutil attach -nomount /Volumes/galaga_image/galaga.dmg

sudo mount_apfs -o rdonly,noexec,noowners /dev/disk#s# /Volumes/galaga_mounted/
```

Sanity Check

- You can access this newly created mounted drive on `/Volumes/galaga_mounted/` , thus all command line references in the workbook will be using this path. Using the Finder or the Terminal, access your newly created mounted volume.
- Use the `ls -l` command to view the contents in the terminal to (hopefully) view the macOS directory structure. You should see an account for " `dlightman` " in the Users directory, hopefully not yours!

```
ls -l /Volumes/galaga_mounted/Users/
```

***When Needed*: Image Unmount Instructions**

- Use the `diskutil list` command to view the list of mounted disks. Find the disk that you want to eject. This one will be the one labeled "(`disk image`)" versus the one labeled "(`synthesized`)." In my example, it would be `/dev/disk3` .
- Use the `diskutil eject` command on the disk you would like to eject.
- Use the `mount` command to view the list of mounted disks. Find the disk that you want to unmount (likely `/Volumes/galaga_image/` if you are following the naming scheme from the examples).
- Use the `umount` command with the mount point to unmount the disk. You will have to use the `sudo` command.

Warning

If you are in the mounted image in Terminal, or have a program using the mounted disk, you will get an error that it cannot be ejected or unmounted.

```
diskutil list

diskutil eject /dev/disk#

mount

sudo umount /Volumes/galaga_image
```

Mount David Lightman's Physical Logical iPhone DMG (`DavidLightman_physical_logical_dump.dmg`)

- Follow nearly the same procedure as mounting the `galaga.E01` image. Select the partition labeled `41504653-0000-11AA-AA11-0030654` for the `mount_apfs` command. If you perform a `diskutil list` , it will show up as an APFS volume named " `physical_logical_dump` ".

```
sudo mkdir /Volumes/davids_iphone/

hdiutil attach -nomount DavidLightman_physical_logical_dump.dmg

sudo mount_apfs -o rdonly,noexec,noowners /dev/disk#s# /Volumes/davids_iphone/
```

- You can access this newly created mounted drive on `/Volumes/davids_iphone/` , thus all command line references in the workbook will be using this path. Using the Finder or the Terminal, access your newly created mounted volume.

```
ls -l /Volumes/davids_iphone/
```