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!

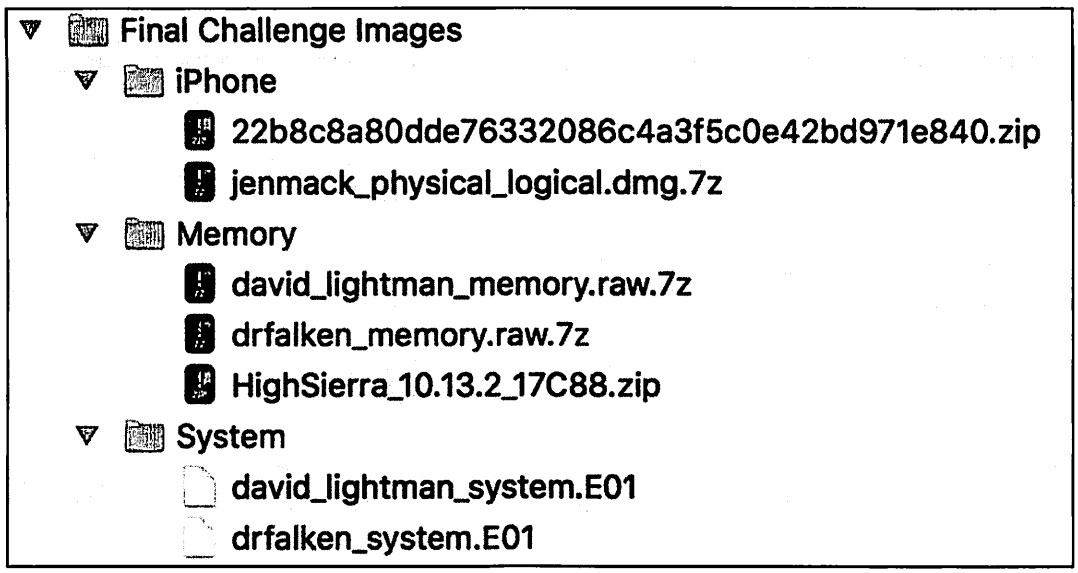
Challenge Preparation

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.
        i. The most complete, innovative, and accurate presentation will win the challenge and the class coin!
        ii. Voting: Each team member will vote for another team (not themselves).
            1. 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 each drive FOR518 – B, as shown in the screenshot.

FOR518 – B USB:



Note: General unarchived sizes are listed in square brackets.

- **David Lightman**
  - `david_lightman_system.E01` – macOS System Image [15GB]
    - Not archived.
    - This image is an newer image than the one provided for the labs during the week. You do not need the galaga.E01 image for this challenge.
  - `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**
  - `drfalken_system.E01` – macOS System Image [19GB]
    - Not archived.
  - `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 a BlackLight 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.
   - *** Be sure to name your mount points unique to the volume you are reviewing. For example:
     i. `/Volumes/davidlightman_image, /Volumes/davidlightman_mounted`
     ii. `/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.
     - `--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/
```

- 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 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
```