FOR518 – Laptop Setup (Pre-class)

Objectives

- Install required software for FOR518 – Mac and iOS Forensic Analysis and Incident Response

Class Preparation

Please ensure you are running macOS 10.13 or newer. This is a vital requirement to be able to mount forensic images. It is possible to use macOS 10.12 however 10.13 is HIGHLY RECOMMENDED to get the full class experience.

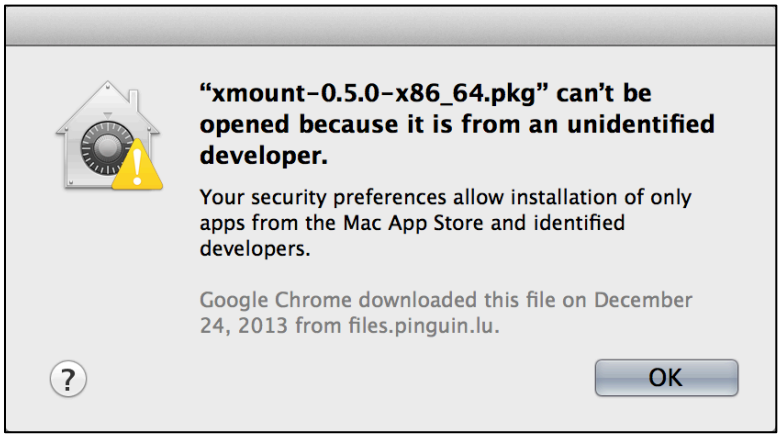
This process should take approximately 1 hour, including download time. Xcode is **very** large and will take a long time to download; depending on your connection this process could take longer.

*You may use your host system **or** a virtual machine; however, this setup has not been fully tested in a virtual machine. If you choose to go this route, please be aware that not all tools may work as intended.*

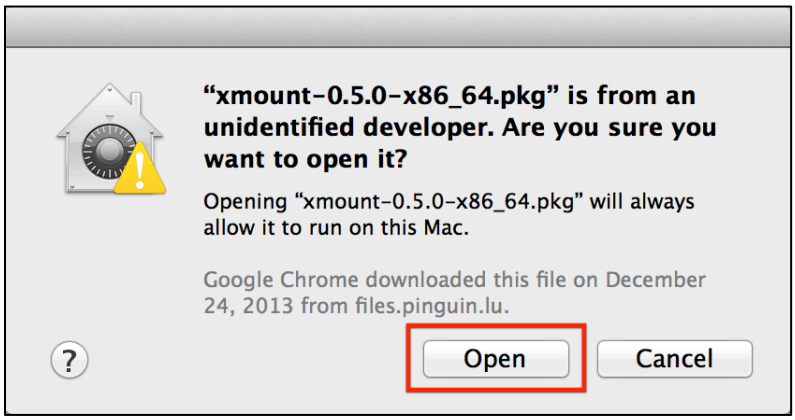
You may download the files at their respective listed websites **or** you may download an archive of these files: `http://for518.com/tools` (excludes tools that are too large or need to be downloaded). **If you are in class**, the Tools directory on your thumb drives will provide these tools. Please use the application "The Unarchiver" to extract the 7zip files (included on thumb drive).

Gatekeeper Settings:

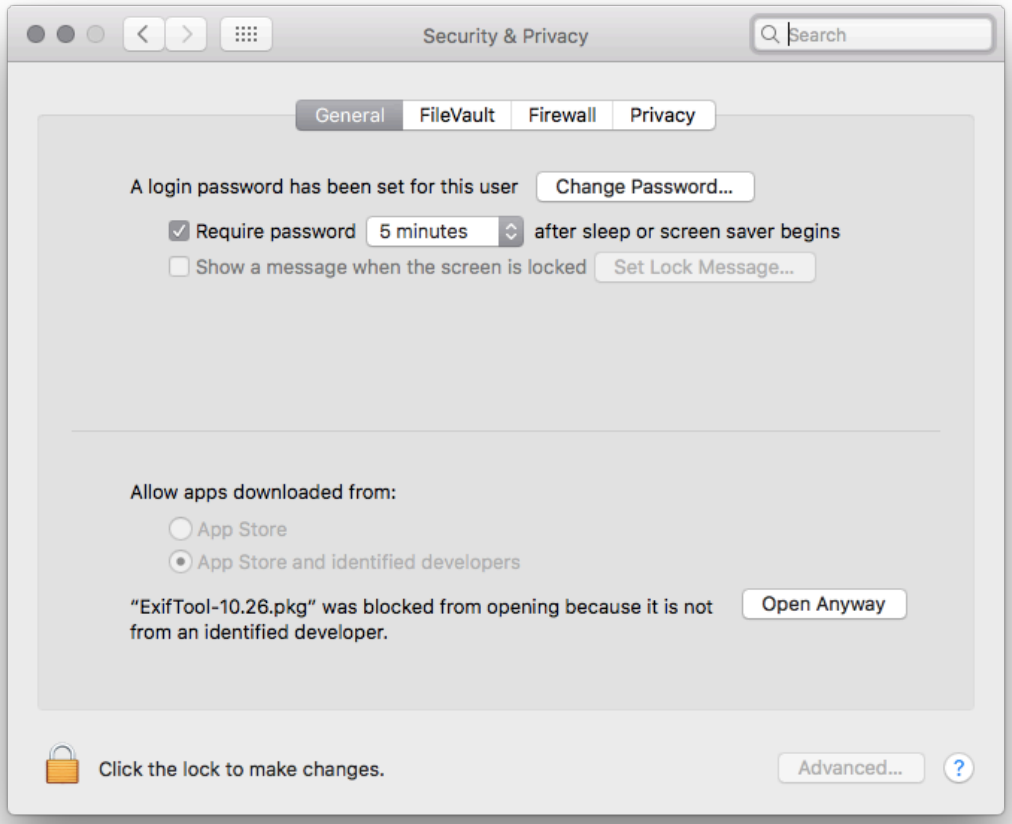
- Some installer files are from "Unidentified Developer" or "Not from the App Store."



- Users may allow these files to be installed by Control+clicking the installer file and choosing "Open." A window will pop-up, then select "Open."



Another option is to use the "Open Anyway" button, shown below, each time you the "Unidentified Developers" or "Not from the App Store" error.



******NOTE**: It is **very** important that steps 1-5 are followed in order to ensure proper software installation.****

1. **Xcode & Xcode Command Line Tools**
    1. If you have not already done so, register for an Apple Developer Account. It requires an Apple ID; if you do not have one, you may register for one at `https://developer.apple.com/register/`

2. Determine your OS version by going to Apple Menu | About This Mac, you will need to download Xcode and Command Line Tools specific for this OS version. This chart may help determine your OS version:
   `https://en.wikipedia.org/wiki/Xcode#Version_comparison_table`

3. Please download the latest **Xcode** available for your operating system from the App Store or `https://developer.apple.com/downloads/`
   a. You may have to go click "More Downloads" to access older versions.

4. Please **also** download the latest **Command Line Tools** (for your version of the OS) from `https://developer.apple.com/downloads/`
   b. You may have to go click "More Downloads" to access older versions.

5. Install **Xcode** (**Note**: This will take a while, grab some coffee.)
   c. If installing via App Store, installation will be done for you.
   d. If installing via DMG file, open the DMG file and drag the application to the `/Applications` directory.

6. Install **Command Line Tools**
   e. Open the DMG file, double-click the package installer and follow the default prompts.

2. **OS X FUSE**
   1. Download OSXFUSE from `http://osxfuse.github.io/`
   2. Open the DMG file, double-click the package installer and follow the default prompts.

3. **xmount 64-bit Package**
   1. Download xmount-0.7.6.pkg (or newer) from `http://www.pinguin.lu/`
      a. Click the `XMOUNT` link on the right side under "Projects".
      b. Download the package labeled, "`Mac OS X 64bit package`"
   2. Open the DMG file, double-click the package installer and follow the default prompts.
      a. **If you get the error "OS X Fuse Not Installed Error" please run the "mkdir" command in the box below and then re-run the xmount package installer. *(Make sure you type out "osxfusefs.fs" in each case when using tab completion.)***

```
$ mkdir -p /Library/Filesystems/osxfusefs.fs/Support/osxfusefs.kext
```

4. **The Sleuth Kit**
   1. Download `sleuthkit-4.#.#.tar.gz` from `https://www.sleuthkit.org/sleuthkit/download.php`
   2. Locate and open the `Terminal.app` from `/Applications/Utilities/`
   3. Use the `cd` command to open the default `Downloads` directory.
   4. Use the `tar` command to unpack the `sleuthkit-4.#.#.tar.gz` file.
   5. Once unpacked, use the `cd` command to get into the `sleuthkit-4.#.#.tar.gz` directory.
   6. Configure and install `sleuthkit` using the commands:
      a. `./configure --disable-java`

b. `make`
c. `sudo make install`

```
$ cd ~/Downloads

$ tar -xvf sleuthkit-4.#.#.tar.gz

$ cd sleuthkit-#.#.#

$ ./configure --disable-java

$ make

$ sudo make install
```

5. **exiftool**
   1. Download `ExifTool-9.48.dmg` (or newer) from `http://www.sno.phy.queensu.ca/~phil/exiftool/`
   2. Open the DMG file, double-click the package installer and follow the default prompts.

6. **Synalyze It!**
   1. Download Synalyze It! Pro Trial from `http://www.synalysis.net/downloads/`. This is a 30-day trial; you may also purchase the non-pro version from the App Store.
   2. If purchased from the App Store, it will install automatically.
   3. If you downloaded the trial, unzip the file and move the application to your `/Applications` directory.

7. **SQLite Database Browser:**
   1. Download the latest version of SQLite Database Browser from `http://sqlitebrowser.org/`.
   2. Open the DMG file and drag the SQLite Database Browser application to the `/Applications` directory.

8. **Hex Editors**
   1. You may choose your favorite, the following are recommended:
      i. Hex Fiend
         1. Download from `http://ridiculousfish.com/hexfiend/`
         2. Unzip and move the application to the `/Applications` directory.
      ii. 0xED
         1. Download from `http://www.suavetech.com/0xed/`
         2. Open the BZip2 archive by double clicking, then move the application to the `/Applications` directory.

9. **The Unarchiver**
   1. Download The Unarchiver from the Mac App Store or from `http://unarchiver.c3.cx/unarchiver`, under the “Other Links” heading.
   2. Double-click to unzip.

3. Drag the Unarchiver.app file to the `/Applications` directory.

10. **Homebrew**
    1. Download the Mac package manager Homebrew from `https://brew.sh/`.
    2. This web page will contain a script that you need to copy and paste into your Terminal window.

11. **Volatility**
    1. Change directory back to your home directory using the `cd` command.
    2. Download and install Volatility using Homebrew.
    3. Use the brew install command to do this.
        1. `brew install volatility`

```
$ cd ~

$ brew install volatility
```

12. **John the Ripper**
    1. Change directory back to your home directory using the `cd` command.
    2. Download and install John the Ripper using Homebrew
    3. Use the brew install command to do this.
        1. `brew install john-jumbo`

```
$ cd ~

$ brew install john-jumbo
```