

Mac System Setup Guide (Pre-Class)

Objectives

- Download tool archive here or download at websites listed below: <http://dfir.to/FOR518-PREP>
- Install required software for FOR518 – Mac Forensic Analysis

Class Preparation

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

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

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

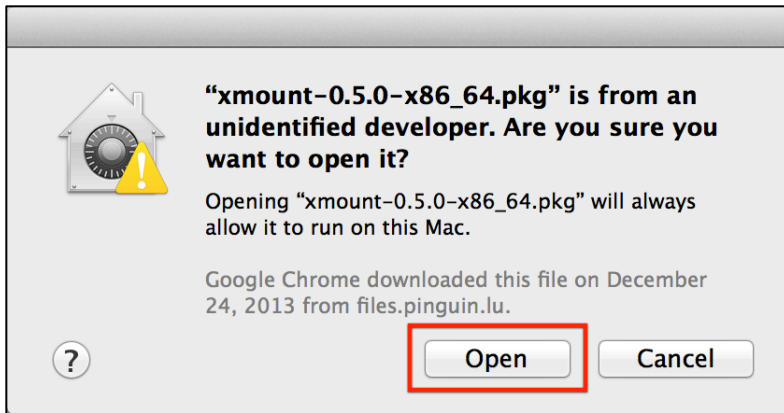
You may download the files at their respective websites listed or you may download an archive of these files at the SANS link here: <http://dfir.to/FOR518-PREP>

Gatekeeper Settings:

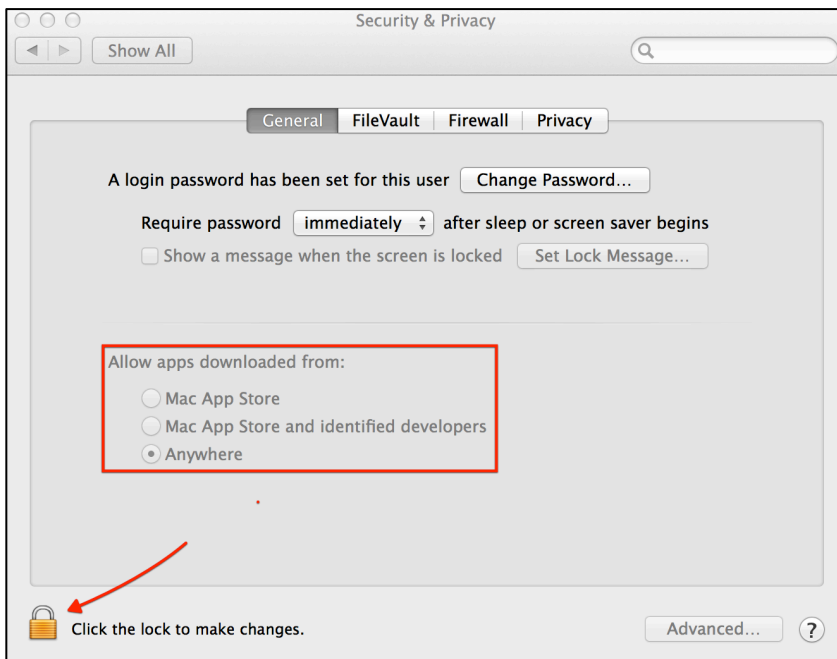
- Some installer files are from “unidentified developers”.



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



- To permanently change this setting, navigate to the Security & Privacy Preferences Panel (Apple Menu | System Preferences | Security & Privacy | General Tab). Select “Anywhere” under “Allow apps downloaded from:”.
 - This may require Administrative privileges.



1. Xcode

- If you have not already done so, register for an Apple Developer Account here. It requires an Apple ID, if you do not have one you may also register for one at <https://developer.apple.com/register/>
 1. Please download the latest Xcode available for your system from the App Store or <https://developer.apple.com/downloads/>
 2. Please download the latest Command Line Tools (for your version of OS X) from <https://developer.apple.com/downloads/>

3. Install Xcode (**Note:** This will take a while, grab some coffee)
 - i. If installing via App Store, installation will be done for you.
 - ii. If installing via DMG file, open the DMG file and drag the application to the /Applications directory.
4. Install Command Line Tools
 - i. 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. libewf

1. Download libewf-#####.tar.gz from <https://53efc0a7187d0baa489ee347026b8278fe4020f6.googleusercontent.com/host/0B3fBvzttpiisMTdoavExWwNsRjg/>.
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 libewf-20131230.tar.gz file.
5. Once unpacked, cd into the libewf-20131230 directory.
6. Configure and install libewf using the commands: ./configure; make; sudo make install.
7. **A summary screen will be shown to you once complete. Ensure the "Fuse support" equals "libosxfuse".**

```

Building:
libcstring support:          local
libcerror support:          local
libcthreads support:        local
libcdata support:           local
libcdatetime support:       local
libclocale support:         local
libcnotify support:         local
libcsplit support:          local
libuna support:             local
libcfile support:           local
libcpath support:           local
libbfio support:            local
libfcache support:          local
libfdata support:           local
libfvalue support:          local
libmfdata support:          local
ADLER32 checksum support:    zlib
DEFLATE compression support: zlib
BZIP2 compression support:   bzip2
libhmac support:            local
MD5 support:                libcrypto
SHA1 support:               libcrypto
SHA256 support:             libcrypto
libcaes support:           local
AES support:                libcrypto
libodraw support:           local
libsmdev support:           local
libsmraw support:           local
libcsystem support:         local
GUID/UUID support:          native
FUSE support:                libosxfuse

Features:
Multi-threading support:     pthread
Wide character type support: no
ewftools are build as static executables: no
Python (pyewf) support:     no
Verbose output:              no
Debug output:                no
Version 1 API compatibility: no
  
```

- i. Like in screenshot above, your output should say “libosxfuse” rather than “no”. If yours does not, try the following troubleshooting:
 1. Find your fuse.h file. In a terminal type `sudo find / -name fuse.h`
 2. Take note of where your fuse.h file is located. For example, the author’s is installed in `/usr/local/include/osxfuse/fuse.h`
 3. Try the command `./configure --with-libfuse=/usr/local/`
 4. If all else fails, send the path to your fuse.h file and the `config.log` file created in the `libewf-YYYYMMDD` directory to your instructor.

```

$ cd ~/Downloads

$ tar xvf libewf-#####.tar.gz

$ cd libewf-#####

$ ./configure

$ make

$ sudo make install

```

4. xmount 64-bit Package

1. Download `xmount-0.5.0-x86_64.pkg` (or newer) from <http://www.penguin.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.

5. The Sleuth Kit

1. Download `sleuthkit-4.1.3.tar.gz` (or newer) from <http://sourceforge.net/projects/sleuthkit/>
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-4.1.3.tar.gz` file.
5. Once unpacked, `cd` into the `sleuthkit-4.1.3.tar.gz` directory.
6. Configure and install `sleuthkit` using the commands: `./configure; make; sudo make install`
 - a. You may need to install the Java JRE and JDK, please visit the following to download and install using default prompts.
 - i. https://www.java.com/en/download/mac_download.jsp
 - ii. <http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>
7. Ensure the install was successful and the `libewf` package was recognized by executing the `mmls -i list` command.

```

nibble:sleuthkit-4.1.3 oompa$ mmls -i list
Supported image format types:
  raw (Single or split raw file (dd))
  ewf (Expert Witness format (encase))

```

- a. If you do not see the string “ewf (Expert Witness format (encase))” in this list something went wrong. Please attempt to reinstall `libewf` and The Sleuth Kit.

```
$ cd ~/Downloads
$ tar -xvf sleuthkit-4.1.3.tar.gz
$ cd sleuthkit-4.1.3
$ ./configure
$ make
$ sudo make install
$ mmls -i list
```

6. **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.

7. **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 for 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.

8. **SQLite Browsers:**

- You may choose your favorite, these are recommended:
- **Firefox & SQLite Manager Add-on**
 1. Firefox
 - a. Download the latest version of Firefox from firefox.com.
 - b. Open the DMG file, drag the Firefox application to the `/Applications` directory.
 2. SQLite Manager Add-on
 - a. From Firefox, download from <http://addons.mozilla.org/en-US/firefox/addon/sqlite-manager/>
 - b. Click the green “+ Add to Firefox” button, press the “Install Now” button, and restart Firefox.
 - i. To ensure successful installation, go to Tools in the menu – you should see “SQLite Manager”.
- **SQLite Database Browser**
 3. Download the latest version of SQLite Database Browser from <http://sqlitebrowser.org/>.

4. Open the DMG file, drag the SQLite Database Browser application to the /Applications directory.

9. Hex Editors

- You may choose your favorite, these 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.

10. iBackupBot

1. Download “iBackupBot for Mac” Trial from <http://www.icopybot.com/download.htm>
2. Open the DMG file, drag the iBackupBot application to the /Applications directory.

11. Spotlight Inspector

1. Download the OSX version (select the appropriate checkbox) of Spotlight Inspector from <http://www.504ensics.com/tools/spotlight-inspector-digital-forensics-app-for-mac-osx/>
 - a. This will require you to input and name and email.
2. Double-click to unzip the archive.
3. Unzip and move the application to the /Applications directory.

12. 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.

13. Create a FOR518 directory

- The exercises for this class will reference a FOR518 folder in the user’s home directory to dump various files for use in other exercises. (~ /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 command below shows how to create this folder in your home directory. You may also use the GUI interface to do this.

```
$ mkdir ~/FOR518
```