Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Table of Contents

Introduction ............................................................................................................................................................................. 4
General Description ................................................................................................................................................................ 4
Supported Devices .................................................................................................................................................................. 4
   Figure 1 - Compatible Devices and Platforms ................................................................................................................. 5
Guided Mode ....................................................................................................................................................................... 6
   Figure 2 - Running Guided Mode ................................................................................................................................... 6
   Figure 3 - Elcomsoft iOS Forensic Toolkit Menu .............................................................................................................. 6
Manual Mode ..................................................................................................................................................................... 7
   Figure 4 - Running Manual Mode ................................................................................................................................... 7
Logging ............................................................................................................................................................................... 7
   Figure 5 - Logging File ................................................................................................................................................... 8
Acquiring Physical Image(s) of iOS Device File system(s) ................................................................................................. 8
   Figure 6 - Placing the Device into DFU Mode ................................................................................................................... 9
   Figure 7 - Loading the Ramdisk with Guided Mode ......................................................................................................... 10
   Figure 8 - Loading the Ramdisk with Manual Mode ...................................................................................................... 10
   Figure 9 - iOS Commands to Load Ramdisk .................................................................................................................. 11
   Figure 10 - Acquiring System Partition with Guided Mode .......................................................................................... 11
   Figure 11 - Acquiring User Partition with Manual Mode .............................................................................................. 12
   Figure 12 - User Partition Transfer Times ..................................................................................................................... 12
Acquiring Logical Partition .................................................................................................................................................. 12
   Figure 13 - Acquiring Users’ Files as Tarball (Logical Acquisition) ................................................................................ 14
Recovering User Lock Passcode from iOS 4.x/5.x Devices

Figure 14 - Brute forcing a Simple Passcode

Figure 15 - Dictionary Attack Against a Complex Passcode

Recovering Encryption Keys and Keychain Data

Figure 16 - Recovering Encryption Keys and Keychain Data with Guided Mode

Figure 17 - Recovering Encryption Keys and Keychain Data with Manual Mode

Decrypting User Partition and Keychain Data

Figure 18 – Decrypting the User Partition with Guided Mode

Figure 19 – Decrypting the Keychain Data with Manual Mode

Analyzing the Data

Figure 20 - Extracted Data

Figure 21 - Analyzing Extracted Data in FTK 4.1
Introduction

Apple products, specifically mobile devices, have become some of the most popular devices around. An article I found on Engadget states that, as of June 10, 2013, Apple has sold 600 million iOS Devices.\(^1\) Since iOS devices can do just about everything, including storing word document files, pictures, text messages, etc., it is very important for investigators to be able to acquire data from these devices during an investigation. One tool that allows investigators to easily recover data comes from the company Elcomsoft. Elcomsoft has many different tools, but their primary tool to recover data from iOS devices is called “Elcomsoft iOS Forensic Toolkit”.

General Description

“Elcomsoft iOS Forensic Toolkit is a set of tools aimed at making the acquisition of iOS devices easier. It consists of Toolkit Ramdisk and a set of tools to load the Ramdisk onto the iOS device.”\(^2\) The tool is an all-in-one, complete solution that allows full, bit-precise device acquisitions and supports all versions of iOS from 3 to 6.\(^3\) It comes with two modes: guided and manual. Guided mode has a menu-based user interface that automates the process. Manual mode allows the user to interact with different tools directly using the command-line interface.\(^2\) Elcomsoft also claims that the tool leaves no traces behind, makes no alterations to device’s contents, and every step of investigation is logged and recorded.\(^3\) The tool costs $100 for the trial version (15 days) and $1,495 for the full version, it and is offered for both Mac and Windows. For more information, visit: [http://www.elcomsoft.com/eift.html](http://www.elcomsoft.com/eift.html).

(Note: This guide will be using the Windows version of the Elcomsoft iOS Forensics Toolkit.)

Supported Devices

Figure 1 below provides a list of the supported devices, as provided by the Elcomsoft website:

---


Figure 1 - Compatible Devices and Platforms

Compatible Devices and Platforms

The Toolkit currently supports the following iOS devices:

- iPhone 3G
- iPhone 3GS
- iPhone 4 (GSM and CDMA models)
- iPhone 4s ***
- iPhone 5 ***
- iPod Touch (1st - 4th generations)
- iPod Touch 5th gen ***
- iPad (1st generation only)
- iPad 2 ***
- iPad with Retina display (3rd and 4th generations) ***
- iPad Mini ***

Supported operating systems:

- iOS 1.3 (up to 3.1.3)
- iOS 4.x - up to iOS 4.3.5 (up to iOS 4.2.10 for iPhone 4 CDMA)
- iOS 5.x
- iOS 6.x - up to iOS 6.1.2

<table>
<thead>
<tr>
<th></th>
<th>iPhone 3G</th>
<th>iPod Touch 1/2</th>
<th>iPhone 3Gs, iPod Touch 3th gen, iPad 1</th>
<th>iPhone 4</th>
<th>iPod Touch 4th gen</th>
<th>iPod Touch 5th gen</th>
<th>iPod 2+, iPad Mini (***</th>
<th>iPhone 4S/5</th>
<th>iPod Touch 5th gen support limited to jailbroken devices only (iOS 5 and 6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical imaging</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logical imaging</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passcode recovery</td>
<td>instant</td>
<td>✓</td>
<td>instant</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keychain decryption</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk decryption(*)</td>
<td>N/A</td>
<td>N/A***</td>
<td>N/A*</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(*) Devices running iOS versions before 3.0 do not have Data Protection enabled and user partition is not encrypted.

(***) Devices originally shipped with iOS 3.x, including those running iOS 4/5 that were upgraded from iOS 3.x without performing "erase install" (i.e. using "Update" option in iTunes as opposed to "Restore"), do not have Data Protection enabled, and user partitions are not encrypted. Therefore, the decryption is not required.

(**) iPhone 4S, iPhone 5, iPad 2+, iPad Mini and iPod Touch 5th gen support is limited to jailbroken devices only (iOS 5 and 6).

EIIFT trial notes

EIIFT trial version has all features and functionalities of the complete version, but is timely limited to 15 days. You can prolong your trial license for a price reduced by the price of the trial version.

---

Guided Mode
When you first acquire the toolkit from Elcomsoft, you will need to download and extract the toolkit from the zipped folder to your desired location. Once you have done so, you can begin using the guided mode of the toolkit by clicking on the Toolkit.cmd file (Figure 2). This will open a console window and present a text-based menu (Figure 3). Guided mode automates the process of retrieving the data for the investigator, making it much easier to use the tool. Guided mode allows you to acquire the system and user data partitions of iOS devices. It also allows you to retrieve a logical extraction of an iOS device, as well as recovering the device passcode, device keys, and the keychain. Guided mode only allows the user to recover simple device passcodes (4-digit passcodes) from an iOS device. To recover complex passcodes (alphanumeric passcodes of any length), an investigator will have to use the manual mode.

Figure 2 - Running Guided Mode

Figure 3 - Elcomsoft iOS Forensic Toolkit Menu
**Manual Mode**

To use the manual mode, begin by opening a command prompt window where the toolkit is located. To easily do this, hold the shift key down and right-click on the folder where the toolkit is located. Then click “Open command window here” (Figure 4). The manual mode option of the Elcomsoft iOS Forensic Toolkit is more advanced, requiring the investigator to use and be comfortable with the command-line tools provided. Manual mode allows for greater flexibility and is the recommended way of retrieving a device acquisition of iOS devices. Manual mode allows you to acquire the system and user data partitions of iOS devices, and has the ability to retrieve a logical extraction of an iOS device, as well as recovering the device passcode, device keys, the keychain. Manual mode allows the user to recover simple device passcodes (4-digit passcodes) as well as complex passcodes (alphanumeric passcodes of any length).

**Figure 4 - Running Manual Mode**

![Running Manual Mode](image)

**Logging**

When you run the guided mode of the toolkit, it will continuously log all related activity in the console onto a text file. Every time the toolkit is started, a new log file is created in the current directory, which contains output of all invoked commands (Figure 5). The file name is saved as: **YYYYMMDD_hhmmssZ.log**
Acquiring Physical Image(s) of iOS Device File system(s)

Most iOS devices have two partitions (System and User), and their names differ between iOS versions:

- iOS 4.x: System is `disk0s1` and User is `disk0s2s1`. 
iOS 5.x: System is disk0s1s1 and User is disk0s1s2.²

To acquire the system partition, the user partition, or both, an investigator can use either guided mode or manual mode. Before you can acquire the physical image(s) of the file system(s), or before acquiring any data, you have to load the toolkit Ramdisk to the device. In order to do this, you have to load the device in DFU (Device Firmware Update) mode. You can either do this by manually putting the device in DFU mode or, more easily, you can use menu item 1 in the guided mode, complete with on-screen instructions (Figure 6).

Figure 6 - Placing the Device into DFU Mode

Once you place the device in DFU mode, you can upload the toolkit Ramdisk and begin acquiring the device. In guided mode, you can load the toolkit Ramdisk in a matter of seconds with a few keys (Figure 7); in manual mode, you will have to enter in a command that will take a little longer to load the Ramdisk to the device (Figure 8). This command will change depending on the type of iOS device you have (Figure 9).
Figure 7 - Loading the Ramdisk with Guided Mode

Figure 8 - Loading the Ramdisk with Manual Mode
Once you upload the toolkit Ramdisk, you can acquire the system (Figure 10) and user (Figure 11) file system partitions. The system partition will typically take between 5-7 minutes to acquire, and the user partition will vary depending on the device and its size (see Figure 12 for more details).

**Figure 10 - Acquiring System Partition with Guided Mode**

<table>
<thead>
<tr>
<th>iPhone 3Gs</th>
<th>iPhone 4 (GSM)</th>
<th>iPhone 4 (CDMA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone2,1</td>
<td>iPhone3,1</td>
<td>iPhone3,3</td>
</tr>
<tr>
<td>ibss</td>
<td>iBSS.n88</td>
<td>iBSS.n92</td>
</tr>
<tr>
<td>ibec</td>
<td>iBEC.n88</td>
<td>iBEC.n92</td>
</tr>
<tr>
<td>kernel</td>
<td>kernelcache.n88</td>
<td>kernelcache.n90</td>
</tr>
<tr>
<td>devicetree</td>
<td>DeviceTree.n88</td>
<td>DeviceTree.n90</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>iPod Touch 3</th>
<th>iPod Touch 4</th>
<th>iPad 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPod3,1</td>
<td>iPod4,1</td>
<td>iPad1,1</td>
</tr>
<tr>
<td>ibss</td>
<td>iBSS.n18</td>
<td>iBSS.k48</td>
</tr>
<tr>
<td>ibec</td>
<td>iBEC.n18</td>
<td>iBEC.k48</td>
</tr>
<tr>
<td>kernel</td>
<td>kernelcache.n18</td>
<td>kernelcache.k48</td>
</tr>
<tr>
<td>devicetree</td>
<td>DeviceTree.n18</td>
<td>DeviceTree.k48</td>
</tr>
</tbody>
</table>

---

Acquiring Logical Partition

Both modes of the Elcomsoft iOS Forensic Toolkit can acquire a logical partition of supported iOS devices as a tarball, a type of Linux archive file (see Figure 13).

During logical acquisition, only actual files are copied to the computer (retaining the directory structure). The process is generally significantly faster than physical acquisition, as the data residing in unallocated areas of the partition does not have to be transferred. Logical acquisition currently cannot access files
with protection classes requiring encryption based on a user-supplied passcode. Such files are not included in logical image.⁵
Figure 13 - Acquiring Users’ Files as Tarball (Logical Acquisition)
Recovering User Lock Passcode from iOS 4.x/5.x Devices

Elcomsoft iOS Forensic Toolkit has the ability to recover lock screen passcodes. "Knowing the original passcode is never required, but may come handy in the case of iOS 4/5/6 devices. The following chart helps to understand whether you’ll need a passcode for a successful acquisition:

- iOS 1.x-3.x: passcode not required. All information will be accessible. The original passcode will be instantly recovered and displayed.
- iOS 4.0-6.x: certain information is protected with passcode-dependent keys, including the following:
  - Email messages
  - Keychains (stored login/password information)
  - Certain third-party application data, if the application requested strong encryption."

The guided mode can be used to recover simple passcodes (4-digit passcodes), while the manual mode can be used to recover simple passcodes, passcodes consisting of only digits with a length not equal to 4, and complex passcodes (alphanumeric passcodes of any length). "Elcomsoft iOS Forensic Toolkit can brute-force iOS 4/5/6 simple 4-digit passcodes in 10-40 minutes ([Figure 14](#)). Complex passcodes can be recovered by using a dictionary attack (Figure 15), but requires more time. You can create your own dictionary list with words you have been provided with, or you can download some commonly used dictionary lists off the Internet.

Figure 14 - Bruteforcing a Simple Passcode

---

Recovering Encryption Keys and Keychain Data

Elcomsoft iOS Forensic Toolkit can access iOS secrets, including most keychain data, opening investigators’ access to highly sensitive data such as login/password information to Web sites and other resources.

“Unlike previously employed methods relying on lengthy dictionary attacks or brute force password recovery, the new toolkit can extract most encryption keys out of the physical device. With encryption keys handily available, access to most information is provided in real-time. A typical acquisition of an iPhone device takes from 20 to 40 minutes (depending on model and memory size); more time is required to process 64-Gb versions of Apple iPad. The list of exceptions is short, and includes user’s passcode, which can be brute-forced or recovered with a dictionary attack.”

Before extracting the encryption keys and keychain data, you must first obtain the passcode to be able to unlock the phone. Extracting the encryption keys is important as they are required to decrypt files stored on the user partition and contents of the keychain. An investigator can use both the guided mode (Figure 16) and the manual mode (Figure 17) to recover the encryption keys and keychain data.

---

7 The keychain is the password management system on Apple devices. It allows a user to store passwords for programs, e-mail accounts, web sites, and more.
Decrypting User Partition and Keychain Data

Once you have recovered the keychain data, the user lock passcode, and acquired the user partition, an investigator can begin decrypting the data. By decrypting this data, all of the information will become readable and accessible to an
investigator. Once again, you can use both the guided mode (Figure 18) and the manual mode (Figure 19) to decrypt the user partition and the keychain data.

**Figure 18 – Decrypting the User Partition with Guided Mode**

![Image of a screen showing the decryption process for a user partition.]

**Figure 19 – Decrypting the Keychain Data with Manual Mode**

![Image of a screen showing the decryption process for a keychain.]

**Analyzing the Data**

Once you have successfully extracted and decrypted all of the data (Figure 20), you can begin analyzing it with forensic acquisition and analysis tools, such as FTK Imager and FTK (Forensic Toolkit) 4.1 (Figure 21). Our research claimed that you can read this type of file (.dmg file format) in EnCase, but we were unable to open the image files.
Figure 20 - Extracted Data

<table>
<thead>
<tr>
<th>Name</th>
<th>Date Modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>keychain.txt</td>
<td>8/5/2013 2:36 PM</td>
<td>Text Document</td>
<td>63 KB</td>
</tr>
<tr>
<td>keys.plist</td>
<td>8/5/2013 12:32 PM</td>
<td>PLIST File</td>
<td>38 KB</td>
</tr>
<tr>
<td>system.dmg</td>
<td>7/18/2013 1:14 PM</td>
<td>dmg Archive</td>
<td>1,331,200 KB</td>
</tr>
<tr>
<td>user.dmg</td>
<td>7/19/2013 11:44 AM</td>
<td>dmg Archive</td>
<td>29,895,704 KB</td>
</tr>
<tr>
<td>user.tar</td>
<td>7/19/2013 1:28 PM</td>
<td>tar Archive</td>
<td>556,140 KB</td>
</tr>
<tr>
<td>user-decrypted.dmg</td>
<td>8/5/2013 1:57 PM</td>
<td>dmg Archive</td>
<td>29,896,704 KB</td>
</tr>
</tbody>
</table>
Figure 21 - Analyzing Extracted Data in FTK 4.1