CHAMPLAIN COLLEGE

LCDI

The Senator Patrick Leahy
Center for Digital Investigation

Elcomsoft iOS Forensic Toolkit Guide

Written by
Colby Lahaie

175 Lakeside Ave, Room 300A
Phone: 802/865-5744
Fax: 802/865-6446
http://www.lcdi.champlain.edu

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

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.

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

Supported Devices

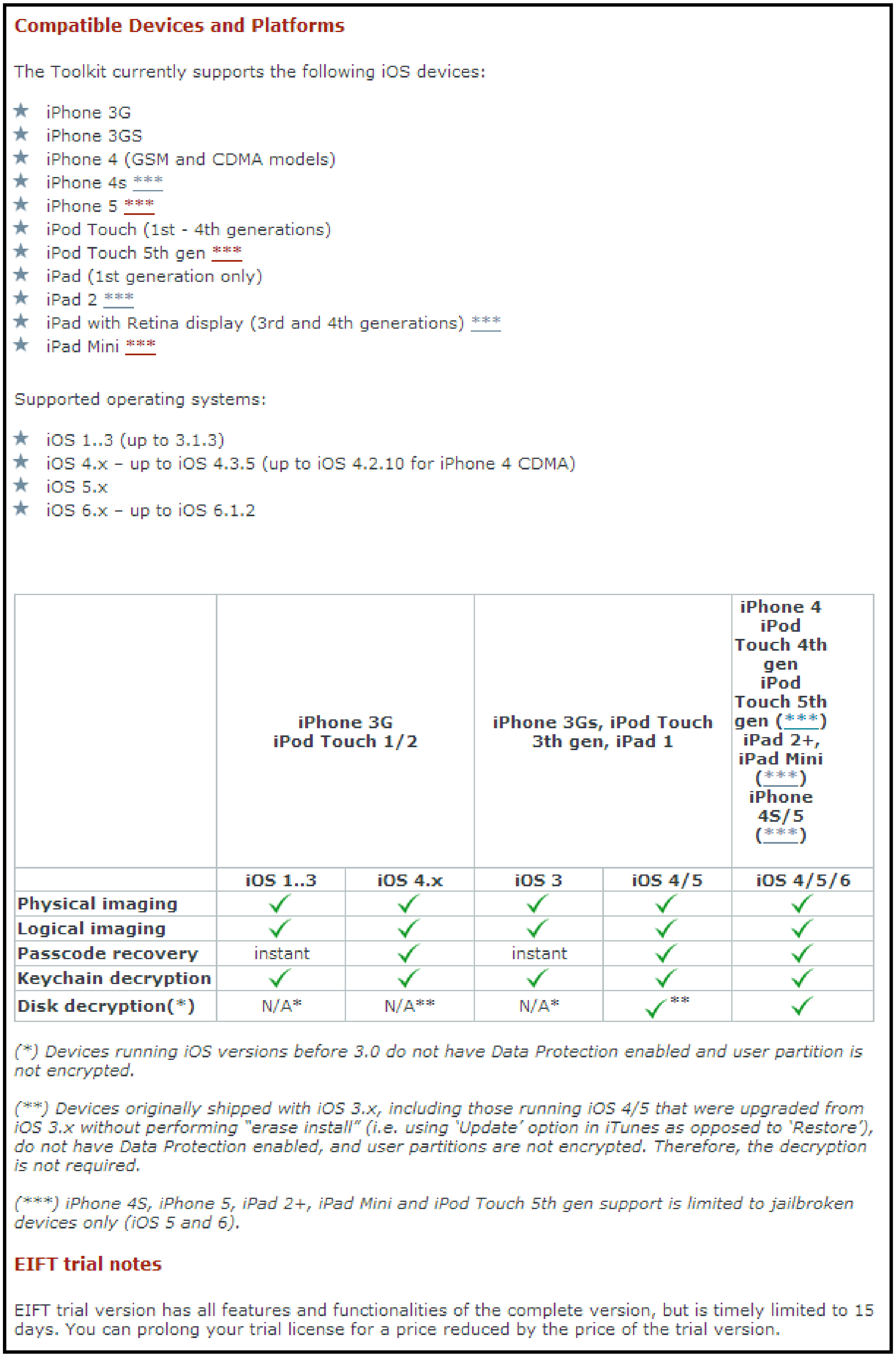
Figure 1 below provides a list of the supported devices, as provided by the Elcomsoft website:

[1] Smith, M. (2013, June 10). Apple has now sold 600 million iOS devices. *Engadget*. Retrieved August 07, 2013, from http://www.engadget.com/2013/06/10/apple-ios-devices-2013/

[2] Elcomsoft. (2012). Elcomsoft iOS Forensic Toolkit. Retrieved June 6, 2013.

[3] Elcomsoft iOS Forensics Toolkit. (n.d.). *Enhanced Forensic Access to IPhone/iPad/iPod Devices Running Apple IOS*. Retrieved July 11, 2013, from http://www.elcomsoft.com/eift.html

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

	iPhone 3G iPod Touch 1/2		iPhone 3Gs, iPod Touch 3th gen, iPad 1		iPhone 4 iPod Touch 4th gen iPod Touch 5th gen (***) iPad 2+, iPad Mini (***) iPhone 4S/5 (***)
	iOS 1..3	**iOS 4.x**	**iOS 3**	**iOS 4/5**	**iOS 4/5/6**
Physical imaging	✓	✓	✓	✓	✓
Logical imaging	✓	✓	✓	✓	✓
Passcode recovery	instant	✓	instant	✓	✓
Keychain decryption	✓	✓	✓	✓	✓
Disk decryption(*)	N/A*	N/A**	N/A*	✓**	✓

(*) 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).

EIFT trial notes

EIFT 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.

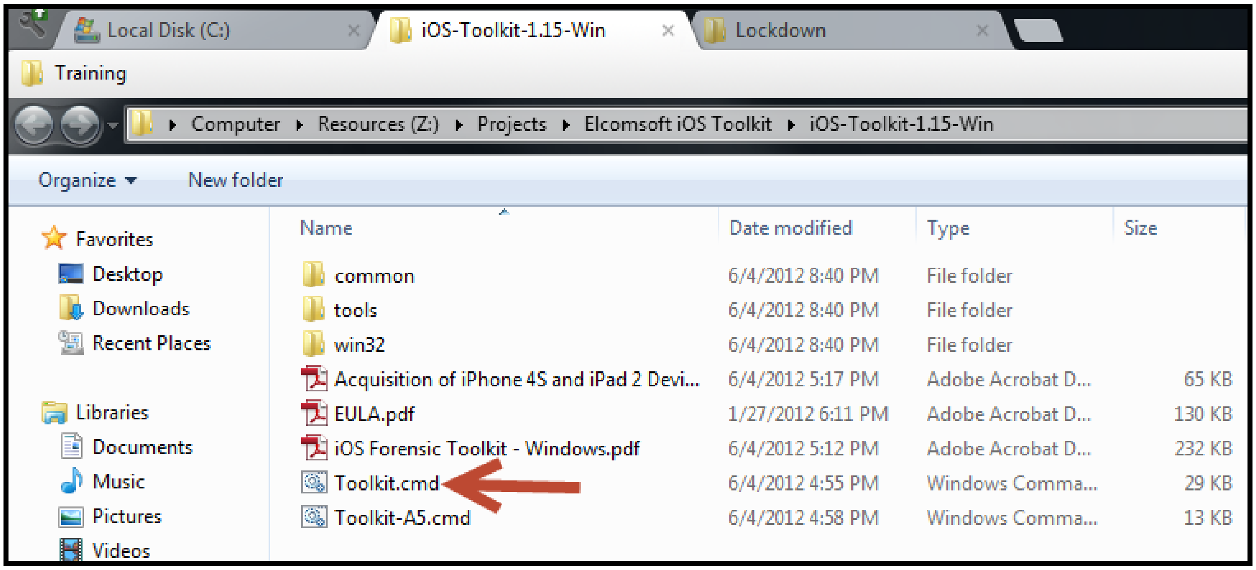
[4]

[4] Elcomsoft iOS Forensics Toolkit. (n.d.). *Enhanced Forensic Access to IPhone/iPad/iPod Devices Running Apple IOS*. Retrieved July 11, 2013, from http://www.elcomsoft.com/eift.html

Guided Mode

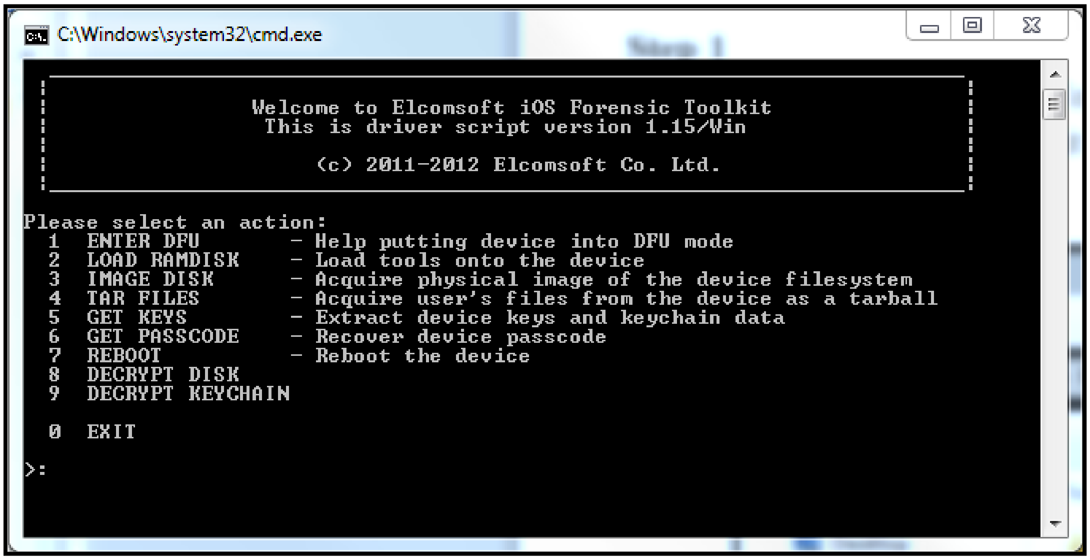
When you first acquire the toolkit from Elcomsoft, you will need to download and extract the toolkit from the zipped folder to your desired location. Once you have done so, you can begin using the guided mode of the toolkit by clicking on the Toolkit.cmd file (Figure 2). This will open a console window 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



Name	Date modified	Type	Size
common	6/4/2012 8:40 PM	File folder	
tools	6/4/2012 8:40 PM	File folder	
win32	6/4/2012 8:40 PM	File folder	
Acquisition of iPhone 4S and iPad 2 Devi...	6/4/2012 5:17 PM	Adobe Acrobat D...	65 KB
EULA.pdf	1/27/2012 6:11 PM	Adobe Acrobat D...	130 KB
iOS Forensic Toolkit - Windows.pdf	6/4/2012 5:12 PM	Adobe Acrobat D...	232 KB
Toolkit.cmd	6/4/2012 4:55 PM	Windows Comma...	29 KB
Toolkit-A5.cmd	6/4/2012 4:58 PM	Windows Comma...	13 KB

Figure 3 - Elcomsoft iOS Forensic Toolkit Menu

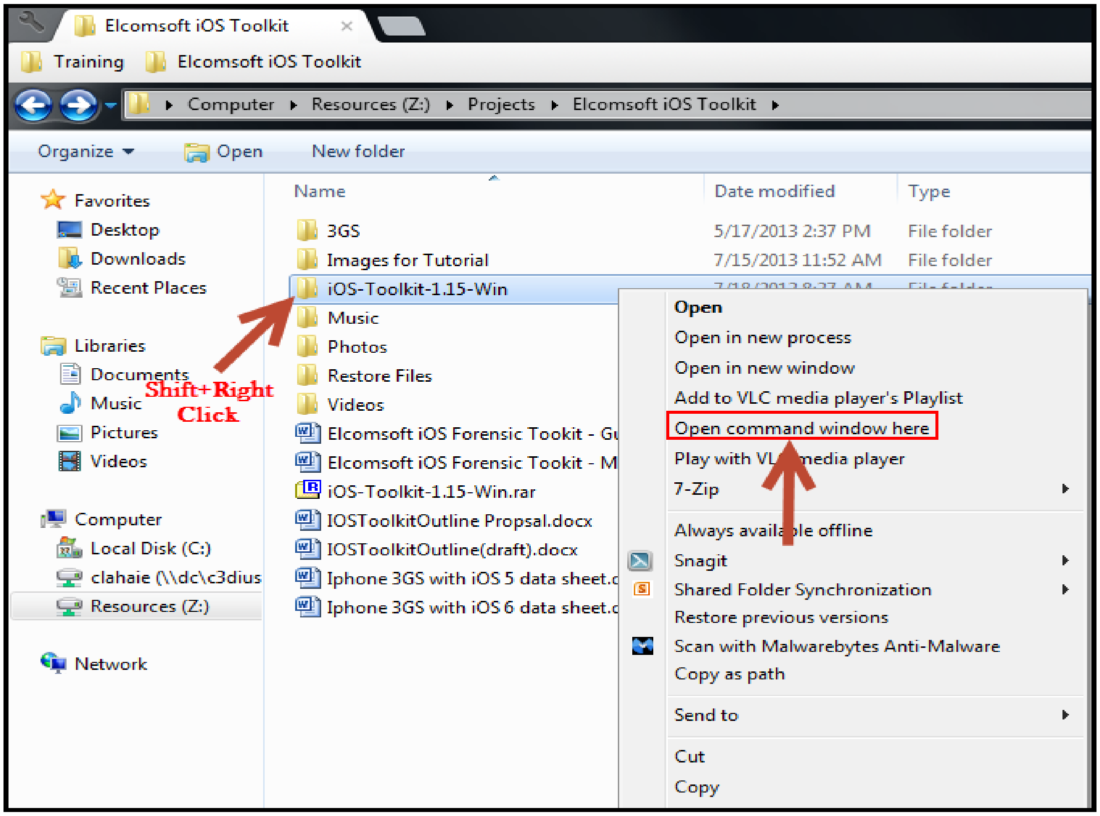


```
 ------------------------------------------------------------------
 |                                                                |
 |             Welcome to Elcomsoft iOS Forensic Toolkit          |
 |              This is driver script version 1.15/Win            |
 |                                                                |
 |                   (c) 2011-2012 Elcomsoft Co. Ltd.             |
 ------------------------------------------------------------------

Please select an action:
  1  ENTER DFU       - Help putting device into DFU mode
  2  LOAD RAMDISK    - Load tools onto the device
  3  IMAGE DISK      - Acquire physical image of the device filesystem
  4  TAR FILES       - Acquire user's files from the device as a tarball
  5  GET KEYS        - Extract device keys and keychain data
  6  GET PASSCODE    - Recover device passcode
  7  REBOOT          - Reboot the device
  8  DECRYPT DISK
  9  DECRYPT KEYCHAIN

  0  EXIT

>:
```

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

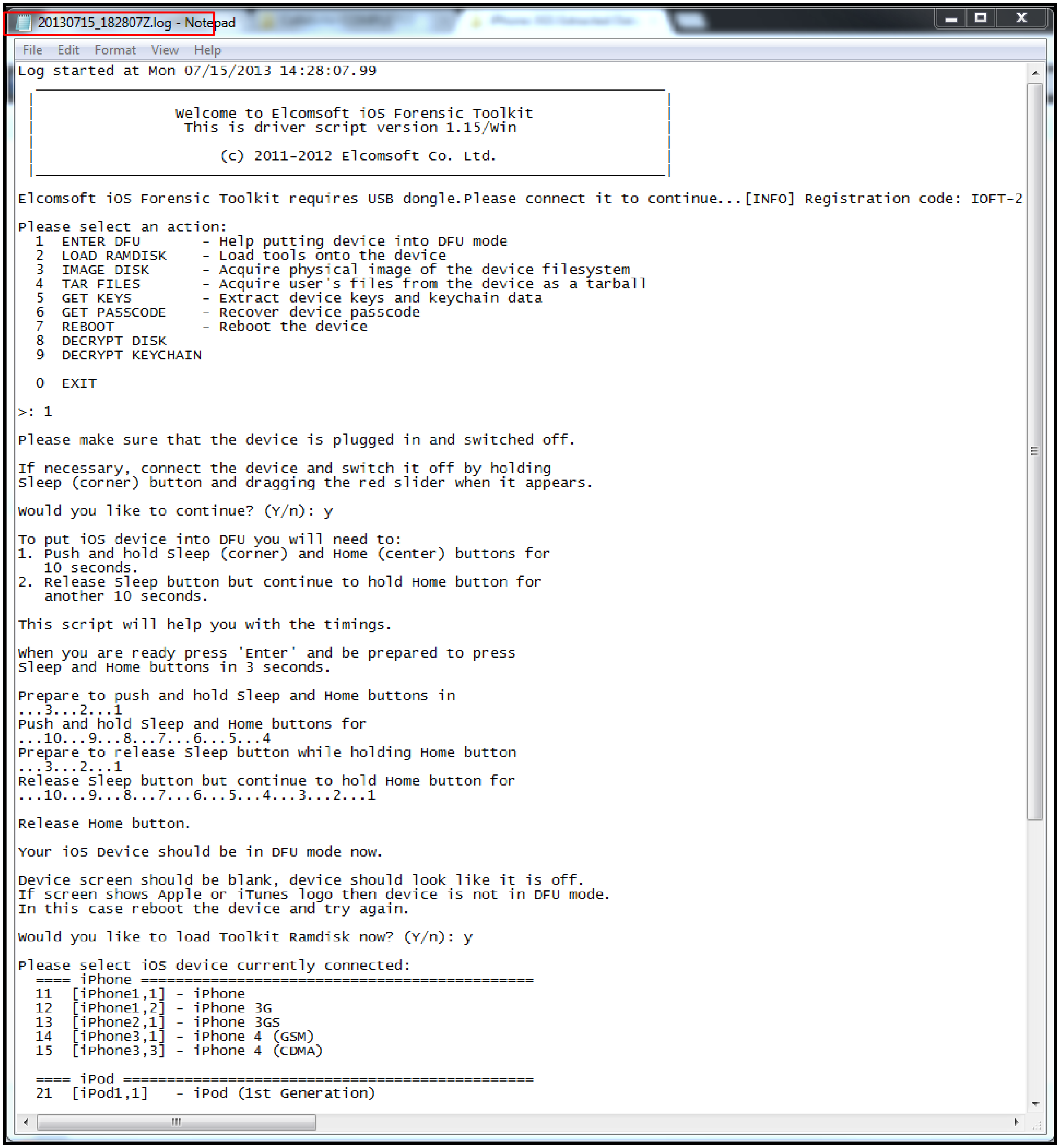


Name	Date modified	Type
3GS	5/17/2013 2:37 PM	File folder
Images for Tutorial	7/15/2013 11:52 AM	File folder
iOS-Toolkit-1.15-Win	7/18/2013 8:27 AM	File folder
Music		
Photos		
Restore Files		
Videos		
Elcomsoft iOS Forensic Tookit - Gu		
Elcomsoft iOS Forensic Tookit - M		
iOS-Toolkit-1.15-Win.rar		
IOSToolkitOutline Propsal.docx		
IOSToolkitOutline(draft).docx		
Iphone 3GS with iOS 5 data sheet.d		
Iphone 3GS with iOS 6 data sheet.d		

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**

Figure 5 - Logging File



```
Log started at Mon 07/15/2013 14:28:07.99
  ______________________________________________________________________
 |                                                                      |
 |                Welcome to Elcomsoft iOS Forensic Toolkit             |
 |                 This is driver script version 1.15/Win               |
 |                                                                      |
 |                   (c) 2011-2012 Elcomsoft Co. Ltd.                   |
 |______________________________________________________________________|

Elcomsoft iOS Forensic Toolkit requires USB dongle.Please connect it to continue...[INFO] Registration code: IOFT-2

Please select an action:
  1  ENTER DFU       - Help putting device into DFU mode
  2  LOAD RAMDISK    - Load tools onto the device
  3  IMAGE DISK      - Acquire physical image of the device filesystem
  4  TAR FILES       - Acquire user's files from the device as a tarball
  5  GET KEYS        - Extract device keys and keychain data
  6  GET PASSCODE    - Recover device passcode
  7  REBOOT          - Reboot the device
  8  DECRYPT DISK
  9  DECRYPT KEYCHAIN

  0  EXIT

>: 1

Please make sure that the device is plugged in and switched off.

If necessary, connect the device and switch it off by holding
Sleep (corner) button and dragging the red slider when it appears.

Would you like to continue? (Y/n): y

To put iOS device into DFU you will need to:
1. Push and hold Sleep (corner) and Home (center) buttons for
   10 seconds.
2. Release Sleep button but continue to hold Home button for
   another 10 seconds.

This script will help you with the timings.

When you are ready press 'Enter' and be prepared to press
Sleep and Home buttons in 3 seconds.

Prepare to push and hold Sleep and Home buttons in
...3...2...1
Push and hold Sleep and Home buttons for
...10...9...8...7...6...5...4
Prepare to release Sleep button while holding Home button
...3...2...1
Release Sleep button but continue to hold Home button for
...10...9...8...7...6...5...4...3...2...1

Release Home button.

Your iOS Device should be in DFU mode now.

Device screen should be blank, device should look like it is off.
If screen shows Apple or iTunes logo then device is not in DFU mode.
In this case reboot the device and try again.

Would you like to load Toolkit Ramdisk now? (Y/n): y

Please select iOS device currently connected:
  ==== iPhone =============================================
  11  [iPhone1,1] - iPhone
  12  [iPhone1,2] - iPhone 3G
  13  [iPhone2,1] - iPhone 3GS
  14  [iPhone3,1] - iPhone 4 (GSM)
  15  [iPhone3,3] - iPhone 4 (CDMA)

  ==== iPod ===============================================
  21  [iPod1,1]   - iPod (1st Generation)
```

Acquiring Physical Image(s) of iOS Device File system(s)

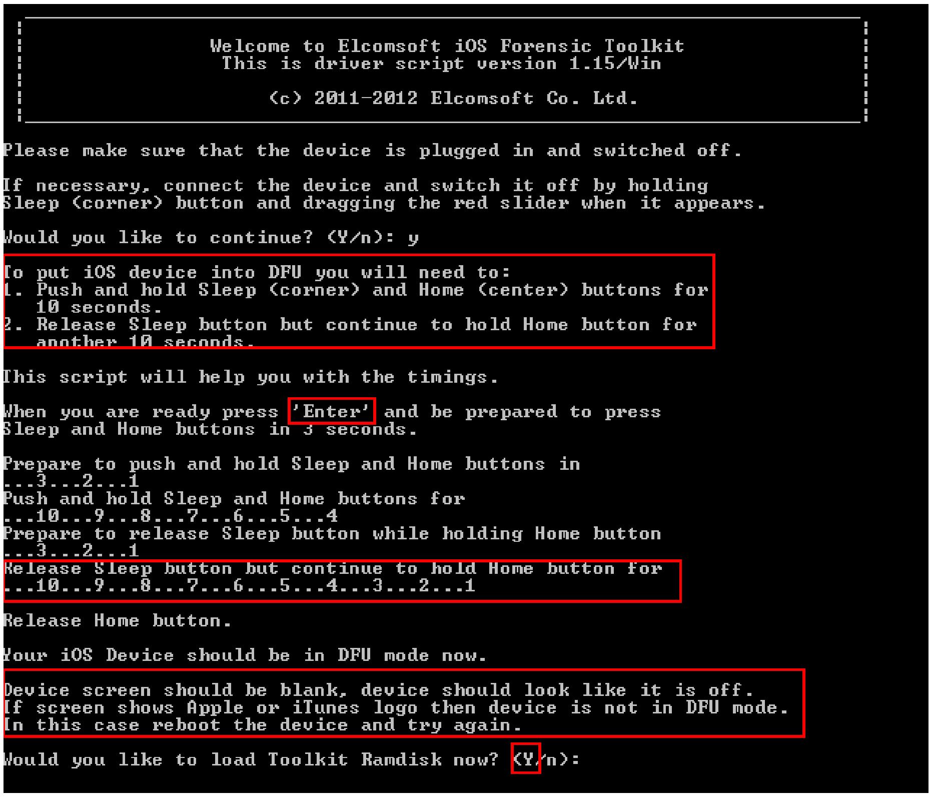
Most iOS devices have two partitions (System and User), and their names differ between iOS versions:

- 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).

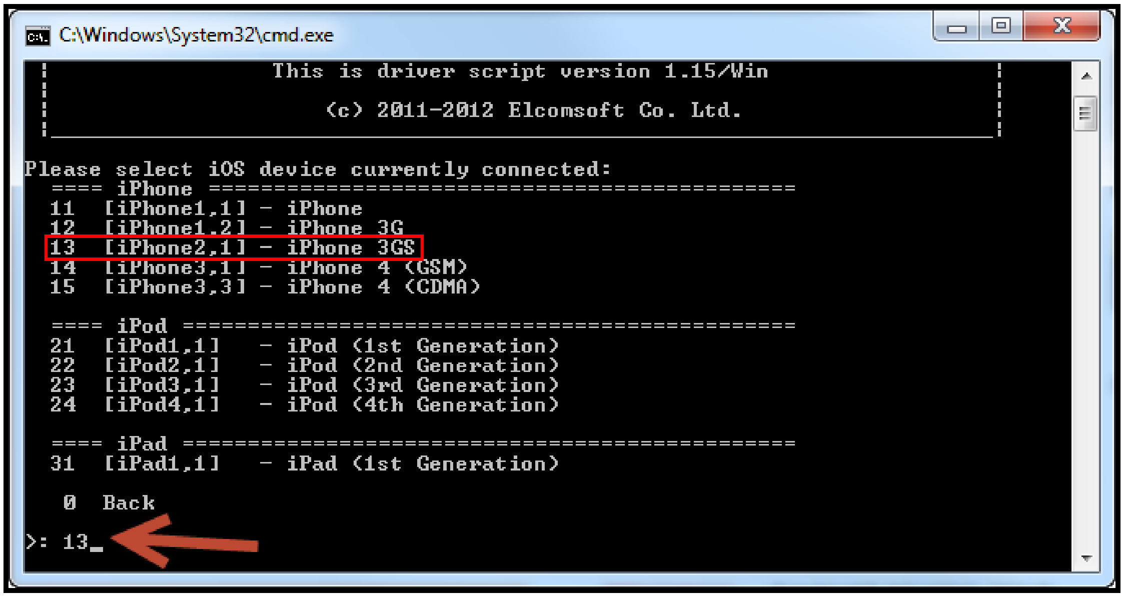
Figure 6 - Placing the Device into DFU Mode



```
                  Welcome to Elcomsoft iOS Forensic Toolkit
                   This is driver script version 1.15/Win

                     (c) 2011-2012 Elcomsoft Co. Ltd.

Please make sure that the device is plugged in and switched off.

If necessary, connect the device and switch it off by holding
Sleep (corner) button and dragging the red slider when it appears.

Would you like to continue? (Y/n): y

To put iOS device into DFU you will need to:
1. Push and hold Sleep (corner) and Home (center) buttons for
   10 seconds.
2. Release Sleep button but continue to hold Home button for
   another 10 seconds.

This script will help you with the timings.

When you are ready press 'Enter' and be prepared to press
Sleep and Home buttons in 3 seconds.

Prepare to push and hold Sleep and Home buttons in
...3...2...1
Push and hold Sleep and Home buttons for
...10...9...8...7...6...5...4
Prepare to release Sleep button while holding Home button
...3...2...1
Release Sleep button but continue to hold Home button for
...10...9...8...7...6...5...4...3...2...1

Release Home button.

Your iOS Device should be in DFU mode now.

Device screen should be blank, device should look like it is off.
If screen shows Apple or iTunes logo then device is not in DFU mode.
In this case reboot the device and try again.

Would you like to load Toolkit Ramdisk now? (Y/n):
```

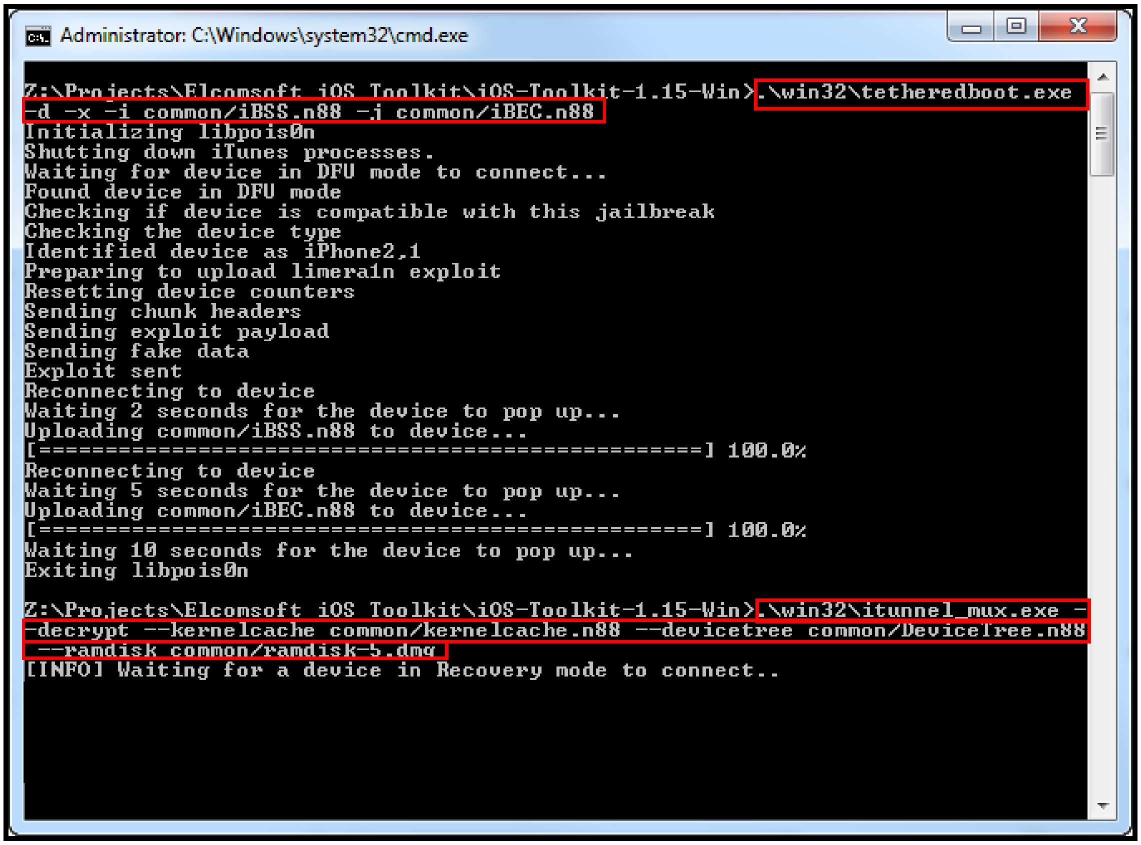
Once you place the device in DFU mode, you can upload the toolkit Ramdisk and begin acquiring the device. In guided mode, you can load the toolkit Ramdisk in a matter of seconds with a few keys (Figure 7); in manual mode, you will have to enter in a command that will take a little longer to load the 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



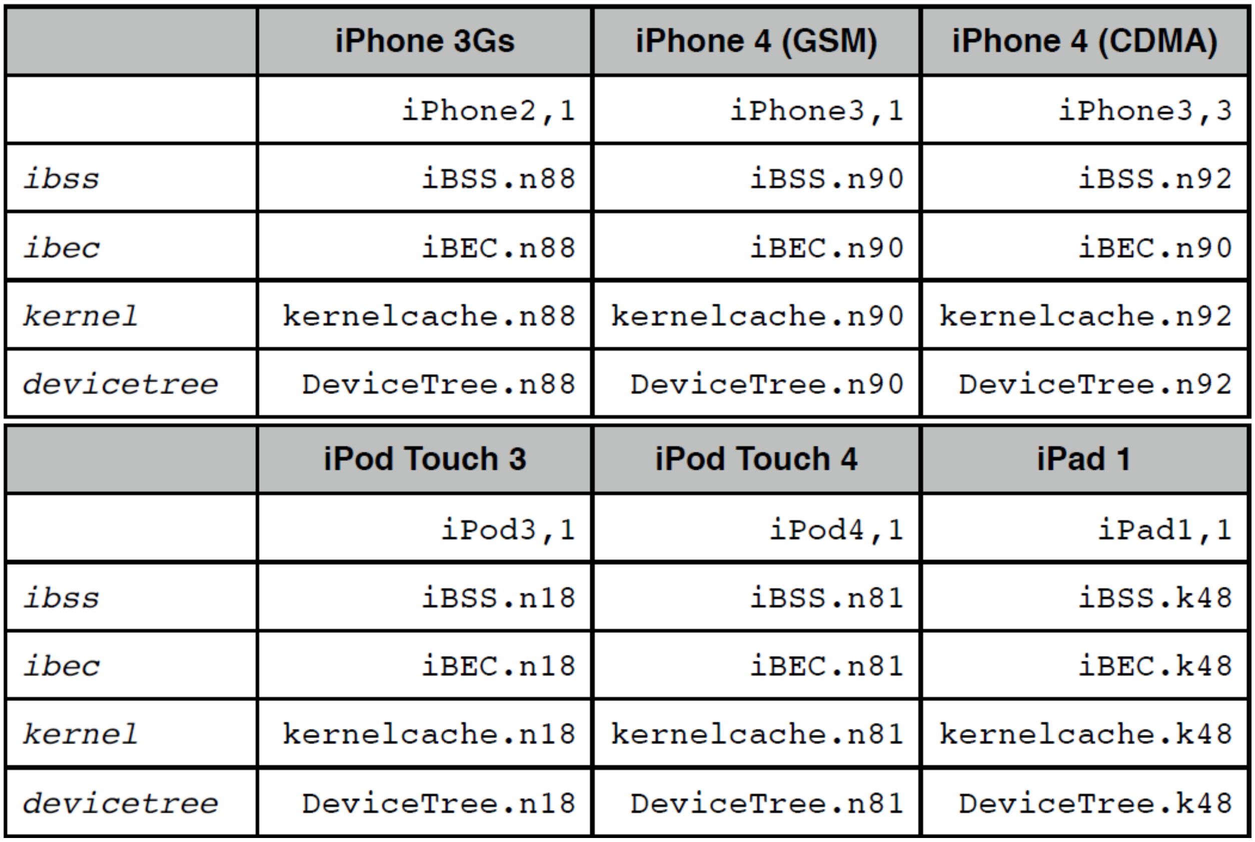
```
 |                  This is driver script version 1.15/Win                  |
 |                                                                          |
 |                    (c) 2011-2012 Elcomsoft Co. Ltd.                      |
 |__________________________________________________________________________|

Please select iOS device currently connected:
  ==== iPhone =============================================
  11  [iPhone1,1] - iPhone
  12  [iPhone1,2] - iPhone 3G
  13  [iPhone2,1] - iPhone 3GS
  14  [iPhone3,1] - iPhone 4 (GSM)
  15  [iPhone3,3] - iPhone 4 (CDMA)

  ==== iPod ===============================================
  21  [iPod1,1]   - iPod (1st Generation)
  22  [iPod2,1]   - iPod (2nd Generation)
  23  [iPod3,1]   - iPod (3rd Generation)
  24  [iPod4,1]   - iPod (4th Generation)

  ==== iPad ===============================================
  31  [iPad1,1]   - iPad (1st Generation)

   0  Back

>: 13_
```

Figure 8 - Loading the Ramdisk with Manual Mode



```
Z:\Projects\Elcomsoft iOS Toolkit\iOS-Toolkit-1.15-Win>.\win32\tetheredboot.exe
-d -x -i common/iBSS.n88 -j common/iBEC.n88
Initializing libpois0n
Shutting down iTunes processes.
Waiting for device in DFU mode to connect...
Found device in DFU mode
Checking if device is compatible with this jailbreak
Checking the device type
Identified device as iPhone2,1
Preparing to upload limera1n exploit
Resetting device counters
Sending chunk headers
Sending exploit payload
Sending fake data
Exploit sent
Reconnecting to device
Waiting 2 seconds for the device to pop up...
Uploading common/iBSS.n88 to device...
[==================================================] 100.0%
Reconnecting to device
Waiting 5 seconds for the device to pop up...
Uploading common/iBEC.n88 to device...
[==================================================] 100.0%
Waiting 10 seconds for the device to pop up...
Exiting libpois0n

Z:\Projects\Elcomsoft iOS Toolkit\iOS-Toolkit-1.15-Win>.\win32\itunnel_mux.exe -
-decrypt --kernelcache common/kernelcache.n88 --devicetree common/DeviceTree.n88
 --ramdisk common/ramdisk-5.dmg
[INFO] Waiting for a device in Recovery mode to connect..
```

Figure 9 - iOS Commands to Load Ramdisk

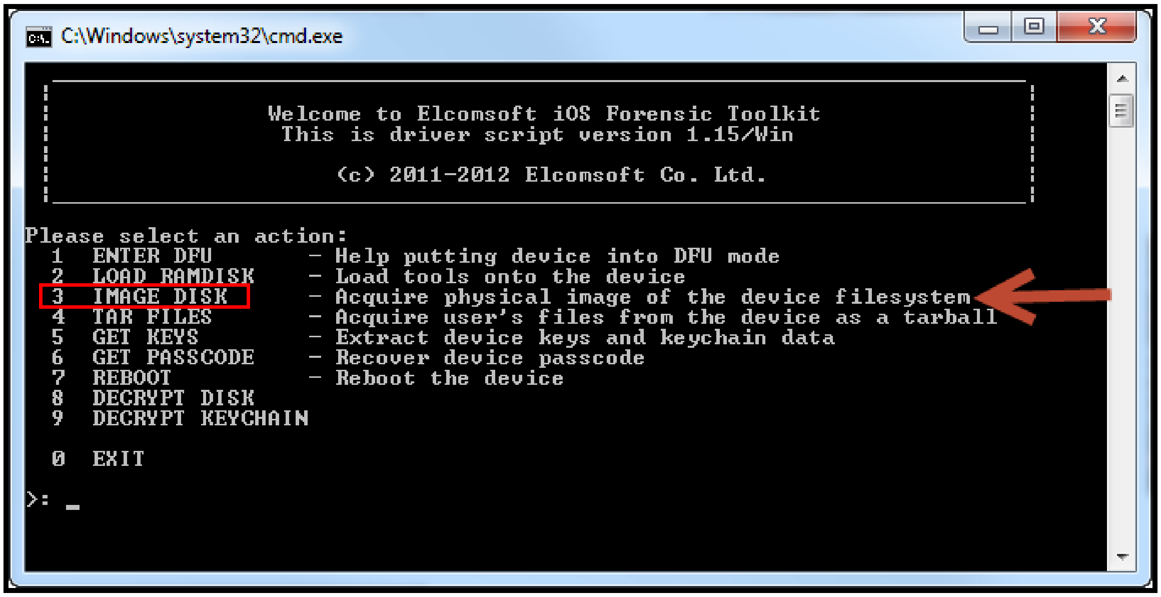


	iPhone 3Gs	iPhone 4 (GSM)	iPhone 4 (CDMA)
	iPhone2,1	iPhone3,1	iPhone3,3
ibss	iBSS.n88	iBSS.n90	iBSS.n92
ibec	iBEC.n88	iBEC.n90	iBEC.n90
kernel	kernelcache.n88	kernelcache.n90	kernelcache.n92
devicetree	DeviceTree.n88	DeviceTree.n90	DeviceTree.n92
	iPod Touch 3	**iPod Touch 4**	**iPad 1**
	iPod3,1	iPod4,1	iPad1,1
ibss	iBSS.n18	iBSS.n81	iBSS.k48
ibec	iBEC.n18	iBEC.n81	iBEC.k48
kernel	kernelcache.n18	kernelcache.n81	kernelcache.k48
devicetree	DeviceTree.n18	DeviceTree.n81	DeviceTree.k48

[5]

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).

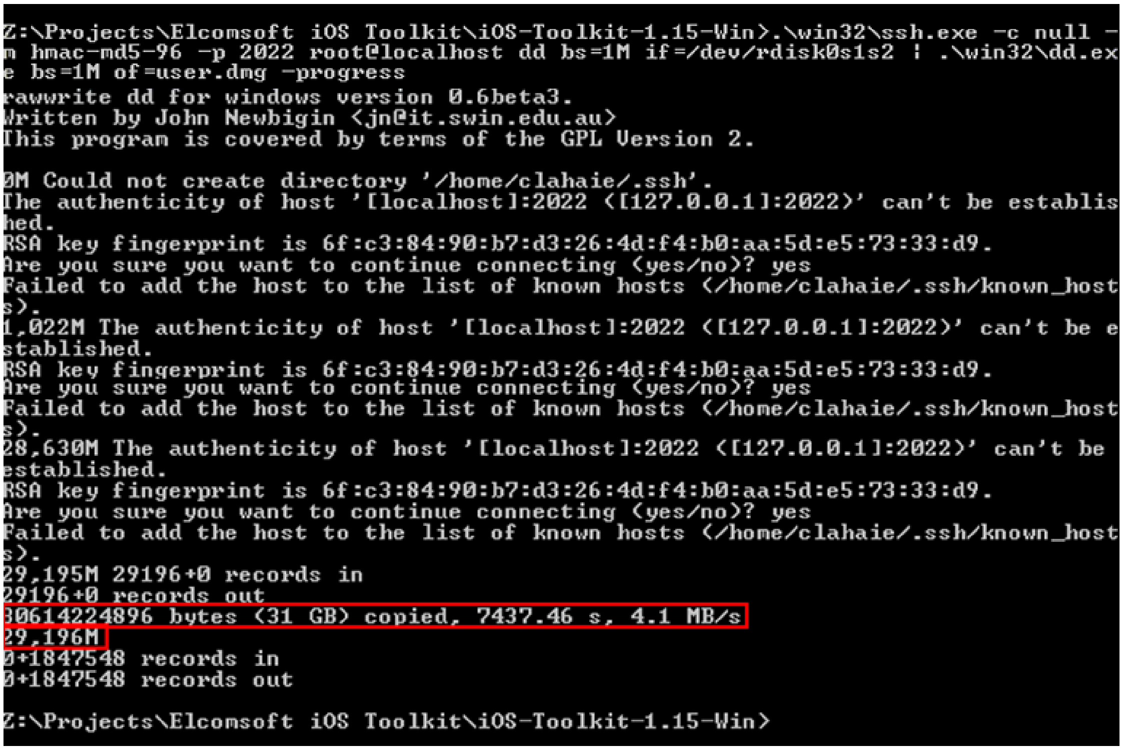
Figure 10 - Acquiring System Partition with Guided Mode



```
           Welcome to Elcomsoft iOS Forensic Toolkit
            This is driver script version 1.15/Win

                (c) 2011-2012 Elcomsoft Co. Ltd.

Please select an action:
  1  ENTER DFU         - Help putting device into DFU mode
  2  LOAD RAMDISK      - Load tools onto the device
  3  IMAGE DISK        - Acquire physical image of the device filesystem
  4  TAR FILES         - Acquire user's files from the device as a tarball
  5  GET KEYS          - Extract device keys and keychain data
  6  GET PASSCODE      - Recover device passcode
  7  REBOOT            - Reboot the device
  8  DECRYPT DISK
  9  DECRYPT KEYCHAIN

  0  EXIT

>: _
```

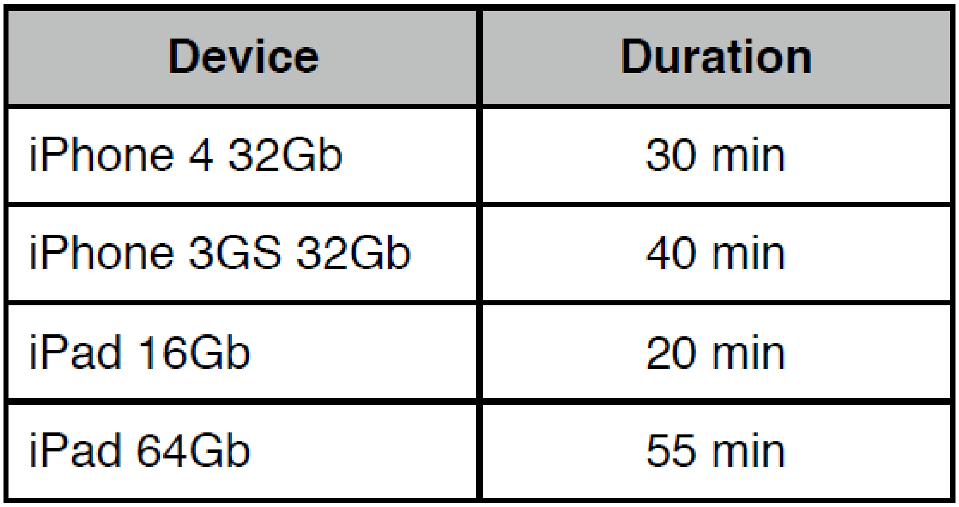
[5] Elcomsoft. (2012). Elcomsoft iOS Forensic Toolkit. Retrieved June 6, 2013.

Figure 11 - Acquiring User Partition with Manual Mode



```
Z:\Projects\Elcomsoft iOS Toolkit\iOS-Toolkit-1.15-Win>.\win32\ssh.exe -c null -
m hmac-md5-96 -p 2022 root@localhost dd bs=1M if=/dev/rdisk0s1s2 | .\win32\dd.ex
e bs=1M of=user.dmg -progress
rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.

0M Could not create directory '/home/clahaie/.ssh'.
The authenticity of host '[localhost]:2022 ([127.0.0.1]:2022)' can't be establis
hed.
RSA key fingerprint is 6f:c3:84:90:b7:d3:26:4d:f4:b0:aa:5d:e5:73:33:d9.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/clahaie/.ssh/known_host
s).
1,022M The authenticity of host '[localhost]:2022 ([127.0.0.1]:2022)' can't be e
stablished.
RSA key fingerprint is 6f:c3:84:90:b7:d3:26:4d:f4:b0:aa:5d:e5:73:33:d9.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/clahaie/.ssh/known_host
s).
28,630M The authenticity of host '[localhost]:2022 ([127.0.0.1]:2022)' can't be
established.
RSA key fingerprint is 6f:c3:84:90:b7:d3:26:4d:f4:b0:aa:5d:e5:73:33:d9.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/clahaie/.ssh/known_host
s).
29,195M 29196+0 records in
29196+0 records out
30614224896 bytes (31 GB) copied, 7437.46 s, 4.1 MB/s
29,196M
0+1847548 records in
0+1847548 records out

Z:\Projects\Elcomsoft iOS Toolkit\iOS-Toolkit-1.15-Win>
```

Figure 12 - User Partition Transfer Times



Device	Duration
iPhone 4 32Gb	30 min
iPhone 3GS 32Gb	40 min
iPad 16Gb	20 min
iPad 64Gb	55 min

[5]

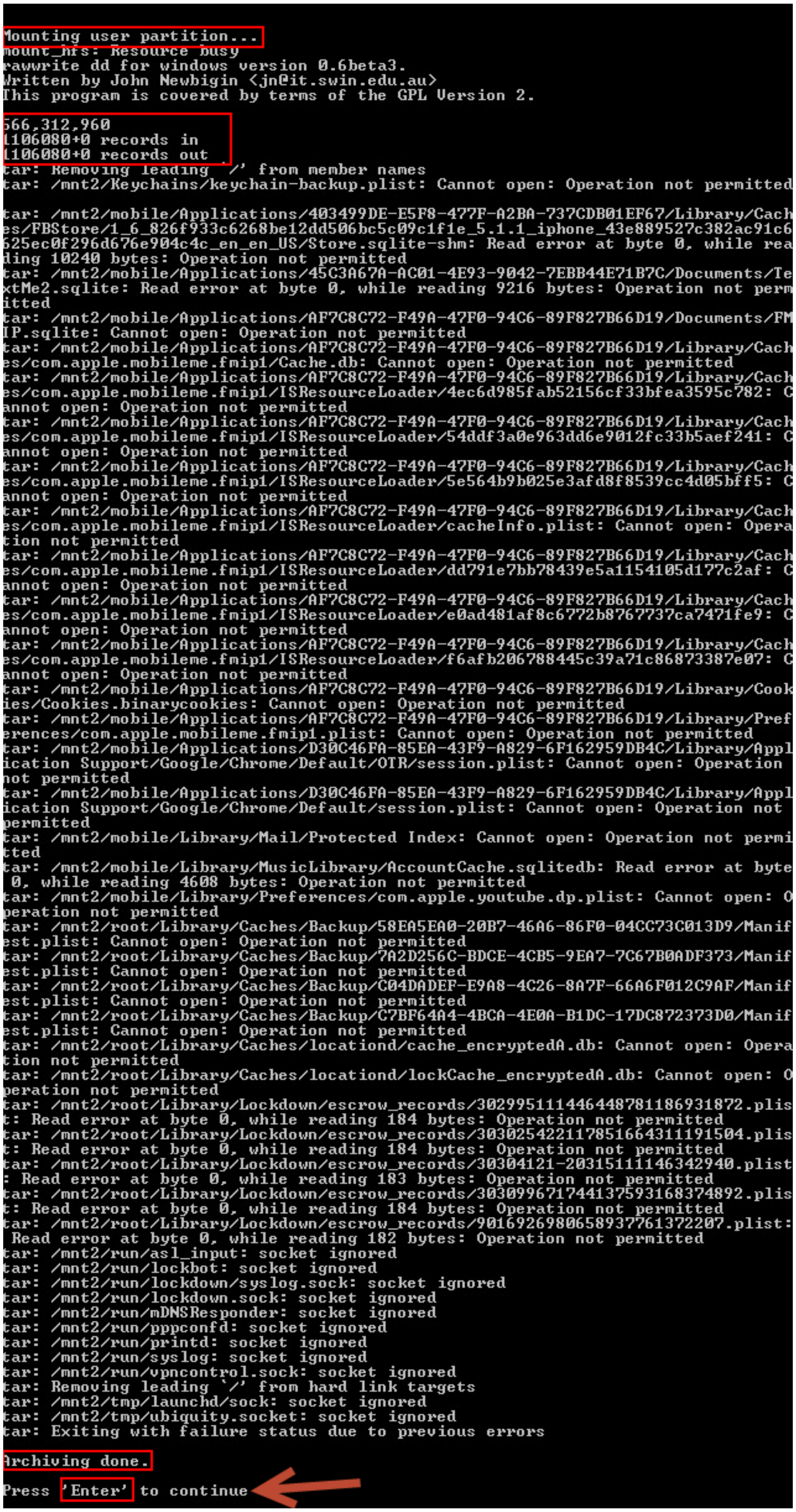
Acquiring Logical Partition

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)



```
Mounting user partition...
mount_hfs: Resource busy
rawwrite dd for windows version 0.6beta3.
Written by John Newbigin <jn@it.swin.edu.au>
This program is covered by terms of the GPL Version 2.

566,312,960
1106080+0 records in
1106080+0 records out
tar: Removing leading `/' from member names
tar: /mnt2/Keychains/keychain-backup.plist: Cannot open: Operation not permitted

tar: /mnt2/mobile/Applications/403499DE-E5F8-477F-A2BA-737CDB01EF67/Library/Cach
es/FBStore/1_6_826f933c6268be12dd506bc5c09c1f1e_5.1.1_iphone_43e889527c382ac91c6
625ec0f296d676e904c4c_en_en_US/Store.sqlite-shm: Read error at byte 0, while rea
ding 10240 bytes: Operation not permitted
tar: /mnt2/mobile/Applications/45C3A67A-AC01-4E93-9042-7EBB44E71B7C/Documents/Te
xtMe2.sqlite: Read error at byte 0, while reading 9216 bytes: Operation not perm
itted
tar: /mnt2/mobile/Applications/AF7C8C72-F49A-47F0-94C6-89F827B66D19/Documents/FM
IP.sqlite: Cannot open: Operation not permitted
tar: /mnt2/mobile/Applications/AF7C8C72-F49A-47F0-94C6-89F827B66D19/Library/Cach
es/com.apple.mobileme.fmip1/Cache.db: Cannot open: Operation not permitted
tar: /mnt2/mobile/Applications/AF7C8C72-F49A-47F0-94C6-89F827B66D19/Library/Cach
es/com.apple.mobileme.fmip1/ISResourceLoader/4ec6d985fab52156cf33bfea3595c782: C
annot open: Operation not permitted
tar: /mnt2/mobile/Applications/AF7C8C72-F49A-47F0-94C6-89F827B66D19/Library/Cach
es/com.apple.mobileme.fmip1/ISResourceLoader/54ddf3a0e963dd6e9012fc33b5aef241: C
annot open: Operation not permitted
tar: /mnt2/mobile/Applications/AF7C8C72-F49A-47F0-94C6-89F827B66D19/Library/Cach
es/com.apple.mobileme.fmip1/ISResourceLoader/5e564b9b025e3afd8f8539cc4d05bff5: C
annot open: Operation not permitted
tar: /mnt2/mobile/Applications/AF7C8C72-F49A-47F0-94C6-89F827B66D19/Library/Cach
es/com.apple.mobileme.fmip1/ISResourceLoader/cacheInfo.plist: Cannot open: Opera
tion not permitted
tar: /mnt2/mobile/Applications/AF7C8C72-F49A-47F0-94C6-89F827B66D19/Library/Cach
es/com.apple.mobileme.fmip1/ISResourceLoader/dd791e7bb78439e5a1154105d177c2af: C
annot open: Operation not permitted
tar: /mnt2/mobile/Applications/AF7C8C72-F49A-47F0-94C6-89F827B66D19/Library/Cach
es/com.apple.mobileme.fmip1/ISResourceLoader/e0ad481af8c6772b8767737ca7471fe9: C
annot open: Operation not permitted
tar: /mnt2/mobile/Applications/AF7C8C72-F49A-47F0-94C6-89F827B66D19/Library/Cach
es/com.apple.mobileme.fmip1/ISResourceLoader/f6afb206788445c39a71c86873387e07: C
annot open: Operation not permitted
tar: /mnt2/mobile/Applications/AF7C8C72-F49A-47F0-94C6-89F827B66D19/Library/Cook
ies/Cookies.binarycookies: Cannot open: Operation not permitted
tar: /mnt2/mobile/Applications/AF7C8C72-F49A-47F0-94C6-89F827B66D19/Library/Pref
erences/com.apple.mobileme.fmip1.plist: Cannot open: Operation not permitted
tar: /mnt2/mobile/Applications/D30C46FA-85EA-43F9-A829-6F162959DB4C/Library/Appl
ication Support/Google/Chrome/Default/OTR/session.plist: Cannot open: Operation
not permitted
tar: /mnt2/mobile/Applications/D30C46FA-85EA-43F9-A829-6F162959DB4C/Library/Appl
ication Support/Google/Chrome/Default/session.plist: Cannot open: Operation not
permitted
tar: /mnt2/mobile/Library/Mail/Protected Index: Cannot open: Operation not permi
tted
tar: /mnt2/mobile/Library/MusicLibrary/AccountCache.sqlitedb: Read error at byte
 0, while reading 4608 bytes: Operation not permitted
tar: /mnt2/mobile/Library/Preferences/com.apple.youtube.dp.plist: Cannot open: O
peration not permitted
tar: /mnt2/root/Library/Caches/Backup/58EA5EA0-20B7-46A6-86F0-04CC73C013D9/Manif
est.plist: Cannot open: Operation not permitted
tar: /mnt2/root/Library/Caches/Backup/7A2D256C-BDCE-4CB5-9EA7-7C67B0ADF373/Manif
est.plist: Cannot open: Operation not permitted
tar: /mnt2/root/Library/Caches/Backup/C04DADEF-E9A8-4C26-8A7F-66A6F012C9AF/Manif
est.plist: Cannot open: Operation not permitted
tar: /mnt2/root/Library/Caches/Backup/C7BF64A4-4BCA-4E0A-B1DC-17DC872373D0/Manif
est.plist: Cannot open: Operation not permitted
tar: /mnt2/root/Library/Caches/locationd/cache_encryptedA.db: Cannot open: Opera
tion not permitted
tar: /mnt2/root/Library/Caches/locationd/lockCache_encryptedA.db: Cannot open: O
peration not permitted
tar: /mnt2/root/Library/Lockdown/escrow_records/302995111446448781186931872.plis
t: Read error at byte 0, while reading 184 bytes: Operation not permitted
tar: /mnt2/root/Library/Lockdown/escrow_records/303025422117851664311191504.plis
t: Read error at byte 0, while reading 184 bytes: Operation not permitted
tar: /mnt2/root/Library/Lockdown/escrow_records/30304121-20315111146342940.plist
: Read error at byte 0, while reading 183 bytes: Operation not permitted
tar: /mnt2/root/Library/Lockdown/escrow_records/303099671744137593168374892.plis
t: Read error at byte 0, while reading 184 bytes: Operation not permitted
tar: /mnt2/root/Library/Lockdown/escrow_records/9016926980658937761372207.plist:
 Read error at byte 0, while reading 182 bytes: Operation not permitted
tar: /mnt2/run/asl_input: socket ignored
tar: /mnt2/run/lockbot: socket ignored
tar: /mnt2/run/lockdown/syslog.sock: socket ignored
tar: /mnt2/run/lockdown.sock: socket ignored
tar: /mnt2/run/mDNSResponder: socket ignored
tar: /mnt2/run/pppconfd: socket ignored
tar: /mnt2/run/printd: socket ignored
tar: /mnt2/run/syslog: socket ignored
tar: /mnt2/run/vpncontrol.sock: socket ignored
tar: Removing leading `/' from hard link targets
tar: /mnt2/tmp/launchd/sock: socket ignored
tar: /mnt2/tmp/ubiquity.socket: socket ignored
tar: Exiting with failure status due to previous errors

Archiving done.

Press 'Enter' to continue
```

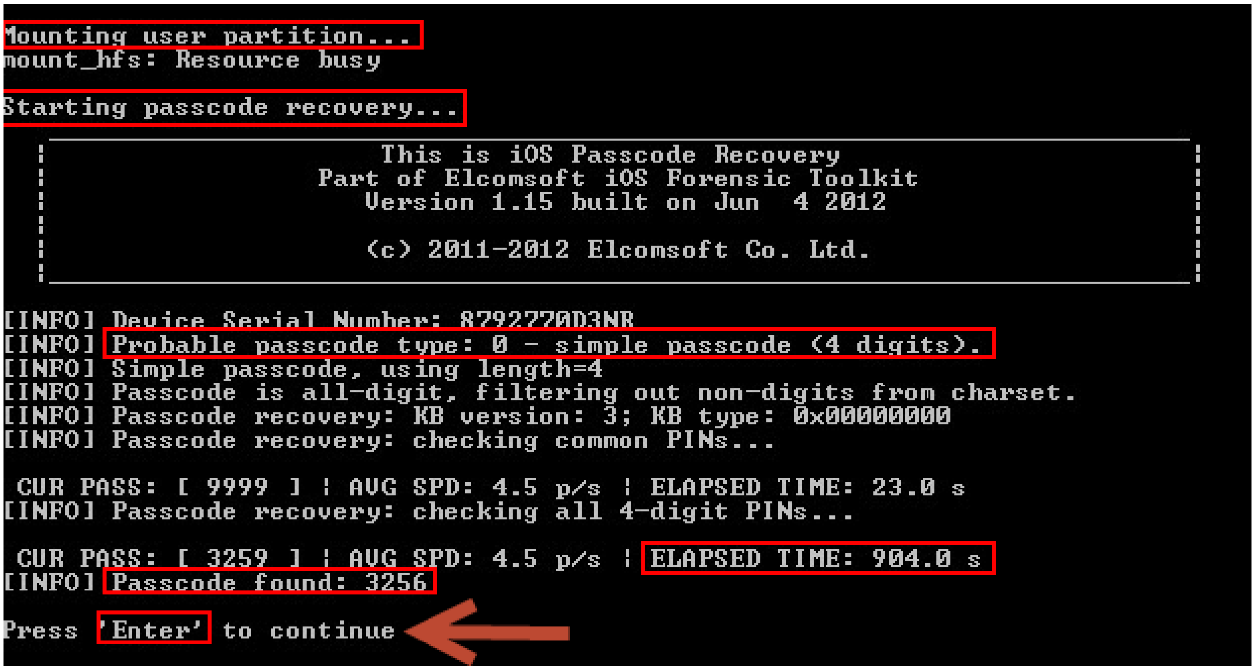
Recovering User Lock Passcode from iOS 4.x/5.x Devices

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."[6]

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."[6] You can create your own dictionary list with words you have been provided with, or you can download some commonly used dictionary lists off of the Internet.

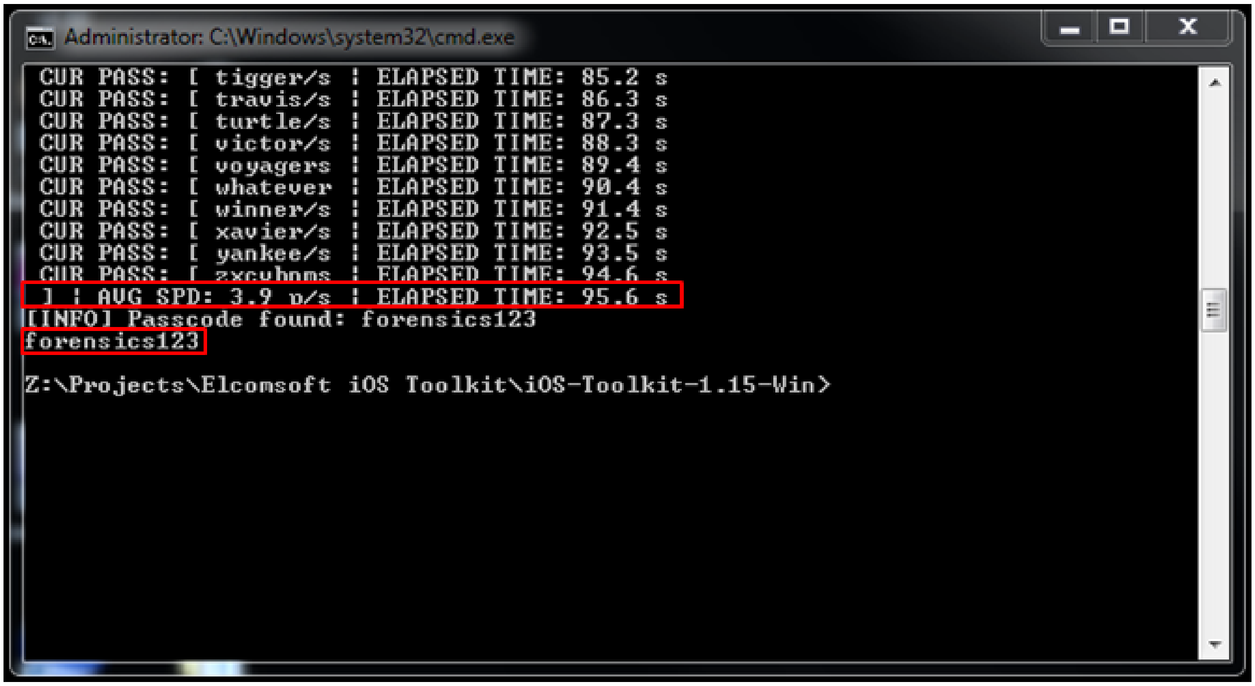
Figure 14 - Bruteforcing a Simple Passcode



```
Mounting user partition...
mount_hfs: Resource busy

Starting passcode recovery...
    ________________________________________________________________________
   ¦                    This is iOS Passcode Recovery                       ¦
   ¦                Part of Elcomsoft iOS Forensic Toolkit                  ¦
   ¦                   Version 1.15 built on Jun  4 2012                    ¦
   ¦                                                                        ¦
   ¦                   (c) 2011-2012 Elcomsoft Co. Ltd.                     ¦
   ¦________________________________________________________________________¦

[INFO] Device Serial Number: 8792770D3NR
[INFO] Probable passcode type: 0 - simple passcode (4 digits).
[INFO] Simple passcode, using length=4
[INFO] Passcode is all-digit, filtering out non-digits from charset.
[INFO] Passcode recovery: KB version: 3; KB type: 0x00000000
[INFO] Passcode recovery: checking common PINs...

 CUR PASS: [ 9999 ] ¦ AVG SPD: 4.5 p/s ¦ ELAPSED TIME: 23.0 s
[INFO] Passcode recovery: checking all 4-digit PINs...

 CUR PASS: [ 3259 ] ¦ AVG SPD: 4.5 p/s ¦ ELAPSED TIME: 904.0 s
[INFO] Passcode found: 3256

Press 'Enter' to continue
```

[6] Elcomsoft iOS Forensics Toolkit. (n.d.). *Enhanced Forensic Access to IPhone/iPad/iPod Devices Running Apple IOS*. Retrieved July 11, 2013, from http://www.elcomsoft.com/eift.html

Figure 15 - Dictionary Attack Against a Complex Passcode



```
 CUR PASS: [ tigger/s ¦ ELAPSED TIME: 85.2 s
 CUR PASS: [ travis/s ¦ ELAPSED TIME: 86.3 s
 CUR PASS: [ turtle/s ¦ ELAPSED TIME: 87.3 s
 CUR PASS: [ victor/s ¦ ELAPSED TIME: 88.3 s
 CUR PASS: [ voyagers ¦ ELAPSED TIME: 89.4 s
 CUR PASS: [ whatever ¦ ELAPSED TIME: 90.4 s
 CUR PASS: [ winner/s ¦ ELAPSED TIME: 91.4 s
 CUR PASS: [ xavier/s ¦ ELAPSED TIME: 92.5 s
 CUR PASS: [ yankee/s ¦ ELAPSED TIME: 93.5 s
 CUR PASS: [ zxcvbnms ¦ ELAPSED TIME: 94.6 s
  ] ¦ AVG SPD: 3.9 p/s ¦ ELAPSED TIME: 95.6 s
[INFO] Passcode found: forensics123
forensics123

Z:\Projects\Elcomsoft iOS Toolkit\iOS-Toolkit-1.15-Win>
```

Recovering Encryption Keys and Keychain Data

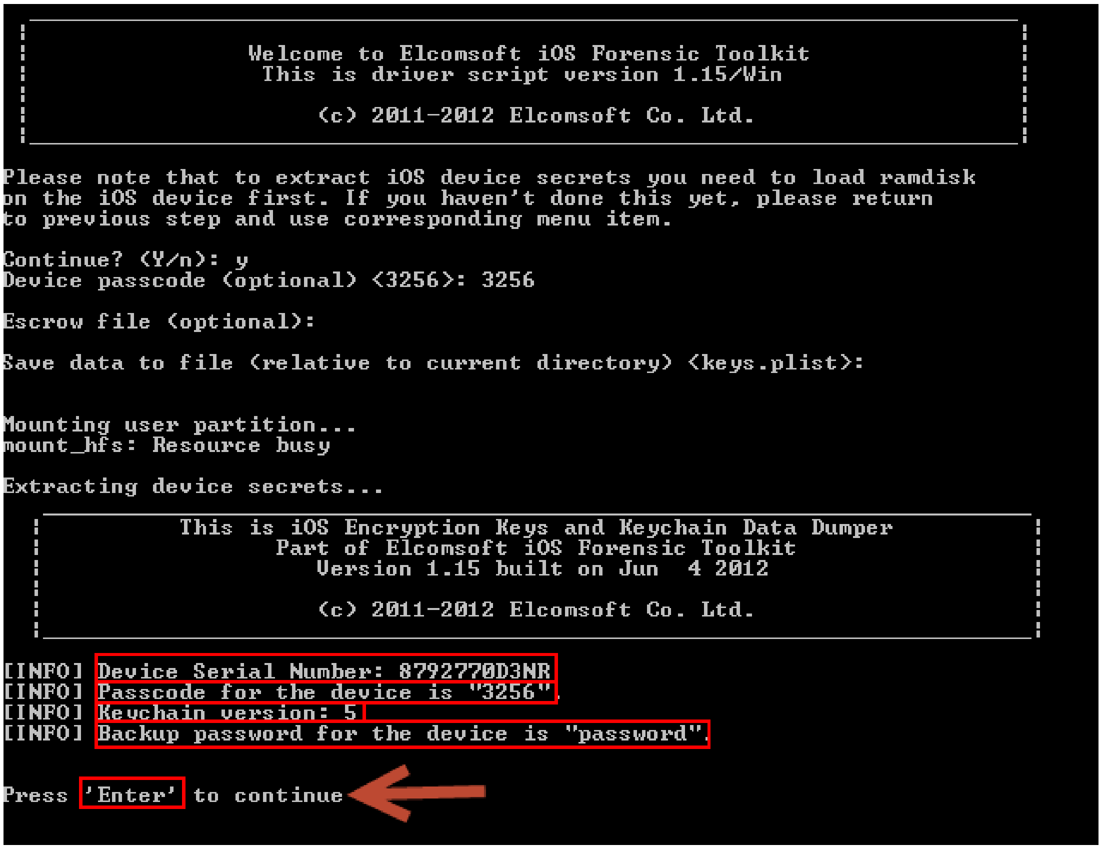
Elcomsoft iOS Forensic Toolkit can access iOS secrets, including most keychain data,[7] opening investigators' access to highly sensitive data such as login/password information to Web sites and other resources.

> "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."[6]

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.

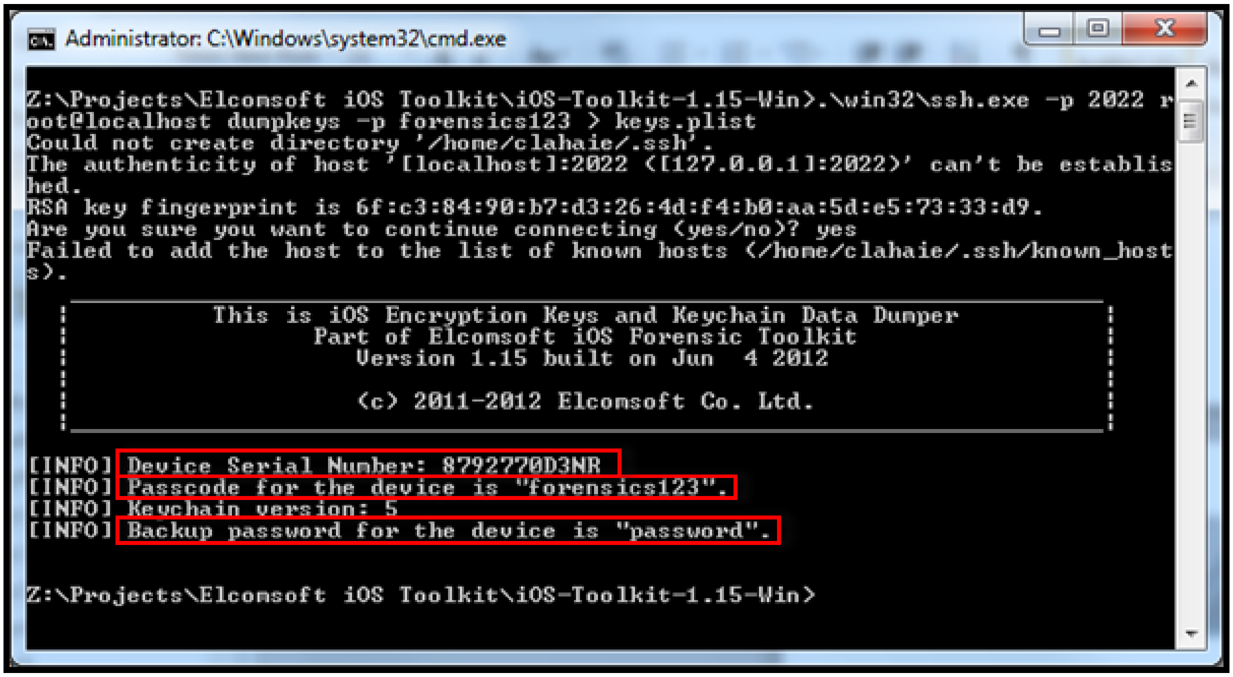
[7] The keychain is the password management system on Apple devices. It allows a user to store passwords for programs, e-mail accounts, web sites, and more.

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



```
                 Welcome to Elcomsoft iOS Forensic Toolkit
                  This is driver script version 1.15/Win

                    (c) 2011-2012 Elcomsoft Co. Ltd.

Please note that to extract iOS device secrets you need to load ramdisk
on the iOS device first. If you haven't done this yet, please return
to previous step and use corresponding menu item.

Continue? (Y/n): y
Device passcode (optional) <3256>: 3256

Escrow file (optional):

Save data to file (relative to current directory) <keys.plist>:


Mounting user partition...
mount_hfs: Resource busy

Extracting device secrets...

            This is iOS Encryption Keys and Keychain Data Dumper
                   Part of Elcomsoft iOS Forensic Toolkit
                     Version 1.15 built on Jun  4 2012

                      (c) 2011-2012 Elcomsoft Co. Ltd.

[INFO] Device Serial Number: 8792770D3NR
[INFO] Passcode for the device is "3256".
[INFO] Keychain version: 5
[INFO] Backup password for the device is "password".


Press 'Enter' to continue
```

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

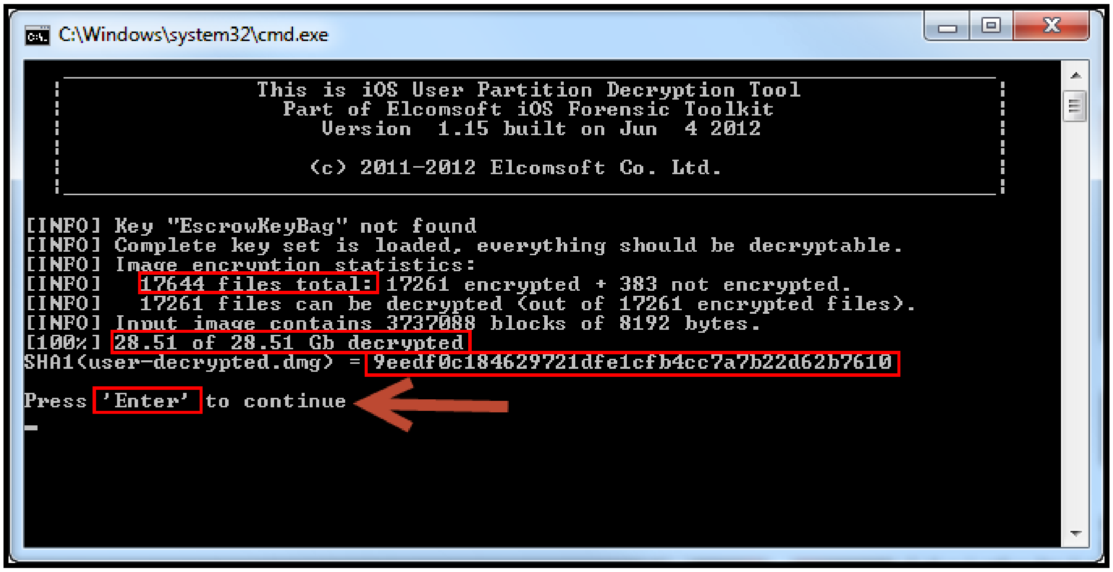


```
Z:\Projects\Elcomsoft iOS Toolkit\iOS-Toolkit-1.15-Win>.\win32\ssh.exe -p 2022 r
oot@localhost dumpkeys -p forensics123 > keys.plist
Could not create directory '/home/clahaie/.ssh'.
The authenticity of host '[localhost]:2022 ([127.0.0.1]:2022)' can't be establis
hed.
RSA key fingerprint is 6f:c3:84:90:b7:d3:26:4d:f4:b0:aa:5d:e5:73:33:d9.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts (/home/clahaie/.ssh/known_host
s).

           This is iOS Encryption Keys and Keychain Data Dumper
                  Part of Elcomsoft iOS Forensic Toolkit
                    Version 1.15 built on Jun  4 2012

                     (c) 2011-2012 Elcomsoft Co. Ltd.

[INFO] Device Serial Number: 8792770D3NR
[INFO] Passcode for the device is "forensics123".
[INFO] Keychain version: 5
[INFO] Backup password for the device is "password".


Z:\Projects\Elcomsoft iOS Toolkit\iOS-Toolkit-1.15-Win>
```

Decrypting User Partition and Keychain Data

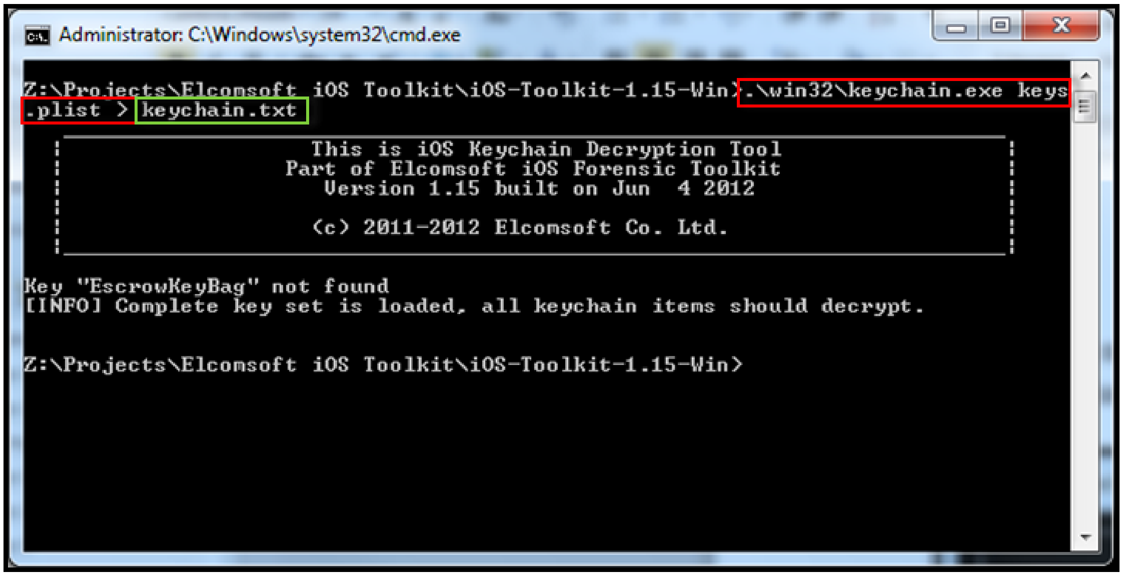
Once you have recovered the keychain data, the user lock passcode, and acquired the user partition, an investigator can begin decrypting the data. By decrypting this data, all of the information will become readable and accessible to an investigator. Once again, you can use both the guided mode (Figure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



```
                      This is iOS User Partition Decryption Tool
                        Part of Elcomsoft iOS Forensic Toolkit
                          Version  1.15 built on Jun  4 2012

                          (c) 2011-2012 Elcomsoft Co. Ltd.

[INFO] Key "EscrowKeyBag" not found
[INFO] Complete key set is loaded, everything should be decryptable.
[INFO] Image encryption statistics:
[INFO]   17644 files total: 17261 encrypted + 383 not encrypted.
[INFO]   17261 files can be decrypted (out of 17261 encrypted files).
[INFO] Input image contains 3737088 blocks of 8192 bytes.
[100%] 28.51 of 28.51 Gb decrypted
SHA1(user-decrypted.dmg) = 9eedf0c184629721dfe1cfb4cc7a7b22d62b7610

Press 'Enter' to continue
_
```

Figure 19 – Decrypting the Keychain Data with Manual Mode

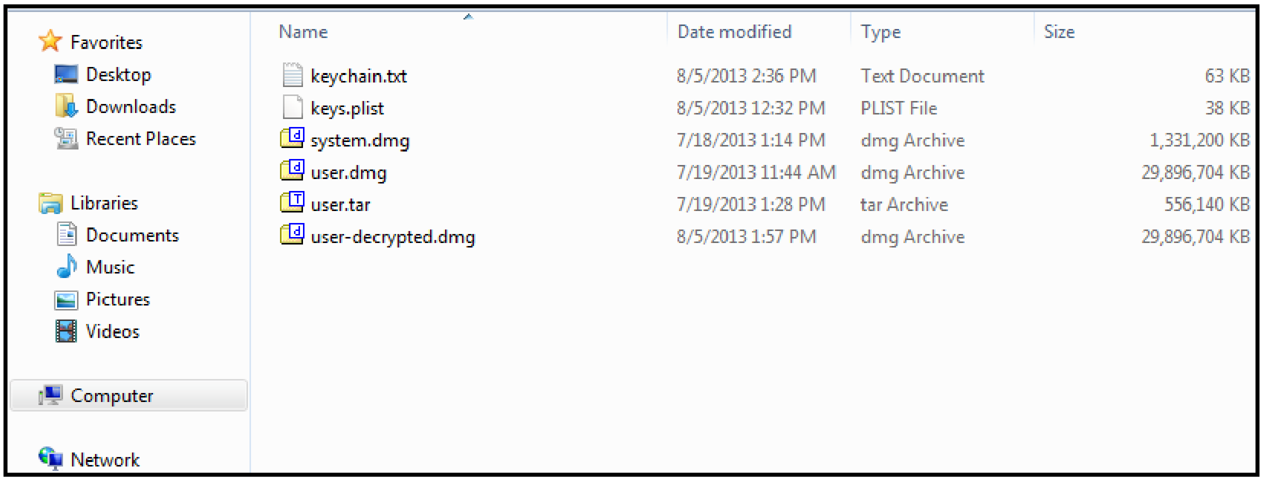


```
Z:\Projects\Elcomsoft iOS Toolkit\iOS-Toolkit-1.15-Win>.\win32\keychain.exe keys
.plist > keychain.txt

                      This is iOS Keychain Decryption Tool
                        Part of Elcomsoft iOS Forensic Toolkit
                          Version 1.15 built on Jun  4 2012

                          (c) 2011-2012 Elcomsoft Co. Ltd.

Key "EscrowKeyBag" not found
[INFO] Complete key set is loaded, all keychain items should decrypt.


Z:\Projects\Elcomsoft iOS Toolkit\iOS-Toolkit-1.15-Win>
```

Analyzing the Data

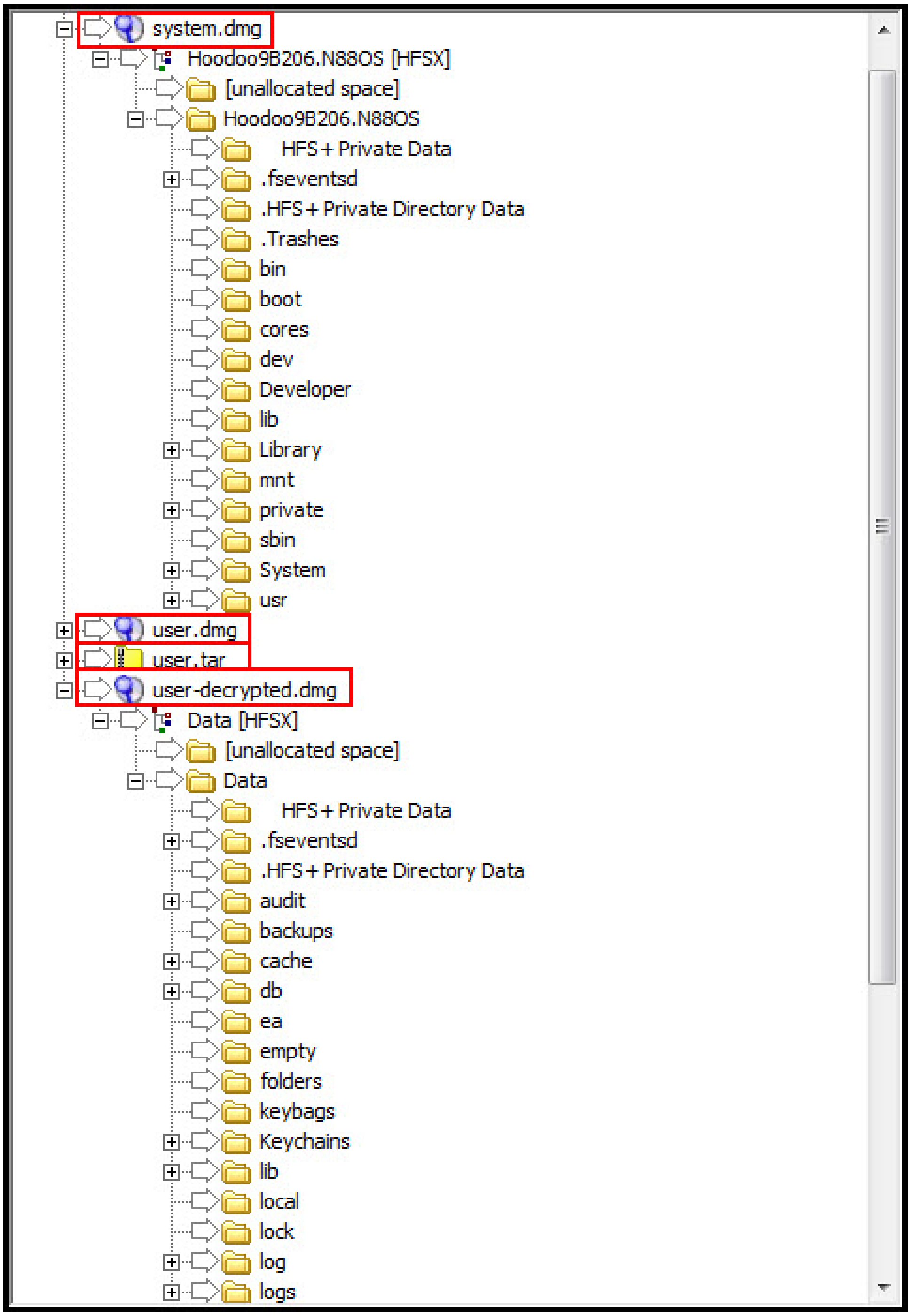
Once you have successfully extracted and decrypted all of the data (Figure 20), you can begin analyzing it with forensic acquisition and analysis tools, such as FTK Imager and FTK (Forensic Toolkit) 4.1 (Figure 21). Our research claimed that you can read this type of file (.dmg file format) in EnCase,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

Figure 20 - Extracted Data



Name	Date modified	Type	Size
keychain.txt	8/5/2013 2:36 PM	Text Document	63 KB
keys.plist	8/5/2013 12:32 PM	PLIST File	38 KB
system.dmg	7/18/2013 1:14 PM	dmg Archive	1,331,200 KB
user.dmg	7/19/2013 11:44 AM	dmg Archive	29,896,704 KB
user.tar	7/19/2013 1:28 PM	tar Archive	556,140 KB
user-decrypted.dmg	8/5/2013 1:57 PM	dmg Archive	29,896,704 KB

Figure 21 - Analyzing Extracted Data in FTK 4.1



```
system.dmg
    Hoodoo9B206.N88OS [HFSX]
        [unallocated space]
        Hoodoo9B206.N88OS
            HFS+ Private Data
            .fseventsd
            .HFS+ Private Directory Data
            .Trashes
            bin
            boot
            cores
            dev
            Developer
            lib
            Library
            mnt
            private
            sbin
            System
            usr
user.dmg
user.tar
user-decrypted.dmg
    Data [HFSX]
        [unallocated space]
        Data
            HFS+ Private Data
            .fseventsd
            .HFS+ Private Directory Data
            audit
            backups
            cache
            db
            ea
            empty
            folders
            keybags
            Keychains
            lib
            local
            lock
            log
            logs
```