ACQUISITION AND ANALYSIS OF IOS DEVICES

MATTIA EPIFANI
SANS FORENSICS PRAGUE
PRAGUE, 10 OCTOBER 2013
When we are dealing with the forensics acquisition of an iOS device we have to answer **3 questions** before starting the operation:

1. What is the model?
2. What is the iOS version installed?
3. Is the device locked with a pass code?
   1. Simple passcode?
   2. Complex passcode?
# iPhone Model Chart

<table>
<thead>
<tr>
<th>Device name</th>
<th>Model number</th>
<th>Internal Name</th>
<th>Identifier</th>
<th>Year</th>
<th>Capacity (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone 5S (CDMA)</td>
<td>A1457-A1518-A1528-A1530</td>
<td>N53AP</td>
<td>iPhone6,2</td>
<td>2013</td>
<td>16, 32</td>
</tr>
<tr>
<td>iPhone 5S (GSM)</td>
<td>A1433–A1533</td>
<td>N51AP</td>
<td>iPhone6,1</td>
<td>2013</td>
<td>16, 32, 64</td>
</tr>
<tr>
<td>iPhone 5C (CDMA)</td>
<td>A1507 – A1516 – A1526 – A1529</td>
<td>N49AP</td>
<td>iPhone5,4</td>
<td>2013</td>
<td>16, 32</td>
</tr>
<tr>
<td>iPhone 5C (GSM)</td>
<td>A1456 – A1532</td>
<td>N48AP</td>
<td>iPhone5,3</td>
<td>2013</td>
<td>16, 32</td>
</tr>
<tr>
<td>iPhone 5 rev.2</td>
<td>A1429 - A1442</td>
<td>N42AP</td>
<td>iPhone5,2</td>
<td>2012</td>
<td>16, 32, 64</td>
</tr>
<tr>
<td>iPhone 5</td>
<td>A1428</td>
<td>N41AP</td>
<td>iPhone5,1</td>
<td>2012</td>
<td>16, 32, 64</td>
</tr>
<tr>
<td>iPhone 4s (China)</td>
<td>A1431</td>
<td>N94AP</td>
<td>iPhone4,1</td>
<td>2011</td>
<td>8, 16, 32, 64</td>
</tr>
<tr>
<td>iPhone 4S</td>
<td>A1387</td>
<td></td>
<td></td>
<td>2011</td>
<td>8, 16, 32, 64</td>
</tr>
<tr>
<td>iPhone 4 - CDMA</td>
<td>A1349</td>
<td>N92AP</td>
<td>iPhone3,2</td>
<td>2011</td>
<td>8, 16, 32</td>
</tr>
<tr>
<td>iPhone 4 - GSM</td>
<td>A1332</td>
<td>N90AP</td>
<td>iPhone3,1</td>
<td>2010</td>
<td>8, 16, 32</td>
</tr>
<tr>
<td>iPhone 3GS (China)</td>
<td>A1325</td>
<td>N88AP</td>
<td>iPhone2,1</td>
<td>2009</td>
<td>8, 16, 32</td>
</tr>
<tr>
<td>iPhone 3GS</td>
<td>A1303</td>
<td></td>
<td></td>
<td>2009</td>
<td>8, 16, 32</td>
</tr>
<tr>
<td>iPhone 3G (China)</td>
<td>A1324</td>
<td>N82AP</td>
<td>iPhone1,2</td>
<td>2009</td>
<td>8, 16</td>
</tr>
<tr>
<td>iPhone 3G</td>
<td>A1241</td>
<td></td>
<td></td>
<td>2008</td>
<td>8, 16</td>
</tr>
<tr>
<td>iPhone 2G</td>
<td>A1203</td>
<td>M68AP</td>
<td>iPhone1,1</td>
<td>2007</td>
<td>4, 8, 16</td>
</tr>
</tbody>
</table>
IDENTIFY THE MODEL

- The model number is located on the back of the device
IDENTIFY THE MODEL AND THE OPERATING SYSTEM

- **Tool:** ideviceinfo (libimobiledevice.org)
- It works *also if the device is locked by a passcode*

santoku@santoku:~$ ideviceinfo –s

- **DeviceClass:** iPhone
- **DeviceName:** EpiPhone
- **HardwareModel:** N94AP
- **ProductVersion:** 6.1.3
- **TelephonyCapability:** true
- **UniqueDeviceID:** 26ccdbcb74b2ab8e9e97aa096883a10442c6f2ef
- **WiFiAddress:** 84:fc:fe:d3:ac:e2
IS THE DEVICE LOCKED?

- Digits only
- Length = 4 (simple passcode)
IS THE DEVICE LOCKED?

- Digits only
- Length > 4 (simple passcode)
IS THE DEVICE LOCKED?

- Contains non digits
- Any length
PHYSICAL VS LOGICAL ACQUISITION

- Physical acquisition → Bit-by-bit image of the device
- Logical acquisition → Extract (part of) the file system
- What is NOT available in a logical acquisition?
  - Email
  - Geolocation database (Consolidated.db)
  - Apps “Cache” folder (es. Opened files in Dropbox)
  - Executables
PHYSICAL ACQUISITION

- If the device is an **iPhone 4** then we can perform a physical acquisition as long as:
  1. Device is not locked
  or
  2. Device is locked with a passcode that can be cracked within a “reasonable time”
- If the device is an **iPhone4s** or **iPhone5** we can perform a physical acquisition only if:
  1. The device is jailbroken (**mandatory!**) \(\Rightarrow\) Up to **iOS 6.1.2**
  2. The same conditions with the lock code
- If the device is **iPhone5s** or **iPhone5c**… no way at the moment!
HOW LONG DOES IT TAKE TO CRACK? (IPHONE 4)

<table>
<thead>
<tr>
<th></th>
<th>Length</th>
<th>Avg. Crack time</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Digits</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>20 minutes</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>35 hours</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>2 weeks</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>4.5 months</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>40 years</td>
</tr>
<tr>
<td><strong>lowercase letters &amp; spacebar</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>3 weeks</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>1.5 years</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>1000 years</td>
</tr>
<tr>
<td><strong>Mixed case letters &amp; spacebar</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>11 days</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>1.6 years</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>88 years</td>
</tr>
<tr>
<td>Tool Name</td>
<td>Type</td>
<td>Device Compatibility</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>UFED Cellebrite</td>
<td>Commercial</td>
<td>iPhone 4</td>
</tr>
<tr>
<td>AccessData MPE+</td>
<td>Commercial</td>
<td>iPhone 4</td>
</tr>
<tr>
<td>Katana Lantern</td>
<td>Commercial</td>
<td>iPhone 4</td>
</tr>
<tr>
<td>iXAM</td>
<td>Commercial</td>
<td>iPhone 4</td>
</tr>
<tr>
<td>XRY</td>
<td>Commercial</td>
<td>iPhone 4</td>
</tr>
<tr>
<td>Elcomsoft iOS Forensic Toolkit</td>
<td>Commercial</td>
<td>iPhone 4/4s/5</td>
</tr>
<tr>
<td>iPhone Data Protection Tools</td>
<td>Opensource</td>
<td>iPhone 4 (up to iOS 5)</td>
</tr>
</tbody>
</table>
Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 1.20/Win for A5+

(c) 2011-2013 Elcomsoft Co. Ltd.

Please select an action:
1 N/A
2 N/A
3 GET PASSCODE - Recover device passcode
4 GET KEYS - Extract device keys and keychain data
5 DECRYPT KEYCHAIN
6 IMAGE DISK - Acquire physical image of the device filesystem
7 DECRYPT DISK
8 TAR FILES - Acquire user’s files from the device as a tarball
9 REBOOT - Reboot the device
0 EXIT

>:
What can we do if we have iPhone 4S/5/5s/5c with iOS 7 and without lock code?

Logical acquisition (or simply a backup!)

**Forensic tools**
- Oxygen Forensics, UFED Cellebrite, AccessData MPE+, XRY, MobilEdit, etc.

**iTunes + Backup parser/analyster**
- iPhone Backup Analyzer 2 Opensource
- iBackupBot Commercial
- iPhone Backup Extractor Commercial
IPHONE BACKUP ANALYZER

- SMS / iMessage
- Call Logs
- Address Book
- Note
- Network
- Skype
- WhatsApp
- Viber
- Known WiFi
- Safari History
- Safari Bookmarks
- Safari State
- Thumbnails

 Decode and Explore iPhone backup

 XML Plist viewer

 Binary Plist viewer

 SQLITE Browser

 Hex viewer

 Text viewer

 Image and EXIF viewer
IPHONE BACKUP ANALYZER – MAIN WINDOW
IPHONE BACKUP ANALYZER – SQLITE AND PLIST
IPHONE BACKUP ANALYZER – CALLS AND MESSAGES
IPHONE BACKUP ANALYZER – WHATSAPP AND SKYPE
LOGICAL ACQUISITION AND BACKUP

- What can we do if we have:
  - iPhone 4s or iPhone 5 protected with a lock code and is not jailbroken
  - iPhone 5s/5c is protected with a lock code
- We need to answer another question:
  Do we have access to any PC the device was synced with?
  1. If not...we can not perform an acquisition!
  2. If yes...
     1. Is it a not password protected backup available in the PC? → We can analyze it!
     2. Is it a password protected backup available in the PC? → We can try to crack it!
     3. Are the lockdown certificates available? → We can access the device!!!
LOCKDOWN CERTIFICATES

- Stored in:
  - C:\Program Data\Apple\Lockdown
  - C:\Users\[username]\AppData\roaming\Apple Computer\Lockdown
  - C:\Documents and Settings\[username]\Application Data\Apple Computer\Lockdown
  - /private/var/db/lockdown
  - We can take the certificate and copy into another machine → We will then have access to the device!
An iPhone 4S was seized from Mattia Epifani, a very dangerous WiFi wardriver.
The iPhone is locked with a 4 digit passcode and isn’t jailbroken (iOS 6.1.3).
A personal computer was also seized in Mattia’s flat.
We are searching for:
- WiFi password stored on the device
- Personal email password
- SMS sent and received
- WhatsApp contacts and chats
Using iTunes we can make a **backup of an iOS device**

In order to perform the backup it is essential to find out whether:

- The phone is not protected by a lock code, or
- Do we know the lock code, or
- Can we obtain the synchronization certificates for the device from a trusted computer

The **keychain file** stores WiFi, e-mail and third-party applications passwords

If the backup is **not encrypted** → keychain file is encrypted using a key hard-coded into the device

If the backup is **password protected** → keychain file is **encrypted using the user-chosen password**
Researchers at the Russian software company Elcomsoft have analyzed the communication protocol between iDevice and Apple iCloud. They were able to emulate the correct commands to retrieve the contents of a user's iCloud storage.

The download operations are completely transparent to the device owner, so an attacker can monitor user activities every time a new backup is created online.
Download Backup from iCloud

Apple ID (example@example.com)

Password

Sign In
Download Backup from iCloud

Mattia Epifani
mattiaep@hotmail.it
1321763630

<table>
<thead>
<tr>
<th>Device Info</th>
<th>Updated</th>
<th>Download Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone 4 + 1</td>
<td>October 10, 2010 16:00</td>
<td>Not started</td>
</tr>
<tr>
<td>SN: DN: 392355DTCO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDID: 26ccbedb74b2a1baf89e7e036883a10442dc526f</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Backup Size: 3191.8 MB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Restore original file names
- Download only specific data

Download
<table>
<thead>
<tr>
<th>Model</th>
<th>Logical Acquisition</th>
<th>Physical Acquisition</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone 3G</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>iPhone 3Gs</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>iPhone 4</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>iPhone 4s</td>
<td>Yes</td>
<td>Only if jailbroken (iOS 6.1.2)</td>
</tr>
<tr>
<td>iPhone 5</td>
<td>Yes</td>
<td>Only if jailbroken (iOS 6.1.2)</td>
</tr>
<tr>
<td>iPhone 5s</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>iPhone 5c</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
## LOCKED IPHONE

<table>
<thead>
<tr>
<th>Model</th>
<th>Logical Acquisition</th>
<th>Physical Acquisition</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone 3G</td>
<td>Yes, with lockdown</td>
<td>Yes, if code is «easy» enough</td>
</tr>
<tr>
<td>iPhone 3Gs</td>
<td>Yes, with lockdown</td>
<td>Yes, if code is «easy» enough</td>
</tr>
<tr>
<td>iPhone 4</td>
<td>Yes, with lockdown</td>
<td>Yes, if code is «easy» enough</td>
</tr>
<tr>
<td>iPhone 4s</td>
<td>Yes, with lockdown</td>
<td>Only if jailbroken (iOS 6.1.2) and If code is «easy» enough</td>
</tr>
<tr>
<td>iPhone 5</td>
<td>Yes, with lockdown</td>
<td>Only if jailbroken (iOS 6.1.2) and If code is «easy» enough</td>
</tr>
<tr>
<td>iPhone 5s</td>
<td>Yes, with lockdown</td>
<td>No</td>
</tr>
<tr>
<td>iPhone 5c</td>
<td>Yes, with lockdown</td>
<td>No</td>
</tr>
</tbody>
</table>
• The iPhone Wiki
  http://theiphonewiki.com
• iOS Support Matrix
  http://iossupportmatrix.com/
• Elcomsoft iOS Forensic Toolkit
  http://www.elcomsoft.it/eift.html
• Elcomsoft Phone Password Breaker
  http://www.elcomsoft.it/eppb.html
• iPhone Backup Unlocker
• AccessData Mobile Phone Examiner Plus
  http://www.accessdata.com/mpe-ios-support/
• Cellebrite UFED Touch
  http://www.cellebrite.com/mobile-forensics/capabilities/ios-forensics
Mattia Epifani

- Digital Forensics Expert
- Owner @ REALITY NET – System Solutions
- President @ DFA Association
- GMOB, CEH, CHFI, CCE, CIFI, ECCE, AME, ACE, MPSC

Mail    mattia.epifani@realitynet.it
Twitter @mattiaep
Linkedin http://www.linkedin.com/in/mattiaepifani