

# *iPhone and 3G Technology*



(b)(6)



Homeland  
Security

Senior Instructor  
Technical Operations Division  
Federal Law Enforcement Training Center

# The Future Is Now

3G or Third Generation Technology has finally arrived

iPhone and AT&T was the first true 3G device with service

All major carriers have advertised true 3G device

Finally something to sink our teeth in!!!!



**Homeland  
Security**

# 3G Technology

## 2<sup>nd</sup> Generation

CDMA

SMS, MMS, EDGE, 1x-EVDO

GSM

SMS, MMS, GRPS

ETDMA

Same

iDEN

Same

No full use of Broadband

## 3<sup>rd</sup> Generation

IMT-2000

International Mobile  
Telecommunications 2000

UMTS

Universal Mobile  
Telecommunications System

CDMA2000

Code Division Multiple Access  
2000

HSPDA

High-Speed Packet Download  
Access



**Homeland  
Security**

# 3G Technology

Although the aforementioned 3G standards are different they all one thing in common – Structure

By its very nature the apps running in this environment need structure

They need defined architecture

No longer only carrier based file structures



**Homeland  
Security**

# iPhone Technology

iPhone uses core Apple OS X 10.5 (Leopard) as the core of its operating system – often called Core

iPhone 4, 8, & 16GB      iPhone 3G 8 & 16GB

iPhone uses GSM as its air interface technology

The iPhones' processor is ARM or advances RISC machine as opposed to Intel

Due to touch screen nature (GUI) the use of accelerometers and proximity sensors are require

Radios including GSM, Wi-Fi and Bluetooth systems exist



**Homeland  
Security**

# iPhone Technology

iPhone employs User Friendly Frameworks (dll) for proprietary hardware sensors multi touch systems

(b)(7)e

OpenSSH is also used because of ARM's Unix like architecture



**Homeland  
Security**

# iPhone Artifacts

Certain data streams are seen with the normal GUI interface

(b)(7)e



**Homeland  
Security**

# iPhone Artifacts

## Keyboard Cache

(b)(7)e

Several dozen may exist



**Homeland  
Security**



# iPhone Artifacts

(b)(7)e



**Homeland  
Security**

# iPhone Artifacts

(b)(7)e



**Homeland  
Security**

# System Needs

(b)(7)e



**Homeland  
Security**

# System Needs

What version do I have?

Look and see – Settings>General About

Won't I change or alter evidence?

The beauty of understanding and controlling iPhone forensics

Once we understand and control where we work we will do no harm



**Homeland  
Security**

# Device Layout

The iPhone uses flash technology, partition tables and a formatted *file system* to store information

1<sup>st</sup> Partition – root partition is used to storing all the system files and factory preloaded applications. Approximately 300 MB in size

2<sup>nd</sup> Partition – user or media partition is used to store everything else.

(b)(7)e



**Homeland  
Security**

# Device Layout

## Configuration

### Block Devices

/dev/disk0      Disk

/dev/disk0s1    Systems

/dev/disk0s2    Media

### Raw Devices

/dev/rdisk0     Disk

/dev/rdisk0s1   System

/dev/rdisk0s2   Media



**Homeland  
Security**

# Communication

What must we ensure before any examination with a mobile began?      Connection

The iPhone can establish connection in three formats

Serial Port - Through Docking Station (Apple File Conn./AFC)

802.11 Wi Fi – A Secure Broadcast

Bluetooth – A connection technology with limitations

iTunes is the key communications software used

(b)(7)e



**Homeland  
Security**

# Communication

iTunes is the key communications software used

(b)(7)e



**Homeland  
Security**



# iPhone Firmware

Firmware updates allow functionality

This will allow for use of update system services

Numerous locations available – use tested sites from [apple.com](http://apple.com)

(b)(7)e



**Homeland  
Security**

# iPhone Recovery Tools

(b)(7)e



**Homeland  
Security**



# Homeland Security