Fall 2014

IOS Device Forensics

Lauren Drish
Governors State University

IOS DEVICE FORENSICS

By

LAUREN DRISH
B.A., University of Illinois at Chicago, 2011

A GRADUATE PROJECT

Submitted in partial fulfillment of the requirements

For the Degree of Masters of Science
With a Major in Computer Science

GOVERNORS STATE UNIVERSITY
University Park, IL 60484

Fall 2014

Acknowledgements

I would like to acknowledge my Chairperson, Dr. Shih, and Committee members, Dr. Park and Professor Buenger, for helping me with this project. Thank you so much for all the help you offered and did for me.   I would also like to acknowledge Dan O’Day for all the help that he gave me in the beginning of my project. I am very, very thankful for all the help you gave me, as well as the information you provided.

Contents

Abstract

Many people today have an iPhone, iPad or iPod. Not many would realize that valuable information is stored on these devices. When a crime occurs, an iOS Device could hold key information to help solve said crime that criminals are not aware are present on the device. This can include GPS information as well as application history on the device itself.

The project I wish to do and complete is to create a class where students can learn the about iOS Forensics. Student will be able to learn the basics of an iDevice, as well as how to work with forensics tools to acquire the information in an efficient manner. The class will also introduce forensic tools that can be used with iOS Devices. These tools can include Open Source and Commercial forensic tools. This class will be offered to both Graduates and Undergraduates at Governors State University. It will act as a beginner's class, for individuals who want to learn more and have an interest in iOS Forensics.

Chapter 1 – Introduction

IOS devices are becoming a bigger part of everyday life. Many people in the world have an iPhone, iPod or iPad. These devices can hold a wealth of information. This information can include contacts, pictures, Short Message Service (SMS) messages and much more. Many users may believe that once something is deleted off the device, it is gone forever. Just like in computer forensics, deleting an item does not mean that it is gone from the device. The item can be retrieved from the device. This can be important for evidence that can be held on the device and can be used in investigations if the opportunity is provided.

Like any field in digital forensics, there are certain procedures and strategies that need to be known to extract the data in a safe and efficient manner. A person cannot just go into a computer and break their way into it to gain the information an investigator would need. This is the same for iOS devices. It is important for individuals to know the correct ways to access this data on the device.

This report will discuss the class that was created for Governors State University, which is called iOS Device Forensics. This class will give an introduction to iOS Forensics for individuals that are interested in this subject. For the book chosen for this class was Andrew Hoog and Katie Strzempka's book *iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad, and iOS Devices*. The following chapters in this report will express what will be covered in each section or chapter, as well as what was learned in each section.

Chapter 2 – Methods

The materials used to find the information for the class was primarily the apple development library[1], Andrew Hoog and Katie Strzempka's book *iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad, and iOS Devices* and information that was provided through discussion with Dan O'Day. Some informative websites were also found for additional information. All materials are included in the bibliography at the end of this report.

From the information that was provided or found, PowerPoint presentations were prepared for eleven weeks. These presentations then cover material that would be in that week's class. The students that participate in the class will also become familiar with the tool iPhone Analyzer, which can be found at crypticbit.com.

The class will also include a final project, will have students doing a hands on project. The students will be able use what they have learned to retrieve data from a device or backup. This project will take up the last three weeks in the semester. Once finished with the project, students will then be able to present their work for other classmates.

Undergraduate vs Graduate

It should be understood that there will be an undergraduate section and a graduate section for the class. The graduates that will be in this class will have to

[1] (Apple)

complete a paper as part of their grade. The paper has a few options that the student can choose from. One of these choices is the student will chose a tool in iOS device forensics to research on. They will give details on where the tool was found, what the tool is able to do and how the tool is unique. Another topic that the student may choose is to pick a feature on the new iOS 8 and explain the pros and cons for it. Students will explore the feature and give insight on how this feature could be of use in a digital forensics investigation.

Chapter 3 – Week One: Introduction to iOS Forensics

This is the first week of class for the students. This is the time that the students will be able to go over the syllabus and ask any questions that they would have. This week will also touch on why these devices are important. As stated before, these devices have the capability to store valuable information that could be of use in investigations.

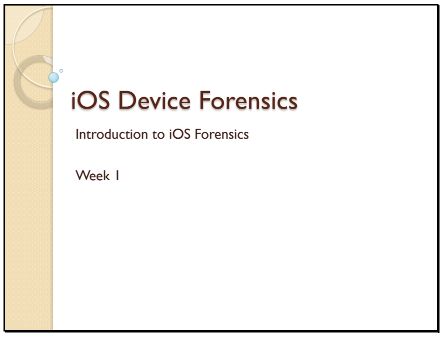
Students will also be able to learn about the different iOS versions that have been offered up to the point of today's current version of iOS, which is iOS 8. Students will also learn about the different models for iPods, iPads and iPhones. Forensic artifacts, which are known as something that would be of interest, are discussed along with the difference between Logical[2] and Physical[3] Acquisitions. The difference between technical analysis and 'Forensic' examination is.

[2] Copying the active file system from a device into another file.
[3] A physically bit-by-bit copy of the file system that is created.

A technical analysis is used to authenticate data through explanation of the technical features of the data. A ‘Forensic’ Examination attempts to understand the evidence that is found from the acquisition. In simpler terms, the analysis explains how to get the evidence whereas an examination determines whether or not a conclusion of guilty or not guilty.

PowerPoint Presentation for Week One

Slide 1

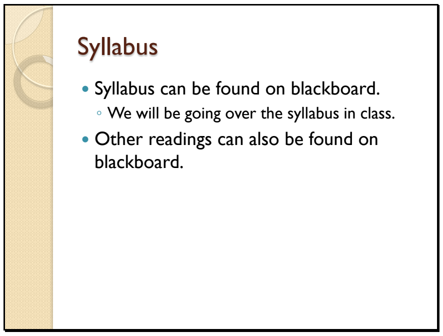


iOS Device Forensics

Introduction to iOS Forensics

Week 1

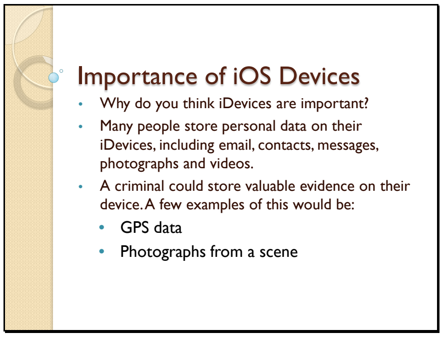
Slide 2



Syllabus

- Syllabus can be found on blackboard.
  - We will be going over the syllabus in class.
- Other readings can also be found on blackboard.

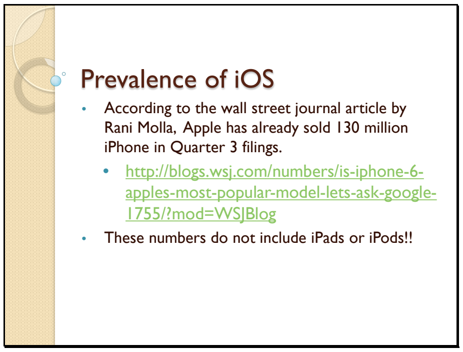
Slide 3



Importance of iOS Devices

- Why do you think iDevices are important?
- Many people store personal data on their iDevices, including email, contacts, messages, photographs and videos.
- A criminal could store valuable evidence on their device. A few examples of this would be:
  - GPS data
  - Photographs from a scene

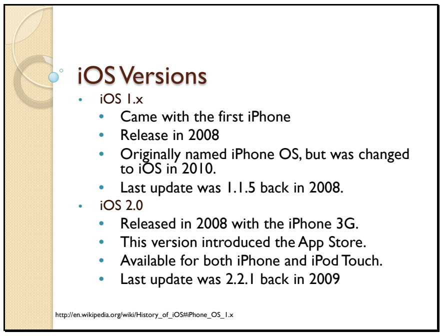
Slide 4



Prevalence of iOS

- According to the wall street journal article by Rani Molla, Apple has already sold 130 million iPhone in Quarter 3 filings.
  - http://blogs.wsj.com/numbers/is-iphone-6-apples-most-popular-model-lets-ask-google-1755/?mod=WSJBlog
- These numbers do not include iPads or iPods!!

Slide 5

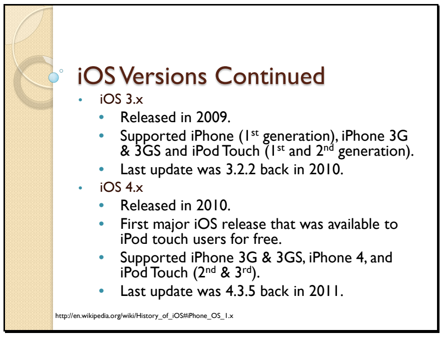


iOS Versions

- iOS 1.x
  - Came with the first iPhone
  - Release in 2008
  - Originally named iPhone OS, but was changed to iOS in 2010.
  - Last update was 1.1.5 back in 2008.
- iOS 2.0
  - Released in 2008 with the iPhone 3G.
  - This version introduced the App Store.
  - Available for both iPhone and iPod Touch.
  - Last update was 2.2.1 back in 2009

http://en.wikipedia.org/wiki/History_of_iOS#iPhone_OS_1.x

Slide 6

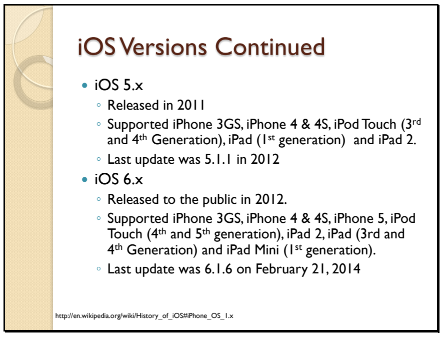


iOS Versions Continued

- iOS 3.x
  - Released in 2009.
  - Supported iPhone (1st generation), iPhone 3G & 3GS and iPod Touch (1st and 2nd generation).
  - Last update was 3.2.2 back in 2010.
- iOS 4.x
  - Released in 2010.
  - First major iOS release that was available to iPod touch users for free.
  - Supported iPhone 3G & 3GS, iPhone 4, and iPod Touch (2nd & 3rd).
  - Last update was 4.3.5 back in 2011.

http://en.wikipedia.org/wiki/History_of_iOS#iPhone_OS_1.x

Slide 7

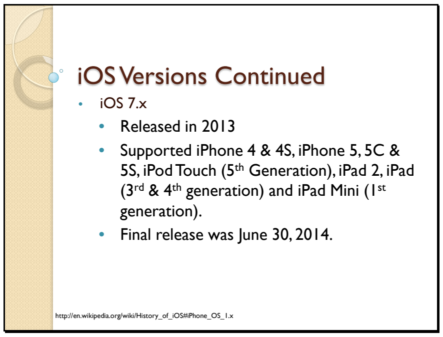


iOS Versions Continued

- iOS 5.x
  - Released in 2011
  - Supported iPhone 3GS, iPhone 4 & 4S, iPod Touch (3rd and 4th Generation), iPad (1st generation) and iPad 2.
  - Last update was 5.1.1 in 2012
- iOS 6.x
  - Released to the public in 2012.
  - Supported iPhone 3GS, iPhone 4 & 4S, iPhone 5, iPod Touch (4th and 5th generation), iPad 2, iPad (3rd and 4th Generation) and iPad Mini (1st generation).
  - Last update was 6.1.6 on February 21, 2014

http://en.wikipedia.org/wiki/History_of_iOS#iPhone_OS_1.x

Slide 8

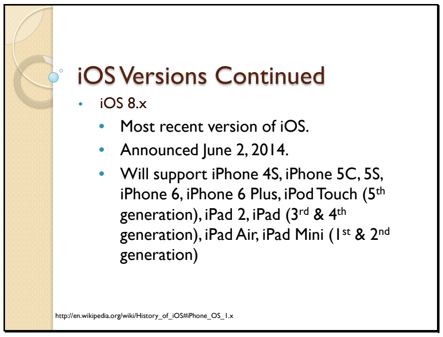


iOS Versions Continued

- iOS 7.x
  - Released in 2013
  - Supported iPhone 4 & 4S, iPhone 5, 5C & 5S, iPod Touch (5th Generation), iPad 2, iPad (3rd & 4th generation) and iPad Mini (1st generation).
  - Final release was June 30, 2014.

http://en.wikipedia.org/wiki/History_of_iOS#iPhone_OS_1.x

Slide 9

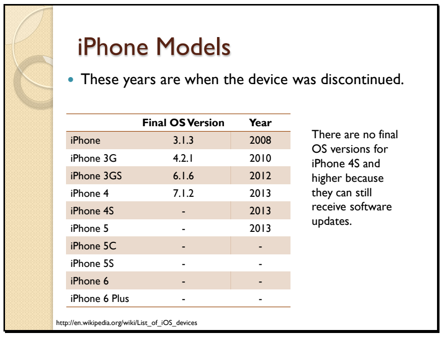


iOS Versions Continued

- iOS 8.x
  - Most recent version of iOS.
  - Announced June 2, 2014.
  - Will support iPhone 4S, iPhone 5C, 5S, iPhone 6, iPhone 6 Plus, iPod Touch (5th generation), iPad 2, iPad (3rd & 4th generation), iPad Air, iPad Mini (1st & 2nd generation)

http://en.wikipedia.org/wiki/History_of_iOS#iPhone_OS_1.x

Slide 10



iPhone Models

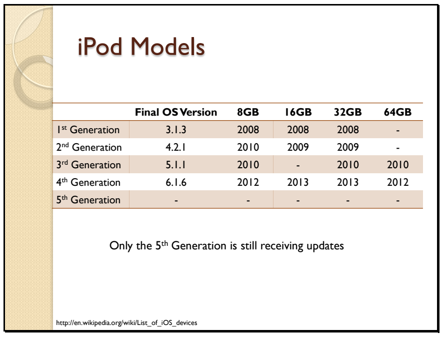
- These years are when the device was discontinued.

	Final OS Version	Year
iPhone	3.1.3	2008
iPhone 3G	4.2.1	2010
iPhone 3GS	6.1.6	2012
iPhone 4	7.1.2	2013
iPhone 4S	-	2013
iPhone 5	-	2013
iPhone 5C	-	-
iPhone 5S	-	-
iPhone 6	-	-
iPhone 6 Plus	-	-

There are no final OS versions for iPhone 4S and higher because they can still receive software updates.

http://en.wikipedia.org/wiki/List_of_iOS_devices

Slide 11



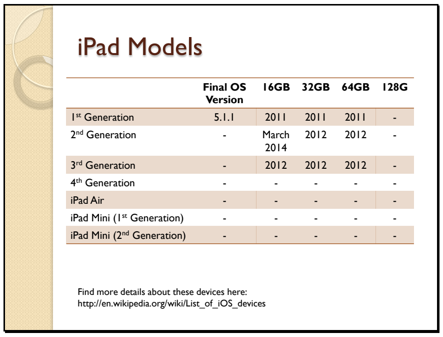
iPod Models

	Final OS Version	8GB	16GB	32GB	64GB
1st Generation	3.1.3	2008	2008	2008	-
2nd Generation	4.2.1	2010	2009	2009	-
3rd Generation	5.1.1	2010	-	2010	2010
4th Generation	6.1.6	2012	2013	2013	2012
5th Generation	-	-	-	-	-

Only the 5th Generation is still receiving updates

http://en.wikipedia.org/wiki/List_of_iOS_devices

Slide 12

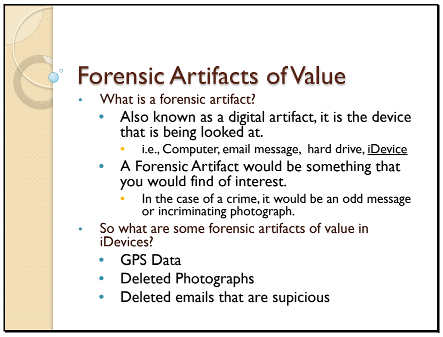


iPad Models

	Final OS Version	16GB	32GB	64GB	128G
1st Generation	5.1.1	2011	2011	2011	-
2nd Generation	-	March 2014	2012	2012	-
3rd Generation	-	2012	2012	2012	-
4th Generation	-	-	-	-	-
iPad Air	-	-	-	-	-
iPad Mini (1st Generation)	-	-	-	-	-
iPad Mini (2nd Generation)	-	-	-	-	-

Find more details about these devices here:
http://en.wikipedia.org/wiki/List_of_iOS_devices

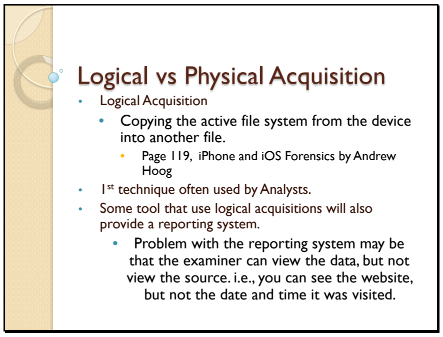
Slide 13



Forensic Artifacts of Value

- What is a forensic artifact?
  - Also known as a digital artifact, it is the device that is being looked at.
    - i.e., Computer, email message, hard drive, iDevice
  - A Forensic Artifact would be something that you would find of interest.
    - In the case of a crime, it would be an odd message or incriminating photograph.
- So what are some forensic artifacts of value in iDevices?
  - GPS Data
  - Deleted Photographs
  - Deleted emails that are supicious

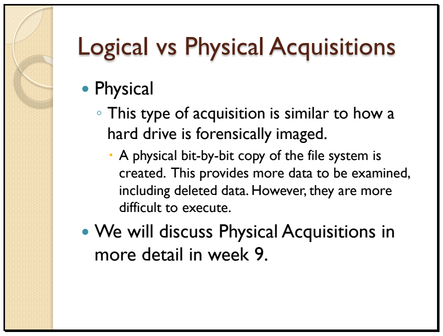
Slide 14



Logical vs Physical Acquisition

- Logical Acquisition
  - Copying the active file system from the device into another file.
    - Page 119, iPhone and iOS Forensics by Andrew Hoog
- 1st technique often used by Analysts.
- Some tool that use logical acquisitions will also provide a reporting system.
  - Problem with the reporting system may be that the examiner can view the data, but not view the source. i.e., you can see the website, but not the date and time it was visited.

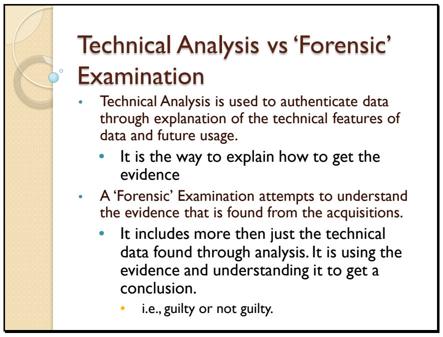
Slide 15



Logical vs Physical Acquisitions

- Physical
  - This type of acquisition is similar to how a hard drive is forensically imaged.
    - A physical bit-by-bit copy of the file system is created. This provides more data to be examined, including deleted data. However, they are more difficult to execute.
- We will discuss Physical Acquisitions in more detail in week 9.

Slide 16



Technical Analysis vs 'Forensic' Examination

- Technical Analysis is used to authenticate data through explanation of the technical features of data and future usage.
  - It is the way to explain how to get the evidence
- A 'Forensic' Examination attempts to understand the evidence that is found from the acquisitions.
  - It includes more then just the technical data found through analysis. It is using the evidence and understanding it to get a conclusion.
    - i.e., guilty or not guilty.

Chapter 4 – Week Two: iDevice Hardware

In week two, students will become familiar with the hardware in an iDevice. Most iPods, iPhones and iPads have a solid state drive. This drive is called a NAND flash. What this drive does is it uses memory to store the data, rather than having an actual drive in the device. The hardware section also includes file systems that are stored on the device. Most iDevices will use a HFS+ type file system. This is important to know because this is where the data can be contained.

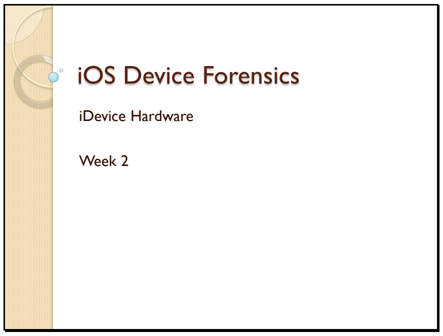
There is a folder[4] within the file system that is discussed that allows the user to see the folders containing Application, Library and Media. The Application folder contains the applications that are stored on the device. The media folder contains all the pictures, videos and other media type data on the device. The library may have the most useful data. This folder contains the address book, calendar, favorites, mail, and messages.

[4] /private/var2/mobile

Students will learn about the disk partitioning scheme of an iDevice in this week as well. The device has two partitions. The first partition contains the firmware, where the second partition contains the data. Encryption is discussed, from version iOS 3 to iOS 8. Students will also learn about the operating modes. The modes include Normal, Recovery and DFU. The presentation slides also give students insight on how to access these modes. The presentation concludes with telling students what the difference between a soft reset, which doesn't lose data, and a hard reset, which resets the entire device.

PowerPoint Presentation for Week Two

Slide 1

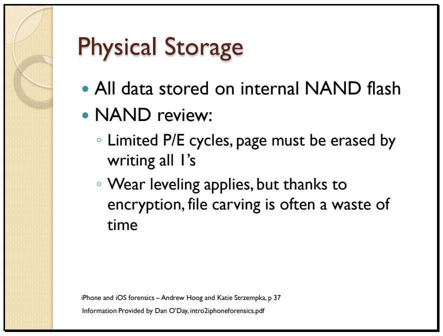


iOS Device Forensics

iDevice Hardware

Week 2

Slide 2

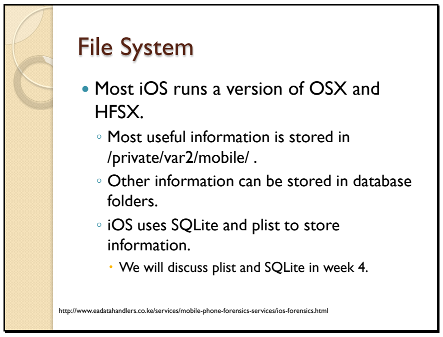


Physical Storage

- All data stored on internal NAND flash
- NAND review:
  - Limited P/E cycles, page must be erased by writing all 1's
  - Wear leveling applies, but thanks to encryption, file carving is often a waste of time

iPhone and iOS forensics – Andrew Hoog and Katie Strzempka, p 37
Information Provided by Dan O'Day, intro2iphoneforensics.pdf

Slide 3

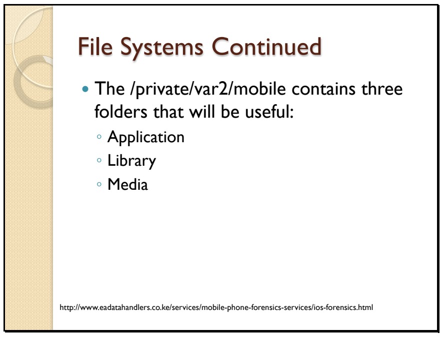


File System

- Most iOS runs a version of OSX and HFSX.
  - Most useful information is stored in /private/var2/mobile/ .
  - Other information can be stored in database folders.
  - iOS uses SQLite and plist to store information.
    - We will discuss plist and SQLite in week 4.

http://www.eadatahandlers.co.ke/services/mobile-phone-forensics-services/ios-forensics.html

Slide 4

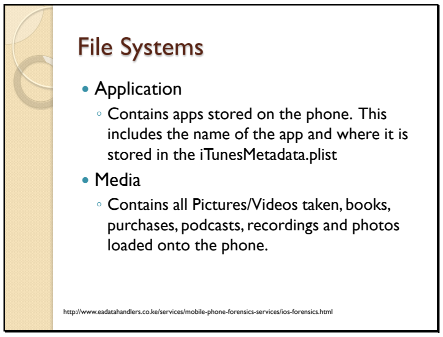


File Systems Continued

- The /private/var2/mobile contains three folders that will be useful:
  - Application
  - Library
  - Media

http://www.eadatahandlers.co.ke/services/mobile-phone-forensics-services/ios-forensics.html

Slide 5

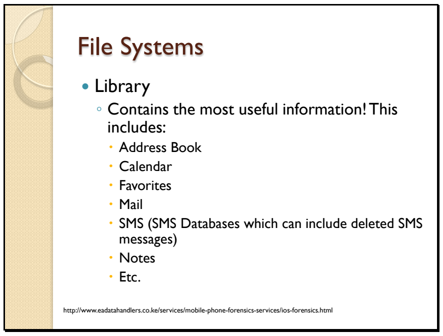


File Systems

- Application
  - Contains apps stored on the phone. This includes the name of the app and where it is stored in the iTunesMetadata.plist
- Media
  - Contains all Pictures/Videos taken, books, purchases, podcasts, recordings and photos loaded onto the phone.

http://www.eadatahandlers.co.ke/services/mobile-phone-forensics-services/ios-forensics.html

Slide 6

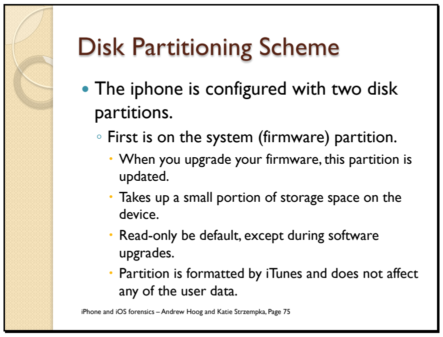


File Systems

- Library
  - Contains the most useful information! This includes:
    - Address Book
    - Calendar
    - Favorites
    - Mail
    - SMS (SMS Databases which can include deleted SMS messages)
    - Notes
    - Etc.

http://www.eadatahandlers.co.ke/services/mobile-phone-forensics-services/ios-forensics.html

Slide 7

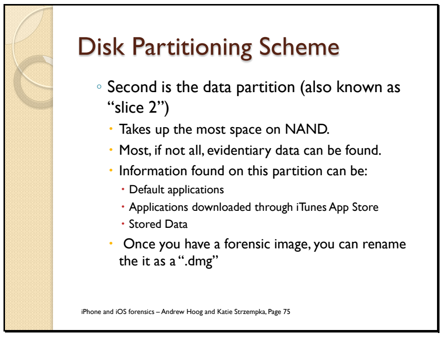


Disk Partitioning Scheme

- The iphone is configured with two disk partitions.
  - First is on the system (firmware) partition.
    - When you upgrade your firmware, this partition is updated.
    - Takes up a small portion of storage space on the device.
    - Read-only be default, except during software upgrades.
    - Partition is formatted by iTunes and does not affect any of the user data.

iPhone and iOS forensics – Andrew Hoog and Katie Strzempka, Page 75

Slide 8

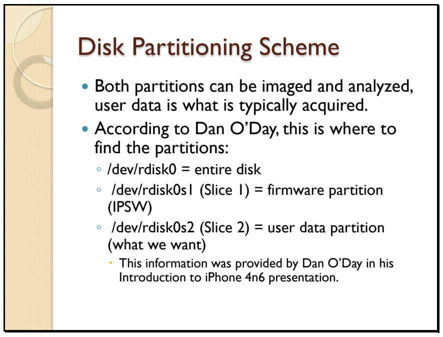


Disk Partitioning Scheme

  - Second is the data partition (also known as "slice 2")
    - Takes up the most space on NAND.
    - Most, if not all, evidentiary data can be found.
    - Information found on this partition can be:
      - Default applications
      - Applications downloaded through iTunes App Store
      - Stored Data
    - Once you have a forensic image, you can rename the it as a ".dmg"

iPhone and iOS forensics – Andrew Hoog and Katie Strzempka, Page 75

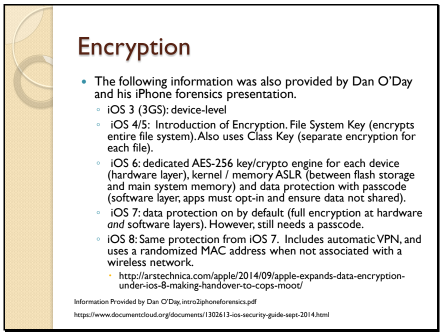
Slide 9



Disk Partitioning Scheme

- Both partitions can be imaged and analyzed, user data is what is typically acquired.
- According to Dan O'Day, this is where to find the partitions:
  - /dev/rdisk0 = entire disk
  - /dev/rdisk0s1 (Slice 1) = firmware partition (IPSW)
  - /dev/rdisk0s2 (Slice 2) = user data partition (what we want)
    - This information was provided by Dan O'Day in his Introduction to iPhone 4n6 presentation.

Slide 10



Encryption

- The following information was also provided by Dan O'Day and his iPhone forensics presentation.
  - iOS 3 (3GS): device-level
  - iOS 4/5: Introduction of Encryption. File System Key (encrypts entire file system). Also uses Class Key (separate encryption for each file).
  - iOS 6: dedicated AES-256 key/crypto engine for each device (hardware layer), kernel / memory ASLR (between flash storage and main system memory) and data protection with passcode (software layer, apps must opt-in and ensure data not shared).
  - iOS 7: data protection on by default (full encryption at hardware *and* software layers). However, still needs a passcode.
  - iOS 8: Same protection from iOS 7. Includes automatic VPN, and uses a randomized MAC address when not associated with a wireless network.
    - http://arstechnica.com/apple/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/

Information Provided by Dan O'Day, intro2iphoneforensics.pdf

https://www.documentcloud.org/documents/1302613-ios-security-guide-sept-2014.html

Slide 11

Encryption

- Good News though!
- File system is mostly unlocked once device is booted up
- Baseline encryption is NOT tied to passcode/PIN
- Data protection is, however - but only if passcode/PIN enabled!
- According to arstechnica.com, with iOS 8, even with a warrant, Apple is unable to gain entry into the device. It is protected by the user's passcode.
  - Need the passcode to get the information.

Information Provided by Dan O'Day, intro2iphoneforensics.pdf
http://arstechnica.com/apple/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/

Slide 12

Operating Modes

- Normal Mode
  - Every day use of the device
- Recovery and DFU
  - To perform certain functions, must place device in device failsafe utility (DFU) or recovery mode
  - Bypasses loading of OS
  - DFU mode = black screen
  - Recovery mode

Some of the Information was provided by Dan O'Day, intro2iphoneforensics.pdf
iPhone and iOS Forensics – Andrew Hoog and Katie Strzempka, Page 37

Slide 13

Operating Modes

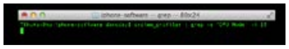
- Recovery mode
  - Power off device
  - Hold down Home button and plug in while holding

Some of this information was Provided by Dan O'Day, intro2iphoneforensics.pdf
iPhone and iOS Forensics – Andrew Hoog and Katie Strzempka, Page 37

Slide 14

Operating Modes

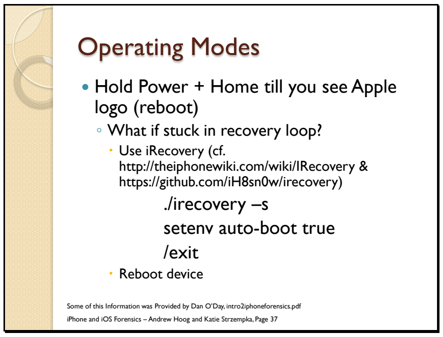
- How to verify your in DFU mode:
  - DFU mode = black screen
  - Connect device and ensure powered off
  - Hold down Power + Home for about 10 seconds
  - Release Power, but continue holding Home for about 10 more seconds
  - Release Home button (screen should now be black)
  - Mac Terminal command:



```
[illegible]
```

Some of this information was Provided by Dan O'Day, intro2iphoneforensics.pdf
iPhone and iOS Forensics – Andrew Hoog and Katie Strzempka, Page 37

Slide 15



Operating Modes

- Hold Power + Home till you see Apple logo (reboot)
  - What if stuck in recovery loop?
    - Use iRecovery (cf. http://theiphonewiki.com/wiki/IRecovery & https://github.com/iH8sn0w/irecovery)

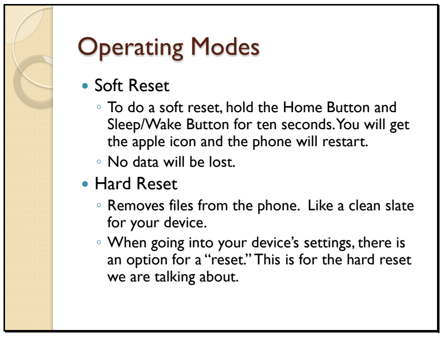
```
./irecovery –s
setenv auto-boot true
/exit
```

    - Reboot device

Some of this Information was Provided by Dan O'Day, intro2iphoneforensics.pdf

iPhone and iOS Forensics – Andrew Hoog and Katie Strzempka, Page 37

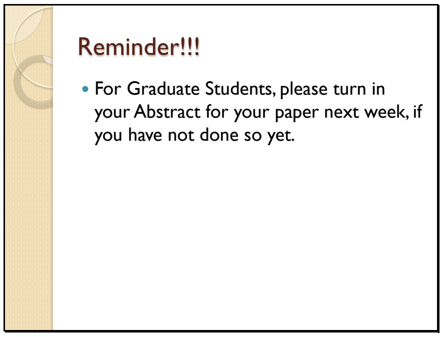
Slide 16



Operating Modes

- Soft Reset
  - To do a soft reset, hold the Home Button and Sleep/Wake Button for ten seconds. You will get the apple icon and the phone will restart.
  - No data will be lost.
- Hard Reset
  - Removes files from the phone. Like a clean slate for your device.
  - When going into your device's settings, there is an option for a "reset." This is for the hard reset we are talking about.

Slide 17



Reminder!!!

- For Graduate Students, please turn in your Abstract for your paper next week, if you have not done so yet.

Chapter 5 – Week Three: iOS Operating System

This presentation will go into iOS 7 and iOS 8. These two operating systems are the most used, with iOS 7 quickly being replaced with iOS 8. The operating system for an iOS device has four main layers: the Core OS, Core Services, Media and Cocoa Touch.

The Core OS contains low-level features. These features can include networking and Memory management. Along with these features, the framework and keychain services are found in this layer of the OS.[5] Keychain services work with certificates on the device.

Core Services are responsible for holding the technologies to support certain features. A few of these features include Location, iCloud, Social Media and Networking. As in the Core OS, Keychain Services are also implemented in this layer. To put simply, Keychain services allow data storage and protection within the keychain database that is on the device.[6] The Media layer[7] of the device holds the graphics, audio and video technologies for the device. This is good to know in a forensics setting. That is because some evidence that can be found on an iOS device can be video, picture, audio or a combination of one or more of these areas.

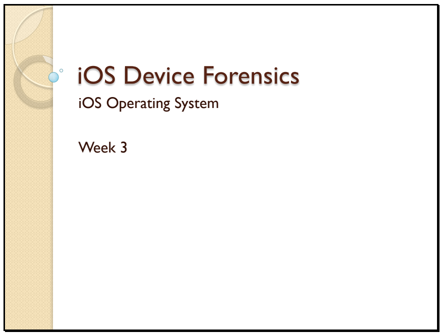
The last layer is the Cocoa Touch[8]. This layer contains the infrastructure for how the device looks. This can also include information on multitasking, push notifications and touch-based input for the device. What is meant by touch-based input is the device recognizing when a user touches the screen on the iDevice. The framework for the user's Address Book can also be found on this layer.

[5] (Apple, 2014)
[6] (Apple, 2014)
[7] (Apple, 2014)
[8] (Apple, 2014)

The presentation slides for this week touch on the differences between iOS 8 and iOS 7. IOS 8 has more capabilities in photo editing and notifications are also easier to manage. IOS 8 also has some new features, which include HealthKit and the new Apple Pay system. The week concludes with a glimpse into Third Party Applications. Third Party Applications are applications that are not apple approved. The two locations were applications can be stored, /var/mobile/Application and var/stash/Application, are shown to the students. A device normally has to be jailbroken (which will be discussed in week 8) in order for these types of applications to be installed.

PowerPoint Presentation for Week Three

Slide 1

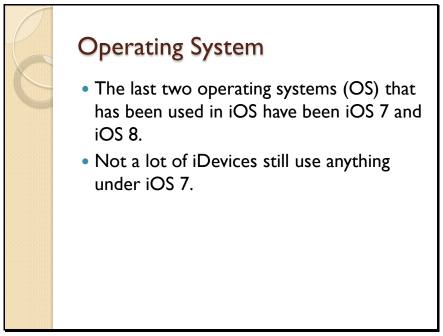


iOS Device Forensics

iOS Operating System

Week 3

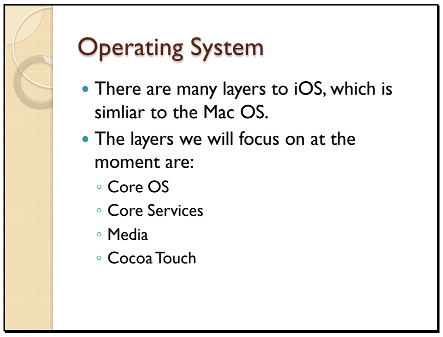
Slide 2



Operating System

- The last two operating systems (OS) that has been used in iOS have been iOS 7 and iOS 8.
- Not a lot of iDevices still use anything under iOS 7.

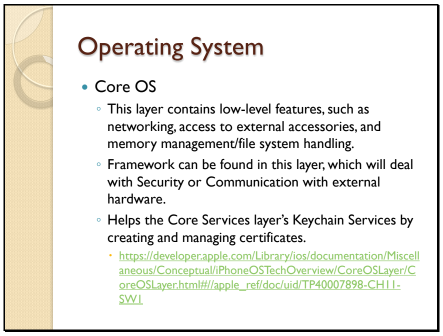
Slide 3



Operating System

- There are many layers to iOS, which is simliar to the Mac OS.
- The layers we will focus on at the moment are:
  - Core OS
  - Core Services
  - Media
  - Cocoa Touch

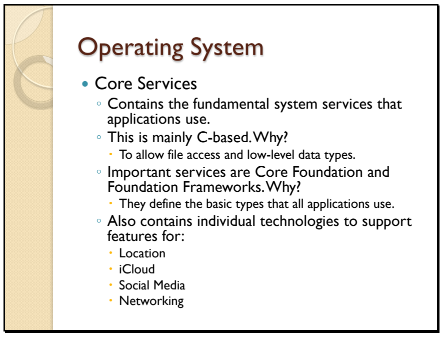
Slide 4



Operating System

- Core OS
  - This layer contains low-level features, such as networking, access to external accessories, and memory management/file system handling.
  - Framework can be found in this layer, which will deal with Security or Communication with external hardware.
  - Helps the Core Services layer's Keychain Services by creating and managing certificates.
    - https://developer.apple.com/Library/ios/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/CoreOSLayer/CoreOSLayer.html#//apple_ref/doc/uid/TP40007898-CH11-SW1

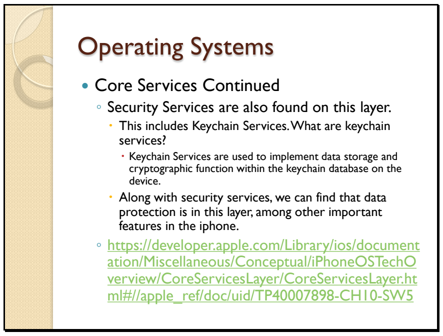
Slide 5



Operating System

- Core Services
  - Contains the fundamental system services that applications use.
  - This is mainly C-based. Why?
    - To allow file access and low-level data types.
  - Important services are Core Foundation and Foundation Frameworks. Why?
    - They define the basic types that all applications use.
  - Also contains individual technologies to support features for:
    - Location
    - iCloud
    - Social Media
    - Networking

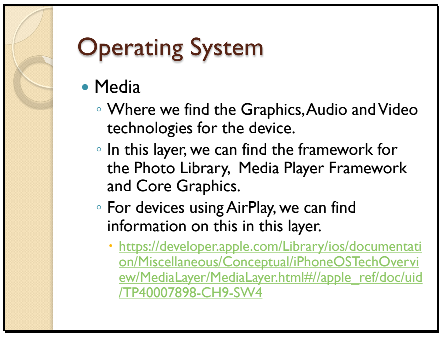
Slide 6



Operating Systems

- Core Services Continued
  - Security Services are also found on this layer.
    - This includes Keychain Services. What are keychain services?
      - Keychain Services are used to implement data storage and cryptographic function within the keychain database on the device.
    - Along with security services, we can find that data protection is in this layer, among other important features in the iphone.
  - https://developer.apple.com/Library/ios/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/CoreServicesLayer/CoreServicesLayer.html#//apple_ref/doc/uid/TP40007898-CH10-SW5

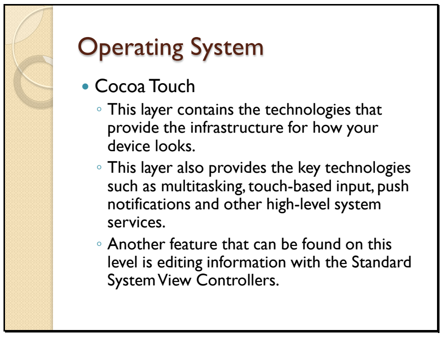
Slide 7



Operating System

- Media
  - Where we find the Graphics, Audio and Video technologies for the device.
  - In this layer, we can find the framework for the Photo Library, Media Player Framework and Core Graphics.
  - For devices using AirPlay, we can find information on this in this layer.
    - https://developer.apple.com/Library/ios/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/MediaLayer/MediaLayer.html#//apple_ref/doc/uid/TP40007898-CH9-SW4

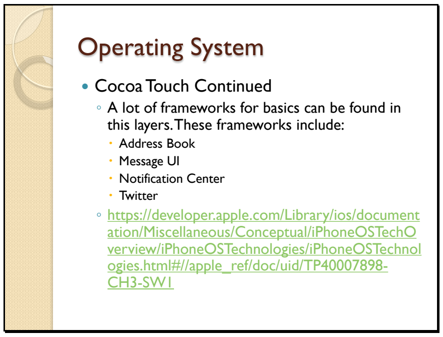
Slide 8



Operating System

- Cocoa Touch
  - This layer contains the technologies that provide the infrastructure for how your device looks.
  - This layer also provides the key technologies such as multitasking, touch-based input, push notifications and other high-level system services.
  - Another feature that can be found on this level is editing information with the Standard System View Controllers.

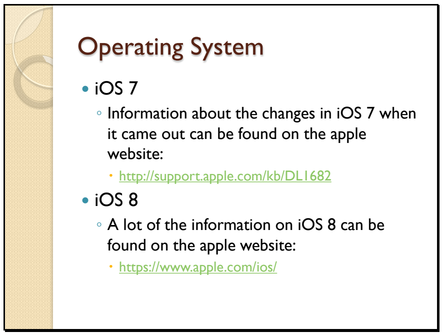
Slide 9



Operating System

- Cocoa Touch Continued
  - A lot of frameworks for basics can be found in this layers. These frameworks include:
    - Address Book
    - Message UI
    - Notification Center
    - Twitter
  - https://developer.apple.com/Library/ios/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/iPhoneOSTechnologies/iPhoneOSTechnologies.html#//apple_ref/doc/uid/TP40007898-CH3-SW1

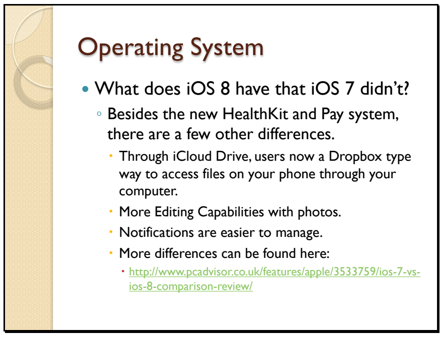
Slide 10



Operating System

- iOS 7
  - Information about the changes in iOS 7 when it came out can be found on the apple website:
    - http://support.apple.com/kb/DL1682
- iOS 8
  - A lot of the information on iOS 8 can be found on the apple website:
    - https://www.apple.com/ios/

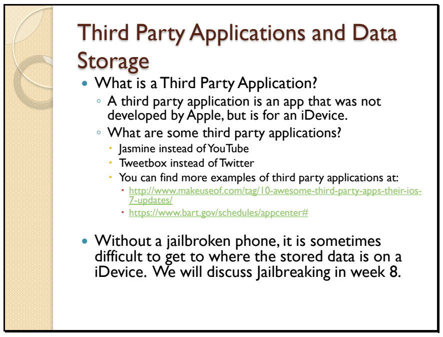
Slide 11



Operating System

- What does iOS 8 have that iOS 7 didn't?
  - Besides the new HealthKit and Pay system, there are a few other differences.
    - Through iCloud Drive, users now a Dropbox type way to access files on your phone through your computer.
    - More Editing Capabilities with photos.
    - Notifications are easier to manage.
    - More differences can be found here:
      - http://www.pcadvisor.co.uk/features/apple/3533759/ios-7-vs-ios-8-comparison-review/

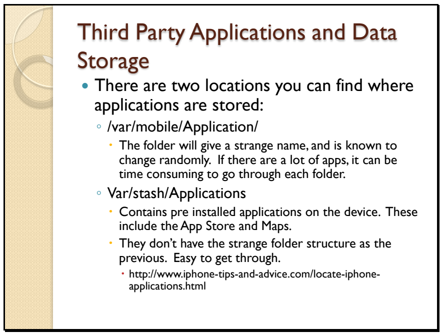
Slide 12



Third Party Applications and Data Storage

- What is a Third Party Application?
  - A third party application is an app that was not developed by Apple, but is for an iDevice.
  - What are some third party applications?
    - Jasmine instead of YouTube
    - Tweetbox instead of Twitter
    - You can find more examples of third party applications at:
      - http://www.makeuseof.com/tag/10-awesome-third-party-apps-their-ios-7-updates/
      - https://www.bart.gov/schedules/appcenter#
- Without a jailbroken phone, it is sometimes difficult to get to where the stored data is on a iDevice. We will discuss Jailbreaking in week 8.

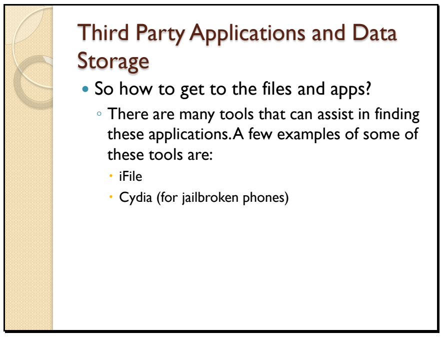
Slide 13



Third Party Applications and Data Storage

- There are two locations you can find where applications are stored:
  - /var/mobile/Application/
    - The folder will give a strange name, and is known to change randomly. If there are a lot of apps, it can be time consuming to go through each folder.
  - Var/stash/Applications
    - Contains pre installed applications on the device. These include the App Store and Maps.
    - They don't have the strange folder structure as the previous. Easy to get through.
      - http://www.iphone-tips-and-advice.com/locate-iphone-applications.html

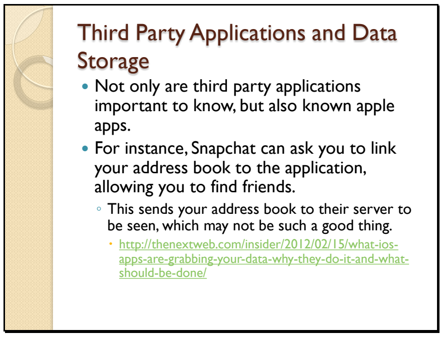
Slide 14



Third Party Applications and Data Storage

- So how to get to the files and apps?
  - There are many tools that can assist in finding these applications.A few examples of some of these tools are:
    - iFile
    - Cydia (for jailbroken phones)

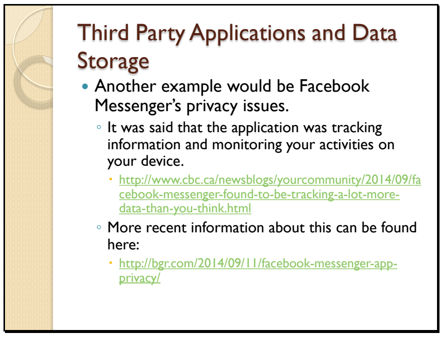
Slide 15



Third Party Applications and Data Storage

- Not only are third party applications important to know, but also known apple apps.
- For instance, Snapchat can ask you to link your address book to the application, allowing you to find friends.
  - This sends your address book to their server to be seen, which may not be such a good thing.
    - http://thenextweb.com/insider/2012/02/15/what-ios-apps-are-grabbing-your-data-why-they-do-it-and-what-should-be-done/

Slide 16



Third Party Applications and Data Storage

- Another example would be Facebook Messenger's privacy issues.
  - It was said that the application was tracking information and monitoring your activities on your device.
    - http://www.cbc.ca/newsblogs/yourcommunity/2014/09/facebook-messenger-found-to-be-tracking-a-lot-more-data-than-you-think.html
  - More recent information about this can be found here:
    - http://bgr.com/2014/09/11/facebook-messenger-app-privacy/

Chapter 6 – Week Four and Week Five

Weeks four and five both deal heavily in SQLite, which is a version of Structured Query Language (SQL). SQL will be discussed in more detail within week four's summary.

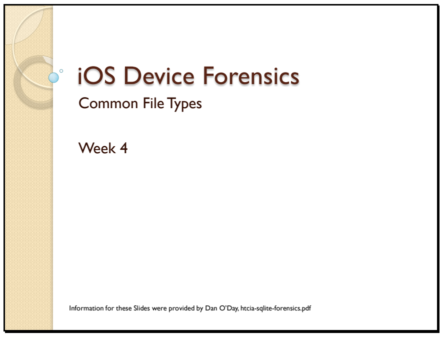
Week Four: Common File Types

Week four begins with an explanation of Property Lists (plist) and Binary Property Lists (bplist). A property list, or plist, are data representations used to store, organize and access various data types on the device, according to the apple developer library. A Binary Property List, or bplist, is similar to plist. The file size is condensed by storing certain files in binary. This allowed the application to run more efficiently. The data that can be found in plists are strings, number, binary data and dates. To traverse this data, it is good to know SQLite[9], seeing as this is a well-known database that iOS devices tend to use. SQL is known to be a relational database management engine and, according to sqlite.org, is the most widely deployed database engine.

A relational database means that it contains tables. These tables then have a Primary Key, which is a unique identifier for a record. These tables also have a Foreign Key, which shows a relationship between records on different tables. This is the basic structure for this type of database. The tables then have different types of data that can be stored. These data can be identified as NULL, Integer[10], Real[11], Text[12] or BLOB[13]. The lecture continues to give students examples of how to do queries in SQLite with a table. One-To-One relationships and One-To-Many relationships are explained in this week's lecture as well, along with examples. An example for a JOIN, which joins the two tables to gain a result, is given to students to help understand how it works.

PowerPoint Presentation for Week Four

Slide 1



iOS Device Forensics

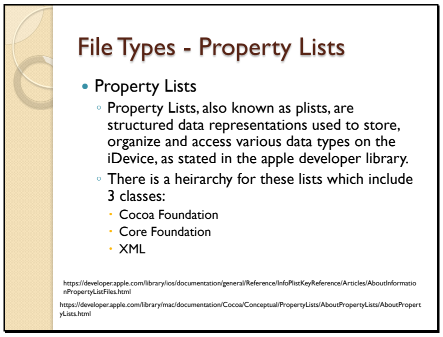
Common File Types

Week 4

Information for these Slides were provided by Dan O'Day, htcia-sqlite-forensics.pdf

[9] A part of SQL
[10] Signed integer, 1-8 bytes
[11] Floating point value, 8-Byte IEEE
[12] Text string, encoded UTF-8 or 16
[13] Binary large object

Slide 2



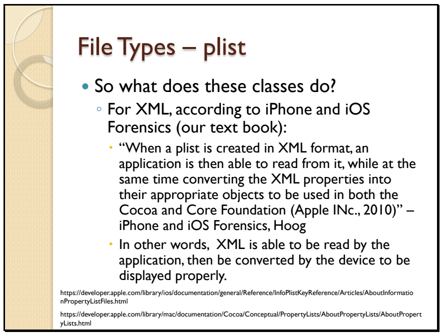
File Types - Property Lists

- Property Lists
  - Property Lists, also known as plists, are structured data representations used to store, organize and access various data types on the iDevice, as stated in the apple developer library.
  - There is a heirarchy for these lists which include 3 classes:
    - Cocoa Foundation
    - Core Foundation
    - XML

https://developer.apple.com/library/ios/documentation/general/Reference/InfoPlistKeyReference/Articles/AboutInformationPropertyListFiles.html

https://developer.apple.com/library/mac/documentation/Cocoa/Conceptual/PropertyLists/AboutPropertyLists/AboutPropertyLists.html

Slide 3



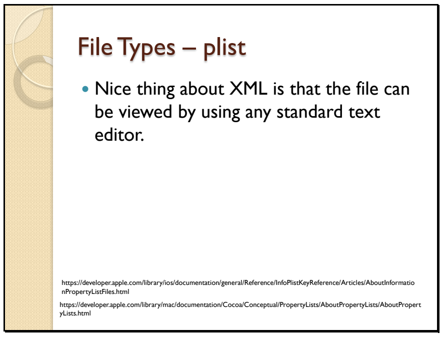
File Types – plist

- So what does these classes do?
  - For XML, according to iPhone and iOS Forensics (our text book):
    - "When a plist is created in XML format, an application is then able to read from it, while at the same time converting the XML properties into their appropriate objects to be used in both the Cocoa and Core Foundation (Apple INc., 2010)" – iPhone and iOS Forensics, Hoog
    - In other words, XML is able to be read by the application, then be converted by the device to be displayed properly.

https://developer.apple.com/library/ios/documentation/general/Reference/InfoPlistKeyReference/Articles/AboutInformationPropertyListFiles.html

https://developer.apple.com/library/mac/documentation/Cocoa/Conceptual/PropertyLists/AboutPropertyLists/AboutPropertyLists.html

Slide 4



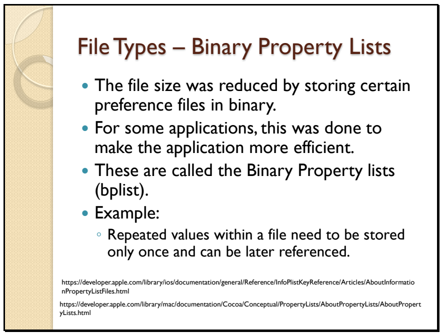
File Types – plist

- Nice thing about XML is that the file can be viewed by using any standard text editor.

https://developer.apple.com/library/ios/documentation/general/Reference/InfoPlistKeyReference/Articles/AboutInformationPropertyListFiles.html

https://developer.apple.com/library/mac/documentation/Cocoa/Conceptual/PropertyLists/AboutPropertyLists/AboutPropertyLists.html

Slide 5



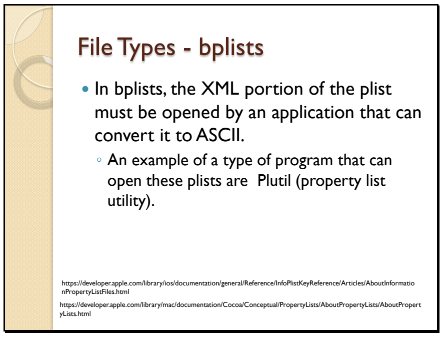
File Types – Binary Property Lists

- The file size was reduced by storing certain preference files in binary.
- For some applications, this was done to make the application more efficient.
- These are called the Binary Property lists (bplist).
- Example:
  - Repeated values within a file need to be stored only once and can be later referenced.

https://developer.apple.com/library/ios/documentation/general/Reference/InfoPlistKeyReference/Articles/AboutInformationPropertyListFiles.html

https://developer.apple.com/library/mac/documentation/Cocoa/Conceptual/PropertyLists/AboutPropertyLists/AboutPropertyLists.html

Slide 6



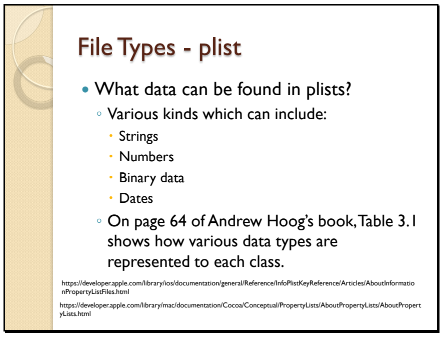
File Types - bplists

- In bplists, the XML portion of the plist must be opened by an application that can convert it to ASCII.
  - An example of a type of program that can open these plists are Plutil (property list utility).

https://developer.apple.com/library/ios/documentation/general/Reference/InfoPlistKeyReference/Articles/AboutInformationPropertyListFiles.html

https://developer.apple.com/library/mac/documentation/Cocoa/Conceptual/PropertyLists/AboutPropertyLists/AboutPropertyLists.html

Slide 7



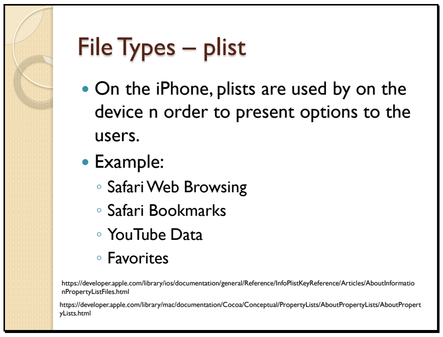
File Types - plist

- What data can be found in plists?
  - Various kinds which can include:
    - Strings
    - Numbers
    - Binary data
    - Dates
  - On page 64 of Andrew Hoog's book, Table 3.1 shows how various data types are represented to each class.

https://developer.apple.com/library/ios/documentation/general/Reference/InfoPlistKeyReference/Articles/AboutInformationPropertyListFiles.html

https://developer.apple.com/library/mac/documentation/Cocoa/Conceptual/PropertyLists/AboutPropertyLists/AboutPropertyLists.html

Slide 8



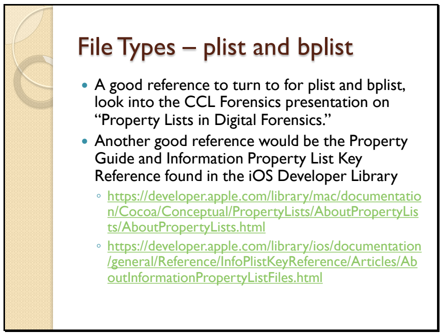
File Types – plist

- On the iPhone, plists are used by on the device n order to present options to the users.
- Example:
  - Safari Web Browsing
  - Safari Bookmarks
  - YouTube Data
  - Favorites

https://developer.apple.com/library/ios/documentation/general/Reference/InfoPlistKeyReference/Articles/AboutInformationPropertyListFiles.html

https://developer.apple.com/library/mac/documentation/Cocoa/Conceptual/PropertyLists/AboutPropertyLists/AboutPropertyLists.html

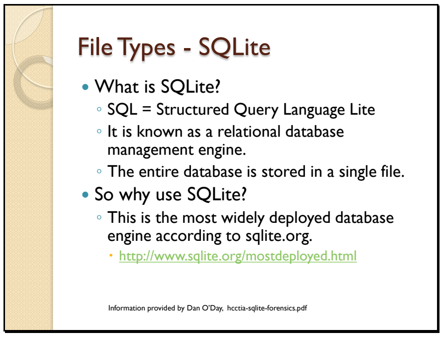
Slide 9



File Types – plist and bplist

- A good reference to turn to for plist and bplist, look into the CCL Forensics presentation on "Property Lists in Digital Forensics."
- Another good reference would be the Property Guide and Information Property List Key Reference found in the iOS Developer Library
  - https://developer.apple.com/library/mac/documentation/Cocoa/Conceptual/PropertyLists/AboutPropertyLists/AboutPropertyLists.html
  - https://developer.apple.com/library/ios/documentation/general/Reference/InfoPlistKeyReference/Articles/AboutInformationPropertyListFiles.html

Slide 10

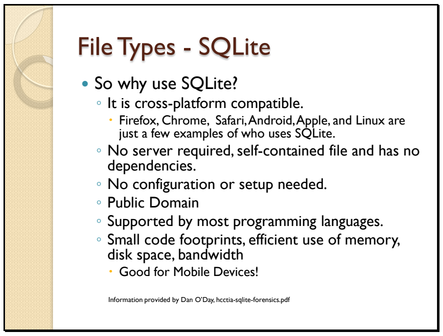


File Types - SQLite

- What is SQLite?
  - SQL = Structured Query Language Lite
  - It is known as a relational database management engine.
  - The entire database is stored in a single file.
- So why use SQLite?
  - This is the most widely deployed database engine according to sqlite.org.
    - http://www.sqlite.org/mostdeployed.html

Information provided by Dan O'Day, hcctia-sqlite-forensics.pdf

Slide 11

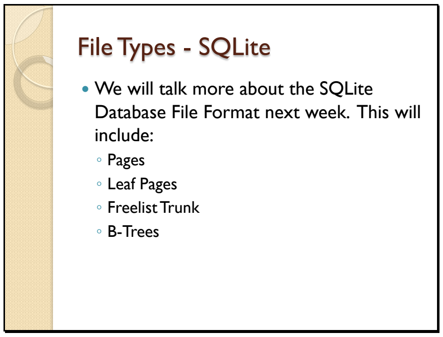


File Types - SQLite

- So why use SQLite?
  - It is cross-platform compatible.
    - Firefox, Chrome, Safari, Android, Apple, and Linux are just a few examples of who uses SQLite.
  - No server required, self-contained file and has no dependencies.
  - No configuration or setup needed.
  - Public Domain
  - Supported by most programming languages.
  - Small code footprints, efficient use of memory, disk space, bandwidth
    - Good for Mobile Devices!

Information provided by Dan O'Day, hcctia-sqlite-forensics.pdf

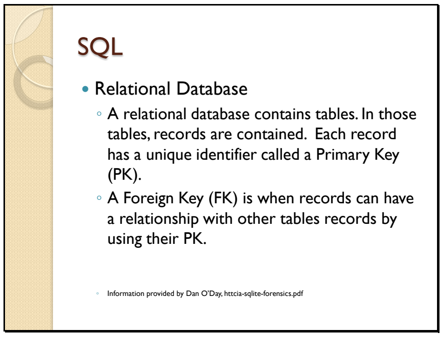
Slide 12



File Types - SQLite

- We will talk more about the SQLite Database File Format next week. This will include:
  - Pages
  - Leaf Pages
  - Freelist Trunk
  - B-Trees

Slide 13

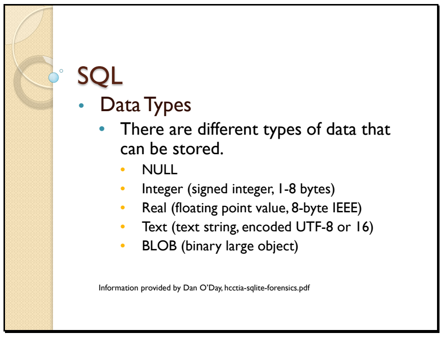


SQL

- Relational Database
  - A relational database contains tables. In those tables, records are contained. Each record has a unique identifier called a Primary Key (PK).
  - A Foreign Key (FK) is when records can have a relationship with other tables records by using their PK.

- Information provided by Dan O'Day, httcia-sqlite-forensics.pdf

Slide 14

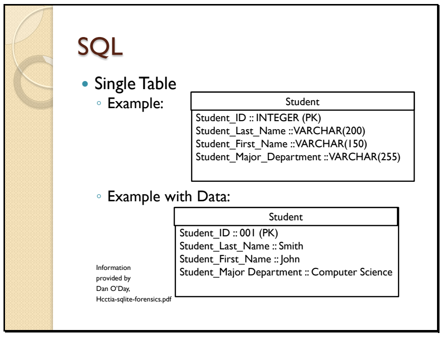


SQL

- Data Types
  - There are different types of data that can be stored.
    - NULL
    - Integer (signed integer, 1-8 bytes)
    - Real (floating point value, 8-byte IEEE)
    - Text (text string, encoded UTF-8 or 16)
    - BLOB (binary large object)

Information provided by Dan O'Day, hcctia-sqlite-forensics.pdf

Slide 15



SQL

- Single Table
  - Example:

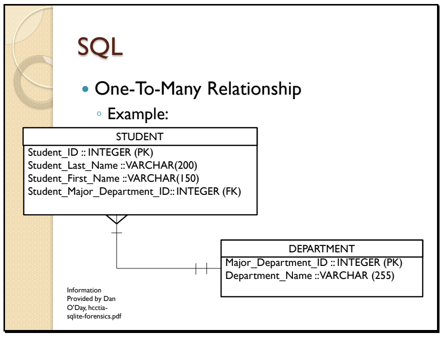
Student
Student_ID :: INTEGER (PK)
Student_Last_Name ::VARCHAR(200)
Student_First_Name ::VARCHAR(150)
Student_Major_Department ::VARCHAR(255)

  - Example with Data:

Student
Student_ID :: 001 (PK)
Student_Last_Name :: Smith
Student_First_Name :: John
Student_Major Department :: Computer Science

Information provided by Dan O'Day, Hcctia-sqlite-forensics.pdf

Slide 16



SQL

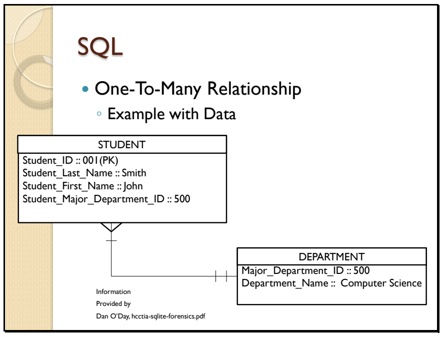
- One-To-Many Relationship
  - Example:

STUDENT
Student_ID :: INTEGER (PK)
Student_Last_Name ::VARCHAR(200)
Student_First_Name ::VARCHAR(150)
Student_Major_Department_ID:: INTEGER (FK)

DEPARTMENT
Major_Department_ID :: INTEGER (PK)
Department_Name ::VARCHAR (255)

Information Provided by Dan O'Day, hcctia-sqlite-forensics.pdf

Slide 17



SQL

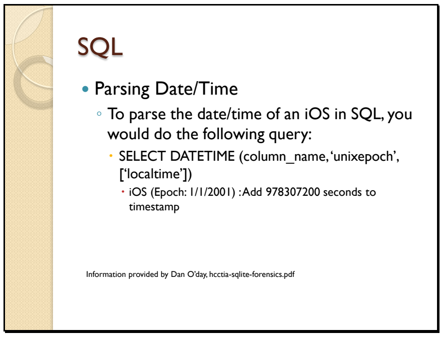
- One-To-Many Relationship
  - Example with Data

STUDENT
Student_ID :: 001(PK)
Student_Last_Name :: Smith
Student_First_Name :: John
Student_Major_Department_ID :: 500

DEPARTMENT
Major_Department_ID :: 500
Department_Name :: Computer Science

Information Provided by Dan O'Day, hcctia-sqlite-forensics.pdf

Slide 18

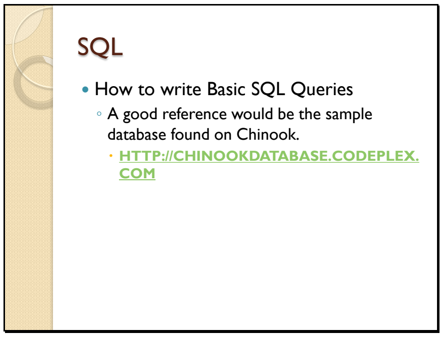


SQL

- Parsing Date/Time
  - To parse the date/time of an iOS in SQL, you would do the following query:
    - SELECT DATETIME (column_name, 'unixepoch', ['localtime'])
      - iOS (Epoch: 1/1/2001) :Add 978307200 seconds to timestamp

Information provided by Dan O'day, hcctia-sqlite-forensics.pdf

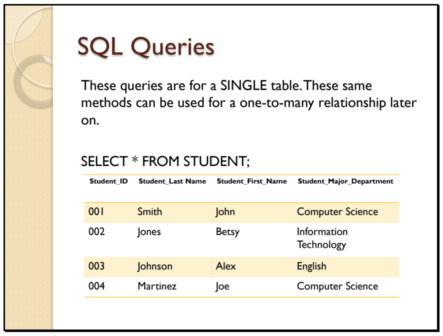
Slide 19



SQL

- How to write Basic SQL Queries
  - A good reference would be the sample database found on Chinook.
    - HTTP://CHINOOKDATABASE.CODEPLEX.COM

Slide 20



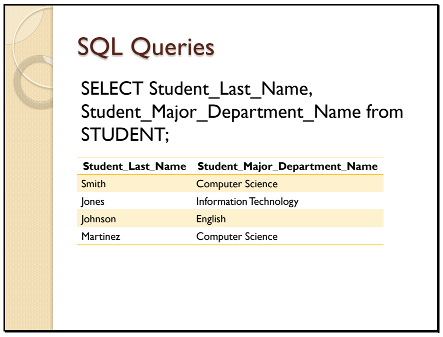
SQL Queries

These queries are for a SINGLE table. These same methods can be used for a one-to-many relationship later on.

SELECT * FROM STUDENT;

Student_ID	Student_Last Name	Student_First_Name	Student_Major_Department
001	Smith	John	Computer Science
002	Jones	Betsy	Information Technology
003	Johnson	Alex	English
004	Martinez	Joe	Computer Science

Slide 21

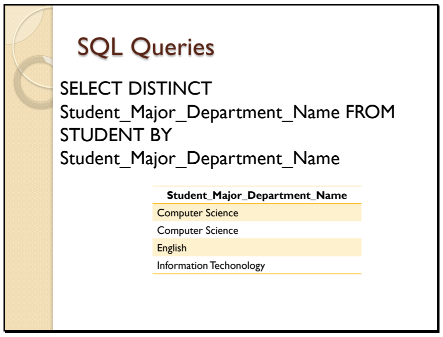


SQL Queries

SELECT Student_Last_Name, Student_Major_Department_Name from STUDENT;

Student_Last_Name	Student_Major_Department_Name
Smith	Computer Science
Jones	Information Technology
Johnson	English
Martinez	Computer Science

Slide 22

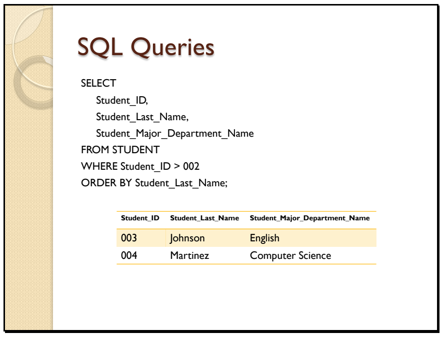


SQL Queries

SELECT DISTINCT Student_Major_Department_Name FROM STUDENT BY Student_Major_Department_Name

Student_Major_Department_Name
Computer Science
Computer Science
English
Information Techonology

Slide 23

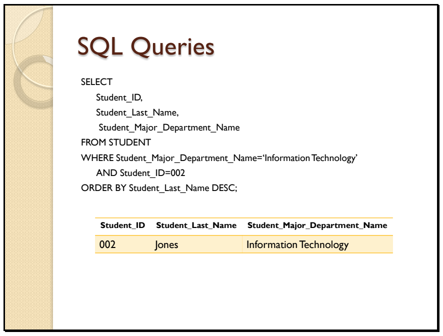


SQL Queries

```
SELECT
    Student_ID,
    Student_Last_Name,
    Student_Major_Department_Name
FROM STUDENT
WHERE Student_ID > 002
ORDER BY Student_Last_Name;
```

Student_ID	Student_Last_Name	Student_Major_Department_Name
003	Johnson	English
004	Martinez	Computer Science

Slide 24

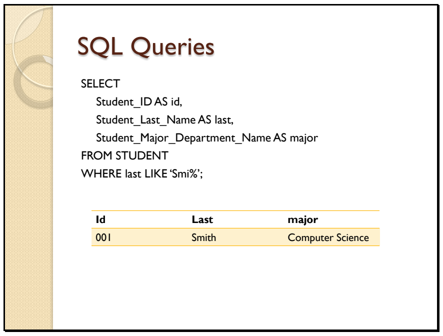


SQL Queries

```
SELECT
    Student_ID,
    Student_Last_Name,
     Student_Major_Department_Name
FROM STUDENT
WHERE Student_Major_Department_Name='Information Technology'
    AND Student_ID=002
ORDER BY Student_Last_Name DESC;
```

Student_ID	Student_Last_Name	Student_Major_Department_Name
002	Jones	Information Technology

Slide 25

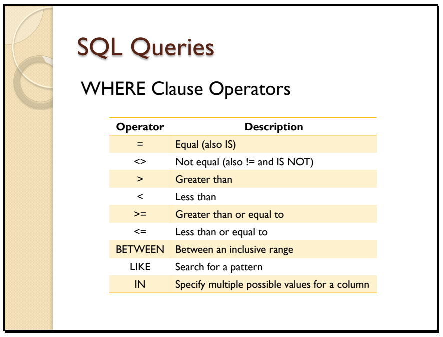


SQL Queries

```
SELECT
    Student_ID AS id,
    Student_Last_Name AS last,
    Student_Major_Department_Name AS major
FROM STUDENT
WHERE last LIKE 'Smi%';
```

Id	Last	major
001	Smith	Computer Science

Slide 26

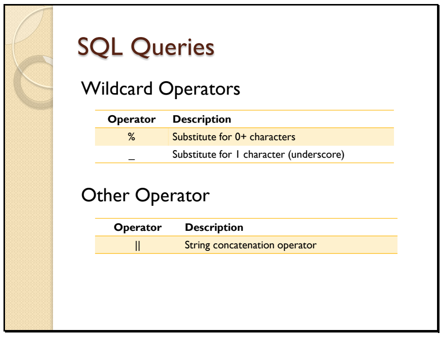


SQL Queries

WHERE Clause Operators

Operator	Description
=	Equal (also IS)
<>	Not equal (also != and IS NOT)
>	Greater than
<	Less than
>=	Greater than or equal to
<=	Less than or equal to
BETWEEN	Between an inclusive range
LIKE	Search for a pattern
IN	Specify multiple possible values for a column

Slide 27



SQL Queries

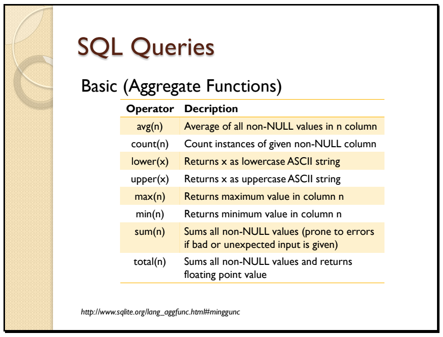
Wildcard Operators

Operator	Description
%	Substitute for 0+ characters
_	Substitute for 1 character (underscore)

Other Operator

Operator	Description
||	String concatenation operator

Slide 28



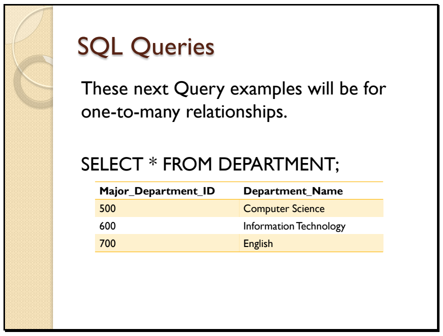
SQL Queries

Basic (Aggregate Functions)

Operator	Decription
avg(n)	Average of all non-NULL values in n column
count(n)	Count instances of given non-NULL column
lower(x)	Returns x as lowercase ASCII string
upper(x)	Returns x as uppercase ASCII string
max(n)	Returns maximum value in column n
min(n)	Returns minimum value in column n
sum(n)	Sums all non-NULL values (prone to errors if bad or unexpected input is given)
total(n)	Sums all non-NULL values and returns floating point value

http://www.sqlite.org/lang_aggfunc.html#mingguno

Slide 29



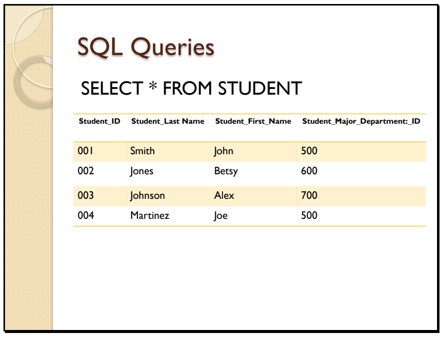
SQL Queries

These next Query examples will be for one-to-many relationships.

SELECT * FROM DEPARTMENT;

Major_Department_ID	Department_Name
500	Computer Science
600	Information Technology
700	English

Slide 30

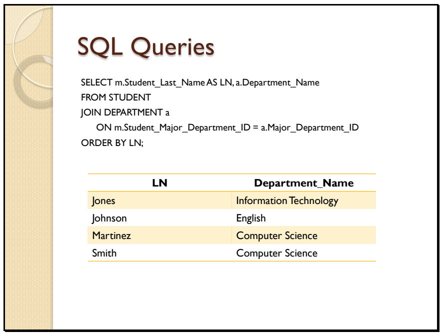


SQL Queries

SELECT * FROM STUDENT

Student_ID	Student_Last Name	Student_First_Name	Student_Major_Department:_ID
001	Smith	John	500
002	Jones	Betsy	600
003	Johnson	Alex	700
004	Martinez	Joe	500

Slide 31

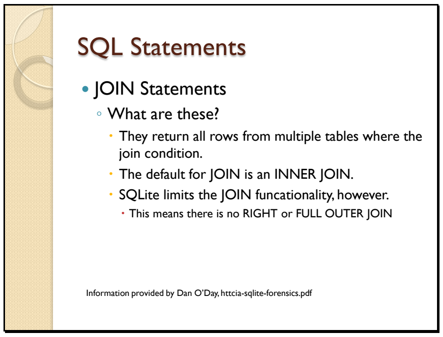


SQL Queries

```
SELECT m.Student_Last_Name AS LN, a.Department_Name
FROM STUDENT
JOIN DEPARTMENT a
    ON m.Student_Major_Department_ID = a.Major_Department_ID
ORDER BY LN;
```

LN	Department_Name
Jones	Information Technology
Johnson	English
Martinez	Computer Science
Smith	Computer Science

Slide 32

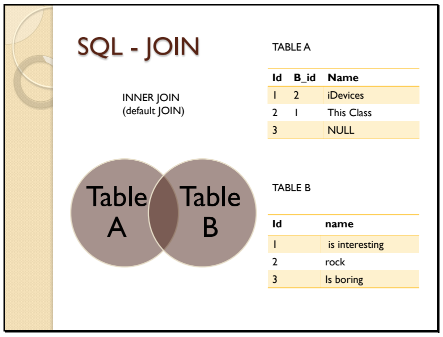


SQL Statements

- JOIN Statements
  - What are these?
    - They return all rows from multiple tables where the join condition.
    - The default for JOIN is an INNER JOIN.
    - SQLite limits the JOIN funcationality, however.
      - This means there is no RIGHT or FULL OUTER JOIN

Information provided by Dan O'Day, httcia-sqlite-forensics.pdf

Slide 33



SQL - JOIN

INNER JOIN
(default JOIN)

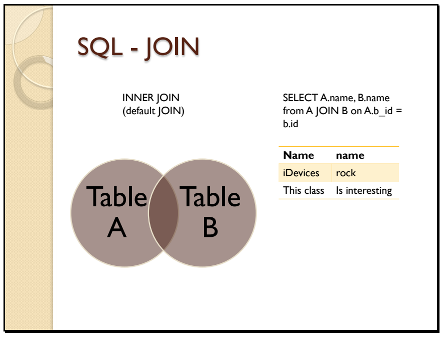
TABLE A

Id	B_id	Name
1	2	iDevices
2	1	This Class
3		NULL

TABLE B

Id	name
1	is interesting
2	rock
3	Is boring

Slide 34



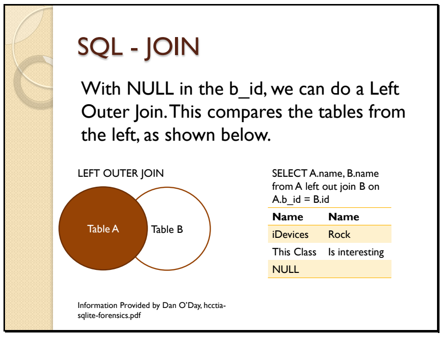
SQL - JOIN

INNER JOIN
(default JOIN)

SELECT A.name, B.name from A JOIN B on A.b_id = b.id

Name	name
iDevices	rock
This class	Is interesting

Slide 35



SQL - JOIN

With NULL in the b_id, we can do a Left Outer Join. This compares the tables from the left, as shown below.

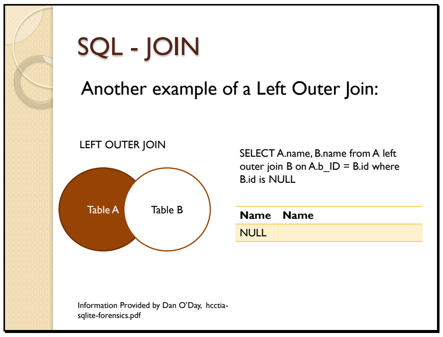
LEFT OUTER JOIN

SELECT A.name, B.name from A left out join B on A.b_id = B.id

Name	Name
iDevices	Rock
This Class	Is interesting
NULL	

Information Provided by Dan O'Day, hcctia-sqlite-forensics.pdf

Slide 36



SQL - JOIN

Another example of a Left Outer Join:

LEFT OUTER JOIN

SELECT A.name, B.name from A left outer join B on A.b_ID = B.id where B.id is NULL

Name	Name
NULL	

Information Provided by Dan O'Day, hcctia-sqlite-forensics.pdf

Week Five: Advanced SQLite Analysis

Week five continues with SQLite analysis, giving a bit more detail about the pages in SQL. Page size is discussed, expressing that a SQLite database can grow to 140 terabytes. These pages can be used for a single purpose which could be the following options: Lock-Byte, Freelist, B-Tree, Payload or Pointer.

The Lock-Byte page is not used by SQLite, but its purpose is to lock a file. Freelist are not active pages. However, this is an important page to know because this is the page where deleted data may reside within the database. If a criminal has deleted incriminating evidence on an iOS device, the data may not have been erased from the device. It could be stored, and eventually found, in this area. These pages are organized by trunk pages, which hold numbers for the freelist leaf pages. Now a trunk page contains arrays that contain 4-byte integers. These bytes translate where the data can be found. For instance, the first number contains the page number of the next freelist trunk page, were as the second number is the number of leaf page pointers it follows. A leaf page contains no information that is used in the database because SQLite does not read or write.

A B-Tree, also known as Binary Trees, contain key and data storage. SQLite recognizes two types of B-Trees: Table and Index. Table b-trees store data in leaves, which has a key that corresponds to a row id. An index b-tree has only keys, where no data is stored. With that in mind, a B-Tree page can be one of two things: An interior page or a leaf page. An interior page contains keys with pointers to page numbers. However, a leaf page only contains keys. If the table b-tree is a leaf page, each key will have associated data.

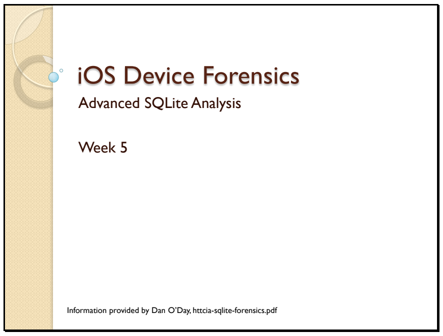
Payload is important for index b-trees. The payload is the arbitrary length section of the table. When the payload exceeds threshold, only the first few bytes are stored on the b-tree. The balance is stored in a linked list. This information is key to know when looking through plists.

This week's presentation also introduces a Many-To-Many relationship in SQL databases, as well as CASE statements. A CASE statement looks through a list of conditions, and returns one of many possible results. SQLite temporary files are also introduced, which include WAL files, Shared-Memory files, Temporary Databases, and rollback journals. A rollback journal allows restoration of a database. This can be very useful in the case of a corrupted database. The presentation goes into detail of how a rollback journal is done, which includes a series of locks on the journal until the new rollback is created. When this is done, the lock is released. Similar to a rollback journal is the Write-Ahead log. This is faster for applications with more writing permissions than read permissions. The write-ahead log allows for multiple transactions to occur, where the rollback journal does not.

Week five's presentation concludes with Deleted Record Recovery. Not many would know that even if data is deleted off of a device, it does not mean that the data is gone, due to free pages and the other pages discussed during this lecture. To try and recover this data, examiners would carve for the database. By carve, we mean to reconstruct. When an examiner states that they will be carving for database, they will be attempting to reconstruct the database to gain information. The examiner would then parse the trees for the information. Students will be informed that the entire database will not be recovered. What is suggested is that they carve for individual SQLite records. It is also mentioned that most approaches are proprietary to tool manufactures in mobile device forensics.

PowerPoint Presentation for Week Five

Slide 1



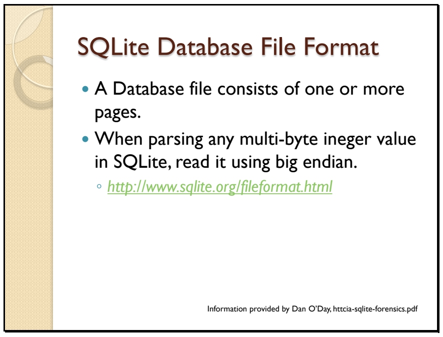
iOS Device Forensics

Advanced SQLite Analysis

Week 5

Information provided by Dan O'Day, httcia-sqlite-forensics.pdf

Slide 2

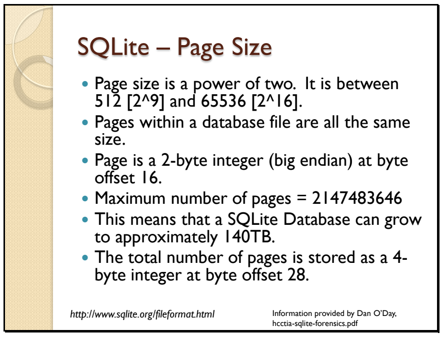


SQLite Database File Format

- A Database file consists of one or more pages.
- When parsing any multi-byte ineger value in SQLite, read it using big endian.
  - http://www.sqlite.org/fileformat.html

Information provided by Dan O'Day, httcia-sqlite-forensics.pdf

Slide 3



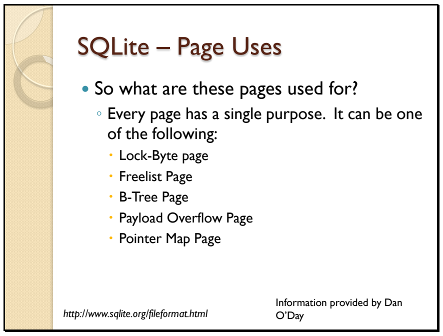
SQLite – Page Size

- Page size is a power of two. It is between 512 [2^9] and 65536 [2^16].
- Pages within a database file are all the same size.
- Page is a 2-byte integer (big endian) at byte offset 16.
- Maximum number of pages = 2147483646
- This means that a SQLite Database can grow to approximately 140TB.
- The total number of pages is stored as a 4-byte integer at byte offset 28.

http://www.sqlite.org/fileformat.html

Information provided by Dan O'Day, hcctia-sqlite-forensics.pdf

Slide 4



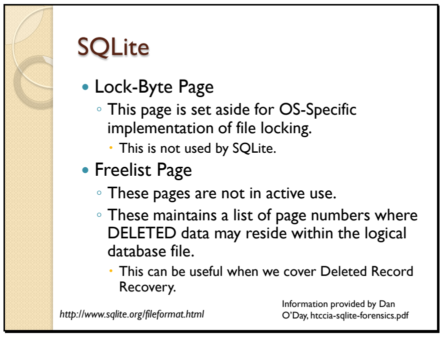
SQLite – Page Uses

- So what are these pages used for?
  - Every page has a single purpose. It can be one of the following:
    - Lock-Byte page
    - Freelist Page
    - B-Tree Page
    - Payload Overflow Page
    - Pointer Map Page

http://www.sqlite.org/fileformat.html

Information provided by Dan O'Day

Slide 5



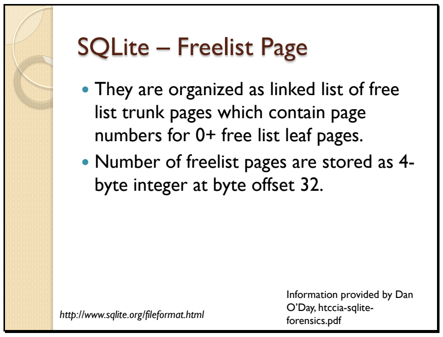
SQLite

- Lock-Byte Page
  - This page is set aside for OS-Specific implementation of file locking.
    - This is not used by SQLite.
- Freelist Page
  - These pages are not in active use.
  - These maintains a list of page numbers where DELETED data may reside within the logical database file.
    - This can be useful when we cover Deleted Record Recovery.

http://www.sqlite.org/fileformat.html

Information provided by Dan O'Day, htccia-sqlite-forensics.pdf

Slide 6



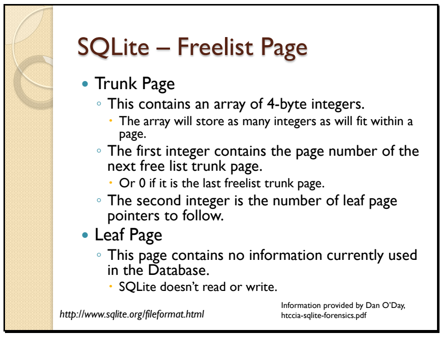
SQLite – Freelist Page

- They are organized as linked list of free list trunk pages which contain page numbers for 0+ free list leaf pages.
- Number of freelist pages are stored as 4-byte integer at byte offset 32.

http://www.sqlite.org/fileformat.html

Information provided by Dan O'Day, htccia-sqlite-forensics.pdf

Slide 7



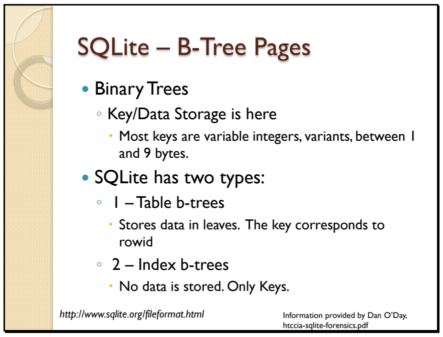
SQLite – Freelist Page

- Trunk Page
  - This contains an array of 4-byte integers.
    - The array will store as many integers as will fit within a page.
  - The first integer contains the page number of the next free list trunk page.
    - Or 0 if it is the last freelist trunk page.
  - The second integer is the number of leaf page pointers to follow.
- Leaf Page
  - This page contains no information currently used in the Database.
    - SQLite doesn't read or write.

http://www.sqlite.org/fileformat.html

Information provided by Dan O'Day, htccia-sqlite-forensics.pdf

Slide 8



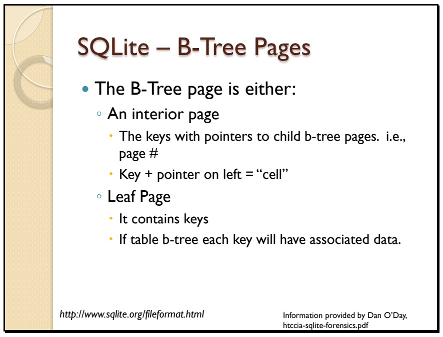
SQLite – B-Tree Pages

- Binary Trees
  - Key/Data Storage is here
    - Most keys are variable integers, variants, between 1 and 9 bytes.
- SQLite has two types:
  - 1 – Table b-trees
    - Stores data in leaves. The key corresponds to rowid
  - 2 – Index b-trees
    - No data is stored. Only Keys.

http://www.sqlite.org/fileformat.html

Information provided by Dan O'Day, htccia-sqlite-forensics.pdf

Slide 9



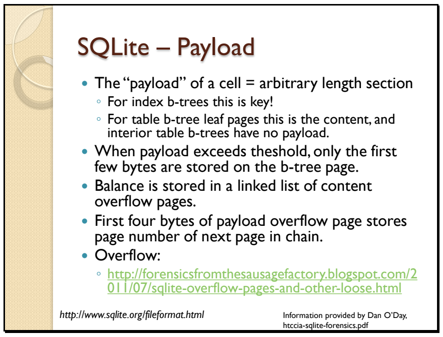
SQLite – B-Tree Pages

- The B-Tree page is either:
  - An interior page
    - The keys with pointers to child b-tree pages. i.e., page #
    - Key + pointer on left = "cell"
  - Leaf Page
    - It contains keys
    - If table b-tree each key will have associated data.

http://www.sqlite.org/fileformat.html

Information provided by Dan O'Day, htccia-sqlite-forensics.pdf

Slide 10



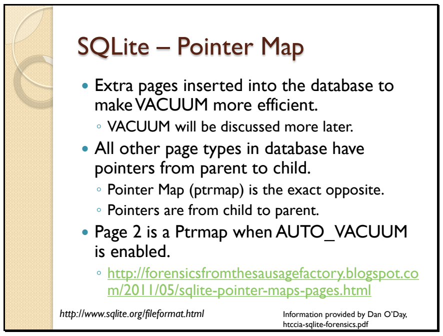
SQLite – Payload

- The "payload" of a cell = arbitrary length section
  - For index b-trees this is key!
  - For table b-tree leaf pages this is the content, and interior table b-trees have no payload.
- When payload exceeds theshold, only the first few bytes are stored on the b-tree page.
- Balance is stored in a linked list of content overflow pages.
- First four bytes of payload overflow page stores page number of next page in chain.
- Overflow:
  - http://forensicsfromthesausagefactory.blogspot.com/2011/07/sqlite-overflow-pages-and-other-loose.html

http://www.sqlite.org/fileformat.html

Information provided by Dan O'Day, htccia-sqlite-forensics.pdf

Slide 11



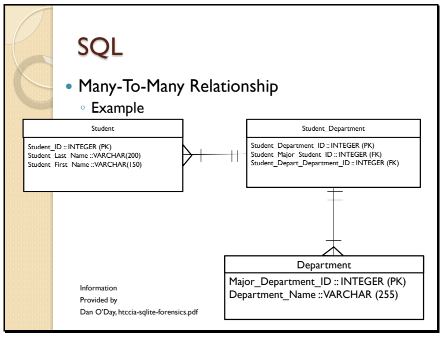
SQLite – Pointer Map

- Extra pages inserted into the database to make VACUUM more efficient.
  - VACUUM will be discussed more later.
- All other page types in database have pointers from parent to child.
  - Pointer Map (ptrmap) is the exact opposite.
  - Pointers are from child to parent.
- Page 2 is a Ptrmap when AUTO_VACUUM is enabled.
  - http://forensicsfromthesausagefactory.blogspot.com/2011/05/sqlite-pointer-maps-pages.html

http://www.sqlite.org/fileformat.html

Information provided by Dan O'Day, htccia-sqlite-forensics.pdf

Slide 12



SQL

- Many-To-Many Relationship
  - Example

Student

Student_ID :: INTEGER (PK)
Student_Last_Name ::VARCHAR(200)
Student_First_Name ::VARCHAR(150)

Student_Department

Student_Department_ID :: INTEGER (PK)
Student_Major_Student_ID :: INTEGER (FK)
Student_Depart_Department_ID :: INTEGER (FK)

Department

Major_Department_ID :: INTEGER (PK)
Department_Name ::VARCHAR (255)

Information
Provided by
Dan O'Day, htccia-sqlite-forensics.pdf

Slide 13

SQL

- The Tables we will use for examples for Many-To-Many Relationships:

Student

Student_ID	Student_Last_Name	Student_First_Name
001	Smith	John

Department

Major_Department_ID	Department_Name
500	Computer Science

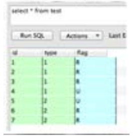
Student_Department

Student_Department_ID	Student_Department_Student_ID	Student_Depart_Deparment_ID
1	001	500

Slide 14

SQL – CASE Statements

- CASE Statements
  - Using the Chinook database, we know the type values:
    - 1 is sent
    - 2 is received
    - 3 is an error
  - We also know the flag values:
    - R is read
    - U is unread



```
select * from test
```

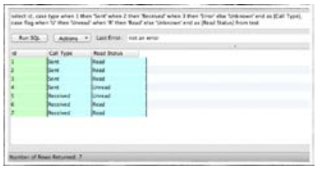
id	type	flag
1	1	R
2	1	R
3	1	R
4	1	U
5	2	U
6	2	R
7	2	R

Information Provided by Dan O'Day and Chinook

Slide 15

SQL – CASE Statements

- This is an example using what we learned last week to work with CASE statements.



```
select id, case type when 1 then 'Sent' when 2 then 'Received' when 3 then 'Error' else 'Unknown' end as [Call Type],
case flag when 'U' then 'Unread' when 'R' then 'Read' else 'Unknown' end as [Read Status] from test
```

not an error

id	Call Type	Read Status
1	Sent	Read
2	Sent	Read
3	Sent	Read
4	Sent	Unread
5	Received	Unread
6	Received	Read
7	Received	Read

Number of Rows Returned: 7

Information Provided by Dan O'Day and Chinook

Slide 16

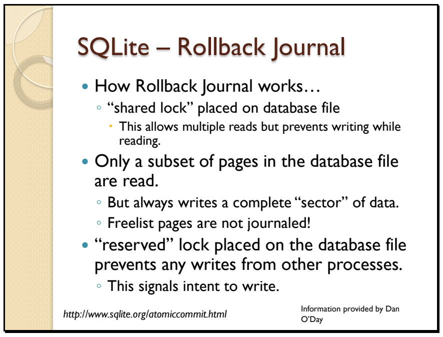
SQLite - Rollback Journal

- What is a rollback journal?
  - This allows restoration of a database to its original state.
  - When writing to a database with a rollback journal, it creates the rollback journal file with original data being altered.
  - It is stored in the same folder as the database with '-journal' filename suffix.
  - This is the default behavior of SQLite.

http://www.sqlite.org/atomiccommit.html

Information provided by Dan O'Day

Slide 17



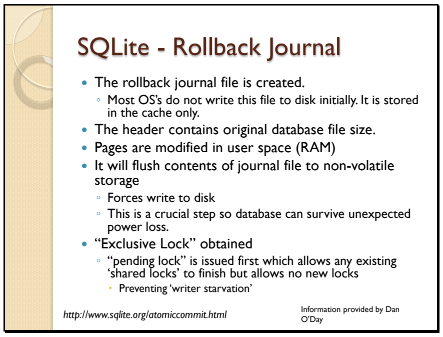
SQLite – Rollback Journal

- How Rollback Journal works…
  - "shared lock" placed on database file
    - This allows multiple reads but prevents writing while reading.
- Only a subset of pages in the database file are read.
  - But always writes a complete "sector" of data.
  - Freelist pages are not journaled!
- "reserved" lock placed on the database file prevents any writes from other processes.
  - This signals intent to write.

http://www.sqlite.org/atomiccommit.html

Information provided by Dan O'Day

Slide 18



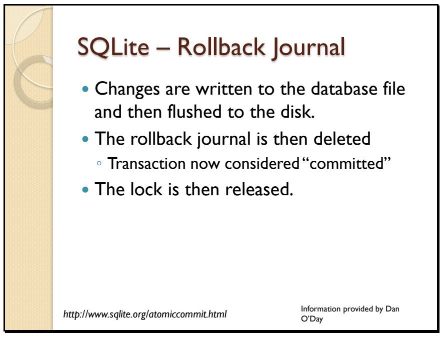
SQLite - Rollback Journal

- The rollback journal file is created.
  - Most OS's do not write this file to disk initially. It is stored in the cache only.
- The header contains original database file size.
- Pages are modified in user space (RAM)
- It will flush contents of journal file to non-volatile storage
  - Forces write to disk
  - This is a crucial step so database can survive unexpected power loss.
- "Exclusive Lock" obtained
  - "pending lock" is issued first which allows any existing 'shared locks' to finish but allows no new locks
    - Preventing 'writer starvation'

http://www.sqlite.org/atomiccommit.html

Information provided by Dan O'Day

Slide 19



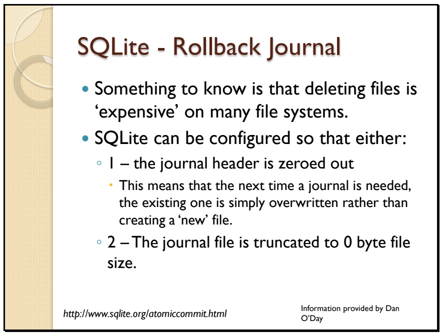
SQLite – Rollback Journal

- Changes are written to the database file and then flushed to the disk.
- The rollback journal is then deleted
  - Transaction now considered "committed"
- The lock is then released.

http://www.sqlite.org/atomiccommit.html

Information provided by Dan O'Day

Slide 20



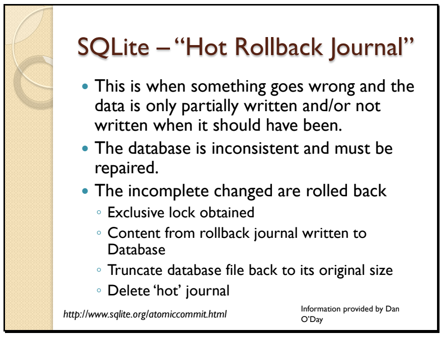
SQLite - Rollback Journal

- Something to know is that deleting files is 'expensive' on many file systems.
- SQLite can be configured so that either:
  - 1 – the journal header is zeroed out
    - This means that the next time a journal is needed, the existing one is simply overwritten rather than creating a 'new' file.
  - 2 – The journal file is truncated to 0 byte file size.

http://www.sqlite.org/atomiccommit.html

Information provided by Dan O'Day

Slide 21



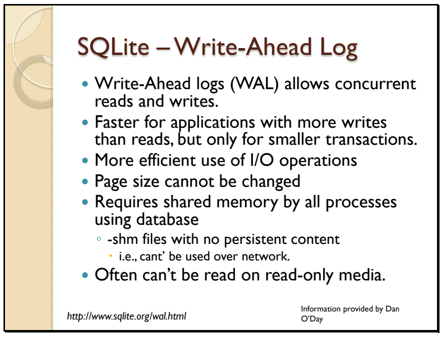
SQLite – "Hot Rollback Journal"

- This is when something goes wrong and the data is only partially written and/or not written when it should have been.
- The database is inconsistent and must be repaired.
- The incomplete changed are rolled back
  - Exclusive lock obtained
  - Content from rollback journal written to Database
  - Truncate database file back to its original size
  - Delete 'hot' journal

http://www.sqlite.org/atomiccommit.html

Information provided by Dan O'Day

Slide 22



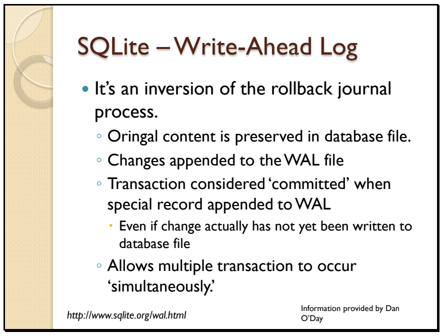
SQLite – Write-Ahead Log

- Write-Ahead logs (WAL) allows concurrent reads and writes.
- Faster for applications with more writes than reads, but only for smaller transactions.
- More efficient use of I/O operations
- Page size cannot be changed
- Requires shared memory by all processes using database
  - -shm files with no persistent content
    - i.e., cant' be used over network.
- Often can't be read on read-only media.

http://www.sqlite.org/wal.html

Information provided by Dan O'Day

Slide 23



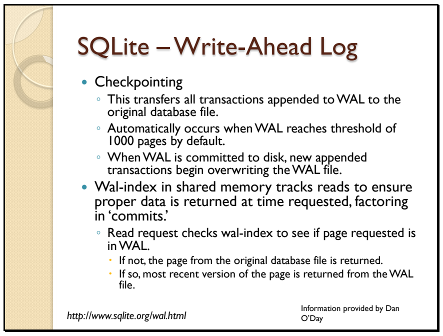
SQLite – Write-Ahead Log

- It's an inversion of the rollback journal process.
  - Oringal content is preserved in database file.
  - Changes appended to the WAL file
  - Transaction considered 'committed' when special record appended to WAL
    - Even if change actually has not yet been written to database file
  - Allows multiple transaction to occur 'simultaneously.'

http://www.sqlite.org/wal.html

Information provided by Dan O'Day

Slide 24



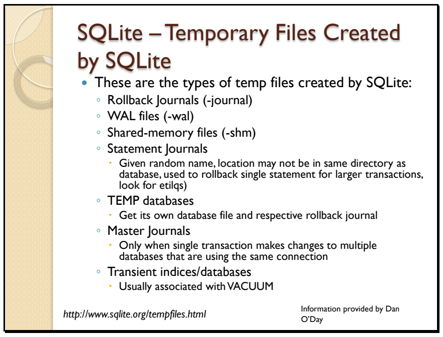
SQLite – Write-Ahead Log

- Checkpointing
  - This transfers all transactions appended to WAL to the original database file.
  - Automatically occurs when WAL reaches threshold of 1000 pages by default.
  - When WAL is committed to disk, new appended transactions begin overwriting the WAL file.
- Wal-index in shared memory tracks reads to ensure proper data is returned at time requested, factoring in 'commits.'
  - Read request checks wal-index to see if page requested is in WAL.
    - If not, the page from the original database file is returned.
    - If so, most recent version of the page is returned from the WAL file.

http://www.sqlite.org/wal.html

Information provided by Dan O'Day

Slide 25



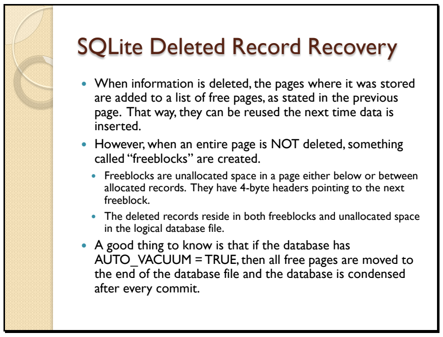
SQLite – Temporary Files Created by SQLite

- These are the types of temp files created by SQLite:
  - Rollback Journals (-journal)
  - WAL files (-wal)
  - Shared-memory files (-shm)
  - Statement Journals
    - Given random name, location may not be in same directory as database, used to rollback single statement for larger transactions, look for etilqs)
  - TEMP databases
    - Get its own database file and respective rollback journal
  - Master Journals
    - Only when single transaction makes changes to multiple databases that are using the same connection
  - Transient indices/databases
    - Usually associated with VACUUM

http://www.sqlite.org/tempfiles.html

Information provided by Dan O'Day

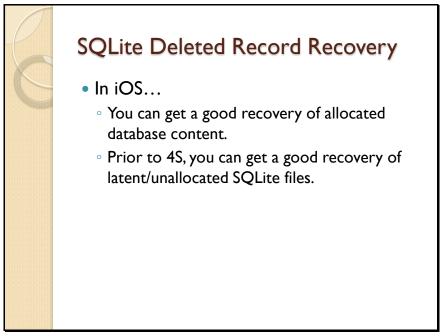
Slide 26



SQLite Deleted Record Recovery

- When information is deleted, the pages where it was stored are added to a list of free pages, as stated in the previous page. That way, they can be reused the next time data is inserted.
- However, when an entire page is NOT deleted, something called "freeblocks" are created.
  - Freeblocks are unallocated space in a page either below or between allocated records. They have 4-byte headers pointing to the next freeblock.
  - The deleted records reside in both freeblocks and unallocated space in the logical database file.
- A good thing to know is that if the database has AUTO_VACUUM = TRUE, then all free pages are moved to the end of the database file and the database is condensed after every commit.

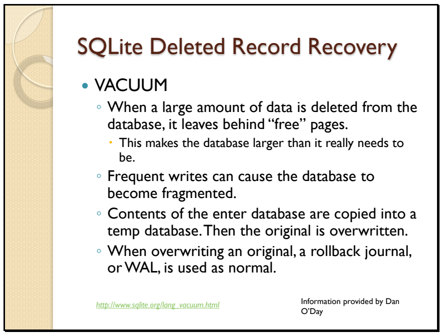
Slide 27



SQLite Deleted Record Recovery

- In iOS…
  - You can get a good recovery of allocated database content.
  - Prior to 4S, you can get a good recovery of latent/unallocated SQLite files.

Slide 28



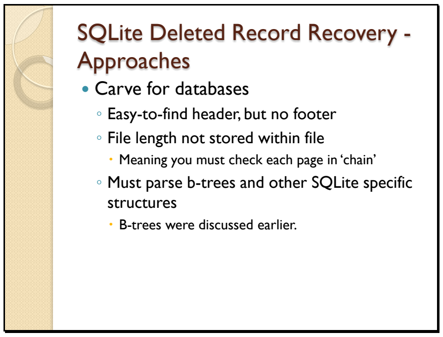
SQLite Deleted Record Recovery

- VACUUM
  - When a large amount of data is deleted from the database, it leaves behind "free" pages.
    - This makes the database larger than it really needs to be.
  - Frequent writes can cause the database to become fragmented.
  - Contents of the enter database are copied into a temp database. Then the original is overwritten.
  - When overwriting an original, a rollback journal, or WAL, is used as normal.

http://www.sqlite.org/lang_vacuum.html

Information provided by Dan O'Day

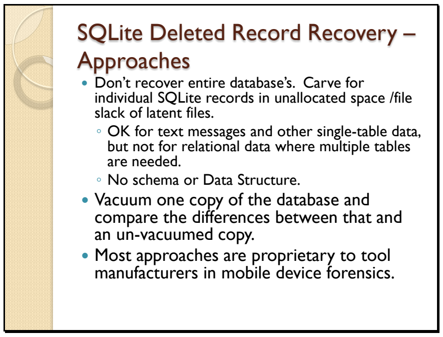
Slide 29



SQLite Deleted Record Recovery - Approaches

- Carve for databases
  - Easy-to-find header, but no footer
  - File length not stored within file
    - Meaning you must check each page in 'chain'
  - Must parse b-trees and other SQLite specific structures
    - B-trees were discussed earlier.

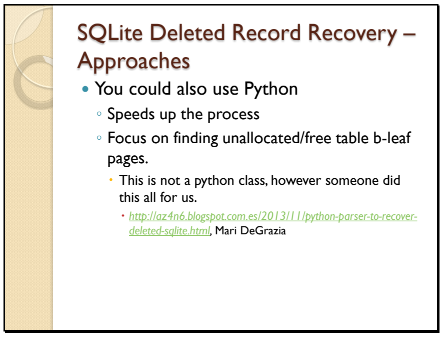
Slide 30



SQLite Deleted Record Recovery – Approaches

- Don't recover entire database's. Carve for individual SQLite records in unallocated space /file slack of latent files.
  - OK for text messages and other single-table data, but not for relational data where multiple tables are needed.
  - No schema or Data Structure.
- Vacuum one copy of the database and compare the differences between that and an un-vacuumed copy.
- Most approaches are proprietary to tool manufacturers in mobile device forensics.

Slide 31



SQLite Deleted Record Recovery – Approaches

- You could also use Python
  - Speeds up the process
  - Focus on finding unallocated/free table b-leaf pages.
    - This is not a python class, however someone did this all for us.
      - *http://az4n6.blogspot.com.es/2013/11/python-parser-to-recover-deleted-sqlite.html*, Mari DeGrazia

Chapter 7 – Week Six: Analysis Strategies and Commercial Tools

Week six begins with file carving. File carving was discussed briefly in the previous week. To refresh, file carving is a process that specifies file types, which are searched and extracted. [14] File carving examines the binary data, and then identifies the file based on their file header. It is also good to know that if

[14] (Hoog & Strzempka, Acquistions: File Carving, 2011)

the file format has a known header; it will be scanned from header until it does find the footer. Only when these steps are done, the data is saved to a disk for examination.

During file carving, one should remember that files do not always stay pristine. Files are sometimes fragmented, similar to a computer having fragmented files. It is important to know about fragment files because when the file carving techniques require that the data is sequential in the image. What this just means is that the carving will not produce a full file it is fragmented.

Fragmenting can happen in many ways. One way for fragmenting can occur is the memory type, as well as the process of saving a file to nonvolatile storage. This can also mean that larger files, such as videos, are harder to recover. The process of file carving normally includes a configuration file for the tool, the data carving tool itself and the disk image that has the desired data. The tool will find the data, and the results will be grouped by the file type upon completion.

Students will learn about string extractions. Strings are extracted using ASCII[15] printable strings. This type of extraction is normally used on a Linux workstation. In this setting, these strings are normally at least four characters long. This type of analysis is effective for quick examination for information that can be of interest. However, this technique is not refined. [16]

[15] American Standard Code for Information Interchange. This is a code that represents a single unique character.

[16] (Hoog & Strzempka, Acquisitions: Strings, 2011)

When doing this type of analysis, there are a few options to keep in mind, which are given to the students. For instance, "—all" options tell strings to examine the entire file and "—radix" options tell strings to print the offset within the file where the string is found.[17] The "—radix" can also be helpful when combining strings to find evidence.

String extraction can be very useful and powerful. With a combination of searching and filters, examiners can determine important data such as phone numbers, name, locations, GPS coordinates and dates. One must remember that other tools can be used to find more data.

Students will learn this week about metadata as well. Metadata is data that gives more information on a data. A device can hold exchangeable image file (EXIF) data, EXIF geolocation and embedded timestamps, which are types of metadata. The EXIF data is normally associated with digital pictures and videos, and can give information about Date, Time and Location of the media. For example, a digital picture's EXIF data would tell what date the picture was taken, what time the picture was taken and where the picture was taken. EXIF Geolocation, also known as a geotag, stores the longitude and latitude of where the picture or video was taken. This can be crucial in an investigation, especially if a photograph or video of the crime scene is discovered on the device. The embedded timestamp gives an accurate time as to when the media was taken, helping investigators determine a timeline. It is important to note that timestamps work on absolute time. This just means that it is in the number of seconds since

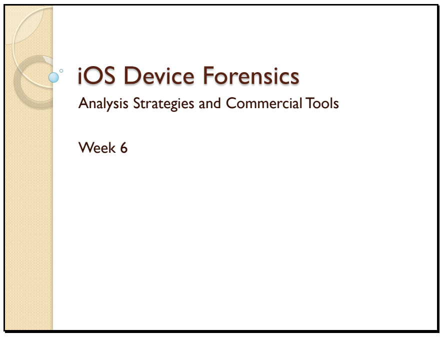
[17] (Hoog & Strzempka, Acquisitions: Strings, 2011)

January 1st, 2001. Thankfully, tools are available to calculate the time for examiners so they do not have to do the calculations by time.

The presentation concludes with tools that examiners might use in the field. These tools include Cellebrite UFED, Katana Forensics Lantern, Elcom iOS Forensic Toolkit and AccessData Mobile Phone Examiner Plus. Each tool is given a brief explanation. Most of these tools require a license purchase in order for it to be used.

PowerPoint Presentation for Week Six

Slide 1

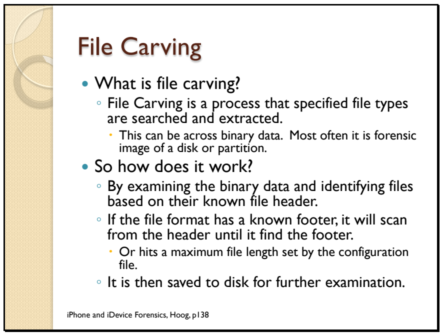


iOS Device Forensics

Analysis Strategies and Commercial Tools

Week 6

Slide 2

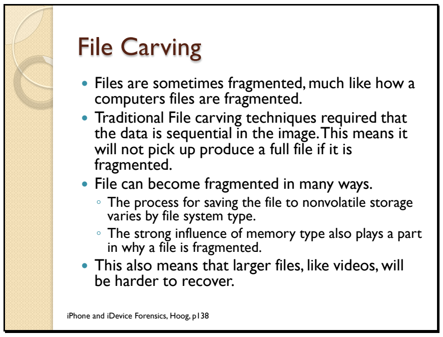


File Carving

- What is file carving?
  - File Carving is a process that specified file types are searched and extracted.
    - This can be across binary data. Most often it is forensic image of a disk or partition.
- So how does it work?
  - By examining the binary data and identifying files based on their known file header.
  - If the file format has a known footer, it will scan from the header until it find the footer.
    - Or hits a maximum file length set by the configuration file.
  - It is then saved to disk for further examination.

iPhone and iDevice Forensics, Hoog, p138

Slide 3

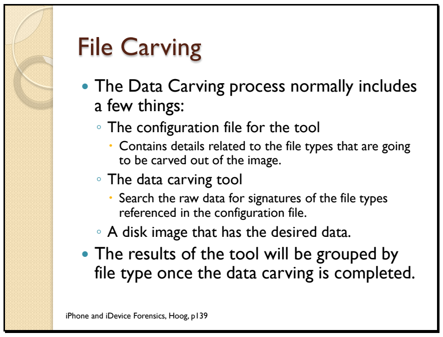


File Carving

- Files are sometimes fragmented, much like how a computers files are fragmented.
- Traditional File carving techniques required that the data is sequential in the image. This means it will not pick up produce a full file if it is fragmented.
- File can become fragmented in many ways.
  - The process for saving the file to nonvolatile storage varies by file system type.
  - The strong influence of memory type also plays a part in why a file is fragmented.
- This also means that larger files, like videos, will be harder to recover.

iPhone and iDevice Forensics, Hoog, p138

Slide 4

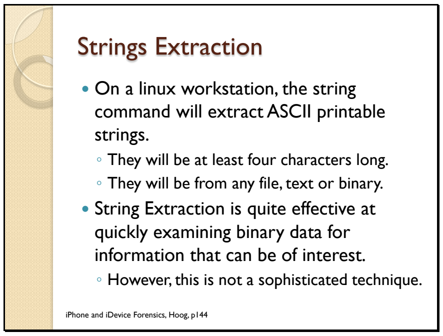


File Carving

- The Data Carving process normally includes a few things:
  - The configuration file for the tool
    - Contains details related to the file types that are going to be carved out of the image.
  - The data carving tool
    - Search the raw data for signatures of the file types referenced in the configuration file.
  - A disk image that has the desired data.
- The results of the tool will be grouped by file type once the data carving is completed.

iPhone and iDevice Forensics, Hoog, p139

Slide 5

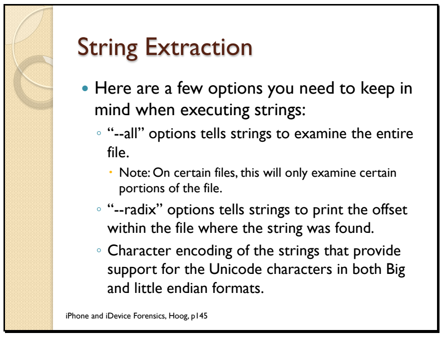


Strings Extraction

- On a linux workstation, the string command will extract ASCII printable strings.
  - They will be at least four characters long.
  - They will be from any file, text or binary.
- String Extraction is quite effective at quickly examining binary data for information that can be of interest.
  - However, this is not a sophisticated technique.

iPhone and iDevice Forensics, Hoog, p144

Slide 6

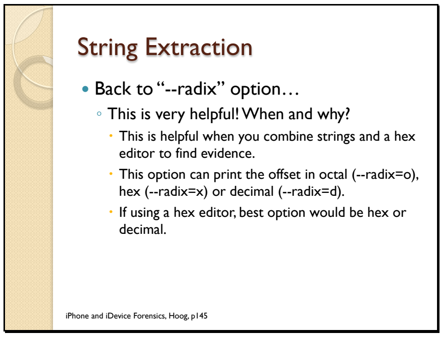


String Extraction

- Here are a few options you need to keep in mind when executing strings:
  - "--all" options tells strings to examine the entire file.
    - Note: On certain files, this will only examine certain portions of the file.
  - "--radix" options tells strings to print the offset within the file where the string was found.
  - Character encoding of the strings that provide support for the Unicode characters in both Big and little endian formats.

iPhone and iDevice Forensics, Hoog, p145

Slide 7

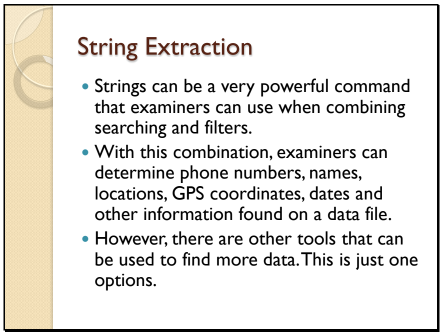


String Extraction

- Back to "--radix" option…
  - This is very helpful! When and why?
    - This is helpful when you combine strings and a hex editor to find evidence.
    - This option can print the offset in octal (--radix=o), hex (--radix=x) or decimal (--radix=d).
    - If using a hex editor, best option would be hex or decimal.

iPhone and iDevice Forensics, Hoog, p145

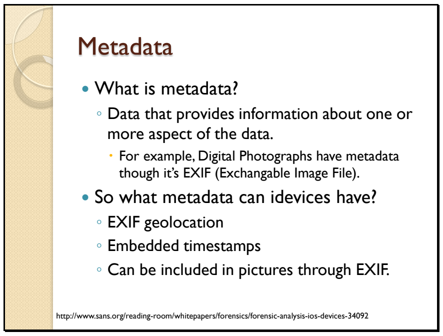
Slide 8



String Extraction

- Strings can be a very powerful command that examiners can use when combining searching and filters.
- With this combination, examiners can determine phone numbers, names, locations, GPS coordinates, dates and other information found on a data file.
- However, there are other tools that can be used to find more data. This is just one options.

Slide 9

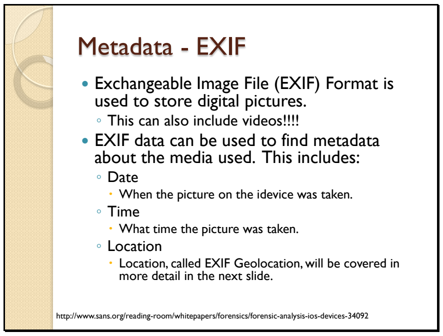


Metadata

- What is metadata?
  - Data that provides information about one or more aspect of the data.
    - For example, Digital Photographs have metadata though it's EXIF (Exchangable Image File).
- So what metadata can idevices have?
  - EXIF geolocation
  - Embedded timestamps
  - Can be included in pictures through EXIF.

http://www.sans.org/reading-room/whitepapers/forensics/forensic-analysis-ios-devices-34092

Slide 10



Metadata - EXIF

- Exchangeable Image File (EXIF) Format is used to store digital pictures.
  - This can also include videos!!!!
- EXIF data can be used to find metadata about the media used. This includes:
  - Date
    - When the picture on the idevice was taken.
  - Time
    - What time the picture was taken.
  - Location
    - Location, called EXIF Geolocation, will be covered in more detail in the next slide.

http://www.sans.org/reading-room/whitepapers/forensics/forensic-analysis-ios-devices-34092

Slide 11

Metadata – EXIF Geolocation

- Geolocation, or a Geotag, is the GPS data that can be found in an image's header.
- What it stores is the longitude and latitude of where the picture or video was taken.
  - This can be very beneficial for when there are incriminating pictures found on a phone that can help a case.

http://www.sans.org/reading-room/whitepapers/forensics/forensic-analysis-ios-devices-34092

Slide 12

Metadata – EXIF Geolocation

- Surprisingly, there are apps on iTunes that can show you EXIF data for photographs.
- Some require you to pay for the service, while others are free.
- However, they may not be able to retrieve all the information that a forensics tool can.

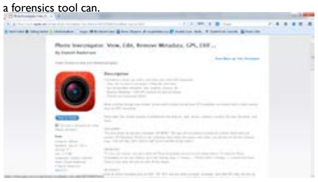


Photo Investigator: View, Edit, Remove Metadata, GPS, EXIF ...

Description

http://www.sans.org/reading-room/whitepapers/forensics/forensic-analysis-ios-devices-34092

Slide 13

Metadata – Embedded Timestamp

- Everything in iOS has a Timestamp to when the volume was created.
- It should be noted that when working with timestamps, it will be provided in CF Absolute Time.
  - This means that the number of seconds since January 1st, 2001.
- The formula to find the time of the timestamp is the following:
  - =CreatedTime/(60*60*24)+DATE(2001,1,1)
- Thankfully there are tools that can help us translate the time for us.
  - http://www.epochconverter.com/

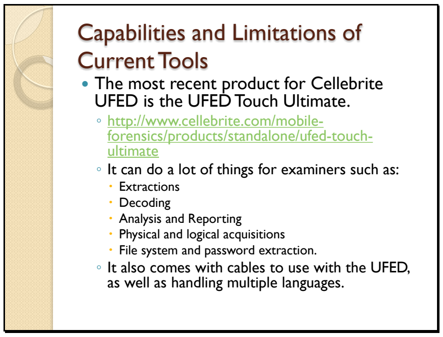
http://www.sans.org/reading-room/whitepapers/forensics/forensic-analysis-ios-devices-34092

Slide 14

Metadata – Embedded Timestamp

- Here are some examples of places to find Embedded Timestamps:
  - Pictures
  - Notes
  - Text Messages
  - GPS
- A good reference for more information about Timestamps and Time Utilities would be on the Mac Developer Library:
  - https://developer.apple.com/library/mac/documentation/CoreFoundation/Reference/CFTimeUtils/Reference/reference.html

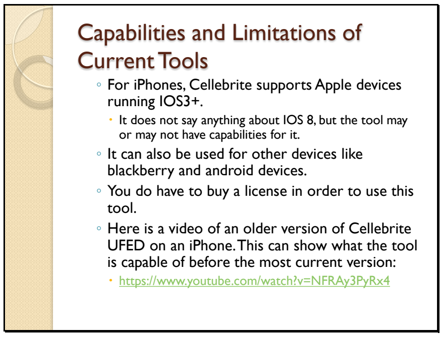
Slide 15



Capabilities and Limitations of Current Tools

- The most recent product for Cellebrite UFED is the UFED Touch Ultimate.
  - http://www.cellebrite.com/mobile-forensics/products/standalone/ufed-touch-ultimate
  - It can do a lot of things for examiners such as:
    - Extractions
    - Decoding
    - Analysis and Reporting
    - Physical and logical acquisitions
    - File system and password extraction.
  - It also comes with cables to use with the UFED, as well as handling multiple languages.

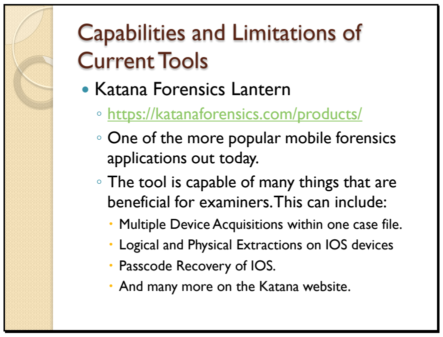
Slide 16



Capabilities and Limitations of Current Tools

- For iPhones, Cellebrite supports Apple devices running IOS3+.
  - It does not say anything about IOS 8, but the tool may or may not have capabilities for it.
- It can also be used for other devices like blackberry and android devices.
- You do have to buy a license in order to use this tool.
- Here is a video of an older version of Cellebrite UFED on an iPhone. This can show what the tool is capable of before the most current version:
  - https://www.youtube.com/watch?v=NFRAy3PyRx4

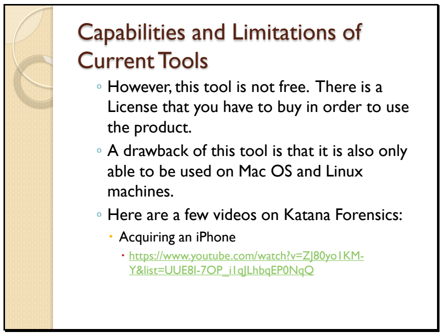
Slide 17



Capabilities and Limitations of Current Tools

- Katana Forensics Lantern
  - https://katanaforensics.com/products/
  - One of the more popular mobile forensics applications out today.
  - The tool is capable of many things that are beneficial for examiners. This can include:
    - Multiple Device Acquisitions within one case file.
    - Logical and Physical Extractions on IOS devices
    - Passcode Recovery of IOS.
    - And many more on the Katana website.

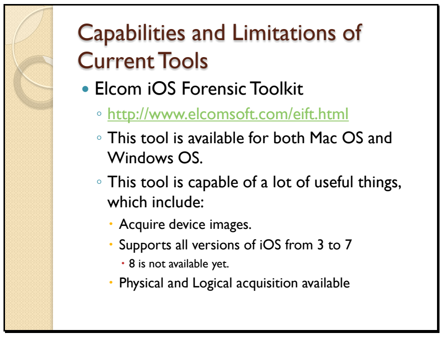
Slide 18



Capabilities and Limitations of Current Tools

- However, this tool is not free. There is a License that you have to buy in order to use the product.
- A drawback of this tool is that it is also only able to be used on Mac OS and Linux machines.
- Here are a few videos on Katana Forensics:
  - Acquiring an iPhone
    - https://www.youtube.com/watch?v=ZJ80yo1KM-Y&list=UUE8I-7OP_i1qJLhbqEP0NqQ

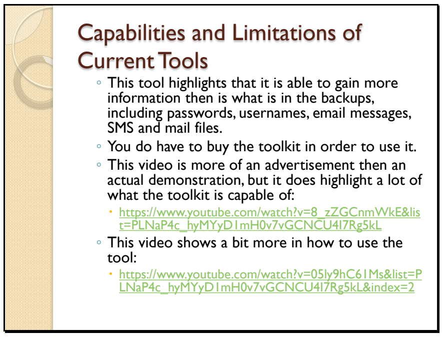
Slide 19



Capabilities and Limitations of Current Tools

- Elcom iOS Forensic Toolkit
  - http://www.elcomsoft.com/eift.html
  - This tool is available for both Mac OS and Windows OS.
  - This tool is capable of a lot of useful things, which include:
    - Acquire device images.
    - Supports all versions of iOS from 3 to 7
      - 8 is not available yet.
    - Physical and Logical acquisition available

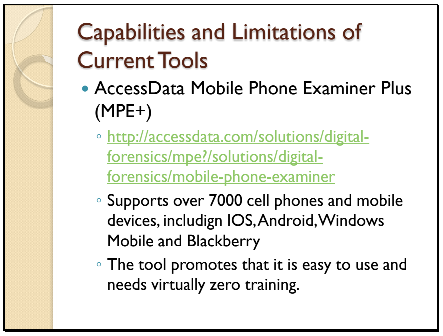
Slide 20



Capabilities and Limitations of Current Tools

- This tool highlights that it is able to gain more information then is what is in the backups, including passwords, usernames, email messages, SMS and mail files.
- You do have to buy the toolkit in order to use it.
- This video is more of an advertisement then an actual demonstration, but it does highlight a lot of what the toolkit is capable of:
  - https://www.youtube.com/watch?v=8_zZGCnmWkE&list=PLNaP4c_hyMYyD1mH0v7vGCNCU4I7Rg5kL
- This video shows a bit more in how to use the tool:
  - https://www.youtube.com/watch?v=05ly9hC61Ms&list=PLNaP4c_hyMYyD1mH0v7vGCNCU4I7Rg5kL&index=2

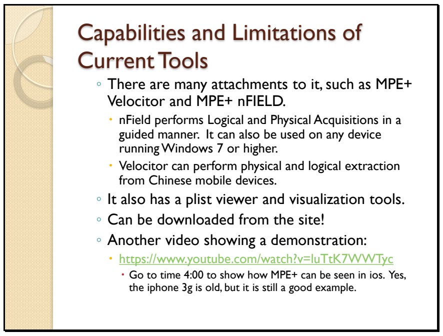
Slide 21



Capabilities and Limitations of Current Tools

- AccessData Mobile Phone Examiner Plus (MPE+)
  - http://accessdata.com/solutions/digital-forensics/mpe?/solutions/digital-forensics/mobile-phone-examiner
  - Supports over 7000 cell phones and mobile devices, includign IOS, Android, Windows Mobile and Blackberry
  - The tool promotes that it is easy to use and needs virtually zero training.

Slide 22



Capabilities and Limitations of Current Tools

- There are many attachments to it, such as MPE+ Velocitor and MPE+ nFIELD.
  - nField performs Logical and Physical Acquisitions in a guided manner. It can also be used on any device running Windows 7 or higher.
  - Velocitor can perform physical and logical extraction from Chinese mobile devices.
- It also has a plist viewer and visualization tools.
- Can be downloaded from the site!
- Another video showing a demonstration:
  - https://www.youtube.com/watch?v=luTtK7WWTyc
    - Go to time 4:00 to show how MPE+ can be seen in ios. Yes, the iphone 3g is old, but it is still a good example.

Chapter 8 – Week Seven: Introduction to iOS Security

Week seven gives students an introduction to iOS security. Students are then introduced to wiping the device through different methods. The first discussed is iCloud Remote Wiping. This option allows the device to be erased through iCloud. The application "Find my iPhone" is an example of this. If the device is lost, missing or stolen, the device can be erased remotely. It is confirmed by using the users Apple ID and password.

The next method is just a secure erase. This wipes the clean, which can be done through the "erase all content and settings" option in the device. This option was not always available to the devices. Up until iOS 2.0, the devices would not be securely erased. With the release of iOS 3.0, apple introduced hardware-level encryption which allowed a faster and secure wipe process.[18] With the standard hardware encryption generates an encryption key. When the device is erased, the encryption key is wiped and lost. With no encryption key, the data cannot be interpreted.

Keychains are also mentioned once more in this presentation. The keychain works as a secure storage container, which holds passwords and multiple applications. In iOS, each application has access to its own keychain items, which means that applications cannot access other applications items. Keychain backups are also discussed, which happens whenever the device's data is backed up. The keychain remains encrypted with the keys throughout the

[18] (Hollington, 2013)

backup, however. Examples are then given to the students to help explain this point.

NSProtectionNone is a hardware deduced key by the application or OS data. If a file is created without specifying any accessibility constant, it is marked as NSProtectionNone. Before iOS 5, apple could return the NSProtectionNone data from locked devices. Up until iOS 8, apple could get information off a locked device. Due to apple's new privacy policy, apple cannot gain access to an iOS 8 device.

This point is important to know when dealing with search warrants for devices. Even with a warrant from law enforcement, Apple cannot gain access to an iOS 8 device without the user's passcode. Normally with the proper paperwork, law enforcement agencies can get the data off a device to help with a case. This is still true with iOS 7 and below. According to Zdziarksi, some user generated active files that can be provided are Photos, Video, Contact and Call History.

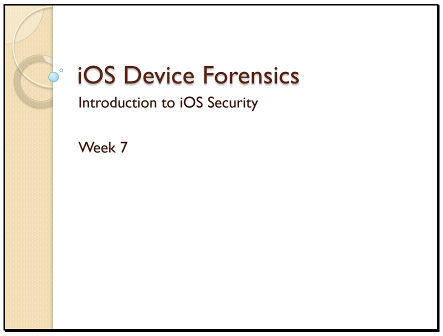
This presentation also goes back to discussing encryption, which was discussed in week two's lecture. Data protection is discussed, including how it is constructed and managed by a hierarchy of keys. They build on the encryption technologies that already exist on the iOS device.

For data protection, there are classes that can be assigned when a new file is created. These basic classes are complete protection, protected unless open, protected until first user authentication and no protection. Complete protection can be compared to unlocking an iDevice using a passcode or fingerprint. Protected unless open allows encryption that runs in the background, such as when an attachment is being downloaded. Protected until first user authentication acts like complete protection, but does not remove the decrypt key when the device is locked. No protection means that the device is only protected with the unique user id (UID). [19]

To conclude this presentation, iOS Backup is discussed. Backups can occur through iTunes or through the iCloud. The iPhone Analyzer is useful for working with backups that need to be decrypted without a passcode.

PowerPoint Presentation for Week Seven

Slide 1

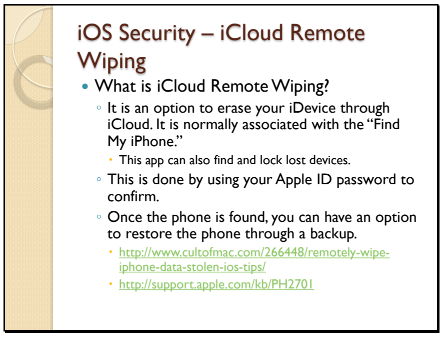


iOS Device Forensics

Introduction to iOS Security

Week 7

Slide 2

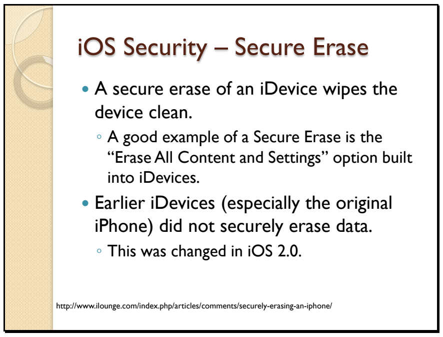


iOS Security – iCloud Remote Wiping

- What is iCloud Remote Wiping?
  - It is an option to erase your iDevice through iCloud. It is normally associated with the "Find My iPhone."
    - This app can also find and lock lost devices.
  - This is done by using your Apple ID password to confirm.
  - Once the phone is found, you can have an option to restore the phone through a backup.
    - http://www.cultofmac.com/266448/remotely-wipe-iphone-data-stolen-ios-tips/
    - http://support.apple.com/kb/PH2701

[19] (Apple, 2014)

Slide 3

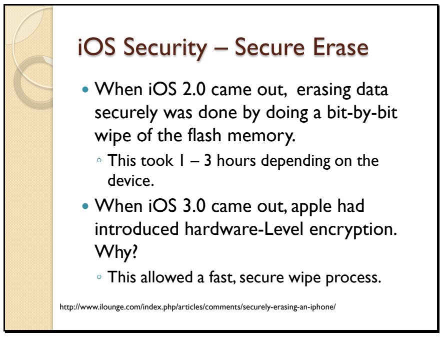


iOS Security – Secure Erase

- A secure erase of an iDevice wipes the device clean.
  - A good example of a Secure Erase is the “Erase All Content and Settings” option built into iDevices.
- Earlier iDevices (especially the original iPhone) did not securely erase data.
  - This was changed in iOS 2.0.

http://www.ilounge.com/index.php/articles/comments/securely-erasing-an-iphone/

Slide 4

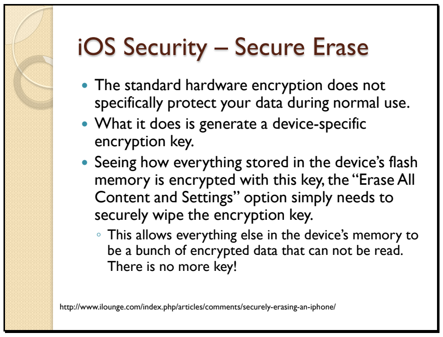


iOS Security – Secure Erase

- When iOS 2.0 came out, erasing data securely was done by doing a bit-by-bit wipe of the flash memory.
  - This took 1 – 3 hours depending on the device.
- When iOS 3.0 came out, apple had introduced hardware-Level encryption. Why?
  - This allowed a fast, secure wipe process.

http://www.ilounge.com/index.php/articles/comments/securely-erasing-an-iphone/

Slide 5

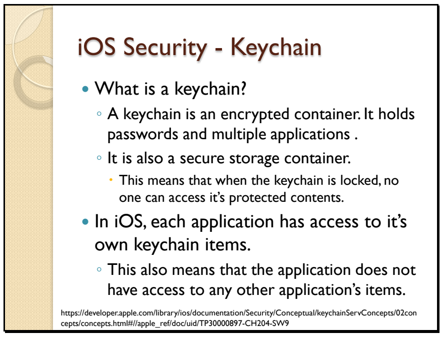


iOS Security – Secure Erase

- The standard hardware encryption does not specifically protect your data during normal use.
- What it does is generate a device-specific encryption key.
- Seeing how everything stored in the device’s flash memory is encrypted with this key, the “Erase All Content and Settings” option simply needs to securely wipe the encryption key.
  - This allows everything else in the device’s memory to be a bunch of encrypted data that can not be read. There is no more key!

http://www.ilounge.com/index.php/articles/comments/securely-erasing-an-iphone/

Slide 6

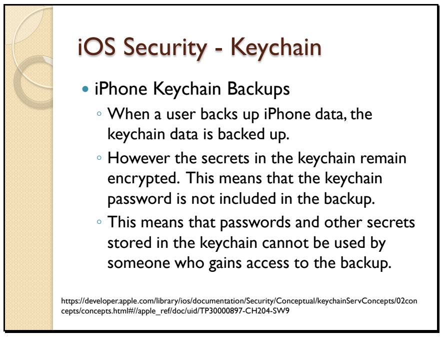


iOS Security - Keychain

- What is a keychain?
  - A keychain is an encrypted container. It holds passwords and multiple applications .
  - It is also a secure storage container.
    - This means that when the keychain is locked, no one can access it’s protected contents.
- In iOS, each application has access to it’s own keychain items.
  - This also means that the application does not have access to any other application’s items.

https://developer.apple.com/library/ios/documentation/Security/Conceptual/keychainServConcepts/02concepts/concepts.html#//apple_ref/doc/uid/TP30000897-CH204-SW9

Slide 7

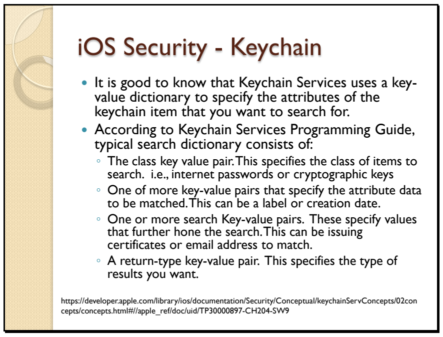


iOS Security - Keychain

- iPhone Keychain Backups
  - When a user backs up iPhone data, the keychain data is backed up.
  - However the secrets in the keychain remain encrypted. This means that the keychain password is not included in the backup.
  - This means that passwords and other secrets stored in the keychain cannot be used by someone who gains access to the backup.

https://developer.apple.com/library/ios/documentation/Security/Conceptual/keychainServConcepts/02concepts/concepts.html#//apple_ref/doc/uid/TP30000897-CH204-SW9

Slide 8

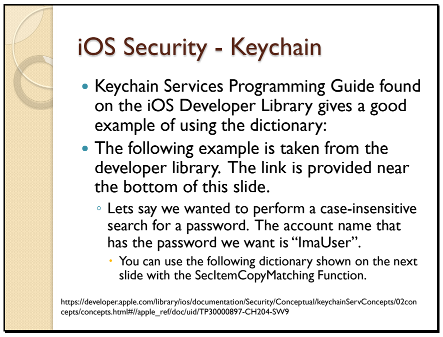


iOS Security - Keychain

- It is good to know that Keychain Services uses a key-value dictionary to specify the attributes of the keychain item that you want to search for.
- According to Keychain Services Programming Guide, typical search dictionary consists of:
  - The class key value pair.This specifies the class of items to search. i.e., internet passwords or cryptographic keys
  - One of more key-value pairs that specify the attribute data to be matched.This can be a label or creation date.
  - One or more search Key-value pairs. These specify values that further hone the search.This can be issuing certificates or email address to match.
  - A return-type key-value pair. This specifies the type of results you want.

https://developer.apple.com/library/ios/documentation/Security/Conceptual/keychainServConcepts/02concepts/concepts.html#//apple_ref/doc/uid/TP30000897-CH204-SW9

Slide 9

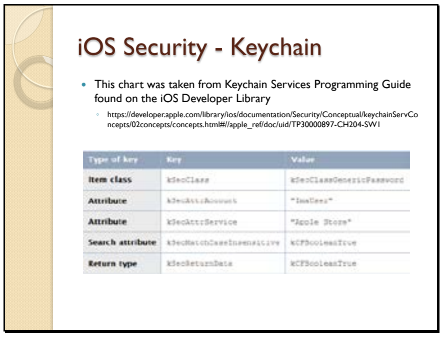


iOS Security - Keychain

- Keychain Services Programming Guide found on the iOS Developer Library gives a good example of using the dictionary:
- The following example is taken from the developer library. The link is provided near the bottom of this slide.
  - Lets say we wanted to perform a case-insensitive search for a password. The account name that has the password we want is "ImaUser".
    - You can use the following dictionary shown on the next slide with the SecItemCopyMatching Function.

https://developer.apple.com/library/ios/documentation/Security/Conceptual/keychainServConcepts/02concepts/concepts.html#//apple_ref/doc/uid/TP30000897-CH204-SW9

Slide 10

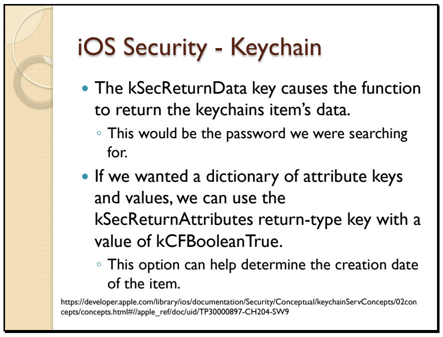


iOS Security - Keychain

- This chart was taken from Keychain Services Programming Guide found on the iOS Developer Library
  - https://developer.apple.com/library/ios/documentation/Security/Conceptual/keychainServConcepts/02concepts/concepts.html#//apple_ref/doc/uid/TP30000897-CH204-SW1

Type of key	Key	Value
Item class	kSecClass	kSecClassGenericPassword
Attribute	kSecAttrAccount	"ImaUser"
Attribute	kSecAttrService	"Apple Store"
Search attribute	kSecMatchCaseInsensitive	kCFBooleanTrue
Return type	kSecReturnData	kCFBooleanTrue

Slide 11

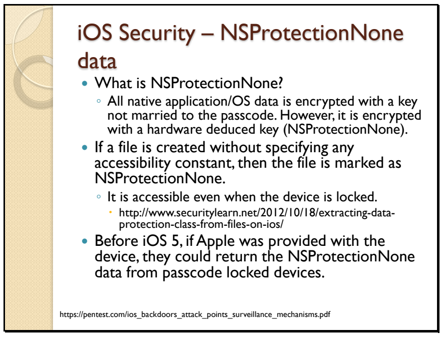


iOS Security - Keychain

- The kSecReturnData key causes the function to return the keychains item's data.
  - This would be the password we were searching for.
- If we wanted a dictionary of attribute keys and values, we can use the kSecReturnAttributes return-type key with a value of kCFBooleanTrue.
  - This option can help determine the creation date of the item.

https://developer.apple.com/library/ios/documentation/Security/Conceptual/keychainServConcepts/02concepts/concepts.html#//apple_ref/doc/uid/TP30000897-CH204-SW9

Slide 12

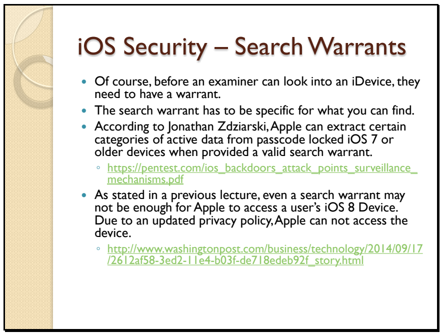


iOS Security – NSProtectionNone data

- What is NSProtectionNone?
  - All native application/OS data is encrypted with a key not married to the passcode. However, it is encrypted with a hardware deduced key (NSProtectionNone).
- If a file is created without specifying any accessibility constant, then the file is marked as NSProtectionNone.
  - It is accessible even when the device is locked.
    - http://www.securitylearn.net/2012/10/18/extracting-data-protection-class-from-files-on-ios/
- Before iOS 5, if Apple was provided with the device, they could return the NSProtectionNone data from passcode locked devices.

https://pentest.com/ios_backdoors_attack_points_surveillance_mechanisms.pdf

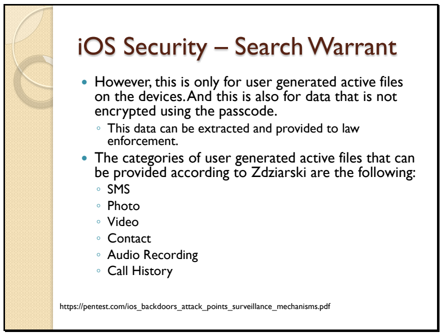
Slide 13



iOS Security – Search Warrants

- Of course, before an examiner can look into an iDevice, they need to have a warrant.
- The search warrant has to be specific for what you can find.
- According to Jonathan Zdziarski, Apple can extract certain categories of active data from passcode locked iOS 7 or older devices when provided a valid search warrant.
  - https://pentest.com/ios_backdoors_attack_points_surveillance_mechanisms.pdf
- As stated in a previous lecture, even a search warrant may not be enough for Apple to access a user's iOS 8 Device. Due to an updated privacy policy, Apple can not access the device.
  - http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html

Slide 14

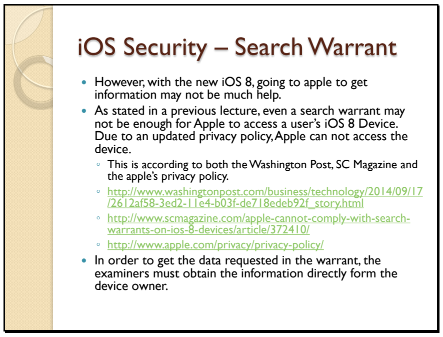


iOS Security – Search Warrant

- However, this is only for user generated active files on the devices. And this is also for data that is not encrypted using the passcode.
  - This data can be extracted and provided to law enforcement.
- The categories of user generated active files that can be provided according to Zdziarski are the following:
  - SMS
  - Photo
  - Video
  - Contact
  - Audio Recording
  - Call History

https://pentest.com/ios_backdoors_attack_points_surveillance_mechanisms.pdf

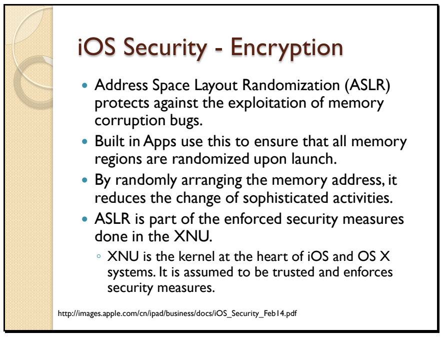
Slide 15



iOS Security – Search Warrant

- However, with the new iOS 8, going to apple to get information may not be much help.
- As stated in a previous lecture, even a search warrant may not be enough for Apple to access a user's iOS 8 Device. Due to an updated privacy policy, Apple can not access the device.
    - This is according to both the Washington Post, SC Magazine and the apple's privacy policy.
    - http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html
    - http://www.scmagazine.com/apple-cannot-comply-with-search-warrants-on-ios-8-devices/article/372410/
    - http://www.apple.com/privacy/privacy-policy/
- In order to get the data requested in the warrant, the examiners must obtain the information directly form the device owner.

Slide 16

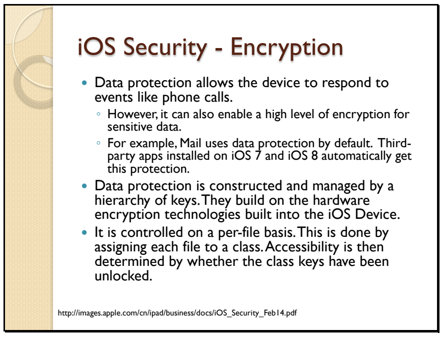


iOS Security - Encryption

- Address Space Layout Randomization (ASLR) protects against the exploitation of memory corruption bugs.
- Built in Apps use this to ensure that all memory regions are randomized upon launch.
- By randomly arranging the memory address, it reduces the change of sophisticated activities.
- ASLR is part of the enforced security measures done in the XNU.
    - XNU is the kernel at the heart of iOS and OS X systems. It is assumed to be trusted and enforces security measures.

http://images.apple.com/cn/ipad/business/docs/iOS_Security_Feb14.pdf

Slide 17

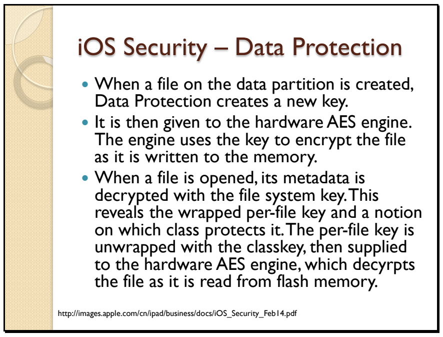


iOS Security - Encryption

- Data protection allows the device to respond to events like phone calls.
    - However, it can also enable a high level of encryption for sensitive data.
    - For example, Mail uses data protection by default. Third-party apps installed on iOS 7 and iOS 8 automatically get this protection.
- Data protection is constructed and managed by a hierarchy of keys. They build on the hardware encryption technologies built into the iOS Device.
- It is controlled on a per-file basis. This is done by assigning each file to a class. Accessibility is then determined by whether the class keys have been unlocked.

http://images.apple.com/cn/ipad/business/docs/iOS_Security_Feb14.pdf

Slide 18

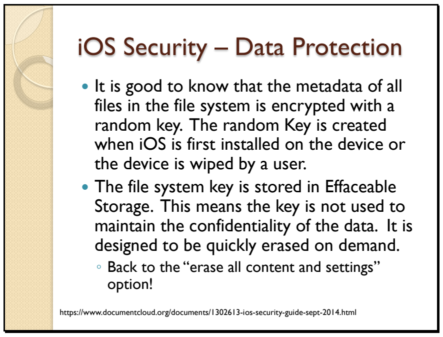


iOS Security – Data Protection

- When a file on the data partition is created, Data Protection creates a new key.
- It is then given to the hardware AES engine. The engine uses the key to encrypt the file as it is written to the memory.
- When a file is opened, its metadata is decrypted with the file system key. This reveals the wrapped per-file key and a notion on which class protects it. The per-file key is unwrapped with the classkey, then supplied to the hardware AES engine, which decyrpts the file as it is read from flash memory.

http://images.apple.com/cn/ipad/business/docs/iOS_Security_Feb14.pdf

Slide 19

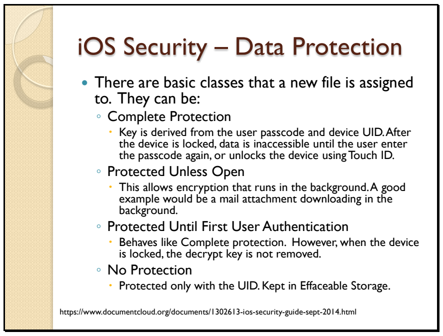


iOS Security – Data Protection

- It is good to know that the metadata of all files in the file system is encrypted with a random key. The random Key is created when iOS is first installed on the device or the device is wiped by a user.
- The file system key is stored in Effaceable Storage. This means the key is not used to maintain the confidentiality of the data. It is designed to be quickly erased on demand.
  - Back to the "erase all content and settings" option!

https://www.documentcloud.org/documents/1302613-ios-security-guide-sept-2014.html

Slide 20

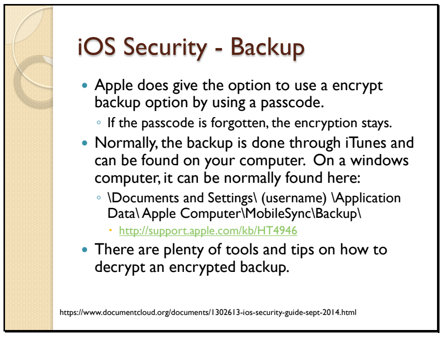


iOS Security – Data Protection

- There are basic classes that a new file is assigned to. They can be:
  - Complete Protection
    - Key is derived from the user passcode and device UID. After the device is locked, data is inaccessible until the user enter the passcode again, or unlocks the device using Touch ID.
  - Protected Unless Open
    - This allows encryption that runs in the background. A good example would be a mail attachment downloading in the background.
  - Protected Until First User Authentication
    - Behaves like Complete protection. However, when the device is locked, the decrypt key is not removed.
  - No Protection
    - Protected only with the UID. Kept in Effaceable Storage.

https://www.documentcloud.org/documents/1302613-ios-security-guide-sept-2014.html

Slide 21

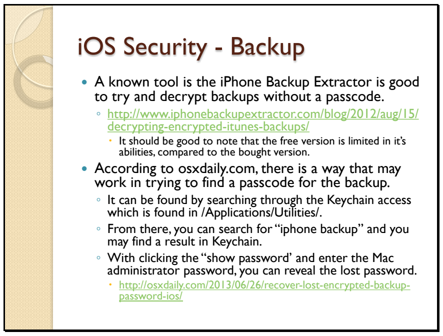


iOS Security - Backup

- Apple does give the option to use a encrypt backup option by using a passcode.
  - If the passcode is forgotten, the encryption stays.
- Normally, the backup is done through iTunes and can be found on your computer. On a windows computer, it can be normally found here:
  - \Documents and Settings\ (username) \Application Data\ Apple Computer\MobileSync\Backup\
    - http://support.apple.com/kb/HT4946
- There are plenty of tools and tips on how to decrypt an encrypted backup.

https://www.documentcloud.org/documents/1302613-ios-security-guide-sept-2014.html

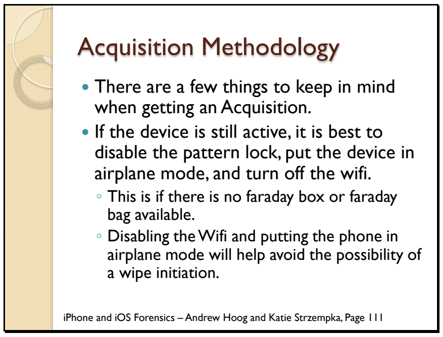
Slide 22



iOS Security - Backup

- A known tool is the iPhone Backup Extractor is good to try and decrypt backups without a passcode.
  - http://www.iphonebackupextractor.com/blog/2012/aug/15/decrypting-encrypted-itunes-backups/
    - It should be good to note that the free version is limited in it's abilities, compared to the bought version.
- According to osxdaily.com, there is a way that may work in trying to find a passcode for the backup.
  - It can be found by searching through the Keychain access which is found in /Applications/Utilities/.
  - From there, you can search for "iphone backup" and you may find a result in Keychain.
  - With clicking the "show password' and enter the Mac administrator password, you can reveal the lost password.
    - http://osxdaily.com/2013/06/26/recover-lost-encrypted-backup-password-ios/

Slide 23

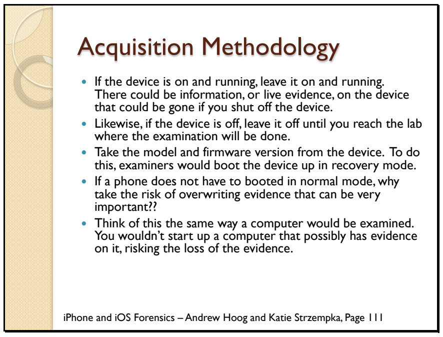


Acquisition Methodology

- There are a few things to keep in mind when getting an Acquisition.
- If the device is still active, it is best to disable the pattern lock, put the device in airplane mode, and turn off the wifi.
  - This is if there is no faraday box or faraday bag available.
  - Disabling the Wifi and putting the phone in airplane mode will help avoid the possibility of a wipe initiation.

iPhone and iOS Forensics – Andrew Hoog and Katie Strzempka, Page 111

Slide 24



Acquisition Methodology

- If the device is on and running, leave it on and running. There could be information, or live evidence, on the device that could be gone if you shut off the device.
- Likewise, if the device is off, leave it off until you reach the lab where the examination will be done.
- Take the model and firmware version from the device. To do this, examiners would boot the device up in recovery mode.
- If a phone does not have to booted in normal mode, why take the risk of overwriting evidence that can be very important??
- Think of this the same way a computer would be examined. You wouldn't start up a computer that possibly has evidence on it, risking the loss of the evidence.

iPhone and iOS Forensics – Andrew Hoog and Katie Strzempka, Page 111

Chapter 9- Week Eight: Jailbreaking

This week's lecture introduces students to Jailbreaking. When a user jailbreaks their device, it means that the device allows the user to modify the operating system. This allows the user to add unofficial application installers on the device to install and use third party applications. This is one of the reasons a user jailbreaks their device. With iPhones, jailbreaking may be used so the phone can work with a different carrier. Jailbreaking also lets the user to manipulate the device. An example of this manipulation is changing the user interface, or changing the application icons. This information can be found on idownloadblog.com.[20]

Not only does jailbreaking allows users to manipulate the look of the device, but it can also allow tweaks, modifications and extensions to be applied. An example of a tweak that can be applied to a jailbroken device is to allow 5 icons on an iPhone instead

[20] (iDownloadBlog, 2014)

of the standard 4. The worst thing that can happen when jailbreaking a device, it can become unresponsive. There is a fix to this, which is to restore the device's firmware back to the stock version. Updating the iOS in a jailbroken device can be a little tricky. If the update is done, it will overwrite the jailbreak.

A big question students may ask about jailbreaking would be if it was legal or legal. Jailbreaking became legal in the USA in 2012[21]. However, jailbreaking an iDevice may void the warranty it has. The warranty on an iDevice becomes void the minute that the person jailbreaks the device. [22] According to idownloadblog.com, there is a small work around for this. If the device is reset to factory settings in iTunes, the device is reset to how the user bought it.

Students are then introduced to the three ways that a device, or iPhone, can be jailbroken. These ways are untethered, semitethered and tethered. The most desirable jailbreak is to be untethered. This allows the user to reboot the device with no consequences. Semitethered does not allow a reboot without some problems with the applications or tweaks. To get the device to function properly, a tethered boot must be performed. A tethered is the least desirable of the three. A reboot must be done with a tethered boot with access to a computer. [23] Firmware is discussed briefly, due to the firmware slice being replaced with a hacked firmware. The hacked firmware allows third party applications to be installed on the device. To find the firmware, one can go to www.iclarified.com.[24]

Being that this is a forensics class for iOS devices, acquisition on these types of devices are discussed. It is stressed to the students these acquisitions need to be very

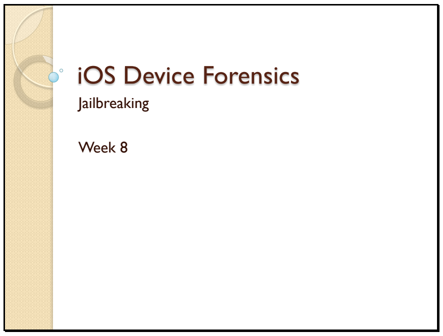
[21] (iDownloadBlog, 2014)
[22] (Apple, 2014)
[23] (iDownloadBlog, 2011)
[24] (iClarified, 2008)

careful. Andrew Hoog discusses in his book that there are three steps to acquire the device: create a wireless network, remotely connect to the device and finally image the device. [25]

The wireless network needs to be static on the forensic workstation, making sure that the IP address will not change. The examiner then will connect to the device over secure shell (SSH), which is a known cryptographic network protocol. The device is finally imaged by using a program called netcat. Netcat will create a tunnel that allows the connected devices to communicate. By initiating a dd[26] command, the workstations desktop will create a file with the image on it. It is mentioned that this is one method to acquire an image, but the risk is still high for loosing data due to the device being jailbroken.

PowerPoint Presentation for Week Eight

Slide 1

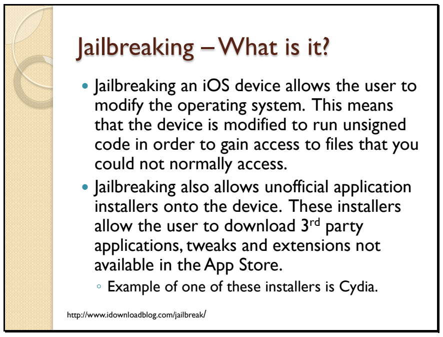


iOS Device Forensics

Jailbreaking

Week 8

Slide 2



Jailbreaking – What is it?

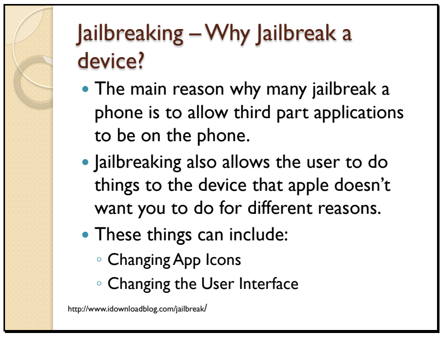
- Jailbreaking an iOS device allows the user to modify the operating system. This means that the device is modified to run unsigned code in order to gain access to files that you could not normally access.
- Jailbreaking also allows unofficial application installers onto the device. These installers allow the user to download 3rd party applications, tweaks and extensions not available in the App Store.
    - Example of one of these installers is Cydia.

http://www.idownloadblog.com/jailbreak/

[25] (Hoog & Strzempka, Acquisitons: Jailbroken Device, 2011)

[26] is a way to copy and convert files and can be accessed through SSH

Slide 3

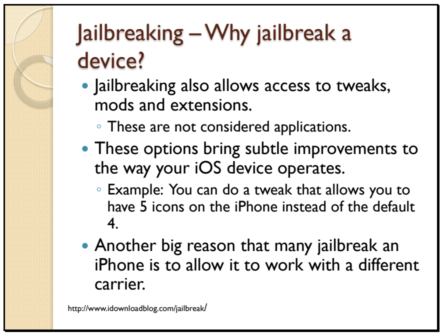


Jailbreaking – Why Jailbreak a device?

- The main reason why many jailbreak a phone is to allow third part applications to be on the phone.
- Jailbreaking also allows the user to do things to the device that apple doesn't want you to do for different reasons.
- These things can include:
  - Changing App Icons
  - Changing the User Interface

http://www.idownloadblog.com/jailbreak/

Slide 4

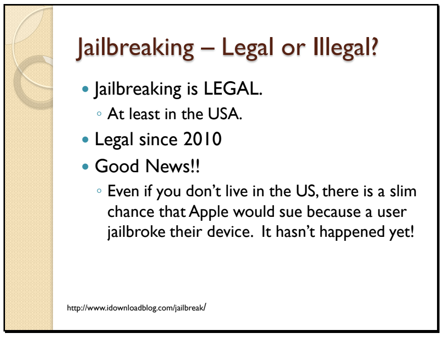


Jailbreaking – Why jailbreak a device?

- Jailbreaking also allows access to tweaks, mods and extensions.
  - These are not considered applications.
- These options bring subtle improvements to the way your iOS device operates.
  - Example: You can do a tweak that allows you to have 5 icons on the iPhone instead of the default 4.
- Another big reason that many jailbreak an iPhone is to allow it to work with a different carrier.

http://www.idownloadblog.com/jailbreak/

Slide 5

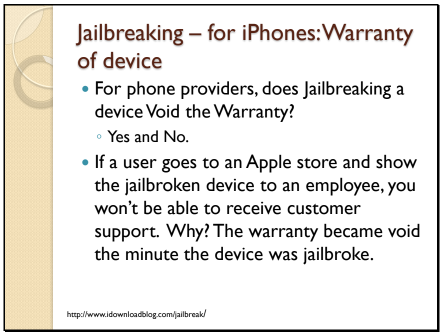


Jailbreaking – Legal or Illegal?

- Jailbreaking is LEGAL.
  - At least in the USA.
- Legal since 2010
- Good News!!
  - Even if you don't live in the US, there is a slim chance that Apple would sue because a user jailbroke their device. It hasn't happened yet!

http://www.idownloadblog.com/jailbreak/

Slide 6

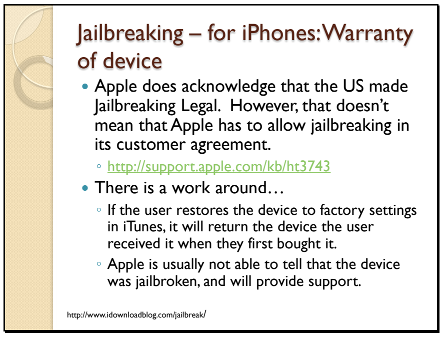


Jailbreaking – for iPhones: Warranty of device

- For phone providers, does Jailbreaking a device Void the Warranty?
  - Yes and No.
- If a user goes to an Apple store and show the jailbroken device to an employee, you won't be able to receive customer support. Why? The warranty became void the minute the device was jailbroke.

http://www.idownloadblog.com/jailbreak/

Slide 7

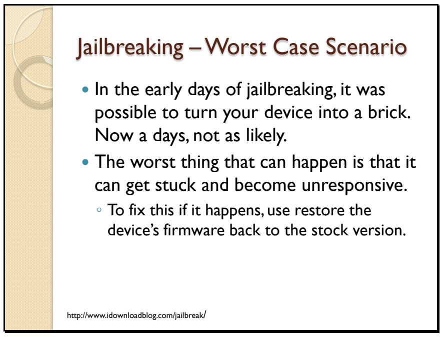


Jailbreaking – for iPhones: Warranty of device

- Apple does acknowledge that the US made Jailbreaking Legal. However, that doesn't mean that Apple has to allow jailbreaking in its customer agreement.
  - http://support.apple.com/kb/ht3743
- There is a work around…
  - If the user restores the device to factory settings in iTunes, it will return the device the user received it when they first bought it.
  - Apple is usually not able to tell that the device was jailbroken, and will provide support.

http://www.idownloadblog.com/jailbreak/

Slide 8

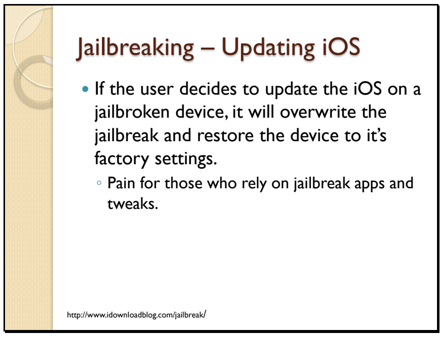


Jailbreaking – Worst Case Scenario

- In the early days of jailbreaking, it was possible to turn your device into a brick. Now a days, not as likely.
- The worst thing that can happen is that it can get stuck and become unresponsive.
  - To fix this if it happens, use restore the device's firmware back to the stock version.

http://www.idownloadblog.com/jailbreak/

Slide 9

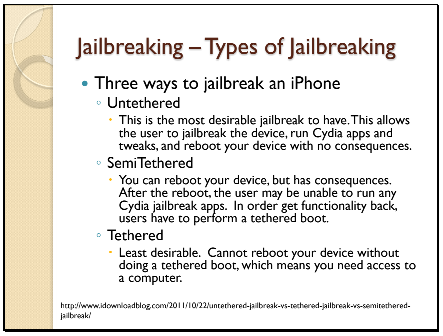


Jailbreaking – Updating iOS

- If the user decides to update the iOS on a jailbroken device, it will overwrite the jailbreak and restore the device to it's factory settings.
  - Pain for those who rely on jailbreak apps and tweaks.

http://www.idownloadblog.com/jailbreak/

Slide 10

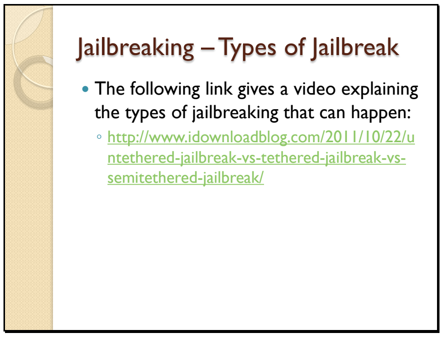


Jailbreaking – Types of Jailbreaking

- Three ways to jailbreak an iPhone
  - Untethered
    - This is the most desirable jailbreak to have. This allows the user to jailbreak the device, run Cydia apps and tweaks, and reboot your device with no consequences.
  - SemiTethered
    - You can reboot your device, but has consequences. After the reboot, the user may be unable to run any Cydia jailbreak apps. In order get functionality back, users have to perform a tethered boot.
  - Tethered
    - Least desirable. Cannot reboot your device without doing a tethered boot, which means you need access to a computer.

http://www.idownloadblog.com/2011/10/22/untethered-jailbreak-vs-tethered-jailbreak-vs-semitethered-jailbreak/

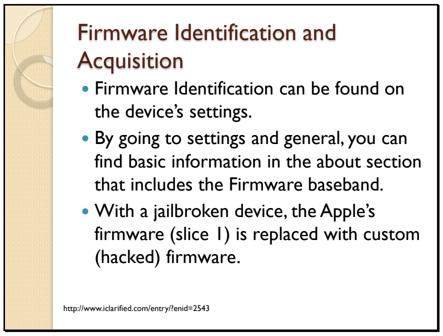
Slide 11



Jailbreaking – Types of Jailbreak

- The following link gives a video explaining the types of jailbreaking that can happen:
  - http://www.idownloadblog.com/2011/10/22/untethered-jailbreak-vs-tethered-jailbreak-vs-semitethered-jailbreak/

Slide 12

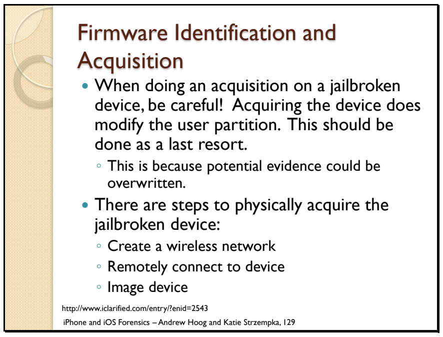


Firmware Identification and Acquisition

- Firmware Identification can be found on the device's settings.
- By going to settings and general, you can find basic information in the about section that includes the Firmware baseband.
- With a jailbroken device, the Apple's firmware (slice 1) is replaced with custom (hacked) firmware.

http://www.iclarified.com/entry/?enid=2543

Slide 13

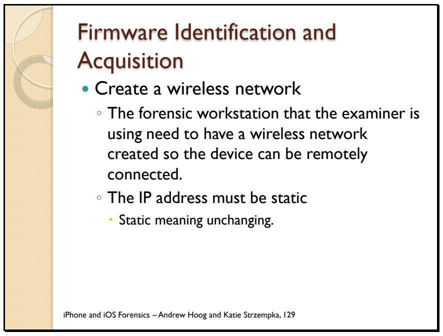


Firmware Identification and Acquisition

- When doing an acquisition on a jailbroken device, be careful! Acquiring the device does modify the user partition. This should be done as a last resort.
  - This is because potential evidence could be overwritten.
- There are steps to physically acquire the jailbroken device:
  - Create a wireless network
  - Remotely connect to device
  - Image device

http://www.iclarified.com/entry/?enid=2543
iPhone and iOS Forensics – Andrew Hoog and Katie Strzempka, 129

Slide 14

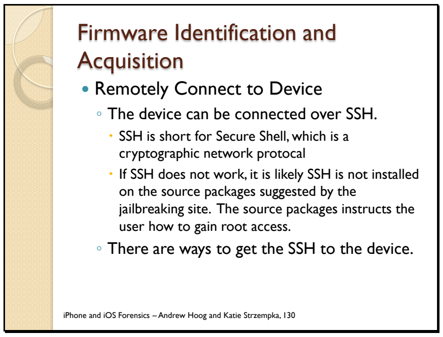


Firmware Identification and Acquisition

- Create a wireless network
  - The forensic workstation that the examiner is using need to have a wireless network created so the device can be remotely connected.
  - The IP address must be static
    - Static meaning unchanging.

iPhone and iOS Forensics – Andrew Hoog and Katie Strzempka, 129

Slide 15

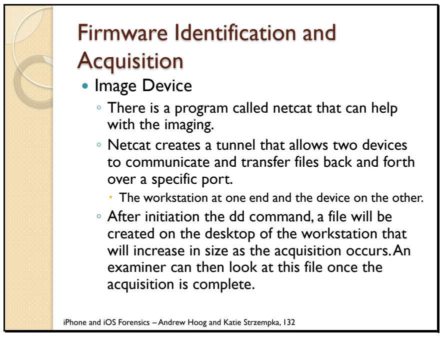


Firmware Identification and Acquisition

- Remotely Connect to Device
  - The device can be connected over SSH.
    - SSH is short for Secure Shell, which is a cryptographic network protocal
    - If SSH does not work, it is likely SSH is not installed on the source packages suggested by the jailbreaking site. The source packages instructs the user how to gain root access.
  - There are ways to get the SSH to the device.

iPhone and iOS Forensics – Andrew Hoog and Katie Strzempka, 130

Slide 16

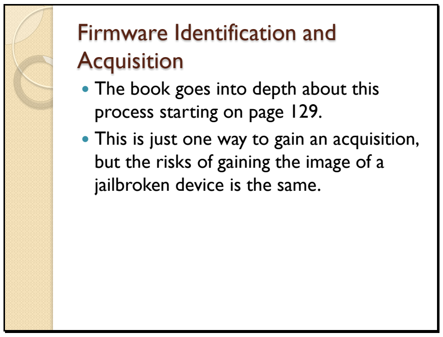


Firmware Identification and Acquisition

- Image Device
  - There is a program called netcat that can help with the imaging.
  - Netcat creates a tunnel that allows two devices to communicate and transfer files back and forth over a specific port.
    - The workstation at one end and the device on the other.
  - After initiation the dd command, a file will be created on the desktop of the workstation that will increase in size as the acquisition occurs. An examiner can then look at this file once the acquisition is complete.

iPhone and iOS Forensics – Andrew Hoog and Katie Strzempka, 132

Slide 17



Firmware Identification and Acquisition

- The book goes into depth about this process starting on page 129.
- This is just one way to gain an acquisition, but the risks of gaining the image of a jailbroken device is the same.

Chapter 10 – Week Nine: Physical Acquisition

Week nine starts off with non-forensically sound methods for physical acquisitions. Jailbreaking, which was discussed in the previous week's presentation, is considered a non-forensically sound method. This is because the examiners can tamper with the user data.

Secure Shell (SSH), dd and netcat are considered non-forensically sound as well. These methods were discussed in the previous week as well. SSH allows examiners to access the files stored on the device, making this method non-forensically sound.[27] In UNIX, dd is a way to copy and convert files and can be accessed through SSH. One has to be careful when using dd because if you access the wrong file, the device can be damaged. [28] This makes it non-forensically sound as well. Netcat is non-forensically sound due to communicating over a port that could be secure or unsecure.

There are forensically sound methods for doing an acquisition. One well known method is the Zdziarski method. Jonathon Zdziarski was a former researcher for McAfee, Inc.[29]. The Zdziarski method is not so much an application, but a toolkit that allows acquisitions to occur. What this method does is allows the examiner to execute a bit-by-bit copy of the device's user partition. The partition gained, which is read-only, stays isolated from the partition containing the users data. Because the user's data isn't violated, the method is sound.

This method may seem familiar to the jailbreaking method. There are differences between the two. The Zdziarski method caters more to forensic recovery. It deals with read-only partitions on the device. Jailbreaking, however, focuses more on hacking into the device. Hacking into the device might interfere with the user's data, which is not good.

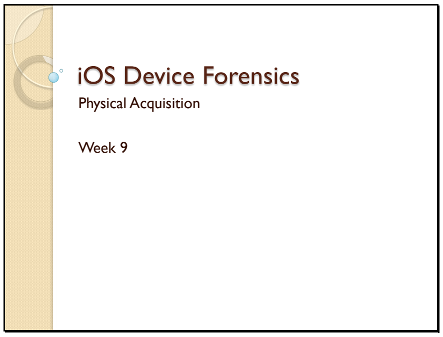
Another forensically sound method that is mentioned is Lantern Lite/Imager.[30] [31] This is a free software that uses bootloader from the jailbreak took redsn0w. This software will then obtain a physical image of an iPhone 4. Sadly, this tool is known for its work with iPhone 4, and not with any other device. This is forensically sound because

[27] (Lee, 2011)
[28] (Rubin, MacKenzie, & Kemp, 2010)
[29] (Hoog & Strzempka, Acquisitions: Zdziarski Technique, 2011)
[30] (Whitfield, 2012)
[31] (Cavanaugh, 2012)

it takes advantage of DFU mode. It is mentioned that it can be compared to software that is used by police, Katana Lantern.

PowerPoint Presentation for Week Nine

Slide 1

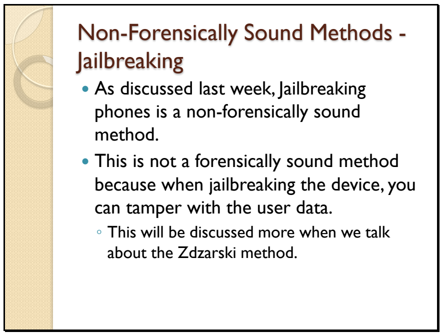


iOS Device Forensics

Physical Acquisition

Week 9

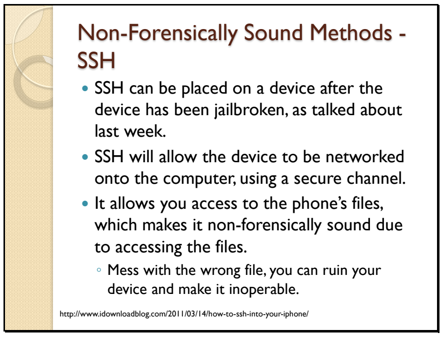
Slide 2



Non-Forensically Sound Methods - Jailbreaking

- As discussed last week, Jailbreaking phones is a non-forensically sound method.
- This is not a forensically sound method because when jailbreaking the device, you can tamper with the user data.
  - This will be discussed more when we talk about the Zdzarski method.

Slide 3

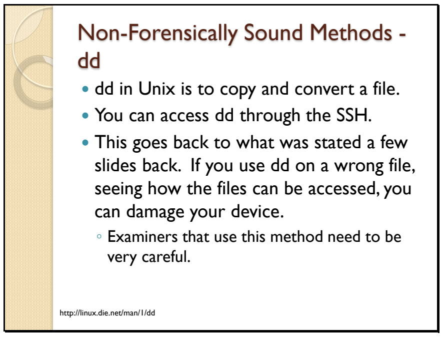


Non-Forensically Sound Methods - SSH

- SSH can be placed on a device after the device has been jailbroken, as talked about last week.
- SSH will allow the device to be networked onto the computer, using a secure channel.
- It allows you access to the phone's files, which makes it non-forensically sound due to accessing the files.
  - Mess with the wrong file, you can ruin your device and make it inoperable.

http://www.idownloadblog.com/2011/03/14/how-to-ssh-into-your-iphone/

Slide 4

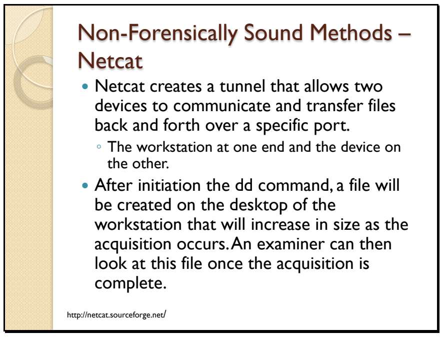


Non-Forensically Sound Methods - dd

- dd in Unix is to copy and convert a file.
- You can access dd through the SSH.
- This goes back to what was stated a few slides back. If you use dd on a wrong file, seeing how the files can be accessed, you can damage your device.
  - Examiners that use this method need to be very careful.

http://linux.die.net/man/1/dd

Slide 5

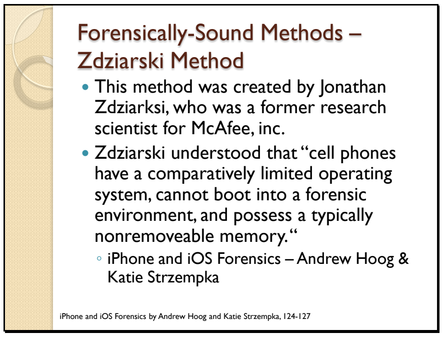


Non-Forensically Sound Methods – Netcat

- Netcat creates a tunnel that allows two devices to communicate and transfer files back and forth over a specific port.
  - The workstation at one end and the device on the other.
- After initiation the dd command, a file will be created on the desktop of the workstation that will increase in size as the acquisition occurs. An examiner can then look at this file once the acquisition is complete.

http://netcat.sourceforge.net/

Slide 6

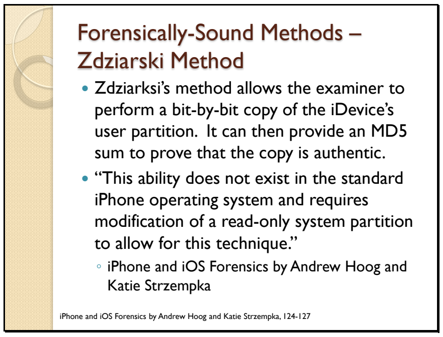


Forensically-Sound Methods – Zdziarski Method

- This method was created by Jonathan Zdziarksi, who was a former research scientist for McAfee, inc.
- Zdziarski understood that "cell phones have a comparatively limited operating system, cannot boot into a forensic environment, and possess a typically nonremoveable memory."
  - iPhone and iOS Forensics – Andrew Hoog & Katie Strzempka

iPhone and iOS Forensics by Andrew Hoog and Katie Strzempka, 124-127

Slide 7

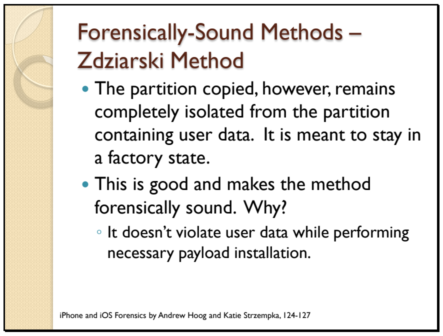


Forensically-Sound Methods – Zdziarski Method

- Zdziarksi's method allows the examiner to perform a bit-by-bit copy of the iDevice's user partition. It can then provide an MD5 sum to prove that the copy is authentic.
- "This ability does not exist in the standard iPhone operating system and requires modification of a read-only system partition to allow for this technique."
  - iPhone and iOS Forensics by Andrew Hoog and Katie Strzempka

iPhone and iOS Forensics by Andrew Hoog and Katie Strzempka, 124-127

Slide 8

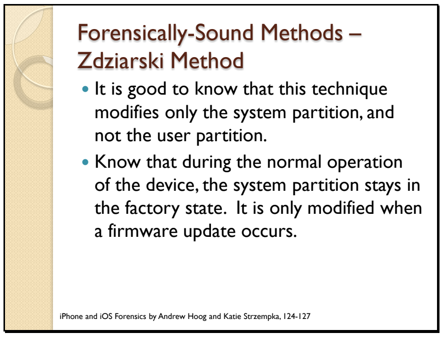


Forensically-Sound Methods – Zdziarski Method

- The partition copied, however, remains completely isolated from the partition containing user data. It is meant to stay in a factory state.
- This is good and makes the method forensically sound. Why?
  - It doesn't violate user data while performing necessary payload installation.

iPhone and iOS Forensics by Andrew Hoog and Katie Strzempka, 124-127

Slide 9

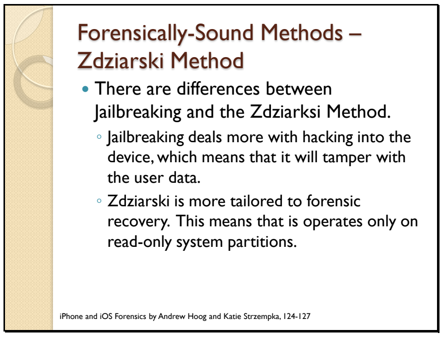


Forensically-Sound Methods – Zdziarski Method

- It is good to know that this technique modifies only the system partition, and not the user partition.
- Know that during the normal operation of the device, the system partition stays in the factory state. It is only modified when a firmware update occurs.

iPhone and iOS Forensics by Andrew Hoog and Katie Strzempka, 124-127

Slide 10

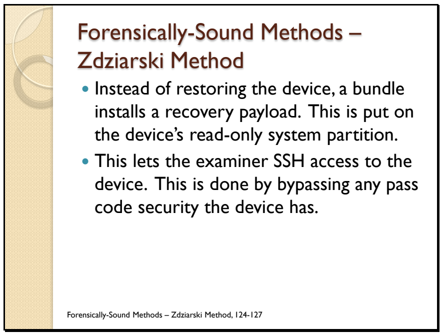


Forensically-Sound Methods – Zdziarski Method

- There are differences between Jailbreaking and the Zdziarksi Method.
  - Jailbreaking deals more with hacking into the device, which means that it will tamper with the user data.
  - Zdziarski is more tailored to forensic recovery. This means that is operates only on read-only system partitions.

iPhone and iOS Forensics by Andrew Hoog and Katie Strzempka, 124-127

Slide 11

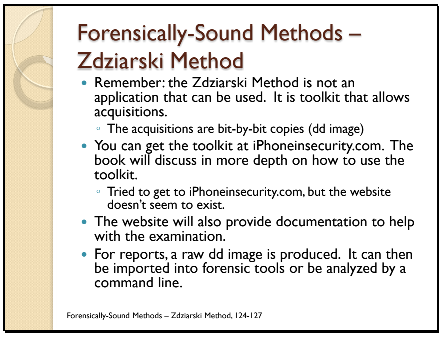


Forensically-Sound Methods – Zdziarski Method

- Instead of restoring the device, a bundle installs a recovery payload. This is put on the device's read-only system partition.
- This lets the examiner SSH access to the device. This is done by bypassing any pass code security the device has.

Forensically-Sound Methods – Zdziarski Method, 124-127

Slide 12

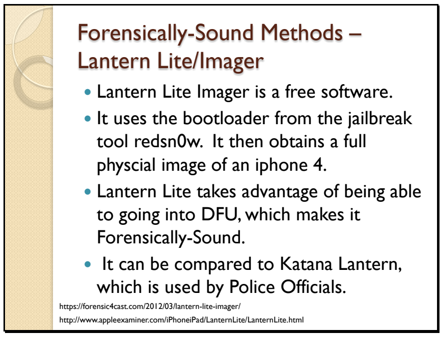


Forensically-Sound Methods – Zdziarski Method

- Remember: the Zdziarski Method is not an application that can be used. It is toolkit that allows acquisitions.
  - The acquisitions are bit-by-bit copies (dd image)
- You can get the toolkit at iPhoneinsecurity.com. The book will discuss in more depth on how to use the toolkit.
  - Tried to get to iPhoneinsecurity.com, but the website doesn't seem to exist.
- The website will also provide documentation to help with the examination.
- For reports, a raw dd image is produced. It can then be imported into forensic tools or be analyzed by a command line.

Forensically-Sound Methods – Zdziarski Method, 124-127

Slide 13



Forensically-Sound Methods – Lantern Lite/Imager

- Lantern Lite Imager is a free software.
- It uses the bootloader from the jailbreak tool redsn0w. It then obtains a full physcial image of an iphone 4.
- Lantern Lite takes advantage of being able to going into DFU, which makes it Forensically-Sound.
- It can be compared to Katana Lantern, which is used by Police Officials.

https://forensic4cast.com/2012/03/lantern-lite-imager/
http://www.appleexaminer.com/iPhoneiPad/LanternLite/LanternLite.html

Chapter 11 – Week Ten: Advanced iOS Security

In week ten, the topic for the presentation is advanced iOS security and advanced logical acquisitions. The first thing covered in this area is file_relay, which deals with backdoors in iOS. Zdziarski had done research on this, which can be found in his own presentation found on his website[32]. He found that file_relay helps examiners bypass the backup encryption found on iTunes. Zdziarski believes that this is the biggest area of intelligence on the device. File_Relay can be used to gain access to personal data onteh device. This data can be email and Facebook accounts, as well as GPS logs, Photos and User Databases. User databases can be very useful because it contains short message service (SMS) database, which are also text messages, calendars and the address book.

Next in advanced logical acquisitions is Pairing Authentication, which uses lockdownd. Lockdownd is just a daemon that provides system information to clients. To understand this, one has to understand pairing. Pairing happens when you give permission for a device to access the other device. For example, whenever a person plugs their iDevice into a computer, the user allows the computer to access the device. This is a pairing. According to Zdziarski, Juice Jacking can be used to establish a pairing. Juice Jacking, according to howtogeek.com, Juice Jacking is “leveraging the USB data/power

[32] (Zdziarski, 2014)

cable to illegitimately access the phone's data and/or inject malicious code onto the device."[33] By the definition provided, this can be a bad thing.

This can also bypass the backup encryption. Another note about Pairing Authentication to make is that all of the lockdownd protocols have been documented in the libimobiledevice project[34]. Libimobiledevice is a cross-platform softare protocol library. It provides tools to communicate with iOS devices. The downside to this, however, is that its services have not been looked at since its creation in 2009.

Packet sniffers are on iDevices, and are active on every iOS device, under com.apple.mobile.pcapd[35]. Sadly, there is no indicator to the user that this is running. The big question, then, is why are packet sniffers on iOS Devices? There are many theories as to why they are present. One such theory is so that developers are testing their applications. Zdziarski slightly debunks this because the sniffers are enabled on devices on non-developer mode. Apple's reasoning for having packet sniffers on the device is to help with troubleshooting and diagnosing issues with applications. With the new iOS 8, this ability is restricted to USB interface. Even through there is some controversy on this, it is still useful to know for examiners, so they could use packet sniffers to their advantage.

The last thing that advanced logical acquisition talks about is house_arrest. Apple states that house_arrest is used by iTunes to transfer documents to and from the device.[36] Zdziarksi, however, believes that it is used to copy documents to and from third party application. This allows access to the preference folders. The preference folders can be

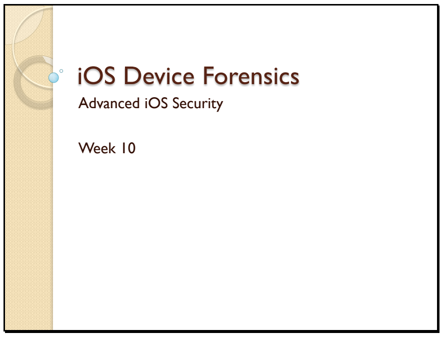
[33] (Fitzpatrick, 2013)
[34] (LibiMobileDevice, 2009)
[35] (Apple, 2014)
[36] (Apple, 2014)

useful because it provides storage for Facebook and photos. Not only this, but house_arrest can assist in recovering deleted messages.

Theories as to why these methods exist are discussed in the end of the presentation, as well as Zdziarski explaining why they are not viable. For instance, a theory is that it is used for developers for debugging. Zdziarski states that developers do not need to bypass backup encryption and do not need to access sensitive content in order to debug.[37]

PowerPoint Presentation for Week Ten

Slide 1

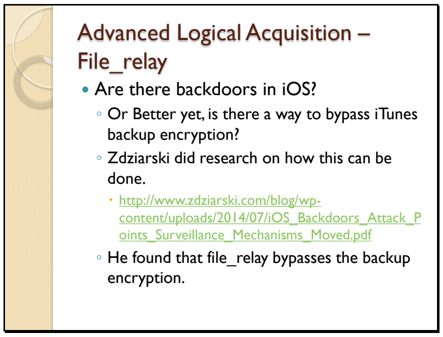


iOS Device Forensics

Advanced iOS Security

Week 10

Slide 2

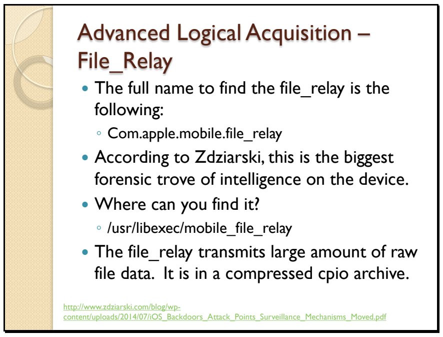


Advanced Logical Acquisition – File_relay

- Are there backdoors in iOS?
  - Or Better yet, is there a way to bypass iTunes backup encryption?
  - Zdziarski did research on how this can be done.
    - http://www.zdziarski.com/blog/wp-content/uploads/2014/07/iOS_Backdoors_Attack_Points_Surveillance_Mechanisms_Moved.pdf
  - He found that file_relay bypasses the backup encryption.

[37] (Zdziarski, 2014)

Slide 3

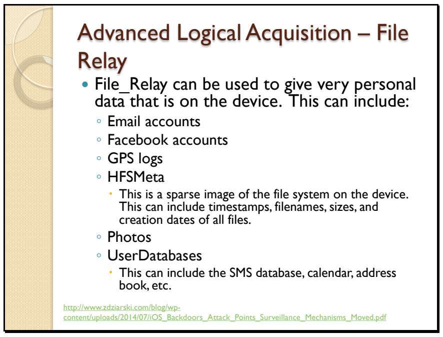


Advanced Logical Acquisition – File_Relay

- The full name to find the file_relay is the following:
  - Com.apple.mobile.file_relay
- According to Zdziarski, this is the biggest forensic trove of intelligence on the device.
- Where can you find it?
  - /usr/libexec/mobile_file_relay
- The file_relay transmits large amount of raw file data. It is in a compressed cpio archive.

http://www.zdziarski.com/blog/wp-content/uploads/2014/07/iOS_Backdoors_Attack_Points_Surveillance_Mechanisms_Moved.pdf

Slide 4

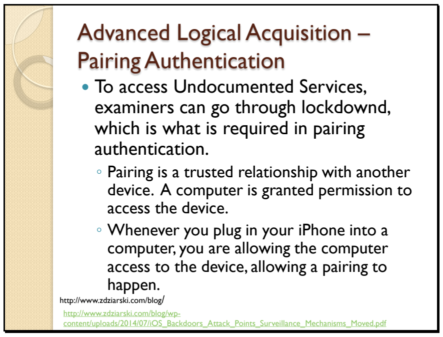


Advanced Logical Acquisition – File Relay

- File_Relay can be used to give very personal data that is on the device. This can include:
  - Email accounts
  - Facebook accounts
  - GPS logs
  - HFSMeta
    - This is a sparse image of the file system on the device. This can include timestamps, filenames, sizes, and creation dates of all files.
  - Photos
  - UserDatabases
    - This can include the SMS database, calendar, address book, etc.

http://www.zdziarski.com/blog/wp-content/uploads/2014/07/iOS_Backdoors_Attack_Points_Surveillance_Mechanisms_Moved.pdf

Slide 5



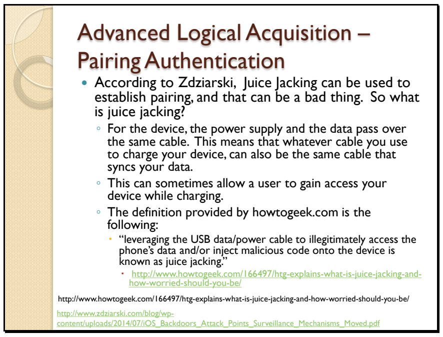
Advanced Logical Acquisition – Pairing Authentication

- To access Undocumented Services, examiners can go through lockdownd, which is what is required in pairing authentication.
  - Pairing is a trusted relationship with another device. A computer is granted permission to access the device.
  - Whenever you plug in your iPhone into a computer, you are allowing the computer access to the device, allowing a pairing to happen.

http://www.zdziarski.com/blog/

http://www.zdziarski.com/blog/wp-content/uploads/2014/07/iOS_Backdoors_Attack_Points_Surveillance_Mechanisms_Moved.pdf

Slide 6



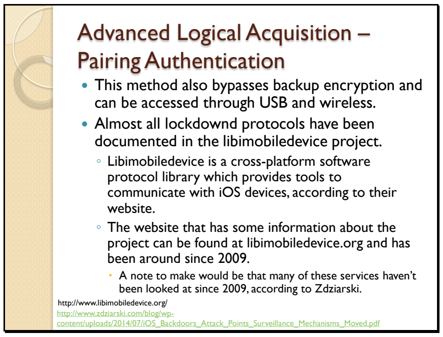
Advanced Logical Acquisition – Pairing Authentication

- According to Zdziarski, Juice Jacking can be used to establish pairing, and that can be a bad thing. So what is juice jacking?
  - For the device, the power supply and the data pass over the same cable. This means that whatever cable you use to charge your device, can also be the same cable that syncs your data.
  - This can sometimes allow a user to gain access your device while charging.
  - The definition provided by howtogeek.com is the following:
    - "leveraging the USB data/power cable to illegitimately access the phone's data and/or inject malicious code onto the device is known as juice jacking."
      - http://www.howtogeek.com/166497/htg-explains-what-is-juice-jacking-and-how-worried-should-you-be/

http://www.howtogeek.com/166497/htg-explains-what-is-juice-jacking-and-how-worried-should-you-be/

http://www.zdziarski.com/blog/wp-content/uploads/2014/07/iOS_Backdoors_Attack_Points_Surveillance_Mechanisms_Moved.pdf

Slide 7

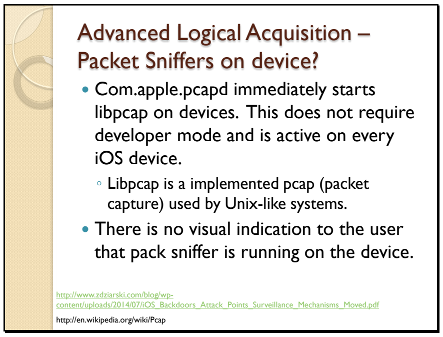


Advanced Logical Acquisition – Pairing Authentication

- This method also bypasses backup encryption and can be accessed through USB and wireless.
- Almost all lockdownd protocols have been documented in the libimobiledevice project.
  - Libimobiledevice is a cross-platform software protocol library which provides tools to communicate with iOS devices, according to their website.
  - The website that has some information about the project can be found at libimobiledevice.org and has been around since 2009.
    - A note to make would be that many of these services haven't been looked at since 2009, according to Zdziarski.

http://www.libimobiledevice.org/
http://www.zdziarski.com/blog/wp-content/uploads/2014/07/iOS_Backdoors_Attack_Points_Surveillance_Mechanisms_Moved.pdf

Slide 8

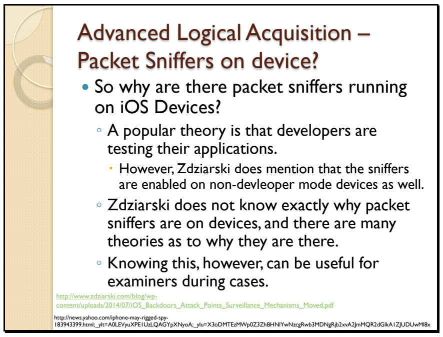


Advanced Logical Acquisition – Packet Sniffers on device?

- Com.apple.pcapd immediately starts libpcap on devices. This does not require developer mode and is active on every iOS device.
  - Libpcap is a implemented pcap (packet capture) used by Unix-like systems.
- There is no visual indication to the user that pack sniffer is running on the device.

http://www.zdziarski.com/blog/wp-content/uploads/2014/07/iOS_Backdoors_Attack_Points_Surveillance_Mechanisms_Moved.pdf
http://en.wikipedia.org/wiki/Pcap

Slide 9

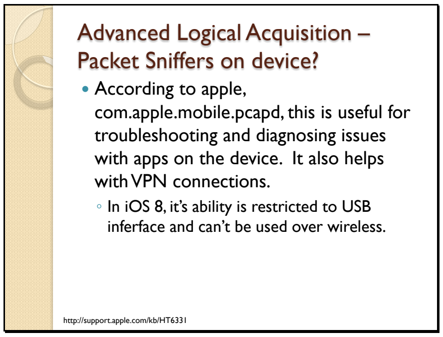


Advanced Logical Acquisition – Packet Sniffers on device?

- So why are there packet sniffers running on iOS Devices?
  - A popular theory is that developers are testing their applications.
    - However, Zdziarski does mention that the sniffers are enabled on non-devleoper mode devices as well.
  - Zdziarski does not know exactly why packet sniffers are on devices, and there are many theories as to why they are there.
  - Knowing this, however, can be useful for examiners during cases.

http://www.zdziarski.com/blog/wp-content/uploads/2014/07/iOS_Backdoors_Attack_Points_Surveillance_Mechanisms_Moved.pdf
http://news.yahoo.com/iphone-may-rigged-spy-183943399.html;_ylt=A0LEVyuXPE1UzLQAGYpXNyoA;_ylu=X3oDMTEzMWp0Z3ZhBHNlYwNzcgRwb3MDNgRjb2xvA2JmMQR2dGlkA1ZJUDUwMl8x

Slide 10

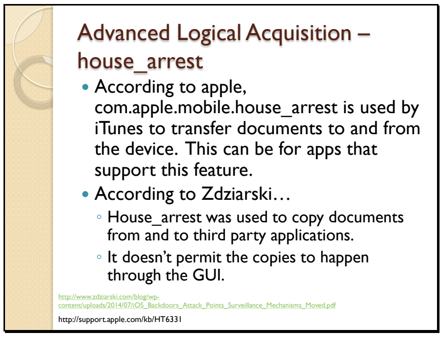


Advanced Logical Acquisition – Packet Sniffers on device?

- According to apple, com.apple.mobile.pcapd, this is useful for troubleshooting and diagnosing issues with apps on the device. It also helps with VPN connections.
  - In iOS 8, it's ability is restricted to USB inferface and can't be used over wireless.

http://support.apple.com/kb/HT6331

Slide 11



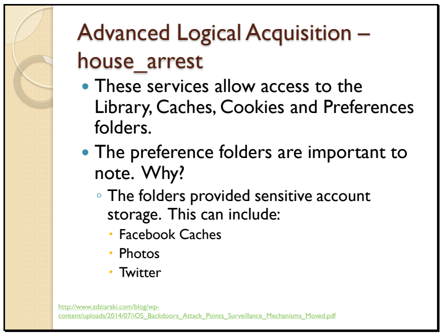
Advanced Logical Acquisition – house_arrest

- According to apple, com.apple.mobile.house_arrest is used by iTunes to transfer documents to and from the device. This can be for apps that support this feature.
- According to Zdziarski…
  - House_arrest was used to copy documents from and to third party applications.
  - It doesn't permit the copies to happen through the GUI.

http://www.zdziarski.com/blog/wp-content/uploads/2014/07/iOS_Backdoors_Attack_Points_Surveillance_Mechanisms_Moved.pdf

http://support.apple.com/kb/HT6331

Slide 12

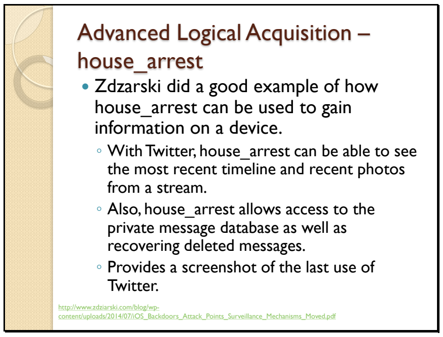


Advanced Logical Acquisition – house_arrest

- These services allow access to the Library, Caches, Cookies and Preferences folders.
- The preference folders are important to note. Why?
  - The folders provided sensitive account storage. This can include:
    - Facebook Caches
    - Photos
    - Twitter

http://www.zdziarski.com/blog/wp-content/uploads/2014/07/iOS_Backdoors_Attack_Points_Surveillance_Mechanisms_Moved.pdf

Slide 13

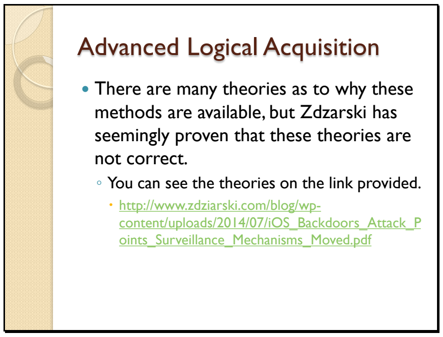


Advanced Logical Acquisition – house_arrest

- Zdzarski did a good example of how house_arrest can be used to gain information on a device.
  - With Twitter, house_arrest can be able to see the most recent timeline and recent photos from a stream.
  - Also, house_arrest allows access to the private message database as well as recovering deleted messages.
  - Provides a screenshot of the last use of Twitter.

http://www.zdziarski.com/blog/wp-content/uploads/2014/07/iOS_Backdoors_Attack_Points_Surveillance_Mechanisms_Moved.pdf

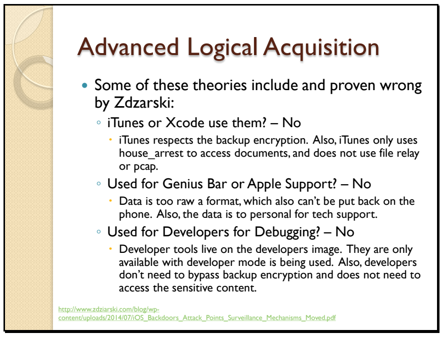
Slide 14



Advanced Logical Acquisition

- There are many theories as to why these methods are available, but Zdzarski has seemingly proven that these theories are not correct.
  - You can see the theories on the link provided.
    - http://www.zdziarski.com/blog/wp-content/uploads/2014/07/iOS_Backdoors_Attack_Points_Surveillance_Mechanisms_Moved.pdf

Slide 15



Advanced Logical Acquisition

- Some of these theories include and proven wrong by Zdzarski:
  - iTunes or Xcode use them? – No
    - iTunes respects the backup encryption. Also, iTunes only uses house_arrest to access documents, and does not use file relay or pcap.
  - Used for Genius Bar or Apple Support? – No
    - Data is too raw a format, which also can't be put back on the phone. Also, the data is to personal for tech support.
  - Used for Developers for Debugging? – No
    - Developer tools live on the developers image. They are only available with developer mode is being used. Also, developers don't need to bypass backup encryption and does not need to access the sensitive content.

http://www.zdziarski.com/blog/wp-content/uploads/2014/07/iOS_Backdoors_Attack_Points_Surveillance_Mechanisms_Moved.pdf

Chapter 12 – Week Eleven: Forensic Reporting and Presentation

The last week of presentations for students covers Forensic Reporting and Presentation. This is important because examiners need to know how to properly document their findings in cases, as well as presenting said findings to others or in court. A forensic report is a report of what tools were used during the investigation, as well as what was found. The report can go to supervisors, clients, attorneys or the Judge and Jury.

As stated before, investigators or examiners should put what steps were taken to gain the evidence. It is important to note the order in which they handled the evidence. This creates a timeline that the evidence has gone through, which can help assist with showing a chain of custody. [38]

There are many websites that can help one create and see a forensic report. Another important thing to do when reporting is to take notes of what is done. This can include screenshots, bookmarking evidence or making notes through a digital recorder or hand writing them.[39] Reports need to be detailed to show how one got the data.

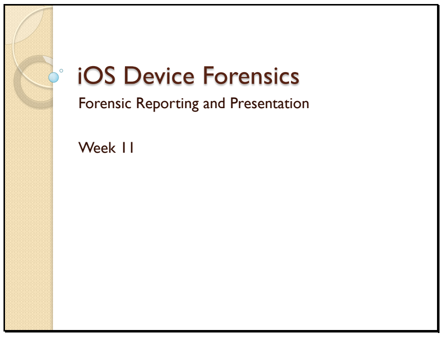
[38] (Christly)
[39] (Garcia, 2010)

As important forensic reporting is, communicating properly with others about the evidence is equally important. According to Shayne Sherman in his document *A digital forensic practitioner's guide to giving evidence in a court of law*, the use of PowerPoints and charts are very useful. What an examiner needs to remember is that not everyone may know technical terms, and using PowerPoints and charts can help others understand the information.

The week's presentation concludes with looking into what makes iOS analysis 'forensic'. For this, the lecture refers back to week one's look into technical analysis and forensic examinations. One must remember that technical analysis is how the examiner retrieved the evidence where a forensic examination is how one interprets the evidence to determine innocence or guilt.

PowerPoint Presentation for Week Eleven

Slide 1

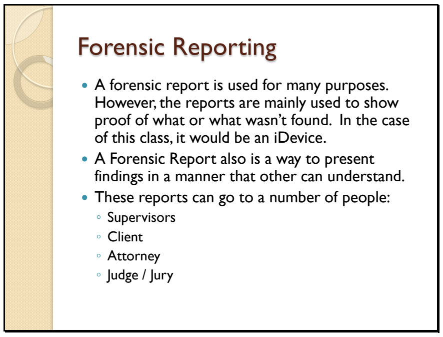


iOS Device Forensics

Forensic Reporting and Presentation

Week 11

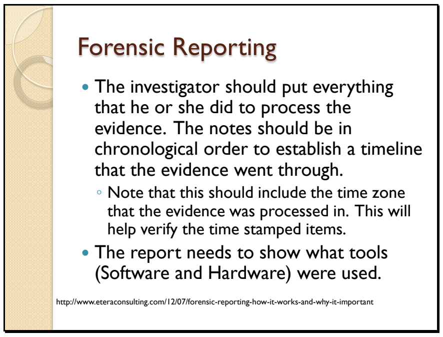
Slide 2



Forensic Reporting

- A forensic report is used for many purposes. However, the reports are mainly used to show proof of what or what wasn't found. In the case of this class, it would be an iDevice.
- A Forensic Report also is a way to present findings in a manner that other can understand.
- These reports can go to a number of people:
  - Supervisors
  - Client
  - Attorney
  - Judge / Jury

Slide 3

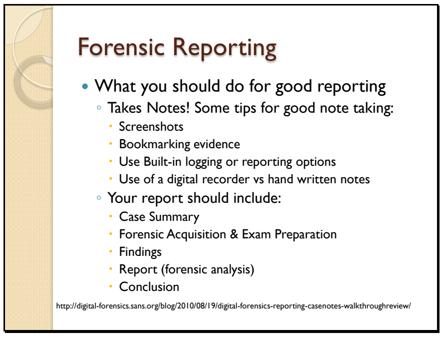


Forensic Reporting

- The investigator should put everything that he or she did to process the evidence. The notes should be in chronological order to establish a timeline that the evidence went through.
  - Note that this should include the time zone that the evidence was processed in. This will help verify the time stamped items.
- The report needs to show what tools (Software and Hardware) were used.

http://www.eteraconsulting.com/12/07/forensic-reporting-how-it-works-and-why-it-important

Slide 4

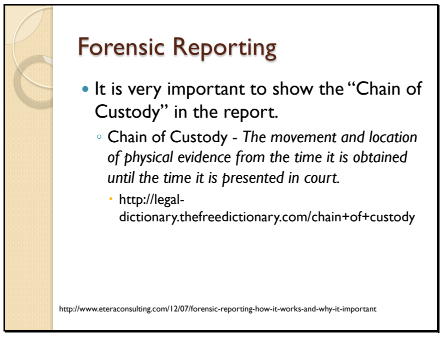


Forensic Reporting

- What you should do for good reporting
  - Takes Notes! Some tips for good note taking:
    - Screenshots
    - Bookmarking evidence
    - Use Built-in logging or reporting options
    - Use of a digital recorder vs hand written notes
  - Your report should include:
    - Case Summary
    - Forensic Acquisition & Exam Preparation
    - Findings
    - Report (forensic analysis)
    - Conclusion

http://digital-forensics.sans.org/blog/2010/08/19/digital-forensics-reporting-casenotes-walkthroughreview/

Slide 5

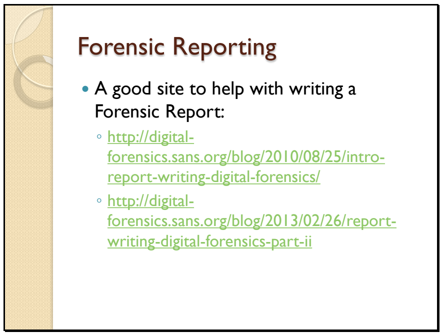


Forensic Reporting

- It is very important to show the "Chain of Custody" in the report.
  - Chain of Custody - *The movement and location of physical evidence from the time it is obtained until the time it is presented in court.*
    - http://legal-dictionary.thefreedictionary.com/chain+of+custody

http://www.eteraconsulting.com/12/07/forensic-reporting-how-it-works-and-why-it-important

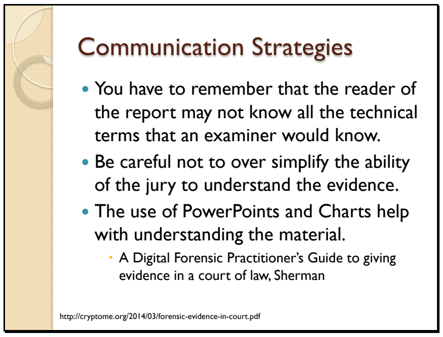
Slide 6



Forensic Reporting

- A good site to help with writing a Forensic Report:
  - http://digital-forensics.sans.org/blog/2010/08/25/intro-report-writing-digital-forensics/
  - http://digital-forensics.sans.org/blog/2013/02/26/report-writing-digital-forensics-part-ii

Slide 7

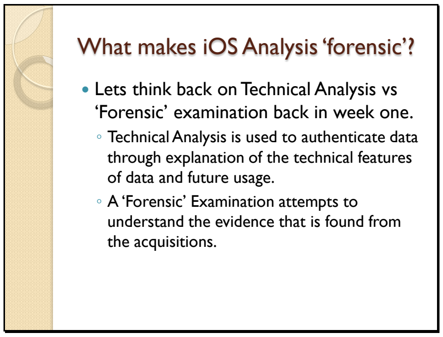


Communication Strategies

- You have to remember that the reader of the report may not know all the technical terms that an examiner would know.
- Be careful not to over simplify the ability of the jury to understand the evidence.
- The use of PowerPoints and Charts help with understanding the material.
  - A Digital Forensic Practitioner's Guide to giving evidence in a court of law, Sherman

http://cryptome.org/2014/03/forensic-evidence-in-court.pdf

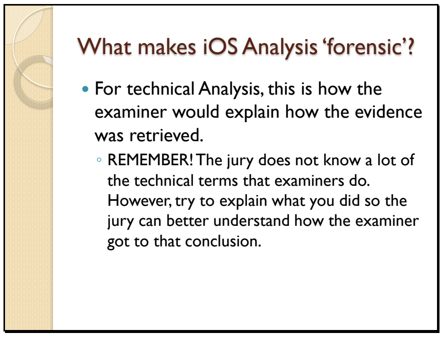
Slide 8



What makes iOS Analysis 'forensic'?

- Lets think back on Technical Analysis vs 'Forensic' examination back in week one.
  - Technical Analysis is used to authenticate data through explanation of the technical features of data and future usage.
  - A 'Forensic' Examination attempts to understand the evidence that is found from the acquisitions.

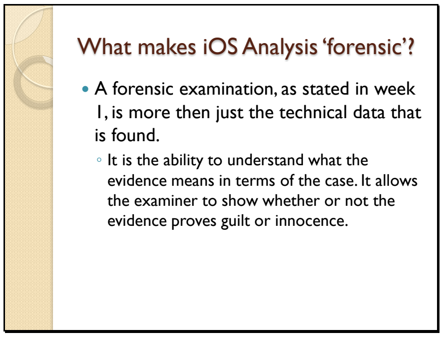
Slide 9



What makes iOS Analysis 'forensic'?

- For technical Analysis, this is how the examiner would explain how the evidence was retrieved.
  - REMEMBER! The jury does not know a lot of the technical terms that examiners do. However, try to explain what you did so the jury can better understand how the examiner got to that conclusion.

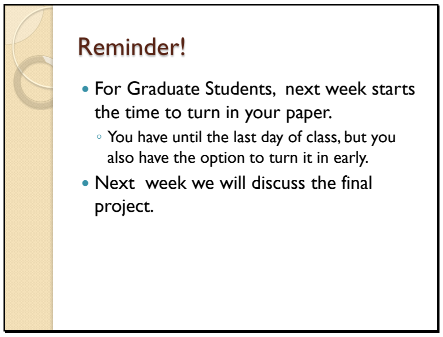
Slide 10



What makes iOS Analysis 'forensic'?

- A forensic examination, as stated in week 1, is more then just the technical data that is found.
  - It is the ability to understand what the evidence means in terms of the case. It allows the examiner to show whether or not the evidence proves guilt or innocence.

Slide 11



Reminder!

- For Graduate Students, next week starts the time to turn in your paper.
  - You have until the last day of class, but you also have the option to turn it in early.
- Next week we will discuss the final project.

Chapter 13 – Weeks Twelve through Fifteen: The Final Project

The remaining time for the semester will be spent on the student's working on a project using what they have learned in the class. The first phase of the project is giving the students a backup of a device containing evidence of a guilty party. The students then are encouraged to work either individually or in groups to retrieve the evidence. By the end of week fourteen, students or groups will turn in a report of their findings based on the backup that was provided. Week fifteen will be reserved for the student or group to present the project to others in a mock trail setting. Student will be encouraged to dress professionally, as if they were presenting to a real trial.

The Backup Provided for Students

The backup that was prepared contains two fake parties, Wayne Tarsle and Mark Bytes. Emails were set up for the each party, as well as an apple ID for each. Emails, as well as iMessages, were exchanged between the two fake individuals, setting up a scenario where Wayne sends evidence to Mark in exchange for money. The evidence in question was two plain sheets of paper with "Evidence #1" and "Evidence #2" written on them. The pictures of these sheets of paper were then sent to each respective email address. This was all done on an Apple iPhone 4s.

Chapter 14 – Conclusion

At the end of the semester, students should have a basic understanding of iOS device forensics, as well as some key concepts in this field. The field is constantly growing and changing with each new update and release that iOS has. This makes it difficult to find accurate information on this subject, especially with a forensic standpoint. Thankfully, there are plenty of internet sources, like the Apple Developer Library, that can have this information. This also shows that having developing a class for interested individuals can be beneficial as well.

Bibliography

AccessData. (2014). *Mobile Phone Examiner Plus*. Retrieved October 5, 2014, from AccessData: http://accessdata.com/solutions/digital-forensics/mpe?/solutions/digital-forensics/mobile-phone-examiner

Apple. (2007, August 8). *Time Utilities Reference.* Retrieved October 23, 2014, from Apple, Mac Developer Library: https://developer.apple.com/library/mac/documentation/CoreFoundation/Reference/CFTimeUtils/Reference/reference.html

Apple. (2010, 24 3). *About Property Lists.* Retrieved September 28, 2014, from Apple, Mac Developer Library: https://developer.apple.com/library/mac/documentation/Cocoa/Conceptual/PropertyLists/AboutPropertyLists/AboutPropertyLists.html

Apple. (2013, September 18). *iOS 7.* Retrieved September 25, 2014, from Apple: http://support.apple.com/kb/DL1682

Apple. (2014, November 8). *Apple Support :Unauthorized Modification ofiOS can Cause Security Vulnerabilities, Instability, Shortened Battery Life, and Other Issues*. Retrieved November 13, 2014, from Apple: http://support.apple.com/kb/ht3743

Apple. (2014, September 30). *ICloud: Erase your device.* Retrieved October 11, 2014, from Apple Support: http://support.apple.com/kb/PH2701

Apple. (2014, September 17). *Information Property List Key Reference.* Retrieved September 28, 2014, from Apple, iOS Developer Library: https://developer.apple.com/library/IOs/documentation/General/Reference/InfoPlistKeyReference/Articles/AboutInformationPropertyListFiles.html

Apple. (2014, February). *iOS Security .* Retrieved October 11, 2014, from Apple: http://images.apple.com/cn/ipad/business/docs/iOS_Security_Feb14.pdf

Apple. (2014, September 1). *iOS Security Guide Sept 2014*. Retrieved September 19, 2014, from iOS Security Guide Sept 2014: https://www.documentcloud.org/documents/1302613-ios-security-guide-sept-2014.html

Apple. (2014, September 17). *iOS Technology Overview*. Retrieved October 11, 2014, from Core OS Layer: https://developer.apple.com/Library/ios/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/CoreOSLayer/CoreOSLayer.html#//apple_ref/doc/uid/TP40007898-CH11-SW1

Apple. (2014, September 17). *iOS Technology Overview*. Retrieved September 25, 2014, from Core Services Layer: https://developer.apple.com/Library/ios/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/CoreServicesLayer/CoreServicesLayer.html#//apple_ref/doc/uid/TP40007898-CH10-SW5

Apple. (2014, September 17). *iOS Technology Overview*. Retrieved September 25, 2014, from Media Layer: https://developer.apple.com/Library/ios/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/MediaLayer/MediaLayer.html#//apple_ref/doc/uid/TP40007898-CH9-SW4

Apple. (2014, September 17). *iOS Technology Overview*. Retrieved September 25, 2014, from Cocoa Touch Layer: https://developer.apple.com/Library/ios/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/iPhoneOSTechnologies/iPhoneOSTechnologies.html#//apple_ref/doc/uid/TP40007898-CH3-SW1

Apple. (2014, October 8). *iOS: About Diagnostic Capabilities*. Retrieved October 26, 2014, from Apple Support: http://support.apple.com/kb/HT6331

Apple. (2014, February 11). *Keychain Services Programming Guide.* Retrieved October 11, 2014, from Apple, iOS Developer Library: https://developer.apple.com/library/ios/documentation/Security/Conceptual/k eychainServConcepts/02concepts/concepts.html#//apple_ref/doc/uid/TP30000897-CH204-SW1

Apple. (2014, February 11). *Keychain Services Programming Guide.* Retrieved October 11, 2014, from Apple, iOS Developer Library: https://developer.apple.com/library/ios/documentation/Security/Conceptual/keychainServConcepts/02concepts/concepts.html#//apple_ref/doc/uid/TP30000897-CH204-SW9

Apple. (2014, September 17). *Privacy - Our Privacy Policy*. Retrieved October 11, 2014, from Apple: http://www.apple.com/privacy/privacy-policy/

Apple. (2014, September). *The Biggest iOS Release Ever*. Retrieved September 25, 2014, from Apple: https://www.apple.com/ios/

Apple. (n.d.). *iOS Developer Library*. Retrieved November 3, 2014, from iOS Developer Library: https://developer.apple.com/library/ios/navigation/

BART. (n.d.). *Third Party Apps*. Retrieved September 28, 2014, from Bay Area Rapid Transit: https://www.bart.gov/schedules/appcenter

Carman, A. (2014, September 18). *Apple cannot comply with search warrants on iOS 8 devices*. Retrieved October 11, 2014, from SCMagazine: http://www.scmagazine.com/apple-cannot-comply-with-search-warrants-on-ios-8-devices/article/372410/

Cavanaugh, S. (2012, January). *Lantern Lite*. Retrieved October 23, 2014, from Lantern Lite: http://www.appleexaminer.com/iPhoneiPad/LanternLite/LanternLite.html

Cellebrite. (2014). *UFED Touch Ultimate*. Retrieved October 5, 2014, from Cellebrite: http://www.cellebrite.com/mobile-forensics/products/standalone/ufed-touch-ultimate

Chavanu, B. (2013, September 23). *10 AwesomeThird-Party Apps & their iOS 7 Updates*. Retrieved September 25, 2014, from MakeUseOf: http://www.makeuseof.com/tag/10-awesome-third-party-apps-their-ios-7-updates/

Chinook. (2012, December 11). *Chinook Database*. Retrieved 28 September, 2014, from CodePlex: http://chinookdatabase.codeplex.com/

Christly, J. (n.d.). *Forensic Reporting: How it Works and Why is it Important?* Retrieved September 20, 2014, from eTera Consulting: http://www.eteraconsulting.com/12/07/forensic-reporting-how-it-works-and-why-it-important

DataHandler. (n.d.). *You Work. We Back Up.* Retrieved September 19, 2014, from eDataHandlers web site: http://www.eadatahandlers.co.ke/services/mobile-phone-forensics-services/ios-forensics.html

DC1743. (2011, July 2). *SQLite overflow pages and other loose ends...* Retrieved September 28, 2014, from Forensics from the Sausage Factory: http://forensicsfromthesausagefactory.blogspot.com/2011/07/sqlite-overflow-pages-and-other-loose.html

DC1743. (2011, May 4). *SQLite Pointer Maps Pages.* Retrieved September 28, 2014, from Forensics from the Sausage Factory: http://forensicsfromthesausagefactory.blogspot.com/2011/05/sqlite-pointer-maps-pages.html

DeGrazia, M. (2013, November 6). *Python Parser to Recover Deleted SQLite Database Data* . Retrieved September 28, 2014, from Another Forensics Blog: http://az4n6.blogspot.com.es/2013/11/python-parser-to-recover-deleted-sqlite.html

Elcomsoft. (2014). *Coporate & Forensic Solutions.* Retrieved October 5, 2014, from Elcomsoft: http://www.elcomsoft.com/eift.html

Farivar, C. (2014, September 17). *Apple expands data encryption under iOS 8, making handover to cops moot*. Retrieved September 19, 2014, from arstechnica: http://arstechnica.com/apple/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/

Fitzpatrick, J. (2013, July 1). *HTG Explains: What is Juice Jacking and How Worried Should You Be?* Retrieved October 26, 2014, from HowToGeek : http://www.howtogeek.com/166497/htg-explains-what-is-juice-jacking-and-how-worried-should-you-be/

Garcia, J. (2010, August 19). *Digital Forensics Reporting: CaseNotes Walkthrough/Review*. Retrieved September 20, 2014, from SANS Digital Forensics and Incident Response Blog: http://digital-forensics.sans.org/blog/2010/08/19/digital-forensics-reporting-casenotes-walkthroughreview/

Garnett, B. (2010, August 25). *Intro to Report Writing For Digital Forensics.* Retrieved September 20, 2014, from SANS Digital Forensics & Incident Response: http://digital-forensics.sans.org/blog/2010/08/25/intro-report-writing-digital-forensics/

Garnett, B. (2013, February 26). *Report Writing for Digital Forensics: Part II.* Retrieved September 20, 2014, from SANS Digital Forensics & Incident Response:

http://digital-forensics.sans.org/blog/2013/02/26/report-writing-digital-forensics-part-ii

Giacobbi, G. (2006, November 1). *What is Netcat?* Retrieved October 23, 2014, from Netcat: http://netcat.sourceforge.net/

Guide, T., & Scharr, J. (2014, July 21). *Your iPhone May Be Rigged to Spy on You.* Retrieved October 26, 2014, from Yahoo News: http://news.yahoo.com/iphone-may-rigged-spy-183943399.html;_ylt=A0LEVyuXPE1UzLQAGYpXNyoA;_ylu=X3oDMTEzMWp0Z3ZhBHNlYwNzcgRwb3MDNgRjb2xvA2JmMQR2dGlkA1ZJUDUwMl8x

Hollington, J. (2013, March 11). *Securely Erasing an iPhone*. Retrieved October 11, 2014, from All things iPod, iPhone and Beyond: http://www.ilounge.com/index.php/articles/comments/securely-erasing-an-iphone/

Hoog, A., & Strzempka, K. (2011). Acquisitions: Handling Evidence. In A. Hoog, & K. Strzempka, *IPhone and iOS Forensics: Investigation, Analysis, and Mobile Security for Apple iPhone, iPad, and iOS Devices* (p. 111). Waltham, MA: Syngress.

Hoog, A., & Strzempka, K. (2011). Acquisitions: Jailbroken Device. In A. Hoog, & K. Strzempka, *IPhone and iOS Forensics: Investigation, Analysis, and Mobile Security for Apple iPhone, iPad, and iOS Devices* (p. 132). Waltham, MA: Syngress.

Hoog, A., & Strzempka, K. (2011). Acquisitions: Jailbroken Device. In A. Hoog, & K. Strzempka, *IPhone and iOS Forensics: Investigation, Analysis, and Mobile Security for Apple iPhone, iPad, and iOS Devices* (p. 130). Waltham, MA: Syngress.

Hoog, A., & Strzempka, K. (2011). Acquisitions: Strings. In A. Hoog, & K. Strzempka, *IPhone and iOS Forensics: Investigation, Analysis, and Mobile Security for Apple iPhone, iPad, and iOS devices* (pp. 144-145). Waltham, MA: Syngress.

Hoog, A., & Strzempka, K. (2011). Acquisitions: Zdziarski Technique. In A. Hoog, & K. Strzempka, *IPhone and iOS Forensics: Investigations, Analysis, and Mobile Security for Apple iPhone, iPad and iOS Devices* (pp. 124-127). Waltham, MA: Syngress.

Hoog, A., & Strzempka, K. (2011). Acquisitons: Jailbroken Device. In A. Hoog, & K. Strzempka, *IPhone and iOS Forensics: Investigation, Analysis, and Mobile Security for Apple iPhone, iPad, and iOS Devices* (p. 129). Waltham, MA: Syngress.

Hoog, A., & Strzempka, K. (2011). Acquistions: File Carving. In K. Strzempka, & A. Hoog, *IPhone and iOS Forensic: Investigation, Analysis, and Mobile Security for Apple iPhone, iPad and iOS Devices* (pp. 138-139). Waltham, MA: Syngress.

Hoog, A., & Strzempka, K. (2011). Device Features and Functions. In A. Hoog, & K. Strzempka, *IPhone and iOS Forensics: Investigation, Analysis, and Mobile Security for Apple iPhone, iPad, and iOS Devices* (p. 37). Waltham, MA: Syngress.

Hoog, A., & Strzempka, K. (2011). File System and Data Storage: iPhone Disk Partitions. In A. Hoog, & K. Strzempka, *IPhone and iOS Forensics: Investigation, Analysis, and Mobile Security forApple iPhone, iPad, and iOS Devices* (p. 75). Waltham, MA: Syngress.

Horowitz, P. (2013, June 26). *Recover a Lost Encrypted Backup Password for an iPhone, iPad, & iPod touch.* Retrieved October 11, 2014, from OSXDaily: http://osxdaily.com/2013/06/26/recover-lost-encrypted-backup-password-ios/

iClarified. (2008, December 31). *How to Find the Firmware and Baseband Version of your iPhone*. Retrieved October 23, 2014, from iClarified: http://www.iclarified.com/entry/?enid=2543

iDownloadBlog. (2011, October 20). *Untethered Jailbreak vs Tethered Jailbreak vs SemiTethered Jailbreak Whats the Difference*. Retrieved October 23, 2014, from iDownloadBlog: http://www.idownloadblog.com/2011/10/22/untethered-jailbreak-vs-tethered-jailbreak-vs-semitethered-jailbreak/

iDownloadBlog. (2014). *iDownloadBlog.com*. Retrieved October 23, 2014, from How to Jailbreak the iPhone, iPad, iPod Touch and Apple TV : http://www.idownloadblog.com/jailbreak/

Katana Forensics. (2014). *LANTERN Device Acquisition and Analysis.* Retrieved October 5, 2014, from Katana Forensics: https://katanaforensics.com/products/

Lauren, O. (2014, September 15). *Facebook Messenger found to be tracking 'a lot more data than you think'.* Retrieved September 25, 2014, from CBC News: http://www.cbc.ca/newsblogs/yourcommunity/2014/09/facebook-messenger-found-to-be-tracking-a-lot-more-data-than-you-think.html

Lee, C. (2011, March 14). *How to SSH into your iPhone*. Retrieved October 23, 2014, from iDownloadblog: http://www.idownloadblog.com/2011/03/14/how-to-ssh-into-your-iphone/

LeFebvre, R. (n.d.). *How To Remotely Wipe Your iPhone Data When Stolen [iOS Tips].* Retrieved October 11, 2014, from Cult of Mac: http://www.cultofmac.com/266448/remotely-wipe-iphone-data-stolen-ios-tips/

LibiMobileDevice. (2009). *A cross-platform software protocol library and tools to communicate with iOS® devices*. Retrieved October 26, 2014, from LibiMobileDevice web site: http://www.libmobiledevice.org/

Malureanu, A. (2012, August 15). *Decrypting encrypted iTunes backups.* Retrieved October 11, 2014, from iPhoneBackupExtractor.com: http://www.iphonebackupextractor.com/blog/2012/aug/15/decrypting-encrypted-itunes-backups/

Martin, J. (2014, September 9). *IOS7 vs iOS 8 comparison review: The new features which make this free update a no-brainer.* Retrieved September 25, 2014, from PCAdvisor: http://www.pcadvisor.co.uk/features/apple/3533759/ios-7-vs-ios-8-comparison-review/

Molla, R. (2014, September 12). *Is iPhone 6 Apple's Most Popular Model? Let's Ask Google*. Retrieved November 2, 2014, from The Wall Street Journal: http://blogs.wsj.com/numbers/is-iphone-6-apples-most-popular-model-lets-ask-google-1755/?mod=WSJBlog

O'Day, D. (2014, April 2). Introduction to iPhone 4n6. West Lafayette, Indiana, United States of America.

O'Day, D. (2014). SQLite Forensic Analysis. Lake County, Illinois, United States of America.

Panzarino, M. (2012, February 15). *What iOS apps are grabbing your data, why they do it and what should be done.* Retrieved September 25, 2014, from TNW: http://thenextweb.com/insider/2012/02/15/what-ios-apps-are-grabbing-your-data-why-they-do-it-and-what-should-be-done/

Proffitt, T. (2012, November 5). *Forensic Analysis on iOS Devices* . Retrieved October 5, 2014, from SANS : http://www.sans.org/reading-room/whitepapers/forensics/forensic-analysis-ios-devices-34092

Reed, B. (2014, September 11). *Security researcher find Facebook Messenger is loaded with 'spyware type code'.* Retrieved October 23, 2014, from BGR: http://bgr.com/2014/09/11/facebook-messenger-app-privacy/

Rubin, P., MacKenzie, D., & Kemp, S. (2010). *dd(1) - Linux man page*. Retrieved October 23, 2014, from dd(1) - Linux man page: http://linux.die.net/man/1/dd

Shane, S. (2006, December 4). *A Digital Forensics Practitioner's Guide to Giving Evidence in the Court of Law.* Retrieved September 20, 2014, from Cryptome: http://cryptome.org/2014/03/forensic-evidence-in-court.pdf

SQLite. (n.d.). *Atomic Commit in SQLite*. Retrieved September 28, 2014, from SQLite: http://www.sqlite.org/atomiccommit.html

SQLite. (n.d.). *Most Widely Deployed SQL Database Engine*. Retrieved September 28, 2014, from SQLite: http://www.sqlite.org/mostdeployed.html

SQLite. (n.d.). *SQL As Understood By SQLite*. Retrieved September 28, 2014, from SQLite: https://www.sqlite.org/lang_vacuum.html

SQLite. (n.d.). *SQLite Database File Format*. Retrieved September 28, 2014, from SQLite: http://www.sqlite.org/fileformat.html

SQLite. (n.d.). *SQLite's Use of Temporary Disk Files*. Retrieved September 28, 2014, from SQLite: https://www.sqlite.org/tempfiles.html

SQLite. (n.d.). *Write-Ahead Logging*. Retrieved September 28, 2014, from SQLite: http://www.sqlite.org/wal.html

Timberg, C. (2014, September 18). *Apple will no longer unlock most iPhones, iPads for police, even with search warrants*. Retrieved October 11, 2014, from The Washington Post: http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html

Whitfield, L. (2012, March 24). *Lantern Lite Imager*. Retrieved October 23, 2014, from Forensic 4cast: https://forensic4cast.com/2012/03/lantern-lite-imager/

Wikipedia. (2014, October 22). *pcap*. Retrieved October 26, 2014, from Wikipedia: http://en.wikipedia.org/wiki/Pcap

Wikipedia. (n.d.). *History of iOS.* Retrieved November 2, 2014, from Wikipedia: https://en.wikipedia.org/wiki/History_of_iOS#iPhone_OS_1.x

Wikipedia. (n.d.). *List of iOS Devices.* Retrieved November 2, 2014, from Wikipedia: http://en.wikipedia.org/wiki/List_of_iOS_devices

Zdziarski, J. (2014, July 18). *Identifying Back Doors, Attack Points, and Surveillance Mechanisms in iOS Devices*. Retrieved October 11, 2014, from Identifying Back Doors, Attack Points, and Surveillance Mechanisms in iOS Devices: http://www.zdziarski.com/blog/wp-content/uploads/2014/07/iOS_Backdoors_Attack_Points_Surveillance_Mechanisms_Moved.pdf