iPhone Forensics

Cybersecurity

Digital Forensics, Day 2

Class Objectives

By the end of class today, students will be able to:

- [ ] Identify the methods used in smartphone forensics.
- [ ] Describe databases and file structures of iPhone’s flash drive.
- [ ] Locate identifiable evidence on the iPhone that established ownership.
- [ ] Use Autopsy to view and tag evidence in an iPhone image.
- [ ] Extract image content for use in other applications (logs, text, pictures video, audio).

Warm Up Activity

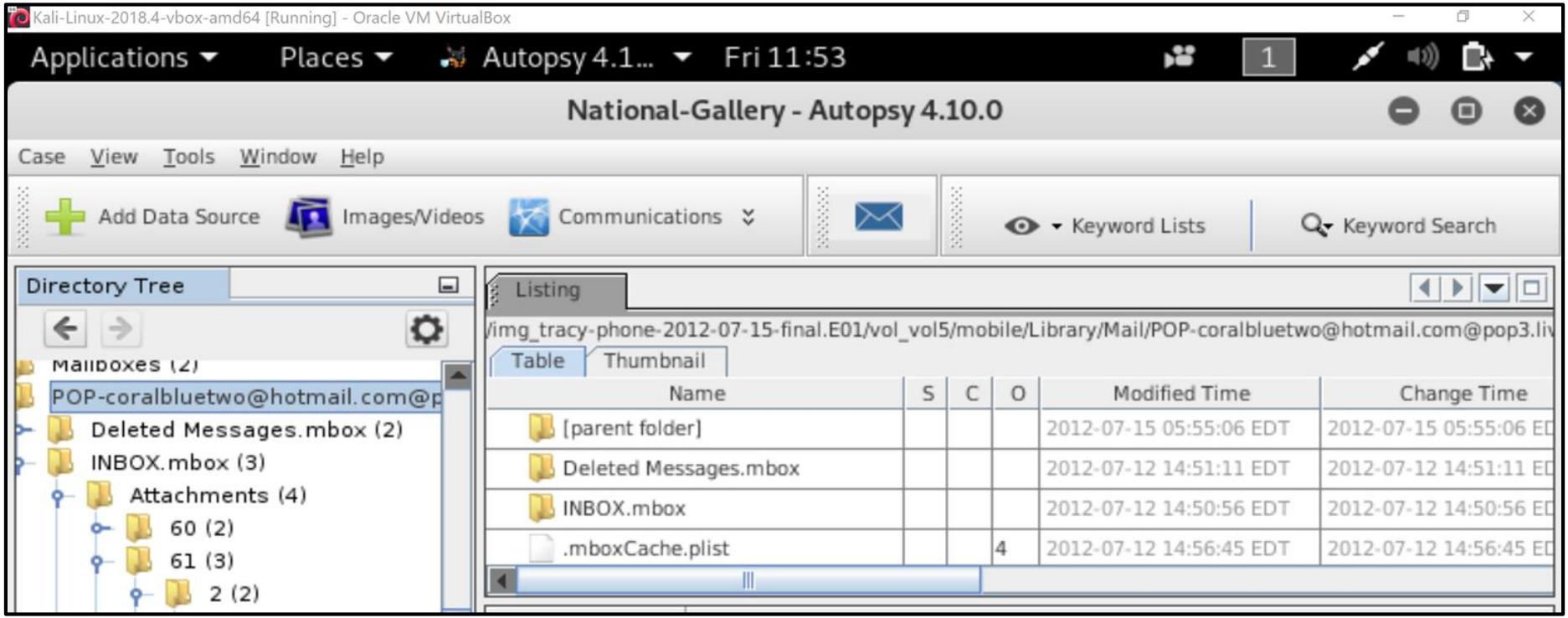
In this activity, you will review the steps for creating a new case and ingesting an image file. You will also learn how to find and display a file without using the Directory Tree.

Activities/1-Stu_WarmUp_1

Suggested Time:
20 minutes

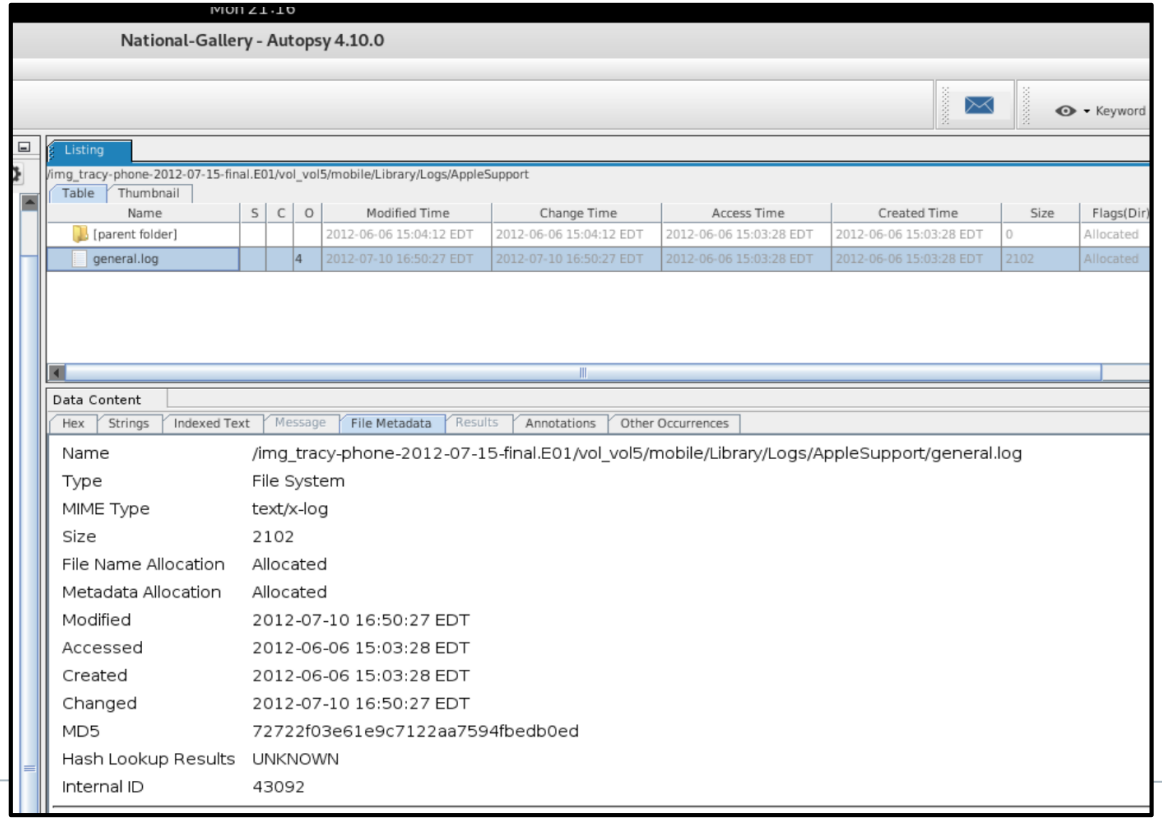
Review: How to View Text and Metadata using an Iphone Image

The main panes in the user interface: **Directory Tree**, **Listing**, and **Data Content**



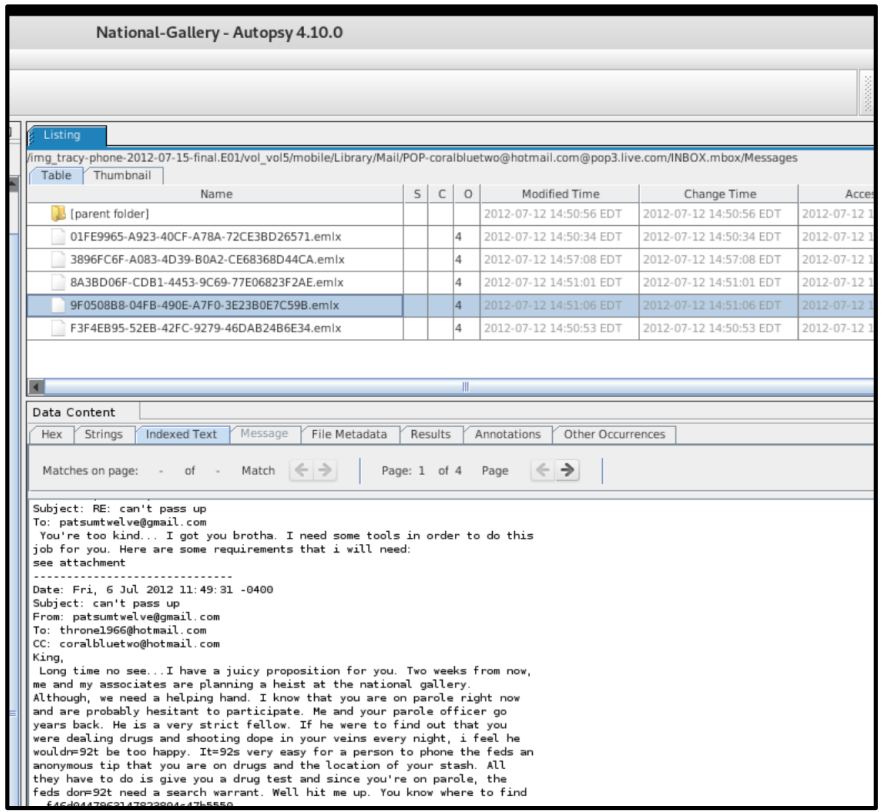
Review: How to View Text and Metadata using an Iphone Image

Capturing file metadata using the File Metadata tab in the Data Content pane reveals the location in the image (Name), mime type, size, creation date, and md5 hash



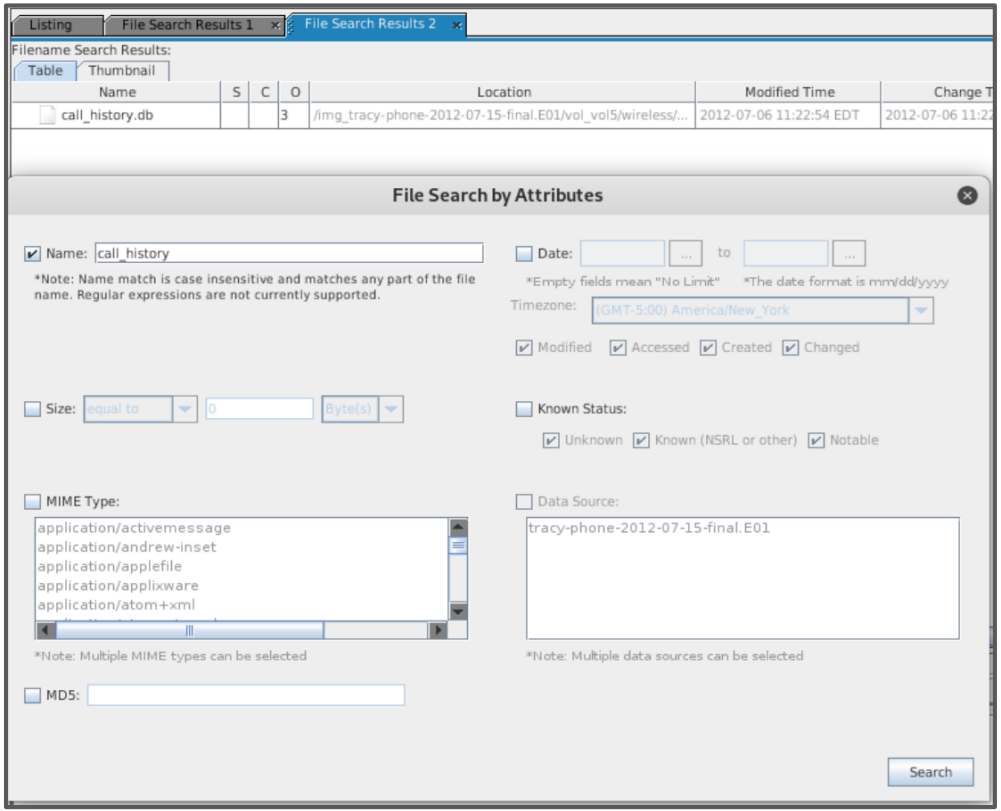
Review: How to View Text and Metadata using an Iphone Image

The Indexed Text tab is used to display text in the image in a human readable format.



Review: How to View Text and Metadata using an Iphone Image

If you know the file name, searching for a file in the iPhone image is faster than using the Directory Tree.



Introduction to iPhone Forensics

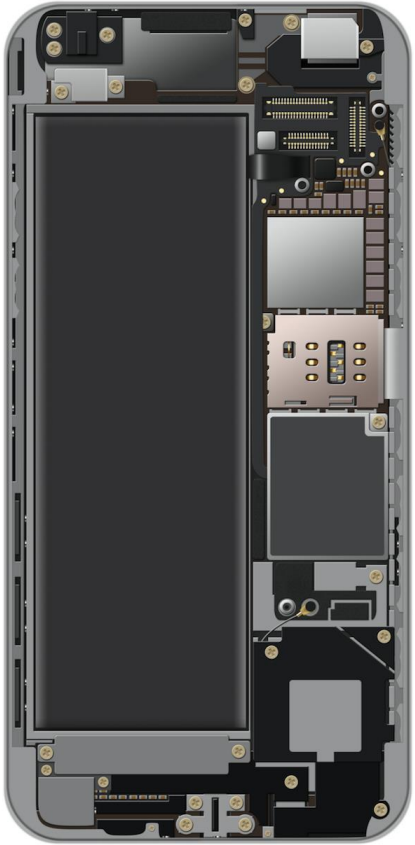
iPhone, an introduction

First released in June of 2007

Runs on iOS operating system

Currently 700 million iPhones in use (*compared to 2.3 billion Android phones.*)

The phone data is *encrypted* and has been involved in several high profile forensic cases



Where’s the Data? File systems and Data Storage

It is important to know where data is stores, how to access it, and how to recover it.

Instead of external storage, iPhones uses *flash memory*.

Contains two disk partitions:

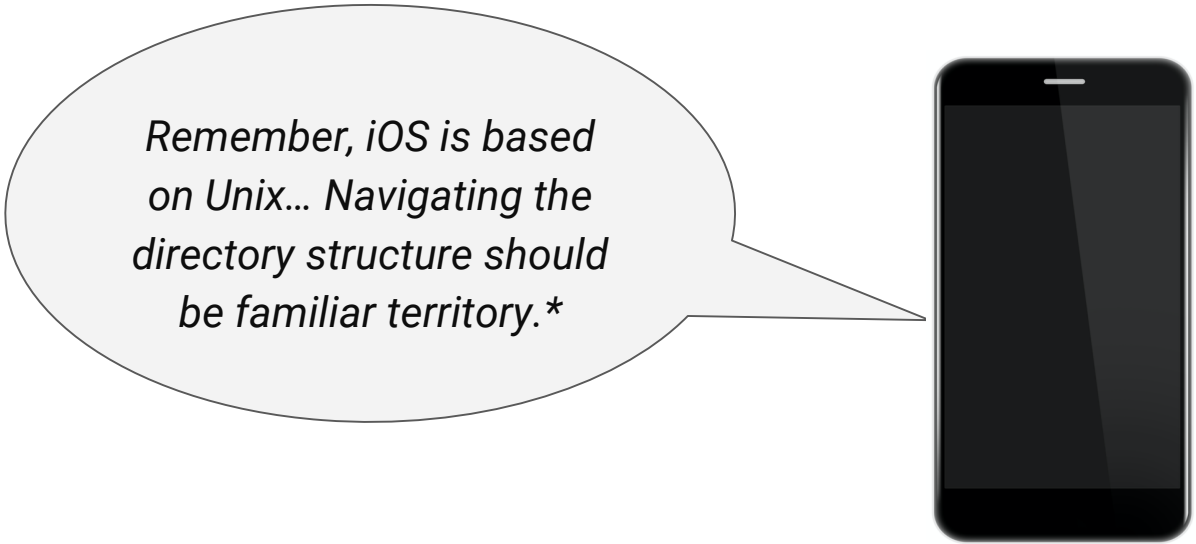
- Root partition used for operating systems and applications
- Var partition used for data

Remember: Data is first imaged using bit-level-copy. iPhone texts, GPS coordinates, cell tower locations can all be recovered.

Important Directories, Databases, and Files

For our investigation, the following directories contain evidence for investigations:

`/mobile, /Applications, /Library, /root,  /Logs, /logs`



Important Directories, Databases and Files

iPhone users store data in SQL databases and other files.

SQL (System Query Language) is a programming language used to read, write, and update database files.

Databases are used to store information. For example: an address book.

Important Directories / Databases, and Files

Name:	Contents:
AddressBook.sqlitedb	Contact info, personal data like name, email address, etc.
AddressBookImages.sqlitedb	Images associated with saved contacts
Calendar.sqlitedb	Calendar details and events information
CallHistory.db	Call logs including phone numbers and timestamps
sms.db	Text and multimedia messages along with timestamps
voicemail.db	Voicemail messages
Safari/Bookmarks	Saved URL addresses
Envelope Index	Email addresses on phone
consolidated.db	GPS tracking data
locationd	Google coordinates of places

Important Directories / Databases, and Files

iPhone also has data stored in Property Lists (`plists`)

`plists` store configuration information, call history and cache information

`Maps/History.plist` tracks location searches

`Map/Bookmarks.plist` contains bookmarks

`Safari/History` contains internet browsing history

Is this Tracy’s iPhone?

Activity: Is this Tracy’s iPhone?

In this activity, you will analyze the contents of Tracy's iPhone image in order to begin establishing your case.

Activities/2-Stu_Evidence_1

Suggested Time:
20 Minutes

Is this Tracy's iPhone? Review

	Findings	Location in iPhone Image
Device Model	iPhone1.2	vol/5/mobile/Library/Logs/AppleSupport/general.log
Device Serial Number	86004482Y7H	vol/5/mobile/Library/Logs/AppleSupport/general.log
OS Version Number	4.2.1	vol/5/mobile/Library/Logs/AppleSupport/general.log
Installation Timestamp	7/10/2012 16:50:27	vol/5/mobile/Library/Logs/AppleSupport/general.log
Email Address	tracy.sumtwelve@nationalgallerydc.org, tracysumtwelve@gmail.com, coralbluetwo@gmail.com	vol/5/mobile/Library/Mail
Phone Number	703-340-9661	**Indexed Text:** vol5/logs/lockdown.log.1 set_formated_phone_ numbe: New phone number 1 (703) 340-9661 to insert into the ark
ICCID	89014103255195342366	vol/logs/lockdown.log.1

Is this Tracy's iPhone? Review

How are the IMEI, ICCD and IMSI used to establish unique device identification?

The **International Mobile Equipment Identification** (IMEI) is a unique 15-17 digit code stored on the phone used to indentify the physical hardware (phone).

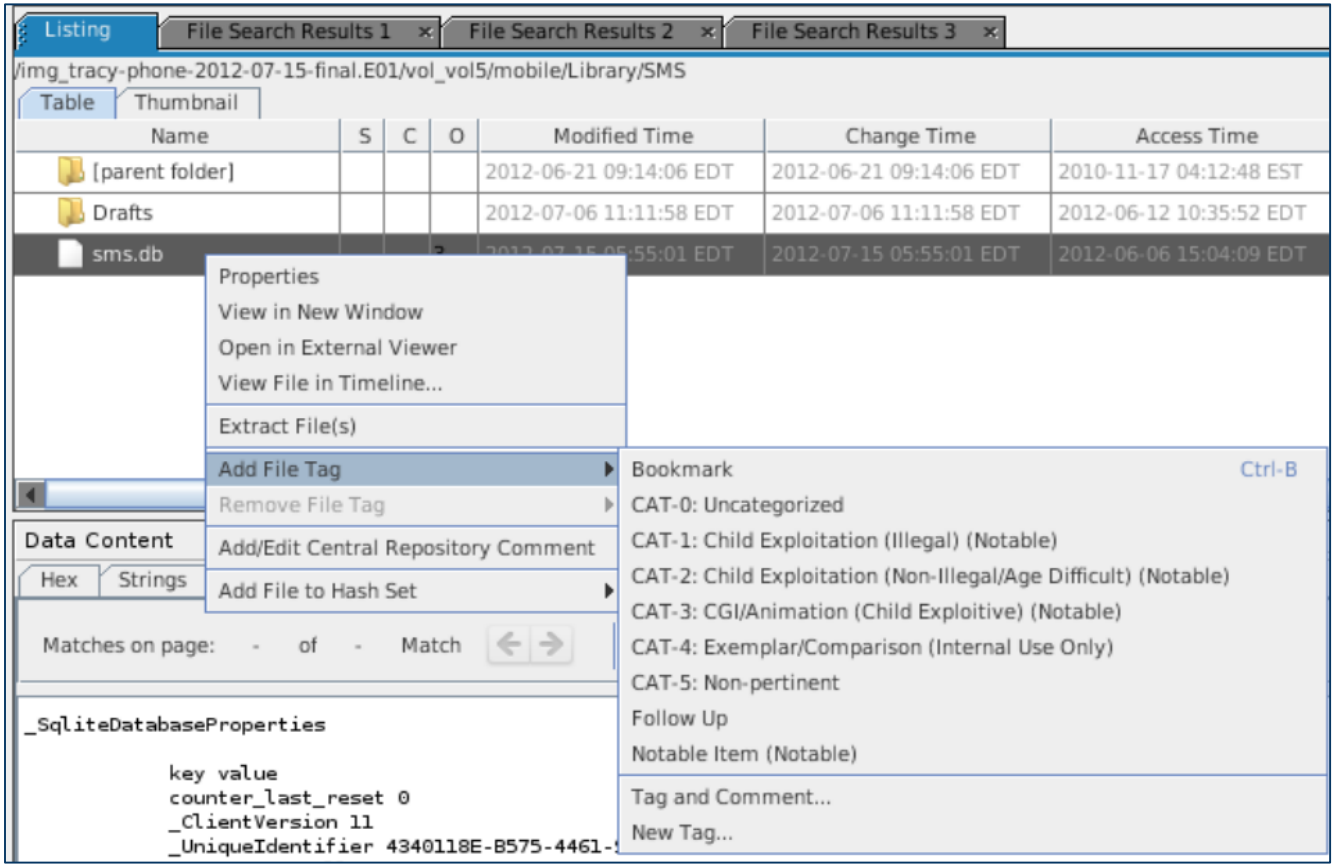
A **Subscriber Identity Module** or **Subscriber Identification Module** (SIM), widely known as a SIM card, is an **Integrated Circuit Card ID** (ICCID)that is intended to securely store the **International Mobile Subscriber Identity** (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store contact information on many SIM cards.

Tagging Evidence

Autopsy includes a tag evidence feature, allowing investigators to find information easier.

Pre-defined tags include:
Follow Up, *Notable*, and *Child Exploitation*.

Bookmarking the SMS Database



Locate the sms.db file in the iPhone image using the **Tools->Files Search by Attributes**.

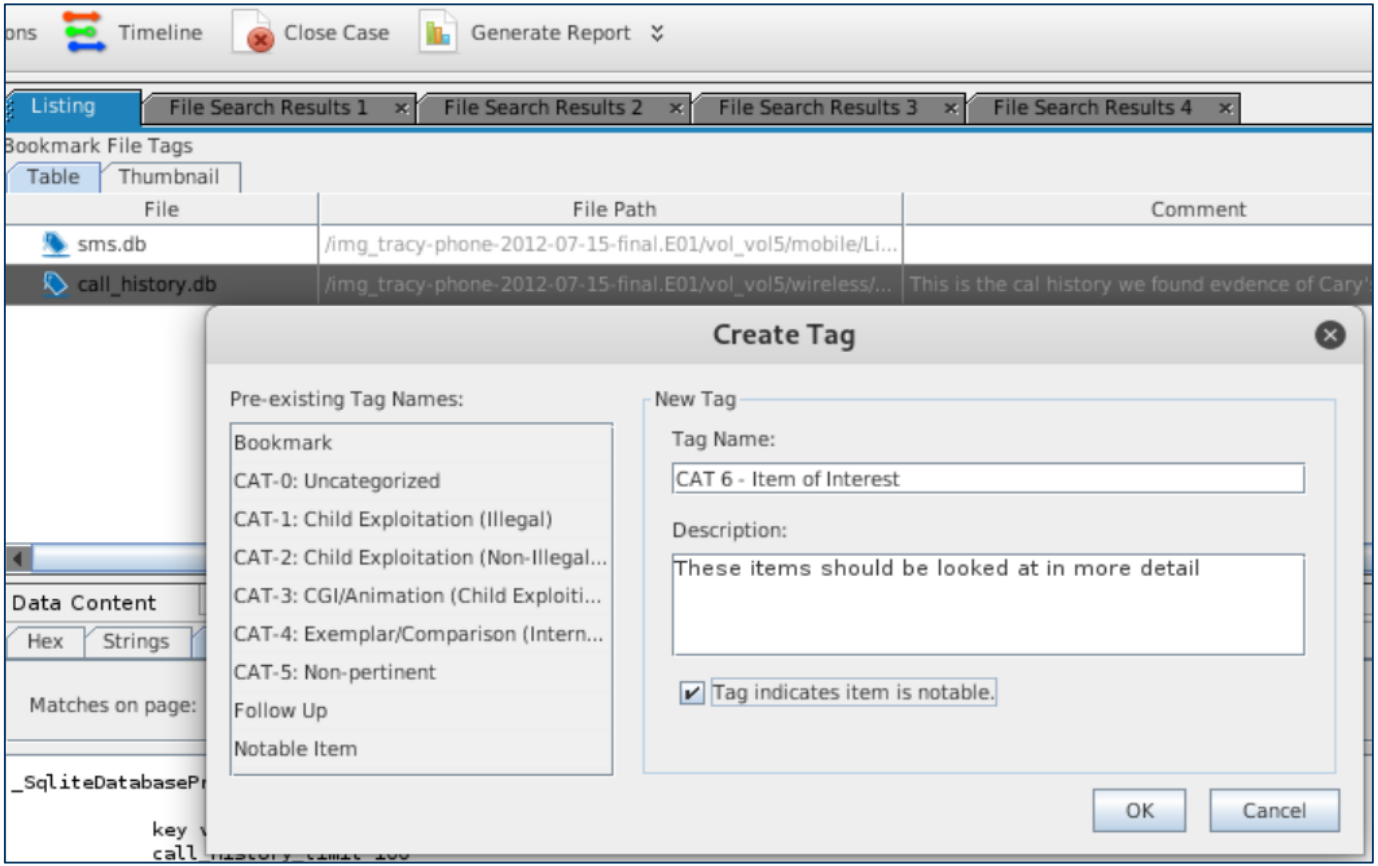
Click on the sms.db entry in the **Listings** pane.

Right-click and select **Add Tag -> Bookmark**.

A yellow upside-down triangle will appear next to the sms.db entry in the Listing pane.

The bookmarked entry can be found in the **Directory Tree** under **Tags**.

Creating a new tag to the database



A company may have a tagging scheme that can be used in Autopsy.

Right-click and select **Add Tag -> New Tag**.

The **Create Tag** window is displayed to add a new tag and comment.

The new tag entry can be found in the Directory Tree under Tags

Activity: Tagging Evidence

In this activity, you will tag the major Database and Files in the iPhone image file

Activities/3-Stu_Tagging

Suggested Time:
10 Minutes

Extracting Data for Offline Analysis

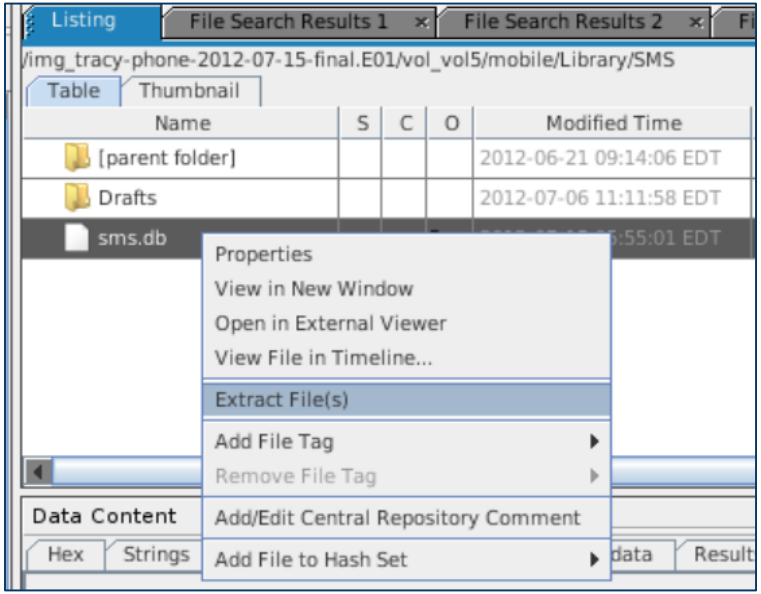
Extracting Data for Offline Analysis

Some investigators may extract the entire directory tree for offline viewing, which facilitates viewing videos and pictures.

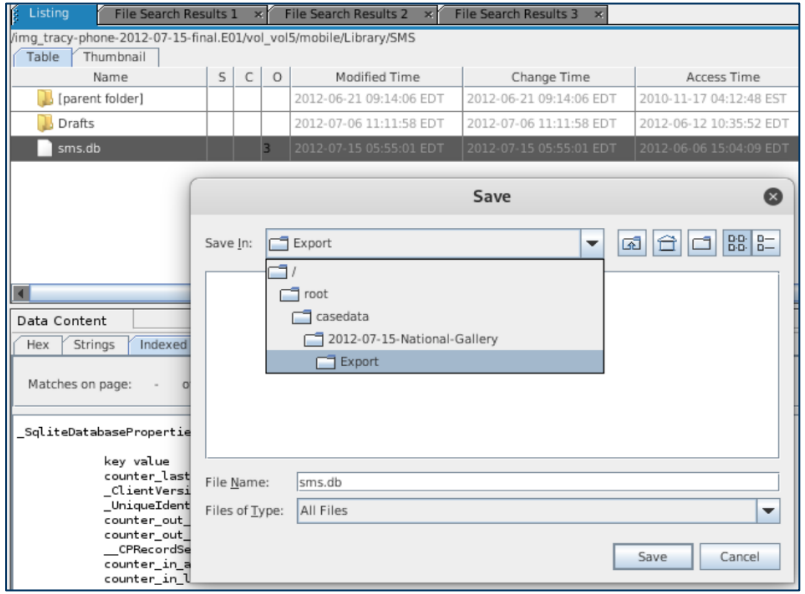
- Viewing videos and pictures is a much easier process with offline extraction.
- Not all data can be viewed in a text editor.
- The databases are viewed using SQLite or any SQL software.

In the next demo, we'll demo how to extract a file or an entire directory for viewing within Kali Linux and other operating systems.

Exporting a Single File



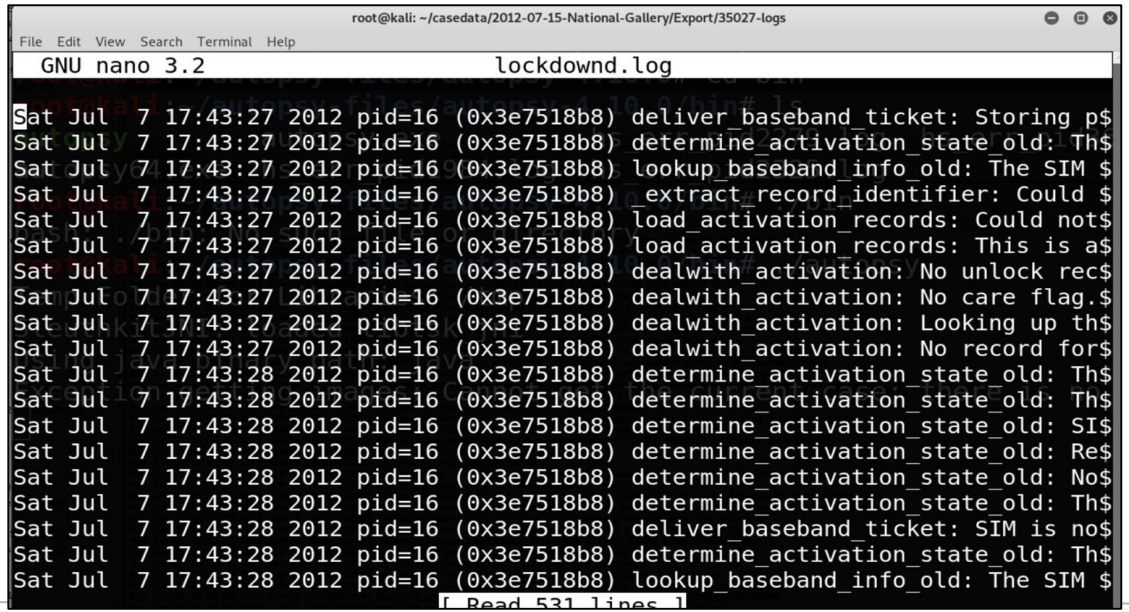
Select the sms.db database. Right-click and select Export Files



By default, the files are placed in the Export directory for the case.

Export directory is located in the `casedata` directory.
This file can only be viewed with a SQL application

Exporting an entire directory



Select the vol5/logs directory in the Directory Tree pane.

Right-click and select Export Files, and export the entire directory to the Export directory in Kali.

Navigate to the Export directory

Open a new terminal window and navigate to the Export directory that contains the extracted directory. (Image 1)

View the lockdownd.log file in the nano editor. (image 2)

Activity: Extracting Data for Offline Analysis

In this activity you will practice exporting a single file and an entire directory for offline analysis.

Activities/4-Stu_Extract

Suggested Time:
10 minutes

Class Objectives

By the end of class today, students will be able to:

- Identify the methods used in smartphone forensics.
- Describe databases and file structures of iPhone’s flash drive.
- Locate identifiable evidence on the iPhone that established ownership.
- Use Autopsy to view and tag evidence in an iPhone image.
- Extract image content for use in other applications (logs, text, pictures video, audio).