



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**

Kali-Linux-2018.4-vbox-amd64 [Running] - Oracle VM VirtualBox

Applications ▾ Places ▾ Autopsy 4.1... ▾ Fri 11:53

National-Gallery - Autopsy 4.10.0

Case View Tools Window Help

+ Add Data Source Images/Videos Communications ▾

Keyword Lists Keyword Search

Directory Tree

- Mailboxes (2)
 - POP-coralbluetwo@hotmail.com@pop3.liv
 - Deleted Messages.mbox (2)
 - INBOX.mbox (3)
 - Attachments (4)
 - 60 (2)
 - 61 (3)
 - 2 (2)

Listing

Table Thumbnail

/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.liv

Name	S	C	O	Modified Time	Change Time
[parent folder]				2012-07-15 05:55:06 EDT	2012-07-15 05:55:06 EDT
Deleted Messages.mbox				2012-07-12 14:51:11 EDT	2012-07-12 14:51:11 EDT
INBOX.mbox				2012-07-12 14:50:56 EDT	2012-07-12 14:50:56 EDT
.mboxCache.plist			4	2012-07-12 14:56:45 EDT	2012-07-12 14:56:45 EDT

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

The screenshot displays the National-Gallery - Autopsy 4.10.0 interface. The top bar shows the application name and version. Below it, a search bar with a magnifying glass icon and a 'Keyword' label is visible. The main window is divided into two panes. The left pane, titled 'Listing', shows a file tree with a table of files. The right pane, titled 'Data Content', shows the file metadata for the selected file.

File Listing Table:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
[parent folder]				2012-06-06 15:04:12 EDT	2012-06-06 15:04:12 EDT	2012-06-06 15:03:28 EDT	2012-06-06 15:03:28 EDT	0	Allocated
general.log			4	2012-07-10 16:50:27 EDT	2012-07-10 16:50:27 EDT	2012-06-06 15:03:28 EDT	2012-06-06 15:03:28 EDT	2102	Allocated

Data Content - File Metadata Tab:

Name	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Logs/AppleSupport/general.log
Type	File System
MIME Type	text/x-log
Size	2102
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2012-07-10 16:50:27 EDT
Accessed	2012-06-06 15:03:28 EDT
Created	2012-06-06 15:03:28 EDT
Changed	2012-07-10 16:50:27 EDT
MD5	72722f03e61e9c7122aa7594fbedb0ed
Hash Lookup Results	UNKNOWN
Internal ID	43092

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.

The screenshot displays the National-Gallery - Autopsy 4.10.0 interface. The top section shows a file listing table with columns for Name, S, C, O, Modified Time, Change Time, and Access. The selected file is 9F0508B8-04F8-490E-A7F0-3E23B0E7C598.emlx. Below the table, the Data Content section is active, showing the Indexed Text tab. The email content is displayed in a text area, including the subject, to, from, and body text.

National-Gallery - Autopsy 4.10.0

Listing

/img_tracy-phone-2012-07-15-final.E01/vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Messages

Name	S	C	O	Modified Time	Change Time	Access
[parent folder]				2012-07-12 14:50:56 EDT	2012-07-12 14:50:56 EDT	2012-07-12 14:50:56 EDT
01FE9965-A923-40CF-A78A-72CE3BD26571.emlx			4	2012-07-12 14:50:34 EDT	2012-07-12 14:50:34 EDT	2012-07-12 14:50:34 EDT
3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx			4	2012-07-12 14:57:08 EDT	2012-07-12 14:57:08 EDT	2012-07-12 14:57:08 EDT
8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx			4	2012-07-12 14:51:01 EDT	2012-07-12 14:51:01 EDT	2012-07-12 14:51:01 EDT
9F0508B8-04F8-490E-A7F0-3E23B0E7C598.emlx			4	2012-07-12 14:51:06 EDT	2012-07-12 14:51:06 EDT	2012-07-12 14:51:06 EDT
F3F4EB95-52EB-42FC-9279-46DAB24B6E34.emlx			4	2012-07-12 14:50:53 EDT	2012-07-12 14:50:53 EDT	2012-07-12 14:50:53 EDT

Data Content

Hex Strings Indexed Text Message File Metadata Results Annotations Other Occurrences

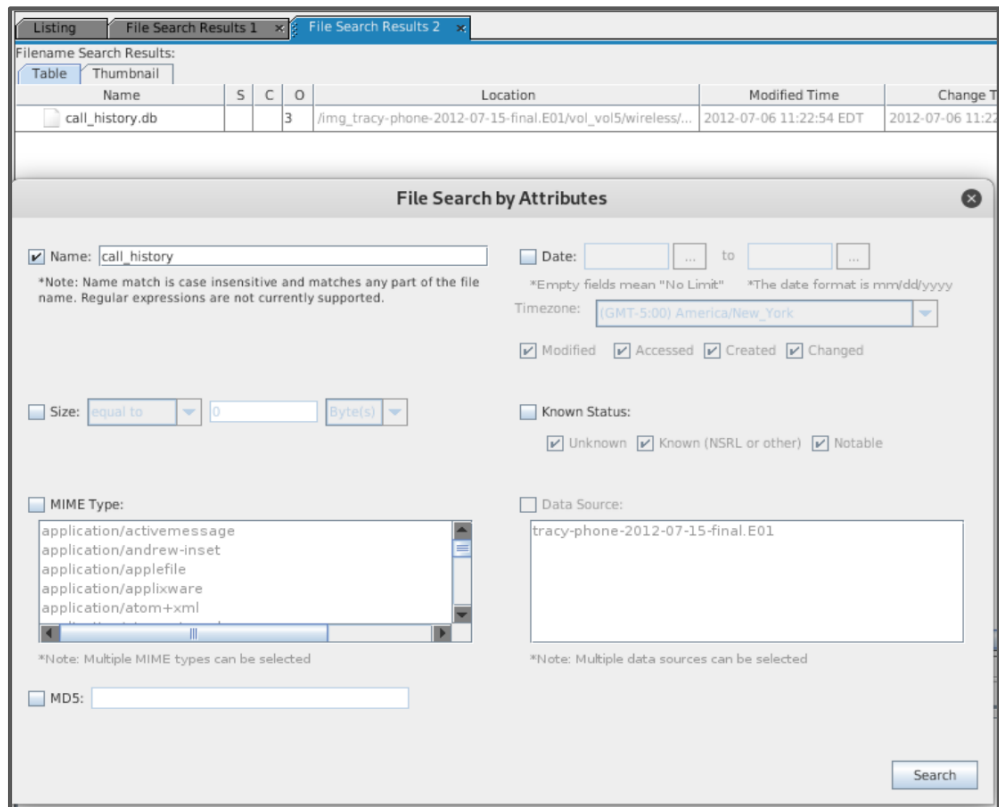
Matches on page: - of - Match < > Page: 1 of 4 Page < >

Subject: RE: can't pass up
To: patsumtelve@gmail.com
You're too kind... I got you brotha. I need some tools in order to do this job for you. Here are some requirements that i will need:
see attachment

Date: Fri, 6 Jul 2012 11:49:31 -0400
Subject: can't pass up
From: patsumtelve@gmail.com
To: throne1966@hotmail.com
CC: coralbluetwo@hotmail.com
King,
Long time no see...I have a juicy proposition for you. Two weeks from nov, me and my associates are planning a heist at the national gallery. Although, we need a helping hand. I know that you are on parole right now and are probably hesitant to participate. He and your parole officer go years back. He is a very strict fellow. If he were to find out that you were dealing drugs and shooting dope in your veins every night, i feel he wouldn't be too happy. It's very easy for a person to phone the feds an anonymous tip that you are on drugs and the location of your stash. All they have to do is give you a drug test and since you're on parole, the feds don't need a search warrant. We'll hit me up. You know where to find

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

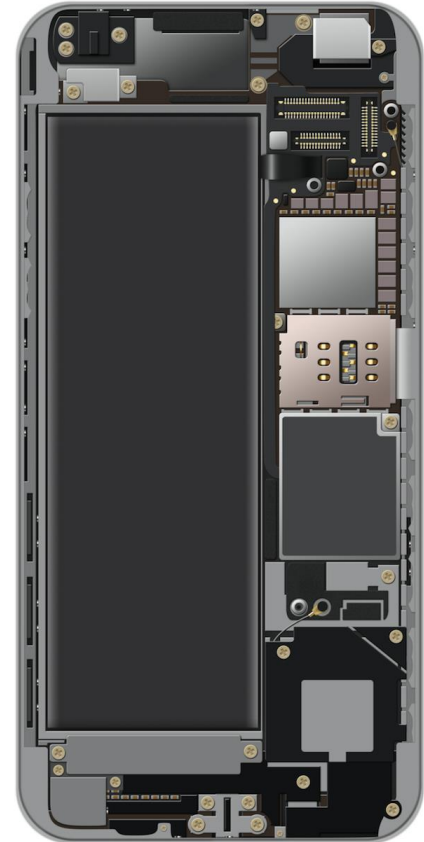


First released in June of 2007

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

*Remember, iOS is based on Unix... Navigating the directory structure should be familiar territory.**



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 (`plist`s)



`plist`s 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

The screenshot shows a file listing pane with the following table:

Name	S	C	O	Modified Time	Change Time	Access Time
[parent folder]				2012-06-21 09:14:06 EDT	2012-06-21 09:14:06 EDT	2010-11-17 04:12:48 EST
Drafts				2012-07-06 11:11:58 EDT	2012-07-06 11:11:58 EDT	2012-06-12 10:35:52 EDT
sms.db				2012-07-15 05:55:01 EDT	2012-07-15 05:55:01 EDT	2012-06-06 15:04:09 EDT

A context menu is open over the 'sms.db' file, showing the following options:

- Properties
- View in New Window
- Open in External Viewer
- View File in Timeline...
- Extract File(s)
- Add File Tag (selected)
- Remove File Tag
- Add/Edit Central Repository Comment
- Add File to Hash Set

The 'Add File Tag' option is expanded, showing a list of categories (CAT-0 to CAT-5) and other options like 'Follow Up', 'Notable Item (Notable)', 'Tag and Comment...', and 'New Tag...'. The 'Ctrl-B' shortcut is visible next to the 'Bookmark' option.

Below the file listing, the 'Data Content' pane is visible, showing the 'Hex' and 'Strings' tabs. The 'Strings' tab is selected, displaying the following text:

```
_SqliteDatabaseProperties  
  
key value  
counter_last_reset 0  
_ClientVersion 11  
_UniqueIdentifier 4340118E-B575-4461-...
```

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

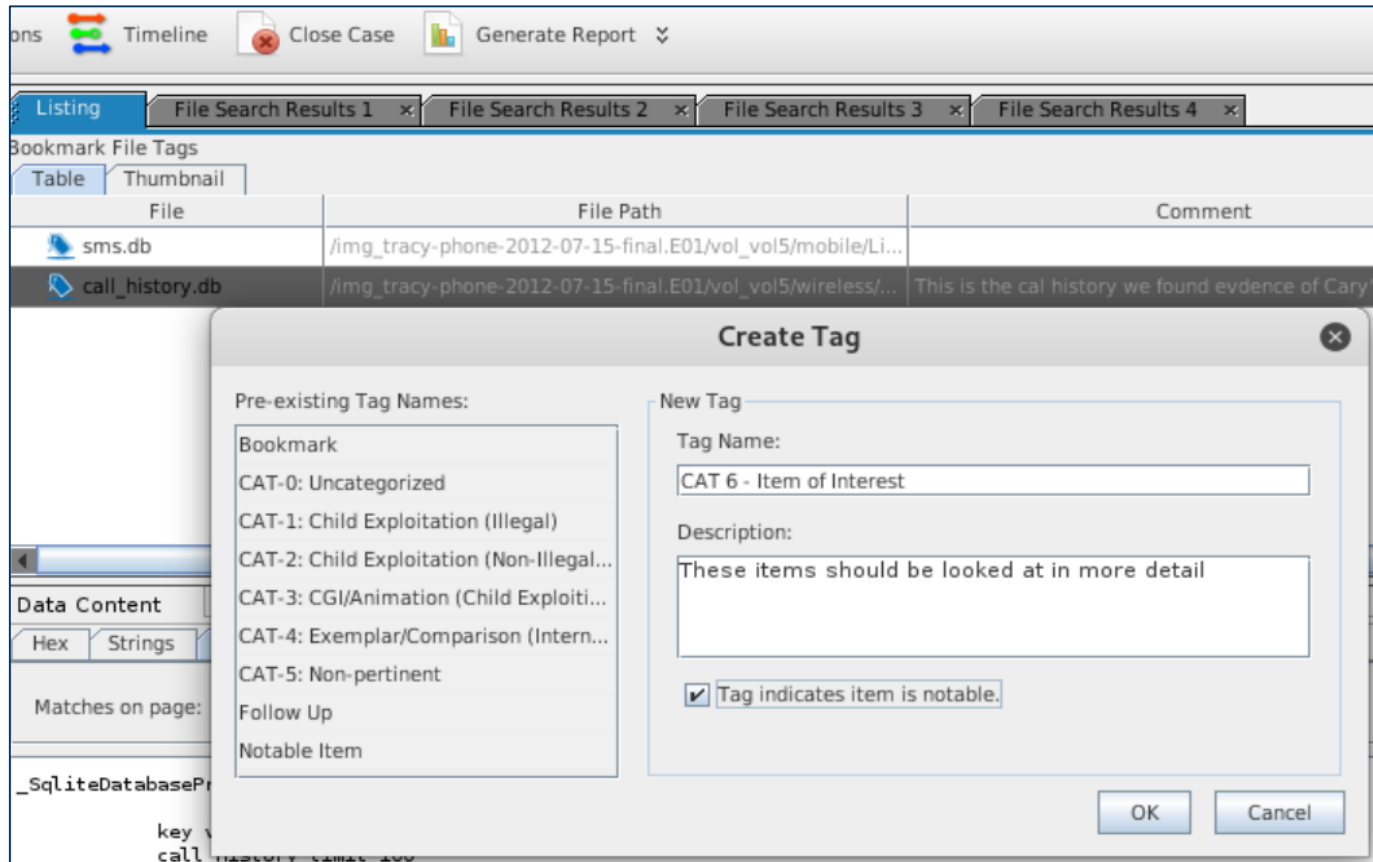
Click on the sms.db entry in the **Listings** pane.

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

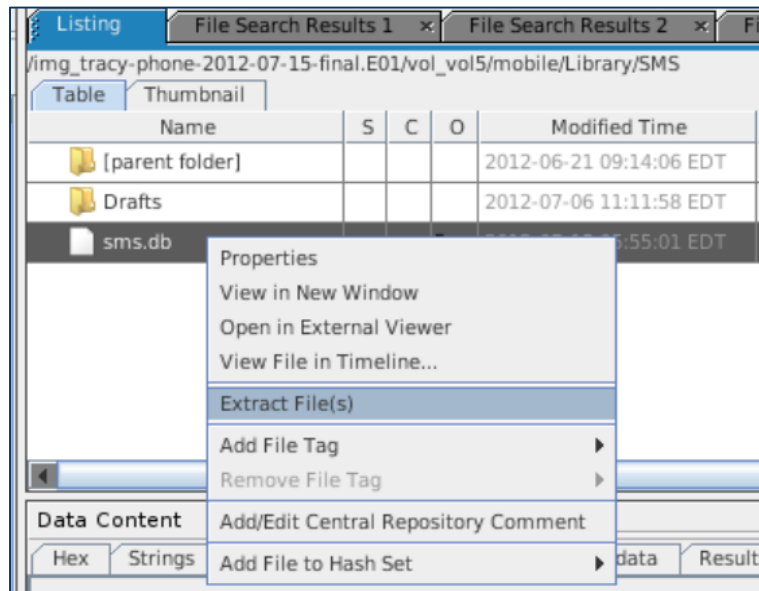
Extracting Data for Offline Analysis

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

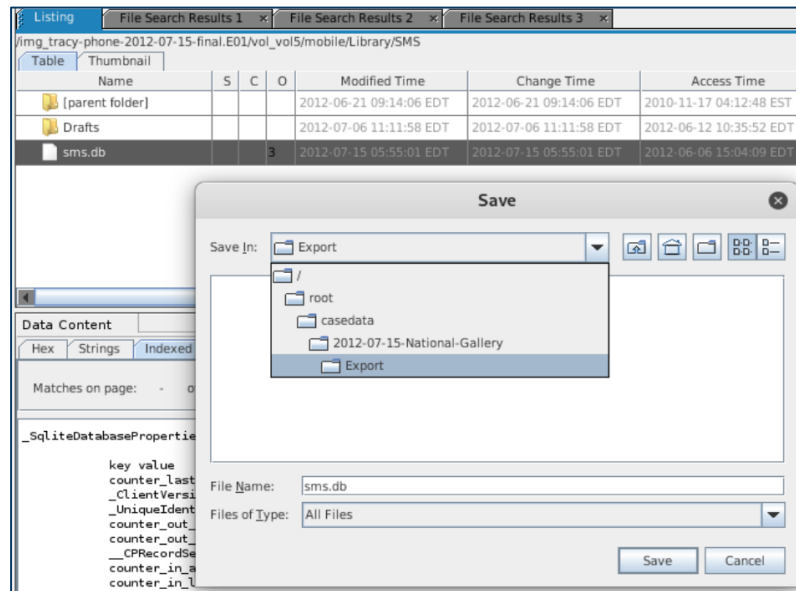
- Viewing videos and pictures is a much easier process with offline extraction.
- Not all data can be viewed in a text editor.
- The databases are viewed using SQLite or any SQL software.

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

```
root@kali: ~/casedata/2012-07-15-National-Gallery/Export/35027-logs
File Edit View Search Terminal Help
root@kali:~/casedata/2012-07-15-National-Gallery/Export# ls
35027-logs cd autopsy-files/
root@kali:~/casedata/2012-07-15-National-Gallery/Export# cd 35027-logs/
root@kali:~/casedata/2012-07-15-National-Gallery/Export/35027-logs# ls
AppleSupport keybagd.log lockdownd.log lockdownd.log.1-slack
CrashReporter keybagd.log-slack lockdownd.log.1 lockdownd.log-slack
root@kali:~/casedata/2012-07-15-National-Gallery/Export/35027-logs#
```

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)

```
root@kali: ~/casedata/2012-07-15-National-Gallery/Export/35027-logs
File Edit View Search Terminal Help
GNU nano 3.2 lockdownd.log
Sat Jul 7 17:43:27 2012 pid=16 (0x3e7518b8) deliver_baseband_ticket: Storing p$
Sat Jul 7 17:43:27 2012 pid=16 (0x3e7518b8) determine_activation_state_old: Th$
Sat Jul 7 17:43:27 2012 pid=16 (0x3e7518b8) lookup_baseband_info_old: The SIM $
Sat Jul 7 17:43:27 2012 pid=16 (0x3e7518b8) extract_record_identifier: Could $
Sat Jul 7 17:43:27 2012 pid=16 (0x3e7518b8) load_activation_records: Could not$
Sat Jul 7 17:43:27 2012 pid=16 (0x3e7518b8) load_activation_records: This is a$
Sat Jul 7 17:43:27 2012 pid=16 (0x3e7518b8) dealwith_activation: No unlock rec$
Sat Jul 7 17:43:27 2012 pid=16 (0x3e7518b8) dealwith_activation: No care flag.$
Sat Jul 7 17:43:27 2012 pid=16 (0x3e7518b8) dealwith_activation: Looking up th$
Sat Jul 7 17:43:27 2012 pid=16 (0x3e7518b8) dealwith_activation: No record for$
Sat Jul 7 17:43:28 2012 pid=16 (0x3e7518b8) determine_activation_state_old: Th$
Sat Jul 7 17:43:28 2012 pid=16 (0x3e7518b8) determine_activation_state_old: Th$
Sat Jul 7 17:43:28 2012 pid=16 (0x3e7518b8) determine_activation_state_old: SI$
Sat Jul 7 17:43:28 2012 pid=16 (0x3e7518b8) determine_activation_state_old: Re$
Sat Jul 7 17:43:28 2012 pid=16 (0x3e7518b8) determine_activation_state_old: No$
Sat Jul 7 17:43:28 2012 pid=16 (0x3e7518b8) determine_activation_state_old: Th$
Sat Jul 7 17:43:28 2012 pid=16 (0x3e7518b8) deliver_baseband_ticket: SIM is no$
Sat Jul 7 17:43:28 2012 pid=16 (0x3e7518b8) determine_activation_state_old: Th$
Sat Jul 7 17:43:28 2012 pid=16 (0x3e7518b8) lookup_baseband_info_old: The SIM $
[ Read 531 lines ]
```



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).