NLECTC NIJ
Criminal Justice
Electronic Crime Technology
Center of Excellence

Lantern

Version 2.0.4

EVALUATION REPORT

December 2011

NLECTC NIJ

Criminal Justice
Electronic Crime Technology
Center of Excellence

NIJ Electronic Crime Technology Center of Excellence
550 Marshall St., Suite B
Phillipsburg, NJ 08865
www.ECTCoE.org

NIJ ECTCOE TESTING AND EVALUATION PROJECT STAFF

Robert J. O’Leary, CFCE; DFCP
Russell Yawn, CFCE
Chester Hosmer
Mark Davis, Ph.D.
Donald Stewart, CFCE; ACE
Randy Becker, CFCE
Jacob Fonseca
Michael Terminelli, ACE
Victor Fay-Wolfe, Ph.D.
Kristen McCooey, CCE; ACE
Laurie Ann O’Leary

Table of Contents

Introduction

The National Institute of Justice (NIJ) Electronic Crime Technology Center of Excellence (ECTCoE) has been assigned the responsibility of conducting electronic crime and digital evidence tool, technology and training testing and evaluations in support of the NIJ Research, Development, Testing and Evaluation (RDT&E) process.

The National Institute of Justice RDT&E process helps ensure that NIJ's research portfolios are aligned to best address the technology needs of the criminal justice community. The rigorous process has five phases:

- **Phase I: Determine technology needs principally in partnership with the Law Enforcement and Corrections Technology Advisory Council (LECTAC) and the appropiate Technology Working Group (TWG).** NIJ identifies criminal justice practitioners' functional requirements for new tools and technologies. (For more information on LECTAC and the TWGs, visit http://www,justnet.org).
- **Phase II: Develop technology program plans to address those needs.** NIJ creates a multiyear research program to address the needs identified in Phase I. One of the first steps is to determine whether products that meet those needs currently exist or whether they must be developed. If a solution is already available, Phases II and III are not necessary, and NIJ moves directly to demonstration, testing and evaluation in Phase IV. If solutions do not currently exist, they are solicited through annual, competitively awarded science and technology solicitations and TWG members help review the applications.
- **Phase III: Develop solutions**. Appropriate solicitations are developed and grantees are selected through an open, competitive, peer-reviewed process. After grants are awarded, the grantee and the NIJ program manager then work collaboratively to develop the solutions.
- **Phase IV: Demonstrate, test, evaluate and adopt potential solutions into practice.** A potential solution is tested to determine how well it addresses the intended functional requirement. NIJ then works with first-adopting agencies to facilitate the introduction of the solution into practice. After adoption, the solution's impact on practice is evaluated. During the testing and evaluation process, performance standards and guides are developed (as appropriate) to ensure safety and effectiveness; not all new solutions will require the publication of new standards or guides.
- **Phase V: Build capacity and conduct outreach to ensure that the new tool or technology benefits practitioners.** NIJ publishes guides and standards and provides technology assistance to second adopters.[1]

The High Priority Criminal Justice Technology Needs are organized into five functional areas:

- Protecting the Public.
- Ensuring Officer Safety.
- Confirming the Guilty and Protecting the Innocent.
- Improving the Efficiency of Justice.
- Enabling Informed Decision-Making.

The NIJ ECTCoE tool, technology and training evaluation and testing reports support the NIJ RDT&E process, which addresses high priority needs for criminal justice technology.

[1] *National Institute of Justice High-Priority Criminal Justice Technology Needs,* March 2009 NCJ 225375.

Overview

With the Apple® product line of iPhone, iPad and iPod Touch becoming more and more popular, there is a need for state and local law enforcement to have access to a cost-effective tool to process these devices. As the number of these devices on the market continues to grow, state and local law enforcement processing digital evidence will encounter them in greater numbers. These devices use an operating system derived from the Apple Mac OS X® operating system, and although traditional examination tools will work, they produce results that may be difficult to interpret. Lantern, a tool native to the OS X operating system, provides more meaningful results to an investigator.

Product Information

Lantern, from Katana Forensics,[2] makes the task of recovering and examining the data contained on any iPhone, iPad or iPod a simple process and presents the examiner with easily understandable results. Lantern is one of the few products that can process these devices using the native Mac OS X operating system. According to Katana's website, (Fall 2010):

> "Lantern is the most cost-effective Mac-based tool for the iOS Devices (iPhone, iPod Touch, iPad)." Additionally, "The iPhone, iPod Touch and iPad has given examiners great pains in the extraction of evidence. Katana's tools are developed so that it can be used by law enforcement and civilian examiners alike. With case backlog, limited resources and time, Katana's tools are designed to quickly extract the data and present it is an intuitive manner. Katana uses the tools available to it from the operating system, so there isn't a need to add external viewers to view the data."

Product Description

The following is a description of Lantern from the Katana Forensic website:

> "Katana Forensics, a leading authority in iOS forensics, has developed Lantern. Lantern is an application to analyze data from iOS devices, backup files and physical images. Lantern was specifically designed for the law enforcement, government and corporate examiners."

> "Lantern 2 is the fastest and most cost-effective iOS forensic solution. Lantern was designed to acquire and analyze data from iOS devices (iPhone, iPod Touch, iPad)."

Lantern will Acquire from the following iOS devices:

- iPhones.
- iPads.
- iPod Touch.

Lantern will Analyze the following types of files:

- iOS Devices.
- Backup files.
- Physical RAW dd and .dmg image files of iOS Devices.

[2] http://katanaforensics.com/

Special Features

The following are some special features listed on Lantern's website:

- Start to immediately examine data while Lantern 2 is still processing.
- Lantern 2 carves for images and video from physical images.
- Logical and physical e-mail analysis.
- Document analysis to include third-party applications.
- Timeline analysis and geographic data taken to the next level.
- More mapping than any other application using more powerful Google Earth KMZ exporting.

Target Customers

From the Katana Forensics website:

> "Lantern is sold only to Law Enforcement Agencies, Government Agencies and Corporate examiners."

Evaluation and Testing of Lantern

Test Bed Configuration

Latern was used to examine two iPhones, a 3GS and a 4, and an iPad. An iPod Touch was not evaluated in this review. The details for each device are included below.

iPhone 4

- Memory 64GB.
- Model A1332 30GB.
- Version 4.2.1 (8C148).
- 146 Applications.
- 337 Photos.
- 76 Videos.
- 1454 Songs.

iPhone 3G

- Memory 8GB.
- Model.
- Version.
- Applications.
- Photos.
- Videos.
- Songs.

iPad

- Memory 16GB.
- Model MC349LL.
- Version 4.2.1 (8C148).
- 149 Applications.
- 191 Photos.
- 3 Videos.
- 881 Songs.

Initial Setup

Members of the NIJ ECTCoE used each of the devices so that the usage and the data contained would be known.The two iPhones were used over an extended period of time and the iPad was used for eight months. These devices were used in real-world settings so that the data contained would be similar to the type of data encountered by state and local law enforcement personnel during the examination of such devices. Some of the features used include, but were not limited to:

- Phone calls to include incoming, outgoing and missed.
- E-mail sent and received.
- Web searches.
- Text messages sent received and deleted.
- Photographs taken on the iPhone 4 only.
- Movies taken using the iPhone 4 only.
- Photographs stored on the device.
- Calendar.
- Mapping where applicable.

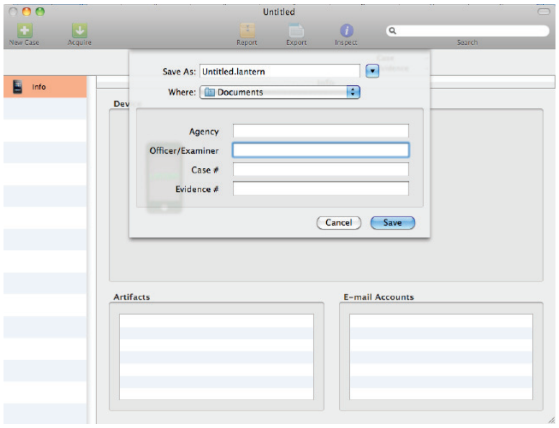
Testing

The following steps were taken in the testing of the Lantern software:

1. For each device, the SIM card was removed and the device placed into airplane mode.[3]

2. Each device was connected to a MacBook Pro laptop running version 10.6.6 of the OS X operating system with the Lantern software, version 2.0.4.

3. A new case was started.



Save As: Untitled.lantern

Where: Documents

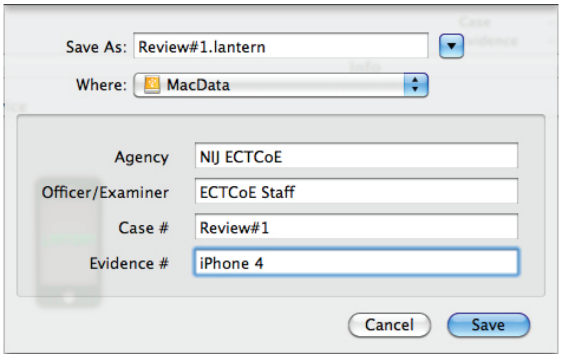
Agency

Officer/Examiner

Case #

Evidence #

When a new case is started the user is presented with this screen. For this test, the agency is the "NIJ ECTCoE," the Officer/Examiner is "ECTCoE Staff," the Case # is "Review#1" and the Evidence number is "iPhone 4."



Save As: Review#1.lantern

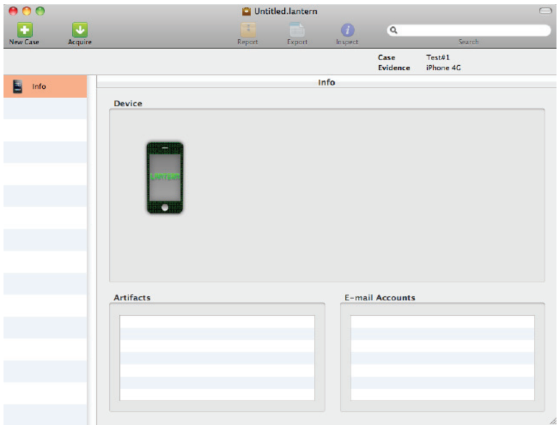
Where: MacData

Agency: NIJ ECTCoE

Officer/Examiner: ECTCoE Staff

Case #: Review#1

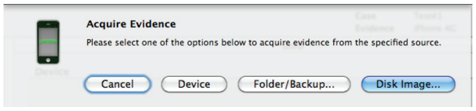
Evidence #: iPhone 4



Case: Test#1

Evidence: iPhone 4G

4. After the case information is entered and the Acquire button selected, the user is asked what type of data is to be acquired or used.



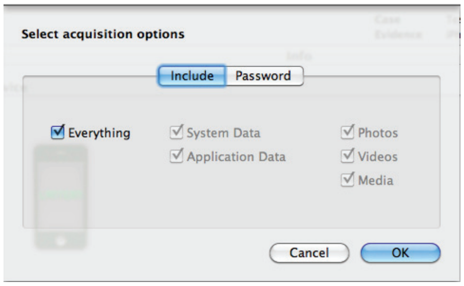
Acquire Evidence

Please select one of the options below to acquire evidence from the specified source.

Lantern will process an individual device, a selected folder/backup, or a disk image produced by other tools. The Device button was selected for this review.

5. On the Select acquisition options screen, the Everything option was selected.

[3] Flight mode, also called airplane mode, is a setting available on many cell phones and other electronic devices that, when engaged, suspends many of the device's signal transmitting functions – thereby disabling the device's capacity to place or receive calls or text messages – while still permitting use of other functions that do not require signal transmission (e.g., games, built-in camera, MP3 player). The name is derived from the fact that it permits the user to operate the device while on board a commercial aircraft while in flight, where the operation of cell phones and other devices that send or receive signals is generally prohibited due to the potential impact on aircraft avionics and the potential for interference with ground cell networks. (http://en.wikipedia.org/wiki/Flight_mode)



Select acquisition options

Include | Password

☑ Everything

☑ System Data

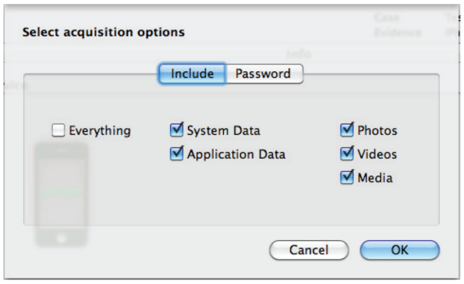
☑ Application Data

☑ Photos

☑ Videos

☑ Media

The user can also select only those areas of interest.



Select acquisition options

Include | Password

☐ Everything

☑ System Data

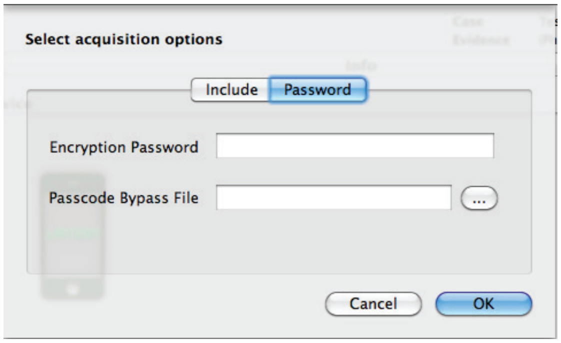
☑ Application Data

☑ Photos

☑ Videos

☑ Media

6. The passcode bypass screen was presented. If the device has a password enabled, or the passcode file has been obtained, that information can be entered on this screen.



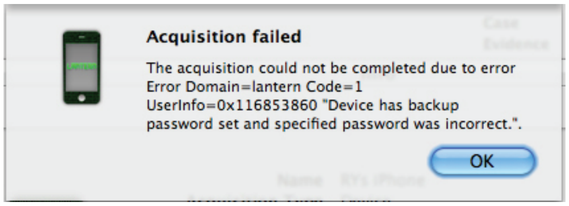
Select acquisition options

Include | Password

Encryption Password

Passcode Bypass File

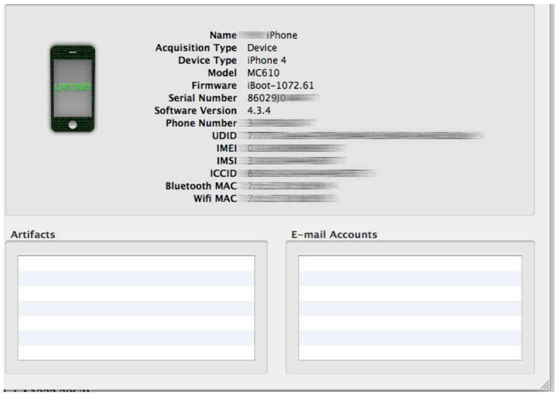
If the device under examination has a password that is unknown or the passcode file cannot be obtained, the user will be presented with the following notification.



Acquisition failed

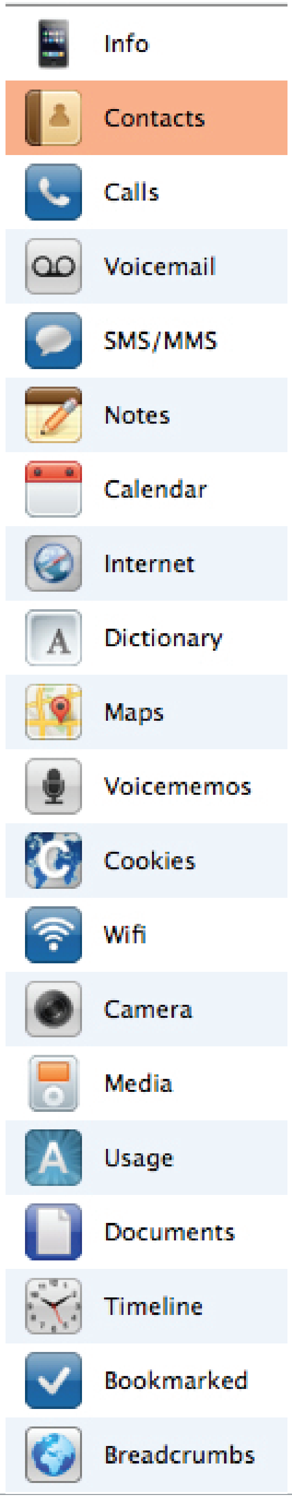
The acquisition could not be completed due to error Error Domain=lantern Code=1 UserInfo=0x116853860 "Device has backup password set and specified password was incorrect.".

7. Once the Acquire button is selected, the acquisition process begins. After a few seconds, the information relating to the device is displayed.



Name	[redacted] iPhone
Acquisition Type	Device
Device Type	iPhone 4
Model	MC610
Firmware	iBoot-1072.61
Serial Number	86029J0[redacted]
Software Version	4.3.4
Phone Number	[redacted]
UDID	[redacted]
IMEI	[redacted]
IMSI	[redacted]
ICCID	[redacted]
Bluetooth MAC	[redacted]
Wifi MAC	[redacted]

8. Each device was acquired and the results viewed in the Lantern interface. On the right side of the interface is a column with the different report sections that are available as shown in the screenshot on the next page. A report for each device was produced.



Results

The menu oriented down the left-hand side of the screen allows the examiner or the case agent to quickly inspect those areas of interest. Most applications create an image of the data. Lantern does not and copies out those areas defined at the start of the processing. This feature allows the examiner to further process the recovered data with other tools available to the examiner or tools that the examiner is familiar with. For example, an examiner might want to further examine the database file that contains the SMS messages. Using an application that can interpret the SQLite database format, the examiner can further examine the recovered data.

The following list is a description of each section of the reports and the information it contains.

- Info

  The info tab contained all of the information that was displayed during the initial acquisition which was identical to what had been displayed on the device.

- Contacts

  The contacts listed in under this tab were compared to the contacts of the synced computer for accuracy. All of the contact information was there and Lantern was able to distinguish between the originating contact, whether entered into the address book and then synced with the device or entered directly on each device.

- Calls

  Lantern was able to recover the recent phone calls made with each device and was able to determine whether the call was outgoing, incoming or missed along with the associated date and time stamps. Note: This did not apply to the iPad.

- Voicemail

  Lantern was able to recover the voicemails that had been left on each device, including deleted voicemail messages with date and time stamps of the message recording. When highlighting a voicemail message, the examiner can listen to the voicemail message by using the built-in function of preview found in the OS X operating system. Note: This did not apply to the iPad.

- SMS/MMS

  Lantern recovered sent, received and deleted SMS/MMS messages with date and time stamps of when the message was sent or received. Note: This did not apply to the iPad.

- Notes

  Lantern was able to recover all of the notes on each device.

- Calendar

  Lantern was able to recover all of the calendar entries that were still active on each device.

- Internet

  Lantern successfully recovered the Internet history and the sites visited from each device.

- Dictionary

  Lantern recovered the plist file that contains the words as entered by the user as well as displays the index order of when a word was entered on each device.

- Maps

  Lantern recovered all of the locations previously searched for using the map function on each device.

- Voicememos

  Lantern was able to recover active voicememos on each device including the date and time when it was recorded. As with the voicemail messages, the examiner can listen to each voicememo using the preview function of OS X. Note: This did not apply to the iPad.

- Cookies

  Lantern was able to interpret all of the cookies contained on each device and was able to include the application name or website address, the name of the cookie, domain, path value and the expiration date.

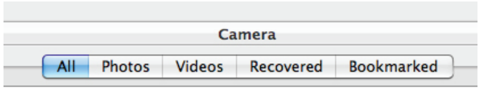
- Wifi

  Lantern displayed the wifi access points each device has been associated with in the past. Included in the results were the date of the event, the event type, whether it was a first join event or a last join event, the SSID of the access point, the MAC address of the access point and whether security was enabled on the access point.

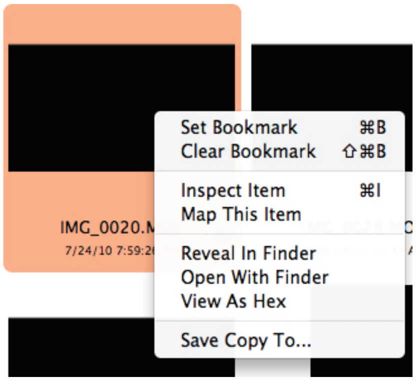
- Camera

  Lantern was able to recover all of the images stored and/or taken with each device, including the deleted images/videos. Note: This did not apply to the iPad.

  Under the camera tab is where the user will find all of the still images and/or the videos taken or stored on his device. Note: This was only the iPhone 4. The iPhone 3 and iPad tested in this review were not capable of taking pictures or video. When this report section is selected, the user is presented with a tabbed display as shown.



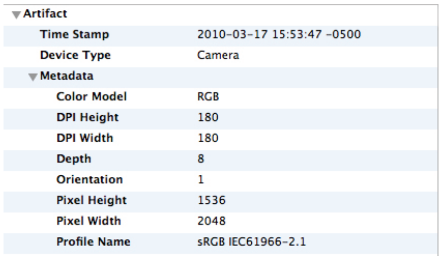
When the All button is selected, all of the media contained on this device is presented. When the Photos button is selected, only the still images are displayed and are sorted by date and time stamp. When the user selects an image and right-clicks, additional information is available as depicted in the follow examples as applies to both still images and video files.



Selecting Set Bookmark will include the selected image into the report and Clear Bookmark removes that image from the report.

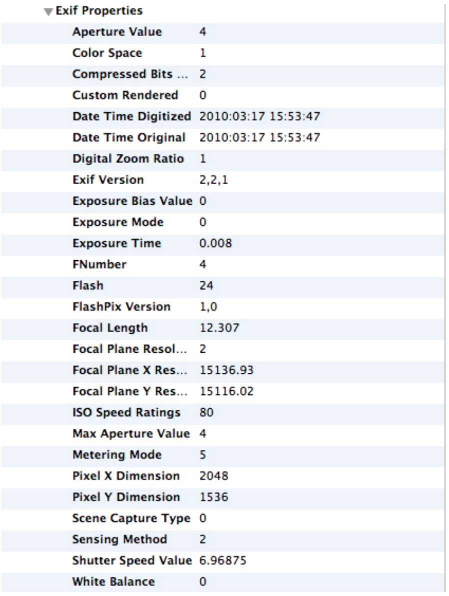
Information that is available from the Inspect menu option:

❐ Artifact Data



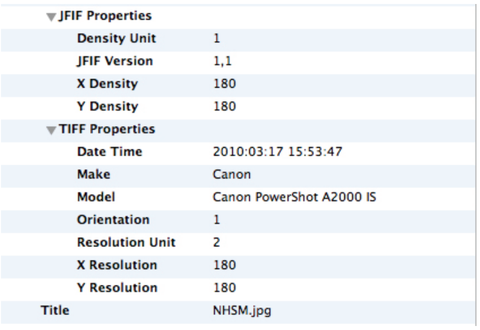
▼Artifact	
Time Stamp	2010-03-17 15:53:47 -0500
Device Type	Camera
▼Metadata	
Color Model	RGB
DPI Height	180
DPI Width	180
Depth	8
Orientation	1
Pixel Height	1536
Pixel Width	2048
Profile Name	sRGB IEC61966-2.1

❐ Exif Properties



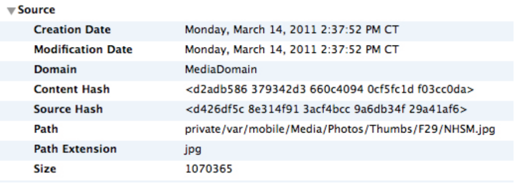
▼Exif Properties	
Aperture Value	4
Color Space	1
Compressed Bits ...	2
Custom Rendered	0
Date Time Digitized	2010:03:17 15:53:47
Date Time Original	2010:03:17 15:53:47
Digital Zoom Ratio	1
Exif Version	2,2,1
Exposure Bias Value	0
Exposure Mode	0
Exposure Time	0.008
FNumber	4
Flash	24
FlashPix Version	1,0
Focal Length	12.307
Focal Plane Resol...	2
Focal Plane X Res...	15136.93
Focal Plane Y Res...	15116.02
ISO Speed Ratings	80
Max Aperture Value	4
Metering Mode	5
Pixel X Dimension	2048
Pixel Y Dimension	1536
Scene Capture Type	0
Sensing Method	2
Shutter Speed Value	6.96875
White Balance	0

❐ JFIF/TIFF Information



▼JFIF Properties	
Density Unit	1
JFIF Version	1,1
X Density	180
Y Density	180
▼TIFF Properties	
Date Time	2010:03:17 15:53:47
Make	Canon
Model	Canon PowerShot A2000 IS
Orientation	1
Resolution Unit	2
X Resolution	180
Y Resolution	180
Title	NHSM.jpg

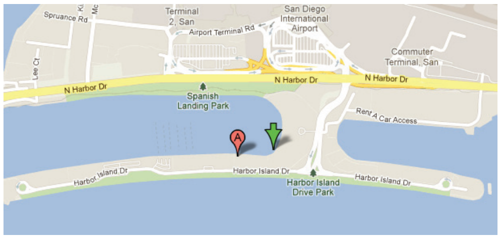
- Additional source data



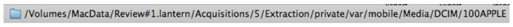
▼ Source

Creation Date	Monday, March 14, 2011 2:37:52 PM CT
Modification Date	Monday, March 14, 2011 2:37:52 PM CT
Domain	MediaDomain
Content Hash	<d2adb586 379342d3 660c4094 0cf5fc1d f03cc0da>
Source Hash	<d426df5c 8e314f91 3acf4bcc 9a6db34f 29a41af6>
Path	private/var/mobile/Media/Photos/Thumbs/F29/NHSM.jpg
Path Extension	jpg
Size	1070365

- Selecting Map This Item will display the location where the image was taken, if the GPS data is available and is based on the assisted GPS data that was recorded at the time.

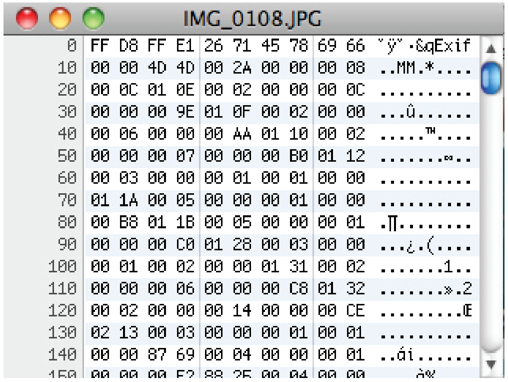


- Selecting Reveal in Finder will show the location on the examiner's machine where this data was written.



/Volumes/MacData/Review#1.lantern/Acquisitions/5/Extraction/private/var/mobile/Media/DCIM/100APPLE

- Open With Finder will open the selected image using the default graphic image application. View as Hex will show the selected data in a hex viewer.



IMG_0108.JPG

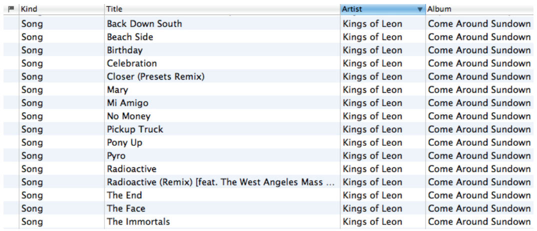
```
  0  FF D8 FF E1 26 71 45 78 69 66  ˇÿˇ·&qExif
 10  00 00 4D 4D 00 2A 00 00 00 08  ..MM.*....
 20  00 0C 01 0E 00 02 00 00 00 0C  ..........
 30  00 00 00 9E 01 0F 00 02 00 00  ...û......
 40  00 06 00 00 00 AA 01 10 00 02  .....™....
 50  00 00 00 07 00 00 00 B0 01 12  .......∞..
 60  00 03 00 00 00 01 00 01 00 00  ..........
 70  01 1A 00 05 00 00 00 01 00 00  ..........
 80  00 B8 01 1B 00 05 00 00 00 01  .∏........
 90  00 00 00 C0 01 28 00 03 00 00  ...¿.(....
100  00 01 00 02 00 00 01 31 00 02  .......1..
110  00 00 00 06 00 00 00 C8 01 32  .......».2
120  00 02 00 00 00 14 00 00 00 CE  .........Œ
130  02 13 00 03 00 00 00 01 00 01  ..........
140  00 00 87 69 00 04 00 00 00 01  ..ái......
150  00 00 00 F2 88 25 00 04 00 00  ....à%....
```

- The last option, Save Copy To, will allow the examiner to export a copy of the selected image out for further use and/or processing.

Media

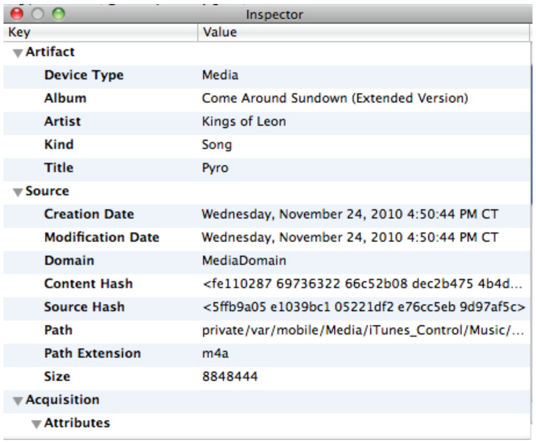
This software was able to successfully recover all of the audio files contained on this device. Lantern was not able to recover the imported video, in this case, a mp4 movie file.

Under the Media tab the examiner will find all of the audio files contained on the device.



Kind	Title	Artist	Album
Song	Back Down South	Kings of Leon	Come Around Sundown
Song	Beach Side	Kings of Leon	Come Around Sundown
Song	Birthday	Kings of Leon	Come Around Sundown
Song	Celebration	Kings of Leon	Come Around Sundown
Song	Closer (Presets Remix)	Kings of Leon	Come Around Sundown
Song	Mary	Kings of Leon	Come Around Sundown
Song	Mi Amigo	Kings of Leon	Come Around Sundown
Song	No Money	Kings of Leon	Come Around Sundown
Song	Pickup Truck	Kings of Leon	Come Around Sundown
Song	Pony Up	Kings of Leon	Come Around Sundown
Song	Pyro	Kings of Leon	Come Around Sundown
Song	Radioactive	Kings of Leon	Come Around Sundown
Song	Radioactive (Remix) [feat. The West Angeles Mass ...	Kings of Leon	Come Around Sundown
Song	The End	Kings of Leon	Come Around Sundown
Song	The Face	Kings of Leon	Come Around Sundown
Song	The Immortals	Kings of Leon	Come Around Sundown

Just as with several other choices, the user can right click on the audio file and see additional information about that file.

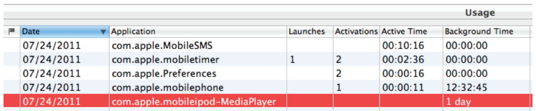


Inspector

Key	Value
▼ **Artifact**	
Device Type	Media
Album	Come Around Sundown (Extended Version)
Artist	Kings of Leon
Kind	Song
Title	Pyro
▼ **Source**	
Creation Date	Wednesday, November 24, 2010 4:50:44 PM CT
Modification Date	Wednesday, November 24, 2010 4:50:44 PM CT
Domain	MediaDomain
Content Hash	<fe110287 69736322 66c52b08 dec2b475 4b4d...
Source Hash	<5ffb9a05 e1039bc1 05221df2 e76cc5eb 9d97af5c>
Path	private/var/mobile/Media/iTunes_Control/Music/...
Path Extension	m4a
Size	8848444
▼ **Acquisition**	
▼ **Attributes**	

Usage

The data found under this tab gives the user an idea about how many times an application has been used as well as how long that application has been running either in the foreground or in the background.

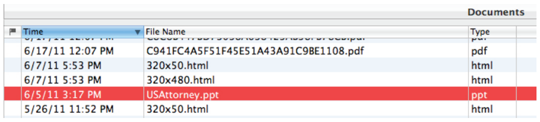


Usage

	Date	Application	Launches	Activations	Active Time	Background Time
	07/24/2011	com.apple.MobileSMS			00:10:16	00:00:00
	07/24/2011	com.apple.mobiletimer	1	2	00:02:36	00:00:00
	07/24/2011	com.apple.Preferences		2	00:00:16	00:00:00
	07/24/2011	com.apple.mobilephone		1	00:00:11	12:32:45
	07/24/2011	com.apple.mobileipod-MediaPlayer				1 day

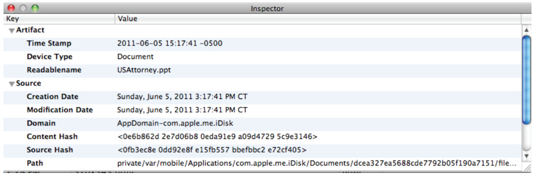
Documents

Any documents, such as pdf files, text files, word files, powerpoint files a well as some graphic image files that were downloaded from the Internet can be found under this section.



Documents

	Time	File Name	Type
	6/17/11 12:07 PM	C941FC4A5F51F45E51A43A91C9BE1108.pdf	pdf
	6/7/11 5:53 PM	320x50.html	html
	6/7/11 5:53 PM	320x480.html	html
	6/5/11 3:17 PM	USAttorney.ppt	ppt
	5/26/11 11:52 PM	320x50.html	html

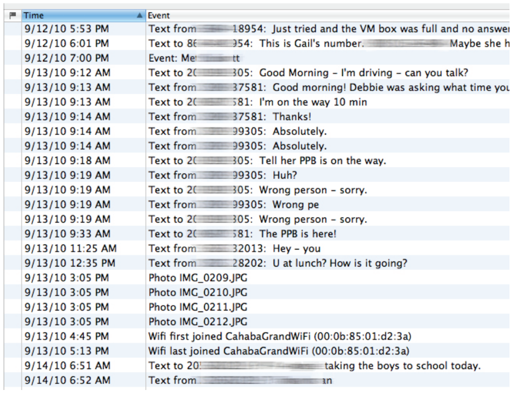


Inspector

Key	Value
▼ Artifact	
Time Stamp	2011-06-05 15:17:41 -0500
Device Type	Document
Readablename	USAttorney.ppt
▼ Source	
Creation Date	Sunday, June 5, 2011 3:17:41 PM CT
Modification Date	Sunday, June 5, 2011 3:17:41 PM CT
Domain	AppDomain-com.apple.me.iDisk
Content Hash	<0e6b862d 2e7d06b8 0eda91e9 a09d4729 5c9e3146>
Source Hash	<0fb3ec8e 0dd92e8f e15fb557 bbefbbc2 e72cf405>
Path	private/var/mobile/Applications/com.apple.me.iDisk/Documents/dcea327ea5688cde7792b05f190a7151/file...

Timeline

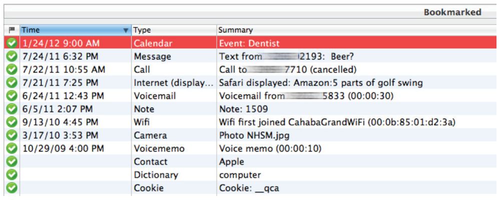
This section will list all of the events associated with each device and display the events chronologically. As with the other sections, the inspector will reveal additional data about a selected entry.



	Time	Event
	9/12/10 5:53 PM	Text from [redacted]18954: Just tried and the VM box was full and no answe
	9/12/10 6:01 PM	Text to 86[redacted]954: This is Gail's number. [redacted] Maybe she h
	9/12/10 7:00 PM	Event: Me[redacted]tt
	9/13/10 9:12 AM	Text to 2([redacted]305: Good Morning - I'm driving - can you talk?
	9/13/10 9:13 AM	Text from [redacted]37581: Good morning! Debbie was asking what time you
	9/13/10 9:13 AM	Text to 2([redacted]581: I'm on the way 10 min
	9/13/10 9:14 AM	Text from [redacted]37581: Thanks!
	9/13/10 9:14 AM	Text from [redacted]99305: Absolutely.
	9/13/10 9:14 AM	Text from [redacted]99305: Absolutely.
	9/13/10 9:18 AM	Text to 2([redacted]305: Tell her PPB is on the way.
	9/13/10 9:19 AM	Text from [redacted]99305: Huh?
	9/13/10 9:19 AM	Text to 2([redacted]305: Wrong person - sorry.
	9/13/10 9:19 AM	Text from [redacted]99305: Wrong pe
	9/13/10 9:19 AM	Text to 2([redacted]305: Wrong person - sorry.
	9/13/10 9:33 AM	Text to 2([redacted]581: The PPB is here!
	9/13/10 11:25 AM	Text from [redacted]32013: Hey - you
	9/13/10 12:35 PM	Text from [redacted]28202: U at lunch? How is it going?
	9/13/10 3:05 PM	Photo IMG_0209.JPG
	9/13/10 3:05 PM	Photo IMG_0210.JPG
	9/13/10 3:05 PM	Photo IMG_0211.JPG
	9/13/10 3:05 PM	Photo IMG_0212.JPG
	9/13/10 4:45 PM	Wifi first joined CahabaGrandWiFi (00:0b:85:01:d2:3a)
	9/13/10 5:13 PM	Wifi last joined CahabaGrandWiFi (00:0b:85:01:d2:3a)
	9/14/10 6:51 AM	Text to 20[redacted]taking the boys to school today.
	9/14/10 6:52 AM	Text from [redacted]an

Bookmarked

The Bookmarked section only displays those items that have been bookmarked by the examiner.

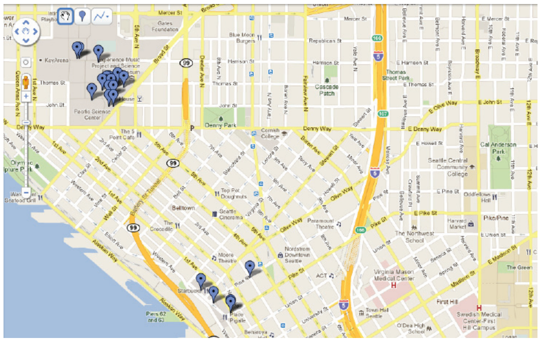


Bookmarked

	Time	Type	Summary
✓	1/24/12 9:00 AM	Calendar	Event: Dentist
✓	7/24/11 6:32 PM	Message	Text from [redacted]2193: Beer?
✓	7/22/11 10:55 AM	Call	Call to [redacted]7710 (cancelled)
✓	7/21/11 7:25 PM	Internet (display...	Safari displayed: Amazon:5 parts of golf swing
✓	6/24/11 12:43 PM	Voicemail	Voicemail from [redacted]5833 (00:00:30)
✓	6/5/11 2:07 PM	Note	Note: 1509
✓	9/13/10 4:45 PM	Wifi	Wifi first joined CahabaGrandWiFi (00:0b:85:01:d2:3a)
✓	3/17/10 3:53 PM	Camera	Photo NHSM.jpg
✓	10/29/09 4:00 PM	Voicememo	Voice memo (00:00:10)
✓		Contact	Apple
✓		Dictionary	computer
✓		Cookie	Cookie: __qca

Breadcrumbs

The Breadcrumbs section will allow the user to export a list containing the data of when still images or video are recovered, if applicable, and export that data into CVS, KMZ or XML formats. Exporting the data into a KMZ file and importing into an application such as Google Maps allows the user to plot the GPS coordinates on a map.



Conclusion

Each respective device was captured utilizing the Lantern software. Due to the overwhelming amount of data recovered by this software, it isn't feasible to include the full report on each device in this evaluation. However, upon request, the full report will be made available with personal information redacted.

The tested features of Lantern performed as advertised. Lantern is a product that captures the logical data from the iPhone, iPod and iPad. It does not capture a full physical image, nor does it claim to. Of the data captured, the output of Lantern is impressive. It is one of the few, if not the only tool, that allows the examiner to hear the voicemail messages recovered from the device along with the associated metadata. It should be noted that the voicemail messages were recovered from the device itself and from no other source.

The application is easy to use and the interface layout is logical and intuitive. It is as easy as putting the device in airplane mode, connecting to a computer running Lantern, and selecting the areas sought or defined by the court order, search warrant or consent.