Table of Contents

Introduction ................................................................................................................................................................1

Overview.....................................................................................................................................................................3
  Product Information ..............................................................................................................................................3
  Product Description .............................................................................................................................................3
  Special Features ...................................................................................................................................................4
  Target Customers .................................................................................................................................................4

Evaluation and Testing of Lantern ...........................................................................................................................5
  Test Bed Configuration.........................................................................................................................................5
    iPhone 4 ........................................................................................................................................................5
    iPhone 3G .....................................................................................................................................................5
    iPad ..............................................................................................................................................................5
    Initial Setup ...................................................................................................................................................5
  Testing ..................................................................................................................................................................6
  Results .............................................................................................................................................................8

Conclusion ...............................................................................................................................................................13
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 appropriate 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.

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, 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 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.

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.

iPhone 3G

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

iPad

- Memory 16GB.
- Model MC349LL.
**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.

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.”

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.

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)
The user can also select only those areas of interest.

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.

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.

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

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.
Evaluation and Testing of Lantern

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 following examples as applies to both still images and video files.

### Artifact Data

<table>
<thead>
<tr>
<th>Artifact</th>
<th>Time Stamp</th>
<th>2010-03-17 15:53:47 -0500</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Device Type</td>
<td>Camera</td>
</tr>
<tr>
<td></td>
<td>Color Model</td>
<td>RGB</td>
</tr>
<tr>
<td></td>
<td>DMR Height</td>
<td>180</td>
</tr>
<tr>
<td></td>
<td>DMR Width</td>
<td>180</td>
</tr>
<tr>
<td></td>
<td>Depth</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Orientation</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Pixel Height</td>
<td>1536</td>
</tr>
<tr>
<td></td>
<td>Pixel Width</td>
<td>2048</td>
</tr>
<tr>
<td></td>
<td>Profile Name</td>
<td>sRGB:EC81965-2.1</td>
</tr>
</tbody>
</table>

### Exif Properties

<table>
<thead>
<tr>
<th>Exif Properties</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Aperture Value</td>
<td>4</td>
</tr>
<tr>
<td>Color Space</td>
<td>1</td>
</tr>
<tr>
<td>Compressed Bits</td>
<td>2</td>
</tr>
<tr>
<td>Custom Rendered</td>
<td>0</td>
</tr>
<tr>
<td>Date Time Digitalized</td>
<td>2010-03-17 15:53:47</td>
</tr>
<tr>
<td>Date Time Original</td>
<td>2010-03-17 15:53:47</td>
</tr>
<tr>
<td>Digital Zoom Ratio</td>
<td>1</td>
</tr>
<tr>
<td>Exif Version</td>
<td>2.2.1</td>
</tr>
<tr>
<td>Exposure Bias Value</td>
<td>0</td>
</tr>
<tr>
<td>Exposure Mode</td>
<td>0</td>
</tr>
<tr>
<td>Exposure Time</td>
<td>0.004</td>
</tr>
<tr>
<td>Fnumber</td>
<td>4</td>
</tr>
<tr>
<td>Flash</td>
<td>24</td>
</tr>
<tr>
<td>FlashPix Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Focal Length</td>
<td>12.357</td>
</tr>
<tr>
<td>Focal Plane Resol</td>
<td>2</td>
</tr>
<tr>
<td>Focal Plane X Resol</td>
<td>15136.33</td>
</tr>
<tr>
<td>Focal Plane Y Resol</td>
<td>15138.02</td>
</tr>
<tr>
<td>ISO Speed Ratings</td>
<td>80</td>
</tr>
<tr>
<td>Max Aperture Value</td>
<td>4</td>
</tr>
<tr>
<td>Metering Mode</td>
<td>5</td>
</tr>
<tr>
<td>Pixel X Dimension</td>
<td>2048</td>
</tr>
<tr>
<td>Pixel Y Dimension</td>
<td>1536</td>
</tr>
<tr>
<td>Scene Capture Type</td>
<td>0</td>
</tr>
<tr>
<td>Sensing Method</td>
<td>2</td>
</tr>
<tr>
<td>Shutter Speed Value</td>
<td>6.96875</td>
</tr>
<tr>
<td>White Balance</td>
<td>0</td>
</tr>
</tbody>
</table>

### JFIF/TIFF Information

<table>
<thead>
<tr>
<th>JFIF Properties</th>
<th>Density Unit</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>JFIF Version</td>
<td>1.1</td>
</tr>
<tr>
<td></td>
<td>Y Density</td>
<td>180</td>
</tr>
<tr>
<td>TIFF Properties</td>
<td>Date Time</td>
<td>2010-03-17 15:53:47</td>
</tr>
<tr>
<td></td>
<td>Make</td>
<td>Canon</td>
</tr>
<tr>
<td></td>
<td>Model</td>
<td>Canon PowerShot A2000 IS</td>
</tr>
<tr>
<td></td>
<td>Orientation</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Resolution X</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>X Resolution</td>
<td>180</td>
</tr>
<tr>
<td></td>
<td>Y Resolution</td>
<td>180</td>
</tr>
<tr>
<td></td>
<td>Title</td>
<td>IMG_0108.jpg</td>
</tr>
</tbody>
</table>
Additional source data

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.

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.
Evaluation and Testing of Lantern

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.

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.

Bookmarked

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

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.