NLECTC NIJ

Criminal Justice
Electronic Crime Technology
Center of Excellence

Secure View

Version 3.4.0

EVALUATION REPORT

August 2012

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.
Michael Terminelli, ACE
Randy Becker, CFCE
Jacob Fonseca
Victor Fay-Wolfe, Ph.D.
Kristen McCooey, CCE; ACE
Laurie Ann O'Leary

Table of Contents

Introduction **1**

Overview **3**

Product Information 3

Product Description 3

Special Features 3

Target Customers 4

Law Enforcement Applications 4

Test Bed Configuration **5**

Evaluation and Testing of Secure View **7**

User Interface 7

Test 1 – LG VX-9100 10

Test 2 – Sanyo SCP-3100 10

Test 3 – RIM BlackBerry 8310 11

Test 4 – Apple iPhone 4S 11

Test 5 – LG C729 Double Play 12

Conclusion **13**

This report is current at the time of writing. Please be sure to check the vendor website for the latest version and updates.

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 NIJ 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.
- 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 world becoming more mobile every day, law enforcement is required to analyze greater numbers of mobile devices during the course of investigations. Many tools exists to aid law enforcement in processing these device; however, not every tool will support every device.

Susteen claims their software, Secure View, will acquire and analyze data from over 4,000 mobile phones. Secure View is a software platform that installs onto a computer workstation. Secure View also includes a toolkit of cables and hardware for connecting devices to the workstation.

Product Information

The following information is from Susteen's website:

> Susteen has leveraged our experience and cellphone data transfer (DataPilot) and created a mobile device investigation tool called Secure View. Secure View was introduced to the law enforcement world in 2007, and Susteen has increased our user base steadily since. We have been a cornerstone of many cellphone investigations and we are continuing to push the envelope to introduce better products and features. Our technology team has created features for analytics (svProbe), intelligence gathering (svSmart), password unlocking (svPin) and integration tool (svLoader). We will continue to gather market information to create products that standardize and streamline law enforcement processes.
>
> Our commitment and understanding of the law enforcement market shows in the many different law enforcement agencies that use our product. We continue to create and maintain relationships to stay as a market leader. We welcome open dialogue with users and nonusers to create and better our products. We hope to continue to produce products to help put "bad guys" behind bars.

Product Description

The following information is from Susteen's website:

> The "Go To" tool for the cellphone forensic investigator, whether from the law enforcement, consultant, corporate or the military world.
>
> You'll have access to unified advances in support, data management and reporting. Secure View should be the most versatile tool in your arsenal. Complete Data Cable Kit included.

Special Features

The following information is from the Susteen's website:

- Streamline Acquisition Process.
- Enhanced Smart Phone Acquisition of Text (SMS/MMS) Data.
- Complete Data Processing Capability.
- Bookmarking and Noting Features.
- Complete Report with Secondary Evidence Report Option.
- Web History Analytics.
- Time Line Analytics.
- Social Network Analytics.
- WHQL (Microsoft Tested and Approved) Driver.
- Supporting Windows 32 and 64 Bit.
- Widely used and trusted by local, state and federal government agencies.

- Acquire, analyze and report on one easy to use platform.
- Product training and certification available.
- Forensic process with MD5 HASHING.
- Audit trail features.
- Word search capabilities.
- Licensing options available.
- Supports 4000+ phones.
- Includes complete cable kit.
- Includes hard-sided carrying case.

Target Customers

The target customers for Susteen's Secure View are state and local law enforcement organizations that maintain a separate unit for forensic examinations of digital media. Secure View is a forensic grade acquisition and analysis tool that is capable of creating reports that can be customized with an organization's and investigator's information and notes. These reports are created and presented in an easy-to-read format.

Law Enforcement Applications

Secure View is designed to assist state and local law enforcement with the logical acquisition of and reporting on examinations of cell phones.

Test Bed Configuration

Prior to downloading Secure View, the user manual was reviewed. The manual is informative and contains screenshots of the installation, configuration and use of the program. A detailed explanation of each type of report that can be generated is provided in the user manual.

The test machine is a Dell Optiplex 760 with a clean Windows 7 x64 installation, 4GB of RAM and a 2.66 GHz Intel Core 2 Duo processor. Installed on this machine was the Secure View application.

The phones that were selected for testing were chosen because they represent the different types of widely used phone technologies (CDMA and GSM).

Evaluation and Testing of Secure View

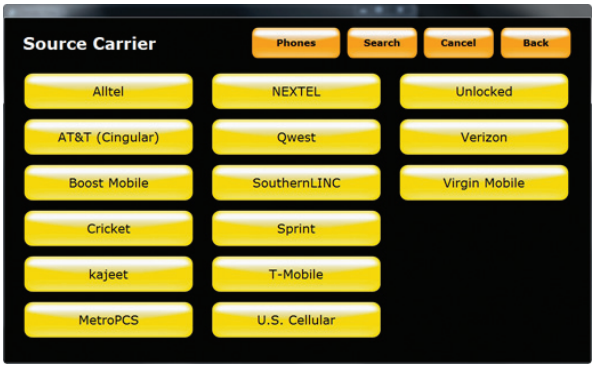
User Interface

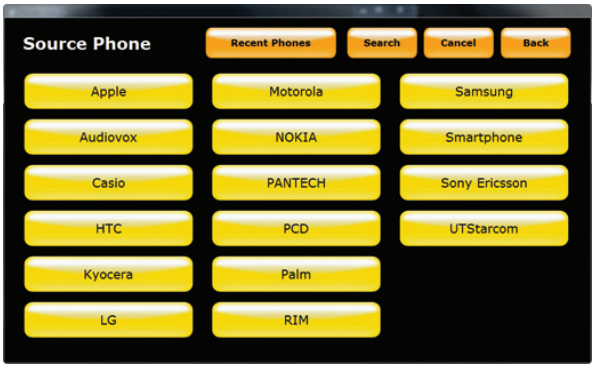
The interface for extraction from a device is easy to follow. Large, colorful buttons direct the user through the extraction process. When started, the application displays the startup menu, with the options to extract information from a new device, analyze a previous extraction or print a report from a previous extraction or analysis.

Each extraction in the following tests to were performed with the following procedure:

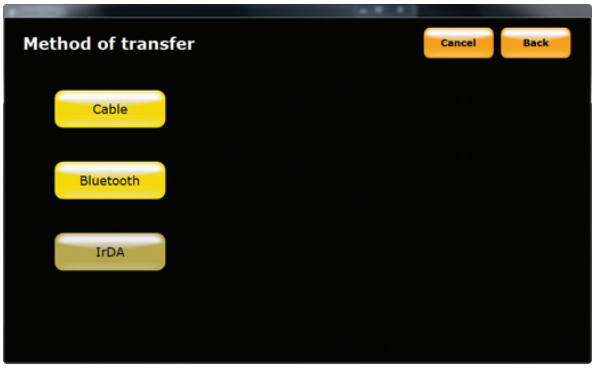
1. Selected “AQUIRE” from the welcome screen.
2. Selected “Phone” from the following prompt.

3. Selected the carrier, manufacturer and model of the device to be extracted.

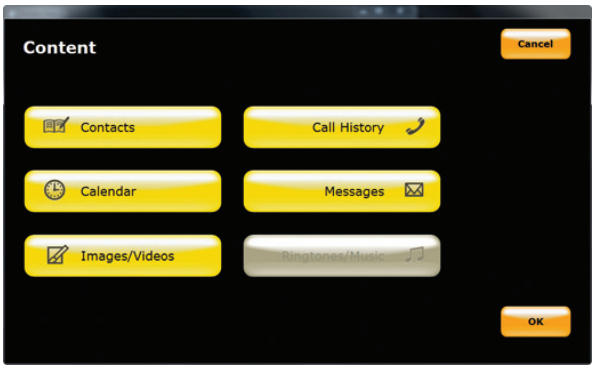




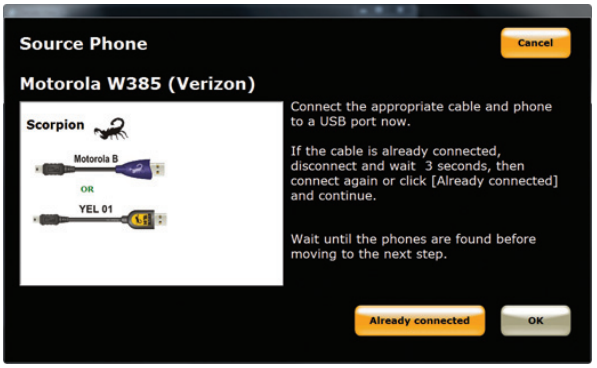
4. Selected the method of transfer (these tests were performed using Cable).



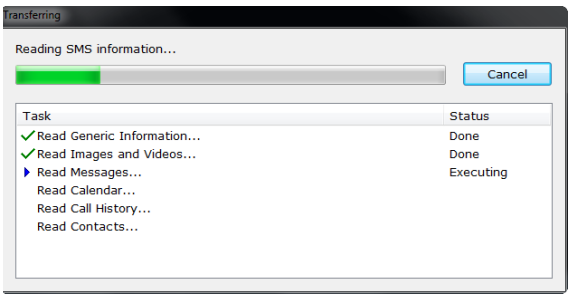
5. Selected the content to be extracted.



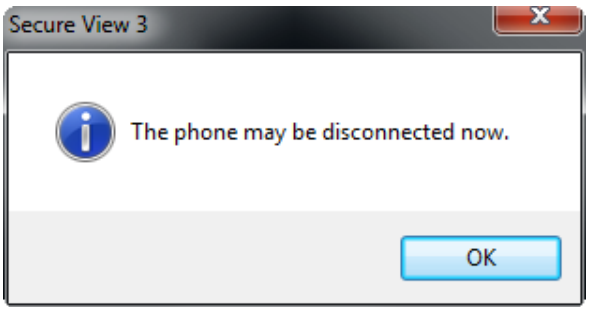
6. Followed the instructions to connect the device and clicked “OK”.



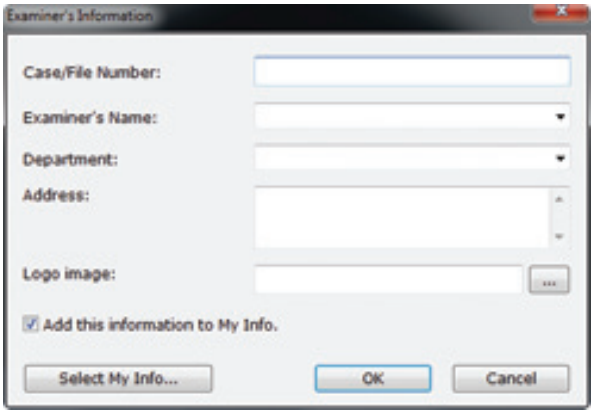
7. While the information is being extracted, the tool displays a progress bar.



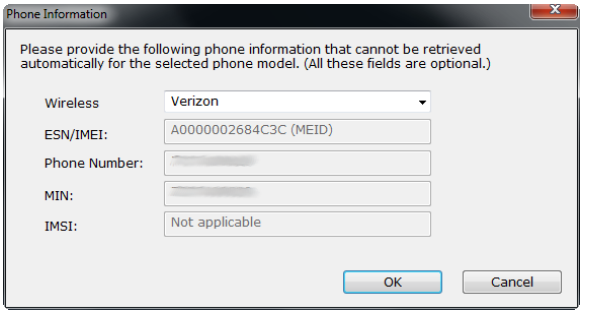
8. When the extraction is complete, the phone may be disconnected.

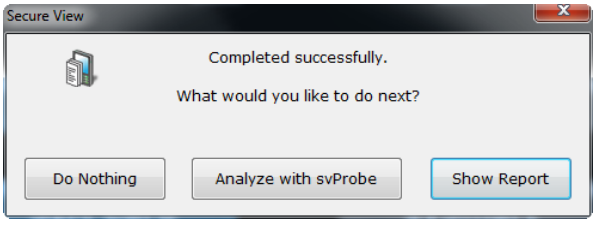


9. Information about the examiner and case can be input.



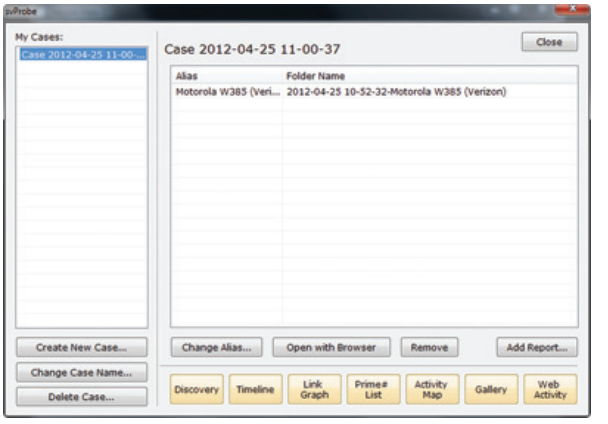
10. Phone information can be verified before moving on to analysis or reporting.



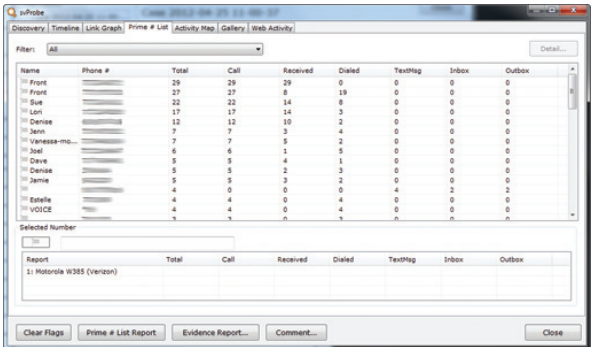


11. Once the information has been extracted from the device, it can be analyzed further using svProbe, or viewed in a report.

12. The svProbe module allows for browsing and filtering through data discovered on the device. When svProbe is first opened, new cases can be created in the left most pane and extractions can be added to the case.

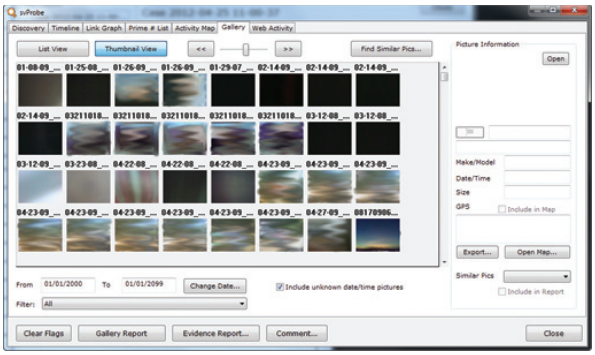


13. Secure View's svProbe analysis tool has seven distinct tools; Discovery, Timeline, Link Graph, Prime # List, Activity Map, Gallery and Web Activity. Using these tools, information can be pulled from the phone and filter using tab specific options. For example, the Discovery tab can be filtered with options like keywords and/or date/time. Link Graph gives the ability to link two device extractions together and determine how frequently contact between the two devices occurred. Prime # List breaks down the phone's interactions to individual number statistics, including phone calls and text messages.



14. The Activity Map shows times where device activity is greatest over a time period.

15. The Gallery is used to view all image files discovered on the device.



16. A report can be viewed within the tool or exported in HTML format. Secure View can provide two different report types: a complete report and an evidence report. A complete report includes all information discovered on the device, while an evidence report is information selected by the user to be included.

Test 1 – LG VX-9100

This test was performed to determine how well Secure View acquires data from an LG VX-9100.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

The following steps were performed:

1. Launched the Secure View application and clicked the Acquire button.
2. Clicked Phone on the Acquire menu.
3. Clicked Verizon on the Source Carrier menu.
4. Clicked LG on the Source Phone menu.
5. Clicked VX9100 (enV2) on the Source Phone Model screen.
6. Selected cable as the method of transfer.
7. Selected Contacts, Calendar, Messages, Images/Videos and Ringtones/Music from the Content menu and clicked OK.
8. Followed instructions to set the phone to Sync Data.
9. Connected the phone to the PC with the Yellow 2 Bear cable as instructed by Secure View.
10. After the communication ports were discovered, clicked OK to begin the acquisition.

Results

Secure View found 71 contacts, 19 calendar events, 102 sent messages, 231 received messages, 63 images, 37 videos and 35 ringtones/music. The results match the data retrieved when manually examining the phone, except for messages. On the phone, there are actually 125 sent messages and 291 received messages. The extra messages that were not found by the tool appear to be MMS messages. The tool did not claim to support extraction of MMS messages from this phone model, so this result is expected.

Test 2 – Sanyo SCP-3100

This test was performed to determine how well Secure View acquires data from a Sanyo SCP-3100.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

The following steps were performed:

1. Launched the Secure View application and clicked the Acquire button.
2. Clicked Phone on the Acquire menu.
3. Clicked Sprint on the Source Carrier menu.
4. Clicked Sanyo on the Source Phone menu.
5. Clicked SCP-3100 on the Source Phone Model screen.
6. Selected Contacts, Call History, Calendar and Messages from the Content menu and clicked OK.
7. Connected the phone to the PC with the Brown 1 Dog cable as instructed by Secure View.
8. After the communication ports were discovered, clicked OK to begin the acquisition.

Results

Secure View found 105 contacts, 20 dialed calls, 20 received calls, 20 missed calls, one calendar event and two received messages. The results match the data retrieved when manually examining the phone.

Test 3 – RIM BlackBerry 8310

This test was performed to determine how well Secure View acquires data from a RIM BlackBerry 8310.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

The following steps were performed:

1. Launched the Secure View application and clicked the Acquire button.
2. Clicked Phone on the Acquire menu.
3. Clicked AT&T on the Source Carrier menu.
4. Clicked RIM on the Source Phone menu.
5. Clicked BlackBerry 8310 (Curve) on the Source Phone Model screen.
6. Selected Contacts, Call History, Calendar, Messages, Files and Other Data from the Content menu and clicked OK.
7. Connected the phone to the PC with the Yellow 1 Scorpion cable as instructed by Secure View.
8. After the communication ports were discovered, clicked OK to begin the acquisition.
9. A communication error occurred when acquiring files, so the test was restarted without selecting Files on the Content menu.
10. After a successful acquisition without Files selected, the test was restarted with only Files selected from the Content menu.
11. After another communication error when acquiring Files, the last step was repeated several times and a communication error occurred each time.

Results

Secure View found 218 contacts, seven dialed calls, 24 calendar events, 40 sent messages, 22 received messages, two browser bookmarks and two browser URLs. The results match the data retrieved when manually examining the phone.

Test 4 – Apple iPhone 4S

This test was performed to determine how well Secure View acquires data from an Apple iPhone 4S.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

The following steps were performed:

1. Launched the Secure View application and clicked the Acquire button.
2. Clicked Phone on the Acquire menu.
3. Clicked AT&T on the Source Carrier menu.
4. Clicked Apple on the Source Phone menu.
5. Clicked iPhone 4/4S on the Source Phone Model screen.
6. Selected Contacts, Call History, Calendar, Messages, Files and Other Data from the Content menu and clicked OK.
7. Connected the phone to the PC with the White 01 Dinosaur cable as instructed by Secure View.
8. After the communication ports were discovered, clicked OK to begin the acquisition.

Results

Secure View found 107 contacts, 55 dialed calls, 28 received calls, 17 missed calls, 76 calendar events, 1,345 sent messages, 4,687 received messages, 1,108 files (images and sounds) and 55 other data files that include Web history and cookies. The items retrieved were as expected. The 4,687 received messages include both outgoing and incoming messages from Apple's iMessage system. The Apple iMessages are

displayed with just message text, no to/from information, and the dates are incorrectly parsed. MMS messages are not displayed.

Test 5 – LG C729 Double Play

This test was performed to determine how well Secure View acquires data from an LG C729.

Prior to starting the test, the phone's battery was fully charged and the phone was powered on.

The following steps were performed:

1. Launched the Secure View application and clicked the Acquire button.
2. Clicked Phone on the Acquire menu.
3. Clicked T-Mobile on the Source Carrier menu.
4. Clicked LG on the Source Phone menu.
5. Clicked doupleplay (C729) on the Source Phone Model screen.
6. Selected Contacts, Call History, Calendar, Messages, Files and Other Data from the Content menu and clicked OK.
7. Connected the phone to the PC with the YEL 02 Bear cable as instructed by Secure View.
8. After the communication ports were discovered, clicked OK to begin the acquisition.

Results

Secure View found 90 contacts, 41 dialed calls, 20 received calls, 22 missed calls, 47 calendar events, 94 sent messages, 126 received messages, 72 files (images and sounds) and other data files that include Web history and cookies. The items retrieved were as expected after performing a manual analysis.

Conclusion

Secure View performed well during the testing. The software is easy to operate and has a straightforward extraction procedure. Once information has been extracted from a device, the data is easy to read. Connection issues during testing were overcome by deselecting items that were not able to be extracted.

Secure View performs logical extractions. This means that deleted data has a very low chance of being recovered.

Analysis of information following an investigation is simple. The user interface is intuitive and easy to learn. Reporting is limited and lacks customization, but does provide space for the investigator name and department. Secure View's Link Graph ability to combine multiple extractions and show connections between devices could be useful during an investigation with multiple devices.