NLECTC NIJ
Criminal Justice
Electronic Crime Technology
Center of Excellence

WebCase

Version 1.9b

EVALUATION REPORT

May 2012

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

Current investigative methods for doing live online investigations are limited. The "Print Screen" option shows only a web page, not whether it was altered or even when it was collected, and a manually written report can contain errors. WebCase simplifies and streamlines the investigative process by including critical details in reports.

Product Information

The following is taken from the Vere Software website, the company that developed WebCase Online Investigation Management Tool[2]:

> WebCase was designed by experienced law enforcement professionals to help you collect Internet information in a usable, evidential, reportable manner. Built to manage the cases you initiate.
>
> The WebCase software is list priced at $995 per licensed dongle. Included is the security dongle along with a CD that contains the software, a user manual, reference material and videos on using the WebCase software. There are no renewal fees once you purchase the software and there are multiple user options with a single license.

Product Description

The following was taken from the Vere Software website:

> The investigator utilizes the evidence collection console to record and manage online investigative activity. The saved data is hashed and stored in a secure environment within the tool. Reports based on the collected evidence can then be printed or published to CD/DVD for distribution. WebCase enables its users to search for, collect, preserve and report any and all online data, including:
>
> - Web captures.
> - Video recordings.
> - TCIP/IP collection.
> - Image capture.
> - Attached files.
> - Keystroke logging.
> - Automatic domain lookups.
> - Automatic Geo-location of IP addresses.

Special Features

The following list of special features was taken from the product website:

- Simplify the online evidence collection process.
- Aid the investigator to preserve online evidence.
- Provide for the proper collection of legal defensible evidence.
- Offer complete undercover identity and suspect information control.
- Provide reports in a usable, understandable format.
- Full screen capture.
- HTML capture.

[2] http://veresoftware.com/index.php?page=webcase

- 64-bit compatibility.
- Supports Windows Operating Systems: XP to Windows 7 and Internet Explorer 6 through 8.

System Requirements

The following system requirements are taken from the WebCase web page[3]:

> WebCase currently operates only on Microsoft® Windows operating system versions XP, Vista and Win 7 Microsoft 32 bit and 64 bit systems. The software requires Microsoft .NET version 2.0 framework or later. If you don't have it, the WebCase installer provides it during installation. WebCase is compliant with Internet Explorer 6, 7 and 8. Internet access is required to receive software updates and to capture active web pages. WebCase can be used to record applications that do not require an Internet connection.

Hardware Minimum Requirements

- An Intel-based PC with a minimum of a Pentium 4 or equivalent processor.
- 100 MB of disk space.
- 1 GB of RAM.
- Currently WebCase does not support Apple OS.
- Currently WebCase only supports Internet Explorer 6 through 8.

[3] http://veresoftware.com/index.php?page=webcase-system-requirements

Test Bed Configuration

The following is the system used for testing:

- Computer:
  - ❑ Gateway Mid Tower PC (Gateway Test PC):
  - ❑ Hewlett-Packard 64-bit.
  - ❑ AMD Athlon II X 4 2.90 GHz.
  - ❑ 6.0 GB Ram installed.
  - ❑ Operating system: Microsoft Windows 7 Service pack 1 Home Edition.

Installation of WebCase

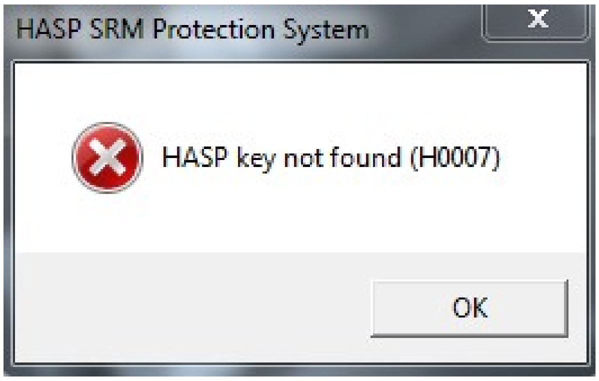
Prior to installing the WebCase software, the WebCase User Manual was downloaded and reviewed. The 97-page manual is informative, includes clear screen shots of the application and detailed descriptions of the installation process. The installation instructions address configuration of antivirus software to allow the WebCase program and its components to access the Internet. It also provides instructions to adjust user settings for both Windows 7 and Windows Vista. During the installation the WebCase software will install the following components on the investigation computer:

- WebCase software.
- Security dongle drivers.
- Vere software toolbar.
- Data Burner ActiveX Control.
- 7-Zip compression tool.
- HASP run-time drivers.

Following the instructions provided, WebCase was installed successfully and the test computer was restarted, completing the installation process.

Initial Configuration

After rebooting the computer, the WebCase software must be configured and registered prior to initiating an investigation. The investigator must have the Aladdin security dongle inserted into the investigative computer to enable the WebCase software. If the security dongle is not inserted the following alert will be displayed.

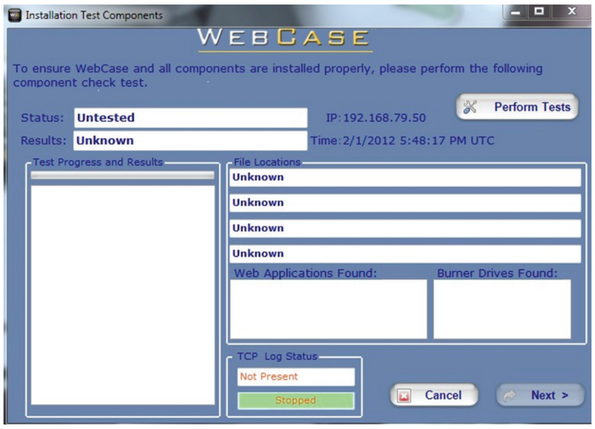

HASP SRM Protection System

HASP key not found (H0007)

WebCase requires configuration by a WebCase administrator. The administrator will create, manage and configure settings for investigator profiles. The point of contact for WebCase updates for the licensing agency or individual must also be completed. The default password provided for the administrator account may be changed once the administrator logs on. The administrator selects the appropriate time zone and WebCase will sync with the National Institute of Standards and Technology (NIST) atomic clock, enabling WebCase to accurately display the date and time stamp associated with any investigation.

As part of the configuration of the WebCase software, the investigator is asked to select a hash algorithm, which WebCase will use to secure and authenticate the evidence that is collected in the case. The following hash algorithms are available to choose from, MD5, SHA1, SHA256, SHA384 and SHA512. The default hash is MD5 and was used in this testing.

Upon completion of the administrator setup, WebCase performs a system test to make sure all the components were configured and work properly.



To ensure WebCase and all components are installed properly, please perform the following component check test.

Status: Untested

Results: Unknown

IP: 192.168.79.50

Time: 2/1/2012 5:48:17 PM UTC

Test Progress and Results

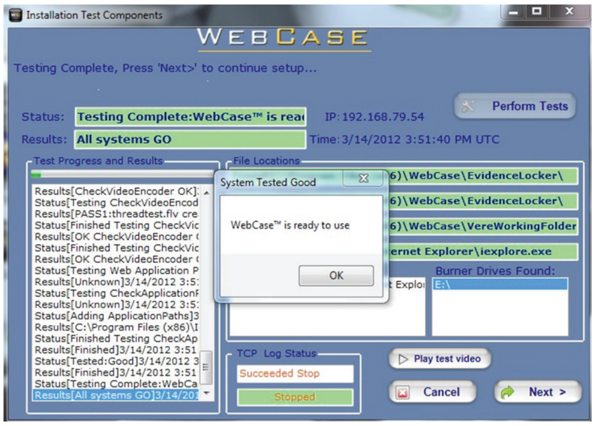
File Locations: Unknown / Unknown / Unknown / Unknown

Web Applications Found:

Burner Drives Found:

TCP Log Status: Not Present / Stopped

When the WebCase software is properly installed and the testing has successfully completed, the following notification screen will be displayed.



Testing Complete, Press 'Next>' to continue setup...

Status: Testing Complete:WebCase™ is rea

Results: All systems GO

IP: 192.168.79.54

Time: 3/14/2012 3:51:40 PM UTC

Test Progress and Results

```
Results[CheckVideoEncoder OK]:
Status[Testing CheckVideoEncod
Results[PASS1:threadtest.flv cre
Status[Finished Testing CheckVic
Results[OK CheckVideoEncoder (
Status[Finished Testing CheckVic
Results[OK CheckVideoEncoder (
Status[Testing Web Application P
Results[Unknown]3/14/2012 3:5:
Status[Testing CheckApplicationF
Results[Unknown]3/14/2012 3:5:
Status[Adding ApplicationPaths]3
Results[C:\Program Files (x86)\I
Status[Finished Testing CheckAp
Results[Finished]3/14/2012 3:51
Status[Tested:Good]3/14/2012 3
Results[Finished]3/14/2012 3:51
Status[Testing Complete:WebCa
Results[All systems GO]3/14/201
```

File Locations:

```
6)\WebCase\EvidenceLocker\
6)\WebCase\EvidenceLocker\
6)\WebCase\VereWorkingFolder
ernet Explorer\iexplore.exe
```

t Exploi

Burner Drives Found: E:\

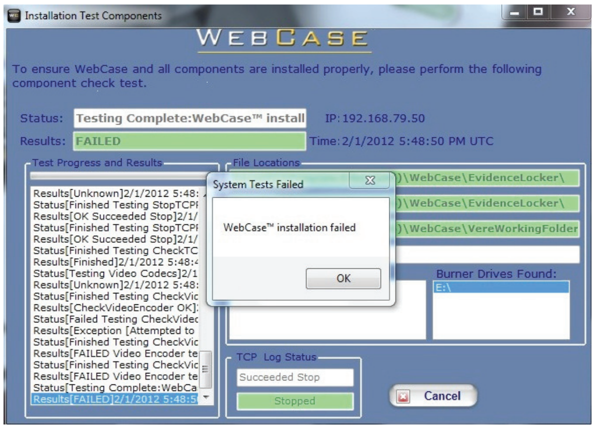
TCP Log Status: Succeeded Stop / Stopped

System Tested Good

WebCase™ is ready to use

Note: If the investigator is using a PC for the investigation, an error message indicating the installation failed will display if the investigation computer is not configured with a microphone and audio device. The WebCase user manual states that for the WebCase video function to work properly, a microphone and speakers must be plugged into the investigative PC during WebCase installation and use. A simple USB headset with a microphone will suffice.

If using a laptop with a built-in microphone as the investigating computer, WebCase does not display the error message.



To ensure WebCase and all components are installed properly, please perform the following component check test.

Status: Testing Complete:WebCase™ install

Results: FAILED

IP: 192.168.79.50

Time: 2/1/2012 5:48:50 PM UTC

Test Progress and Results

```
Results[Unknown]2/1/2012 5:48:
Status[Finished Testing StopTCPI
Results[OK Succeeded Stop]2/1/
Status[Finished Testing StopTCPI
Results[OK Succeeded Stop]2/1/
Status[Finished Testing CheckTC
Results[Finished]2/1/2012 5:48:
Status[Testing Video Codecs]2/1
Results[Unknown]2/1/2012 5:48:
Status[Finished Testing CheckVic
Results[CheckVideoEncoder OK]:
Status[Failed Testing CheckVidec
Results[Exception [Attempted to
Status[Finished Testing CheckVic
Results[FAILED Video Encoder te
Status[Finished Testing CheckVic
Results[FAILED Video Encoder te
Status[Testing Complete:WebCa
Results[FAILED]2/1/2012 5:48:5
```

File Locations:

```
)\WebCase\EvidenceLocker\
)\WebCase\EvidenceLocker\
)\WebCase\VereWorkingFolder
```

Burner Drives Found: E:\

TCP Log Status: Succeeded Stop / Stopped

System Tests Failed

WebCase™ installation failed

Administrative Configuration

The WebCase Software includes a robust set of configuration options. Prior to using WebCase to conduct an investigation, WebCase requires the administrator to create investigator accounts. The administrator is able to manage and monitor all investigator accounts.

Once the administrator has configured the software, the selected options are saved in the Administrators Panel. When this step is completed, the administrator has the option to assign investigators and begin an investigation or to log off of the WebCase software.

Evaluation and Testing of WebCase
Testing Focus

The following WebCase data collection, preservation and presentation functions were tested:

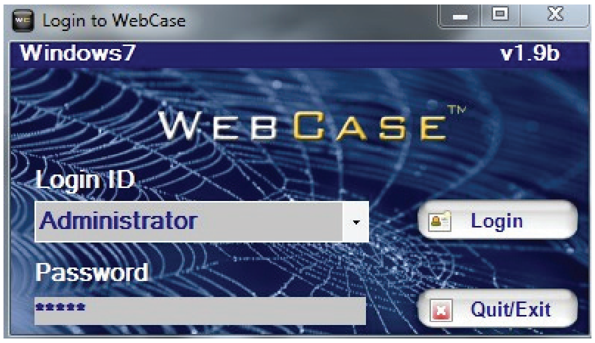
- Key Logging of an Internet investigation activity.
- Archiving of a web page.
- Web page screen capture.
- Report generation.
- HTML/Source code capture.
- Domain registration.
- Location information of the Internet Protocol Address.
- Capture a video recording of a web page/chat conversation.
- Attaching a file to the case.
- Logging and securing evidence collected in the case.

Starting an Investigation

To start an investigation using WebCase, the investigator selects the WebCase Icon.

1. The log on screen will appear.

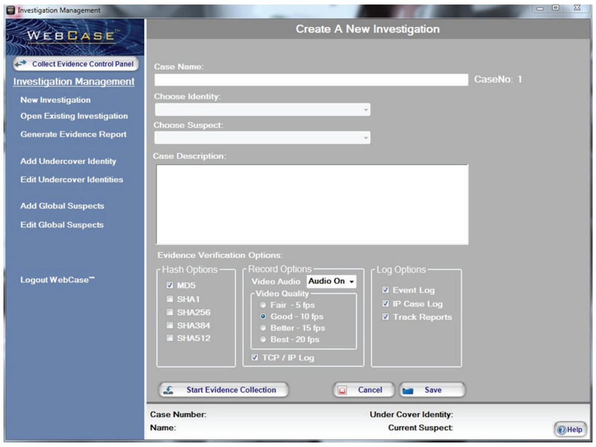
2. The login ID field lists the investigator accounts previously created by the WebCase administrator.



Login ID: Administrator

Password: *****

3. In the Investigation Management window, selecting the “New Investigation” displays the following window.



Case Name:

CaseNo: 1

Choose Identity:

Choose Suspect:

Case Description:

Evidence Verification Options:

Hash Options: ☑ MD5 □ SHA1 □ SHA256 □ SHA384 □ SHA512

Record Options: Video Audio: Audio On; Video Quality: ○ Fair - 5 fps ● Good - 10 fps ○ Better - 15 fps ○ Best - 20 fps; ☑ TCP / IP Log

Log Options: ☑ Event Log ☑ IP Case Log ☑ Track Reports

Case Number:

Name:

Under Cover Identity:

Current Suspect:

4. The investigator fills in the information for the case name, an undercover identity if required, the suspect(s) involved and a description of the case. Evidence Verification Options, such as hash algorithm or Video/Recording, may also be adjusted.

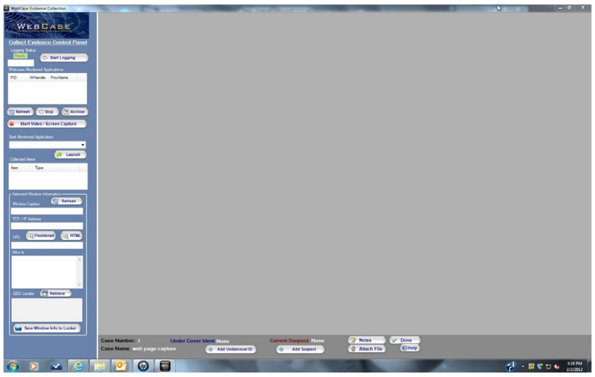
5. Once the case options are configured, evidence can be collected. Selecting the “Save” option saves the case data. Selecting the “Start Evidence Collection” option opens the WebCase Evidence Collection Control Panel interface initiating the investigation.

When continuing an existing investigation, WebCase will display the “Open Existing Investigation” window. This window displays options for the investigator to manage the investigation, such as adding and editing suspect information or an undercover identity. These options are explained in detail in the WebCase User Manual.

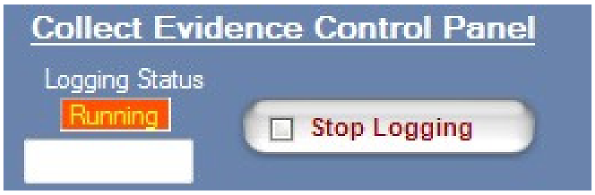
Test: WebCase Standard Operation

The following steps were performed to test WebCase using the www.justnet.org website:

1. Logged in as the administrator.
2. Created a new investigator name. Once created, the administrator was logged off and the investigator account was logged on.
3. Created a suspect named “John Doe.”
4. Created a new case named “TEST 1.”
5. The default MD5 hash was selected for evidence verification.
6. Selected Open Existing Investigation option and selected the investigation named “TEST 1” to start the evidence collection process, at which time the WebCase Evidence Collection interface was displayed.



7. To start the key logging function of WebCase, the Start Logging tab was selected from the WebCase Collect Evidence Control Panel. The logging display window confirmed the application was running. Detailed descriptions of each of the functions of the Evidence Control Panel are contained in the WebCase User Manual.

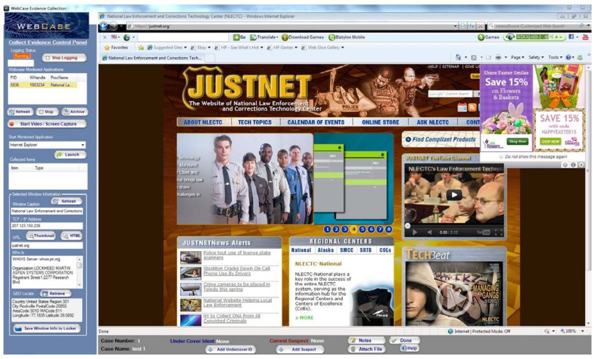


The Start logging tab activates two separate functions within WebCase: a key logger and a TCP/IP logger. These features add a form of verification to the evidence collected during the investigation. The key logger records the investigator’s keystrokes during the logged session. Mouse movements and clicks are not collected. The TCP/IP logger records all data received via the Internet connection. This function was tested by typing the following terms into the Bing search engine field on the Internet Explorer Web browser:

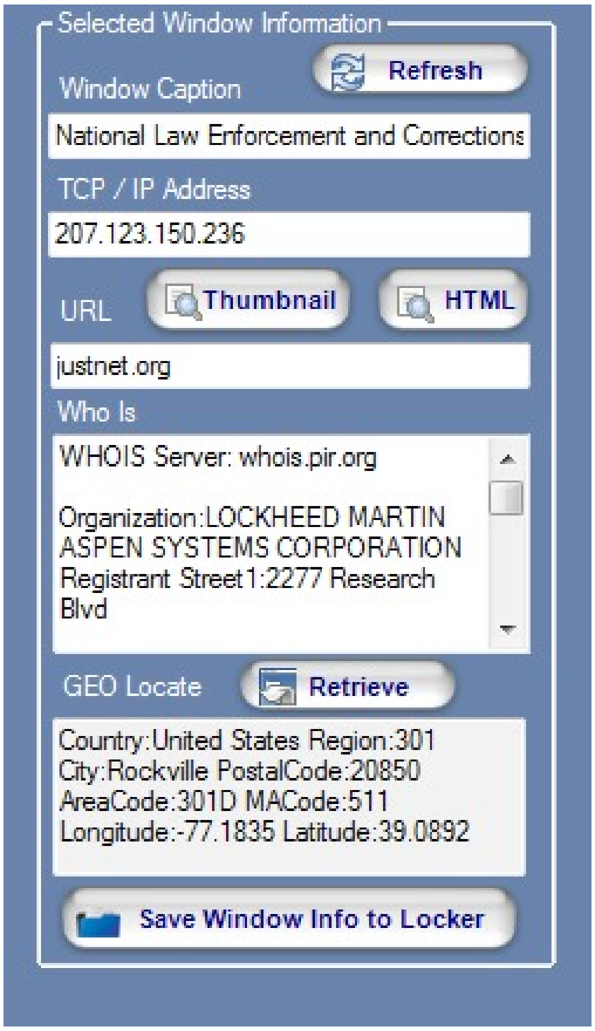
- “Google.com.”
- “50 ways to.”
- “Espn.”
- “Hacking facebook.”
- <Backspace> <backspace> <backspace>. Note: These are actual key presses of Backspace on the keyboard.

8. The WebCase Launch option was selected from the Collect Evidence Control Panel and the Internet Explorer browser was selected from the drop down window. Internet Explorer is the only Web browser that is compatible with WebCase at this time. Internet Explorer opened up in the WebCase Control Panel.

9. The URL "www.Justnet.org" was typed in the address bar of Internet Explorer. The Justnet.org home page was displayed in the WebCase control Panel.



The Collect Evidence Control Panel was populated with the following information:



Window Caption: National Law Enforcement and Corrections

TCP / IP Address: 207.123.150.236

URL: justnet.org

Who Is:
WHOIS Server: whois.pir.org

Organization:LOCKHEED MARTIN ASPEN SYSTEMS CORPORATION
Registrant Street1:2277 Research Blvd

GEO Locate:
Country:United States Region:301
City:Rockville PostalCode:20850
AreaCode:301D MACode:511
Longitude:-77.1835 Latitude:39.0892

10. The Save Window Info to Locker feature was accessed to capture the information gathered. The information was then hashed by WebCase, and placed in the WebCase Evidence locker.

11. The Archive feature in the Collect Evidence Control Panel was selected to archive the www.Justnet.org web page. The archived page was then saved as evidence and stored in the WebCase evidence locker. The collected items window in the control panel window confirmed the page was saved.

12. The Start Video feature was selected to test the WebCase video recording and screen capture functions. A 10-second video of the Justnet YouTube channel was captured from the homepage. After capturing the video, it was saved in WebCase in the .flv format.

13. The Start Video feature was again selected to test the recording of an ongoing live chat session. To simulate a chat session between an investigator and a suspect, two Yahoo chat accounts were created. After logging on to Yahoo, the Start Recording tab was accessed and a chat session was recorded.

14. The Start Video/Screen Capture feature was selected again to test the WebCase screen capture capability. The Justnet.org website homepage was captured and saved into the WebCase evidence locker.

15. The HTML feature was selected to collect the HTML data of the Justnet.org website. This information was then saved to the WebCase evidence locker.

16. The Thumbnail feature was selected to capture a thumbnail image of the Justnet.org homepage. The evidence was then saved in the WebCase evidence locker.

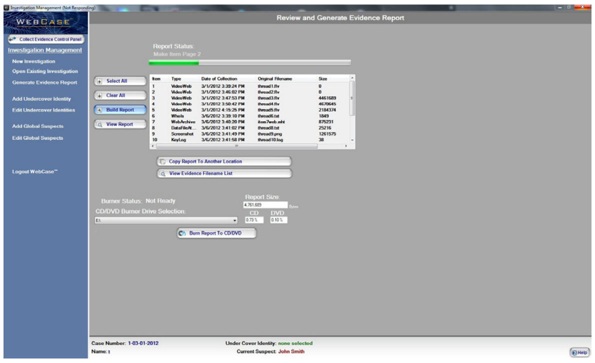
17. WebCase offers the feature of adding files to the case. Selecting "Attach File" displays a window to navigate to the file to be added. An image name "wave4w.jpg" in the pictures folder was selected.

WebCase hashed the file and confirmed it was saved in the collected items window.

18. After collecting the evidence and confirming it was listed in the Collected Items window, the Done option was selected, closing the current investigation.

19. In the Investigation Management Window, the Generate Report option was selected and case items were displayed. At this step, items can be selected and added to the report.

20. The Build Report option was selected and WebCase generated an HTML report. The WebCase report is HTML based and the user must permit the Active X controls and allow blocked content in Internet Explorer for the report to display properly.



Review and Generate Evidence Report

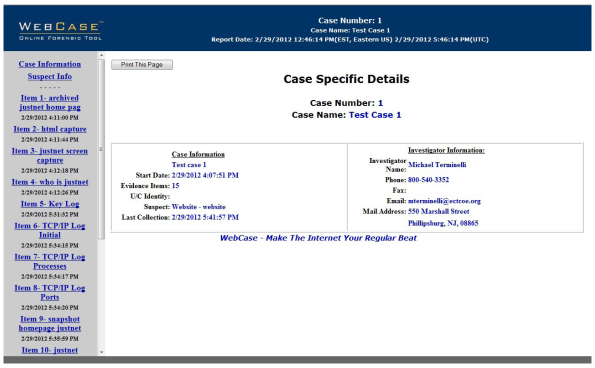
Report Status:
Make Item Page 2

Item	Type	Date of Collection	Original Filename	Size
1	VideoWeb	3/1/2012 3:39:24 PM	thread1.flv	0
2	VideoWeb	3/1/2012 3:46:02 PM	thread2.flv	0
3	VideoWeb	3/1/2012 3:47:53 PM	thread3.flv	4461689
4	VideoWeb	3/1/2012 3:50:42 PM	thread4.flv	4670645
5	VideoWeb	3/1/2012 4:15:25 PM	thread5.flv	2184374
6	WhoIs	3/6/2012 3:39:10 PM	thread6.txt	1849
7	WebArchive	3/6/2012 3:40:20 PM	item7web.mht	875231
8	DataFileAt...	3/6/2012 3:41:02 PM	thread8.txt	25216
9	Screenshot	3/6/2012 3:41:49 PM	thread9.png	1261575
10	KeyLog	3/6/2012 3:41:58 PM	thread10.log	38

Burner Status: Not Ready
CD/DVD Burner Drive Selection: E:\
Report Size: 4,761,689 Bytes
CD 0.73 %
DVD 0.10 %

Case Number: 1-03-01-2012
Name: t
Under Cover Identity: none selected
Current Suspect: John Smith

The initial WebCase Report HTML page opens in the default Web browser and displays the details of the investigation including the case and Investigator information and the evidence collected during the case. The Evidence list identifies the date and time the evidence was collected.



Case Number: 1
Case Name: Test Case 1
Report Date: 2/29/2012 12:46:14 PM(EST, Eastern US) 2/29/2012 5:46:14 PM(UTC)

Case Information
Suspect Info
- - - - -
Item 1- archived justnet home pag
2/29/2012 4:11:00 PM
Item 2- html capture
2/29/2012 4:11:44 PM
Item 3- justnet screen capture
2/29/2012 4:12:18 PM
Item 4- who is justnet
2/29/2012 4:12:26 PM
Item 5- Key Log
2/29/2012 5:31:32 PM
Item 6- TCP/IP Log Initial
2/29/2012 5:34:15 PM
Item 7- TCP/IP Log Processes
2/29/2012 5:34:17 PM
Item 8- TCP/IP Log Ports
2/29/2012 5:34:20 PM
Item 9- snapshot homepage justnet
2/29/2012 5:35:59 PM
Item 10- justnet

Case Specific Details

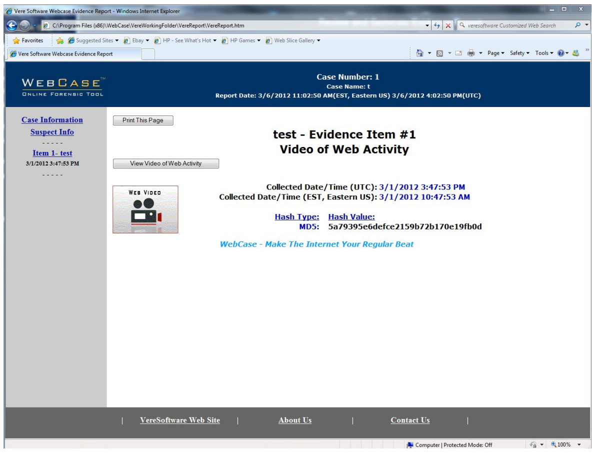
Case Number: 1
Case Name: Test Case 1

Case Information
Test case 1
Start Date: 2/29/2012 4:07:51 PM
Evidence Items: 15
U/C Identity:
Suspect: Website - website
Last Collection: 2/29/2012 5:41:57 PM

Investigator Information:
Investigator Name: Michael Terminelli
Phone: 800-540-3352
Fax:
Email: mterminelli@ectcoe.org
Mail Address: 550 Marshall Street
Phillipsburg, NJ, 08865

WebCase - Make The Internet Your Regular Beat

Selecting an evidence item displays the information associated with that evidence item, including the date and time the evidence was collected, the name assigned to the evidence, a link to open and view the evidence and the hash value WebCase generated for that piece of evidence.


Vere Software Webcase Evidence Report - Windows Internet Explorer
C:\Program Files (x86)\WebCase\VereWorkingFolder\VereReport\VereReport.htm
veresoftware Customized Web Search
Favorites
Suggested Sites
Ebay
HP - See What's Hot
HP Games
Web Slice Gallery
Vere Software Webcase Evidence Report
Page
Safety
Tools
WEBCASE
ONLINE FORENSIC TOOL
Print This Page
View Video of Web Activity
WEB VIDEO
VereSoftware Web Site
About Us
Contact Us
Computer | Protected Mode: Off
100%

Case Number: 1
Case Name: t
Report Date: 3/6/2012 11:02:50 AM(EST, Eastern US) 3/6/2012 4:02:50 PM(UTC)

Case Information
Suspect Info
- - - - -
Item 1- test
3/1/2012 3:47:53 PM
- - - - -

test - Evidence Item #1
Video of Web Activity

Collected Date/Time (UTC): 3/1/2012 3:47:53 PM
Collected Date/Time (EST, Eastern US): 3/1/2012 10:47:53 AM

Hash Type: Hash Value:
MD5: 5a79395e6defce2159b72b170e19fb0d

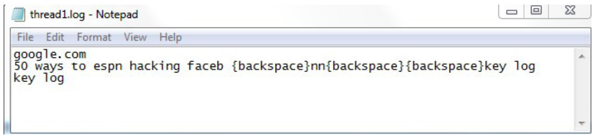
WebCase - Make The Internet Your Regular Beat

Results

The report was used to verify each individual section of this test. The following is a list of those results:

- Key Logging

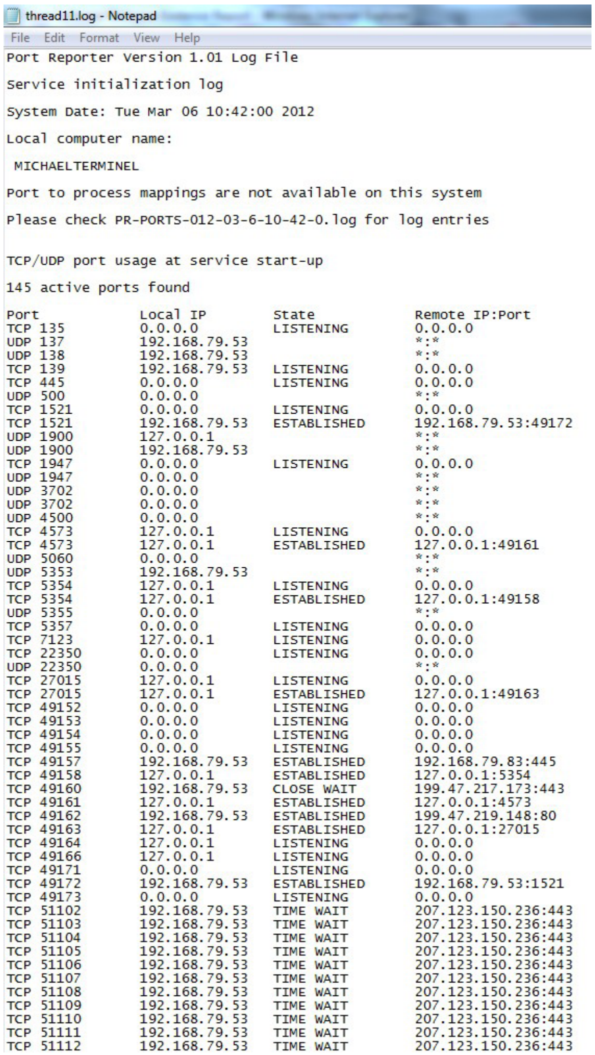
  After opening the key log evidence item, it was confirmed that WebCase captured the key strokes used in the investigation.



```
google.com
50 ways to espn hacking faceb {backspace}nn{backspace}{backspace}key log
key log
```

- TCP/IP

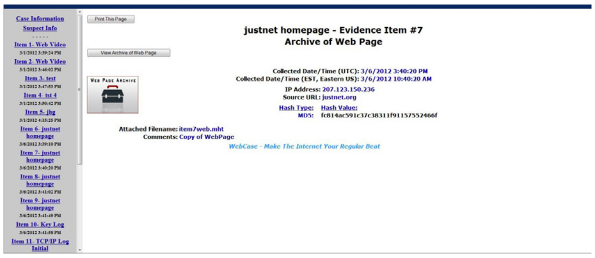
  The TCP/IP reports confirmed that all the ports were working properly on the investigation computer and were accessing the website that was under investigation. WebCase displays this information in a text format.



```
Port Reporter Version 1.01 Log File

Service initialization log

System Date: Tue Mar 06 10:42:00 2012

Local computer name:

 MICHAELTERMINEL

Port to process mappings are not available on this system

Please check PR-PORTS-012-03-6-10-42-0.log for log entries


TCP/UDP port usage at service start-up

145 active ports found

Port            Local IP        State           Remote IP:Port
TCP 135         0.0.0.0         LISTENING       0.0.0.0
UDP 137         192.168.79.53                   *:*
UDP 138         192.168.79.53                   *:*
TCP 139         192.168.79.53   LISTENING       0.0.0.0
TCP 445         0.0.0.0         LISTENING       0.0.0.0
UDP 500         0.0.0.0                         *:*
TCP 1521        0.0.0.0         LISTENING       0.0.0.0
TCP 1521        192.168.79.53   ESTABLISHED     192.168.79.53:49172
UDP 1900        127.0.0.1                       *:*
UDP 1900        192.168.79.53                   *:*
TCP 1947        0.0.0.0         LISTENING       0.0.0.0
UDP 1947        0.0.0.0                         *:*
UDP 3702        0.0.0.0                         *:*
UDP 3702        0.0.0.0                         *:*
UDP 4500        0.0.0.0                         *:*
TCP 4573        127.0.0.1       LISTENING       0.0.0.0
TCP 4573        127.0.0.1       ESTABLISHED     127.0.0.1:49161
UDP 5060        0.0.0.0                         *:*
UDP 5353        192.168.79.53                   *:*
TCP 5354        127.0.0.1       LISTENING       0.0.0.0
TCP 5354        127.0.0.1       ESTABLISHED     127.0.0.1:49158
UDP 5355        0.0.0.0                         *:*
TCP 5357        0.0.0.0         LISTENING       0.0.0.0
TCP 7123        127.0.0.1       LISTENING       0.0.0.0
TCP 22350       0.0.0.0         LISTENING       0.0.0.0
UDP 22350       0.0.0.0                         *:*
TCP 27015       127.0.0.1       LISTENING       0.0.0.0
TCP 27015       127.0.0.1       ESTABLISHED     127.0.0.1:49163
TCP 49152       0.0.0.0         LISTENING       0.0.0.0
TCP 49153       0.0.0.0         LISTENING       0.0.0.0
TCP 49154       0.0.0.0         LISTENING       0.0.0.0
TCP 49155       0.0.0.0         LISTENING       0.0.0.0
TCP 49157       192.168.79.53   ESTABLISHED     192.168.79.83:445
TCP 49158       127.0.0.1       ESTABLISHED     127.0.0.1:5354
TCP 49160       192.168.79.53   CLOSE WAIT      199.47.217.173:443
TCP 49161       127.0.0.1       ESTABLISHED     127.0.0.1:4573
TCP 49162       192.168.79.53   ESTABLISHED     199.47.219.148:80
TCP 49163       127.0.0.1       ESTABLISHED     127.0.0.1:27015
TCP 49164       127.0.0.1       LISTENING       0.0.0.0
TCP 49166       127.0.0.1       LISTENING       0.0.0.0
TCP 49171       0.0.0.0         LISTENING       0.0.0.0
TCP 49172       192.168.79.53   ESTABLISHED     192.168.79.53:1521
TCP 49173       0.0.0.0         LISTENING       0.0.0.0
TCP 51102       192.168.79.53   TIME WAIT       207.123.150.236:443
TCP 51103       192.168.79.53   TIME WAIT       207.123.150.236:443
TCP 51104       192.168.79.53   TIME WAIT       207.123.150.236:443
TCP 51105       192.168.79.53   TIME WAIT       207.123.150.236:443
TCP 51106       192.168.79.53   TIME WAIT       207.123.150.236:443
TCP 51107       192.168.79.53   TIME WAIT       207.123.150.236:443
TCP 51108       192.168.79.53   TIME WAIT       207.123.150.236:443
TCP 51109       192.168.79.53   TIME WAIT       207.123.150.236:443
TCP 51110       192.168.79.53   TIME WAIT       207.123.150.236:443
TCP 51111       192.168.79.53   TIME WAIT       207.123.150.236:443
TCP 51112       192.168.79.53   TIME WAIT       207.123.150.236:443
```

■ WebArchive

WebCase captured the entire scrolling page of Justnet.org. If the investigation computer is connected to the Internet when the archived web page is viewed, the hyperlink displays the current version of the website from the Internet, and not the version archived in the WebCase report. It is recommended that the investigation computer is disconnected from the Internet when viewing the WebCase report.



justnet homepage - Evidence Item #7
Archive of Web Page

Collected Date/Time (UTC): 3/6/2012 3:40:20 PM
Collected Date/Time (EST, Eastern US): 3/6/2012 10:40:20 AM
IP Address: 207.123.150.236
Source URL: justnet.org
Hash Type: Hash Value:
MD5: fc814ac591c37c38311f91157552466f

Attached Filename: item7web.mht
Comments: Copy of WebPage

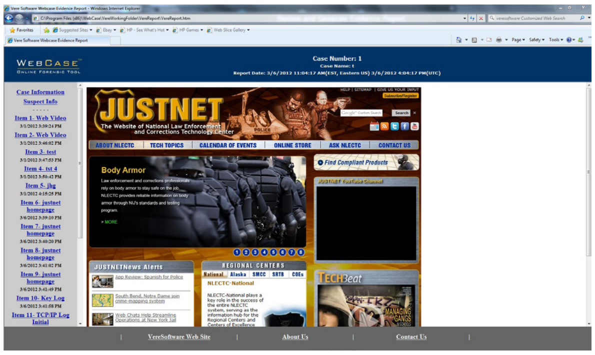
WebCase - Make The Internet Your Regular Beat

■ Video Capture

The video capture feature of WebCase successfully captured the video selected from the Justnet.org homepage and successfully captured the chat session.

■ Screen Capture

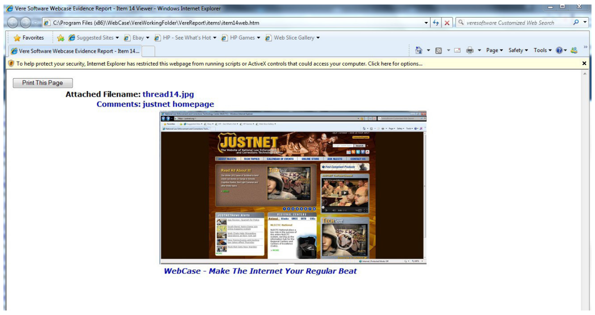
The WebCase report showed that the screen capture was successful in capturing a scrolling jpeg image of the Justnet.org home page.



Case Number: 1
Case Name: 1
Report Date: 3/6/2012 11:04:17 AM(EST, Eastern US) 3/6/2012 4:04:17 PM(UTC)

■ Thumbnail Image Capture

WebCase successfully captured a thumbnail image of the Justnet.org homepage.


Vere Software Webcase Evidence Report - Item 14 Viewer - Windows Internet Explorer
C:\Program Files (x86)\WebCase\VereWorkingFolder\VereReport\items\item14web.htm
veresoftware Customized Web Search
Favorites
Suggested Sites
Ebay
HP - See What's Hot
HP Games
Web Slice Gallery
Vere Software Webcase Evidence Report - Item 14...
Page
Safety
Tools
Print This Page
JUSTNET

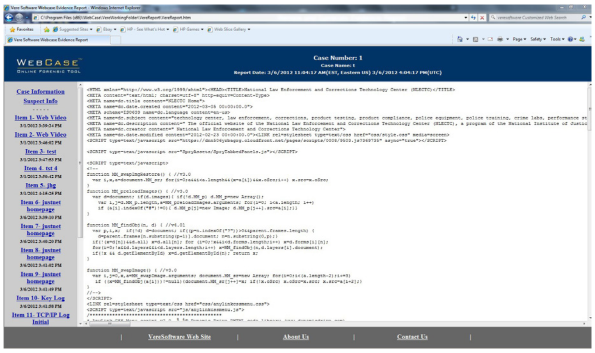
To help protect your security, Internet Explorer has restricted this webpage from running scripts or ActiveX controls that could access your computer. Click here for options...

Attached Filename: thread14.jpg
Comments: justnet homepage

WebCase - Make The Internet Your Regular Beat

- HTML Capture

  WebCase successfully captured the HTML code for the Justnet.org website and displayed the information in text format.

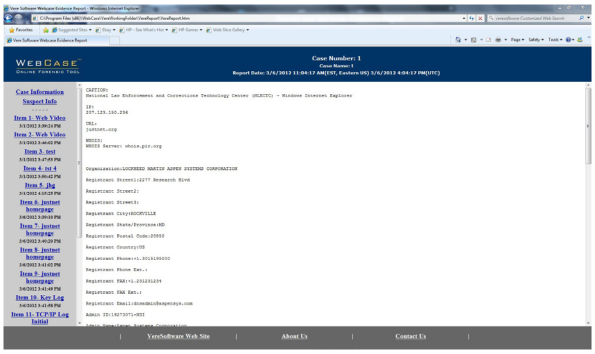


Case Number: 1
Case Name: t
Report Date: 3/6/2012 11:04:17 AM(EST, Eastern US) 3/6/2012 4:04:17 PM(UTC)

```
<HTML xmlns="http://www.w3.org/1999/xhtml"><HEAD><TITLE>National Law Enforcement and Corrections Technology Center (NLECTC)</TITLE>
<META content="text/html; charset=utf-8" http-equiv=Content-Type>
<META name=dc.title content="NLECTC Home">
<META name=dc.date.created content="2012-03-05 00:00:00.0">
<META scheme=ISO639 name=dc.language content=en-us>
<META name=dc.subject content="technology center, law enforcement, corrections, product testing, product compliance, police equipment, police training, crime labs, performance st
<META name=dc.description content=" The official website of the National Law Enforcement and Corrections Technology Center (NLECTC), a program of the National Institute of Justic
<META name=dc.creator content=" National Law Enforcement and Corrections Technology Center">
<META name=dc.date.modified content="2012-02-23 00:00:00.0"><LINK rel=stylesheet type=text/css href="css/style.css" media=screen>
<SCRIPT type=text/javascript src="https://dnn506yrbagrg.cloudfront.net/pages/scripts/0008/9503.js?369735" async="true"></SCRIPT>

<SCRIPT type=text/javascript src="SpryAssets/SpryTabbedPanels.js"></SCRIPT>

<SCRIPT type=text/javascript>
<!--
function MM_swapImgRestore() { //v3.0
  var i,x,a=document.MM_sr; for(i=0;a&&i<a.length&&(x=a[i])&&x.oSrc;i++) x.src=x.oSrc;
}
function MM_preloadImages() { //v3.0
  var d=document; if(d.images){ if(!d.MM_p) d.MM_p=new Array();
    var i,j=d.MM_p.length,a=MM_preloadImages.arguments; for(i=0; i<a.length; i++)
    if (a[i].indexOf("#")!=0){ d.MM_p[j]=new Image; d.MM_p[j++].src=a[i];}}
}

function MM_findObj(n, d) { //v4.01
  var p,i,x;  if(!d) d=document; if((p=n.indexOf("?"))>0&&parent.frames.length) {
    d=parent.frames[n.substring(p+1)].document; n=n.substring(0,p);}
  if(!(x=d[n])&&d.all) x=d.all[n]; for (i=0;!x&&i<d.forms.length;i++) x=d.forms[i][n];
  for(i=0;!x&&d.layers&&i<d.layers.length;i++) x=MM_findObj(n,d.layers[i].document);
  if(!x && d.getElementById) x=d.getElementById(n); return x;
}

function MM_swapImage() { //v3.0
  var i,j=0,x,a=MM_swapImage.arguments; document.MM_sr=new Array; for(i=0;i<(a.length-2);i+=3)
   if ((x=MM_findObj(a[i]))!=null){document.MM_sr[j++]=x; if(!x.oSrc) x.oSrc=x.src; x.src=a[i+2];}
}
//-->
</SCRIPT>
<LINK rel=stylesheet type=text/css href="css/anylinkcssmenu.css">
<SCRIPT type=text/javascript src="js/anylinkcssmenu.js">
/***********************************************
```

- Whois Information and Domain registration information

  WebCase displays the domain registration information in text format, and confirmed that the URL address for Justnet.org is registered to LOCKHEED MARTIN ASPEN SYSTEMS CORPORATION. WebCase also supplies the phone number, street address and e-mail information for the registrant from the Whois database entry.



Case Number: 1
Case Name: t
Report Date: 3/6/2012 11:04:17 AM(EST, Eastern US) 3/6/2012 4:04:17 PM(UTC)

```
CAPTION:
National Law Enforcement and Corrections Technology Center (NLECTC) - Windows Internet Explorer

IP:
207.123.150.236

URL:
justnet.org

WHOIS:
WHOIS Server: whois.pir.org


Organization:LOCKHEED MARTIN ASPEN SYSTEMS CORPORATION

Registrant Street1:2277 Research Blvd

Registrant Street2:

Registrant Street3:

Registrant City:ROCKVILLE

Registrant State/Province:MD

Registrant Postal Code:20850

Registrant Country:US

Registrant Phone:+1.3015195000

Registrant Phone Ext.:

Registrant FAX:+1.231231234

Registrant FAX Ext.:

Registrant Email:dnsadmin@aspensys.com

Admin ID:19273071-NSI

Admin Name:Aspen Systems Corporation
```

- Attached File

  The Attached Image file, wave4w.jpg, was accessed in the WebCase report. The file was correctly attached to the report and displayed properly.

Test: Evidence Integrity

WebCase secures the evidence collected by using a date and time via the atomic clock at NIST. The evidence gathered in each investigation is date and time stamped at the time it is captured and then hashed using the algorithm that was selected by the investigator in the WebCase set up procedure. The evidence is then stored in a container and cannot be accessed by normal means. WebCase also copies files to an Evidence Locker folder so that individual files can be viewed by the investigator. The following steps were performed to verify that WebCase maintains the integrity of the evidence gathered.

The file to be tested for integrity is an image file named wave4w.jpg, which was attached to the case earlier in the testing process. The following procedure was conducted to determine if the integrity of the collected evidence is maintained when accessing the Evidence Locker folder:

1. Accessed the Evidence Locker folder.

2. Opened the image file named wave4w.jpg with Windows Live Photo Gallery.

3. Inverted the image using the editing function and saved it back to the Evidence Locker folder, leaving the same file name.

4. Closed all open folders and launched the WebCase software.

5. Generated the evidence report for the case.

6. Opened the case report and accessed the evidence image item wave4w.jpg.

Results

It was confirmed that the evidence image item wave4w.jpg did retain its original properties and no manipulation of the photo was detected. The hash values in the WebCase report confirmed that the attached file was not altered.

Test: Evidence Integrity #2

The following steps were performed to ensure that WebCase did not use the files from the Evidence Locker Folder:

1. Accessed the Evidence Locker folder.

2. Deleted file named wave4w.jpg from the evidence locker folder.

3. Closed all open folders and launched the WebCase software.

4. Generated the evidence report for the case.

5. Opened the case report and accessed the evidence image item wave4w.jpg.

Results

It was confirmed that the evidence image item wave4w.jpg was properly displayed in the report and the hash value confirmed that the image wave4w.jpg was not altered.

Conclusion

The tested features of the WebCase Online Forensic Tool performed as advertised in the WebCase documentation and website. The software is designed to capture online chat conversations, web pages and social networking sites as they appeared at the time an investigator viewed them. WebCase uses a hash algorithm to ensure the integrity of evidence collected in a case.

The installation and use of the software is simple. A seasoned investigator most likely would not require training for the operation of WebCase. If needed, the developer offers training opportunities and an online eLearning page containing instructional videos on the operation of the software.

The multiuser capabilities with a single license are a valuable feature for an agency with multiple investigators, enabling both joint and independent investigations. The WebCase program generates an easy to read HTML report that can be copied to CD, DVD or other media.