NLECTC NIJ

Criminal Justice
Electronic Crime Technology
Center of Excellence

US-LATT

Version 1.60

EVALUATION REPORT

June 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.
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

During the past several years, computer forensic examiners have discussed the potential loss of evidence when seizing a computer that is powered on and the power cord is pulled at the time of seizure. Simply pulling the plug on a running computer causes the loss of data in Random Access Memory (RAM) and other information that might be of evidentiary value, such as the programs that were running at the time of seizure, the windows that were minimized, online chat conversations, connections to remote storage or computers, and system data.

Wetstone Technologies, Inc. has created a forensic tool called USB Live Acquisition and Triage Tool (US-LATT) to capture the volatile data listed above and more. The development of US-LATT was funded by NIJ.

Product Information

The following excerpts from the US-LATT documentation describe the tool, the functions it performs and how the tool can be used:

- What is US-LATT?

  US-LATT is a system for live investigation and triage of potentially compromised or evidence-containing computers and related devices. The product consists of both a data acquisition hardware component and a software-analysis component. The hardware component is a specially configured USB drive containing a set of configuration files and data collection components. The analysis functions allow for the importing of collected information and subsequent analysis.

- Why use US-LATT?

  Responding to the misuse of systems can be a tremendous task. Also, as most investigative departments only have a limited number of experienced investigators with knowledge of particular systems, having experts to send out in the field to investigate individual systems is impractical. US-LATT enables potentially less experienced field investigators to quickly collect a variety of critical information about the suspect's computer, eliminating the need for an expert to travel to a target site. In addition, US-LATT provides the ability to investigate systems while they are running, eliminating the need to take critical systems offline during initial triage.

- How is US-LATT Used?

  By inserting a USB device into the suspect system, data can be gathered from a live machine and analyzed later in the laboratory. US-LATT collects data from a target machine without the need of any specialized software installation. A customized US-LATT can be quickly created and deployed to collect data pertinent to an investigation.

The documentation also says US-LATT collects the following information from a running computer:

- Running Process List and Information.
- Installed Services and Drivers.
- Physical Memory Dump.
- Installed Application List.
- Critical Registry Data.
- Hardware Configuration Information.
- Active Encrypted File Systems.
- Event Logs.
- Desktop Screenshot.
- Individual Window Screenshot.

- Live Network Information.
- System Data.
- Logged In Users.
- User Accounts.

US-LATT can also acquire information from running programs such as Firefox, Outlook and Skype without altering the state of the running program.

System Requirements

Shown below are the system requirements identified by Wetstone Technologies, Inc. for using US-LATT.

Target Systems

US-LATT currently supports the triage of the following target platforms:

- Microsoft® Windows® XP Professional.
- Microsoft® Windows® 2000 Professional.
- Microsoft® Windows® XP 64-bit.
- Microsoft® Windows® Vista.
- Microsoft® Windows® Vista 64-bit.
- Microsoft® Windows® Server 2003.
- Microsoft® Windows® Server 2008.
- Microsoft® Windows® 7.
- Microsoft® Windows® 7 64-Bit.

Target System Requirements and Suggestions

Although no software needs to be directly installed on each target system, the system needs to meet the following minimum operational state:

1. An available USB slot.
2. The target system must be running and a user must be logged in or the investigator must have valid login credentials.
3. Autorun should be enabled; if not, the investigator can manually start US-LATT.

US-LATT Configuration Application

In order to properly support installing and running the US-LATT Token Configuration Utility program on an investigator's machine, a computer system must meet or exceed the following minimum requirements. As with any modern application, increased resources may result in improved performance.

- Microsoft Windows® 2000, XP, Vista, or 7.
- Microsoft .Net Framework version 4.0.
- 50 MB of free disk space.
- 256 MB RAM.
- An available USB slot.

Test Bed Configuration

Computer Platforms

These computers were used as test beds because (1) US-LATT supports only Windows-based computers, (2) they are used on a daily basis for both business and personal activities and (3) they represent computers that criminal justice personnel would encounter in the field.

The following computers were used for this evaluation of US-LATT. All are configured with multiple programs used both in business and personal activities. All of these computers have Internet access either through hard-wired or wireless connections.

The first test computer is a shop-built desktop computer with a 1 terabyte hard drive and a 64-bit processor. Below are additional details of this computer.

Windows edition

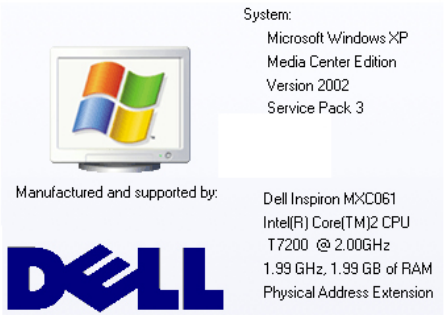
Windows 7 Professional

Copyright © 2009 Microsoft Corporation. All rights reserved.

System

Processor:	AMD Phenom(tm) II X4 925 Processor 2.80 GHz
Installed memory (RAM):	8.00 GB (3.37 GB usable)
System type:	32-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

The second test computer is a Dell laptop computer with an 80 gigabyte hard drive and a 32-bit processor. Below are additional details of this computer. Note that it was configured with multiple user accounts, one of which did not have administrator's privileges.



The third test computer is a Samsung laptop computer with a 600 gigabyte hard drive and a 32-bit processor. Below are additional details of this laptop computer.

Windows edition

Windows 7 Home Premium

Copyright © 2009 Microsoft Corporation. All rights reserved.

Service Pack 1

System

Manufacturer:	Samsung Electronics
Processor:	Intel(R) Core(TM) i5 CPU M 460 @ 2.53GHz 2.53 GHz
Installed memory (RAM):	4.00 GB (3.79 GB usable)
System type:	64-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

Following is an example of the programs installed on all computers:

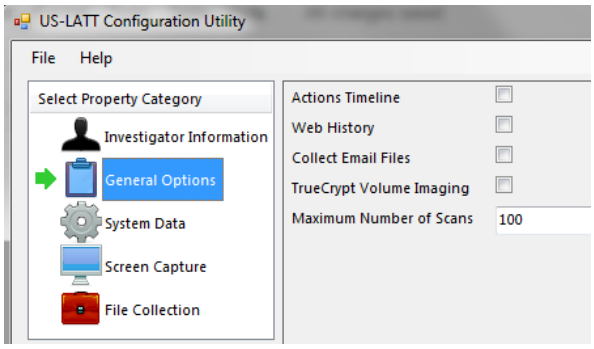
- Microsoft Internet Browser.
- Mozilla Firefox Internet Browser.
- Google Chrome.
- Microsoft Office 10.
- TrueCrypt (a 1 megabyte TrueCrypt volume was mounted for this test).
- Various media creation programs.
- FTP programs.
- iTunes.
- Various file compression programs.
- Avast antivirus.
- Software development programs.
- Multimedia creation programs.
- Computer forensics programs.

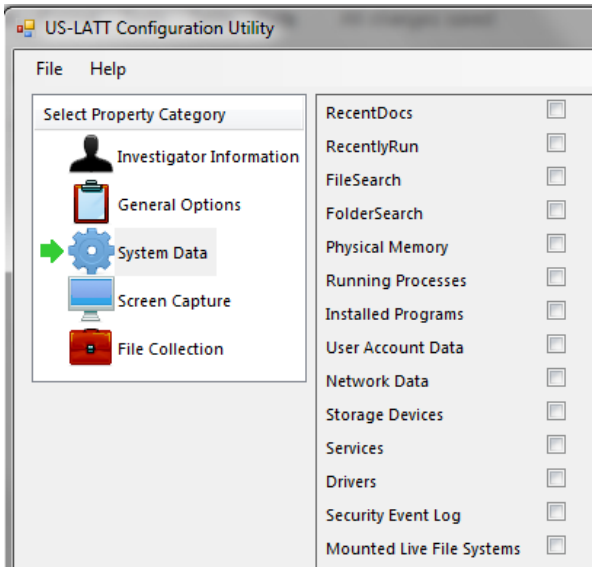
- Financial programs.
- Mapping programs.

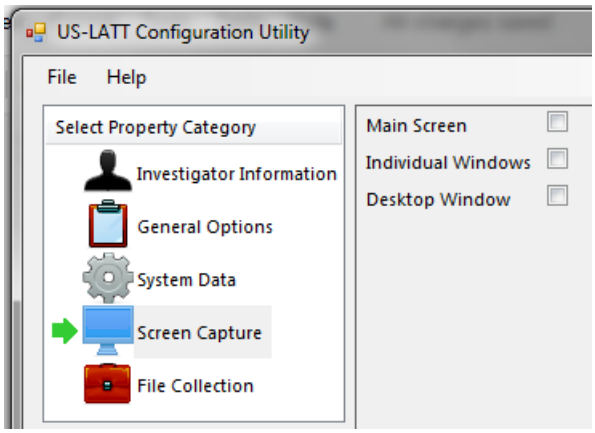
The US-LATT Thumb Drive

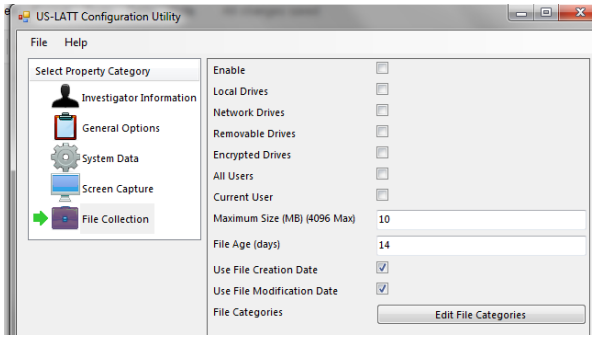
US-LATT is available in sizes ranging from 4 GB to 2 TB devices. The device used in this evaluation was provided on a 32 GB thumb drive. The capacity of US-LATT dictates the amount of data that can be acquired. In other words, if the computer to be examined has 4 GB of RAM, then a US-LATT thumb drive must be larger than 4 GB because not only will the 4 GB of RAM be written to the thumb drive, but all other information (running programs, running processes, screenshots, etc.) that is reported will be written as well. Wetstone reports that a new version with the capability to save data to any external drive will circumvent this limitation.

Before using US-LATT, it is necessary to download and install the configuration utility that is available from Wetstone Technologies, Inc. on the investigator's computer. Instructions on access to the configuration utility are provided in the US-LATT documentation. This configuration utility allows the user to configure the tool and select the data to be acquired from the target computer. Once US-LATT has been initially configured, the configuration utility is not needed until the user changes the acquisition options. The following images provide an overview of the acquisition options for US-LATT. Note that version 1.60 was used in this evaluation process and all selections were enabled for this evaluation.









Evaluation and Testing of US-LATT

The basic procedures for using US-LATT are as follows:

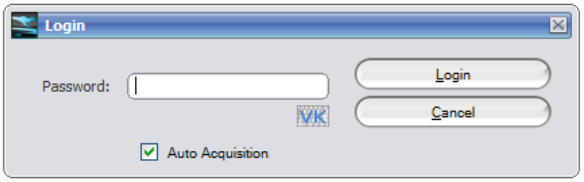
1. Configure the US-LATT thumb drive on the investigator's computer.
2. Insert the configured thumb drive into a target computer.
3 Run the program to acquire the volatile data.
4. Remove the thumb drive from the target computer.
5. Analyze the acquired data on the investigator's computer.

Test: Shop-Built Computer

This test was performed on the shop-built computer (64-bit processor running Windows 7 32-bit operating system with 8 GB RAM).

The shop-built computer is connected to a local area network with other computers, printers and network attached storage. The active profile on this computer had administrator rights, but the User Account Control (UAC) didn't allow US-LATT to initialize using autorun. This is a situation that may be encountered in volatile data collections. Without the autorun functionality, it was necessary to use the Windows Explorer application to navigate to the logical volume that was assigned to the US-LATT thumb drive, then locate and run the file named "KDMv2.exe" that mounts the secure partition.

A login window appears when KDMv2.exe starts. The "Auto Acquisition" option should be checked. Enter the password, and click on the "Login" button.



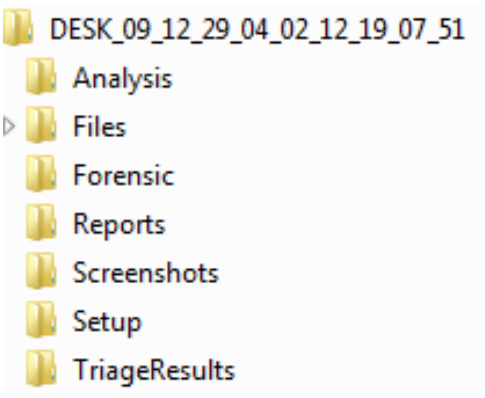
On this particular computer, the UAC required confirmation in order to allow the program to run. Also, the Avast antivirus program intercepted and halted the US-LATT program until Avast was allowed to disable protection for the US-LATT program. US-LATT then began acquiring data and copying it to the thumb drive.

The time required for US-LATT to complete its tasks depends on the type and amount of data selected via the configuration tool. Many factors can affect the amount of time required to complete the acquisition. For example, if the target computer acquisition includes a large amount of RAM or a mounted TrueCrypt container, then the acquisition will require time and available space on the thumb drive. In this test, without a mounted TrueCrypt container, the acquisition process took approximately 40 minutes and wrote approximately 12.8 GB of data to the thumb drive. That 12.8 GB of data included the 7.87 GB of RAM memory. Note that this system contained 8 GB of memory. However, according to Wetstone Technologies, Inc., there is some memory area that is, in basic terminology, protected by the operating system and unavailable to any outside process. It is expected that a small amount of RAM memory will not be acquired.

Results

After US-LATT completed its tasks, all of the acquired data was stored on the US-LATT USB device. The folder structure shown below was created on the USB device. Note that the parent folder name reflected the NETBIOS name of the target computer

[DESK_09_12_29] in this case, followed by the date and time of acquisition (4/2/12 @ 7:07:51 pm).

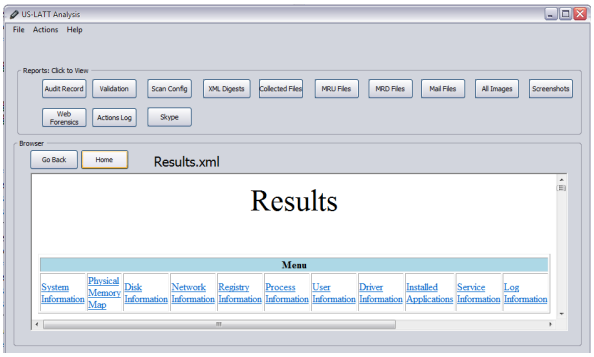


The acquired data has two important aspects.

The first aspect is the ease of reviewing all the data that was acquired. US-LATT provides a reporting application that provides an easy-to-read analysis report.

The second aspect is the ability to acquire the contents of RAM from a live system. US-LATT does this by dumping the contents into a file that can be read by most forensic software or a hex editor. This file is similar to a dd or disk dump image.

Shown below is the main page of the analysis report. Embedded in the analysis report are other reports, such as Audit Report, Validation Report, etc. From the main menu, the investigator can easily view the results of the acquisition process.



Following is the information provided in the 'Results Menu' section of the report.

- The "System Information" option provided the following details.

Operating System Information	
Operating System:	Windows 7
Version:	6.1
Service Pack:	0.0
Kernel Version:	7600
IP address	192.168.0.2
Time Zone	Pacific Standard Time

Processor	
Count:	4
CPU:	AMD Quad-Core Opteron (Shanghai RB-C2) / Embedded Opteron (Shanghai RB-C2) / Athlon Dual-Core (Regor / Propus RB-C2) / Phenom II (Callisto / Heka / Deneb RB-C2), 45nm
Speed:	2.80031GHz
Family:	15
Model:	4
Stepping:	2

- The "Physical Memory Map" option provided the following details (in hexadecimal). It was confirmed that the Region Size for the four *.bin files, when converted to decimal, matched the byte count (file size) for the four files. The area assigned to the remaining Region Types (Reserved, ACPI Reclaim, and ACPI NVS) was not acquired. According to Wetstone Technologies, Inc., some areas of RAM are protected and off limits to any external program or application.

Physical Memory Map				
Region Begin	Region End	Region Size	Region Type	Filename(s)
0x00000000`00000000	0x00000000`0009F000	0x00000000`0009F000	OS Memory	TriageResults\physmem1.bin
0x00000000`0009F000	0x00000000`000A0000	0x00000000`00001000	Reserved	
0x00000000`000E0000	0x00000000`00100000	0x00000000`00020000	Reserved	
0x00000000`00100000	0x00000000`D7FA0000	0x00000000`D7EA0000	OS Memory	TriageResults\physmem2.bin
0x00000000`D7FA0000	0x00000000`D7FAE000	0x00000000`0000E000	ACPI Reclaim	
0x00000000`D7FAE000	0x00000000`D7FF0000	0x00000000`00042000	ACPI NVS	
0x00000000`D7FF0000	0x00000000`D8000000	0x00000000`00010000	Reserved	
0x00000000`FEC00000	0x00000000`FEC01000	0x00000000`00001000	Reserved	
0x00000000`FEE00000	0x00000000`FEF00000	0x00000000`00100000	Reserved	
0x00000000`FF700000	0x00000001`00000000	0x00000000`00900000	Reserved	
0x00000001`00000000	0x00000002`20000000	0x00000001`20000000	OS Memory	TriageResults\physmem3.bin TriageResults\physmem4.bin

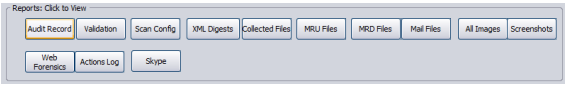
- The "Disk Information" option provided details on disk usage. Analysis of this information matched the configuration of this computer.

- Physical drives (only one was installed in this test computer).
- Disk volumes being used by the system (C:, D:, E:, F:, G:, H:, I:, J:). The assignment of eight volumes accounted for the computer hard drive [C:], a CD-Drive [D:] and a six-slot multicard reader [E: F: G: H: I: J:] installed in this computer.
- USB Device History (listing Name and Serial Number). There were 180 devices listed on the test computer. This particular computer has had many thumb drives connected.
- The "Network Information" option provided a list of adapters. This list was compared to those adapters reported with the "ipconfig /all" command. The US-LATT reported an enabled Ethernet adapter that was not reported by the "ipconfig /all" command. Upon further examination, it was determined that this extra adapter was a miniport interface that Microsoft Windows treats as a network adapter.
- The "Registry Information" option provided details on Recent Searches, OpenSave MRU, Recent Docs, and Last Visited MRU:
  - Recent Searches – 74 different search strings were listed. Analysis of the search strings revealed that they were in fact search strings entered on this computer.
  - OpenSave MRU (Recent Files) – Four different files were listed. Analysis of these file names revealed that they were in fact most recently opened files.
  - Recent Docs – 140 different files were listed. Analysis of these file revealed that they were in fact files that were recently opened.
  - Last Visited MRU – 24 different files were listed. Analysis of these locations revealed that they were in fact folders that were recently accessed.
- The "Process Information" option provided 87 different entries. This information can be used to articulate whether or not errant processes, such as a virus or malware, were running at the time of acquisition.
- The "User Information" provided information on Logged In Users and User Accounts. Two Logged in Users were correctly listed and six User Accounts were correctly listed.

User Accounts			
Name	**Comment**	**Bad P/W Attempts**	**Last Logon**
Administrator	Built-in account for administering the computer/domain	0	993 days 21 hours 31 minutes 13 seconds
ASPNET	Account used for running the ASP.NET worker process (aspnet_wp.exe)	0	
Guest	Built-in account for guest access to the computer/domain	0	0 days 0 hours 0 minutes 34 seconds
HomeGroupUser$	Built-in account for homegroup access to the computer	0	
Randy		0	0 days 2 hours 53 minutes 4 seconds
__vmware_user__	VMware User	0	0 days 2 hours 52 minutes 3 seconds

- The "Driver Information" option provided a list of 217 drivers that were loaded at the time of acquisition. Again, this information enables an investigator to articulate the presence, or absence, of any errant processes.
- The "Installed Applications" option provided a list of 199 applications. Analysis of these applications revealed that they were in fact applications installed on this computer.
- The "Service Information" option provided a list of 455 different services. This information can be used to articulate whether or not some errant service, such as a virus or malware, was running at the time of acquisition.
- The "Login-Logout Actions Log" option provided a list of 1,023 entries. Analysis of this information did not reveal anything of forensic value and actually all 1,023 entries had the same event code and occurred within a four-day time period two months prior to testing.

Following is the information provided in the "Reports: Click to View" section of the report.



- Audit Record: Provided an event timeline of what was done during the acquisition process.
- Validation: Creates a hash for acquired files for future confirmation that the acquired data was not tampered with.
- Scan Config: A display of the US-LATT configuration settings used in the acquisition process.
- XML Digests: MD5 hashes of the various XML files.
- Collected Files: This is a list of the actual files collected during the acquisition process. Note that it is the modified, created or access dates falling within the 'age' set by the configuration utility setting that determines which files are collected. In this case 1,459 files were collected. The types of files collected were based on the settings in the configuration utility and in this case included BIN, CFG, DAT, DB, DLL, DOCX, EXE, HTM, HTML, ICO, INF, INI, JPG, MDB, PNG, SQL, SYS, TMP, TXT, WAV, XML and ZIP. The following information was detailed for each file:
  - Thumbnail (if available).
  - Copied Filename.
  - Original Filename.
  - Owner.
  - MD5 Hash.
  - Filesize.
  - Modified Time.
  - Created Time.
  - Access Time.
  - Readonly.
  - Hidden.
  - Archive.
- MRU Files: A list of files that were most recently accessed. In this case four files were collected. The following information was detailed for each file:
  - Thumbnail (if available).
  - Copied Filename.
  - Original Filename.
  - Owner.
  - MD5 Hash.
  - Filesize.
  - Modified Time.
  - Created Time.
  - Access Time.
  - Readonly.
  - Hidden.
  - Archive.
- MRD Files: A list of files reported in the My Recent Documents directory of the target computer. In this case, 47 files were collected. The following information was detailed for each file:
  - Thumbnail (if available).
  - Copied Filename.
  - Original Filename.
  - Owner.
  - MD5 Hash.
  - Filesize.
  - Modified Time.
  - Created Time.
  - Access Time.

- Readonly.
- Hidden.
- Archive.

- Mail Files: PST files were collected. The computer used in this testing accessed email mainly via Web-based clients for the past year. The PST files created by Outlook but no longer used were identified an collected. Wetstone reports that Thunderbird and Outlook email client information will also be collected. Futhermore, Wetstone reports that US-LATT will collect email from an active (running) Outlook email client without affecting the operation of Outlook.

- All Images: The All Images XML file provides a thumbnail view report of the images that were accessed or modified on the computer and collected.

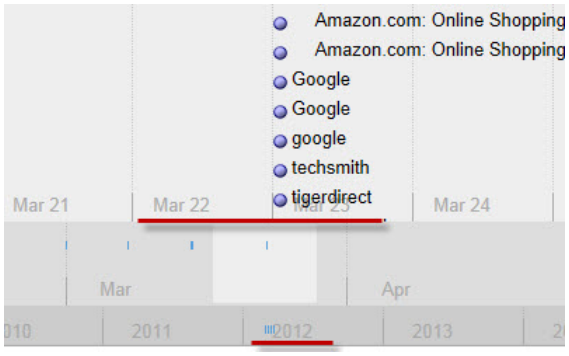
> The **All Images** option creates an XML file containing thumbnails of all the images captured during the triage. These images include those acquired that fit the file collection criteria in the configuration as well as screenshots, and images found in the MRU and My Recent Documents.

- Screenshots: This report contains images of all the windows that were active and/or minimized at the time of the acquisition. This feature can be very useful to capture volatile data. In this test, US-LATT acquired screen captures of minimized Word and Excel files created on the computer screen that were open but had not been saved.

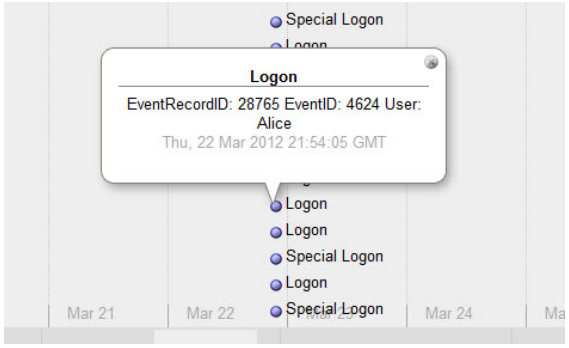
- Web Forensics and Actions Log: Refer to the excerpt below from the US-LATT documentation.

  The application consists of two parts, the XML reports and the analysis functions. The top list box contains all the XML files associated with the case. Selecting an XML report will load into the browser widget below. The second list box, in the middle of the screen, contains analysis functions. The analysis functions currently available are Validate XML Signatures and View All Images Thumbnails. Validate XML Signatures launches sigverify.exe, which performs a signature check on the XML files to verify they have not been altered. This is the same sigverify.exe stored in the forensic directory of the case. View All Images Thumbnails creates an XML file containing thumbnails of all the images captured during the triage. These images include those acquired that fit the file collection criteria in the configuration, as well as screenshots and images found in the MRU and My Recent Document.

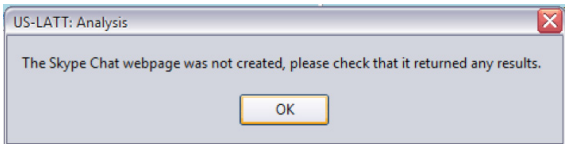
- The Web Forensics report is an HTML report that uses the Web browser on the investigator's computer to display the Web browsing habits of the suspect in a time line view. The time line has the date, the month and the year displayed on the bottom of the report. Each entry can be viewed by simply clicking on the dot to read the information regarding the browsing history. US-LATT can capture data from both Internet Explorer and Firefox.



- The Actions Log is also an HTML report of logon information, reboots and power on and off times. This information creates a computer use time line.



- Skype: Note that Skype was not being used on the target computer. Shown below is a message presented when clicking on the Skype Report button.



- Subsequent tests of the US-LATT Skype capture capability were performed on other test computers and the Skype data was identified and capture. The Skype information collected includes the Call Log, Chat Log and Skype Files Transfer Log.
  - The Skype Call Log reveals the user that made the call, the duration of the call, whether the call was picked up, the direction (outgoing in incoming), the start time of the call, the Skype ID of the person receiving the call and whether it was missed.

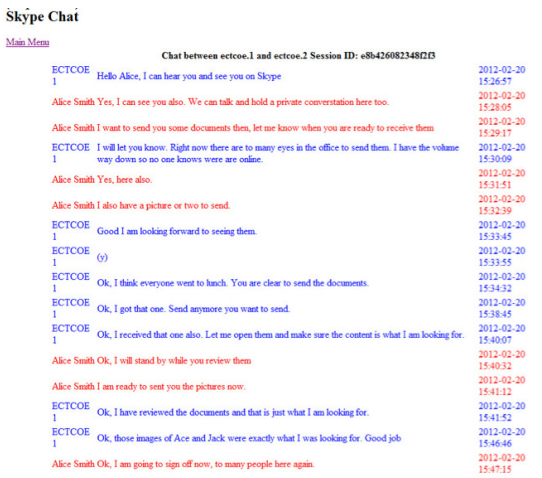
Skype Forensics Menu
Calls | File Transfers | Chat Logs

Skype Calls

Main Menu

HostID	Duration	Pick up State	Direction	Start Time	Audience	Missed Call
ectcoe.1	1372 seconds	Call was picked	Outgoing	2012-02-20 15:25:43	ectcoe.2	No

  - The Skype Chat below reflects the communication between Skype user ECTCOE1 and Alice Smith.



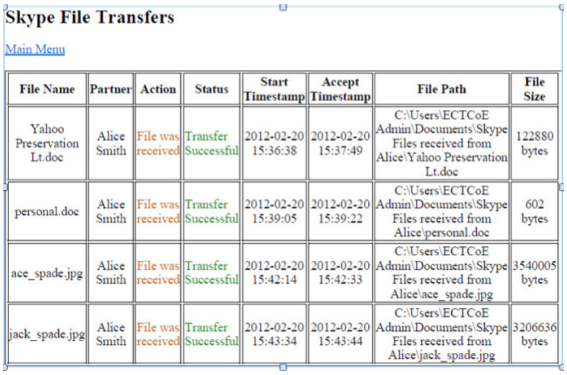
Skype Chat

Main Menu

Chat between ectcoe.1 and ectcoe.2 Session ID: e8b4260823482f3

ECTCOE 1	Hello Alice, I can hear you and see you on Skype	2012-02-20 15:26:57
Alice Smith	Yes, I can see you also. We can talk and hold a private conversation here too.	2012-02-20 15:28:05
Alice Smith	I want to send you some documents then, let me know when you are ready to receive them	2012-02-20 15:29:17
ECTCOE 1	I will let you know. Right now there are to many eyes in the office to send them. I have the volume way down so no one knows were are online.	2012-02-20 15:30:09
Alice Smith	Yes, here also.	2012-02-20 15:31:51
Alice Smith	I also have a picture or two to send.	2012-02-20 15:32:39
ECTCOE 1	Good I am looking forward to seeing them.	2012-02-20 15:33:45
ECTCOE 1	(y)	2012-02-20 15:33:55
ECTCOE 1	Ok, I think everyone went to lunch. You are clear to send the documents.	2012-02-20 15:34:32
ECTCOE 1	Ok, I got that one. Send anymore you want to send.	2012-02-20 15:38:45
ECTCOE 1	Ok, I received that one also. Let me open them and make sure the content is what I am looking for.	2012-02-20 15:40:07
Alice Smith	Ok, I will stand by while you review them	2012-02-20 15:40:32
Alice Smith	I am ready to sent you the pictures now.	2012-02-20 15:41:12
ECTCOE 1	Ok, I have reviewed the documents and that is just what I am looking for.	2012-02-20 15:41:52
ECTCOE 1	Ok, those images of Ace and Jack were exactly what I was looking for. Good job	2012-02-20 15:46:46
Alice Smith	Ok, I am going to sign off now, to many people here again.	2012-02-20 15:47:15

  - The Skype File Transfer log reveals the name of the file, who it came from, the action being received, the status as successful, the start and the accept times and dates, the file location on the hard drive and the size of the file.

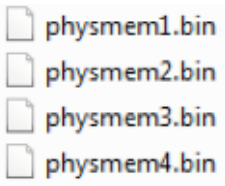


Skype File Transfers

Main Menu

File Name	Partner	Action	Status	Start Timestamp	Accept Timestamp	File Path	File Size
Yahoo Preservation Lt.doc	Alice Smith	File was received	Transfer Successful	2012-02-20 15:36:38	2012-02-20 15:37:49	C:\Users\ECTCoE Admin\Documents\Skype Files received from Alice\Yahoo Preservation Lt.doc	122880 bytes
personal.doc	Alice Smith	File was received	Transfer Successful	2012-02-20 15:39:05	2012-02-20 15:39:22	C:\Users\ECTCoE Admin\Documents\Skype Files received from Alice\personal.doc	602 bytes
ace_spade.jpg	Alice Smith	File was received	Transfer Successful	2012-02-20 15:42:14	2012-02-20 15:42:33	C:\Users\ECTCoE Admin\Documents\Skype Files received from Alice\ace_spade.jpg	3540005 bytes
jack_spade.jpg	Alice Smith	File was received	Transfer Successful	2012-02-20 15:43:34	2012-02-20 15:43:44	C:\Users\ECTCoE Admin\Documents\Skype Files received from Alice\jack_spade.jpg	3206636 bytes

- The target computer was equipped with 8 GB of RAM. US-LATT captured this memory and saved it in the folder named “TriageResults” in file segments shown below with .bin filename extensions. Note that in this case, the size of these four files equaled 7.87 GB. This total acquired size and the protected areas of RAM account for the reported amount of RAM. Analysis of the files “physmem3.bin” and “physmem4.bin” with a hex editor revealed they contained only 00h, indicating that not all of RAM memory was being utilized at the time of acquisition. Further analysis revealed the end of the file physmem.2.bin also contained the 00h character, indicating there was insufficient data in RAM to fill this file.



- These .bin files, which are raw data dumps of RAM, can be analyzed using various forensic tools, such as Encase, Forensic Toolkit or WinHex. Passwords were found within these .bin files that would have been lost had the computer been turned off before acquiring the RAM data with US-LATT. The RAM data can be used to create a dictionary of character strings to access password-protected documents and data.
- According the US-LATT documentation, the tool will acquire the contents of a mounted TrueCrypt volume (see below). This computer contained a 1

MB TrueCrypt volume that contained files. During the first test of US-LATT on this computer, the 1 MB TrueCrypt container was not mounted. The following in an except from the US-LATT documentation:

- When selected, the US-LATT device will collect information about any live file systems mounted on the target machine, such as TrueCrypt drives. This information will be displayed under Disk Information in results.xml.
- In subsequent tests on computers with TrueCrypt volumes mounted, US-LATT properly acquired the data in the mounted TrueCrypt container.

Test: Dell Laptop

This test was performed on the Dell laptop with the Windows XP operating system and 2 GB of RAM. This test computer has multiple user accounts, one with administrator privileges. The following steps were performed for this test:

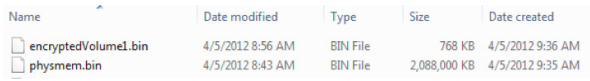
1. Prior to running US-LATT, the non-admin account was logged on and an unsaved Notepad file was created, and two other programs were opened and minimized.
2. The US-LATT thumb drive, configured with all options enabled, was inserted while the non-admin account was active. A message window was displayed indicating that administrator rights were required to run the program. The non-admin account was logged off and the account with administrator privileges was logged on. The Notepad application in the non-admin account had to be closed before the non-admin account could be logged off. The option to save the file was not selected.
3. A password was required to log into the account with administrator privileges. It is important for the investigator to understand that certain features (memory collection, encrypted volume dump, security event logs, etc.) of US-LATT can only be run on a user account with administrator privileges. US-LATT will still collect basic information without an administrator login.

Results

The activity in the non-admin account prior to logging off was not found in the memory dump. No information was associated with the two minimized programs that were running when the non-admin account was logged off.

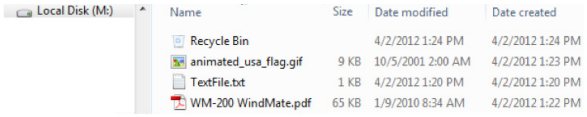
Running US-LATT after logging onto the admin account on this computer caused an Avast antivirus dialog box to appear. After disabling the Avast protection for US-LATT to run, Windows produces a dialog box in which the option to “Protect my computer…” needed to be unchecked before proceeding.

In this test US-LATT placed one file named “physmem.bin” into the TriageResults folder. Also, the testing on this computer revealed that the mounted 1 MB TrueCrypt volume was acquired and placed into the TriageResults folder into a file named “encryptedVolume1.bin.”



Multiple programs are available to view the acquired TrueCrypt volume. For this evaluation, the FTK Imager version 3 program was used and all of the files that were in the TrueCrypt container were available for

viewing unencrypted. As shown below, FTK Imager was used to mount the acquired TrueCrypt container, resulting in an assignment of local disk M.



Analysis of the RAM memory dump revealed the password that was entered to gain access to the user account with administrator privileges, but not the password required to mount the TrueCrypt container.

US-LATT's analyze.exe program was run and the results were similar to the shop-built computer test.

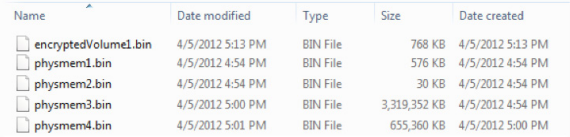
Test: Samsung Laptop

This test was performed on the Samsung laptop with the Windows 7 64-bit operating system and 4 GB RAM. This test computer has TrueCrypt full disk encryption enabled. This computer is configured with one user account that requires a password.

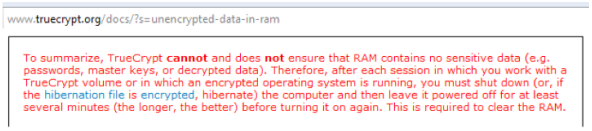
The US-LATT thumb drive configured with all options enabled was inserted into an available USP port. Running US-LATT in this test did not cause an Avast antivirus alert to display and the US-LATT program initialized automatically.

Results

US-LATT placed four files constituting the RAM memory dump into the TriageResults folder. The mounted TrueCrypt volume (the same 1 MB TrueCrypt container file used in the previous tests) was also acquired and placed into the TriageResults folder.



Analysis of the RAM memory dump revealed the password entered to access the user account as well as the password required to mount the TrueCrypt container. The full disk encryption password that was entered at the time the computer booted up was not found.



The 1 MB TrueCrypt volume was identified and acquired by US-LATT. A check of the file revealed it contained all the files stored in the TrueCrypt volume. Note that US-LATT will only acquire a readable TrueCrypt volume if it is mounted at the time the triage is performed.

Conclusion

This program is a valuable tool to have available. US-LATT captures RAM, which can contain passwords, providing access to files and data that would not be accessible had the computer simply been shut down at the time of seizure. This tool also provides screen captures of minimized windows, even when the data in the minimized window has not been saved to the computer hard drive. US-LATT also captures information from the Operating System Registry Keys, which can be valuable for investigative purposes.

Several files had their date and time stamps changed during the running of US-LATT, but there was no evidence that file data was modified. It was also noticed that the US-LATT thumb drive was registered in the USB device list. This is expected with any USB device that is connected to a running computer system without write-protection.

US-LATT provides robust features and functionality that can be used in the field to capture volatile digital evidence from computers running Microsoft Windows Operating Systems. During the testing and evaluation of the US-LATT Token, the tool was found to perform every task tested. The user guide provides detailed information on the configuration and use of US-LATT as well as the review and analysis of the results. This tool will generate a comprehensive report of the triage results and enable the user to assess the investigative value of the data on the computer. US-LATT also includes a signature validated tool to verify that the evidence has not been tampered with since being collected. US-LATT is a valuable resource for the computer crime investigator and digital evidence examiner.

It is important for the user to understand that running computers are in a constant state of flux. Running processes, even those that are unseen to the user, may change files. For example, inserting a USB drive into a running computer may cause the operating system to load hardware drivers. Executing a program such as US-LATT will create running processes. These processes will interact with the computer operating system and applications, resulting in files on the computer being changed. Over the course of these tests, it was determined that the actions of booting a computer, logging onto the operating system, inserting the US-LATT and executing the program resulted in some changes to files on the computer. After analysis, it was determined that the files that were altered or added as a result of these tests were operating system and application files, and not user data.