# **OSForensics** Comparison

Written by:

Colby Lahaie

Researched by:

Colby Lahaie, Kyle Porto, and David Leberfinger



# The Senator Patrick Leahy Center for Digital Investigation Champlain College

Date: 11/7/2012



#### **Disclaimer:**

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

#### Contents

C	ontents	3	1
1	Intro	oduction	3
	1.1	Background	3
	1.2	Terminology	3
	1.3	Research Questions	4
2	Met	thodology and Methods	4
	Figu	ure 1 – OSForensics Options	5
	Figu	ure 2 – Analysis in Progress/Complete	6
	2.1	Data Collection	7
	Tabl	le 1 – Data Generation	7
	Tabl	le 2 – Reference Set for Testing Computer	9
	Tabl	le 3 - Software	9
	2.2	Analysis	10
	2.2.	1 Hashing	10
	Figu	ure 3 – Verify/Create Hash Function	10
	2.2.2	2 Indexing	10
	Figu	ure 4 – Creating an Index	11
	Figu	ure 5 – Searching the Index	12
	Figu	ure 6 – Email Searching	13
	Figu	ure 7 – Email Advanced Search Options	13
	Figu	ure 8 – Keyword Searching	15

Figure 9 – Advanced Search Options	15
2.2.3 File System Browsing	16
Figure 10 – Internet History for Internet Explorer	16
Figure 11 – Internet History for Google Chrome	17
Figure 12 – Internet History for Mozilla Firefox	18
2.2.4 Recent Activity	18
Figure 13 – Recent Activity: Summary	18
Figure 14– Recent Activity: Internet Activity	19
Figure 15 – Download Activity	20
Figure 16 – Example of Timeline in Recent Activity	21
2.2.5 USB Registry Activity	21
Figure 17 – Some USB activity	22
2.2.6 Deleted Files	22
Figure 18 – Deleted File Configuration	23
Figure 19 – Deleted File Search Screen	23
2.2.7 Encrypted Drives	24
2.2.8 EnCase Evidence Processor	24
Figure 20 – EnCase Evidence Processor	24
2.2.9 Report Generation	25
Figure 21 – OSForensics Case Report	25
Figure 22 – Adding Evidence to Case	26
Results	26
Table 4 – Time Comparison	26
Conclusion	27
Further Work	28
References	28

3

4

5

6



#### 1 Introduction

This project is intended to review a restricted version of OSForensics, a free tool created by PassMark Software, to see if it could be used as an alternative to higher priced forensic tools. This will hopefully provide law enforcement agencies with another resource that can help them in their everyday investigations. This project will analyze the effectiveness and accuracy of the OSForensics software as compared to EnCase, one of the most widely used acquisition and analysis tools, and one of the tools we have available here at the LCDI. Although the free OSForensics edition has limited capabilities when compared to the OSForensics pro edition, it is capable of a similar level of analysis as other professional grade forensics software. To see the differences between the OSForensics free and pro editions, you can go to the OSForensics site: <a href="http://www.osforensics.com/compare.html">http://www.osforensics.com/compare.html</a>.

#### 1.1 Background

For this project, we conducted all of the tests at the LCDI and produced our own results. We generated all of our data (web browsing, downloading of files, deletion of files, installing software, USB registry activity, etc.) on a test hard drive, which we then acquired and analyzed with OSForensics and EnCase v7. There has been prior research conducted on capabilities of OSForensics, but we could not find research comparing it to another tool. The LCDI wanted to compare OSForensics to industry professional grade forensics software with a student influence.

#### 1.2 Terminology

**Acquisition** – This is an important step in any digital investigation, and OSForensics has several different options pertaining to acquisition. There is an option to install OS to a USB drive for acquisition purposes, which would be especially useful to implement into a field environment, and there is also a simple drive acquisition function where the program simply makes an image of the acquired drive for further analysis.

**Deleted File Search** – The Deleted Files Search Module can be used to recover files deleted from the file system (i.e. deleted files no longer in recycling bin). This is especially useful for recovering files that the user may have attempted to remove from the system to hide his or her involvement in criminal activities.

**File Carving** – File carving allows the user to view the raw disk data and sort through it to find missing, deleted, or partial files as they appear on the raw disk. OSForensics has a raw disk viewer option which can do this; however, the data carving option attempts to reassemble any of the mentioned files in slack space.

**File System Browser** – The File System Browser provides an explorer-like view and also offers an overview of the devices associated with the case. Additionally, the Browser includes forensic specific information rather than a plain explorer window.

**Hashing** – The Verify/Create Hash module is used for verifying the integrity of files by calculating their hash values. It can also be used to create a hash of a whole partition, physical disk drive, or a simple text string.

Hashing allows the user to create a unique set of characters that corresponds to a file. Think of it like fingerprinting a file, with the hash representing a unique fingerprint. The utility has a simple file browser where the user browses for a file and a hash is created. You can also store hash sets.

**Indexing** – Indexing allows you to search within the content of several files at once. Unlike the other search modules which only inspect filenames and other surface criteria, indexing allows you to perform deep searches inside the content of PDF documents, Word files, E-mails, image meta-data, and other files.

OSForensics Comparison Report – Review Date: 01/1/2013



Indexing in OSForensics is extremely user-friendly. The program is GUI focused, making it simple to create an index of bookmarked items that can be used later in a forensic investigation.

**Raw Disk Viewer** – The Raw Disk Viewer module allows the user to analyze the raw sectors of all devices added to the case, along with all physical disks and partitions (including mounted images) attached to the system. This module is able to perform a more in-depth inspection of a drive, looking beyond the data stored in the file system's files and directories. This level of analysis is necessary when information of interest is suspected to be hidden within the raw sectors of the drive, which are not normally accessible via the normal operating system mechanisms (e.g. free clusters, file slack space).

**Recent Activity** – The Recent Activity module scans the system for evidence of recent activity, such as accessed websites, USB drives, wireless networks, and recent downloads. This is especially useful for identifying trends and patterns of the user, along with any material that has been accessed within a certain amount of time. This option has the ability to gather recent activity from a live machine and an acquired image of a hard drive.

**Searching** – OSForensics has many different search options, including a search of the list of indexed files to recover a specific previously indexed file. This is particularly helpful when dealing with a large case. Another helpful built-in search is the deleted file search. OSForensics searches for any files on the hard drive that are marked for deletion and attempts to recover them if they are not already overwritten. The mismatch file search allows the user to find any files whose raw bytes do not match up with the file extension. There are also many basic search functions within OSForensics such as the hash function, raw disk viewer, etc.

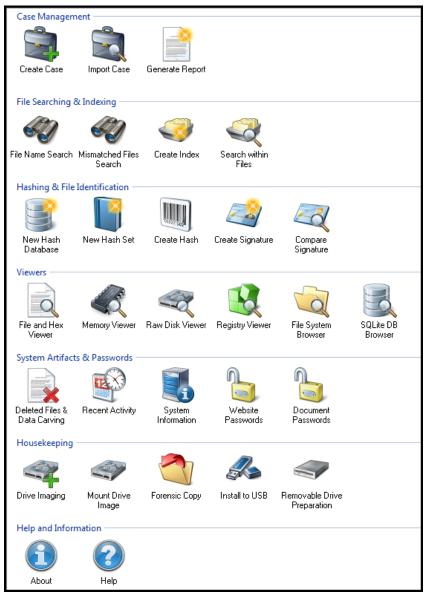
#### **1.3 Research Questions**

- 1. What are the capabilities of OSForensics?
- 2. What is OSForensics not capable of doing?
- 3. How accurate is OSF or ensics when it comes to retrieving and analyzing data from a hard drive?
- 4. Is OSForensics forensically sound?
- 5. How does OSF or ensics compare to industry standard proprietary software, such as EnCase?

#### 2 Methodology and Methods

We initially researched OSForensics to see how it worked, and we found that there are 28 different options that the free edition of OSForensics has available to an investigator (see Figure 1 – OSForensics Options).

#### **Figure 1 – OSForensics Options**



Since there are so many options available in OSForensics, and because we had a limited number of researchers and time, we narrowed them down to what we thought were the most relevant options for a forensic investigation. Below is a list of the options that we tested in OSForensics.

- Internet Activity
- Downloaded File Search
- USB Registry Activity

OSF orensics Comparison Report – Review Date: 01/1/2013

- MRU (Most Recently Used Software)
- Deleted File Recovery
- Encrypted Drives
- Hashing
- Indexing
- Email Searching
- Keyword Searching
- Report Generation

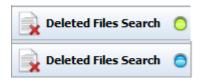
Windows 7 64bit was then formatted and reinstalled on a 250 GB hard drive, which we generated data on for testing with OSForensics. (Please refer to the "Reference Set" attached to the report.)

Following this, we imaged the test hard drive with both OSForensics and EnCase v7. Like most forensic tools, OSForensics creates an MD5 hash of the hard drive before and after acquisition, to show that the data has not been altered in anyway. When we acquired the hard drive, the two hashes matched, proving to us that OSForensics is forensically sound; however, we wanted to further test the validity, so we conducted tests with a 32GB USB drive, as described below.

We used a USB write-blocking registry tweak to make sure that we could alter or change data before we connected the USB drive to the computer. To test that this registry tweak worked, we tried adding data to the USB flash drive. We were unable to add or change data on the USB drive because the disk was write-protected, meaning it was forensically sound. While acquiring the hard drive, OSForensics locks the USB drive so that the data is inaccessible during the process, preventing further data alteration. OSForensics again generated matching MD5 hashes before and after acquisition, proving that OSForensics is indeed forensically sound and able to be used in the field.

One of OSForensics and EnCase's overlapping functions is the ability to conduct multiple types of analysis at the same time. In OSForensics, you have to manually select a process and start it, but in EnCase v7, you can use the "Process Evidence" tool, which will run multiple processes at once. When a function/process is in use, there will be a green flashing circle next to it, and once the tool is done analyzing, the green circle will turn blue (seen below in Figure 2 – Analysis in Progress/Complete). However, it is useful to keep in mind that OSForensics, and most forensic acquisition and analysis tools such as EnCase as well, use a lot of memory, therefore running multiple tools at one time might slow down the examination or cause freezing.

#### Figure 2 – Analysis in Progress/Complete





#### an Data Conection

#### Table 1 - Data Generation

Date	Time	Action / Variable	User Interface / Software	Data
10/16/2012	9:45 am	Logged into system as "lcdi"		
	9:50 am	Downloaded Google Chrome	Internet Explorer	
	9:51 am	Opened Chrome, downloaded iTunes	Google Chrome	
	9:55 am	Installed iTunes	iTunes Installer	
	9:58 am	Opened iTunes	iTunes	
	10:03 am	Downloaded Thunderbird	Google Chrome	
	10:18 am	Installed Thunderbird	Thunderbird Installer	
	10:21 am	Opened Thunderbird	Thunderbird	
	11:31 am	Created Gmail account	Google Chrome	Username: LCDIOSForensics@gmail.com Password: Te\$t@cc0unT
	11:35 am	Setup Gmail account on Thunderbird client	Thunderbird	
	11:53 am	Downloaded mail to Thunderbird	Thunderbird	
	11:53 am	Opened and deleted mail	Thunderbird	Titles: "Import Your Contacts and Old Email", "Customize Gmail With Colors and Themes", "Get Gmail on Your Mobile Phone"
	12:00 pm	Composed and sent email	Thunderbird	Title: "Test Mail" To: Dleberfinger@gmail.com
	12:01 pm	Added items to cart on Newegg.com	Google Chrome	
	12:31 pm	Watched Youtube videos	Google Chrome	
	12:37 pm	Google Search	Google Chrome	"Nissan Delta Wing"
		Visited Nissan.com and Nissanusa.com	Google Chrome	
	12:40 pm	Delete installers from Downloads folder		"itunes64setup.exe" and "Thunderbird Setup 16.0.1"
	12:42 pm	Emptied recycling bin		
	12:48 pm	Created and saved image file	Paint	"Beautiful Art.jpg"



Date	Time	Action / Variable	User Interface / Software	Data
	1:00 pm	Viewed files in Sample Pictures folder	Windows Photo Viewer	
	1:06 pm	Signed into Chrome	Google Chrome	
	1:07 pm	Copied article on dogs and saved	Word Pad	"Dogs.rtf"
	1:08 pm	Made changes to "Dogs.rtf" and saved	Word Pad	"Dogs2.rtf"
	1:09 pm	Google search for "dogs", downloaded two images	Google Chrome	"beer.jpg" and "timba.jpg"
	1:13 pm	Opened Incognito window and watched videos on Youtube.com	Google Chrome	Searched for: "dan bull", "dogs", and "cats"
	1:22 pm	Downloaded video through Keepvid.com	Google Chrome	"Funny Cats.mp4"
	1:26 pm	Logged off system		
10/18/2012	8:35 am	Logged into system as "lcdi"		
	8:36 am	Downloaded TrueCrypt	Google Chrome	
	8:50 am	Created new partition with 20 GB of space	Disk Management	"Local Disk 2 (R:)"
	8:53 am	Formatted outer volume with AES-256 encryption and SHA-512 hash algorithms	TrueCrypt	Password: "Te\$t@cc0unT"
	9:00 am	Moved files to outer volume of (R:)		"timba.jpg", "beer.jpg", "dogs.rtf", "dogs2.rtf", and "Funny Cats.mp4"
	9:05 am	Created and encrypted inner, hidden volume with password.	TrueCrypt	Password: "guesshowmuchilovecats"
	9:08 am	Removed drive letter to keep (R:) drive from showing when not mounted	Disk Management	
	9:16 am	Opened video from (R:) drive		"Funny Cats.mp4"
	9:22 am	Opened Incognito window	Google Chrome	
	9:23 am	Downloaded images to hidden (R:) drive	Google Chrome	"coco.jpg", "cats.jpg", and "Bennie on Butt.jpg"



#### Table 2 - Reference Set for Testing Computer

Reference Set ID	OSForensics Drive Reference Set
Parent	OSForensics_Drive_Relefence_Set
Storage location	Z:\LCDI\Projects\OSForensics
Reference Set type	Operating System (Windows 7)
Container	VMware
Created Date	8/7/2012
Created by	Colby Lahaie
Memory	6 GB Physical
Processor	2.66 GHz Quad Core
Storage	SCSI – 232 GB
CD/DVD	IDE – Auto (Connected at power on)
Floppy	Auto (not connected)
Network	NAT
USB	Auto connect, USB2 support
Sound Card	Connected at power on, using default card
Printer	Connected at power on
Operating System	Windows 7 Professional x64
Standards & Formats:	English (US)
Location:	US
Languages:	No Supplemental language support
Default input language:	English (US), US keyboard
Product Key:	None
Computer name:	C3DI-DISPLAY
Date & Time:	Set to real time
Time Zone:	UTC-05:00 Eastern Time (US & Canada)
Automatically adjust	YES
for daylight savings:	
NTP/server:	yes/time.windows.com
Network:	Default settings (DHCP)
Workgroup:	WORKGROUP

#### Table 3 - Software

Product	Version	Comments
Windows 7 Professional	x64 bit	n/a
Google Chrome	22.0.1229.94 m	
Apple iTunes	10.7.0.21	
Mozilla Thunderbird	16.0.1	
Mozilla Firefox	16.0.1	
TrueCrypt	7.1a	
Piriform CCleaner	3.23.1823 (64- bit)	
VMware Player	3.1.6 build-	



Product	Version	Comments
	744570	
VMware vCenter Converter Standalone Client	5.0.0 build- 470252	

#### 2.2 Analysis

#### 2.2.1 Hashing

OSForensics has the capability to create hashes and hash sets for a single file, a simple text string, or an entire volume with SHA-1, MD5, CRC32, or SHA-256 hashes. An investigator can calculate the hash of the file, text string, or volume and then compare it to a known hash value by copying the known hash value into the Comparison Hash field. The Verify/Create Hash function can be used to hash files and folders on a live computer or a forensic image (see

Figure 3 – Verify/Create Hash Function below). EnCase also has the ability to hash the drive and the files/folders on the drive. The hash completion time will vary depending upon the size of the file or drive being hashed.

#### Figure 3 - Verify/Create Hash Function

Verify /	Create Hash	Help
	○ File	
Volume	N. \PhysicalDrive0: Partition 0 (200.00MB NTFS)	Calculate
Hash Funciton	MD5 Vpper case output 📝	
Progress Data Hashed	SHA-1 MD5 CRC32 SHA-256	
Calculated Hash		
Comparison Hash Selected Hash	The comparison hash is an optional field Function Description	
MD5 (Messag to not be collis	e-Digest algorithm 5) is an internet standard cryptographic hash function. MD5 has been fo ion resistant and therefore not suitable for many security applications. ularity, MD5 is still used in many situations where security is not of high importance or for leg	

#### 2.2.2 Indexing

Create Index and Search Index are tools found in OSForensics that can be used to index data. Before creating an index, you must have an active case open. Indexing allows an investigator to search the contents of many files at once, accelerating the search process. The Create Index option scans the content of emails and other files on the hard drive, OSForensics Comparison Report – Review Date: 01/1/2013 Page 10 of 30



and then constructs an index of the words found. The process of indexing can take a few hours to complete, depending on the size of the drive and the indexing options selected (see Figure 4 – Creating an Index below). When we indexed the hard drive, it took 5 hours and 10 minutes to complete, and it took less than 5 minutes to search the index. The Search Index option allows an examiner to easily and speedily locate text via the created index (see Figure 5 – Searching the Index below).

Create Index	Create Index
Step 1 of 5         What kind of files would you like to index?         Images         Image	Step 5 of 5         Files Indexed       145       Start Time       12/17/12 10:00:24         Emails Indexed       Finish Time       12/17/12 10:00:44         Errors       0       Time Elapsed       00:00:20         Warnings       4       Peak Phys. Mem. Used       90.MB         Total Bytes       98.19 MB       Peak Virt. Mem. Used       1391 MB         Unique Words       10318       Max File & Emails       232
Unallocated Sectors  All Other Supported File Types Unknown Files I would like to manually specify types during the advanced configuration step  Next	Current Action Finished Current File New Index Cancel Open Log

#### **Figure 4 – Creating an Index**



#### Figure 5 – Searching the Index

Sea	arch Ind	ex		
Enter Sea	arch Words	ccleaner	Search	Advanced
Index	k to Search	My Index - Partition_1-0	Use Word	List File
Files (57)	Images (0	Emails (0) Email Attachments (0) Unallocated (0) Timeline Browse Index History		
	CCleaner Partition_	.exe are SYSTEM SECURITY Hardware Interface Component Categories CLSID AppID Invalid eTime Invalid allocation alKey deKey <mark>ccleaner</mark> portable Options False Unchecked Checked Google Chrome VIRTUAL CHECK CHANGED WINDOW 1-0:\Program Files\CCleaner/CCleaner.ccleaner.cclean	Software Pirifo	rm
	rmCClean Partition_	64.exe tion detail exception exception boost thread resource error invalid iterator VIRTUAL CHECK CHANGED WINDOW MESSAGE CCleaner Software er Pirform CCleaner Pirform CCleaner ondInstance ssState ssValue Application Ended updatesuccess 1-0:\Program Files\CCleaner(CCleaner(CCleaner64.exe 4/2012, 6:49 PM Score: 273 Matched: 1	Piriform <mark>cclean</mark>	er
	Translatio Partition_	<b>xe</b> \dvanced Shell msctls msctls Shell Shell Please while Setup loading VERSION nyName Pinform ption <mark>CCleaner</mark> Installer ICopyright Copyright Pinfo n version encoding standalone assembly xmlns schemas microsoft 1-0\?program Files\CCleaner\uninst.exe 4/2012, 7:31 PM Score: 16 Matched: 1	orm ctName <mark>CC</mark>	eaner
9	Chcete st Partition_	i <b>1.dli</b> Im cannot reloc nosti VKliknite venie programu <mark>CCleaner</mark> piriform <mark>ccleaner</mark> aktualiz Pomoc adanie aktualiz programu zobrazenie programu dostup iahnu program <mark>CCleaner</mark> venie Piriform Aktualiz dostupn Chyba 1-01:Program Flies\CCleaner\Lang\lang-1051.dli 4/2012, 10:52 PM Score: 194 Matched: 1	on verzia progra	mu
	versioni vi Partition_	i <b>2.dll</b> Im cannot reloc UKlikoni vizituar faqen internet <mark>CCleaner</mark> piriform <mark>ccleaner</mark> Verifikoj azhurnimet Ndihm verifikuar azhurnimet <mark>CCleaner</mark> Klikoni ndih zitoni faqen internet shkarkuar HKlikoni vizituar faqen internet 1-0:\Program Files\CCleaner\Lang\lang-1052.dll 4/2012, 10:52 PM Score: 223 Matched: 1	ım <mark>CCleaner CCl</mark>	eaner
2	onlinehj lp Partition_	i <mark>3.dll</mark> Im cannot reloc Alternativ EKlicka <mark>CCleaners</mark> hemsida hemsida piriform <mark>ccleaner</mark> efter uppdateringar Online Klicka efter uppdateringar <mark>CCleaner</mark> InEn version tillg nglig nedladdning hemsidan ladda Piriforms 1-0:\Program Files\CCleaner\Lang\lang-1053.dll 4/2012, 10:52 PM Score: 223 Matched: 1	online Klicka <mark>CCl</mark>	eaners
2	Download Partition_	1 <b>.dll</b> Im cannot reloc Einstellungen FHier gelangst <mark>CCleaner</mark> piriform <mark>ccleaner</mark> Updates suchen Online Hilfe <mark>CCleaner</mark> Updates <mark>CCleaner</mark> Online Hilfe ge chten Webseite Download besuchen gelangen Piriform Website Update 1-0:\Program Flies\CCleaner\Lang\lang-1031.dll 4/2012, 10:52 PM Score: 216 Matched: 1	langentEine Ve	rsion
٩	Desitgeu Partition_	( <b>7.dll</b> im cannot reloc Opcions visitar <mark>CCleaner CCleaner</mark> piriform <mark>ccleaner</mark> Comprova ualitzacions actualitzacions <mark>CCleaner</mark> veure ajuda leanermHi versi o visitar Piriform actualitzaci connexi servidor actualitzaci Versi baixar acord 1-0:\Program Files\CCleaner\Lang\lang-1027.dll 4/2012, 10:52 PM Score: 223 Matched: 1	lisponible desca	rre <mark>g</mark> ar
2	Windows Partition_	15.dll Im cannot reloc piriform <mark>ccleaner CCleaner</mark> Piriform <mark>CCleaner CCleaner CCleaner</mark> SHUTDOWN <mark>CCleaner CCleaner CCleaner</mark> uCCleaner Windows Ir Windows Firefox Mozilla Opera Safari Google Chrome Thunderbird Index Hotfix 1-01:Program Files/CCleaner(Lang/lang-1025.dll 4/2012, 10:52 PM Score: 115 Matched: 1	ternet Explorer	

#### 2.2.2.1 Email Search

OSForensics has the ability to search for emails as part of the Search Index options. EnCase v7 can also search for emails with the Evidence Processor tool, which will be covered later in this report. Before conducting an email search, an index of the drive must first be created. When indexing the drive, select the Email option as a type of file to search for. Once the indexing is complete, the user can enter a search word and will be prompted with the results of the search. The search tabs allow an investigator to narrow the results to specific categories of search hits, prompted by a number beside the category denoting the hits filtered into that tab. For example, if there are any search hits in the "emails" tab, clicking the tab will allow the search hits to be tailored for keywords within emails on the acquired drive (see Figure 6 – Email Searching below). An investigator can view email attachments as well, if they contain the search term. He or she can also use the Deleted File Search tool to filter and find deleted email files

(\*.pst,\*.ost,\*.dbx,\*.idx,\*.mbx,\*.eml,\*.mbox). Using the "Advanced..." button, an investigator has the ability to search through emails based on a particular email address. He or she can view emails from the sender's email address and/or the receiver's email address (Figure 7 – Email Advanced Search Options).



#### **Figure 6 – Email Searching**

Sea	irch Index		
er Sea	rch Words gmail		Search Advance
Index	to Search My Index - Partition_1-0	•	Use Word List File
⊨s (179	Images (0) Emails (6) Email Attachments (0) Unallocated (0) Timeline Browse Index History		
	Get Gmail on your mobile phone [image: Access Gmail on your mobile phone] <http: #utm_source="wel-emi&lt;/td" en="" inti="" mail="" mobile="" www.google.com=""><td></td><td></td></http:>		
	From: Gmail Team <mail-noreply@google.com> To: LCDI Test <lcdiosforensics@gmail.com> CC:</lcdiosforensics@gmail.com></mail-noreply@google.com>		
	Partition_1-0:\Users\LCDI\AppData\Roaming\Thunderbird\Profiles\f17z11e9.default\Mail\pop.gmail.com\Trash*6201 Date: 10/16/2012, 10:32 AM Score: 80 Matched: 1		
	Get Gmail on your mobile phone [image: Access Gmail on your mobile phone] <http: #utm_source="wel-eml&lt;/td" en="" intl="" mail="" mobile="" www.google.com=""><td></td><td></td></http:>		
	From: Gmail Team <mail-noreply@google.com> To: LCDI Test <lcdiosforensics@gmail.com> CC:</lcdiosforensics@gmail.com></mail-noreply@google.com>		
	Partition_1-0:\Users\LCDI\AppData\Roaming\Thunderbird\Profiles\f17z11e9.default\Mail\pop.gmail.com\Inbox*6201 Date: 10/16/2012, 10:32 AM Score: 80 Matched: 1		
	Customize Gmail with colors and themes inbox with colors and themes, check out the Themes tab under Settings. Customize Gmail <a href="https://mail.google.com/mail/#settings/theme">https://mail.google.com/mail/#settings/theme</a>	:5>	
	From: Gmail Team <mail-noreply@google.com> To: LCDI Test <lcdiosforensics@gmail.com> CC:</lcdiosforensics@gmail.com></mail-noreply@google.com>		
	UC: Parition_1-0:\Users\LCDI\AppData\Roaming\Thunderbird\Profiles\f17z11e9.default\Mail\pop.gmail.com\Trash*3185 Date: 10/16/2012, 10:32 AM Score: 74 Matched: 1		
	Customize Gmail with colors and themes inbox with colors and themes, check out the Themes tab under Settings. Customize Gmail <a href="https://mail.google.com/mail/#settings/theme">https://mail.google.com/mail/#settings/theme</a>	IS>	
	From: Gmail Team <mail-noreply@google.com> To: LCDI Test <lcdiosforensics@gmail.com> CC:</lcdiosforensics@gmail.com></mail-noreply@google.com>		
	Darition_1-0:\Users\LCDI\AppData\Roaming\Thunderbird\Profiles\f17z11e9.default\Mail\pop.gmail.com\Inbox*3185 Date: 10/16/2012, 10:32 AM Score: 74 Matched: 1		
	Import your contacts and old email a pain to switch email accounts, and we hope this makes the transition to Gmail a bit easier The Gmail Team Please note that importing is	not	
	From: Gmail Team <mail-noreply@google.com> To: LCDI Test <lcdiosforensics@gmail.com></lcdiosforensics@gmail.com></mail-noreply@google.com>		
	CC: Partition_1-0:\Users\LCDI\AppData\Roaming\Thunderbird\Profiles\f17z11e9.default\Mail\pop.gmail.com\Inbox*0 Date: 10/16/2012, 10:32 AM Score: 39 Matched: 1		

#### Figure 7 – Email Advanced Search Options

	Match	Any search words	All search words	
	Maximum Results	5000		
	Date Range			
	🔲 Use Date	Range		
	From: 20-1	Dec-2012	To: 20-Dec-2012	0-
	Email Search Op	ions		
	From gma	ail		
Forensi	To lcdi			
	сс			

#### 2.2.2.2 Keyword Search

To perform a keyword search (part of the Search Index options) in OSForensics, the drive in question must be indexed, if it has not been already. Using the search bar at the top of the screen, an investigator can search for any string(s) or file type(s). Wildcard characters (\*) and (?) can also be used in the search terms to search for multiple words in order to return a larger set of results. An asterisk character (\*) in a search term represents any number of characters, while a question mark (?) represents any single character. This performs an advanced search such as "zoom\*," which would return all pages containing words beginning with "zoom." Similarly, "z??m" would return all pages containing four letter words beginning with 'z' and ending with 'm'. Also, "\*car\*" would produce results for any words containing "car" within them. Placing a hyphen character before a search term will exclude that search term from being included in the search results. For example, a search for "cat-dog" would return all pages containing the word "cat" but not the word "dog." See Figure 8 – Keyword Searching below for a search example using the search term "c?t." Additionally, an investigator can use the "Advanced..." option to narrow down the maximum number of results and date range, which can be seen in Figure 9 – Advanced Search Options. OSForensics also has the option to import a list of search terms through the "Use Word List File" button.

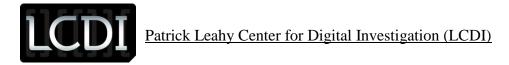
The search option in EnCase v7 allows you to search for keywords using the following search options: ANSI Latin – 1, UTF8, UTF7, Unicode, Unicode Big-endian, GREP, Case Sensitive, and Whole Word. There are also different GREP symbols used, which you can see in Figure below.

#### Figure 8 – Keyword Searching

Enter Sea	arch Words 6?	nce
Index	x to Search My Index - Partition_1-0 🔹 Use Word List File	
Files (166	64) Images (0) Emails (0) Email Attachments (0) Unallocated (0) Timeline Browse Index History	
1105 (100	1ee7aadd217e7b87fd03fdce7fc2c8fce3848daa7e6d1e914e74f89e6924983c.cat	
3	Partition_1-0:\Windows\winsxs\Catalogs\1ee7aadd217e7b87fd03fdce7fc2c8fce3848daa7e6d1e914e74f89e6924983c.cat Date: 10/16/2012, 1:57 PM Score: 44 Matched: 1	
	amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4053_none_88e046c92fae6f57.cat cat	
I	Partition_1-0:\Windows\winsxs\Manifests\amd64_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4053_none_88e046c92fae6f57.cat Date: 10/16/2012, 1:57 PM Score: 44 Matched: 1	
-	2fb5151347a73fb9282c03b4d919f15c91167938cb8890cf57f41aaf3e4c4bd5.cat 	
	Partition_1-0:\Windows\winsxs\Catalogs\2fb5151347a73fb9282c03b4d919f15c91167938cb8890cf57f41aaf3e4c4bd5.cat Date: 10/16/2012, 1:57 PM Score: 44 Matched: 1	
0	Newegg.com - Intel Motherboards %2f696x88.jpg" class="noline" target="" title="Cut from the Same Silicon. A Duo with Limitless Potential_0_Top"> <img< td=""><td></td></img<>	
10-00	Partition_1-0:\Users\LCDI\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0000bd Date: 10/16/2012, 4:03 PM Score: 22 Matched: 1	
4	f_000164 tl)?\"Y \" \ "N \" }cat"+"ch(e ){ }return hp');	
	Partition_1-0:\Users\LCDI\AppData\Local\Google\Chrome\User Data\Default\Cache\f_000164 Date: 10/16/2012, 4:20 PM Score: 5 Matched: 1	
3	f_000173 *** ** ** ** */ #cat{ background: #F4F4F4; color: #222222; font-family: Arial	
	Partition_1-0:\Users\LCDI\AppData\Local\Google\Chrome\User Data\Default\Cache\f_000173 Date: 10/16/2012, 4:21 PM Score: 35 Matched: 1	
7	<pre>f_00022a', infiniti:'1361547'}); function pingDoubleclick( type, cat, events){ var axel= Math.random()+ ""; var</pre>	
	Partition_1-0:\Users\LCDI\AppData\Local\Google\Chrome\User Data\Default\Cache\f_00022a Date: 10/16/2012, 4:39 PM Score: 12 Matched: 1	
3	f_000246 lb-ft). SULEV vehicles are available in California and some northeastern states. S CVT, SV, SR and SL models only."	-
	Partition_1-0:\Users\LCDI\AppData\Local\Google\Chrome\User Data\Default\Cache\f_000246 Date: 10/16/2012, 4:39 PM Score: 4 Matched: 1	
No.	setupapi.dev.log sig: Success: A valid signature was found in an installed catalog sig: Cat:'C:\Windows\system32\CatRoot\{}\	
	Partition_1-0:\Windows\inf\setupapi.dev.log Date: 10/18/2012, 12:50 PM Score: 106 Matched: 1	

#### **Figure 9 – Advanced Search Options**

- A	ndex Advanced		
Match	O Any search words	All search words	
Maximum Results	5000		
Date Range			
🔽 Use Date R	ange		
	1		
		Te. 20 Nov. 2012	Trees and
From: 11-No	w-2012	To: 30-Nov-2012	
		To: 30-Nov-2012	
Email Search Optio		To: 39-Nov-2012	
		To: 0-Nov-2012	
Email Search Optio		To: 0-Nov-2012	
Email Search Optio		To: 0-Nov-2012	



#### 2.2.3 File System Browsing

OSForensics has a tool known as "File System Browser," which is nearly identical to the tree pane feature in EnCase. This tool allows an investigator to browse an acquired drive's file content and export the folders and files associated with the internet history for Internet Explorer (Figure 10 – Internet History for Internet Explorer), Google Chrome (

Figure 11 – Internet History for Google Chrome), and Mozilla Firefox (Figure 12 – Internet History for Mozilla Firefox). It also displays every file and folder on the hard drive. Using Recent Activity, OSForensics's history viewer, an examiner could then analyze the files displayed. Unlike OSForensics, EnCase does not have a built in history viewer, so in order to examine these files, an examiner would have to export the index.dat file out of the image and then use a separate history viewer, such as Mandiant's Web Historian, to view the evidence.

#### Figure 10 - Internet History for Internet Explorer

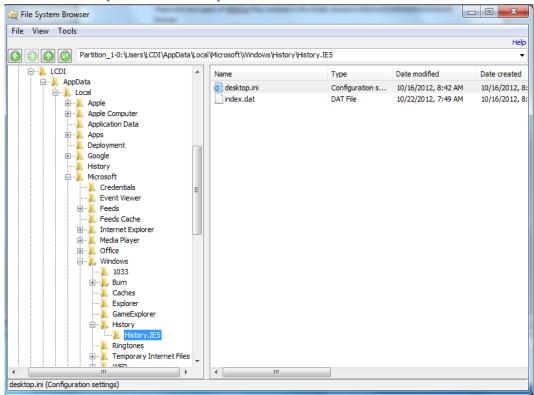


Figure 11 - Internet History for Google Chrome

ile View Tools					н
Partition_1-0:\Users\LCDI\AppDa	ta <b> </b> Loca	ll\Google\Chrome\User Data\Default			
All Users	*	Name	Туре	Date modified	Date create
👜 🕌 dahaie		Cache	File folder	10/22/2012, 7:55 AM	10/16/2012
· → . Default		Extensions	File folder	10/16/2012, 8:50 AM	10/16/2012
		JumpListIcons	File folder	10/22/2012, 8:03 AM	10/22/2012
Display		JumpListIconsOld	File folder	10/22/2012, 8:02 AM	10/22/2012
		Local Storage	File folder	10/18/2012, 12:23 PM	10/16/2012
		Media Cache	File folder	10/18/2012, 11:01 AM	10/18/2012
AppData		Pepper Data	File folder	10/16/2012, 10:36 AM	10/16/2012
E-Local		Sync Data	File folder	10/16/2012, 12:05 PM	10/16/2013
👾 📜 Apple	=	User StyleSheets	File folder	10/16/2012, 8:50 AM	10/16/2013
🕀 📜 Apple Computer		Archived History	File	10/16/2012, 8:50 AM	10/16/2013
📙 Application Data		Archived History-journal	File	10/16/2012, 8:50 AM	10/16/2013
🗄 🖳 📕 Apps		Bookmarks	File	10/16/2012, 8:50 AM	10/16/2013
		Bookmarks.bak	BAK File	10/16/2012, 8:50 AM	10/16/2013
🖃 🦺 Google		Cookies	File	10/22/2012, 8:03 AM	10/16/2013
⊡		Cookies-journal	File	10/22/2012, 8:03 AM	10/16/2013
⊡…】 User Data ⊡…】 Default		Current Session	File	10/22/2012, 8:03 AM	10/16/2013
⊡… <mark>↓ Default</mark>		Current Tabs	File	10/22/2012, 8:03 AM	10/16/201
H-L Extensions		Favicons	File	10/22/2012, 7:55 AM	10/16/2013
	ns	Favicons-journal	File	10/22/2012, 7:55 AM	10/16/2013
		History	File	10/22/2012, 8:03 AM	10/16/2013
Local Stora		History Index 2012-10	File	10/22/2012, 8:03 AM	10/16/2013
📜 Media Cach		History Index 2012-10-journal	File	10/22/2012, 8:03 AM	10/18/2012
🕀 🗐 😥 😥 🕀 😥 🕀 😥	a	History Provider Cache	File	10/22/2012, 8:03 AM	10/16/2013
Sync Data		History-journal	File	10/22/2012, 8:03 AM	10/16/2012
User Styles	nei 🔔	Last Session	File	10/22/2012, 7:55 AM	10/16/2012
			-1	10/00/0010 7 55 111	10/10/10011



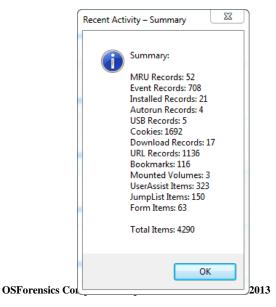
Figure 12 – Internet History for Mozilla Firefox

le View Tools					
					He
Partition_1-0:\Users\LCDI\AppDa	ta\Loca	l\Mozilla\Firefox\Profiles\wqbc4	ar.default		
	*	Name	Туре	Date modified	Date create
		📗 Cache	File folder	10/22/2012, 7:58 AM	10/22/2012
All Users		🌗 mozilla-media-cache	File folder	10/18/2012, 10:01 AM	10/18/2012
		OfflineCache	File folder	10/22/2012, 7:58 AM	10/22/2012
		🐌 startupCache	File folder	10/22/2012, 7:05 AM	10/22/2012
		light thumbnails	File folder	10/22/2012, 7:05 AM	10/18/2012
Default User		urldassifier.pset	PSET File	10/22/2012, 7:58 AM	10/18/2012
🕀 🖳 Display		urlclassifier 3. sqlite	SQLITE File	10/22/2012, 7:58 AM	10/18/2012
🚊 📜 AppData	=				
🚊 🕌 Local					
👜 📜 Apple					
🕀 🔒 Apple Computer					
Application Data					
🕀 🕂 📙 Apps					
😟 🚽 🔒 Google					
······································					
🖻 ·· 📙 Mozilla					
🖻 🕌 Firefox					
i → Mozilla Firefox					
⊡…), Profiles					
i∰, wqbc4lar.defau					
	-	< III			

#### 2.2.4 Recent Activity

Recent Activity can be used to view Web Browser History, Registry Activity, Windows Event Logs, and Windows Jump Lists performed on the computer. To use the recent activity feature, first click on Recent Activity on the tool bar on the left, then select the drive, image, or partition that needs to be searched and click scan. By default, the settings will scan all activity on the drive. If the search only needs results from a certain time frame, select "search date range only" and set the date range in the boxes below. Once the scan is complete, a window will pop up giving you a summary of all records found, which you can see in Figure 13 – Recent Activity: Summary below.

#### Figure 13 - Recent Activity: Summary





Recent Activity has a file list showing the results, which include internet history and activity. Each activity can include the activity type, the source URL, where the file was downloaded to, the username in use, the size of the file, the access and download date and time, and the location of the file that contains the information. By double clicking on one of the items in the file list, it will open up the host website URL in a web browser (see Figure 14– Recent Activity: Internet Activity below). There is also a timeline option that shows you a bar graph of everything that was done on the computer.

Figure 14- Recent Activity: Internet Activity

OSForensics - Test	
🔇 Start	Recent Activity
📓 Manage Case	🖲 Search all items 🛛 💿 Search date range only 🗌 Include dateless items 🔽 Scan
🎻 File Name Search	From: 28-Nov-2012
Create Index	🔘 Live Acquisition of Current Machine 🔵 Scan Drive: Partition_1-0:\
Search Index	File List Timeline
Recent Activity	ChromeSetup.exe Activity Type: Firefox Download Item
Deleted Files Search	Source URL: https://dl.google.com/tag/s/appguid%30%788A690345-D564-463C-AFF1-A69D9E530F96%7D%26iid%3D%7B2DBE2D7F-C777-C6E5-18 Downloaded to: file:///C./Users/Display/Downloads Username: Display File size: 588.3 KB Download Time: 8/25/2011, 12:26 PM
🎻 Mismatch File Search	install_flashplayer10_chrd_aih.exe Activity Type: Firefox Download Item
Remory Viewer	Source URL: http://aihdownload.adobe.com/bin/install_flashplayer10_chrd_aih.exe Downloaded to: file:///iC/Users/Display/Downloads
🥰 Raw Disk Viewer	Username: Display File size: 732.7 KB Download Time: 8/25/2011, 12:20 PM jxpiinstall.exe
🧑 File System Browser	Activity Type: Firefox Download Item Source URL: http://sdic-esd.sun.com/ESD6/JSCDL/jdk/6u27-b07/jxpiinstall.exe?AuthParam=1314292106_db04c9c4da77374b28e32a511e5a5af0&Gro Downloaded to: file:///C:/Users/Display/Downloads
SQLite DB Browser	Username: Display File size: 887.3 KB Download Time: 8/25/2011, 12:19 PM
Passwords	Activity Type: Chrome Download Item Source URL: http://cvcl.mit.edu/hybrid/cat2.jpg
System Information	Downloaded to: C:\Users\LCDI\Downloads Username: LCDI File size: 434.4 KB Download Time: 10/18/2012, 3:23 PM
Verify / Create Hash	https://ieonline.microsoft.com/?ep=ntp Activity Type: Internet Explorer URL Item Username: Display
Hash Sets	Access Time: 2/27/2012, 4:26 PM Location: Partition_1-0\Documents and Settings\Display\Local Settings\History\History.IE5\index.dat
ignature Signature	file:///C:/Users/Display/Desktop/Windows%20Compatibility%20Report.htm Activity Type: Internet Explorer URL Item
a Compare Signature	Usemame: Display Access Time: 1/9/2012, 8:18 AM
Trive Preparation	Location: Partition_1-0:\Documents and Settings\Display\Local Settings\History\History.IE5\index.dat  file:///C:/\$WINDOWS.~BT/Sources/Panther/appcompat_detailed.htm
a Drive Imaging	Activity Type: Internet Explorer URL Item Username: Display
Image Mount Drive Image	Access Time: 11/18/2011, 1:24 PM Location: Partition_1-0:\Documents and Settings\Display\Local Settings\History\History.IE5\index.dat
orensic Copy	file:///C:/Pictures/DSCN7919.JPG Activity Type: Internet Explorer URL Item Username: Display
📣 Install to USB	Access Time: 11/11/2011, 2:48 PM Location: Partition _1-0:\Documents and Settings\Display\Local Settings\History\History.HE5\index.dat
Negister	file:///C:/Pictures/6131210076_e0a12cc2d9_b.jpg Activity Type: Internet Explorer URL Item
(1) About	Username: Display Access Time: 11/11/2011, 1:49 PM Location: Partition 1-0\Documents and Settings\Display\Local Settings\History\History.HE5\index.dat
Exit	File:///C:/Pictures/6131209826_d49bb487c8_b.jpg         Activity Type: Internet Explorer URL Item         Username: Display         Access Time: 11/11/2011, 2:30 PM         Location: Partition_1-0:\Documents and Settings\Display\Local Settings\History\History.His

#### 2.2.4.1 Downloaded Activity

As mentioned previously, Recent Activity has the ability to find everything that was downloaded to the computer. It is also possible to find all download activity for Internet Explorer, Google Chrome, and Mozilla Firefox. In EnCase v7, you have to export the index.dat files for each browser and then open them with Mandiant's Web Historian to do this. After the Recent Activity tool has scanned the live hard drive or forensic image, an investigator can sort the data by date range

OSForensics Comparison Report – Review Date: 01/1/2013



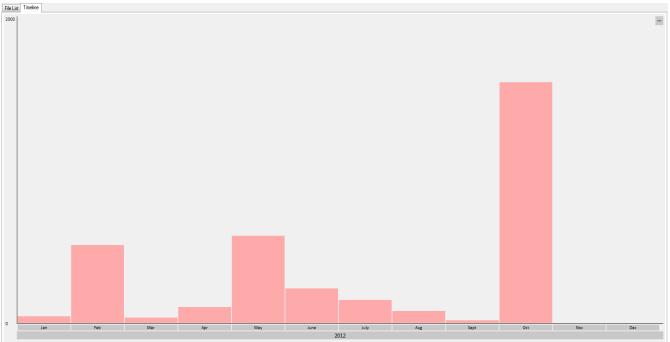
and type of result, making it easier to find the downloaded data needed. OSForensics displays what type of activity it was, what source/website it came from, where the data was downloaded to, what username was logged in when the data was downloaded, and what date and time the data was downloaded (See Figure 15 – Download Activity below for more details).

#### **Figure 15 – Download Activity**

File List	Timeline Timeline Filter Active (Remove) Scope: Oct-2012
ę	Firefox Setup 16.0.1.exe Activity Type: Chrome Download Item Source URL: http://download.cdn.mozilla.net/pub/mozilla.org/firefox/releases/16.0.1/win32/en-US/Firefox%20Setup%2016.0.1.exe Downloaded to: C:\Users\cdnhaiwe\Downloads Username: clahaie File size: 17.39 MB Download Time: 10/16/2012, 7:13 AM
Q	beer.jpg Activity Type: Chrome Download Item Source URL: http://t0.gstatic.com/images?q=tbn:ANd9GcSUblRfIICNHPBL8i33zFHy-7gbY0V8KxB4pawrV82d3kLfdXCU6yVN6HH9tQ Downloaded to: C:\Users\LCD1\Pictures Username: LCDI File size: 10.64 KB Download Time: 10/16/2012, 12:09 PM
Q	timba.jpg Activity Type: Chrome Download Item Source URL: http://upload.wikimedia.org/wikipedia/commons/thumb/4/43/Timba%2B1.jpg/220px-Timba%2B1.jpg Downloaded to: C:\Users\LCDI\Pictures Username: LCDI File size: 15.17 KB Download Time: 10/16/2012, 12:11 PM
ę	cat2.jpg Activity Type: Chrome Download Item Source URL: http://cvcl.mit.edu/hybrid/cat2.jpg Downloaded to: C:\Users\LCDI\Downloads Username: LCDI File size: 434.4 KB Download Time: 10/18/2012, 3:23 PM
	iTunes64Setup.exe         Activity Type: Chrome Download Item         Source URL: http://appldnld.apple.com/ITunes10/041-7197.20120912.Frt4R/ITunes64Setup.exe         Downloaded to: C:\Users\LCDI\Downloads         Username: LCDI       File size: 76.79 MB         Download Time: 10/16/2012, 8:53 AM
ę	Thunderbird Setup 16.0.1.exe Activity Type: Chrome Download Item Source URL: http://download.cdn.mozilla.net/pub/mozilla.org/thunderbird/releases/16.0.1/win32/en-US/Thunderbird%20Setup%2016.0.1.exe Downloaded to: C:\Users\LCDI\Downloads Usermame: LCDI File size: 17.87 MB Download Time: 10/16/2012, 9:03 AM
Q	TrueCrypt Setup 7.1a.exe Activity Type: Chrome Download Item Source URL: http://www.truecrypt.org/download/transient/083b9efaa4/TrueCrypt%20Setup%207.1a.exe Downloaded to: C:\Users\LCDI/Downloads Username: LCDI File size: 3.31 MB Download Time: 10/18/2012, 7:36 AM
	https://mail.google.com/mail/?pli=1&auth=DQAAAIIAAACrp3r0b1FBV3ZjcfbzBmEGNFS3PVcZ8SDpVEF4J-z8uxONb_n3F8DJ4lVV9S9xPbtvmXDdxVua3XK1: Activity Type: Chrome URL Item Username: LCDI Access Time: 10/16/2012, 10:44 AM Location: Partition_1-0:\Users\LCDI\AppData\Local\Google\Chrome\User Data\Default\History
	https://mail.google.com/mail/?shva=1         Activity Type: Chrome URL Item         Username: LCDI         Access Time: 10/16/2012, 10:44 AM         Location: Partition 1-0:\Users\LCDI\AboData\Local\Goodle\Chrome\User Data\Default\History

#### 2.2.4.2 Most Recently Used Software

The Recent Activity feature in OSF or ensics can also be used to see what recent software was installed and used on the computer. The program can see activity from as far back as when the hard drive was first used (or created in some cases). One useful feature of the Recent Activity tool is the "Timeline" tab. When clicking on the "Timeline" tab, the results will appear in a bar graph, showing the number of activities for each period of time (see Figure 16 – Example of Timeline in Recent Activity). By clicking on the bars in the graph, activity is shown from a year to year basis all the way down to hour by hour. By right clicking on any bar, the results can be exported or viewed in OSF or ensics.

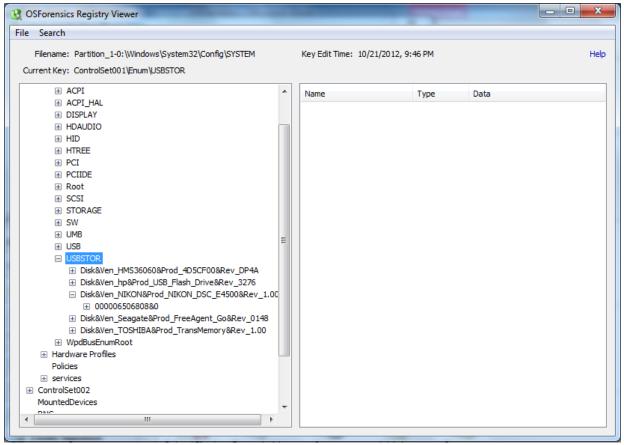


#### Figure 16 – Example of Timeline in Recent Activity

#### 2.2.5 USB Registry Activity

OSForensics, like EnCase, has the ability to find USB registry history. With OSForensics, there is a built in tool called Registry Viewer that allows an examiner to view the registry files of a hard drive, whether it is live or has already been acquired. Before the registry viewer opens, the tool automatically finds all registry files (unlike EnCase, in which they must be manually found) on a drive, such as NTUSER.DAT, DEFAULT, SAM, SECURITY, SOFTWARE, and SYSTEM files. Once a drive is selected along with the registry file(s) needed, in this case SYSTEM, finding USB registry activity or other data follows a similar process to finding the data with EnCase v7 (see Figure 17 – Some USB activity).

#### Figure 17 - Some USB activity



#### 2.2.6 Deleted Files

OSForensics has a built in tool called Deleted File Search that allows an investigator to find all deleted data in the acquisition image. EnCase does not have a specific deleted file recovery feature. In order to retrieve deleted files correctly in OSForensics, an investigator has to click on the Deleted File Search tool, then press the "config" button and select the "File Carving (slow)" option, which can be seen in Figure 18 – Deleted File Configuration below. An examiner has the choice to either verify the images or further carve the files in EXT2 with the "EXT2 Carving (very slow)" option.

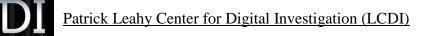
Depending on the size of the acquired hard drive, the Deleted File Search can take up to a few hours to complete. Once the Deleted File Search has finished, it will produce a list of all the deleted files found in the acquired image (see Figure 19 – Deleted File Search Screen below). Filters can also be applied to the deleted files to narrow down results and find the deleted files needed more easily. These filters include: images (\*.gif,\*.png,\*.bmp,\*.jpg,\*.jpeg,\*.tiff,\*.tif); office documents (\*.doc,\*.docx,\*.ppt,\*.pptx,\*.xls,\*.xlsx); compressed files (\*.zip,\*.rar,\*.7z,\*.gz); and email files (\*.pst,\*.ost,\*.dbx,\*.idx,\*.mbx,\*.eml,\*.mbox).

#### Figure 18 – Deleted File Configuration

Deleted File Search Configuration								
Configuration Help								
Quality (	Excellent or Goo	d 🔻						
Case Sen	Case Sensitive							
Include F	olders							
Match WI	nole Word Only							
Multiple s	reams only							
File Carvir	ng (slow)	$\checkmark$						
Image Ve	rification (very slo	w) 📃						
EXT2 Car	ving (very slow)							
File Size Limits:								
Min	КВ							
Мах	КВ							
		OK						

#### **Figure 19 – Deleted File Search Screen**

Disk	Partition_1-0: [Image File]			Search	Config
er String	*.gif;*.png;*.bmp;*.jpg;*.jpeg;*.tiff;*.tif	Presets	Images	s •	Apply Filte
eted Files Fo	und				
99 Size:	_ATK831[1].png 567 Bytes, Attributes: A-I-, Location: Partition_1-0:\_unknown_\ ed: 10/16/2012, 8:48 AM, Modified: 10/16/2012, 8:48 AM, Accessed: 16-Oct-2012 13:48				P
99 Size:	I].gif 43 Bytes, Attributes: A-F, Location: Partition_1-0:\_unknown_\ ed: 10/18/2012, 12:24 PM, Modified: 10/18/2012, 12:24 PM, Accessed: 18-Oct-2012 17:24				8
99 Size	I].gif 43 Bytes, Attributes: A-F, Location: Partition_1-0:\Users\LCDIAppData\Roaming\Apple Computer\MobileSync\Backup\ ed: 10/18/2012, 12:24 PM, Modified: 10/18/2012, 12:24 PM, Accessed: 18-Oct-2012 17:24				P
99 Size	dping[1].gif 43 Bytes, Attributes: A-F, Location: Partition_1-0\_unknown_\ ed: 10/18/2012, 12:24 PM, Modified: 10/18/2012, 12:24 PM, Accessed: 18-Oct-2012 17:24				8
99 Size:	ground-gradient[1].png 394 Bytes, Attributes: A-I-, Location: Partition_1-0:\Users\LCDNAppData\LocaNVMware\VMware vCenter Converter Standalone Client\ ed: 10/18/2012, 12:24 PM, Modified: 10/18/2012, 12:24 PM, Accessed: 18-Oct-2012 17:24				P
99 Size:	vser-spin-info[1].png 559 Bytes, Attributes: A-I-, Location: Partition_1-0:\_unknown_\ ted: 10/16/2012, 8:49 AM, Modified: 10/16/2012, 8:49 AM, Accessed: 16-Oct-2012 13:49				2
99 Size:	ble_sprite_dark[1].png 397 Bytes, Attributes: A-I-, Location: Partition_1-0:\_unknown_\ ted: 10/16/2012, 8:49 AM, Modified: 10/16/2012, 8:49 AM, Accessed: 16-Oct-2012 13:49				P
99 Size	useI-arrow-left[1].png 223 Bytes, Attributes: A-I-, Location: Partition_1-0:\Users\LCDNAppData\Roaming\Apple Computer\MobileSync\Backup\ ted: 10/16/2012, 8:49 AM, Modified: 10/16/2012, 8:49 AM, Accessed: 16-Oct-2012 13:49				8
99 Size:	useI-arrow-right[1].png 223 Bytes, Attributes: A-I-, Location: Partition_1-0:\_unknown_\ ed: 10/16/2012, 8:49 AM, Modified: 10/16/2012, 8:49 AM, Accessed: 16-Oct-2012 13:49				P
66 Size:	ed 'bmp' file 0.bmp 48.05 KB pr: 149416, Byte Offset: 76500992				8
65 Size:	ed 'bmp' file 1.bmp 441.3 KB pr: 3181699, Byte Offset: 1629029888				
68 Size:	ed 'bmp' file 10.bmp 4.95 KB xr: 6637008, Byte Offset: 3398148096				P



#### 2.2.7 Encrypted Drives

An attempt was made to image a drive that was encrypted with TrueCrypt, but OSForensics was unable to image the TrueCrypt partition. We were able to acquire the encrypted drive with EnCase v7, but we were unable to view the contents of the drive; all we could see was scrambled data.

#### 2.2.8 EnCase Evidence Processor

EnCase v7also has the capabilities for hash analysis, email searching, and keyword searching, and EnCase can run certain programs faster than OSForensics. Using a built-in tool called Process Evidence, an investigator can hash the drive, search for emails, and search for keywords all at the same time. It can also be used to find internet artifacts and to create an index (see Figure 20 – EnCase Evidence Processor). By clicking on one of the options (highlighted in blue), you can change options or add different keywords. This allows an investigator to easily conduct an analysis in less time.

EnCase Evidence Pro	cessor	a market	-		100	Same of the	
Evidence Name							
💷 👻 🛄 Split Mo	ode 👻 🚰 Edit						-
Acquire	Process	Name			Previously	Current	
		Partition 1			Processed	Time Zone (UTC-05:00) Eastern Time (US &	Canada)
	(III)	Turtuon 1				(ore-os.oo) custern mile (os d	cunuduj
Current processing							
🛄 👻 🛄 Split Mo	ode 🔻 🚰 Edit 🛃	Save Settings 📴 Load Settings		Sea	rch for keywor	ds	
	Task		Enabled		AND DECEMBER OF A DECEMBER OF A		
Recover Fold			M	Use	his facility to search r	raw text for specific keywords.	The keywords
🔒 File signatur			•	and	heir settings are spec	cified below.	
Protected file			M				
Thumbnail cr	and the second se			Current processing options			
🚩 Hash analysi			M	current processing options			
Expand comp	bound files	120		Ci	at		
Find email			M		its		
Find internet	and the second se			Ic	di		
Search for ke			M				
Index text an	d metadata						
👂 🍶 Modules				E .			
			ОК	Ca	ncel		

#### Figure 20 – EnCase Evidence Processor



#### 2.2.9 Report Generation

OSForensics has a built in Report Generation tool, located under Case Management, which creates an HTML report of the contents of the case (see Figure 21 – OSForensics Case Report). The report has different headings, which are: exported files, attachments, notes, undeleted files, emails, and bookmarks. Once you add a piece of evidence to the report, you will see it under one of the headings. It will show the title of the file, the date the evidence was added to the case, the full path location of the file, and notes. Some will also show the module, which is just the tool that was used to retrieve the data, such as the Recent Activity tool. EnCase v7 also has a Report Generation tool that provides the same type of content, but in a more professional report format than OSForensics. When we first tried creating the report, the outputted report was empty. After further testing, we found that in order to create a report a piece of evidence needs to be added or bookmarked from the acquired image to the case. This can be done by right clicking on the evidence and clicking "Add to Case." Then, you can either choose "File(s)," "List of Selected Items," or "List of All Items," which you ...

can see in

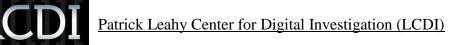
Figure 22 – Adding Evidence to Case.

## Figure 21 – OSForensics Case Report

Case Repo	rt: 'OSForen	sics Comp	are'			
Investigator: Colby Lahaie Date: 12/20/2012, 10:20 Al	M, GMT -5:00					
OSForensics Ex	xports					
Title	OSF Module	Date Added	• Fil	ename 🔹 🔹	Not	es 🏾 🕈
jxpiinstall.exe	Recent Activity	12/20/2012, 10:19 AM	RA 2012-12-20 15-19	-46.html		
Exported Files						
Title	Date Added	• Filename	¢ Origia	nal Path 🔹	Not	es 🗘
	12/20/2012, 10:18 AM	f_0000bd	Partition_1- 0:\Users\LCDI\AppData\ Data\Default\Cache\f_0	Local\Google\Chrome\User 000bd		
Attachments						
Title	÷	Date Added	÷	Filename +	Not	
N/A		Date Added		riiename 👻	NOU	•
Notes						
				2007		-
N/A	Date Added	Filename	•	Not	es	
Undeleted Files	_					
Undeleted Files	5					
Title	Date Added	6	Original Fil	ename	•	Notes 🔹
	12/20/2012, 10:20 AM	datastores.xml				
Emails						
	Title +	Date Added 🔹	Filename	•	Notes	
			h6201_index.html			
	12/20	/2012, 10:20 AM Inbo	x0_index.html			

#### Figure 22 – Adding Evidence to Case

	Open	Shift+Enter		
	Open With			
	Open Containing Folder			
	View with Internal Viewer	Enter		
	Copy File(s) to Clipboard	Ctrl+C		
	Copy Title			
	Show File Properties	Ctrl+I		
	Print			
Forei	Bookmark	• <u> </u>		
	Add to Case	۲.	File(s)	Ctrl+S
	Export List of Selected Items to	•	List of Selected Items	
	Export List of All Items to	•	List of All Items	
	Delete	T		



#### **3** Results

To compare OSForensics with EnCase v7 using all of the processes described above, we used the time it took for each process to complete as our test comparison. Below you will find a time comparison table for OSForensics & EnCase v7.

#### **Table 4 – Time Comparison**

(All times are approximate, based off of the time it took to find a certain piece of evidence and/or search through the evidence. Times also vary based on the amount of data on a drive as well as the performance of the computer that was used for testing each component.)

Item	OSForensics Time	EnCase Time
Acquisition	3 hours 33 Minutes	1 hours 57 minutes
Internet History	Approximately 9 minutes	*Approximately 15 minutes (We had to use Mandiant's Web Historian to view the evidence)
USB Registry History	Approximately 20 minutes	Approximately 20 minutes
Most Recently Used Software	Approximately 1 minute	Approximately 10 minutes
Deleted Files	Approximately 52 minutes	Approximately 2+ hours
Encrypted Drives	Unknown (OSForensics cannot image encrypted drives)	Unknown
Hashing	51 minutes using SHA-1 hashing algorithm on a 212.7 GB image	*Approximately 2 hours 43 minutes
Email Search	Index: 5 hours 10 minutes Index Scan: 5 minutes	*Approximately 2 hours 43 minutes
Keyword Search	Dependent upon number of index entries and search terms; typically it will take a few seconds to a few minutes	*Approximately 2 hours 43 minutes
Downloaded File Search	8 minutes	15 minutes
Report	Approximately 1-5 seconds or more (Dependent	Approximately 1-5 seconds or more (Dependent

	-	
-		1000

Generation	upon amount of evidence added to case)	upon amount of evidence added to case)	
Total Time	Approximately 11 hours 10 minutes	tes Approximately 7 hours 42 minutes	

\*These searches were conducted at the same time; therefore, times will be the same.

#### 4 Conclusion

OSForensics is a powerful forensic acquisition and analysis tool that is easily comparable to other leading tools in the industry, such as EnCase v7. OSForensics has similar features to that of EnCase, and the only thing that OSForensics could not do out of the options that we were able to conduct research on, was acquire encrypted drives. The data produced by OSForensics is accurate; we were able to find the same information while using EnCase v7 and OSForensics in a side-by-side comparison. Also, after testing quite a few different scenarios, we found OSForensics to be forensically sound, as it did not alter or change the data during acquisition.

Overall, OSForensics compares well to EnCase v7 because it can retrieve the same data, while being much more user friendly. Additionally, everything can be done within the OSForensics application. There are two tools in OSForensics (Recent Activity and Deleted Files Search) that outperform EnCase v7. They are simple point-and-click tools that can obtain data in a few minutes. With the Deleted Files Search, you can recover deleted files as soon as you create the case. In EnCase v7, it takes a longer time to recover deleted files, and you have to click through different tabs to find the tool to recover deleted files. The Recent Activity tool in OSForensics is easy to use, and it can obtain all of the activity performed on the computer, including internet data, all within OSForensics. EnCase v7 can obtain internet index.dat files, but you have to open them with a separate software (Mandiant's Web Historian).

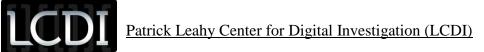
Although OSForensics is extremely user friendly and can do everything within the software, the total time to complete all of the options tested in OSForensics took approximately 3 hours and 28 minutes longer than with EnCase v7. EnCase v7's advantage is the Process Evidence tool that can gather all of the required data (the data we tested in this project) in a short amount of time. Overall, OSForensics has a more user-friendly feel and layout and is much easier to navigate than EnCase v7, but EnCase v7 takes a considerably shorter amount of time. In general, they are both useful tools to have, as they are both accurate and forensically sound and produce the same results.

#### 5 Further Work

There are still many options in OSForensics that we would be interested in researching. There are numerous built in tools, such as the Compare Signature tool and the SQLite DB Browser tool, which are very important and could help an investigator during a case that we did not have the time or resources to investigate. If we had more time for this project and more students to research this project, we could cover all of the tools within OSForensics and conduct a full comparison with EnCase v7. We instead chose the tools that would be commonly used during a forensic investigation.

#### **6** References

PassMark Software Pty Ltd. (2012). *OSForensics*. Retrieved from PassMark Software: http://www.osforensics.com/index.html



Williams, M. (2010). *OSForensics gives up your PC's deepest, darkest secrets*. Retrieved from betanews: http://betanews.com/2011/05/17/osforensics-gives-up-your-pc-s-deepest-darkest-secrets/