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

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: http://www.osforensics.com/compare.html.

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.

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 OSForensics when it comes to retrieving and analyzing data from a hard drive?
4. Is OSForensics forensically sound?
5. How does OSForensics 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

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

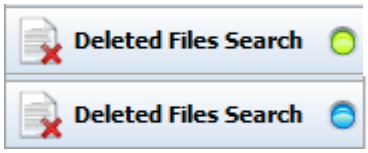
Windows 7 64bit was then formatted and reinstalled on a 250 GB hard drive, which we generated data on for testing with OSForensics. (Please refer to the "Reference Set" attached to the report.)

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



2.1 Data Collection

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
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 for daylight savings:	YES
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	

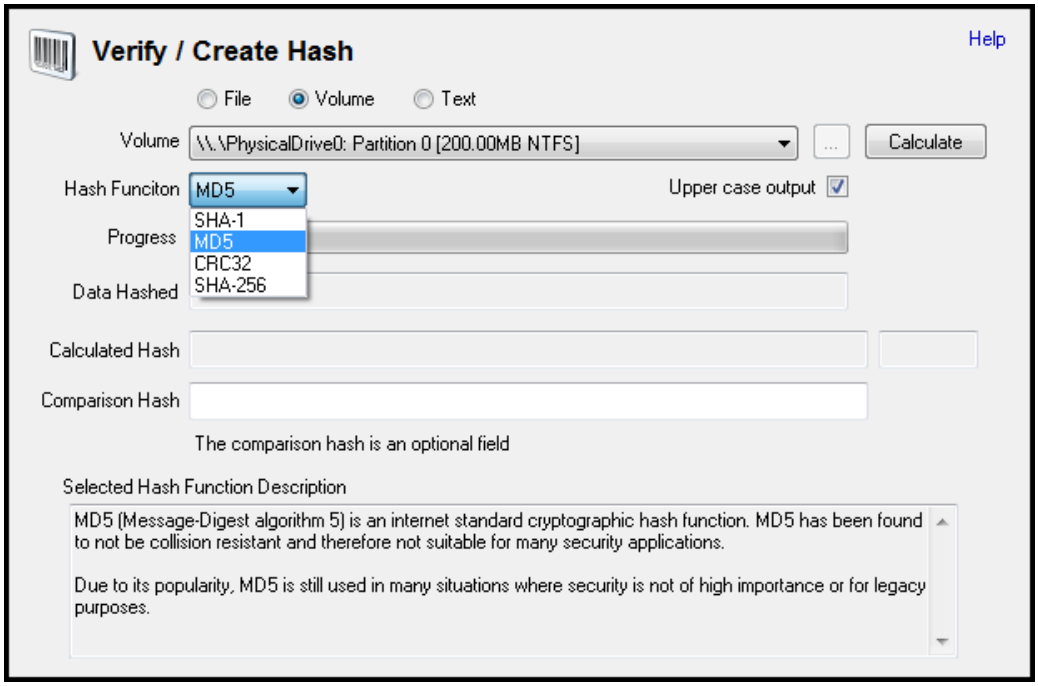
2.2 Analysis

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



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,

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).

Figure 4 – Creating an Index

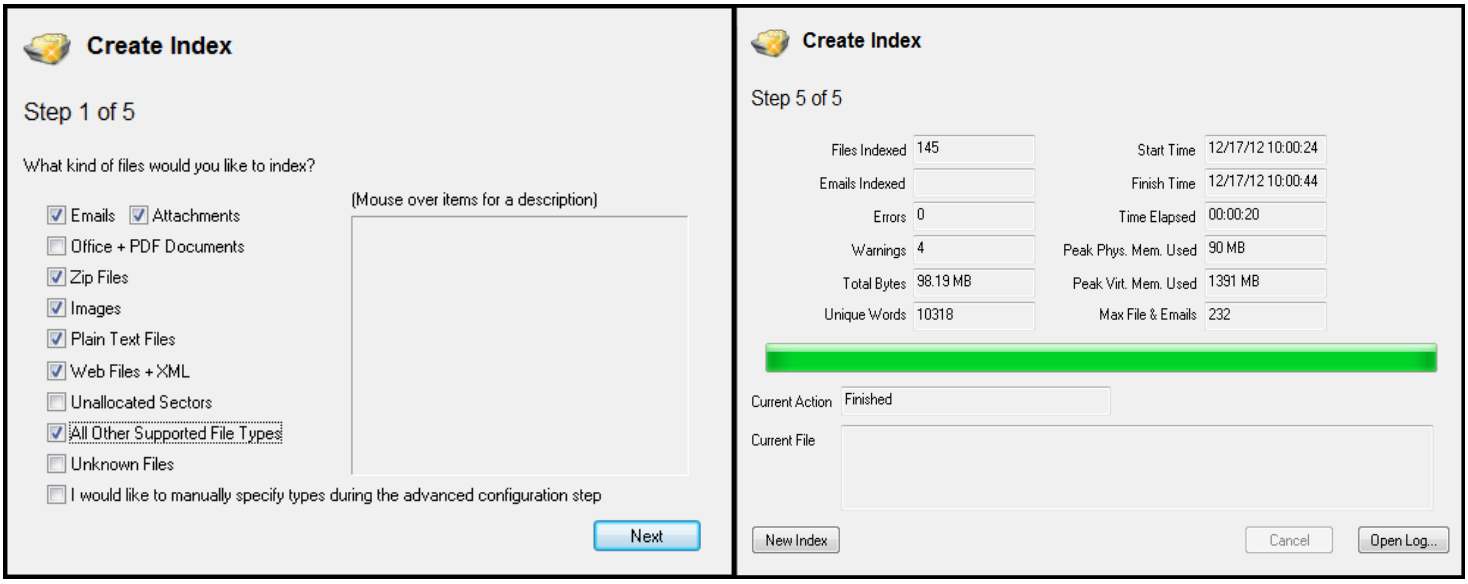
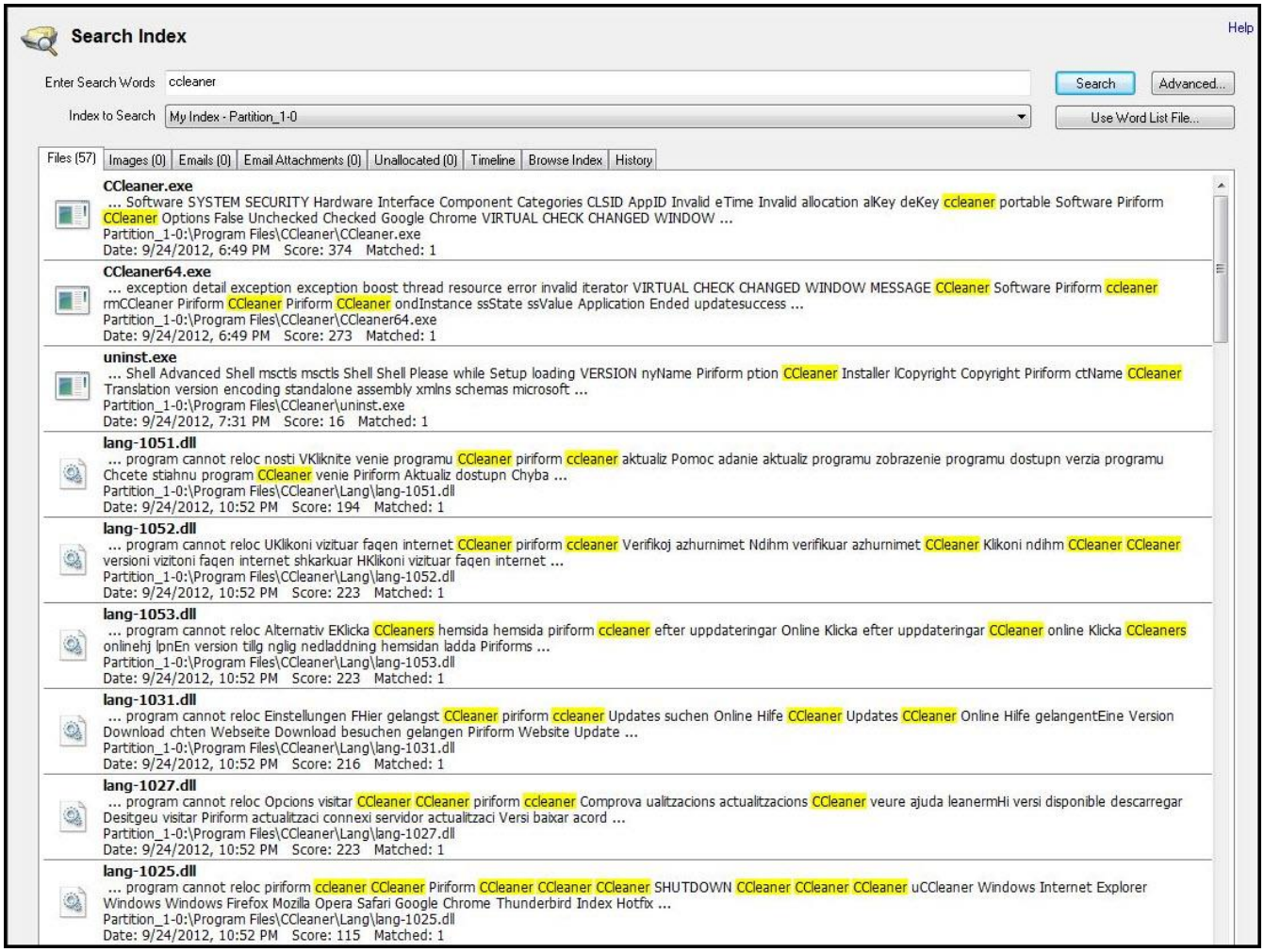


Figure 5 – Searching the Index



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

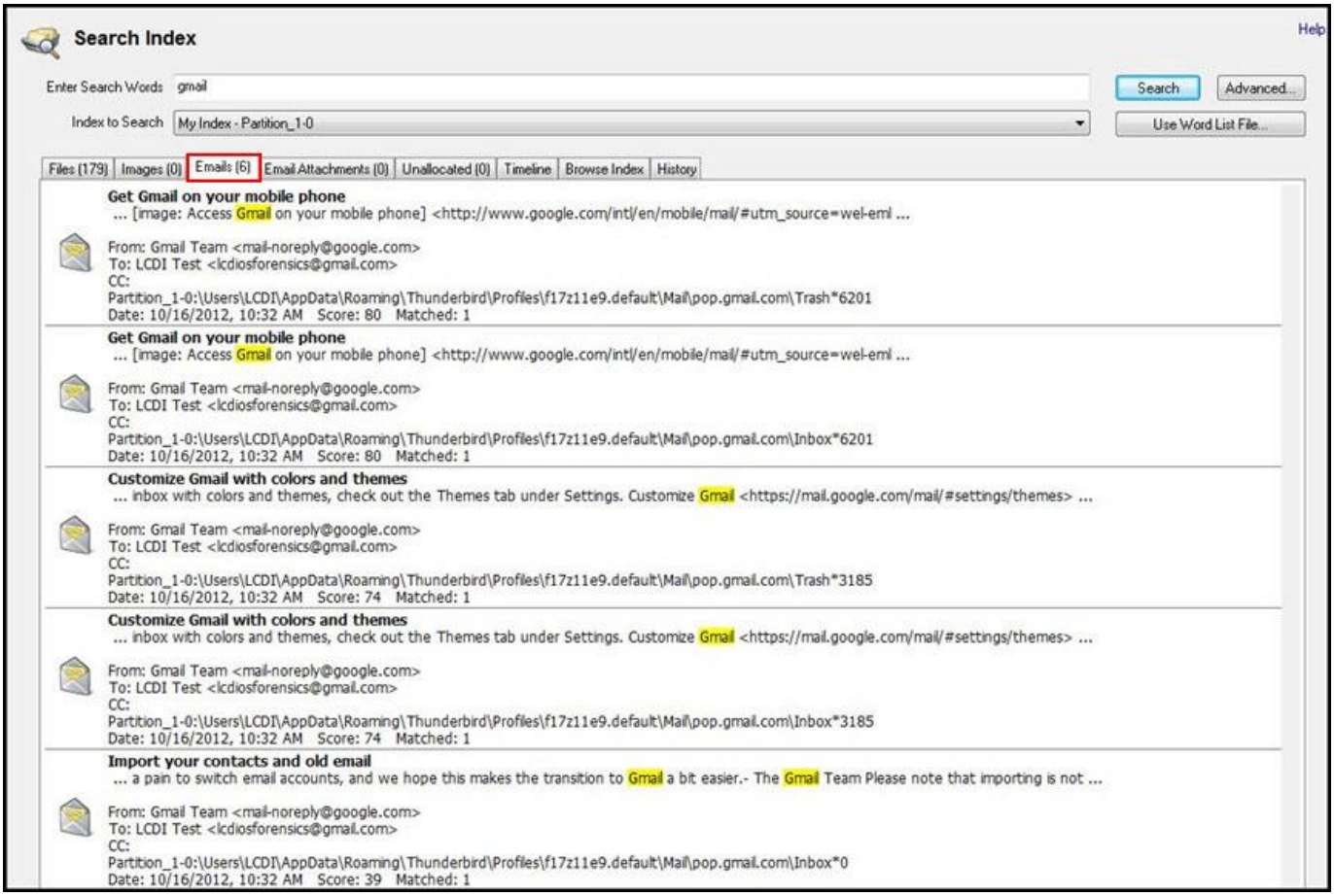
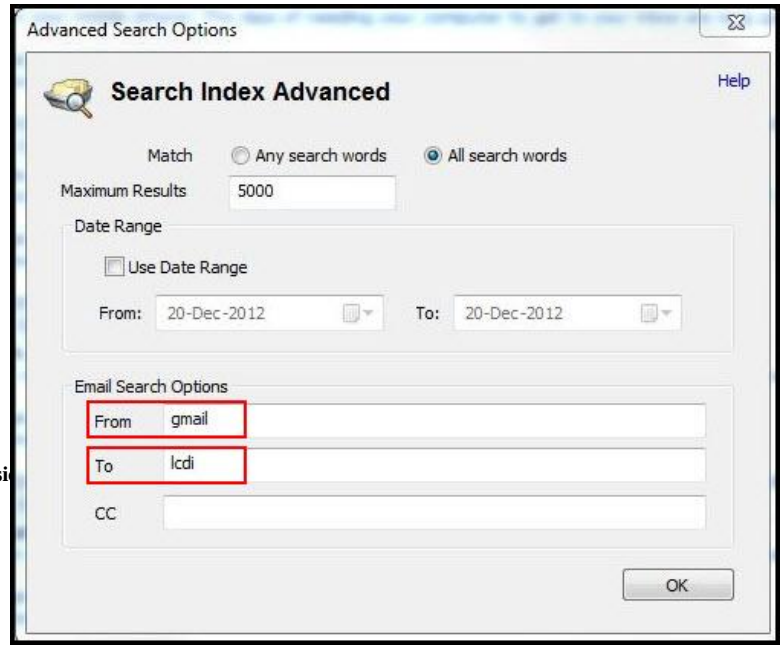


Figure 7 – Email Advanced Search Options



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

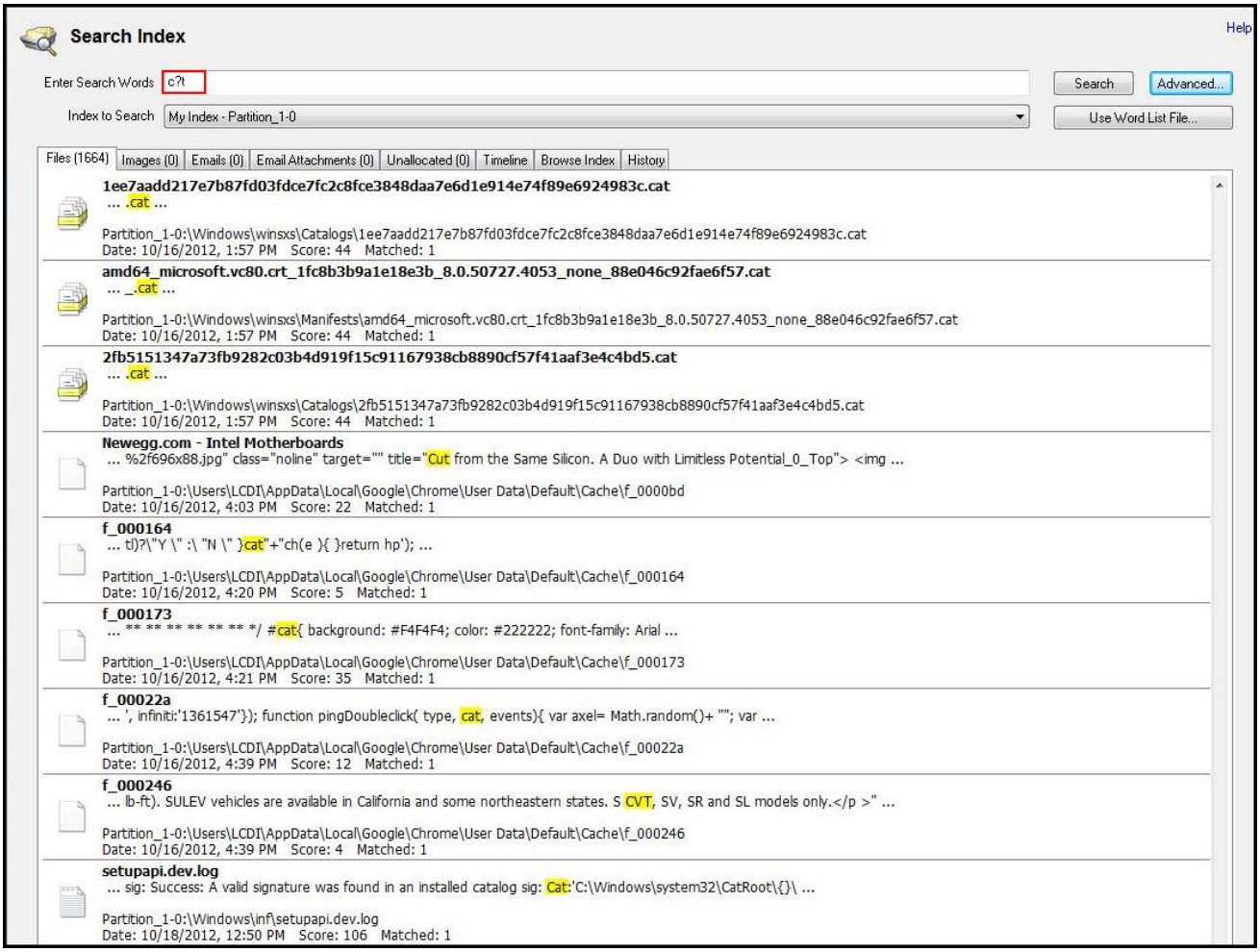
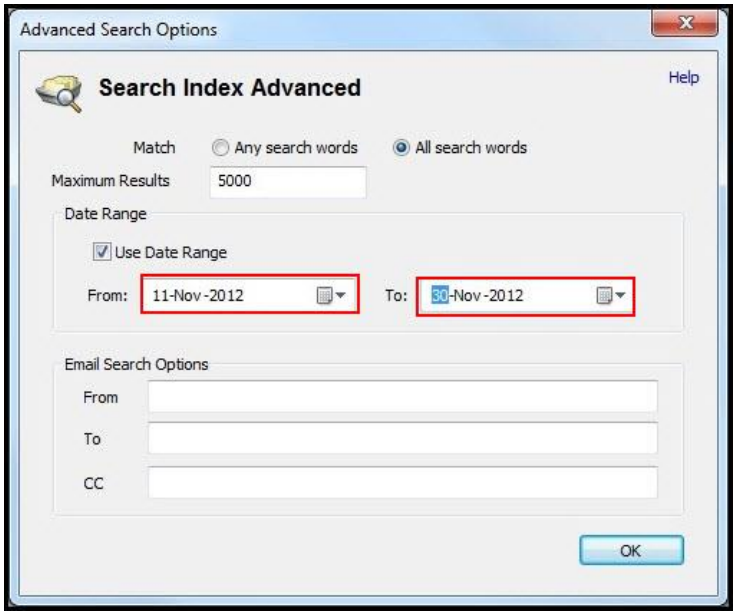


Figure 9 – Advanced Search Options



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

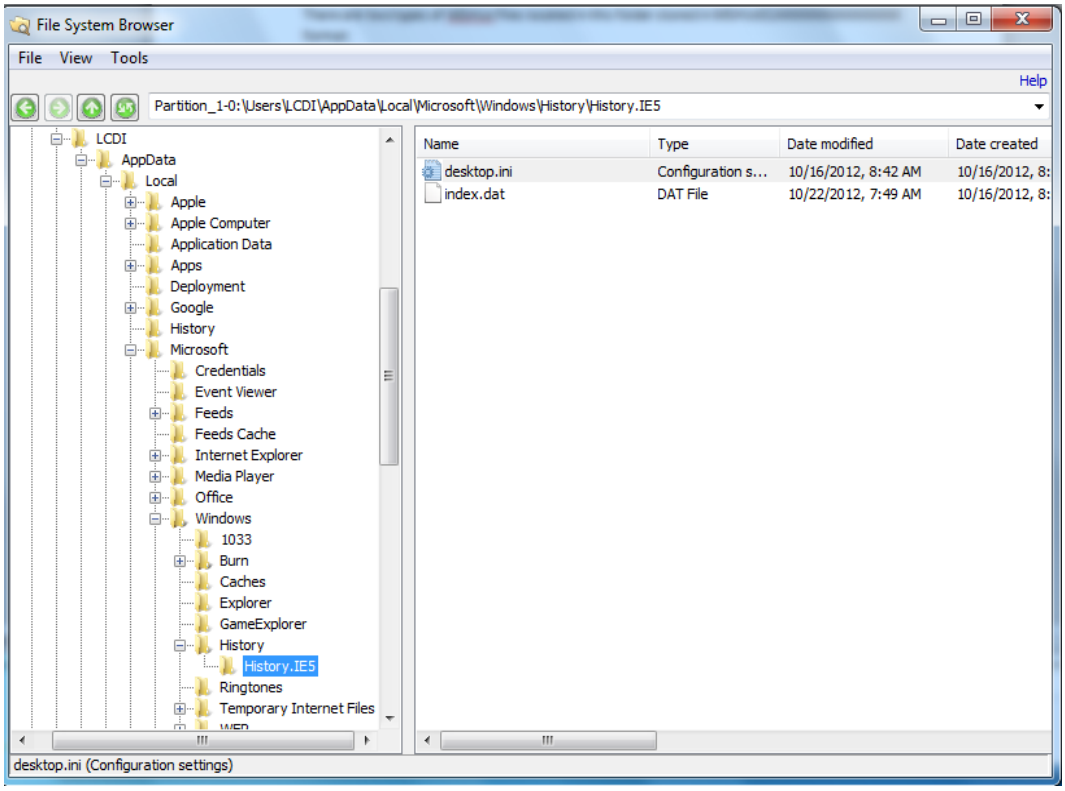


Figure 11 – Internet History for Google Chrome

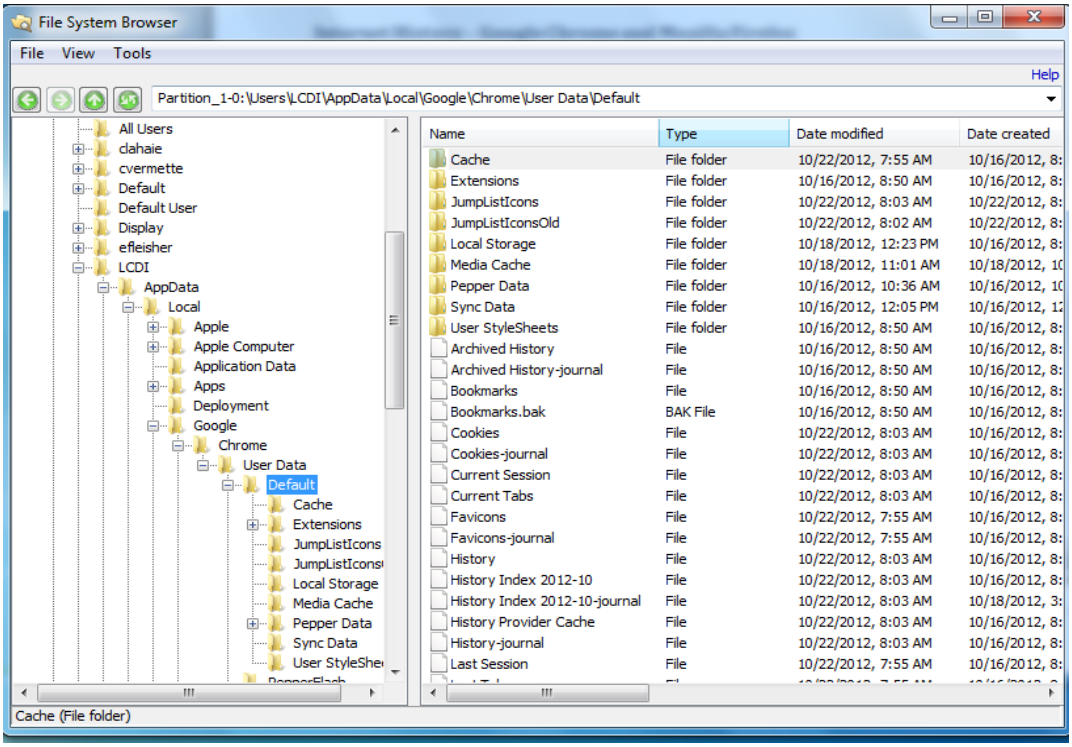
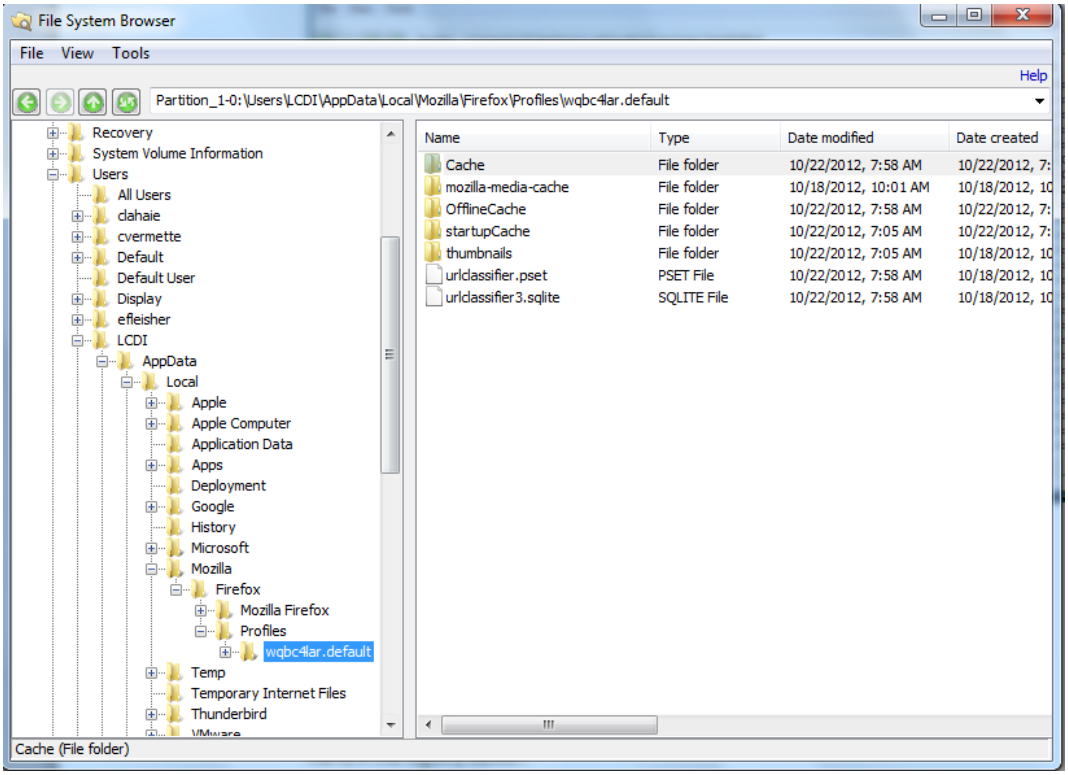


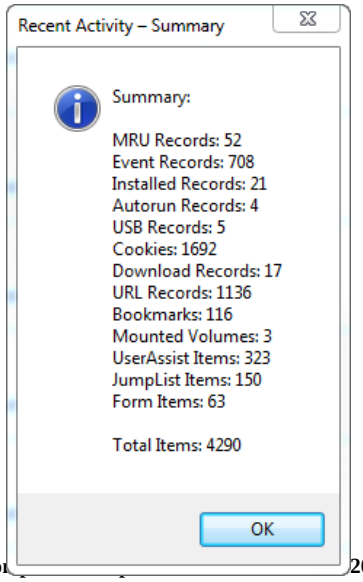
Figure 12 – Internet History for Mozilla Firefox



2.2.4 Recent Activity

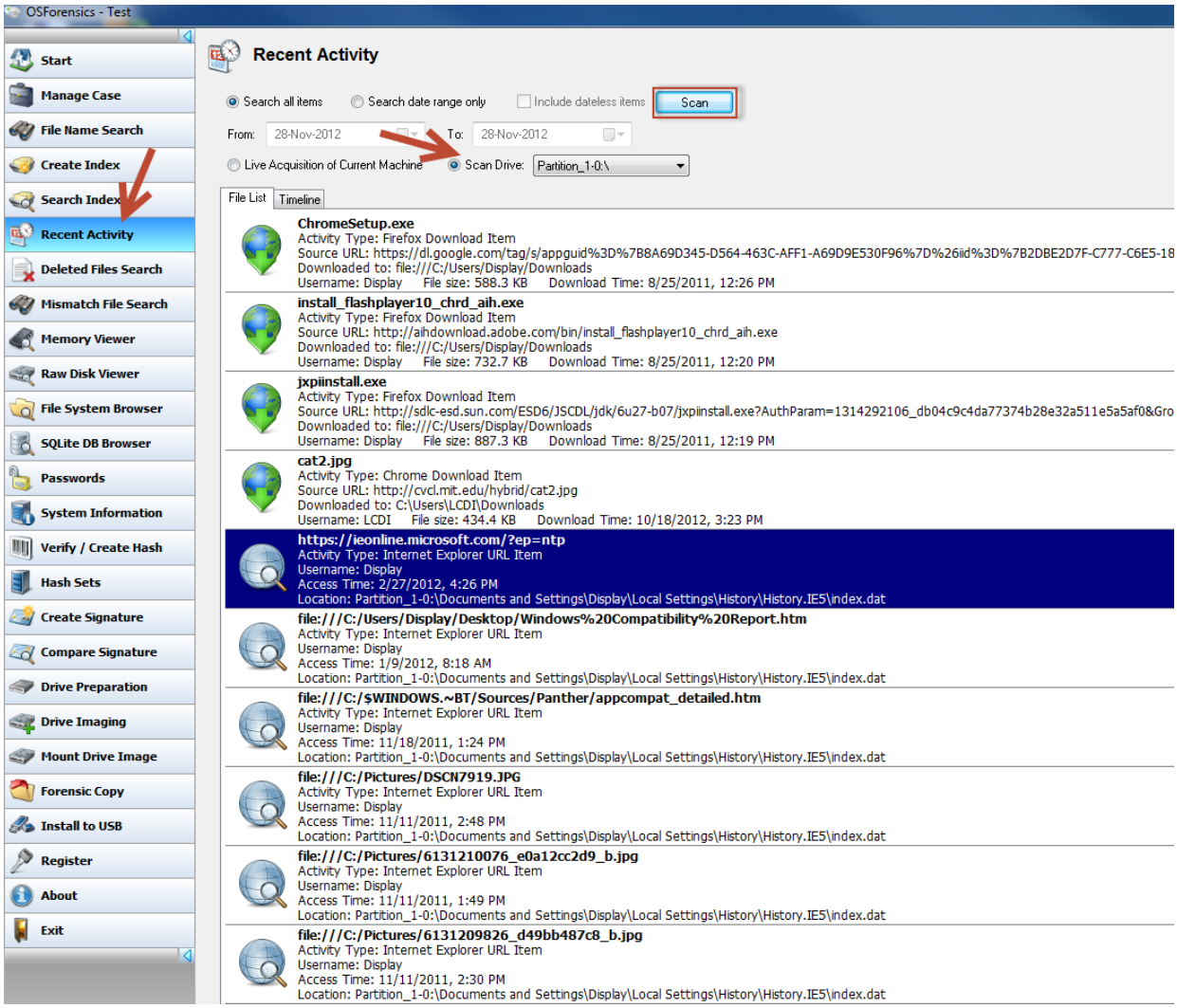
Recent Activity can be used to view Web Browser History, Registry Activity, Windows Event Logs, and Windows Jump Lists performed on the computer. To use the recent activity feature, first click on Recent Activity on the tool bar on the left, then select the drive, image, or partition that needs to be 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

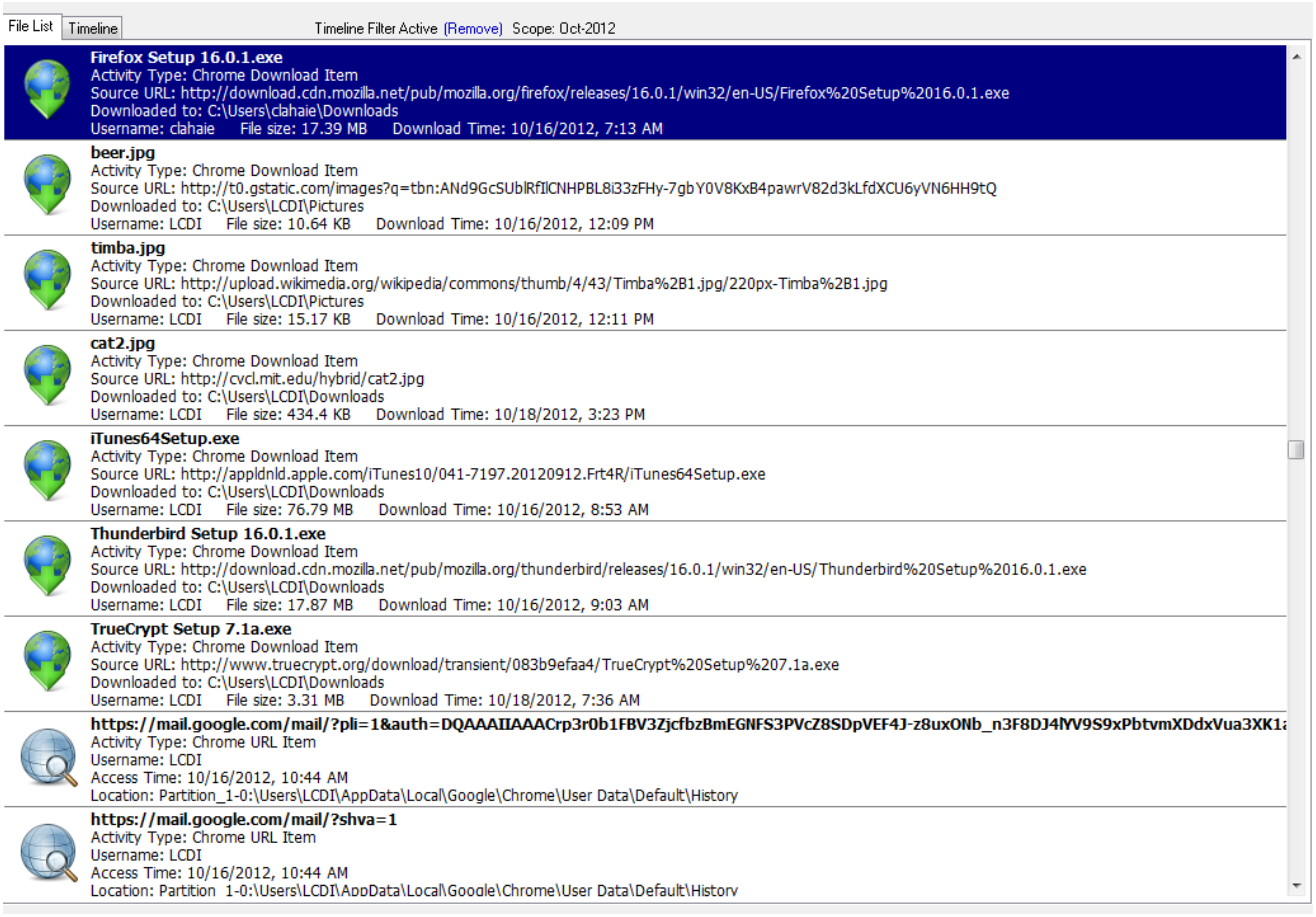


2.2.4.1 Downloaded Activity

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

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).

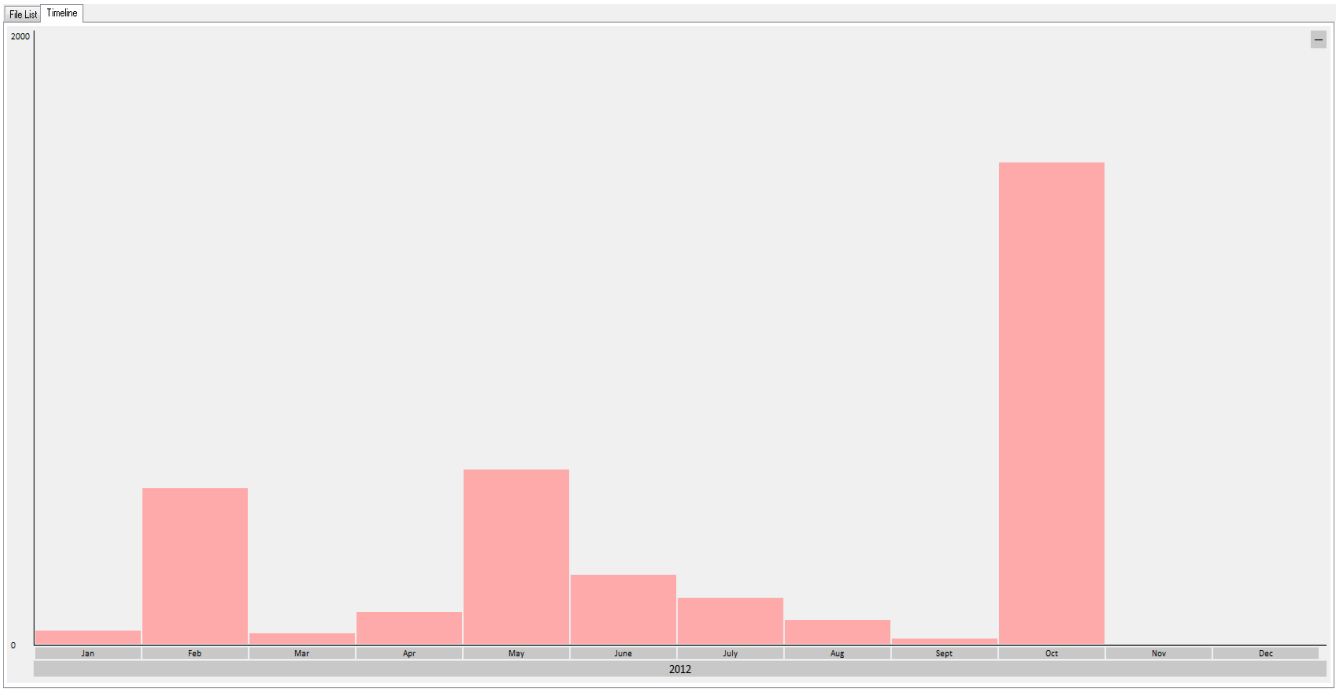
Figure 15 – Download Activity



2.2.4.2 Most Recently Used Software

The Recent Activity feature in OSForensics 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 OSForensics.

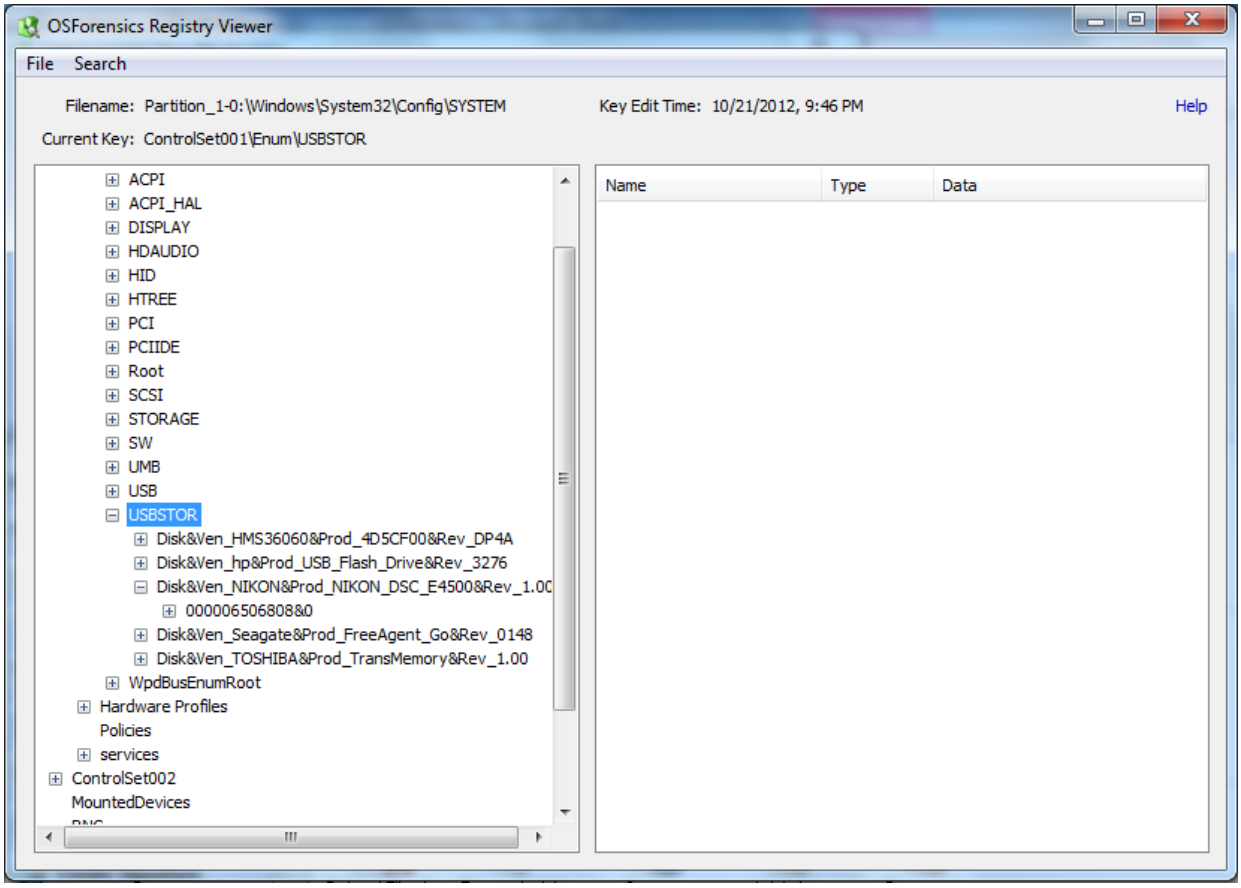
Figure 16 – Example of Timeline in Recent Activity



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

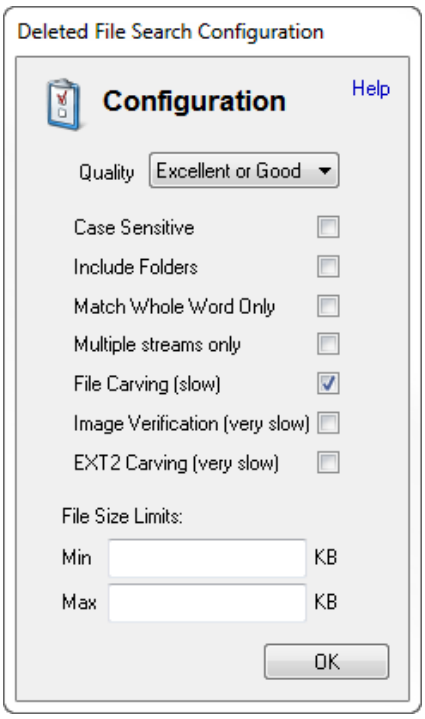
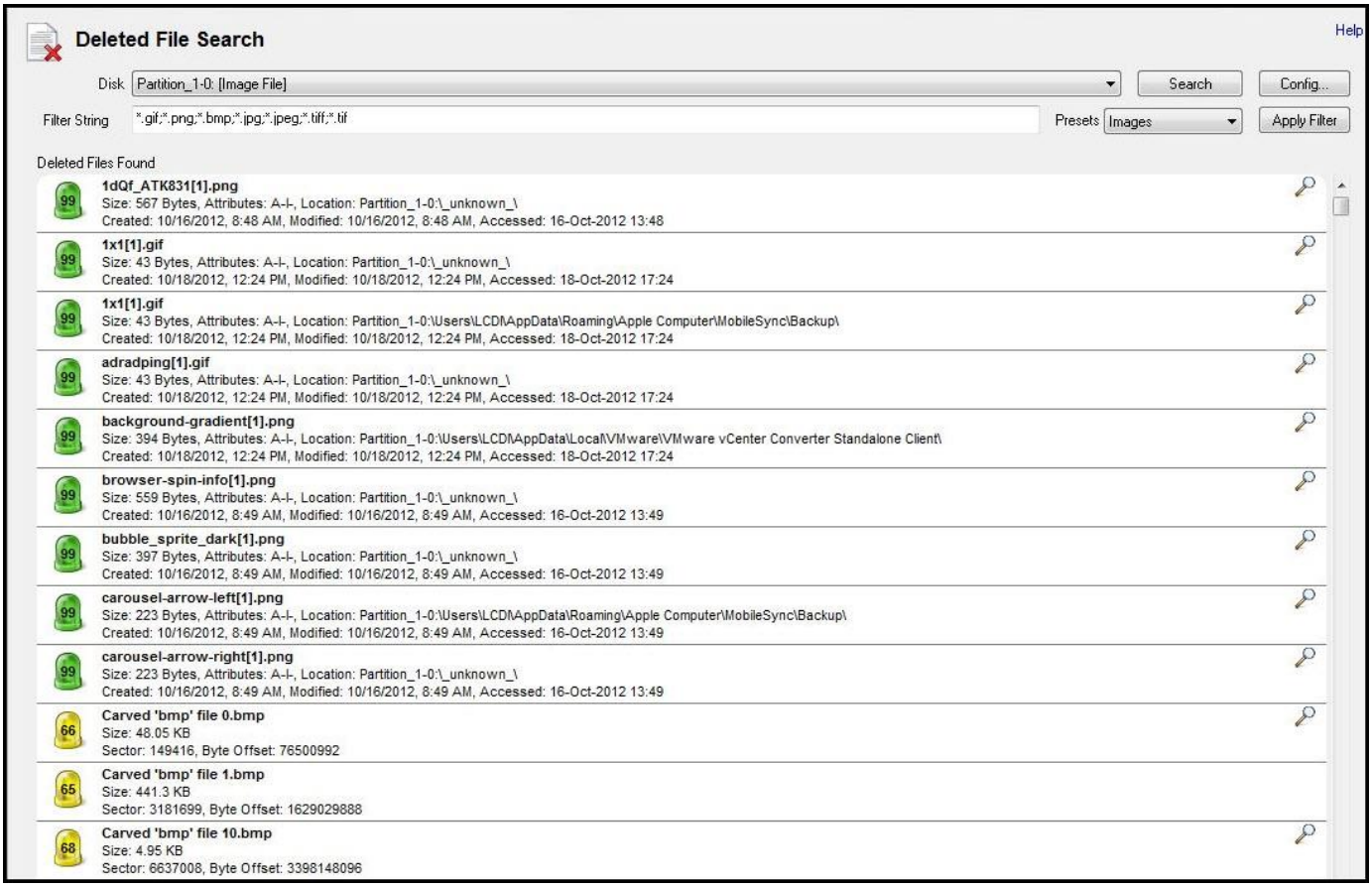


Figure 19 – Deleted File Search Screen



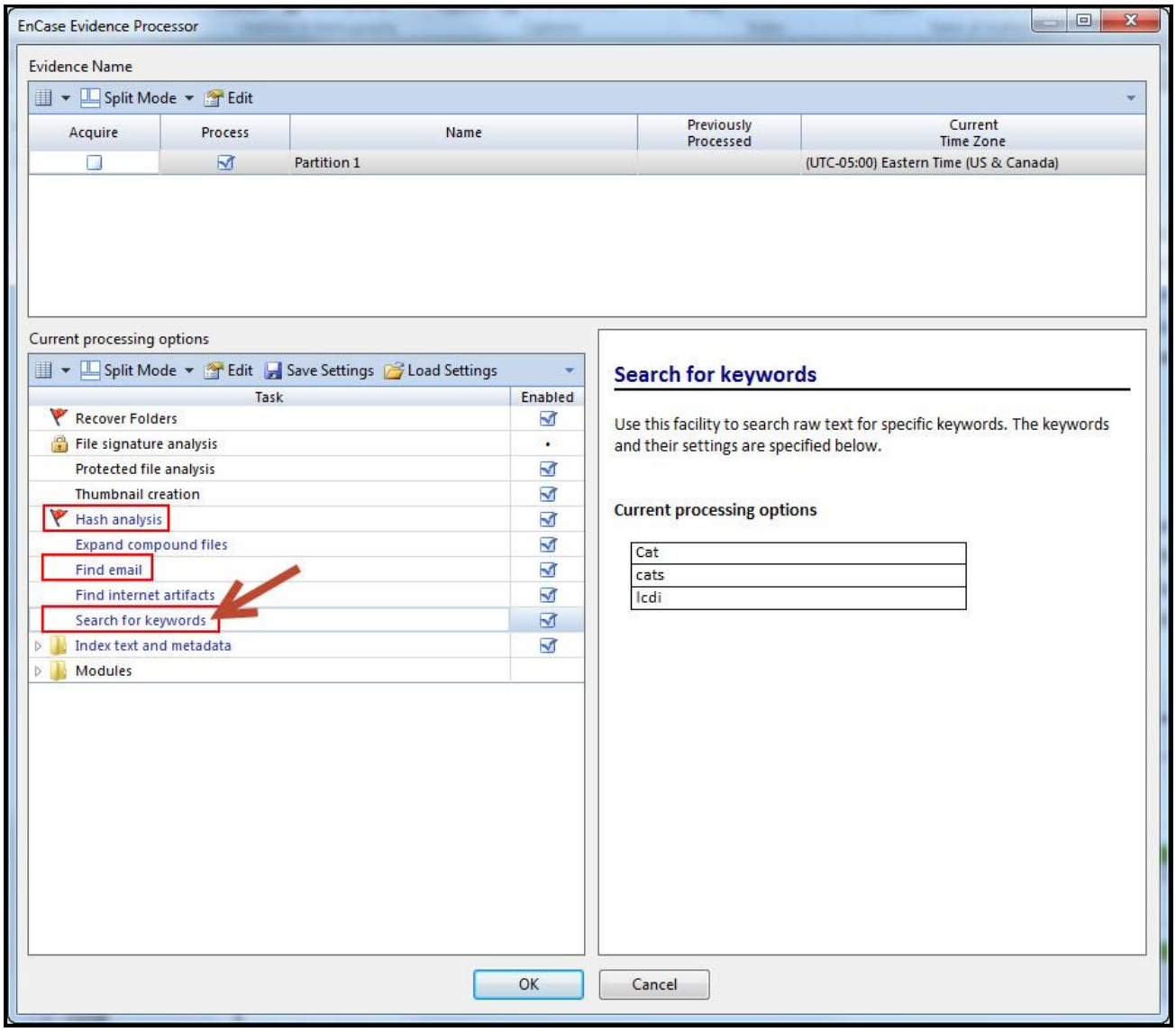
2.2.7 Encrypted Drives

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.

Figure 20 – EnCase Evidence Processor

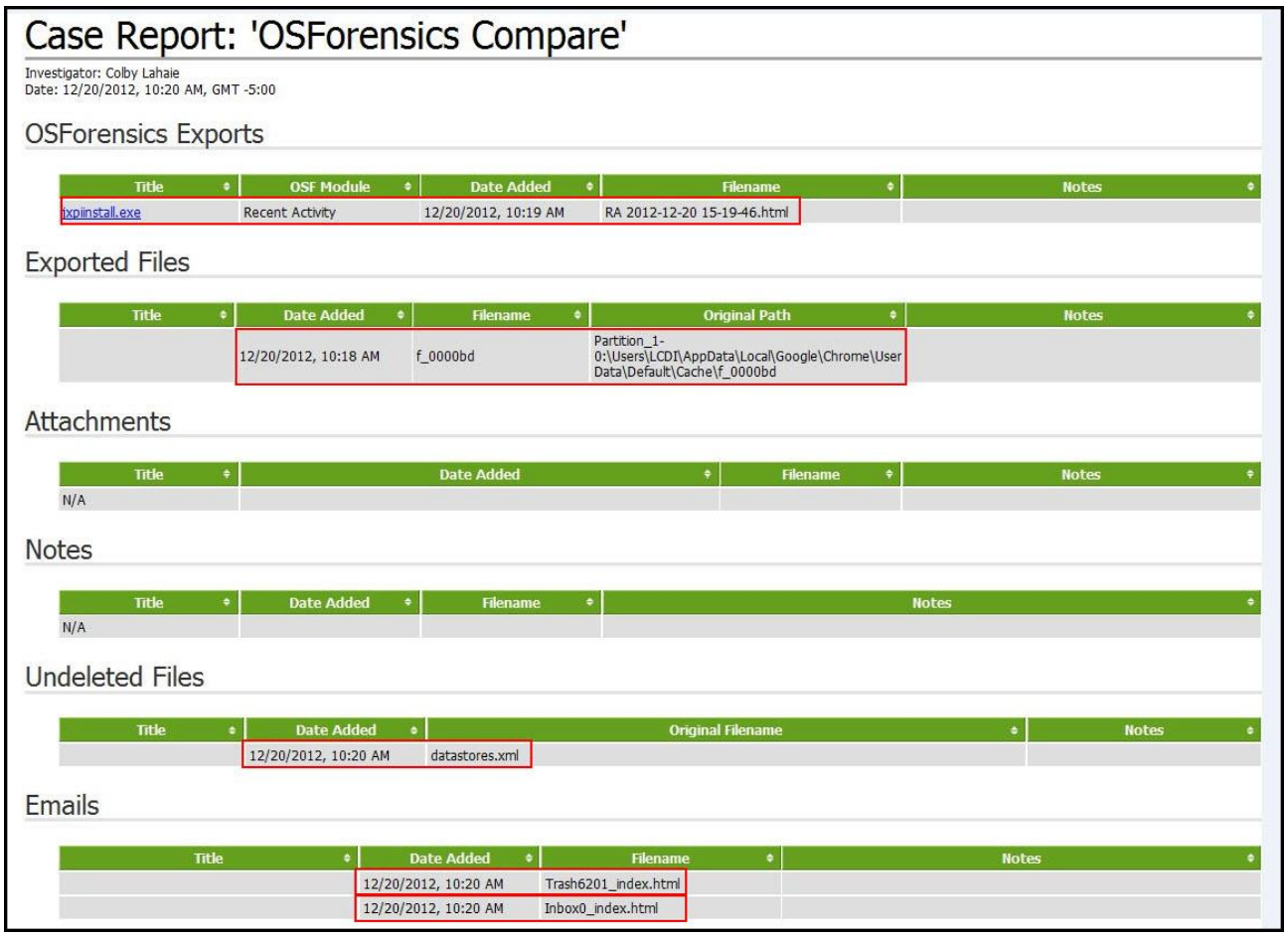


2.2.9 Report Generation

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 Report: 'OSForensics Compare'

Investigator: Colby Lahaie
Date: 12/20/2012, 10:20 AM, GMT -5:00

OSForensics Exports

Title	OSF Module	Date Added	Filename	Notes
ixpiinstall.exe	Recent Activity	12/20/2012, 10:19 AM	RA 2012-12-20 15-19-46.html	

Exported Files

Title	Date Added	Filename	Original Path	Notes
	12/20/2012, 10:18 AM	f_0000bd	Partition_1-0:\Users\LCDI\AppData\Local\Google\Chrome\User Data\Default\Cache\f_0000bd	

Attachments

Title	Date Added	Filename	Notes
N/A			

Notes

Title	Date Added	Filename	Notes
N/A			

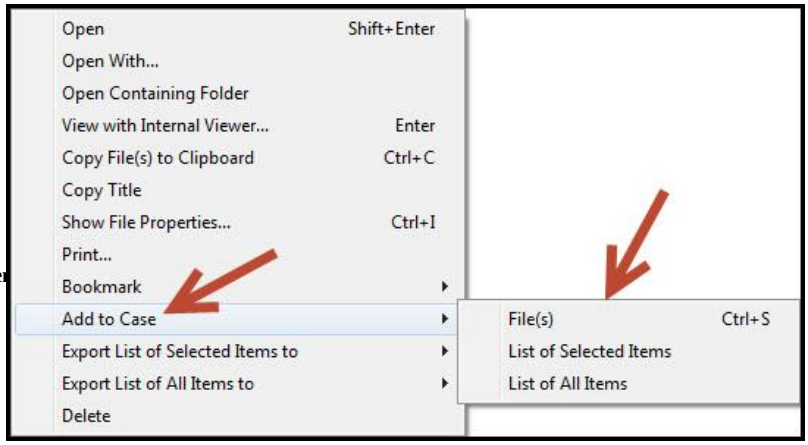
Undeleted Files

Title	Date Added	Original Filename	Notes
	12/20/2012, 10:20 AM	datastores.xml	

Emails

Title	Date Added	Filename	Notes
	12/20/2012, 10:20 AM	Trash6201_index.html	
	12/20/2012, 10:20 AM	Inbox0_index.html	

Figure 22 – Adding Evidence to Case



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*

Generation	*upon amount of evidence added to case)*	*upon amount of evidence added to case)*
Total Time	***Approximately 11 hours 10 minutes***	***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/