CHAMPLAIN COLLEGE

LCDI

The Senator Patrick Leahy Center for Digital Investigation

Internet Evidence Finder Report

Written and Researched by
Nick Murray

175 Lakeside Ave, Room 300A
Phone: 802/865-5744
Fax: 802/865-6446
http://www.lcdi.champlin.edu

July 2013

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

Introduction

Parsing internet data can be a difficult task. Internet Evidence Finder (IEF) can find and retrieve any and all supported internet related artifacts, benefitting the investigation by speeding up the process of parsing the data. It provides artifact information for: web browsers (Google Chrome, Mozilla Firefox, Internet Explorer, etc.); chat programs (AIM, Google Talk, Yahoo Messenger); email (Gmail, Hotmail, Yahoo Mail); and torrent programs (Ares, Frostwire, eMule) among others.

Manually looking for this information often proves to be a difficult and time consuming task. Many of the artifact files are filled with what may seem like unimportant data and are not easy to read. These files, though they might hold crucial data, contain a lot of seemingly random letters, symbols, and words that probably do not mean much, unless the person viewing them knows what he or she is viewing, such as a Digital Forensic Examiner. Because the data is challenging to interpret, a Digital Forensic Examiner should confirm any and all of the results from IEF with the actual artifacts located on the evidence.

Figure 2 is a picture of a Chrome cache file that IEF found. IEF also has a rebuild webpages feature that attempts to rebuild a webpage exactly as the user saw it at the time of access, allowing investigators a glimpse into the user's activity. Figure 3 is screenshot of part of a page that IEF has rebuilt. Again, a Forensic Examiner should conduct further research to verify that the information presented is accurate.

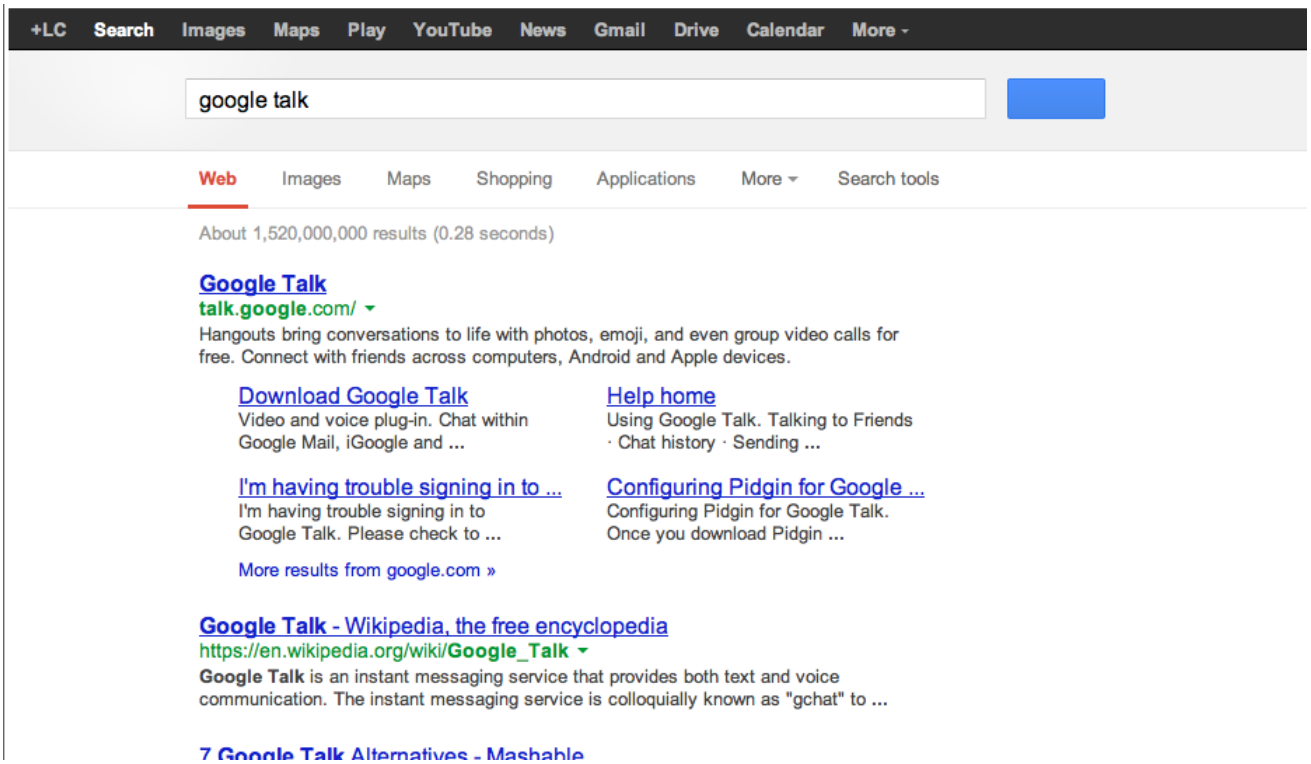
Figure 1 is a screen shot of all of the artifacts IEF 5.6 supports, along with the programs we generated data on, received results from, and did not receive results from.

Figure 1

Figure 2

e="2"==c("utmcvr");d(ic,c("utmcid"));d(jc,c("utmccn"));d(nc,c("utmcsr"));d(oc,c("utmcmd"));d(pc,c("utmctr"));d(qc
a!=b:!/^\d+$/[ia](a)};var Uc=function(){this.filters=[]};Uc[x].add=function(a,b){this.filters[n]({name:a,s:b})};Uc[x].
{"file:"==J[z][A]&&a[ta]()}function nd(a){a.get(Ib)||a.set(Ib,J.title,h);a.get(Hb)||a.set(Hb,J[z].pathname+J[z][va],h)}
("x");a.Wa=d}catch(k){H(135)}qd=a}},td=function(){sd();
for(var a=qd,b=W[za],a=b.appName+b.version+a.language+b.platform+b.userAgent+a.javaEnabled+a.Q+a.P+(J.co
[1]);else{d=d+"."+d;try{c=new ActiveXObject(d+".7"),c=c.GetVariable("$version")}catch(f){}if(!e)try{c=new Ac
{}if(!e)try{c=new ActiveXObject(d),c=c.GetVariable("$version")}catch(k){}e&&(c=e[y](" ")[1][y](","),c=e[0]+"."
b=a[0],c=b.lastIndexOf(":"),d=b.lastIndexOf(".");this.h=this.i=this.l="";-1==c&&-1==d?this.h=b:-1==c&&-1!=d?(th
(d+1,c),this.h=b[B](c+1)):(this.i=b[B](0,d),this.h=b[B](d+1));this.k=a[ja](1);this.Ma=!this.l&&"_require"==this.h;thi
"_createAsyncTracker",Y[x].Sa,33);T(Y[x],"_getAsyncTracker",Y[x].Ta,34);this.I=new Ja;this.p=[]};E=Y[x];E.Na
h};E.push=function(a){var b=Z.Va[ya](this,arguments),b=Z.p.concat(b);for(Z.p=[];0E.O=function(a){try{if(a.s)a.s[
{if(!this.Na(a.k[0],b,a.k[2])){if(!a.Pa){var c=Oa(""+a.k[1]);var d=c[A],e=J[z][A];var f;if(f="https:"==d||d==e?h:"htt
("://")||c[u]==k[u]&&c[pa]==k[pa]))for(var s="http:"==c[A]?80:443,t=M.S,b=0;bl}f=Be&&!ld()}f&&(a.Pa=Ia(c.url
M.r(a,b||"")};E.Ta=function(a){return M.u(a)};var yd=function(){function a(a,b,c,d){g==f[a]&&(f[a]={});g==f[a][b
{f[a][b]=g;var c=h,d;for(d=0;dCd[w];Yb++)Kc=Cd[ma](Yb),Lc=Ma[Kc],Jc+=g!=Lc?Lc:Kc;f+=Jc;c[n](f)}b+=k+c[
{"":"0"};Ma[s]="1";Ma[t]="2";Ma[Za]="3";var mb=1;e.Ra=function(a){return g!=f[a]};e.A=function(){for(var a
b(a,"k",c)};e.N=function(a,c){return b(a,"v",c)};e.L=function(a){c(a,"k")};e.M=function(a)
{c(a,"v")};T(e,"_setKey",e.f,89);T(e,"_setValue",e.o,90);T(e,"_getKey",e.getKey,87);T(e,"_getValue",e.N,88);T(e
{return"number"!=typeof a&&(g==Number||!(a instanceof Number))||m.round(a)!=a||da(a)||a==ba?l:h};var zd=functi
(a=Ea(),zd(h).hid=a);return a},Dd=function(a){a.set(Kb,Ad());var b=zd();if(b&&b.dh==a.get(O)){var c=b.sid;c&&(
(".",1*b[1]||H(112),a.set(Q,1*b[0]),a.set(Vb,1*b[1]))};var Ed,Fd=function(a,b,c,d){var e=a.c(bb,""),f=a.c(P,"/");d
c=a.c(P,"/"),d=a.c(Wa,"");X("__utma",cd(a),c,b,d,a.get(cb));X("__utmb",dd(a),c,b,d,a.get(db));X("__utmc",""+a.b(
X("__utmv",e,c,b,d,a.get(cb)):X("__utmv","",c,b,"",-1)},Wc=function(a){var b=a.b(O,1);if(!bd(a,$c(b,pd("__utma"

Figure 3



Prior Work:

There have been a small number of blogs published on various forensics sites that have reviewed or evaluated IEF. The first blog [1]we researched talked primarily about IEF's aesthetics and ease of use; nothing was mentioned of how accurate the program was or how the program results compared to the investigator's notes. The second blog[2] we viewed was the only one we researched to review IEF and discuss how accurate the results were. They make mention of how the reported times were accurate to their notes in their review. The third review,[3] like the first, is more of a tutorial of how to use IEF and makes no reference to the accuracy of the program. Whoever was conducting the evaluation also ran IEF on a failing drive that "experienced many read errors [sic]." We could not find any other reviews or evaluations of IEF.

Purpose and Scope:

The purpose of this project is to evaluate Internet Evidence Finder as well as determine what information is relayed to the investigator and how accurate this information is. Two supported evidence items will be used for IEF to parse: a drive that will be used to generate data and an image of that drive. The IEF results from both will be compared for inconsistencies. Secondary to this, we will be creating a tutorial outlining how local law enforcement can make use of IEF.

Research Questions:

1. Does Internet Evidence Finder accurately report user generated information from the supported applications?
2. How accurate is the information given in relation to timestamp information, content, location, URL, and users as compared to our notes?

Methodology and Methods

For this project, our team used a Window 7 computer with a premade image that is a used as a standard installation on all of our computers at the LCDI. We researched all of the artifacts that IEF supports, giving us a better understanding of which artifacts we would be able to generate data for. We made the decision to download and install all of the programs, create the necessary accounts where needed or applicable, generate the data, and document any and all of the steps we took during this process. I used two computers for this experiment. The computer used to generate data on is called the Data Computer. The second computer, called the Com Computer, was used to communicate with the Data computer when the chat programs were used. On the Com computer, we downloaded and installed all of the necessary chat programs and created accounts when needed. After the programs were installed and the accounts were created, we began sending messages back and forth between the Com Computer and Data Computer. After we finished with the chat programs, we concentrated on the Cloud programs. We downloaded the programs needed and installed them; Flickr did not have an application to download, so we generated information on their website using Opera. We then generated data for Email (Gmail, Hotmail, and Yahoo Mail). We created an account for Hotmail and used the accounts we had created for the chat programs to log into Gmail and Yahoo. We sent out emails in a circular fashion, so that

[1] Forensic Focus. (n.d.). Internet Evidence Finder (IEF). Retrieved July 14, 2013, from http://www.forensicfocus.com/c/aid=54/reviews/2013/internet-evidence-finder-ief/

[2] Krause, J. (2013, March 15). Review: Internet Evidence Finder (IEF) v6.0.Forensiccom RSS. Retrieved July 14, 2013, from http://forensiccontrol.com/resources/reviews/review-internet-evidence-finder-v6-0/

[3] O'Leary, R. J. (2012, November 7). Internet Evidence Finder Version 5.6.0. Justnet. Retrieved July 14, 2013, from https://www.justnet.org/pdf/IEF-Report-11-7-12.pdf

each account would have sent an email and received an email. We then began downloading, installing, and generating data with the peer to peer programs individually. After we generated data with the P2P programs, we generated data on the social networking sites. During the process of generating data on the social networking sites, we connected two different iPhones to the Data Computer; we backed up one phone. During the course of generating data for the chat programs, Cloud programs, Email, Mobile IOS backups, P2P programs, and Social Networking sites, we used all of the supported Web browsers to generate data. Once all of the data was generated on the Data computer, we shut down all of the programs that were still running and then shut down the computer. We then removed the hard drive, connected it to a write blocker, and took an image of the hard drive using FTK Imager. To analyze the hard drive, we plugged it into a write blocker hooked up to the Com Computer and ran IEF on the hard drive. Additionally, the image was loaded onto the Com Computer and IEF was run against it. After both the reports were generated, we compared the results; both sets of results were identical. We took the report for the image and compared it to our notes. Figure 4 is a table of our results.

Figure 4

Program	Data Generated	IEF results	
AIM	X	N/A	AIM was used but no data was generated due to a log setting in the program that was not enabled. Therefor no logs were saved locally to the computer
Google Talk	X	N/A	Google Talk was used but no data was generated due to a log setting in the program that was not enabled. Therefor no logs were saved locally to the computer
Mail.ru Chat	X	N/A	This program was not used because it was in Russian
Messenger Plus	X	N/A	This program was not used because this add-on is no longer supported.
ICQ	X	N/A	ICQ was used but no data was generated due to a log setting in the program that was not enabled. Therefor no logs were saved locally to the computer
MIRC	✓	✓	Results were mostly accurate, in one case a timestamp was off by one minute
ooVoo	✓	✓	The Results from this were accurate and reflected our notes
Second Life	X	N/A	This Program was not used because we decided not to use this program
Skype	✓	✓	Results show three categories of artifacts, one containing complete information.
Trillian	✓	✓	The results were accurate but contained a lot of repeated results
Windows Live Messenger	X	N/A	This Program was not used because it is no longer supported by Microsoft
World of Warcraft	X	N/A	This Program was not used because we decided not to use this program
Yahoo Messenger	✓	✓	The results were encrypted and the timestamps

			were off
Dropbox	✓	✓	The results that were recovered were accurate but there were a couple of pictures missing from the results
Flickr	✓	✓	This service was used but data was not generated during its use
Google Docs	✓	✓	Returned results for 2 pictures
Google Drive	✓	✓	Returned several results for one category but there was not identifying information. The other category returned accurate results and had identifying information
Sky Drive	✓	✓	Returned multiple results, some with the same information repeated. There was one file on in the results that was not generated by the user
Gmail	✓	✓	These results showed both email fragments and what IEF interpreted as whole emails. Both of these categories returned accurate results
Hotmail	✓	X	This Service was used but IEF did not return any results
Yahoo Mail	✓	X	This Service was used but IEF did not return any results
iOS backup	X	N/A	A phone was synced to the computer but the phone never saved a backup to the computer.
Torrent file artifacts	✓	✓	Returned repeated results for the same file. Timestamp information for file was incorrect
Ares search Keywords	✓	✓	Returned repeated results for the same keyword search
Emule	✓	✓	Returned results for keyword search
Gigatribe	X	N/A	This program was used but the user did not generate chat data during its use.
Limewire	X	N/A	This Program was not used because it has been discontinued and we had no way to get access to it.
FrostWire	✓		Returned results for configuration files
Shareaza	X	N/A	This program was used but the user did not generate chat data during its use.
Bebo	X	N/A	This service was used but data was not generated during its use.
Facebook	✓		Return results but the results were not user generated
Google+	X	N/A	This service was used but data was not generated during its use. IEF only finds chat related artifacts on this service only if the log chat option is selected.
LinkedIn	X	N/A	This service was used but data was not generated during its use. IEF only finds chat related artifacts on this service only if the log chat option is selected.

MySpace	X	N/A	This service was used but data was not generated during its use. IEF only finds chat related artifacts on this service only if the log chat option is selected.
Twitter	✓	✓	Returned results but had no identifying information
Chrome	✓	✓	Return thousands of results over several categories. The information looked at appears to be accurate
Firefox	✓	✓	Return thousands of results over several categories. The information looked at appears to be accurate
Internet Explorer	✓	✓	Returned results from before the project was started. No results return from the time from of this project
Opera	✓	✓	Returned accurate results but some of the same results were repeated multiple times
Safari	✓	✓	Returned accurate results but some of the same results were repeated multiple times

Reference Set:

1 Software

Program Name	Version
AIM	8.0.1.5
Google Talk	1.0.0.105
Mail.ru Chat	N/A
Messenger Plus	N/A
ICQ	Build 6017
MIRC	7.32
ooVoo	3.5.8.22
Second Life	N/A
Skype	6.3.0.107
Trillian	5.3 build 15
Windows Live Messenger	N/A
World of Warcraft	N/A
Yahoo Messenger	11.5.0.228
Dropbox	2.0.26
Flickr	N/A
Google Docs	N/A
Google Drive	1.10.4769.0632
Sky Drive	17.0.2011.0627
Gmail	N/A
Hotmail	N/A
Yahoo Mail	N/A

iOS backup	N/A
Torrent file artifacts	N/A
Ares search Keywords	2.2.4
Emule	0.50a
Gigatribe	3.04.009
Limewire	N/A
FrostWire	5.5.6.0
Shareaza	N/A
Bebo	N/A
Facebook	N/A
Google+	N/A
LinkedIn	N/A
MySpace	N/A
Twitter	N/A
Chrome	65.96.32832
Firefox	21.0
Internet Explorer	10.0.9200.16618
Opera	12.15.1748
Safari	5.34.57.2

2 Equipment

Data Computer	
Memory	*4GB*
Processors	*Intel Core2 Quad Q9450 @ 2.66Ghz*
HDD	*1TB, Western Digital SATA*
OS	*Windows 7*
Com Computer	
Memory	*16GB*
Processors	*Intel Core i7-3770K CPU 3.50GHz*
HDD	*500GB, Western Digital SATA*
OS	*Windows 7*

2.1 Write Blocker

Wiebetech Forensic Ultradockv4

2.2 FTK Imager

Version 3.1.1.8

Results

During the process of generating data on the Data Computer, we took careful notes of what actions we performed and when so we could compare them to the results we retrieved from IEF. IEF claims to support a variety of internet-based programs, but each one should be tested with IEF to see how accurate the information given is. Figure 1 shows all of the programs supported by IEF 5.6.8.

Figure 5 is an artifact report from IEF that shows the number of results IEF was able to recover. Both the Image and the Drive showed identical results to

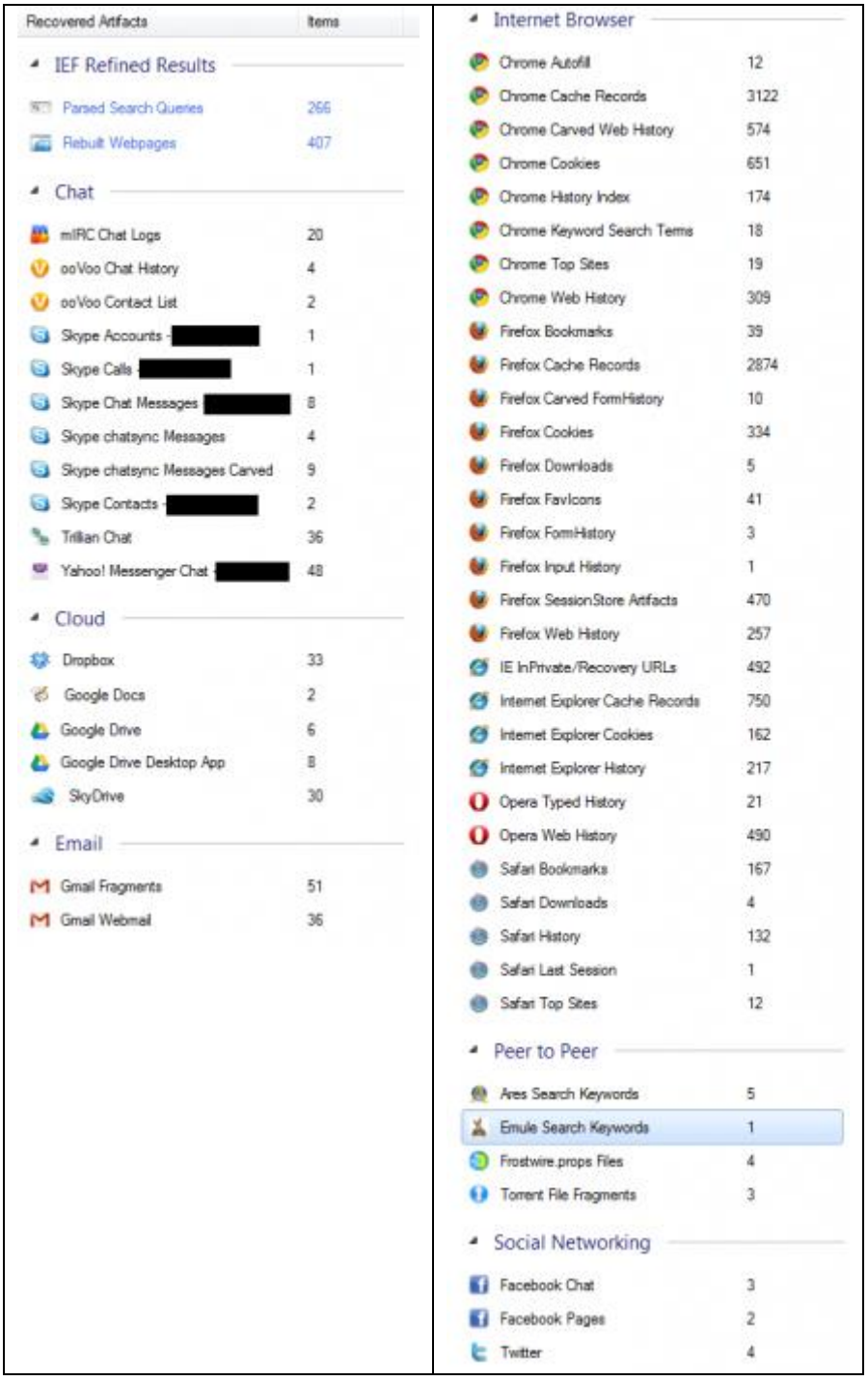
Figure 5, the IEF results from the drive. Beyond this, we will discuss each artifact, if applicable, and how the report compares to our notes.

Note: IEF reports time stamps in UTC while we recorded our notes using EST. The time conversion from UTC to EST is a difference of four hours. We will not be explaining the time conversions for each artifact. The times will, and should be, a difference of about four hours: i.e. if we say that IEF reported that we googled "something" at 1300 and our notes say we googled "something" at 0900, then this is correct.

IEF Report

Of the 24 programs that were used to generate data, IEF returned results for 22 of them (see Figure 1).

Figure 5



Recovered Artifacts	Items
IEF Refined Results	
Parsed Search Queries	266
Rebuilt Webpages	407
Chat	
mIRC Chat Logs	20
ooVoo Chat History	4
ooVoo Contact List	2
Skype Accounts - [redacted]	1
Skype Calls - [redacted]	1
Skype Chat Messages - [redacted]	8
Skype chatsync Messages	4
Skype chatsync Messages Carved	9
Skype Contacts - [redacted]	2
Trillian Chat	36
Yahoo! Messenger Chat - [redacted]	48
Cloud	
Dropbox	33
Google Docs	2
Google Drive	6
Google Drive Desktop App	8
SkyDrive	30
Email	
Gmail Fragments	51
Gmail Webmail	36

Internet Browser	
Chrome Autofill	12
Chrome Cache Records	3122
Chrome Carved Web History	574
Chrome Cookies	651
Chrome History Index	174
Chrome Keyword Search Terms	18
Chrome Top Sites	19
Chrome Web History	309
Firefox Bookmarks	39
Firefox Cache Records	2874
Firefox Carved FormHistory	10
Firefox Cookies	334
Firefox Downloads	5
Firefox FavIcons	41
Firefox FormHistory	3
Firefox Input History	1
Firefox SessionStore Artifacts	470
Firefox Web History	257
IE InPrivate/Recovery URLs	492
Internet Explorer Cache Records	750
Internet Explorer Cookies	162
Internet Explorer History	217
Opera Typed History	21
Opera Web History	490
Safari Bookmarks	167
Safari Downloads	4
Safari History	132
Safari Last Session	1
Safari Top Sites	12
Peer to Peer	
Ares Search Keywords	5
Emule Search Keywords	1
Frostwire.props Files	4
Torrent File Fragments	3
Social Networking	
Facebook Chat	3
Facebook Pages	2
Twitter	4

Chat

Chat programs are used to easily and quickly communicate. Chat artifacts can be generated from a number of different locations, such as from a downloaded chat program or a website. We used several programs supported by IEF to attempt to generate data.

AIM

We used AIM to generated data, including adding a contact, sending messages, receiving messages, and sending files, but IEF did not report any information. AIM was not set up to log chat information.

Google Talk

We used Google Talk to generated data, including adding a contact, making a call, sending and receiving messages, and sending and receiving files. IEF did not report any information. Like AIM, Google talk was not set up to log any chat information.

ICQ

We used ICQ to generated data, including sending and receiving messages and adding a contact. ICQ was not set up to log any chat information either and did not report any information.

MIRC

We used MIRC to generate data, but we were unfamiliar with the program. IEF does not display any timestamp information in the report (Figure 6), but does display the contents of the logs from MIRC containing time stamp information. The IEF report contained one abnormal result; the Mirc log (Figure 7) shown in IEF displays us joining a MIRC channel at 14:56:56 on 6/5/13 while our notes show that we joined the MIRC channel at 14:55. This log also shows that we closed the channel at 14:58:21 on the same day, which matches our notes (14:58). We are not sure why the join times were recorded differently and the close times are the same, but one theory is that it may have taken some time to join the channel.

Figure 6

	#	Fragment	Source	Located At
	19	<click to view>	G: - (Unallocated Clust...	Physical Sector 65184...
	20	<click to view>	G:\ - G:\Users\nmurra...	Physical Sector 92947...
	1	<click to view>	G:\$MFT	File offset 153548232
	5	<click to view>	G:\System Volume Inf...	File offset 225472054
	6	<click to view>	G:\System Volume Inf...	File offset 375375304
	8	<click to view>	G:\System Volume Inf...	File offset 390193152
	9	<click to view>	G:\System Volume Inf...	File offset 390196790
	10	<click to view>	G:\System Volume Inf...	File offset 986973640

Figure 7

```
Session Start: Wed Jun 05 14:56:56 2013
Session Ident: #ChamplainDFResearch
03[14:56] * Now talking in #ChamplainDFResearch
03[14:56] * *.SwiftIRC.net sets mode: +nt
01[14:57] <@jsmithyolo420> #ChamplainDFResearch
02[14:57] * /join: insufficient parameters
02[14:58] * Disconnected
Session Close: Wed Jun 05 14:58:21 2013
```

Note: MIRC displays its timestamp data in local time, in this case EST, so no time conversion is necessary when looking at MIRC results.

ooVoo

IEF reports that there are two contacts for ooVoo: "n perry" and "john smith." These results as well as the email addresses listed for each user match our notes. These chat artifacts (Figure 8) recovered from ooVoo are consistent with the messages sent and times sent in our notes. .

Figure 8

#	Message	Date/Time - UTC (yy…
1	omg	2013-06-05 19:32:26
2	lol	2013-06-05 19:37:41
3	LMFAO	2013-06-05 19:59:52
4	yolo	2013-06-05 20:02:13

Skype

IEF reported one account for Skype, "john smith," which is the account we created for the Data Computer. IEF reports two contacts for Skype, "n perry" and "Echo / Sound Test Service." The "n perry" contact is the account created on the Test Computer, and the "Echo / Sound…" account is a default contact. IEF reports that on 6/5/13 an outbound call was made to nperry at 20:12:44, and our notes confirm that this call was made at 16:12 on the same day. IEF displays a number of results for Skype chat artifacts (Figure 9.1, Figure 9.2

, Figure 9.3

), but each result is comparable to the others and contains specific information such as the timestamp and message The Skype Chat Messages (Figure 9.1) have the most accurate information; every entry matched our notes. Articles five and six in Figure 9.1 correspond with calls placed. Figure 9.1 also displays messages sent within the Skype Chat. Figure 9.2

displays the incomplete results from certain applications such as the Skype chatsync, as well as an incorrect time stamp for the third item (our notes say the messages were sent at 16:14). Skype chatsync Messages Carved (Figure 9.3

) does not show that the message "ih" was sent.

Skype Chat Messages

Figure 9.1

#	Date/Time - UTC (yy…	Author	From Display Name	Message
1	2013-06-05 20:09:56	jsmithyolo420	john smith	Hi n perry, I'd lik…
2	2013-06-05 20:10:11	nperry69	n perry	User was granted auth…
3	2013-06-05 20:11:05	jsmithyolo420	john smith	asdfghjkl;
4	2013-06-05 20:11:45	nperry69	n perry	qwerty
5	2013-06-05 20:12:44	jsmithyolo420	john smith	jsmithyolo420, nperry69
6	2013-06-05 20:13:32	jsmithyolo420	john smith	jsmithyolo420, nperry69
7	2013-06-05 20:14:03	jsmithyolo420	john smith	olleh
8	2013-06-05 20:15:34	nperry69	n perry	ih

Skype chatsync Messages

Figure 9.2

#	Date/Time - UTC (yy…	Participants	Message
1	2013-06-05 20:11:16	jsmithyolo420; nperry69	asdfghjkl;
2	2013-06-05 20:14:03	jsmithyolo420; nperry69	qwerty
3	2013-06-05 20:15:34	jsmithyolo420; nperry69	olleh
4	-Not Found-	jsmithyolo420; nperry69	ih

Skype chatsync Messages Carved

Figure 9.3

#	Date/Time - UTC (yy…	Message
1	2013-06-05 20:11:16	asdfghjkl;
2	2013-06-05 20:14:03	qwerty
3	2013-06-05 20:15:34	olleh
4	2013-06-05 20:11:16	asdfghjkl;
5	2013-06-05 20:14:03	qwerty
6	2013-06-05 20:15:34	olleh
7	2013-06-05 20:11:16	asdfghjkl;
8	2013-06-05 20:14:03	qwerty
9	2013-06-05 20:15:34	olleh

Trillian

The results from Trillian (Figure 10) matched our notes, but contained a number of repeated artifacts. This message corresponds with the same message ("big ups" sent: 16:30 6/5/13) that we sent and then recorded in our notes.

Figure 10

#	Date/Time - UTC (yy...	Type	From User	To User	Message
3	2013-06-05 20:30:03	Outgoing Private Mess...	jsmithyolo420	nperry69	big ups
7	2013-06-05 20:30:03	Outgoing Private Mess...	jsmithyolo420	nperry69	big ups
12	2013-06-05 20:30:03	Outgoing Private Mess...	jsmithyolo420	nperry69	big ups
16	2013-06-05 20:30:03	Outgoing Private Mess...	jsmithyolo420	nperry69	big ups
22	2013-06-05 20:30:03	Outgoing Private Mess...	jsmithyolo420	nperry69	big ups
28	2013-06-05 20:30:03	Outgoing Private Mess...	jsmithyolo420	nperry69	big ups
33	2013-06-05 20:30:03	Outgoing Private Mess...	jsmithyolo420	nperry69	big ups
36	2013-06-05 20:30:03	Outgoing Private Mess...	jsmithyolo420	nperry69	big ups

Yahoo Messenger

We were unable to match the results from Yahoo Messenger (Figure 11) to our notes because the messages were encrypted and the timestamp information is not accurate. The username in Figure 11 matches the username for the account that we created.

Figure 11

#	Date/Time UTC (yyy...	Sender	Recipient	Message
1	2002-12-20 23:32:36	jsmithyolo420	Unknown	|♦`♦6♦?9♦♦♦♦==♦┘it...
2	2007-04-24 01:32:40	Unknown	jsmithyolo420	♦j□♦v ♦♦l♦♦♦¶e
3	2012-08-15 19:34:25	jsmithyolo420	Unknown	♦♦og♦♦♦♦♦♦♦5/♦♦it...
4	2001-05-07 00:09:55	jsmithyolo420	Unknown	¶♦[lf]Y♦┴F♦y♦OP□♂]ith...
5	2001-01-15 16:06:44	Unknown	jsmithyolo420	d"0♦<d♦├;♦&:8♦┐
6	1998-09-26 18:18:46	jsmithyolo420	Unknown	j3l^r(xXj/5|6[lf]□mi♦iNi...
7	1998-09-26 07:13:10	jsmithyolo420	Unknown	jSl^rh1QjO5|6┬`miT'Gi...
8	2006-09-27 17:08:16	jsmithyolo420	Unknown	j"mitXMXj♦♦w6♦♦(o┘...
9	2012-01-18 12:50:14	jsmithyolo420	Unknown	jpmqt0>fk420[tab]fmi ↕...
10	2004-01-10 13:40:07	jsmithyolo420	Unknown	♦z♦p♦a♦v■.3u••♦‼Q]h...
11	2004-04-16 15:47:12	jsmithyolo420	Unknown	jsmcM♦~olo♦r♦k
12	2004-04-16 15:47:12	jsmithyolo420	Unknown	jsm‼N♦~olo♦r

Cloud

Cloud storage is a new technology that allows users to quickly and easily store any and all data onto one of the many cloud services, allowing access from almost anywhere. When cloud services are accessed, they leave behind a large number of artifacts. . We used several cloud services to generate data for IEF.

Dropbox

We used both the application and web versions of Dropbox to generate data. The Dropbox results from IEF closely match our notes as well as the original files located on Dropbox, with the exception of one image, "Boston City Flow.jpg" (Figure 12), and one wallpaper, "Ocarina-of-Time-Wallpaper-the-legend-of-zelda-ocarina-of-time-33855205-1920-1080.png" (Figure 13), which appear to be missing from the IEF report but appear on Dropbox. Figure 14 is a picture of what IEF interprets to be the directory structure of Dropbox. There is a cached reference to the files located on Dropbox, but there is no reference to the files in the Dropbox directory structure. The IEF references do not contain any content found within the files, only their names, directory structure, and location on the disk. Figure 15 is the local Dropbox folder on the Data Computer.

Figure 12

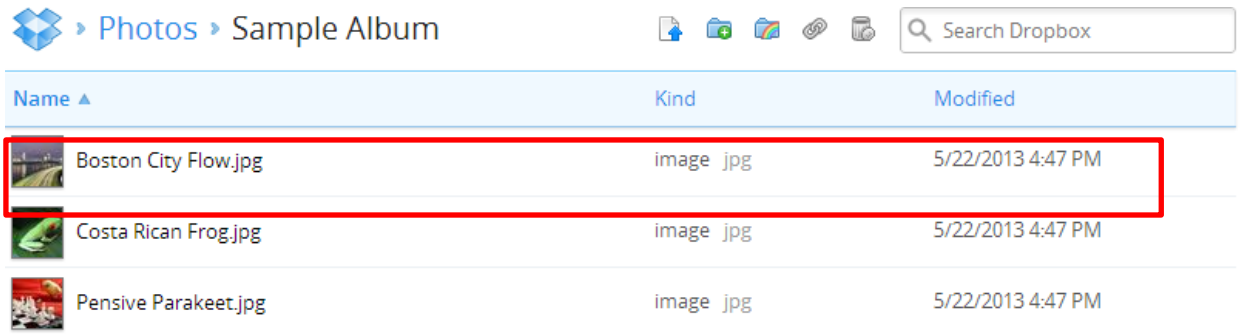


Figure 13

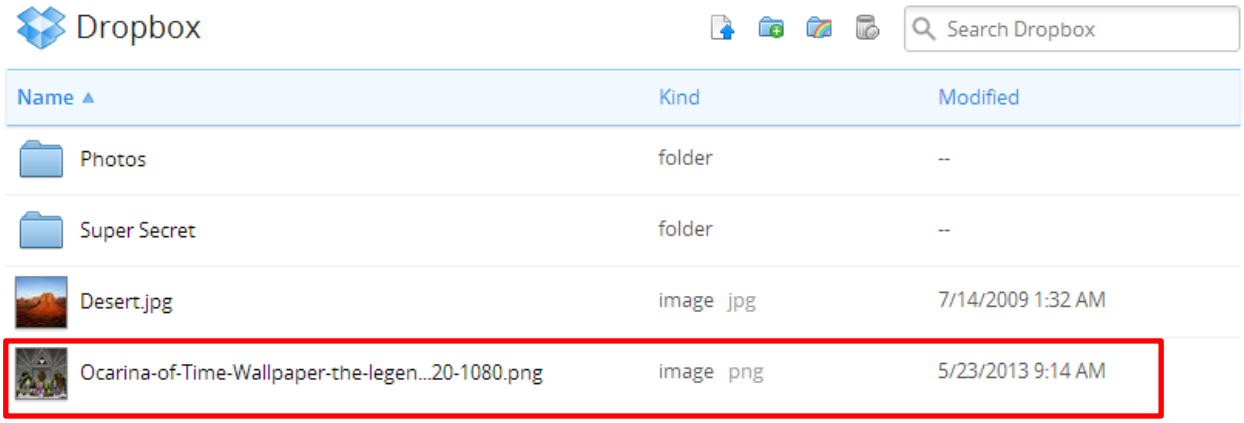
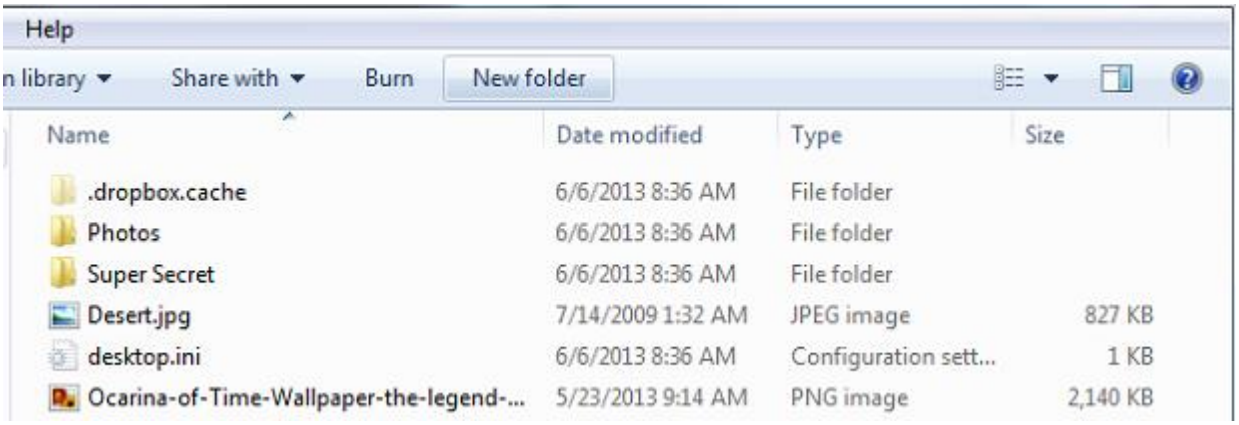


Figure 14

/desert.jpg	IEF Data.E01 - Partition 2 (999.99 GB) - H:\pagefile.sys
/photos	IEF Data.E01 - Partition 2 (999.99 GB) - H:\pagefile.sys
/photos/sample album	IEF Data.E01 - Partition 2 (999.99 GB) - H:\pagefile.sys
/photos/sample album/costa rican frog.jpg	IEF Data.E01 - Partition 2 (999.99 GB) - H:\pagefile.sys
/photos/sample album/pensive parakeet.jpg	IEF Data.E01 - Partition 2 (999.99 GB) - H:\pagefile.sys
/super secret	IEF Data.E01 - Partition 2 (999.99 GB) - H:\pagefile.sys
/super secret/foryoureyesonly.txt	IEF Data.E01 - Partition 2 (999.99 GB) - H:\pagefile.sys

Figure 15

Other pictures used during this project are located in another section of the folder structure.



Flickr

On 6/6/13 at 08:43, we went to Flickr on the Opera browser and created an account. At 08:56. our notes say that four pictures were uploaded to Flickr. However, there was an issue uploading the pictures to Flickr, which may explain why IEF did not return any results for Flickr.

Google Docs

Google Docs now exists within Google Drive (refer to Figure 17 and Figure 18 for the Google Docs content). The Google Docs results from IEF match our notes for the picture of "Ocarina-of-Time-Wallpaper-the-legend-of-zelda-ocarin a-of-time-33855205-1920-1080.png." However, there seems to be missing data (see Figure 19 for a complete list of Google Drive/Docs files), and this is likely because of the way Google Docs exists within Google Drive. The results from the Google Drive Desktop App (Figure 19) show all of the files located on Google Drive. The IEF report (Figure 16) contains file information for the pictures that were uploaded.

Figure 16

#	fileName	Owner Email	Owner Name	Last Edited	Last Modified By Loc...	File Size
1	Penguins.jpg	lcdiforensictest@gmail...	Lcdiforensictest	2009-07-14 05:32:31	2009-07-14 05:32:31	759 KB
2	Ocarina-of-Time-Wallp...	lcdiforensictest@gmail...	Lcdiforensictest	2013-06-06 19:19:36	2013-06-06 19:19:29	2 MB

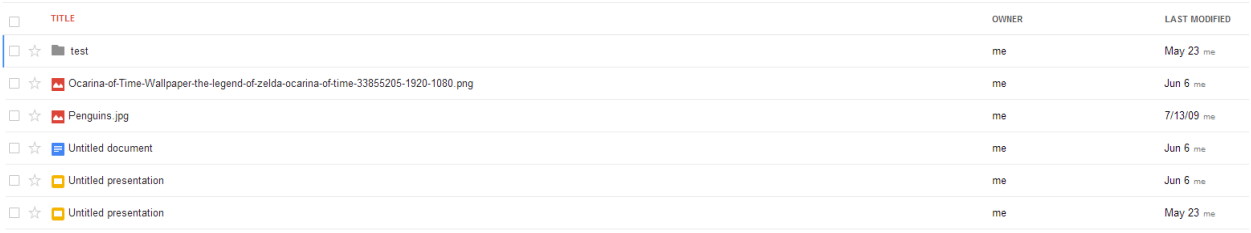
Google Drive

The Google drive results do not contain a large amount of identifying data to tie to our notes, but the one document that is related to our notes appears to have accurate time stamp info. The IEF references do not contain any content from the files found or the files' names. Figure 17 is from the IEF report; there is only one file with timestamp information. This time matches the time a Google Presentation was created in our notes. Figure 18 displays the contents of Google Drive as accessed through Chrome.

Figure 17

File Name	Author Name	Author Email	File Size	Last Modified (yyyy-...	Last Modified Name	Last Modified Email
	lcdiforensictest	lcdiforensictest@gmail...				
	lcdiforensictest	lcdiforensictest@gmail...	3746083KB			
	lcdiforensictest	lcdiforensictest@gmail...	777835KB		lcdiforensictest	lcdiforensictest@gmail...
	lcdiforensictest	lcdiforensictest@gmail...	2190413KB			
	lcdiforensictest	lcdiforensictest@gmail...	0KB	2013-06-06 19:14:27	lcdiforensictest	lcdiforensictest@gmail...

Figure 18



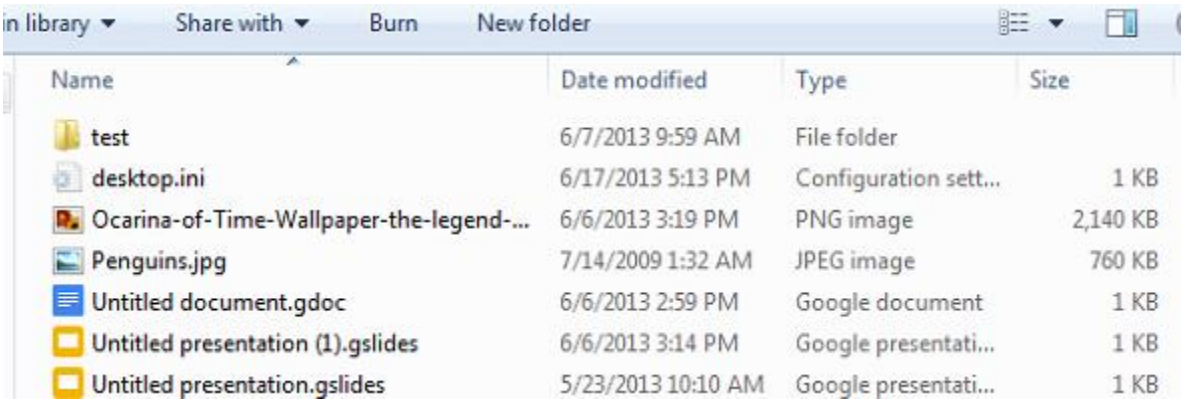
Google Drive Desktop App

The Desktop App results from IEF match our notes, including all files uploaded and created as well as timestamp information. The IEF references do not display any content from within the files. The Created Date for June 6th in Figure 19 is accurate to the notes we took. The other documents seen were from a previous project. Figure 20 is the local Google Drive folder on the Data Computer.

Figure 19

#	File Name	Modified Date (Cloud...	Modified Date (Local...	Created Date (yyyy-...
1	root			
2	Untitled presentation	2013-05-23 14:09:59	2013-05-23 14:09:59	2013-05-23 14:09:42
3	Untitled document	2013-06-06 18:59:24	2013-06-06 18:59:24	2013-06-06 18:59:20
4	test	2013-05-23 14:12:53	2013-05-23 14:12:53	2013-05-23 14:06:16
5	Untitled presentation	2013-06-06 19:14:27	2013-06-06 19:14:27	2013-06-06 19:14:00
6	Untitled document	2013-05-23 14:07:38	2013-05-23 14:07:38	2013-05-23 14:07:17
7	Ocarina-of-Time-Wallp...	2013-06-06 19:19:36	2013-06-06 19:19:36	2013-06-06 19:19:36
8	Penguins.jpg	2009-07-14 05:32:31	2009-07-14 05:32:31	2013-05-23 14:18:17

Figure 20

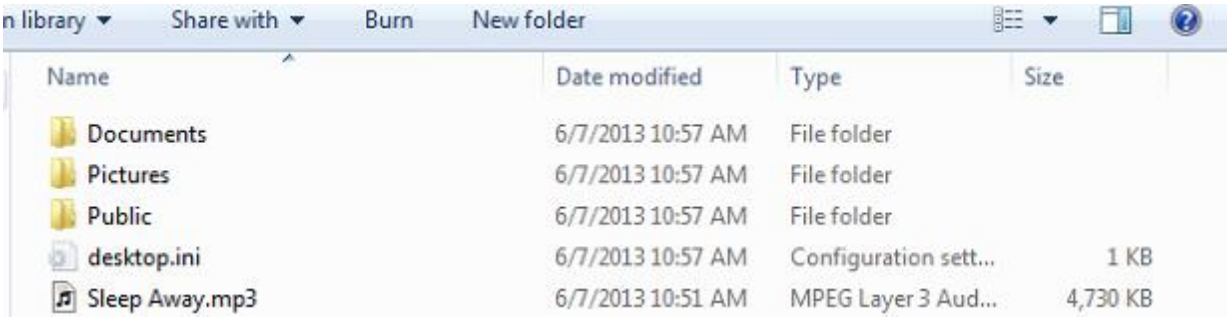


Skydrive

The Skydrive results from IEF match our notes for a portion of the data, but are not completely accurate. The directory structure appears in IEF, but it is shown multiple times. The file we uploaded appears five separate times while the time stamp is off by approximately four years and two months. Our notes show that we uploaded the file at 10:50 on 6/7/13. The information that IEF gives is the timestamp information of the file itself, not when the file was uploaded. Additionally, there appears to be an extra file recovered that we did not upload, as noted in Figure 21. Figure 22 is the local SkyDrive folder on the Data Computer

Figure 21

Figure 22



Email

Tens of billions of emails are sent everyday through various email services. Faster and easier than its physical counterpart, email traffic is steadily increasing. A large number of artifacts are left behind when an email service is used, so we used a handful of IEF's supported email services to generate data.

Gmail Fragments

The Gmail Fragment results from IEF that we received were a disorganized grouping of sections of emails. Figure 23 and Figure 24 show the IEF reports of some of the email fragments we looked at; some contain time stamp information (Figure 23) while others do not (Figure 24). We see some references to emails from our notes, but another portion seem to be missing. Figure 25 and Figure 26 are screenshots of the emails from the Gmail Account we created.

Figure 23

3ays, and 6 others\u003c/b\u003e","idcl, Here\u0026#39;s what\u0026#39;s trending on Twitter this week. Molly Smith @WCAX_Molly I love a little in",0,"","","\u003cb\u003eJun 6\u003c/b\u003e","Thu, Jun 6, 2013 at 9:36 AM",1370617788544000,,[]
,,0,[]
,,[]
,,,[0]
,,"n-ypqvsberafvpgrfg\u003dtznvy.pbz-705e8@postmaster.twitter.com",,,,0]
,["13f197bff1efabdd","13f197bff1efabdd","13f197bff1efabdd",0,0,["^all","^i","^smartlabel_notification"]
,["^all","^cob-processed-gmr","^i","^os_notification","^smartlabel_notification","^sq_ig_i_personal"]
,"\u003cspan class\u003d"zF" email\u003d"no-reply@dropbox.com" name\u003d"Dropbox"\u003eDropbox\u003c/span\u003e","\u003cb\u003e\u0026raquo;\u003c/b\u003e\u0026nbsp;","\u003cb\u003eYou've linked a new computer to Dropbox\u003c/b\u003e","Hi John, We see that you\u0026#39;ve linked a new computer, \u0026#39;research-8\u0026#39;, to your Dropbox. Awesome",0,"","","\u003cb\u003eJun 6\u003c/b\u003e","Thu, Jun 6, 2013 at 8:35 AM",1370617788544000,,[]
,,0,[]
,,[]
,,,[0]
,,"no-reply@d

Figure 24

ŽW,œg+7@kâ€™Lvar GM_TIMING_START_CHUNK2 = new Date().getTime();var VIEW_DATA=[["v","EB_KrGP_Jv0.en.","8","dd1cc0830f5f7b2d"]
,["ti","Inbox",25,0,0,"in:inbox",[]
,"2b",-1,0,25,0,[]
,[]
]
,["tb",0,[["13f1063e46c16e74","13f1063e46c16e74","13f1063e46c16e74",0,0,["^all","^i","^iim","^io_im","^io_imc3","^smartlabel_notification","^us"]
,["^all","^cob-processed-gmr","^i","^ia","^iim","^io_im","^io_imc3","^os_notification","^smartlabel_notification","^sq_ig_i_personal","^us"]
,"\u003cspan class\u003d"zF" email\u003d"noreply@ceruleanstudios.com" name\u003d"Trillian"\u003eTrillian\u003c/span\u003e","\u003cb\u003e\u0026raquo
\u0026quot;jsmithyolo420\u0026quot; requires e-mail confirmation\u003c/b\u003e","Thanks for choosing Trillian! Your Trillian Account is currently unconfirm
4,

Figure 25

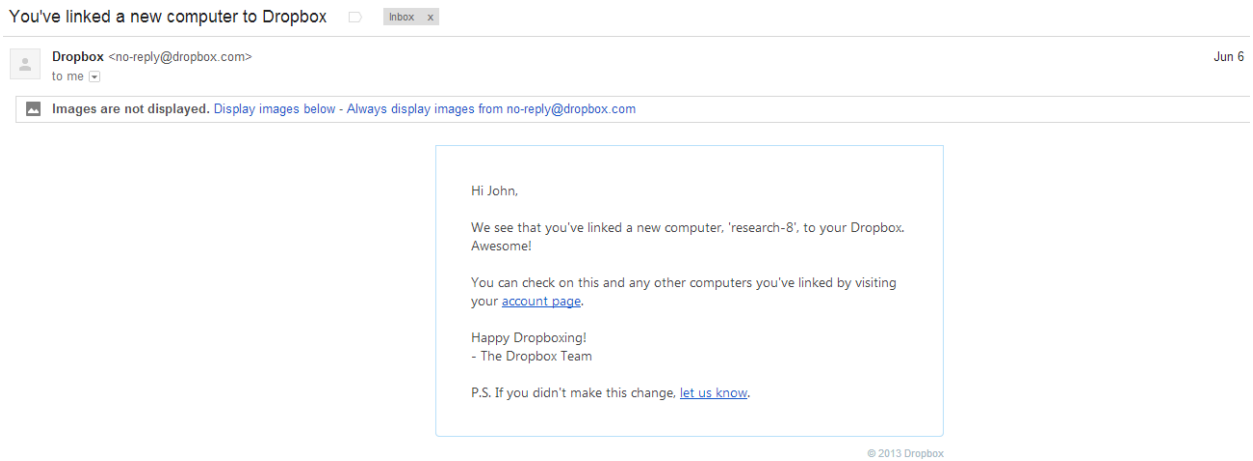
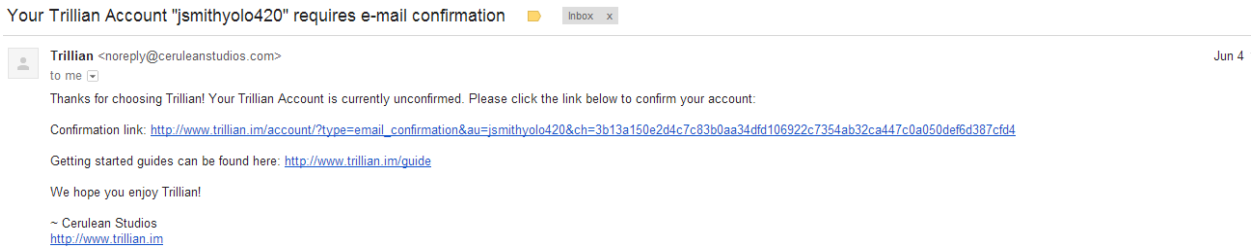


Figure 26



Gmail Webmail

The Webmail results (Figure 27, Figure 28) from IEF were much easier to read and analyze than the fragments from our Gmail account (Figure 23, Figure 24), and IEF put the data in a user-friendly report format for each artifact. See Figure 25 and Figure 26 for screenshots of the actual emails.

Figure 27

Email(s)	Dropbox <no-reply@dropbox.com\" name=\"Dropbox>
Status	Unread
Subject	You've linked a new computer to Dropbox
Snippet	Hi John, We see that you\u0026#39;ve linked a new computer, \u0026#39;research-8\u0026#39;, to your Dropbox. Awesome
Attachments	None
Date/Time (Local)	Thu, Jun 6, 2013 at 8:35 AM
Date/Time (Epoch microseconds)	1370617788544000
Source	IEF Data.E01 - Partition 2 (999.99 GB) - H:\pagefile.sys
Located At	File offset 722918015

Figure 28

Email(s)	Trillian <noreply@ceruleanstudios.com\" name=\"Trillian>
Status	Read
Subject	Your Trillian Account "jsmithyolo420" requires e-mail confirmation
Snippet	Thanks for choosing Trillian! Your Trillian Account is currently unconfirmed. Please click the link
Attachments	None
Date/Time (Local)	Tue, Jun 4, 2013 at 2:12 PM
Date/Time (Epoch microseconds)	1370370014343000
Source	IEF Data.E01 - Partition 2 (999.99 GB) - H:\pagefile.sys
Located At	File offset 756477542

Hotmail Webmail

IEF did not return any results from Hotmail despite data being generated for it. On 6/11/13 at 9:31, we composed an email with the subject “the rain” and the message “in spain,” and then sent the message at 9:36. It was not located by IEF.

Yahoo Webmail

IEF did not return any results from Yahoo Webmail despite the fact that data was generated on our test computer. On 6/11/13 at 9:11, we composed an email with the subject "hello" and the message "hellllooooo," and then sent the message at 9:19. IEF did not locate this Email.

Mobile Backups

Cell phones are another commonly used commodity, most notably the iPhone. There are tens of millions of iPhone users around the world. When an iPhone is synced to a computer, it often creates a backup of the phone on the local computer. IEF can then parse this backup and recover a great deal of information.

iOS backup

IEF did not return any results from the iOS backups. On 6/11/13 at 15:01, we plugged in our iPhone 4, and at 15:42 we unplugged it. At 15:43, we plugged in an iPhone 3GS. On 6/12/13 at 10:30, we installed iTunes. At 10:36, we synced the iPhone 3GS to iTunes, and then unplugged the phone at 11:02. There is no backup located on the Data Computer, suggesting that no data was generated, however.

Web History

There was additional web history for Google Chrome, Firefox, and Internet Explorer that was not generated by the user during this project, such as cache records, web history, cookies, keyword search terms, form history, favorites, downloads, etc. This data was likely retained from the Image that was used to set up the Data computer, as referenced previously.

Google Chrome

We used Chrome throughout the project for downloading files, visiting webpages, and other internet-based tasks. At the beginning of the project, we used Chrome to download AIM; IEF reported the search for the phrase "aim" on Google (Figure 29) at 20:21:36 on 6/3/13. This matches our notes for when we searched for "aim" (16:21 6/3/13). Later we used Google to sign into Gmail (Figure 30), which IEF reported to be at 20:50:35 on 6/3/13, matching our notes (16:50 6/3/13). On 6/11/13 at 12:19, according to our notes, we googled "teamviewer" (Figure 31); IEF reported this activity at 16:19:38 on the same day.

The autofill section reports all of the saved autofill information. On 6/11/13 at 13:41, our notes say that Chrome saved the profile information for Bebo on Chrome; IEF reports (Figure 32) that we saved the information at 17:42:07 on the same day. The difference of about a minute could be due to the gap in-between clicking the button and recording the time by our team; most likely this result is only off by seconds but we have no way to confirm this.

Figure 29

Page URL	https://www.google.com/search?q=aim&oq=aim&aqs=chrome.0.57j0l2j5.8155j0&sourceid=chrome&ie=UTF-8
Title	aim - Google Search
Visited On - UTC (yyyy-mm-dd)	2013-06-03 20:21:36
Body	(not found)
Source	IEF Data.E01 - Partition 2 (999.99 GB) - H:\Users\nmurray\AppData\local\Google\Chrome\User Data\Default\History Index 2013-06
Located At	Table: pages_content(docid: 8), Table: INFO(rowid: 8)

Figure 30

Page URL	https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&scc=1<mpl=default<mplcache=2
Title	Gmail: Email from Google
Visited On - UTC (yyyy-mm-dd)	2013-06-03 20:50:35
Body	(not found)
Source	IEF Data.E01 - Partition 2 (999.99 GB) - H:\Users\nmurray\AppData\local\Google\Chrome\User Data\Default\History Index 2013-06
Located At	Table: pages_content(docid: 10), Table: INFO(rowid: 10)

Figure 31

Page URL	https://www.google.com/search?q=teamviewer&oq=teamviewer&aqs=chrome.0.57j5j0l2.3393j0&sourceid=chrome&ie=UTF-8
Title	teamviewer - Google Search
Visited On - UTC (yyyy-mm-dd)	2013-06-11 16:19:38
Body	(not found)
Source	IEF Data.E01 - Partition 2 (999.99 GB) - H:\Users\nmurray\AppData\local\Google\Chrome\User Data\Default\History Index 2013-06
Located At	Table: pages_content(docid: 47), Table: INFO(rowid: 47)

Figure 32

7	Email	lcdiforensictest	1	2013-06-03 20:51:10	IEF Data.E01 - Partitio...	Table: autofill(pair_id: ...
8	loginId	lcdiforensictest@gmail...	1	2013-06-03 20:52:44	IEF Data.E01 - Partitio...	Table: autofill(pair_id: ...
9	email	lcdiforensictest@gmail...	1	2013-06-11 17:32:50	IEF Data.E01 - Partitio...	Table: autofill(pair_id: ...
10	DisplayName	Id Cl	1	2013-06-11 17:42:07	IEF Data.E01 - Partitio...	Table: autofill(pair_id: ...
11	session_key	lcdiforensictest@gmail...	1	2013-06-11 18:48:23	IEF Data.E01 - Partitio...	Table: autofill(pair_id: ...
12	session[username_or_...	lcdiforensictest@gmail...	1	2013-06-11 19:24:53	IEF Data.E01 - Partitio...	Table: autofill(pair_id: ...

Firefox

Mozilla Firefox was used by the team to download chat programs. IEF reports that on 6/4/13 at 16:43:31, we visited http://www.mozilla.com/en-US/firefox/21.0/firstrun/ (Figure 33), which matches our notes for when we first ran Firefox at 12:43 on the same day. Our notes say that on 6/4/13 at 13:59, we googled "Trillian" and IEF reports the search at 17:59:38 on the same day (Figure 34). Additionally, our notes list that we downloaded MIRC at 13:17 on 6/4/13, which corresponds with our IEF reports (Figure 35).

Figure 33

Date Visited - UTC (yyyy-mm-dd)	2013-06-04 16:43:31
URL	http://www.mozilla.org/en-US/firefox/21.0/firstrun/
Title	Welcome to Firefox
Visit Count	1
Visit Type	TRANSITION_REDIRECT_PERMANENT
Is Typed	no
Last Visited - UTC (yyyy-mm-dd)	2013-06-04 16:43:31
ID	10
Source	IEF Data.E01 - Partition 2 (999.99 GB) - H:\Users\nmurray\AppData\roaming\Mozilla\Firefox\Profiles\8v7buhwt.default\places.sqlite
Located At	Table: moz_places(id: 10), Table: moz_historyvisits(id: 2)

Figure 34

Date Visited - UTC (yyyy-mm-dd)	2013-06-04 17:59:38
URL	https://www.google.com/search?q=trilliam&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a&channel=fflb#gs_rn=15&gs_ri=psy-ab&sugge US%3Aofficial&channel=fflb&sclient=psy-ab&oq=trillia&gs_l=&pbx=1&bav=on.2,or.r_qf.&bvm=bv.47244034,d.dmg&fp=c9d97f49e507a36a&biw=1280&bih=887
Title	trillian - Google Search
Visit Count	1
Visit Type	TRANSITION_LINK
Is Typed	no
Last Visited - UTC (yyyy-mm-dd)	2013-06-04 17:59:38
ID	38
Source	IEF Data.E01 - Partition 2 (999.99 GB) - H:\Users\nmurray\AppData\roaming\Mozilla\Firefox\Profiles\8v7buhwt.default\places.sqlite
Located At	Table: moz_places(id: 38), Table: moz_historyvisits(id: 30)

Figure 35

Date Visited - UTC (yyyy-mm-dd)	2013-06-04 17:17:30
URL	http://software-files-a.cnet.com/s/software/13/11/93/05/mirc732.exe?lop=link&ptype=3001&ontid=2150&siteId=4&edId=3&spi=a1667336a92aa08af53f284c81ce1547&pid=13119305&psid=10001733&token=1370402245_19cb867773efa58bfe8b9b281a4a3016&fileName=mirc732.exe
Title	mirc732.exe
Visit Count	0
Visit Type	TRANSITION_DOWNLOAD
Is Typed	no
Last Visited - UTC (yyyy-mm-dd)	2013-06-04 17:17:30
ID	20
Source	IEF Data.E01 - Partition 2 (999.99 GB) - H:\Users\nmurray\AppData\roaming\Mozilla\Firefox\Profiles\8v7buhwt.default\places.sqlite
Located At	Table: moz_places(id: 20), Table: moz_historyvisits(id: 12)

Internet Explorer

We used Internet Explorer for multiple tasks throughout the project such as logging into Gmail, signing up for Skype, downloading opera, and other internet-based actions. Unfortunately, our results that IEF reported did not match our notes. The results showed a range of activity starting on 5/1/13 at 14:27:01 and ending on 5/8/13 at 17:02:16, and one entry on 7/31/8936 at 15:51:21; however, we began this project on June 3rd 2013. On 6/5/13 at 13:57, our notes show that Internet Explorer was used to download a program called Team Viewer, and on 6/6/13, our notes say Internet Explorer was used to Download Opera. We cannot say for certain why there are no results for the data we generated.

Opera

We first ran Opera on 6/6/13 at 8:25, according to our notes. IEF reports that we opened first opened Opera at 12:25:48 on the same day. Figure 36 shows a portion of the results from the IEF report. IEF is displaying multiple results for the same data, which is not accurate; the time stamp information confirms that this page was only visited once. It is important to note that multiple results may not necessarily mean a website was visited multiple times. Results should always be manually verified.

Figure 36

#	Visited - UTC (yyyy-m...	URL	Title	Source	Located At
9	2013-06-06 12:25:48	http://redir.opera.com/www.opera.com/firstrun/	http://redir.opera.com...	G:\Users\nmurray\Ap...	File offset 46
71	2013-06-06 12:25:48	http://redir.opera.com/www.opera.com/firstrun/	(http://redir.opera.com...	G:\System Volume Inf...	File offset 397369390
1...	2013-06-06 12:25:48	http://redir.opera.com/www.opera.com/firstrun/	yhttp://redir.opera.co...	G:\System Volume Inf...	File offset 408203310
2...	2013-06-06 12:25:48	http://redir.opera.com/www.opera.com/firstrun/	http://redir.opera.com...	G:\System Volume Inf...	File offset 1001754670
2...	2013-06-06 12:25:48	http://redir.opera.com/www.opera.com/firstrun/	http://redir.opera.com...	G:\System Volume Inf...	File offset 64180270
3...	2013-06-06 12:25:48	http://redir.opera.com/www.opera.com/firstrun/	http://redir.opera.com...	G:\System Volume Inf...	File offset 76779566
3...	2013-06-06 12:25:48	http://redir.opera.com/www.opera.com/firstrun/	http://redir.opera.com...	G:\System Volume Inf...	File offset 1292132398

Safari

IEF reports on 6/7/13 at 15:03:46, we opened Safari for the first time, matching the information found in our notes (11:03 6/7/13). The IEF results for Safari (Figure 37) also have repeat entries. Figure 37 shows that the same page was visited six times within the same second. Again, it is important to understand that multiple results may not necessarily mean a website was visited multiple times.

Figure 37

#	URL	Title	Last Visit Date	Visit Count	Source	Located At
31	http://www.apple.com/safari/welcome/	Apple	2013-06-07 15:03:45	1	G:\Users\nmurray\Ap...	n/a
35	http://www.apple.com/safari/welcome/	Apple	2013-06-07 15:03:45	1	G:\System Volume Inf...	n/a
39	http://www.apple.com/safari/welcome/	Apple	2013-06-07 15:03:45	1	G:\System Volume Inf...	n/a
70	http://www.apple.com/safari/welcome/	Apple	2013-06-07 15:03:45	1	G:\System Volume Inf...	n/a
1...	http://www.apple.com/safari/welcome/	Apple	2013-06-07 15:03:45	1	G:\System Volume Inf...	n/a
1...	http://www.apple.com/safari/welcome/	Apple	2013-06-07 15:03:45	1	G:\System Volume Inf...	n/a

Peer to Peer

Peer to Peer programs are a quick and easy way to share and receive files. Using torrents users can rapidly download anything from movies, programs, music, pictures, etc. much of this traffic is illegal. Many artifacts are created when using these programs. We used several Peer to Peer programs to generated data for IEF.

Torrent File Fragments

On 6/11/13 at 15:40, we used Chrome to search for "Ubuntu torrent" and downloaded "ubuntu-13.04-desktop-amd64.iso" at 15:41. The torrent file results from IEF partially match our notes. The name of the file is correct, but the file timestamp information is not accurate. Our notes show that we downloaded the torrent file on 6/11/13 at 15:41. The MAC timestamp information for the actual file does not match this time either. Figure 38 shows the timestamp information and the file name. Additionally, IEF shows three results but there was only one file that was downloaded.

Figure 38

#	Name	Created On - UTC (y...	Files Included in Torr...	Source	Located At
1	ubuntu-13.04-desktop-...	2013-04-25 08:35:28	-Not Found-	G:\System Volume Inf...	File offset 848465921
2	ubuntu-13.04-desktop-...	2013-04-25 08:35:28	-Not Found-	G:\System Volume Inf...	File offset 466079745
3	ubuntu-13.04-desktop-...	2013-04-25 08:35:28	-Not Found-	G:\System Volume Inf...	File offset 1303257089

Ares search keywords

On 6/11/13, we downloaded the Peer to Peer program Ares. After we installed the program, we conducted searches for "xubuntu." The Ares keyword results from IEF match our notes, but IEF displays multiple results (Figure 39) for the same keyword. The keyword "xubuntu" is shown five times despite us searching for it only once. There is no time stamp information to compare to our notes, but our notes say that we searched for "xubuntu" once on 6/11/13 at 10:21

Figure 39

xubuntu	IEF Data.E01 - Partition 2 (999.99 GB) - H:\Users\nmurr...	File offset 633472
xubuntu	IEF Data.E01 - Partition 2 (999.99 GB) - H:\System Volu...	File offset 773020288
xubuntu	IEF Data.E01 - Partition 2 (999.99 GB) - H:\System Volu...	File offset 167025280
xubuntu	IEF Data.E01 - Partition 2 (999.99 GB) - H:\System Volu...	File offset 192338560
xubuntu	IEF Data.E01 - Partition 2 (999.99 GB) - H:\System Volu...	File offset 248306304

eMule Search Keywords

On 6/11/13, we downloaded the Peer to Peer program eMule. After we installed the program, we conducted searches for "xubuntu." The Emule keyword results from IEF match our notes. Despite not getting eMule to properly connect to the server(s), the program recorded the search keyword. On 6/11/13 at 10:53, we attempted to search for "xubuntu", and IEF reported that the search was conducted, leaving out the timestamp information (Figure 40).

Figure 40

	#	Search Keyword	Source	Located At
	1	xubuntu	G:\Users\nmurray\Ap...	File Offset 2

Limewire/Frostwire

Limewire has been discontinued, and as a result, was not used for this project. On 6/11/13, we downloaded the Peer to Peer program Ares. After we installed the program, we conducted searches for "xubuntu." The Frostwire results from IEF are for .prop files that contain configuration data for the program. Figure 41 is the contents of a .prop file reported by IEF. The timestamp information reported in this file correlates to when we turned the computer off and when it was turned back on; 0n 6/11/13 at 12:12, we restarted the computer and we reported it coming back on at 12:18. IEF did not retrieve any keyword searches from Frostwire.

Figure 41

```
#FrostWire properties file
#Tue Jun 11 12:17:12 EDT 2013
AVERAGE_UPTIME=379
SHOW_PROMOTION_OVERLAYS=true
UI_TRANSFERS_DIVIDER_LOCATION=311
DEFAULT_TORRENT_DATA_DIR_SETTING=C\:\\Users\\nmurray\\FrostWire\\Torrent Data
BTMEDIATOR_COLUMN_SORT_INDEX=13
DIRECTORY_FOR_SAVING_FILES=C\:\\Users\\nmurray\\FrostWire
COUNTRY=
DIRECTORY_FOR_OPEN_DESKTOP_EXPLORER=C\:\\Users\\nmurray\\FrostWire
LAST_EXPIRE_TIME=1370966147401
SHOW_HIDE_EXIT_DIALOG=false
SEED_FINISHED_TORRENTS=false
WINDOW_Y=212
WINDOW_X=128
LIBRARY_FROM_DEVICE_DATA_DIR_SETTING=C\:\\Users\\nmurray\\FrostWire\\From
Device
DIRECTORIES_TO_INCLUDE_FOR_FILES=C\:\\Users\\nmurray\\Music;C\:\\Users\\nmurray\\Frc
Device;C\:\\Users\\nmurray\\FrostWire\\Torrent Data;C\:\\Users\\nmurray\\Videos
TORRENTS_DIR_SETTING=C\:\\Users\\nmurray\\FrostWire\\Torrents
TOTAL_UPTIME=379
INSTALLED=true
CHAT_SERVER=chat.frostwire.com
RUN_ONCE=true
LAST_FILECHOOSER_DIR=C\:\\Program Files (x86)\\FrostWire 5
SHOW_FROSTWIRE_RECOMMENDATIONS=true
CHAT_IRC_NICK=
```

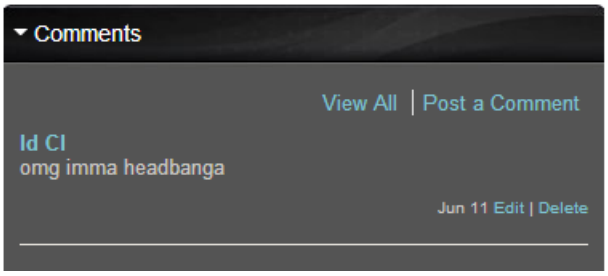
Social Networking

Billions of people use social networking sites such as Facebook, Google+, and Twitter. Not only is a large amount of personal information found on these sites, but a number of artifacts are generated by their use as well. We used several social networking sites to generate data for IEF.

Bebo

IEF did not return any results from Bebo. On 6/11/13 at 13:29, we visited bebo.com and created an account. At 13:43, we posted a comment on the Bebo profile (Figure 42). IEF parses for Bebo chats only, which may have resulted in the lack of data.

Figure 42



Facebook Chat

No Facebook Chat artifacts were generated during this project. Figure 44 shows a chat from a previous project. These messages do not match our notes from Facebook. The timestamp information in Figure 43 corresponds to our installation of Trillian; however, we did not send this message.

Figure 43

n/a	n/a	2013-06-04 18:20:17	n/a	n/a	0	n/a	looking at https://www.trillian.im/account/?type=email...
n/a	n/a	2013-06-04 18:08:40	n/a	n/a	0	n/a	looking at https://www.trillian.im/download/\n| referred ...
n/a	n/a	2013-06-04 18:08:40	n/a	n/a	0	n/a	looking at https://www.trillian.im/download/\n| referred ...

Figure 44

Facebook Pages

The Facebook Pages result (Figure 45) from IEF does not appear to be related to our notes. Further research into the link in Figure 45 lead us to believe it is likely related to a 2D design program called "DESIGN TOOLS - 2D DESIGN," which appears to be a program for designing 2D images. This link may be a reference to a Facebook cookie, but it is not related to our notes.

Figure 45

"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">

Google+

We did not generate any chat information on Google+ during this project, so IEF did not return any results. On 6/11/13 at 14:07, we updated our name on Google+ because Google had an issue with the previous username. We changed our name to "john smith." At 14:08, we attempted to make a post but there was an error posting.

LinkedIn

We did not generate any LinkedIn emails, so IEF did not return any results from LinkedIn. On 6/11/13 at 14:29, we posted a status on LinkedIn but IEF did not register this because this version of IEF does not support LinkedIn statuses.

MySpace

We did not generate any messages on MySpace for this project; therefore IEF did not return any results from MySpace.

Twitter

Our Twitter results do not display anything other than the source of the entries and the sector offset. On 6/11/13 at 15:27, we sent a tweet. IEF does not show any identifying information (timestamps, screen name, tweet text, etc.) to compare to our notes. The results (**Error! Reference source not found.**) we retrieved do show that we visited the twitter website, but do not provide us the content of the tweets.

Figure 46

Name	(not found)
Screen Name	(not found)
Created At	(not found)
Tweet Text	(not found)
In Reply To	(not found)
Status ID	(not found)
Tweet Source	(not found)
Geo	(not found)
Retweeted	(not found)
Profile Img URL	
Source	IEF Data.E01 - Partition 2 (999.99 GB) - H:\Users\r
Located At	File offset 1030

Conclusion

IEF presents the user with information related to internet use and artifacts. It parses internet artifacts and displays the data in a readable report format. We used 24 of the 40 programs that IEF supports to generate data, and IEF returned results for 22 of them. IEF can parse internet artifacts related to web browsers, chat programs, cloud services, and email, among others. This information can be very important to an investigator in a criminal case to refute or corroborate evidence. Most of our results appeared to be accurate and matched our notes, but a few of the results were patently inaccurate. For example, none of the Internet Explorer history matched our notes. In fact, IEF reported that it was another user who had generated our data several weeks before we started the project, nor did the Facebook chat messages (Figure 43) match the notes we took. It is important to remember that IEF is an automatic tool, and the results should be confirmed by a professional forensic examiner, who will manually find the artifact on the image and verify the information is accurate. IEF is user-friendly as well as easy to use. With only a few clicks, the task of processing data can be started. However, some portions of the data could be hard to understand, such as the information contained within a cookie file. These files are often confusing to read and seemingly cluttered. In some cases, there is no easy way to understand what Information IEF shows you. Fortunately, in most cases IEF presents clear and accurate data, as seen in Figure 47. Again, this information should be verified manually. Carl Sagan is quoted as saying "absence of evidence is not evidence of absence!" Even if IEF does not present information for an artifact does not mean it does not exist.

Figure 47

#	Message	Date/Time - UTC (yy...	Message ID	From ID:	To IDs:
1	omg	2013-06-05 19:32:26	1	jsmithyolo420	nperry0010
2	lol	2013-06-05 19:37:41	2	nperry0010	jsmithyolo420
3	LMFAO	2013-06-05 19:59:52	3	jsmithyolo420	nperry0010
4	yolo	2013-06-05 20:02:13	4	nperry0010	jsmithyolo420

Further Work

The programs that were not used to generate data by our team could be investigated using IEF, such as Second Life and World of Warcraft. AIM, Google Talk, and ICQ all have a logging option that must be manually turned on in order for IEF to gather information. These programs could be used more to generate data at another time. The chat/email functions on the Social Media sites could also be used to generate data for another project. IEF 6 could be used against the same image used here, and the results could be compared. Additionally, further research into why the IEF result for Google Drive (Figure 17) displays files sizes that are 1000 times larger than the file's actual size, as well as research into why IEF did not find any Hotmail or Yahoo Webmail artifacts could also be beneficial.

Further questions to be answered include:

1. What does it mean when time stamps are inaccurate?
2. Did IEF parse the artifacts incorrectly?
3. Where are the timestamps being pulled from?
4. If they are wrong, why are they wrong?

Reference

Supported Artifacts | Magnet Forensics. (n.d.). *Magnet Forensics*. Retrieved July 14, 2013, from http://www.magnetforensics.com/software/internet-evidence-finder/supported-artifacts/

Forensic Focus. (n.d.). *Internet Evidence Finder (IEF)*. Retrieved July 14, 2013, from http://www.forensicfocus.com/c/aid=54/reviews/2013/internet-evidence-finder-ief/

O'Leary, R. J. (2012, November 7). Internet Evidence Finder Version 5.6.0. *Justnet*. Retrieved July 14, 2013, from https://www.justnet.org/pdf/IEF-Report-11-7-12.pdf

Krause, J. (2013, March 15). Review: Internet Evidence Finder (IEF) v6.0.*Forensiccom RSS*. Retrieved July 14, 2013, from http://forensiccontrol.com/resources/reviews/review-internet-evidence-finder-v6-0/