

Facebook Forensics

Kelvin Wong, *captain@vxrl.org*, Security Researcher
Anthony C. T. Lai, *darkfloyd@vxrl.org*, Security Researcher
Jason C. K. Yeung, *taku@vxrl.org*, Security Researcher
W. L. Lee, *leng@vxrl.org*, Security Researcher
P. H. Chan, *sweeper@vxrl.org*, Security Researcher

Table of Contents

Abstract	2
1 Introduction	3
1.1 Background	3
1.2 Aims and Objective.....	3
1.3 Scope and Methodology.....	3
1.4 Testing Platforms	4
1.5 Tools Used	4
2 Facebook Protocol Format	6
2.1 Feed.....	6
2.2 Comment.....	7
2.3 Message.....	8
2.4 Chat	8
3 Forensics on Common Facebook Activities	10
3.1 Friend Search	10
3.2 Comments	10
3.3 Events.....	11
3.4 Photos.....	13
3.5 Chats.....	13
3.6 Notification Email.....	15
4 Facebook Forensics in Virtual Environment	17
5 Facebook Forensics in Mobile Devices	19
5.1 iPhone.....	19
5.2 Android	21
6 Conclusions	23
References	24
Who am I?.....	24

Abstract

Facebook activities have grown in popularity along with its social networking site. However, many cases involve potential grooming offences in which the use of Facebook platform and Facebook App for mobile needs to be investigated. As various activities such as instant chats, wall comments and group events could create a number of footprints in different memory locations, the purpose of this study is to discover their evidences on various platforms or devices.

The analysis process mainly uses various physical and logical acquisition tools for memory forensics, as well as Internet evidence finding tools for web browser cache searching or rebuilding. After locating the evidence of a Facebook activity, its footprints could be examined by referring to the response from corresponding Facebook communication. The same activity may be tested several times with different contents to increase the accuracy.

Throughout the research, there are some significant findings. Facebook core objects could be located in different memory units including RAM, browser cache, pagefiles, unallocated clusters and system restore point of a computer. More importantly, these findings are matched with those in virtual machines and the corresponding snapshot images. Although separate sets of results are obtained from iPhone or Android phone due to the difference between Facebook App and a standard web browser, evidence could still be located in the file system using mobile device forensics tools.

1 Introduction

Facebook is a website providing social network service, launched in February 2004, operated and privately owned by Facebook Incorporation [1]. Its goal is to give people the power to share, and make the world more open and connected [2]. Facebook users may create a personal profile, add other users as friends, and exchange messages (including automatic feed notifications when they update their profile information. Additionally, users may share their status, news stories, notes, photos, videos, and allow their friends (or friends of friends) to comment on them. Furthermore, users may join common-interest groups, organize events, and create fans pages for a workplace/business, a school/college, or even a brand/product. However, it is unavoidable that this platform may also provide incentives for criminals to carry out illegal activities such as drugs business and sex trading.

1.1 Background

Facebook was founded by Mark Zuckerberg with his college roommates and fellow computer science students Eduardo Saverin, Dustin Moskovitz and Chris Hughes [3]. The website's membership was initially limited by the founders to Harvard students, but was expanded to other colleges in the Boston area, the Ivy League, and Stanford University. It gradually added support for students at various other universities before opening to high school students, and, finally, to anyone aged 13 and over. As of January 2011, Facebook has more than 600 million active users [4, 5]. However, there are 7.5 million children under 13 with accounts, violating the site's terms, based on ConsumersReports.org on May 2011 [6]. It is not hard to imagine that criminals might use these accounts to hide their real identity.

Facebook cases are already found and reported with it. No matter computer forensic examiners or crime investigators should also need to understand the approach to extract and obtain digital evidence from suspect's computer for inspection purpose. Carrying out forensics studies over Facebook activities could be valuable for them and law enforcement units.

1.2 Aims and Objective

Due to the popularity of Facebook and its potential for being misused, the main objective of this study is to find out the evidence of Facebook activities on various platforms or devices. This can be achieved by analysing:

- What are Facebook evidences
- Where are Facebook evidences located
- How to find out Facebook evidences

These aims contributed as knowledge base and techniques sharing to investigators from forensics perspective.

1.3 Scope and Methodology

This study only limits to find out evidence of Facebook activities in a physical and virtual machine or device. However, providing the real identity of a Facebook account owner who performs those activities will not be covered. Besides analyzing the format of protocol that Facebook used for data exchange, this project also attempts to identify footprints for the following Facebook activities:

- search friends
- post news feed on wall
- comment on others wall post
- create event
- send event message to group
- chatting

The approach of this research is to try various tools on searching and extracting footprints from the following memory areas and devices:

- volatile memory (RAM)
- browser cache file
- virtual machine image files
- virtual machine snapshot files
- iPhone file system dump
- Android phone file system dump

The results will also be supplemented with findings from photos uploaded by users and Facebook automatic notification emails to provide more detailed and comprehensive forensics analysis.

1.4 Testing Platforms

Our studies have been carried out in both physical personal computers or mobile devices and VMware virtual machines on the following platforms.

- Operating systems:
 - MS Windows
 - iPhone iOS 4.3
 - Android
- Web browsers:
 - MS Internet Explorer version 8
 - Google Chrome version 11.0

1.5 Tools Used

We have used the following tools in our research.

1.5.1 Internet Evidence Analytical Tools

Internet Evidence Finder (www.jadsoftware.com) – Internet Evidence Finder (IEF) is a software application that can search a hard drive or files for Internet related artifacts [7]. It is a data recovery tool that is geared towards digital forensics examiners but is designed to be straightforward and simple to use. It searches the selected drive, folder (and sub-folders, optionally), or file (memory dumps, pagefile.sys, hiberfil.sys, etc) for Internet artifacts. A case folder is created containing the recovered artifacts and the results are viewed through its Report Viewer where reports can be created and data exported to various formats [7].

Facebook JPG Finder (www.jadsoftware.com) – Facebook JPG Finder (FJF) is a tool that searches a selected folder (and optionally, sub-folders) for possible Facebook JPG images [8]. These images are identified by running several filters on the file name. The file name contains the Facebook user/profile ID and therefore can indicate which Facebook user the photo came from. An HTML report file is created in a case folder containing the file name, the created/modified/last accessed times, a link to the possible Facebook profile, an MD5 hash of the image, and the image itself. All located images are also copied into the output folder [8].

CacheBack (www.cacheback.ca) – CacheBack is the leading forensic Net analysis tool specializing in browser cache, history and chat discovery for forensic investigations [9]. It is the only Internet forensic tool on the market today that supports all five top browsers. It is also the leading finder of Internet evidence and related artifacts that consolidates everything into a single, comprehensive user interface. Web pages are easily rebuilt offline by the simple click of the mouse which allows evidence to be presented “in its original state” thereby offering a more visual impact to courts and

jurors. Government and law enforcement agencies turn to CacheBack to quickly rebuild cached web pages, locate and identify photographic evidence, and comb through complex Internet histories. In addition, it has become an indispensable tool for generating compelling visual reports, criminal activity timelines, and uncovering probative artifacts for criminal proceedings. Furthermore, it is fast becoming the tool of choice to support investigations involving or revealing child exploitation offences, terrorism, criminal premeditation, social networking, crimes against persons, corporate fraud, and theft [9].

1.5.2 Memory Analytical Tools

Helix (www.e-fense.com) – Helix is a bootable sound environment to boot any x86 system, and making forensic images of all internal devices or physical memory (32 and 64 bit) [10].

Win32dd (www.moonsols.com/windows-memory-toolkit/) – MoonSols Windows Memory Toolkit (Win32dd) is a toolkit for memory dump conversion and acquisition on Windows [11]. It had been designed to deal with various types of memory dumps such as VMWare memory snapshot, Microsoft crash dump and even Windows hibernation file [11].

Forensic Toolkit (www.accessdata.com) – Forensic Toolkit (FTK) is a leading computer forensics and image acquisition software solution, because it is designed with an enterprise-class architecture that is database driven [12]. It is proven to deliver the most robust analysis, and it provides the fastest processing on the market. FTK's database-driven design prevents the crashing that is so common with memory-based tools. The solution scales to handle massive data sets and lays the foundation to expand into a full lab infrastructure [12].

1.5.3 Mobile Device Forensics Tools

XRY 5.0 (www.msab.com) – XRY is a complete mobile device forensic system that can be used on any Windows operating system [13]. Recovering data from thousands of different mobiles and even deleted data. The easy to use tools will allow user to configure reports within a matter of minutes. It is also a software application which allows user to perform a secure forensic extraction of data from a wide variety of mobile devices, such as smartphones, GPS navigation units, 3G modems, portable music players and the latest tablet processors such as the iPad [13].

Oxygen Forensics Suite 2011 (www.oxygen-forensic.com) – Oxygen Forensic Suite 2011 is a mobile forensic software that goes beyond standard logical analysis of cell phones, smartphones and PDAs [14]. Using advanced proprietary protocols permits it to extract much more data than usually extracted by logical forensic tools, especially for smartphones [14].

2 Facebook Protocol Format

Before locating any Facebook evidence, we need to know the format of Facebook protocol that may appear in RAM or browser cache. Therefore, we attempted to identify the protocol format of Facebook feed, comment, message and chat located in RAM and browser cache on a virtual machine. In the following analysis, two Facebook accounts have been set up for performing Facebook activities. *jdis@vxrl.org* is the tester account responsible for wall posting, commenting, messaging and chatting on his own whereas *jason.yeung@yahoo.com* is the helper account responsible for replying to and chatting with the tester. Snapshot of tester’s virtual machine status was taken before starting of any Facebook activities while after these testing activities have been completed, RAM and browser cache was dumped from the tester’s virtual machine using Win32dd and CacheBack respectively. The whole acquisition process was repeated twice for consistency concern.

2.1 Feed

In this part, tester posted a feed “2this is a POST test2” on his own wall, but we could not identify it from both his RAM and browser cache. However, replied message “2good to see you POST2” posted by the helper could be identified on both RAM and browser cache of tester’s machine. Two occurrences were identified with this reply message as shown in Figure 1, and their protocol formats were summarized in Table 1.

```
for (;);{"t":"msg","c":"p_100002239013747","s":3,"ms":[{"updates":["(function(){CSS.show(this);;}).
apply(DOM.find(this.getRelativeTo(),\".uiUfiComments\\\"))\",\"(function(){DataStore.set(this, \\\"seqnum\\
\", \\\"80230\\\");;}).apply(DOM.find(this.getRelativeTo(),\"\\\"))\",\"(function(){fc_expand(this, false);;}).
apply(DOM.find(this.getRelativeTo(),\"textarea\\\"))\",\"(function(){(!((DOM.scrpy(this, \\\"#optimistic_co
mment_2523124662_0\\\"))).length + (DOM.scrpy(this, \\\".comment_80230\\\"))).length)) && DOM.appendChild(D
OM.find(this, \\\"_commentList\\\"), HTML(\\\"\\u003ccli class=\\\"uiUfiComment comment_80230 ufiItem uiUfi
UnseenItem\\\">\\u003cdiv class=\\\"UIImageBlock clearfix uiUfiActorBlock\\\">\\u003ca class=\\\"act
orPic UIImageBlock_Image UIImageBlock_SMALL Image\\\" href=\\\"http://\\\"/\\\"/www.facebook.com\\\"/jaso
n.ckeyeung\\\" tabindex=\\\"-1\\\">\\u003cimg class=\\\"uiProfilePhoto uiProfilePhotoMedium img\\\" s
rc=\\\"http://\\\"/\\\"/profile.ak.fbcdn.net\\\"/hprofile-ak-snc4\\\"/49146_635527479_3483_q.jpg\\\" alt=\\
\\\"\\\" /\\\">\\u003c\\\"/a>\\u003cdiv class=\\\"commentContent UIImageBlock_Content UIImageBlock_SMAL
L_Content\\\">\\u003ca class=\\\"actorName\\\" href=\\\"http://\\\"/\\\"/www.facebook.com\\\"/jason.ckeye
ung\\\" data-hovercard=\\\"\\\"/ajax/hovercard\\\"/user.php?id=635527479\\\">Jason Yeung\\u003c\\\"/a
> \\u003cspan data-jid=\\\"text\\\">\\u200e2good to see you POST2\\u003c\\\"/span>\\u003cdiv class=\\
\\\"commentActions fsm fwn fcg\\\">\\u003cabbr title=\\\"Monday, April 18, 2011 at 4:29pm\\\" data-da
te=\\\"Mon, 18 Apr 2011 01:29:36 -0700\\\" class=\\\"timestamp\\\">2 seconds ago\\u003c\\\"/abbr>
```

(a)

```
"alert_type":54,"alert_id":505370,"time_created":1303115376,"from_uids":{"635527479":635527479},"fro
m_uid":635527479,"context_id":"108962369188396","total_count":1,"unread":true,"app_id":19675640871,"
oid":"108962369188396","owner":"100002239013747","text":"2good to see you POST2","object_id":"","sto
ry_type":22,"num_credits":0,"userId":"100002239013747","fromId":null,"title":"\\u003cspan class=\\\"bl
ueName\\\">Jason Yeung\\u003c\\\"/span> commented on your status.","body":null,"link":"http://\\\"/www.facebo
ok.com\\\"/permalink.php?story_fbid=108962369188396&id=100002239013747"
```

(b)

Figure 1: Reply to Facebook feed extracted from RAM and browser cache in (a) HTML format and (b) JSON format

Facebook Protocol Format	Analysis
<pre>••• class="actorPic UIImageBlock_Image UIImageBlock_SMALL_Image" href="«helper's profile URL»" tabindex="-1"><div class=\\\"commentContent UIImageBlock_Content UIImageBlock_SMALL_Content">«helper's full name» \\u200e«content of reply»<div class="commentActions fsm fwn fcg"><abbr title="«local</pre>	<p>HTML format could be identified on both RAM and browser cache. It appears to be the body of the reply itself.</p>

<pre>time»" data-date="«time in GMT-7»" class="timestamp">«last post's time» ...</pre>	
<pre>... "alert_type":«alert type», "alert_id":«alert id», "time_created":«unix timestamp», "from_uids":{ "635527479":635527479 }, "from_uid":635527479, "context_id":"«context id»", "total_count":1, "unread":true, "app_id":«app id», "oid":"«feed id»", "owner":"«feed owner id»", "text":"«content of feed»", "object_id":"", "story_type":22, "num_credits":0 }, "userId":"«tester's profile id»", "fromId":null, "title":"«helper's full name» commented on your status.", "body":null, "link":"http://www.facebook.com/permalink.php?story_fbid =«feed id»&id=«feed owner id»" ... </pre>	<p>JSON format could be identified on both RAM and browser cache.</p> <p>It appears to be the notification badge on top left corner of Facebook frame.</p>

Table 1: Protocol format analysis of reply to Facebook feed.

Note that the protocol format in Table 1 is unescaped to make it easier to read. For HTML format, character is unescaped twice from “\\” to “\”, from “\\” to “/”, and from “\u003c” to “<”. For JSON format, “/” and “\u003c” is unescaped to “/” and “<” respectively.

2.2 Comment

On the other way round, helper post a feed “2a long night!2” on his wall and tester was then make a comment “2yes, it really is2” to it. Although we could not identify the original feed that tester commented on, the testing comment itself could be identified from both RAM and browser cache of tester’s machine as shown in Figure 2 and Table 2.

<pre>"ms": [{"updates": [{"function() {CSS.show(this);}).apply(DOM.find(this.getRelativeTo(), \".uiUfiCommen ts\");), \"(function() {DataStore.set(this, \"seqnum\", \"15815303\");}).apply(DOM.find(this.getRelativ eTo(), \"\");), \"(function() {fc_expand(this, false);}).apply(DOM.find(this.getRelativeTo(), \"textare\ \");), \"(function() {!(DOM.scry(this, \"#optimistic_comment_1869046244_0\")).length + (DOM.scry(this, \".comment_15815303\")).length}) && DOM.appendContent(DOM.find(this, \".commentList\"), HTML(\"\\u0 03cli class=\\\"uiUfiComment comment_15815303 ufiItem uiUfiUnseenItem\\\">\\u003cdiv class=\\\"UIIma geBlock clearfix uiUfiActorBlock\\\">\\u003ca class=\\\"actorPic UIImageBlock_Image UIImageBlock_SMA LL_Image\\\" href=\\\"http://www.facebook.com/profile.php?id=100002239013747\\\" tabindex=\\ -1\\\">\\u003cimg class=\\\"uiProfilePhoto uiProfilePhotoMedium img\\\" src=\\\"http://stat ic.ak.fbcdn.net/rsrc.php/v1/y9/r/IB7NOFmPw2a.gif\\\" alt=\\\"\\\" />\\u003c/a>\\ u003cdiv class=\\\"commentContent UIImageBlock_Content UIImageBlock_SMALL_Content\\\">\\u003ca clas s=\\\"actorName\\\" href=\\\"http://www.facebook.com/profile.php?id=100002239013747\\\" dat a-hovercard=\\\"/ajax/hovercard/user.php?id=100002239013747\\\">David Robinson\\u003c/a> \\u003cspan data-jsid=\\\"text\\\">\\u200e2yes, it really is2\\u003c/span></pre>
--

Figure 2: Facebook comment extracted from RAM and browser cache in HTML format.

Facebook Protocol Format	Analysis
<pre>... class="actorPic UIImageBlock_Image UIImageBlock_SMALL_Image" href="«tester's profile URL»" tabindex="-1"><img class="uiProfilePhoto uiProfilePhotoMedium img"</pre>	<p>This format could be identified on both RAM and browser cache.</p>

<pre>src="http://static.ak.fbcdn.net/rsrc.php/v1/y9/r/IB7NOFm Pw2a.gif" alt="" /><div class="commentContent UIImageBlock_Content UIImageBlock_SMALL_Content">«tester's full name» \\u200e«content of comment» ...</pre>	
--	--

Table 2: Protocol format analysis of Facebook comment.

2.3 Message

This time, tester send a private message to the helper titled “2MESSAGE is always good jy2” with body text “2do you think so?2”. This message was not identified on both RAM and browser cache neither. However, replied message “2yes I guess so?” from helper could be identified solely on RAM. We attempted to identify if there is any logical format but was not successful.

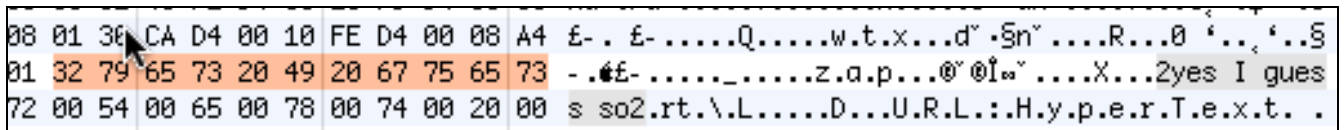


Figure 3: Memory segment showing the private replied message.

Private message appears to be randomly stored in memory merely, which is demonstrated on the screenshot in Figure 3. In this case, we could not make any summary regarding to the format of protocol on Facebook messaging.

2.4 Chat

Format analysis on Facebook chat is the easiest and most consistent one. All chatting history could be identified on both RAM and browser cache with identical format. Moreover, the chatting history was so well-structured that most commercial tools could easily extracted and embedded this as a feature of their product. For example, a chat message from tester to helper was extracted in RAM of tester’s machine as shown in Figure 4 and Table 3.

<pre>for (;);{"t":"msg","c":"p_100002239013747","s":14,"ms":[{"msg":{"text":"2what is the best restauran t in hong kong?2","time":1303115825598,"clientTime":1303115824391,"msgID":"1862585188"},"from":10000 2239013747,"to":635527479,"from_name":"David Robinson","from_first_name":"David","from_gender":1,"to _name":"Jason Yeung","to_first_name":"Jason","to_gender":2,"type":"msg"}]}</pre>

Figure 4: Facebook chat extracted from RAM in JSON format.

Facebook Protocol Format	Analysis
<pre>{ "t": "msg", "c": "p_100002239013747", "s": 14, "ms": [{ "msg": { "text": "«content of chat»", "time": «unix timestamp», "clientTime": «local unix timestamp», "msgID": "1862585188" }, "from": «sender's profile id», "to": «recipient's profile id», "from_name": «sender's full name», "from_first_name": «sender's first name», "from_gender": 1, "to_name": «recipient's full name», }] }</pre>	<p>JSON format could be identified on both RAM and browser cache. It appears to be the body of the chat itself.</p>

<pre>"to_first_name": "«recipient's first name»", "to_gender": 2, "type": "msg" }] }</pre>	
---	--

Table 3: Protocol format analysis of Facebook chat.

3 Forensics on Common Facebook Activities

We have found that friend search, comments and reply posted by friends could be found from browser cache. The trace of browser cache file from CacheBack software and screenshots are attached in the following subsections.

3.1 Friend Search

Icon	URL ID	Links	Type	Alert	URL
	312				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=ant&viewer=100001519874025&rsp=search&sid=0.505282011118
	96				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=jas&viewer=100001519874025&rsp=search&sid=0.028834945056
	231				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=jason%20y&viewer=100001519874025&rsp=search&sid=0.02883
	59				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=jason%20yeung&viewer=100001519874025&rsp=search&sid=0.0
	22				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=al&viewer=100001519874025&rsp=search&sid=0.1483879087027
	40				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=alb&viewer=100001519874025&rsp=search&sid=0.1483879087027
	253				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=albert%20h&viewer=100001519874025&rsp=search&sid=0.14838
	186				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=albert%20ho&viewer=100001519874025&rsp=search&sid=0.1483
	94				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=r&viewer=100001519874025&rsp=search&sid=0.4317952773999
	142				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=ra&viewer=100001519874025&rsp=search&sid=0.4317952773999
	183				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=ray&viewer=100001519874025&rsp=search&sid=0.4317952773999
	271				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=ray%20&viewer=100001519874025&rsp=search&sid=0.4317952
	167				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=ray%20a&viewer=100001519874025&rsp=search&sid=0.4317952
	320				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=ray%20aw&viewer=100001519874025&rsp=search&sid=0.43179
	43				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=f&viewer=100001519874025&rsp=search&sid=0.5996259080711
	215				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=fran&viewer=100001519874025&rsp=search&sid=0.59962590807
	182				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=franco&viewer=100001519874025&rsp=search&sid=0.599625908
	223				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=franco%20b&viewer=100001519874025&rsp=search&sid=0.59962
	179				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=franco%20bar&viewer=100001519874025&rsp=search&sid=0.59962
	12				http://www.facebook.com/ajax/typeahead/search.php?__a=1&value=franco%20bares&viewer=100001519874025&rsp=search&sid=0.5

Figure 5: Friend search.

3.2 Comments

We have shown you wall post and reply and the corresponding footprints found from browser cache file.



```

\\www.facebook.com\\profile.php?id=100000771259268\\ tabindex=\\-1\\>\\u003cing
class=\\uiProfilePhoto uiProfilePhotoMedium img\\\" src=\\\"http://
\\static.ak.fbcdn.net\\rsrc.php\\v1\\y9\\r\\IB7N0PmPv2a.gif\\\" alt=\\\"\\\"
\\/>\\u003c\\a\\u003cdiv class=\\\"commentContent UIImageBlock_Content
UIImageBlock_SMALL_Content\\\">\\u003c class=\\\"actorName\\\" href=\\\"http://
\\www.facebook.com\\profile.php?id=100000771259268\\\" data-hovercard=\\\"\\\"/\\ajax
\\hovercard\\user.php?id=100000771259268\\\">Belle Bell\\u003c\\a> \\u003cspan data-
jsid=\\\"text\\\">\\u200e1G Duo and 1G RAM\\u003c\\span>\\u003cdiv class=\\\"commentAction
fsu fm fcg\\\">\\u003cabbr title=\\\"Saturday, March 19, 2011 at 7:59pm\\\" data-date=
\\\"Sat, 19 Mar 2011 04:58:18 -0700\\\" class=\\\"timestamp\\\">2 seconds ago\\u003c\\abbr
\\u00b7 \\u003cspan class=\\\"comment_like_2584746 fsu fm fcg\\\">\\u003cbutton class=
\\\"stat_elem as_link cmnt_like_link\\\" type=\\\"submit\\\" name=\\\"like_comment_id
[2584746]\\\" value=\\\"2584746\\\" title=\\\"Like this comment\\\">\\u003cspan class=
\\\"default_message\\\">Like\\u003c\\span>\\u003cspan class=\\\"saving_message\\\">Unlike
\\u003c\\span>\\u003c\\button>\\u003c\\span>\\u003c\\div>\\u003c\\div>\\u003c
\\div>\\u003c\\li>\\\"));.apply(DOM.find(this.getRelativeTo(),\"\\\"),\"\\\"),\"(function()

```

(a)

(b)

Browser	Text	Hex	Picture	Video	Links	Audit	Report
33	853						
34	124						
35	843						
36	288						
37	844						

```

:OL_URL_RAWVALUE: http://www.facebook.com/event.php?eid=1987125768176134pending
:OL_URL_FILE_EXT:
:OL_URL_CATEGORY:
:OL_URL_HOST: facebook.com
:OL_URL_WEBPAGE_TITLE: Wave Party (3)
:OL_URL_VARIABLES: eid=1987125768176134pending
:OL_URL_BASE_PATH: C:\
:OL_URL_CACHE_ROOT_PATH:
:OL_URL_FILE_RELATIVE_PATH:
:OL_URL_HTTP_METADATA:
:OL_URL_SOURCE_HISTORY_FILE: C:\FB Forensics output2 - chrome\CacheGrab.Windows\Chrome\0000003.History\History
:OL_URL_MAP_FILE_OFFSET:
:OL_URL_DATA_BLOCK_FILE:
:OL_URL_DATA_BLOCK_FILE_OFFSET:
:OL_URL_GZIP_ENCODED: No
:OL_URL_PICTURE_HEIGHT: 0
:OL_URL_PICTURE_WIDTH: 0
:OL_URL_PARD: 0
:OL_URL_EXPIRY_DATE:
:OL_URL_FILE_CREATED:
:OL_URL_FILE_LAST_ACCESSED: 2011-03-19 03:08:02
:OL_URL_ORIGINAL_PATH: \documents and settings\administrator\local settings\application data\google\chrome\user data\default\History

```

Figure 8: Facebook event in cache file of Google Chrome browser.

Browser	Text	Hex	Picture	Video	Links	Audit	Report
31	428						
32	777						
33	853						

```

for (j);{"t":"msg","c":"p_662436133","s":8,"ms":{"app_id":30729425562,"event_name":"beep_event","response":{"_ar":1,"error":0,"errorSummary":"","errorDescription":"","errorIsWarning":false,"silentError":0,"payload":{"alertId":102085440,"platformType":null,"applicationName":"Events","alert":{"time_sent":1300507072,"to_user":662436133,"recipient_vc":null,"alert_type":35,"alert_id":102085440,"time_created":1300507072,"from_uids":{"635527479":635527479,"from_uid":635527479,"context_id":198712576817613,"total_count":1,"unread":true,"app_id":2344061033,"eid":198712576817613,"text":{"good,I'm coming!},"user_id":662436133,"from_id":null,"title":"","u003cspan class=\"blueName\">Jason Yeung\u003c\/span> wrote on the Wall for \u003cspan class=\"blueName\">Wave Party\u003c\/span>","body":null,"link":"http://www.facebook.com/event.php?eid=198712576817613#wall_posts","userPic":null,"icon":"","images\/icons\/event.gif","applicationId":2344061033,"type":"NotificationBeep"},"html":"\u003cdiv class=\"UIBeep\">\u003cdiv class=\"UIBeepNonIntentional\" href=\"http://www.facebook.com/event.php?eid=198712576817613#wall_posts\">\u003cdiv class=\"UIBeepIcon\">\u003cdiv class=\"beeper icon img sp dcxdsx sc9b76\">\u003cdiv>\u003cspan class=\"beeper_x\">&nbsp;\u003c\/span>\u003cdiv class=\"UIBeepTitle\">\u003cspan class=\"blueName\">Jason Yeung\u003c\/span> wrote on the Wall for \u003cspan class=\"blueName\">Wave Party\u003c\/span>\u003cdiv class=\"\u003cdiv>\u003c\/a>\u003cdiv>","isIntentional":false},"css":{"awtL8","u003c","invalidate_cache":[0],"resource_map":{"type":"css","permanent":1,"src":"http://b.static.ak.fbcdn.net\/rsrc.php\/v1\/y9\/r\/On3006P6FR.css"}},"hasCapture":true,"type":"app_msg"}}}

```

Figure 9: Create Facebook event.

Property	Value	Icon	URL ID	Links	Type	Alert	URL	Rebuilt	File Exists
ction	Messaged		604				http://0.197.channel.facebook.com/x/28117902/627276521/false/p_662436133=5	No	Yes
ctionDateLocal	2011-03-18 23:57:47 [-0400 DST		147				http://0.197.channel.facebook.com/x/255004874/627276521/false/p_662436133=6	No	Yes
ctionDateUTC	2011-03-19 03:57:47 [UTC]		428				http://0.197.channel.facebook.com/x/2420374171/376164660/false/p_662436133=7	No	Yes
acheFileCreated	2010-05-04 18:18:45		777				http://0.197.channel.facebook.com/x/1454983013/376164660/false/p_662436133=8	No	Yes
acheFileExt	True		785				http://0.197.channel.facebook.com/x/3796318943/1028370698/true/p_662436133=9	No	Yes
acheFileHash	1A6639C85EA129F4BF6D5079		43				http://0.197.channel.facebook.com/x/274301380/1828370698/false/p_662436133=10	No	Yes

```

for (j);{"t":"msg","c":"p_662436133","s":9,"ms":{"app_id":30729425562,"event_name":"beep_event","response":{"_ar":1,"error":0,"errorSummary":"","errorDescription":"","errorIsWarning":false,"silentError":0,"payload":{"alertId":102085440,"platformType":null,"applicationName":"Events","alert":{"time_sent":1300507072,"to_user":662436133,"recipient_vc":null,"alert_type":35,"alert_id":102085440,"time_created":1300507072,"from_uids":{"635527479":635527479,"from_uid":635527479,"context_id":198712576817613,"total_count":1,"unread":true,"app_id":2344061033,"eid":198712576817613,"text":{"good,I'm coming!},"user_id":662436133,"from_id":null,"title":"","u003cspan class=\"blueName\">Jason Yeung\u003c\/span> wrote on the Wall for \u003cspan class=\"blueName\">Wave Party\u003c\/span>","body":null,"link":"http://www.facebook.com/event.php?eid=198712576817613#wall_posts","userPic":null,"icon":"","images\/icons\/event.gif","applicationId":2344061033,"type":"NotificationBeep"},"html":"\u003cdiv class=\"UIBeep\">\u003cdiv class=\"UIBeepNonIntentional\" href=\"http://www.facebook.com/event.php?eid=198712576817613#wall_posts\">\u003cdiv class=\"UIBeepIcon\">\u003cdiv class=\"beeper icon img sp dcxdsx sc9b76\">\u003cdiv>\u003cspan class=\"beeper_x\">&nbsp;\u003c\/span>\u003cdiv class=\"UIBeepTitle\">\u003cspan class=\"blueName\">Jason Yeung\u003c\/span> wrote on the Wall for \u003cspan class=\"blueName\">Wave Party\u003c\/span>\u003cdiv class=\"\u003cdiv>\u003c\/a>\u003cdiv>","isIntentional":false},"css":{"awtL8","u003c","invalidate_cache":[0],"resource_map":{"type":"css","permanent":1,"src":"http://b.static.ak.fbcdn.net\/rsrc.php\/v1\/y9\/r\/On3006P6FR.css"}},"hasCapture":true,"type":"app_msg"}}}

```

Figure 10: Wall post of Facebook event.

Source	Located At	Subject	Snippet	Original Author
C:\pagefile.sys	File Offset 432191...	Please bring your l...	This party requires you to bring you laptop!\n\nCheers!\n\nRegards,\n\nAnthony	198712576817613
C:\pagefile.sys	File Offset 432192...	Java Programmer	Hi Anthony,\n\nDo you know any Java programmers who is now available for short..	707118295

Figure 11: Facebook message to a group of people who joined the events.

3.4 Photos

We could locate the pictures in the target machine with FJF software. From the figure, we have found that we will know photo from which Facebook profile through the “uid” value in the link of image.

Full path: c:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\3BUBOT1X\158324_131944690210546_131942046877477_40471_1432_t[1].jpg
Short name: 158324_131944690210546_131942046877477_40471_1432_t[1].jpg
Created time: 3/19/2011 3:21:20 AM (UTC)
Modified time: 3/19/2011 3:21:23 AM (UTC)
Last Accessed time: 3/19/2011 4:16:13 AM (UTC)
MD5: 919aa2b56bbea9e121ea17864bec0985

This photo possibly belongs to Facebook: user ID # [131942046877477](#)



Full path: c:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\3BUBOT1X\179859_489965476133_662436133_6139382_679101_s[1].jpg
Short name: 179859_489965476133_662436133_6139382_679101_s[1].jpg
Created time: 3/19/2011 3:21:17 AM (UTC)
Modified time: 3/19/2011 3:21:17 AM (UTC)
Last Accessed time: 3/19/2011 4:16:13 AM (UTC)
MD5: c646a3453a3385031f13eef527cb3c3b

This photo possibly belongs to Facebook: user ID # [662436133](#)



Figure 12: Photos in Facebook.

3.5 Chats

Facebook has a built-in instant chatting facility. The chat messages are cached in small html files with file name of pattern P_XXXXXXXX.htm or P_XXXXXXXX.txt. which could be found in RAM, browser cache, pagefiles, unallocated clusters and system restore point. As described in the last section, the chat message header is stored in a JSON object with the key “text”. Figure 13 shows the results that are using IEF software version 4 to extract messages.



(a)

Sender ID	Sender Name	Recipient ID	Recipient Name	Message Text
100001149375085	Kelvin Captain	622052660	Maggie Lam	please upload a photo
622052660	Maggie Lam	100001149375085	Kelvin Captain	咩٧ (conv...
622052660	Maggie Lam	100001149375085	Kelvin Captain	^^
622052660	Maggie Lam	100001149375085	Kelvin Captain	睇夠...
100001149375085	Kelvin Captain	622052660	Maggie Lam	try again
622052660	Maggie Lam	100001149375085	Kelvin Captain	我係...
100001149375085	Kelvin Captain	622052660	Maggie Lam	just reboot the system
100001149375085	Kelvin Captain	622052660	Maggie Lam	hello
100001149375085	Kelvin Captain	622052660	Maggie Lam	what moive you are wa...
622052660	Maggie Lam	100001149375085	Kelvin Captain	你果...
622052660	Maggie Lam	100001149375085	Kelvin Captain	有冇heart...
212300220	Mark P P P P P	1123402994	Richard X X X X	Another Message
100001149375085	Kelvin Captain	622052660	Maggie Lam	I am in PolyU
622052660	Maggie Lam	100001149375085	Kelvin Captain	你果...

(b)

Sender ID	Sender Name	Recipient ID	Recipient Name	Message Text
100001149375085	Kelvin Captain	622052660	Maggie Lam	please upload a photo
622052660	Maggie Lam	100001149375085	Kelvin Captain	咩٧ (conv...
622052660	Maggie Lam	100001149375085	Kelvin Captain	^^
622052660	Maggie Lam	100001149375085	Kelvin Captain	睇夠...
100001149375085	Kelvin Captain	622052660	Maggie Lam	try again
622052660	Maggie Lam	100001149375085	Kelvin Captain	我係...
100001149375085	Kelvin Captain	622052660	Maggie Lam	just reboot the system
100001149375085	Kelvin Captain	622052660	Maggie Lam	hello
100001149375085	Kelvin Captain	622052660	Maggie Lam	what moive you are wa...
622052660	Maggie Lam	100001149375085	Kelvin Captain	你果...
622052660	Maggie Lam	100001149375085	Kelvin Captain	有冇heart...
212300220	Mark P P P P P	1123402994	Richard X X X X	Another Message
100001149375085	Kelvin Captain	622052660	Maggie Lam	I am in PolyU
622052660	Maggie Lam	100001149375085	Kelvin Captain	你果...

(c)

Figure 13: Live chat room messages extracted with IEF software.

From the following figures, we could find that chat logs and history could be retrieved in the browser cache file.

Browser	Text	Hex	Picture	Video	Links	Audit	Report
25	6235		3	http://0.60.channel.facebo	No	Yes	Exists
26	6463		3	http://0.60.channel.facebo	No	Yes	Exists
27	6687		3	http://0.60.channel.facebo	No	Yes	Exists
28	244?		3	Unlicensed	No	Yes	Exists

```
for (;);{"t":"msg","c":"p_100000771259268","s":4,"ms":[{"msg":{"text":"Hi Jo","time":1300534298304,"clientTime":1300534296969,"msgID":"4188832242"},"from":100000771259268,"to":100000682519377,"from_name":"Belle Bell","from_first_name":"Belle","to_name":"Jo Ng","to_first_name":"Jo","type":"msg"}}
```

(a)

Browser	Text	Hex	Picture	Video	Links	Audit	Report
26	6463		3	http://0.60.channel.facebo	No	Yes	Exists
27	6687		3	http://0.60.channel.facebo	No	Yes	Exists
28	244?		3	Unlicensed	No	Yes	Exists

```
for (;);{"t":"msg","c":"p_100000771259268","s":7,"ms":[{"msg":{"text":"are you here","time":1300535016966,"clientTime":1300535016172,"msgID":"888659852"},"from":100000771259268,"to":100000682519377,"from_name":"Belle Bell","from_first_name":"Belle","to_name":"Jo Ng","to_first_name":"Jo","type":"msg"}}
```

(b)

Figure 14: Facebook chat.

```

COL_URL_SOURCE_HISTORY_FILE: C:\FD\FORNSAC\OUT\PC2 - CHROME\CHROME\WINDOWS\CHROME\USER\00000000.HISTORY\HISTORY
COL_URL_MAP_FILE_OFFSET: 0
COL_URL_DATA_BLOCK_FILE:
COL_URL_DATA_BLOCK_FILE_OFFSET: 0
COL_URL_GZIP_ENCODED: No
COL_URL_PICTURE_HEIGHT: 0
COL_URL_PICTURE_WIDTH: 0
COL_URL_PARD: 0
COL_URL_EXPIRY_DATE:
COL_URL_FILE_CREATED:
COL_URL_FILE_LAST_ACCESSED: 2011-03-19 03:08:02
COL_URL_ORIGINAL_PATH: \documents and settings\administrator\local settings\application data\google\chrome\user data\default\History
COL_URL_CACHE_FILE_SIZE: 0
COL_URL_TIME_REBUILT:
COL_URL_REBUILT_METHOD:
COL_URL_TIME_ADDED: 2011-03-19 05:18:20
COL_URL_FILEID: 8
COL_URL_LAST_VISITED:
COL_URL_BOOKMARK_COMMENT:
COL_URL_BOOKMARK_ID:

```

Figure 15: Physical cache file of Google Chrome browser.

3.6 Notification Email

In the past, we could obtain the IP address via Facebook notification email header but it is no longer valid right now. The reason we still discussed about it is because from investigation perspective, we would like to know the Facebook user's IP address and it may be existent in another form of Facebook notification email in the future. We have extracted one of the samples that we could discover the IP address of the user. It is found that the IP is encoded in Base64 as highlighted in Figure 16. Originally, the real IP is shown. However, it only displays MTI3LjAuMC4x (i.e. 127.0.0.1) nowadays.

```

Delivered-To: xxxxxxxx@gmail.com
Received: by 10.231.6.20 with SMTP id 20cs216348ibx;
    Sun, 26 Sep 2010 03:02:12 -0700 (PDT)
Received: by 10.142.226.1 with SMTP id ylmr4957704wfg.292.1285495331709;
    Sun, 26 Sep 2010 03:02:11 -0700 (PDT)
Return-Path: <notification+o=96s009@facebookmail.com>
Received: from mx-out.facebook.com (outmail019.sncl.tfbnw.net [69.63.178.178])
    by mx.google.com with ESMTP id g9si10571629wfd.17.2010.09.26.03.02.10;
    Sun, 26 Sep 2010 03:02:10 -0700 (PDT)
Received-SPF: pass (google.com: domain of notification+o=96s009@facebookmail.com designates
    69.63.178.178 as permitted sender) client-ip=69.63.178.178;
Authentication-Results: mx.google.com; spf=pass (google.com: domain of
    notification+o=96s009@facebookmail.com designates 69.63.178.178 as permitted sender)
smtp.mail=notification+o=96s009@facebookmail.com; dkim=pass header.i=@facebookmail.com
Return-Path: <notification+o=96s009@facebookmail.com>
DKIM-Signature: v=1; a=rsa-sha1; d=facebookmail.com; s=20100618; c=relaxed/relaxed;
    q=dns/txt; i=@facebookmail.com; t=1285495330;
    h=From:Subject:Date:To:MIME-Version:Content-Type;
    bh=2KbrCOfR4IrTDHbW+2ZA8IHGx1E=;
    b=SZ6eaGJUwdyeb21LhVaaKyFqB4j1hfV+qmiQ5A/1BUVPzb2hXV4vbrBxRc4Ooaeg
    D+SsZ/L4n7RJzvS3J3agPA==;
Received: from [10.18.255.124] ([10.18.255.124:54529] helo=mx-out.facebook.com)
    by mta010.sncl.facebook.com (envelope-from <notification+o=96s009@facebookmail.com>)
    (ecelerity 2.2.2.45 r(34067)) with ESMTP
    id 60/1C-22380-22A1F9C4; Sun, 26 Sep 2010 03:02:10 -0700
DKIM-Signature: v=1; a=rsa-sha1; d=facebookmail.com; s=201006181024; c=relaxed/relaxed;
    q=dns/txt; i=@facebookmail.com; t=1285495330;
    h=From:Subject:Date:To:MIME-Version:Content-Type;
    bh=2KbrCOfR4IrTDHbW+2ZA8IHGx1E=;
    b=X1m2y8je5LpOU/NOLVdvC6braEsbhYPbpHMPPr1GN83kwluMuLQ5uKaGvpeLulxeZ
    OiQ+PxinoZp8ETCd8hlezmN7FGgCPPy1VMc2Y61DyLpzle8sU9uzLNLziI8EZSHb
    8b4izvFUzqKUNVltafqFVuKot9FeizJi4ymDppfrvoU;
Received: from [10.32.174.117] ([10.32.174.117:58272])
    by mta026.sncl.facebook.com (envelope-from <notification+o=96s009@facebookmail.com>)
    (ecelerity 2.2.2.45 r(34222M)) with ECSTREAM
    id E9/E6-03488-22A1F9C4; Sun, 26 Sep 2010 03:02:10 -0700
X-Facebook: from zuckmail ([MTI3LjAuMC4x])
    by www.facebook.com with HTTP (ZuckMail);
Date: Sun, 26 Sep 2010 03:02:10 -0700
To: =?UTF-8?B?TWFfnZ2llIOiYk+Wlsw==?= <maggie4949@gmail.com>
From: Facebook <notification+o=96s009@facebookmail.com>
Reply-to: =?UTF-8?B?5Zue6KaG55WZ6KiA?=
<c+2lu3krg00000aacqwk0m001g2gg3hjhz000000ao4zn50000091ed9nr1ls1j@reply.facebook.com>
Subject: =?UTF-8?B?Q2hvaSBMaW5nIFRpbmct?
    =?UTF-8?B?5bCNIEVzdGhlciBldWkg55qE6Lr?
    =?UTF-8?B?5rOB5YGa5Ye65Zue5oeJ44CC?=
Message-ID: <51d1132ca669a2b9eee997aa004e8b01@www.facebook.com>
X-Priority: 3
X-Mailer: ZuckMail [version 1.00]

```



```
X-Facebook-Notify: feed_comment_reply; from=1327860409; uid=622052660; owner=645205361;
oid=146890245349367; mailid=309174fG2513c534G5cfd700G37
X-Facebook-PseudoCamp: 1
Errors-To: notification+o=96s009@facebookmail.com
X-FACEBOOK-PRIORITY: 0
MIME-Version: 1.0
Content-Transfer-Encoding: quoted-printable
Content-Type: text/plain; charset="UTF-8"
```

Figure 12: Email notification header

Alternatively, we could now obtain Facebook user's IP address by social engineering together with phishing URL through myiptest.com service. Firstly, go to <http://www.myiptest.com> and on the page "Get Someones IP" you will see:

- *Link for person* – the link that you need to give your friend.
- *Redirect URL*(optional) – the specified URL that your friend will be redirect to after clicking the above link.
- *Link for you* – the link that you can check if your friend has clicked your link.

Secondly, fill in the "Redirect URL" (whatever you want, e.g. LNK.IN or TinyURL). Thirdly, copy the URL from "Link for person" and send it to your friend via Facebook message or chat. Finally, follow the URL from "Link for you" and you will get your friend's IP after he or she clicks on your link. Since this trick requires the other person's cooperation, you need to become a friend with the person in Facebook in order to increase the chance of success.

4 Facebook Forensics in Virtual Environment

The goal of this study is to check whether footprints of Facebook activities could be discovered in virtual machine image as well. Here are the two types of virtual machine image files that could be examined:

- *.vmdk – virtual machine disk file
- *.vmem – virtual machine memory file or snapshot memory file

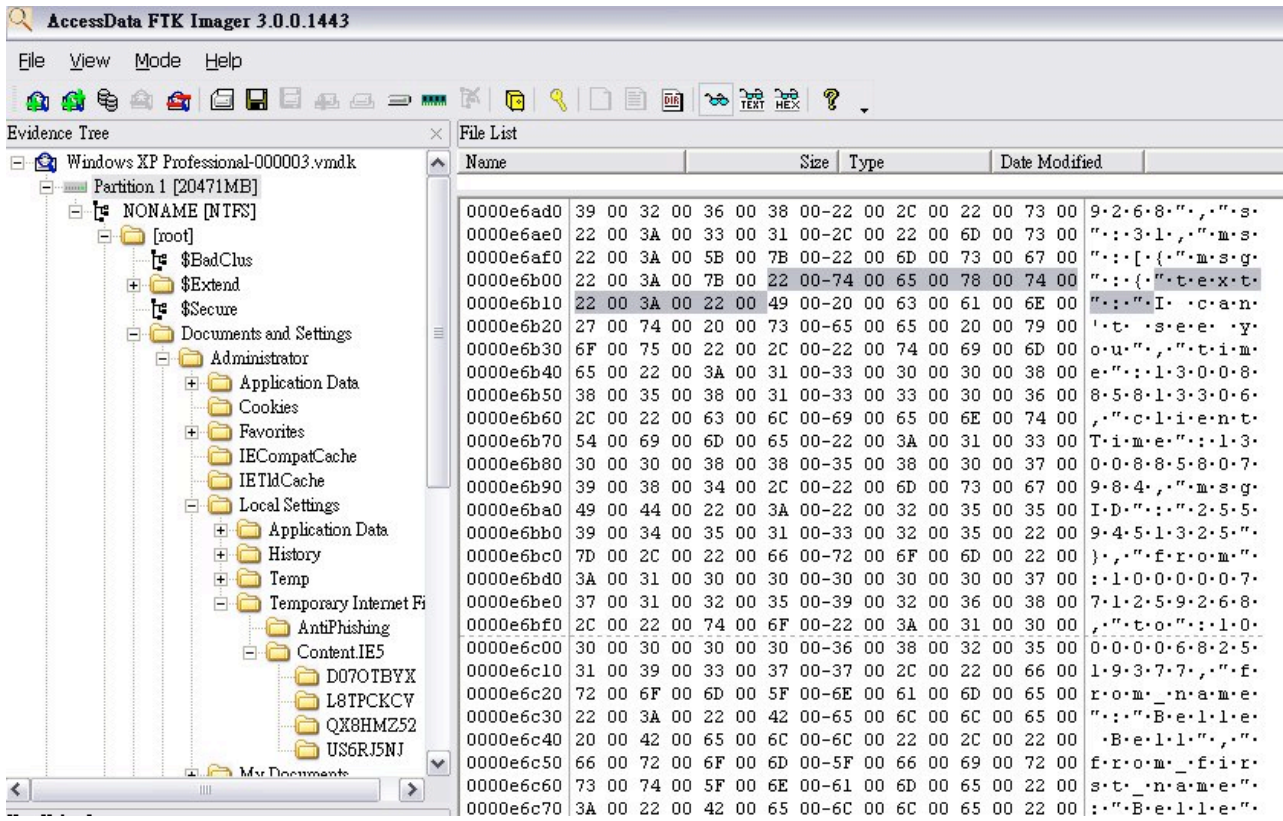
vmware	23/3/2011 21:35	文字文件	130 KB
Windows XP Professional	23/3/2011 21:35	VMware virtual machine BIOS	9 KB
Windows XP Professional	23/3/2011 21:35	VMware snapshot metadata	2 KB
Windows XP Professional	23/3/2011 21:35	VMware virtual machine configuration	3 KB
Windows XP Professional	23/3/2011 21:35	VMware suspended virtual machine state	136,570 KB
Windows XP Professional-000003	23/3/2011 21:32	VMware virtual disk file	6,464 KB
Windows XP Professional-Snapshot3.vmem	23/3/2011 21:32	VMEM 檔案	2,097,152...
Windows XP Professional-Snapshot3	23/3/2011 21:32	VMware virtual machine snapshot	136,570 KB
Windows XP Professional-000002	23/3/2011 21:30	VMware virtual disk file	4,190,144...
Windows XP Professional.vmem	23/3/2011 20:48	VMEM 檔案	2,097,152...
vmware-0	23/3/2011 17:09	文字文件	84 KB
vmware-1	23/3/2011 6:46	文字文件	169 KB
vmware-2	22/3/2011 21:44	文字文件	72 KB
Windows XP Professional	22/3/2011 21:16	VMware team member	2 KB
Windows XP Professional-Snapshot2.vmem	11/12/2009 0:52	VMEM 檔案	524,288 KB
Windows XP Professional-Snapshot2	11/12/2009 0:52	VMware virtual machine snapshot	136,072 KB
Windows XP Professional-000001	11/12/2009 0:51	VMware virtual disk file	3,268,288...
Windows XP Professional-Snapshot1.vmem	8/12/2009 16:26	VMEM 檔案	524,288 KB
Windows XP Professional-Snapshot1	8/12/2009 16:26	VMware virtual machine snapshot	133,827 KB
Windows XP Professional	8/12/2009 16:25	VMware virtual disk file	2,024,640...

Figure 17: Virtual machine image files

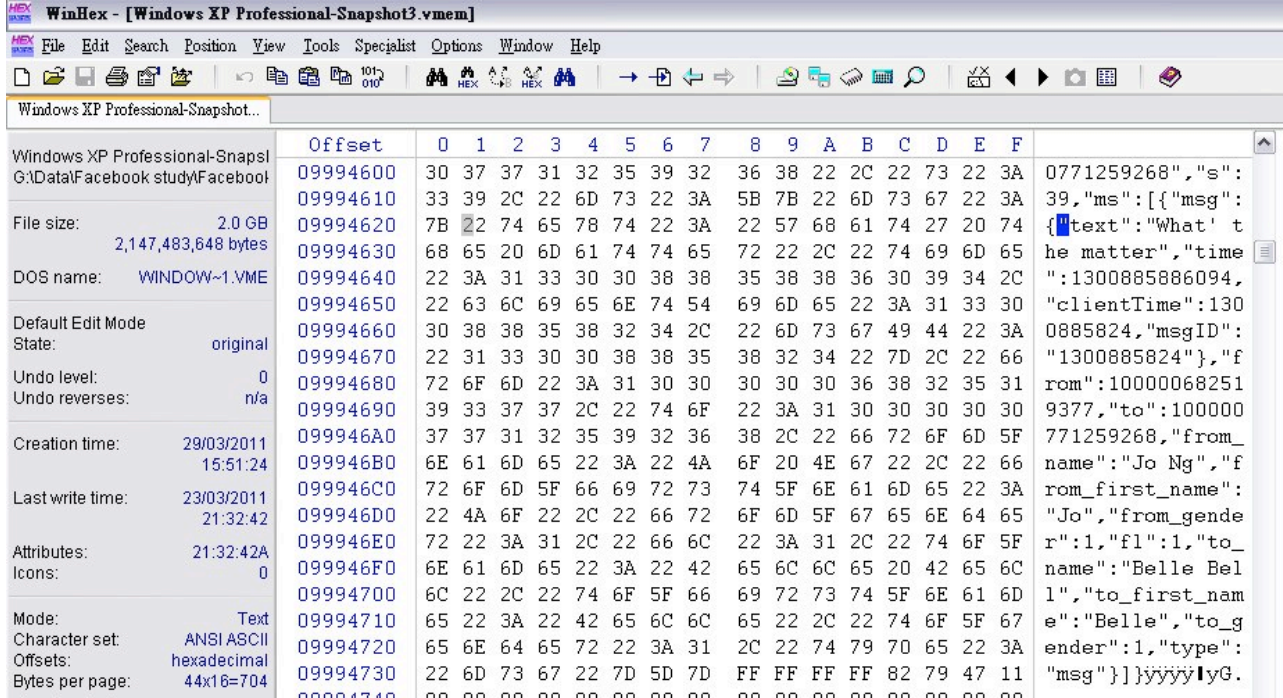
Firstly, we input some testing messages to Facebook chat in virtual environment. Secondly, we mounted the two types of virtual machine image files, which mentioned before, with FTK Imager v3. Thirdly, we take a string search of the JSON key `"text"` and the Facebook chat message we have typed into could be figured out.



(a)



(b)



(c)

Figure 18: Search of Facebook chat message by JSON key "text" from virtual machine image files.

From the above testing, we could discover the footprints of Facebook chat messages in virtual environment, and obtain the same evidence as physical machine successfully.

5 Facebook Forensics in Mobile Devices

iPhone and Android are the most popular smart phone in recent years and developers have been provided a large room to enhance their functionality. Facebook App is one of the most adopted application installed in such mobile devices, which could be downloaded from “iTunes Store” and “Android Market” free of charge. Therefore, it is worth to examine mobile devices for Facebook evidence.

5.1 iPhone

We have conducted the logical acquisition under testing environment:

- Hardware: iPhone 3GS (no jail-break)
- Operating System: iOS version 4.3
- File system: HFS+

However, we have not carried out the test for the iPhone which is jail-broken and physical acquisition of iPhone data.










Type	Name	Description
	com.facebook.Facebook	Path: c:\private\var\mobile\Applications\com.facebook.Facebook\ Name: com.facebook.Facebook
	Library	Path: c:\private\var\mobile\Applications\com.facebook.Facebook\Library\
	Cookies	Path: c:\private\var\mobile\Applications\com.facebook.Facebook\Library\Cookies\
	Cookies.plist	Path: c:\private\var\mobile\Applications\com.facebook.Facebook\Library\Cookies\Cookies.plist
	Cookies.binarycookies	Path: c:\private\var\mobile\Applications\com.facebook.Facebook\Library\Cookies\Cookies.binarycookies
	Preferences	Path: c:\private\var\mobile\Applications\com.facebook.Facebook\Library\Preferences\
	com.facebook.Facebook.plist	Path: c:\private\var\mobile\Applications\com.facebook.Facebook\Library\Preferences\com.facebook.Facebook.plist Name: com.facebook.Facebook.plist
	Documents	Path: c:\private\var\mobile\Applications\com.facebook.Facebook\Documents\
	friends.db	Path: c:\private\var\mobile\Applications\com.facebook.Facebook\Documents\friends.db

Figure 19: Files bundled in Facebook App could be extracted by Oxygen and XRY.

From Figure 19, here are the files to be examined:

- com.facebook.Facebook.plist – property list of Facebook App login users
- friends.db – SQLite database of buddy list chatting in chat room
- dynamic-text.dat – keyboard cache of iPhone, like a keylogger
- iPhone backup files in iTunes installation folder of a personal computer


```

    <key>pic_square</key>
    <string>http://static.ak.fbcdn.net/rsrc.php/vl/y9/r/IB7N0FmPw2a.gif</string>
  </dict>
</dict>
<key>100001149375085</key>
<dict>
  <key>100001149375085</key>
  <dict>
    <key>admin</key>
    <false/>
    <key>af</key>
    <false/>
    <key>cs</key>
    <true/>
    <key>is_page</key>
    <false/>
    <key>name</key>
    <string>Kelvin Captain</string>
    <key>pic</key>
    <string>http://static.ak.fbcdn.net/rsrc.php/vl/yh/r/C5yt7Cqf3zU.jpg</string>
    <key>pic_square</key>
    <string>http://static.ak.fbcdn.net/rsrc.php/vl/yo/r/UlIqmHJn-SK.gif</string>
  </dict>
</dict>
<key>622052660</key>
<dict>
  <key>622052660</key>
  <dict>
    <key>admin</key>
    <false/>

```

Figure 20: Contents of com.facebook.facebook.plist file.

letter	uid	first_name	last_name	name	pic_square	phone	cell	email
1	L	622052660	Maggie	Lam	Maggie Lam	http://profile.ak.		
2	L	100001013358449	Sandy	Lam	Sandy Lam	http://profile.ak.		fb6bd158c1f2364d56cfdcf08e33a2a3ba2bf5edcaac1f47f1ecf7a7062e7de
3	O	100000508695932	Ingrid	Oct	Ingrid Oct	http://profile.ak.		
4	B	100000771259268	Belle	Bell	Belle Bell	http://static.ak.fl		2b543a372fe4dd518caab19cca0c2dc1b52b66dd0f4fb20a28026fd6e02a75ad

Figure 21: Data in friends.db file.

```

dynamic-text.dat
5 7 8 9 A B C D E F
5 00 53 61 74 75 72 64 61 79 el.Date.Saturday
3 72 73 00 61 6D 00 69 6E 00 .Time.hrs.am.in.
3 65 6E 00 77 69 6C 6C 00 79 room.When.will.y
3 76 65 00 4E 6F 65 6C 00 42 ou.arrive.Noel.B
5 6C 6C 00 43 68 61 74 00 63 elle.bell.Chat.c
3 6E 65 73 65 00 73 68 61 72 hat.chinese.shar
3 79 6F 75 00 66 6F 75 6E 64 e.Have.you.found
3 79 6F 75 00 70 69 63 6B 00 .it.If.you.pick.
5 00 79 6F 75 00 6D 6F 6E 65 it.give.you.mone
7 6F 76 00 6D 61 70 00 67 6F y.www.gov.map.go
3 6F 6D 00 43 61 70 74 61 69 v.LAN.com.Captai
7 72 65 6E 73 69 63 73 00 74 n.vm.forensics.t
4 65 72 00 75 73 69 6E 67 00 he.matter.using.
5 00 74 68 65 00 72 65 73 75 see.see.the.resu
3 79 6F 75 00 74 61 6C 6B 69 lt.are.you.talki
3 00 00 00 DD 22 67 6D 61 69 ng.....Y"gmai
3 53 49 00 02 77 61 70 00 01 l..GBSCSI..wap..
3 01 77 6F 6D 61 63 68 00 01 wonhot..womach..
3 63 63 77 6D 6F 62 69 6C 65 wsgt..pccwmobile
1 6F 70 65 72 00 01 50 6F 6C ..nw..noner..Pol

```

Figure 22: Search from dynamic-text.dat file.

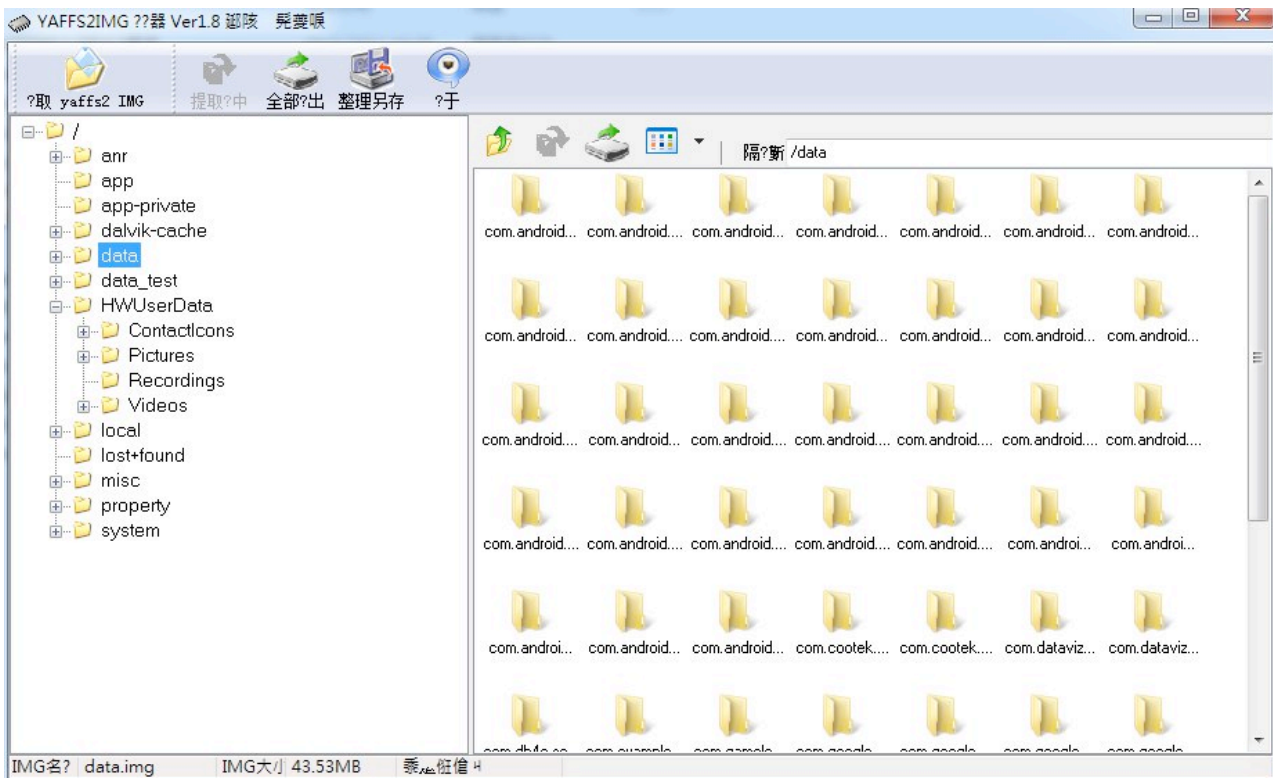


Figure 24: Android system and data files opened with YAFFS2IMG browser.

Name	Object	Type	Schema
albums	table	table	CREATE TABLE albums (_id INTEGER PRIMARY KEY,aid ...
android_metadata	table	table	CREATE TABLE android_metadata (locale TEXT)
chatconversations	table	table	CREATE TABLE chatconversations (_id INTEGER PRIMAR...
chatmessages	table	table	CREATE TABLE chatmessages (_id INTEGER PRIMARY KE...
default_user_images	table	table	CREATE TABLE default_user_images (_id INTEGER PRIMA...
events	table	table	CREATE TABLE events (_id INTEGER PRIMARY KEY,even...
friends	table	table	CREATE TABLE friends (_id INTEGER PRIMARY KEY,user...
info_contacts	table	table	CREATE TABLE info_contacts (_id INTEGER PRIMARY KE...
key_value	table	table	CREATE TABLE key_value (_id INTEGER PRIMARY KEY,...
mailbox_messages	table	table	CREATE TABLE mailbox_messages (_id INTEGER PRIMAR...
mailbox_profiles	table	table	CREATE TABLE mailbox_profiles (_id INTEGER PRIMARY...
mailbox_threads	table	table	CREATE TABLE mailbox_threads (_id INTEGER PRIMARY ...
notifications	table	table	CREATE TABLE notifications (_id INTEGER PRIMARY KE...
perf_sessions	table	table	CREATE TABLE perf_sessions (_id INTEGER PRIMARY KE...
photos	table	table	CREATE TABLE photos (_id INTEGER PRIMARY KEY,pid ...
search_results	table	table	CREATE TABLE search_results (_id INTEGER PRIMARY K...
stream_photos	table	table	CREATE TABLE stream_photos (_id INTEGER PRIMARY K...
user_statuses	table	table	CREATE TABLE user_statuses (_id INTEGER PRIMARY KE...
user_values	table	table	CREATE TABLE user_values (_id INTEGER PRIMARY KEY...
CHAT_INDEX	index	index	CREATE INDEX CHAT_INDEX ON chatmessages (friend_uid)
mailbox_profiles_id	index	index	CREATE INDEX mailbox_profiles_id ON mailbox_profiles(id)
mailbox_threads_tid	index	index	CREATE INDEX mailbox_threads_tid ON mailbox_threads(tid)
sqlite_autoindex_key_value_1	index	index	

Figure 25: User information in Facebook App *.db files opened with SQLite Database Browser

We could discover more information from Android device with correlated Gmail account for further investigation.

6 Conclusions

Facebook core is a social graph, with objects such as people, photos and events, as well as connections between them such as friend relationships, shared content and photo tags [15]. Properties of objects can be accessed by sending HTTP requests to Facebook Graph API and all responses are JSON objects. Since these objects could be displayed on a web browser, they need to be converted to HTML format with additional layout information. Therefore, Facebook comments and chats identified could be in JSON or HTML formats with the same key `"text"`. Although these formats might be too simple which could be used by other applications as well, further signatures might be able to assist uniquely identifying that the footprint is coming from Facebook but not elsewhere. Of course, this might also increase the footprint's false negative rate.

Moreover, we could identify most of the legitimate Facebook footprints from RAM or browser cache file for several common Facebook activities such as comments, events and chats. These footprints include Facebook user profile ID, the message contents and corresponding timestamps. Same results could also be found in virtual machine image files. In addition, footprints of Facebook activities could be matched in some data files bundled with Facebook App for mobile devices. However, further investigation is required to verify whether the genuine account owner is involved in the case.

Finally, we have used various handy forensics tools to extract the Facebook messages from various platforms, virtual machines and mobile devices, which are relevant to forensics practitioners as well examiners. Hopefully, the research findings could be contributed to them as a valuable reference.

References

- [1] Eric Eldon, 2008 Growth Puts Facebook In Better Position to Make Money, *VentureBeat (San Francisco)*, 18 December 2008.
- [2] Facebook – Info, Facebook Inc., retrieved 15 June 2011, available at <http://www.facebook.com/facebook?sk=info>
- [3] Nicholas Carlson, At Last – The Full Story Of How Facebook Was Founded, *Business Insider*, 5 March 2010.
- [4] Nicholas Carlson, Goldman to clients: Facebook has 600 million users, *MSNBC*, 5 January 2011.
- [5] Nicholas Carlson, Facebook Has More Than 600 Million Users, Goldman Tells Clients, *Business Insider*, 5 January 2011.
- [6] Jeffrey Fox, Five million Facebook users are 10 or younger, *ConsumerReports.org*, 10 May 2011.
- [7] Internet Evidence Finder v4 – Standard Edition, JADsoftware Inc., retrieved 20 June 2011, available at http://www.jadsoftware.com/go/?page_id=141
- [8] Facebook JPG Finder v1.2.1, JADsoftware Inc., retrieved 20 June 2011, available at http://www.jadsoftware.com/go/?page_id=176
- [9] CacheBack – Introduction, SiQuest Corp., retrieved 20 June 2011, available at <http://cacheback.ca/default.asp?tabno=1>
- [10] Cyber Security & Computer Forensics Software, e-fense, retrieved 20 June 2011, available at <https://www.e-fense.com/products.php>
- [11] MoonSols Windows Memory Toolkit, MoonSols, retrieved 20 June 2011, available at <http://www.moonsols.com/windows-memory-toolkit/>
- [12] FTK Data Sheet, AccessData, retrieved 20 June 2011, available at http://accessdata.com/downloads/media/FTK_DataSheet.pdf
- [13] What is XRY, Micro Systemation, retrieved 20 June 2011, available at <http://www.msab.com/xry/what-is-xry>
- [14] Oxygen Forensic Suite 2011, Oxygen Software Co., retrieved 20 June 2011, available at <http://www.oxygen-forensic.com/en/>
- [15] Graph API – Facebook Developers, Facebook Inc., retrieved 20 June 2011, available at <http://developers.facebook.com/docs/reference/api/>

Who am I?

Valkyrie-X Security Research Group (VXRL) focuses on offensive security research, threat and malware analysis, reverse engineering and forensics studies.