

Facebook Forensics in Different Systems

EN 650.757.01 Advanced Computer Forensics

Ruiyang Liu

Abstract	2
1 Introduction	3
1.1 Research Background	3
1.2 Research Aims and Methods	3
1.3 Research Forensics Tools	5
2 Facebook Protocol Format in Browser Cache	6
3 Facebook Forensics on Linux VM	10
Facebook Evidence in Linux Virtual Disk Snapshot File (.vdi)	10
Facebook Evidence in Linux Memory Dump file (.sav)	12
4 Facebook Forensics on Android VM	17
Facebook Evidence in Android Virtual Disk Snapshot File (.vdi)	18
Facebook Evidence in Android Memory Dump file (.sav)	22
5 Facebook Forensics on Windows 7 VM	29
Facebook Evidence in Windows7 Virtual Disk Snapshot File (.vdi)	29
Facebook Evidence in Win7 Memory Dump file (.sav)	30
6 Conclusion	33
7 Future Work	36

Abstract

Facebook, was founded in 2004 by Mark Zuckerberg, and over 1.62 billion users visited Facebook daily in 2019. The research focuses on the differences in forensics against Facebook under different systems. The study of Facebook forensics includes user information, chat function, post and comment function. In this paper, we will introduce the forensic tools used to make Facebook forensic snapshot disk file and memory dump process, as well as the forensic process and methods. We will also compare the similarities and differences of disk file and memory dump of three different systems in the above three main information forensics.

1 Introduction

1.1 Research Background

Facebook, was founded in 2004 by Mark Zuckerberg while he was studying at Harvard, is operated and managed by Facebook Inc. now.¹ Over 1.62 billion users visited Facebook daily in 2019.² The sheer online ubiquity of Facebook is astounding. As of February 2012, Facebook had over 845 million users (more than the population of Europe) who spent more than 9.7 billion minutes per day on the site. Users share four billion pieces of content per day, including uploads of 250 million photos, and Facebook is now integrated with over seven million websites and applications. Most of the Facebook users join groups and making post. These group posts may contain illegitimate information and being harmful to other users. What's more, among 12- to 17-year old teen, approximately 40% of them are using Facebook. With so many people using Facebook, criminals may easily hide their real identity. The study of Facebook forensics can help reduce information leakage, online crime, etc.

1.2 Research Aims and Methods

The research will analyze and study facebook forensic evidence on three different systems: Linux, Windows 7 and Android mobile. The research will analyze and study facebook forensic evidence on three different systems: Linux OS, Windows 7 OS and Android OS. Experiment environment should be set up properly, which is foundation to start the research. Our

¹ Phillips, Sarah. "A Brief History of Facebook." The Guardian, Guardian News and Media, 25 July 2007, www.theguardian.com/technology/2007/jul/25/media.newmedia

² Aboulhosn, Sarah. "18 Facebook Statistics Every Marketer Should Know in 2020." Sprout Social, 21 Jan. 2020, www.sproutsocial.com/insights/facebook-stats-for-marketers/

investigation in this experiment has started the moment we installed the applications or browsed the Facebook web on the systems. We have also created two dummy accounts for the experiments(main account *Ruiyang Liu* and helper account *Rayon Liu*). All detail steps, credentials and communication activities were properly documented. After all the prerequisite are well managed, being able to know what kinds of the Facebook activities and evidences existed are the key to start the forensic progress. After snapshotted the VMs, we can get the virtual disk files whose extensions are .vdi., and the dumps of volatile state information whose extensions are .sav. The analysis were conducted manually by searching several keyword related to experiment in forensically sounds manner. Finally, using image reader to access and analyze the dumps is the research final aim.

This research project identifies the following Facebook activity footprints:

- 1) Facebook login and account information
- 2) Facebook friends information
- 3) Facebook chatting
- 4) Facebook post and reply to the post

This research includes facebook memory footprints searching and extracting:

- 1) Web browser cache file
- 2) Linux OS dump
- 3) Windows 7 OS dump
- 4) Android OS dump

1.3 Research Forensics Tools

This research used the following software or forensic tools:

- 1) Hxd Hex Editor: Hxd Hex Editor is a multi-functional hexadecimal editor viewer. It also supports binary file viewing. Editing and creating ASCII, hexadecimal, decimal, float, double and binary data is also supported. Besides, researchers can make file patches, searching and replacing code through Hxd Hex Editor.
- 2) Virtual Box Windows 7 Virtual Machine: Windows 7 is one of the most famous operating system developed by Microsoft. Considering that there will be interference from other software when running this research directly on the PC, an absolutely new Windows 7 virtual machine is used for the experiment.
- 3) ChromeCacheView: ChromeCacheView is a cache data cloning tool that can copy the data you cached on your browser to a specified folder and save it. ChromeCacheView can intercept all cached data on the Chrome browser, including information such as access address, content, and timestamps. In this research, using ChromeCacheView to analyze the Facebook web forensic evidence on Windows 11 computer.
- 4) FTK imager: FTK® Imager is a data preview and imaging tool that lets you quickly assess electronic evidence to determine if further analysis with a forensic tool such as Forensic Toolkit (FTK®) is warranted. In this research, we use both Hxd Hex Editor and FTK imager to gather information of the dumps. However, I suggest to use HxdHexEditor as the primary tool, since it process lookups quicker.
- 5) Virtual Box Linux Virtual Machine: Linux is a family of open-source Unix-like operating systems based on the Linux kernel, an operating system kernel first released on September 17,

1991, by Linus Torvalds. Linux is one of the most prominent examples of free and open-source software collaboration.

6) Virtual Box Android 9.0 Virtual Machine: Android is a mobile OS based on a modified version of the Linux kernel and other open source software, designed primarily for mobile devices. Android is developed by a consortium of developers known as the Open Handset Alliance and commercially sponsored by Google. Analyzing Facebook evidence on Android OS system is critical because most Facebook users chat and post using their mobile phone.

7) Plist Editor: Plist Editor, is a file editing tool that helps users edit Plist files, can run under the Windows7 OS. The Plist Editor can edit Plist files in XML format and binary format, and supports color-coding, replacement, and undo of the code in the file.

2 Facebook Protocol Format in Browser Cache

Before locating any Facebook evidence on VMs, we need to know the format of Facebook protocol that may appear in VM dumps or browser cache. Therefore, we attempted to identify the protocol format of Facebook post, comment, message and chat located in Windows 11 machine browser cache. In the following analysis, two Facebook accounts have been set up for performing Facebook activities. 1094635582@qq.com (User name *Ruiyang Liu*) is the tester account responsible for wall posting, commenting, messaging and chatting on his own, and testfbforensic@yahoo.com(User name *Rayon Liu*) is the helper account responsible for replying to the post and chatting with the tester. Snapshots and dumps of tester's virtual machine status was taken after finishing any Facebook activities. The whole acquisition process was repeated

twice for consistency concern. All files and information in this part is gathered through ChromeCacheView.

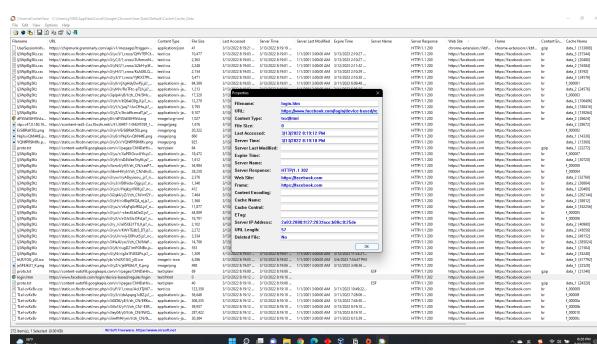
Prerequisite:

- Windows PC or VM
- Chrome Web Browse
- ChromeCacheView V2.00

Research Steps: (Recommended to clear browser cache each time you do operation.)

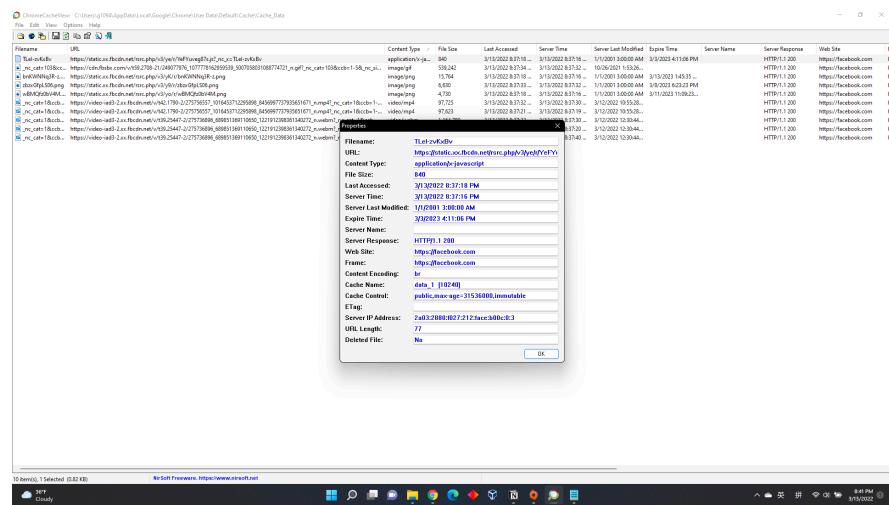
- i. Open Chrome Web Browser and surf www.facebook.com
- ii. Enter your facebook username and password to login
- iii. Send a chatting message to your facebook friend
- iv. Post something and reply
- v. Turn on the ChromeCacheView to check the Chrome cache

When we login to Facebook in Chrome, we are able to get login.html. By checking the web browser cache, we can find out all the login or logout activity details, including timestamps and server IP address.



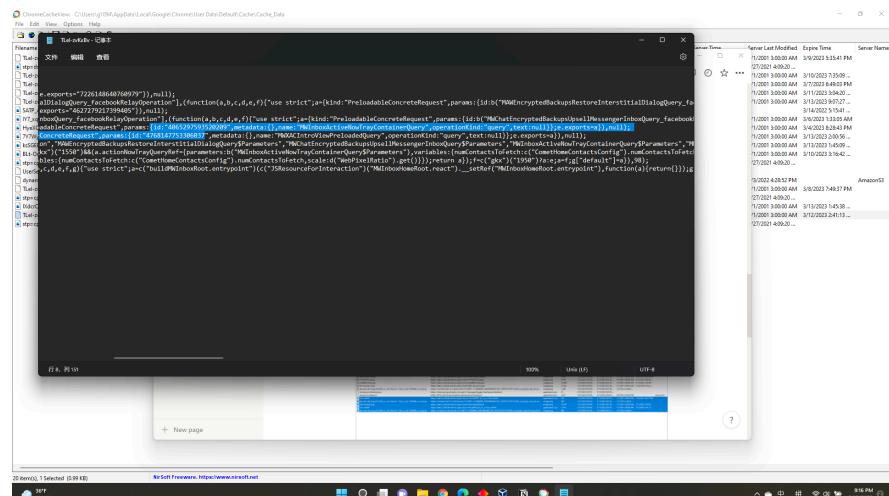
Login info in chrome cache

Next, we send messages to Facebook friends. We are able to get accountID when we look at the cache packets.



Wireshark (1 item) Selected (0.82 KB) Wi-Fi Frequency: https://www.facebook.com

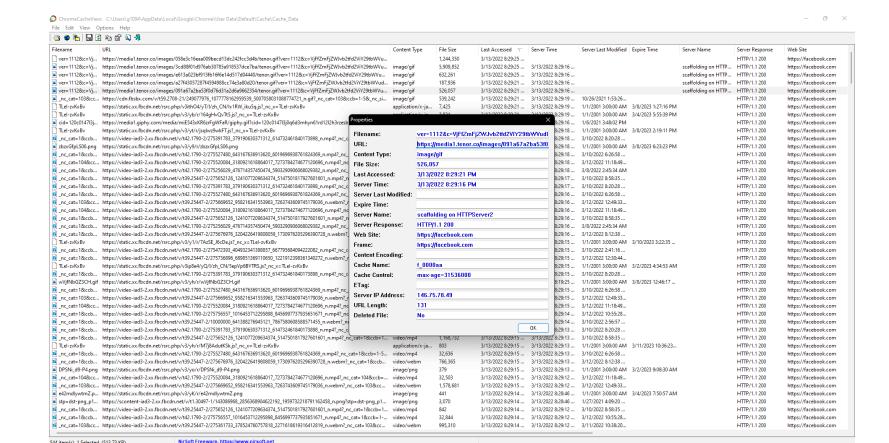
Chat Packet in Chrome Cache



Wireshark (1 item) Selected (0.89 KB) Wi-Fi Frequency: https://www.facebook.com

Chat Packet detail

Further, when we send memes to Facebook friends, we can get the meme image url in the cache.

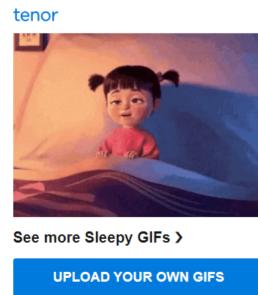
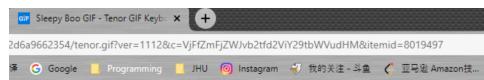


Wireshark (1 item) Selected (0.89 KB) Wi-Fi Frequency: https://www.facebook.com

Chat Gif Meme packet



Chat meme in FB

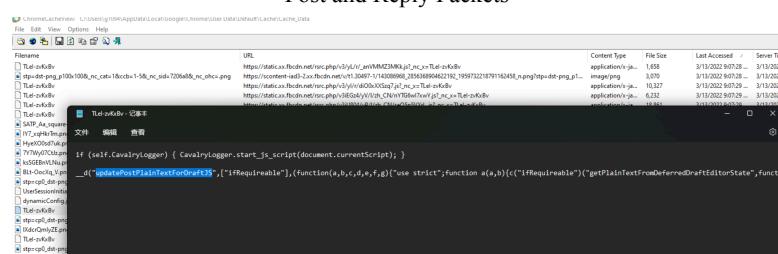


Cache Packet URL corresponds

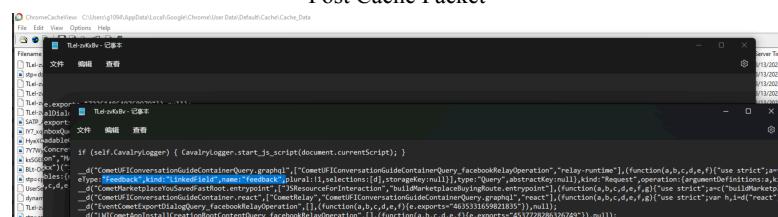
Finally, the test account post something, and the helper account reply to the post. In the cache packets, we are able to see the post and reply activities.

Tlei-zvKbV						
https://cp0_dst-png_p32x32_nc_cat18ccb1-58_nc_sid=7206a8_nc_oh.png	https://scontent.xx.fbcdn.net/rsrc.php/v3/y/n/ivmxFXZP_jjt_mc_x-Tlei-zvKbV	application/x-javascript	244	3/13/2022 9:07:40...	3/13/2022 9:07:38...	1/1/2001 3:00:00 AM 3/20/2023 7:49:37 PM
!ldcrOnlyZE.png	https://scontent.xx.fbcdn.net/v/11.30497-1/14308968_2856368904622192_1959732218791162450_n.jpg?tp=cp0_dst-pn...	image/png	848	3/13/2022 9:07:40...	3/13/2022 9:07:38...	1/2/2021 4:09:20...
Tlei-zvKbV	https://static.xx.fbcdn.net/rsrc.php/v3/y/ldcrOnlyZE.png	image/png	10,247	3/13/2022 9:07:40...	3/13/2022 9:07:38...	1/1/2001 3:00:00 AM 3/13/2022 1:45:38...
https://cp0_dst-png_p32x32_nc_cat18ccb1-58_nc_sid=7206a8_nc_oh.png	https://scontent.xx.fbcdn.net/v/11.30497-1/14308968_2856368904622192_1959732218791162450_n.jpg?tp=cp0_dst-png_p32x3...	image/png	1,014	3/13/2022 9:07:43...	3/13/2022 9:07:42...	1/1/2001 3:00:00 AM 3/12/2023 2:41:13...
			848	3/13/2022 9:07:53...	3/13/2022 9:07:51...	1/2/2021 4:09:20...

Post and Reply Packets



Post Cache Packet



Reply(Feedback) Cache Packet

3 Facebook Forensics on Linux VM

Prerequisite:

- Linux VM in Virtual Box
- Hxd Hex Editor
- FTK Imager (Optional)
- Chrome Web Browser in the VM

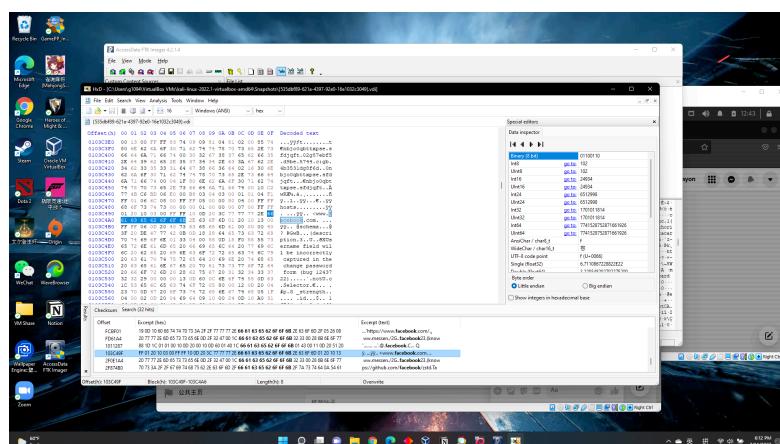
VM Dump Creation Steps:

- I. Set up a Linux VM and then install Chrome in the VM
- II. Open Chrome Web Browser and surf www.facebook.com
- III. Enter your facebook username and password to login
- IV. Send a chatting message to one of your facebook friends
- V. Post a feed and reply to itself, reply to helper account's post, and helper reply to tester's post.

Facebook Evidence in Linux Virtual Disk Snapshot File (.vdi)

The analysis were conducted manually by searching several keyword.

First, we search for keyword *Facebook* and Facebook URL. We can see multiple results and their excerpt(hex) is the same.



Searching *Facebook* keyword found in Linux vdi file

Secondly, we search for Facebook URL (www.facebook.com). And we can see the information about I changed the password for my test account.

Offset	Excerpt (Hex)	Excerpt (text)
S80257	32 30 30 36 33 30 33 34 2C 31 2C 30 2C 32 0E 77 77 77 2E 66 61 63 65 62 6F 6B 2E 63 6F 6D	20066102.0 www.facebook.com
S8EC27	25 22 39 34 7C 6E 3A 79 34 0A 68 74 70 73 34 77 77 77 2E 66 61 63 65 62 6F 6B 2E 63 6F 6D	2099141.0 https://www.facebook.com
S8EC77	33 09 30 00 31 39 30 35 09 58 74 70 73 34 77 77 77 2E 66 61 63 65 62 6F 6B 2E 63 6F 6D	3.0.19065.https://www.facebook.com
S8EC9C	61 63 65 62 6F 6F 6B 2E 63 6F 6D 34 33 3A 77 77 77 2E 66 61 63 65 62 6F 6B 2E 63 6F 6D	facebook.com:443/www.facebook.com
FCBEFD	01 13 04 00 19 0D 10 0E 68 74 70 73 3A 2F 77 77 77 2E 66 61 63 65 62 6F 6B 2E 63 6F 6D	...https://www.facebook.com
103C49B	00 07 00 FF FF 01 20 10 03 00 FF 10 10 00 20 3C 77 77 77 2E 66 61 63 65 62 6F 6B 2E 63 6F 6D	->www.facebook.com

Searching *Facebook URL* keyword found in Linux vdi file

The third search were to find our profile name or user ID once we logged into the social media. Profile name is different with username. Username used to login into the social media while profile name were the name displayed in our social media account. When I want to search *Liu* as my last name of my Facebook username or Ruiyang as my first name of my Facebook username, I get nothing in Virtual disk snapshot file. As a result, you cannot find Facebook username in VM .vdi.

The Fourth search were to find our login email information. The keyword I choose to search my login email is the partial email. To be more specific, my test account is 1094635582@qq.com, I try to search *1094* or *qq.com*. But we also cannot get any login email information in Virtual disk snapshot file.

The fifth search is the friend's account name and our chatting message. I tried to search *text* or specific chat message like *te3xt*. We still cannot find any information.



Facebook Chat message on Linux VM

The screenshot shows the HxD Hex Editor interface. The main window displays a memory dump with columns for Offset(h), Decoded text, and raw hex values. A context menu is open over the text area, with 'Information' selected. A modal dialog titled 'Information' shows an error message: 'Can't find 'te3xt''. The 'OK' button is visible at the bottom right of the dialog.

Searching *text_message* keyword not found in Linux vdi file

Facebook Evidence in Linux Memory Dump file (.sav)

User, Login and Friend Evidence in Linux Memory Dump

We use the same steps and keywords as previously done in Linux virtual disk snapshot file.

First, we search my account name, and we can get UserID information and my username.

Searching username keyword and find userID in Linux memory dump

Also, as we search the key word of the username, we can find Facebook login information. The login information includes username and the login time.

Searching username and get login info in Linux memory dump

Second, we try to find more user information by searching login email. It is certain that this email address is the Facebook information, since this email address is the unique email for Facebook account. Though we are able to find login email in the memory, we cannot find other information through this evidence.

Searching login email in Linux memory dump

Third, we use Facebook friend's username keyword. In Linux, we found facebook friend URL, i.e. php website link. And also, we can find friend userID using friend's username as keyword.

Searching friend username in Linux memory dump

Offset(h)	00	01	02	03	04	05	06	07	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	Decoded text	
25DAE6B8	7B	ED	02	28	11	22	72	75	56	E7	57	74	68	50	72	69	6F	28	33	01	01	EA	06	29	1A	..,RunWithPriority(3A,&_			
25DAE6B4	7B	28	65	65	77	20	42	02	28	29	A0	F8	30	05	43	73	75	74	6F	6D	00	07	09	28	1B	(new_A,"0"),0xCustoma_8A			
25DAEAO0	E0	09	67	02	22	78	22	40	D8	07	22	3A	5B	52	22	65	6C	61	70	59	72	65	66	74	70	C_A..0,_e_0,[{"RelayPrefet_8A			
25DAEBC0	65	74	73	65	61	63	43	20	C2	05	62	20	08	61	20	10	02	22	5B	5D	2C	5B	22	61	64	5_A..0,_e_0,[{"RelayPrefet_8A			
25DAEBD0	70	5F	20	26	03	73	65	63	65	53	74	61	75	73	50	72	76	69	21	86	03	53	72	67	63	5_A..0,_e_0,[{"RelayPrefet_8A			
25DAEF4	63	79	60	41	87	05	43	6F	6D	78	67	21	3F	04	51	75	65	75	72	75	CB	50	41	8F	74	65	72	73	5_A..0,_e_0,[{"RelayPrefet_8A
25DAFB10	F5	36	32	36	37	30	34	35	63	31	38	31	39	37	37	30	36	34	33	22	24	21	20	19	21	20	19	5_A..0,_e_0,[{"RelayPrefet_8A	
25DAFB2C	5F	56	62	62	6F	78	22	3A	7B	22	63	40	41	02	6C	65	74	70	9C	04	72	75	65	2C	20	AB	03	5_A..0,_e_0,[{"RelayPrefet_8A	
25DAFB48	73	65	74	19	03	64	61	74	61	40	07	03	76	65	77	21	81	40	2B	04	68	61	74	5F	73	5_A..0,_e_0,[{"RelayPrefet_8A			
25DAFB40	20	83	04	62	61	72	5F	63	21	B8	06	81	63	74	5F	72	61	6E	69	66	67	73	20	DD	7B	22	5_A..0,_e_0,[{"RelayPrefet_8A		
25DAFB80	73	60	A9	1F	22	3A	32	20	22	62	75	64	79	5F	64	22	32	31	30	30	37	39	35	30	31	30	30	31	5_A..0,_e_0,[{"RelayPrefet_8A
25DAFB9C	37	35	32	31	31	38	39	20	E8	01	75	73	80	51	E0	0E	12	02	5F	69	4F	0E	02	66	69	6C	20	5_A..0,_e_0,[{"RelayPrefet_8A	
25DAFB80	97	01	22	55	40	24	02	22	6E	61	6D	40	0D	00	H6	75	20	52	61	79	67	6F	20	12	21	17	22	5_A..0,_e_0,[{"RelayPrefet_8A	
25DAFB04	07	77	59	62	75	63	65	68	B0	03	6E	64	65	69	45	20	7D	28	8A	58	0C	38	30	35	38	27	5_A..0,_e_0,[{"RelayPrefet_8A		
25DAFB00	30	32	34	31	33	36	31	30	33	03	66	69	72	73	20	C3	04	74	36	73	74	6F	57	63	69	65	68	5_A..0,_e_0,[{"RelayPrefet_8A	
25DACC0C	77	22	3A	6E	75	60	5C	70	5D	7D	22	22	70	72	62	07	5F	69	63	75	74	72	20	DC	04	78	5_A..0,_e_0,[{"RelayPrefet_8A		
25DACC08	22	72	65	20	20	0A	69	68	74	73	3A	5C	2F	2C	73	74	6F	21	6F	1D	2F	65	61	64	33	5_A..0,_e_0,[{"RelayPrefet_8A			
25DACC04	23	31	2E	78	28	66	62	63	64	66	2E	65	75	5C	2F	76	56	27	74	31	2E	33	30	34	39	18	5_A..0,_e_0,[{"RelayPrefet_8A		
25DACC0C	5D	30	5C	2F	74	34	34	33	30	38	34	35	30	34	35	30	34	35	34	34	24	31	39	18	5_A..0,_e_0,[{"RelayPrefet_8A				
25DACC07C	31	38	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	5_A..0,_e_0,[{"RelayPrefet_8A	
25DACC08	67	3F	73	74	09	70	5D	70	30	32	74	73	4D	22	0F	18	5F	70	34	70	75	4C	36	56	27	5F	65	5_A..0,_e_0,[{"RelayPrefet_8A	
25DACC04	63	63	61	74	3D	31	24	63	63	62	3D	31	2D	35	60	11	21	08	06	37	32	30	36	31	60	18	5_A..0,_e_0,[{"RelayPrefet_8A		
25DACC0D0	0E	16	6F	63	63	3D	38	57	6F	54	78	70	38	47	37	77	41	5D	42	44	49	39	42	60	1B	5_A..0,_e_0,[{"RelayPrefet_8A			
25DACC0E	68	74	3D	09	00	BC	1F	2E	6F	68	3D	30	35	57	41	54	52	37	65	70	56	64	52	74	6C	64	5_A..0,_e_0,[{"RelayPrefet_8A		
25DACL08	30	34	68	70	4C	45	6A	30	73	4A	61	17	5F	73	76	49	70	43	47	51	67	44	58	4D	2B	68	40	4pLEdEsJa_svlpTCSzQgnRM-1	

Searching friend username and find his userID in Linux memory dump

Chat Evidence in Linux Memory Dump

Forth, the main Facebook account *Ruiyang* chat with the helper account Liu Rayon, and following is the screenshot of our chat.



Screenshot of chatting in Linux

In the ram reader, we search chatting keywords, such as *good noon*, *te3st*, etc. In the Linux memory dump, I find multiple evidences. They appear multiple times but I don't know the reason why. This might be my gap research regarding them appearing so much times. Following is the result of the search of chatting evidence.

Evidence1 of chatting in Linux Memory dump

Evidence 2 of chatting in Linux Memory dump

Post and Comment Evidence in Linux Memory Dump

There are some elements to take into account. First, we are trying to find evidence of a post. But if the user did not post on this Linux virtual machine, can we find evidence in the Linux Memory dump. Secondly, whether the results of the forensic evidence will be different if the user comments under his own post and under someone else's post.

In the first step, I started by posting on a Linux virtual machine and commenting on my post.



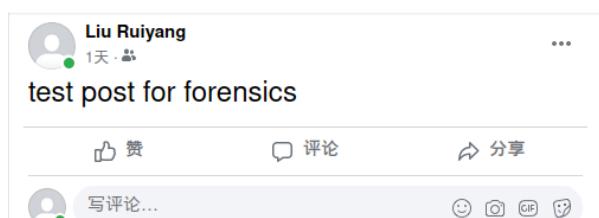
Post and comment to myself in Linux VM

By searching the keyword, we are able to find both posting evidence and comment evidence as following.

Posting evidence in Linux Memory Dump

Comment(Feedback) evidence in Linux Memory Dump

To check the whether we can get forensic evidence from posting in other devices. We first post something from my Windows local machine, as following.



Posting from Windows local machine

I tried multiple keywords to find this post, but there's nothing in the Linux memory dump. As result, when you post from other devices, you cannot find forensic evidence in the RAM.

Second, We use helper account to post and the main account reply the post as following.



Then, we search the comment keyword try to find evidence in the Linux memory. And we can find some evidence.

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B Decoded text
2CAD7748 20 74 77 36 61 32 7A 6E 71 A0 BF 02 A0 09 A0 E2 18 5F 41 1F 0A 28 61 6E 6F 6E 79 6D tw6a2zng . . . A..(anonym
2CAD7754 6F 75 73 29 A7 A9 00 2D 24 9F E0 01 5F 07 73 34 35 6B 66 6C 37 39 21 3F 05 6C 78 6C us)$@.-cY@_..s45ktl71?1x1
2CAD7780 61 79 61 C8 BF 21 5B 40 7F 12 62 6F 60 68 31 70 72 20 74 6F 33 38 30 65 31 36 1E eya!_..8..bufohlp..to382e16.
2CAD7790 09 68 A7 C0 1F 10 76 76 37 61 74 33 32 39 20 74 68 77 6F 34 7A 5D 65 21 9E 41 BF 03 .hsA..tv7at329 thwoizme!Z@i.
2CAD77B8 A0 08 A0 08 E2 1B FF 00 6F 22 13 0C 6C 78 62 32 20 66 31 73 69 70 30 66 6E E2 06 5F . .A.y.^..lxh2 fisiipofa.
2CAD77D4 12 69 6A 6B 68 72 3D 20 6C 67 63 70 65 51 69 E7 CO 77 09 72 71 30 .1jkhraan pvlqigcvQF1iA..xq0
2CAD77F0 65 33 68 70 78 72 3F 02 21 21 2A 6C 67 63 70 65 51 69 E7 CO 77 09 72 71 30 .esxcY.A.Y!A..mAy@.Toas >
2CAD780C 65 33 68 70 78 72 3F 02 21 2A 6C 67 63 70 65 51 69 E7 CO 77 09 72 71 30 .1jkhraan pvlqigcvQF1iA..xq0
2CAD7830 77 78 78 31 74 33 20 2C 89 00 00 80 00 7F E2 00 FF 0C 6D 73 30 35 73 69 77 73 74 .a..dededug0 hpfvrmrgz...bt
2CAD7860 52 00 61 00 79 00 6F 00 6E 20 13 02 DF 00 11 20 09 E2 00 9F CO 84 04 6D 6F 60 .wxixt3 .A..A.y.ms05siwst
2CAD7884 66 66 79 26 3F 02 0C 9C E0 14 FF 20 46 00 09 20 03 10 4C 00 66 00 7B 00 20 00 ifycit..8..A..5.. . . . . .
2CAD7890 52 00 61 00 79 00 6F 00 6E 20 13 02 DF 00 11 20 09 E2 00 9F CO 84 04 6D 6F 60 .RmJY..o...a...8..VhA.m.
2CAD787C 31 75 80 BE 00 17 20 1F 16 [7...6E 65 20 46 6F 00 20 75 6E 75 21 .. 4C 65 75 20 52 ] iue6.. good for you! Liu Rayon
2CAD7898 61 79 6F 6B E0 00 5F 11 6D 36 75 69 65 6F 66 33 20 69 63 63 30 70 65 71 E9 01 avonh..Y..mguieoF3 1ccpneamé
2CAD78B4 1F 42 1F 11 62 31 66 31 36 6E 70 34 20 6B 64 68 33 71 37 64 38 20 E4 01 1F 40 1F 15 .B..blf16np4 hdh3q7ds a..8..
2CAD78D0 6A 71 34 71 63 69 32 71 20 61 33 62 64 38 6F 33 76 20 B6 27 F3 20 80 78 40 97 13 75 jgigci2q_a3b3q9o3v ..6 €.8Y.u
2CAD78EC 65 33 6B 66 6B 73 35 20 70 77 35 34 6A 61 37 6E 00 A0 00 C1 7F 40 1F E5 00 3F 07 73 e3kfk5 pw54ja7n..A.8.A.?..s
2CAD7908 67 68 31 6F 67 68 3B 62 06 5F 15 68 75 35 70 6A 67 6C 20 6D 3E 6B 38 36 37 70 73 gnlogh8d..hus5pjg11 mskh67ps
2CAD7924 F2 AC AE 1E 1A E4 01 DF 11 6C 72 61 7A 78 64 35 70 20 6E 6F 39 67 72 38 69 64 3B AB d..@..A..B..lrazzd5p oo9qr5id:
2CAD7940 5F A2 9F C0 16 72 60 66 67 37 34 62 76 2C 44 72 E8 08 FE 00 OD EO D1 14 97 01 02 cY@.. hzawbc8m6..cJ@..no0je
2CAD795C 37 74 20 BF 11 72 60 67 37 34 62 76 2C 44 72 E8 08 FE 00 OD EO D1 14 97 01 02 7c ..rgf74bv.DrA..pya.a.A.Y.
2CAD7950 00 60 BF E1 00 66 65 36 6B 64 60 72 58 6F 87 70 29 78 CO 1F C4 36 00 20 C2 .`A..B..fe6kkdd0rXNxp)xA.A..A
2CAD7954 28 A8 9F 40 1F 41 3F 11 72 6D 6C 67 71 30 73 62 20 64 72 75 35 65 72 62 20 EO 05 (EY.A..rmlqq0ab dzquseb a.
2CAD7980 BF E0 00 5F C4 1F 02 84 6B DE 4B CF 40 4F 41 3F E4 00 3F 07 73 66 35 60 78 78 8C 37 .A..A..,KPI@7a7a..7..sf5mnx17
2CAD79CC E0 02 5F 40 1F 0F 69 30 39 71 74 7A 77 62 20 6E 37 66 69 31 71 78 45 37 00 00 E2 0C a..@..10sqgzaw..n7flqxE7..a.
2CAD79E8 3F 0B 74 38 62 34 7A 69 67 5A 4D 8A 14 32 E1 01 BF 10 6C 36 30 64 32 71 36 73 20 64 7..t5b4xigZH5..24..l.160d2dq6s d
```

Comment evidence in Linux Memory Dump

4 Facebook Forensics on Android VM

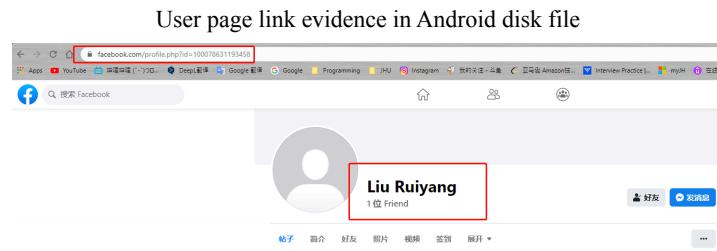
Overall, the process of finding forensic evidence is similar to previous one on Linux VM. We try to search keywords manually using hex editor.

Facebook Evidence in Android Virtual Disk Snapshot File (.vdi)

First thing to notice is that much more readable comparing to Linux VM disk file. There are much less garbled code in hex editor. And this might also be my gap research, what is the reason of the amount of garbled code in the hex editor.

First, we use the keyword `my.username` to try to gather user information in the Android disk file.

One evidence I got is the link to my main Facebook page as following.



Also, we are able to get userID and other several information like profile picture size, short name, etc. in the Android disk file as following

Other user information found in Android disk file

Second, we try to find friends information using friend username as keyword. One thing we can
got is the Facebook website alert showing we add helper account *Rayon Liu* as our friend.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	Decoded text
00SEF44	4E	47	5C	22	2C	5C	22	72	65	71	75	63	73	74	5F	74	79	70	65	5C	22	3A	5C	22	6E	7F	72	6D	NG,....,"request_type":\"norm al\"},....,r6..rich_notification_native_template_view(nt_context:@def)...s....see n.state.....SEEN AND RE ADB...should enable feed in junction...b...should open s ocial.player...S...sort key s.....,1647216849.....,164720680127583924Or...title...Text WithEntities...Text
00SEF510	61	6C	5C	22	7D	29	51	00	00	00	00	72	36	00	00	72	69	63	65	5F	6E	74	69	66	69	65	66	69	65
00SEF52C	63	61	74	69	6E	5F	6E	61	74	69	75	65	7F	74	65	6D	70	66	71	64	75	6F	76	69	65	77	28	65	
00SEF548	E6	74	5F	63	6E	74	65	78	74	6A	64	65	66	21	00	00	00	73	0A	00	00	00	73	65	65	65	65	65	
00SEF564	E5	7F	73	64	61	74	65	01	01	00	00	00	00	00	00	00	53	45	45	4E	5F	41	4E	44	5F	52	45	45	45
00SEF580	41	44	62	1C	00	00	00	73	68	65	7C	6C	64	5F	6E	61	62	65	65	6F	66	65	65	69	6E	69	65	69	
00SEF59C	6A	65	63	74	69	6F	6E	01	00	00	62	19	00	00	00	73	68	6F	75	6C	64	5F	6F	70	65	6F	73	73	
00SEF5B8	6F	63	69	61	6C	5F	70	61	69	75	72	01	01	00	03	09	00	00	73	6F	72	74	5F	6B	65	79	65	79	
00SEF5D4	73	01	01	03	00	00	00	00	00	00	00	00	00	00	00	00	00	31	36	34	37	32	31	36	34	38	34	38	
00SEF5F0	39	13	00	00	00	00	00	00	00	00	00	31	36	34	37	32	30	36	31	37	32	38	35	31	33	39	32	39	
00SEF5E0C	01	00	00	00	00	00	00	00	00	00	30	72	05	00	00	74	69	74	6C	65	01	10	00	00	05	64	78	74	
00SEF5F28	57	69	74	68	45	6E	74	69	74	65	73	00	73	04	00	00	74	65	78	74	01	01	27	00	00	00	00	00	
00SEF5F44	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	74	65	78	74	01	27	00	00	00	00	00	00	00
00SEF5F60	6E	72	65	65	65	66	4C	72	65	71	75	65	73	7E	00	00	72	6D	00	00	74	69	74	6C	65	28	60	72	
00SEF5F7C	6C	63	61	74	69	6F	6E	3A	22	68	6F	6D	65	5F	62	72	62	6C	65	22	29	01	10	00	00	00	54	61	72
00SEF5F98	65	70	74	57	74	69	64	45	6E	74	69	74	69	65	73	00	76	11	00	00	00	61	67	72	65	67	61	71	72
00SEF5F4B	74	65	64	5F	72	61	6E	67	65	73	01	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00SEF5F4D0	67	63	70	01	01	00	00	00	00	00	00	00	00	00	00	00	45	6E	74	69	74	79	41	74	52	61	6E	61	
00SEF5F4EC	67	65	00	69	06	00	00	00	00	00	00	6C	65	67	74	68	01	01	00	00	00	00	00	00	00	00	00	00	
00SEF5F508	73	75	74	01	01	00	00	00	00	00	00	00	00	00	00	74	65	78	74	01	01	27	00	00	00	00	00	00	00
00SEF5F24	04	69	75	20	52	61	79	6F	20	61	63	65	70	74	65	64	20	79	6F	72	72	20	66	72	69	65	72	69	
00SEF5F450	6E	65	64	20	72	65	71	75	73	74	72	00	72	19	00	00	74	69	74	6C	65	26	60	63	61	61	63	61	
00SEF5F5C	74	65	69	68	23	72	73	55	6D	61	72	79	22	29	01	10	00	00	54	65	74	57	74	69	68	65	65	65	
00SEF5F78	45	74	69	74	69	65	73	00	76	11	00	00	61	67	72	65	67	61	74	65	4F	72	61	6E	61	6E	61	6E	
00SEF5F94	67	65	73	00	01	00	00	00	00	00	00	00	00	00	00	76	00	00	00	00	00	00	00	01	00	01	00	00	00

Friend Acceptance Alert found in Android disk file

Second Friend Alert found in Android disk file

Moreover, we also can get a little friend user information in the disk file. The information is not too much, and the information is provided by a static web log. We can probably guess that the

Little friend information in Android disk file

specific user information of our friend here is not saved in a file. Rather, some web logs are saved in the file, and these web caches reveal very little friend information.

Third, we try to search user login email to find some helpful information. One evidence is the login evidence. As shown in the log, we are able to identify login action and its time because of the Android application logs.

Login evidence using email keyword in Android disk file

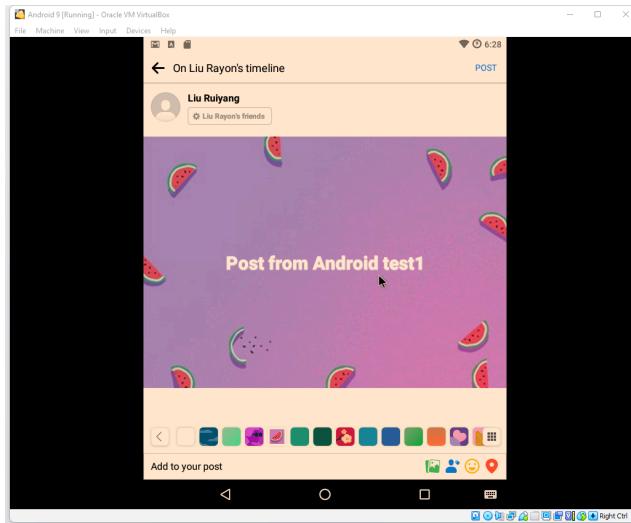
Further, the email keyword help me got the username.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	Decoded text
007DTDB38	37	38	38	3A	6F	61	75	74	68	32	3A	68	74	74	70	73	3A	2F	7F	77	77	77	2E	6F	6F	67	6C	78:auth2=https://www.googleapis.com/auth/calogic....	
007DTDB54	65	61	70	69	73	2B	63	6F	6D	2F	61	75	68	72	63	63	6C	6F	67	31	00	00	00	01	02	03	04	L[...],sso_data={"user_id": "1000783611193458","access_toke	
007DTDB70	37	06	00	01	1D	84	50	02	73	73	6F	5F	64	61	74	61	7B	22	75	73	65	74	69	64	22	3A	22	78:auth2=https://www.googleapis.com/auth/calogic....	
007DTDB8C	31	30	30	37	38	36	33	31	39	33	34	35	38	32	22	61	63	65	63	73	73	74	6F	65	6B	65	6C	78:auth2=https://www.googleapis.com/auth/calogic....	
007DTDB88	62	22	3A	22	45	41	41	41	55	61	51	48	6A	42	41	42	47	38	56	65	7D	52	48	45	78	78:auth2=https://www.googleapis.com/auth/calogic....			
007DTDBC4	4A	7A	66	55	36	47	38	60	51	42	49	38	45	4D	57	73	69	55	6E	76	30	6F	37	62	48	52	55:EE=AAAAAU8A3j81ABAG8XKmuRNKhZDfUzz61QBL8EMWwsUvwoV7koJ		
007DTDBE0	68	55	59	54	5A	41	66	58	5A	43	76	79	67	53	46	63	66	54	61	66	75	45	45	68	48	6B	6F	78:auth2=https://www.googleapis.com/auth/calogic....	
007DTBFC4	4A	4B	68	6E	43	43	49	48	50	38	59	42	41	49	45	34	50	51	74	44	61	6C	75	49	55	52:JkHnCCINPn8yBAI4E#DofalDUEDuZB2ZCbbn1QaUvQy8zD5t2CYw1yizG			
007DTCC18	5A	42	53	62	6E	58	38	63	55	61	76	71	72	38	79	74	6D	54	43	59	77	39	65	67	72	74:auth2=https://www.googleapis.com/auth/calogic....			
007DTCD34	43	47	32	4D	69	44	56	52	61	76	7D	66	54	60	55	78	6C	6F	48	44	53	66	59	72	31	73:auth2=https://www.googleapis.com/auth/calogic....			
007DTCD50	75	34	33	44	63	37	76	30	52	51	4D	4A	67	56	74	33	43	39	4C	47	57	31	52	59	39:auth2=https://www.googleapis.com/auth/calogic....				
007DTCD66	37	74	4F	54	77	5A	44	22	2C	72	75	63	75	62	4E	65	63	2A	22	31	30	39	34	33	33:auth2=https://www.googleapis.com/auth/calogic....				
007DTCD88	35	38	32	40	71	7A	62	63	6F	6D	22	2C	22	6E	61	65	23	2A	22	4C	69	75	52	75	69	79:auth2=https://www.googleapis.com/auth/calogic....			
007DTCA4	61	6E	67	22	7D	61	4B	00	00	01	8F	21	45	58	50	3A	63	6F	2D	6E	7F	6F	67	6C	65	6E	and="K...":EXE=google.com/androi		
007DTCC60	61	6E	64	72	6F	69	64	2E	67	6D	73	3A	33	38	31	38	61	34	35	64	30	37	31	39	33	33:android.com/androi			
007DTCDC3	35	34	36	38	62	31	39	61	66	30	35	65	63	36	35	32	63	65	64	35	37	38	38	33	33:5f48bd1a95e0fc562ed5788:com/androi				
007DTCEFC	74	68	32	32	20	65	6D	69	61	30	31	34	38	31	36	31	34	31	36	32	52	4A	00	00	05	78:auth2=https://www.googleapis.com/auth/calogic....			
007DTDL14	57	63	6F	6D	2E	67	62	67	65	62	61	6E	74	62	6F	69	64	62	67	6D	73	22	61	75	74:auth2=https://www.googleapis.com/auth/calogic....				
007DTDD30	23	63	6F	66	66	72	6D	2E	43	72	65	64	65	74	69	61	6C	73	53	74	61	74	65	72	70:auth2=https://www.googleapis.com/auth/calogic....				
007DTDD46	69	22	23	2B	72	73	74	61	74	75	73	22	23	62	63	6E	66	69	65	77	75	72	61	62	65	62:auth2=https://www.googleapis.com/auth/calogic....			
007DTDD68	22	72	65	73	65	74	5F	75	72	6C	22	32	68	64	74	70	73	3C	2F	5C	2F	61	63	63	6F	78:auth2=https://www.googleapis.com/auth/calogic....			
007DTDD84	75	64	73	74	72	67	6F	67	65	6E	25	63	6F	5C	2F	52	65	73	65	74	50	69	63	6F	72	22:auth2=https://www.googleapis.com/auth/calogic....			
007DTDDA0	63	75	74	75	70	5F	75	72	6C	22	3A	68	74	70	73	7A	3C	25	2F	61	63	63	6F	75	76:auth2=https://www.googleapis.com/auth/calogic....				
007DTDB7C	74	73	2E	67	6F	67	65	2C	63	6F	5C	2F	52	65	73	65	74	50	69	63	6F	75	72	22	70:auth2=https://www.googleapis.com/auth/calogic....				
007DTDBD8	63	6F	66	65	72	73	72	6C	22	3A	68	74	70	73	3A	5C	2F	61	63	63	6F	75	73	65	75:auth2=https://www.googleapis.com/auth/calogic....				
007DTDD75	75	74	73	74	72	67	6F	67	65	6E	25	63	6F	5C	2F	52	65	73	65	74	50	69	63	6F	72	22:auth2=https://www.googleapis.com/auth/calogic....			

Forth, I continue the conversation with the helper account in the Android VM and search using the chat content keywords. But I am not able to find any information or content related to the chat log. I will elaborate on the specific content of the chat logs in the next analysis of Android memory dump.

Fifth, I tried to find the forensic for posted content and the commenting on the post. The results here are unusual. First the same steps as if I were doing it on a Linux VM, I first published some content with my own account and then commented on myself. At the same time, I also comment on content posted by friends or others. Finally, I try to find evidence by searching for the keywords of the published content and the keywords of the comments.

First, I can find what I have posted, but I find evidence of my comments by keyword or post evidence location.



Posting using Android Facebook App in Android VM

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E	0F 10 11 12 13 14 15 16 17 18 19 1A 1B	Decoded text
007F1E08	00 00 00 7E 0E 00 00 00 64 65 6C 69 67 68 74 5F 72 61 6E 67 65 73 01 01 00 00 00		...v....delight_ranges.....
007F1E04	00 00 00 7E 00 00 00 69 6D 61 67 65 5F 72 61 6E 67 65 73 01 01 00 00 00 00		...V....image_ranges.....
007F1E20	00 00 00 7E 06 00 00 00 00 72 61 6E 67 65 73 01 01 00 00 00 00 00 00 00 00		...V....range
007F1E3C	00 74 65 78 74 01 01 17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		text.....Post from And
007F1E58	62 6F 6C 64 20 00		roid test1.r....message_mark
007F1E90	69 63 68 74 65 78 74 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		down_han....v....message_i
007F1EAC	64 6F 77 68 5F 65 74 6D 6C 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		lichtext.....i....messag
007F1EBC	65 5F 74 72 75 65 63 61 74 69 6F 6E 5F 6C 69 6E 65 5F 6C 69 6D 69 74 01 01 00 00		e_transcription_line_limit..
007F1E94	00 76 1C 00 00 00 00 6D 75 6C 74 69 63 69 6E 67 75 61 6C 5F 61 75 74 68 6F 72 5F 64 69		v....multiLingualAuthor_d
007F1F00	65 5F 74 68 72 65 61 64 5F 67 65 74 61 64 61 74 61 01 17 00 00 00 4E 61 72 72 61		alects.....z....narrati
007F1F1C	74 69 76 65 54 68 72 65 61 64 4D 65 74 61 64 61 74 61 00 62 14 00 00 00 69 73 5F 65		ve_thread_metadata....Narr
007F1F38	6C 69 67 69 62 6C 65 5F 66 6F 72 5F 74 68 72 65 61 64 01 00 69 00 00 00 70 6F		tiveThreadMetadata.b....is_e
007F1F54	73 69 74 69 6E 68 01 00 72 06 00 00 00 74 68 72 65 61 64 01 00 00 00 00 00 72 3D 00		ligible_for_thread....i....po
007F1F70	00 00 6E 65 67 61 74 69 76 65 5F 66 65 65 62 62 61 63 6B 5F 61 63 74 69 6F 73 28		sition_x....thread....rs
007F1F8C	61 63 74 69 6F 68 6C 6F 63 61 74 66 67 6E 3A 22 70 72 6F 66 69 6C 65 22 2C 66 69		..negative_feedback_actions(
007F1F88	72 73 74 3A 35 30 29 01 21 00 00 00 4E 65 67 61 74 69 76 65 4F 65 64 62 61 63 6B		action_location:"profile", fi
007F1F94	41 63 74 69 6F 68 73 43 4F 6E 65 63 74 69 67 6E 00 76 00 00 00 65 64 67 65 73		rst:50),..., _NegativeFeedback
007F1F00	01 01 00		ActionsConnection.v....edges
007F1F1C	62 6F 76 65 5F 66 6C 64 01 00 69 12 00 00 00 6E 75 6D 5F 61 63 74 69 6F 73 5F 61		book_fold....i....num_actions_a
007F2018	66 6F 6C 64 64 01 00 00 76 1D 00 00 00 00 6E 65 77 73 65 65 64 5F 75 73 65 72 5F		folded...v....newsfeed_user
007F2034	65 64 75 63 61 74 69 6F 68 74 65 6D 73 01 01 00 00 00 00 00 00 00 00 00 00 00 00		education_items....r....
007F2050	00 00 6F 6E 67 6F 69 6E 67 5F 63 72 69 73 69 73 5F 69 6E 66 6F 01 00 00 00 00 00		..ongoing_crisis_info....r....
007F206C	00 00 00 70 61 67 65 5F 65 78 63 75 73 76 65 5F 70 6F 73 74 5F 69 6E 66 6F 28		...page_exclusive_post_info(
007F2088	6C 6F 63 61 74 69 6F 68 3A 22 74 69 6D 65 6C 69 6E 65 22 29 01 00 00 00 00 00 00 00		location:"timeline")....r

Posting evidence found in Android disk file

Second, rather unusually, I found evidence of the comment content in the Linux VM from the previous experiment. But I did not find any comment evidence of operation in Android VM.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	Decoded text	
005DFDF4	56	75	64	44	6F	78	44	63	35	7D	59	78	4F	44	67	31	4D	54	59	35	4E	6A	66	4D	54	VudBoxDmcsMxYzODg1MTY5Nj1fMTI				
005DFDF5	41	34	46	51	30	4E	66	45	31	54	45	79	74	6A	7B	76	00	00	00	61	74	61	63	A4NjQ9N1ELMtEYszkzv.....atcc						
005DFDFC	6B	65	65	74	73	01	01	00	00	00	72	06	00	00	61	75	74	68	6F	72	01	hments.....r....author.								
005DFDF8	04	00	00	05	55	73	62	01	00	00	00	00	31	30	30	37	38	33	31	31	39	31	31	31	User.....10007863119					
005DFDF4	34	33	35	38	72	04	00	00	62	6F	79	01	10	00	00	54	65	78	74	57	69	74	68	45	3458R.....body....TextWithEn					
005DFDF6	74	69	74	69	65	73	00	06	00	00	63	6F	6C	6F	72	52	7F	62	61	67	65	73	01	01	00	tities.v.....color_ranges.				
005DFDF7	00	00	00	00	00	00	00	00	00	00	64	65	69	67	68	74	5F	72	61	67	65	73	01	01	00v....delight_ranges.				
005DFDF8	00	00	00	00	00	00	00	00	00	00	72	61	67	65	73	01	01	00	00	00	00	00	00	00	00v....ranges.				
005DFDFB	00	00	00	00	45	6E	74	69	74	79	11	54	61	67	65	70	02	00	00	00	65	74	69	74EntityAtRange.r....entit					
005DFDD0	79	01	04	00	00	00	00	55	73	65	72	01	00	00	00	00	00	31	30	30	37	39	30	31	31	y.....User.....100079017				
005DFDFC	35	32	31	31	39	69	00	00	00	00	65	6E	67	74	68	01	01	09	00	00	69	06	00	00	6521981.....length.....1.					
005E0008	6F	66	66	73	65	74	01	01	0E	00	00	00	00	73	00	04	00	00	74	65	78	74	01	01	17	00	00	offset.....s.....text.		
005E0024	00	00	00	00	67	67	6F	64	20	66	72	20	79	76	75	21	20	4C	69	75	20	52	61	78	6F	68	00good for you! Liu Mayan!		
005E0040	72	12	00	00	00	00	62	6F	64	79	5F	61	72	6B	64	7F	77	5E	68	74	6D	61	00	00	00	00	00	r.....body_markdown.htm.		
005E0052	62	20	00	00	00	00	63	61	6F	57	65	73	65	5F	63	6E	73	74	69	75	74	65	67	5F	62	61	64can see constituents.		
005E0078	67	65	75	70	73	65	6C	60	01	01	02	62	11	00	00	63	61	6F	75	69	65	77	65	72	52	ge_upsell.....b....can viewer				
005E0094	65	66	65	75	64	75	01	01	01	02	00	00	63	61	6E	76	75	69	65	77	65	72	52	65	64	69delete.b....can_viewer_edt			
005EO0B0	74	01	01	01	02	12	00	00	00	63	61	6E	75	66	65	77	65	72	55	75	70	76	76	74	65	64	L.....b....can viewer_update_v.			
005EO0CC	67	76	76	76	74	75	01	00	01	73	17	00	00	00	63	61	6E	6D	65	6E	74	56	71	74	61	63	cmvnote.....s.....comment_attache			
005EO0E8	60	65	65	74	57	74	79	70	65	01	01	04	00	00	00	00	00	04	4E	45	73	18	00	00	00	00	00NONEs.		
005EO104	03	63	6F	6D	65	65	6E	74	57	6F	77	74	65	72	55	66	73	68	62	67	77	6C	72	6F	65	00	hment_type.....s.....comment_attache			
005EO120	00	00	02	00	00	00	00	00	63	6F	6D	65	6E	74	75	70	61	72	65	74	74	00	00	00	00	00	00	comment_owner_fishbowl_role.		
005EO13C	00	00	00	00	63	6F	6D	65	6E	74	5F	70	72	69	76	61	63	75	79	75	76	61	6C	75	65	01	01	0F	00	comment_parent.....s.....comment_privacy_value.
005EO158	00	00	00	00	00	00	00	44	45	46	41	54	54	50	52	49	56	41	43	59	72	1D	00	00	00	63	6F	00	DEFUALT_PRIVACY_Ctr.....co	
005EO174	6D	65	72	63	65	5F	74	68	72	65	01	64	74	5F	70	65	70	69	76	73	63	6F	74	78	74	01	00	commerce_thread_replay_context.		

Some comment evidence found in Android disk file

Facebook Evidence in Android Memory Dump file (.sav)

User, Login and Friend Evidence in Android Memory Dump

We use the same steps and keywords as previously done in Android memory dump file.

First, we search my account name, and we can get UserID information, the birthday, and my login attempt log.

User ID and birthday information found in Android Memory Dump

Login Attempt evidence in Android Memory Dump

Moreover, When we login to the account, we can see the login evidence show that the password

of the account is being encrypted, i.e., `Facebook.account.login.encryption.jobs.Password`.

Facebook Login Encrypted Password in Android Memory Dump

Second, We search the email keyword, and get similar user information, such as user birthdate,

UserUid, etc.

Third, we search friends keyword to find friend information. The same as we observed in Android disk file, we can find earlier friend accept alert in Windows local machine. Also, we can get little friend information, such as friend's username, friend keyID.

Friend Acceptance Alert in Android Memory Dump

Little Friend information in Android Memory Dump

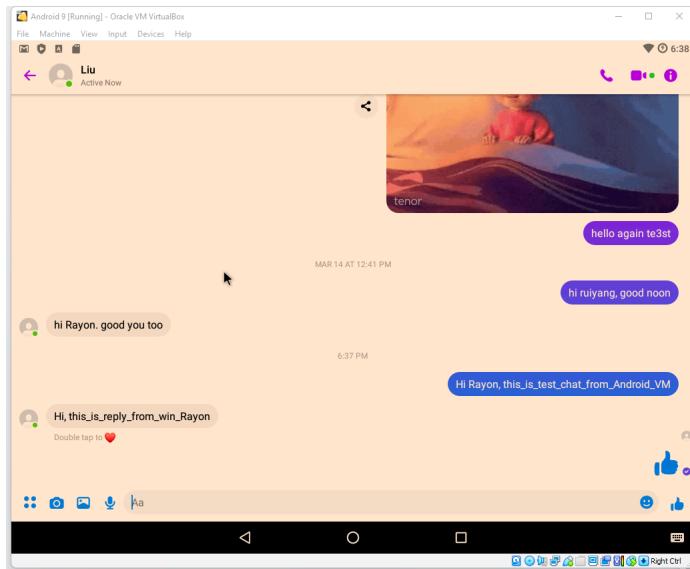
Chat Evidence in Android Memory Dump

Before you can do Facebook chat in Android Virtual Machine, you need to install Android Facebook chat software and then you can do the function of chatting with your friends. After installing the chat software, we need to authorize the Facebook account login feature. After

authorization, you will be able to chat with your friends. When we search for evidence of login, we also find forensic evidence of authorized login to Facebook chat application.

Facebook Chat Application Authorized Login Found in Android Memory Dump

After we installed the chat application, we chat with helper account as the same procedure as we do in Linux VM.



In Android memory dump, we are able to gather both chat message we sent and the message our friend sent to me. Also, we can get additional information, such as userKey, username and the *messageActorType* to inform us that the log is a Facebook message evidence.

Message I sent to my friend evidence in Android Memory Dump

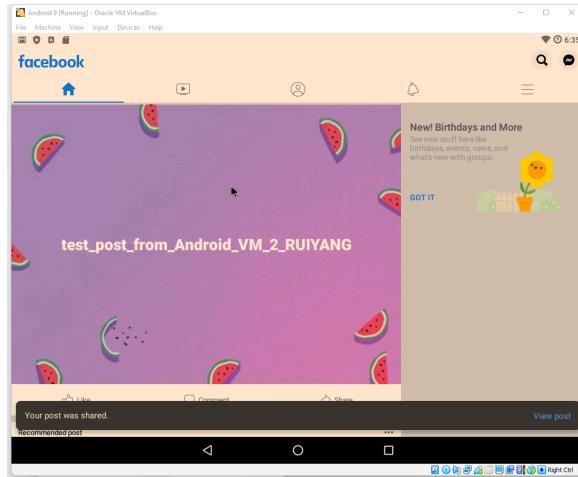
Message friend sent to me evidence in Android Memory Dump

Moreover, we can even get evidence of previous chat contents in earlier experiments.

Earlier chat content found in Android Memory Dump

Post and Comment Evidence in Android Memory Dump

First, we post some content in the Android VM Facebook software. Then we search in Hex Editor using the posting content keywords. We can get the forensic evidence of our published content, and the visibility range *ALL_FRIENDS*.

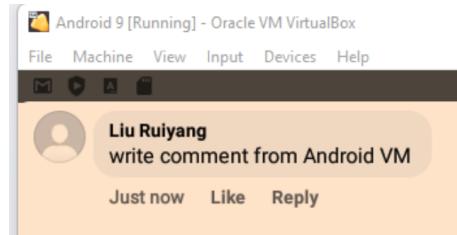


Posting from Android VM Facebook App

Offset(h)	Decoded text
53B6997C	Bà.I.àXá.-i.á.j.ç@.!..à%4.
53B69998	(ÿ@...ÿ.íá>..£\Á2.CJ.Há-
53B699B4	.í i.....(p@D...P.!..E.i).fi
53B699D0	'Be.w\$" "i...-~&.Hf. (%q)f
53B699EC	.W..tO.> ..<j`..Y.##0.0%>,<
53B69A08	(\$s..#\$S...\$C'....'...."
53B69A24	a;.. =x....PrivacyOptionr.
53B69A40	.Zc+fh ..image... .I@...s..
53B69A5C	name... .@.friends.s...id.
53B69A78	.@..lcf72e7d6d4bc018dd7e7
53B69A94	adfe772da65.s.. %leg v...grap
53B69AB0	h_api_p€".json... ".@.J"val
53B69ACC	","."ALL_FRIENDS")à.Ž.F.Z.Wi
53B69AE8	chEntitie >@.text..#@N ..te
53B69B04	st_po ..from Android VM 2 RU
53B69B20	LYANG A.Á.scope... .!Pc..S@
53B69B3C	..!+...icon_iAíá+.rl 4ÄX.o
53B69B58	pAs.s(first:50,is_selected .
53B69B74	:true)... 5.P€ ..!sContent .
53B69B90	n /%.~VA-.edges... /@... .
53B69BAC	4.7.E '!..rA.node.@íá.'á..
53B69BCE	..ty!@...r.. .product_matc
53B69BE4	h_info... .P€.M9..StoryI ..
53B69C00	r@.admin.toggle!..tttings..
53B69C1C	K`4.A@%.T'S.S #.s@EA8.tatu

Posting Evidence in Android Memory Dump

Second, we test whether it is possible to get forensic evidence by commenting under our own published content and commenting under other people's published content. First we tested commenting under a friend's post. We can see the content of our comment in the Android Memory dump.



Write comment to other people's post

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	Decoded text									
00AE53D0	20	08	18	E8	42	E8	42	E8	42	E8	07	D8	07	D8	07	D8	07	DA	05	84	42	E8	42	E8	42	E8	..ABeBaBeBaU.O.U..BeBeBa											
00AE53E0	20	08	18	E8	42	E8	42	E8	42	E8	07	07	07	07	07	07	07	9C	42	F1	F2	F2	C9	C9	42	E8	..1B1B1B1..r..\B8B6B8..E8B8..B8											
00AE5408	40	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	CB	38	98	00	00	00	01	00	00	00	00	00	00	00	00	00					
00AE5424	32	07	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05	05						
00AE5440	FF	00	FF	00	FF	00	FF	00	FF	00	FF	00	FF	00	FF	00	FF																					
00AE545C	00	0E	66	01	00	01	00	92	01	01	93	81	92	04	05	08	38	98	00	00	00	02	00	00	28	07	00	00	00	00	00	00						
00AE5478	20	07	05	LC	00	07	02	SC	41	37	08	08	61	FC	2C	FC	FF	00	FF	00	FF	00	FF	00	FF	00	FF	00	FF	00	FF	00	FF					
00AE5494	00	0E	FF	00	FF	00	FF	00	FF	00	FF	00	FF	00	FF	00	FF	00	FF																			
00AE54B0	00	0E	FF	00	FF	00	EC	00	01	00	00	92	01	01	93	80	93	04	08	30	31	43	01	00	00	00	00	00	00	00	00	00	00					
00AE54CC	00	21	06	66	61	20	66	00	1F	79	3A	00	34	35	20	47	41	54	00	43	02	44	50	45	48	54	FD	00	00	00	00	00	00					
00AE54E8	55	53	49	43	55	50	49	43	48	52	50	70	65	1F	00	CA	DE	60	C2	EA	04	00	CA	3B	D3	66	1F	00	00	00	00	00	00					
00AE5504	75	64	63	66	5F	61	63	74	69	76	65	73	74	61	74	75	73	74	6F	17	61	70	68	51	4C	00	39	36	00	00	00							
00AE5520	32	00	43	11	00	00	00	70	75	75	65	65	65	65	65	65	65	65	65	65	65	65	65	65	65	65	65	65	65	65	65	65						
00AE553C	65	65	65	50	56	45	40	37	3D	77	77	77	77	77	77	77	77	61	63	65	62	6F	68	65	2B	20	26	04	00	00	00	00	00	00				
00AE5558	CF	00	20	20	25	20	25	20	71	02	18	00	40	1B	03	73	65	65	65	62	18	65	72	73	5F	65	62	73	65	62	73	65	62					
00AE5574	70	09	69	67	0E	00	00	09	40	32	6E	77	07	07	03	CD	70	07	00	02	11	01	FB	1E	00	00	00	00	00	00	00	00	00	00				
00AE5590	A6	CD	80	1A	DE	50	5C	BB	0F	00	91	S6	D6	H8	80	03	04	06	65	22	29	A0	27	00	00	00	00	00	00	00	00	00	00					
00AE55AC	20	07	04	03	04	00	00	5B	07	07	0B	17	10	00	00	80	31	55	44	2D	30	00	A9	E8	5A	56	00	00	00	00	00	00	00	00	00	00		
00AE55C8	CD	01	00	01	00	01	00	61	67	20	1A	00	00	07	6F	00	72	73	00	39	40	5F	08	EB	05	00	00	00	00	00	00	00	00	00				
00AE55E4	3B	20	32	30	5D	57	00	00	03	20	00	AC	03	18	72	00	00	80	00	EB	E8	61	67	67	62	65	67	00	00	00	00	00	00					
00AE5600	61	73	64	65	62	71	61	67	65	73	74	30	1A	72	65	65	3A	00	73	00	21	4D	70	31	61	6E	00	00	00	00	00	00						
00AE561C	64	67	72	61	5F	65	6D	64	61	5F	74	79	20	FT	07	09	68	74	00	72	73	74	7A	31	20	AO	00	00	00	00	00	00	00	00	00	00		
00AE5638	00	EF	61	60	65	C6	9A	CD	A8	35	06	04	00	32	DC	60	21	A0	0F	1D	00	0D	3F	63	60	11	6E	73	00	00	00	00	00	00	00	00	00	00
00AE5654	79	73	75	78	69	67	63	65	76	75	77	65	72	6C	61	73	74	5F	67	72	41	42	00	74	00	00	00	00	00	00	00	00	00	00				
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00	40	23	37	00	14	29	00	00	00	00	00	00	00	00	00	00			
00AE5670	00	39	31	35	31	30	38	39	36	34	31	20	90	00	35	38	33	36	00</td																			

Comment other people's post evidence found in Android Memory Dump

Then we comment below the content we post. Strangely, we can roughly see that the forensic evidence found in Hex Editor is our comment, but that evidence is not complete (i.e., not a complete sentence, and not exactly identical to the comment). It remains unclear to me whether this is a common pattern or just a special case of my personal experiment.



Write comment to myself's post

Not complete evidence of comment in Android Memory Dump

5 Facebook Forensics on Windows 7 VM

Overall, the process of finding forensic evidence is similar to previous two on Linux VM and Android VM. We try to search keywords manually using hex editor.

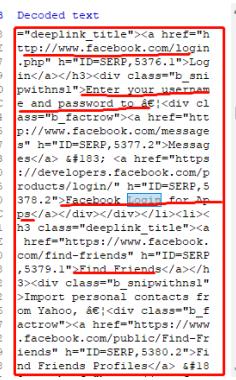
Facebook Evidence in Windows7 Virtual Disk Snapshot File (.vdi)

Compared to the first two operating systems, you can see a lot of web information and web cache style content in the disk file of windows 7. But compared to the first two operating systems, we get less information in the disk file.

First we still try to retrieve user information using username keywords, email keywords and login keywords first. We can get the information in the form of web HTML displayed directly in Hex Editor, which is something that neither Linux nor Android systems see. We can see the information of our login screen, including the user trying to login and requesting a password. But we do not see further information about the user's personal information. And I didn't find information about login email in the Win7 disk file.

```

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B Decoded text
036642B4 3D 22 64 65 65 70 6C 69 6E 6B 5F 74 69 74 6C 65 63 61 20 68 72 65 66 3D 22 68 ="deeplink_title"><a href="n
036642D0 74 74 70 3B 2F 2F 77 77 2E 44 3D 53 45 52 50 2C 35 33 37 36 2E 31 22 62 5F 73 6C 69
036642EC 2E 70 69 70 22 20 68 3D 22 49 44 3D 53 45 52 50 2C 35 33 37 36 2E 31 22 62 5F 73 6C 69
03664308 69 6E 3C 2F 61 3E 3C 2F 68 33 3E 3C 64 69 72 20 63 6C 61 73 73 3D 22 62 5F 73 6C 69
03664324 70 77 69 74 68 6E 73 6C 22 3E 45 6E 74 65 72 20 79 6F 75 72 20 75 73 65 72 6E 61 69
03664340 65 20 61 6E 64 20 70 61 73 77 6F 72 64 20 74 6F 20 E2 80 A0 3C 61 69 76 20 63 69
0366435C 61 73 73 3D 22 62 5F 66 61 63 74 72 6F 77 77 22 3E 3C 61 20 68 72 65 66 3D 22 68 74 74
03664378 73 2A 2F 2B 77 77 77 2E 66 61 63 65 62 6F 6F 6B 2E 63 6F 6D 2F 65 73 73 61 67
03664394 73 22 20 68 3D 22 49 44 3D 53 45 52 50 2C 33 33 37 37 2E 32 22 3E 4D 65 73 73 61 67
036643B0 65 73 3C 2F 61 3B 20 26 23 31 38 33 3B 20 3E 61 20 68 72 65 66 3D 22 68 74 74 70 73
036643CC 3A 2F 2F 64 65 76 65 6F 70 65 72 73 2E 61 63 65 62 6F 6B 2E 63 6F 6D 2F 70
036643E8 72 6F 64 75 63 74 73 2F 6C 6F 67 69 6E 2F 22 20 68 3D 22 49 44 3D 53 45 52 50 2C 35
03664404 33 37 38 2B 32 32 3E 46 61 63 65 62 6F 6F 6B 20 4C 6F 67 69 6B 20 66 6F 72 20 41 70 378.2">Facebook Login for Me
03664420 70 73 3C 2F 61 3B 3C 2F 64 69 76 3E 3C 2F 6C 69 3B 3C 6C 69 3E 3C
0366443C 68 33 20 63 6C 61 73 73 3D 22 64 65 65 70 66 69 6E 6B 5F 74 69 74 6C 65 65 22 3E 3C 61
03664458 20 68 72 65 66 3D 22 68 74 74 70 3A 2F 2F 77 77 2E 66 61 63 65 62 6F 6B 2E
03664474 63 6F 6D 2F 66 69 6E 64 2D 66 72 65 65 6E 64 73 22 20 63 2D 24 49 44 3D 53 45 52 50
03664490 2C 35 33 37 39 2E 31 22 3E 46 69 6E 64 20 46 72 69 65 66 64 73 3C 2F 61 3E 3C 2F 62
036644AC 33 3E 3C 69 76 20 63 6C 61 73 73 3D 22 62 5F 73 6E 69 70 77 69 74 68 6E 73 6C 22
036644C8 3E 49 6D 70 6F 72 74 20 70 65 72 73 6F 6E 61 6C 20 63 6F 6E 74 61 63 74 20 66 67
036644E4 6F 6D 20 59 61 69 6F 67 2C 20 E2 80 A0 3C 64 69 76 20 63 6F 6E 61 73 73 3D 22 62 5F 66
03664500 61 63 74 72 6F 77 22 3E 3C 61 20 68 72 65 66 3D 22 68 74 74 70 73 3A 2F 2F 77 77 77
0366451C 2E 66 61 63 65 62 6F 67 2B 6E 65 6F 6D 70 75 76 62 6C 69 63 2B 46 65 6E 64 2D 46 72
03664538 69 65 6E 63 73 22 68 3D 22 49 44 3D 53 45 52 50 2C 35 33 38 30 2E 32 22 3E 46 66
03664554 6E 64 20 46 72 69 65 6E 64 73 20 50 52 6F 66 69 6C 65 73 3C 2F 61 3E 20 26 23 31 38
.....
```



Login page HTML in win7 disk file

Secondly, we chatted with our Facebook friends in Win7 virtual machine, but we did not find any evidence of chat by searching chat content keywords or chat user name keywords.

Third, we post some content in Win7 Virtual Machine and then reply to what we have posted. We can find the posted content and the evidence of our comments on our own posted content in the disk file.

Post evidence in Win7 Disk File

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	Decoded text
031F6E1C	63	74	69	6F	EE	54	79	70	65	22	3A	22	68	74	74	70	3A	5C	2F	2F	73	63	68	65	6D	61	2E	ctionType":"http://\\schemas.microsoft.com\\...\\LikeAction","userInter	
031F6E38	67	67	5C	2F	4C	69	65	61	63	74	69	67	6E	22	2C	22	75	63	75	49	6E	74	65	72	61	22	;"InteractionCounter","int		
031F6E54	63	74	69	6F	EE	43	6F	75	64	72	34	30	7D	2C	78	22	52	75	30	34	70	74	79	65	22	;"InteractionType","http://\\schemas.			
031F6E70	63	29	4A	6E	75	62	61	63	74	69	67	EE	43	6F	75	6E	74	65	72	22	69	66	74	65	22	;"InteractionAction","http://\\schemas.			
031F6E8C	61	74	69	6F	EE	54	79	70	65	22	3A	22	68	74	70	3A	5C	2F	2C	73	63	68	65	6D	61	2E	org\\/schema		
031F6EAC	2E	6F	72	67	5C	2F	53	68	61	72	65	41	63	74	69	66	2E	22	2C	22	75	73	65	72	4E	74	;"UserInteractionEnabled","userIn		
031F6ECC	72	61	73	74	69	6F	63	43	6F	75	6E	74	22	3A	30	7D	55	25	22	63	6F	6D	65	74	73	22	;"ReactCountOn","0!01","commentCo		
031F6ECD	75	6E	74	22	3A	31	2C	22	63	6F	6D	65	67	74	23	3A	5B	7B	2C	75	30	30	34	70	74	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate			
031F6EFC	70	65	22	3A	22	43	6F	6D	65	67	EE	74	22	3C	22	60	64	65	6E	74	69	66	65	72	22	3A	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate		
031F6FD8	31	31	35	38	38	38	30	34	33	37	35	34	39	32	2C	22	64	61	74	65	43	72	65	61	74	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate			
031F6FD4	64	22	3A	22	32	30	32	32	30	33	2D	32	32	36	54	31	33	3A	32	31	33	35	2D	30	37	30	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate		
031F6FD50	63	22	22	74	75	78	74	22	3A	74	65	73	74	69	72	65	60	76	79	55	63	6F	6D	65	6E	2E	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate		
031F6FD6C	5E	72	75	69	71	6E	67	5F	73	65	60	66	22	2D	22	6D	65	6E	74	69	65	6E	73	22	3E	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate			
031F6FD8C	66	4C	62	22	61	75	74	68	6F	72	22	3A	22	5C	75	30	30	34	30	74	70	65	62	30	22	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate			
031F6FDA4	65	72	73	6F	EE	22	22	6E	61	6D	65	22	3A	22	4C	69	75	20	52	75	69	79	61	6E	72	22	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate		
031F6DCA	22	75	62	6C	22	3A	22	68	74	70	73	3A	5C	2F	2C	77	77	77	2E	66	61	63	65	62	6F	2E	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate		
031F6DDC	65	2E	63	6F	6D	5C	2F	70	72	6F	66	65	6C	65	7E	60	70	22	2C	69	64	65	6E	74	69	2E	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate		
031F6DF8	65	72	62	3A	22	31	30	30	37	38	36	33	31	31	39	33	34	35	38	22	7D	7D	5D	2C	22	2E	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate		
031F6E14	75	74	68	6F	72	72	78	75	7C	50	30	34	30	34	30	74	79	70	65	22	3A	22	50	65	73	6F	2E	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate	
031F6E30	22	22	6E	61	6D	65	22	3A	22	4C	65	75	20	52	75	69	79	61	6E	67	22	2C	65	64	65	6E	2E	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate	
031F6E4C	74	69	66	69	55	72	22	3A	31	30	30	37	38	36	33	31	39	33	34	35	38	22	2C	22	75	72	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate		
031F6E63	65	22	68	74	74	70	73	70	5A	5C	2F	2F	77	77	77	2E	60	61	63	65	62	6F	65	6E	2E	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate			
031F6E94	65	2C	70	72	6F	66	69	66	65	7E	60	68	70	22	2C	69	6D	61	67	65	22	3A	22	75	76	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate			
031F6EA0	22	73	61	6D	65	41	72	33	2A	66	75	6C	6C	22	61	64	62	75	73	22	3A	22	65	6E	75	2E	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate		
031F6EB6	65	7D	7C	2T	73	63	72	69	70	74	3E	3C	60	69	6B	20	72	65	3D	22	61	6C	74	65	2E	;"commentContent": [{"u": "10040405pe","comment": "Identifier"}, {"u": "1158830443754522d","dateCreate			

Comment myself evidence in Win7 Disk File

Finally, we tried to comment on content posted by other users as well as our own friends, but I didn't find any forensic evidence.

Facebook Evidence in Win7 Memory Dump file (.sav)

User, Login and Friend Evidence in Win7 Memory Dump

As in the previous two system experiments, I tried to use username keywords, email keywords to search for login and user information. Surprisingly, in the win7 virtual machine, the user login and login password are displayed directly in the win7 memory dump without encryption. In other words, one can get the Facebook login password directly in the win7 memory dump.

User Login info and Password shows in the Win7 Memory Dump

But in Win7 memory dump, I tried to search for friend username and other keywords and didn't find friend information.

Chat Evidence in Android Memory Dump

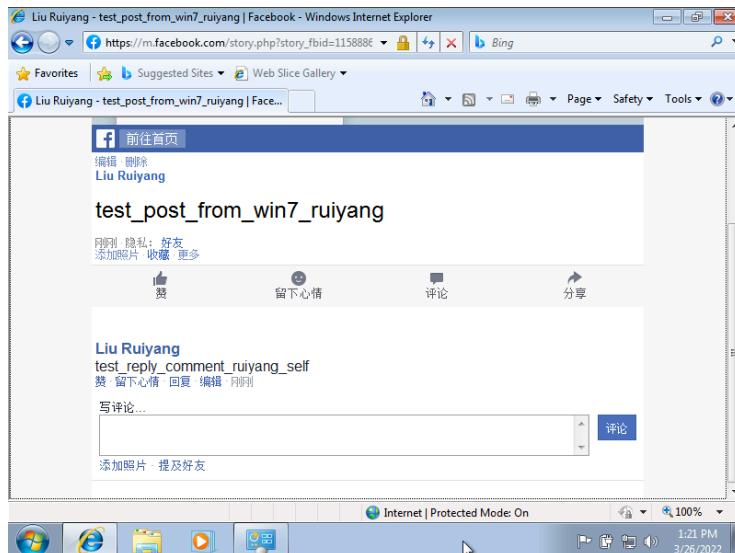
First, you need to talk to your friend in the web page of Win7 Virtual Machine. Then try to search the chat content keywords in Hex editor to try to find the chat forensic evidence. But I can only find a few uncertain words in the Win7 memory dump of the chats I sent, and I can't find any of the chats that the helper account replied to me.



Uncertain chat evidence in Win7 Memory Dump

Post and Comment Evidence in Android Memory Dump

As the same experiment in the first two systems, I first made a post in the Win7 VM and then commented on myself. Then I look for post evidence and comment evidence in Hex editor.



Post and comment to myself in Win7 VM

Post evidence found in Win7 Memory Dump

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B	Decoded text
0898BBC8	00 7B 20 13 00 6F 20 71 00 64 60 77 00 3A 20 C3 00 70 20 2D 00 20 20 A9 00 6F 20 A9	.i ..o q.d'w.: Á.p -. @.o @
0898BBC4	00 69 20 17 04 20 00 23 00 38 20 07 00 39 20 49 00 39 20 25 00 60 AD 00 62 60 D3	.i ..o #.8 ..9 I.9 %;..b'Ó
0898BC00	E0 05 9D 00 2D 20 15 00 6F 20 83 00 74 20 05 00 6D E0 00 1B C0 2F 00 68 20 6B 00 64	A...o f.t ..m.hA/h.k.d
0898BC1C	20 51 E1 03 03 04 41 49 00 6C 60 05 00 65 60 3D E1 01 6B 00 66 20 43 00 6E 20 49 00 2D	Q4..AI.l'..*^A.k.f C.n I.-
0898BC38	20 2F 00 65 21 09 00 65 20 47 00 73 20 55 00 61 20 23 00 6C 20 53 E0 05 79 00 3A Al	/..!..e O.s U.a #.1 S.A.y.;
0898BC54	17 00 20 20 A3 80 BF E1 03 27 00 62 20 7B 00 2E 20 05 00 6A 20 81 00 62 20 41 41 CD	.. 6EÁ.'b (.. ..j ..b AAi
0898BC70	00 67 20 F3 02 6F 00 75 20 63 00 64 20 63 00 63 20 0B 40 7B 00 72 20 49 02 23 00 36	..g ó.o.u c.d c.c .@.r I.#.6
0898BC8C	20 13 00 38 20 49 00 62 20 03 40 BD 04 2F 00 2A 20 0D 20 01 00 3E 20 07 02 2F 00 00	..8 I.b .#%/-'*.] ..> ..-/.
0898BCA8	20 5B 00 38 00 A8 00 01 A9 57 94 62 0E 20 0E 0F FF 00 E0 FF 00 E0 FF 00 E0	[.8...EW'b.. Áy.Áy.Áy.Á
0898BCC4	FF 00 A0 00 45 F3 01 67 00 25 38 1F 00 0F 97 62 00 60 5A 40 07 A8 04 A6 00 41 51 48	y..Eó.g.%8..-b..#8..!.AOH
0898BCE0	68 35 6F 47 68 75 62 70 6A 57 37 41 25 33 41 31 00 38 40 04 1F 36 34 38 33 32 35 37	h5GhubbpWTA3A1.88..6483257
0898BCFC	39 31 26 6A 61 78 6F 65 73 74 3D 32 32 30 34 38 26	916jazoeat=20248d-comm...te
0898BD18	F8 74 3D 74 20 17 00 5F 72 65 70 6C 75 5F C0 17 1E 72 75 69 75 61 62 67 5F 73 65 80	x=t.. reply Á..ruiyang..sel
0898BD34	66 72 64 72 00 B7 28 F4 92 1D 97 62 08 38 74 36 00 60 94 40 07 0A 00 19 93 08 D0 1B	frd..]A'..-b..8t6..-'8...,"B.
0898BD50	93 08 58 E4 37 A0 97 06 FF FF 25 02 73 00 02 20 0D 07 3B 00 01 07 A8 99 40 07 40 A8	"Xa7..-yy%.s..,..,"m@.8.
0898BD6C	E0 01 00 06 FF FF 01 01 4E 00 0A 20 10 07 19 00 09 07 99 D4 42 08 20 0A E0 02 00 02	A..yy..N..,.....,"Ó8..Á..,
0898BD88	FF FF C1 26 65 40 33 40 3F 02 A0 F8 A4 60 1F 06 68 E8 37 00 20 1D 7F 20 0B 06 FF FF	y9Ae@338?..m..h@7..,..,y
0898BDA4	2D 01 6D 00 00 20 31 08 0A 00 0B 07 68 98 40 07 32 0B 10 20 E5 37 00 80 D9 2F 07	..m.., 1....h@8..,..,(A7.eU/.
0898BDC0	C0 00 0E 01 61 06 31 00 04 20 13 06 FF 00 03 07 88 69 2B 60 1F 01 30 E7 E0 01 9F 04	A...l..l..,..y..,i..,"ogA.Y.
0898BDDC	B0 07 25 00 09 20 1F 04 38 00 08 07 58 20 7F 40 6B 00 90 20 3F OC F8 9E 9F 08 28 00	*.k., ..8..,X ..8k.., ?ežY(.
0898BDF8	D9 00 27 20 1F 03 00 03 23 07 20 06 60 AB 00 D0 20 9F OC 28 3D 01 07 06 00 D6 01 F2	U'....#, ..*..B Y.(8...Ó.ó
0898BE14	D9 00 27 20 1F 03 00 03 23 07 20 06 60 AB 00 D0 20 9F OC 28 3D 01 07 06 00 D6 01 F2	U'....#, ..*..B Y.(8...Ó.ó
0898BE30	02 5F 00 0D 20 18 07 27 00 OC 07 72 00 5F 00 40 3F 00 5F 21 21 00 65 28 E5 00 2E 28,...,r..,87..!!..e(A..(
0898BE4C	19 02 36 00 33 26 FB 00 39 20 05 00 38 20 05 00 39 60 05 00 25 20 0D 00 41 27 73 00	..6.3q@.9 ..8..9*.7.% ..A's.
0898BE68	61 21 D3 00 65 20 2D 48 31 E0 15 2B 00 73 27 65 00 63 20 23 00 32 20 01 80 3D 48 7F	a!Ó.e -Hiâ.+.s'e.c #.2 ..é=H.
.....

Comment evidence found in Win7 Memory Dump

6 Conclusion

My research focuses on the differences in forensics against Facebook under different systems.

First, I logged in to my Facebook account, chatted with friends, posted content, and commented on other people's posted content under Linux, Android, and Win7 respectively. Then I need to use tools like Hex Editor or FTK to read the disk file and memory dump, and finally use manual search for some relevant keywords to get forensic evidence. Next I will discuss the similarities and differences in the evidence between the three systems.

First, in terms of user information, user login information, and user friend information, the Linux disk file can search for Facebook keywords, but there is no valid user information, user login emails, or friend information revealed. In the Linux memory dump, we can get login information, login time, user ID and friend ID information, but I was not able to get more details about the user. In Android disk file, the readability is higher than Linux, we can get the link of Facebook user's homepage link, user login information, user ID and friend's log of accepting

friend request prompt. In Android memory dump, we can get more information, such as user ID, user birthday, user login request log, user login encrypted password, friend request consent log and so on. Also, we can see the log information that Facebook authorized its chat software to log in. In Win7 disk file, its readability is also better and there is a lot of HTML cached inside the disk file. But we can get very little information about the user, I couldn't find the user ID and the email keyword used to log in. In Win7 memory dump, we can see not only the login request and login email, but even the password used by the user to login in plain text. But other user information and friend information is not found in the Win7 memory dump.

Second, the chat with friends feature is a very important feature of Facebook, so the differences in the three different systems where evidence of information can be obtained are discussed next. In the Linux disk file, no forensic evidence of the chat content was found. In the Linux memory dump, we can get the content of the chats we sent and the content of the chats our friends sent back. In the Android disk file, we can not only see the content of the chat between the two parties, but we can also get the username and user ID of the person we are chatting with, and surprisingly, we can even see evidence of previous chats in the Linux system. It is assumed that the previous chat logs were cached in memory when Android loaded the previous chat logs. In the Win7 disk file, the same as the Linux disk file, no chat-related evidence was found. In the Win7 memory dump, only an incomplete sentence of the sent chat log was obtained, and no evidence of any received chat logs could be seen. So it is not sure how much chat logs can be obtained in Win7 memory dump and its chatting storage logic.

Finally, the post and comment functions are the most basic features of Facebook, and in each system I have posted some content. And in terms of comments, I commented both under what I posted and under what other users posted, as a way to see if they would make a difference in terms of forensics. No evidence of post or comment was found in the Linux disk file. In the Linux memory dump, it is possible to get content posted by yourself in Linux, comments on yourself and comments on others. But there is no evidence of posts in other systems, even though the Linux virtual machine is running. In the Android disk file, the forensic evidence of the post can be obtained, but no evidence related to the comments can be found. In Android memory dump, not only can we get the evidence of the posted content, we can also see the visible range of this post. In the comment forensic evidence, I only found one vague comment evidence (the evidence is not a complete sentence). In the Win7 disk file, we can find evidence of both the post and the comment. In Win7 memory dump, which has almost the same form of evidence as its disk file, we can get evidence of both post and comment.

As you can see, the three systems have different forensic evidence that can be obtained at the three main levels and the readability of the content seen through the hex editor is not the same. Below is my table of whether forensic evidence can be obtained for different files with different features.

	Facebook and URL	Username	Friend account	Email	Login	Post	Comment	Chat
Linux VDI	Yes	No	No	No	No	No	No	No
Android VDI	Yes	Yes	Yes	Yes	Yes	Uncertain	Partial	No
Win7 VDI	Yes	Html cache	No	No	Yes	Yes	Yes	No
Linux Memory Dump	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Android Memory Dump	Yes	Yes (Password encrypted)	Yes	Yes (Password encrypted)	Yes	Yes	Yes	Yes
Win7 Memory Dump	Yes	Yes (Shows password)	Yes (Not so much info)	No	Yes	Yes	Yes	Uncertain(Not complete)

7 Future Work

Due to time constraints, the study has many questions that remain to be addressed.

1. Why the readability of disk file and memory dump of the three systems are very different and what causes it.
2. Why many messages appear many times, for example, a chat content may appear many times in different places in the memory dump, what is the reason.
3. Is there a more comprehensive and efficient way to find evidence of Facebook forensics other than using tools like Hex editor to search for keywords manually.