



Title	Investigating and analyzing the web-based contents on Chinese Shanzhai mobile phones
Author(s)	Fang, J; Jiang, L; He, MF; Yiu, SM; Hui, LCK; Chow, KP
Citation	The 7th International Workshop on Systematic Approaches to Digital Forensic Engineering (IEEE/SADFE 2012), Vancouver, BC., 26-28 September 2012, p. 1297-1309
Issued Date	2012
URL	http://hdl.handle.net/10722/189648
Rights	Creative Commons: Attribution 3.0 Hong Kong License

Investigating and Analysing the Web-based Contents on Chinese Shanzhai Mobile Phones

Junbin Fang, Zoe Lin Jiang, Mengfei He, S.M. Yiu, Lucas C.K. Hui and K.P. Chow

Abstract

Chinese Shanzhai mobile phone has had a huge commercial market in China and overseas and was found to be involved in criminal cases. In this paper, a MTK-based Shanzhai phone with private web browser was investigated to extract user's web browsing data in the form of sites visited, received emails, attempted Internet searches and etc. Based on the findings, extracting Internet search conducted and web email received from the binary image was demonstrated. Besides, deleted browsing history can be recovered from snapshots in memory help reconstruct user's browsing activity and timeline analysis.

Author

Dr. Junbin Fang is an associate professor in the Department of Optoelectronic Engineering and the Key Laboratory of Optoelectronic Information and Sensing Technologies of Guangdong Higher Education Institutes at Jinan University, Guangzhou, China. He is also working in the Department of Computer Science at The University of Hong Kong, Hong Kong, China. His research interests include mobile forensics, information security and quantum cryptography.

1. Introduction

The use of mobile phone has increased dramatically in the last decade. Globally, the number of mobile cellular subscriptions reached 5.3 billion in 2011, reported by the International Telecommunications Union (ITU). And vendors shipped 371.8 million units in Q1 2011, growing 19.8 per cent year-over-year (IDC).¹ With the mobility and the portability, mobile phones have been part of people's daily life, which inevitably holds information of people's actions, whereabouts, and intentions. However, these advantages of mobile phone can be utilized by a criminal as a criminal tool anytime and anywhere, which leads to the necessity of mobile phone forensics. Mobile phone forensics is a branch of digital forensics that focuses on extracting information from a mobile phone as digital evidence in all kinds (criminal and civil) of court cases. With the fast evolution of mobile phone technologies, the amount and the types of data that can be found from a mobile phone are increasing. Traditionally, information that can be recovered from a

¹ Robin Wauters. "Worldwide Mobile Phone Market Grew 20% In Q1 2011, Fueled By Smartphone Boom." Last modified April 28, 2011. <http://techcrunch.com/2011/04/28/worldwide-mobile-phone-market-grew-20-in-q1-fueled-by-smartphone-boom/>.

phone includes phonebook, call logs, and short message service (SMS) messages,² even deleted items. Advanced smart phones also include wider varieties of data such as e-mails, media and web browsing data. The data can be stored in several storage media inside the phone, such as the SIM (Subscriber Identity Module) card, internal flash memory and external memory card.³ In terms of forensic, obtaining evidence from the internal flash memory is more challenging as SIM card and memory card can be taken down from mobile phone and therefore both of them can be investigated independently and deeply with external card reader.

Benefit from the “turn-key” development solution provided by MediaTek (MTK)⁴ and Spreadtrum,⁵ Chinese Shanzhai mobile phone (Shanzhai phone for short) has had a huge commercial market in China and overseas in recent years due to its high cost-performance ratios. Shanzhai phone is very cheap. For example, the price of a fake version of Apple's iPhone4S in the market is only \$130, and it can be down to \$60 for a cheaper (low-end) version. Unfortunately, with the worldwide spreading, more and more Shanzhai phones are found to be involved in criminal cases. However, little research findings on Shanzhai phone forensics has been published. One of the possible reasons may be that there is almost no existing official documents about the internal flash memory, the file systems and other related information for Shanzhai phones. The other reason may be that researchers did not expect the huge potential market of such low-price mobile phones so that little attention has been paid to it before.

In the paper, we provide the first step towards the forensics investigation on the web-based content on Shanzhai phone. Based on reverse engineering, we tried to provide important information of how an MTK-based Shanzhai phone manages and stores the web browsing data in its internal flash memory with its private web browser. This information provides insights on how to retrieve deleted web browsing history and helping the investigators rebuild the sequence of web addresses the user visited. The rest of the paper is organized as follows. Section 2 reviews the current work related to web forensics and Shanzhai phone forensics. Section 3 introduces the acquisition of Shanzhai phone's internal flash memory. Section 4 details how to analyse and extract the web browsing data from the memory dump. Recovery of deleted browsing history and timeline analysis are described in Section 5. Section 6 concludes the paper.

2. Related Work

Traditionally, web forensics research is targeted to PC-based web browsers, such as Microsoft Internet Explorer, Mozilla Firefox, Google Chrom, Opera and Safari.

Jones and Rohyt described the IE and Firefox 2 Web browser forensics after simulating an actual crime in two different publications⁶. Two free tools, the Pasco and Web Historian, were introduced for IE forensics with two commercial tools, the IE History and FTK tools. Forensics in Firefox 2 using a cache

² Shafik G. Punja and Richard P. Mislán, "Mobile Device Analysis," *Small Scale Digital Device Forensics Journal* 2 (2008): 1–16.

³ S. Willassen. "Forensic Analysis of Mobile Phone Internal Memory", *Advances in Digital Forensics* 194 (2005): 191-204.

⁴ MediaTek. "MediaTek." <http://www.mediatek.com/en/index.php>.

⁵ Spreadtrum. "Spreadtrum." <http://www.spreadtrum.com>.

⁶ Keith J Jones and Blani Rohyt. "Web browser forensic." Accessed January 19, 2012. <http://www.securityfocus.com/infocus/1827>.

file and an analysis method using the cache file structure were also suggested in the publications. Pereira⁷ explained in detail the changes in the history system that occurred when Firefox 2 was updated to Firefox 3 and proposed a new method of searching deleted history information using unallocated fields. Oh et al.⁸ proposed an advanced evidence collection and analysis methodology for web forensics by performing integrated analysis across various browsers at the same time and using timeline analysis to detect the online movements of a suspect over time. A web forensics tool, named WEFA (Web Browser Forensic Analyzer), was also developed for the integrated analysis, which allows the investigator to examine the five leading web browsers (i.e. IE, Firefox, Chrome, Safari and Opera) existing in one system in parallel.

At present, there are a lot of tools for web forensics or forensics toolkits providing web browser investigation function, such as Netanalysis, Encase, FTK, etc. However, these methodologies and tools are originally designed for web browsers running on PC platform. When the scenario is moved to mobile phone platform, the investigation will become more challenging since the OS, the file system and the web browsers of the target are quite different with those on computer platform. Furthermore, the wide variety of mobile browsers also makes the forensic investigation more complicated.

Although there have been some mobile forensic toolkits that are dedicated to mobile OS, such as Android, iOS, Symbian and Windows Mobile, the toolkits cannot be used for Shanzhai phones since they are OS dependent. For Shanzhai phone forensics, Zhang⁹ discussed the recovery of MTK mobile phone flash file system, however, no detailed information is given. Fang et al.¹⁰ investigated how Shanzhai phone handles the addition and deletion of basic information in binary level as well as how to recover the historical data from memory image for timeline analysis. EDEC announced its Tarantula cell phone analysis system to target mobile phones using Chinese-manufactured chipsets and the system is further integrated into Logicube's CellXtract® cell phone forensic platform.¹¹ But both the systems didn't provide the function for web forensics.

3. Internal Flash Memory Acquisition

Flash memory is currently the most dominant non-volatile solid-state storage technology for mobile phone. Similar to other brands of mobile phones, Shanzhai phones use flash memory as internal memory devices to store hard-coded system software, system files, user data, etc. Compared with reading data from the two other major storage units in mobile phones, i.e. SIM card and external memory card, retrieving data from internal flash memory is more complex and difficult as the memory chip cannot be read directly using external memory readers, except it is removed from the printed circuit board (PCB). Nowadays, the methodologies for internal data collection can be classified into two approaches: physical and logical. The physical approach performs data extraction at a low level and allows obtaining the full

⁷ Murilo Tito Pereira. "Forensic analysis of the Firefox3 internet history and recovery of deleted SQLite records." *Digital Investigation* 5 (2009): 93-103.

⁸ Junghoon Oh, Seungbong Lee and Sangjin Lee. "Advanced evidence collection and analysis of web browser activity." *Digital Investigation* 8 (2011): S62-S70.

⁹ Zhi-wei Zhang. "The research of MTK mobile phones flash file system recovery." *Netinfo Security* 11 (2010): 34-36

¹⁰ Junbin Fang et al. "Forensic Analysis of Pirated Chinese Shanzhai Mobile Phones." *Advances in Digital Forensics VIII* (2012): 117-130.

¹¹ Logicube. "Logicube Integrates EDEC's Tarantula To Target Mobile Devices Based on Chinese Chipsets." Last modified March 04, 2012. <http://www.logicube.com/logicube-integrates-edecs-tarantula-to-target-mobile-devices-based-on-chinese-chipsets/>.

memory image of contents of the entire phone memory, usually with the help of special hardware equipment. The logical approach uses communication protocols offered by the phone at a higher level, while the amount of acquired data is limited since the API provided by the phone were not developed for forensic purposes but to operate the phone as a modem. Another problem of logical approach is that contents deleted cannot be recovered in most cases.

As one of the physical approaches for internal memory acquisition, flasher tools may be the most convenient way to get a complete memory dump,¹² compared with the other two physical approaches - JTAG approach and physical extraction approach. Flasher tools are mainly used by mobile phone manufacturer and service providers to recover user data from dead or faulty mobile phones that otherwise will not provide access to data stored on their internal memory. They can also be used to update or replace software that is stored in the mobile phone. The forensic use of flasher tools is already being taught to future digital forensic examiners in Purdue's College of Technology in the United States of America.¹³ It is also being used by European investigators in mobile forensic cases.

In this paper, we go for the easier solution of using a flasher tool to obtain the memory dump instead of using JTAG or physical extraction since our focus is more on how the information is stored in the memory. In principle, the flasher tool connects with the UART interface (Rx and Tx pins) of Shanzhai phone's processor and run a serial communication protocol to communicate with the processor. When the power button of the Shanzhai phone is pressed, a boot loader inside the processor will be executed and can read/write from/to all registers and memory addresses, then the host software can successfully retrieve a full memory dump from the phone, as complete as JTAG approach does.

4. Analyzing Web Browsing Data in Memory Image

Experiments were conducted on a typical model of Shanzhai phone, which is an imitated version of Apple's iPhone4. The model is equipped with a MediaTek MT6253 processor and a 16M byte NOR flash chip (Toshiba TC58FYM7T8C). After an image of the internal flash memory chip is dumped using flasher tool, the binary data will be analysed to extract related web information for forensic investigation. MT6253 is Mediatek's first monolithic GSM/GPRS handset chip solution that offers highest level of integration with lowest power consumption and best-in-class features. Such that most of Shanzhai phone models were developed on this platform. The memory allocation scheme of the Shanzhai phone under test followed the default configuration in MTK's turn-key solution. As shown in Figure 1, the Toshiba TC58FYM7T8C chip integrates 16 MB NOR flash memory and 4 MB RAM and the 16 MB flash memory was divided into two areas at offset 0xE0000 (corresponding to 14 MB). The first 14MB area was used as read-only memory (ROM) to store hard-coded system software, while the remaining 2MB area was used to store system files and user data. The 2MB area contained two drives in FAT12 format. One was for user data storage, which can be shown as a USB massive storage when the phone is connected to a computer. The other one was used as non-volatile random-access memory (NVRAM) for storing system files such as phonebook, SMS, call log, temporary files, etc. Noted that the NVRAM drive was invisible to normal user from computer or Shanzhai phone's UI.

¹² K. Jonkers. "The forensic use of mobile phone flasher boxes." *Digital Investigation* 6 (2010): 168-178.

¹³ Purdue University. "Expert: 'Flasher' technology digs deeper for digital evidence." Accessed January 10, 2012. <http://phys.org/news95611284.html>

4.1 Web browsing data extraction

Before going into the memory image to analyse the web-based information, the first step is to identify the type of the web browser used in the Shanzhai phone. If the web browser is one kind of the famous mobile browsers, the investigation would be easier as there may be a lot of previous research works and tools for the leading mobile browsers. Although it was reported at the end of 2011 that MediaTek and Opera Integrate Mini Browser on Feature Phones, the built-in browser of the Shanzhai phone is not Opera Mini but a private browser of Mediatek and there is not an existing tool can be applied to this browser. Since documents and references for the private browser are lack, reverse engineering is required to analyse the management of web browsing data, including browsing history, cache, bookmarks, cookies and etc.

In the experiments, after a series of common web browsing operations, a set of memory images were dumped from the Shanzhai phone and were further investigated, mainly the NVRAM area associated with the hard-coded area. Then, the organization of related files storing web browsing data in NVRAM was identified as follows:

1. Browsing history: With the private browser, the browsing history is stored in two different files. The web address shown in address bar is classified into two categories, manual input and redirected links. The first kind of web address is stored under directory `"/bra"` with filename `"history.dat"`, while the last kind of web address is saved under the same directory with filename `"history2.dat"`. The format of a browsing history recorded in file `"history2.dat"` is as the example shown in Figure 2. The record is combined by two parts, header and body. The header field is 7 bytes length with a `"FF"` start character and the third byte indicates the number of the remaining bytes of the record. The last 4 bytes in header is the Unix timestamp of accessing the website. The body field comprises the accessed web address and the title of the webpage visited, which are separated by a `"00"` byte. Note that the format for records in file `"history.dat"` is the same as that in Figure 2, except that there is not webpage title field.
2. Cache: When user accesses a webpage, the content of the webpage is retrieved to local as cached Internet files. In the Shanzhai phone, cached Internet file is renamed and placed under the directory `"/stk/cache"`. In the directory, there is a file named `"index.dat"`, which is used to manage and index all the cached files stored in this directory. Every time when the Internet files are saved, the `index.dat` file will be updated. An example of the file allocation table (FAT) of the cache directory is shown in Figure 3.
3. Cookies: Cookies of browsing history are saved in the directory `"/stk/cookie/"`. The management of cookies is similar to that of cached Internet files. In the directory, a file name `"index.dat"` is used to manage and index all the files storing Cookies in that directory.
4. Bookmark: Bookmarks of the private browser were stored in a file named `"BKM.dat"` under directory `"/bra"` in the NVRAM area.

4.2 Analyzing Internet Search History and Web-Based Email

The above findings are related to the management and basic format of the web browsing data in the Shanzhai phone. From the perspective of forensics, critical evidence can be found in the suspect's web

browsing data, including not only websites visited, but also Internet searches conducted and web-based email. For example, in the case of Neil Entwhistle, he was convicted of murdering his wife and baby daughter after forensic investigators found a Google search for "how to kill with a knife" in his computer's web history.¹⁴

In this section, two experiments of analysing Internet search history and web-based email were demonstrated.

Internet search is helpful for people to get information effectively. At present, there are several popular search engines, such as Google, Yahoo, Baidu, Bing, etc. To investigate the Internet search conducted on the Shanzhai phone, we first extracted all the entries of browsing history using the pattern of "FF*****http". Then a web address history with a general HTTP URL structure of Google search engine was found. As shown in Figure 4, the URL string located in memory image is "http://www.google.com.hk/search?hl=zhTW&newwindow=1&sky=ee&ie=Big5&q=hacking+hijack&btnG=%e6%90%9c%e5%b0%8b". In this string, the search words are the value after the variable *q*, revealing that the suspect searched on Google using keywords "hacking" and "hijack", which implies that the suspect has been interested in these techniques.

Web-based email is a typical web application and all the main functions can be operated online using a browser. Different with other kinds of web browsing data, web-based email usually involve more personal information. And web-based email can be cached only when the content of the email has been shown in the browser. For example, reading an email brings the message up in the browser and causes it to be cached, while sending an email does not since the browser doesn't display the sent mail, except that the user read the mail in sent box. In Figure 5 through Figure 7, an experiment of extracting web-based email from the binary image is demonstrated. Noted that two email accounts in qq.com were used to send and receive email, respectively.

To investigate the web-based email which was read on the Shanzhai phone, we first extracted all the entries of browsing history using the pattern of "FF*****http", same as did in investigating Internet search. Then the URL of reading email in mail.qq.com can be found. As shown in Figure 5, the URL is:

"http://w94.mail.qq.com/cgi-bin/readmail?hitttype=0&sid=6hdm9SM2Jra8mQBQW8jT5vNw,5,zTOTzKDy2&folderid=1&t=readmail&s=&mailid=ZC3021-A_46smR3sSErj9vC09cd27&lp=0&lpq=&to=".

From this URL, two useful values can be extracted as:

- The unique id for the web session (sid): 6hdm9SM2Jra8mQBQW8jT5vNw,5,zTOTzKDy2
- The unique id of the mail which was read (mailed): ZC3021-A_46smR3sSErj9vC09cd27

As the URL and the unique ids are known, the next step is to find the related cache file for this URL in the memory image. Taking the URL as a keyword to search in the index file of Cache or search directly in the image, a map between the cached file of the URL can be found. As shown in Figure 6, the cache file for the reading email is "S2f84d54.wml".

After the file "S2f84d54.wml" was carved and reconstructed, it can be displayed in a wml parser. As shown in Figure 7, the wml file is parsed and contains the following information:

¹⁴ AFP. "Briton Googled 'how to kill' days before murders: court." Accessed February 14, 2010. http://afp.google.com/article/ALeqM5hNX7099fMvF7_qHCpy1Bz4VhtR6A.

- Email service provider: QQ mailbox
- Email sender: Andy1
- Email receiver: testone
- Time: 10:28AM on July 21, 2012
- Subject: how to become a hacker
- Content: Thinking Like a Hacker...

Besides, accounts for this email can also be found in the raw format of the wml file:

- Email sending account: 1910159914@qq.com
- Email receiving account: 2576406269@qq.com.

Combining the findings in Internet search history and email, we can deduce that the user had put some effort in this kind of technique.

5. Recovery of Deleted Browsing History and Timeline Analysis

Most of web browsers provide function for clearing web browsing data, such as the cache, browsing history, cookies and etc. Users may delete the logs of web browsing to protect their privacy. Additionally, some web browsers can be configured to reset web browsing data periodically. In web forensics, if a suspect has performed such function on his web browser to destroy the trace of his activity, investigation will be more difficult.

For PC-based web browsers, recovery of deleted web browser information depends on the data clean-up mechanism of the browsers. For example, in Firefox, log files are reinitialized and only the temporary files used by SQLite in unallocated space of disk are possible to be carved and recovered.

For Shanzhai phones, it was found that there are multiple copies of user data in the binary image.¹⁵ The copies are created at different time points due to the erasure and allocation mechanism of flash memory. Since flash memory can only be “erased” a block at a time and cannot offer arbitrary random-access rewrite or erase operations, we observed that when the data in Shanzhai phone's web browser is updated, the new data will be stored in a newly erased block and the old data will be left untouched in the old block. This operation leaves multiple copies of data items until the memory space is revoked and overwritten by some other data.

From the viewpoint of forensics, this characteristic can be utilized to recover more information, even when the web browsing data in Shanzhai phone was deleted automatically or intentionally.

This section details the results of recovering deleted browsing history and analysing user's web browsing activity. In the experiment, the following web browsing operations were performed on the Shanzhai phone in sequence:

- Step 1: User started the web browser and typed a test URL "http://i.cs.hku.hk/~jbfang" into the address bar of the browser.

¹⁵ Junbin Fang et al. "Forensic Analysis of Pirated Chinese Shanzhai Mobile Phones." *Advances in Digital Forensics VIII* (2012): 117-130.

- Step 2: User opened the test webpage, which contains 3 links to Google, Yahoo and Wikipedia separately.
- Step 3: User clicked the link of "Google" in the test webpage and the browser jumped to the homepage of Google's search engine ("http://www.google.com.hk").
- Step 4: User searched "hacking hijack" in Google and waited for the results returned.
- Step 5: User deleted two entries of browsing history related to Google.
- Step 6: User typed URL "www.ask.com" into the address bar of the browser and accessed the website.
- Step 7: User searched "hacking hijack" in ask.com.

After the operations, a memory image was dumped from the Shanzhai phone and was investigated. Using pattern matching, we found 9 memory segments for browsing history in the binary image. One memory segment corresponds to a copy of browsing history after one operation and can be viewed as a snapshot. The snapshots of browsing history after every step are shown in Figure 8 through 14, noted as S1, S2, S3, S4, S5, S6, S7, correspondingly.

The snapshots in Figure 8 through Figure 11 show that every newly added record of browsing history is simply appended to the old records and causes to a new memory segment for browsing history. Snapshot in Figure 12 demonstrates the memory operation mechanism for deleting entries in browsing history. Deleting browsing history records didn't really erase the deleted entries in the file, but marked the deleted entries as invalid with a terminal symbol "FE". In this case, the deleted records of browsing history still exist in the logical file as well as in the previous snapshots, thus it can be recovered from both the current memory segment and the previous ones. However, in the snapshots in Figure 13 and 14, the cases are different. The deleted entries were overwritten by the newly added record. Therefore, the deleted record of browsing history can only be recovered from the previous snapshots.

For this experiment, since the deleted browsing history can be recovered in the snapshots and the records have timestamp, the timeline of the user's web browsing activity can be rebuilt quickly using the timestamp information, i.e. the sequence for the snapshots is: S1-S2-S3-S4-S5-S6-S7. Nevertheless, if the phone was set to a wrong time purposely, timeline analysis may not be so straightforward since the timestamp in the records may not be able to reflect the real sequence of the web addresses accessed. In this case, the relative position of the records in snapshots could be taken into consideration to help deduce the actual sequence of user's web browsing activities. For example, even the timestamps were unbelievable, we can recognize that the user activity of accessing "www.google.com" is before visiting "www.ask.com" according to the mechanism of Shanzhai phone for adding/deleting records in browsing history.

6. Conclusion

This paper presents a preliminary work on the investigation of the web-based contents on an MTK-based Shanzhai mobile phone by analysing the memory dump extracted from the phone using a flasher tool. The analysis reveals important details about how the web browsing data is managed and stored with the private web browser of the Shanzhai phone. Based on the analysis, Internet searches conducted and web-based email received can be extracted from the binary image. Besides, valuable historical data pertaining to multiple snapshots and deleted browsing history can be obtained from a memory dump as long as the

associated memory locations have not been overwritten. This information can be used to help rebuild the time sequence of user's web browsing activities.

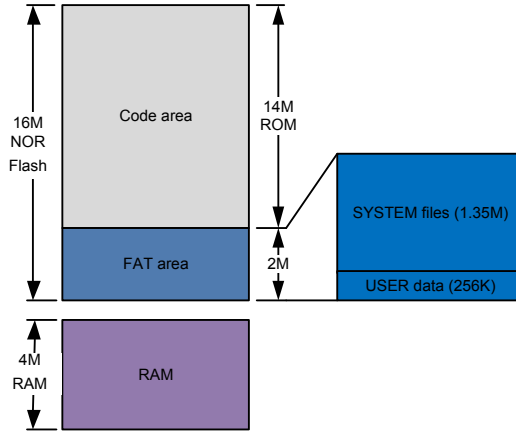


Figure 1. A typical memory allocation scheme of Shanzhai Phone

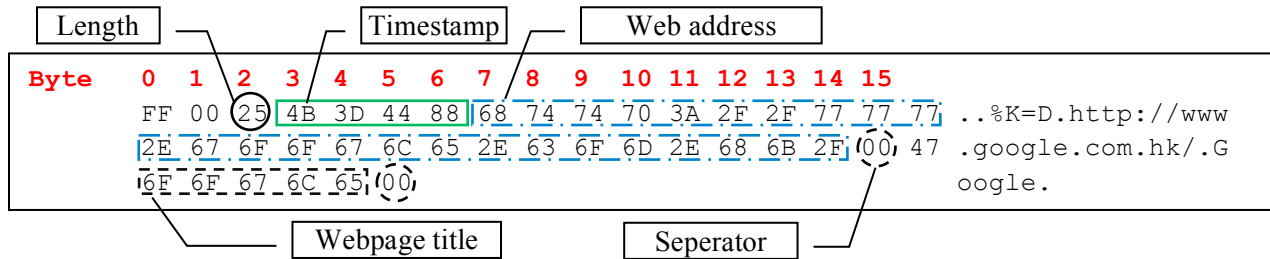


Figure 2. An example of a browsing history record in memory image

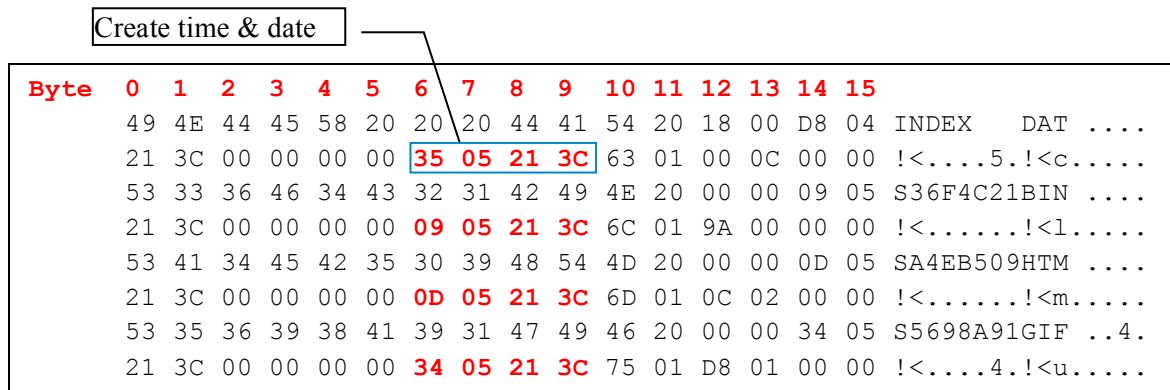


Figure 3. An example of cached Internet files record in memory image

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00ECF070	63	6F	6D	2E	68	6B	2F	00	47	6F	6F	67	6C	65	00	FF	gom.hk/.Google..
00ECF080	00	91	4B	3D	44	C1	68	74	74	70	3A	2F	2F	77	77	77	..K=D.http://www
00ECF090	2E	67	6F	6F	67	6C	65	2E	63	6F	6D	2E	68	6B	2F	73	.google.com.hk/s
00ECF0A0	65	61	72	63	68	3F	68	6C	3D	7A	68	2D	54	57	26	6E	earch?hl=zh-TW&n
00ECF0B0	65	77	77	69	6E	64	6F	77	3D	31	26	73	6B	79	3D	65	ewwindow=1&sky=e
00ECF0C0	65	26	69	65	3D	42	69	67	35	26	71	3D	68	61	63	6B	e&ie=Big5&q=hack
00ECF0D0	69	6E	67	2B	68	69	6A	61	63	6B	26	62	74	6E	47	3D	ing+hijack&btnG=
00ECF0E0	25	65	36	25	39	30	25	39	63	25	65	35	25	62	30	25	%e6%90%9c%e5%b0%
00ECF0F0	38	62	2B	00	68	61	63	6B	69	6E	67	20	68	69	6A	61	8b+.hacking hija
00ECF100	63	6B	20	2D	20	47	6F	6F	67	6C	65	20	E6	90	9C	E5	ck - Google
00ECF110	B0	8B	00	FE	06	BA	00	00	00	00	00	00	00	00	00	00

Figure 4. Extracting Internet search history in memory image

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00F3A710	FF	00	B5	4B	3D	44	92	68	74	74	70	3A	2F	2F	77	39	..K=D.http://w9
00F3A720	34	2E	6D	61	69	6C	2E	71	71	2E	63	6F	6D	2F	63	67	4.mail.qq.com/cg
00F3A730	69	2D	62	69	6E	2F	72	65	61	64	6D	61	69	6C	3F	68	i-bin/readmail?h
00F3A740	69	74	74	79	70	65	3D	30	26	73	69	64	3D	36	68	64	ittype=0&sid=6hd
00F3A750	6D	39	53	4D	32	4A	72	61	38	6D	51	42	51	57	38	6A	m9SM2Jra8mQBQW8j
00F3A760	54	35	76	4E	77	2C	35	2C	7A	54	4F	54	7A	4B	44	79	T5vNw,5,zTOTzKDY
00F3A770	32	26	66	6F	6C	64	65	72	69	64	3D	31	26	74	3D	72	2&folderid=1&t=r
00F3A780	65	61	64	6D	61	69	6C	26	73	3D	26	6D	61	69	6C	69	eadmail&s=&maili
00F3A790	64	3D	5A	43	33	30	32	31	2D	41	5F	34	36	73	6D	52	d=ZC3021-A_46smR
00F3A7A0	33	73	53	45	72	70	6A	39	76	43	30	39	63	64	32	37	3sSErpj9vC09cd27
00F3A7B0	26	6C	70	3D	30	26	6C	70	67	3D	26	74	6F	3D	00	51	&lp=0&lpq=&to=.Q
00F3A7C0	51	E9	82	AE	E7	AE	B1	00	FE	00	05	00	00	00	00	00	Q.....

Figure 5. The browsing history for the received web-email

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00F3C520	50	0A	15	88	08	35	A6	DC	4B	3E	96	11	53	32	66	38	P....5..K>..S2f8
00F3C530	34	64	35	34	2E	77	6D	6C	00	68	74	74	70	3A	2F	2F	4d54.wml}.http://
00F3C540	77	39	34	2E	6D	61	69	6C	2E	71	71	2E	63	6F	6D	2F	w94.mail.qq.com/
00F3C550	63	67	69	2D	62	69	6E	2F	72	65	61	64	6D	61	69	6C	cgi-bin/readmail
00F3C560	3F	68	69	74	74	79	70	65	3D	30	26	73	69	64	3D	36	?hittype=0&sid=6
00F3C570	68	64	6D	39	53	4D	32	4A	72	61	38	6D	51	42	51	57	hdm9SM2Jra8mQBQW
00F3C580	38	6A	54	35	76	4E	77	2C	35	2C	7A	54	4F	54	7A	4B	8jT5vNw,5,zTOTzK
00F3C590	44	79	32	26	66	6F	6C	64	65	72	69	64	3D	31	26	74	Dy2&folderid=1&t
00F3C5A0	3D	72	65	61	64	6D	61	69	6C	26	73	3D	26	6D	61	69	=readmail&s=&mai
00F3C5B0	6C	69	64	3D	5A	43	33	30	32	31	2D	41	5F	34	36	73	lid=ZC3021-A_46s
00F3C5C0	6D	52	33	73	53	45	72	70	6A	39	76	43	30	39	63	64	mR3sSErpj9vC09cd
00F3C5D0	32	37	26	6C	70	3D	30	26	6C	70	67	3D	26	74	6F	3D	27&lp=0&lpq=&to=

Figure 6. The cached file for the received web-email

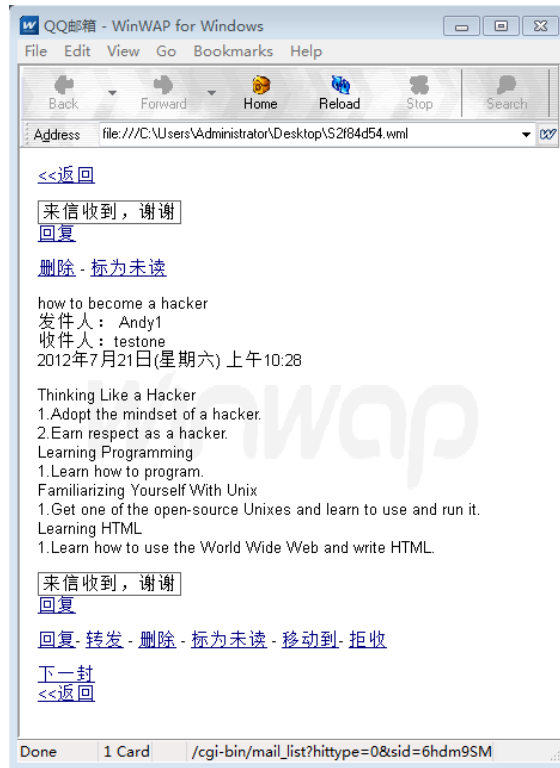


Figure 7. Screenshot of web browsing cache file "S2f84d54.wml"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00EDCE00	FF	00	20	4B	3D	3E	17	68	74	74	70	3A	2F	2F	69	2E	␣. K=>.http://i.
00EDCE10	63	73	2E	68	6B	75	2E	68	6B	2F	7E	6A	62	66	61	6E	cs.hku.hk/~jbfan
00EDCE20	67	00	00	FE	07	AA	00	00	00	00	00	00	00	00	00	00	g.....

Figure 8. S1 - Snapshot after step 1 (timestamp: 01 Jan 2010 00:13:11).

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00EDA200	FF	00	20	4B	3D	3E	17	68	74	74	70	3A	2F	2F	69	2E	␣. K=>.http://i.
00EDA210	63	73	2E	68	6B	75	2E	68	6B	2F	7E	6A	62	66	61	6E	cs.hku.hk/~jbfan
00EDA220	67	00	00	FF	00	31	4B	3D	3E	19	68	74	74	70	3A	2F	g....1K=>.http:/
00EDA230	2F	69	2E	63	73	2E	68	6B	75	2E	68	6B	2F	7E	6A	62	/i.cs.hku.hk/~jb
00EDA240	66	61	6E	67	3F	74	3D	33	37	37	35	30	00	46	6F	72	fang?t=37750.For
00EDA250	65	6E	73	69	63	73	00	FE	07	76	00	00	00	00	00	00	ensics...v.....

Figure 9. S2 - Snapshot after step 2 (timestamp: 01 Jan 2010 00:13:13).

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00ED6E00	FF	00	20	4B	3D	3E	17	68	74	74	70	3A	2F	2F	69	2E	␣. K=>.http://i.
00ED6E10	63	73	2E	68	6B	75	2E	68	6B	2F	7E	6A	62	66	61	6E	cs.hku.hk/~jbfan
00ED6E20	67	00	00	FF	00	31	4B	3D	3E	19	68	74	74	70	3A	2F	g....1K=>.http:/
00ED6E30	2F	69	2E	63	73	2E	68	6B	75	2E	68	6B	2F	7E	6A	62	/i.cs.hku.hk/~jb
00ED6E40	66	61	6E	67	3F	74	3D	33	37	37	35	30	00	46	6F	72	fang?t=37750.For
00ED6E50	65	6E	73	69	63	73	00	FF	00	25	4B	3D	3E	1F	68	74	ensics...%K=>.ht
00ED6E60	74	70	3A	2F	2F	77	77	77	2E	67	6F	6F	67	6C	65	2E	tp://www.google.
00ED6E70	63	6F	6D	2E	68	6B	2F	00	47	6F	6F	67	6C	65	00	FE	com.hk/.Google..
00ED6E80	07	4E	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.N.....

Figure 10. S3 - Snapshot after step 3 (timestamp: 01 Jan 2010 00:13:19).

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00ECDC00	FF	00	20	4B	3D	3E	17	68	74	74	70	3A	2F	2F	69	2E	␣. K=>.http://i.
00ECDC10	63	73	2E	68	6B	75	2E	68	6B	2F	7E	6A	62	66	61	6E	cs.hku.hk/~jbfan
00ECDC20	67	00	00	FF	00	31	4B	3D	3E	19	68	74	74	70	3A	2F	g...lK=>.http://
00ECDC30	2F	69	2E	63	73	2E	68	6B	75	2E	68	6B	2F	7E	6A	62	/i.cs.hku.hk/~jb
00ECDC40	66	61	6E	67	3F	74	3D	33	37	37	35	30	00	46	6F	72	fang?t=37750.For
00ECDC50	65	6E	73	69	63	73	00	FF	00	25	4B	3D	3E	1F	68	74	ensics...%K=>.ht
00ECDC60	74	70	3A	2F	2F	77	77	2E	67	6F	6F	6F	67	6C	65	2E	tp://www.google.
00ECDC70	63	6F	6D	2E	68	6B	2F	00	47	6F	6F	67	6C	65	00	FF	com.hk/.Google..
00ECDC80	00	91	4B	3D	3E	46	68	74	74	70	3A	2F	2F	77	77	77	..K=>Fhttp://www
00ECDC90	2E	67	6F	6F	67	6C	65	2E	63	6F	6D	2E	68	6B	2F	73	.google.com.hk/s
00ECDCA0	65	61	72	63	68	3F	68	6C	3D	7A	68	2D	54	57	26	6E	earch?hl=zh-TW&n
00ECDCB0	65	77	77	69	6E	64	6F	77	3D	31	26	73	6B	79	3D	65	ewindow=1&sky=e
00ECDCC0	65	26	69	65	3D	42	69	67	35	26	71	3D	68	61	63	6B	e&ie=Big5&q=hack
00ECDCD0	69	6E	67	2B	68	69	6A	61	63	6B	26	62	74	6E	47	3D	ing+hijack&btnG=
00ECDCE0	25	65	36	25	39	30	25	39	63	25	65	35	25	62	30	25	%e6%90%9c%e5%b0%
00ECDCF0	38	62	2B	00	68	61	63	6B	69	6E	67	20	68	69	6A	61	8b+.hacking hija
00ECDD00	63	6B	20	2D	20	47	6F	6F	67	6C	65	20	E6	90	9C	E5	ck - Google
00ECDD10	B0	8B	00	FE	06	BA	00	00	00	00	00	00	00	00	00	00

Figure 11. S4 - Snapshot after step 4 (timestamp: 01 Jan 2010 00:13:58).

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00F31400	FF	00	20	4B	3D	3E	17	68	74	74	70	3A	2F	2F	69	2E	␣. K=>.http://i.
00F31410	63	73	2E	68	6B	75	2E	68	6B	2F	7E	6A	62	66	61	6E	cs.hku.hk/~jbfan
00F31420	67	00	00	FF	00	31	4B	3D	3E	19	68	74	74	70	3A	2F	g...lK=>.http://
00F31430	2F	69	2E	63	73	2E	68	6B	75	2E	68	6B	2F	7E	6A	62	/i.cs.hku.hk/~jb
00F31440	66	61	6E	67	3F	74	3D	33	37	37	35	30	00	46	6F	72	fang?t=37750.For
00F31450	65	6E	73	69	63	73	00	FE	07	76	4B	3D	3E	1F	68	74	ensics...vK=>.ht
00F31460	74	70	3A	2F	2F	77	77	2E	67	6F	6F	6F	67	6C	65	2E	tp://www.google.
00F31470	63	6F	6D	2E	68	6B	2F	00	47	6F	6F	67	6C	65	00	FE	com.hk/.Google..
00F31480	07	4E	4B	3D	3E	46	68	74	74	70	3A	2F	2F	77	77	77	.NK=>Fhttp://www
00F31490	2E	67	6F	6F	67	6C	65	2E	63	6F	6D	2E	68	6B	2F	73	.google.com.hk/s
00F314A0	65	61	72	63	68	3F	68	6C	3D	7A	68	2D	54	57	26	6E	earch?hl=zh-TW&n
00F314B0	65	77	77	69	6E	64	6F	77	3D	31	26	73	6B	79	3D	65	ewindow=1&sky=e
00F314C0	65	26	69	65	3D	42	69	67	35	26	71	3D	68	61	63	6B	e&ie=Big5&q=hack
00F314D0	69	6E	67	2B	68	69	6A	61	63	6B	26	62	74	6E	47	3D	ing+hijack&btnG=
00F314E0	25	65	36	25	39	30	25	39	63	25	65	35	25	62	30	25	%e6%90%9c%e5%b0%
00F314F0	38	62	2B	00	68	61	63	6B	69	6E	67	20	68	69	6A	61	8b+.hacking hija
00F31500	63	6B	20	2D	20	47	6F	6F	67	6C	65	20	E6	90	9C	E5	ck - Google
00F31510	B0	8B	00	FE	06	BA	00	00	00	00	00	00	00	00	00	00

Figure 12. S5 - Snapshot after step 5.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00F29000	FF	00	20	4B	3D	3E	17	68	74	74	70	3A	2F	2F	69	2E	␣. K=>.http://i.
00F29010	63	73	2E	68	6B	75	2E	68	6B	2F	7E	6A	62	66	61	6E	cs.hku.hk/~jbfan
00F29020	67	00	00	FF	00	31	4B	3D	3E	19	68	74	74	70	3A	2F	g...lK=>.http://
00F29030	2F	69	2E	63	73	2E	68	6B	75	2E	68	6B	2F	7E	6A	62	/i.cs.hku.hk/~jb
00F29040	66	61	6E	67	3F	74	3D	33	37	37	35	30	00	46	6F	72	fang?t=37750.For
00F29050	65	6E	73	69	63	73	00	FF	00	19	4B	3D	43	62	68	74	ensics...K=Cbht
00F29060	74	70	3A	2F	2F	77	77	2E	61	73	6B	2E	63	6F	6D		tp://www.ask.com
00F29070	2F	00	00	FF	00	43	4B	3D	43	66	68	74	74	70	3A	2F	/...CK=Cfhttp://
00F29080	2F	77	77	77	2E	61	73	6B	2E	63	6F	6D	3A	38	30	2F	/www.ask.com:80/
00F29090	3F	74	3D	30	34	32	37	39	00	41	73	6B	2E	63	6F	6D	?t=04279.Ask.com
00F290A0	20	2D	20	57	68	61	74	27	73	20	59	6F	75	72	20	51	- What's Your Q
00F290B0	75	65	73	74	69	6F	6E	3F	00	FE	07	14	6B	79	3D	65	uestion?...ky=e
00F290C0	65	26	69	65	3D	42	69	67	35	26	71	3D	68	61	63	6B	e&ie=Big5&q=hack
00F290D0	69	6E	67	2B	68	69	6A	61	63	6B	26	62	74	6E	47	3D	ing+hijack&btnG=
00F290E0	25	65	36	25	39	30	25	39	63	25	65	35	25	62	30	25	%e6%90%9c%e5%b0%
00F290F0	38	62	2B	00	68	61	63	6B	69	6E	67	20	68	69	6A	61	8b+.hacking hija
00F29100	63	6B	20	2D	20	47	6F	6F	67	6C	65	20	E6	90	9C	E5	ck - Google
00F29110	B0	8B	00	FE	06	BA	00	00	00	00	00	00	00	00	00	00

Figure 13. S6 - Snapshot after step 6 (timestamp: 01 Jan 2010 00:35:50).

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00F5B800	FF	00	20	4B	3D	3E	17	68	74	74	70	3A	2F	2F	69	2E	└. K=>.http://i.
00F5B810	63	73	2E	68	6B	75	2E	68	6B	2F	7E	6A	62	66	61	6E	cs.hku.hk/~jbfan
00F5B820	67	00	00	FF	00	31	4B	3D	3E	19	68	74	74	70	3A	2F	g....lK=>.http:/
00F5B830	2F	69	2E	63	73	2E	68	6B	75	2E	68	6B	2F	7E	6A	62	/i.cs.hku.hk/~jb
00F5B840	66	61	6E	67	3F	74	3D	33	37	37	35	30	00	46	6F	72	fang?t=37750.For
00F5B850	65	6E	73	69	63	73	00	FF	00	19	4B	3D	43	62	68	74	ensics....K=Cbht
00F5B860	74	70	3A	2F	2F	77	77	77	2E	61	73	6B	2E	63	6F	6D	tp://www.ask.com
00F5B870	2F	00	00	FF	00	43	4B	3D	43	66	68	74	74	70	3A	2F	/....CK=Cfhttp:/
00F5B880	2F	77	77	77	2E	61	73	6B	2E	63	6F	6D	3A	38	30	2F	/www.ask.com:80/
00F5B890	3F	74	3D	30	34	32	37	39	00	41	73	6B	2E	63	6F	6D	?t=04279.Ask.com
00F5B8A0	20	2D	20	57	68	61	74	27	73	20	59	6F	75	72	20	51	- What's Your Q
00F5B8B0	75	65	73	74	69	6F	6E	3F	00	FF	00	60	4B	3D	44	62	uestion?...`K=Db
00F5B8C0	68	74	74	70	3A	2F	2F	77	77	77	2E	61	73	6B	2E	63	http://www.ask.c
00F5B8D0	6F	6D	3A	38	30	2F	77	65	62	3F	71	3D	68	61	63	6B	om:80/web?q=hack
00F5B8E0	69	6E	67	2B	68	69	6A	61	63	6B	26	71	73	72	63	3D	ing+hijack&qsrc=
00F5B8F0	30	26	6F	3D	30	26	6C	3D	64	69	72	00	41	73	6B	2E	0&o=0&l=dir.Ask.
00F5B900	63	6F	6D	20	2D	20	57	68	61	74	27	73	20	59	6F	75	com - What's You
00F5B910	72	20	51	75	65	73	74	69	6F	6E	3F	00	FE	06	B1	00	r Question?.....

Figure 14. S7 - Snapshot after step 7 (timestamp: 01 Jan 2010 00:40:02).