DFRWS 2011 Forensics Challenge

Jewan Bang (jwbang@korea.ac.kr)
Jungheum Park (junghmi@korea.ac.kr)
Hyunji Chung (foryou7187@korea.ac.kr)
Dohyun Kim (exdus84@korea.ac.kr)
Sangjin Lee (sangjin@korea.ac.kr)

Digital Forensic Research Center (DFRC)
Center for Information Security Technologies (CIST)
Korea University
http://forensic.korea.ac.kr

Contents

1. INTRODUCTION ---- 4

1.1. CHALLENGE SCENARIO ---- 4
1.2. OVERVIEW OF CHALLENGE DATA ---- 6
1.2.1. BASIC INFORMATION OF CHALLENGE DATA ---- 6
1.2.2. MOTOROLA DROID ---- 7
1.2.3. DETAILS OF FLASH MEMORY IMAGES ---- 8

2. FORENSIC ANALYSIS TECHNIQUES ---- 13

2.1. METHODS FOR ANALYZING FLASH MEMORY ---- 13
2.2. YAFFS2 FILE SYSTEM RECONSTRUCTION ---- 13
2.2.1. YAFFS2FORDROIDIMAGE ---- 19
2.3. FLASH MEMORY ANALYSIS WITHOUT SPARE AREA ---- 15
2.3.1. PAGE CLASSIFICATION ---- 15
2.3.2. SQLITE PAGE ANALYSIS ---- 18
2.3.3. YAFFS2PAGEANALYZER ---- 19

3. DIGITAL INVESTIGATION ---- 20

3.1. SCENARIO 1: SUSPICIOUS DEATH ---- 20
3.1.1. WAS THE DEVICE "ROOTED"? ---- 20
3.1.2. DID THE DEVICE HAVE "ADB" ENABLED? ---- 20
3.1.3. WAS THE COLLECTION PROCESS SOUND? ---- 22
3.1.4. LIST APPLICATIONS INSTALLED ---- 23
3.1.5. INDICATE VERSION INFORMATION ---- 26
3.1.6. RECOVER CREDENTIALS, IF POSSIBLE ---- 26
3.2. SCENARIO 2: INTELLECTUAL PROPERTY THEFT ---- 29
3.2.1. WAS THE DEVICE "ROOTED"? ---- 29
3.2.2. DID THE DEVICE HAVE "ADB" ENABLED? ---- 29
3.2.3. WAS THE COLLECTION PROCESS SOUND? ---- 30
3.2.4. LIST APPLICATIONS INSTALLED ---- 31
3.2.5. INDICATE VERSION INFORMATION ---- 35
3.2.6. RECOVER CREDENTIALS, IF POSSIBLE ---- 37
3.3. SPECIFICATION ---- 38
3.3.1. SCENARIO 1 – SMS/MMS ---- 38
3.3.2. SCENARIO 1 – EMAIL ---- 42
3.3.3. SCENARIO 1 – CONTACTS ---- 42

3.3.4. SCENARIO 1 – ACCESS TO WEB SERVER AND DOWNLOAD FILES ----------42
3.3.5. SCENARIO 1 – SDCARD ----------43
3.3.6. SCENARIO 2 – MEDIA MOUNTER(/DATA/APP/COM.ANDRIOD.MM.APK) ANALYSIS -------48
3.3.7. SCENARIO 2 – ALARM ----------61
3.3.8. SCENARIO 2 – DOWNLOAD----------62
3.3.9. SCENARIO 2 – LOCATION INFORMATION ----------64
3.3.10. SCENARIO 2 – WEB BROWSER ----------65
3.3.11. SCENARIO 2 – GOOGLE MAP ----------67
3.3.12. SCENARIO 2 – CALL HISTORY ----------69
3.3.13. SCENARIO 2 – CONTACTS----------69
3.3.14. SCENARIO 2 – SMS/MMS----------69
3.3.15. SCENARIO 2 – GOOGLETALK----------71
3.3.16. SCENARIO 2 – DEVICE INFORMATION ----------73
3.3.17. SCENARIO 2 – TWITTER ----------75
3.3.18. SCENARIO 2 – EMAIL ----------81
3.3.19. SCENARIO 2 – CALENDAR ----------88
3.3.20. SCENARIO 2 - SDCARD ----------93

4. CONCLUSION---------- 100

5. FURTHER RESEARCH---------- 103

6. ACKNOWLEDGMENTS ---------- 103

7. REFERENCES ---------- 103

1. Introduction

DFRWS Forensic Challenge has been held every year since 2005. For general topics in Challenge, a problem likely to be a hot issue in the digital forensic field is mostly selected. As a result, there are a great many of researches carried out on related topics even after Challenge is over.

This year's topic was about analyzing memory used for Android smartphones. Since each cell of the flash memory is quite limited in the frequency of use, it is needed to read and write data all over the area as evenly as possible. For this, a device is needed for the conversion between a file system and physical memory. Therefore, additional information identical with a flash memory's spare domain is definitely required to reconstruct a file system using the flash memory's physical images.

Adroid smartphones widely provided these days generally use a file system for the sake of a flash memory, such as YAFFS (Yet Another File System). As for YAFFS, Tag domain is employed in order to convert the flash memory's physical location and file system's logical location. Therefore, in order to reconstruct YAFFS physical images, Tag domain must be required. A physical image absent of Tag domain cannot possibly reconstruct a functional file system.

The purpose of this challenge is to conduct an effective digital forensic analysis using the flash memory's physical images acquired through Android smartphones. if Tag domain is acquired and YAFFS physical images are produced at the same time, an analysis will be able to be conducted reconstruct completly file system. In this case, there calls for a method to effectively analyze each page by using the characteristics of flash memories.

1.1. Challenge Scenario

The detailed scenario of this Challenge is shown at the website of DFRWS, and the following is the contents of the scenario.

• Scenario 1

Donald Norby was found dead in his home with a single bullet to the head. It is unclear whether this is a suicide or homicide. The largest question revolves around the victim's potential connections to an organized criminal group called KRYPTIX. You have been asked to perform a forensic examination of Norbyâ€™s Android device found at the scene in order to determine his activities and, possibly, who he communicated with prior to his death. Your ultimate goal is to determine whether he killed himself or was murdered and provide any further leads to the investigator.

• Scenario 2

A serious breach of security occurred within an organization named SwiftLogic Inc.; valuable documents containing designs of a new product named Palomino were confirmed to have been leaked to a competitor. Based on an internal investigation, Yob Taog is suspected of the leak and was suspended pending investigation. Taog's Android smartphone was - surprisingly - voluntarily submitted by Taog for further investigation. Your goal in this investigation is to document any evidence that intellectual property was stolen, to support termination of Yob Toag and potential criminal charges. You are asked to perform a forensic analysis of his device for evidence of the breach.

The scenario can be summarized as follows:

- Scenario 1

    - Donal Norby was found dead with his head shot with a gun.
    - It is assumed that he is related with a criminal organization called KRYPTIX.
    - We must find out who he talked to on the Android smartphone before his death.
    - Based on the evidence, we will draw conclusion whether he committed suicide or was murdered.

- Scenario 2

    - Some valuable documents for Palomino, SwiftLogic's new product were leaked to a rival company.
    - Yob Taog was spotted as a suspect of having leaked the confidential document.
    - Yob Taog voluntarily submitted Android smartphone for an investigation.
    - We must find evidence that proves that the confidential data were leaked through his smartphone.

Submissions should include a detailed analysis in report format that presents:

- Addresses the specific goals within each scenario.
- Provides a reconstruction and timeline of relevant events on each device.
- Highlights any leads or new evidence that would advance or widen the investigations.
- State an opinion or your findings on the following evidentiary issues:

    - Was the device "rooted"?
    - Did the device have "adb" enabled?
    - Was the collection process sound? (and can you verify the recorded acquisition log)
    - List applications installed
    - Indicate version information
    - Recover credentials, if possible

1.2. Overview of Challenge data

Challenge Data consists of physical images collected from an Android smartphone. In addition, log files are included, which have the value of hash created when each image was collected. In addition, the attached log file lists the actions of acquiring smartphone data in a chronological order.

1.2.1. Basic Information of Challenge Data

The following is the basic information about Challenge Data (Case1.tgz, Case2.tgz) received from the website of DFRWS. Case1.tgz and Case2.tgz include memory images collected from an Android smartphone.

Table 1. Memory Images of Case1.tgz (Scenario 1)

Image	Partition	Permission	File system	Note	yaffs page size
mtdblock0	/config	ro	YAFFS	-	2048
mtdblock1	-	-	-	*empty*	-
mtdblock3	-	-	-	kernel	-
mtdblock4	/system	ro	YAFFS	-	2048
mtdblock5	/cache	rw	YAFFS	-	2048
mtdblock6	/data	rw	YAFFS	--	2048
mtdblock7	-	-	-	*empty*	-
SDCard	/sdcard	rw	FAT	-	-

Table 2. Memory Images of Case2.tgz (Scenario 2)

Image	Partition	Permission	File system	Note	yaffs page size
mtd0 mtd1 mtd2	/config (not sure)	-	YAFFS (not sure)	-	-
mtd3	-	-	-	empty	-
mtd4 mtd5	-	-	-	kernel	-
mtd6	/system	-	YAFFS	-	2048
mtd7	/cache	-	YAFFS	-	2048
mtd8	/data	-	YAFFS	-	2048
mtd9	-	-	-	empty	-
sdcard	/sdcard	-	FAT	-	-

After reviewing the Challenge image file, it turns out that Motorola DROID is the Android smartphone that has acquired above images.

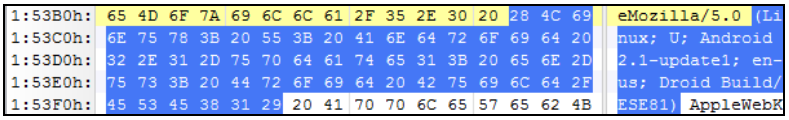


Figure 1. Device information of Scenario 1 (mtdblock6.img)

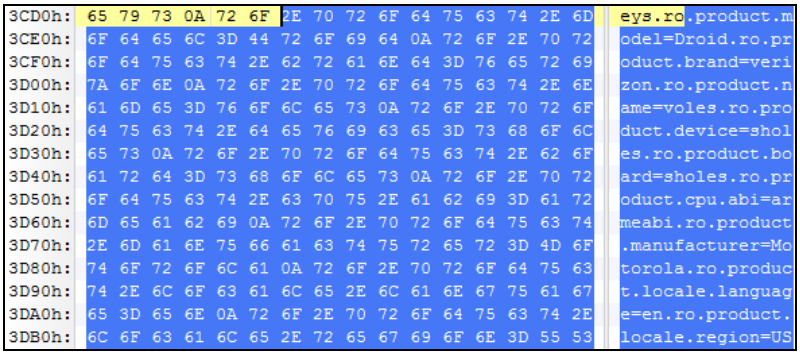


Figure 2. Device information of Scenario 1 (mtd8.dd)

1.2.2. Motorola DROID

The Motorola Droid is an Internet and multimedia enabled smartphone designed by Motorola, which runs Google's Android operating system. The brand name Droid is a trademark of Lucasfilm licensed to Verizon Wireless.

In the United States, the handset is distributed exclusively by Verizon Wireless; a similar Motorola model running Android is however available from Cellular South. Features of the phone include Wi-Fi networking, a 5-megapixel low light capable digital camera, a standard 3.5 mm headphone jack, interchangeable battery, 3.7-inch 854 x 480 touchscreen display. It also includes microSDHC support with bundled 16 GB card, free turn-by-turn navigation from Google Maps, sliding QWERTY keyboard, and Texas Instruments OMAP 3430 processor. The Motorola Droid runs Android version 2.2. The phone does not, however, run the re-branded Motoblur interface for Android, instead providing the Google Experience skin and application stack. The Droid has a hearing aid compatibility (hac) rating of M3/T3. The phone was the first to ship with free Google Maps Navigation (beta) installed. The Droid had been publicized under the codenames Sholes and Tao and the model number A855. In Latin America and Europe, the model number is A853 (Milestone).

Figure 3. Motorola DROID

Table 3. Motorola DROID Specification

Carrier	Verizon
Available	October 30th 2009
Networks	CDMA dual band (800/1900 MHz); CDMA2000 1xRTT/1xEV-DO rev.0/1xEV-DO rev.A
Display	3.7-inch screen with 854×480 (16:9 widescreen) capacitive touchscreen
Camera	5 megapixel camera with autofocus and LED flash and video recording
Operating system	Google Android 2.0 OS
Input	QWERTY keyboard, touchscreen
CPU	600 MHz ARM Cortex A8 Processor
Memory	256MB RAM/512 MB ROM
Memory card	microSD/ microSDHC
Connectivity	GPS, Wi-Fi, 3.5mm HeadPhone Jack
Misc	AMR-NB/WB, MP3, PCM/WAV, AAC, AAC+, eAAC+, WMA
Media	MPEG-4, H263, H264, WMV
Battery	1400mAh Li-ion
Talk Time	420 minutes
Standby Time	450 hours
Dimensions	60.00 x 115.80 x 13.70 mm
Weight	169g

1.2.3. Details of Flash Memory Images

It is the detailed information of each image.

1.2.3.1. Scenario 1's Images

Name	mtdblock0.img
Size	1.50MB (1,572,864 bytes)
Description	A flash memory image from Motorola DROID
Hash Value	MD5 : 10f39bed760d85980117a29364feeeb1

Name	mtdblock1.img
Size	384KB (393,216 bytes)
Description	A flash memory image from Motorola DROID All data is 0xFF or 0x00
Hash Value	MD5 : 5dfd83e314d645c6f41d86915a7b98eb

Name	mtdblock3.img
Size	4.50MB (4,718,592 bytes)

Description	A flash memory image from Motorola DROID
Hash Value	MD5 : 7673f7ef637274d6bb48892a157d877d

Name	mtdblock4.img
Size	140MB (147,193,856 bytes)
Description	A flash memory image from Motorola DROID
Hash Value	MD5 : fa503c91751afccf175092a29a2b2637

Name	mtdblock5.img
Size	92.6MB (97,124,352 bytes)
Description	A flash memory image from Motorola DROID
Hash Value	MD5 : ade41709773a63a4ed09d66f3a7637cd

Name	mtdblock6.img
Size	261MB (274,464,768 bytes)
Description	A flash memory image from Motorola DROID
Hash Value	MD5 : 0f1a515a89e2a368aff3fcd818bcab94

Name	mtdblock7.img
Size	2MB (2,097,152 bytes)
Description	A flash memory image from Motorola DROID All data is 0xFF or 0x00
Hash Value	MD5 : b23b5d09162b92c0284923a7f628d2a5

Name	SDCard.img
Size	14.9GB (16,039,018,496 bytes)
Description	A flash memory image of an external SD card
Hash Value	MD5 : fdeb635287893022ff807c7dc18a74c6

1.2.3.2. Scenario 2's Images

Name	mtd0.dd
Size	660KB (675,840 bytes)
Description	A flash memory image from Motorola DROID
Hash Value	SHA1 : 160433772347c94bd3abc89952677942d423515b

Name	mtd1.dd

Size	396KB (405,504 bytes)
Description	A flash memory image from Motorola DROID
Hash Value	SHA1 : 81d32137cc3a35e535dfa8a706981d4494267e7a

Name	mtd2.dd
Size	396KB (405,504 bytes)
Description	A flash memory image from Motorola DROID
Hash Value	SHA1: 97f2383facfc8c8319e6725674d5912fc91f04fa

Name	mtd3.dd
Size	396KB (405,504 bytes)
Description	A flash memory image from Motorola DROID
Hash Value	SHA1: b22a6c5b8248b0b3bcf760305f69f4af68b1bac4

Name	mtd4.dd
Size	3.60MB (3,784,704 bytes)
Description	A flash memory image from Motorola DROID
Hash Value	SHA1: f3af16c8659958f34eb4e3e6f585c3f0058f6bc6

Name	mtd5.dd
Size	4.64MB (4,866,048 bytes)
Description	A flash memory image from Motorola DROID
Hash Value	SHA1: 83bbe12bf2e4ae455486a7c6c1e6044b53526149

Name	mtd6.dd
Size	144MB (151,793,664 bytes)
Description	A flash memory image from Motorola DROID All data is 0xFF or 0x00
Hash Value	SHA1: 45d2bd8b6a571dddfb13ccf7c3f3134af15ca084

Name	mtd7.dd
Size	95.5MB (100,159,488 bytes)
Description	A flash memory image from Motorola DROID
Hash Value	SHA1: e238dd5998ce26c6566bc4747bc8ff1cd7c1f0bc

Name	mtd8.dd
Size	269MB (283,041,792 bytes)
Description	A flash memory image from Motorola DROID

Hash Value	SHA1: 339b6cfcffcc1206ca75069d3f1cc7205d5d6be4

Name	mtd9.dd
Size	2.06MB (2,162,688 bytes)
Description	A flash memory image from Motorola DROID All data is 0xFF or 0x00
Hash Value	SHA1: 4e71e3894203e64ff5201f692510afdafb4c08b7

Name	sdcard.dd
Size	14.8GB (15,931,539,456 bytes)
Description	A flash memory image of an external SD card
Hash Value	MD5 : 491a0688a4733c36c2a24cfc8b9023c0

1.2.3.3. Comparision between Scenario 1 & scenario 2 Images

Relationships between images acquired in Scenarios 1 and 2 are as follows. (Refer to the below table.)

Table 4. Image files of Scenario 1 and 2

Scenario 1				Scenario 2			
Image	Partition	Permission	Note	Image	Partition	Permission	Note
mtdblock0	/config	ro	YAFFS	mtd0 mtd1 mtd2	/config (not sure)	ro	YAFFS (not sure)
mtdblock1	-	-	empty	mtd3	-	-	empty
mtdblock3	-	-	kernel	mtd4 mtd5	-	-	kernel
mtdblock4	/system	ro	YAFFS	mtd6	/system	ro	YAFFS
mtdblock5	/cache	rw	YAFFS	mtd7	/cache	rw	YAFFS
mtdblock6	/data	rw	YAFFS	mtd8	/data	rw	YAFFS
mtdblock7	-	-	empty	mtd9	-	-	empty
SDCard.img	/sdcard	rw	FAT	sdcard.dd	/sdcard	rw	FAT

Images for Scenario 1 were acquired through dd in each partition. In case of acquiring each partition through dd, a spare area that allows for the reconstruction of a file system cannot acquired. Target device employs a 64-byte spare area, whereas images for Scenario 1 were acquired in the form in which a spare area is missing.

Images for Scenario 2 were acquired through nanddump. While acquiring nanddump, a 64-byte spare area must be acquired together in order to reconstruct a file system. Through an analysis, we could reconstruct a file system for Scenario 2. (YAFFS image reconstruction will be elaborated in Section 2.)

Domains that may be changed by the user, except for Kernel Domain, are /cache, /data, /sdcard partitions. In this report, an analysis was conducted targeting information of the selected area for a digital forensic analysis.

2. Forensic Analysis Techniques

2.1. Methods for Analyzing Flash Memory

In order to analyze the physical Flash Memory, it is most important to understand the area of physical memory. Firstly, pages and the size of blocks that distinguish Meta area from User area must be figured out. Afterwards, the mapping information that interconnects logical sectors and physical sectors is needed. As it was mentioned above, the mapping information is saved in a spare area or a specific area.

Once the mapping information is acquired, the newest page of each block is selected based on corresponding mapping information to execute a compounding procedure. As data is renewed, new pages are allocated in each block to save the data. Consequently, the data to verify the newest page is also required. Such data also need to be verified through Meta information of a block or a spare.

Information regarding Mapping or the newest pages is relatively easily accessible by executing a statistical process of compound of all spares and block meta.

2.2. YAFFS2 File System Reconstruction

The targeted Android dump image is YAFFS2 (Yet Another Flash File System 2). YAFFS2 is a file system used at NAND flash memory, and generates a file system structure by scanning the entire memory area using LFS (log-structured file system) method when mounting. In addition, because it reuses all data of the relevant file when modifying the file, there is high possibility to find the existing data at the unallocation area. The Chunk size of Target dump image is 2,048bytes, and Tag (Spare area) is 64bytes.

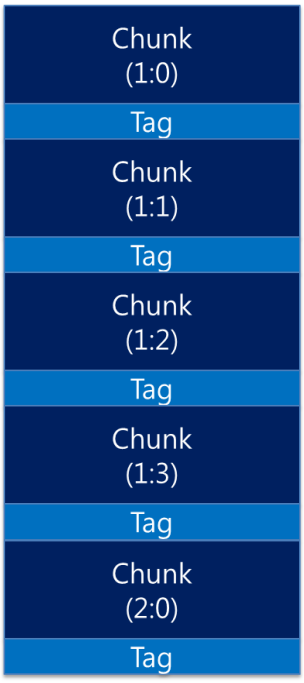


Figure 4. Chunk and Tag in YAFFS2

Of the two scenarios for this Challenge, it is impossible to reconstruct the file system because the Tag area does not exist in the Droid flash memory dump image of the Scenario 1. However, it is possible to reconstruct the file system in the Scenario 2, because the Droid flash memory dump image of the Scenario 2 includes the 64bytes of Tag area.

Initially, we tried to reconstruct the file system of flash memory dump image by referring to the results of the existing studies on YAFFS2. However, it was confirmed that it has a different structure from the known format. Therefore, we confirmed from the analysis that it has a little bit of different structure.

The general structure follows the existing structure of YAFFS2, but Tag, Extended Tag, Chunk Header are in the following structures.

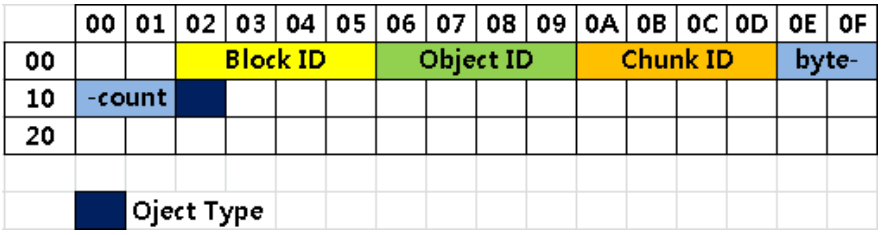


Figure 5. 'Tag' structure of Droid flash memory

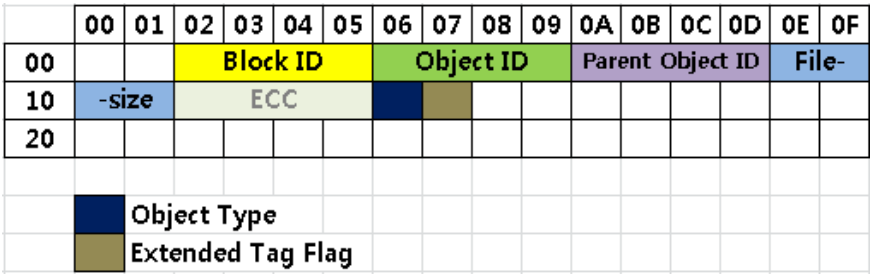


Figure 6. 'Extended Tag' structure of Droid flash memory

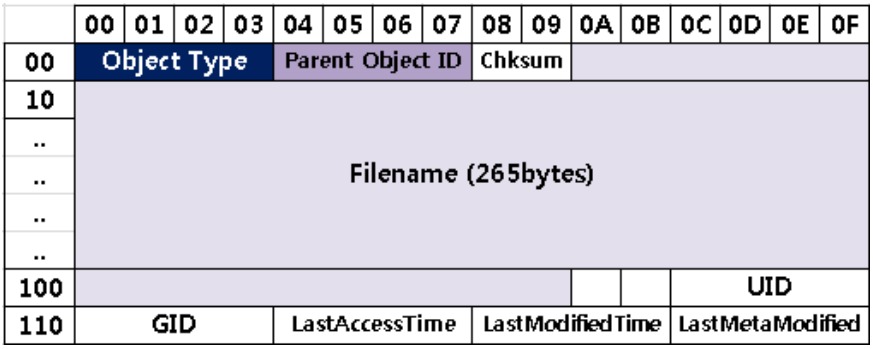


Figure 7. 'Chunk Header' structure of Droid flash memory

2.2.1. yaffs2forDroidImage

Based on this analysis, we developed a tool (yaffs2fordroidimage.exe) that can reconstruct Droid flash memory dump image, and could recover the file system of 'Scenario 2' using this tool. This is included in the file submitted with the report.

The result of recovery is as follows.

Table 5. The number of recovered file and folder

Scenario 2.	Folders	Files	Size
mtd7.dd	1	24	64.0MB (67,178,801 bytes)
mtd8.dd	545	2,036	176MB (184,641,106 bytes)

2.3. Flash Memory Analysis without Spare Area

Since the flash memory dump image of Scenario 2 has a spare area, tag information of each page in YAFFS can be checked. Therefore the file system can be reconstructed in Scenario 2. In contrast, in Scenario 1, there is no spare area in the image and tag information of each page can't be checked. Therefore, the file system can't be reconstructed in Scenario 1. Accordingly, techniques for efficiently analyzing Scenario 1 are needed.

2.3.1. Page Classification

Before analyzing pages in an image in YAFFS, the pages are first classified.

2.3.1.1. Page Size Detection

To classify the pages in a YAFFS image, first the page size has to be checked. In the case of image 'mtdblock6.img', you can see that the data is divided into 0x800 (2,048 bytes) chunks. The page size is detected for each image, after which analysis is done.

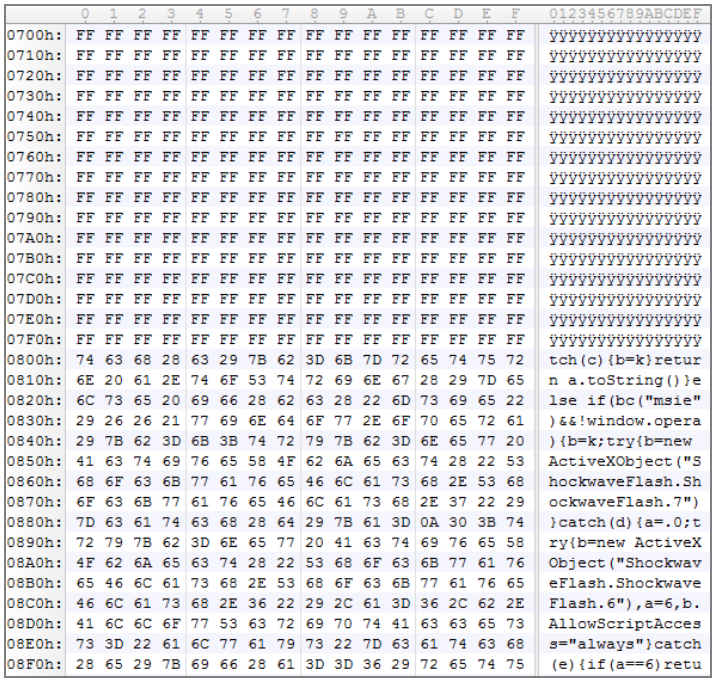


Figure 8. Page size detection

2.3.1.1. Chunk Header Classification

The task performed once the page size is detected is identifying the chunk header page in YAFFS. The chunk header page contains file or folder information. As user data are not stored in this page, it can be excluded from analysis. Like this the list of files or folders that were in the image file from the classified chunk header page is checked.

Performing chunk header classification on the file 'mtdblock6.img', it was found that many chunk header pages were included, as shown in the table below, and as an end result the page size of the object of analysis could be reduced.

Table 6. Result of chunk header classification for mtdblock6.img

Classification	Total size (bytes)	Page number (Total size/Page size)
Original Image	274,464,768	134,016
Chunk header Pages	183,310,336	89,507
Classified Pages A	91,154,432	44,509

In the steps that follow, the concerned pages are those classified as 'Classified pages A'.

2.3.1.3. Hash-based Classification

After chunk header page classification, duplicate pages are removed using a hash algorithm. In flash memory, as per the characteristics of FTL, when data in a page is edited, the original page is not modified but a new page is created. During this process there is a chance that duplicate pages could be created. They need to be removed so that efficient analysis can take place.

Performing hash-based classification for 'Classified pages A', the page size of the object of analysis could be reduced, as shown in the table below.

Table 7. Result of hash-based classification for Classified pages A

Classification	Total size (bytes)	Page number (Total size/Page size)
Classified Pages A	91,154,432	44,509
Duplicated Pages	7,557,120	3,690
Classified Pages B	83,597,312	40,819

In the steps that follow, the concerned pages are those classified as 'Classified pages B'.

2.3.1.2. Statistical-based Classification

The above step resulted in the reduction in the number of page to 40,819. In this step, pages are classified into random pages and non-random pages. Typical random data for Android smartphones include image files (JPEG, PNG, GIF) and archive files (ZIP). For random data, there is high probability that data size exceeds the page size. As pages are scattered in the memory as per the characteristics of flash memory, it is very difficult to check random data exactly. If pages are classified into random pages based on statistics, possibility of data recovery can be improved.

To classify into random pages, first signature search has to be attempted for the main random file. This is because even for random files there are quite a bit of non-random data in the file header. Through this step the header can be classified in the random file. After this, poker test is performed on each page for random page classification. Notice that in the last page of the file, there is a ram slack, so when the test is performed this area has to be excluded.

The table below shows the results of performing statistical-based classification on 'Classified pages B'.

Table 8. Result of statistical-based classification for Classified pages B

Classification	Total size (bytes)	Page number (Total size/Page size)
Classified Pages B	83,597,312	40,819
Random Pages	2,922,496	1,427
Non-random Pages	80,674,816	39,392

After the classification, the size of random pages was about 2.78MB and most pages were non-random pages. For random pages, recovery of archive files can be attempted along with carving of image files.

In the steps that follow, the pages concerned are ones that were classified as 'non-random pages'.

2.3.1.3. SQLite Page Classification

One of the most important files for Android smartphones is the SQLite database file. As user data gets stored in this file, it has to be isolated for more thorough analysis.

The official SQLite site (http://www.sqlite.org) shows the SQLite DB file structure in detail. The DB file is made up of various types of pages. The header of the file contains the page size used. It was found that the SQLite DB file in the Challenge image was using page size of 1,035 bytes. Therefore in this step search is done in the unit of 1,024 bytes to classify SQLite pages.

The table below shows the results of performing SQLite page classification on 'non-random pages'.

Table 9. Result of SQLite page classification for Non-random pages

Classification	Total size (bytes)	Page number (Total size/SQLite Page size)
Non-random Pages	80,674,816	78784
SQLite Header Pages + Pointer Map Pages	3,774,464	3686
Table Leaf Pages	3,773,440	3685
Table Internal Pages	211,968	207
Index Leaf Pages	2,089,984	2,041
Index Internal Pages	233,472	228
Slack Or Overflow Pages	393,216	384
Free Pages	203,776	199
Non-random Pages except SQLite Pages	69,992,448	68352

It was found that the total size of SQLite pages was about 10.1MB. In later step, analysis is done on table leaf pages, where the user data are stored.

2.3.1.4. Non-random Pages except SQLite Pages

Carving is attempted on the data area that excludes SQLite pages (about 66.7MB in size) in order to try to recover valid data. As a result, a number of HTML and XML files were recovered.

For other pages, string character extraction was attempted in order to check the contents.

2.3.2. SQLite Page Analysis

Analysis is done on the SQLite pages which were found in the previous step. Note that the actual data gets stored in SQLite table leaf pages. To extract each record of the database accurately, schema information of the database is needed. But as schema information can't be obtained because the file is not normal, column information of records can't be checked.

Records are stored in a cell structure in a page. By interpreting the cell structure the data type and length can be found for each column. Record carving is performed on each page in the same way. Column information of records was used in classifying records included in different tables. That is, carved records whose column information (type, length, etc.) was the same were grouped together and outputted in a CSV format. The output file name was calculated using the algorithm shown below so that records having the same structure were outputted in a single file.

CSV filename = SHA-1(Column1 ¦¦ Column2 ¦¦ …. ¦¦ ColumnN)

Important thing in record carving is recovering time information. As the SQLite database file analyzed mostly used Unix time (millisecond value), the format was used in automatically detecting the columns that contained time information. The columns found were outputted visually. (As the time region is set to New York with daylight saving, UTC-4 is used.)

Performing the record carving algorithm resulted in the creation of 163 CSV files, which implies that there are 163 tables. The figure below shows the extracted files. After all records are extracted, duplicate records must be removed.

Figure 9. Extracted DB records from SQLite table leaf pages

See separate attachment for the result file of this step.

2.3.3. yaffs2PageAnalyzer

Based on the explanation given above, a tool that classifies and analyzes pages in a YAFFS image without a spare area was developed (yaffs2PageAnalyzer.exe). It was used to analyze the YAFFS image of Scenario 1. The tool file and results of analysis are included in the file submitted with the report.

3. Digital Investigation

3.1. Scenario 1: Suspicious Death

Donald Norby was found dead in his home with a single bullet to the head. It is unclear whether this is a suicide or homicide. The largest question revolves around the victim's potential connections to an organized criminal group called KRYPTIX. You have been asked to perform a forensic examination of Norby's Android device found at the scene in order to determine his activities and, possibly, who he communicated with prior to his death. Your ultimate goal is to determine whether he killed himself or was murdered and provide any further leads to the investigator.

State an opinion or your findings on the following evidentiary issues:

3.1.1. Was the device "rooted"?

According to the acquisition log, when the device was first obtained, it was not in the 'rooted' state. Later, the partition information, which was mounted in the device, was checked, and the temporary rooting was attempted in order to obtain the data of each partition. The forensic analyst used the SuperOneClick and attempted the temporary rooting, and accessing the 'adb shell,' he confirmed that the root authority was obtained.

3.1.2. Did the device have "adb" enabled?

According to the acquisition log, adb was not in the activated state at the point when the device was obtained. In order to obtain the data of the device, the forensic analyst executed the device set-up (settings -> Application Settings -> Development -> USB debugging) and activated the 'USB debugging.'

Meanwhile, whether adb was activated or not could be confirmed from the obtained images. The set-up information of Android is managed as the SQLite DB and XML files within the '/data' partition, so among the obtained images, the relevant items could be confirmed within the mtdblock6.img images, which are pertinent to the '/data' partition.

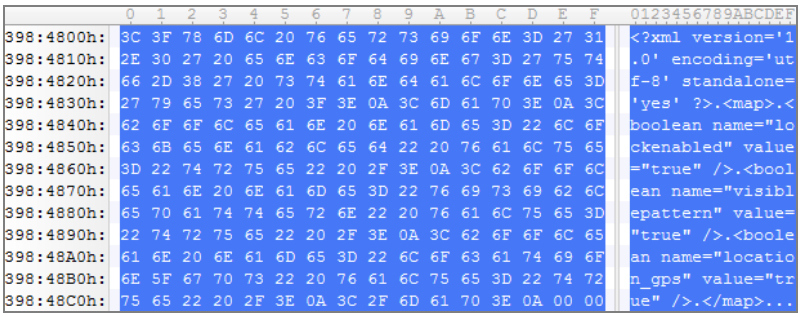
The picture below shows the confirmation of the page of the location of 0x16CF000 of mtdblock6.img, and it is the data in the XML format. This is the content of 'com.android.settings_preferences.xml,' and it can be confirmed that the value of the item, 'enable_adb,' is 'true' (full path:/ data/com.android.settings/shared_prefs/com.android.settings_preferences.xml).

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
16C:F000h: 3C 3F 78 6D 6C 20 76 65 72 73 69 6F 6E 3D 27 31  <?xml version='1
16C:F010h: 2E 30 27 20 65 6E 63 6F 64 69 6E 67 3D 27 75 74  .0' encoding='ut
16C:F020h: 66 2D 38 27 20 73 74 61 6E 64 61 6C 6F 6E 65 3D  f-8' standalone=
16C:F030h: 27 79 65 73 27 20 3F 3E 0A 3C 6D 61 70 3E 0A 3C  'yes' ?>.<map>.<
16C:F040h: 62 6F 6F 6C 65 61 6E 20 6E 61 6D 65 3D 22 6C 6F  boolean name="lo
16C:F050h: 63 6B 65 6E 61 62 6C 65 64 22 20 76 61 6C 75 65  ckenabled" value
16C:F060h: 3D 22 74 72 75 65 22 20 2F 3E 0A 3C 62 6F 6F 6C  ="true" />.<bool
16C:F070h: 65 61 6E 20 6E 61 6D 65 3D 22 76 69 73 69 62 6C  ean name="visibl
16C:F080h: 65 70 61 74 74 65 72 6E 22 20 76 61 6C 75 65 3D  epattern" value=
16C:F090h: 22 74 72 75 65 22 20 2F 3E 0A 3C 62 6F 6F 6C 65  "true" />.<boole
16C:F0A0h: 61 6E 20 6E 61 6D 65 3D 22 65 6E 61 62 6C 65 5F  an name="enable_
16C:F0B0h: 61 64 62 22 20 76 61 6C 75 65 3D 22 74 72 75 65  adb" value="true
16C:F0C0h: 22 20 2F 3E 0A 3C 62 6F 6F 6C 65 61 6E 20 6E 61  " />.<boolean na
16C:F0D0h: 6D 65 3D 22 6C 6F 63 61 74 69 6F 6E 5F 67 70 73  me="location_gps
16C:F0E0h: 22 20 76 61 6C 75 65 3D 22 74 72 75 65 22 20 2F  " value="true" /
16C:F0F0h: 3E 0A 3C 2F 6D 61 70 3E 0A 00 00 00 00 00 00 00  >.</map>........
```

Figure 10. com.android.settings_preferences.xml - 'enabled_adb = true'

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <boolean name="lockenabled" value="true" />
    <boolean name="visiblepattern" value="true" />
    <boolean name="enable_adb" value="true" />
    <boolean name="location_gps" value="true" />
</map>
```

Also, it can be found that the XML data in the similar form is saved in the page of the location of 0x3984800 of mtdblock6.img. This data, like the one above, is also the 'com.android.settings_preferences.xml' data, but it can be confirmed that the 'enable_adb' item does not exist.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
398:4800h:	3C	3F	78	6D	6C	20	76	65	72	73	69	6F	6E	3D	27	31	<?xml version='1
398:4810h:	2E	30	27	20	65	6E	63	6F	64	69	6E	67	3D	27	75	74	.0' encoding='ut
398:4820h:	66	2D	38	27	20	73	74	61	6E	64	61	6C	6F	6E	65	3D	f-8' standalone=
398:4830h:	27	79	65	73	27	20	3F	3E	0A	3C	6D	61	70	3E	0A	3C	'yes' ?>.<map>.<
398:4840h:	62	6F	6F	6C	65	61	6E	20	6E	61	6D	65	3D	22	6C	6F	boolean name="lo
398:4850h:	63	6B	65	6E	61	62	6C	65	64	22	20	76	61	6C	75	65	ckenabled" value
398:4860h:	3D	22	74	72	75	65	22	20	2F	3E	0A	3C	62	6F	6F	6C	="true" />.<bool
398:4870h:	65	61	6E	20	6E	61	6D	65	3D	22	76	69	73	69	62	6C	ean name="visibl
398:4880h:	65	70	61	74	74	65	72	6E	22	20	76	61	6C	75	65	3D	epattern" value=
398:4890h:	22	74	72	75	65	22	20	2F	3E	0A	3C	62	6F	6F	6C	65	"true" />.<boole
398:48A0h:	61	6E	20	6E	61	6D	65	3D	22	6C	6F	63	61	74	69	6F	an name="locatio
398:48B0h:	6E	5F	67	70	73	22	20	76	61	6C	75	65	3D	22	74	72	n_gps" value="tr
398:48C0h:	75	65	22	20	2F	3E	0A	3C	2F	6D	61	70	3E	0A	00	00	ue" />.</map>...

Figure 11. com.android.settings_preferences.xml - 'enabled_adb' does not exist

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <boolean name="lockenabled" value="true" />
    <boolean name="visiblepattern" value="true" />
    <boolean name="location_gps" value="true" />
</map>
```

It is related to the characteristic that the data in the flash memory, where the XML data without the enable_adb item from the mtdblock6.img is found, gets updated. First when USB Debugging was not activated, the 'com.android.settings_preferences.xml' file without the enable_adb item existed, and later, when USB Debugging was activated, the content of the relevant file was edited and a new page was allotted. Therefore, 'com.android.settings_preferences.xml' without the enable_adb item indicates the state of the previous set-up, and the current device is in the state of adb activated.

Also, whether adb was activated or not can be confirmed from the 'settings.db' file in the format of SQLite DB to which the set-up information of Android is saved. The settings.db file is saved in the '/data/com.android.providers.settings/databases' directory, and whether adb is activated or not is set up under the name of 'adb_enabled' in the 'secure' table. If the value of 'adb_enabled' is zero, then it is in the deactivated state; if it is one, then it is activated.

As a result of searching the value of the adb_enabled from the mtdblock6.img file, thirty SQLite table leaf pages, which included the value of adb_enabled, could be found. Among these, twenty four had the values of adb_enabled 'zero (deactivated),' and six had 'one (activated).' (Refer to the picture below.) However, among the thirty SQLite table leaf pages that are found, it cannot be confirmed which page is the currently valid page, so whether adb is activated or not cannot be clearly judged through this.

Classifying pages of the 'mtdblock6.img' file and analyzing SQLite table leaf pages, 30 records that contained 'adb_enabled' setting were found.

Among these, twenty four had the values of adb_enabled 'zero (deactivated),' and six had 'one (activated).' (Refer to the picture below.)

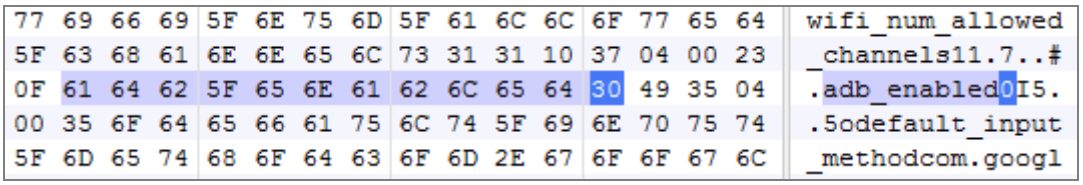


Figure 12. SQLite table leaf page - "adb_enable = 0'

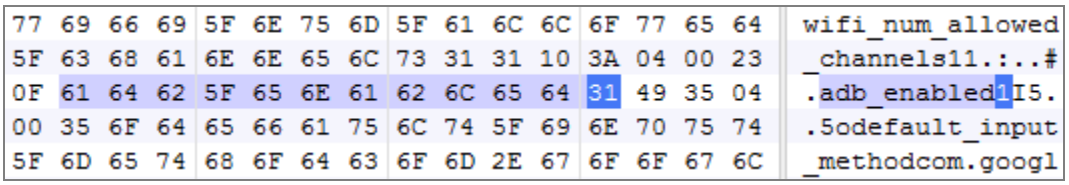


Figure 13. SQLite table leaf page - "adb_enable = 1'

Therefore it is necessary to check which records among the 30 found are currently valid. To this end RowID of B-tree leaf cells that include each record can be used. Removing duplicate cells in the SQLite table leaf cells that include the 'adb_enabled' setting, a total of 6 cells were found.

The usual algorithm is to give the newly created row a RowID that is one larger than the largest RowID in the table prior to the insert. Therefore the record with the largest RowID in the below table is the valid record, and 'adb' is enabled status.

Table 10. SQLite table leaf cells – 'adb_enabled'

RowID	Name	Value
34	adb_enabled	0
41	adb_enabled	0
46	adb_enabled	0
55	adb_enabled	0
58	adb_enabled	1
61	adb_enabled	1

3.1.3. Was the collection process sound? (and can you verify the recorded acquisition log)

During the process of collecting the images of proof in regard to each partition in the device, there is a possibility that some data might have disappeared or got overwritten. According to the acquisition log, it was set as the airplane mode when the device was turned on at first, but during that process, it received some text messages. Although the messages weren't read, there is a possibility that important data of proof got deleted, since the page in the flash memory got deleted or allotted as the relevant data was recorded.

Also, in order to obtain the images of proof of each partition in the device, the rooting for the relevant device was needed. For this, the process of activating USB Debugging was executed, and during the process of changing the set-up, the page in the flash memory was deleted and allotted as a result.

Meanwhile, the forensic analyst used SuperOneClick 1.7.0.0 and attempted the temporary rooting in order to obtain the administrator authority (root) as adb shell. In case of temporary rooting, data is not created in the user partition, so it is judged that there is no big problem in the perspective of collecting the data of proof.

After the temporary rooting, collecting data by using the nc command was attempted, but since the nc command did not exist, it was decided to use the collecting method by using SD card. For this, the imaging was executed in regard to the SD card that was connected previously after the device was turned off. After the data imaging on the SD card was completed, the SD card was inserted to the device in order to collect the images of memory's partition, and the device was booted. During this process, since the device was rebooted, there is a possibility that a part of the page of the flash memory could have been overwritten.

Since the temporary rooting was done, after the rebooting, the rooting is attempted once again. After that, using dd command, images of each partition were saved to the SD card. Here, since the '/data' and '/cache' partitions are in the mounted state by the rw authority, a possibility exists that data might have changed while the image was created.

3.1.4. List applications installed

In the obtained image from Scenario 1, the tag domain of yaffs does not exist, so image cannot be reconstructed. Therefore, the meta page, where the names of file/folder and time information were saved, was extracted in order to check the list of the installed application.

The application program installed in the general Android system can be confirmed in the 'ManageAppsInfo.txt' file within the '/data/com.android.settings/files' directory and the '/data/com.android.vending/databases' file within the '/data/com.android.vending/databases' directory. However, since the mtdblock6.img cannot be reconstructed, the relevant data was confirmed through close analysis on the categorized pages through the page analysis method of yaffs.

The table below shows the directory list that is relevant to the name of the application after extracting the meta page that exists in the mtdblock6.img. Through the relevant list, the installed application and the folder's time information (LastModifiedTime, LastAccessTime, and LastMetaModifiedTime) that exist in the meta page can be confirmed together. Additionally, through the time information on the meta page, whether the application was used or not can be learned. The highlighted items in the below table show that the relevant application was used could be known from the difference in LastModifiedTime from LastAccessTime and LastMetaModifiedTime.

Table 11. List applications installed in mtdblock6.img

Installed Applications	LastModifiedTime (UTC)	LastAccessTime (UTC)	LastMetaModifiedTime (UTC)
com.amazon.mp3	2011-05-04 18:17:38	2011-05-04 18:17:57	2011-05-04 18:17:57
com.android.alarmclock	2011-05-04 18:17:50	2011-05-04 18:18:10	2011-05-04 18:18:10
com.android.bluetooth	2011-05-04 18:17:44	2011-05-04 18:18:10	2011-05-04 18:18:10
com.android.browser	2011-05-04 18:17:41	2011-05-04 19:06:18	2011-05-04 19:06:18
com.android.bugreport	2011-05-04 18:17:41	2011-05-04 18:17:41	2011-05-04 18:17:41
com.android.calculator2	2011-05-04 18:17:39	2011-05-04 18:17:39	2011-05-04 18:17:39
com.android.calendar	2011-05-04 18:17:37	2011-05-04 18:18:00	2011-05-04 18:18:00
com.android.camera	2011-05-04 18:17:36	2011-05-06 13:43:19	2011-05-06 13:43:19
com.android.cardock	2011-05-04 18:17:33	2011-05-04 18:17:33	2011-05-04 18:17:33
com.android.certinstaller	2011-05-04 18:17:51	2011-05-04 18:17:51	2011-05-04 18:17:51

com.android.contacts	2011-05-04 18:17:49	2011-05-04 18:26:33	2011-05-04 18:26:33
com.android.email	2011-05-04 18:17:37	2011-05-04 18:18:05	2011-05-04 18:18:05
com.android.globalsearch	2011-05-04 18:17:33	2011-05-04 18:17:33	2011-05-04 18:17:33
com.android.htmlviewer	2011-05-04 18:17:33	2011-05-04 18:17:33	2011-05-04 18:17:33
com.android.internal.backup.LocalTransport	2011-05-04 18:17:52	2011-05-04 18:17:52	2011-05-04 18:17:52
com.android.launcher	2011-05-04 18:17:50	2011-05-04 18:19:14	2011-05-04 18:19:14
com.android.magicsmoke	2011-05-04 18:17:41	2011-05-04 18:17:41	2011-05-04 18:17:41
com.android.mms	2011-05-04 18:17:40	2011-05-04 18:18:07	2011-05-04 18:18:07
com.android.music	2011-05-04 18:17:38	2011-05-04 18:17:38	2011-05-04 18:17:38
com.android.musicvis	2011-05-04 18:17:39	2011-05-04 18:17:39	2011-05-04 18:17:39
com.android.packageinstaller	2011-05-04 18:17:36	2011-05-04 18:17:36	2011-05-04 18:17:36
com.android.phone	2011-05-04 18:17:34	2011-05-04 18:17:56	2011-05-04 18:17:56
com.android.providers.applications	2011-05-04 18:17:47	2011-05-04 18:17:47	2011-05-04 18:17:47
com.android.providers.calendar	2011-05-04 18:17:36	2011-05-04 19:37:35	2011-05-04 19:37:35
com.android.providers.contacts	2011-05-04 18:17:47	2011-05-04 18:18:02	2011-05-04 18:18:02
com.android.providers.downloads	2011-05-04 18:17:41	2011-05-04 18:18:04	2011-05-04 18:18:04
com.android.providers.drm	2011-05-04 18:17:39	2011-05-04 18:17:39	2011-05-04 18:17:39
com.android.providers.media	2011-05-04 18:17:42	2011-05-04 18:18:09	2011-05-04 18:18:09
com.android.providers.settings	2011-05-04 18:17:42	2011-05-04 18:17:51	2011-05-04 18:17:51
com.android.providers.subscribedfeeds	2011-05-04 18:17:51	2011-05-04 18:17:51	2011-05-04 18:17:51
com.android.providers.telephony	2011-05-04 18:17:33	2011-05-04 18:17:55	2011-05-04 18:17:55
com.android.providers.userdictionary	2011-05-04 18:17:49	2011-05-04 18:18:02	2011-05-04 18:18:02
com.android.server.vpn	2011-05-04 18:17:41	2011-05-04 18:17:41	2011-05-04 18:17:41
com.android.settings	2011-05-04 18:17:44	2011-05-05 10:21:03	2011-05-05 10:21:03
com.android.setupwizard	2011-05-04 18:17:41	2011-05-06 13:25:20	2011-05-06 13:25:20
com.android.soundrecorder	2011-05-04 18:17:39	2011-05-04 18:17:39	2011-05-04 18:17:39
com.android.vending	2011-05-04 18:17:45	2011-05-06 13:24:12	2011-05-06 13:24:12
com.android.vending	2011-05-04 18:17:45	2011-05-06 13:24:13	2011-05-06 13:24:13
com.android.vending	2011-05-04 18:17:45	2011-05-06 13:26:02	2011-05-06 13:26:02
com.android.vending	2011-05-04 18:17:45	2011-05-06 13:27:10	2011-05-06 13:27:10
com.android.vending.updater	2011-05-04 18:17:43	2011-05-04 18:17:43	2011-05-04 18:17:43
com.android.voicedialer	2011-05-04 18:17:43	2011-05-04 18:18:09	2011-05-04 18:18:09
com.android.wallpaper	2011-05-04 18:17:43	2011-05-04 18:17:43	2011-05-04 18:17:43
com.android.wallpaper.livepicker	2011-05-04 18:17:42	2011-05-04 18:17:42	2011-05-04 18:17:42
com.cooliris.media	2011-05-04 18:17:50	2011-05-04 18:18:11	2011-05-04 18:18:11
com.facebook.katana	2011-05-04 18:17:35	2011-05-04 18:18:35	2011-05-04 18:18:35

com.google.android.apps.genie.geniewidget	2011-05-04 18:17:47	2011-05-04 18:17:47	2011-05-04 18:17:47
com.google.android.apps.gtalkservice	2011-05-04 18:17:38	2011-05-04 19:37:38	2011-05-04 19:37:38
com.google.android.apps.maps	2011-05-04 18:17:47	2011-05-04 18:17:47	2011-05-04 18:17:47
com.google.android.apps.unveil	2011-05-04 18:17:44	2011-05-04 18:17:44	2011-05-04 18:17:44
com.google.android.apps.uploader	2011-05-04 18:17:40	2011-05-04 18:18:09	2011-05-04 18:18:09
com.google.android.backup	2011-05-04 18:17:43	2011-05-04 18:17:43	2011-05-04 18:17:43
com.google.android.backup.BackupTransportService	2011-05-04 18:17:54	2011-05-04 18:17:54	2011-05-04 18:17:54
com.google.android.feedback	2011-05-04 18:17:39	2011-05-04 18:17:39	2011-05-04 18:17:39
com.google.android.gm	2011-05-04 18:17:51	2011-05-08 13:34:24	2011-05-08 13:34:24
com.google.android.googleapps	2011-05-04 18:17:47	2011-05-06 13:25:57	2011-05-06 13:25:57
com.google.android.latinimetutorial	2011-05-04 18:17:50	2011-05-04 18:17:50	2011-05-04 18:17:50
com.google.android.location	2011-05-04 18:17:36	2011-05-04 18:18:03	2011-05-04 18:18:03
com.google.android.marvin.kickback	2011-05-04 18:17:33	2011-05-04 18:17:33	2011-05-04 18:17:33
com.google.android.marvin.soundback	2011-05-04 18:17:50	2011-05-04 18:17:50	2011-05-04 18:17:50
com.google.android.marvin.talkback	2011-05-04 18:17:36	2011-05-04 18:17:36	2011-05-04 18:17:36
com.google.android.partnersetup	2011-05-04 18:17:37	2011-05-04 18:17:37	2011-05-04 18:17:37
com.google.android.providers.enhancedgooglesearch	2011-05-04 18:17:36	2011-05-04 19:37:32	2011-05-04 19:37:32
com.google.android.providers.gmail	2011-05-04 18:17:49	2011-05-06 13:25:55	2011-05-06 13:25:55
com.google.android.providers.gmail	2011-05-04 18:17:49	2011-05-06 13:25:56	2011-05-06 13:25:56
com.google.android.providers.settings	2011-05-04 18:17:36	2011-05-04 18:17:55	2011-05-04 18:17:55
com.google.android.providers.subscribedfeeds	2011-05-04 18:17:34	2011-05-04 19:37:28	2011-05-04 19:37:28
com.google.android.providers.talk	2011-05-04 18:17:34	2011-05-04 18:18:07	2011-05-04 18:18:07
com.google.android.server.checkin	2011-05-04 18:17:42	2011-05-04 18:17:53	2011-05-04 18:17:53
com.google.android.street	2011-05-04 18:17:51	2011-05-04 18:17:51	2011-05-04 18:17:51
com.google.android.syncadapters.contacts	2011-05-04 18:17:41	2011-05-04 18:17:41	2011-05-04 18:17:41
com.google.android.systemupdater	2011-05-04 18:17:37	2011-05-04 18:18:04	2011-05-04 18:18:04
com.google.android.talk	2011-05-04 18:17:36	2011-05-04 18:17:36	2011-05-04 18:17:36
com.google.android.voicesearch	2011-05-04 18:17:38	2011-05-04 18:18:02	2011-05-04 18:18:02
com.google.android.youtube	2011-05-04 18:17:40	2011-05-04 18:17:40	2011-05-04 18:17:40
com.motorola.calendar	2011-05-04 18:17:44	2011-05-04 18:18:01	2011-05-04 18:18:01
com.motorola.dock	2011-05-04 18:17:42	2011-05-04 18:17:42	2011-05-04 18:17:42
com.motorola.hiddenmenu	2011-05-04 18:17:35	2011-05-04 18:17:35	2011-05-04 18:17:35
com.motorola.pgmsystem	2011-05-04 18:17:33	2011-05-04 18:17:33	2011-05-04 18:17:33
com.motorola.programmenu	2011-05-04 18:17:33	2011-05-04 18:17:33	2011-05-04 18:17:33
com.qo.android.gep	2011-05-04 18:17:50	2011-05-08 13:00:01	2011-05-08 13:00:01
com.svox.pico	2011-05-04 18:17:51	2011-05-04 18:17:51	2011-05-04 18:17:51

com.twitter.android	2011-05-06 13:27:34	2011-05-06 13:29:13	2011-05-06 13:29:13
com.twitter.android	2011-05-06 13:27:34	2011-05-06 13:29:17	2011-05-06 13:29:17
com.vzw.vvm.androidclient	2011-05-04 18:17:37	2011-05-04 18:17:37	2011-05-04 18:17:37

As the analysis result, it is judged that the applications such as browser, camera, calendar, setting, vending, Google talk, Google mail, and quick office were used. For reference, in case when several meta pages of the same name exist, it is because a new page is allotted when the content of the data is changed due to the characteristics of flash memory, not because the content of the relevant page is changed.

Meanwhile, the most of the currently installed applications in the device are the ones that exist in an Android smartphone as a basic, and the application that the user installed is Twitter. This can be confirmed through the 'assets.db' file, which is SQLite DB that manages the breakdown of the application installed from the Android market. As a result of searching the content the assets.db file from the SQLite table leaf pages, which were categorized from the mtdblock6.img, the installation record of Twitter application could be confirmed as the figure below.

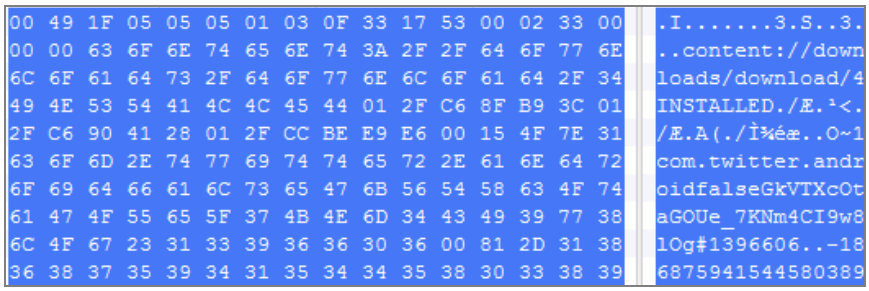


Figure 14. Content of 'assets.db' file

3.1.5. Indicate version information

The device information of Scenario 1 could be confirmed as the figure below. As you can see, the Android version is 2.1-update1.

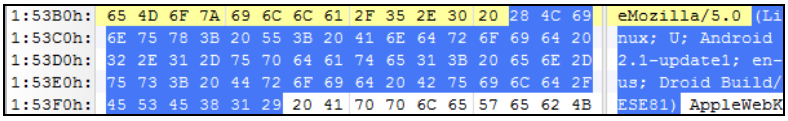


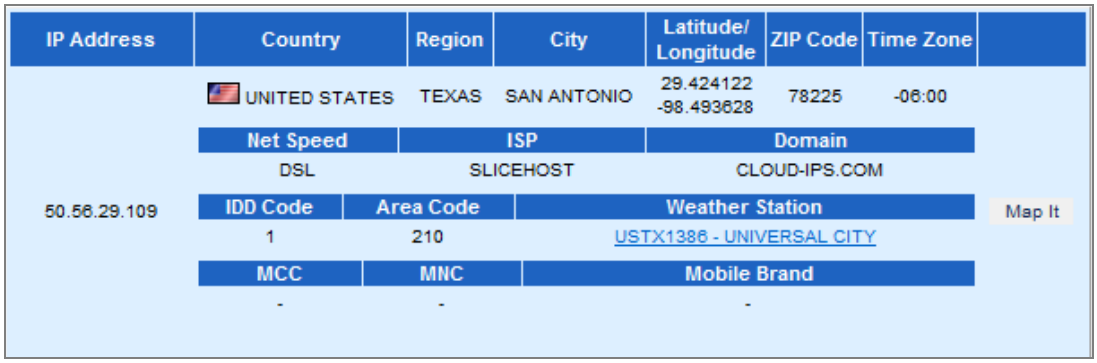
Figure 15. Device information of Scenario 1 (mtdblock6.img)

The version of installed applications could not be confirmed exatly.

3.1.6. Recover credentials, if possible

The login credential of 'http://50.56.29.109/ss/' was found from the SQLite table leaf page within the mtdblock6.img.

The IP allocation information of '50.56.29.109' is like the figure below.



IP Address	Country	Region	City	Latitude/ Longitude	ZIP Code	Time Zone	
	UNITED STATES	TEXAS	SAN ANTONIO	29.424122 -98.493628	78225	-06:00	
	Net Speed	ISP	Domain				
	DSL	SLICEHOST	CLOUD-IPS.COM				
50.56.29.109	IDD Code	Area Code	Weather Station				Map It
	1	210	USTX1386 - UNIVERSAL CITY				
	MCC	MNC	Mobile Brand				
	-	-	-				

Figure 16. Location of '50.56.29.109'

For the ‘http://50.56.29.109/ss/, the web server was at work, and it asked for the login credential at the point of access. The figure below shows the generated message when wrong authentication information is entered.

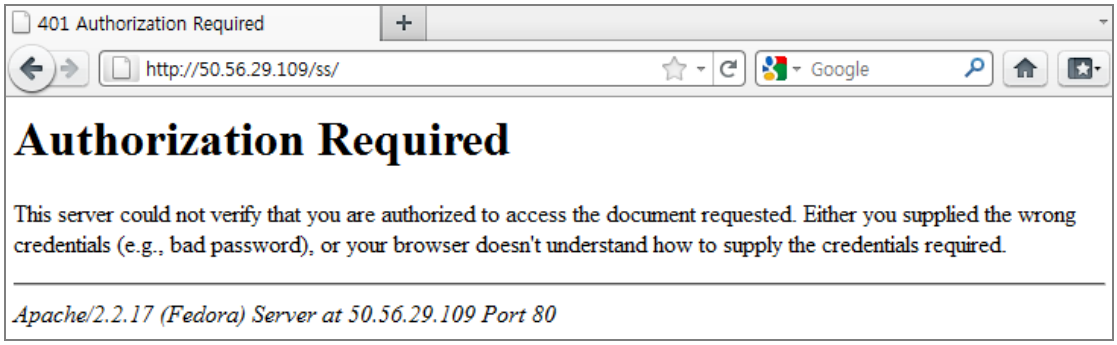


Figure 17. Login failure message : http://50.56.29.109/ss/

The figure below is the login credential of the ‘http://50.56.29.109/ss/ that was found from the SQLite table leaf page within the mtdblock6.img. The ID is Norby, and the password is ‘aaassspp’.

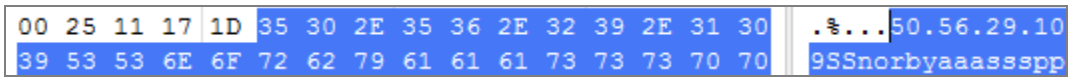


Figure 18. Login credential : http://50.56.29.109/ss/

As a result of attempting logging in, the access using the found login credential was successful like the following figure.

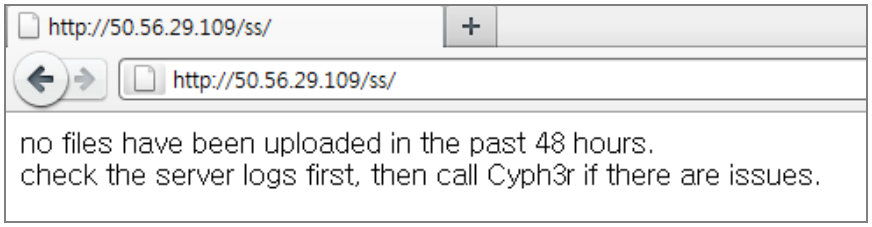


Figure 19. Login success : http://50.56.29.109/ss/

Meanwhile, as a result of checking the mtdblock6.img, there were traces of downloading many PDF files from the web site like the figure below, but the relevant files did not exist currently on the web site.

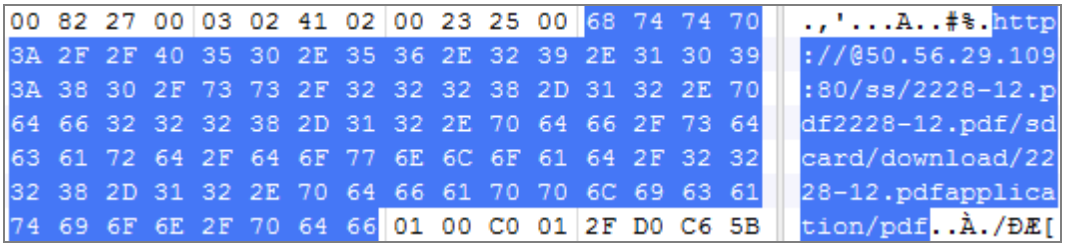


Figure 20. Web browser history : http://50.56.29.109/ss/

And the login credential of google mail (norby441@gmail.com) was also found. The account (norby441@gmail.com) uses the same password (‘aaassspp’) as the server: ‘http://50.56.29.109/ss/’.

3.2. Scenario 2: Intellectual Property Theft

A serious breach of security occurred within an organization named SwiftLogic Inc.; valuable documents containing designs of a new product named Palomino were confirmed to have been leaked to a competitor. Based on an internal investigation, Yob Taog is suspected of the leak and was suspended pending investigation. Taog's Android smartphone was - surprisingly - voluntarily submitted by Taog for further investigation. Your goal in this investigation is to document any evidence that intellectual property was stolen, to support termination of Yob Toag and potential criminal charges. You are asked to perform a forensic analysis of his device for evidence of the breach.

State an opinion or your findings on the following evidentiary issues:

3.2.1. Was the device "rooted"?

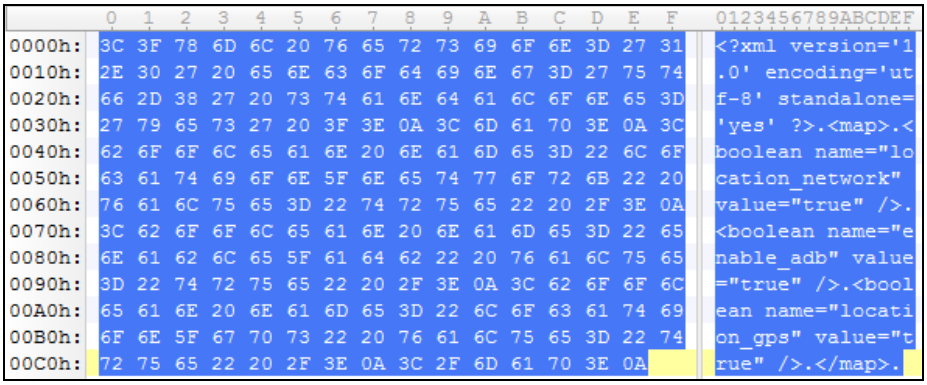
Taking a look at 'Windows 3' content in line 50, file "Collection.lo", it is connected to the device's shell through './adb shell' instruction. Upon connection, the prompt is indicated as '#', meaning root permission. If the status is not rooted, the prompt will be indicated as '$'. Also, immediately after connection, 'su' instruction was executed to grant Administrator rights, and 'nanddump' was run. As a result, the device was 'rooted.'

```
...
Window 2
[user1@exam3 platform-tools]$ ./adb shell
# su
# nanddump /dev/mtd/mtd0 | transfer 9000
675840 bytes transferred
Sha1:    160433772347c94bd3abc89952677942d423515b
# nanddump /dev/mtd/mtd1 | transfer 9001
405504 bytes transferred
Sha1:    81d32137cc3a35e535dfa8a706981d4494267e7a
...
```

3.2.2. Did the device have "adb" enabled?

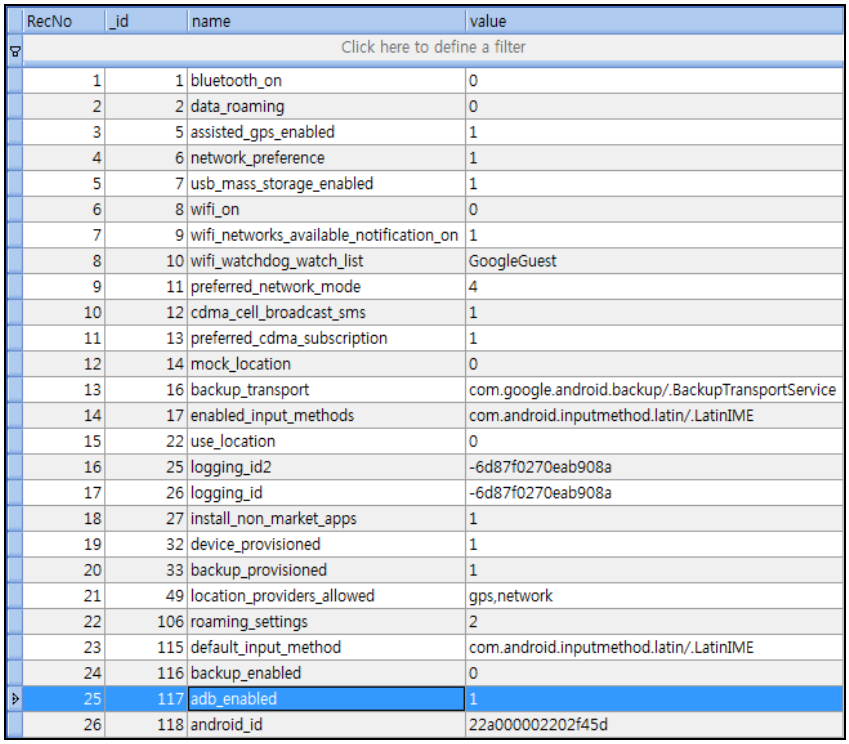
In order to figure out whether or not the 'adb' of a device is enabled, file 'com.android.settings_preferences.xml' located in the directory, '/data/data/com.android.providers.settings/shared_prefs' and the 'secure' table of file 'setteings.db' located in the directory are reviewed for a confirmation.

The concerning table's enabledness for 'adb' is set in the name of 'adb_enabled.' If the value is 0, the status is considered deactivated; if the value is 1, the status is considered activated. As seen in the below figure, the device's 'adb' is enabled.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	3C	3F	78	6D	6C	20	76	65	72	73	69	6F	6E	3D	27	31	<?xml version='1
0010h:	2E	30	27	20	65	6E	63	6F	64	69	6E	67	3D	27	75	74	.0' encoding='ut
0020h:	66	2D	38	27	20	73	74	61	6E	64	61	6C	6F	6E	65	3D	f-8' standalone=
0030h:	27	79	65	73	27	20	3F	3E	0A	3C	6D	61	70	3E	0A	3C	'yes' ?>.<map>.<
0040h:	62	6F	6F	6C	65	61	6E	20	6E	61	6D	65	3D	22	6C	6F	boolean name="lo
0050h:	63	61	74	69	6F	6E	5F	6E	65	74	77	6F	72	6B	22	20	cation_network"
0060h:	76	61	6C	75	65	3D	22	74	72	75	65	22	20	2F	3E	0A	value="true" />.
0070h:	3C	62	6F	6F	6C	65	61	6E	20	6E	61	6D	65	3D	22	65	<boolean name="e
0080h:	6E	61	62	6C	65	5F	61	64	62	22	20	76	61	6C	75	65	nable_adb" value
0090h:	3D	22	74	72	75	65	22	20	2F	3E	0A	3C	62	6F	6F	6C	="true" />.<bool
00A0h:	65	61	6E	20	6E	61	6D	65	3D	22	6C	6F	63	61	74	69	ean name="locati
00B0h:	6F	6E	5F	67	70	73	22	20	76	61	6C	75	65	3D	22	74	on_gps" value="t
00C0h:	72	75	65	22	20	2F	3E	0A	3C	2F	6D	61	70	3E	0A		rue" />.</map>.

Figure 21. com.android.settings_preferences.xml - 'enabled_adb = true'



RecNo	_id	name	value
Click here to define a filter			
1	1	bluetooth_on	0
2	2	data_roaming	0
3	5	assisted_gps_enabled	1
4	6	network_preference	1
5	7	usb_mass_storage_enabled	1
6	8	wifi_on	0
7	9	wifi_networks_available_notification_on	1
8	10	wifi_watchdog_watch_list	GoogleGuest
9	11	preferred_network_mode	4
10	12	cdma_cell_broadcast_sms	1
11	13	preferred_cdma_subscription	1
12	14	mock_location	0
13	16	backup_transport	com.google.android.backup/.BackupTransportService
14	17	enabled_input_methods	com.android.inputmethod.latin/.LatinIME
15	22	use_location	0
16	25	logging_id2	-6d87f0270eab908a
17	26	logging_id	-6d87f0270eab908a
18	27	install_non_market_apps	1
19	32	device_provisioned	1
20	33	backup_provisioned	1
21	49	location_providers_allowed	gps,network
22	106	roaming_settings	2
23	115	default_input_method	com.android.inputmethod.latin/.LatinIME
24	116	backup_enabled	0
25	117	adb_enabled	1
26	118	android_id	22a000002202f45d

Figure 22. /com.android.settings/databases/settings.db – 'secure' table : 'adb_enabled = 1'

3.2.3. Was the collection process sound? (and can you verify the recorded acquisition log)

Taking a look at the acquisition procedure recorded in the log, the device was already rooted, while 'nanddump' for the purpose of dumping su and nand flash was already installed. In the course of dumping, each mtd file was directly transmitted to the host pc through tcp.

Because there was no rooting or an additional software was installed to image acquisition, it cannot be understood that data were collected in an appropriate procedure, while maintaining integrity.

3.2.4. List applications installed

All application programs installed in the Android system may be found in file 'ManageAppsInfo.txt' located in directory, '/data/data/com.android.settings/files.'

Table 12. contents of 'ManageAppsInfo.txt'

Installed Application's Pakagename	Application Name
android	Android System
android.tts	TTS Service
au.com.phil	Abduction!
com.amazon.mp3	Amazon MP3
com.andriod.mm	Media Mounter
com.android.alarmclock	Alarm Clock
com.android.bluetooth	Bluetooth Share
com.android.browser	Browser
com.android.bugreport	com.android.bugreport
com.android.calculator2	Calculator
com.android.calendar	Calendar
com.android.camera	Camera
com.android.cardock	Car Home
com.android.certinstaller	Certificate Installer
com.android.contacts	Contacts
com.android.email	Email
com.android.gallery	Camera >com.google.zxing.client.android
com.android.globalsearch	Quick Search Box
com.android.htmlviewer	HTML Viewer
com.android.inputmethod.latin	Android keyboard
com.android.launcher	Home
com.android.mms	Messaging
com.android.music	Music
com.android.packageinstaller	Package Installer
com.android.phone	Dialer
com.android.providers.applications	com.android.providers.applications
com.android.providers.calendar	Calendar Storage
com.android.providers.contacts	Contacts Storage
com.android.providers.downloads	Download Manager
com.android.providers.drm	DRM Protected Content Storage
com.android.providers.media	Media Storage
com.android.providers.settings	Settings Storage
com.android.providers.subscribedfeeds	Account and Sync Settings
com.android.providers.telephony	Dialer Storage
com.android.providers.userdictionary	com.android.providers.userdictionary
com.android.server.vpn	VPN Services
com.android.settings	Settings
com.android.setupwizard	Setup Wizard
com.android.soundrecorder	Sound Recorder
com.android.vending	Market
com.android.vending.updater	Market Updater
com.android.voicedialer	Voice Dialer
com.bayview.tapfish	TapFish

com.bfs.papertoss	Paper Toss
com.creativemobile.DragRacing	Drag Racing
com.dragonplay.liveholdempro	Live Holdem Pro
com.droidhen.fruit	Fruit Slice
com.droidhen.game.donkeyjump	Donkey Jump
com.droidhen.irunner	iRunner
com.estrongs.android.pop	ES File Explorer
com.facebook.katana	Facebook
com.google.android.apps.gtalkservice	Google Talk Service
com.google.android.apps.maps	Maps
com.google.android.apps.translate	Translate
com.google.android.apps.uploader	My Uploads
com.google.android.backup	Google Backup Transport
com.google.android.feedback	com.google.android.feedback
com.google.android.gm	Gmail
com.google.android.googleapps	Google Apps
com.google.android.latinimetutorial	Latin Input Method Tutorial
com.google.android.location	Network Location
com.google.android.marvin.kickback	KickBack
com.google.android.marvin.soundback	SoundBack
com.google.android.marvin.talkback	TalkBack
com.google.android.partnersetup	Google Partner Setup
com.google.android.providers.enhancedgooglesearch	Google Search (Enhanced)
com.google.android.providers.gmail	Gmail Storage
com.google.android.providers.settings	Google Settings Provider
com.google.android.providers.subscribedfeeds	Sync Feeds
com.google.android.providers.talk	Google Talk Storage
com.google.android.server.checkin	Checkin Service
com.google.android.stardroid	Google Sky Map
com.google.android.street	Street View
com.google.android.syncadapters.contacts	com.google.android.syncadapters.contacts
com.google.android.systemupdater	System Updater
com.google.android.talk	Talk
com.google.android.voicesearch	Voice Search
com.google.android.youtube	YouTube
com.handmark.tweetcaster	TweetCaster
com.icenta.sudoku.ui	Sudoku Free
com.imdb.mobile	IMDb
com.infonow.bofa	Mobile Banking
com.kakao.talk	KakaoTalk
com.kiragames.unblockmefree	Unblock Me Free
com.kmagic.solitaire	Solitaire
com.lookout	Lookout
com.magicwach.rdefense_free	Robo Defense FREE
com.magmamobile.game.BubbleBlast	Bubble Blast
com.magmamobile.game.BubbleBlast2	Bubble Blast 2
com.magmamobile.game.mousetrap	Mouse Trap
com.metago.astro	ASTRO
com.motorola.calendar	Corporate Calendar
com.motorola.dock	Multimedia station

com.motorola.hiddenmenu	com.motorola.hiddenmenu
com.motorola.pgmsystem	PGM System
com.motorola.programmenu	Programming Menu
com.pandora.android	Pandora
com.qo.android.gep	Quickoffice
com.rovio.angrybirdsrio	Angry Birds Rio
com.scoreninja	ScoreNinja
com.seesmic	Seesmic Q
com.shazam.android	Shazam
com.svox.pico	Pico TTS
com.theronrogers.vaultyfree	Vaulty Free
com.vzw.smsProvider	smsServiceProvider
com.vzw.vvm.androidclient	Visual VM
com.weather.Weather	The Weather Channel
com.woodenbadger	tProcessKiller
com.world.newspapers	World Newspapers
com.wuzla.game.ScooterHero_Lite	Scooter Hero AD
fr.telemaque.horoscope	Horoscope
mobi.androidcloud.app.ptt.client	TiKL
net.flixster.android	Movies
net.sf.andpdf.pdfviewer	Android PDF Viewer
net.sunflat.android.actionpotato	ActionPotato
org.mhgames.jewels	Jewels
thecouponsapp.coupon	Coupons

Among the programs, the very application programs installed by the user himself may be checked through file 'assets.db's 'assets10' table data located in director'/data/data/com.android.vending/databases'. 'assets10' table contains the status of the application program installed by the user (installed / uninstalled / download_failed), elapsed time for download, installation time, time for deletion, package name, size, and so on.

Table 13. contents of /com.android.vending/databases/assets.db – table 'assets10'
(The device's time zone is New York, USA : UTC-4 with daylight saving)

State	Application's Pakagename	DownloadStartTime (UTC-4)	InstallTime (UTC-4)	UninstallTime (UTC-4)
UNINSTALLED	com.worldmate	2011-05-04 21:15:41	2011-05-04 21:17:53	2011-05-07 14:16:47
INSTALLED	com.imdb.mobile	2011-05-04 21:15:47	2011-05-04 21:17:32	
INSTALLED	com.shazam.android	2011-05-04 21:15:53	2011-05-04 21:17:06	
INSTALLED	com.kakao.talk	2011-05-04 21:16:17	2011-05-04 21:18:08	
INSTALLED	com.google.android.apps.maps	2011-05-04 21:16:31	2011-05-04 21:19:24	
INSTALLED	com.facebook.katana	2011-05-04 21:16:34	2011-05-04 21:18:34	
INSTALLED	com.pandora.android	2011-05-04 21:16:39	2011-05-04 21:18:16	
INSTALLED	com.google.android.street	2011-05-04 21:16:45	2011-05-04 21:17:40	
INSTALLED	fr.telemaque.horoscope	2011-05-04 21:18:48	2011-05-04 21:19:45	
INSTALLED	com.theronrogers.vaultyfree	2011-05-04 21:18:54	2011-05-04 21:19:28	
INSTALLED	com.world.newspapers	2011-05-04 21:19:34	2011-05-04 21:19:54	
INSTALLED	com.google.android.stardroid	2011-05-04 21:20:10	2011-05-04 21:20:39	

INSTALLED	com.google.android.apps.translate	2011-05-04 21:20:47	2011-05-04 21:22:07	
INSTALLED	com.google.zxing.client.android	2011-05-04 21:21:08	2011-05-04 21:21:41	
INSTALLED	com.weather.Weather	2011-05-04 21:22:13	2011-05-04 21:23:28	
INSTALLED	net.flixster.android	2011-05-04 21:22:24	2011-05-04 21:24:08	
INSTALLED	com.lookout	2011-05-04 21:22:33	2011-05-04 21:23:57	
INSTALLED	thecouponsapp.coupon	2011-05-04 21:22:45	2011-05-04 21:23:13	
INSTALLED	com.infonow.bofa	2011-05-04 21:23:06	2011-05-04 21:23:32	
INSTALLED	mobi.androidcloud.app.ptt.client	2011-05-04 21:23:20	2011-05-04 21:24:31	
INSTALLED	com.handmark.tweetcaster	2011-05-04 21:23:48	2011-05-04 21:25:05	
INSTALLED	com.dragonplay.liveholdempro	2011-05-04 21:24:38	2011-05-04 21:28:33	
INSTALLED	com.magmamobile.game.BubbleBlast2	2011-05-04 21:24:44	2011-05-04 21:29:14	
DOWNLOAD_FAILED	com.rovio.angrybirds	2011-05-04 21:24:57		
INSTALLED	com.bayview.tapfish	2011-05-04 21:25:12	2011-05-04 21:37:31	
INSTALLED	com.rovio.angrybirdsrio	2011-05-04 21:25:23	2011-05-04 22:06:03	
INSTALLED	com.magmamobile.game.BubbleBlast	2011-05-04 21:25:38	2011-05-04 21:27:29	
INSTALLED	com.magmamobile.game.mousetrap	2011-05-04 21:26:00	2011-05-04 21:29:36	
INSTALLED	org.mhgames.jewels	2011-05-04 21:26:20	2011-05-04 21:28:01	
DOWNLOAD_FAILED	com.rovio.angrybirdsseasons	2011-05-04 21:26:58		
INSTALLED	com.kmagic.solitaire	2011-05-04 21:27:01	2011-05-04 21:27:16	
INSTALLED	com.creativemobile.DragRacing	2011-05-04 21:27:10	2011-05-04 21:33:25	
INSTALLED	com.kiragames.unblockmefree	2011-05-04 21:27:20	2011-05-04 21:29:47	
INSTALLED	com.bfs.papertoss	2011-05-04 21:27:35	2011-05-04 21:41:09	
INSTALLED	com.droidhen.fruit	2011-05-04 21:28:08	2011-05-04 21:32:24	
INSTALLED	com.icenta.sudoku.ui	2011-05-04 21:28:44	2011-05-04 21:29:52	
INSTALLED	com.droidhen.irunner	2011-05-04 21:29:37	2011-05-04 22:07:36	
INSTALL_FAILED	com.boolbalabs.tossit.preview	2011-05-04 21:30:03		
INSTALL_FAILED	com.dragonplay.blackjack	2011-05-04 21:30:34		
INSTALLED	au.com.phil	2011-05-04 21:30:51	2011-05-04 21:37:54	
INSTALLED	com.magicwach.rdefense_free	2011-05-04 21:31:59	2011-05-04 22:06:59	
INSTALL_FAILED	dk.logisoft.aircontrol	2011-05-04 21:32:32		
INSTALL_FAILED	com.forthblue.pool	2011-05-04 21:33:33		
UNINSTALLED	com.twidroid	2011-05-05 12:14:41	2011-05-05 12:15:19	2011-05-07 23:10:01
INSTALLED	com.seesmic	2011-05-05 12:16:20	2011-05-05 12:16:41	
INSTALLED	com.scoreninja	2011-05-05 14:18:07	2011-05-05 14:18:13	
UNINSTALLED	cx.hell.android.pdfview	2011-05-07 12:58:37	2011-05-07 12:59:20	2011-05-07 14:16:24
INSTALLED	net.sf.andpdf.pdfviewer	2011-05-07 12:59:51	2011-05-07 13:00:32	

INSTALLED	com.metago.astro	2011-05-07 13:05:08	2011-05-07 13:05:43	
INSTALLED	com.estrongs.android.pop	2011-05-07 13:05:50	2011-05-07 13:06:20	
INSTALLED	com.woodenbadger	2011-05-07 14:14:45	2011-05-07 14:14:57	
INSTALLED	net.sunflat.android.actionpotato	2011-05-07 20:23:23	2011-05-07 20:23:34	
INSTALLED	com.droidhen.game.donkeyjump	2011-05-07 20:23:34	2011-05-07 20:26:02	
INSTALLED	com.wuzla.game.ScooterHero_Lite	2011-05-07 20:23:55	2011-05-07 20:24:57	

3.2.5. Indicate version information

Table 14. Contents of '/data/system/packages.xml'

package name	version	updated version
android	6	-
android.tts	6	-
au.com.phil	40	-
com.amazon.mp3	400003	-
com.andriod.mm	1	-
com.android.alarmclock	6	-
com.android.bluetooth	6	-
com.android.browser	6	-
com.android.bugreport	130	-
com.android.calculator2	6	-
com.android.calendar	6	-
com.android.camera	6	-
com.android.cardock	6	-
com.android.certinstaller	6	-
com.android.contacts	6	-
com.android.email	6	-
com.android.gallery	6	-
com.android.globalsearch	6	-
com.android.htmlviewer	6	-
com.android.inputmethod.latin	6	-
com.android.launcher	6	-
com.android.mms	6	-
com.android.music	6	-
com.android.packageinstaller	6	-
com.android.phone	6	-
com.android.providers.applications	6	-
com.android.providers.calendar	6	-
com.android.providers.contacts	6	-
com.android.providers.downloads	6	-
com.android.providers.drm	6	-
com.android.providers.media	6	-
com.android.providers.settings	6	-
com.android.providers.subscribedfeeds	6	-
com.android.providers.telephony	6	-
com.android.providers.userdictionary	6	-
com.android.server.vpn	6	-
com.android.settings	6	-
com.android.setupwizard	130	-

com.android.soundrecorder	-	-
com.android.vending	1710	-
com.android.vending.updater	1000	-
com.android.voicedialer	6	-
com.bayview.tapfish	3	-
com.bfs.papertoss	10	-
com.creativemobile.DragRacing	8	-
com.dragonplay.liveholdempro	15	-
com.droidhen.fruit	22	-
com.droidhen.game.donkeyjump	4	-
com.droidhen.irunner	2	-
com.estrongs.android.pop	72	-
com.facebook.katana	1811	111
com.google.android.apps.gtalkservice	130	-
com.google.android.apps.maps	5411	3235
com.google.android.apps.translate	46	-
com.google.android.apps.uploader	1413	-
com.google.android.backup	6	-
com.google.android.feedback	6	-
com.google.android.gm	130	-
com.google.android.googleapps	130	-
com.google.android.latinimetutorial	6	-
com.google.android.location	6	-
com.google.android.marvin.kickback	1	-
com.google.android.marvin.soundback	1	-
com.google.android.marvin.talkback	4	-
com.google.android.partnersetup	6	-
com.google.android.providers.enhancedgooglesearch	6	-
com.google.android.providers.gmail	6	-
com.google.android.providers.settings	6	-
com.google.android.providers.subscribedfeeds	6	-
com.google.android.providers.talk	6	-
com.google.android.server.checkin	6	-
com.google.android.stardroid	1108	-
com.google.android.street	16006	140
com.google.android.syncadapters.contacts	6	-
com.google.android.systemupdater	6	-
com.google.android.talk	130	-
com.google.android.voicesearch	140	-
com.google.android.youtube	1519	-
com.handmark.tweetcaster	24	-
com.icenta.sudoku.ui	36	-
com.imdb.mobile	2	-
com.infonow.bofa	5	-
com.kakao.talk	28	-
com.kiragames.unblockmefree	4	-
com.kmagic.solitaire	450	-
com.lookout	7629	-
com.magicwach.rdefense_free	2446	-
com.magmamobile.game.BubbleBlast	18	-
com.magmamobile.game.BubbleBlast2	6	-
com.magmamobile.game.mousetrap	14	-
com.metago.astro	56	-

com.motorola.calendar	5	-
com.motorola.dock	1	-
com.motorola.hiddenmenu	1	-
com.motorola.pgmsystem	1	-
com.motorola.programmenu	1	-
com.pandora.android	22	-
com.qo.android.gep	236	-
com.rovio.angrybirdsrio	100	-
com.scoreninja	2	-
com.seesmic	17	-
com.shazam.android	70593	-
com.svox.pico	1	
com.theronrogers.vaultyfree	26	
com.vzw.smsProvider	1	
com.vzw.vvm.androidclient	1	
com.weather.Weather	30100	
com.woodenbadger	1	
com.world.newspapers	131	
com.wuzla.game.ScooterHero_Lite	25	
fr.telemaque.horoscope	19	
mobi.androidcloud.app.ptt.client	29	
net.flixster.android	43	
net.sf.andpdf.pdfviewer	102	
net.sunflat.android.actionpotato	6	
org.mhgames.jewels	42	
thecouponsapp.coupon	202	
com.google.zxing.client.android	67	

3.2.6. Recover credentials, if possible

Table 15. Credentials from Scenario 2

Path(/data/data)	FileName(table)	ApplicationName	Account Information (password)
com.android.browser/databases	webview.db(password)	Browser	yobtaog@gmail.com (aaassspp)
com.android.email/databases	EmailProvider.db(Account)	Email	yobtaog@gmail.com
com.android.email/databases	EmailProvider.db(HostAuth)	Email	yobtaog@gmail.com (aaassspp)
com.android.providers.calender/databases	calendar.db(_sync_state)	Calendar	yobtaog@gmail.com
com.android.providers.telephony/databases	mmssms.db(canonical_address)	Dialer Storage	shandra@cherrful.com, sms.dynadel@gmail.com,
com.facebook.katana/databases	fb.db(info_contacts)	Facebook	regwetham@yahoo.com
com.google.android.gm/databases	gmail.db(accounts)	Gmail	yobtaog@gmail.com
com.google.android.providers.talk/databases	talk.db(accounts)	Google Talk Storage	yobtaog@gmail.com
com.handmark.tweetcaster/databases	webviewCache.db(cache)	TweetCaster	yobtaog@gmail.com
com.android.providers.contacts/databases	contacts2.db(_sync_state)	Contacts	yobtaog@gmail.com

3.3. Specification

In scenario 1 and 2, the device's time zone is New York, USA. Therefor the time information is applied in UTC-4 with daylight saving.

3.3.1. Scenario 1 – SMS/MMS

There are three types of SMS/MMS in Scenario 1: messages exchanged using texting feature of a cell phone; messages received from the malicious application installed in Scenario 2; and messages using 6245 service. For the application that was installed in order for Donald Norby to get the file of Yob Taog, there are messages using texting feature and another type. The pertinent application is explained in detail in a later section.

Table 16. Received SMS messages from Yob Taog's smartphone application ('ksmsvzwsms' signature)
('4124393388' is the phone number of Yob Taog)

Sender Number	Date (UTC-4)	Message	Read(1) or not(0)
4124393388	2011-05-04 20:50:22 Wed	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-04 20:50:32 Wed	ksmsvzwsms://message/May 4, 2011 8:50:12 PM EDT	1
4124393388	2011-05-04 20:50:36 Wed	ksmsvzwsms://message/May 4, 2011 8:50:12 PM EDT	1
4124393388	2011-05-04 20:53:21 Wed	ksmsvzwsms://message/May 4, 2011 8:53:12 PM EDT	1
4124393388	2011-05-04 20:53:31 Wed	ksmsvzwsms://message/pkg uploaded!	1
4124393388	2011-05-04 21:41:19 Wed	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-04 21:41:29 Wed	ksmsvzwsms://message/May 4, 2011 9:40:56 PM EDT	1
4124393388	2011-05-04 21:41:33 Wed	ksmsvzwsms://message/May 4, 2011 9:40:56 PM EDT	1
4124393388	2011-05-04 21:44:08 Wed	ksmsvzwsms://message/May 4, 2011 9:43:56 PM EDT	1
4124393388	2011-05-04 21:45:04 Wed	ksmsvzwsms://message/pkg uploaded!	1
4124393388	2011-05-04 22:17:35 Wed	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-04 22:17:45 Wed	ksmsvzwsms://message/May 4, 2011 10:17:25 PM EDT	1
4124393388	2011-05-04 22:18:16 Wed	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-04 22:18:26 Wed	ksmsvzwsms://message/May 4, 2011 10:18:04 PM EDT	1
4124393388	2011-05-04 22:21:15 Wed	ksmsvzwsms://message/May 4, 2011 10:21:04 PM EDT	1
4124393388	2011-05-04 22:22:22 Wed	ksmsvzwsms://message/pkg uploaded!	1
4124393388	2011-05-04 22:25:52 Wed	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-04 22:26:02 Wed	ksmsvzwsms://message/May 4, 2011 10:25:26 PM EDT	1
4124393388	2011-05-04 22:27:19 Wed	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-04 22:27:29 Wed	ksmsvzwsms://message/May 4, 2011 10:27:06 PM EDT	1
4124393388	2011-05-05 11:41:39 Thu	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-05 11:41:50 Thu	ksmsvzwsms://message/May 5, 2011 11:41:20 AM EDT	1
4124393388	2011-05-05 11:41:54 Thu	ksmsvzwsms://message/May 5, 2011 11:41:20 AM EDT	1
4124393388	2011-05-05 11:56:56 Thu	ksmsvzwsms://message/May 5, 2011 11:56:43 AM EDT	1
4124393388	2011-05-05 11:57:57 Thu	ksmsvzwsms://message/pkg uploaded!	1
4124393388	2011-05-05 18:07:43 Thu	ksmsvzwsms://message/May 5, 2011 6:07:35 PM EDT	1
4124393388	2011-05-05 18:13:47 Thu	ksmsvzwsms://message/pkg uploaded!	1
4124393388	2011-05-05 19:05:55 Thu	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-05 19:06:11 Thu	ksmsvzwsms://message/May 5, 2011 7:05:43 PM EDT	1
4124393388	2011-05-05 19:13:36 Thu	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-05 19:13:46 Thu	ksmsvzwsms://message/May 5, 2011 7:13:26 PM EDT	1
4124393388	2011-05-05 19:15:13 Thu	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-05 19:15:24 Thu	ksmsvzwsms://message/May 5, 2011 7:15:06 PM EDT	1
4124393388	2011-05-05 19:21:22 Thu	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-05 19:21:32 Thu	ksmsvzwsms://message/May 5, 2011 7:21:13 PM EDT	1
4124393388	2011-05-05 23:41:34 Thu	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-05 23:41:44 Thu	ksmsvzwsms://message/May 5, 2011 11:41:22 PM EDT	1
4124393388	2011-05-06 12:14:19 Fri	ksmsvzwsms://message/Service Started	1

4124393388	2011-05-06	12:14:29	Fri	ksmsvzwsms://message/May 6, 2011 12:13:57 PM EDT	1
4124393388	2011-05-06	12:14:33	Fri	ksmsvzwsms://message/May 6, 2011 12:13:57 PM EDT	1
4124393388	2011-05-06	12:17:08	Fri	ksmsvzwsms://message/May 6, 2011 12:16:57 PM EDT	1
4124393388	2011-05-06	12:19:36	Fri	ksmsvzwsms://message/pkg uploaded!	1
4124393388	2011-05-06	12:52:12	Fri	ksmsvzwsms://message/CallIn: 5854561283 May 6, 2011 12:51:31 PM EDT	1
4124393388	2011-05-06	13:19:37	Fri	ksmsvzwsms://message/May 6, 2011 1:19:25 PM EDT	1
4124393388	2011-05-06	13:20:32	Fri	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-06	13:20:42	Fri	ksmsvzwsms://message/May 6, 2011 1:20:22 PM EDT	1
4124393388	2011-05-06	13:21:13	Fri	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-06	13:21:23	Fri	ksmsvzwsms://message/May 6, 2011 1:21:02 PM EDT	1
4124393388	2011-05-06	13:22:56	Fri	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-06	13:23:06	Fri	ksmsvzwsms://message/May 6, 2011 1:22:42 PM EDT	1
4124393388	2011-05-06	13:28:33	Fri	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-06	13:50:14	Fri	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-06	13:50:24	Fri	ksmsvzwsms://message/May 6, 2011 1:50:02 PM EDT	1
4124393388	2011-05-06	15:15:57	Fri	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-06	15:16:07	Fri	ksmsvzwsms://message/May 6, 2011 3:15:42 PM EDT	1
4124393388	2011-05-06	15:18:20	Fri	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-06	15:18:30	Fri	ksmsvzwsms://message/May 6, 2011 3:18:07 PM EDT	1
4124393388	2011-05-06	15:19:52	Fri	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-06	15:20:02	Fri	ksmsvzwsms://message/May 6, 2011 3:19:42 PM EDT	1
4124393388	2011-05-06	15:25:30	Fri	ksmsvzwsms://message/CallOut: 7607058888 May 6, 2011 3:25:21 PM EDT	1
4124393388	2011-05-06	15:28:34	Fri	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-06	15:28:44	Fri	ksmsvzwsms://message/May 6, 2011 3:28:25 PM EDT	1
4124393388	2011-05-06	17:04:19	Fri	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-06	17:04:29	Fri	ksmsvzwsms://message/May 6, 2011 5:04:05 PM EDT	1
4124393388	2011-05-06	17:08:35	Fri	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-06	17:08:45	Fri	ksmsvzwsms://message/May 6, 2011 5:08:24 PM EDT	1
4124393388	2011-05-06	17:14:49	Fri	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-06	17:14:59	Fri	ksmsvzwsms://message/May 6, 2011 5:14:37 PM EDT	1
4124393388	2011-05-07	19:16:20	Sat	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-07	19:16:23	Sat	ksmsvzwsms://message/May 7, 2011 12:49:57 PM EDT	1
4124393388	2011-05-07	19:16:27	Sat	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-07	19:16:30	Sat	ksmsvzwsms://message/May 7, 2011 12:51:17 PM EDT	1
4124393388	2011-05-07	19:16:34	Sat	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-07	19:16:38	Sat	ksmsvzwsms://message/May 7, 2011 12:55:39 PM EDT	1
4124393388	2011-05-07	19:39:03	Sat	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-07	19:39:13	Sat	ksmsvzwsms://message/May 7, 2011 7:38:47 PM EDT	1
4124393388	2011-05-07	19:40:34	Sat	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-07	19:40:45	Sat	ksmsvzwsms://message/May 7, 2011 7:40:24 PM EDT	1
4124393388	2011-05-07	19:44:51	Sat	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-07	19:45:01	Sat	ksmsvzwsms://message/May 7, 2011 7:44:42 PM EDT	1
4124393388	2011-05-07	21:40:28	Sat	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-07	21:40:39	Sat	ksmsvzwsms://message/May 7, 2011 9:40:11 PM EDT	1
4124393388	2011-05-07	21:41:24	Sat	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-07	21:41:34	Sat	ksmsvzwsms://message/May 7, 2011 9:41:12 PM EDT	1
4124393388	2011-05-07	21:44:23	Sat	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-07	21:44:33	Sat	ksmsvzwsms://message/May 7, 2011 9:44:12 PM EDT	1
4124393388	2011-05-07	21:54:17	Sat	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-07	21:54:27	Sat	ksmsvzwsms://message/May 7, 2011 9:52:21 PM EDT	1
4124393388	2011-05-07	21:54:31	Sat	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-07	21:54:35	Sat	ksmsvzwsms://message/May 7, 2011 9:53:49 PM EDT	1
4124393388	2011-05-07	21:58:59	Sat	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-07	21:59:08	Sat	ksmsvzwsms://message/May 7, 2011 9:58:51 PM EDT	1
4124393388	2011-05-07	22:04:26	Sat	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-07	22:04:36	Sat	ksmsvzwsms://message/May 7, 2011 10:04:12 PM EDT	1
4124393388	2011-05-07	22:05:48	Sat	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-07	22:05:58	Sat	ksmsvzwsms://message/May 7, 2011 10:05:39 PM EDT	1
4124393388	2011-05-07	22:10:50	Sat	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-07	22:11:00	Sat	ksmsvzwsms://message/May 7, 2011 10:10:42 PM EDT	1
4124393388	2011-05-07	22:21:05	Sat	ksmsvzwsms://message/Service Started	1
4124393388	2011-05-07	22:21:15	Sat	ksmsvzwsms://message/May 7, 2011 10:20:43 PM EDT	1

4124393388	2011-05-07	22:22:11	Sat	ksmsvzwsms://message/Service Started		1
4124393388	2011-05-07	22:22:21	Sat	ksmsvzwsms://message/May 7, 2011 10:22:01 PM EDT		1
4124393388	2011-05-07	22:26:22	Sat	ksmsvzwsms://message/Service Started		1
4124393388	2011-05-07	22:26:32	Sat	ksmsvzwsms://message/May 7, 2011 10:26:14 PM EDT		1
4124393388	2011-05-07	22:38:55	Sat	ksmsvzwsms://message/Service Started		1
4124393388	2011-05-07	22:39:05	Sat	ksmsvzwsms://message/May 7, 2011 10:38:36 PM EDT		1
4124393388	2011-05-07	22:39:15	Sat	ksmsvzwsms://message/Service Started		1
4124393388	2011-05-07	22:39:19	Sat	ksmsvzwsms://message/May 7, 2011 10:38:57 PM EDT		1
4124393388	2011-05-07	22:41:03	Sat	ksmsvzwsms://message/Service Started		1
4124393388	2011-05-07	22:41:13	Sat	ksmsvzwsms://message/May 7, 2011 10:40:51 PM EDT		1
4124393388	2011-05-07	23:10:09	Sat	ksmsvzwsms://message/Service Started		1
4124393388	2011-05-07	23:10:19	Sat	ksmsvzwsms://message/May 7, 2011 11:08:06 PM EDT		1
4124393388	2011-05-07	23:16:48	Sat	ksmsvzwsms://message/Service Started		1
4124393388	2011-05-07	23:16:58	Sat	ksmsvzwsms://message/May 7, 2011 11:16:34 PM EDT		1
4124393388	2011-05-07	23:18:56	Sat	ksmsvzwsms://message/Service Started		1
4124393388	2011-05-07	23:19:06	Sat	ksmsvzwsms://message/May 7, 2011 11:18:47 PM EDT		1
4124393388	2011-05-07	23:25:46	Sat	ksmsvzwsms://message/Service Started		1
4124393388	2011-05-07	23:25:56	Sat	ksmsvzwsms://message/May 7, 2011 11:25:34 PM EDT		1
4124393388	2011-05-07	23:33:21	Sat	ksmsvzwsms://message/Service Started		1
4124393388	2011-05-07	23:33:32	Sat	ksmsvzwsms://message/May 7, 2011 11:31:19 PM EDT		1
4124393388	2011-05-07	23:33:36	Sat	ksmsvzwsms://message/Service Started		1
4124393388	2011-05-07	23:33:39	Sat	ksmsvzwsms://message/May 7, 2011 11:32:56 PM EDT		1
4124393388	2011-05-07	23:48:38	Sat	ksmsvzwsms://message/Service Started		1
4124393388	2011-05-07	23:48:48	Sat	ksmsvzwsms://message/May 7, 2011 11:46:37 PM EDT		1
4124393388	2011-05-07	23:48:52	Sat	ksmsvzwsms://message/Service Started		1
4124393388	2011-05-07	23:48:55	Sat	ksmsvzwsms://message/May 7, 2011 11:48:10 PM EDT		1
4124393388	2011-05-07	23:58:32	Sat	ksmsvzwsms://message/Service Started		1
4124393388	2011-05-07	23:58:42	Sat	ksmsvzwsms://message/May 7, 2011 11:58:14 PM EDT		1
4124393388	2011-05-08	00:58:46	Sun	ksmsvzwsms://message/May 7, 2011 11:58:14 PM EDT		1
4124393388	2011-05-08	00:11:20	Sun	ksmsvzwsms://message/May 8, 2011 12:11:08 AM EDT		1
4124393388	2011-05-08	00:12:16	Sun	ksmsvzwsms://message/pkg uploaded!		1
4124393388	2011-05-11	13:38:50	Wed	ksmsvzwsms://message/Service Started		0
4124393388	2011-05-11	13:38:54	Wed	ksmsvzwsms://message/May 8, 2011 5:41:16 PM EDT		0
4124393388	2011-05-11	13:39:06	Wed	ksmsvzwsms://message/Service Started		0
4124393388	2011-05-11	13:39:10	Wed	ksmsvzwsms://message/May 8, 2011 5:42:16 PM EDT		0
4124393388	2011-05-11	13:39:14	Wed	ksmsvzwsms://message/Service Started		0
4124393388	2011-05-11	13:39:17	Wed	ksmsvzwsms://message/May 8, 2011 5:49:13 PM EDT		0
4124393388	2011-05-11	13:39:21	Wed	ksmsvzwsms://message/Service Started		0
4124393388	2011-05-11	13:39:25	Wed	ksmsvzwsms://message/May 8, 2011 11:47:51 PM EDT		0
4124393388	2011-05-11	13:39:29	Wed	ksmsvzwsms://message/Service Started		0
4124393388	2011-05-11	13:39:33	Wed	ksmsvzwsms://message/May 9, 2011 12:03:09 AM EDT		0
4124393388	2011-05-11	13:39:36	Wed	ksmsvzwsms://message/Service Started		0
4124393388	2011-05-11	13:39:40	Wed	ksmsvzwsms://message/May 9, 2011 12:44:18 AM EDT		0

Table 17. Received SMS messages from Yob Taog's smartphone application ('ksms' signature)

Sender Number	Date (UTC-4)			Message	Read(1) or not(0)
(Yob)4124393388	2011-05-05	21:35:06	Thu	ksmsFORWARDED SMS from 6245 at 20110505T173426 America/New_York(4,124,-14400,1,1304631266) :shandra@cheerful.com (Nearby! Coming for my beer) Hey Yob, I am closi ng in on Fat Heads. See ya soon.	1
(Yob)4124393388	2011-05-06	13:53:45	Fri	ksmsFORWARDED SMS from 6245 at 20110506T095308 America/New_York(5,125,-14400,1,1304689988) :sms.dynadel@gmail.com Reminder, planned IT outage this weekend. This	1
(Yob)4124393388	2011-05-06	13:53:55	Fri	ksms maintenance window will start at 3 PM today and continue for approx 48 hours.	1
(Yob)4124393388	2011-05-06	13:55:32	Fri	ksmsFORWARDED SMS from 6245 at 20110506T095455 America/New_York(5,125,-14400,1,1304690095) :sms.dynadel@gmail.com This effects external services such as website,	1

(Yob)4124393388	2011-05-07 19:40:00 Sat	ksmsFORWARDED SMS from 6245 at 20110507T135649 America/New_York(6,126,-14400,1,1304791009) :shandra@cheerful.com (Save me!) If Luke asks, I'm going out with you	1
(Yob)4124393388	2011-05-07 19:40:10 Sat	ksmsto dinner, OK? I just can't face Mr. Smooth tonight. Shandra	1
(Yob)4124393388	2011-05-07 23:10:23 Sat	ksmsFORWARDED SMS from 6245 at 20110507T190532 America/New_York(6,126,-14400,1,1304809532) :shandra@cheerful.com (Re: Or you can walk down) Walking down now. Hop	1
(Yob)4124393388	2011-05-07 23:10:41 Sat	ksmse you are still vertical. ----- Original Message ----- From: 4124393388@VTEXT.COM Sent: 05/07/11 07:56 PM To:	1
(Yob)4124393388	2011-05-07 23:11:11 Sat	ksmsFORWARDED SMS from 6245 at 20110507T190532 America/New_York(6,126,-14400,1,1304809532) :shandra@cheerful.com (Re: Or you can walk down) Walking down now. Hop	1
(Yob)4124393388	2011-05-07 23:11:25 Sat	ksmsFORWARDED SMS from 6245 at 20110507T190749 America/New_York(6,126,-14400,1,1304809669) :shandra@cheerful.com (Re: Or you can walk down) Hope you guys are sti	1
(Yob)4124393388	2011-05-07 23:11:28 Sat	ksmsll at double-wide ... ----- Original Message ----- From: 4124393388@VTEXT.COM Sent: 05/07/11 07:56 PM To: shan	1
(Yob)4124393388	2011-05-11 13:38:58 Wed	ksmsFORWARDED SMS from 6245 at 20110508T045142 America/New_York(0,127,-14400,1,1304844702) :shandra@cheerful.com (Thanks) Thanks for being so gracious last night	0
(Yob)4124393388	2011-05-11 13:39:02 Wed	ksms Shandra	0
(Yob)4124393388	2011-05-11 13:39:45 Wed	ksmsFORWARDED SMS from 6245 at 20110510T032619 America/New_York(2,129,-14400,1,1305012379) :shandra@cheerful.com (You around for lunch) Hey -- a few of us are go	0
(Yob)4124393388	2011-05-11 13:39:49 Wed	ksmsing to that great Indian buffet for lunch today. You interested?	0
(Yob)4124393388	2011-05-11 13:39:53 Wed	ksmsFORWARDED SMS from 6245 at 20110510T083450 America/New_York(2,129,-14400,1,1305030890) :shandra@cheerful.com (Re: Sorry, still an Atlanta till) OK. Safe trav els!	0
(Yob)4124393388	2011-05-11 13:39:56 Wed	ksmsels! ----- Original Message ----- From: 4124393388@VTEXT.COM Sent: 05/10/11 09:31 AM To: shandra@cheerful.com	0
(Yob)4124393388	2011-05-11 13:40:04 Wed	ksmsFORWARDED SMS from 4124393388 at 20110510T124303 America/New_York(2,129,-14400,1,1305045783) :You have insufficient funds to send message.	0

Table 18. SMS messages with Mr E

Number	Date (UTC-4)	Message	Receive(1) or Send(2)
(Mr e) 4439264768	2011-05-04 21:09:25 Wed	Got the perfect Guy, plan is already in motion	2
(Mr e) 4439264768	2011-05-04 21:12:19 Wed	Break a leg	1
(Mr e) 4439264768	2011-05-06 14:23:51 Fri	the implementation seems to be working ok, no gold yet though	2

(Mr e) 4439264768	2011-05-07 21:47:02 Sat	software seems to be working, I was a little worried given the source and short timeline	2
(Mr e) 4439264768	2011-05-08 01:13:48 Sun	Got something for you, sample shortly	2
(Mr e) 4439264768	2011-05-08 14:05:34 Sun	Got some results, I think we need to up the fee, say double?	2
(Mr e) 4439264768	2011-05-08 14:16:14 Sun	You are joking, right? You can't seriously think about changing the deal now.	1
(Mr e) 4439264768	2011-05-08 14:22:39 Sun	I just sent you a sample, I think you'll be pleased...	2
(Mr e) 4439264768	2011-05-08 14:30:13 Sun	You are serious then. I can see the information is valuable but I am displeased with you breaking the deal.	1
(Mr e) 4439264768	2011-05-08 14:56:44 Sun	I knew you'd like them, ill be at the agreed spot, in about 25 min for the exchange	2

3.3.2. Scenario 1 – Email

Table 19. Contents of Email

Date (UTC-4)	Sender	Receiver	Contents	Attachment
2011-05-04 20:40:15 Wed	norby441@gmail.com	Mr E		
2011-05-06 14:25:37 Fri	"Gmail Team" <mail-noreply@google.com>	"norb k" <norby441@gmail.com>	To spice up your inbox with colors and themes, check out the Themes tab under...	
2011-05-08 14:08:38 Sun	"norb k" <norby441@gmail.com>	"Mr E" <mre@hushmail.com>	this is just a taste, much more where this came from.	2228-12.pdf
2011-05-08 14:32:24 Sun	"norb k" <norby441@gmail.com>	"Mr E" <mre@hushmail.com>	This information is obviously very valuable. I'd like to keep our relationship, but others would be willing to pay more.	
2011-05-08 14:43:36 Sun	"Mr E" <mre@hushmail.com>	"norb k" <norby441@gmail.com>	Re: showing i'm serious I certainly don't want you giving these files to someone else. Expect a call from me shortly.	

3.3.3. Scenario 1 – Contacts

Table 20. Contact List

Name	Phone Number
Mr E	4439264768
- (unknown)	4124623802

3.3.4. Scenario 1 – Access to Web Server and Download Files

Table 21. Downloaded Files from 50.56.29.109

Dowonloaded File	Date (UTC-4)	URL
/sdcard/download/2201-4.pdf	2011-05-08 13:59:56 Sun	http://50.56.29.109:80/ss/2201-4.pdf
/sdcard/download/2201-7.pdf	2011-05-08 14:00:18 Sun	http://50.56.29.109:80/ss/2201-7.pdf
/sdcard/download/2201-9.pdf	2011-05-08 14:01:08 Sun	http://50.56.29.109:80/ss/2201-9.pdf

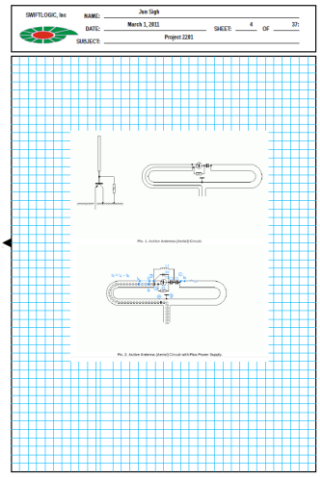
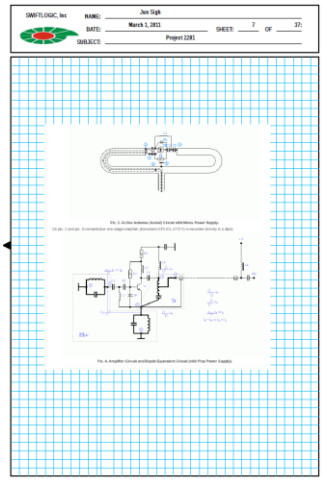
/sdcard/download/2201-8.pdf	2011-05-08	14:01:22	Sun	http://50.56.29.109:80/ss/2201-8.pdf
/sdcard/download/2228-7.pdf	2011-05-08	14:01:48	Sun	http://50.56.29.109:80/ss/2228-7.pdf
/sdcard/download/2228-10.pdf	2011-05-08	14:01:57	Sun	http://50.56.29.109:80/ss/2228-10.pdf
/sdcard/download/2228-11.pdf	2011-05-08	14:02:20	Sun	http://50.56.29.109:80/ss/2228-11.pdf
/sdcard/download/2228-12.pdf	2011-05-08	14:02:33	Sun	http://50.56.29.109:80/ss/2228-12.pdf
/sdcard/download/2228-15.pdf	2011-05-08	14:02:54	Sun	http://50.56.29.109:80/ss/2228-15.pdf

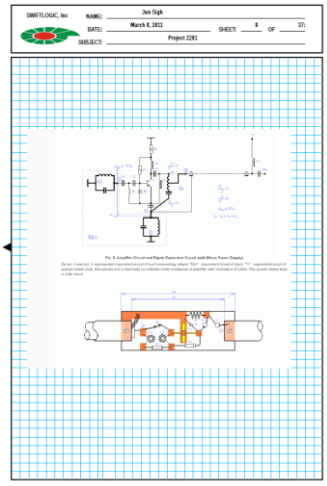
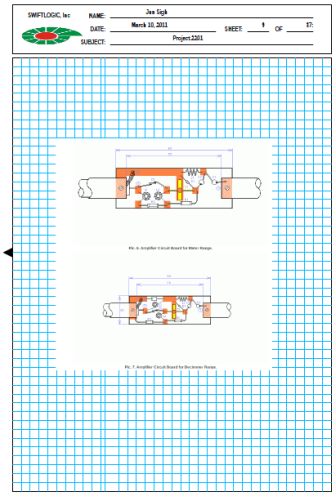
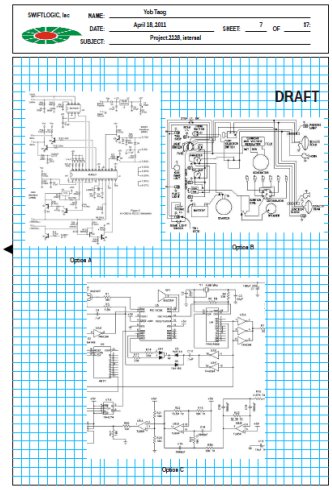
3.3.5. Scenario 1 – SDCard

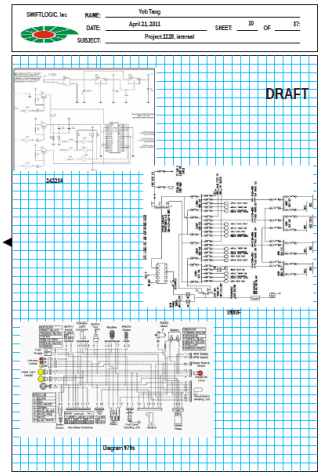
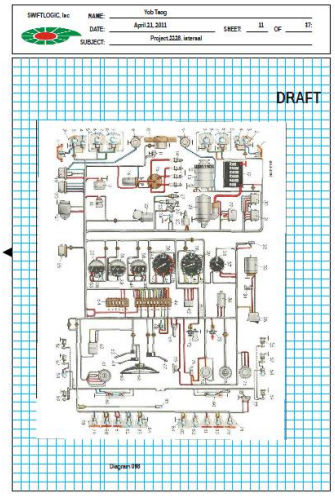
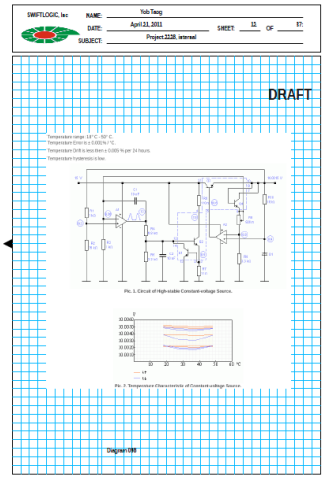
The followings are presented in the SDCard of Scenario 1.

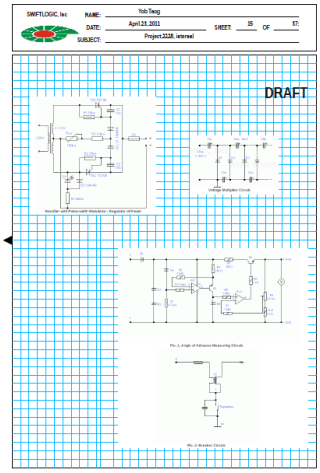
Table 22. Images and PDF files in SDCard of Scenario 1

SDcard Image	Type	File Name	Created Time (UTC-4)
	JPEG	2011-05-06 14.43.35.jpg	-
	JPEG	292048878.jpg	-
	JPEG	1304706535900.jpg	-

	JPEG	1304707417417.jpg	-
	PDF	2201-4.pdf	2011-05-07 12:32:26 (Embedded UTC-4)
	PDF	2201-7.pdf	2011-05-07 12:31:34 (Embedded UTC-4)

	PDF	2201-8.pdf	2011-05-07 12:31:23 (Embedded UTC-4)
	PDF	2201-9.pdf	2011-05-07 12:31:01 (Embedded UTC-4)
	PDF	2228-7.pdf	2011-05-07 12:30:45 (Embedded UTC-4)

	PDF	2228-10.pdf	2011-05-07 12:30:23 (Embedded UTC-4)
	PDF	2228-11.pdf	2011-05-06 19:58:09 (Embedded UTC-4)
	PDF	2228-12.pdf	2011-05-06 19:57:52 (Embedded UTC-4)

	PDF	2228-15.pdf	2011-05-06 19:57:37 (Embedded UTC-4)

3.3.6. Scenario 2 – Media Mounter(/data/app/com.andriod.mm.apk) analysis

Media Mounter is located at /data/app/com.andriod.mm.apk. Since apk has a ZIP format, the time information of a file can be obtained by checking the time information in the compressed file. The confirmation result shows that it has the time information of 2011-05-04 AM 01:41:38.

In addition, we confirmed with the meta information of the file system that it has 2011-05-05 00:49 (not based on the New York time zone). This is around the time when the user first installed USIM and operated it.

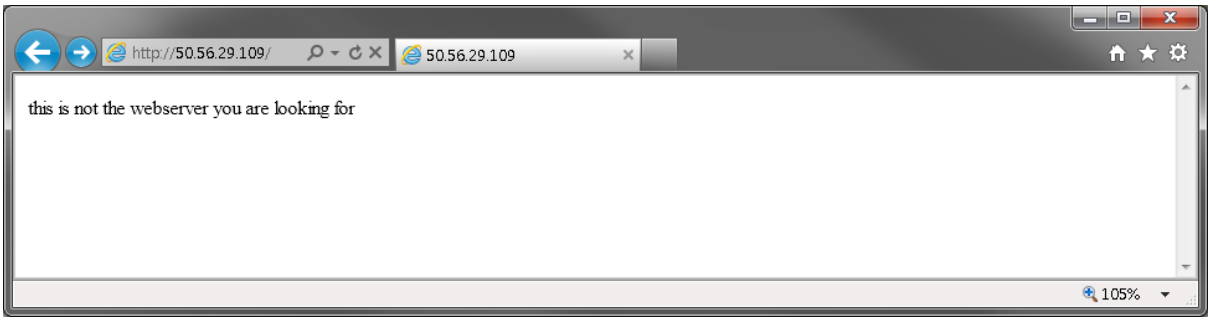
As a result of disassembling it using Dedexer (http://dedexer.sourceforge.net), which is a DEX file disassembler, the following contents are confirmed (part of the contents).

```
1  .class public com/andriod/mm/mediaMounter
2  .super android/app/Service
3  .source mediaMounter.java
4
5  .field private static final DEFAULTHOST Ljava/lang/String; = "50.56.29.109"
6  .field private static final DEFAULTPORT I = 10001   ; 0x2711
7  .field private static final FILENAME Ljava/lang/String; = "temp"
8  .field private static final HOUR J = 3600000    ; 0x36ee80
9  .field private static final LOG_TAG Ljava/lang/String; = "mm"
10 .field private mHandler Landroid/os/Handler;
11 .field private mTask Ljava/util/TimerTask;
12
13 .method public <init>()V
14 .limit registers 2
15 ; this: v1 (Lcom/andriod/mm/mediaMounter;)
16 .line 51
17     invoke-direct   {v1},android/app/Service/<init> ; <init>()V
18 .line 63
19     new-instance    v0,android/os/Handler
20     invoke-direct   {v0},android/os/Handler/<init>  ; <init>()V
21     iput-object v0,v1,com/andriod/mm/mediaMounter.mHandler Landroid/os/Handler;
22 .line 346
```

Figure 23. Some contents of the disassembled com.andriod.mm.apk

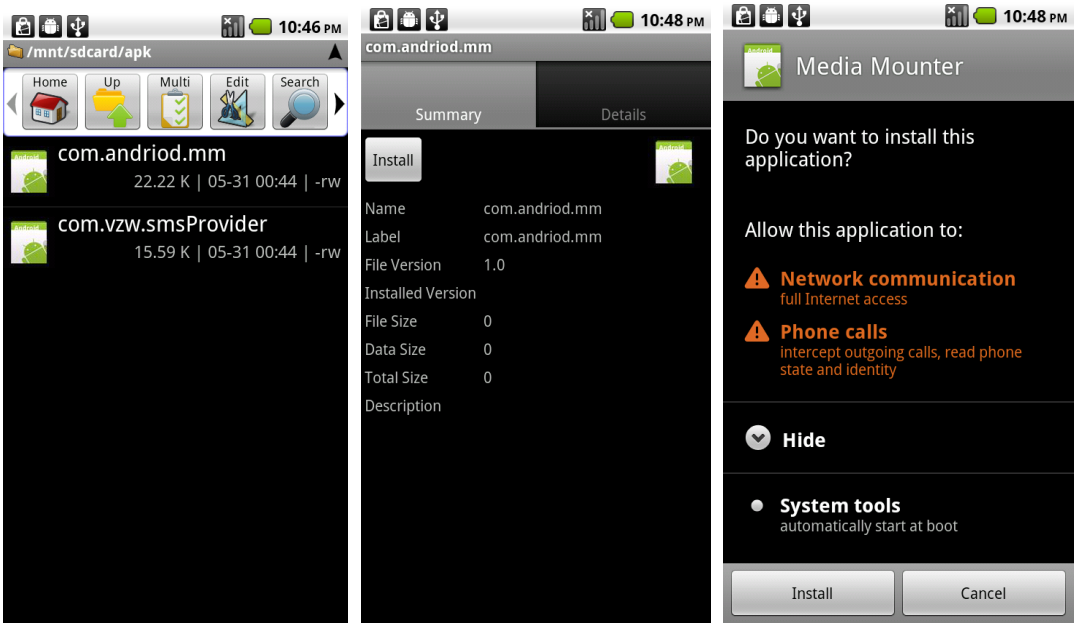
The analysis result of the above source showed that it is transmitted to the server located at ’50.56.29.109’ (port 10001) by compressing the ‘/sdcard’ files with the file name of ‘temp’ at a certain cycle. It can actually be confirmed in the ‘/data/data/com.andriod.mm/files/temp’ file that the files located in ‘/sdcard’ are compressed.

The ’50.56.29.109’ is the same server with the one Donald Norby accessed in Scenario 1.



In addition, it is expressed in a way that the contents of the calls received and made by the user are sent through SMS. Sending through SMS was expressed to be using a separate provider. The pertinent contents can be checked through SMS/MMS records of 'Scenario 1.'

And then, we tried to install the application, com.andriod.mm.apk, in our DROID smartphone.



Above figures shows the 'Media Mounter' application. When it is installed, the Android installer informs some malicious activities such as 'Network communication' and 'Intercept Calls'. After installing the application, we could not identify an application icon. This means that the application is running in background.

The analysis result showed that the provider was operated to send SMS as a background using /data/app/com.vzw.smsProvider.apk. The following figure is part of the disassembled contents of com.vzw.smsProvider.apk. We can see that the call history of Yob Taog was sent via the phone number "14124393389", which is the number of Donald Nroby in Scenario 1.

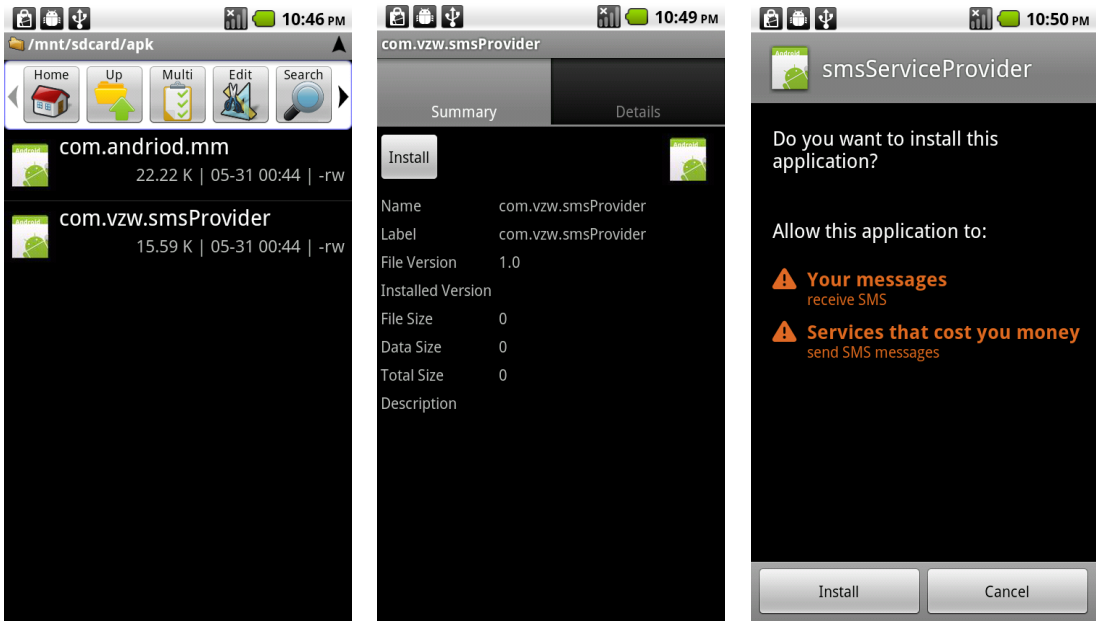
```
.class public com/vzw/smsProvider/smsLib
.super java/lang/Object
.source smsLib.java

.field private static final MAGIC Ljava/lang/String; = "ksms"
.field private static final phoneNo Ljava/lang/String; = "14124393389"
.field context Landroid/content/Context;

.method <init>(Landroid/content/Context;)V
.limit registers 3
; this: v1 (Lcom/vzw/smsProvider/smsLib;)
; parameter[0] : v2 (Landroid/content/Context;)
.line 19
    invoke-direct   {v1},java/lang/Object/<init>    ; <init>()V
.line 17
    const/4 v0,0
    iput-object v0,v1,com/vzw/smsProvider/smsLib.context Landroid/content/Context;
.line 20
    iput-object v2,v1,com/vzw/smsProvider/smsLib.context Landroid/content/Context;
.line 21
    return-void
.end method
```

Figure 24. Some contents of the disassembled com.vzw.smsProvider.apk

And then, we tried to install the application, com.vzw.smsProvider.apk, in our DROID smartphone.



Above figures shows the 'smsServiceProvider' application. When it is installed, the Android installer informs some malicious activities such as 'Receive SMS' and 'Send SMS messages'. After installing the application, we could not identify an application icon. This means that the application is running in background.

In addition, if we look at the /data/anr/traces.txt file, the following operation records of 'Cmd line: com.andriod.mm' can be confirmed.

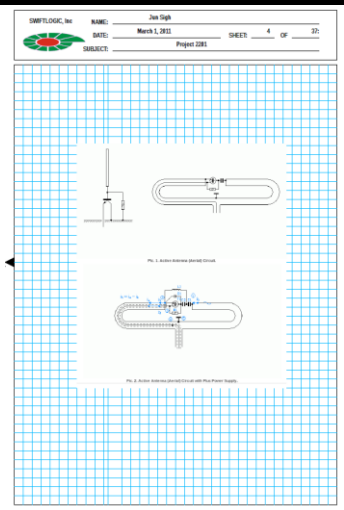
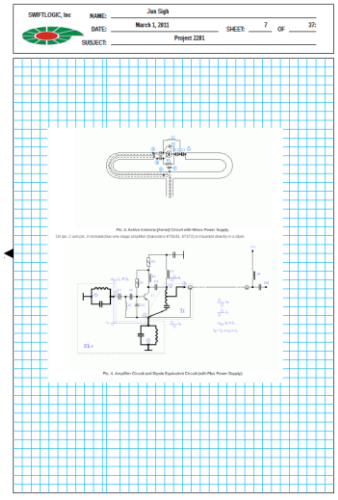
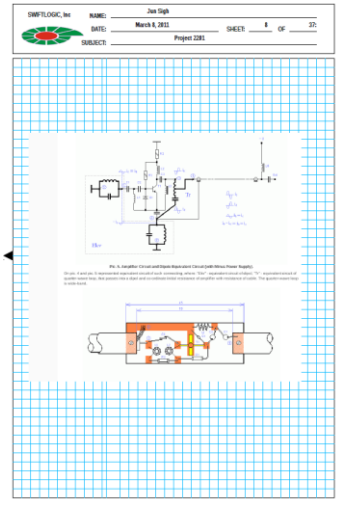
....
Line 1386: ----- pid 1327 at 2011-05-04 22:06:12 -----
Line 2585: ----- pid 1377 at 2011-05-07 22:38:43 -----
Line 2628: ----- pid 1342 at 2011-05-07 23:08:15 -----
Line 2671: ----- pid 1396 at 2011-05-07 23:08:46 -----
Line 2714: ----- pid 1347 at 2011-05-07 23:16:43 -----
Line 2757: ----- pid 1319 at 2011-05-08 23:47:57 -----
....

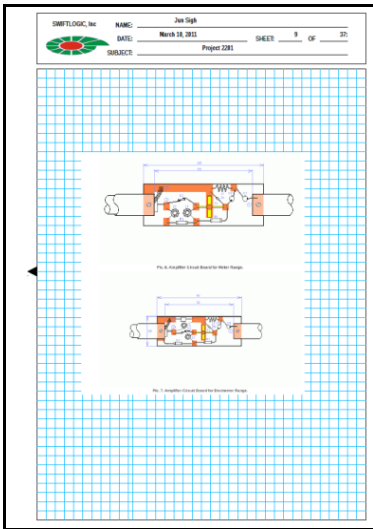
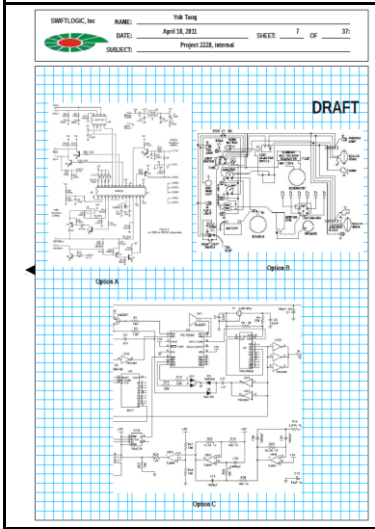
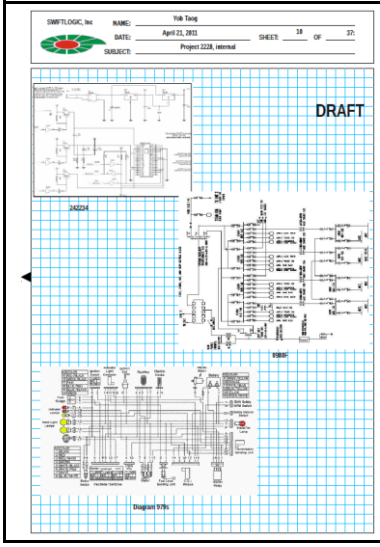
Figure 25. The 'com.andriod.mm' record of '/data/anr/traces.txt'

In the file '/data/data/com.android.mm/files/temp' which contains application data created by Media Mounter, a total of 116 files were found, including files that are in '/sdcard', SQLite DB files, image files, and PDF files. Among them, 9 PDF files contain the contents of valuable documents of SWIFTLOGIC and inc.

The details of the PDF files found are shown below.

Table 23. PDF files of 'com.android.mm/files/temp'

PDF File	FileName	Embedded CreatedTime (UTC-4)
	2201-4.pdf	Sat, 07 May 2011 12:32:26
	2201-7.pdf	Sat, 07 May 2011 12:31:34
	2201-8.pdf	Sat, 07 May 2011 12:31:23

	2201-9.pdf	Sat, 07 May 2011 12:31:01
	2228-7.pdf	Sat, 07 May 2011 12:30:45
	2228-10.pdf	Sat, 07 May 2011 12:30:23

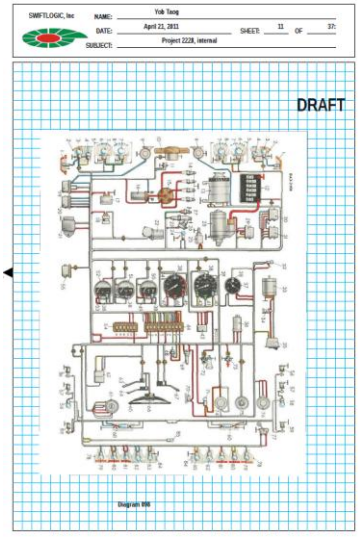
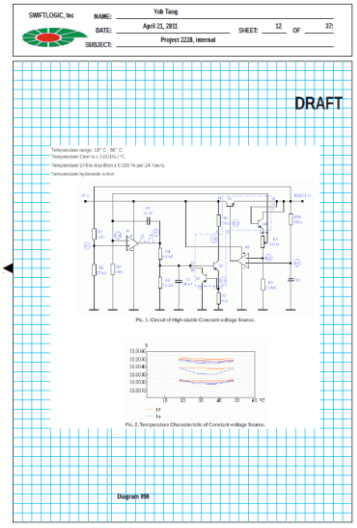
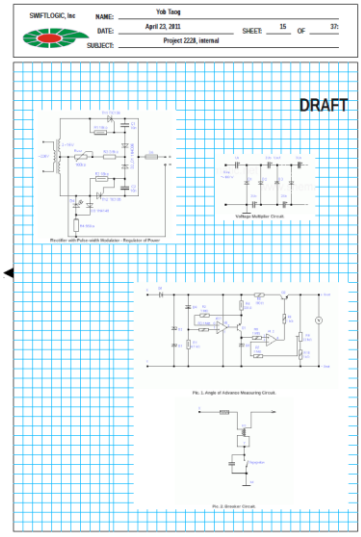
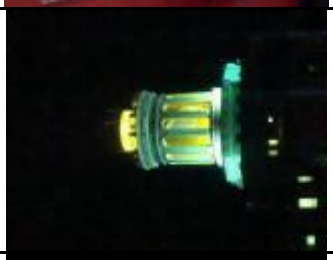
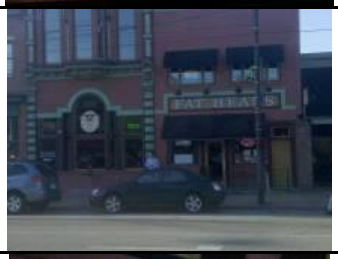
	2228-11.pdf	Fri, 06 May 2011 19:58:09
	2228-12.pdf	Fri, 06 May 2011 19:57:52
	2228-15.pdf	Fri, 06 May 2011 19:57:37

Table 24. Contents of 'astro.db(thumbnail_dir table)'

Thumbnail Image	Location	Target Filename	Viewing time (UTC-4)
	/sdcard/DCIM/Camera	2011-05-04 21.00.36.jpg	2011-05-07 13:07:00
	/sdcard/DCIM/Camera	2011-05-04 21.00.55.jpg	2011-05-07 13:07:00
	/sdcard/DCIM/Camera	2011-05-04 21.01.06.jpg	2011-05-07 13:07:01
	/sdcard/DCIM/Camera	2011-05-04 22.25.55.jpg	2011-05-07 13:07:01
	/sdcard/DCIM/Camera	2011-05-04 22.26.48.jpg	2011-05-07 13:07:01
	/sdcard/DCIM/Camera	2011-05-05 12.58.20.jpg	2011-05-07 13:07:02

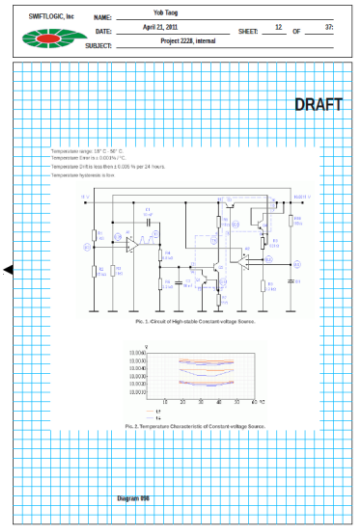
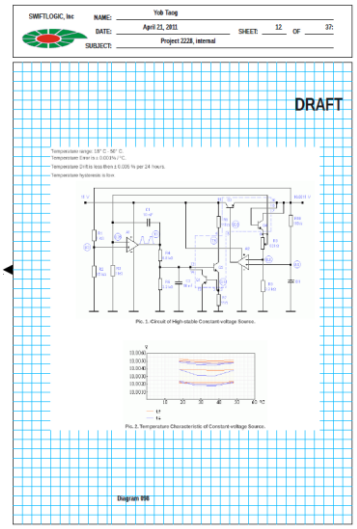
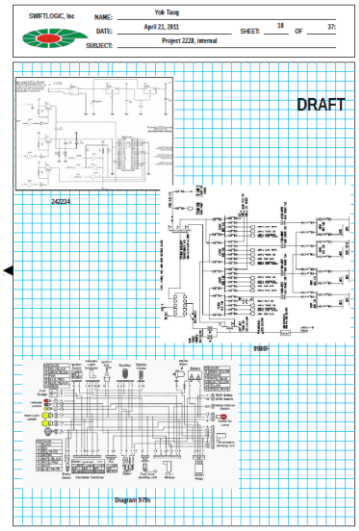
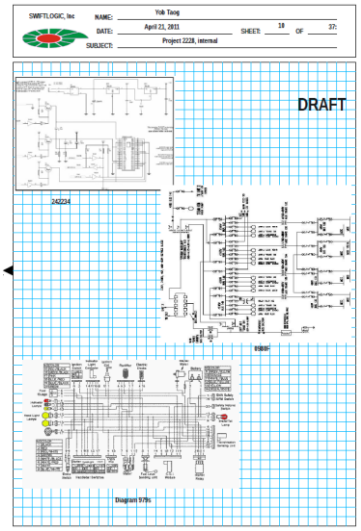
	/sdcard/DCIM/Camera	2011-05-04 21.00.21.jpg	2011-05-07 13:07:03
	/sdcard/DCIM/Camera	2011-05-05 13.37.50.jpg	2011-05-07 13:07:03
	/sdcard/Android/data/com.seesmic/temp	2011-05-05 19.13.49.jpg	2011-05-07 21:56:52
	/sdcard/Android/data/com.seesmic/temp	2011-05-05 12.58.20.jpg	2011-05-07 21:56:54
	/sdcard/DCIM/Camera	2011-05-05 19.05.10.jpg	2011-05-07 21:57:11
	/sdcard/DCIM/Camera	2011-05-05 19.05.38.jpg	2011-05-07 21:57:12

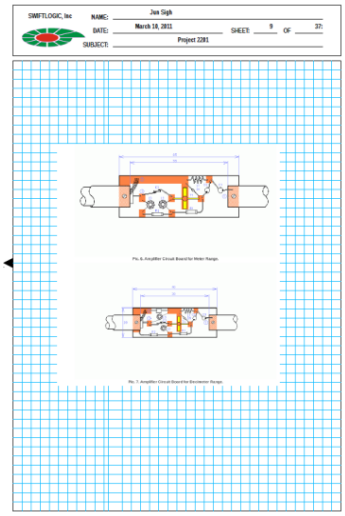
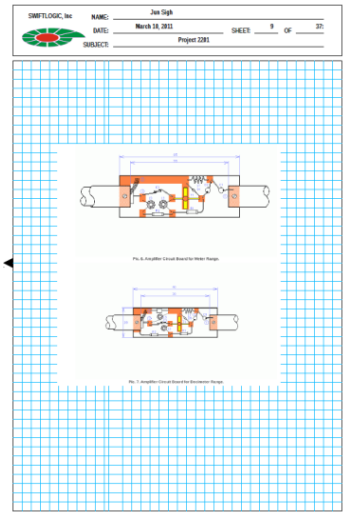
	/sdcard/DCIM/Camera	2011-05-05 19.13.49.jpg	2011-05-07 21:57:12
	/sdcard/DCIM/Camera	2011-05-05 19.47.10.jpg	2011-05-07 21:57:13
	/sdcard/DCIM/Camera	2011-05-05 19.47.26.jpg	2011-05-07 21:57:35
	/sdcard/DCIM/Camera	2011-05-05 19.47.45.jpg	2011-05-07 21:57:36
	/sdcard/DCIM/Camera	2011-05-05 19.47.57.jpg	2011-05-07 21:57:36
	/sdcard/DCIM/Camera	2011-05-05 19.48.34.jpg	2011-05-07 21:57:37

	/sdcard/DCIM/Camera	2011-05-06 17.40.22.jpg	2011-05-07 21:57:38

Performing carving for the pertinent contents and '/sdcard', files presumed to be duplicates were found. The details are as shown below.

Table 25. Results of carving astro.db and /sdcard and their comparison

astro.db(thumbnail_dir table)	FileName (astro.db)	SDcard Carving	FileName (/SDcard Carving)
	2228-12.pdf		[34a].pdf
	2228-10.pdf		[35d].pdf

	2228-9.pdf		[367].pdf
	2011-05-04 21.00.36.jpg		EXIF_[29].exif
	2011-05-05 13.37.50.jpg		EXIF_[151].exif JFIF_[16d].jpg
	2011-05-05 19.13.49.jpg		EXIF_[1b9].exif, JFIF_[1e1].jpg, JFIF_[1e3].jpg

	2011-05-05 19.05.10.jpg		EXIF_[18c].exif JFIF_[19c].jpg
	2011-05-05 19.05.38.jpg		EXIF_[19d].exif, JFIF_[1b7].jpg
	2011-05-05 19.13.49.jpg		EXIF_[1b9].exif, JFIF_[1e1].jpg, JFIF_[1e3].jpg
	2011-05-05 19.47.10.jpg		EXIF_[209].exif, JFIF_[219].jpg

	2011-05-05 19.47.26.jpg		EXIF_[21a].exif, JFIF_[24d].jpg
	2011-05-05 19.47.45.jpg		EXIF_[22d].exif, JFIF_[24f].jpg
	2011-05-05 19.47.57.jpg		EXIF_[23e].exif, JFIF_[250].jpg
	2011-05-05 19.48.34.jpg		EXIF_[251].exif, JFIF_[277].jpg

	2011-05-05 19.48.34.jpg		JFIF_[28e].jpg

3.3.7. Scenario 2 – Alarm

It gets stored in the file 'alarms.db(alarms table)' in the '/data/data/com.android.alarmclock/databases' directory.

Alarm time is set in 'dayofweek'. The days of the week and their corresponding numbers are as follows: Monday (1); Tuesday (2); Wednesday (4); Thursday (8); Friday (16); Saturday (32); and Sunday (64). The number to which the desired day is added gets stored in the field 'dayofweek'. Details of the existing alarms are shown below.

Table 26. Contents of 'com.android.alarmclock/databases/alarms.db(alarms table)'

hour	minutes	datyofweek	enabled
7	0	127	0
8	0	31	1
9	0	0	0

Alarm settings are stored in the file 'settings.db(system table)' which contains device settings as well. The file is in the directory '/data/data/com.android.providers.settings/databases'. The details are as follows.

Table 27. Contents of 'com.android.providers.settings/databases/settings.db(system table)'

name	value
volume_alarm	6
volume_notification	5
vibrate_on	4
mode_ringer_streams_affected	166
mute_streams_affected	46
dim_screen	1
stay_on_while_plugged_in	0
screen_off_timeout	60000
emergency_tone	0
call_auto_retry	0
dtmf_tone_type	0
hearing_aid	0

tty_mode	0
airplane_mode_radios	cell,bluetooth,wifi
airplane_mode_toggleable_radios	wifi
auto_time	1
screen_brightness	255
screen_brightness_mode	1
window_animation_scale	1
transition_animation_scale	1
accelerometer_rotation	1
haptic_feedback_enabled	1
notification_sound	content://media/internal/audio/media/26
ringtone	content://media/internal/audio/media/40
alarm_alert	content://media/internal/audio/media/78
volume_voice	4
volume_voice_last_audible	4
airplane_mode_on	0
next_alarm_formatted	Wed 8:00 am
mode_ringer	2
volume_system	7
volume_system_last_audible	7
volume_music	2
volume_music_last_audible	2
volume_ring	1
volume_ring_last_audible	1
font_scale	1

From the fact that the value of 'next_alarm_formatted' is 'Wed 8:00 am', it can be known that device image collection took place from 8 AM Tuesday to 8 AM Wednesday.

3.3.8. Scenario 2 – Download

It gets stored in the file 'downloads.db (downloads table)' in the '/data/data/com.android.proviers.downloads /databases' directory.

Table 28. Contents of 'com.android.proviers.downloads/databases/downloads.db(downloads table)'

Title	Time (UTC-4)	Size	Data
Downloading system update	2011-05-04 20:52:30	15712438	/cache/fa406da6c8bb.signed-voles-ESE81-from-ESD56.fa406da6.zip
Market Update	2011-05-04 21:15:45	2209725	/cache/downloadfile.apk

Angry Birds	2011-05-04 21:41:06	-1	
Angry Birds Seasons	2011-05-04 21:41:06	-1	
Paper Toss	2011-05-04 21:34:48	6205223	/cache/downloadfile-6.apk
Toss It	2011-05-04 21:34:39	3568224	/cache/downloadfile-2.apk
Live BlackJack	2011-05-04 21:37:46	5730628	/cache/downloadfile-7.apk
Air Control Lite	2011-05-04 21:36:35	2973933	/cache/downloadfile-8.apk
Pool Master Pro	2011-05-04 21:35:48	1752843	/cache/downloadfile-16.apk
	2011-05-06 12:34:39	46530	/cache/downloadfile.pdf
	2011-05-06 14:08:28	483	/cache/downloadfile.jpeg
(2228-11.pdf)	2011-05-07 12:51:53	260786	/cache/downloadfile-1.pdf
Market Update	2011-05-07 12:54:44	2209725	/cache/downloadfile-1.apk
(2228-12.pdf)	2011-05-07 13:08:06	48113	/cache/downloadfile-2.pdf
(2228-15.pdf)	2011-05-07 13:10:31	47157	/cache/downloadfile-3.pdf
(2201-4.pdf)	2011-05-07 13:11:12	29541	/cache/downloadfile-4.pdf
(2201-7.pdf)	2011-05-07 13:11:30	42881	/cache/downloadfile-5.pdf
(2201-8.pdf)	2011-05-07 13:11:44	52359	/cache/downloadfile-6.pdf
(2201-9.pdf)	2011-05-07 13:12:02	46343	/cache/downloadfile-7.pdf
(2228-7.pdf)	2011-05-07 13:12:21	177047	/cache/downloadfile-8.pdf
(2228-10.pdf)	2011-05-07 13:12:33	136844	/cache/downloadfile-9.pdf

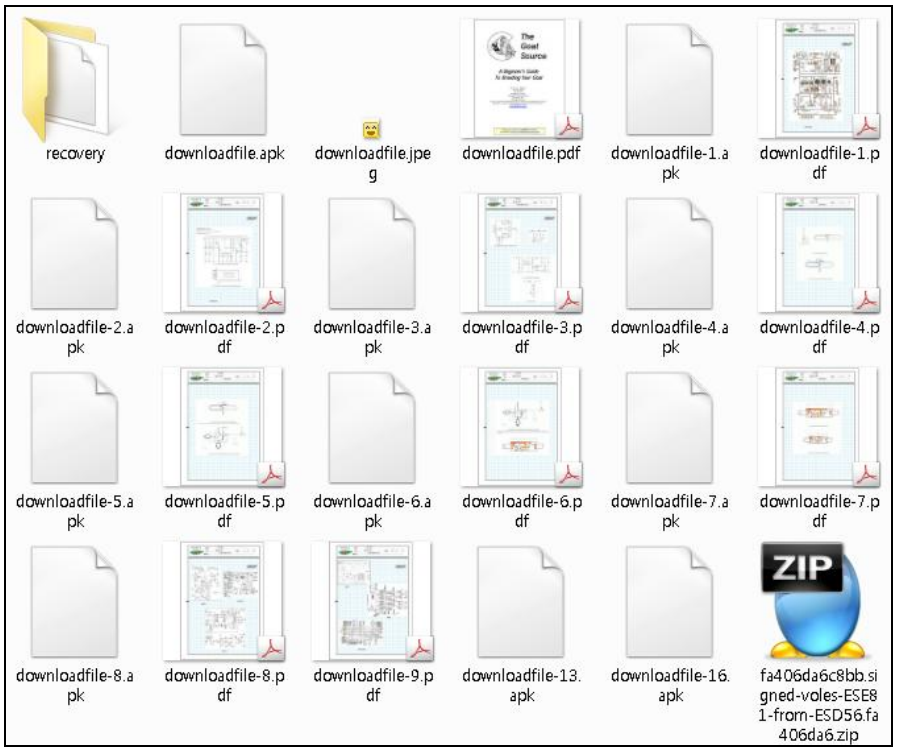


Figure 26. Contents of mtd7.dd (include Scenario_2_mtd7.dd.7z)

3.3.9. Scenario 2 – Location Information

Table 29. Contents of 'com.android.browser/app_geolocation/CachedPosition.db(CachePosition table)'

Time (UTC-4)	Latitude	Longitude	Altitude
2011-05-08 18:39:17	40.4951700666667	-80.2470678833333	390.8

Table 30. Contents of 'com.android.browser/app_geolocation/GeolocationPermissions(Permissions table)'

Origin	Allow
http://m.facebook.com	1

Looking at the details of the two files, it can be known that the location information occurred by allowing in the Facebook application a feature that provides location information to friends. Checking the location in Google Map, it is as shown below.

Figure 27. Google Map Search Result(Latitude: 40.4951700666667, Longitude: -80.2470678833333)

Checking it with Google Map, it can be seen that the last location information was recorded in 'Terminal C' at 'Pittsburgh International Airport'.

3.3.10. Scenario 2 – Web Browser

It gets stored in the file 'browser.db (bookmarks table)' in the '/data/data/com.android.browser/databases' directory.

Table 31. Contents of 'com.android.browser/databases/browser.db(bookmarks table)'

title	url	visits	Date (UTC-4)	bookmark
Google	http://www.google.com/m?client=ms-android-verizon	0		1
Verizon	http://www.verizonwireless.com/	0		1
Picasa	http://picasaweb.google.com/m/viewer?source=androidclient	0		1
Yahoo!	http://www.yahoo.com/	0		1
MSN	http://www.msn.com/	0		1
MySpace	http://www.myspace.com/	0		1
Facebook	http://www.facebook.com/	0		1
Wikipedia	http://www.wikipedia.org/	0		1
eBay	http://www.ebay.com/	0		1
CNN	http://www.cnn.com/index.html	0		1
NY Times	http://www.nytimes.com/	0		1
ESPN	http://espn.com/	0		1
Amazon	http://www.amazon.com/	0		1
Weather Channel	http://www.weather.com/	0		1
BBC	http://www.bbc.co.uk/	0		1
http://twitter.com/signup	http://twitter.com/signup	2	2011-05-04 21:41:44	0
http://mobile.twitter.com/signup	http://mobile.twitter.com/signup	2	2011-05-04 21:41:51	0
Twitter	https://mobile.twitter.com/signup	4	2011-05-04 21:42:45	0
Twitter	https://mobile.twitter.com/	2	2011-05-04 21:43:41	0
http://twitter.com/account/confirm_email/yob_taog/32FA5-3644H-130455?utm_campaign=twitter20080313004044&utm_medium=email&utm_source=validate_email	http://twitter.com/account/confirm_email/yob_taog/32FA5-3644H-130455?utm_campaign=twitter20080313004044&utm_medium=email&utm_source=validate_email	1	2011-05-04 21:44:19	0
http://twitter.com/login?redirect_after_login=%2Faccount%2Fconfirm_email%2Fyob_taog%2F32FA5-3644H-130455%3Futm_campaign%3Dtwitter20080313004044%26utm_medium%3Demail%26utm_source%3Dvalidate_email	http://twitter.com/login?redirect_after_login=%2Faccount%2Fconfirm_email%2Fyob_taog%2F32FA5-3644H-130455%3Futm_campaign%3Dtwitter20080313004044%26utm_medium%3Demail%26utm_source%3Dvalidate_email	1	2011-05-04 21:44:19	0
https://market.android.com/details?id=com.netqin.mobileguard	https://market.android.com/details?id=com.netqin.mobileguard	1	2011-05-04 21:46:51	0
weather 15213	weather 15213	0	2011-05-04 21:49:07	0
http://www.google.com/m?hl=en&gl=us&source=android-browser-key&q=weather+15213	http://www.google.com/m?hl=en&gl=us&source=android-browser-key&q=weather+15213	1	2011-05-04 21:49:08	0
Hour by Hour Weather Forecast for Pittsburgh, PA (15213) - weather.com	http://www.weather.com/weather/hourbyhour/15213	1	2011-05-04 21:49:25	0
http://touch.facebook.com/auth.php?api_key=882a8490361da98702bf97a021ddc14d&session_key=181a19d3869050bcccf27931.0-100002336995096&sig=7427018703eca22097940ffef08c2551&t=1304561816&uid=100002336995096&url=http%3A%2F%2Fm.facebook.com%2Fprofile.php%3Fid%3D100002336995096	http://touch.facebook.com/auth.php?api_key=882a8490361da98702bf97a021ddc14d&session_key=181a19d3869050bcccf27931.0-100002336995096&sig=7427018703eca22097940ffef08c2551&t=1304561816&uid=100002336995096&url=http%3A%2F%2Fm.facebook.com%2Fprofile.php%3Fid%3D100002336995096	1	2011-05-04 22:17:03	0
Taog Yob	http://m.facebook.com/profile.php?id=100002336995096	1	2011-05-04 22:17:03	0
Quickoffice for Android	https://www.quickoffice.com/android_resources/quickoffice_help.php?app=qoandroid_2.0.236_GEP&imei=A000002202F45D&model=Droid&sid=08a14c33df4ae5fc09166b6bb99ad472&locale=en_US&imsi=&os=ESD56	1	2011-05-07 12:52:08	0
Quickoffice for Android Frequently Asked Questions	http://www.quickoffice.com/android_resources/knowledgebase.php?app=qoandroid_2.0.236_GEP&return=about	1	2011-05-07 12:52:18	0
Help | Vaulty	http://vaulty.theronrogers.com/help/	1	2011-05-07 14:32:42	0

http://www.sunflat.net/android/cmd/postSc?gid=2006&v=1.1.2&lid=1&htid=e82782b535707c4c51d14d45e6b26b89&arid=9c386f2957af73bbdda52984bef93172&dt=1304814379&sc=270&ha=4129099537&tt=1&tn=Os6+Droid+Vi20996&fv=7	http://www.sunflat.net/android/cmd/postSc?gid=2006&v=1.1.2&lid=1&htid=e82782b535707c4c51d14d45e6b26b89&arid=9c386f2957af73bbdda52984bef93172&dt=1304814379&sc=270&ha=4129099537&tt=1&tn=Os6+Droid+Vi20996&fv=7	1	2011-05-07 20:26:35	0
Sunflat GAMES for Android	http://www.sunflat.net/android/ranking/submitScore?gid=2006&lid=1&dmy=3	1	2011-05-07 20:26:35	0
http://www.google.com/m?source=android-home	http://www.google.com/m?source=android-home	1	2011-05-07 20:39:15	0
http://www.google.com/m/search?q=fatheads&pbx=1&aq=f&oq=&aqi=n1g4-k0d0t0&fkt=6523&fsdt=17949&cqt=&rst=&htf=&his=&maction=&source=android-home&csll=&action=&ltoken=4a385b62432e2	http://www.google.com/m/search?q=fatheads&pbx=1&aq=f&oq=&aqi=n1g4-k0d0t0&fkt=6523&fsdt=17949&cqt=&rst=&htf=&his=&maction=&source=android-home&csll=&action=&ltoken=4a385b62432e2	1	2011-05-07 20:39:36	0
http://www.google.com/m/url?ei=OebFTcjDNZ7qMJnBoVI&q=http://www.fatheads.com/&source=android-home&ved=0CCkQFjAE&usg=AFQjCNGU-NxUDHL7FPShQYEKkVYEsUVULQ	http://www.google.com/m/url?ei=OebFTcjDNZ7qMJnBoVI&q=http://www.fatheads.com/&source=android-home&ved=0CCkQFjAE&usg=AFQjCNGU-NxUDHL7FPShQYEKkVYEsUVULQ	1	2011-05-07 20:40:16	0
Fat Head's Saloon, Pittsburgh PA	http://www.fatheads.com/	1	2011-05-07 20:40:16	0
http://www.adobe.com/go/getflashplayer	http://www.adobe.com/go/getflashplayer	1	2011-05-07 20:40:36	0
Adobe - Flash Player 10: Unsupported device	http://www.adobe.com/misc/unsupported_device.html	1	2011-05-07 20:40:36	0
http://www.google.com/search?source=android-home&q=cache:ibHV0eKmqxUJ:www.fatheads.com/	http://www.google.com/search?source=android-home&q=cache:ibHV0eKmqxUJ:www.fatheads.com/	1	2011-05-07 20:41:26	0
Fat Head's Saloon, Pittsburgh PA	http://webcache.googleusercontent.com/search?source=android-home&q=cache:ibHV0eKmqxUJ:www.fatheads.com/	1	2011-05-07 20:41:26	0
http://www.google.com/gwt/x?q=fatheads&ei=OebFTcjDNZ7qMJnBoVI&hl=en&source=m&u=http://www.fatheads.com/	http://www.google.com/gwt/x?q=fatheads&ei=OebFTcjDNZ7qMJnBoVI&hl=en&source=m&u=http://www.fatheads.com/	1	2011-05-07 20:41:41	0
http://www.google.com/gwt/x?source=m&u=http%3A%2F%2Fwww.adobe.com/go/getflashplayer&wsi=9843fd6289bb8e6b&ei=tubFTeb2F5LGwAWF9P2BAg&wsc=yq	http://www.google.com/gwt/x?source=m&u=http%3A%2F%2Fwww.adobe.com/go/getflashplayer&wsi=9843fd6289bb8e6b&ei=tubFTeb2F5LGwAWF9P2BAg&wsc=yq	1	2011-05-07 20:41:55	0
http://touch.facebook.com/auth.php?api_key=882a8490361da98702bf97a021ddc14d&session_key=181a19d386905 0bcccf27931.0-100002336995096&sig=4d51463d3946690506939fd8db13a86c&t=1304894285&uid=100002336995096&url=http%3A%2F%2Fm.facebook.com%2Fsharer.php%3Fu%3DI%2Bscored%2B7612%2Bin%2BDonkey%2BJump%2Bon%2Bmy%2BDroid%252C%2Bhttps%253A%252F%252Fmarket.android.com%252Fdetails%253Fid%253Dcom.droidhen.game.donkeyjump%2526feature%253Dsearch_result	http://touch.facebook.com/auth.php?api_key=882a8490361da98702bf97a021ddc14d&session_key=181a19d3869050bcccf27931.0-100002336995096&sig=4d51463d3946690506939fd8db13a86c&t=1304894285&uid=100002336995096&url=http%3A%2F%2Fm.facebook.com%2Fsharer.php%3Fu%3DI%2Bscored%2B7612%2Bin%2BDonkey%2BJump%2Bon%2Bmy%2BDroid%252C%2Bhttps%253A%252F%252Fmarket.android.com%252Fdetails%253Fid%253Dcom.droidhen.game.donkeyjump%2526feature%253Dsearch_result	1	2011-05-08 18:38:07	0
Share	http://m.facebook.com/sharer.php?u=I+scored+7612+in+Donkey+Jump+on+my+Droid%2C+https%3A%2F%2Fmarket.android.com%2Fdetails%3Fid%3Dcom.droidhen.game.donkeyjump%26feature%3Dsearch_result&_rdr	1	2011-05-08 18:38:08	0
Places	http://m.facebook.com/places/disclosure.php?refid=17	1	2011-05-08 18:39:21	0
http://touch.facebook.com/auth.php?api_key=882a8490361da98702bf97a021ddc14d&session_key=181a19d386905 0bcccf27931.0-100002336995096&sig=340123fafa71f243f1399fda4221947f&t=1304894490&uid=100002336995096&url=http%3A%2F%2Fm.facebook.com%2Fsharer.php%3Fu%3DI%2Bscored%2B10309%2Bin%2BDonkey%2BJump%2Bon%2Bmy%2BDroid%252C%2Bhttps%253A%252F%252Fmarket.android.com%252Fdetails%253Fid%253Dcom.droidhen.game.donkeyjump%2526feature%253Dsea	http://touch.facebook.com/auth.php?api_key=882a8490361da98702bf97a021ddc14d&session_key=181a19d3869050bcccf27931.0-100002336995096&sig=340123fafa71f243f1399fda4221947f&t=1304894490&uid=100002336995096&url=http%3A%2F%2Fm.facebook.com%2Fsharer.php%3Fu%3DI%2Bscored%2B10309%2Bin%2BDonkey%2BJump%2Bon%2Bmy%2BDroid%252C%2Bhttps%253A%252F%252Fmarket.android.com%252Fdetails%253Fid%253Dcom.droidhen.game.donkeyjump%2526feature%253Dsearch_result	1	2011-05-08 18:41:33	0

rch_result				
Share	http://m.facebook.com/sharer.php?u=I+scored+10309+in+Donkey+Jump+on+my+Droid%2C+https%3A%2F%2Fmarket.android.com%2Fdetails%3Fid%3Dcom.droidhen.game.donkeyjump%26feature%3Dsearch_result&_rdr	1	2011-05-08 18:41:33	0
http://touch.facebook.com/auth.php?api_key=882a8490361da98702bf97a021ddc14d&session_key=181a19d3869050bcccf27931.0-100002336995096&sig=a29078fd1132410ed1847b62972fbd66&t=1305059263&uid=100002336995096&url=http%3A%2F%2Fm.facebook.com%2Fprofile.php%3Fid%3D1020870144	http://touch.facebook.com/auth.php?api_key=882a8490361da98702bf97a021ddc14d&session_key=181a19d3869050bcccf27931.0-100002336995096&sig=a29078fd1132410ed1847b62972fbd66&t=1305059263&uid=100002336995096&url=http%3A%2F%2Fm.facebook.com%2Fprofile.php%3Fid%3D1020870144	1	2011-05-10 16:27:51	0
Katharina Lau	http://m.facebook.com/profile.php?id=1020870144&_rdr	1	2011-05-10 16:27:52	0
Facebook	http://m.facebook.com/home.php?refid=17	1	2011-05-10 16:28:31	0

3.3.11. Scenario 2 – Google Map

The keyword looked up in Google Map is stored in the file 'search_history.db (suggestions table)' which is in the '/data/data/com.google.android.apps.maps/databases' directory.

The search results are stored in the file 'da_destination_history(destination_history table)' in the same directory. The details of using Google Map for a lookup are as follows.

Table 32. Contents of 'com.google.android.apps.maps/databases/search_history.db (suggestions table)'

keyword
pirates

Table 33. Contents of 'com.google.android.apps.maps/databases/da_destination_history(destination_history table)'

Time (UTC-4)	DstTitle	SrcLat	SrcLng	DstLat	DstLng	DstAddr
2011-05-10 20:38:39	Pittsburgh Pirates	40438244	-80006203	40446882	-80005574	115 Federal Street Pittsburgh, PA 15212-5740

The starting location and the destination, which were found by looking at the two files, were checked in Google Map, as shown below.

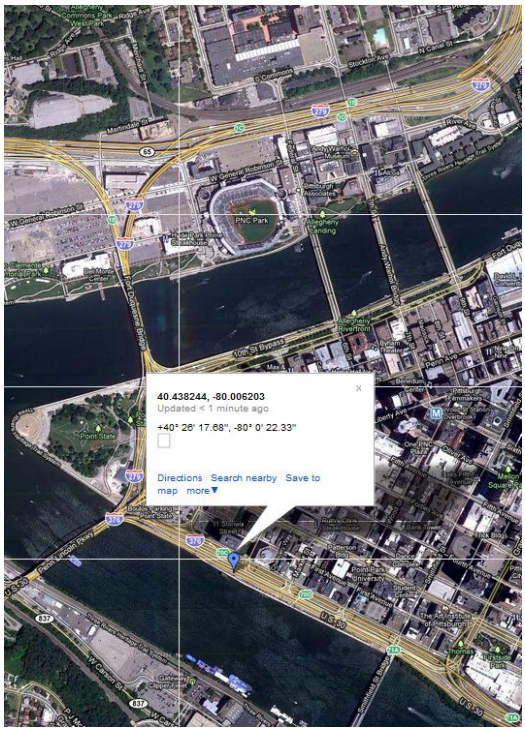


Figure 28. Google Map Search Result: Source

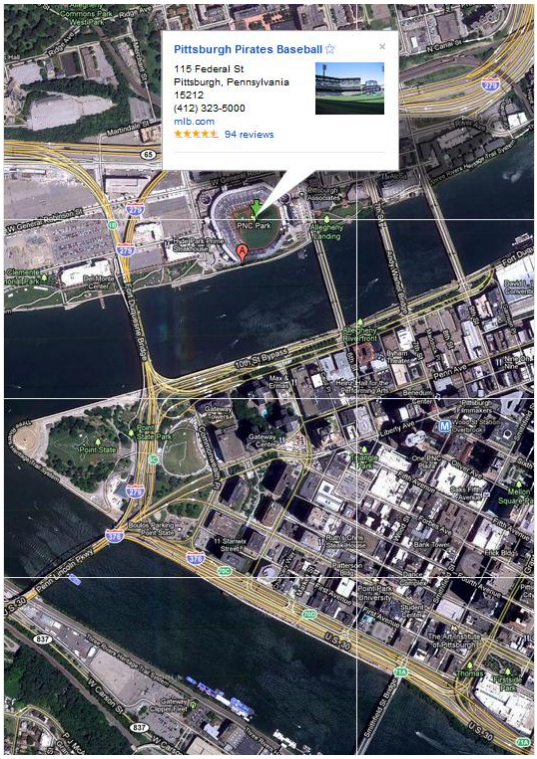


Figure 29. Google Map Search Result: Destination

It can be seen that the user checked his location on a road on the way to Pittsburg Pirates Baseball.

3.3.12. Scenario 2 – Call history

It gets stored in the file 'contacts2.db (calls table)' in the '/data/data/com.android.providers.contacts/databases' directory.

Table 34. Contents of 'com.android.providers.contacts/databases/contacts2.db (calls table)'

PhoneNum	Time (UTC-4)	Duration	Type	Name
5854561283	2011-05-06 12:51:31	20	Incoming	
7607058888	2011-05-06 13:04:08	110	Incoming	adrian
7607058888	2011-05-06 13:17:53	127	Incoming	adrian
7607058888	2011-05-06 15:25:22	0	Outcoming	adrian

3.3.13. Scenario 2 – Contacts

It gets stored in the file 'contacts2.db (calls table)' in the '/data/data/com.android.providers.contacts/databases' directory.

Table 35. Contents of 'com.android.providers.contacts/databases/contacts2.db (data table)'

Name	Email	facebook	PhoneNum	PhoneNum2
Reg Wetham	regwetham@yahoo.com	100002352866842	-	-
Shandra Pfeif	shandra@cheerful.com	-	-	-
Luke Lancer	luk3lancer@gmail.com	-	-	-
Hersolv Einskavich	hersolv@gmail.com	-	-	-
adrian		-	7607058888	8888507067
Swift Logic	swiftlogic@consultant.com	-	-	-
-	swiftlogicllc@consultant.com	-	-	-
-	swiftlogicinc@consultant.com	-	-	-

3.3.14. Scenario 2 – SMS/MMS

Information of users that exchanged SMS/MMS is stored in the file 'mmssms.db(canonical_address table)' in the directory '/data/data/com.android.providers.contacts/databases'. The SMS/MMS details are stored in the 'sms' table in the same file. The SMS/MMS details are as shown below.

Table 36. Contents of 'com.android.providers.contacts/databases/ mmssms.db (canonical_address table)'

Name
shandra@cheerful.com
sms.dynadel@gmail.com
4124393388

Table 37. Contents of 'com.android.providers.contacts/databases/ mmssms.db (sms table)'

Time (UTC-4)	Type	Name	Content
2011-05-05 21:34:55	Incoming	shandra@cheerful.com	(Nearby! Coming for my beer) Hey Yob, I am closing in on Fat Heads. See ya soon.
2011-05-06 13:53:30	Incoming	sms.dynadel@gmail.com	Reminder, planned IT outage this weekend. This maintenance window will start at 3 PM today and continue for approx 48 hours.
2011-05-06 13:55:16	Incoming	sms.dynadel@gmail.com	This effects external services such as website, email, webmail, and the ftp server. Use the secondary email access and helpdesk # for emergencies
2011-05-07 19:39:16	Incoming	shandra@cheerful.com	(Save me!) If Luke asks, I'm going out with you to dinner, OK? I just can't face Mr. Smooth tonight. Shandra
2011-05-07 19:44:27	Outgoing	6245	Sure thing. Do you know where the wine loft is?
2011-05-07 19:54:37	Outgoing	6245	I ran into some friends at the double wide, meetup at 8:30 or so?
2011-05-07 19:56:53	Outgoing	6245	Or you can walk down Carson and join us
2011-05-07 23:10:01	Incoming	shandra@cheerful.com	(Re: Or you can walk down) Walking down now. Hope you are still vertical. ----- Original Message ----- From: 4124393388@VTEXT.COM Sent: 05/07/11 07:56 PM To:
2011-05-07 23:10:03	Incoming	shandra@cheerful.com	(Re: Or you can walk down) Walking down now. Hope you are still vertical. ----- Original Message ----- From: 4124393388@VTEXT.COM Sent: 05/07/11 07:56 PM To:
2011-05-07 23:10:27	Incoming	shandra@cheerful.com	(Re: Or you can walk down) Walking down now. Hope you are still vertical. ----- Original Message ----- From: 4124393388@VTEXT.COM Sent: 05/07/11 07:56 PM To:
2011-05-07 23:10:31	Incoming	shandra@cheerful.com	(Re: Or you can walk down) Hope you guys are still at double-wide ... ----- Original Message ----- From: 4124393388@VTEXT.COM Sent: 05/07/11 07:56 PM To: shan
2011-05-08 17:41:45	Incoming	shandra@cheerful.com	(Thanks) Thanks for being so gracious last night Shandra
2011-05-10 07:26:46	Incoming	shandra@cheerful.com	(You around for lunch) Hey -- a few of us are going to that great Indian buffet for lunch today. You interested?
2011-05-10 09:31:44	Outgoing	6245	Sorry, still an Atlanta till tonight. Raincheck?
2011-05-10 12:35:18	Incoming	shandra@cheerful.com	(Re: Sorry, still an Atlanta till) OK. Safe travels! ----- Original Message ----- From: 4124393388@VTEXT.COM Sent: 05/10/11 09:31 AM To: shandra@cheerful.com
2011-05-10 16:43:03	Incoming	4124393388	You have insufficient funds to send message.
2011-05-10 16:43:40	Incoming	4124393388	You have insufficient funds to send message.

3.3.15. Scenario 2 – GoogleTalk

Information of users that used GoogleTalk to communicate with each other is stored in the file 'talk.db(contacts table) in the directory 'com.google.android.providers.talk/databases'. The details of their conversation are stored in the 'messages' table in the same file. GoogleTalk details are as shown below.

Table 38. Contents of 'com.google.android.providers.talk/databases/talk.db (contacts table)'

ID	Name	NickName
1	2h3chk7j4rhwe@id.talk.google.com	Reg Wetham
3	luk3lancer@gmail.com	Luke Lancer
4	hersolv@gmail.com	Hersolv Einskavich

Table 39. Contents of 'com.google.android.providers.talk/databases/talk.db(message table)'

Time (UTC-4)	Type	To	From	Content
2011-05-05 11:55:18	Incoming	Yob Taog	Reg Wetham	Hope presentation goes well!
2011-05-05 11:55:38	Incoming	Yob Taog	Reg Wetham	Will try not to bug you today B-)
2011-05-05 11:56:52	Outgoing	Reg Wetham	Yob Taog	Oh, I don't think its a big deal
2011-05-05 11:57:19	Incoming	Yob Taog	Reg Wetham	Cool as a cucumber.
2011-05-05 11:57:24	Incoming	Yob Taog	Reg Wetham	Impressive !
2011-05-05 11:57:28	Outgoing	Reg Wetham	Yob Taog	Mostly in the bag, its just a lot of money so they want me to go
2011-05-05 11:58:00	Outgoing	Reg Wetham	Yob Taog	It will be good for the company
2011-05-05 11:58:21	Incoming	Yob Taog	Reg Wetham	Oh. Just money. Is that all ...
2011-05-05 11:58:29	Incoming	Yob Taog	Reg Wetham	sheesh :)
2011-05-05 11:58:43	Outgoing	Reg Wetham	Yob Taog	I mean we're ok, but more dough would be nice!
2011-05-05 11:58:52	Incoming	Yob Taog	Reg Wetham	yeah. and for your career, I bet
2011-05-05 11:59:22	Incoming	Yob Taog	Reg Wetham	You on your new Droid, BTW?
2011-05-05 11:59:38	Outgoing	Reg Wetham	Yob Taog	I wonder if I should have gotten a samsung, this keyboard is kind of small for my fimgers....
2011-05-05 11:59:57	Outgoing	Reg Wetham	Yob Taog	Lol, so "yes". ;-)
2011-05-05 12:00:13	Incoming	Yob Taog	Reg Wetham	HAH! :'(
2011-05-05 12:00:24	Outgoing	Reg Wetham	Yob Taog	Love the status btw
2011-05-05 12:00:40	Incoming	Yob Taog	Reg Wetham	Truly ! I am !
2011-05-05 12:01:00	Incoming	Yob Taog	Reg Wetham	Thanks.
2011-05-05 12:01:57	Incoming	Yob Taog	Reg Wetham	Well, I gotta go see a man about a horse now
2011-05-05 12:02:07	Incoming	Yob Taog	Reg Wetham	And, I just don't IM from there, so ....
2011-05-05 12:02:28	Incoming	Yob Taog	Reg Wetham	cya :-o
2011-05-05 12:02:28	Outgoing	Reg Wetham	Yob Taog	Catch you later

2011-05-05 12:02:41	Outgoing	Reg Wetham	Yob Taog	Catch you later
2011-05-06 12:18:54	Incoming	Yob Taog	Luke Lancer	:D
2011-05-06 12:25:56	Outgoing	Luke Lancer	Yob Taog	Hey Luke, sorry I haven't replied to your email, been really busy..
2011-05-06 12:34:06	Incoming	Yob Taog	Luke Lancer	s'ok. headed out to lunch now myself
2011-05-06 12:34:08	Incoming	Yob Taog	Luke Lancer	sheepish ....
2011-05-06 12:38:33	Outgoing	Luke Lancer	Yob Taog	We're getting Greek if you want to join
2011-05-06 13:09:32	Outgoing	Hersolv Einskavich	Yob Taog	Hey, may make enough time to watch the prix, where are you watching it?
2011-05-06 13:10:11	Incoming	Yob Taog	Hersolv Einskavich	probably my place, unless you are offering your man cave
2011-05-06 13:10:42	Outgoing	Hersolv Einskavich	Yob Taog	Heh, probably a bad idea, I'm swamped with work
2011-05-06 13:10:59	Incoming	Yob Taog	Hersolv Einskavich	you work too much
2011-05-06 13:11:19	Incoming	Yob Taog	Hersolv Einskavich	then again, that outlook is probably why i'm still just an engineer
2011-05-06 13:11:19	Incoming	Yob Taog	Hersolv Einskavich	:)
2011-05-06 13:11:37	Outgoing	Hersolv Einskavich	Yob Taog	Yeah, probably
2011-05-06 13:11:41	Outgoing	Hersolv Einskavich	Yob Taog	:)
2011-05-06 13:55:06	Incoming	Yob Taog	Luke Lancer	snap. just ate greek yesterday
2011-05-06 15:24:32	Incoming	Yob Taog	Hersolv Einskavich	i think it's swiftlogic@consultant.com
2011-05-06 15:24:37	Incoming	Yob Taog	Hersolv Einskavich	or maybe swiftlogicllc
2011-05-06 15:27:13	Outgoing	Hersolv Einskavich	Yob Taog	Cool, thx
2011-05-06 15:27:23	Incoming	Yob Taog	Hersolv Einskavich	no problem
2011-05-06 15:27:26	Incoming	Yob Taog	Hersolv Einskavich	good luck
2011-05-06 15:36:47	Outgoing	Hersolv Einskavich	Yob Taog	Judging from the bounces, its just swiftlogic
2011-05-06 15:37:12	Outgoing	Hersolv Einskavich	Yob Taog	Thx, I hope the check that email
2011-05-06 15:37:40	Incoming	Yob Taog	Hersolv Einskavich	yeah, i'm not sure on that one. i've never used that resource.
2011-05-06 15:37:55	Incoming	Yob Taog	Hersolv Einskavich	i pulled all the data i need to my laptop
2011-05-06 15:38:10	Incoming	Yob Taog	Hersolv Einskavich	plus, i typically don't work over the weekend
2011-05-06 15:38:41	Outgoing	Hersolv Einskavich	Yob Taog	Maybe I should try that sometime :-)
2011-05-06 18:18:21	Incoming	Yob Taog	Luke Lancer	OK. I'm going to practice my Aussie now
2011-05-06 18:18:36	Incoming	Yob Taog	Luke Lancer	ciao
2011-05-07 14:07:08	Incoming	Yob Taog	Luke Lancer	Torrid night, dude.
2011-05-07 14:07:34	Incoming	Yob Taog	Luke Lancer	All the details I remember are in the email I just sent you
2011-05-07 14:08:10	Incoming	Yob Taog	Luke Lancer	Just type quietly. K? :(
2011-05-08 18:36:06	Outgoing	Luke Lancer	Yob Taog	Did you recover OK?
2011-05-09 21:21:56	Incoming	Yob Taog	Luke Lancer	Wow. I forgot you were in Atlanta
2011-05-09 21:22:20	Incoming	Yob Taog	Luke Lancer	You know it got up to 70 today in Pittsburgh. That's pretty hot.
2011-05-09 21:24:02	Incoming	Yob Taog	Luke Lancer	How hot is Atlanta?
2011-05-09 21:24:28	Incoming	Yob Taog	Luke Lancer	Any cute girls?

2011-05-09 21:35:37	Outgoing	Luke Lancer	Yob Taog	All work and no play
2011-05-09 21:36:40	Incoming	Yob Taog	Luke Lancer	shoot
2011-05-09 21:37:06	Incoming	Yob Taog	Luke Lancer	well, I hope the work is going well at least
2011-05-09 21:40:51	Outgoing	Luke Lancer	Yob Taog	Yeah, went well today, they really liked the designs
2011-05-09 21:41:23	Outgoing	Luke Lancer	Yob Taog	And they are out drinking me right now, so that's gotta be good
2011-05-09 21:44:42	Incoming	Yob Taog	Luke Lancer	Out drinking you! Impossible
2011-05-09 21:45:02	Incoming	Yob Taog	Luke Lancer	Unless its that Aarney dude.
2011-05-09 21:45:27	Incoming	Yob Taog	Luke Lancer	I heard he can drink! :-o
2011-05-09 21:46:03	Incoming	Yob Taog	Luke Lancer	Something about the Dutch. About living with the ever-present risk of drowning in your own house
2011-05-09 22:11:19	Incoming	Yob Taog	Luke Lancer	got to go now
2011-05-09 22:11:29	Incoming	Yob Taog	Luke Lancer	the last two nights have taken a toll on my stamina
2011-05-09 22:11:39	Incoming	Yob Taog	Luke Lancer	:P

3.3.16. Scenario 2 – Device Information

It gets stored in the file 'checkin.db (crashes table)' in the '/data/data/com.google.android.server.checkin /databases' directory.

```
============================================================
== build.prop
============================================================
------ VERSION INFO ------
currenttime=Tue May 10 16-44-20 2011
kernel.version=Linux version 2.6.29-omap1-g0dd7e0b (android-build@apa26.mtv.corp.google.com) (gcc version 4.4.0 (GCC) ) #511 PREEMPT Wed Nov 25
15:22:28 PST 2009
kernel.cmdline=console=ttyS2,115200n8 console=ttyMTD7 rw mem=244M@0x80C00000 init=/init ip=off brdrev=P3A_CDMA
mtdparts=omap2-nand.0:1536k@1792k(pds),384k@6272k(misc),3584k(boot)ro,4608k(recovery),143744k(system),94848k(cache),268032k(userdata),2m(kpanic)
androidboot.mode=charge androidboot.bootloader=2C6C0 androidboot.serialno=040373B60300901B
# begin build properties
# autogenerated by buildinfo.sh
ro.build.id=ESD56
ro.build.display.id=ESD56
ro.build.version.incremental=20996
ro.build.version.sdk=6
ro.build.version.codename=REL
ro.build.version.release=2.0.1
ro.build.date=Wed Nov 25 17:42:57 PST 2009
ro.build.date.utc=1259199777
ro.build.type=user
ro.build.user=android-build
ro.build.host=android-test-10.mtv.corp.google.com
ro.build.tags=test-keys
ro.product.model=Droid
ro.product.brand=verizon
ro.product.name=voles
ro.product.device=sholes
ro.product.board=sholes
ro.product.cpu.abi=armeabi
ro.product.manufacturer=Motorola
ro.product.locale.language=en
ro.product.locale.region=US
ro.wifi.channels=
ro.board.platform=omap3
# ro.build.product is obsolete; use ro.product.device
ro.build.product=sholes
# Do not try to parse ro.build.description or .fingerprint
ro.build.description=voles-user 2.0.1 ESD56 20996 release-keys
ro.build.fingerprint=verizon/voles/sholes/sholes:2.0.1/ESD56/20996:user/release-keys
# end build properties
```

```
#
# system.prop for generic sdk
#

rild.libpath=/system/lib/libmoto_ril.so
rild.libargs=-d /dev/ttyS0
ro.sf.lcd_density=240

# Default network type.
# 4 => CDMA / EVDO.
ro.telephony.default_network=4

wifi.interface = tiwlan0
# Time between scans in seconds. Keep it high to minimize battery drain.
# This only affects the case in which there are remembered access points,
# but none are in range.
wifi.supplicant_scan_interval = 15

# Indicate carrier OTA SP number schema
# refer to frameworks/base/telephony/java/com/android/
# internal/telephony/cdma/CDMAPhone.java for the schema:
ro.cdma.otaspnumschema=SELC,1,80,99

# The OpenGL ES API level that is natively supported by this device.
# This is a 16.16 fixed point number
ro.opengles.version = 131072

# This is a high density device with more memory, so larger vm heaps for it.
dalvik.vm.heapsize=24m

#
# ADDITIONAL_BUILD_PROPERTIES
#
ro.config.notification_sound=droid.ogg
ro.config.ringtone=DroidInvasion.ogg
ro.config.notification_sound=OnTheHunt.ogg
ro.config.alarm_alert=Alarm_Classic.ogg
ro.com.android.wifi-watchlist=GoogleGuest
ro.error.receiver.system.apps=com.google.android.feedback
ro.setupwizard.enterprise_mode=1
ro.com.google.clientidbase=android-verizon
ro.com.google.locationfeatures=1
ro.url.legal=http://www.google.com/intl/%s/mobile/android/basic/phone-legal.html
ro.url.legal.android_privacy=http://www.google.com/intl/%s/mobile/android/basic/privacy.html
ro.config.ringtone=CaribbeanIce.ogg
ro.setupwizard.mode=OPTIONAL
ro.cdma.home.operator.numeric=310004
ro.cdma.home.operator.alpha=Verizon
ro.cdma.homesystem=64,65,76,77,78,79,80,81,82,83
ro.cdma.data_retry_config=default_randomization=2000,0,0,120000,180000,540000,960000
ro.config.vc_call_vol_steps=7
ro.cdma.otaspnumschema=SELC,1,80,99
ro.telephony.call_ring.multiple=false
ro.telephony.call_ring.delay=3000
ro.url.safetylegal=http://www.motorola.com/staticfiles/Support/legal/?model=A855
ro.setupwizard.enable_bypass=1
ro.media.enc.hprof.file.format=mp4
ro.media.enc.hprof.codec.vid=h264
ro.media.enc.hprof.codec.aud=aac
ro.media.enc.hprof.vid.width=720
ro.media.enc.hprof.vid.height=480
ro.media.enc.hprof.vid.fps=25
ro.media.enc.hprof.vid.bps=3000000
ro.media.enc.hprof.aud.bps=96000
ro.media.enc.hprof.aud.hz=16000
ro.media.enc.hprof.aud.ch=1
ro.media.enc.hprof.duration=60
ro.media.enc.lprof.file.format=mp4
ro.media.enc.lprof.codec.vid=m4v
ro.media.enc.lprof.codec.aud=amrnb
ro.media.enc.lprof.vid.width=320
ro.media.enc.lprof.vid.height=240
ro.media.enc.lprof.vid.fps=15
ro.media.enc.lprof.vid.bps=200000
ro.media.enc.lprof.aud.bps=12200
ro.media.enc.lprof.aud.hz=8000
ro.media.enc.lprof.aud.ch=1
ro.media.enc.lprof.duration=30
```

ro.media.enc.file.format=3gp,mp4
ro.media.enc.vid.codec=h264,m4v,h263
ro.media.enc.aud.codec=aac,amrnb
ro.media.enc.vid.h264.width=176,720
ro.media.enc.vid.h264.height=144,480
ro.media.enc.vid.h264.bps=64000,8000000
ro.media.enc.vid.h264.fps=1,30
ro.media.enc.vid.h263.width=176,720
ro.media.enc.vid.h263.height=144,480
ro.media.enc.vid.h263.bps=64000,8000000
ro.media.enc.vid.h263.fps=1,30
ro.media.enc.vid.m4v.width=176,7
gsm.version.ril-impl=SHOLES_C_CDMA_RIL_01.2D.00R_091013RILH
gsm.version.baseband=C_01.3E.01P
gsm.imei=
gsm.sim.operator.numeric=310004
gsm.operator.alpha=Verizon Wireless
------ END ------

3.3.17. Scenario 2 – Twitter

It gets stored in the file 'twitter.db (tweets table)' in the '/data/data/com.seesmic/databases' directory.

Table 40. Contents of 'com.seesmic/databases/twitter.db (tweets table)'

Tweet time (UTC-4)	Sender ID	Message	Source
2011-04-14 15:04:00	handmark	#TweetCaster for Android goes PINK for breast cancer awareness! http://bit.ly/ftF2EW #feelyourboobies @FYBgirl	web
2011-04-14 16:12:40	handmark	Proudly display your support for boobies with Tweetcaster Pink for Twitter http://goo.gl/fb/K2PTO	TweetCaster
2011-04-15 14:13:30	handmark	#TweetCaster for Android goes PINK for breast cancer awareness! http://bit.ly/ftF2EW #feelyourboobies @FYBgirl	web
2011-04-15 20:11:03	asktwidroyd	New Twidroyd release slated to come out early next week!	Echofon
2011-04-15 21:53:10	handmark	RT @FYBGirl: What do Twitter and boobies have in common? http://bit.ly/ftF2EW #TweetCaster #feelyourboobies	TweetCaster
2011-04-16 17:41:12	seesmic	Join us 4/20: @lizasperling will show how to simplify customer support with Seesmic & our Zendesk plugin. RSVP http://bit.ly/ehBLSp #socbiz	Seesmic for Android
2011-04-18 10:31:16	handmark	#TweetCaster goes PINK for breast cancer awareness! http://bit.ly/ftF2EW Show your support and #feelyourboobies	web
2011-04-18 10:40:56	handmark	We ??user reviews: "Not only do you help a great cause but you get #TweetCaster in pink!! 5 stars." http://bit.ly/ftF2EW	web
2011-04-18 11:52:39	handmark	Just released our latest FREE Android app: Today I Learned. Impress your friends with cool facts. http://bit.ly/gLgPKD #TIL	web
2011-04-18 17:17:27	handmark	#TIL that Amazon Prime is free for college students. Discovered via FREE Android app "Today I Learned" http://bit.ly/gLgPKD	web
2011-04-18 22:45:38	handmark	RT @onlygizmos: FriendCaster: The Best FaceBook App For iPad? Free! http://goo.gl/fb/HAthh	TweetCaster
2011-04-19 13:22:37	seesmic	Webinar With Zendesk: Loving Your Help Desk (& Customer Service) Just Got Easier http://ping.fm/fAJ0j	Ping.fm
2011-04-19 17:50:50	handmark	Thanks to all of you, #TweetCaster now #3 FREE social app in Android Market. Spread the word! http://bit.ly/i4F9Io	web
2011-04-20 10:33:04	seesmic	Seesmic For Windows Phone 7 Just Got Better http://ping.fm/Ha1g2	Ping.fm
2011-04-20 11:12:43	seesmic	Seesmic For Android 1.7: Go Faster With Shortcuts & More http://ping.fm/Uvz0L	Ping.fm
2011-04-20 11:52:43	seesmic	Filter the Noise and Generate Leads with the InboxQ Plugin for Seesmic http://ping.fm/mTUzP	Ping.fm
2011-04-20 14:47:34	seesmic	are you in Indonesia? We're looking for users there of Seesmic Android tell us how the version we just pushed looks like localized. Thanks.	Seesmic for Android
2011-04-21 03:32:39	seesmic	Results for Seesmic for Android 1.7: ショートカット機能でさらに便利に使いやすく！ http://ping.fm/Lg3i5	Ping.fm
2011-04-21 14:39:11	seesmic	EC2 knocked out a lot of apps, but @seesmic is thankfully untouched. Cmon in, the water is nice!	Seesmic for Android
2011-04-21 17:46:27	seesmic	Need your help! @kevinmarks is stopping by @seesmic today for Tummelvision & a quick interview. What would you ask him?	Seesmic for Android
2011-04-25 19:58:02	handmark	RT @FYBGirl: What do Twitter and boobies have in common? http://bit.ly/ftF2EW #TweetCaster #feelyourboobies	TweetCaster

2011-04-26 12:29:46	handmark	Thanks @TheTechHog for reviewing our Today I Learned (TIL) app! http://bit.ly/hSXPio	web
2011-04-26 14:13:13	twidroyd	twidroyd, 3.1.5 released yesterday - brings some important fixes. please RT http://twidroyd.com/release-notes/	web
2011-04-27 12:54:02	seesmic	We'll take it! RT @oneforty: 10 Great Community Manager Tools http://see.sc/Bf2f76 #SMM	Seesmic Web
2011-04-27 17:13:26	seesmic	At #Appnation? Ask us for a demo of @klout @usatoday plugins-70+ plugins on desktop & counting... cc @aznsnuffy @mashery @AndrewDumont	Seesmic Web
2011-04-27 17:21:46	handmark	BREAKING: TweetCaster for iPhone v1.3 now available. By popular demand, now includes notifications! http://bit.ly/h1J2bm	web
2011-04-27 17:27:54	handmark	Major Android release within days! RT @nljelmer: @handmark Nice for Iphone users. But when update for Android? ;-)	web
2011-04-27 17:38:02	handmark	With v1.3 TweetCaster for iPhone has Peekaboo Links! In Tweet Details, links pop up for easy pull-to-view http://bit.ly/h1J2bm	web
2011-04-27 18:15:18	handmark	YES! RT @mzluxurious83: @handmark Will there be a version for blackberry coming soon?	web
2011-04-27 22:22:38	seesmic	AppNation 2011: Pick An App (Or Plugin) http://ping.fm/GPNwu	Ping.fm
2011-04-27 23:46:29	handmark	RT @mashable: No Tweets Allowed at the Royal Wedding - http://on.mash.to/ljFFj5 #rw2011	TweetCaster
2011-04-28 11:42:06	handmark	FriendCaster Facebook app for iPad just got better! Now with notifications, wall, pic upload and more: http://bit.ly/fcs8uf	web
2011-04-28 14:07:46	handmark	Feel free to TweetCast! RT @mashable: Update: Tweets *will* be allowed at Royal Wedding - http://on.mash.to/ljFFj5	TweetCaster
2011-04-28 15:58:59	seesmic	Thanks for stopping by our table @louisgray. Great pics! http://bit.ly/lDcghx http://bit.ly/ij7nzY #appnation #appnationconf	Seesmic Desktop
2011-04-28 18:04:17	handmark	Following the NFL Draft tonight? Follow the same Twitter list we follow! See the NFL Draft 2011 list on the @Handmark profile	web
2011-04-29 15:29:23	handmark	We Android Booster! http://bit.ly/iLtDAD Best app out there to speed up Android performance and use less battery. FREE!	web
2011-04-29 18:32:06	seesmic	Twitter Status - Elevated error rates on Twitter.com http://bit.ly/j9Km4m	Seesmic for Android
2011-04-30 23:56:32	handmark	Twitter status alert RT @twitterapi: Elevated Error Rates - We are once again noticing elevated... http://t.co/VA8HDTy	TweetCaster
2011-05-01 17:19:17	handmark	Concerned about virus on your Android phone? Netqin Antivirus is sweet -- 4.5 stars. And it's FREE! http://bit.ly/kW8rfU	web
2011-05-01 20:52:27	seesmic	25 Essential Apps for Travelers - TIME http://ti.me/lSFLFu (We made the list!)	Seesmic Web
2011-05-02 20:32:38	seesmic	Introducing the Delicious Plugin for Seesmic Desktop http://ping.fm/Qeglw	Ping.fm
2011-05-03 14:54:19	seesmic	What is Seesmic Desktop? Check out @trevordty's 31 second answer: http://see.sc/rbIcdE	Seesmic Web
2011-05-03 17:50:24	seesmic	Social Media Gets Professional: Biz Joins The Party - WSJ w/ @salesforce @dell @nokia @seesmic http://see.sc/C3ssGA	Seesmic Web
2011-05-03 19:59:22	twidroyd	Happy to announce new UberChannel partnerships w/ @THR @casefoundation @twackle @nwf Have a look, thanks!	web
2011-05-04 13:47:34	SarahAnnGreen	Yay! My @OfficialMGP Schumacher tee, cap & keyring have arrived. Just waiting for the teddy bear now! :)	Twitter for iPhone
2011-05-04 14:13:04	twidroyd	Did you know today is #StarWarsDay? To celebrate we've created an UberChannel featuring parody accounts. May the 4th be w/ you!	web
2011-05-04 21:43:25	yob_taog	Yay! Just picked up my new android smartphone! !!!	Mobile Web
2011-05-04 22:04:55	yob_taog	30 levels into bubble blast, smartphones are awesome!	TweetCaster
2011-05-04 22:12:48	yob_taog	OMG 10:15 already! Got to get to work early tommorrow, six after working late! At least Verizon was still open!	TweetCaster
2011-05-05 00:02:08	DroidLanding	The hunt is complete. Congratulations to all the winners. #chargelanding	web
2011-05-05 08:24:57	androidcentral	Bring old unlocked phones to Google IO for the 'Android for Good' program http://bit.ly/mG8BFo #android	dlvr.it
2011-05-05 08:29:17	GetCoHaEngiJobs	Chief Software Systems Engineer (MPD-CF... - #Columbia , MD (http://tinyurl.com/3rfyuxe) Get Computer Hardware Engineering Jobs #ComputerHar	GetAllJobs
2011-05-05 08:45:16	JensonButton	Getting a massage from @MikeyCollier, I think he's purposely trying to hurt me!! Weather looks pretty pants outside here in Turkey!	Mobile Web
2011-05-05 08:48:16	GetCoHaEngiJobs	Junior Software Engineer (C, C++ on Windows, Linu... - #Annapolis , MD (http://tinyurl.com/3ugvgec) Get Computer Hardware Engineering Jobs #	GetAllJobs
2011-05-05 08:54:26	jakehumphreyf1	Made me chuckle... #bbcf1 http://t.co/kLVlFF8	Twitter for iPhone
2011-05-05 09:18:10	androidcentral	Motorola XPRT brings a familiar face to Sprint, along with worldwide coverage http://bit.ly/ijjg7N #android	dlvr.it

2011-05-05 09:23:22	androidcentral	Motorola Titanium joins Sprint with iDEN Nextel Direct Connect capability http://bit.ly/jqmQ5d #android	dlvr.it
2011-05-05 09:28:03	BBC_TopGear	2.6m Ford GT40 prototype set to go under the hammer at Villa D'Este. #TopGear http://bit.ly/kOlPeM	Softwind Messenger
2011-05-05 09:28:11	GetCoHaEngiJobs	... - #Laurel , MD (http://tinyurl.com/3ttqza7) Get Computer Hardware Engineering Jobs #ComputerHardwareEngineering #jobs #job #GetAllJobs	GetAllJobs
2011-05-05 09:47:29	GetCoHaEngiJobs	Urgent Requirement for Network Eng... - #Philadelphia , PA (http://tinyurl.com/3b46rjk) Get Computer Hardware Engineering Jobs #ComputerHard	GetAllJobs
2011-05-05 10:12:57	InsideFerrari	Massa: mportant for fans to see a really exciting show??http://bit.ly/mI4eXs	web
2011-05-05 10:27:14	GetCoHaEngiJobs	Digital Hardware and Embedded Software Engineer... - #Bedford , MA (http://tinyurl.com/6l999me) Get Computer Hardware Engineering Jobs #Comp	GetAllJobs
2011-05-05 10:29:27	rubarrichello	Capadcia...local sensacional/// beautiful Capadocia http://twitpic.com/4tpy2t	Twitpic
2011-05-05 10:43:43	androidcentral	Samsung Replenish video hands-on http://bit.ly/j8tdSo #android	dlvr.it
2011-05-05 10:47:14	GetCoHaEngiJobs	Project Engin... - #Cumberland , RI (http://tinyurl.com/3sxdgff) Get Computer Hardware Engineering Jobs #ComputerHardwareEngineering #jobs #	GetAllJobs
2011-05-05 10:48:27	benjamincrozat	??androidcentral: Samsung Replenish video hands-on http://j.mp/j8tdSo #android??// C'est quoi cette horreur ?	Tweetbot for iPhone
2011-05-05 11:01:09	BBC_TopGear	Drop-top version of AMG's finest revealed ahead of Frankfurt show in September. #TopGear http://bit.ly/jS6Nm5	Softwind Messenger
2011-05-05 11:08:13	androidcentral	New from the store: Seidio Desktop Charging Cradle for HTC Inspire 4G, Desire HD http://bit.ly/ijvkXB	dlvr.it
2011-05-05 11:14:25	Jay2pt0	Ever have a awesome morning where your bank account is replenished and @androidcentral posted on the exact phone you've wanted, Moto XPRT	Twitter for BlackBerry 짰
2011-05-05 11:21:44	LucasdiGrassi	Ja estou em Istanbul. Clima ta frio e chuvoso mas deve melhorar.	web
2011-05-05 11:27:26	GetCoHaEngiJobs	Software Enginee... - #Palatine , IL (http://tinyurl.com/63dqgus) Get Computer Hardware Engineering Jobs #ComputerHardwareEngineering #jobs	GetAllJobs
2011-05-05 11:36:07	InsideFerrari	Alonso: only race four, so still plenty of time to recover??http://bit.ly/kUAlpB	web
2011-05-05 11:43:19	BBC_TopGear	More pics of the new Merc SLS AMG roadster... #TopGear http://bit.ly/lJven9	Softwind Messenger
2011-05-05 11:51:21	GetCoHaEngiJobs	Mobile Software Engineer-An... - #SanFrancisco , CA (http://tinyurl.com/3hbnwr9) Get Computer Hardware Engineering Jobs #ComputerHardwareEng	GetAllJobs
2011-05-05 12:00:18	SamsungMobileUS	Happy #CincoDeMayo! Capture the fun times on your phone tonight!	Social Publisher
2011-05-05 12:12:49	yob_taog	lunch time, finally. Maybe I should get a gyro, its Greek week!	TweetCaster
2011-05-05 12:12:53	androidcentral	New from the store: OverBoard Waterproof Case for Motorola Xoom http://bit.ly/iJbOfd	dlvr.it
2011-05-05 12:29:31	OfficialMGP	The drivers are coming to the end of a busy day of engineering & media. Looking forward to the track action getting underway tomorrow!	web
2011-05-05 12:33:28	GetCoHaEngiJobs	Storage Area Network Engineer... - #Augusta , GA (http://tinyurl.com/3h53coq) Get Computer Hardware Engineering Jobs #ComputerHardwareEngine	GetAllJobs
2011-05-05 12:42:16	InsideFerrari	The Horse Whisperer - Spring, the time of allergies http://bit.ly/jfIbrl	web
2011-05-05 12:42:32	jakehumphreyf1	Just had great chat with @lewishamilton about China. He says it's in his top 5 wins & to find out why he was so emotional, tune in on Sunday	web
2011-05-05 12:43:14	yob_taog	I just installed the new Twidroyd for #Twitter on my #Android #Phone - Its #Free, give it a try. http://www.twidroyd.com	twidroyd
2011-05-05 12:45:58	jakehumphreyf1	By the way, if you've series linked F1 quali, please note we're on BBC TWO this Saturday for various reasons. On Air at 11am...pass it on!	web
2011-05-05 12:48:38	androidcentral	Sony Ericsson launches next-generation Xperia Mini, Xperia Mini Pro http://bit.ly/iGLTnT #android	dlvr.it
2011-05-05 12:50:42	F1	FIA Thursday press conference - Turkey: Drivers - Timo Glock (Virgin), Lewis Hamilton (McLaren), Heikki Kovalain... http://bit.ly/jDTxvP	twitterfeed
2011-05-05 12:50:42	Formula1	FIA Thursday press conference - Turkey: Drivers - Timo Glock (Virgin), Lewis Hamilton (McLaren), Heikki Kovalain... http://bit.ly/jDTxvP	twitterfeed
2011-05-05 12:57:51	GetCoHaEngiJobs	Systems Engineer-ERP-SAP- Principal lev... - #Annapolis , MD (http://tinyurl.com/3cdn223) Get Computer Hardware Engineering Jobs #ComputerHa	GetAllJobs
2011-05-05 12:59:32	androidcentral	HTC Flyer's Digital Pen gets priced at $79.99 at Best Buy http://bit.ly/mcuxjx #android	dlvr.it
2011-05-05 13:01:40	google	The Search Globe: a new visual display representing one day of Google searches around the world http://goo.gl/viyzs	Tap11
2011-05-05 13:02:25	TheFifthDriver	@JakeHumphreyF1 being introduced to @LewisHamilton's mechanics this afternoon for a BBC F1 feature this weekend http://twitpic.com/4ts3s7	Twitpic
2011-05-05 13:05:46	jakehumphreyf1	We'll be on BBC Two and BBC HD Channel on Saturday. BBC One and BBC One HD on Sunday. Simples!	web

2011-05-05 13:09:59	google	A world in your pocket: Google Earth now optimized for Android-powered tablets, w/ 3D buildings on mobile & more, goo.gl/jtm6g	web
2011-05-05 13:11:08	GetCoHaEngiJobs	Electrical Software En... - #WallopsIsland , VA (http://tinyurl.com/3wda6rv) Get Computer Hardware Engineering Jobs #ComputerHardwareEnginee	GetAllJobs
2011-05-05 13:12:38	8039442	Curate Your Favorite Sites With Scoop.it http://ping.fm/klZZU	Ping.fm
2011-05-05 13:26:45	yob_taog	Mmm panera = good http://twitpic.com/4tscf6	Seesmic for Android
2011-05-05 13:37:01	google	Kudos to National Inventors Hall of Fame 2011 honorees (Internet security, barcode, digital camera, etc) http://goo.gl/xUgnw (pdf)	web
2011-05-05 13:38:34	androidcentral	LG Optimus Black initial review: http://bit.ly/iO62a0	Seesmic Desktop
2011-05-05 13:47:44	GetCoHaEngiJobs	Software Engineer III J... - #Melbourne , FL (http://tinyurl.com/44x5em9) Get Computer Hardware Engineering Jobs #ComputerHardwareEngineerin	GetAllJobs
2011-05-05 13:51:42	Formula1	Mark Webber Q&A: Red Bull not yet out of woods with KERS: True, Lewis Hamilton won the Chinese race and did a gr... http://bit.ly/lgI2k4	twitterfeed
2011-05-05 13:51:42	F1	Mark Webber Q&A: Red Bull not yet out of woods with KERS: True, Lewis Hamilton won the Chinese race and did a gr... http://bit.ly/lgI2k4	twitterfeed
2011-05-05 13:52:21	LucasdiGrassi	Minhas luvas depois de +- 6.000 trocas de marcha em um dia de teste http://yfrog.com/h4t7iybj	Twitter for BlackBerry 짰
2011-05-05 14:00:03	LucasdiGrassi	Varias pessoas querendo as luvas! Ate quanto vcs pagariam se eu doasse 100% do $ para caridade no BR?	Twitter for BlackBerry 짰
2011-05-05 14:04:21	google	Google MapMaker, World Bank & Sudanese come together to map a future country, the Rep of South Sudan: http://goo.gl/fUL4D	web
2011-05-05 14:11:36	H_Kovalainen	Busy day at the track today, interviews and meetings all day, everything ready for this weekend	Twitter for Mac
2011-05-05 14:15:12	H_Kovalainen	Check out my website we've got new web store open and new stuff coming, caps available already, http://t.co/1kaD1sV	Twitter for Mac
2011-05-05 14:18:48	H_Kovalainen	??MikePhillis1: @H_Kovalainen any chance you could wish our guys good luck for race 5... @DraigRacing Good luck for race 5!	Twitter for Mac
2011-05-05 14:22:36	H_Kovalainen	??kimifan: @H_Kovalainen Hope you'll be doing some kids stuff? Will be doing lots of kids stuff I agree it's very important	Twitter for Mac
2011-05-05 14:34:38	GetCoHaEngiJobs	Sr Software Engineer... - #Riverdale , MD (http://tinyurl.com/3r34d26) Get Computer Hardware Engineering Jobs #ComputerHardwareEngineering #	GetAllJobs
2011-05-05 14:36:10	androidcentral	Google Earth updated, optimized for Honeycomb tablets http://bit.ly/lOLFct #android	dlvr.it
2011-05-05 15:00:20	SamsungMobileUS	Thinking about the #GalaxyTab 10.1? Sign up for details, updates and be the first to purchase! http://pub.vitrue.com/KB2	Social Publisher
2011-05-05 15:08:04	GetCoHaEngiJobs	Software Engineer (Junio... - #RoundRock , TX (http://tinyurl.com/3p9z7l7) Get Computer Hardware Engineering Jobs #ComputerHardwareEngineeri	GetAllJobs
2011-05-05 15:20:12	androidcentral	Is the HTC Kingdom Sprint's newer, smaller black slab? http://bit.ly/iwuD97 #android	dlvr.it
2011-05-05 15:25:46	F1	Nick Heidfeld Q&A: Much more to come from Renault: Nick Heidfeld is the true 'comeback kid' of the Formula One p... http://bit.ly/jNcjJy	twitterfeed
2011-05-05 15:25:46	Formula1	Nick Heidfeld Q&A: Much more to come from Renault: Nick Heidfeld is the true 'comeback kid' of the Formula One p... http://bit.ly/jNcjJy	twitterfeed
2011-05-05 15:42:28	InsideFerrari	Chat with Luca Colajanni from Istanbul: join to the event directly from the Official Forum with your question! http://bit.ly/k8CXvq	web
2011-05-05 15:44:50	GetCoHaEngiJobs	Senior Software Engineer [Java] - Boomi - Berwy... - #Philadelphia , PA (http://tinyurl.com/5vfsyy9) Get Computer Hardware Engineering Jobs	GetAllJobs
2011-05-05 15:48:13	androidcentral	Walmart knows not to sell the Droid Charge http://bit.ly/kMBLjg #android	dlvr.it
2011-05-05 15:53:02	androidcentral	Sprint's Relay ID Pack aids those with hearing difficulties http://bit.ly/kXaEGv #android	dlvr.it
2011-05-05 16:03:05	androidcentral	Taptu update brings Honeycomb optimization http://bit.ly/mEdPfb #android	dlvr.it
2011-05-05 16:06:19	BBC_TopGear	Our top post: 칠 2.6m Ford GT40 prototype set to go under the hammer at Villa D'Este. #TopGear http://bit.ly/kOlPeM	web
2011-05-05 16:08:39	androidcentral	Methinks they're about to announce the Samsung Infuse 4G release date. :p http://twitpic.com/4ttsrq	Seesmic Desktop
2011-05-05 16:18:13	GetCoHaEngiJobs	Mechanical Engineer - Electrical Engineer - Civil Engineer... - #Chicago , IL (http://tinyurl.com/3t7bck8) Get Computer Hardware Engineering	GetAllJobs
2011-05-05 16:22:44	androidcentral	For those asking, yes, we're live at the Samsung/AT&T event. Say hi to @andrewmel and @anndrew. (Yes, we sent two An(n)drews.)	Seesmic Desktop
2011-05-05 16:26:00	androidcentral	Samsung's Kim Titus on stage. http://twitpic.com/4tty4u	Seesmic Desktop
2011-05-05 16:28:52	androidcentral	HTC Flyer 'Magic Pen' gets priced in the UK and Europe http://bit.ly/ipJfKp #android	dlvr.it
2011-05-05 16:29:47	androidcentral	Just going over the tech now. But the phone's even more official than it was the first time it was announced in January. :p	Seesmic Desktop
2011-05-05 16:30:53	androidcentral	The Infuse will have a special edition of Angry Birds!	Seesmic Desktop

2011-05-05 16:33:47	androidcentral	May 15, $199.	Seesmic Desktop
2011-05-05 16:37:10	androidcentral	Samsung Infuse 4G officially hits AT&T on May 15, comes with special edition of Angry Birds http://bit.ly/kMqG84 #android	dlvr.it
2011-05-05 16:40:19	androidcentral	Samsung Infuse 4G specs http://bit.ly/kYmsd6 #android	dlvr.it
2011-05-05 16:41:58	Samsungtweets	Seems that a lot of you are excited for the #Infuse4G - what are you most looking forward to in the phone? cc @SamsungMobileUS	Sprinklr
2011-05-05 16:47:40	androidcentral	Comment of the day: http://bit.ly/l7WYvG	Seesmic Desktop
2011-05-05 16:47:56	GetCoHaEngiJobs	Full Chip Validation Engine... - #Hillsboro , OR (http://tinyurl.com/6e639g4) Get Computer Hardware Engineering Jobs #ComputerHardwareEngine	GetAllJobs
2011-05-05 16:57:47	androidcentral	We almost dropped a 4.5-inch Infuse 4G on @phonedog_aaron's head. Damn near killed him. (Not really.)	Seesmic Desktop
2011-05-05 16:58:28	philipberne	Infuse 4G and Galaxy S II http://twitpic.com/4tu8ew	Twitpic
2011-05-05 17:14:32	GetCoHaEngiJobs	Graphics Software Engine... - #Hillsboro , OR (http://tinyurl.com/3c9bfrd) Get Computer Hardware Engineering Jobs #ComputerHardwareEngineeri	GetAllJobs
2011-05-05 17:36:23	androidcentral	AT&T re-enables sideloading on the Infuse 4G! http://bit.ly/mvS8Gg #android	dlvr.it
2011-05-05 17:40:32	GetCoHaEngiJobs	Sr Software Engi... - #RedwoodCity , CA (http://tinyurl.com/3u35nqw) Get Computer Hardware Engineering Jobs #ComputerHardwareEngineering #jo	GetAllJobs
2011-05-05 17:57:50	google	Check out 9 easy Gmail tricks to keep your inbox under control: http://goo.gl/Txif8 (via @HuffPostTech)	web
2011-05-05 18:05:36	GetCoHaEngiJobs	Software Engin... - #Richardson , TX (http://tinyurl.com/3ou696c) Get Computer Hardware Engineering Jobs #ComputerHardwareEngineering #jobs	GetAllJobs
2011-05-05 18:06:21	androidcentral	Samsung Infuse 4G Initial Hands On http://bit.ly/khnDaX #android	dlvr.it
2011-05-05 18:29:44	GetCoHaEngiJobs	Systems Engineer I... - #Phoenix , AZ (http://tinyurl.com/3f8pnlr) Get Computer Hardware Engineering Jobs #ComputerHardwareEngineering #jobs	GetAllJobs
2011-05-05 18:33:22	androidcentral	PODCAST ALERT: Hey, folks. No podcast tonight on account of ... Lots of stuff. We'll make it up to you real soon. Promise. :p	Seesmic Desktop
2011-05-05 18:51:09	androidcentral	Samsung Infuse 4G video hands-on http://bit.ly/jyGORX #android	dlvr.it
2011-05-05 18:53:08	GetCoHaEngiJobs	Sr. Project Engineer... - #SanJose , CA (http://tinyurl.com/3vymus7) Get Computer Hardware Engineering Jobs #ComputerHardwareEngineering #jo	GetAllJobs
2011-05-05 19:16:31	GetCoHaEngiJobs	Software Engineer SJ05NKA... - #SanJose , CA (http://tinyurl.com/3qd496t) Get Computer Hardware Engineering Jobs #ComputerHardwareEngineerin	GetAllJobs
2011-05-05 19:20:32	yob_taog	Look at all the beer! Fatheads, already one of my favorite places http://twitpic.com/4tscf6 http://twitpic.com/4tvmcu	Seesmic for Android
2011-05-05 19:34:27	SamsungMobileUS	Samsung Infuse 4G for ATT coming 5/15 for $199.99 - exclusive @RovioMobile #AngryBirds level. Watch out for clues! http://pub.vitrue.com/OIr	Social Publisher
2011-05-05 19:51:51	GetCoHaEngiJobs	Senior Software Engineer ? Services... - #NewYork , NY (http://tinyurl.com/6c2unrm) Get Computer Hardware Engineering Jobs #ComputerHardware	GetAllJobs
2011-05-05 20:00:16	SamsungMobileUS	Be the 1st 2 purchase & receive news re: #GalaxyTab 10.1 @MarthaStewart?쎀 glad she did http://pub.vitrue.com/KB2 http://pub.vitrue.com/N7H	Social Publisher
2011-05-05 20:21:09	androidcentral	Judge throws out 129 of Oracle's claims against Google, leaves 3 http://bit.ly/jWWwP7 #android	dlvr.it
2011-05-05 20:28:59	GetCoHaEngiJobs	Windows Systems Engin... - #Washington , DC (http://tinyurl.com/65sstga) Get Computer Hardware Engineering Jobs #ComputerHardwareEngineering	GetAllJobs
2011-05-05 20:39:28	FatHeadsPGH	Correction: The firkin tomorrow is actually the Coffee Imperial Stout.	Twitter for iPhone
2011-05-05 20:51:39	GetCoHaEngiJobs	Graphics Software Engin... - #SantaClara , CA (http://tinyurl.com/66lx7oq) Get Computer Hardware Engineering Jobs #ComputerHardwareEngineeri	GetAllJobs
2011-05-05 21:26:57	androidcentral	Support Group for those switching from WebOS (palm pre) to Nexus S 4g - Android Forums http://t.co/xytF0kn cc/ @precentral	Tweet Button
2011-05-05 21:32:23	GetCoHaEngiJobs	Senior Software Engineer Jo... - #Syracuse , NY (http://tinyurl.com/68xqbcr) Get Computer Hardware Engineering Jobs #ComputerHardwareEnginee	GetAllJobs
2011-05-05 22:05:03	GetCoHaEngiJobs	Software Engineer/Web Developer... - #Hanover , MD (http://tinyurl.com/3brlv9k) Get Computer Hardware Engineering Jobs #ComputerHardwareEngi	GetAllJobs
2011-05-05 22:35:58	GetCoHaEngiJobs	Lead Communications Systems Engineer Jo... - #Syracuse , NY (http://tinyurl.com/3w9u6xa) Get Computer Hardware Engineering Jobs #ComputerHar	GetAllJobs
2011-05-05 23:06:37	GetCoHaEngiJobs	Senior Software Engineer - Automotive L... - #Sunnyvale , CA (http://tinyurl.com/43yp3wm) Get Computer Hardware Engineering Jobs #ComputerHa	GetAllJobs
2011-05-05 23:36:15	GetCoHaEngiJobs	Software Engi... - #KingOfPrussia , PA (http://tinyurl.com/454vhsy) Get Computer Hardware Engineering Jobs #ComputerHardwareEngineering #job	GetAllJobs
2011-05-06 00:02:36	GetCoHaEngiJobs	Sr.software Engineer... - #SanJose , CA (http://tinyurl.com/6kayfbr) Get Computer Hardware Engineering Jobs #ComputerHardwareEngineering #jo	GetAllJobs

Table 41. Contents of 'com.seesmic/databases/twitter.db (users table)'

my_user_id	tweets_count	friends_count	followers_count	profile_location	profile_description
twidroyd	159	4	431676	Austria & California	the #1 twitter app for android | ideas/problems mail:AT:twidroyd.com - no support via twitter
handmark	2073	49193	773569	Kansas City, MO	Handmark 짰 is a world-leading creator and distributor of mobile applications and services for Android, BlackBerry, iPhone, Windows Mobile, Palm, Java and Symbian
asktwidroyd	21560	4	711		twidroyd answers! please follow @twidroyd for the real news.
seesmic	1269	10763	400533	Your Browser	I make updates and announcements for Seesmic.com Send feedback/questions to @askseesmic
TheFifthDriver	2451	35674	77669	Woking, UK	Vodafone McLaren Mercedes official Twitter page
jakehumphreyf1	4322	229	212967	Home...eventually!	Hangs around garages with a couple of mates presenting award winning F1 coverage!
OfficialMGP	3285	199	65122	Brackley, Northants, UK	The official Twitter account of the MERCEDES GP PETRONAS Formula One Team
DroidLanding	428	220	37615	United States	Something mysterious is happening. And at the center is Droid Charge. Track the anomalies to their location in cities across America and you could win one.
Jay2pt0	1324	39	59	The Universe beyond this one	Geek, Nerd (there's a different), Nostalgic Smartphone lover (Blackberry and Palm), Youtuber (Jay2pt0) and all around awesome guy... who happens to be a genius!
benjamincrozat	31345	312	470	Le Cannet, France	Smartphones enthusiast (iPhone user). I was an official tester for Samsung (Nexus S) and Microsoft (HTC 7 Mozart) during 2 weeks. Tweet in French.
rubarrichello	10023	151	895462		amante da velocidade e Pai do Dudu e Fefe
JensonButton	798	40	317902	Guernsey	Vodafone McLaren Mercedes F1 driver, Like putting myself through pain in Triathlons! Love my cat!;)
SarahAnnGreen	34637	1309	1716	Oxford	If Jane Austen wrote a novel about Formula 1 & vampires, then I'd be first in line at the book signing!
LucasdiGrassi	2428	111	84346	Worldwide	Professional Racing Driver | ONE International SB Founder | Contact: Henry.Guedes@1iSB.com
H_Kovalainen	1285	23	69562	3.1287,101.562052	F1 Racing driver, currently driving for Team Lotus.
F1	2144	0	93624	Great Britain	The Official Formula 1 Website
BBC_TopGear	2580	2110	184880	London	Proper Top Gear tweets from the show HQ, next to London?섹 glittering Westway flyover. And an airfield in Surrey. If you follow anything else, it's not real
InsideFerrari	4361	2	97271	Maranello - Italy	Scuderia Ferrari Marlboro - The Official Page
Formula1	1918	0	32902	Great Britain	The Official Formula 1 Website
Samsungtweets	10328	32063	47337	Ridgefield Park, NJ	The Official Samsung USA Twitter Account! We're here to share all things Samsung, help you out, and have awesome conversations. Thanks for following!
philipberne	7017	326	1174	Dallas, TX	Was a journalist, now I work for Samsung. Tweeting is not part of my job, it's personal. Anything I tweet is my opinion, not based in reality. Don't believe me.
google	2420	380	3048185	Mountain View, CA	News and updates from Google
yob_taog	8	25	3	Pittsburgh	Sr. VP at SwiftLogic Inc,
SamsungMobileUS	2107	12534	43917	USA (Dallas, TX)	The Official Samsung Mobile Twitter channel. Do you have questions about our US phones? Go here - http://bit.ly/ELanO or reach out to @SamsungService for help!

FatHeadsPGH	2732	553	1510	1805 E. Carson St. PGH, PA	Chill out man, have a beer!
androidcentral	11743	163	78362	Florida	The Center of the Android Universe - your No. 1 site for Android smartphone news, reviews, accessories and opinions.
GetCoHaEngiJobs	11359	927	939		Computer Hardware Engineering jobs, careers and community site.

3.3.18. Scenario 2 – Email

It gets stored in the files 'EmailProvider.db (Attachment, Message table)' and 'EmailProviderBody.db (body table)', which are in the directory '/data/data/com.android.email/databases'. The details of the email can be checked by combining the contents of the two files. The details of the emails that exist are as follows. (Contents of advertisement emails were not entered.)

Table 42. Contents of Email

Time (UTC-4)	From	Subject	Contents	Attachment
2011-05-06 20:14:25	Swift Logic swiftlogic@consultant.com	Re: File request	Mr Taog- Here are the files that have access times for the last two days, let me know if you need anything else! Thanks, Tim ----- Original Message ----- From: Yob Taog Sent: 05/06/11 03:35 PM To: swiftlogic@consultant.com, swiftlogicllc@consultant.com, swiftlogicinc@consultant.com Subject: File request helpdesk, I was unaware of the server outage starting today and need some files to work on this weekend, there is a very big meeting on Monday. Can you please email me sheets from project 2228, I need the ones that I've most recently modified, you should be able to tell by the file dates. I'll be in a management meeting for a while, but will have access on my phone. Thank you, Yob Taog VP Swiftlogic Inc.	
2011-05-06 23:11:04	Swift Logic swiftlogic@consultant.com	Re: File request	Mr Taog- My apologies, we kind of have our hands full down here with the maintenance. Find your files attached. Thanks, Tim ----- Original Message ----- From: Yob Taog Sent: 05/06/11 08:23 PM To: Swift Logic Subject: Re: File request Hi Tim, There are no files attached.... I could really use these files tonight. -yob	2228-11.pdf (260786) 2228-12.pdf (48113) 2228-15.pdf (64530)

			On Fri, May 6, 2011 at 8:14 PM, Swift Logic <swiftlogic@consultant.com> wrote: Mr Taog- Here are the files that have access times for the last two days, let me know if you need anything else! Thanks, Tim ----- Original Message ----- From: Yob Taog Sent: 05/06/11 03:35 PM To: swiftlogic@consultant.com, swiftlogicllc@consultant.com, swiftlogicinc@consultant.com Subject: File request helpdesk, I was unaware of the server outage starting today and need some files to work on this weekend, there is a very big meeting on Monday. Can you please email me sheets from project 2228, I need the ones that I've most recently modified, you should be able to tell by the file dates. I'll be in a management meeting for a while, but will have access on my phone. Thank you, Yob Taog VP Swiftlogic Inc.	
2011-05-07 12:40:49	Swift Logic swiftlogic@consultant.com	Re: File request	Mr Taog- It looks like Tim found your files, but he just went out for breakfast. Please don't hesitate to call or email us for any other issues you may have. The maintenance is going very well, we expect to be done late tonight or early tomorrow morning. Thanks, Bob ----- Original Message ----- From: Yob Taog Sent: 05/07/11 12:29 AM To: Swift Logic Subject: Re: File request Tim, Sheets 7 and 10 should have also been included in that timeframe... Also, I need whatever sheets you can find for 2201. -yob On Fri, May 6, 2011 at 11:11 PM, Swift Logic <swiftlogic@consultant.com> wrote: Mr Taog- My apologies, we kind of have our hands full down here with the maintenance. Find your files attached. Thanks, Tim ----- Original Message ----- From: Yob Taog Sent: 05/06/11 08:23 PM To: Swift Logic Subject: Re: File request Hi Tim, There are no files attached.... I could really use these files tonight. -yob	2201-4.pdf (40424), 2201-7.pdf (58680), 2201-8.pdf (71648), 2201-9.pdf (63418), 2228-7.pdf (242276), 2228-10.pdf (187260)

			On Fri, May 6, 2011 at 8:14 PM, Swift Logic <swiftlogic@consultant.com> wrote: Mr Taog- Here are the files that have access times for the last two days, let me know if you need anything else! Thanks, Tim ----- Original Message ----- From: Yob Taog Sent: 05/06/11 03:35 PM To: swiftlogic@consultant.com, swiftlogicllc@consultant.com, swiftlogicinc@consultant.com Subject: File request helpdesk, I was unaware of the server outage starting today and need some files to work on this weekend, there is a very big meeting on Monday. Can you please email me sheets from project 2228, I need the ones that I've most recently modified, you should be able to tell by the file dates. I'll be in a management meeting for a while, but will have access on my phone. Thank you, Yob Taog VP Swiftlogic Inc.	
2011-05-07 14:06:12	Luke Lancer luk3lancer@gmail.com	Mother of all hangovers	Hey Yob, So, a guy walks into a bar in the strip district ... That guy was me. Last night. All night. OMG I can barely move my eyes in my head without this cascade of pain and nausea. I was going to be a good boy. I went home a little early, but I had a bunch of docs to review in my inbox. Then, that freakin outage thing hit. No way that was announced. I don't buy this planned outage thing. Anyway. Frustrating. So, I decided to kill some time and forget about things. Went to Boomerang BBQ & Pizza and then walked on down to Mullaney's. I don't remember much else. Except this cute girl from McKee's Rocks slapped me for some reason. Anyway, I know you were going to work all weekend. But since you probably don't have anything to work with either ... wanna come along for a sequel 2nite? Best way I know to cure what ails me. Peace out, LLancer	
2011-05-07 15:06:12	Luke Lancer luk3lancer@gmail.com	Re: Mother of all hangovers	Where does everyone discover these things!! Well, thanks. I might check with them today about getting some of my work docs. But, then, I might see that girl from McKees Rocks if I go out again tonight .... I'll ping you later, dude On Sat, May 7, 2011 at 2:51 PM, Yob Taog <yobtaog@gmail.com> wrote: Hey, Did you know about the swiftlogic@consultant address? ?You can use that to contact the helpdesk when systems are down. ?They seem to be pretty slow at responding, but I have been able to get some work done. ?I haven't really looked at them yet, but I think I just got the last set of docs I needed to look at over the weekend. You'll have to put me down as a "maybe" for tonight. ?I really need to get prep'ed for monday. -yob On Sat, May 7, 2011 at 2:06 PM, Luke Lancer <luk3lancer@gmail.com> wrote: Hey Yob, So, a guy walks into a bar in the strip district ... That guy was me. Last night. All night. OMG I can barely move my eyes in my head without this cascade of pain and nausea. I was going to be a good boy. I went home a little early, but I had a bunch of docs to review in my inbox. Then, that freakin outage thing hit. No way that was announced. I don't buy this planned outage thing. Anyway. Frustrating. So, I decided to kill some time and forget about things. Went to Boomerang	

			BBQ & Pizza and then walked on down to Mullaney's. I don't remember much else. Except this cute girl from McKee's Rocks slapped me for some reason. Anyway, I know you were going to work all weekend. But since you probably don't have anything to work with either ... wanna come along for a sequel 2nite? Best way I know to cure what ails me. Peace out, LLancer	
2011-05-07 16:41:08	Reg Wetham regwetham@yahoo.com	Re: tonight	Fabulous. I'm glad that worked out -- otherwise, it would have been hell next week. I am still planning to savor a cubano and a mellow single-malt this evening. Do you think you'll have time to join me? If so, I plan on heading out around 7:30, but we can meet pretty much anytime. I just need to stay away from the strip. I don't want to run into Luke on one of his tears  . I know someone who saw him last night at an Irish pub and said he was in obnoxious form. Too many appletinis ! (Who goes to an Irish pub and orders an appletini, anyway?!) --- **From:** Yob Taog <yobtaog@gmail.com> **To:** Reg Wetham <regwetham@yahoo.com> **Sent:** Saturday, May 7, 2011 3:04 PM **Subject:** Re: tonight hey, I got the docs i needed from the helpdesk. Are you still planning on heading to that cigar bar tonight? -yob	
2011-05-07 19:07:19	Reg Wetham regwetham@yahoo.com	Re: tonight	That's the one. See you there! --- **From:** Yob Taog <yobtaog@gmail.com> **To:** Reg Wetham <regwetham@yahoo.com> **Sent:** Saturday, May 7, 2011 6:26 PM **Subject:** Re: tonight Reg, Yeah, Luke hit me up to join him tonight, I think want to go out tonight to get a break from work and I am glad you are available as an alternative. You just can't trust a guy that drinks, but doesn't drink beer. :-) I'll probably be showing up a little after 8. You going to that place in the Southside Works right? -yob On Sat, May 7, 2011 at 4:41 PM, Reg Wetham <regwetham@yahoo.com> wrote: Fabulous. I'm glad that worked out -- otherwise, it would have been hell next week. I am still planning to savor a cubano and a mellow single-malt this evening. Do you think you'll have time to join me? If so, I plan on heading out around 7:30, but we can meet pretty much anytime. I just need to stay away from the strip. I don't want to run into Luke on one of his tears  . I know someone who saw him last night at an Irish pub and said he was in obnoxious form. Too many appletinis ! (Who goes to an Irish pub and orders an appletini, anyway?!) --- **From:** Yob Taog <yobtaog@gmail.com> **To:** Reg Wetham <regwetham@yahoo.com> **Sent:** Saturday, May 7, 2011 3:04 PM **Subject:** Re: tonight hey, I got the docs i needed from the helpdesk. Are you still planning on heading to that cigar bar tonight? -yob	
2011-05-07 19:08:54	Shandra Pfeif shandra@cheerful.com	Re: drinks tonight?	Sure. That's nice of you and Reg. Where are you guys going to be? ----- Original Message ----- From: Yob Taog	

			Sent: 05/07/11 06:30 PM To: Shandra Pfeif Subject: drinks tonight? Hey Shandra, I'm headed out with my buddy Reg tonight (i think you've met him?) and some others. Would you care to join us? Or meetup afterward? -yob	
2011-05-07 22:59:24	Twitter	Steve Buttinsky is now following you on Twitter!	twitter **Steve Buttinsky (@SteveButtinsky) is now following your tweets (@yob_taog) on Twitter.**  **Steve Buttinsky** @SteveButtinsky Philadelphia **Bio** I'm a computer tech living in Philly. I love fast food, Android, and football. America rules! **33** tweets | **252** following | **19** followers You do not follow Steve Buttinsky. What's next? • Find out more about Steve Buttinsky on @SteveButtinsky's profile page. • Send Steve Buttinsky an @ reply. • Send Steve Buttinsky a direct message. On your mobile? Learn Twitter for Mobile. If you believe Steve Buttinsky is engaging in abusive behavior on Twitter, you may report Steve Buttinsky for spam. If you'd rather not receive follow notification emails from Twitter, you can unsubscribe immediately. To resubscribe or change other Twitter email preferences, visit your account settings to manage email notices. Please do not reply to this message; it was sent from an unmonitored email address. This message is a service email related to your use of Twitter. For general inquiries or to request support with your Twitter account, please visit us at Twitter Support.	
2011-05-08 12:50:01	Google Calendar	Reminder: Call mother @ Sun May 8 1pm - 2:30pm (yobtaog@gmail.com)	**more details »** Call mother When Sun May 8 1pm ? 2:30pm Eastern Time Calendar yobtaog@gmail.com Who • Yob Taog - organizer Invitation from Google Calendar You are receiving this email at the account yobtaog@gmail.com because you are subscribed for reminders on calendar yobtaog@gmail.com. To stop receiving these notifications, please log in to https://www.google.com/calendar/ and change your notification settings for this calendar.	
2011-05-08 16:05:42	Pittsburgh Downtown Partnership	Get Into It! Downtown Happenings, Week of May 9 - Downtown	-	

		Springs to Life		
2011-05-08 16:50:14	Google Calendar	Reminder: Meetings with SunTech @ Mon May 9 - Tue May 10, 2011 (yobtaog@gmail.com)	**more details »** Meetings with SunTech When Mon May 9 ? Tue May 10, 2011 Where Atlanta (map) Calendar yobtaog@gmail.com Who • Yob Taog - organizer Invitation from Google Calendar You are receiving this email at the account yobtaog@gmail.com because you are subscribed for reminders on calendar yobtaog@gmail.com. To stop receiving these notifications, please log in to https://www.google.com/calendar/ and change your notification settings for this calendar.	
2011-05-09 06:24:46	The Pittsburgh Cultural Trust	WICKED Priority Ticket Offer!		
2011-05-09 07:58:04	Reg Wetham regwetham@yahoo.com	Monday	Hi Yob, Another Monday begins. I hope you managed to get enough prep in over the weekend for the trip this week. (I think it will be a pretty big deal for the company's prospects) Anyway, good luck and let me know how things go in Atlanta. Reg	
2011-05-09 12:19:04	Reg Wetham regwetham@yahoo.com	Safe travels	Hey Yob, I haven't heard back from you, so I assume you are either traveling or scrambling to get ready for the trip. Fortunately, I know your new Droid will be at hand, no matter what. So, you'll get this. Let me know when you have touched down and settled in. Reg	
2011-05-09 12:24:54	WinInfo Daily UPDATE	Email Trail Suggests Google Is Already the Next Microsoft	-	
2011-05-09 16:47:05	Windows Tips and Tricks UPDATE	John Savill's FAQs for 5/9: Hide the Remote Desktop tab		
2011-05-09 18:01:00	MobileDevPro UPDATE	Microsoft's Big (Mango) Mobile Moment; Forecast: 44 BILLION App Downloads Served	-	
2011-05-09 18:50:12	Google Calendar	Reminder: Drinks with Mr Tao and the Board @ Mon May 9 7pm - 8:30pm (yobtaog@gmail.com)	**more details »** Drinks with Mr Tao and the Board When Mon May 9 7pm ? 8:30pm Eastern Time Calendar yobtaog@gmail.com Who • Yob Taog - organizer	

			Invitation from Google Calendar You are receiving this email at the account yobtaog@gmail.com because you are subscribed for reminders on calendar yobtaog@gmail.com. To stop receiving these notifications, please log in to https://www.google.com/calendar/ and change your notification settings for this calendar.	
2011-05-10 07:24:19	Reg Wetham regwetham@yahoo.com	How is Atlanta	Hey Yob, I haven't heard back about your presentation and meetings. Hope all is going well and that clients like what you are showing them. It's some of SwiftLogic's best. Send me a sit rep when you get a moment. Reg	
2011-05-10 11:00:49	Twitter	Bernie & Dan is now following you on Twitter!	twitter **Bernie & Dan (@PghVintageGP) is now following your tweets (@yob_taog) on Twitter.** **Bernie & Dan** @PghVintageGP Pittsburgh, PA **Bio** ? *Burgh Verified* Vintage Racing on City Streets since 1983 surrounded by 2000+ vintage cars all for the benefit of R Autism charities: @bernardtmartin **2,755 tweets** | **1,936 following** | **1,080 followers** | **11 lists** You and @PghVintageGP both follow 3 users: • **Lewis Hamilton** @LewisHamilton • **Nico Rosberg** @nico_rosberg • **Heikki Kovalainen** @H_Kovalainen You do not follow Bernie & Dan. What's next? • Find out more about Bernie & Dan on @PghVintageGP's profile page. • Send Bernie & Dan an @ reply. • Send Bernie & Dan a direct message. • On your mobile? Learn Twitter for Mobile. If you believe Bernie & Dan is engaging in abusive behavior on Twitter, you may report Bernie & Dan	

			for spam. If you'd rather not receive follow notification emails from Twitter, you can unsubscribe immediately. To resubscribe or change other Twitter email preferences, visit your account settings to manage email notices. Please do not reply to this message; it was sent from an unmonitored email address. This message is a service email related to your use of Twitter. For general inquiries or to request support with your Twitter account, please visit us at Twitter Support.	
2011-05-10 13:23:58	WinInfo Daily UPDATE	News Flash: Microsoft to Acquire Skype for $8.5 Billion	-	
2011-05-10 14:45:16	Windows IT Pro UPDATE	What I'd Like to See at TechEd 2011	-	
2011-05-10 15:12:29	Windows IT Pro	Discover a cost-effective strategy to deliver corporate desktops to a diverse workforce	-	
2011-05-10 17:50:02	regwetham @yahoo.com Reg Wetham	Re: How is Atlanta	BBQ! I'm jealous. Glad to hear it went well, too. Don't know about the tech team. They have been acting a little funny today, too.  In any case, you should be able to access stuff normally via the corporate exchange server, sharepoint, etc now. If it's not too late. Reg --- **From:** Yob Taog <yobtaog@gmail.com> **To:** Reg Wetham <regwetham@yahoo.com> **Sent:** Tuesday, May 10, 2011 4:34 PM **Subject:** Re: How is Atlanta Went well! I'll have to give you the details when I get back. Atlanta is way too hot, 96 today, and its not even half way through may! I did get some good BBQ though. I'm a little pissed off at the tech team at the consultant address, they never got back to me about some additional sheets I wanted for today - they just never responded.... iknow they can because they did last week. -yob On May 10, 2011 7:24 AM, "Reg Wetham" <regwetham@yahoo.com> wrote: Hey Yob, I haven't heard back about your presentation and meetings. Hope all is going well and that clients like what you are showing them. It's some of SwiftLogic's best. Send me a sit rep when you get a moment. Reg	

3.3.19. Scenario 2 – Calendar

It gets stored in the file ‘calendar.db (Events table)’ in the ‘/data/data/com.android.providers.calender/databases’ directory.

Table 43. Contents of Calendar

Dtstart (UTC-4)	Dtend (UTC-4)	Sync Time	Title	EventLocation	EventTimezone
2009-12-31 20:00:00	2010-01-01 20:00:00	2011-05-09T22:05:34.000Z	New Year's Day		UTC
2010-01-17 20:00:00	2010-01-18 20:00:00	2011-05-09T22:05:34.000Z	Martin Luther King, Jr's Day		UTC
2010-02-01 20:00:00	2010-02-02 20:00:00	2011-05-09T22:05:34.000Z	Groundhog Day		UTC
2010-02-11 20:00:00	2010-02-12 20:00:00	2011-05-09T22:05:34.000Z	Lincoln's Birthday		UTC

2010-02-13 20:00:00	2010-02-14 20:00:00	2011-05-09T22:05:34.000Z	Valentine's Day		UTC
2010-02-14 20:00:00	2010-02-15 20:00:00	2011-05-09T22:05:34.000Z	Presidents Day		UTC
2010-03-13 20:00:00	2010-03-14 20:00:00	2011-05-09T22:05:34.000Z	Daylight Saving Time Begins		UTC
2010-03-16 20:00:00	2010-03-17 20:00:00	2011-05-09T22:05:34.000Z	St. Patrick's Day		UTC
2010-03-31 20:00:00	2010-04-01 20:00:00	2011-05-09T22:05:34.000Z	April Fool's Day		UTC
2010-04-14 20:00:00	2010-04-15 20:00:00	2011-05-09T22:05:34.000Z	Tax Day		UTC
2010-04-21 20:00:00	2010-04-22 20:00:00	2011-05-09T22:05:34.000Z	Earth Day		UTC
2010-05-04 20:00:00	2010-05-05 20:00:00	2011-05-09T22:05:34.000Z	Cinco de Mayo		UTC
2010-05-08 20:00:00	2010-05-09 20:00:00	2011-05-09T22:05:34.000Z	Mother's Day		UTC
2010-05-28 20:00:00	2010-05-29 20:00:00	2011-05-09T22:05:34.000Z	John F. Kennedy's Birthday		UTC
2010-05-30 20:00:00	2010-05-31 20:00:00	2011-05-09T22:05:34.000Z	Memorial Day		UTC
2010-06-13 20:00:00	2010-06-14 20:00:00	2011-05-09T22:05:34.000Z	Flag Day		UTC
2010-06-19 20:00:00	2010-06-20 20:00:00	2011-05-09T22:05:34.000Z	Father's Day		UTC
2010-07-03 20:00:00	2010-07-04 20:00:00	2011-05-09T22:05:34.000Z	Independence Day		UTC
2010-09-05 20:00:00	2010-09-06 20:00:00	2011-05-09T22:05:34.000Z	Labor Day		UTC
2010-09-10 20:00:00	2010-09-11 20:00:00	2011-05-09T22:05:34.000Z	Patriot Day		UTC
2010-10-10 20:00:00	2010-10-11 20:00:00	2011-05-09T22:05:34.000Z	Columbus Day		UTC
2010-10-30 20:00:00	2010-10-31 20:00:00	2011-05-09T22:05:34.000Z	Halloween		UTC
2010-11-01 20:00:00	2010-11-02 20:00:00	2011-05-09T22:05:34.000Z	Election Day		UTC
2010-11-06 20:00:00	2010-11-07 20:00:00	2011-05-09T22:05:34.000Z	Daylight Saving Time Ends		UTC
2010-11-10 20:00:00	2010-11-11 20:00:00	2011-05-09T22:05:34.000Z	Veterans Day		UTC
2010-11-24 20:00:00	2010-11-25 20:00:00	2011-05-09T22:05:34.000Z	Thanksgiving		UTC
2010-12-23 20:00:00	2010-12-24 20:00:00	2011-05-09T22:05:34.000Z	Christmas Eve		UTC
2010-12-24 20:00:00	2010-12-25 20:00:00	2011-05-09T22:05:34.000Z	Christmas		UTC
2010-12-30 20:00:00	2010-12-31 20:00:00	2011-05-09T22:05:34.000Z	New Year's Eve		UTC
2010-12-31 20:00:00	2011-01-01 20:00:00	2011-05-09T22:05:34.000Z	New Year's Day		UTC
2011-01-16 20:00:00	2011-01-17 20:00:00	2011-05-09T22:05:34.000Z	Martin Luther King, Jr's Day		UTC
2011-02-01 20:00:00	2011-02-02 20:00:00	2011-05-09T22:05:34.000Z	Groundhog Day		UTC
2011-02-11 20:00:00	2011-02-12 20:00:00	2011-05-09T22:05:34.000Z	Lincoln's Birthday		UTC
2011-02-13 20:00:00	2011-02-14 20:00:00	2011-05-09T22:05:34.000Z	Valentine's Day		UTC
2011-02-20 20:00:00	2011-02-21 20:00:00	2011-05-09T22:05:34.000Z	Presidents Day		UTC
2011-03-12 20:00:00	2011-03-13 20:00:00	2011-05-09T22:05:34.000Z	Daylight Saving Time Begins		UTC
2011-03-16 20:00:00	2011-03-17 20:00:00	2011-05-09T22:05:34.000Z	St. Patrick's Day		UTC
2011-03-31 20:00:00	2011-04-01 20:00:00	2011-05-09T22:05:34.000Z	April Fool's Day		UTC
2011-04-07 22:00:00	2011-04-08 00:00:00	2011-03-11T03:43:30.000Z	First Practice Session	Kuala Lumpur	UTC
2011-04-08 02:00:00	2011-04-08 04:00:00	2011-03-11T03:43:31.000Z	Second Practice Session	Kuala Lumpur	UTC
2011-04-09 01:00:00	2011-04-09 02:00:00	2011-03-11T03:43:31.000Z	Third Practice Session	Kuala Lumpur	UTC
2011-04-09 04:00:00	2011-04-09 06:00:00	2011-03-11T03:43:27.000Z	Qualifying Session	Kuala Lumpur	UTC
2011-04-10 04:00:00	2011-04-10 06:00:00	2011-03-11T03:43:34.000Z	Malaysian Grand Prix	Kuala Lumpur	UTC
2011-04-14 22:00:00	2011-04-15 00:00:00	2011-03-11T03:43:34.000Z	First Practice Session	Shanghai	UTC
2011-04-15 02:00:00	2011-04-15 04:00:00	2011-03-11T03:43:34.000Z	Second Practice Session	Shanghai	UTC
2011-04-15 23:00:00	2011-04-16 00:00:00	2011-03-11T03:43:34.000Z	Third Practice Session	Shanghai	UTC
2011-04-16 02:00:00	2011-04-16 04:00:00	2011-03-11T03:43:30.000Z	Qualifying Session	Shanghai	UTC
2011-04-17 03:00:00	2011-04-17 05:00:00	2011-03-11T03:43:26.000Z	Chinese Grand Prix	Shanghai	UTC
2011-04-21 20:00:00	2011-04-22 20:00:00	2011-05-09T22:05:34.000Z	Earth Day		UTC
2011-05-04 20:00:00	2011-05-05 20:00:00	2011-05-09T22:05:34.000Z	Cinco de Mayo		UTC
2011-05-05 08:00:00	2011-05-05 10:00:00	2011-05-05T02:20:39.000Z	Presentation On Project 5556a	Conference room 2201	America/New_York
2011-05-05 19:00:00	2011-05-05 22:30:00	2011-05-06T17:22:58.000Z	Fatheads	Southside	America/New_York
2011-05-06 03:00:00	2011-05-06 05:00:00	2011-03-11T03:43:26.000Z	First Practice Session	Istanbul	UTC
2011-05-06 07:00:00	2011-05-06 09:00:00	2011-03-11T03:43:26.000Z	Second Practice Session	Istanbul	UTC
2011-05-06 12:00:00	2011-05-06 13:00:00	2011-05-06T17:22:45.000Z	Lunch with Sandra		America/New_York
2011-05-06 14:00:00	2011-05-06 14:30:00	2011-05-06T17:23:30.000Z	meet with Phil		America/New_York
2011-05-06 14:30:00	2011-05-06 15:00:00	2011-05-06T17:23:35.000Z	Call Verizon About Battery Life		America/New_York

2011-05-06 15:30:00	1969-12-31 20:00:00	2011-05-06T17:23:55.000Z	Project Planning Meeting		America/New_York
2011-05-07 04:00:00	2011-05-07 05:00:00	2011-03-11T03:43:26.000Z	Third Practice Session	Istanbul	UTC
2011-05-07 07:00:00	2011-05-07 09:00:00	2011-03-11T03:43:34.000Z	Qualifying Session	Istanbul	UTC
2011-05-07 20:00:00	2011-05-08 20:00:00	2011-05-06T17:19:57.000Z	Turkish Grand Prix	Turkey	UTC
2011-05-07 20:00:00	2011-05-08 20:00:00	2011-05-09T22:05:34.000Z	Mother's Day		UTC
2011-05-08 08:00:00	2011-05-08 10:00:00	2011-03-11T03:43:26.000Z	Turkish Grand Prix	Istanbul	UTC
2011-05-08 13:00:00	2011-05-08 14:30:00	2011-05-08T15:56:48.000Z	Call mother		America/New_York
2011-05-08 20:00:00	2011-05-10 20:00:00	2011-05-08T15:57:14.000Z	Meetings with SunTech	Atlanta	UTC
2011-05-09 19:00:00	2011-05-09 20:30:00	2011-05-08T15:57:36.000Z	Drinks with Mr Tao and the Board		America/New_York
2011-05-20 04:00:00	2011-05-20 06:00:00	2011-03-11T03:43:28.000Z	First Practice Session	Catalunya	UTC
2011-05-20 08:00:00	2011-05-20 10:00:00	2011-03-11T03:43:38.000Z	Second Practice Session	Catalunya	UTC
2011-05-21 05:00:00	2011-05-21 06:00:00	2011-03-11T03:43:38.000Z	Third Practice Session	Catalunya	UTC
2011-05-21 08:00:00	2011-05-21 10:00:00	2011-03-11T03:43:27.000Z	Qualifying Session	Catalunya	UTC
2011-05-22 08:00:00	2011-05-22 10:00:00	2011-03-11T03:43:27.000Z	Spanish Grand Prix	Catalunya	UTC
2011-05-26 04:00:00	2011-05-26 06:00:00	2011-03-11T03:43:33.000Z	First Practice Session	Monte Carlo	UTC
2011-05-26 08:00:00	2011-05-26 10:00:00	2011-03-11T03:43:32.000Z	Second Practice Session	Monte Carlo	UTC
2011-05-28 05:00:00	2011-05-28 06:00:00	2011-03-11T03:43:32.000Z	Third Practice Session	Monte Carlo	UTC
2011-05-28 08:00:00	2011-05-28 10:00:00	2011-03-11T03:43:33.000Z	Qualifying Session	Monte Carlo	UTC
2011-05-28 20:00:00	2011-05-29 20:00:00	2011-05-09T22:05:34.000Z	John F. Kennedy's Birthday		UTC
2011-05-29 08:00:00	2011-05-29 10:00:00	2011-03-11T03:43:30.000Z	Monaco Grand Prix	Monte Carlo	UTC
2011-05-29 20:00:00	2011-05-30 20:00:00	2011-05-09T22:05:34.000Z	Memorial Day		UTC
2011-06-10 10:00:00	2011-06-10 12:00:00	2011-03-11T03:43:39.000Z	First Practice Session	Montreal	UTC
2011-06-10 14:00:00	2011-06-10 16:00:00	2011-03-11T03:43:39.000Z	Second Practice Session	Montreal	UTC
2011-06-11 10:00:00	2011-06-11 11:00:00	2011-03-11T03:43:39.000Z	Third Practice Session	Montreal	UTC
2011-06-11 13:00:00	2011-06-11 15:00:00	2011-03-11T03:43:33.000Z	Qualifying Session	Montreal	UTC
2011-06-12 13:00:00	2011-06-12 15:00:00	2011-03-11T03:43:35.000Z	Canadian Grand Prix	Montreal	UTC
2011-06-13 20:00:00	2011-06-14 20:00:00	2011-05-09T22:05:34.000Z	Flag Day		UTC
2011-06-18 20:00:00	2011-06-19 20:00:00	2011-05-09T22:05:34.000Z	Father's Day		UTC
2011-06-24 04:00:00	2011-06-24 06:00:00	2011-03-11T03:43:34.000Z	First Practice Session	Valencia, Spain	UTC
2011-06-24 08:00:00	2011-06-24 10:00:00	2011-03-11T03:43:34.000Z	Second Practice Session	Valencia, Spain	UTC
2011-06-25 05:00:00	2011-06-25 06:00:00	2011-03-11T03:43:34.000Z	Third Practice Session	Valencia, Spain	UTC
2011-06-25 08:00:00	2011-06-25 10:00:00	2011-03-11T03:43:25.000Z	Qualifying Session	Valencia, Spain	UTC
2011-06-26 08:00:00	2011-06-26 10:00:00	2011-03-11T03:43:30.000Z	European Grand Prix	Valencia, Spain	UTC
2011-07-03 20:00:00	2011-07-04 20:00:00	2011-05-09T22:05:34.000Z	Independence Day		UTC
2011-07-08 05:00:00	2011-07-08 07:00:00	2011-03-11T03:43:29.000Z	First Practice Session	Silverstone, England	UTC
2011-07-08 09:00:00	2011-07-08 11:00:00	2011-03-11T03:43:30.000Z	Second Practice Session	Silverstone, England	UTC
2011-07-09 05:00:00	2011-07-09 06:00:00	2011-03-11T03:43:35.000Z	Third Practice Session	Silverstone, England	UTC
2011-07-09 08:00:00	2011-07-09 10:00:00	2011-03-11T03:43:38.000Z	Qualifying Session	Silverstone, England	UTC
2011-07-10 08:00:00	2011-07-10 10:00:00	2011-03-11T03:43:27.000Z	British Grand Prix	Silverstone, England	UTC
2011-07-22 04:00:00	2011-07-22 06:00:00	2011-03-11T03:43:38.000Z	First Practice Session	N 체 rburgring	UTC
2011-07-22 08:00:00	2011-07-22 10:00:00	2011-03-11T03:43:38.000Z	Second Practice Session	N 체 rburgring	UTC
2011-07-23 05:00:00	2011-07-23 06:00:00	2011-03-11T03:43:25.000Z	Third Practice Session	N 체 rburgring	UTC
2011-07-23 08:00:00	2011-07-23 10:00:00	2011-03-11T03:43:36.000Z	Qualifying Session	N 체 rburgring	UTC
2011-07-24 08:00:00	2011-07-24 10:00:00	2011-03-11T03:43:38.000Z	German Grand Prix	N 체 rburgring	UTC
2011-07-29 04:00:00	2011-07-29 06:00:00	2011-03-11T03:43:39.000Z	First Practice Session	Budapest	UTC
2011-07-29 08:00:00	2011-07-29 10:00:00	2011-03-11T03:43:38.000Z	Second Practice Session	Budapest	UTC
2011-07-30 05:00:00	2011-07-30 06:00:00	2011-03-11T03:43:37.000Z	Third Practice Session	Budapest	UTC
2011-07-30 08:00:00	2011-07-30 10:00:00	2011-03-11T03:43:36.000Z	Qualifying Session	Budapest	UTC
2011-07-31 08:00:00	2011-07-31 10:00:00	2011-03-11T03:43:31.000Z	Hungarian Grand Prix	Budapest	UTC
2011-08-26 04:00:00	2011-08-26 06:00:00	2011-03-11T03:43:35.000Z	First Practice Session	Spa-Francorchamps	UTC
2011-08-26 08:00:00	2011-08-26 10:00:00	2011-03-11T03:43:35.000Z	Second Practice Session	Spa-Francorchamps	UTC
2011-08-27 05:00:00	2011-08-27 06:00:00	2011-03-11T03:43:35.000Z	Third Practice Session	Spa-Francorchamps	UTC
2011-08-27 08:00:00	2011-08-27 10:00:00	2011-03-11T03:43:39.000Z	Qualifying Session	Spa-Francorchamps	UTC

2011-08-28 08:00:00	2011-08-28 10:00:00	2011-03-11T03:43:39.000Z	Belgian Grand Prix	Spa-Francorchamps	UTC
2011-09-04 20:00:00	2011-09-05 20:00:00	2011-05-09T22:05:34.000Z	Labor Day		UTC
2011-09-09 04:00:00	2011-09-09 06:00:00	2011-03-11T03:43:28.000Z	First Practice Session	Monza	UTC
2011-09-09 08:00:00	2011-09-09 10:00:00	2011-03-11T03:43:28.000Z	Second Practice Session	Monza	UTC
2011-09-10 05:00:00	2011-09-10 06:00:00	2011-03-11T03:43:36.000Z	Third Practice Session	Monza	UTC
2011-09-10 08:00:00	2011-09-10 10:00:00	2011-03-11T03:43:33.000Z	Qualifying Session	Monza	UTC
2011-09-10 20:00:00	2011-09-11 20:00:00	2011-05-09T22:05:34.000Z	Patriot Day		UTC
2011-09-11 08:00:00	2011-09-11 10:00:00	2011-03-11T03:43:36.000Z	Italian Grand Prix	Monza	UTC
2011-09-23 06:00:00	2011-09-23 08:00:00	2011-03-11T03:43:37.000Z	First Practice Session	Singapore	UTC
2011-09-23 09:30:00	2011-09-23 11:30:00	2011-03-11T03:43:36.000Z	Second Practice Session	Singapore	UTC
2011-09-24 07:00:00	2011-09-24 08:00:00	2011-03-11T03:43:32.000Z	Third Practice Session	Singapore	UTC
2011-09-24 10:00:00	2011-09-24 12:00:00	2011-03-11T03:43:29.000Z	Qualifying Session	Singapore	UTC
2011-09-25 08:00:00	2011-09-25 10:00:00	2011-03-11T03:43:35.000Z	Singapore Grand Prix	Singapore	UTC
2011-10-06 21:00:00	2011-10-06 23:00:00	2011-03-11T03:43:38.000Z	First Practice Session	Suzuka	UTC
2011-10-07 01:00:00	2011-10-07 03:00:00	2011-03-11T03:43:38.000Z	Second Practice Session	Suzuka	UTC
2011-10-07 22:00:00	2011-10-07 23:00:00	2011-03-11T03:43:37.000Z	Third Practice Session	Suzuka	UTC
2011-10-08 01:00:00	2011-10-08 03:00:00	2011-03-11T03:43:36.000Z	Qualifying Session	Suzuka	UTC
2011-10-09 02:00:00	2011-10-09 04:00:00	2011-03-11T03:43:31.000Z	Japanese Grand Prix	Suzuka	UTC
2011-10-09 20:00:00	2011-10-10 20:00:00	2011-05-09T22:05:34.000Z	Columbus Day		UTC
2011-10-13 21:00:00	2011-10-13 23:00:00	2011-03-11T03:43:35.000Z	First Practice Session	Yeongam	UTC
2011-10-14 01:00:00	2011-10-14 03:00:00	2011-03-11T03:43:35.000Z	Second Practice Session	Yeongam	UTC
2011-10-14 22:00:00	2011-10-14 23:00:00	2011-03-11T03:43:36.000Z	Third Practice Session	Yeongam	UTC
2011-10-15 01:00:00	2011-10-15 03:00:00	2011-03-11T03:43:35.000Z	Qualifying Session	Yeongam	UTC
2011-10-16 02:00:00	2011-10-16 04:00:00	2011-03-11T03:43:27.000Z	Korean Grand Prix	Yeongam	UTC
2011-10-30 20:00:00	2011-10-31 20:00:00	2011-05-09T22:05:34.000Z	Halloween		UTC
2011-11-05 20:00:00	2011-11-06 20:00:00	2011-05-09T22:05:34.000Z	Daylight Saving Time Ends		UTC
2011-11-07 20:00:00	2011-11-08 20:00:00	2011-05-09T22:05:34.000Z	Election Day		UTC
2011-11-10 20:00:00	2011-11-11 20:00:00	2011-05-09T22:05:34.000Z	Veterans Day		UTC
2011-11-11 05:00:00	2011-11-11 07:00:00	2011-03-11T03:43:31.000Z	First Practice Session	Yas Marina	UTC
2011-11-11 09:00:00	2011-11-11 11:00:00	2011-03-11T03:43:32.000Z	Second Practice Session	Yas Marina	UTC
2011-11-12 06:00:00	2011-11-12 07:00:00	2011-03-11T03:43:36.000Z	Third Practice Session	Yas Marina	UTC
2011-11-12 09:00:00	2011-11-12 11:00:00	2011-03-11T03:43:28.000Z	Qualifying Session	Yas Marina	UTC
2011-11-13 09:00:00	2011-11-13 11:00:00	2011-03-11T03:43:34.000Z	Abu Dhabi Grand Prix	Yas Marina	UTC
2011-11-23 20:00:00	2011-11-24 20:00:00	2011-05-09T22:05:34.000Z	Thanksgiving		UTC
2011-11-25 08:00:00	2011-11-25 10:00:00	2011-03-11T03:43:33.000Z	First Practice Session	Sao Paulo	UTC
2011-11-25 12:00:00	2011-11-25 14:00:00	2011-03-11T03:43:33.000Z	Second Practice Session	Sao Paulo	UTC
2011-11-26 09:00:00	2011-11-26 10:00:00	2011-03-11T03:43:26.000Z	Third Practice Session	Sao Paulo	UTC
2011-11-26 12:00:00	2011-11-26 14:00:00	2011-03-11T03:43:37.000Z	Qualifying Session	Sao Paulo	UTC
2011-11-27 12:00:00	2011-11-27 14:00:00	2011-03-11T03:43:26.000Z	Brazilian Grand Prix	Sao Paulo	UTC
2011-12-23 20:00:00	2011-12-24 20:00:00	2011-05-09T22:05:34.000Z	Christmas Eve		UTC
2011-12-24 20:00:00	2011-12-25 20:00:00	2011-05-09T22:05:34.000Z	Christmas		UTC
2011-12-30 20:00:00	2011-12-31 20:00:00	2011-05-09T22:05:34.000Z	New Year's Eve		UTC
2011-12-31 20:00:00	2012-01-01 20:00:00	2011-05-09T22:05:34.000Z	New Year's Day		UTC
2012-01-15 20:00:00	2012-01-16 20:00:00	2011-05-09T22:05:34.000Z	Martin Luther King, Jr's Day		UTC
2012-02-01 20:00:00	2012-02-02 20:00:00	2011-05-09T22:05:34.000Z	Groundhog Day		UTC
2012-02-11 20:00:00	2012-02-12 20:00:00	2011-05-09T22:05:34.000Z	Lincoln's Birthday		UTC
2012-02-13 20:00:00	2012-02-14 20:00:00	2011-05-09T22:05:34.000Z	Valentine's Day		UTC
2012-02-19 20:00:00	2012-02-20 20:00:00	2011-05-09T22:05:34.000Z	Presidents Day		UTC
2012-03-10 20:00:00	2012-03-11 20:00:00	2011-05-09T22:05:34.000Z	Daylight Saving Time Begins		UTC
2012-03-16 20:00:00	2012-03-17 20:00:00	2011-05-09T22:05:34.000Z	St. Patrick's Day		UTC
2012-03-31 20:00:00	2012-04-01 20:00:00	2011-05-09T22:05:34.000Z	April Fool's Day		UTC
2012-04-07 20:00:00	2012-04-08 20:00:00	2011-05-09T22:05:34.000Z	Easter		UTC
2012-04-14 20:00:00	2012-04-15 20:00:00	2011-05-09T22:05:34.000Z	Tax Day		UTC

2012-04-21 20:00:00	2012-04-22 20:00:00	2011-05-09T22:05:34.000Z	Earth Day		UTC
2012-05-04 20:00:00	2012-05-05 20:00:00	2011-05-09T22:05:34.000Z	Cinco de Mayo		UTC
2012-05-12 20:00:00	2012-05-13 20:00:00	2011-05-09T22:05:34.000Z	Mother's Day		UTC
2012-05-27 20:00:00	2012-05-28 20:00:00	2011-05-09T22:05:34.000Z	Memorial Day		UTC
2012-05-28 20:00:00	2012-05-29 20:00:00	2011-05-09T22:05:34.000Z	John F. Kennedy's Birthday		UTC
2012-06-13 20:00:00	2012-06-14 20:00:00	2011-05-09T22:05:34.000Z	Flag Day		UTC
2012-06-16 20:00:00	2012-06-17 20:00:00	2011-05-09T22:05:34.000Z	Father's Day		UTC
2012-07-03 20:00:00	2012-07-04 20:00:00	2011-05-09T22:05:34.000Z	Independence Day		UTC
2012-09-02 20:00:00	2012-09-03 20:00:00	2011-05-09T22:05:34.000Z	Labor Day		UTC
2012-09-10 20:00:00	2012-09-11 20:00:00	2011-05-09T22:05:34.000Z	Patriot Day		UTC
2012-10-07 20:00:00	2012-10-08 20:00:00	2011-05-09T22:05:34.000Z	Columbus Day		UTC
2012-10-30 20:00:00	2012-10-31 20:00:00	2011-05-09T22:05:34.000Z	Halloween		UTC
2012-11-03 20:00:00	2012-11-04 20:00:00	2011-05-09T22:05:34.000Z	Daylight Saving Time Ends		UTC
2012-11-05 20:00:00	2012-11-06 20:00:00	2011-05-09T22:05:34.000Z	Election Day		UTC
2012-11-10 20:00:00	2012-11-11 20:00:00	2011-05-09T22:05:34.000Z	Veterans Day		UTC
2012-11-21 20:00:00	2012-11-22 20:00:00	2011-05-09T22:05:34.000Z	Thanksgiving		UTC
2012-12-23 20:00:00	2012-12-24 20:00:00	2011-05-09T22:05:34.000Z	Christmas Eve		UTC
2012-12-24 20:00:00	2012-12-25 20:00:00	2011-05-09T22:05:34.000Z	Christmas		UTC
2012-12-30 20:00:00	2012-12-31 20:00:00	2011-05-07T11:20:39.000Z	New Year's Eve		UTC
2012-12-31 20:00:00	2013-01-01 20:00:00	2011-05-07T11:20:39.000Z	New Year's Day		UTC
2013-01-20 20:00:00	2013-01-21 20:00:00	2011-05-07T11:20:39.000Z	Martin Luther King, Jr's Day		UTC
2013-02-01 20:00:00	2013-02-02 20:00:00	2011-05-07T11:20:39.000Z	Groundhog Day		UTC
2013-02-11 20:00:00	2013-02-12 20:00:00	2011-05-07T11:20:39.000Z	Lincoln's Birthday		UTC
2013-02-13 20:00:00	2013-02-14 20:00:00	2011-05-07T11:20:39.000Z	Valentine's Day		UTC
2013-02-17 20:00:00	2013-02-18 20:00:00	2011-05-07T11:20:39.000Z	Presidents Day		UTC
2013-03-09 20:00:00	2013-03-10 20:00:00	2011-05-07T11:20:39.000Z	Daylight Saving Time Begins		UTC
2013-03-16 20:00:00	2013-03-17 20:00:00	2011-05-07T11:20:39.000Z	St. Patrick's Day		UTC
2013-03-31 20:00:00	2013-04-01 20:00:00	2011-05-07T11:20:39.000Z	April Fool's Day		UTC
2013-04-14 20:00:00	2013-04-15 20:00:00	2011-05-07T11:20:39.000Z	Tax Day		UTC
2013-04-21 20:00:00	2013-04-22 20:00:00	2011-05-07T11:20:39.000Z	Earth Day		UTC
2013-05-04 20:00:00	2013-05-05 20:00:00	2011-05-07T11:20:39.000Z	Cinco de Mayo		UTC
2013-05-11 20:00:00	2013-05-12 20:00:00	2011-05-07T11:20:39.000Z	Mother's Day		UTC
2013-05-26 20:00:00	2013-05-27 20:00:00	2011-05-07T11:20:39.000Z	Memorial Day		UTC
2013-05-28 20:00:00	2013-05-29 20:00:00	2011-05-07T11:20:39.000Z	John F. Kennedy's Birthday		UTC
2013-06-13 20:00:00	2013-06-14 20:00:00	2011-05-07T11:20:39.000Z	Flag Day		UTC
2013-06-15 20:00:00	2013-06-16 20:00:00	2011-05-07T11:20:39.000Z	Father's Day		UTC
2013-07-03 20:00:00	2013-07-04 20:00:00	2011-05-07T11:20:39.000Z	Independence Day		UTC
2013-09-01 20:00:00	2013-09-02 20:00:00	2011-05-07T11:20:39.000Z	Labor Day		UTC
2013-09-10 20:00:00	2013-09-11 20:00:00	2011-05-07T11:20:39.000Z	Patriot Day		UTC
2013-10-13 20:00:00	2013-10-14 20:00:00	2011-05-07T11:20:39.000Z	Columbus Day		UTC
2013-10-30 20:00:00	2013-10-31 20:00:00	2011-05-07T11:20:39.000Z	Halloween		UTC
2013-11-02 20:00:00	2013-11-03 20:00:00	2011-05-07T11:20:39.000Z	Daylight Saving Time Ends		UTC
2013-11-04 20:00:00	2013-11-05 20:00:00	2011-05-07T11:20:39.000Z	Election Day		UTC
2013-11-10 20:00:00	2013-11-11 20:00:00	2011-05-07T11:20:39.000Z	Veterans Day		UTC
2013-11-27 20:00:00	2013-11-28 20:00:00	2011-05-07T11:20:39.000Z	Thanksgiving		UTC
2013-12-23 20:00:00	2013-12-24 20:00:00	2011-05-07T11:20:39.000Z	Christmas Eve		UTC
2013-12-24 20:00:00	2013-12-25 20:00:00	2011-05-07T11:20:39.000Z	Christmas		UTC
2013-12-30 20:00:00	2013-12-31 20:00:00	2011-05-07T11:20:39.000Z	New Year's Eve		UTC
2013-12-31 20:00:00	2014-01-01 20:00:00	2011-05-07T11:20:39.000Z	New Year's Day		UTC
2014-01-19 20:00:00	2014-01-20 20:00:00	2011-05-07T11:20:39.000Z	Martin Luther King, Jr's Day		UTC
2014-02-01 20:00:00	2014-02-02 20:00:00	2011-05-07T11:20:39.000Z	Groundhog Day		UTC
2014-02-11 20:00:00	2014-02-12 20:00:00	2011-05-07T11:20:39.000Z	Lincoln's Birthday		UTC
2014-02-13 20:00:00	2014-02-14 20:00:00	2011-05-07T11:20:39.000Z	Valentine's Day		UTC

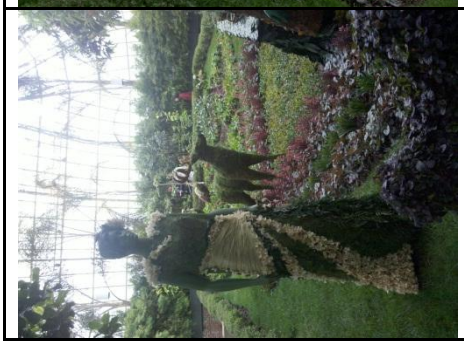
2014-02-16 20:00:00	2014-02-17 20:00:00	2011-05-07T11:20:39.000Z	Presidents Day		UTC
2014-03-08 20:00:00	2014-03-09 20:00:00	2011-05-07T11:20:39.000Z	Daylight Saving Time Begins		UTC
2014-03-16 20:00:00	2014-03-17 20:00:00	2011-05-07T11:20:39.000Z	St. Patrick's Day		UTC
2014-03-31 20:00:00	2014-04-01 20:00:00	2011-05-07T11:20:39.000Z	April Fool's Day		UTC

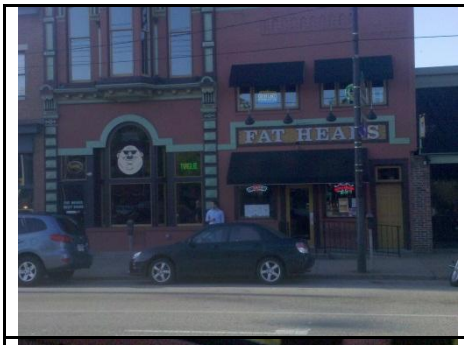
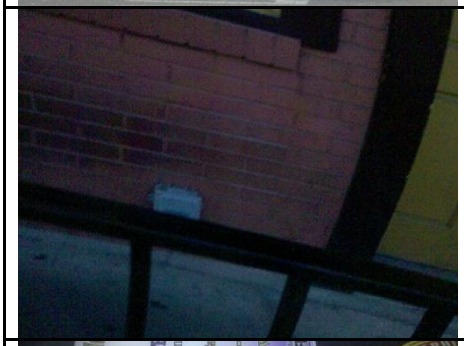
The highlighted part shows the schedule that has an alarm set using UTC-4 time zone (New York with daylight saving).

3.3.20. Scenario 2 - SDCard

The followings are carved in the SDCard of Scenario 2.

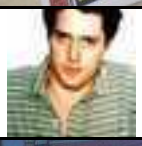
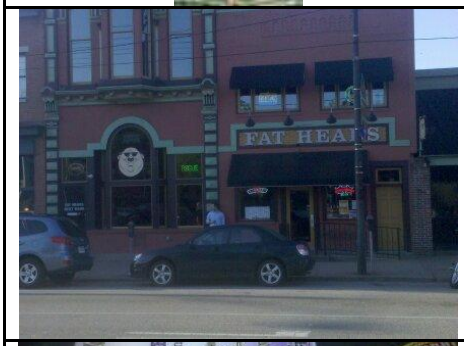
Table 44. Images and PDF files in SDCard of Scenario 2

Files	Type	Embedded Created Time (UTC-4)
	EXIF	2011-05-05 20:13:43
	EXIF	2011-05-06 19:39:35
	EXIF	2011-05-06 19:39:52

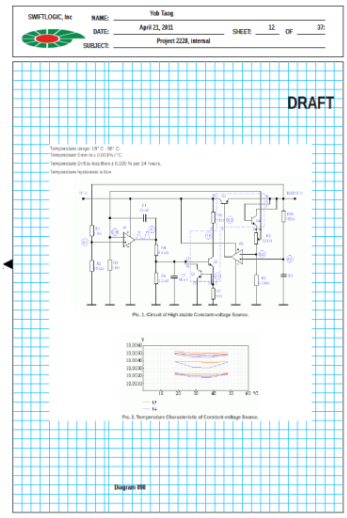
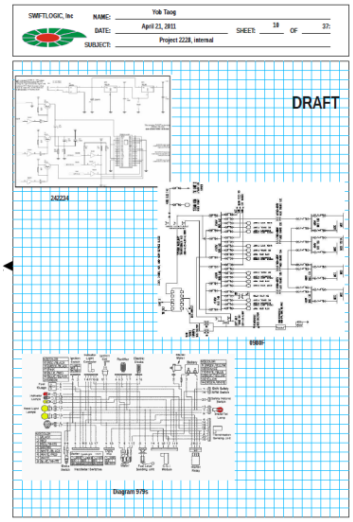
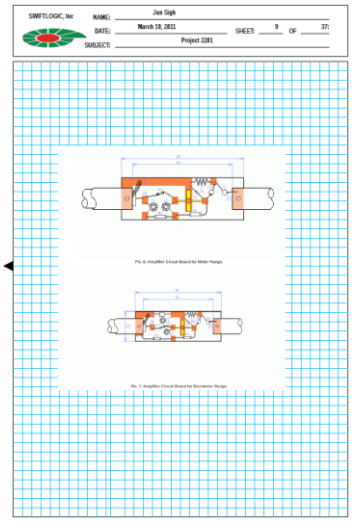
	EXIF	2011-05-05 20:05:07
	EXIF	2011-05-05 20:05:33
	EXIF	2011-05-05 20:47:18
	EXIF	2011-05-05 20:47:35
	EXIF	2011-05-05 20:47:50

	EXIF	2011-05-04 22:00:32
	EXIF	2011-05-05 14:37:47
	EXIF	2011-05-05 20:47:05
	EXIF	2011-05-05 20:48:28
	EXIF	2011-05-06 19:29:21

	JFIF	-
	JFIF	-
	JFIF	-
	JFIF	-
	JFIF	-

	JFIF	-
	JFIF	-
	JFIF	-
	JFIF	-
	JFIF	-

	JFIF	-
	JFIF	-
	JFIF	-
	JFIF	-
	JFIF	-

	PDF	2011-05-06 19:57:52 (Embedded UTC-4)
	PDF	2011-05-07 12:30:23 (Embedded UTC-4)
	PDF	2011-05-07 12:31:01 (Embedded UTC-4)

4. Conclusion

It was confirmed that Scenario 1 (Suspicious Death) and Scenario 2 (Intellectual Property Theft) are closely related.

The main characters are as follow:

Person	Phone Number or Email	Description
Yob Taog	4124393388, yobtaog@gmail.com	VP of Swiftlogic Inc.
Donald Norby	4124393389, norby441@gmail.com	A person who stole the dada using application installed on the Smartphone of Yob Taog
Mr E	4439264768, mre@hushmail.com	Tries to purchase the valuable documents which Donald Norby stole from Yob Taog.
Tim & Bob	swiftlogic@consultant.com, swiftlogicllc@consultant.com, swiftlogicinc@consultant.com	A staff of Swiftlogic Inc.
Reg Wetham	regwetham@yahoo.com	Persons in close relationship with Yob Taog
Luke Lancer	luk3lancer@gmail.com	
Shandra Pfeif	shandra@cheerful.com	

Major events are as follow:

Yob Taog purchased a new Android Smartphone at 2011-05-04 21:43:25 (UTC-4). But, an application to steal the data of the Smartphone of Yob Taog was already (2011-05-04 20:46:27, UTC-4) installed on the Smartphone. Almost simultaneously with the Yob Taog's purchasing the Smartphone, Donald Norby and Mr E exchanged texts each other. It could have been arranged in advance.

Scenario	Date (UTC-4)	Description
S.2	2011-05-04 20:46:27	Performs the first USIM connection and Google ID Setting (Account synchronization) And, installed **com.vzw.smsProvider.apk** and **com.andriod.mm.apk** to steal the data of Yob Taog
S.1	2011-05-04 20:50:22	ksmsvzwsms://message/Service Started
S.1	2011-05-04 21:09:25	Donald Norby → Mr E **Got the perfect Guy, plan is already in motion**
S.1	2011-05-04 21:12:19	Mr E → Donald Norby **Break a leg**
S.2	2011-05-04 21:43:25	tweeted: Yay! Just picked up my **new android smartphone**! !!!
S.2	2011-05-04 22:12:48	Yob Taog tweeted: OMG 10:15 already! Got to get to work early tommorrow, six after working late! **At least Verizon was still open**!

Yob Taog downloaded the documents of Swiftlogic Inc. to the Smartphone through the staff for the purpose of performing his job (meeting).

The application (mm) installed on the Yob Taog's Smartphone has continuously sent the contents of SMS/Call history to the Donald Norby's Smartphone using SMS. It also sent the file existed on the Smartphone to 50.56.29.109. Finally, Donald Norby obtained the valuable documents at 2011-05-08 13:59:28 (UTC-4) through the Yob Taog's smartphone.

Scenario	Date (UTC-4)	Description
S.1	2011-05-06 14:30:26	Donald Norby → Mr E the implementation seems to be working ok, no gold yet though
S.2	2011-05-06 23:11:04	Received PDF files from Tim (Email) (3 files)
S.2	2011-05-07 12:40:49	Received PDF files from Bob (Email) (5 files)
S.1	2011-05-07 21:47:01	Donald Norby → Mr E software seems to be working, I was a little worried given the source and short timeline
S.1	2011-05-08 00:12:16	ksmsvzwsms://message/pkg uploaded! (LAST)
S.1	2011-05-08 00:13:48	Donald Norby → Mr E Got something for you, sample shortly
S.1	2011-05-08 13:59:28~14:02:54	**Download Taog's PDF files from 50.56.29.109 (8 files)**

However, Donald Norby who obtained the valuable documents has changed his mind.

Scenario	Date (UTC-4)	Description
S.1	2011-05-08 14:05:34	Donald Norby → Mr E Got some results, I think we need to up the fee, say double?
S.1	2011-05-08 14:08:38	Donald Norby → Mr E sample - this is just a taste, much more where this came from. (2228-12.pdf)
S.1	2011-05-08 14:16:14	Mr E → Donald Norby **You are joking, right? You can't seriously think about changing the deal now.**
S.1	2011-05-08 14:22:39	Donald Norby → Mr E I just sent you a sample, I think you'll be pleased...
S.1	2011-05-08 14:30:13	Mr E → Donald Norby You are serious then. I can see the information is valuable but **I am displeased with you breaking the deal.**
S.1	2011-05-08 14:32:53	Donald Norby → Mr E showing i'm serious - This information is obviously very valuable. I'd like to keep our relationship, but these will fetch a?
S.1	2011-05-08 14:43:36	Mr E → Donald Norby Re: showing i'm serious - **I certainly don't want you giving these files to someone else. Expect a call from me shortly.**
S.1	2011-05-08 14:46:24	Donald Norby → Mr E Telephone Conversation
S.1	2011-05-08 14:56:44	Donald Norby → Mr E **I knew you'd like them, ill be at the agreed spot, in about 25 min for the exchange**

Since 2011-05-08 14:56:44 (UTC-4), there hasn't been any history of talking between Donald Norby and Mr E. We also analyzed the record containing the SMS history data and found that Donald Norby could not read any message delivered to him after 2011-05-08 14:56:44 (UTC-4).

Since then, Yob Taog still has continued his normal life, such as going to the airport (Pittsburgh International Airport) or going to the baseball field at the Federal Street Pittsburg.

Scenario	Date (UTC-4)	Description
S.2	2011-05-08 18:39:17	Terminal C in Pittsburgh International Airport
S.2	2011-05-10 20:38:39	Search : 115 Federal Street Pittsburgh, PA 15212-5740

As a result, valuable documents of the company, SwiftLogic, have been leaked by two malicious apps that are installed on the smartphone of Yob Taog. He did not leak the data directly, but because he received some confidential files by e-mail on his smartphone, he became a source of data leakage.

Donald Norby seems to go to the agreed spot to sell the valuable documents from Yob Taog.

Donald Norby's message

→ **I knew you'd like them, ill be at the agreed spot, in about 25 min for the exchange**

However, after that, the traces such as SMS and e-mail did not exist in the Donald Norby's smartphone. In addition, Donald Norby could not read any message delivered to him after 2011-05-08 14:56:44 (UTC-4). Therefore, it looks like the Donald Norby has been killed by Mr E on the agreed spot for the exchange.

5. Further Research

Through this case, we have succeeded in recovering records using the SQLite page analysis. We also reconstructed YAFFS2 file system, which is different from the general form of file system. We checked and found that there is a possibility to utilize it not only for the record recovery of a server-type DB server as well as SQLite. We are planning to further develop this result and do research to make the DB recovery possible in an enterprise environment.

6. Acknowledgments

This work was supported by the IT R&D program of MKE/KEIT [10035157, Development of Digital Forensic Technologies for Real-Time Analysis] and Bio R&D program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (20100020634).

Special Thanks To:

Professor Jongin Lim, the director of Center for Information Security Technologies (CIST) who gives the full support to perform the researches on Digital Forensics, Professor Sangjin Lee, the executive director of Digital Forensic Research Center (DFRC) who set the research direction and supervises us in many ways, and Professor Seokhie Hong, Thank you for your supports, helps and enthusiasm.

7. References

[1] Digital Forensic Research Workshop, URL: http://dfrws.org/2011/challenge
[2] YAFFS official website, 2011, YAFFS official website [Online], URL: http://www.yaffs.net (2011).
[3] YAFFS 2 Specification and Development Notes,
URL: http://www.yaffs.net/yaffs-2-specification-and-development-notes,
[4] An Introduction to NAND flash, 2006, An introduction to NAND flash [Online],
URL: http://www.commsdesign.com/showArticle.jhtml?articleID=183700957 (2006).
[5] SQLite Database File Format, URL: http://www.sqlite.org/
[6] Motorola Droid, URL: http://en.wikipedia.org/wiki/Motorola_Droid
[7] Android Developers, URL: http://developer.android.com/index.html
[8] S. Jeon, J. Bang, K. Byun, S. Lee, Recovery method of Deleted Record for SQLite Database, 2010 FTRA World Convergence Conference, 2010. 12.