Digital Forensics Research Workshop Challenge 2011

Data Analysis

Author: Apurva Rustagi

7/24/2011

Contents

1 Introduction

The Digital Forensics Research Workshop (DFRWS) is a non-profit, volunteer organization dedicated to the sharing of knowledge and ideas about digital forensics research. DFRWS organizes an annual challenge to encourage and drive research and development in that domain. The DFRWS challenge is well known among forensics community and has lead to many technical advances and tools for digital forensic investigations.

To solve this challenge, some customized tools were created in C. These tools were used to carve out information from SQLite databases and other records like SMS and browsing history. The details about how these tools work and concept behind them is explained in the accompanying document "Technical Analysis.pdf"

1.1 Challenge Background

Given the variety and impending ubiquity of Android devices along with the wide range of crimes that can involve these systems as a source of evidence, this year's challenge was based on mobile phones running on Android operating system. The challenge had the following two scenarios:

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 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: 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.

1.2 Challenge Data

To investigate the two scenarios, the flash storage and SD card memory dump from the respective devices were provided:

Case	File	SHA hash
Suspicious Death	Case1.tgz	9a756c41cbd3b628fb55d35e695efdee31efa58e
Intellectual Property Theft	Case2.tgz	17bd6109410a0c57439aa8e701354a5f1dfd4ab3

2 Executive Summary

It was found that the two scenarios given in the challenge are related. Mr. Yob Taog (Taog) got his new android phone through Mr. Donald Norby (Norby). Norby had planted malicious software in Taog's phone which regularly sent messages and uploaded pdf files on the server with IP address 50.56.29.109. The intent of planting this malicious software was to get confidential intellectual property documents of SwiftLogic Inc.

Norby had struck a deal with Mr E for passing SwiftLogic documents. But Norby asked for a better a deal after getting hold of the documents. This was not liked by Mr. E but he still agreed to meet Norby at the exchange. This was indicated in an SMS by Mr. E. However this was last SMS read on Norby's phone, suggesting Norby's death after meeting with Mr. E.

3 Acquisition and Verification of Memory Dumps

The acquisition methods for devices in the two scenarios were different. Flash memory from the phone was captured using dd in the first scenario and nanddump in the second scenario. However the device has to be rooted and “android debug bridge” has to be enabled in both the scenarios for access to the flash memory.

This rooting process is clearly logged by Mr. Keith Jones in file acquisition.log for scenario 1. Following rooting process, the SD card was imaged. However, it could have been possible to image the SD card before rooting. This would have saved the SD card from dumping of any possible logs for the rooting process. After the acquisition of SD card, flash memory of the phone was dumped using dd tool. The dd tool ignores the OOB data of 64 bytes occurring after every 128 KB. Hence, the metadata, which is necessary to reconstruct the logical YAFFS file system, is not captured when using dd tool.

Mr. Keith Jones was not able to verify the hashes of data from the phone to the SD Card. This can be done using the busybox toolkit which has been compiled for the ARM platform. The busybox toolkit can be installed on “system” partition of the phone because this area of the phone does not contain any user data. However the post acquisition hashes were verified before starting any analysis.

Image	Post Acquisition Hashes (MD5)	Verification hashes (MD5)
mtdblock0.img	10f39bed760d85980117a29364feeeb1	10F39BED760D85980117A29364FEEEB1
mtdblock1.img	5dfd83e314d645c6f41d86915a7b98eb	5DFD83E314D645C6F41D86915A7B98EB
mtdblock3.img	7673f7ef637274d6bb48892a157d877d	7673F7EF637274D6BB48892A157D877D
mtdblock4.img	fa503c91751afccf175092a29a2b2637	FA503C91751AFCCF175092A29A2B2637
mtdblock5.img	ade41709773a63a4ed09d66f3a7637cd	ADE41709773A63A4ED09D66F3A7637CD
mtdblock6.img	0f1a515a89e2a368aff3fcd818bcab94	0F1A515A89E2A368AFF3FCD818BCAB94
mtdblock7.img	b23b5d09162b92c0284923a7f628d2a5	B23B5D09162B92C0284923A7F628D2A5
SDCard.img	fdeb635287893022ff807c7dc18a74c6	FDEB635287893022FF807C7DC18A74C6

In the second scenario, the collection process was not done and logged in as detailed manner as in scenario 1. The process missed capturing many important details. It first did not capture the nature of partitions as done in scenario 1 using “mount” command in abd shell. The acquisition was done using nanddump and transfer both of which are not available natively on android. Hence their installation details should have been captured. Nanddump tool, unlike dd, captures OOB data too. However, nandread tool which also captures OOB data and is available natively on Android OS should have been used.

The agent, in the second case also missed calculating hash for memory image of mtd3. The remaining hashes were verified before starting any analysis.

Image	Post Acquisition Hashes (SHA1)	Verification hashes (SHA1)
mtd0.dd	**160433772347c94bd3abc89952677942d423515b**	**160433772347C94BD3ABC89952677942D423515B**
mtd1.dd	**81d32137cc3a35e535dfa8a706981d4494267e7a**	**81D32137CC3A35E535DFA8A706981D4494267E7A**
mtd2.dd	**97f2383facfc8c8319e6725674d5912fc91f04fa**	**97F2383FACFC8C8319E6725674D5912FC91F04FA**
mtd3.dd	**NA**	**B22A6C5B8248B0B3BCF760305F69F4AF68B1BAC4**
mtd4.dd	**f3af16c8659958f34eb4e3e6f585c3f0058f6bc6**	**F3AF16C8659958F34EB4E3E6F585C3F0058F6BC6**
mtd5.dd	**83bbe12bf2e4ae455486a7c6c1e6044b53526149**	**83BBE12BF2E4AE455486A7C6C1E6044B53526149**
mtd6.dd	**45d2bd8b6a571dddfb13ccf7c3f3134af15ca084**	**45D2BD8B6A571DDDFB13CCF7C3F3134AF15CA084**
mtd7.dd	**e238dd5998ce26c6566bc4747bc8ff1cd7c1f0bc**	**E238DD5998CE26C6566BC4747BC8FF1CD7C1F0BC**
mtd8.dd	**339b6cfcffcc1206ca75069d3f1cc7205d5d6be4**	**339B6CFCFFCC1206CA75069D3F1CC7205D5D6BE4**
mtd9.dd	**4e71e3894203e64ff5201f692510afdafb4c08b7**	**4E71E3894203E64FF5201F692510AFDAFB4C08B7**
sdcard.dd	**491a0688a4733c36c2a24cfc8b9023c0 (MD5)**	**491A0688A4733C36C2A24CFC8B9023C0 (MD5)**

4 Data correlation

This section presents the correlation which was made between all the evidence in order to answer the challenge questions. Most of the relevant data for this case is provided in the appendix. To retrieve the full data, use the different tools provided with this paper and read, if necessary, the technical paper to understand how tools work.

4.1 Evidence suggesting Norby's search for Swiftlogic employees

Browsing history on Norby's phone suggested that he was looking out for SwiftLogic employees to carry out his plan of stealing SwiftLogic intellectual property documents. The browsing history can be seen in file Case1_Internet_History.xls.

4.2 Evidence on Norby's phone connecting him to Mr. E and Yob Taog

Norby had following two contacts stored on his phone. This clearly suggested that Donald Norby explicitly tried to communicate with Yob Taog. Following contacts were found on his phone:

Name	Email	Phone
mr e	mre@hushmail.com	4439264768
Taog		4124393388
Mr E		443-926-4768

Taog's number has the area code 412 which corresponds to Pittsburgh, Pennsylvania region mentioned in Yob Taog's Facebook profile.

4.3 Norby talking about the malicious software

Following phrase and a text message to Mr. E were recovered from Norby's phone where he talks about the implementation and working of the malicious software.

Software seems to be working, I was a little worried given the source and short timeline
the implementation seems to be working ok, no gold yet though

4.4 Functioning of malicious software

The malicious software forwarded the SMS on Taog's phone to Norby's phone. It also periodically checked the files available and sent notifications whenever something was uploaded on the server. Following sample SMSes on Norby's phone demonstrate this function:

ksmsvzwsms://message/Service Started
ksmsvzwsms://message/May 4, 2011 8:50:12 PM EDT
ksmsvzwsms://message/pkg uploaded!
ksmsFORWARDED SMS from 6245 at 20110505T173426America/New_York(4,124,-14400,1,1304631266) :shandra@cheerful.com (Nearby! Coming for my beer) Hey Yob, I am closi
ksmsng in on Fat Heads. See ya soon.

4.5 Norby's access to webserver 50.56.29.109

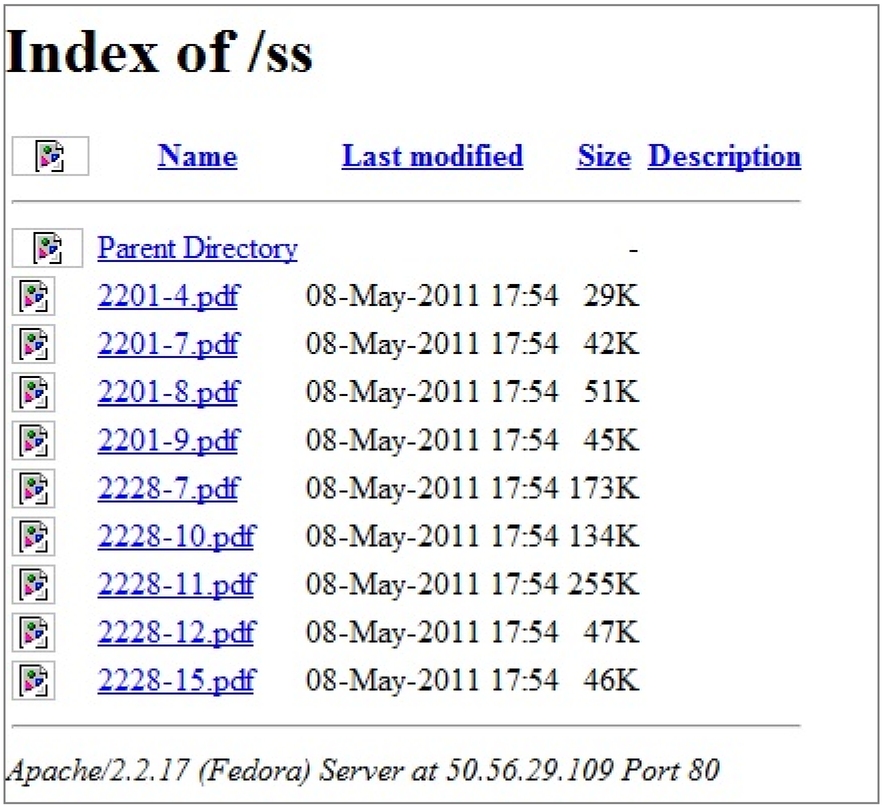
Norby accessed the server 50.56.29.109 for downloading the pdf files uploaded from Taog's phone through the malware. Following are the URL recovered from the browser history:

Title	URL	Unix Time	GMT Time
http://50.56.29.109/ss/	http://50.56.29.109/ss/	012fd0c3924c	8th May 2011 17:59:28
Index of /ss	http://50.56.29.109/ss/	012fd0ddc46f	8th May 2011 18:28:05

The access to this server is password protected and the credentials were recovered as below:

Username	norby
Password	aaassspp

HTML pages were also recovered from Norby's phone showing access to the web server.



Index of /ss

Name	Last modified	Size	Description
Parent Directory		-	
2201-4.pdf	08-May-2011 17:54	29K	
2201-7.pdf	08-May-2011 17:54	42K	
2201-8.pdf	08-May-2011 17:54	51K	
2201-9.pdf	08-May-2011 17:54	45K	
2228-7.pdf	08-May-2011 17:54	173K	
2228-10.pdf	08-May-2011 17:54	134K	
2228-11.pdf	08-May-2011 17:54	255K	
2228-12.pdf	08-May-2011 17:54	47K	
2228-15.pdf	08-May-2011 17:54	46K	

Apache/2.2.17 (Fedora) Server at 50.56.29.109 Port 80

4.6 Evidence from downloads.db

URL	Filename	Local storage	Unix Time
http://@50.56.29.109:80/ss/2201-4.pdf	2201-4.pdf	/sdcard/download/2201-4.pdf	012FD0C3F66B
http://@50.56.29.109:80/ss/2201-7.pdf	2201-7.pdf	/sdcard/download/2201-7.pdf	012FD0C451D8
http://@50.56.29.109:80/ss/2201-8.pdf	2201-8.pdf	/sdcard/download/2201-8.pdf	012FD0C5509B
http://@50.56.29.109:80/ss/2201-9.pdf	2201-9.pdf	/sdcard/download/2201-9.pdf	012FD0C51252
http://@50.56.29.109:80/ss/2228-10.pdf	2228-10.pdf	/sdcard/download/2228-10.pdf	012FD0C5D89D
http://@50.56.29.109:80/ss/2228-11.pdf	2228-11.pdf	/sdcard/download/2228-11.pdf	012FD0C63288
http://@50.56.29.109:80/ss/2228-12.pdf	2228-12.pdf	/sdcard/download/2228-12.pdf	012FD0C65BA5
http://@50.56.29.109:80/ss/2228-15.pdf	2228-15.pdf	/sdcard/download/2228-15.pdf	012FD0C6AC58
http://@50.56.29.109:80/ss/2228-7.pdf	2228-7.pdf	/sdcard/download/2228-7.pdf	012FD0C5B367

The actual pdf files were also found on the SD Card in the Norby's phone. Following are the details of the pdf files found on the SD Card.

File	Created	Modified	Accessed
2201-4.pdf	5/8/2011 13:59:56	5/8/2011 13:59:56	5/8/2011
2201-7.pdf	5/8/2011 14:00:18	5/8/2011 14:00:18	5/8/2011
2201-9.pdf	5/8/2011 14:01:08	5/8/2011 14:01:08	5/8/2011
2201-8.pdf	5/8/2011 14:01:22	5/8/2011 14:01:22	5/8/2011
2228-7.pdf	5/8/2011 14:01:47	5/8/2011 14:01:46	5/8/2011
2228-10.pdf	5/8/2011 14:01:57	5/8/2011 14:01:56	5/8/2011
2228-11.pdf	5/8/2011 14:02:20	5/8/2011 14:02:20	5/8/2011
2228-12.pdf	5/8/2011 14:02:33	5/8/2011 14:02:32	5/8/2011
2228-15.pdf	5/8/2011 14:02:54	5/8/2011 14:02:54	5/8/2011

4.7 Communication between Norby and Mr. E regarding SwiftLogic documents

After downloading the PDF files, Norby informed Mr. E about the result and asked him for a better deal. Following SMS was sent by Norby to Mr. E.

Sender	Receiver	Content
Norby	Mr. E	Got some results, I think we need to up the fee, say double?
Mr. E	Norby	You are joking, right? You can't seriously think about changing the deal now.
Norby	Mr. E	I just sent you a sample, I think you'll be pleased...

Norby then sent a following mail as a sample with 2228-12.pdf in attachment.

From	To	Subject	Messages	Attachment
norby441@gmail.com	mre@hushmail.com	Sample	This is just a taste. Much more where this came from. N.	2228-12.pdf

To demonstrate his seriousness, Norby sent another mail containing some more files.

Subject	Message	Attachment
showing i'm serious	This information is obviously very valuable. I'd like to keep our relationship, but others would be willing to pay much more. Here are some more files to show my good faith. Let me know.	2201-4.pdf 2201-7.pdf 2228-15.pdf 2201-8.pdf 2228-10.pdf

Mr. E was displeased with Norby for asking to double the deal but he still agreed to meet him at a fixed place.

Sender	Receiver	Message
Mr. E	Norby	You are serious then. I can see the information is valuable but I am displeased with you breaking the deal.
Norby	Mr. E	I knew you'd like them, ill be at the agreed spot, in about 25 min for the exchange.

The above message from Mr. E was the last read message that was recovered from Norby's phone. Several unread messages received thereafter were recovered which is according to the description mentioned in the scenario.

4.8 Evidence on Taog's phone

No evidence was found that would suggest any explicit communication by Taog with Norby. Hence it could not be established that Taog intentionally leaked SwiftLogic's intellectual property documents.

A following extract of the malware which has mention of server IP address "50.56.29.109" was recovered from the Taog's phone.

```
Number: _  files!_          , ignored__,,,__/_50.56.29.109__<clinit>__<init>__Adding: __BUFFER_ BUFSIZE__CallIn__CallIn: _ CallOut_          CallOut:
__Compress__D:_
DEFAULTHOST_
DEFAULTPORT__ERROR__EXTRA_STATE_RINGING__Ended__Ended!__Error closing downstream __Error closing upstream _
Exception __F:__FILENAME__FNF__File not found__FileStreamSink.java__HOUR__I__IL__ILII__ILL__J__L__LI__LII__LJ__LL__LLI__LLL__LLLI_
LOG_TAG__Landroid/app/Service;_#Landroid/content/BroadcastReceiver;__Landroid/content/ComponentName;__Landroid/content/Context;__Landroid/conten
t/Intent;__Landroid/net/Uri;__Landroid/os/Bundle;__Landroid/os/Environment;__Landroid/os/Handler;__Landroid/os/IBinder;_$Landroid/telephony/Telephony
Manager;__Landroid/util/Log;__Landroid/widget/Toast;_2Lcom/andriod/lib/io/streamProvider/StreamProvider;_>Lcom/andriod/lib/io/streamProvider/StreamPro
viderSynchronizer;_.Lcom/andriod/lib/io/streamProvider/StreamSink;_0Lcom/andriod/lib/io/streamProvider/StreamSource;_6Lcom/andriod/lib/io/streamProvider
/StreamSynchronizer;_7Lcom/andriod/lib/io/streamProvider/impl/FileStreamSink;_:Lcom/andriod/lib/io/streamProvider/impl/PlainStreamSource;_>Lcom/andrio
d/lib/io/streamProvider/impl/ProcessStreamProvider;_=Lcom/andriod/lib/io/streamProvider/impl/SocketStreamProvider;_ALcom/andriod/lib/io/streamProvider/i
mpl/StandardIOStreamProvider;__Lcom/andriod/lib/log/Log;__Lcom/andriod/lib/log/Logger;__Lcom/andriod/lib/zipper;__Lcom/andriod/mm/R$attr;__Lcom/an
driod/mm/R$drawable;__Lcom/andriod/mm/R$layout;__Lcom/andriod/mm/R$string;__Lcom/andriod/mm/R;__Lcom/andriod/mm/bootComp;__Lcom/andriod/m
m/callIn;__Lcom/andriod/mm/callOut;__Lcom/andriod/mm/mediaMounter$1;__Lcom/andriod/mm/mediaMounter;_"Ldalvik/annotation/EnclosingClass;__Ldalv
ik/annotation/InnerClass;_!Ldalvik/annotation/MemberClasses;__Ldalvik/annotation/Throws;__Ljava/io/BufferedInputStream;__Ljava/io/BufferedOutputStream;
__Ljava/io/ByteArrayInputStream;__Ljava/io/ByteArrayOutputStream;__Ljava/io/Closeableÿÿiz__‹___ ____________________ÿÿÿÿÿÿÿÿÿÿ-
ÝÁ>ð/Ð´¾¾ÿÿÿÿÿÿÿÿÿÿÿÿÿ;__Ljava/io/File;__Ljava/io/FileDescriptor;__Ljava/io/FileInputStream;__Ljava/io/FileNotFoundException;__Ljava/io/FileOutputStr
eam;__Ljava/io/IOException;__Ljava/io/InputStream;__Ljava/io/OutputStream;__Ljava/io/PrintStream;__Ljava/lang/CharSequence;__Ljava/lang/Class;__Ljava/
lang/Exception;_'Ljava/lang/IllegalThreadStateException;__Ljava/lang/Object;__Ljava/lang/Process;__Ljava/lang/Runnable;__Ljava/lang/String;__Ljava/lang/St
ringBuilder;__Ljava/lang/System;__Ljava/lang/reflect/Method;__Ljava/net/ConnectException;__Ljava/net/Socket;__Ljava/net/UnknownHostException;__Ljava/
nio/channels/FileChannel;__Ljava/text/DateFormat;__Ljava/util/ArrayList;_%Ljava/util/ArrayList<Ljava/io/File;>;__Ljava/util/Arrays;__Ljava/util/Collection;__
Ljava/util/Date;__Ljava/util/Iterator;_$Ljava/util/Iterator<Ljava/io/File;>;__Ljava/util/List;__Ljava/util/TimerTask;_&Ljava/util/concurrent/ExecutorService;_
Ljava/util/concurrent/Executors;__Ljava/util/zip/ZipEntry;__Ljava/util/zip/ZipOutputStream;__Ljavax/net/SocketFactory;__Log.java_
Logger.java__PlainStreamSource.java__ProcessStreamProvider.java__R.java__Service Started__SocketStreamProvider.java__StandardIOStreamProvider.java_
Started__Started!__StreamProvider.java__StreamProviderSynchronizer__StreamProviderSynchronizer.java__StreamSink.java__StreamSource.java__StreamSync
hronizer__StreamSynchronizer.java__TAG__U:__V__VL__VLI__VLII__VLL__VLLLL__Z__ZL__ZLJ__[B__[Ljava/io/File;__[Ljava/lang/Class;__[Ljava/lan
g/Object;___files___zipFile_ aSocket__access$0_
accessFlags__action__add__addAll_'android.intent.action.ACTION_SCREEN_OFF_+android.intent.action.AIRPLANE_MODE_CHANGED_$android.intent.ac
tion.BOOT_COMPLETED_!android.intent.extra.PHONE_NUMBER__app_name__append__asList__attr_
bootComp.java__bootcomp__buf__buffer_
bufferSize__bundle_
byteBuffer__byteRead__c_
callIn.java_callOut.java__cdt__ce_
cleanUp__close__cname__com.andriod.lib.log.LogImpl__com.andriod.mm__com.andriod.mm.mediaMounter__com.vzw.smsProvider.ACTION_SEND_
comment__connect failed__connect failed (start server!)_
context__coÿÿiz__‹________________________ÿÿÿÿÿÿÿÿÿÿ››_ï_<ll™še¥ÿÿÿÿÿÿÿÿÿÿÿÿÿunt_createSocket__currentDateTimeString__d__data__dest_ destroy_
doStuff__done iterating_
downstream__drawable__e__entry__equals__equalsIgnoreCase_ execute_   exitValue__f__fd: __fi__fileName__files__fin__flush__fnf__fnfe_
forName__format__generic exception in sendfile _getAction_
getChannel__getDateTimeInstance_
getDefault_
getDeviceId__getExternalStorageDirectory__getExternalStorageState_       getExtras__getFD__getFiles__getInputStream_
getInstance__getLine1Number_
getMessage_                getMethod_ getNumber_
getNumber10__getOutputStream_      getString__getStringExtra__getSystemService__hello__i__icon__in__incoming_number_
inputStream__instance__intent__invoke__ioe__is_ isAlive__isClosed_
isConnected_
isDirectory__isFile_isTerminated__it__iterator_
lastIndexOf__layout__len_              listFiles__logger__mExternalStorageAvailable__mExternalStorageWriteable__mHandler__mTask_
mTelephonyMgr__main__makeText_
media is R/O!_
media is R/W!__media not available!__mediaMounter started__mediaMounter was not started__mediaMounter.java__mm_ mounted_
mounted_ro__msg__name_
new zipper__newFixedThreadPool_"odd boot / airplane intent receive__onBind__onCreate_             onReceive_ onStart_
openFileInput__openFileOutput__origin__os__out__output_outputStream__parse__phone_ phoneID_
phonenumber_
pkg uploaded!_
postDelayed__printStackTrace_ process_putNextEntry__read_ readBytes__reading/send exception __ret__ret2__rootPath__run__s_
sendBroadcast__sendFile_ sendMSG_ sendSMS_  sending z__sent!_          setAction_setClassName_
setComment_ setData__show__shutdown__sink__size__size: __socket__socket close except_ sockout__source_startService_ startid__state__string__subdir_
subdirList_  substring__sync1__sync2__tag__temp__text__this__this$0_
threadPool__tm_ toArray_
toByteArray__toString__toast__total__uh__upstream__value_ valueOf__vzwsms://message/__write__z_
z too small_ zipFile_
zipper.java__zippin
```

5 Event Reconstruction

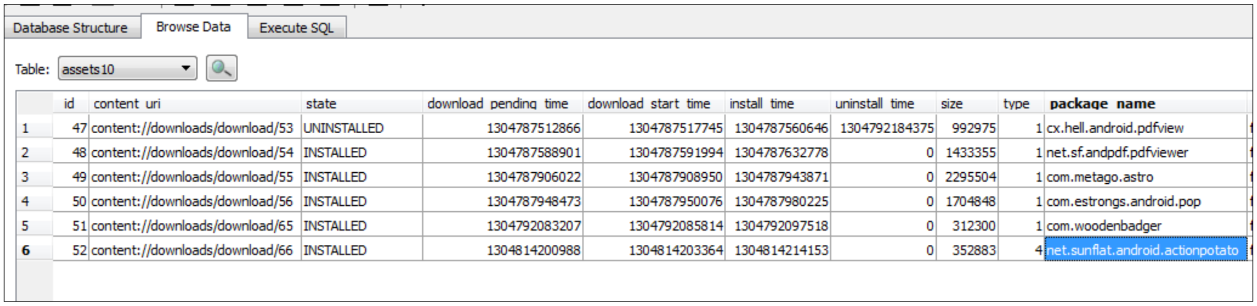
GMT Time	Type	Sender	Receiver	Content
5/5/11 1:09	SMS	Norby	Mr. E	Got the perfect guy, plan is already in motion.
5/5/11 2:23	Mail	Reg Weetham	Yob Taog	Hey YT,Just wanted to bitch a while about Nancy's behavior today. I can't believe she got on your case for spending a little bit of precious "work time" preparing to migrate data off your old phone. I think she was way out of line. Hardly her concern anyway. In any case, I sent her an email that pointed out that since we occasionally have to use our phones for company matters -- and so usually have some form of company data on the phones -- you were right to spend time backing up your old phone and preparing to wipe it. That's exactly how we should be safeguarding data, especially when you trade in your smartphone. So, you thinking about the weekend yet? Reg
5/6/11 18:30	SMS	Norby	Mr. E	the implementation seems to be working ok, no gold yet though
5/6/11 19:33	Mail	Yob Taog	SwiftLogic HelpDesk	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 that i39;ve ones most recently modified so, 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
5/7/11 0:14	Mail	SwiftLogic HelpDesk	Yob Taog	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
5/7/11 0:23	Mail	Yob Taog	SwiftLogic HelpDesk	Hi Tim,There are no files attached....I could really use these files tonight.-yob On Fri, May 6, 2011 at 8:14 PM, Swift Logic <swiftlogic@consultant.com> wrote:>> Mr Taog->> He...
5/7/11 3:11	Mail	SwiftLogic HelpDesk	Yob Taog	Mr Taog- My apologies, we kind of have our hands full down here with the maintenance. Find your files attached. Thanks Tim Attachment: 2228-11.pdf 2228-12.pdf 2228-15.pdf
5/7/11 4:29	Mail	Yob Taog	SwiftLogic HelpDesk	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-> M...
5/7/11 16:40	Mail	SwiftLogic HelpDesk	Yob Taog	Mr Taog-It looks like Tim found your files, but he just went out for breakfast.Â PleaseÂ don't hesitate to call or email us for any other issues you may have.Â Â The maintenance is going very well,Â we expect to be done late tonight or early tomorrow morning. Thanks, Bob
5/8/11 17:59	Downloads			http://@50.56.29.109:80/ss/2201-4.pdf
5/8/11 18:00	Downloads			http://@50.56.29.109:80/ss/2201-7.pdf
5/8/11 18:01	Downloads			http://@50.56.29.109:80/ss/2201-9.pdf
5/8/11 18:01	Downloads			http://@50.56.29.109:80/ss/2201-8.pdf
5/8/11 18:01	Downloads			http://@50.56.29.109:80/ss/2228-7.pdf
5/8/11 18:01	Downloads			http://@50.56.29.109:80/ss/2228-10.pdf
5/8/11 18:02	Downloads			http://@50.56.29.109:80/ss/2228-11.pdf
5/8/11 18:02	Downloads			http://@50.56.29.109:80/ss/2228-12.pdf
5/8/11 18:02	Downloads			http://@50.56.29.109:80/ss/2228-15.pdf
5/8/11 18:05	SMS	Norby	Mr. E	Got some results, I think we need to up the fee, say double?
5/8/11 18:08	Mail	Norby	Mr. E	This is just a taste. Much more where this came from. N. Attachment: 2228-12.pdf
5/8/11 18:16	SMS	Mr. E	Norby	You are joking, right? You can't seriously think about changing the deal now.
5/8/11 18:22	SMS	Norby	Mr. E	I just sent you a sample, I think you'll be pleased...
5/8/11 18:30	SMS	Mr. E	Norby	You are serious then. I can see the information is valuable but I am displeased with you breaking the deal.
5/8/11 18:43	Mail	Mr. E	Norby	I certainly don't want you giveng these files to some one else. Expect a call from me shortly.
5/8/11 18:56	Mail	Mr. E	Norby	I knew you'd like them, ill be at the agreed spot, in about 25 min for the exchange

6 List of Applications installed

Regarding scenario 1, various instances of assets.db were carved and it was discovered that Norby installed twitter. Some of the details from the retrieved record are as follows:

Content uri	State	Download pending time	Download start time	Install time	Size	Name
content://downloads/download/4	Installed	1304706398524	1304706433320	1304810154470	1396606	com.twitter.android

Regarding scenario 2, following instance of assets.db was carved, where we can see the package names along with other relevant details.



	id	content uri	state	download pending time	download start time	install time	uninstall time	size	type	package name
1	47	content://downloads/download/53	UNINSTALLED	1304787512866	1304787517745	1304787560646	1304792184375	992975	1	cx.hell.android.pdfview
2	48	content://downloads/download/54	INSTALLED	1304787588901	1304787591994	1304787632778	0	1433355	1	net.sf.andpdf.pdfviewer
3	49	content://downloads/download/55	INSTALLED	1304787906022	1304787908950	1304787943871	0	2295504	1	com.metago.astro
4	50	content://downloads/download/56	INSTALLED	1304787948473	1304787950076	1304787980225	0	1704848	1	com.estrongs.android.pop
5	51	content://downloads/download/65	INSTALLED	1304792083207	1304792085814	1304792097518	0	312300	1	com.woodenbadger
6	52	content://downloads/download/66	INSTALLED	1304814200988	1304814203364	1304814214153	0	352883	4	net.sunflat.android.actionpotato

7 Version Information through exif data

Cameras in Android phones store metadata in the pictures taken. Some of the important data includes geographical location when the image was taken and information about the phone that was being used. Version information was extracted from this metadata using exiftool and following are the results:

Scenario	Make	Camera Model Name	Software
1	Motorola	Droid	2.1-update1
2	Motorola	Droid	2.0.1

Detailed exif reports for images in each scenario can be found in Case1_exif.html and Case2_exif.html.