

DFRWS2011 Forensic Challenge

Forensic Analysis of Android Systems

Tim Vidas
Matthew Geiger
Eoghan Casey

Scenario 1: Suspicious Death

Donald Norby was found dead in his home
Unclear whether this is a suicide or homicide
Possible involvement with organized crime

Scenario goals:

Forensic exam of victim's Android device
Answer investigators' questions
Did Norby kill himself or was he murdered?

Scenario 2: Intellectual Property Theft

Data breach at SwiftLogic Inc

Yob Taog is suspected of the leak

Scenario goals:

- Forensic exam of suspect's Android device

- Answer investigators' questions

- Did Taog steal the information?

Scenario Twist!

- The murder victim is the data thief
- Norby installed malware on Toag's Android
- The malware exfiltrated files for Norby
- Norby was selling stolen data to criminal group
- Norby attempted to get more \$\$ for the files
- Norby was shot by a member of criminal group
- Toag was innocent and unaware of these activities

Background on Android

Rooting versus recovery partition

Acquisition using nandump versus dd
dd does not obtain spare area

State of the science in 2011

Limited solutions for Android NAND analysis

String extraction and carving

Commercial tools in development (beta)

Parse YAFFS2 and process some databases

Applied to NAND dump with spare area

Unable to parse dd image of partition

Challenge Design

Wanted “layers of difficulty”

Case files are collected with two techniques:

- Recovery image – full nanddump, contains OOB/spare information

- Root + dd style – a scenario that might occur in typical investigation

- Both had ad-hoc acquisition logs

Case files consist of typical phone information (call log data, text messages, etc)

Custom malicious applications, various app obfuscation

- Used an intermediate data storage server

SDCard images (note: wiped with “DFRWS2011” so any 0's are a result of the formatting process or typical operation)

Sign Up

Facebook helps you connect and share with the people in your life.



Wall

Info

Photos

Notes

Friends

Taog Yob

+1 Add Friend

Send Message

Activities and Interests

Activities



Eating

Interests



Android



Apps



Goats



La Llama que llama

Other

BMW USA

Arts and Entertainment

Music

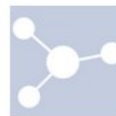


Radiohead



Nine Inch Nails

Books



Matterhorn: A Novel of the

Movies



Reservoir Dogs

Taog Yob is on Facebook.

To connect with Taog, sign up for Facebook today.

Sign Up

It's free and anyone can join. Already a member? Log in.

Wrong Taog Yob? Try again

Taog Yob

Search

Others With a Similar Name

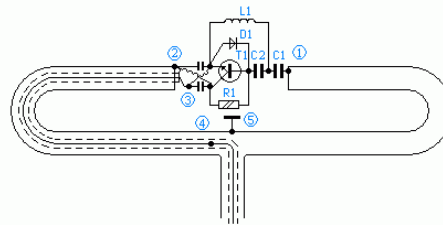


Yob Eagger

More ▾

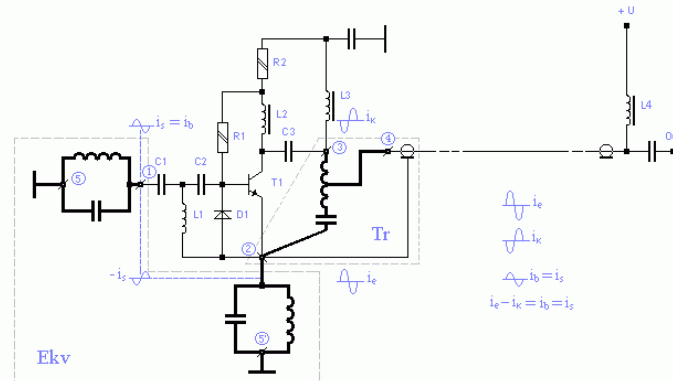
Followers 5





Pic. 3. Active Antenna (Aerial) Circuit with Minus Power Supply.

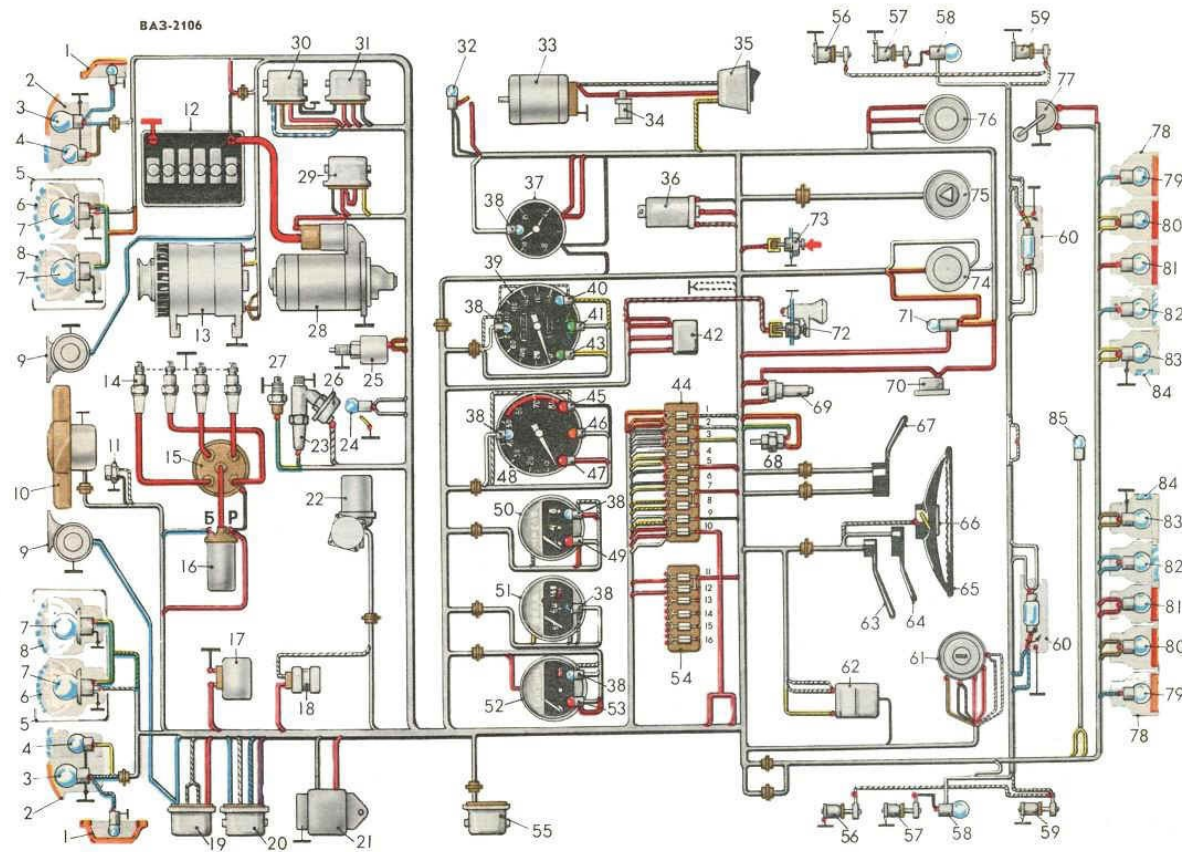
On pic. 2 and pic. 3 nonselective one-stage amplifier (transistors KT3101, KT372) is mounted directly in a dipol.



Pic. 4. Amplifier Circuit and Dipole Equivalent Circuit (with Plus Power Supply).



DRAFT



Case 2 in Cellebrite Physical (beta)

Project Tree

mtd8

Extraction Summary

Device Info

Images

mtdd8.dd

Memory Ranges

Bytes Swapped

Image

File Systems

Image

\$DeletedNodes

root

anr

app

app-private

backup

dalvik-cache

data

dontpanic

local

lost+found

misc

property

system

tombstones

cc_data

Analyzed Data

Chats (3)

Contacts (9)

Emails (65)

Locations (28)

SMS Messages (17)

User Accounts (2)

Web Bookmarks (50)

Welcome

Extraction Summary

Chats (3)

Locations (28)

SMS Messages (17)

Emails (65)

Table View

<input checked="" type="checkbox"/>	Del?	Folder	Status	Parties	Message	Timestamp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Sent	Sent	shandra@cheerful.com	Sorry, still an Atlanta till tonight. Raincheck?	5/10/2011 1:31:44 PM (UTC+0)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inbox	Read	shandra@cheerful.com	(You around for lunch) Hey -- a few of us are going to that great Indian buffet for lunch today. You interested?	5/10/2011 11:26:46 AM (UTC+0)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inbox	Read	shandra@cheerful.com	(Re: Sorry, still an Atlanta till) OK. Safe travels! ----- Original Message -----	5/10/2011 4:35:18 PM (UTC+0)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inbox	Read	4124393388	You have insufficient funds to send message.	5/10/2011 8:43:03 PM (UTC+0)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inbox	Read	4124393388	You have insufficient funds to send message.	5/10/2011 8:43:40 PM (UTC+0)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inbox	Read	shandra@cheerful.com	(Nearby! Coming for my beer) Hey Yob, I am closing in on Fat Heads. See ya soon.	5/6/2011 1:34:55 AM (UTC+0)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inbox	Read	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.	5/6/2011 5:53:30 PM (UTC+0)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inbox	Read	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 eme...	5/6/2011 5:55:16 PM (UTC+0)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inbox	Read	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	5/7/2011 11:39:16 PM (UTC+0)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Sent	Sent	shandra@cheerful.com	Sure thing. Do you know where the wine loft is?	5/7/2011 11:44:27 PM (UTC+0)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Sent	Sent	shandra@cheerful.com	I ran into some friends at the double wide, meetup at 8:30 or so?	5/7/2011 11:54:37 PM (UTC+0)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Sent	Sent	shandra@cheerful.com	Or you can walk down Carson and join us	5/7/2011 11:56:53 PM (UTC+0)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Inbox	Read	shandra@cheerful.com	(Re: Or you can walk down) Walking down now. Hope you are still vertical. ----- Original Message From: 4124393388@VTEXT.COM Sent: 05/10/2011 4:35:18 PM To: shandra@cheerful.com Subject: (Re: Sorry, still an Atlanta till) OK. Safe travels!	5/8/2011 3:10:01 AM (UTC+0)

File system examination

The screenshot displays a file system examination tool interface. On the left, the 'Project Tree' shows a hierarchy starting with 'mtd8', followed by 'Extraction Summary', 'Device Info', 'Images', 'mtd8.dd', 'Memory Ranges', 'Bytes Swapped', 'Image', 'File Systems', and 'Image'. The 'File Systems' section is expanded, showing a 'root' directory with various subdirectories like 'anr', 'app', 'app-private', 'backup', 'com.android.intern', 'com.google.androi', 'pending', 'dalvik-cache', 'data', 'android.tts', 'lib', 'au.com.phil', 'com.amazon.mp3', 'com.andriod.mm', 'files', 'temp', and 'lib'. The 'temp' directory is highlighted.

The main window shows a 'Hex View' of the selected file. The hex data is displayed in columns, with the corresponding ASCII representation on the right. The ASCII column shows a list of files, including 't...nico_rosberg_1150', '44590.jpgPK', '...>...&...A...', '.....thrillbe', 'urne_196930547.jpgPK', '.....>.!jWn...', '.....P.', '.2228-11.pdfPK', '.....>...\$', '.....astro', '.dbPK', '.....>HI', '.....', '....*.2228-12.pdfPK', '.....>Y.&...', '5.....;', '.2228-15.pdfPK', '.....>.4\.b.es...', '.....{a..2201-', '4.pdfPK', '.....', '.....2201-7.pdfPK', '.....>...n..', '....._I', '..2201-8.pdfPK', '.....>...U.....', '.....2201-', '9.pdfPK', 'm.<C.....', '.....2228-7.pdfPK', '.....>.....', '..2228-10.pdfPK', '.....>m.....', '.....!..robo', '_defense_free.bakPK..', '.....>.....'.

Challenge Submissions

All will be available online (and associated tools)

2 team submissions: 2 individual submissions:

Fox-IT in the Netherlands

Korea University

Digital Forensic Research Center

Apurva Rustagi

P. V. Burenin

But we know there were more participants, and we know people were working on it from immediately after release to right before the deadline...

Challenge Participants

Not all participants submitted solutions

GeoIP located IP addresses, (Three different tools)
from *server logs* in the *intermediate server*:

Chemnitz	Germany	
Illinois	USA	
Seoul	Korea	Korea
Seoul	Korea	Korea
Seoul	Korea	Korea
Beijing	China	
Berlin	Germany	
Madrid	Spain	Madrid
Paris	France	Marina Del Ray, CA
India	Mumbai	India
Dallas	Dallas	USA
Russia	Russia	
Texas	Texas	
Seoul	Seoul	Korea
Amsterdam	Delft	Delft, Netherlands

Challenge Participants

Not all participants submitted solutions

The *intermediate server*:

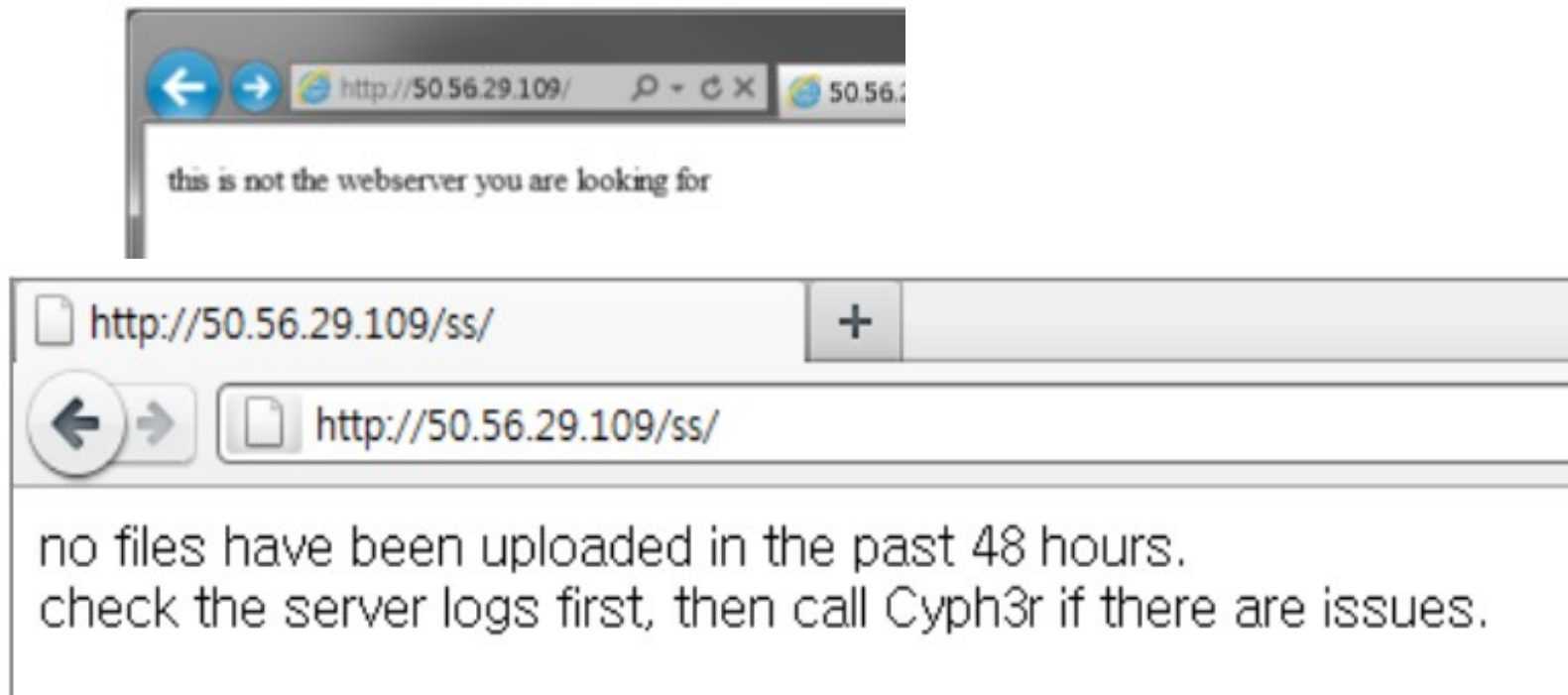


Figure 19. Login success : <http://50.56.29.109/ss/>

Search Mail Search the Web

Show search options
Create a filter

Warning: We believe your account was recently accessed from: South Korea (korea.ac.kr:163.152.165.120). Show details and preferences Ignore

Office 365 Pittsburgh - www.plusconsulting.com - Best Productivity Experience Now in the Cloud

About these

Archive Spam Delete Move to Labels More

1 - 50 of 25

Try on a new inbox: Classic Important first Unread first Starred first Priority Inbox

- ☐ **Windows IT Pro** Last Chance: Storage Challenges in Exchange 2010 - View on Mobile Phone | View as Web page Windows IT Pro The Leading Independent Community for IT ...
- ☐ **WinInfo Daily UPDATE** Circling the Drain, RIM Lays Off 11 Percent of Workfor - View on Mobile Phone | View as Web page Circling the Drain, RIM Lays Off 11 Percent of Workforce ...
- ☐ **Pittsburgh Downtown Part.** Downtown Happenings, Week of July 25 - Week of Monday, July 25 - Sunday, July 31 Thank you to our Renaissance and Visionary Leader ...
- ☐ **Business Technology Upda.** The Social Enterprise: An Interview with NewsGator - View on Mobile Phone | View as Web page Windows IT Pro UPDATE The Social Enterprise: An Interview ...
- ☐ **Windows IT Pro** Nominate Your Favorite Products for the Community Choice Awards - View on Mobile Phone | View as Web page Windows IT Pro is Now Accepting Nominations for the 2011 ...
- ☐ **Google Calendar** Reminder: Project Planning Meeting @ Fri Jul 22 3:30pm - 5pm (yobtaog@gmail.com) - more details » Project Planning Meeting When Fri Jul 22 3:30pm - 5pm Eastern Time Calendar ...
- ☐ **Exchange and Outlook UPD.** Working with Outlook's Personal Folders Backup Utility - View on Mobile Phone | View as Web page Exchange & Outlook UPDATE Working with Outlook's ...
- ☐ **Windows IT Pro** Blogs: The Private Cloud Explained by Otey and Highly Available Hyper-V Workloads Acros... - View on Mobile Phone | View as Web page Windows IT Pro The Leading Independent Community for IT ...
- ☐ **SQL Server Magazine UPDA.** The New Kid in Town: SQL Server Denali - View on Mobile Phone | View as Web page SQLServerMagazineUpdate The New Kid in Town: SQL Server ...
- ☐ **WinInfo Daily UPDATE** Intel Beats Estimates, Offers Upbeat Predictions for Future - View on Mobile Phone | View as Web page Intel Beats Estimates, Offers Upbeat Predictions for ...
- ☐ **Security UPDATE** VMware Virtualization Security - View on Mobile Phone | View as Web page Security Update Security Solutions VMware Virtualization ...
- ☐ **DevProConnections UPDATE** Tim Huckaby: Clearing Up the FUD Around Windows 8, HTML5, and Silverlight - View on Mobile Phone | View as Web page DevProConnections_Silverlight_Edition Windows 8's FUD ...
- ☐ **CloudITPro UPDATE** EMC Improves Cloud Storage Management; Q&A: IDC Analyst on Cloud's Potential; and More - View on Mobile Phone | View as Web page Rich Karpinski From the Cloud by Rich Karpinski EMC And ...
- ☐ **SharePoint Pro UPDATE** To BLOB or Not to BLOB - View on Mobile Phone | View as Web page Sharepoint Pro Update To BLOB or Not to BLOB ...
- ☐ **WinInfo Daily UPDATE** Apple Earnings Lifted by China Sales - View on Mobile Phone | View as Web page Apple Earnings Lifted by China Sales thurrott By Paul ...
- ☐ **Windows IT Pro** Windows IT Pro & Group Policy - Get 7 Extra Issues - View on Mobile Phone | View as Web page Subscribe to Windows IT Pro You're missing the ...
- ☐ **WinInfo Daily UPDATE** Despite Doom and Gloom, Microsoft Wraps Up Record Year - View on Mobile Phone | View as Web page Despite Doom and Gloom, Microsoft Wraps Up Record Year ...
- ☐ **Windows IT Pro UPDATE** Windows Server 8 Hints at Microsoft's Private Cloud Plans - View on Mobile Phone | View as Web page Windows IT Pro UPDATE Windows Server 8 Hints at ...
- ☐ **Windows IT Pro** Smart Tips for Virtualizing Desktops and Apps - View on Mobile Phone | View as Web page Windows IT Pro The Leading Independent Community for IT ...
- ☐ **MobileDevPro UPDATE** Are You Ready for a Mobile App Hackathon?; Practical App-Building Advice; and More - View on Mobile Phone | View as Web page MobileDevPro UPDATE Rich Karpinski Mobile Musings by Rich ...
- ☐ **WinInfo Daily UPDATE** Amazon Tablet Rumors Heat Up - View on Mobile Phone | View as Web page Amazon Tablet Rumors Heat Up thurrott By Paul Thurrott ...
- ☐ **SQL Server Magazine** DAG discovery - ensuring availability and disaster recovery with Paul Robichaux, July 21 - View on Mobile Phone | View as Web page SQL Server Magazine The Smart Guide to Building World ...
- ☐ **Pittsburgh Downtown Part.** Downtown Happenings, Week of July 18 - Week of Monday, July 18 - Sunday, July 24 Thank you to our Renaissance and Visionary Leader ...
- ☐ **Twitter** sophie rossier (@sophiecmrossit) is now following you on Twitter! - Twitter sophie rossier @sophiecmrossit is now following you (@yob_taog). sophiecmrossit sophie ...
- ☐ **Google Calendar** Reminder: Project Planning Meeting @ Fri Jul 15 3:30pm - 5pm (yobtaog@gmail.com) - more details » Project Planning Meeting When Fri Jul 15 3:30pm - 5pm Eastern Time Calendar ...
- ☐ **Windows IT Pro** Mark Minasi's 5 Years of Power Tools eBook Now Available! - View on Mobile Phone | View as Web page Mark Minasi Check out the latest Windows IT Pro's ...

Activity information - Mozilla Firefox

google.com
https://mail.google.com/mail/?ui=2&ik=5db6ca3b42&view=ac

Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity. [Learn more](#)

This account does not seem to be open in any other location. However, there may be sessions that have not been signed out.

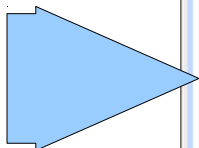
Sign out all other sessions

Recent activity:

If the activity below doesn't look like yours, [change your password immediately](#). [Learn more](#)

Access Type [?] (Browser, mobile, POP3, etc.)	Location (IP address) [?]	Date/Time (Displayed in your time zone)
Unknown	South Korea (korea.ac.kr:163. [REDACTED])	Jul 14
Unknown	South Korea (korea.ac.kr:163. [REDACTED])	Jul 21 (4 days ago)
Browser	* United States (PA) [REDACTED]	9:01 pm (0 minutes ago)
Browser	South Korea (163. [REDACTED])	Jul 23 (2 days ago)
Browser	South Korea (163. [REDACTED])	Jul 23 (2 days ago)
Browser	South Korea (163. [REDACTED])	Jul 23 (2 days ago)
Browser	South Korea (163. [REDACTED])	Jul 23 (2 days ago)
Browser	South Korea (163. [REDACTED])	Jul 22 (3 days ago)
Browser	South Korea (163. [REDACTED])	Jul 22 (3 days ago)
Browser	South Korea (163. [REDACTED])	Jul 22 (3 days ago)
Browser	South Korea (163. [REDACTED])	Jul 22 (3 days ago)
Mobile	South Korea (211. [REDACTED])	Jul 22 (3 days ago)

Alert preference: Show an alert for unusual activity. [change](#)



Fox-IT

Ivo Pooters, Steffen Moorrees & Pascal Arends

- Developed Python utilities
- Presented visual reconstruction of evidence
- Great overall synthesis of evidence and application to the Scenario

Call logs

Contact name	Number(s)	Other info
Mr E	4439264768	Email: mre@hushmail.com
Taog	4124393388	
Mr e	4439264768	

Table 11. Recovered contact records from Norby's phone

Further we used the same script to extract call history records from the user data partition.

Number	Date/time (utc)	Duration (secs)	In/out	Name
4439264768	05/04/2011 11:31:08 PM	341	Out	Mr E
4124623802	05/05/2011 12:04:01 AM	91	Out	
4439264768	05/05/2011 12:38:17 AM	115	Out	Mr E
4124623802	05/05/2011 03:18:33 PM	84	Out	
4439264768	05/08/2011 06:46:24 PM	381	In	Mr E

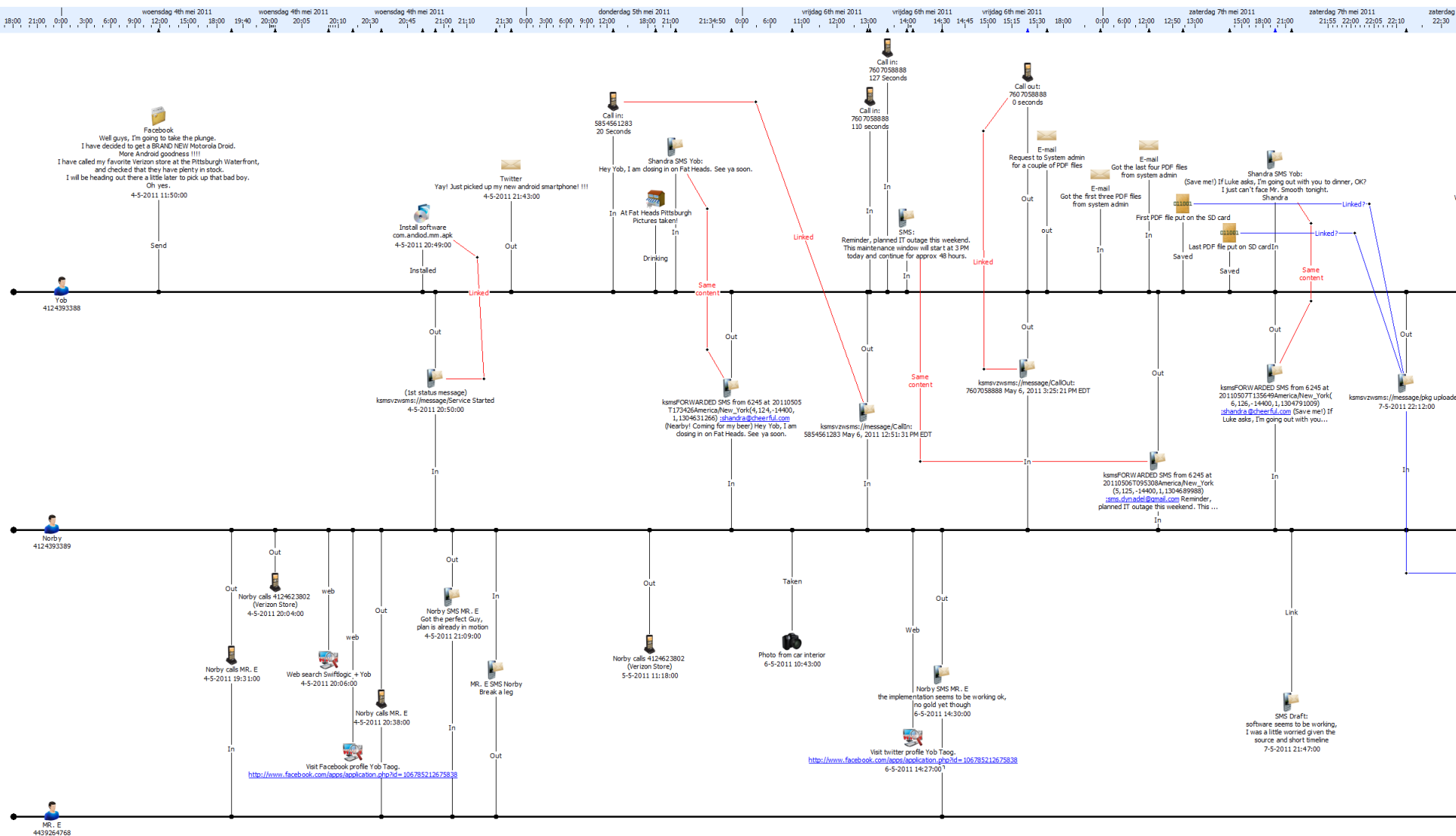
Table 12. Recovered call history records from Norby's Phone

It is very likely that during the period 5/4/2011 to 5/8/2011 Norby was engaged in multiple telephone conversations with the number stored under the name of *mr E*. Further, Norby contacted the number 4124623802 twice with call durations of 91 seconds and 84 seconds respectively. Performing open source investigation on this number leads to a Verizon Wireless store in the Waterfront shopping centre in Pittsburgh.

Kriptix Headquarters?!?!?



Figure 3. Fat Heads



Korea University

Jewan Bang, Jungheum Park, Hyunji Chung, Dohyun Kim,
Sangjin Lee

- Developed Visual studio projects to parse YAFFS2 data
- Very comprehensive report

Korea University YAFFS2 Parser

C:\WINDOWS\system32\cmd.exe

```
X:\DFRWS2011-Challenge\Case2>yaffs2fordroidimage.exe "e2\Case2\mtd8.dd" X:\DFRWS2011-Challenge\Case2\Output
```

```
=====  
Droid flash memory dump reconstructor v0.5  
Digital Forensic Research Center, Korea University.  
=====
```

```
Extracting : cc_data  
Extracting : 010B2080  
Extracting : appwidgets.xml  
Extracting : accounts.db  
Extracting : batterystats.bin.bak  
Extracting : batterystats.bin  
Extracting : stats.bin.bak  
Extracting : stats.bin  
Extracting : pending.bin  
Extracting : status.bin.bak  
Extracting : status.bin  
Extracting : accounts.xml  
Extracting : 010B2080  
Extracting : cameraCalFile.bin  
Extracting : accounts.db-journal  
Extracting : packages.xml  
Extracting : android.accounts.AccountAuthenticator.xml  
Extracting : android.content.SyncAdapter.xml  
Extracting : 010B2418
```

Installed Apps

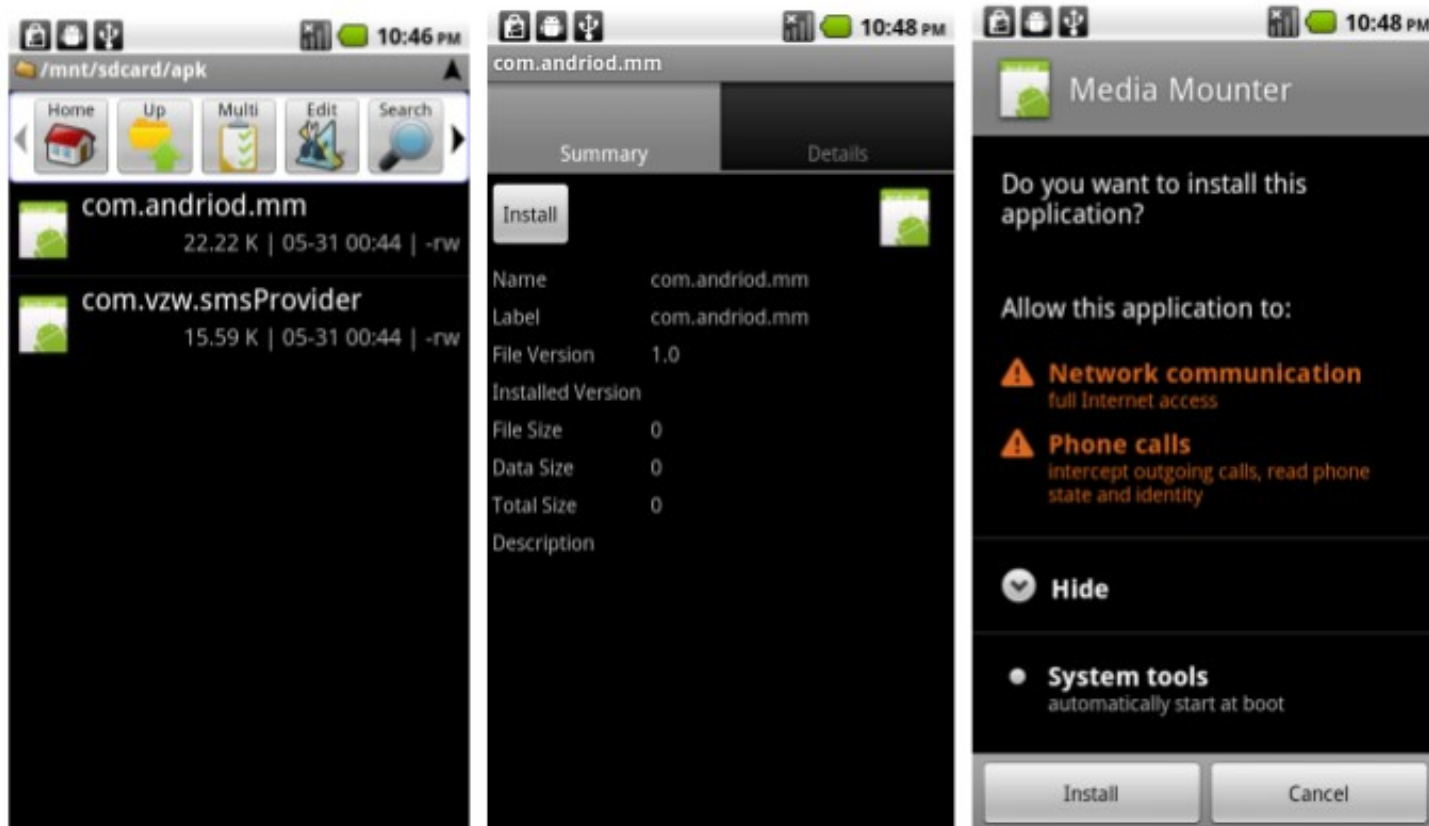
INSTALL_FAILED	com.boolbalabs.tossit.preview	2011-05-04 21:30:03		
INSTALL_FAILED	com.dragonplay.blackjack	2011-05-04 21:30:34		
INSTALLED	au.com.phil	2011-05-04 21:30:51	2011-05-04 21:37:54	
INSTALLED	com.magicwach.rdefense_free	2011-05-04 21:31:59	2011-05-04 22:06:59	
INSTALL_FAILED	dk.logisoft.aircontrol	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	α.hell.android.pdfview	2011-05-07 12:58:37	2011-05-07 12:59:20	2011-05-07 14:16:24

Malicious Apps

```
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
```

“Donor Device”

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 so malicious activities such as ‘Network communication’ and ‘Intercept Calls’. After installing the application, it could not identify an application icon. This means that the application is running in background.

Geo-locate (examples: Facebook “check in”, gmaps search)

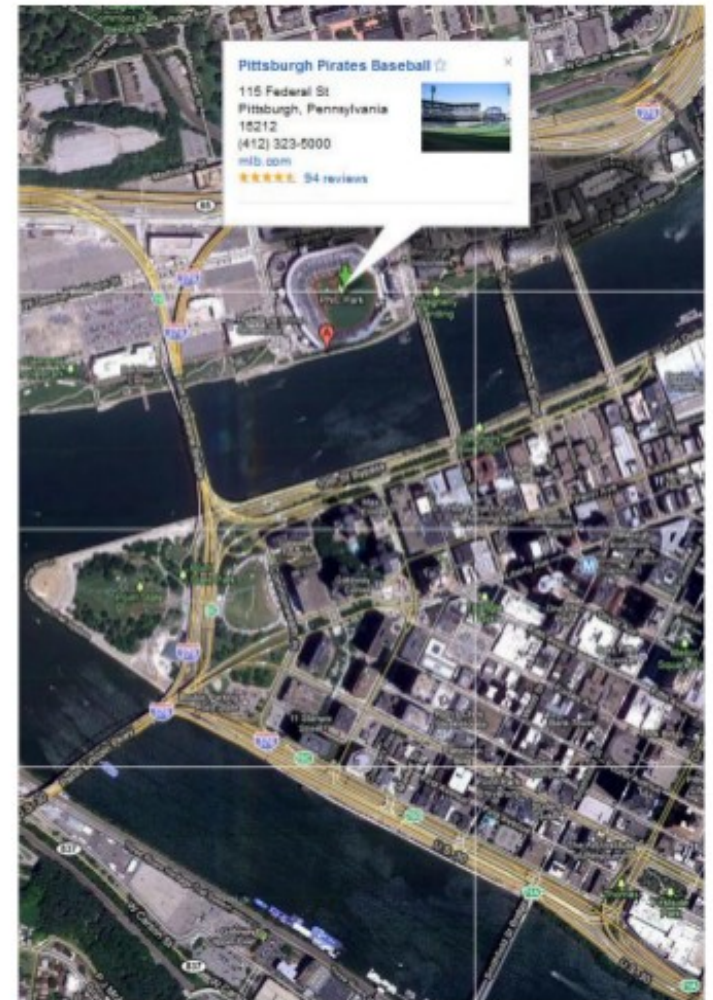


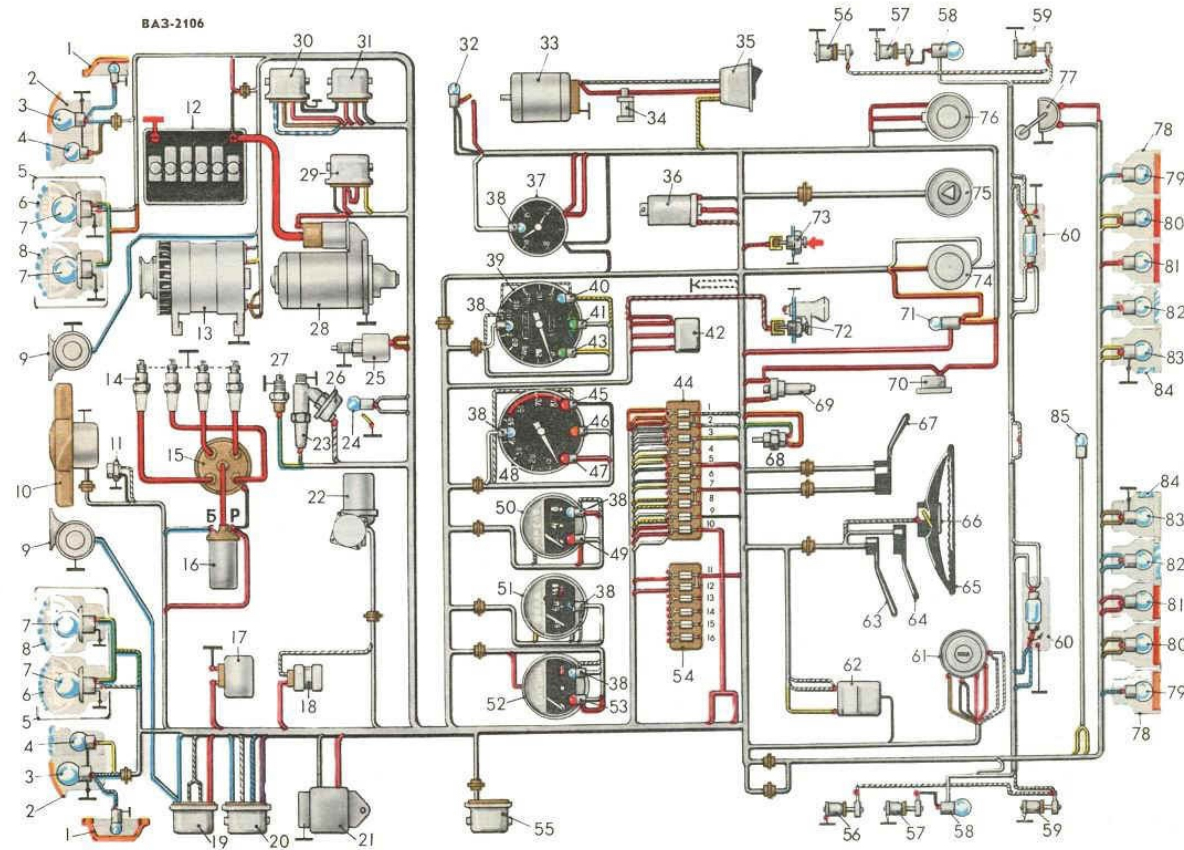
Figure 29. Google Map Search Result: Destination

P. V. Burenin Submission

Some of these downloaded files are very interesting (they are stored in "SDCard/download" folder). The file named "SDCard/download/2228-11.pdf" stores scheme of an old Russian car "BAZ 2106" aka "Жигули шестёрка"...



DRAFT



And the Winner is...

Fox-IT !!

Ivo Pooters, Steffen Moorrees & Pascal Arends

THANKS!

Thanks to all those who participated
□(especially those that submitted ;-)