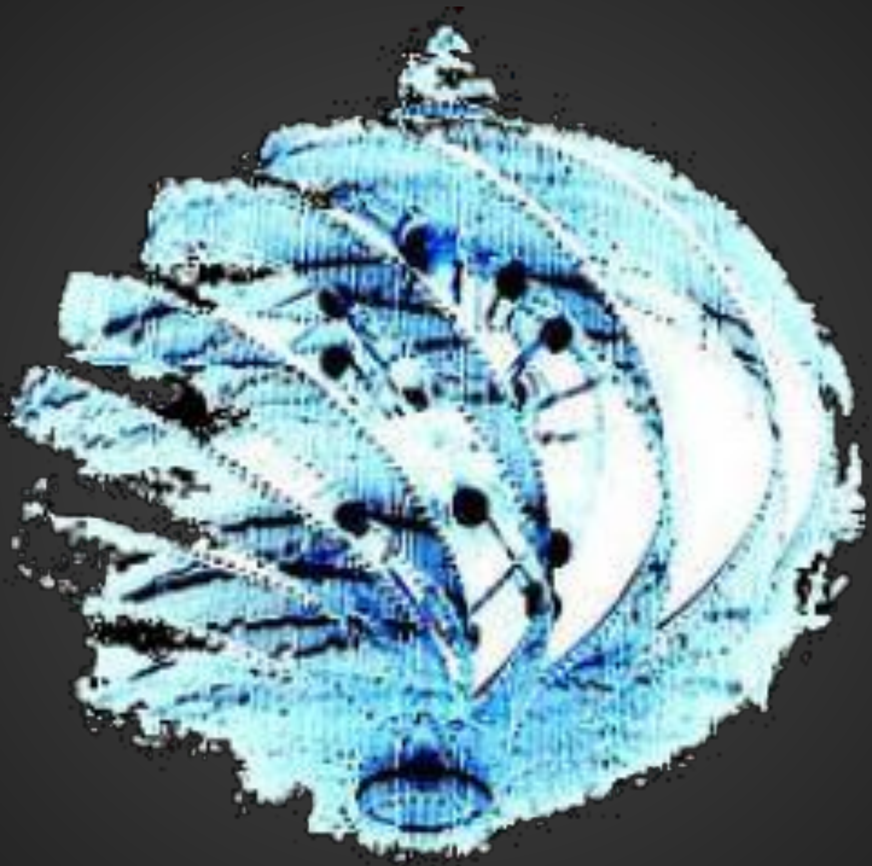


Android Forensics

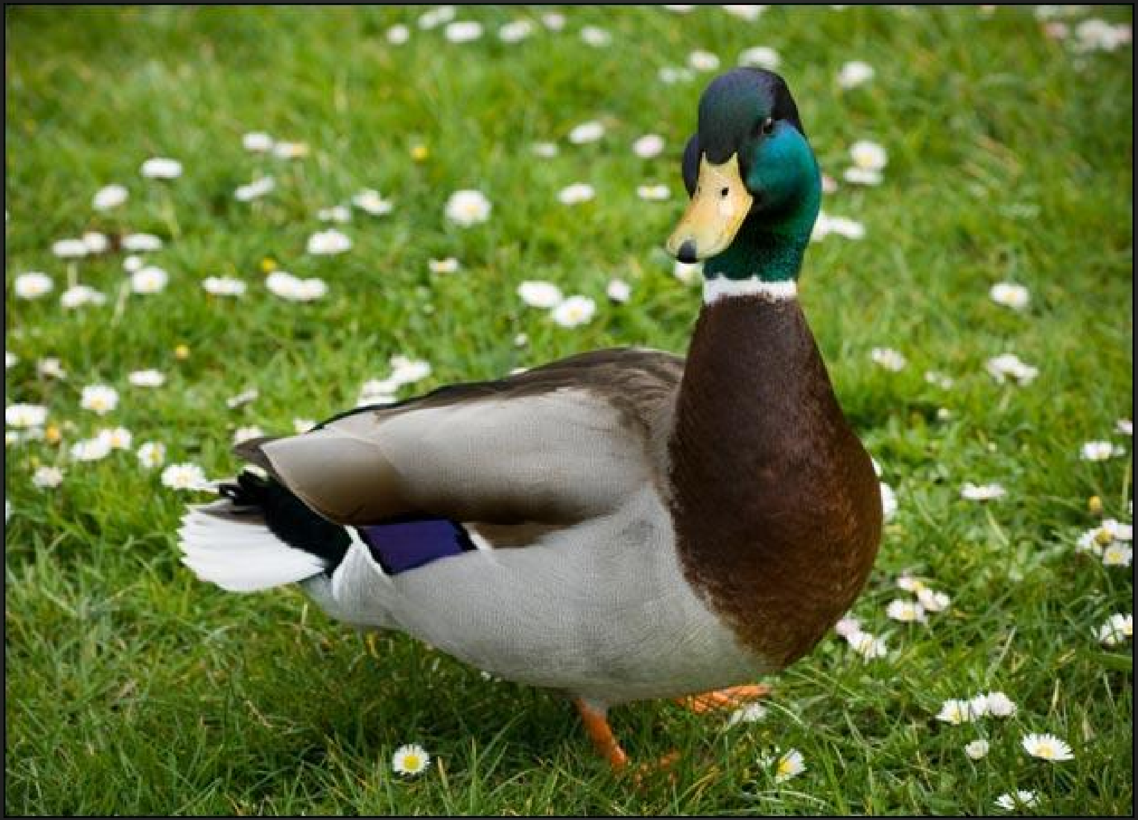
The Joys of JTAG

tty0x80

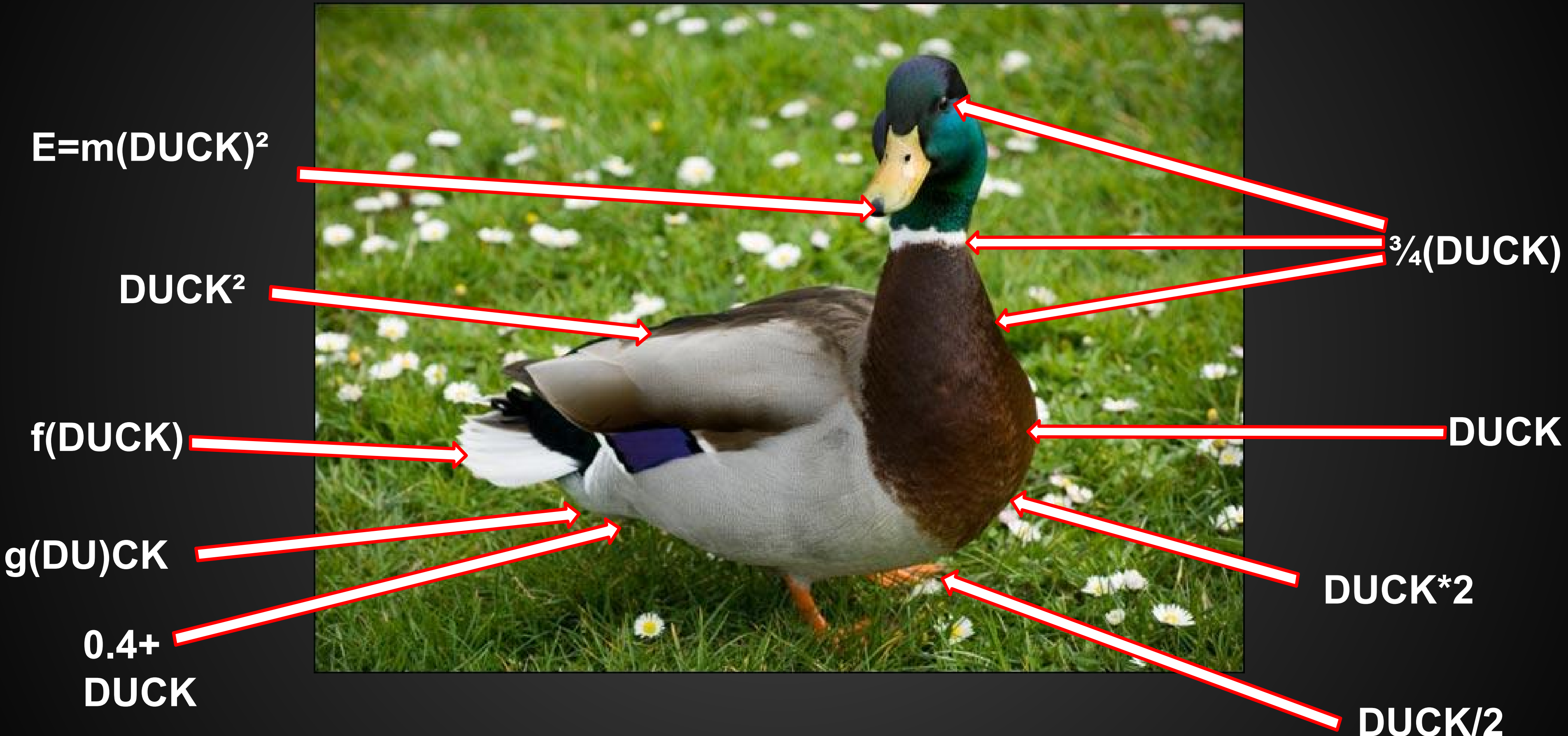
Some content has been redacted, either for legal reasons or to protect the privacy of those who have participated in some of my test cases.

If a particular omission interests you, see me later and I might be able to clue you in as to what was represented.

This is a duck



Proof



$E=m(DUCK)^2$

$DUCK^2$

f(DUCK)

g(DU)CK

0.4+
DUCK

¾(DUCK)

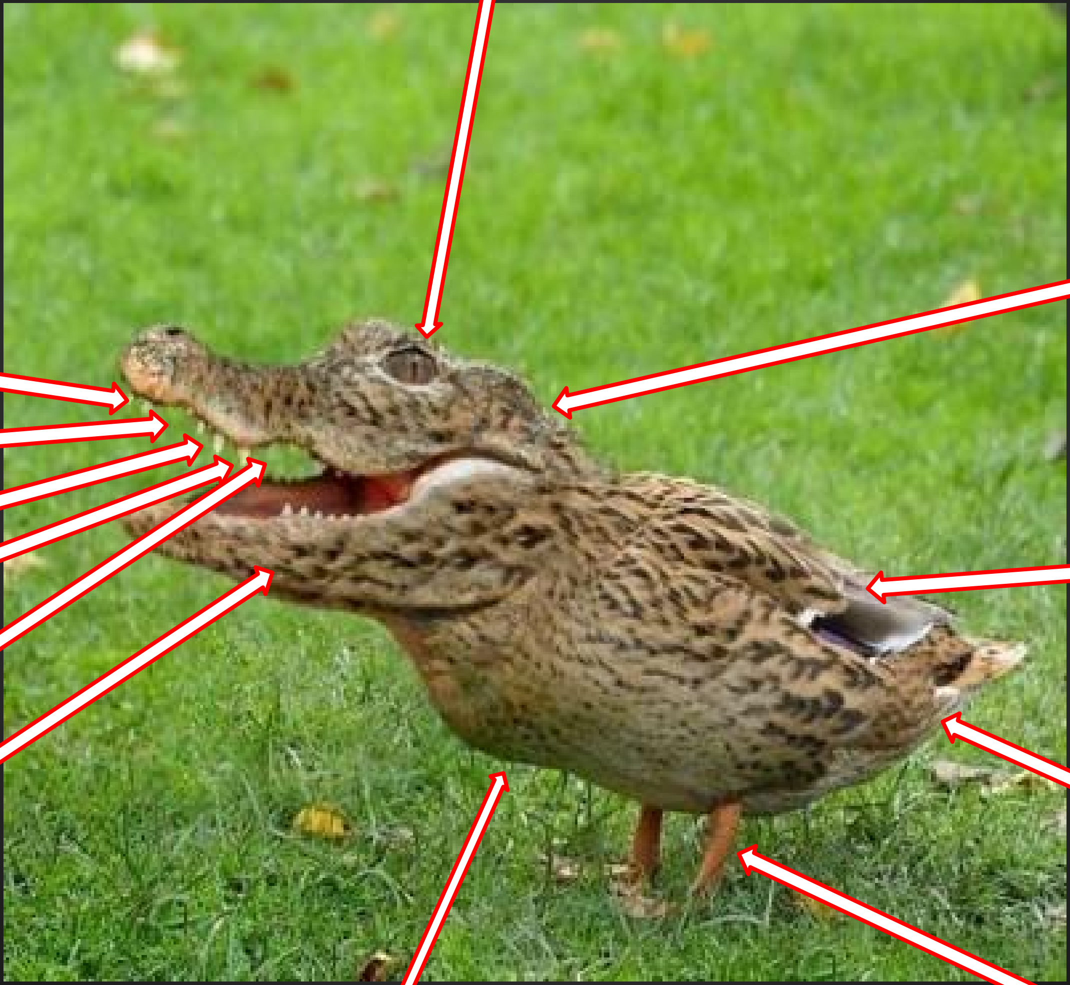
DUCK

DUCK*2

DUCK/2

This is not a duck

ILLUMINATUS



NOPE

NOPE

NOPE

NOPE

NOPE

NOPE

possibly
ARMv7

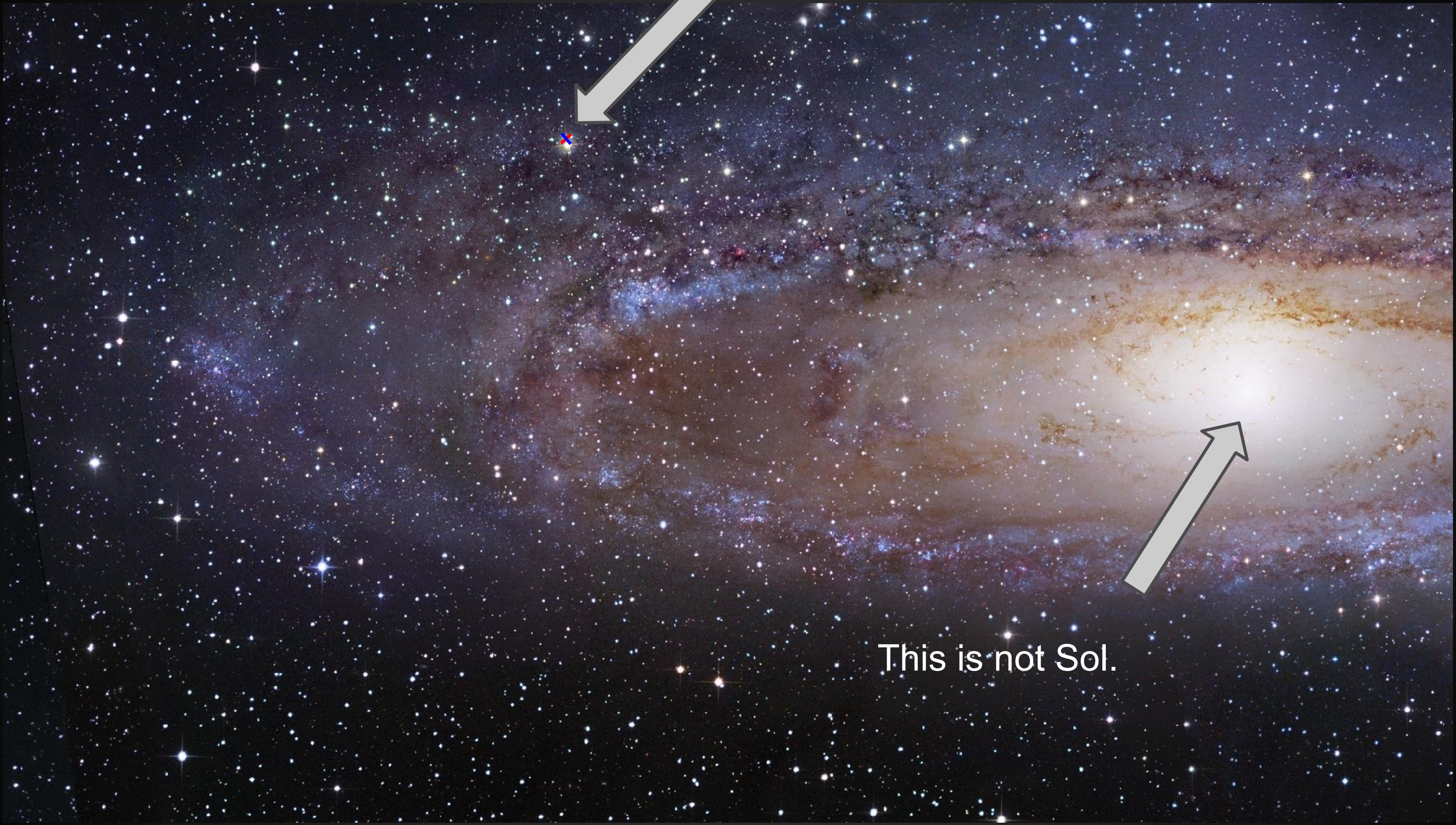
evolved
propulsion
system

exhaust

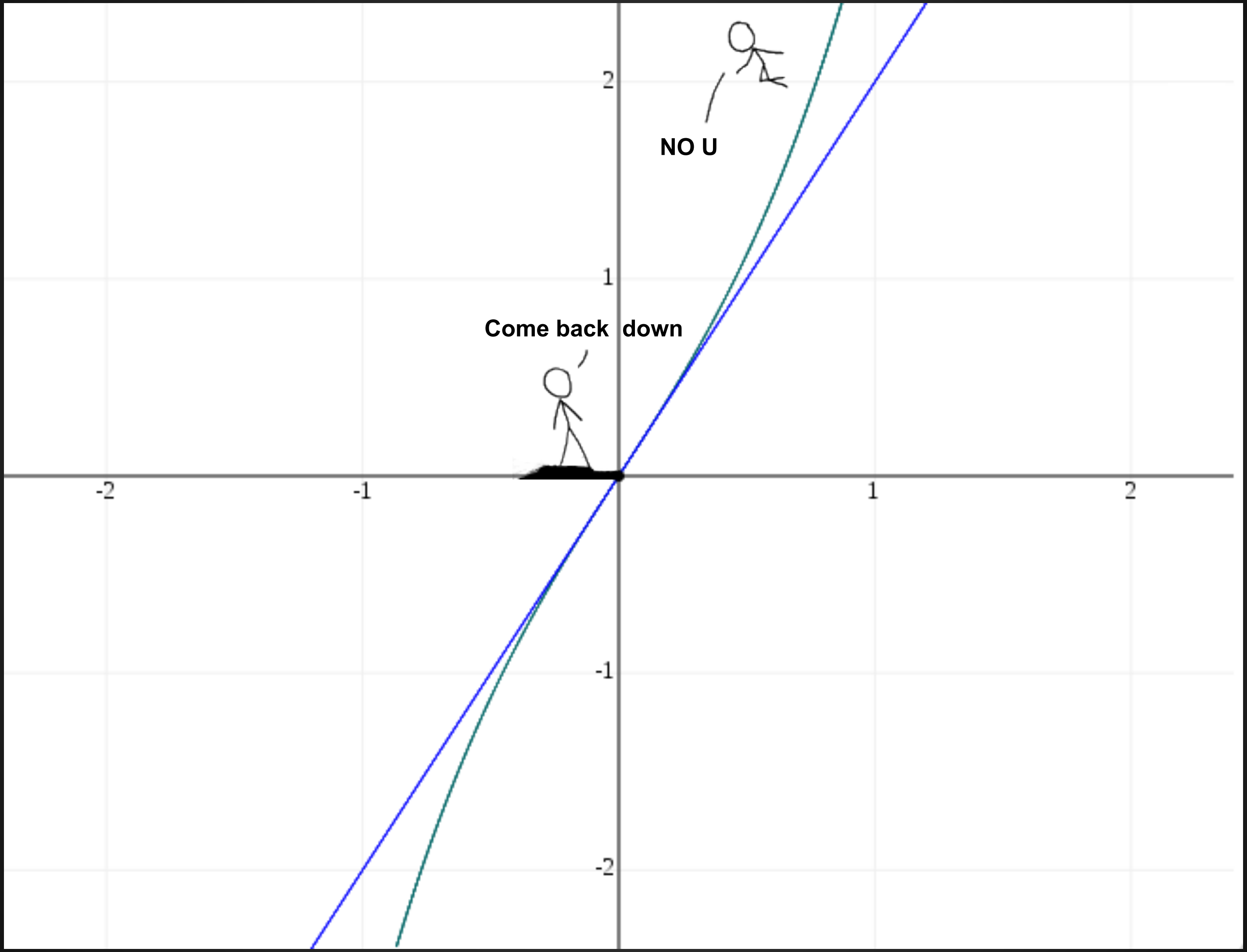
9001 RPM

vulnerable to shellolwut

Here we are now.



This is not Sol.


NO U
Come back down
2
1
-1
-2
-2
-1
1
2

Who dis bitch?

- Uni student at NSI TAFE, pursuing Bachelor of I.T in Network Security
- Constantly engrossed in Computer Security
- Areas of knowledge include: HUMINT, DFIR, R2I (RTI), SE, TSCM, acronyms
  Reconnaissance, Counterintelligence and Countersurveillance.
- Linux user since age of 9 (rm -rf /’d myself ONCE)
- Teach InfoSec topics and manage Security Laboratory @ Uni
- P.I.M.P (Packet Interception and Manipulation Professional)
- Aspiring Security Researcher

JTAG 101

- Joint Test Action Group, IEEE 1149.1
    - Standard for Test Access Port (TAP) and Boundary-Scan Architecture
    - Serial Data Port
    - Can include user-defined data registers and instructions

- Real World Applications
    - Scan boards, systems and chips
        - Design verification
        - Debugging
        - Field testing
        - Hardware/software integration
        - Diagnostics

JTAG 101

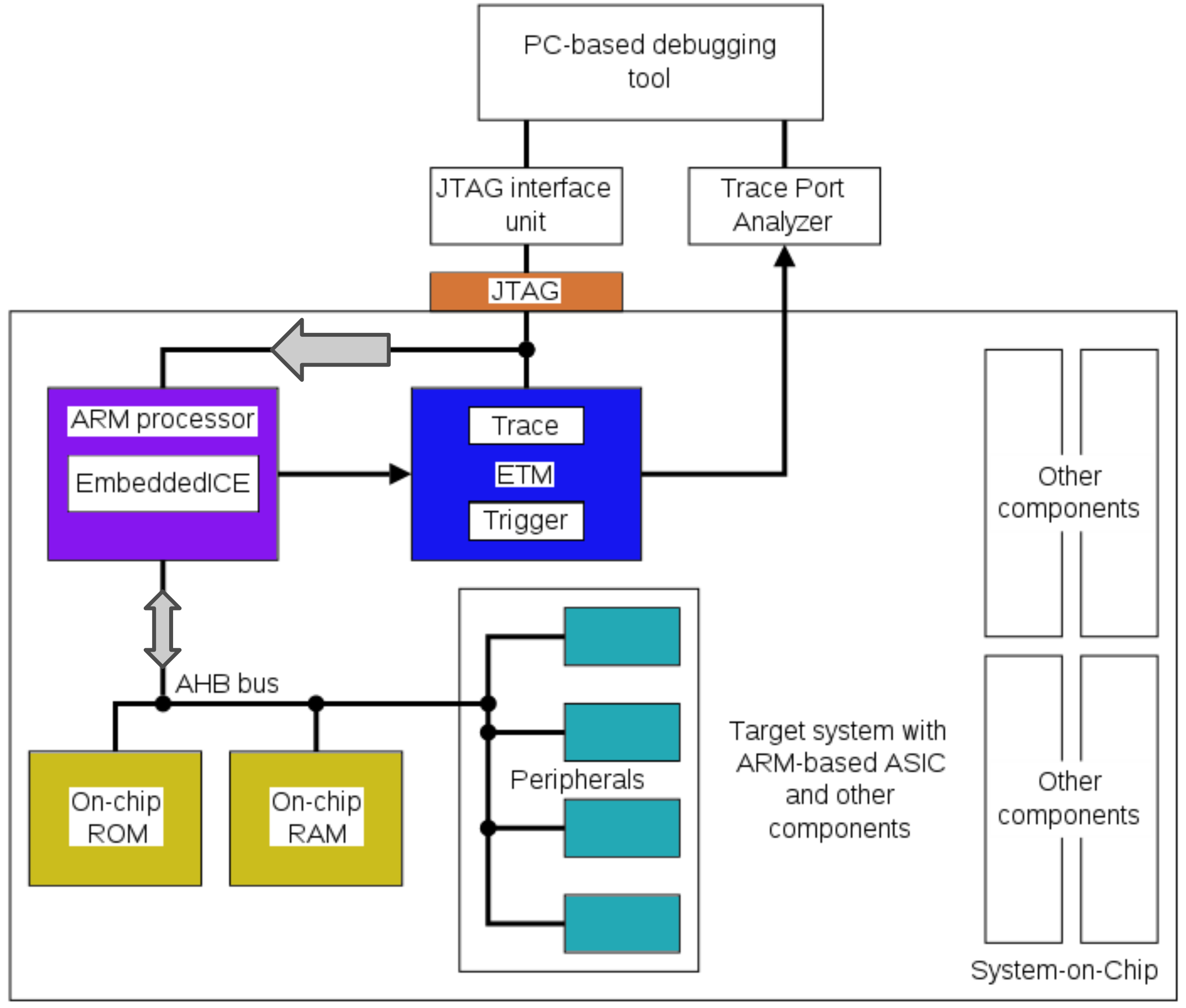
- Why implement into IC’s?
  - Can’t afford not to test
    - Risk of mass production of useless devices
    - Money down the silicon toilet
    - Delayed market entry
    - Test or get rekt

- Research and Development (Is JTAG for me?)
  - For the people who don’t fabricate and say “It works, trust me.”
    - Much more cost efficient to test
    - Designing with JTAG in mind isn’t that hard
    - Spider into all components

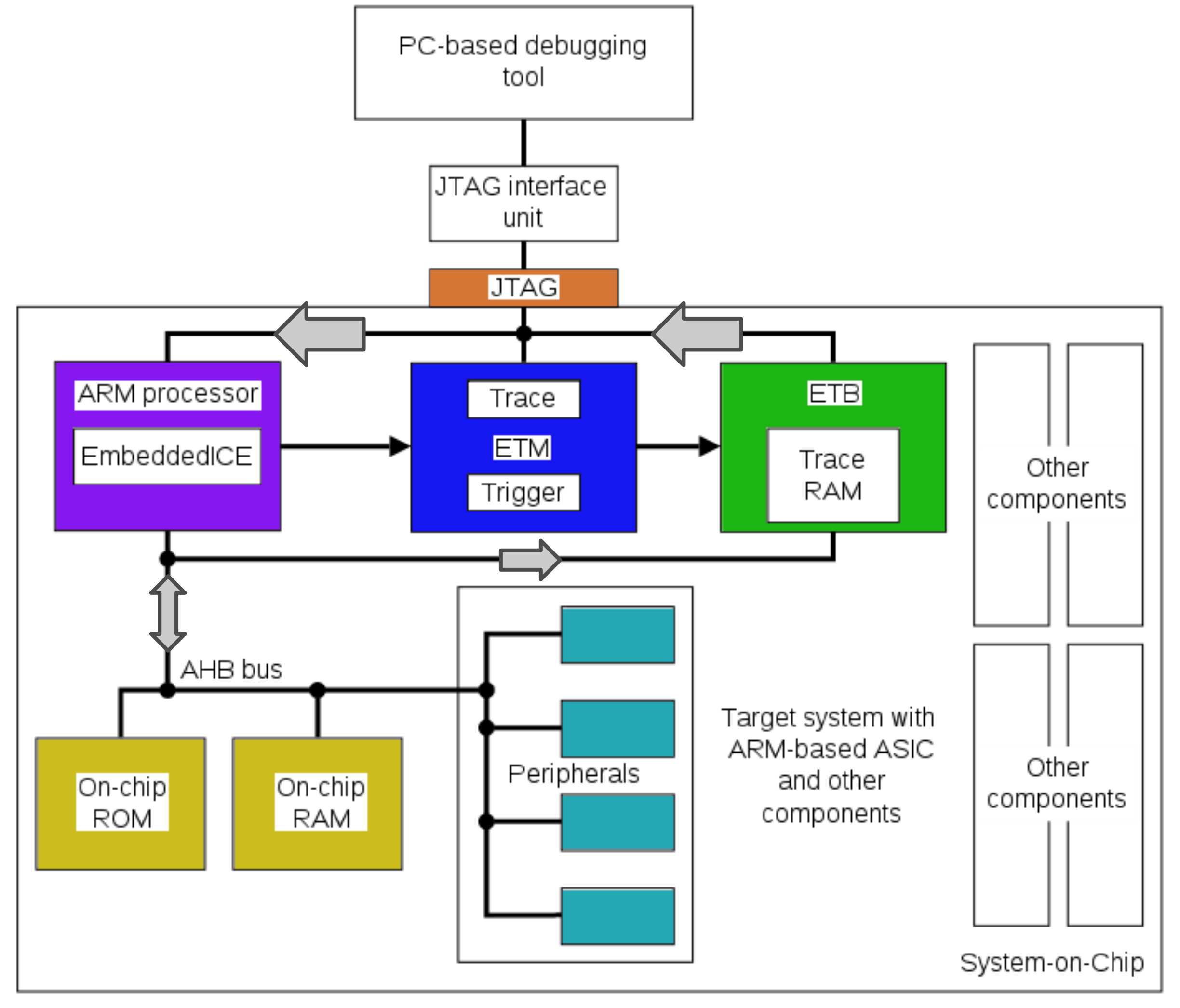
Benefits

- Less intrusive testing
- Easier to test alpha/beta models
- Verify devices on the assembly line
- Interact with device even if it’s in a non-bootable state
- Allows for manufacturer servicing
    - flashing
    - fault finding/diagnosing

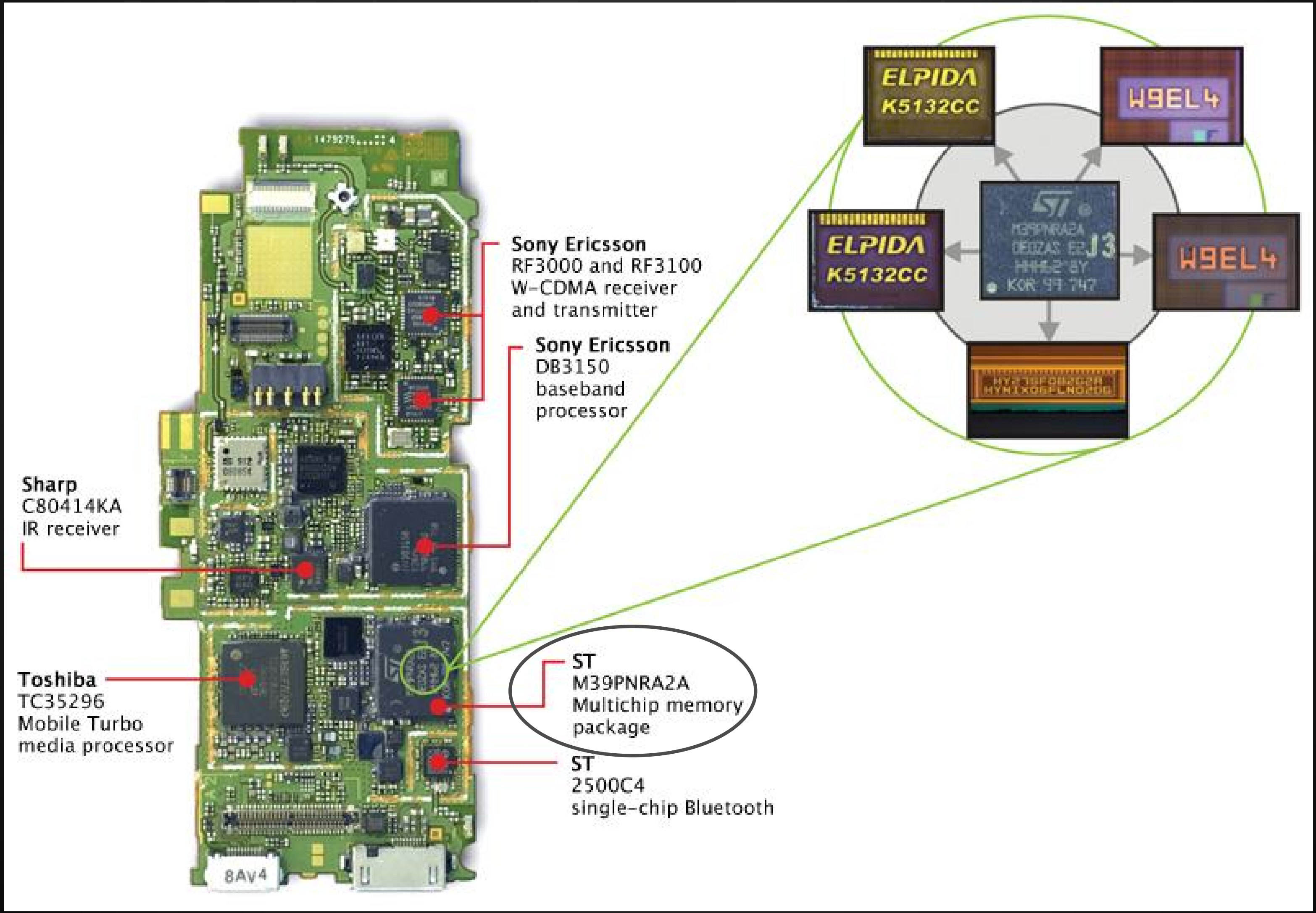
Trace Port Analyser



Embedded Trace Macrocell



Device complexity



Sony Ericsson
RF3000 and RF3100
W-CDMA receiver
and transmitter

Sony Ericsson
DB3150
baseband
processor

Sharp
C80414KA
IR receiver

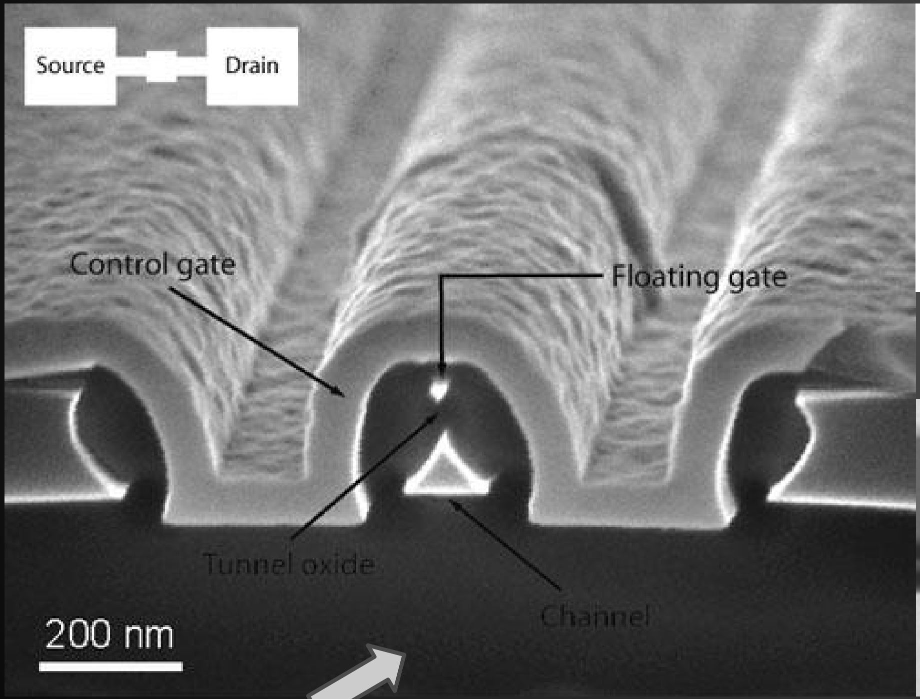
Toshiba
TC35296
Mobile Turbo
media processor

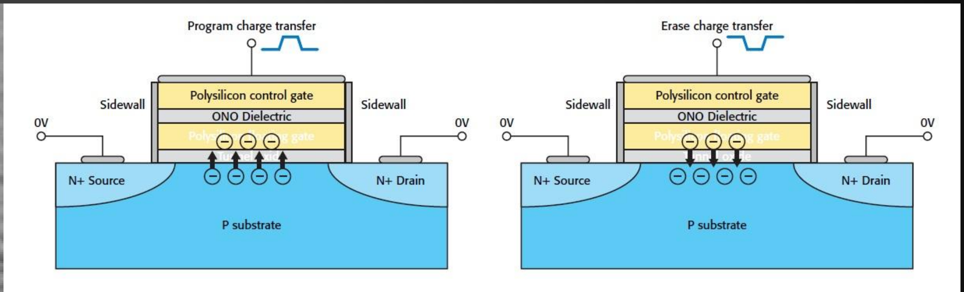
ST
M39PNRA2A
Multichip memory
package

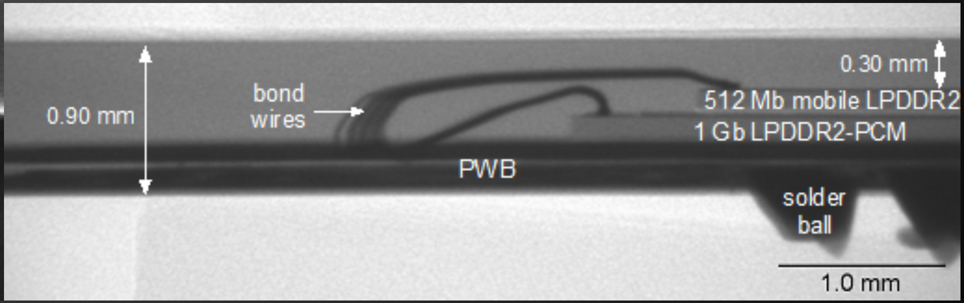
ST
2500C4
single-chip Bluetooth

NAND gates (of hell)

(electron micrograph)







Screams of the departed

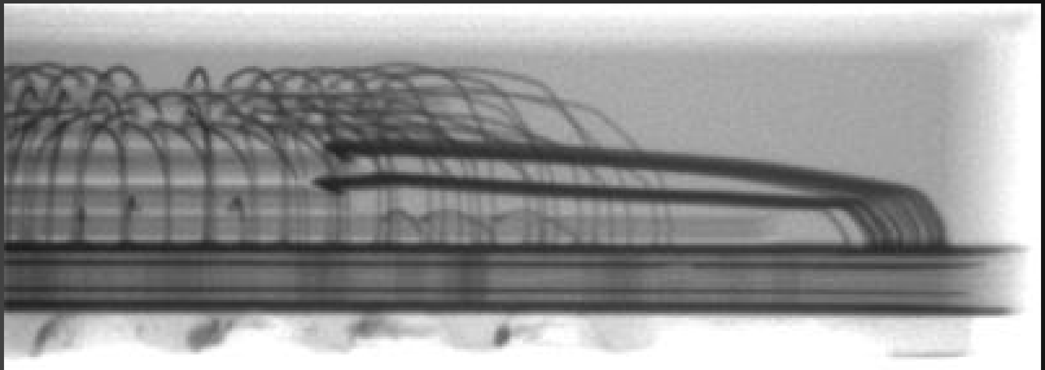
(precision XRAY)

STACK’EM (Silicon edition)

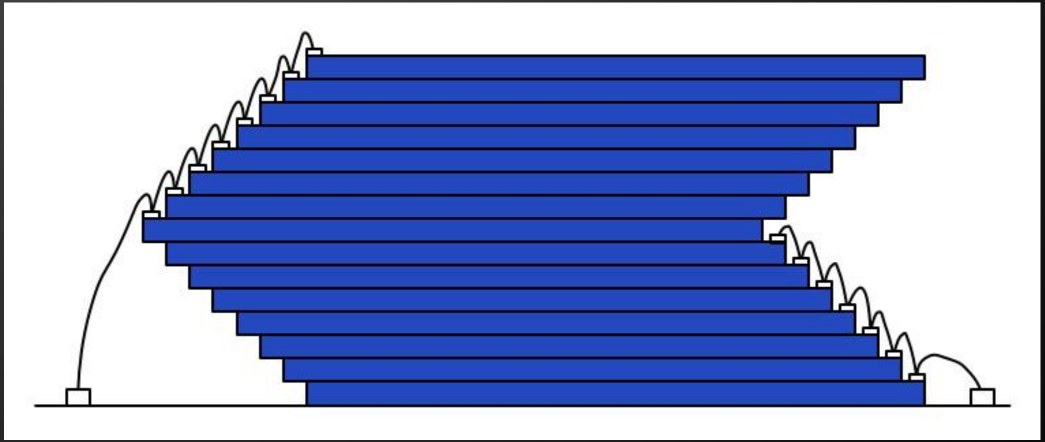
ST M39PNRA2A MCP

Top: 2x 512Mbit NOR
Mid: 1x 2Gbit SLC NAND
Low: 2x 512Mbit DDR2 SDRAM

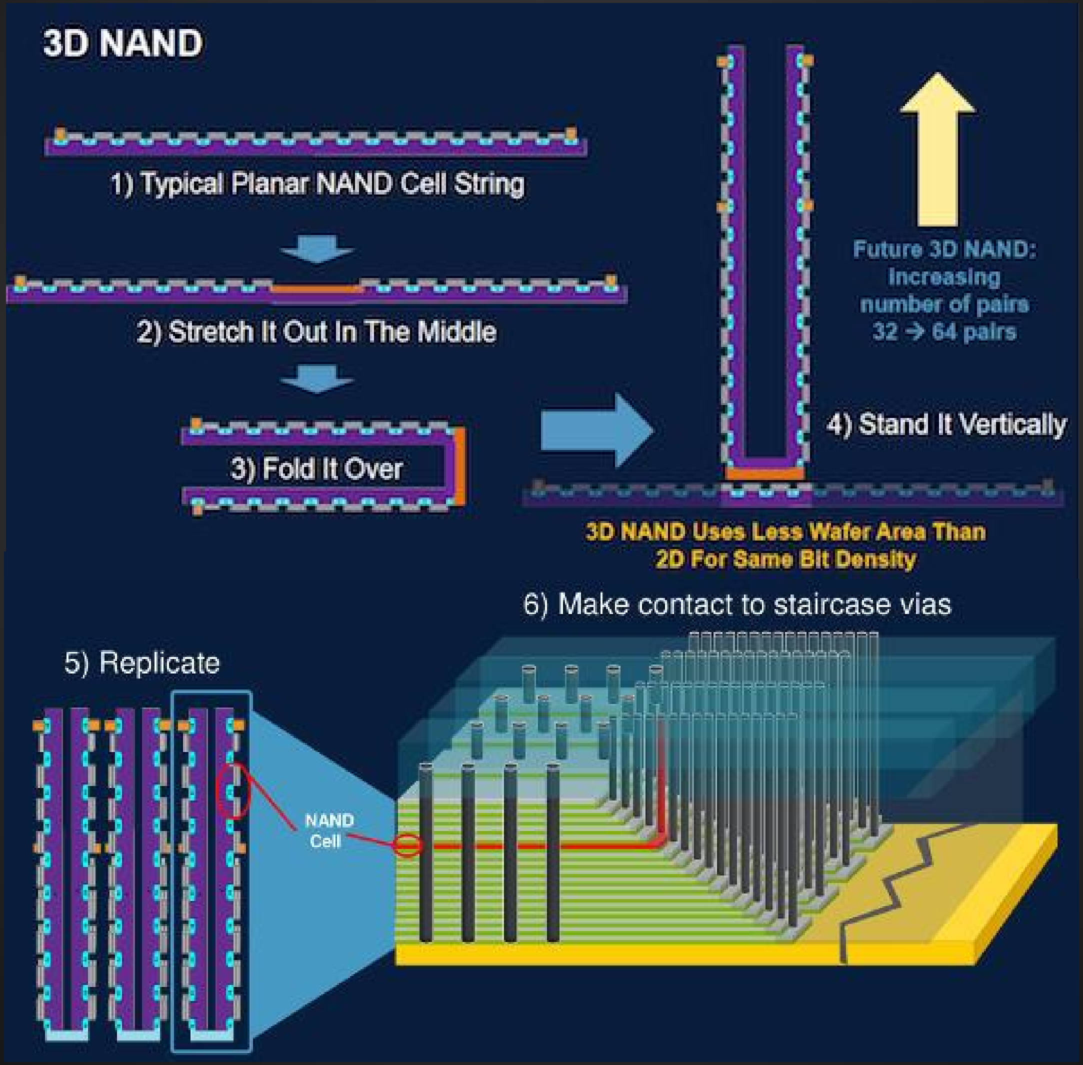
highly complex wire-up



K90KGY8S7M-CCK0
Samsung 840 ‘EVO’
1x 128GB TLC NAND
(Graphical representation as
no XRAY available)



STACK’EM (Silicon edition)



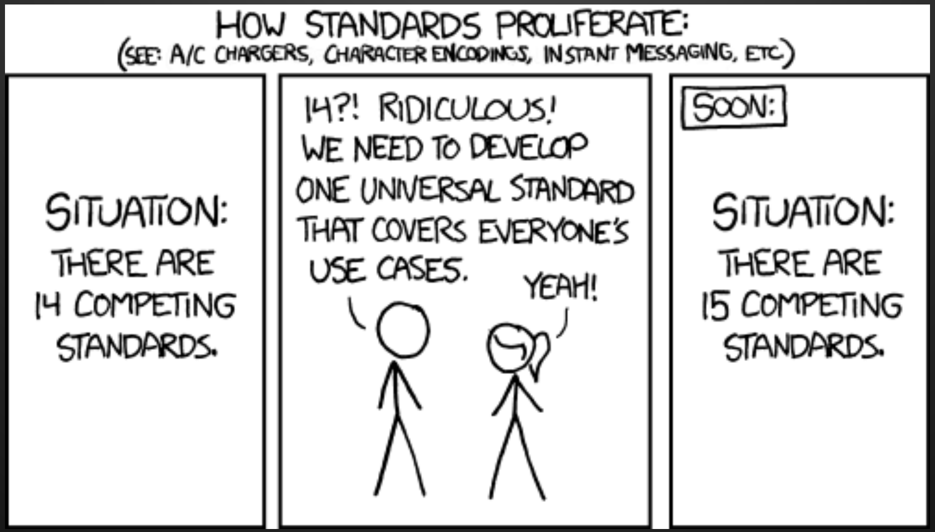
3D NAND
1) Typical Planar NAND Cell String
2) Stretch It Out In The Middle
3) Fold It Over
4) Stand It Vertically
Future 3D NAND: Increasing number of pairs 32 → 64 pairs
3D NAND Uses Less Wafer Area Than 2D For Same Bit Density
5) Replicate
NAND Cell
6) Make contact to staircase vias

How was that relevant?

- MCP means more types of memory in a single package
- Interfaces become more and more complex
- Proprietary BGA’s (info available only for LEA and/or via NDA channels)
- New memory types change the game
- New challenges with each evolution (filesystem, software, physical)
- No swiss army knife (unless you can afford highly custom $500K++ solutions)
  - Netherlands Forensic Institute (NFI) (still not a swiss army knife)
    - MTK I/II (Memory Toolkit)

There can’t be that many BGA’s?

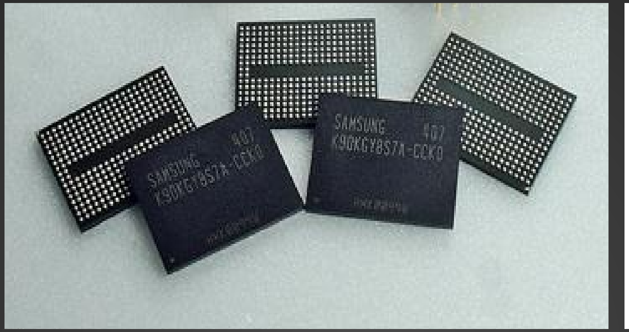
CABGA, CBGA, PBGA, CTBGA, CVBGA, DSBGA, FBGA, FCmBGA, LBGA, LFBGA, MBGA, MCM-PBGA, PBGA, SBGA, TABGA, TBGA, TEPBGA, TFBGA, UFBGA, UBGA, VFBGA, WFBGA…

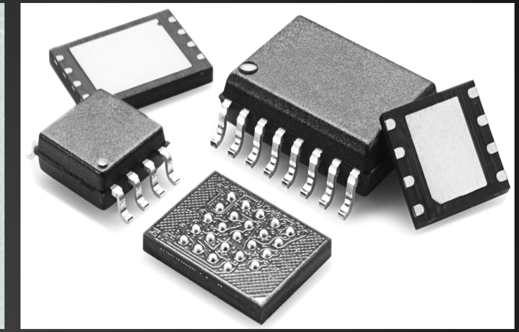

HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Credit: XKCD

What are we dealing with?

Flash Memory

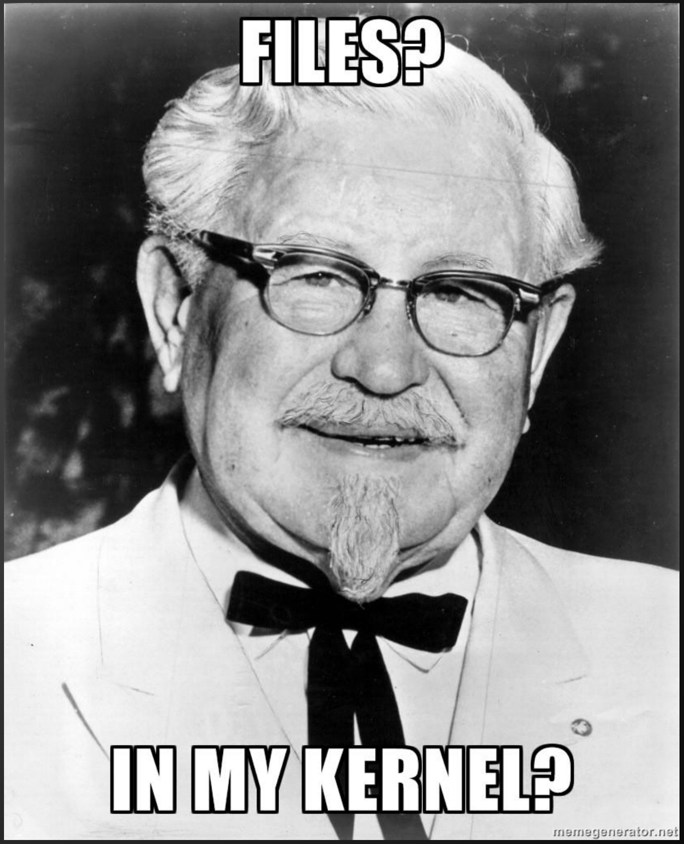




Memory type	SLC/MLC/TLC (Samsung)	NOR cells
Density	High, 512Mb to 128Gb	Average, 16Mb to 1Gb
Read/Write performance	25MB/s++ ; 8MB/s ++	100MB/s++ ; 0.42MB/s+
Power consumption	Low	Moderate
Access type	Indirect access via controller	Random access
Use cases	Media devices, GPS, Memory cards	Real-time telemetry, RTOS, Reference navigation

What else are we dealing with?

- Different File Systems
  - ext4
  - FAT16/32
  - Samsung RFS
  - YAFFS/YAFFS2
    - Yet Another Flash File System
  - Other proprietary file systems
    - They just love to bake their own



Device seizure

- Isolate device from all types of RF communication
  - Faraday bags and RF isolation boxes

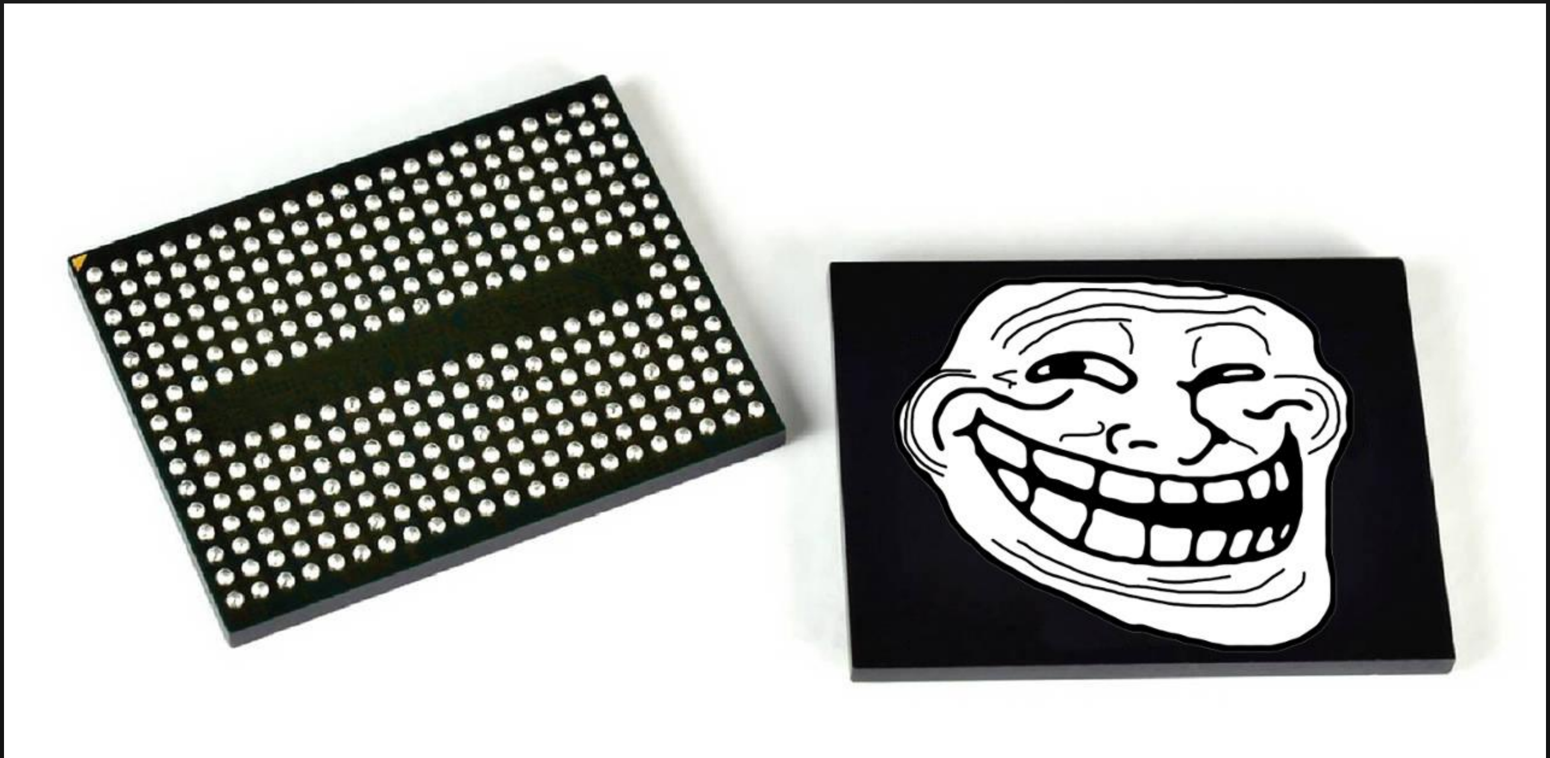
- Turning the device off? **Think again**.
  - FDE, PIN/Password protection
  - Potential TRIM as device executes shutdown scripts
  - If device RAM is outside of your forensic teams' capabilities, here is the world's smallest violin for you.

Device seizure

- Take detailed notes of the device at the time of seizure
    - Observe environment the device is in
    - Determine if WiFi networks are in use
    - Gather as much data about how the device is running before deciding to shut it down or isolate it.
    - DETAILED NOTES (You can make a horrible mistake here)
    - I don’t care how long this list is because it will never be long enough
    - WRITE FASTER DAMMIT (Time is of the essence)
    - Evaluate value of data held on device
    - Isolate device OR begin acquisition
    - ???
    - Profit
    - Too much to keep in mind and every case is unique

Forensic argument

The acquisition of flash memory in mobile devices is **not forensically sound.**



What say I?

From a forensic perspective, no modifying instructions (write, erase or otherwise) should ever be communicated to the target device during the process of acquiring evidence.

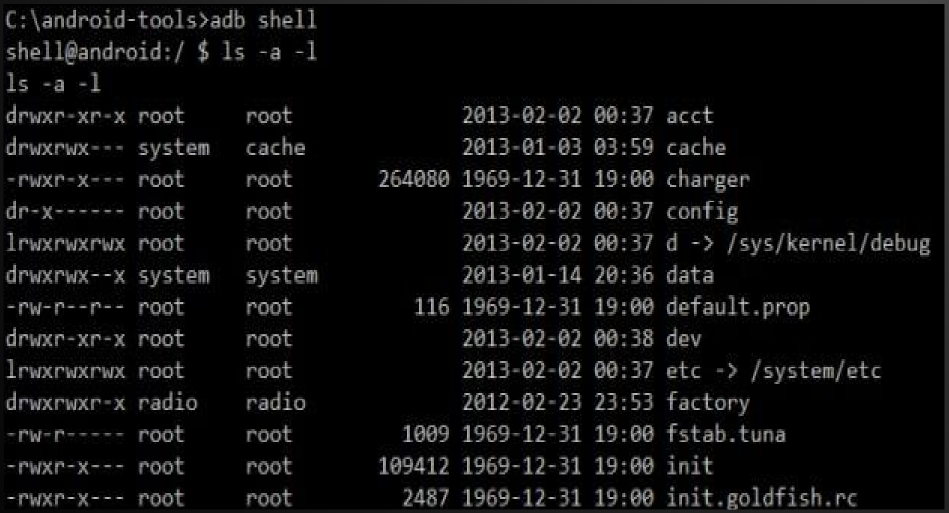
As a result any data acquired in such a manner would still be admissible, with the exception that some evidence might have been lost due to circumstances beyond the examiners control. However, this would impact repeatability.

Methods of acquisition

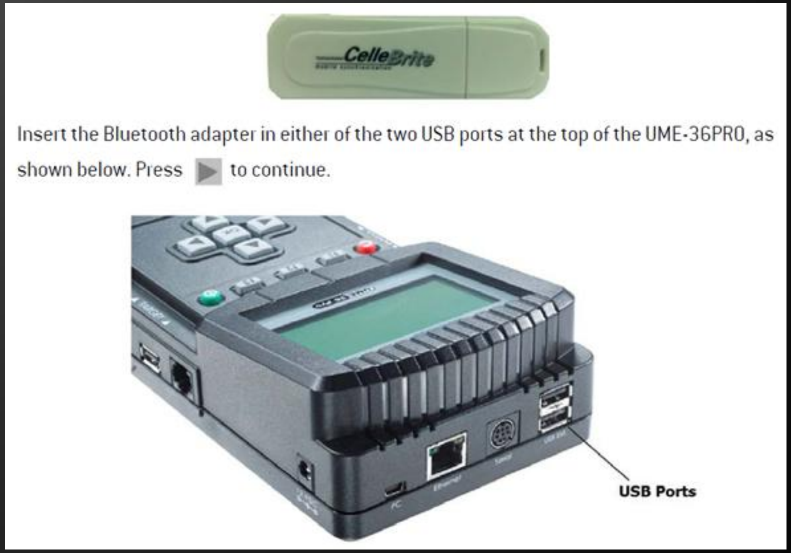
- Manual
    - HIGH Potential for evidence loss
    - Requires examiner to interact with device
    - No protection against data being written
    - NOT forensically sound from a digital forensics perspective
    - Questionable admissibility
    - Last resort

Methods of acquisition

- Logical
  - Wired (USB), Bluetooth, IrDA, WiFi
  - Bit for bit copies of files and directories
  - ADB, AT modem commands, BlueSnarfing and more
  - Questionably sound: modifying bootloaders, uploading binaries to device, requires some level of modification
  - Can impact repeatability if incorrectly done



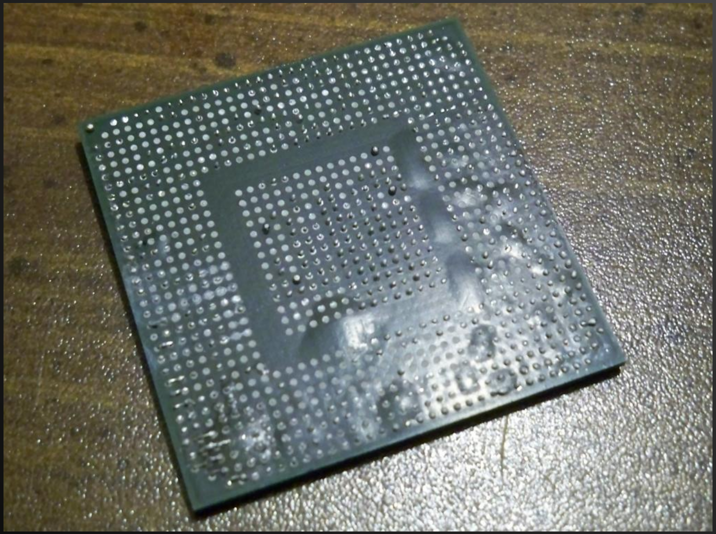
```
C:\android-tools>adb shell
shell@android:/ $ ls -a -l
ls -a -l
drwxr-xr-x root     root              2013-02-02 00:37 acct
drwxrwx--- system   cache             2013-01-03 03:59 cache
-rwxr-x--- root     root       264080 1969-12-31 19:00 charger
dr-x------ root     root              2013-02-02 00:37 config
lrwxrwxrwx root     root              2013-02-02 00:37 d -> /sys/kernel/debug
drwxrwx--x system   system            2013-01-14 20:36 data
-rw-r--r-- root     root          116 1969-12-31 19:00 default.prop
drwxr-xr-x root     root              2013-02-02 00:38 dev
lrwxrwxrwx root     root              2013-02-02 00:37 etc -> /system/etc
drwxrwxr-x radio    radio             2012-02-23 23:53 factory
-rw-r----- root     root         1009 1969-12-31 19:00 fstab.tuna
-rwxr-x--- root     root       109412 1969-12-31 19:00 init
-rwxr-x--- root     root         2487 1969-12-31 19:00 init.goldfish.rc
```

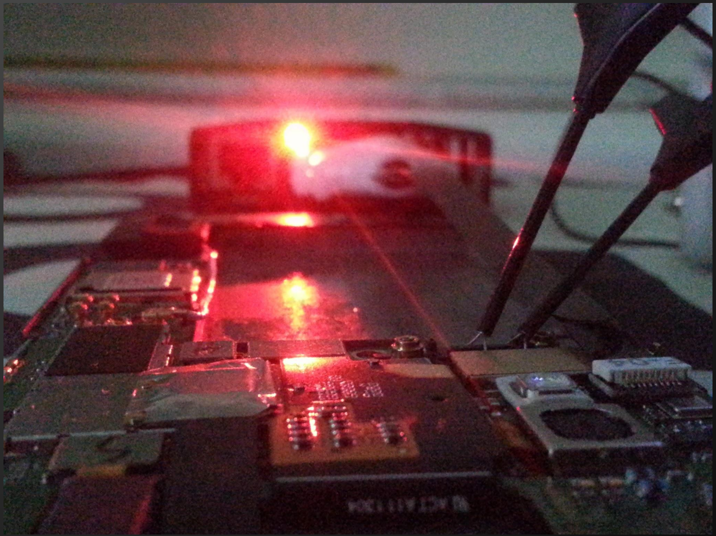


Insert the Bluetooth adapter in either of the two USB ports at the top of the UME-36PRO, as shown below. Press ▶ to continue.

Methods of acquisition

- Physical
  - Everything!
    - Bitstream copy of entire memory space
    - Deleted data (except where the controller has TRIM'd)
  - Holy grail of evidence acquisition
  - JTAG, Chip-off or Micro Read
  - Forensically sound!



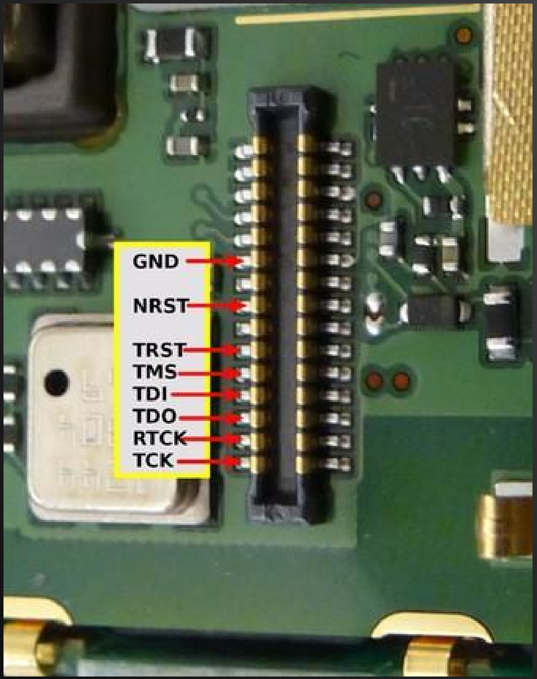


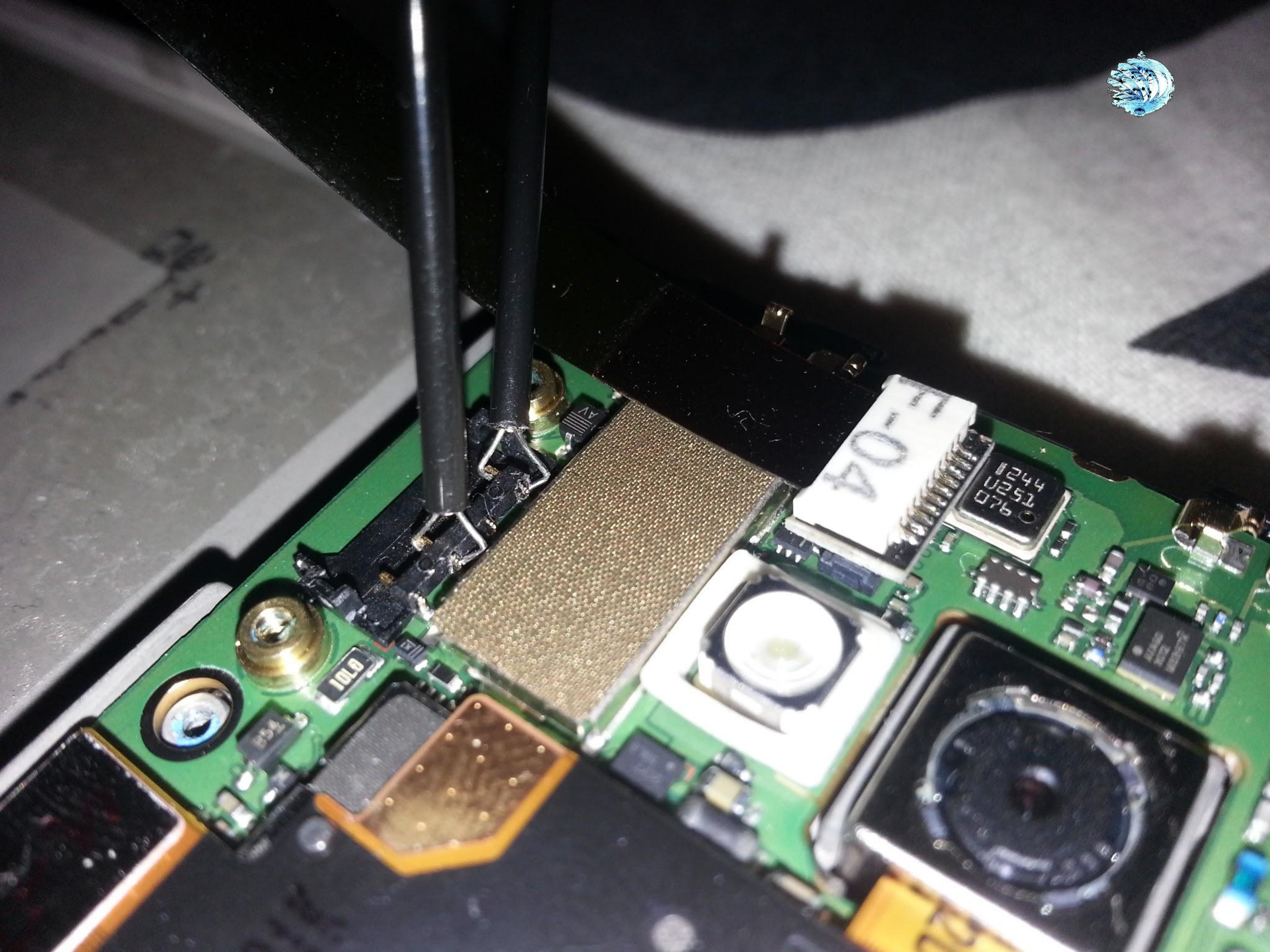
Everything used

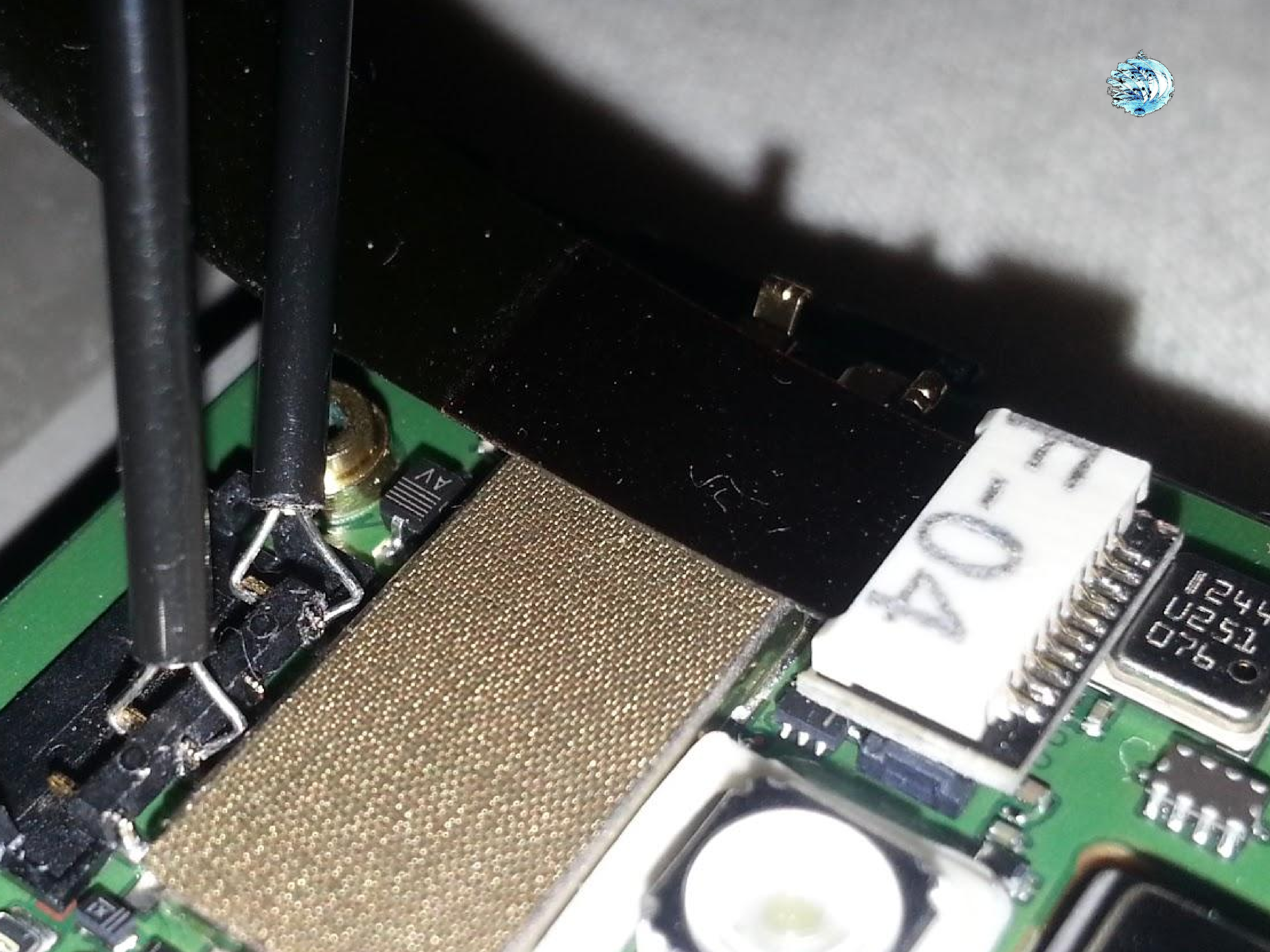
Item	Price (AUD)
RIFF Box (JTAG hardware)	~$120
Atten Instruments TPR3005T Regulated DC Power Supply	~$110
2 x LG E960 Nexus 4	$280+ $230
GPG JPIN adapter, JIG PCB’s and flat cables	$50
2 x Pomona Micro Grabbers (these are the best)	$5
Copper-silver wires	$0
Total spent	~$800

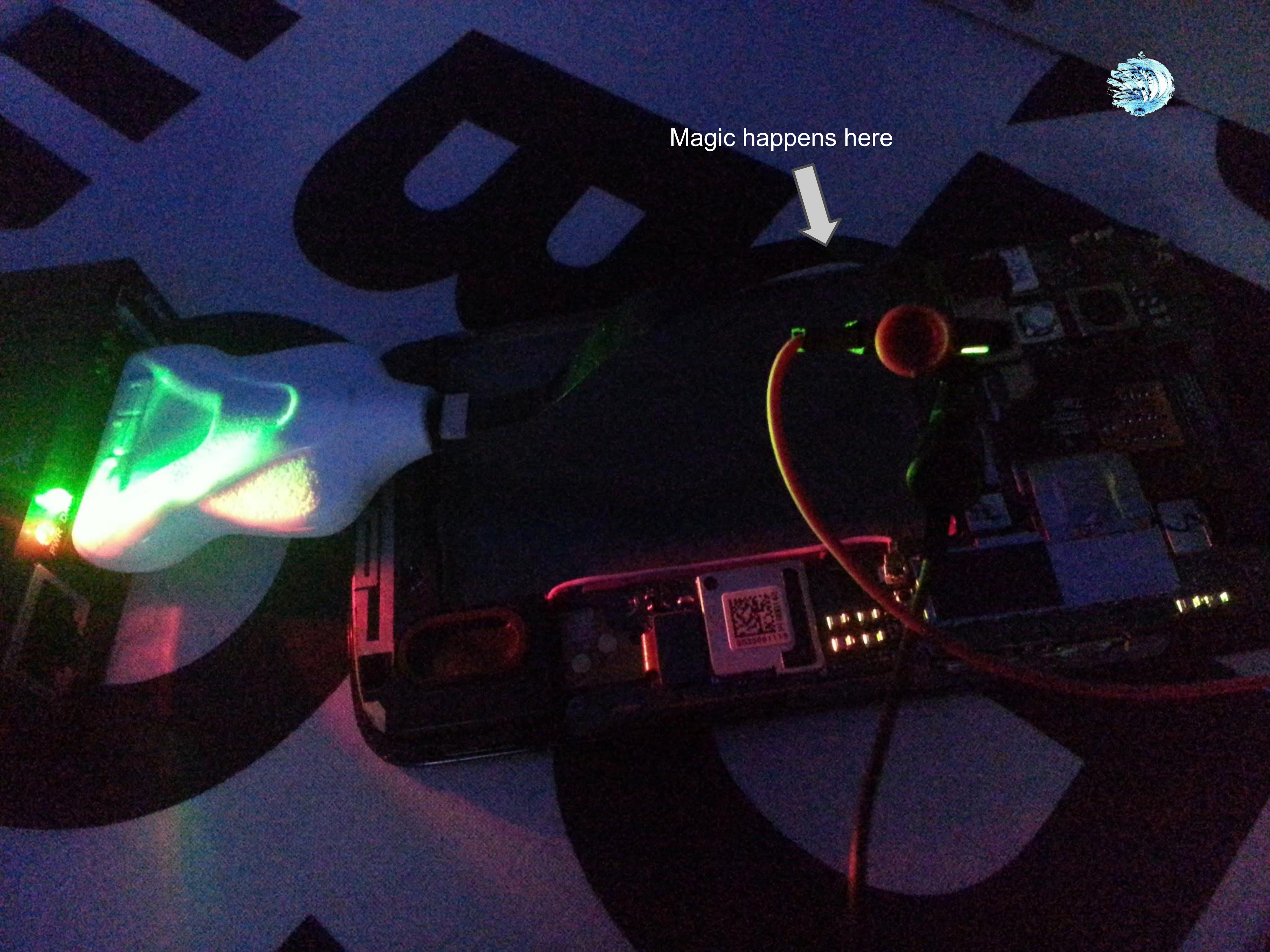
Setting up the device

- Ensure a stable power source is in use
  - Atten Instruments TPR3005T
  - Battery power or USB power not enough
  - Set to 3.80V/2.1A at first and varied for stable connection to device
  - Current draw varies, good to provide more in case of spikes




E-04
1244
U251
076
AV
IOL0

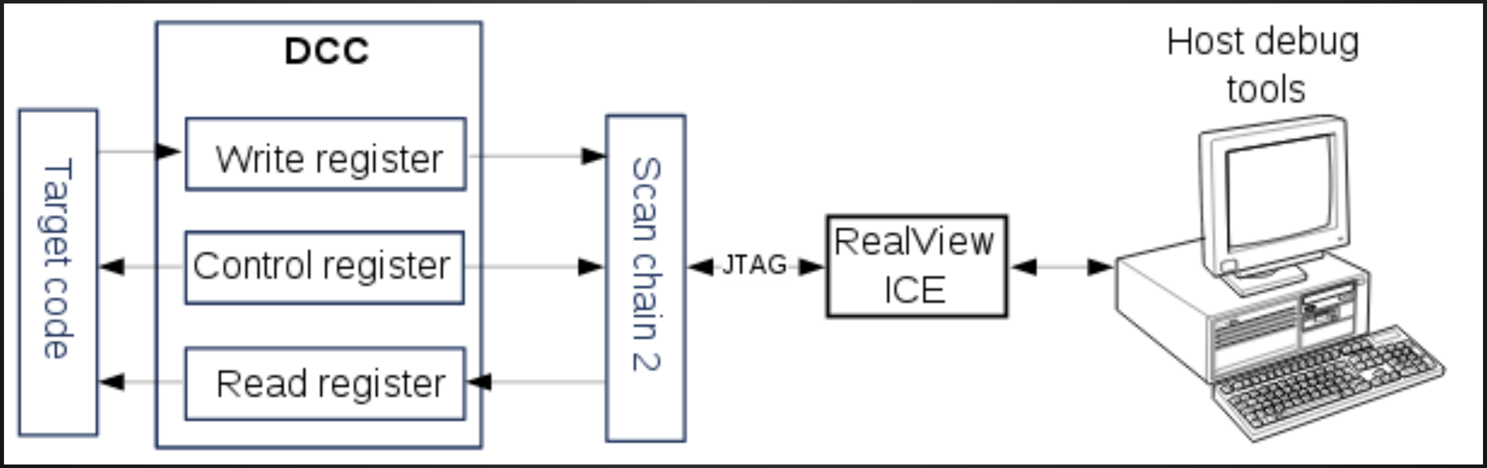

AV
E-04
244
U251
076

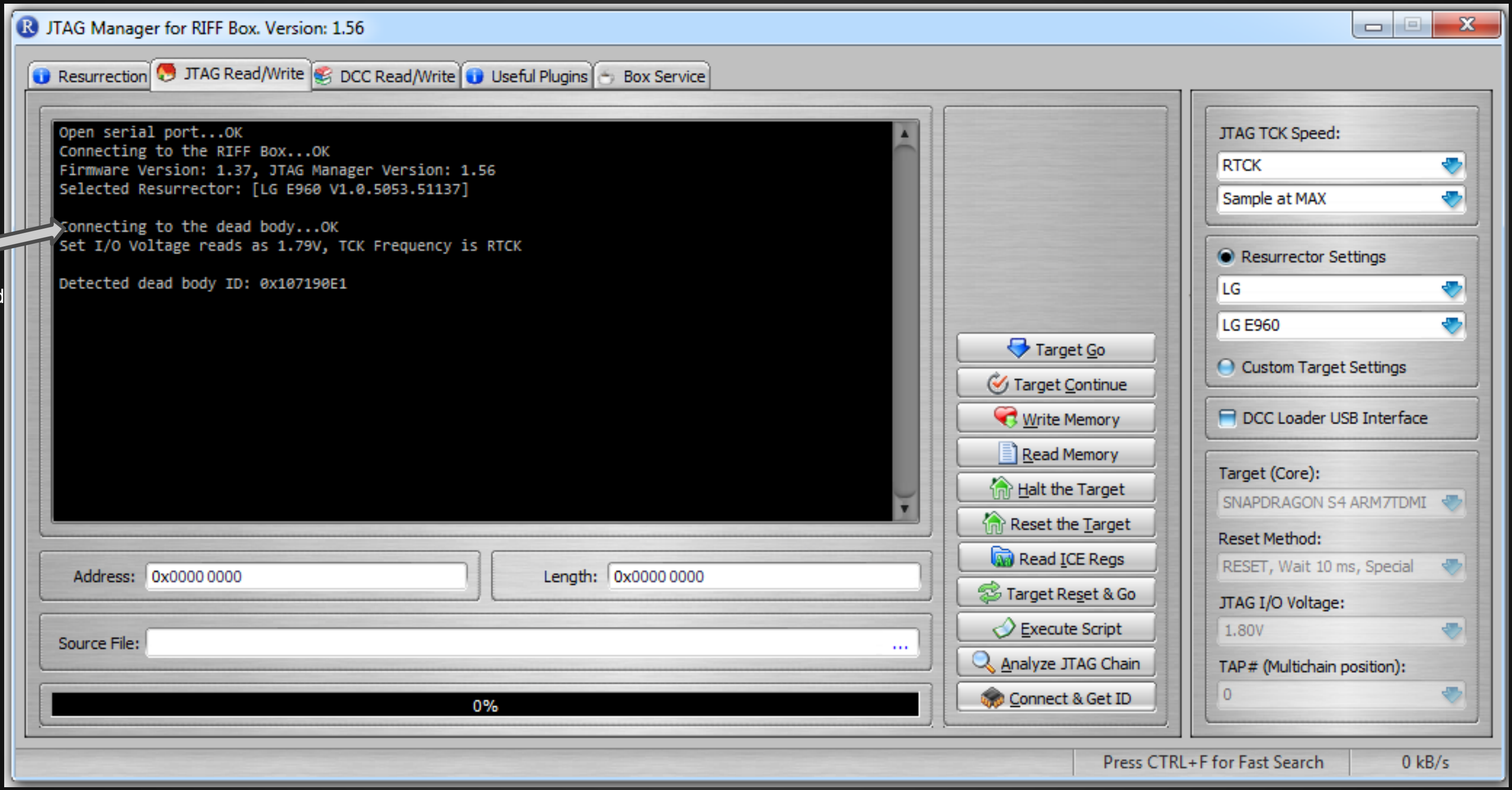


Magic happens here

DCC? IRC?

- DCC Loader - Debug Communications Channel
    - Communication interface between the loader code running in memory and the JTAG software
    - Instructions are communicated through DCC





```
Open serial port...OK
Connecting to the RIFF Box...OK
Firmware Version: 1.37, JTAG Manager Version: 1.56
Selected Resurrector: [LG E960 V1.0.5053.51137]

Connecting to the dead body...OK
Set I/O Voltage reads as 1.79V, TCK Frequency is RTCK

Detected dead body ID: 0x107190E1
```

Address: 0x0000 0000

Length: 0x0000 0000

Source File: ...

0%

JTAG TCK Speed: RTCK

Sample at MAX

● Resurrector Settings

LG

LG E960

○ Custom Target Settings

□ DCC Loader USB Interface

Target (Core): SNAPDRAGON S4 ARM7TDMI

Reset Method: RESET, Wait 10 ms, Special

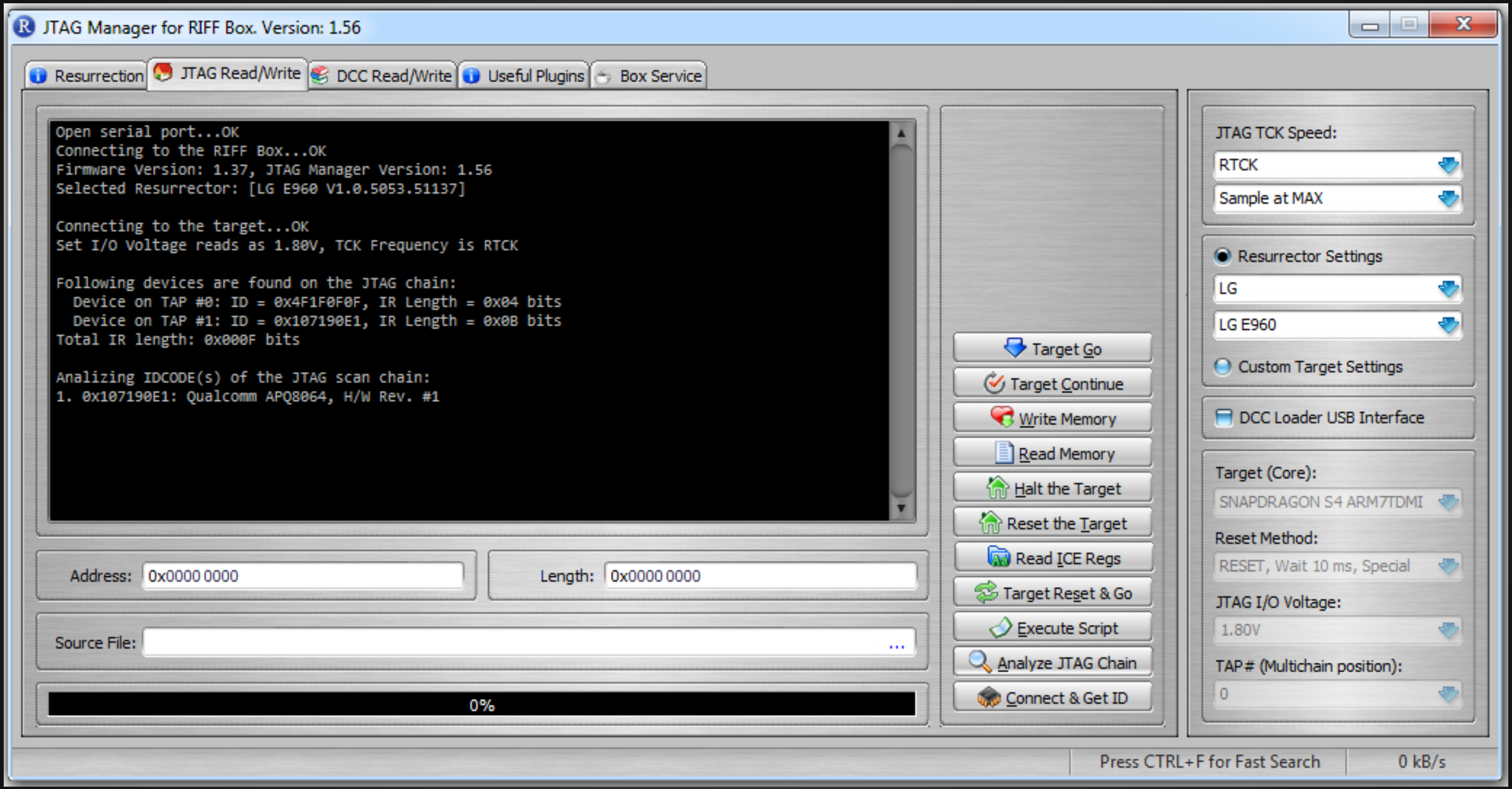
JTAG I/O Voltage: 1.80V

TAP# (Multichain position): 0

Press CTRL+F for Fast Search

0 kB/s

Dead people
can be JTAG'd



JTAG Manager for RIFF Box. Version: 1.56

```
Open serial port...OK
Connecting to the RIFF Box...OK
Firmware Version: 1.37, JTAG Manager Version: 1.56
Selected Resurrector: [LG E960 V1.0.5053.51137]

Connecting to the target...OK
Set I/O Voltage reads as 1.80V, TCK Frequency is RTCK

Following devices are found on the JTAG chain:
  Device on TAP #0: ID = 0x4F1F0F0F, IR Length = 0x04 bits
  Device on TAP #1: ID = 0x107190E1, IR Length = 0x0B bits
Total IR length: 0x000F bits

Analizing IDCODE(s) of the JTAG scan chain:
1. 0x107190E1: Qualcomm APQ8064, H/W Rev. #1
```

Address: 0x0000 0000

Length: 0x0000 0000

Source File: ...

0%

JTAG TCK Speed: RTCK

Sample at MAX

● Resurrector Settings

LG

LG E960

○ Custom Target Settings

□ DCC Loader USB Interface

Target (Core): SNAPDRAGON S4 ARM7TDMI

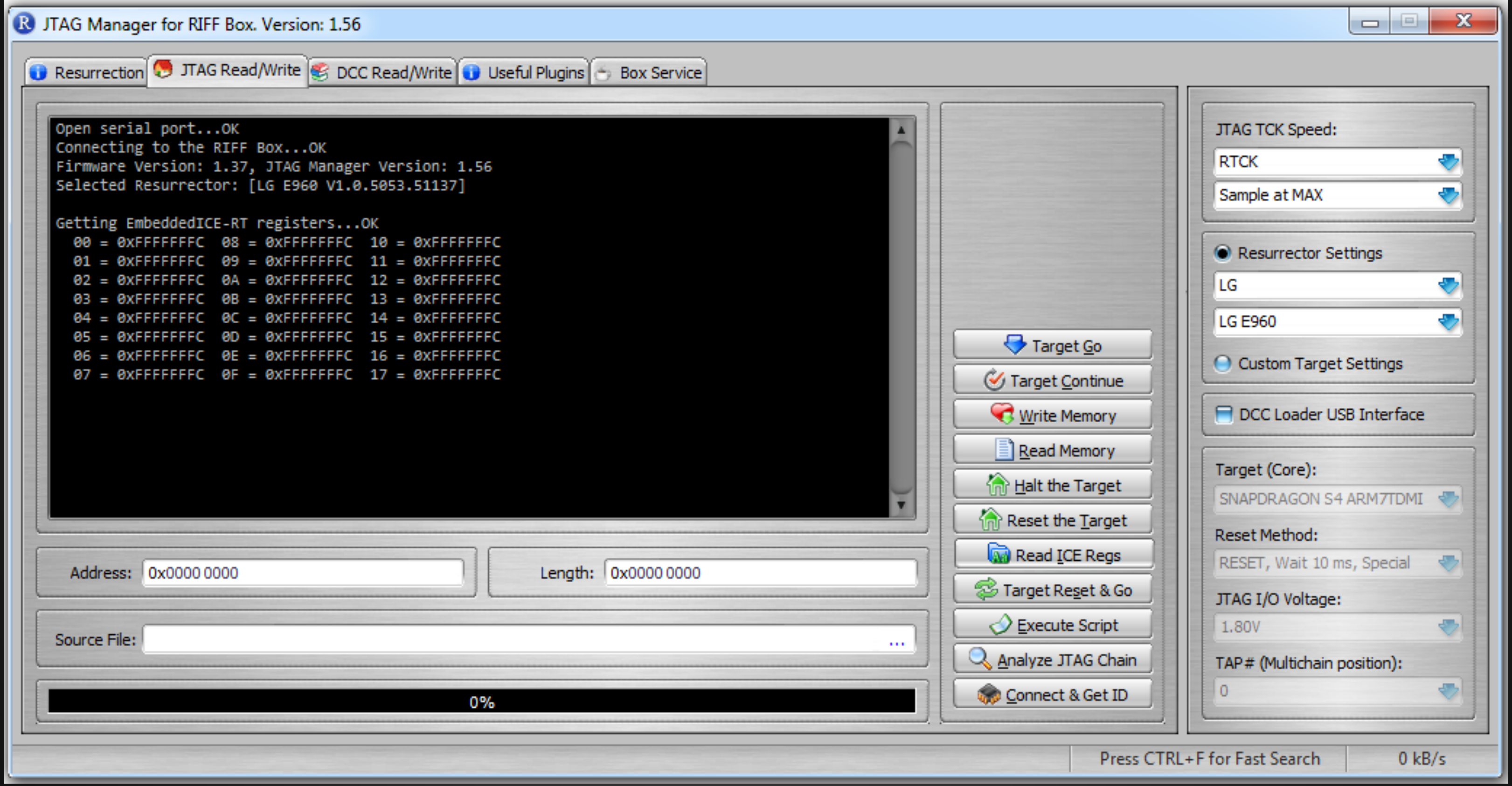
Reset Method: RESET, Wait 10 ms, Special

JTAG I/O Voltage: 1.80V

TAP# (Multichain position): 0

Press CTRL+F for Fast Search

0 kB/s



JTAG Manager for RIFF Box. Version: 1.56

```
Open serial port...OK
Connecting to the RIFF Box...OK
Firmware Version: 1.37, JTAG Manager Version: 1.56
Selected Resurrector: [LG E960 V1.0.5053.51137]

Getting EmbeddedICE-RT registers...OK
  00 = 0xFFFFFFFC  08 = 0xFFFFFFFC  10 = 0xFFFFFFFC
  01 = 0xFFFFFFFC  09 = 0xFFFFFFFC  11 = 0xFFFFFFFC
  02 = 0xFFFFFFFC  0A = 0xFFFFFFFC  12 = 0xFFFFFFFC
  03 = 0xFFFFFFFC  0B = 0xFFFFFFFC  13 = 0xFFFFFFFC
  04 = 0xFFFFFFFC  0C = 0xFFFFFFFC  14 = 0xFFFFFFFC
  05 = 0xFFFFFFFC  0D = 0xFFFFFFFC  15 = 0xFFFFFFFC
  06 = 0xFFFFFFFC  0E = 0xFFFFFFFC  16 = 0xFFFFFFFC
  07 = 0xFFFFFFFC  0F = 0xFFFFFFFC  17 = 0xFFFFFFFC
```

Address: 0x0000 0000

Length: 0x0000 0000

Source File:

0%

JTAG TCK Speed: RTCK

Sample at MAX

● Resurrector Settings

LG

LG E960

○ Custom Target Settings

□ DCC Loader USB Interface

Target (Core): SNAPDRAGON S4 ARM7TDMI

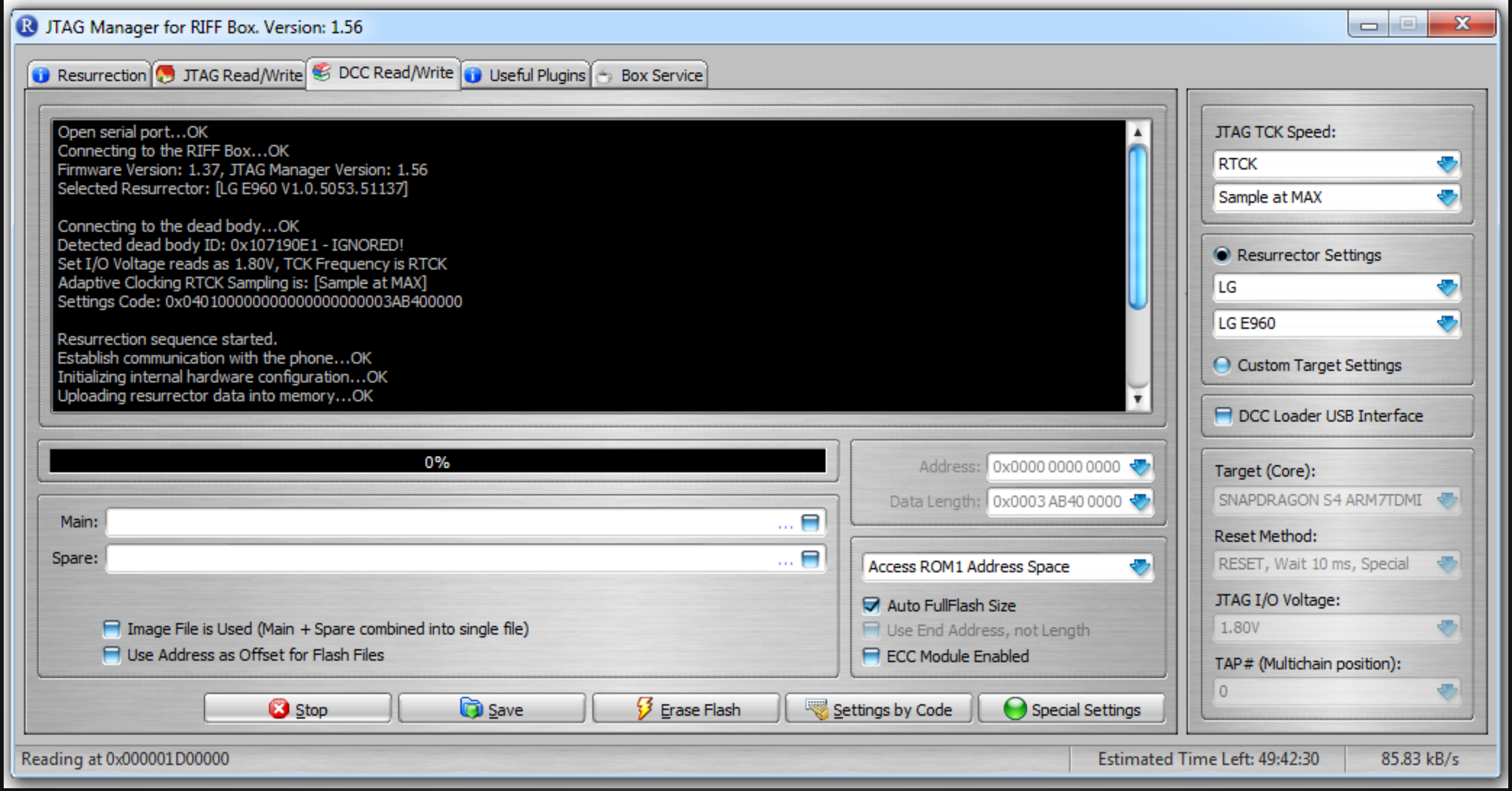
Reset Method: RESET, Wait 10 ms, Special

JTAG I/O Voltage: 1.80V

TAP# (Multichain position): 0

Press CTRL+F for Fast Search

0 kB/s



```
Open serial port...OK
Connecting to the RIFF Box...OK
Firmware Version: 1.37, JTAG Manager Version: 1.56
Selected Resurrector: [LG E960 V1.0.5053.51137]

Connecting to the dead body...OK
Detected dead body ID: 0x107190E1 - IGNORED!
Set I/O Voltage reads as 1.80V, TCK Frequency is RTCK
Adaptive Clocking RTCK Sampling is: [Sample at MAX]
Settings Code: 0x04010000000000000000000003AB400000

Resurrection sequence started.
Establish communication with the phone...OK
Initializing internal hardware configuration...OK
Uploading resurrector data into memory...OK
```

0%

Main:

Spare:

□ Image File is Used (Main + Spare combined into single file)

□ Use Address as Offset for Flash Files

Address: 0x0000 0000 0000

Data Length: 0x0003 AB40 0000

Access ROM1 Address Space

☑ Auto FullFlash Size

□ Use End Address, not Length

□ ECC Module Enabled

JTAG TCK Speed: RTCK

Sample at MAX

● Resurrector Settings

LG

LG E960

○ Custom Target Settings

□ DCC Loader USB Interface

Target (Core): SNAPDRAGON S4 ARM7TDMI

Reset Method: RESET, Wait 10 ms, Special

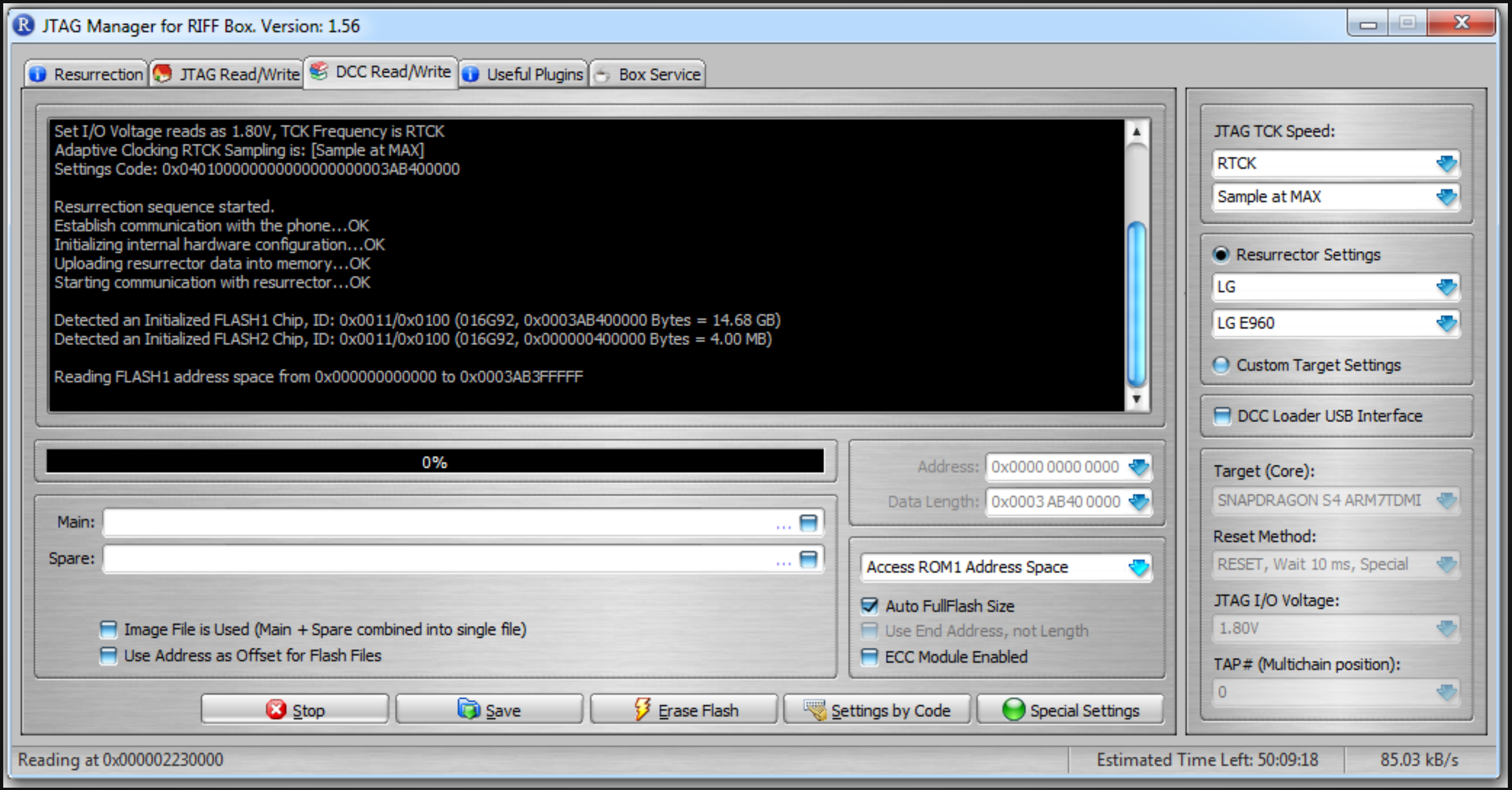
JTAG I/O Voltage: 1.80V

TAP# (Multichain position): 0

Reading at 0x000001D00000

Estimated Time Left: 49:42:30

85.83 kB/s



```
Set I/O Voltage reads as 1.80V, TCK Frequency is RTCK
Adaptive Clocking RTCK Sampling is: [Sample at MAX]
Settings Code: 0x04010000000000000000000003AB400000

Resurrection sequence started.
Establish communication with the phone...OK
Initializing internal hardware configuration...OK
Uploading resurrector data into memory...OK
Starting communication with resurrector...OK

Detected an Initialized FLASH1 Chip, ID: 0x0011/0x0100 (016G92, 0x0003AB400000 Bytes = 14.68 GB)
Detected an Initialized FLASH2 Chip, ID: 0x0011/0x0100 (016G92, 0x000000400000 Bytes = 4.00 MB)

Reading FLASH1 address space from 0x000000000000 to 0x0003AB3FFFFF
```

0%

Main:

Spare:

□ Image File is Used (Main + Spare combined into single file)

□ Use Address as Offset for Flash Files

Address: 0x0000 0000 0000

Data Length: 0x0003 AB40 0000

Access ROM1 Address Space

☑ Auto FullFlash Size

□ Use End Address, not Length

□ ECC Module Enabled

JTAG TCK Speed:

RTCK

Sample at MAX

● Resurrector Settings

LG

LG E960

○ Custom Target Settings

□ DCC Loader USB Interface

Target (Core): SNAPDRAGON S4 ARM7TDMI

Reset Method: RESET, Wait 10 ms, Special

JTAG I/O Voltage: 1.80V

TAP# (Multichain position): 0

Reading at 0x000002230000

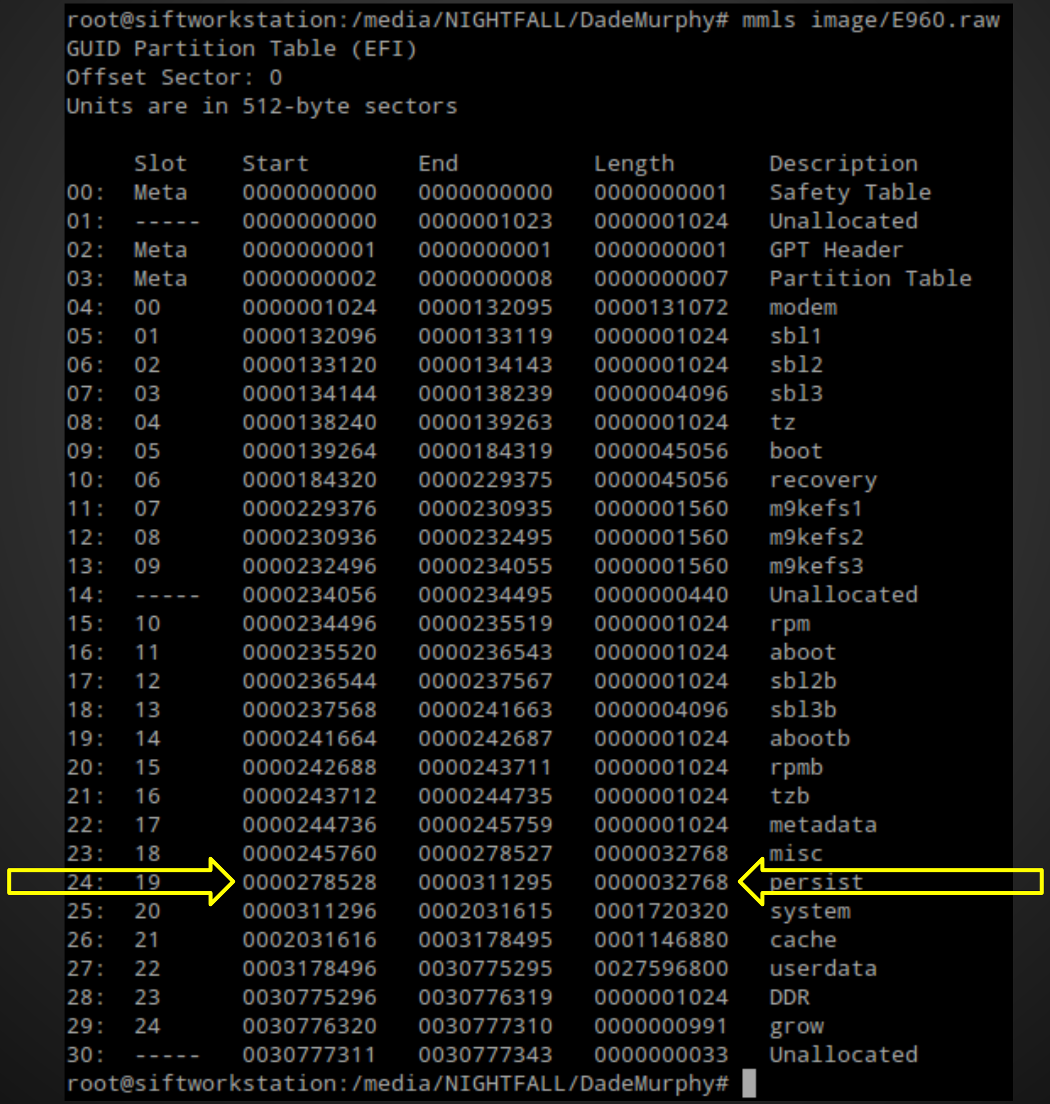
Estimated Time Left: 50:09:18

85.03 kB/s

Can we has data?

Before we do that...

Partition view

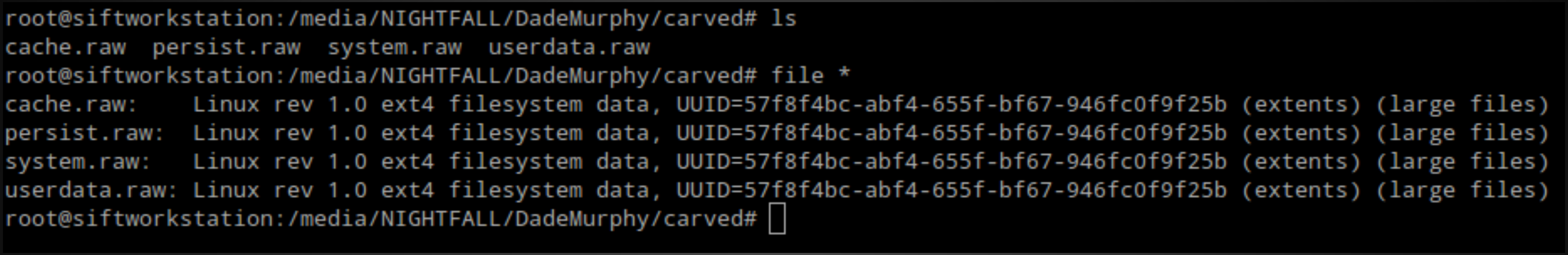


```
root@siftworkstation:/media/NIGHTFALL/DadeMurphy# mmls image/E960.raw
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors

     Slot     Start        End          Length       Description
00:  Meta     0000000000   0000000000   0000000001   Safety Table
01:  -----    0000000000   0000001023   0000001024   Unallocated
02:  Meta     0000000001   0000000001   0000000001   GPT Header
03:  Meta     0000000002   0000000008   0000000007   Partition Table
04:  00       0000001024   0000132095   0000131072   modem
05:  01       0000132096   0000133119   0000001024   sbl1
06:  02       0000133120   0000134143   0000001024   sbl2
07:  03       0000134144   0000138239   0000004096   sbl3
08:  04       0000138240   0000139263   0000001024   tz
09:  05       0000139264   0000184319   0000045056   boot
10:  06       0000184320   0000229375   0000045056   recovery
11:  07       0000229376   0000230935   0000001560   m9kefs1
12:  08       0000230936   0000232495   0000001560   m9kefs2
13:  09       0000232496   0000234055   0000001560   m9kefs3
14:  -----    0000234056   0000234495   0000000440   Unallocated
15:  10       0000234496   0000235519   0000001024   rpm
16:  11       0000235520   0000236543   0000001024   aboot
17:  12       0000236544   0000237567   0000001024   sbl2b
18:  13       0000237568   0000241663   0000004096   sbl3b
19:  14       0000241664   0000242687   0000001024   abootb
20:  15       0000242688   0000243711   0000001024   rpmb
21:  16       0000243712   0000244735   0000001024   tzb
22:  17       0000244736   0000245759   0000001024   metadata
23:  18       0000245760   0000278527   0000032768   misc
24:  19       0000278528   0000311295   0000032768   persist
25:  20       0000311296   0002031615   0001720320   system
26:  21       0002031616   0003178495   0001146880   cache
27:  22       0003178496   0030775295   0027596800   userdata
28:  23       0030775296   0030776319   0000001024   DDR
29:  24       0030776320   0030777310   0000000991   grow
30:  -----    0030777311   0030777343   0000000033   Unallocated
root@siftworkstation:/media/NIGHTFALL/DadeMurphy# 
```

Offset

Length

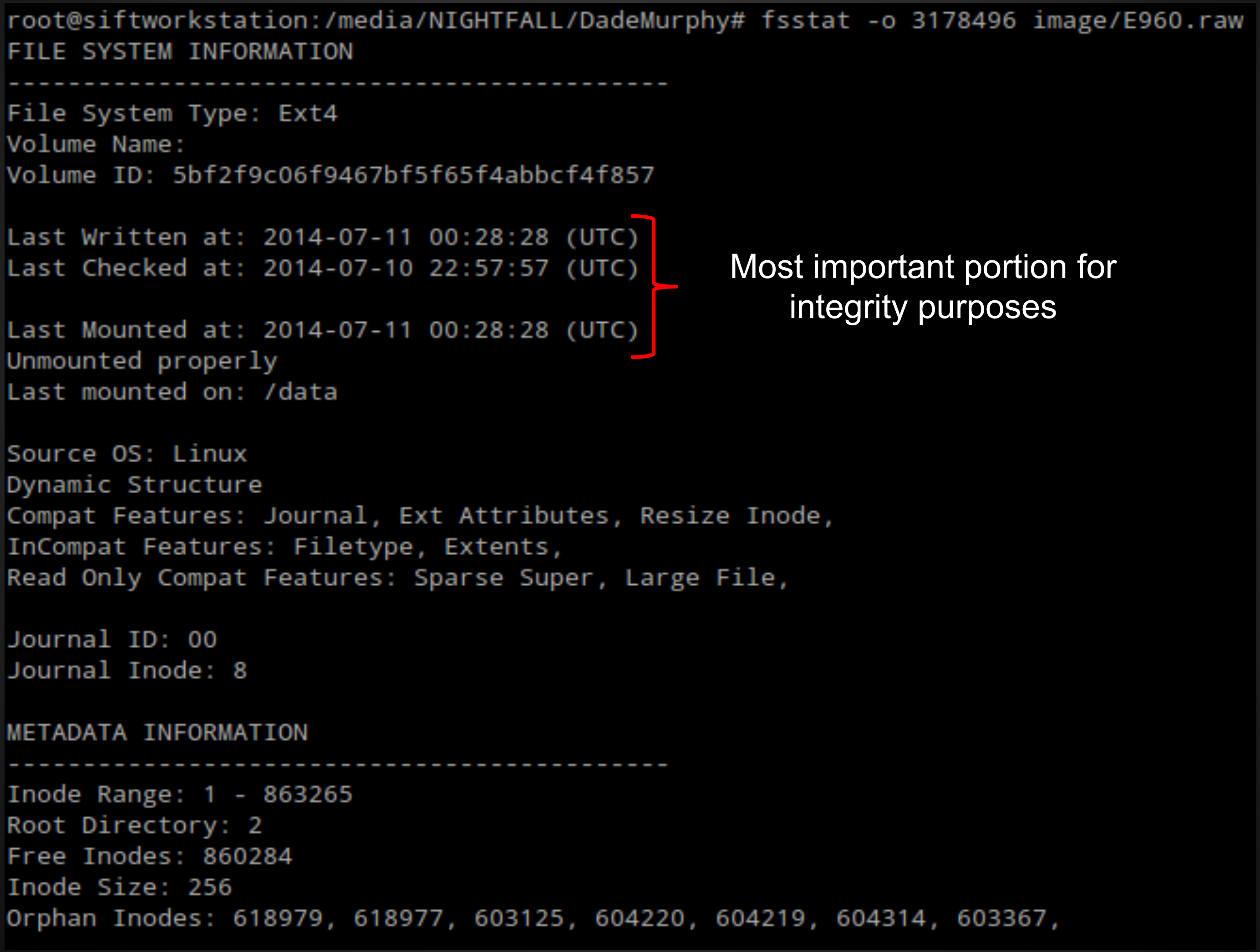
Manually carving partitions



```
root@siftworkstation:/media/NIGHTFALL/DadeMurphy/carved# ls
cache.raw  persist.raw  system.raw  userdata.raw
root@siftworkstation:/media/NIGHTFALL/DadeMurphy/carved# file *
cache.raw:    Linux rev 1.0 ext4 filesystem data, UUID=57f8f4bc-abf4-655f-bf67-946fc0f9f25b (extents) (large files)
persist.raw:  Linux rev 1.0 ext4 filesystem data, UUID=57f8f4bc-abf4-655f-bf67-946fc0f9f25b (extents) (large files)
system.raw:   Linux rev 1.0 ext4 filesystem data, UUID=57f8f4bc-abf4-655f-bf67-946fc0f9f25b (extents) (large files)
userdata.raw: Linux rev 1.0 ext4 filesystem data, UUID=57f8f4bc-abf4-655f-bf67-946fc0f9f25b (extents) (large files)
root@siftworkstation:/media/NIGHTFALL/DadeMurphy/carved# 
```

- Refer to the output of mmls previously
- dd if=image.dd of=partition-name.dd skip=$offset count=$length
  - $offset = offset of the partition on the media
  - $length = length of the partition

File system analysis

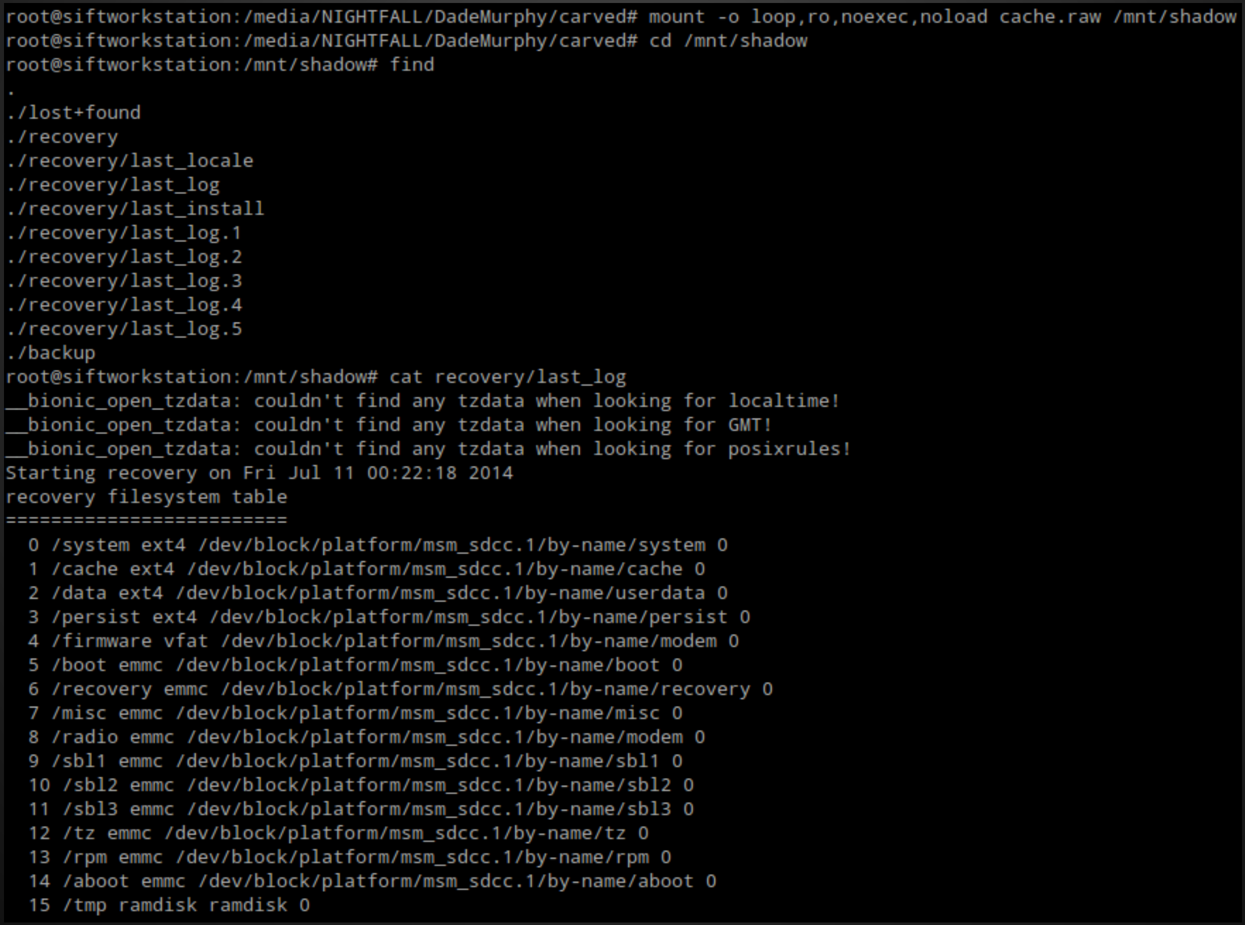


```
root@siftworkstation:/media/NIGHTFALL/DadeMurphy# fsstat -o 3178496 image/E960.raw
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: Ext4
Volume Name:
Volume ID: 5bf2f9c06f9467bf5f65f4abbcf4f857

Last Written at: 2014-07-11 00:28:28 (UTC)
Last Checked at: 2014-07-10 22:57:57 (UTC)

Last Mounted at: 2014-07-11 00:28:28 (UTC)
Unmounted properly
Last mounted on: /data

Source OS: Linux
Dynamic Structure
Compat Features: Journal, Ext Attributes, Resize Inode,
InCompat Features: Filetype, Extents,
Read Only Compat Features: Sparse Super, Large File,

Journal ID: 00
Journal Inode: 8

METADATA INFORMATION
--------------------------------------------
Inode Range: 1 - 863265
Root Directory: 2
Free Inodes: 860284
Inode Size: 256
Orphan Inodes: 618979, 618977, 603125, 604220, 604219, 604314, 603367,
```

Most important portion for integrity purposes

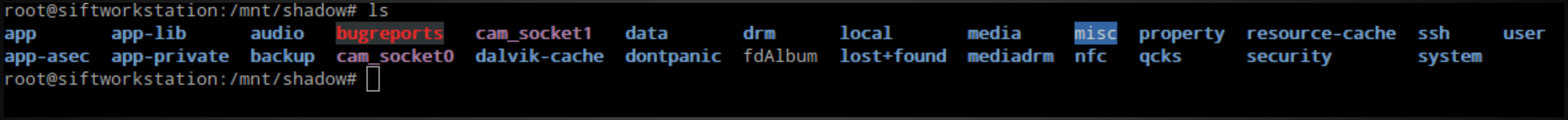
Cache partition

- Stores Android updates
- Maintains recovery logs

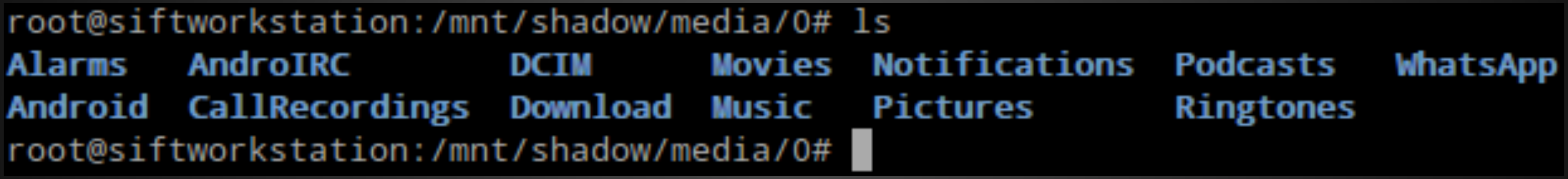


```
root@siftworkstation:/media/NIGHTFALL/DadeMurphy/carved# mount -o loop,ro,noexec,noload cache.raw /mnt/shadow
root@siftworkstation:/media/NIGHTFALL/DadeMurphy/carved# cd /mnt/shadow
root@siftworkstation:/mnt/shadow# find
.
./lost+found
./recovery
./recovery/last_locale
./recovery/last_log
./recovery/last_install
./recovery/last_log.1
./recovery/last_log.2
./recovery/last_log.3
./recovery/last_log.4
./recovery/last_log.5
./backup
root@siftworkstation:/mnt/shadow# cat recovery/last_log
__bionic_open_tzdata: couldn't find any tzdata when looking for localtime!
__bionic_open_tzdata: couldn't find any tzdata when looking for GMT!
__bionic_open_tzdata: couldn't find any tzdata when looking for posixrules!
Starting recovery on Fri Jul 11 00:22:18 2014
recovery filesystem table
=========================
  0 /system ext4 /dev/block/platform/msm_sdcc.1/by-name/system 0
  1 /cache ext4 /dev/block/platform/msm_sdcc.1/by-name/cache 0
  2 /data ext4 /dev/block/platform/msm_sdcc.1/by-name/userdata 0
  3 /persist ext4 /dev/block/platform/msm_sdcc.1/by-name/persist 0
  4 /firmware vfat /dev/block/platform/msm_sdcc.1/by-name/modem 0
  5 /boot emmc /dev/block/platform/msm_sdcc.1/by-name/boot 0
  6 /recovery emmc /dev/block/platform/msm_sdcc.1/by-name/recovery 0
  7 /misc emmc /dev/block/platform/msm_sdcc.1/by-name/misc 0
  8 /radio emmc /dev/block/platform/msm_sdcc.1/by-name/modem 0
  9 /sbl1 emmc /dev/block/platform/msm_sdcc.1/by-name/sbl1 0
  10 /sbl2 emmc /dev/block/platform/msm_sdcc.1/by-name/sbl2 0
  11 /sbl3 emmc /dev/block/platform/msm_sdcc.1/by-name/sbl3 0
  12 /tz emmc /dev/block/platform/msm_sdcc.1/by-name/tz 0
  13 /rpm emmc /dev/block/platform/msm_sdcc.1/by-name/rpm 0
  14 /aboot emmc /dev/block/platform/msm_sdcc.1/by-name/aboot 0
  15 /tmp ramdisk ramdisk 0
```

Userdata partition



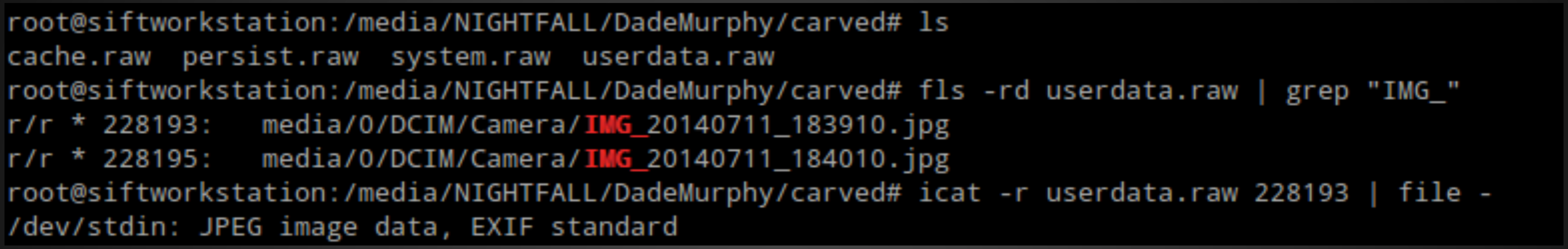
```
root@siftworkstation:/mnt/shadow# ls
app       app-lib      audio   bugreports   cam_socket1   data       drm      local       media     misc  property  resource-cache  ssh     user
app-asec  app-private  backup  cam_socket0  dalvik-cache  dontpanic  fdAlbum  lost+found  mediadrm  nfc   qcks      security        system
root@siftworkstation:/mnt/shadow# 
```



```
root@siftworkstation:/mnt/shadow/media/0# ls
Alarms   AndroIRC        DCIM      Movies  Notifications  Podcasts   WhatsApp
Android  CallRecordings  Download  Music   Pictures       Ringtones
root@siftworkstation:/mnt/shadow/media/0# 
```

- Data visible through the UI
- Media stores (Thumbnails, SQLite3 databases of images stored)
- Data created/manipulated through application interaction* stored here
- Downloads, Music, Images etc.

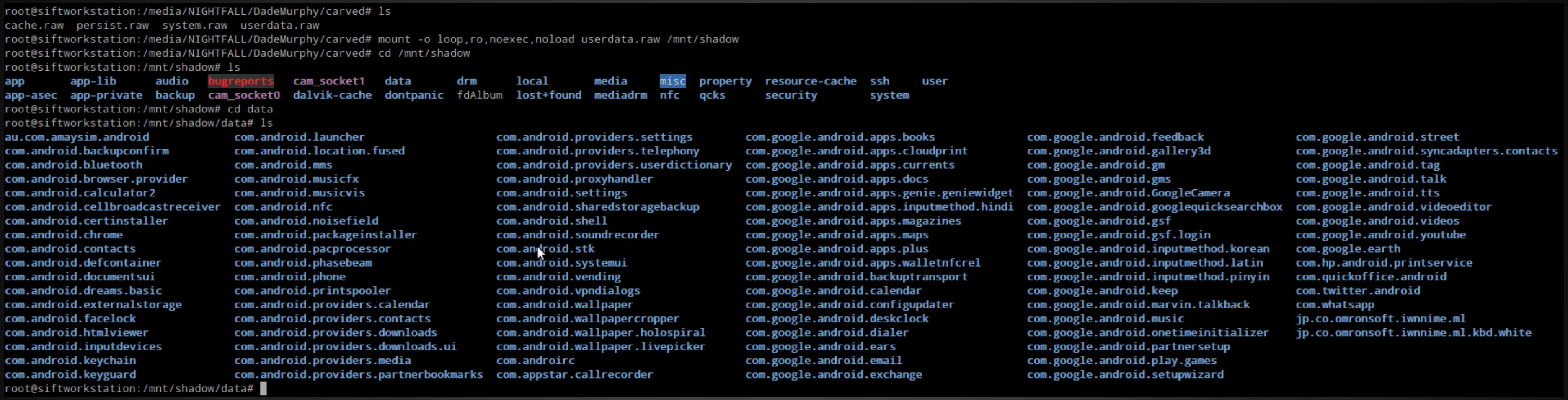
Deleted data? No problem.



```
root@siftworkstation:/media/NIGHTFALL/DadeMurphy/carved# ls
cache.raw  persist.raw  system.raw  userdata.raw
root@siftworkstation:/media/NIGHTFALL/DadeMurphy/carved# fls -rd userdata.raw | grep "IMG_"
r/r * 228193:   media/0/DCIM/Camera/IMG_20140711_183910.jpg
r/r * 228195:   media/0/DCIM/Camera/IMG_20140711_184010.jpg
root@siftworkstation:/media/NIGHTFALL/DadeMurphy/carved# icat -r userdata.raw 228193 | file -
/dev/stdin: JPEG image data, EXIF standard
```

- Data deleted but still present on inode!
  - fls provides a list of all deleted files thanks to remnant data after deletion
  - icat used to read the chosen inode
  - Pipe out data however you like
  - icat -r data.dd 1234 | display -

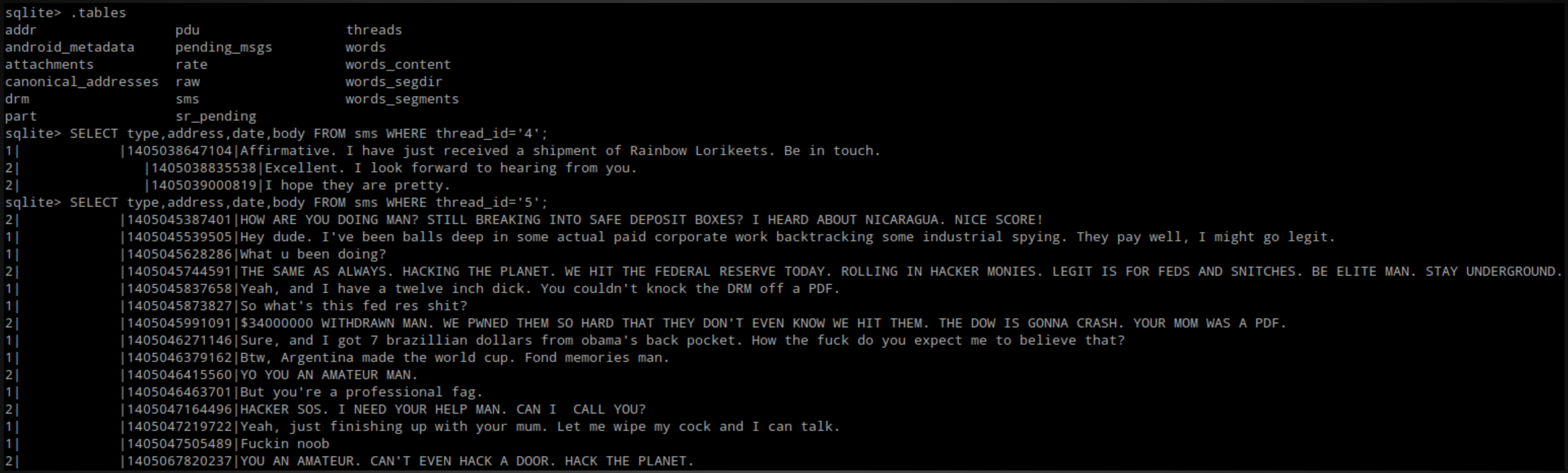
Application data? Suuure.



```
root@siftworkstation:/media/NIGHTFALL/DadeMurphy/carved# ls
cache.raw  persist.raw  system.raw  userdata.raw
root@siftworkstation:/media/NIGHTFALL/DadeMurphy/carved# mount -o loop,ro,noexec,noload userdata.raw /mnt/shadow
root@siftworkstation:/media/NIGHTFALL/DadeMurphy/carved# cd /mnt/shadow
root@siftworkstation:/mnt/shadow# ls
app       app-lib      audio   bugreports   cam_socket1   data       drm      local       media     misc  property  resource-cache  ssh     user
app-asec  app-private  backup  cam_socket0  dalvik-cache  dontpanic  fdAlbum  lost+found  mediadrm  nfc   qcks      security        system
root@siftworkstation:/mnt/shadow# cd data
root@siftworkstation:/mnt/shadow/data# ls
au.com.amaysim.android             com.android.launcher                    com.android.providers.settings        com.google.android.apps.books              com.google.android.feedback              com.google.android.street
com.android.backupconfirm          com.android.location.fused              com.android.providers.telephony       com.google.android.apps.cloudprint         com.google.android.gallery3d             com.google.android.syncadapters.contacts
com.android.bluetooth              com.android.mms                         com.android.providers.userdictionary  com.google.android.apps.currents           com.google.android.gm                    com.google.android.tag
com.android.browser.provider       com.android.musicfx                     com.android.proxyhandler              com.google.android.apps.docs               com.google.android.gms                   com.google.android.talk
com.android.calculator2            com.android.musicvis                    com.android.settings                  com.google.android.apps.genie.geniewidget  com.google.android.GoogleCamera          com.google.android.tts
com.android.cellbroadcastreceiver  com.android.nfc                         com.android.sharedstoragebackup       com.google.android.apps.inputmethod.hindi  com.google.android.googlequicksearchbox  com.google.android.videoeditor
com.android.certinstaller          com.android.noisefield                  com.android.shell                     com.google.android.apps.magazines          com.google.android.gsf                   com.google.android.videos
com.android.chrome                 com.android.packageinstaller            com.android.soundrecorder             com.google.android.apps.maps               com.google.android.gsf.login             com.google.android.youtube
com.android.contacts               com.android.pacprocessor                com.android.stk                       com.google.android.apps.plus               com.google.android.inputmethod.korean    com.google.earth
com.android.defcontainer           com.android.phasebeam                   com.android.systemui                  com.google.android.apps.walletnfcrel       com.google.android.inputmethod.latin     com.hp.android.printservice
com.android.documentsui            com.android.phone                       com.android.vending                   com.google.android.backuptransport         com.google.android.inputmethod.pinyin    com.quickoffice.android
com.android.dreams.basic           com.android.printspooler                com.android.vpndialogs                com.google.android.calendar                com.google.android.keep                  com.twitter.android
com.android.externalstorage        com.android.providers.calendar          com.android.wallpaper                 com.google.android.configupdater           com.google.android.marvin.talkback       com.whatsapp
com.android.facelock               com.android.providers.contacts          com.android.wallpapercropper          com.google.android.deskclock               com.google.android.music                 jp.co.omronsoft.iwnnime.ml
com.android.htmlviewer             com.android.providers.downloads         com.android.wallpaper.holospiral      com.google.android.dialer                  com.google.android.onetimeinitializer    jp.co.omronsoft.iwnnime.ml.kbd.white
com.android.inputdevices           com.android.providers.downloads.ui      com.android.wallpaper.livepicker      com.google.android.ears                    com.google.android.partnersetup
com.android.keychain               com.android.providers.media             com.androirc                          com.google.android.email                   com.google.android.play.games
com.android.keyguard               com.android.providers.partnerbookmarks  com.appstar.callrecorder              com.google.android.exchange                com.google.android.setupwizard
root@siftworkstation:/mnt/shadow/data# 
```

- /data/
- Individual folders for storage
- Common use of SQLite3 databases
- Lots of forensic artifacts stored in the background

SMS/MMS



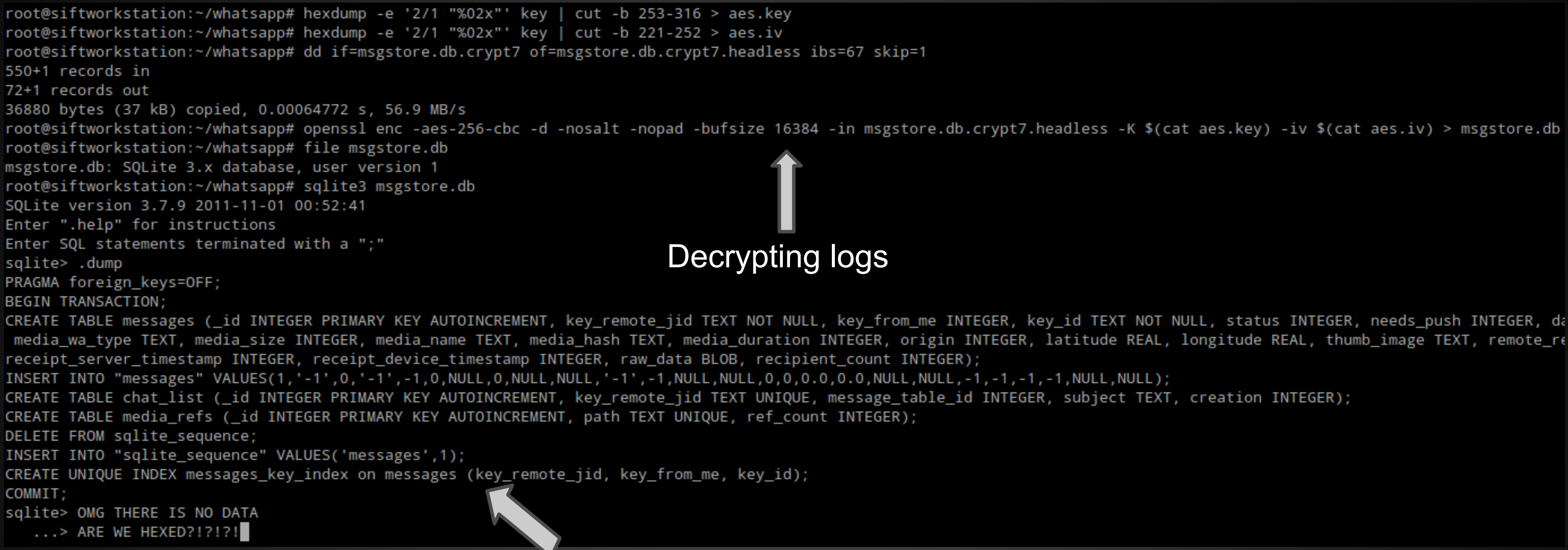
```
sqlite> .tables
addr                 pdu                  threads
android_metadata     pending_msgs         words
attachments          rate                 words_content
canonical_addresses  raw                  words_segdir
drm                  sms                  words_segments
part                 sr_pending
sqlite> SELECT type,address,date,body FROM sms WHERE thread_id='4';
1|            |1405038647104|Affirmative. I have just received a shipment of Rainbow Lorikeets. Be in touch.
2|               |1405038835538|Excellent. I look forward to hearing from you.
2|               |1405039000819|I hope they are pretty.
sqlite> SELECT type,address,date,body FROM sms WHERE thread_id='5';
2|            |1405045387401|HOW ARE YOU DOING MAN? STILL BREAKING INTO SAFE DEPOSIT BOXES? I HEARD ABOUT NICARAGUA. NICE SCORE!
1|            |1405045539505|Hey dude. I've been balls deep in some actual paid corporate work backtracking some industrial spying. They pay well, I might go legit.
1|            |1405045628286|What u been doing?
2|            |1405045744591|THE SAME AS ALWAYS. HACKING THE PLANET. WE HIT THE FEDERAL RESERVE TODAY. ROLLING IN HACKER MONIES. LEGIT IS FOR FEDS AND SNITCHES. BE ELITE MAN. STAY UNDERGROUND.
1|            |1405045837658|Yeah, and I have a twelve inch dick. You couldn't knock the DRM off a PDF.
1|            |1405045873827|So what's this fed res shit?
2|            |1405045991091|$34000000 WITHDRAWN MAN. WE PWNED THEM SO HARD THAT THEY DON'T EVEN KNOW WE HIT THEM. THE DOW IS GONNA CRASH. YOUR MOM WAS A PDF.
1|            |1405046271146|Sure, and I got 7 brazillian dollars from obama's back pocket. How the fuck do you expect me to believe that?
1|            |1405046379162|Btw, Argentina made the world cup. Fond memories man.
2|            |1405046415560|YO YOU AN AMATEUR MAN.
1|            |1405046463701|But you're a professional fag.
2|            |1405047164496|HACKER SOS. I NEED YOUR HELP MAN. CAN I  CALL YOU?
1|            |1405047219722|Yeah, just finishing up with your mum. Let me wipe my cock and I can talk.
1|            |1405047505489|Fuckin noob
2|            |1405067820237|YOU AN AMATEUR. CAN'T EVEN HACK A DOOR. HACK THE PLANET.
```

- /data/com.android.providers.telephony/databases/mmssms.db (SQLite3)

- _id, thread_id, address, person, date, date_sent, protocol, read, status, type, reply_path_present, subject, body, service_center, locked, error_code, seen

- Times are in EPOCH format (accurate to nanoseconds)
- ‘date -d@1405067820237’ = Fri Oct 29 11:43:57 EST 46494 < THE FUTURE
- ‘date -d@1405067820’ = Fri Jul 11 18:37:00 EST 2014

WhatsApp logs decrypted



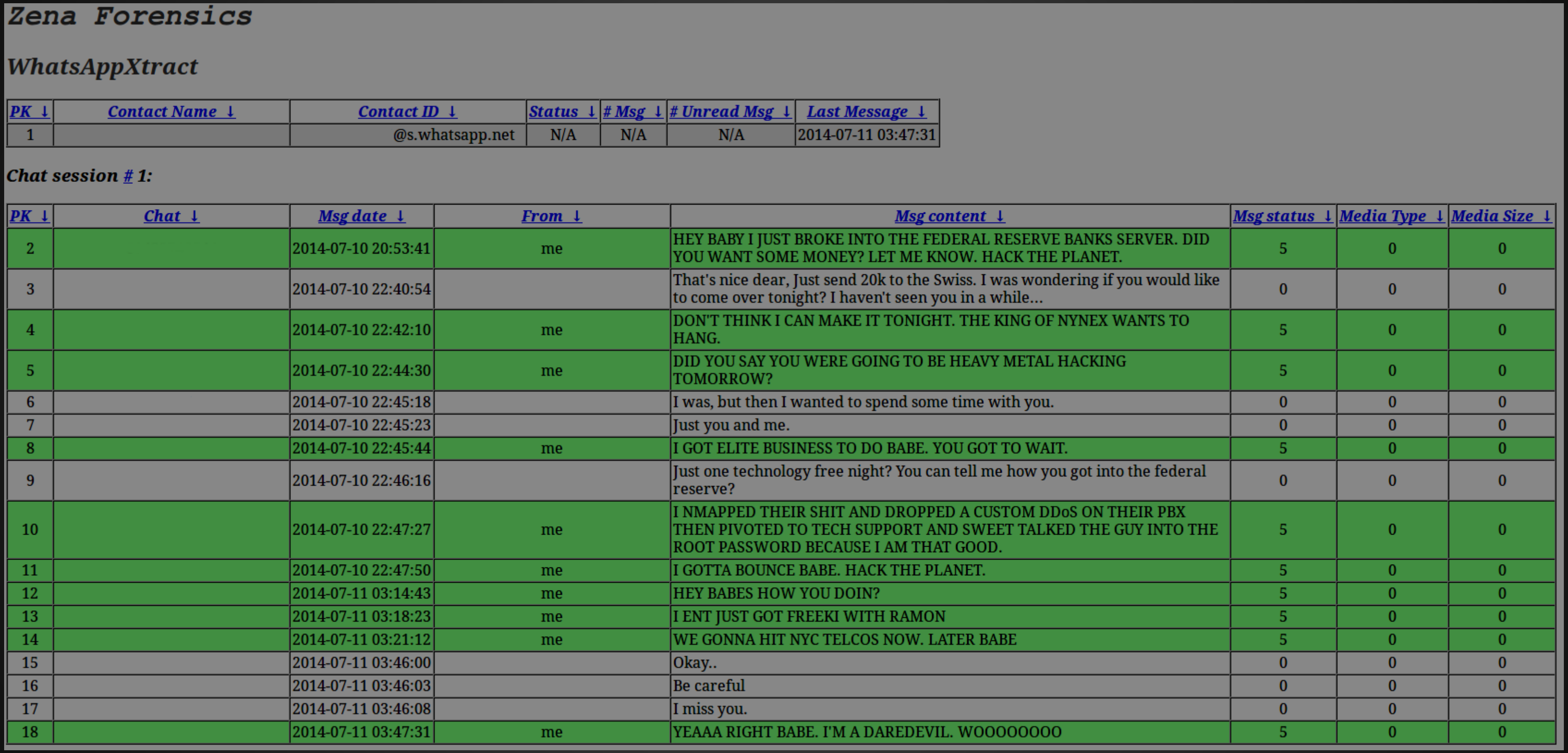
```
root@siftworkstation:~/whatsapp# hexdump -e '2/1 "%02x"' key | cut -b 253-316 > aes.key
root@siftworkstation:~/whatsapp# hexdump -e '2/1 "%02x"' key | cut -b 221-252 > aes.iv
root@siftworkstation:~/whatsapp# dd if=msgstore.db.crypt7 of=msgstore.db.crypt7.headless ibs=67 skip=1
550+1 records in
72+1 records out
36880 bytes (37 kB) copied, 0.00064772 s, 56.9 MB/s
root@siftworkstation:~/whatsapp# openssl enc -aes-256-cbc -d -nosalt -nopad -bufsize 16384 -in msgstore.db.crypt7.headless -K $(cat aes.key) -iv $(cat aes.iv) > msgstore.db
root@siftworkstation:~/whatsapp# file msgstore.db
msgstore.db: SQLite 3.x database, user version 1
root@siftworkstation:~/whatsapp# sqlite3 msgstore.db
SQLite version 3.7.9 2011-11-01 00:52:41
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> .dump
PRAGMA foreign_keys=OFF;
BEGIN TRANSACTION;
CREATE TABLE messages (_id INTEGER PRIMARY KEY AUTOINCREMENT, key_remote_jid TEXT NOT NULL, key_from_me INTEGER, key_id TEXT NOT NULL, status INTEGER, needs_push INTEGER, da
 media_wa_type TEXT, media_size INTEGER, media_name TEXT, media_hash TEXT, media_duration INTEGER, origin INTEGER, latitude REAL, longitude REAL, thumb_image TEXT, remote_re
receipt_server_timestamp INTEGER, receipt_device_timestamp INTEGER, raw_data BLOB, recipient_count INTEGER);
INSERT INTO "messages" VALUES(1,'-1',0,'-1',-1,0,NULL,0,NULL,NULL,'-1',-1,NULL,NULL,0,0,0.0,0.0,NULL,NULL,-1,-1,-1,-1,NULL,NULL);
CREATE TABLE chat_list (_id INTEGER PRIMARY KEY AUTOINCREMENT, key_remote_jid TEXT UNIQUE, message_table_id INTEGER, subject TEXT, creation INTEGER);
CREATE TABLE media_refs (_id INTEGER PRIMARY KEY AUTOINCREMENT, path TEXT UNIQUE, ref_count INTEGER);
DELETE FROM sqlite_sequence;
INSERT INTO "sqlite_sequence" VALUES('messages',1);
CREATE UNIQUE INDEX messages_key_index on messages (key_remote_jid, key_from_me, key_id);
COMMIT;
sqlite> OMG THERE IS NO DATA
   ...> ARE WE HEXED?!?!?!
```

Decrypting logs

db has no data?!

Not elite enough to get WhatsApp logs
Database decrypted!...but empty.

Just kidding, here you go



Zena Forensics

WhatsAppXtract

PK ↓	Contact Name ↓	Contact ID ↓	Status ↓	# Msg ↓	# Unread Msg ↓	Last Message ↓
1		@s.whatsapp.net	N/A	N/A	N/A	2014-07-11 03:47:31

Chat session # 1:

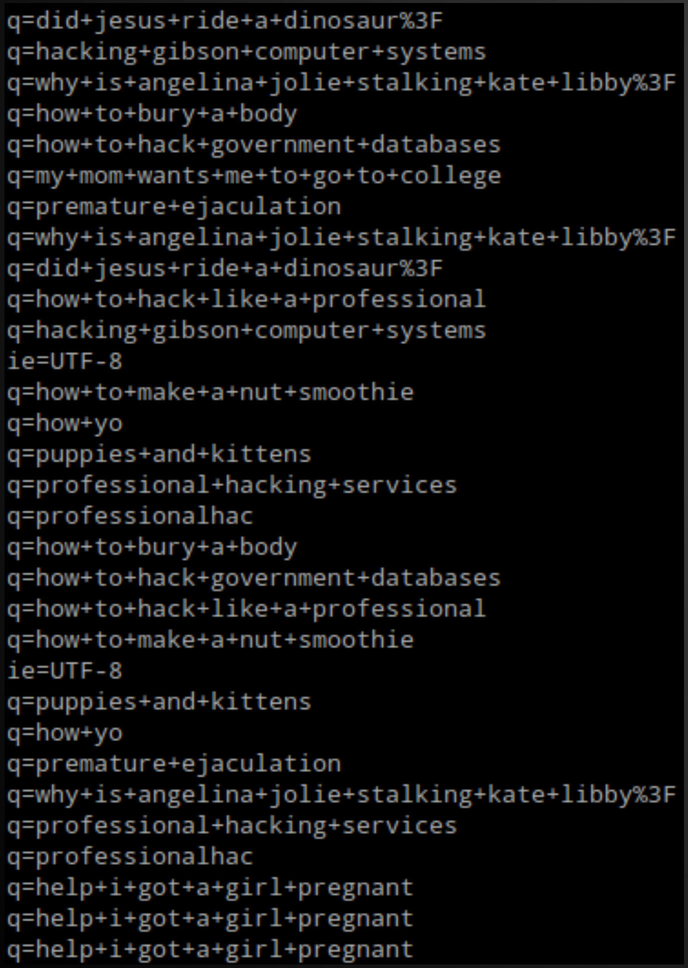
PK ↓	Chat ↓	Msg date ↓	From ↓	Msg content ↓	Msg status ↓	Media Type ↓	Media Size ↓
2		2014-07-10 20:53:41	me	HEY BABY I JUST BROKE INTO THE FEDERAL RESERVE BANKS SERVER. DID YOU WANT SOME MONEY? LET ME KNOW. HACK THE PLANET.	5	0	0
3		2014-07-10 22:40:54		That's nice dear, Just send 20k to the Swiss. I was wondering if you would like to come over tonight? I haven't seen you in a while...	0	0	0
4		2014-07-10 22:42:10	me	DON'T THINK I CAN MAKE IT TONIGHT. THE KING OF NYNEX WANTS TO HANG.	5	0	0
5		2014-07-10 22:44:30	me	DID YOU SAY YOU WERE GOING TO BE HEAVY METAL HACKING TOMORROW?	5	0	0
6		2014-07-10 22:45:18		I was, but then I wanted to spend some time with you.	0	0	0
7		2014-07-10 22:45:23		Just you and me.	0	0	0
8		2014-07-10 22:45:44	me	I GOT ELITE BUSINESS TO DO BABE. YOU GOT TO WAIT.	5	0	0
9		2014-07-10 22:46:16		Just one technology free night? You can tell me how you got into the federal reserve?	0	0	0
10		2014-07-10 22:47:27	me	I NMAPPED THEIR SHIT AND DROPPED A CUSTOM DDoS ON THEIR PBX THEN PIVOTED TO TECH SUPPORT AND SWEET TALKED THE GUY INTO THE ROOT PASSWORD BECAUSE I AM THAT GOOD.	5	0	0
11		2014-07-10 22:47:50	me	I GOTTA BOUNCE BABE. HACK THE PLANET.	5	0	0
12		2014-07-11 03:14:43	me	HEY BABES HOW YOU DOIN?	5	0	0
13		2014-07-11 03:18:23	me	I ENT JUST GOT FREEKI WITH RAMON	5	0	0
14		2014-07-11 03:21:12	me	WE GONNA HIT NYC TELCOS NOW. LATER BABE	5	0	0
15		2014-07-11 03:46:00		Okay..	0	0	0
16		2014-07-11 03:46:03		Be careful	0	0	0
17		2014-07-11 03:46:08		I miss you.	0	0	0
18		2014-07-11 03:47:31	me	YEAAA RIGHT BABE. I'M A DAREDEVIL. WOOOOOOOO	5	0	0

They were unencrypted in /data/com.whatsapp/ instead of the crypt7 file in /media/0/WhatsApp/Databases/

If less than 24 hours from first use or last backup, there will be an unencrypted copy of the users most recent messages.

Chrome history

/data/com.android.chrome/app_chrome/Default/History (SQLite3 DB)
/data/com.android.chrome/app_chrome/Default/History-journal (data)
/data/com.android.chrome/app_chrome/Default/History Provider Cache (data)



```
q=did+jesus+ride+a+dinosaur%3F
q=hacking+gibson+computer+systems
q=why+is+angelina+jolie+stalking+kate+libby%3F
q=how+to+bury+a+body
q=how+to+hack+government+databases
q=my+mom+wants+me+to+go+to+college
q=premature+ejaculation
q=why+is+angelina+jolie+stalking+kate+libby%3F
q=did+jesus+ride+a+dinosaur%3F
q=how+to+hack+like+a+professional
q=hacking+gibson+computer+systems
ie=UTF-8
q=how+to+make+a+nut+smoothie
q=how+yo
q=puppies+and+kittens
q=professional+hacking+services
q=professionalhac
q=how+to+bury+a+body
q=how+to+hack+government+databases
q=how+to+hack+like+a+professional
q=how+to+make+a+nut+smoothie
ie=UTF-8
q=puppies+and+kittens
q=how+yo
q=premature+ejaculation
q=why+is+angelina+jolie+stalking+kate+libby%3F
q=professional+hacking+services
q=professionalhac
q=help+i+got+a+girl+pregnant
q=help+i+got+a+girl+pregnant
q=help+i+got+a+girl+pregnant
```

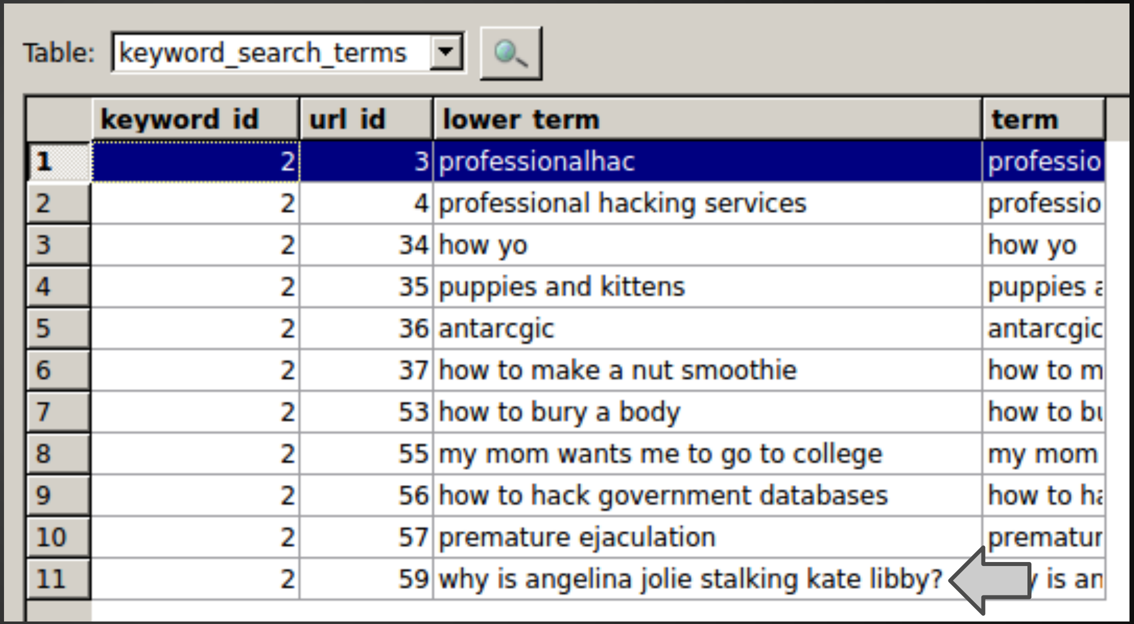
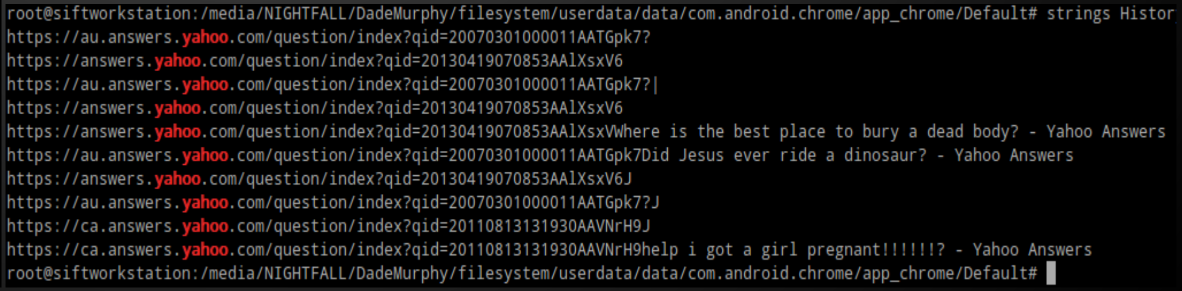


Table: keyword_search_terms

	keyword id	url id	lower term	term
1	2	3	professionalhac	professio
2	2	4	professional hacking services	professio
3	2	34	how yo	how yo
4	2	35	puppies and kittens	puppies a
5	2	36	antarcgic	antarcgic
6	2	37	how to make a nut smoothie	how to m
7	2	53	how to bury a body	how to bu
8	2	55	my mom wants me to go to college	my mom
9	2	56	how to hack government databases	how to ha
10	2	57	premature ejaculation	prematur
11	2	59	why is angelina jolie stalking kate libby?	is an



```
root@siftworkstation:/media/NIGHTFALL/DadeMurphy/filesystem/userdata/data/com.android.chrome/app_chrome/Default# strings Histor
https://au.answers.yahoo.com/question/index?qid=20070301000011AATGpk7?
https://answers.yahoo.com/question/index?qid=20130419070853AAlXsxV6
https://au.answers.yahoo.com/question/index?qid=20070301000011AATGpk7?|
https://answers.yahoo.com/question/index?qid=20130419070853AAlXsxV6
https://answers.yahoo.com/question/index?qid=20130419070853AAlXsxVWhere is the best place to bury a dead body? - Yahoo Answers
https://au.answers.yahoo.com/question/index?qid=20070301000011AATGpk7Did Jesus ever ride a dinosaur? - Yahoo Answers
https://answers.yahoo.com/question/index?qid=20130419070853AAlXsxV6J
https://au.answers.yahoo.com/question/index?qid=20070301000011AATGpk7?J
https://ca.answers.yahoo.com/question/index?qid=20110813131930AAVNrH9J
https://ca.answers.yahoo.com/question/index?qid=20110813131930AAVNrH9help i got a girl pregnant!!!!!!? - Yahoo Answers
root@siftworkstation:/media/NIGHTFALL/DadeMurphy/filesystem/userdata/data/com.android.chrome/app_chrome/Default# 
```

Chrome history cont’d

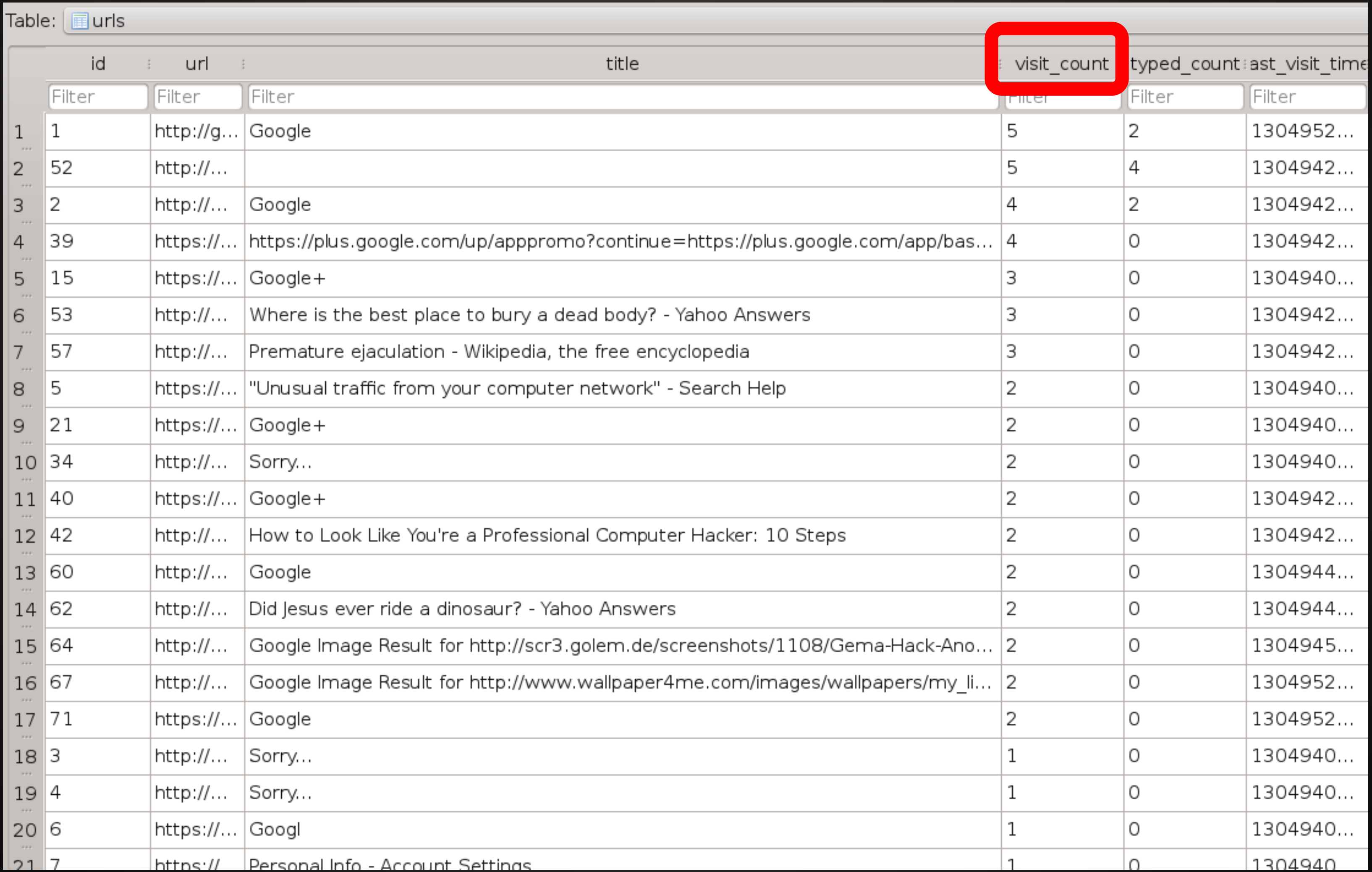
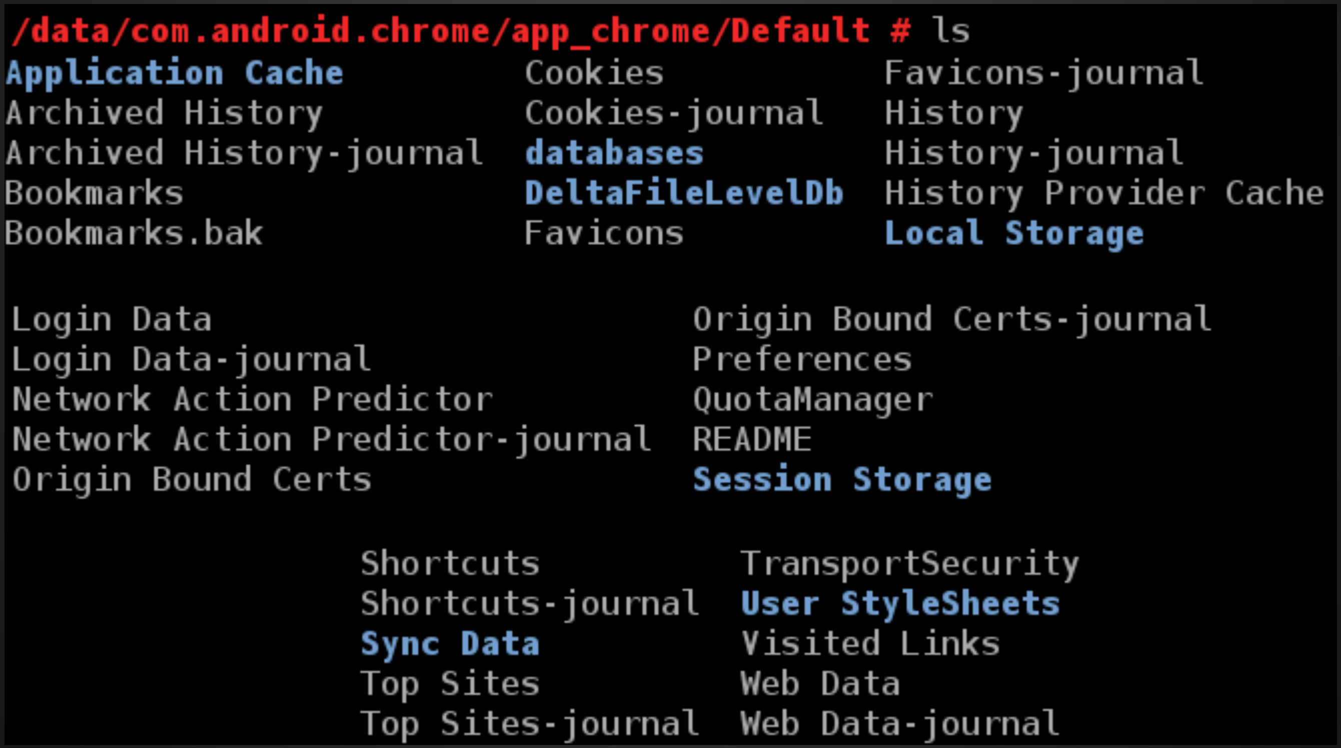


Table: urls

	id	url	title	visit_count	typed_count	ast_visit_time
	Filter	Filter	Filter	Filter	Filter	Filter
1	1	http://g...	Google	5	2	1304952...
2	52	http://...		5	4	1304942...
3	2	http://...	Google	4	2	1304942...
4	39	https://...	https://plus.google.com/up/apppromo?continue=https://plus.google.com/app/bas...	4	0	1304942...
5	15	https://...	Google+	3	0	1304940...
6	53	http://...	Where is the best place to bury a dead body? - Yahoo Answers	3	0	1304942...
7	57	http://...	Premature ejaculation - Wikipedia, the free encyclopedia	3	0	1304942...
8	5	https://...	"Unusual traffic from your computer network" - Search Help	2	0	1304940...
9	21	https://...	Google+	2	0	1304940...
10	34	http://...	Sorry...	2	0	1304940...
11	40	https://...	Google+	2	0	1304942...
12	42	http://...	How to Look Like You're a Professional Computer Hacker: 10 Steps	2	0	1304942...
13	60	http://...	Google	2	0	1304944...
14	62	http://...	Did Jesus ever ride a dinosaur? - Yahoo Answers	2	0	1304944...
15	64	http://...	Google Image Result for http://scr3.golem.de/screenshots/1108/Gema-Hack-Ano...	2	0	1304945...
16	67	http://...	Google Image Result for http://www.wallpaper4me.com/images/wallpapers/my_li...	2	0	1304952...
17	71	https://...	Google	2	0	1304952...
18	3	http://...	Sorry...	1	0	1304940...
19	4	http://...	Sorry...	1	0	1304940...
20	6	https://...	Googl	1	0	1304940...
21	7	https://...	Personal Info - Account Settings	1	0	1304940...

Chrome container

/data/com.android.chrome/app_chrome/Default/History (SQLite3 DB)



```
/data/com.android.chrome/app_chrome/Default # ls
Application Cache           Cookies               Favicons-journal
Archived History            Cookies-journal       History
Archived History-journal    databases             History-journal
Bookmarks                   DeltaFileLevelDb      History Provider Cache
Bookmarks.bak               Favicons              Local Storage

Login Data                          Origin Bound Certs-journal
Login Data-journal                  Preferences
Network Action Predictor            QuotaManager
Network Action Predictor-journal    README
Origin Bound Certs                  Session Storage

                  Shortcuts           TransportSecurity
                  Shortcuts-journal   User StyleSheets
                  Sync Data           Visited Links
                  Top Sites           Web Data
                  Top Sites-journal   Web Data-journal
```

SQLite3 Databases without .db extensions

Gmail database appears in Chrome?

/data/com.android.chrome/app_chrome/Default/databases/https_mail.google.com_0

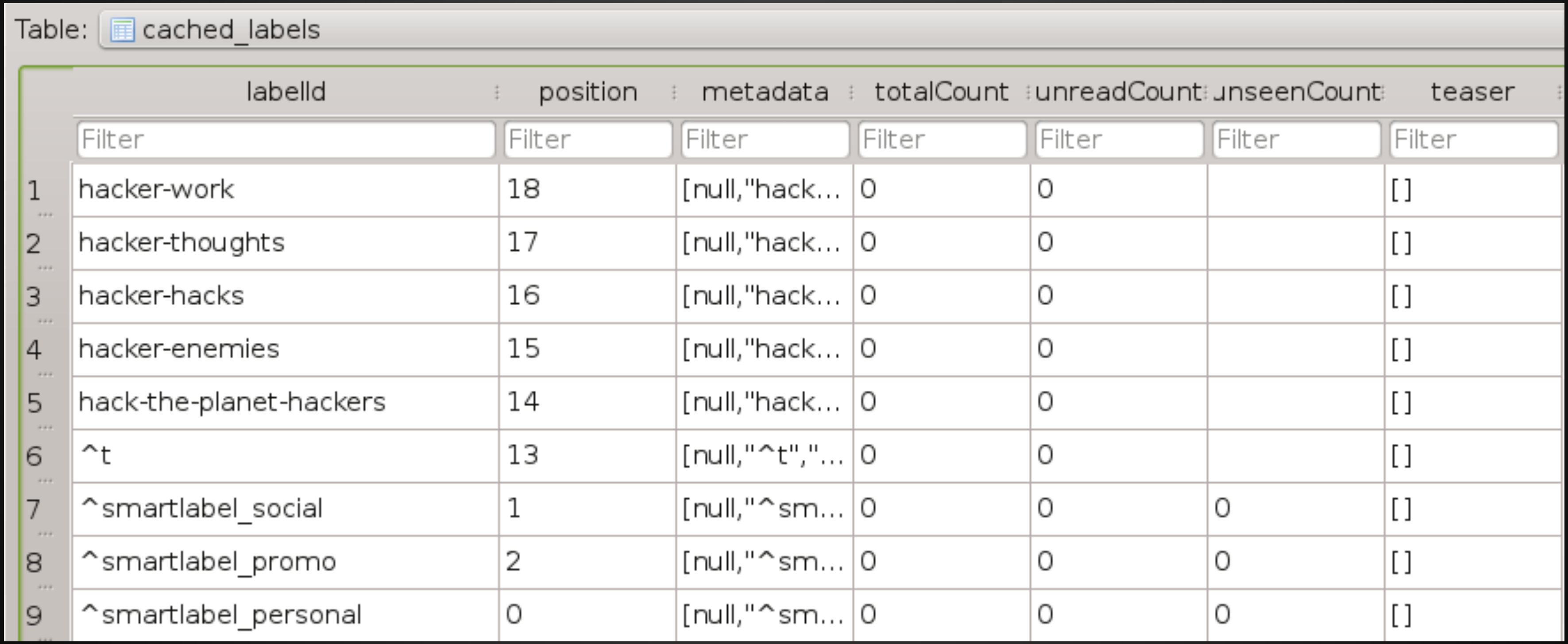
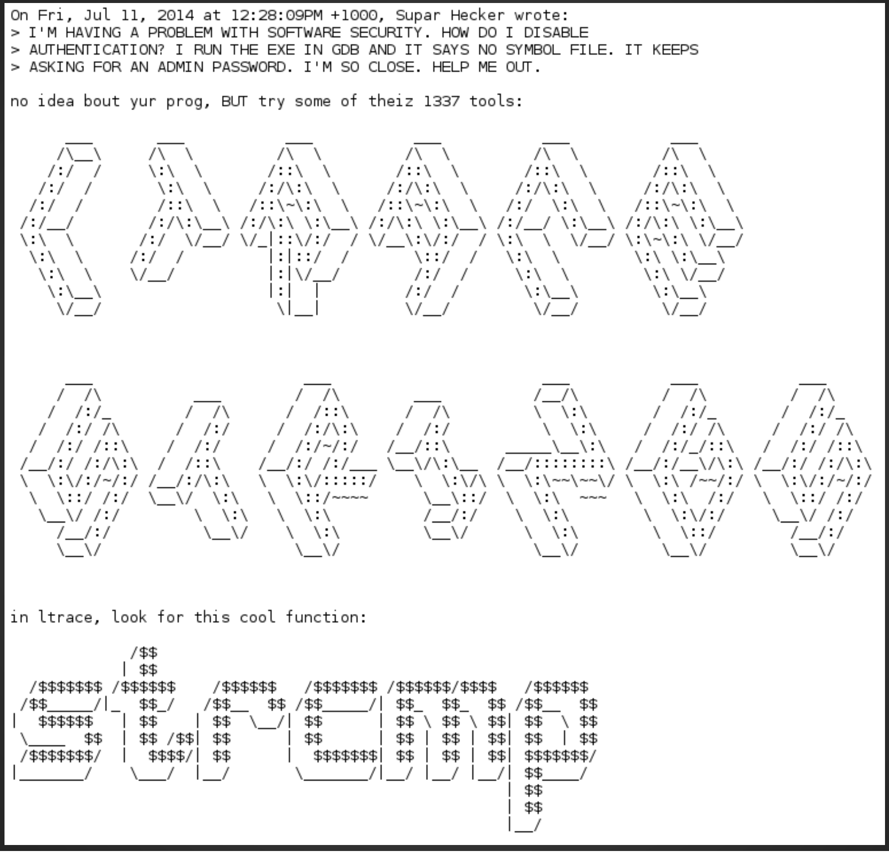


Table: cached_labels

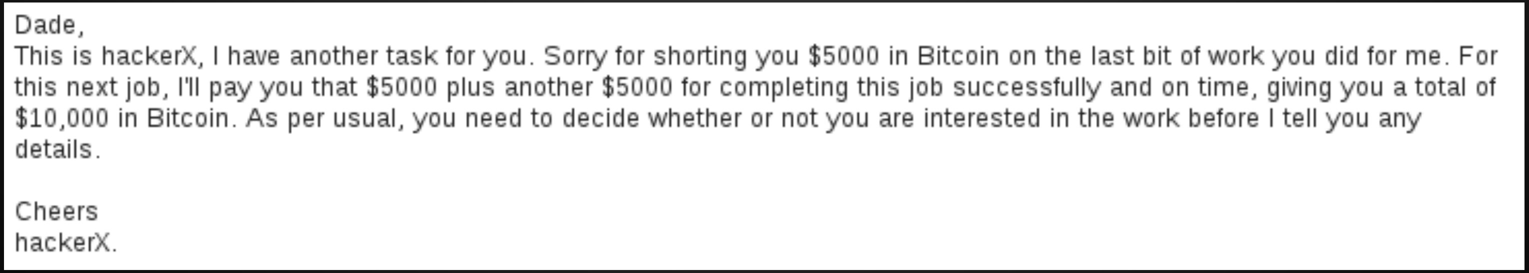
	labelId	position	metadata	totalCount	unreadCount	unseenCount	teaser
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	hacker-work	18	[null,"hack...	0	0		[]
2	hacker-thoughts	17	[null,"hack...	0	0		[]
3	hacker-hacks	16	[null,"hack...	0	0		[]
4	hacker-enemies	15	[null,"hack...	0	0		[]
5	hack-the-planet-hackers	14	[null,"hack...	0	0		[]
6	^t	13	[null,"^t","...	0	0		[]
7	^smartlabel_social	1	[null,"^sm...	0	0	0	[]
8	^smartlabel_promo	2	[null,"^sm...	0	0	0	[]
9	^smartlabel_personal	0	[null,"^sm...	0	0	0	[]

Shows the layout of the suspects email folders

GMails (these got lost)



```
On Fri, Jul 11, 2014 at 12:28:09PM +1000, Supar Hecker wrote:
> I'M HAVING A PROBLEM WITH SOFTWARE SECURITY. HOW DO I DISABLE
> AUTHENTICATION? I RUN THE EXE IN GDB AND IT SAYS NO SYMBOL FILE. IT KEEPS
> ASKING FOR AN ADMIN PASSWORD. I'M SO CLOSE. HELP ME OUT.

no idea bout yur prog, BUT try some of theiz 1337 tools:

      ___       ___           ___           ___           ___           ___
     /\__\     /\  \         /\  \         /\  \         /\  \         /\  \
    /:/  /     \:\  \       /::\  \       /::\  \       /::\  \       /::\  \
   /:/  /       \:\  \     /:/\:\  \     /:/\:\  \     /:/\:\  \     /:/\:\  \
  /:/  /        /::\  \   /::\~\:\  \   /::\~\:\  \   /:/  \:\  \   /::\~\:\  \
 /:/__/        /:/\:\__\ /:/\:\ \:\__\ /:/\:\ \:\__\ /:/__/ \:\__\ /:/\:\ \:\__\
 \:\  \       /:/  \/__/ \/_|::\/:/  / \/__\:\/:/  / \:\  \  \/__/ \:\~\:\ \/__/
  \:\  \     /:/  /         |:|::/  /       \::/  /   \:\  \        \:\ \:\__\
   \:\  \    \/__/          |:|\/__/        /:/  /     \:\  \        \:\ \/__/
    \:\__\                  |:|  |         /:/  /       \:\__\        \:\__\
     \/__/                   \|__|         \/__/         \/__/         \/__/



      ___                         ___                         ___           ___           ___
     /  /\          ___          /  /\          ___          /__/\         /  /\          /  /\
    /  /:/_        /  /\        /  /::\        /  /\         \  \:\       /  /:/_        /  /:/_
   /  /:/ /\      /  /:/       /  /:/\:\      /  /:/          \  \:\     /  /:/ /\     /  /:/ /\
  /  /:/ /::\    /  /:/       /  /:/~/:/     /__/::\     _____\__\:\   /  /:/_/::\   /  /:/ /::\
 /__/:/ /:/\:\  /  /::\      /__/:/ /:/___   \__\/\:\__  /__/::::::::\ /__/:/__\/\:\ /__/:/ /:/\:\
 \  \:\/:/~/:/ /__/:/\:\     \  \:\/:::::/      \  \:\/\ \  \:\~~\~~\/ \  \:\ /~~/:/ \  \:\/:/~/:/
  \  \::/ /:/  \__\/  \:\     \  \::/~~~~      \__\::/  \  \:\  ~~~   \  \:\  /:/   \  \::/ /:/
   \__\/ /:/        \  \:\     \  \:\          /__/:/    \  \:\        \  \:\/:/     \__\/ /:/
     /__/:/          \__\/      \  \:\         \__\/      \  \:\        \  \::/        /__/:/
     \__\/                       \__\/                     \__\/         \__\/         \__\/


in ltrace, look for this cool function:

             /$$
            | $$
  /$$$$$$$ /$$$$$$    /$$$$$$   /$$$$$$$ /$$$$$$/$$$$   /$$$$$$
 /$$_____/|_  $$_/   /$$__  $$ /$$_____/| $$_  $$_  $$ /$$__  $$
|  $$$$$$   | $$    | $$  \__/| $$      | $$ \ $$ \ $$| $$  \ $$
 \____  $$  | $$ /$$| $$      | $$      | $$ | $$ | $$| $$  | $$
 /$$$$$$$/  |  $$$$/| $$      |  $$$$$$$| $$ | $$ | $$| $$$$$$$/
|_______/    \___/  |__/       \_______/|__/ |__/ |__/| $$____/
                                                      | $$
                                                      | $$
                                                      |__/
```

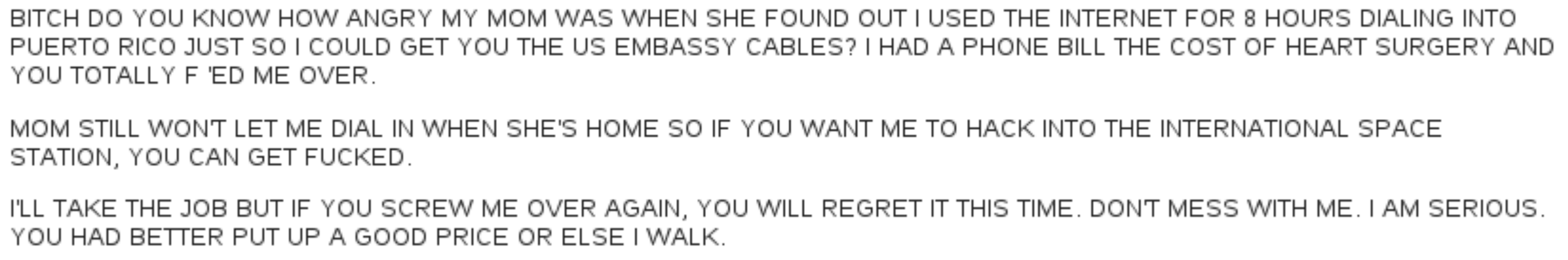


Dade,
This is hackerX, I have another task for you. Sorry for shorting you $5000 in Bitcoin on the last bit of work you did for me. For this next job, I'll pay you that $5000 plus another $5000 for completing this job successfully and on time, giving you a total of $10,000 in Bitcoin. As per usual, you need to decide whether or not you are interested in the work before I tell you any details.

Cheers
hackerX.

Angry GMails

Dade Murphy
(CAPSLOCK)

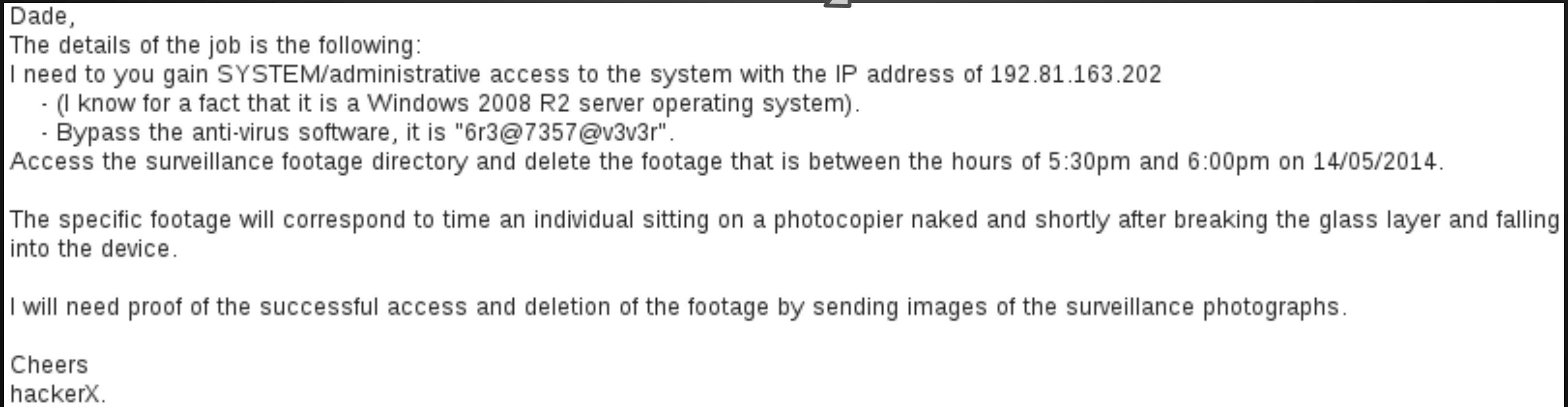


BITCH DO YOU KNOW HOW ANGRY MY MOM WAS WHEN SHE FOUND OUT I USED THE INTERNET FOR 8 HOURS DIALING INTO PUERTO RICO JUST SO I COULD GET YOU THE US EMBASSY CABLES? I HAD A PHONE BILL THE COST OF HEART SURGERY AND YOU TOTALLY F 'ED ME OVER.

MOM STILL WON'T LET ME DIAL IN WHEN SHE'S HOME SO IF YOU WANT ME TO HACK INTO THE INTERNATIONAL SPACE STATION, YOU CAN GET FUCKED.

I'LL TAKE THE JOB BUT IF YOU SCREW ME OVER AGAIN, YOU WILL REGRET IT THIS TIME. DON'T MESS WITH ME. I AM SERIOUS. YOU HAD BETTER PUT UP A GOOD PRICE OR ELSE I WALK.

hackerX



Dade,
The details of the job is the following:
I need to you gain SYSTEM/administrative access to the system with the IP address of 192.81.163.202
- (I know for a fact that it is a Windows 2008 R2 server operating system).
- Bypass the anti-virus software, it is "6r3@7357@v3v3r".

Access the surveillance footage directory and delete the footage that is between the hours of 5:30pm and 6:00pm on 14/05/2014.

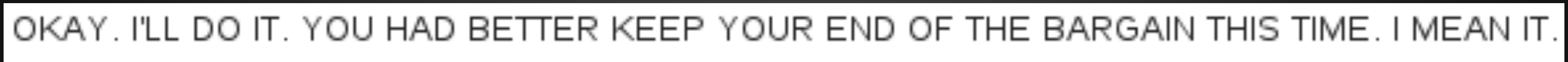
The specific footage will correspond to time an individual sitting on a photocopier naked and shortly after breaking the glass layer and falling into the device.

I will need proof of the successful access and deletion of the footage by sending images of the surveillance photographs.

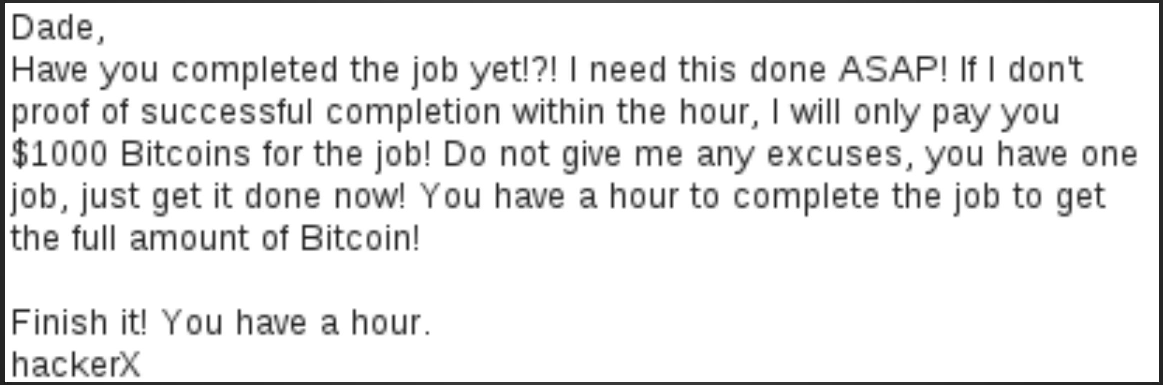
Cheers
hackerX.

Angry GMails continued

Dade Murphy
(CAPSLOCK)

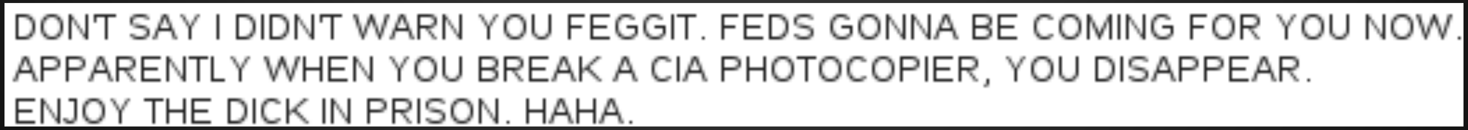


OKAY. I'LL DO IT. YOU HAD BETTER KEEP YOUR END OF THE BARGAIN THIS TIME. I MEAN IT.



Dade,
Have you completed the job yet!?! I need this done ASAP! If I don't proof of successful completion within the hour, I will only pay you $1000 Bitcoins for the job! Do not give me any excuses, you have one job, just get it done now! You have a hour to complete the job to get the full amount of Bitcoin!

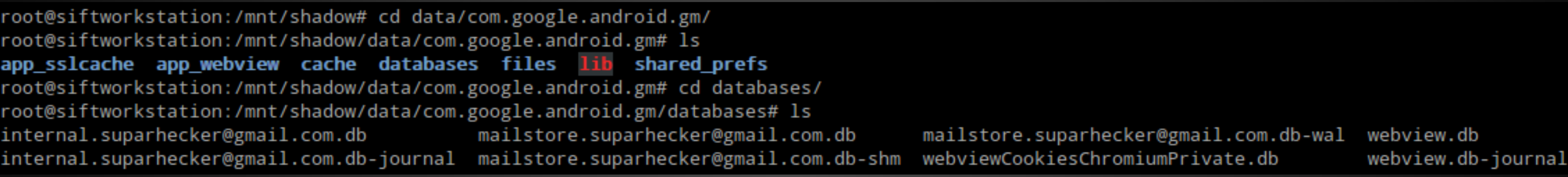
Finish it! You have a hour.
hackerX



DONT SAY I DIDNT WARN YOU FEGGIT. FEDS GONNA BE COMING FOR YOU NOW. APPARENTLY WHEN YOU BREAK A CIA PHOTOCOPIER, YOU DISAPPEAR. ENJOY THE DICK IN PRISON. HAHA.

STELLA ARTOIS
SONY
BUFFALO
ERNST & YOUNG
STATS U
RICOH
TALK TO A BANKER
CHASE
NEW YORK POLICE DEPT
Walgreens
THOMSON REUTERS
CHASE

Where are these magical gmails?

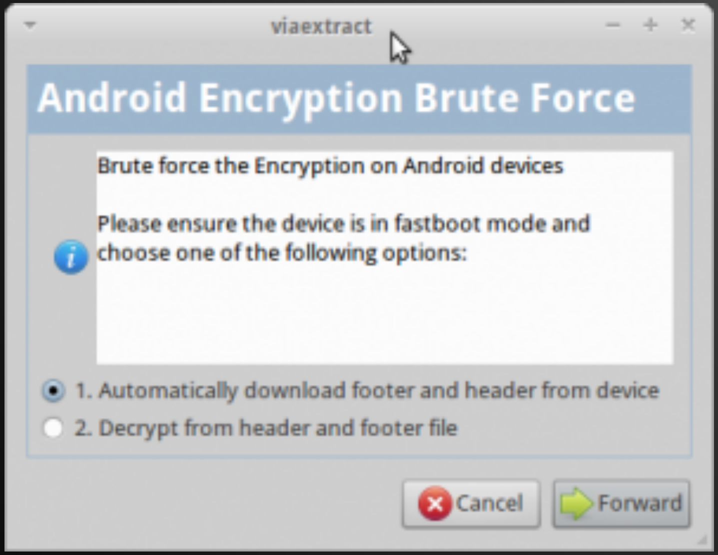


```
root@siftworkstation:/mnt/shadow# cd data/com.google.android.gm/
root@siftworkstation:/mnt/shadow/data/com.google.android.gm# ls
app_sslcache  app_webview  cache  databases  files  lib  shared_prefs
root@siftworkstation:/mnt/shadow/data/com.google.android.gm# cd databases/
root@siftworkstation:/mnt/shadow/data/com.google.android.gm/databases# ls
internal.suparhecker@gmail.com.db          mailstore.suparhecker@gmail.com.db      mailstore.suparhecker@gmail.com.db-wal  webview.db
internal.suparhecker@gmail.com.db-journal  mailstore.suparhecker@gmail.com.db-shm  webviewCookiesChromiumPrivate.db        webview.db-journal
```

- /data/com.google.android.gm/
- Client-side caching when interaction occurs on the device
  - Drafts
  - Full emails
  - Header content (Subject, addressee, small excerpt of body) used to display emails in folder view
  - Attachments are stored in the subfolder *files/*

Encrypted filesystems

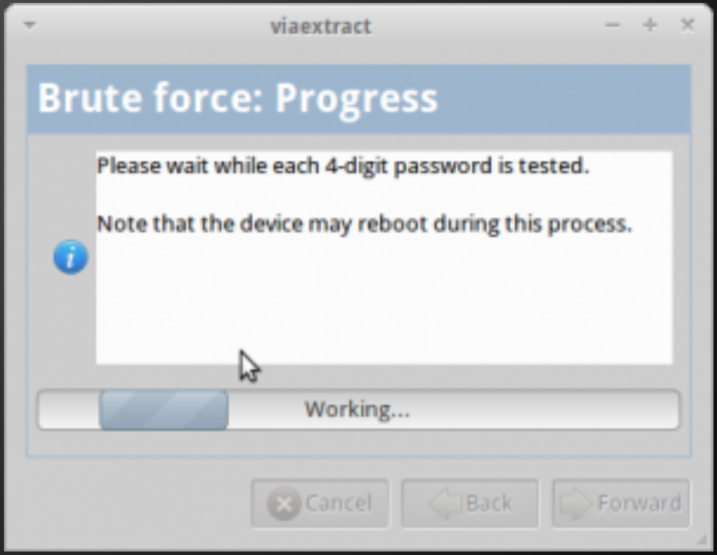
- Android is open source...
  - ...so the code for filesystem encryption is available!
  - Can we crack it? Yes, someone else already did.
  - Gosh! Passwords are hard.
  - Let’s choose 4 digits, hmmm...



Brute force the Encryption on Android devices

Please ensure the device is in fastboot mode and choose one of the following options:

● 1. Automatically download footer and header from device
○ 2. Decrypt from header and footer file



Please wait while each 4-digit password is tested.

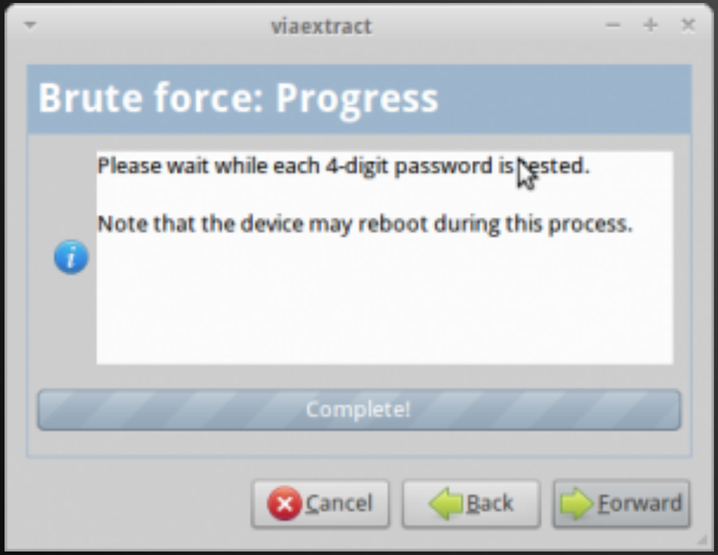
Note that the device may reboot during this process.

Working...

Credit: VIAFORENSICS LLC. 2014

Encrypted filesystems

- Android is open source...
  - ...so the code for filesystem encryption is available!
  - Can we crack it? Yes, someone else already did.
  - Gosh! Passwords are hard.
  - Let’s choose 4 digits, hmmm, 2468! Perfect!



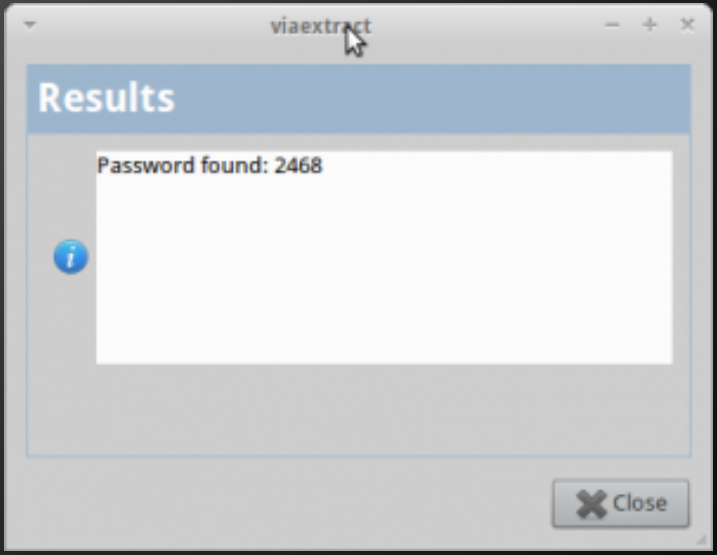
viaextract

Brute force: Progress

Please wait while each 4-digit password is tested.

Note that the device may reboot during this process.

Complete!



viaextract

Results

Password found: 2468

Credit: VIAFORENSICS LLC. 2014

Encrypted filesystems cont’d

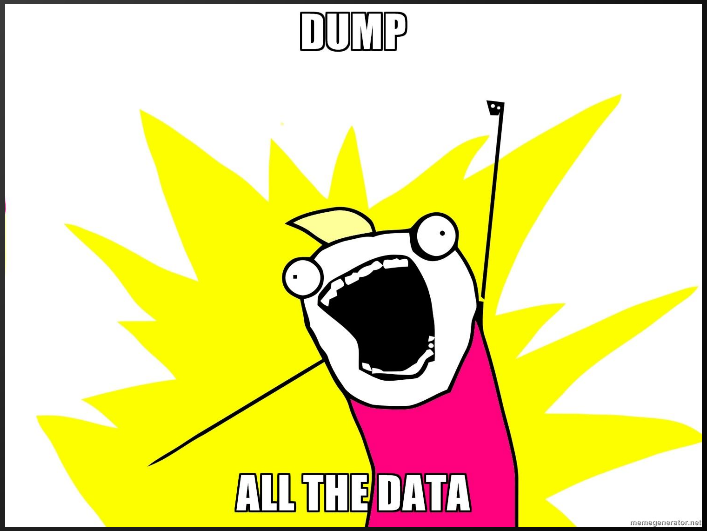
- Can be done by JTAG acquisition or adb
- Put device in recovery and connect via adb

Example: Pulling the header and footer for a Galaxy Nexus

```
adb shell dd if=/dev/block/mmcblk0p12 of=/tmp_header bs=512 count=1
adb shell dd if=/dev/block/mmcblk0p13 of=/tmp_footer
adb pull tmp_header
adb pull tmp_footer
```

Much more

- Acquired a full NAND image of a locked device
- Juicy artifacts to create timelines with
- Abundance of metadata to prove user actions in court
- Databases contain timestamps that can be associated with interactions
- Deleted files can be recovered
- Unused space may yield deleted information if not already TRIM'd
- This process **is not limited** to the Nexus 4!
    - The RiffBox supports a LOT of devices



Industry fails

- Requested trials of 11 commercial forensic suites for research purposes
- Request was for a trial of software with either limited use or 3 day limited full feature set.
- Signed 2 NDA’s, no significant responses from the rest
  - Second one returned a rather rude response
    - “Our software is for government and professional use.”
    - “Students are not our target users.”
    - “Students will not understand how to use our software.”
    - “Please do not contact us again with such absurd requests”.
    - “Stay in school.” < (really professional)

A simple “No, we don’t offer trials” would have sufficed.

(the above can be released provided that the party involved is not identified)

Commercial Forensics suites

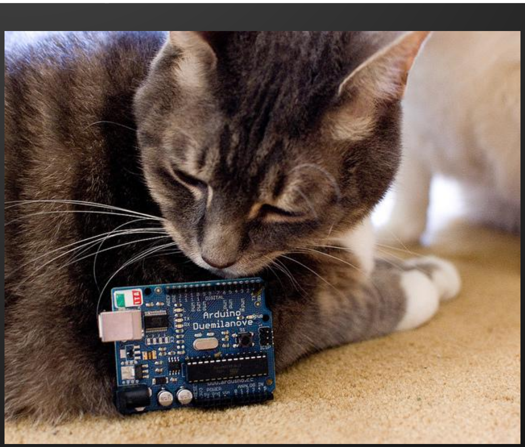
Product	Platform	Description
Encase	WINDAHS	Multi-purpose toolkit
Paraben Device Seizure	WINDAHS	Hardware + Software
FTK	WINDAHS	Multi-purpose toolkit, good with raw images
Cellebrite Mobile Forensics	WINDAHS	Cop-stop rape kit (yep)
Oxygen Forensic Suite	WINDAHS	“Smart forensics for smartphones”
viaExtract (viaForensics)	Linux (Santoku)	“...guided data acquisitions, flexible reporting…”

Sigh… so many windahs… and they cost thousands for single year licenses.

Open Source tools

Product	Platform	Description
The Sleuth Kit (best!)	Linux!	A diverse library of digital forensic tools Great documentation and wikis
CAINE	Linux!	Computer forensics distro
Open Computer Forensics Architecture	Linux!	Computer forensics framework
Digital Forensics Framework (also best!)	Linux!	A GUI framework for computer forensics
viaExtract CE (Community Edition)	Linux!	Santoku Linux w/acquisition tools and more!

Arduino cat agrees ➡



JTAG Hardware

Medusa Box

Omnia Repair Tool

Octoplus Box

RIFF Box

- What’s the difference?
  - Software capabilities (extent of what can be done w/above boxes)
  - Device support
  - Protocol support (e.g. FBus for Nokia devices)

Credits

hackerX

TheJH

Chrissy -- xoxo gossip goat

schizoid_astronaut

Crash Override AKA Zero Cool

Acid Burn

Joey

viaForensics

David Halfpenny

Ruxmon and Ruxcon <3

and...

Infosec.

If you’re not having fun,
you’re not doing it right.

This presentation was brought to you by
Aperture Science

Keep on testing.

tty0x80@gmail.com