FlashMemory SUMMIT

cellebrite
delivering mobile expertise

# Smart Phone Forensics

## Recovery and Imaging of NAND based Smart Devices

Ronen Engler – Senior Manager
Technology & Innovation

# About Cellebrite

- Established in 1999
- Professional staff of ~350 Employees
- Strong focus on R&D with ~170 R&D professionals
- 140,000+ Systems Deployed

# Smart Phones

## Mobile & Retail

*Data transfer, backup, management and Diagnostics*

## Law Enforcement & Security

*Mobile Devices Forensics*

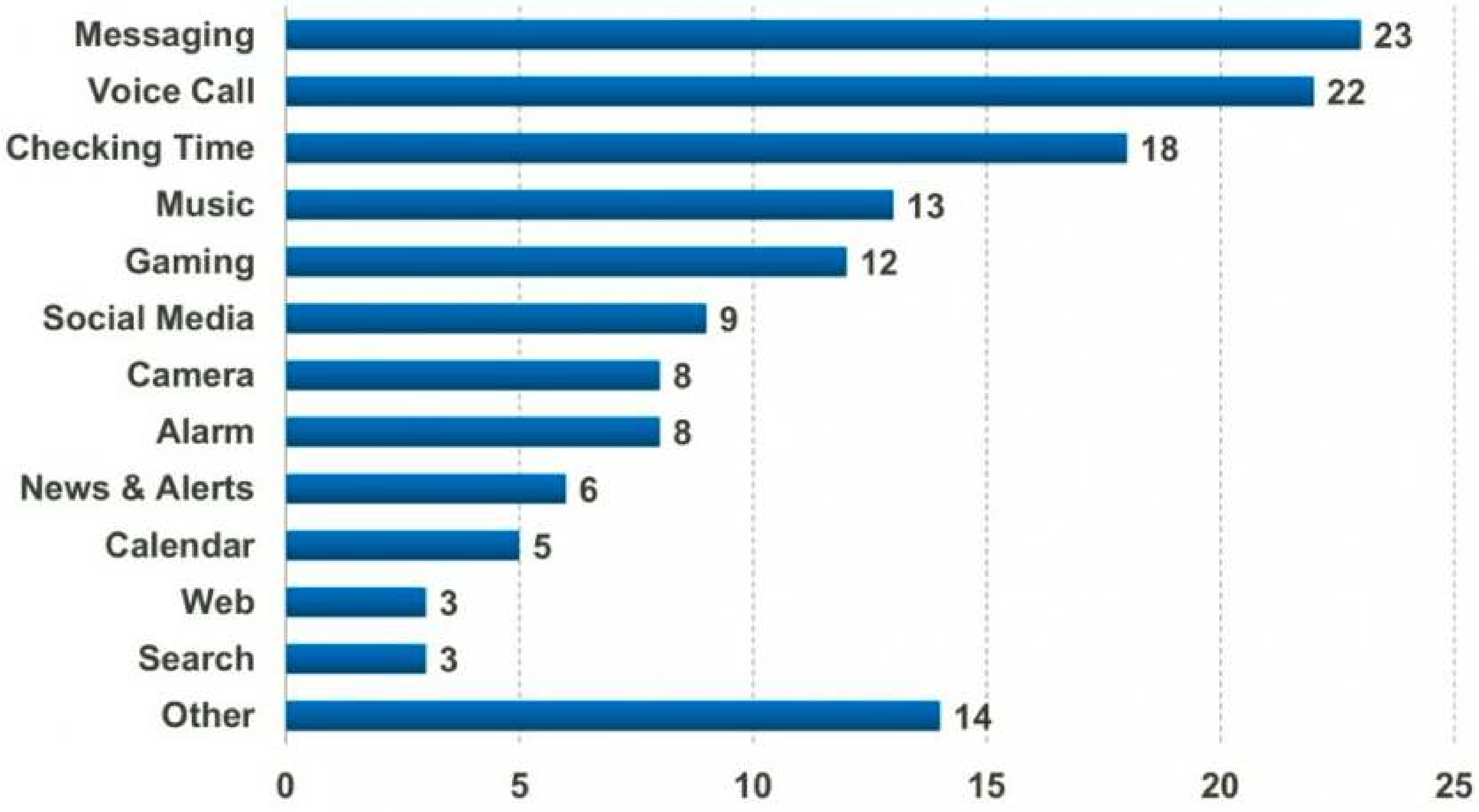
6
7
8
9
0

1:52 P.M.

# Mobile Forensics

# Smartphone Users Reach to Phone ~150x a day

# of times typical user checks phone per day



Source: TomiAhonenAlmanac 2013
http://www.businessinsider.com/mary-meekers-latest-masterful-presentation-on-the-state-of-the-web-2013-5#-52

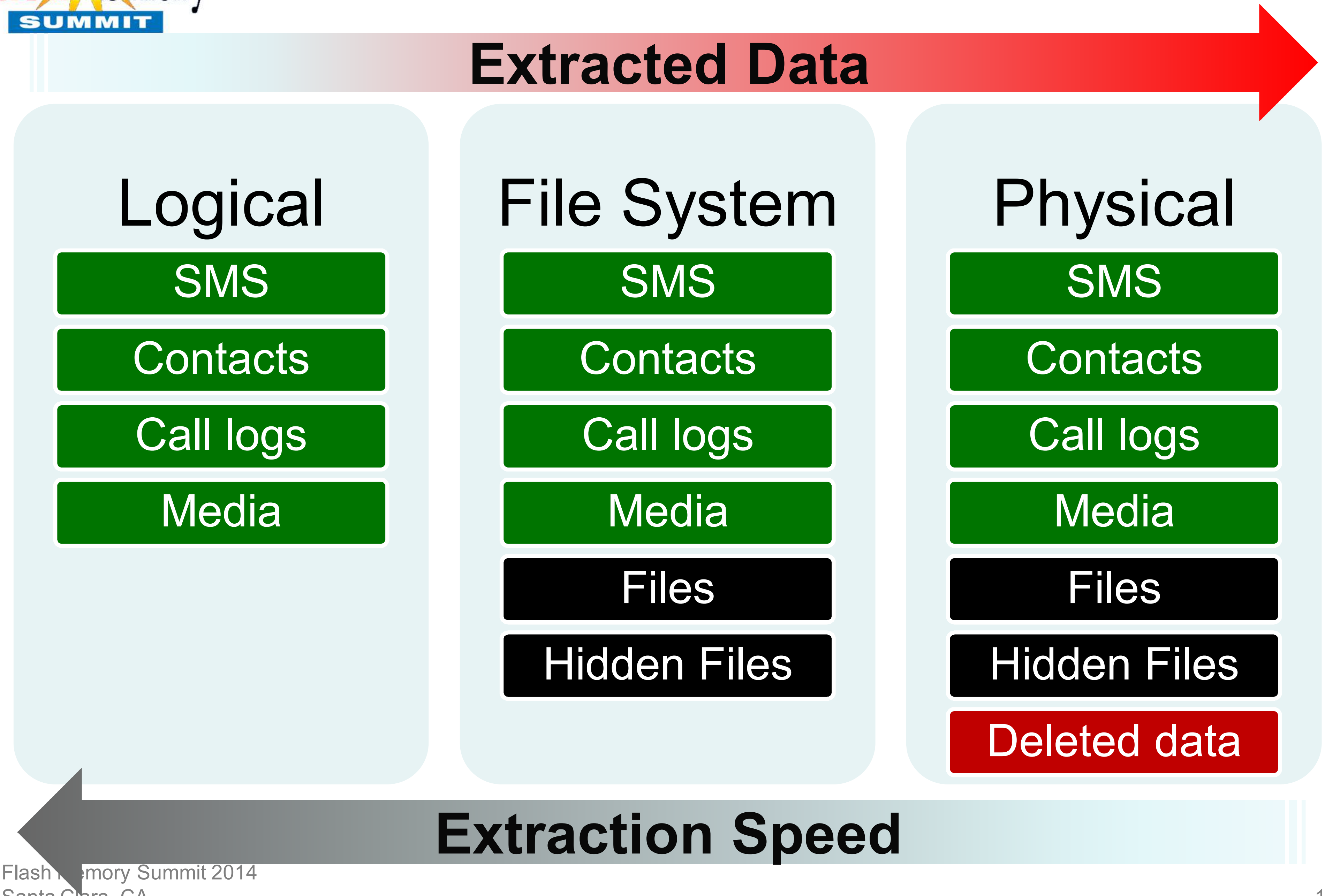
# Who needs Mobile Forensics?

# Process

EXTRACTION
ANALYSIS

# Current Methods

# Logical vs. File System vs. Physical extraction

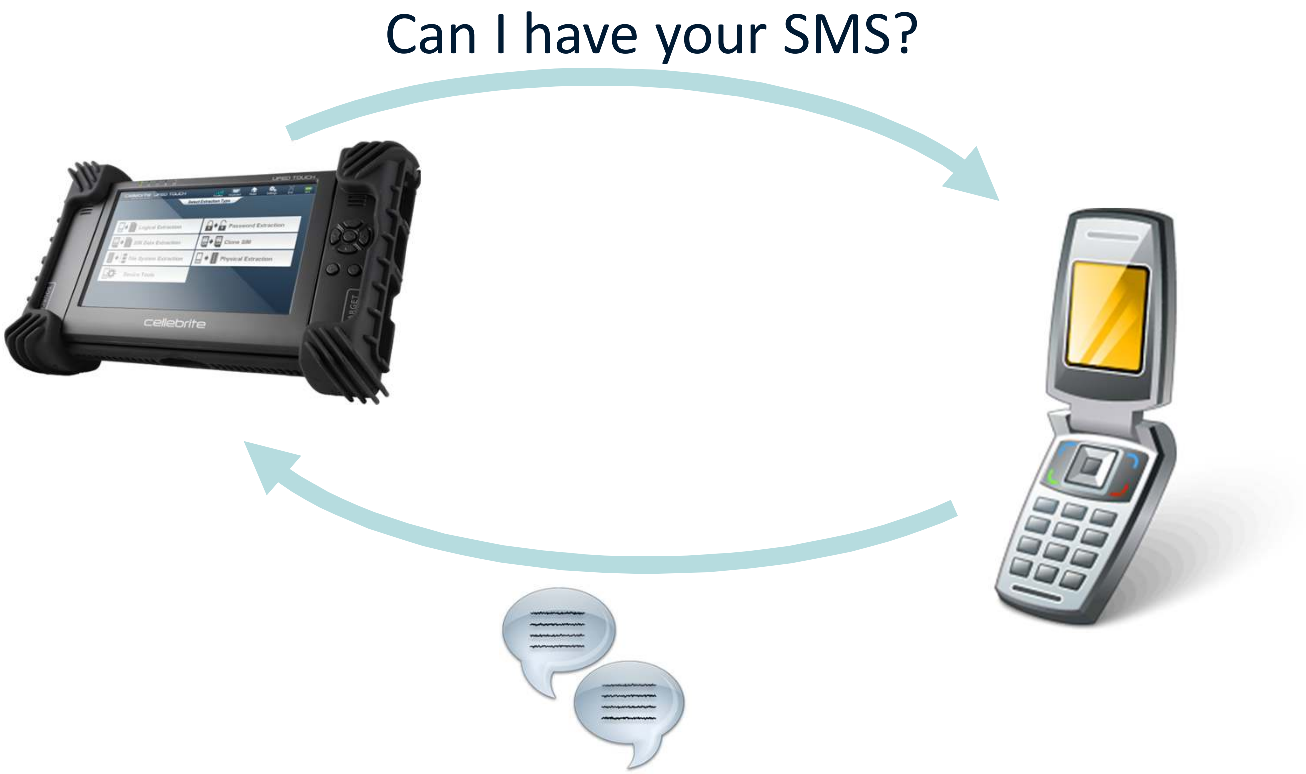


Extracted Data

| Logical | File System | Physical |
|---|---|---|
| SMS | SMS | SMS |
| Contacts | Contacts | Contacts |
| Call logs | Call logs | Call logs |
| Media | Media | Media |
| | Files | Files |
| | Hidden Files | Hidden Files |
| | | Deleted data |

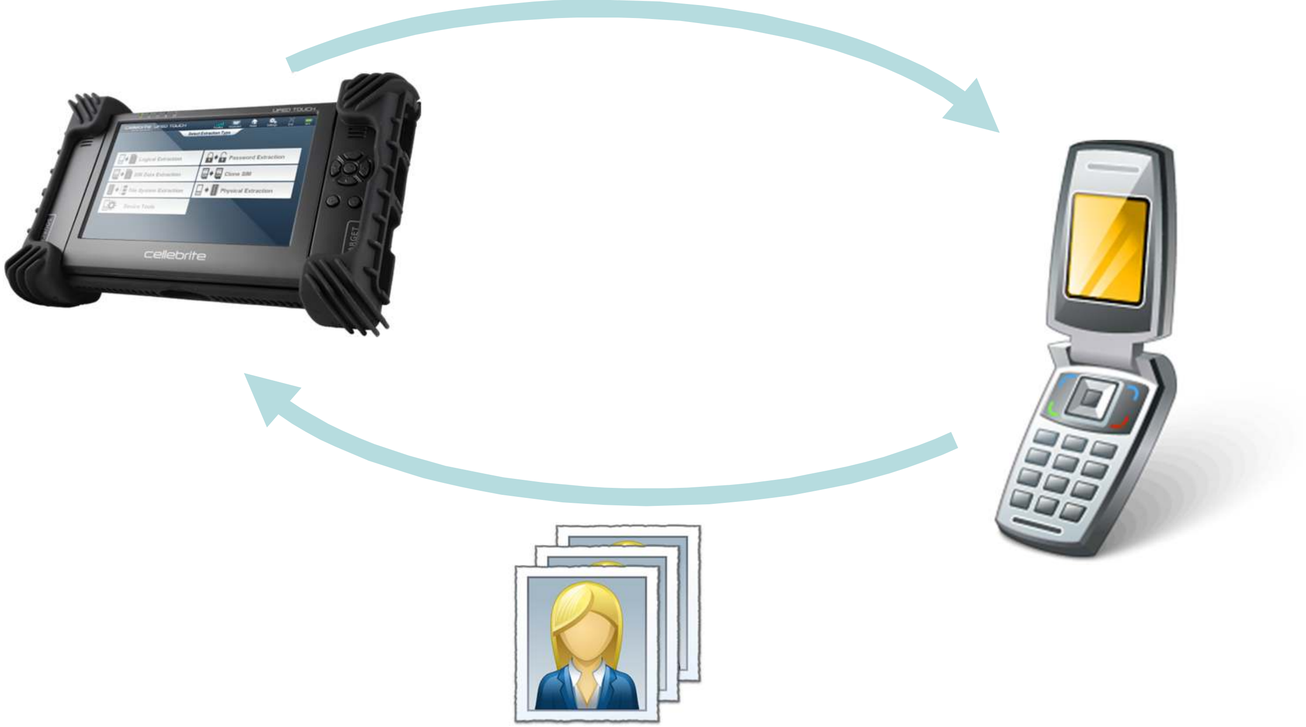
Extraction Speed

# UFED Logical Extraction



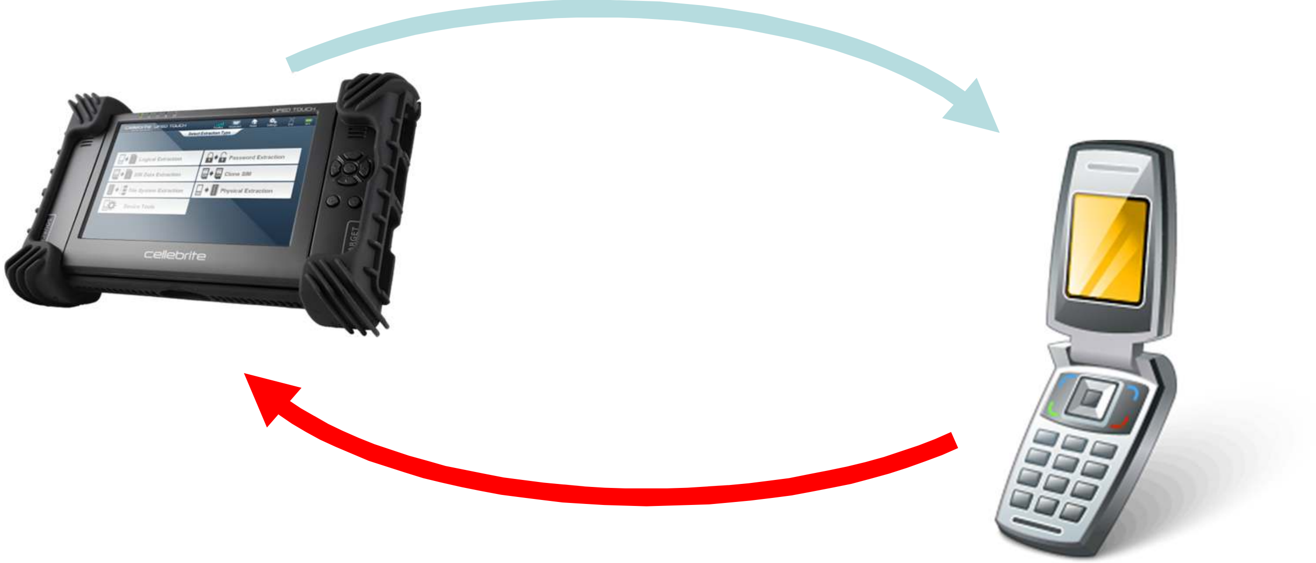
Can I have your SMS?

# UFED Logical Extraction (2)



Can I have your pictures as well?

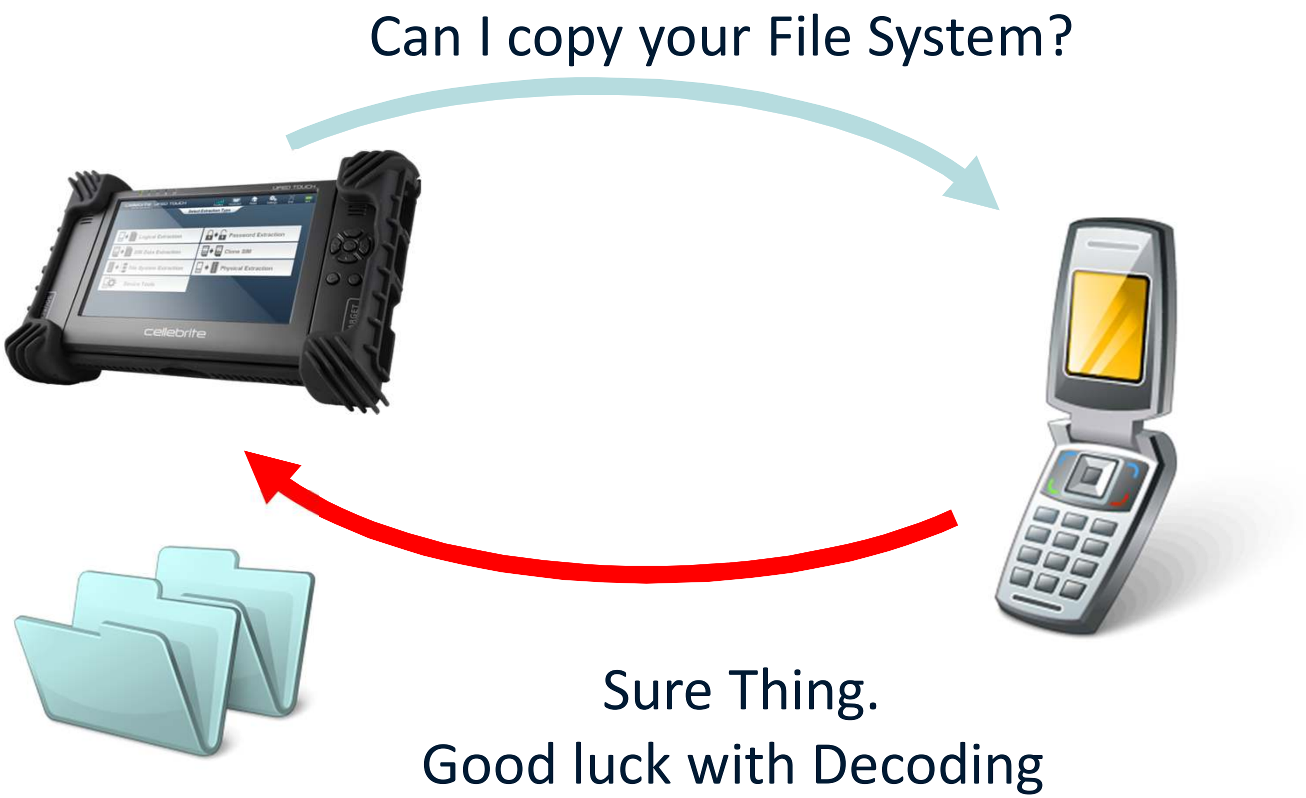
# UFED Logical Extraction (3)



How about the emails, please?

**NO**

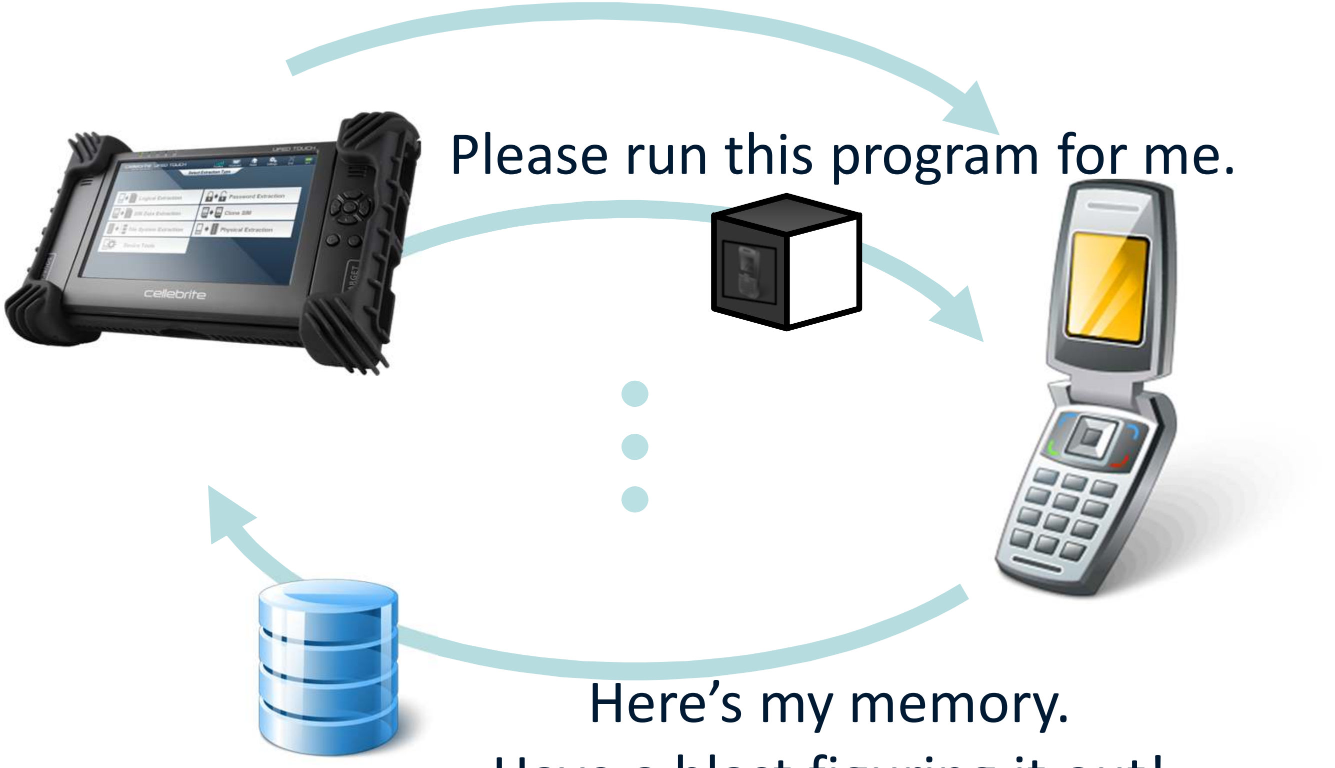
# UFED File System Dump



Can I copy your File System?

Sure Thing.
Good luck with Decoding

# UFED Physical Dump



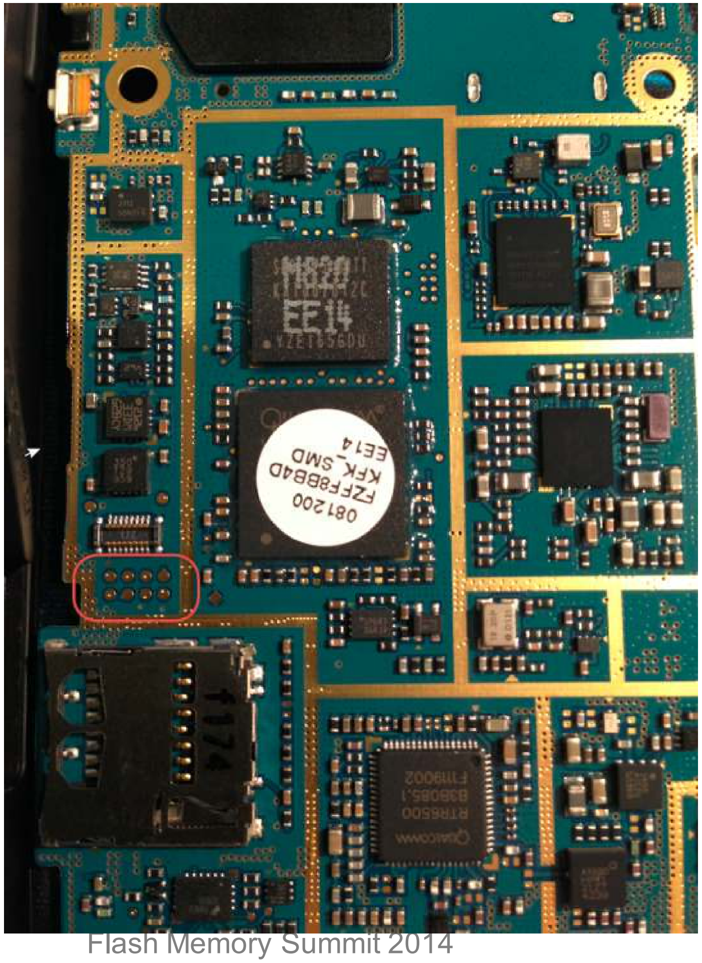
Good morning, sir.

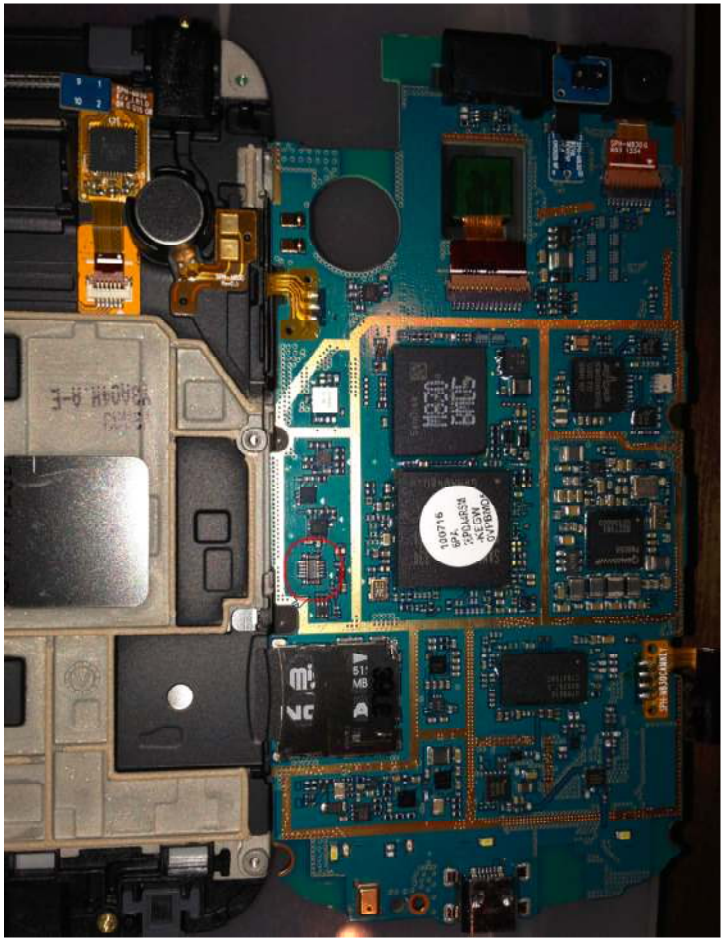
Please run this program for me.

Here’s my memory.
Have a blast figuring it out!

# Current Methods

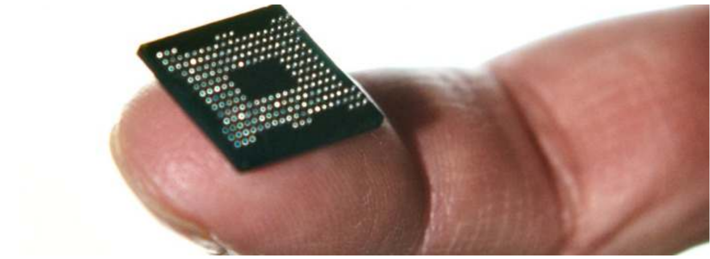
- JTAG



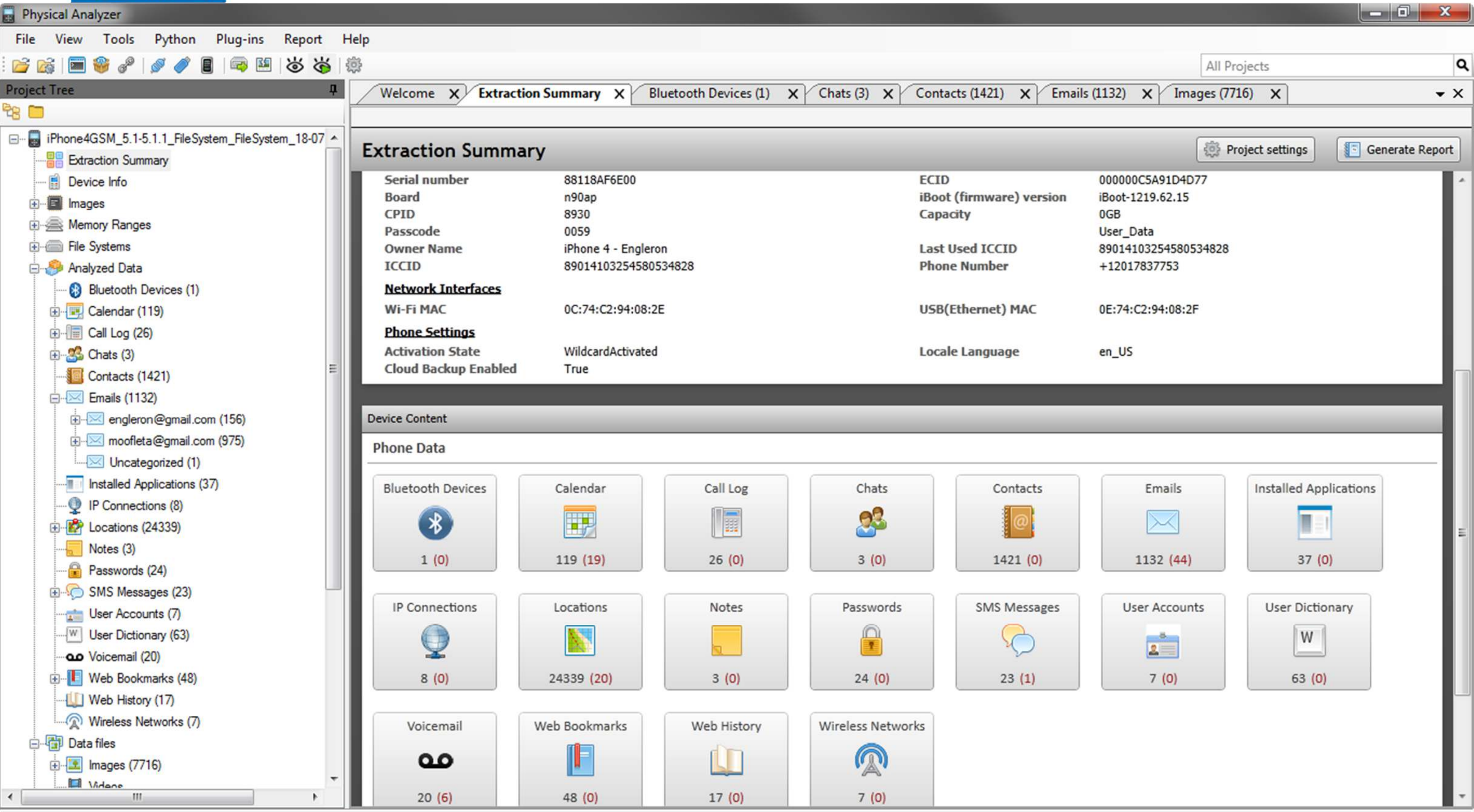


# Current Methods

- CHIP OFF



# Decoding & Analysis



- iPhone4GSM_5.1-5.1.1_FileSystem_FileSystem_18-07
  - Extraction Summary
  - Device Info
  - Images
  - Memory Ranges
  - File Systems
  - Analyzed Data
    - Bluetooth Devices (1)
    - Calendar (119)
    - Call Log (26)
    - Chats (3)
    - Contacts (1421)
    - Emails (1132)
      - engleron@gmail.com (156)
      - moofleta@gmail.com (975)
      - Uncategorized (1)
    - Installed Applications (37)
    - IP Connections (8)
    - Locations (24339)
    - Notes (3)
    - Passwords (24)
    - SMS Messages (23)
    - User Accounts (7)
    - User Dictionary (63)
    - Voicemail (20)
    - Web Bookmarks (48)
    - Web History (17)
    - Wireless Networks (7)
  - Data files
    - Images (7716)
    - Videos

## Extraction Summary

| | | | |
|---|---|---|---|
| Serial number | 88118AF6E00 | ECID | 000000C5A91D4D77 |
| Board | n90ap | iBoot (firmware) version | iBoot-1219.62.15 |
| CPID | 8930 | Capacity | 0GB |
| Passcode | 0059 | | User_Data |
| Owner Name | iPhone 4 - Engleron | Last Used ICCID | 89014103254580534828 |
| ICCID | 89014103254580534828 | Phone Number | +12017837753 |

**Network Interfaces**

| | | | |
|---|---|---|---|
| Wi-Fi MAC | 0C:74:C2:94:08:2E | USB(Ethernet) MAC | 0E:74:C2:94:08:2F |

**Phone Settings**

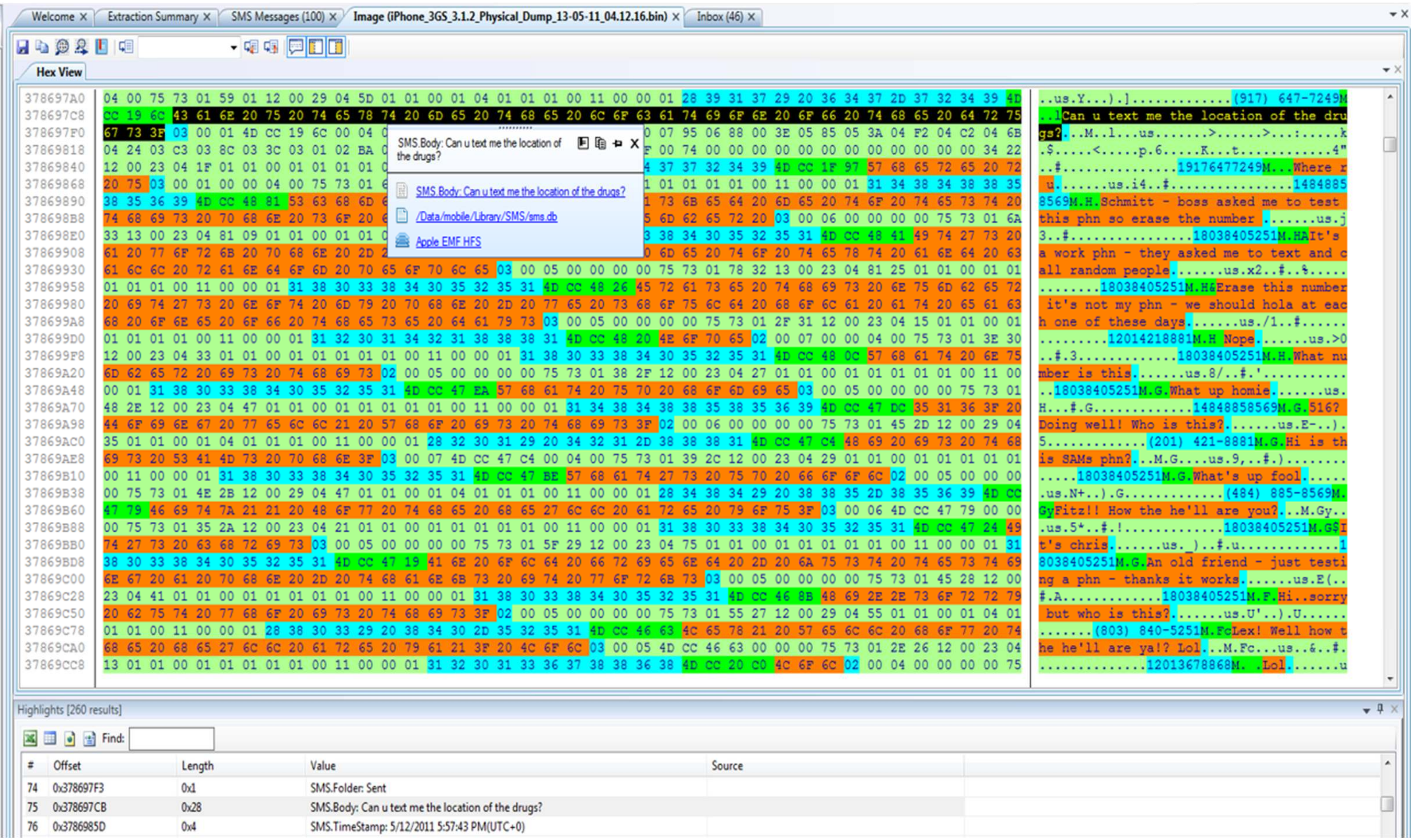
| | | | |
|---|---|---|---|
| Activation State | WildcardActivated | Locale Language | en_US |
| Cloud Backup Enabled | True | | |

Device Content

Phone Data

| Item | Count |
|---|---|
| Bluetooth Devices | 1 (0) |
| Calendar | 119 (19) |
| Call Log | 26 (0) |
| Chats | 3 (0) |
| Contacts | 1421 (0) |
| Emails | 1132 (44) |
| Installed Applications | 37 (0) |
| IP Connections | 8 (0) |
| Locations | 24339 (20) |
| Notes | 3 (0) |
| Passwords | 24 (0) |
| SMS Messages | 23 (1) |
| User Accounts | 7 (0) |
| User Dictionary | 63 (0) |
| Voicemail | 20 (6) |
| Web Bookmarks | 48 (0) |
| Web History | 17 (0) |
| Wireless Networks | 7 (0) |

# Decoding & Analysis



```
378697A0  04 00 75 73 01 59 01 12 00 29 04 5D 01 01 00 01 04 01 01 01 00 11 00 00 01 28 39 31 37 29 20 36 34 37 2D 37 32 34 39 4D  ..us.Y...).]............(917) 647-7249M
378697C8  CC 19 6C 43 61 6E 20 75 20 74 65 78 74 20 6D 65 20 74 68 65 20 6C 6F 63 61 74 69 6F 6E 20 6F 66 20 74 68 65 20 64 72 75  ..lCan u text me the location of the dru
378697F0  67 73 3F 03 00 01 4D CC 19 6C 00 04 0                                  0 07 95 06 88 00 3E 05 85 05 3A 04 F2 04 C2 04 6B  gs?...M..l...us.......>......>...:.....k
37869818  04 24 03 C3 03 8C 03 3C 03 01 02 BA 0                                  F 00 74 00 00 00 00 00 00 00 00 00 00 00 00 34 22  .$.....<.....p.6.....K...t...........4"
37869840  12 00 23 04 1F 01 01 00 01 01 01 01 0                                  4 37 37 32 34 39 4D CC 1F 97 57 68 65 72 65 20 72  ..#...............19176477249M...Where r
37869868  20 75 03 00 01 00 00 04 00 75 73 01 6                                  1 01 01 01 01 00 11 00 00 01 31 34 38 34 38 38 35   u.......us.i4..#................1484885
37869890  38 35 36 39 4D CC 48 81 53 63 68 6D 6                                  1 73 6B 65 64 20 6D 65 20 74 6F 20 74 65 73 74 20  8569M.H.Schmitt - boss asked me to test 
378698B8  74 68 69 73 20 70 68 6E 20 73 6F 20 6                                  5 6D 62 65 72 20 03 00 06 00 00 00 00 75 73 01 6A  this phn so erase the number .......us.j
378698E0  33 13 00 23 04 81 09 01 01 00 01 01 0                                  3 38 34 30 35 32 35 31 4D CC 48 41 49 74 27 73 20  3..#...............18038405251M.HAIt's 
37869908  61 20 77 6F 72 6B 20 70 68 6E 20 2D 2                                  0 6D 65 20 74 6F 20 74 65 78 74 20 61 6E 64 20 63  a work phn - they asked me to text and c
37869930  61 6C 6C 20 72 61 6E 64 6F 6D 20 70 65 6F 70 6C 65 03 00 05 00 00 00 00 75 73 01 78 32 13 00 23 04 81 25 01 01 00 01 01  all random people.......us.x2..#..%.....
37869958  01 01 01 00 11 00 00 01 31 38 30 33 38 34 30 35 32 35 31 4D CC 48 26 45 72 61 73 65 20 74 68 69 73 20 6E 75 6D 62 65 72  .........18038405251M.H&Erase this number
37869980  20 69 74 27 73 20 6E 6F 74 20 6D 79 20 70 68 6E 20 2D 20 77 65 20 73 68 6F 75 6C 64 20 68 6F 6C 61 20 61 74 20 65 61 63   it's not my phn - we should hola at eac
378699A8  68 20 6F 6E 65 20 6F 66 20 74 68 65 73 65 20 64 61 79 73 03 00 05 00 00 00 00 75 73 01 2F 31 12 00 23 04 15 01 01 00 01  h one of these days.......us./1..#......
378699D0  01 01 01 01 00 11 00 00 01 31 32 30 31 34 32 31 38 38 38 31 4D CC 48 20 4E 6F 70 65 02 00 07 00 00 04 00 75 73 01 3E 30  .........12014218881M.H Nope.......us.>0
378699F8  12 00 23 04 33 01 01 00 01 01 01 01 01 00 11 00 00 01 31 38 30 33 38 34 30 35 32 35 31 4D CC 48 0C 57 68 61 74 20 6E 75  ..#.3.............18038405251M.H.What nu
37869A20  6D 62 65 72 20 69 73 20 74 68 69 73 02 00 05 00 00 00 00 75 73 01 38 2F 12 00 23 04 27 01 01 00 01 01 01 01 01 00 11 00  mber is this.......us.8/..#.'..........
37869A48  00 01 31 38 30 33 38 34 30 35 32 35 31 4D CC 47 EA 57 68 61 74 20 75 70 20 68 6F 6D 69 65 03 00 05 00 00 00 00 75 73 01  ..18038405251M.G.What up homie.......us.
37869A70  48 2E 12 00 23 04 47 01 01 00 01 01 01 01 01 00 11 00 00 01 31 34 38 34 38 38 35 38 35 36 39 4D CC 47 DC 35 31 36 3F 20  H...#.G.............14848858569M.G.516? 
37869A98  44 6F 69 6E 67 20 77 65 6C 6C 21 20 57 68 6F 20 69 73 20 74 68 69 73 3F 02 00 06 00 00 00 00 75 73 01 45 2D 12 00 29 04  Doing well! Who is this?.......us.E-..).
37869AC0  35 01 01 00 01 04 01 01 01 00 11 00 00 01 28 32 30 31 29 20 34 32 31 2D 38 38 38 31 4D CC 47 C4 48 69 20 69 73 20 74 68  5.............(201) 421-8881M.G.Hi is th
37869AE8  69 73 20 53 41 4D 73 20 70 68 6E 3F 03 00 07 4D CC 47 C4 00 04 00 75 73 01 39 2C 12 00 23 04 29 01 01 00 01 01 01 01 01  is SAMs phn?...M.G....us.9,..#.)........
37869B10  00 11 00 00 01 31 38 30 33 38 34 30 35 32 35 31 4D CC 47 BE 57 68 61 74 27 73 20 75 70 20 66 6F 6F 6C 02 00 05 00 00 00  .....18038405251M.G.What's up fool.....
37869B38  00 75 73 01 4E 2B 12 00 29 04 47 01 01 00 01 04 01 01 01 00 11 00 00 01 28 34 38 34 29 20 38 38 35 2D 38 35 36 39 4D CC  .us.N+..).G............(484) 885-8569M.
37869B60  47 79 46 69 74 7A 21 21 20 48 6F 77 20 74 68 65 20 68 65 27 6C 6C 20 61 72 65 20 79 6F 75 3F 03 00 06 4D CC 47 79 00 00  GyFitz!! How the he'll are you?...M.Gy..
37869B88  00 75 73 01 35 2A 12 00 23 04 21 01 01 00 01 01 01 01 01 00 11 00 00 01 31 38 30 33 38 34 30 35 32 35 31 4D CC 47 24 49  .us.5*..#.!.............18038405251M.G$I
37869BB0  74 27 73 20 63 68 72 69 73 03 00 05 00 00 00 00 75 73 01 5F 29 12 00 23 04 75 01 01 00 01 01 01 01 01 00 11 00 00 01 31  t's chris.......us._)..#.u.............1
37869BD8  38 30 33 38 34 30 35 32 35 31 4D CC 47 19 41 6E 20 6F 6C 64 20 66 72 69 65 6E 64 20 2D 20 6A 75 73 74 20 74 65 73 74 69  8038405251M.G.An old friend - just testi
37869C00  6E 67 20 61 20 70 68 6E 20 2D 20 74 68 61 6E 6B 73 20 69 74 20 77 6F 72 6B 73 03 00 05 00 00 00 00 75 73 01 45 28 12 00  ng a phn - thanks it works.......us.E(..
37869C28  23 04 41 01 01 00 01 01 01 01 01 00 11 00 00 01 31 38 30 33 38 34 30 35 32 35 31 4D CC 46 8B 48 69 2E 2E 73 6F 72 72 79  #.A............18038405251M.F.Hi..sorry
37869C50  20 62 75 74 20 77 68 6F 20 69 73 20 74 68 69 73 3F 02 00 05 00 00 00 00 75 73 01 55 27 12 00 29 04 55 01 01 00 01 04 01   but who is this?.......us.U'..).U.....
37869C78  01 01 00 11 00 00 01 28 38 30 33 29 20 38 34 30 2D 35 32 35 31 4D CC 46 63 4C 65 78 21 20 57 65 6C 6C 20 68 6F 77 20 74  .......(803) 840-5251M.FcLex! Well how t
37869CA0  68 65 20 68 65 27 6C 6C 20 61 72 65 20 79 61 21 3F 20 4C 6F 6C 03 00 05 4D CC 46 63 00 00 00 75 73 01 2E 26 12 00 23 04  he he'll are ya!? Lol...M.Fc...us..&..#.
37869CC8  13 01 01 00 01 01 01 01 01 00 11 00 00 01 31 32 30 31 33 36 37 38 38 36 38 4D CC 20 C0 4C 6F 6C 02 00 04 00 00 00 00 75  ...............12013678868M. .Lol.......u
```

SMS.Body: Can u text me the location of the drugs?

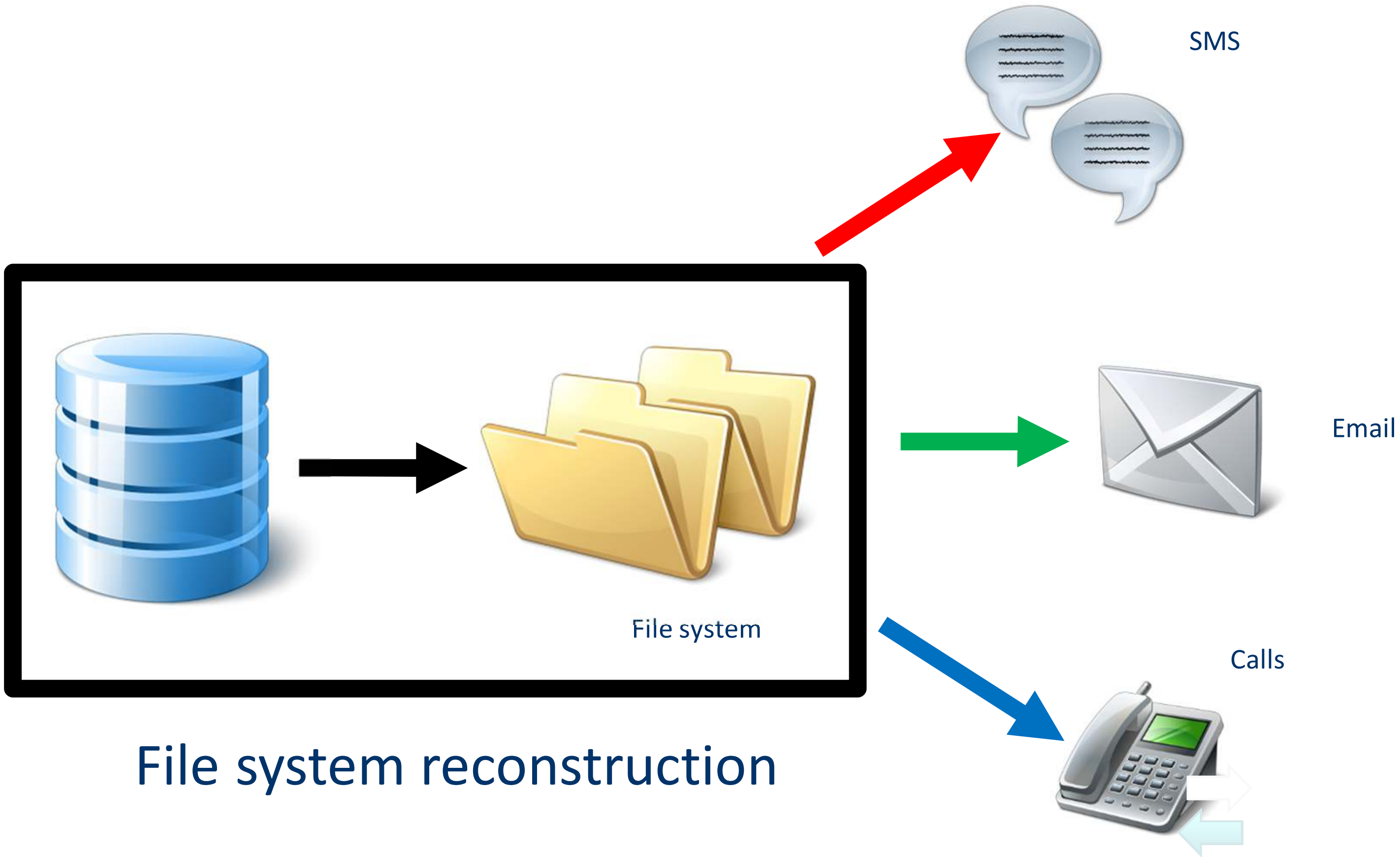
SMS.Body: Can u text me the location of the drugs?

/Data/mobile/Library/SMS/sms.db

Apple EMF HFS

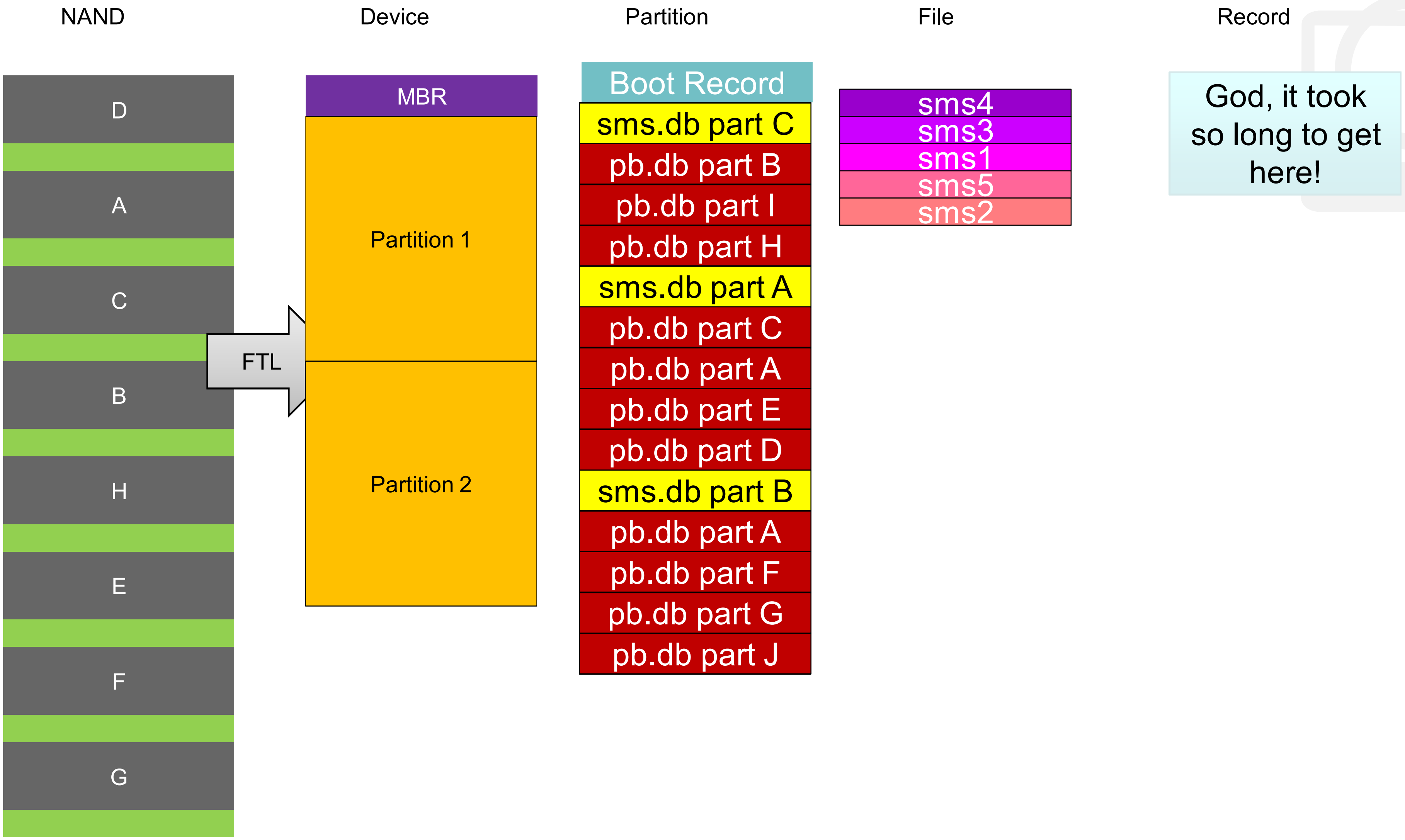
| # | Offset | Length | Value | Source |
|---|---|---|---|---|
| 74 | 0x378697F3 | 0x1 | SMS.Folder: Sent | |
| 75 | 0x378697CB | 0x28 | SMS.Body: Can u text me the location of the drugs? | |
| 76 | 0x3786985D | 0x4 | SMS.TimeStamp: 5/12/2011 5:57:43 PM(UTC+0) | |

# Data Path



File system reconstruction

# Architecture – Memory



NAND

D

A

C

B

H

E

F

G

FTL

Device

MBR

Partition 1

Partition 2

Partition

Boot Record

sms.db part C

pb.db part B

pb.db part I

pb.db part H

sms.db part A

pb.db part C

pb.db part A

pb.db part E

pb.db part D

sms.db part B

pb.db part A

pb.db part F

pb.db part G

pb.db part J

File

sms4

sms3

sms1

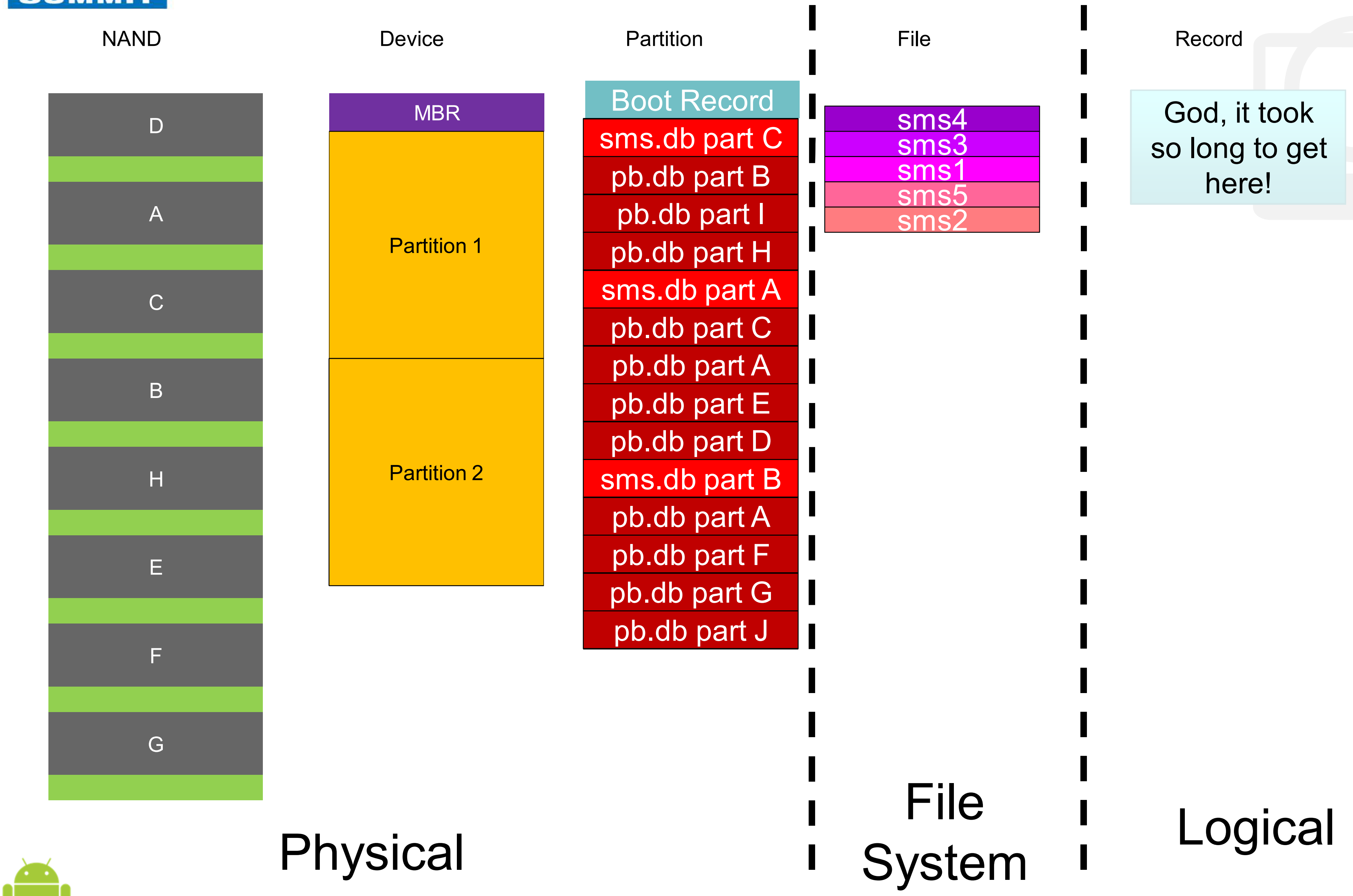
sms5

sms2

Record

God, it took so long to get here!

# Architecture – Memory



NAND

D

A

C

B

H

E

F

G

Device

MBR

Partition 1

Partition 2

Partition

Boot Record

sms.db part C

pb.db part B

pb.db part I

pb.db part H

sms.db part A

pb.db part C

pb.db part A

pb.db part E

pb.db part D

sms.db part B

pb.db part A

pb.db part F

pb.db part G

pb.db part J

Physical

File

sms4

sms3

sms1

sms5

sms2

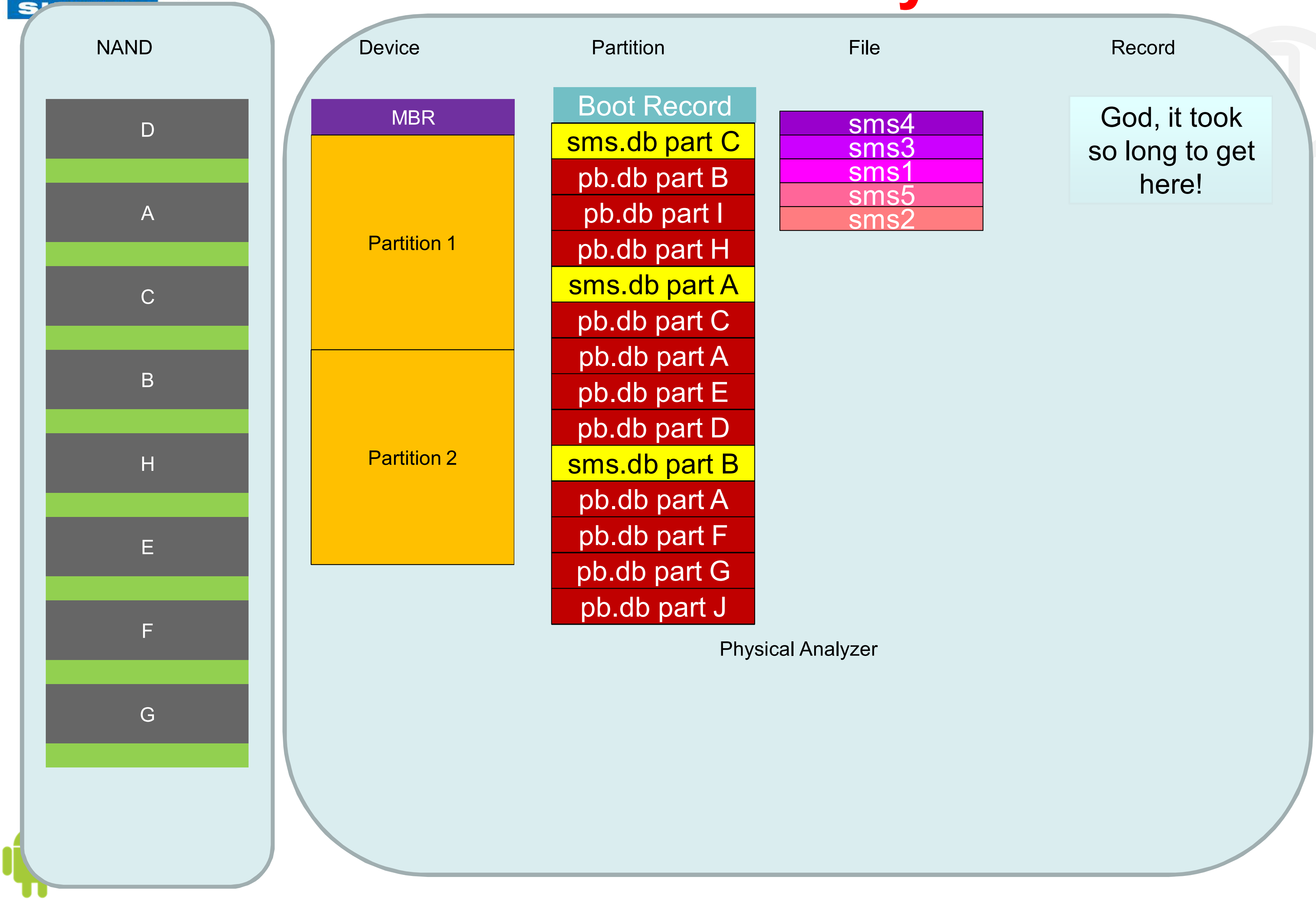
File System

Record

God, it took so long to get here!

Logical

# Architecture – Memory Access



NAND

D

A

C

B

H

E

F

G

Device

MBR

Partition 1

Partition 2

Partition

Boot Record

sms.db part C

pb.db part B

pb.db part I

pb.db part H

sms.db part A

pb.db part C

pb.db part A

pb.db part E

pb.db part D

sms.db part B

pb.db part A

pb.db part F

pb.db part G

pb.db part J

File

sms4

sms3

sms1

sms5

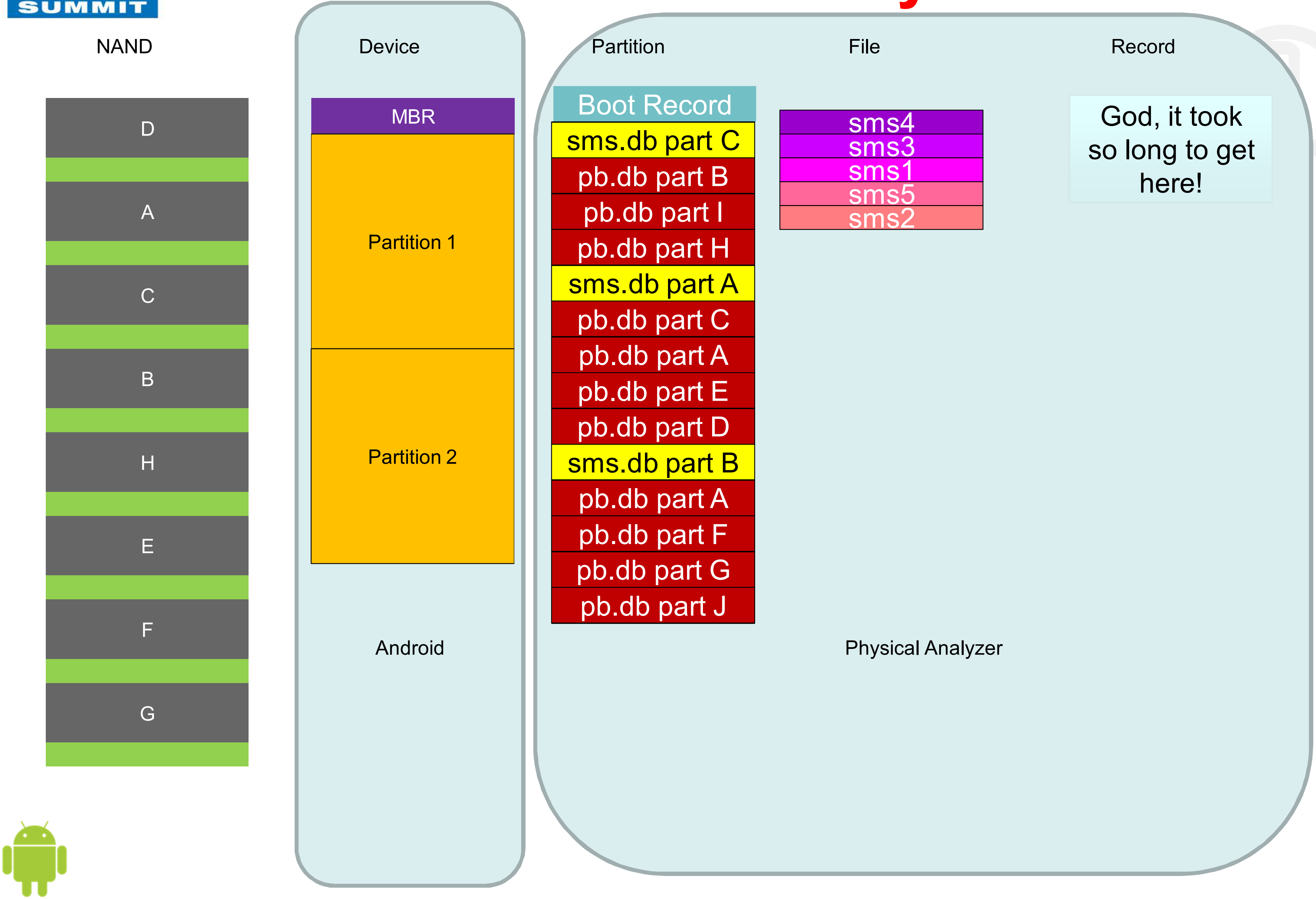
sms2

Record

God, it took so long to get here!

Physical Analyzer

# Architecture – Memory Access



NAND

D

A

C

B

H

E

F

G

Device

MBR

Partition 1

Partition 2

Android

Partition

Boot Record

sms.db part C

pb.db part B

pb.db part I

pb.db part H

sms.db part A

pb.db part C

pb.db part A

pb.db part E

pb.db part D

sms.db part B

pb.db part A

pb.db part F

pb.db part G

pb.db part J

File

sms4

sms3

sms1

sms5

sms2

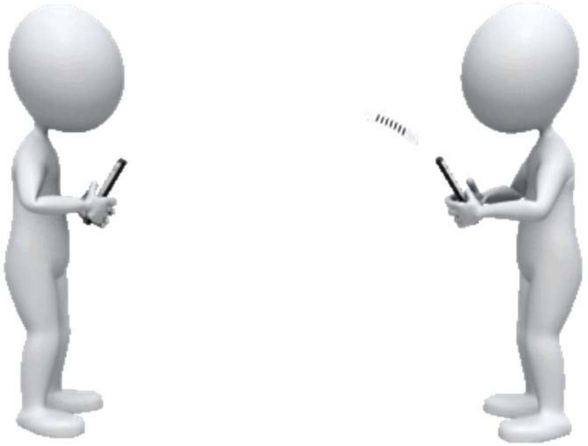
Record

God, it took so long to get here!

Physical Analyzer

# More Challenges

# Summary



# Thank You

Ronen.Engler@Cellebrite.com