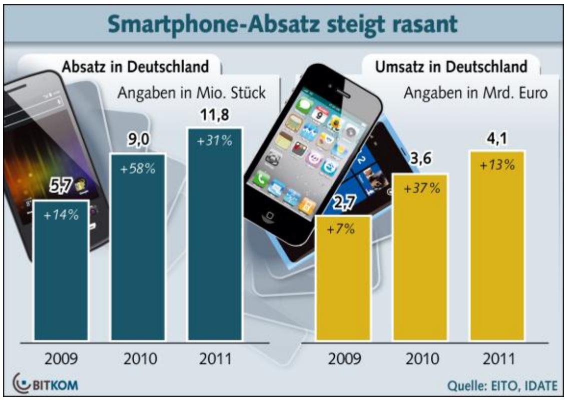
cellebrite
mobile data secured

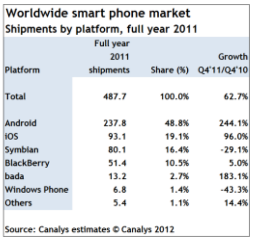
Trends in der Forensik von Mobiltelefonen

2. IT-Forensik Workshop
18. April 2012 in Aachen

Peter Warnke
peterw@cellebrite.com

„Ein Smartphone bitte…“

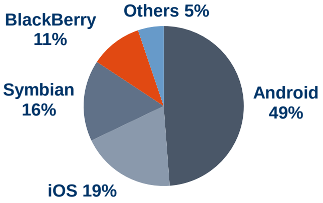




Worldwide smart phone market
Shipments by platform, full year 2011

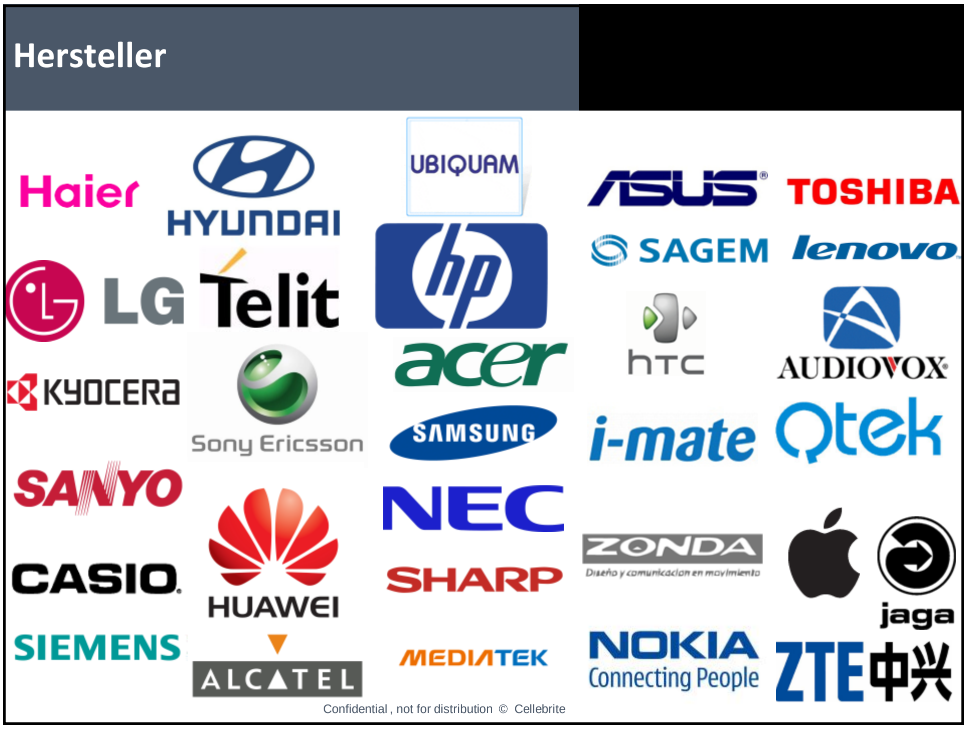
Platform	Full year 2011 shipments	Share (%)	Growth Q4'11/Q4'10
Total	487.7	100.0%	62.7%
Android	237.8	48.8%	244.1%
iOS	93.1	19.1%	96.0%
Symbian	80.1	16.4%	-29.1%
BlackBerry	51.4	10.5%	5.0%
bada	13.2	2.7%	183.1%
Windows Phone	6.8	1.4%	-43.3%
Others	5.4	1.1%	14.4%

Source: Canalys estimates © Canalys 2012



Android, iOS und BlackBerry führend

#1 – Plattformen & Hersteller

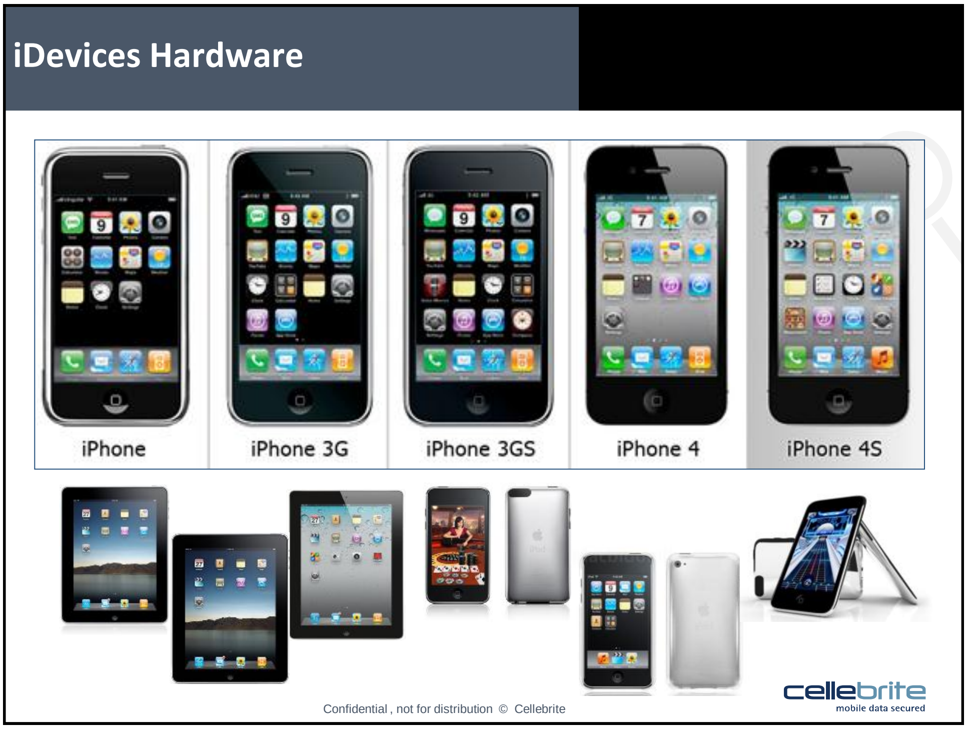


Hersteller

Confidential , not for distribution © Cellebrite

Plattformen

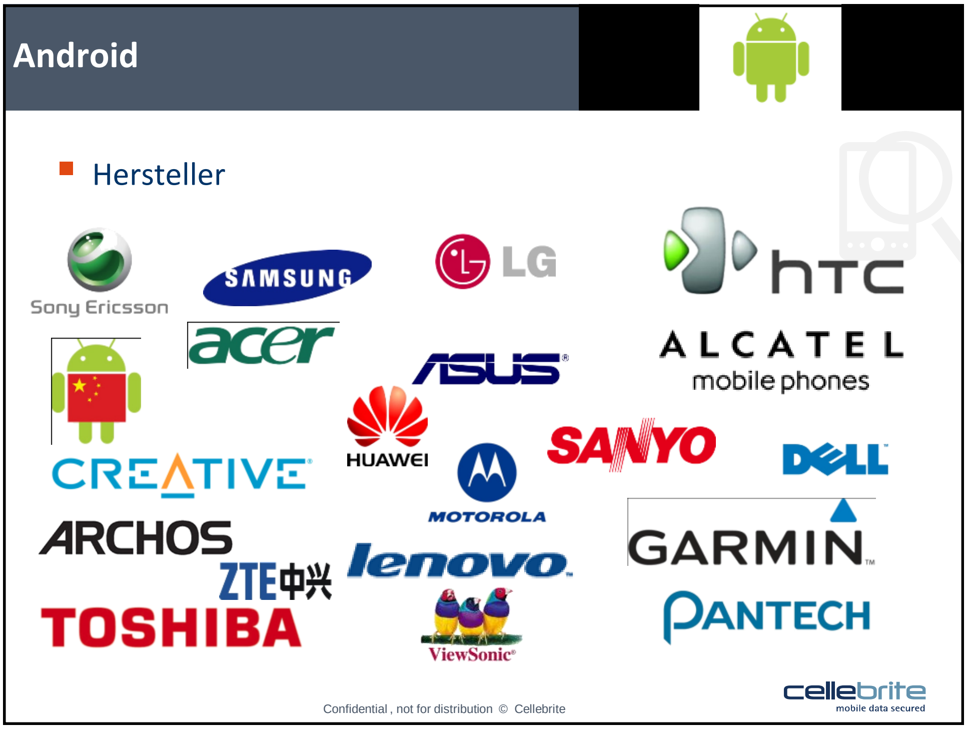
onfidential , not for distribution © Cellebrite



iDevices Hardware

Confidential , not for distribution © Cellebrite

cellebrite
mobile data secured



Android

- Hersteller

Confidential , not for distribution © Cellebrite

cellebrite
mobile data secured

Fake Phones & …

cellebrite
mobile data secured

cellebrite
mobile data secured

#2 – Anschlußmöglichkeiten

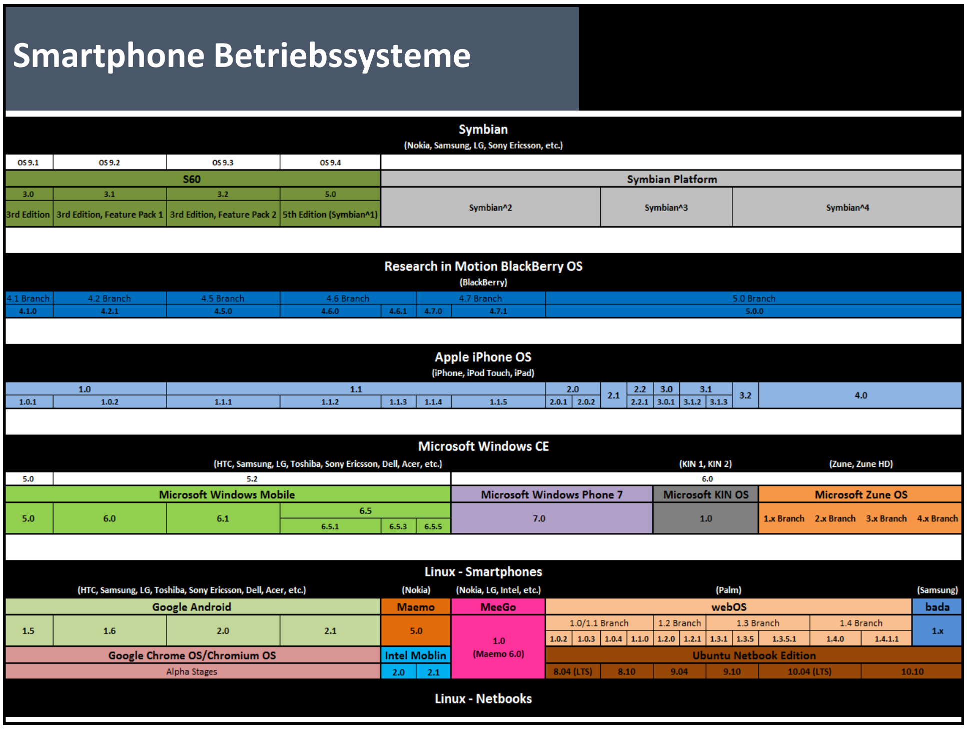
Anschlüsse

Anschlüsse – Smartphones?

Confidential , not for distribution © Cellebrite

cellebrite
mobile data secured

#3 – Betriebssysteme



Smartphone Betriebssysteme

Symbian
(Nokia, Samsung, LG, Sony Ericsson, etc.)

OS 9.1 | OS 9.2 | OS 9.3 | OS 9.4

S60 | Symbian Platform

3.0 | 3.1 | 3.2 | 5.0

3rd Edition | 3rd Edition, Feature Pack 1 | 3rd Edition, Feature Pack 2 | 5th Edition (Symbian^1) | Symbian^2 | Symbian^3 | Symbian^4

Research in Motion BlackBerry OS
(BlackBerry)

4.1 Branch | 4.2 Branch | 4.5 Branch | 4.6 Branch | 4.7 Branch | 5.0 Branch

4.1.0 | 4.2.1 | 4.5.0 | 4.6.0 | 4.6.1 | 4.7.0 | 4.7.1 | 5.0.0

Apple iPhone OS
(iPhone, iPod Touch, iPad)

1.0 | 1.1 | 2.0 | 2.1 | 2.2 | 3.0 | 3.1 | 3.2 | 4.0

1.0.1 | 1.0.2 | 1.1.1 | 1.1.2 | 1.1.3 | 1.1.4 | 1.1.5 | 2.0.1 | 2.0.2 | 2.2.1 | 3.0.1 | 3.1.2 | 3.1.3

Microsoft Windows CE
(HTC, Samsung, LG, Toshiba, Sony Ericsson, Dell, Acer, etc.) | (KIN 1, KIN 2) | (Zune, Zune HD)

5.0 | 5.2 | 6.0

Microsoft Windows Mobile | Microsoft Windows Phone 7 | Microsoft KIN OS | Microsoft Zune OS

5.0 | 6.0 | 6.1 | 6.5 | 7.0 | 1.0 | 1.x Branch | 2.x Branch | 3.x Branch | 4.x Branch

6.5.1 | 6.5.3 | 6.5.5

Linux - Smartphones
(HTC, Samsung, LG, Toshiba, Sony Ericsson, Dell, Acer, etc.) | (Nokia) | (Nokia, LG, Intel, etc.) | (Palm) | (Samsung)

Google Android | Maemo | MeeGo | webOS | bada

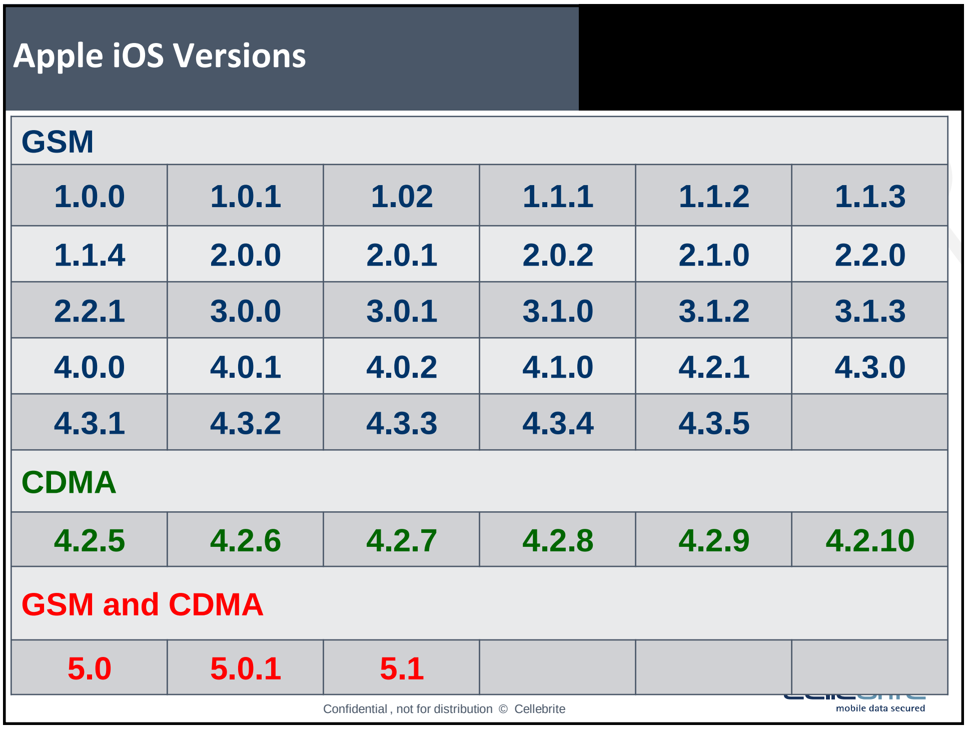
1.5 | 1.6 | 2.0 | 2.1 | 5.0 | 1.0 (Maemo 6.0) | 1.0/1.1 Branch | 1.2 Branch | 1.3 Branch | 1.4 Branch | 1.x

1.0.2 | 1.0.3 | 1.0.4 | 1.1.0 | 1.2.0 | 1.2.1 | 1.3.1 | 1.3.5 | 1.3.5.1 | 1.4.0 | 1.4.1.1

Google Chrome OS/Chromium OS | Intel Moblin | Ubuntu Netbook Edition

Alpha Stages | 2.0 | 2.1 | 8.04 (LTS) | 8.10 | 9.04 | 9.10 | 10.04 (LTS) | 10.10

Linux - Netbooks



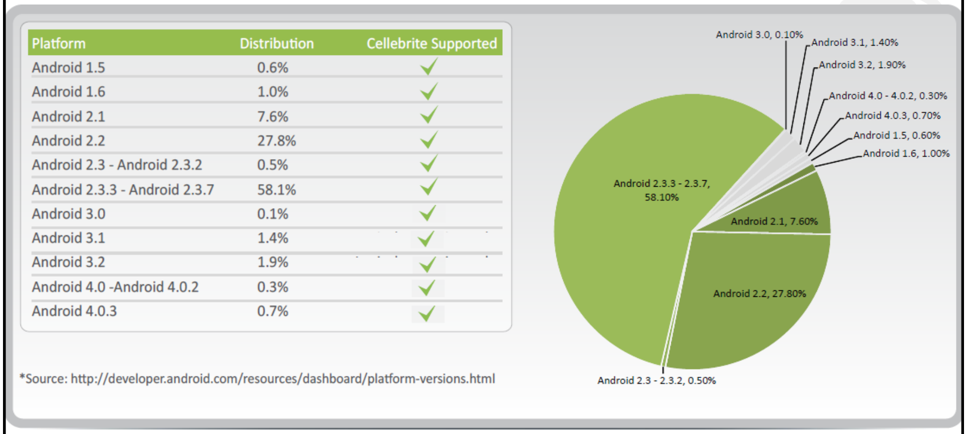
Apple iOS Versions

GSM					
1.0.0	1.0.1	1.02	1.1.1	1.1.2	1.1.3
1.1.4	2.0.0	2.0.1	2.0.2	2.1.0	2.2.0
2.2.1	3.0.0	3.0.1	3.1.0	3.1.2	3.1.3
4.0.0	4.0.1	4.0.2	4.1.0	4.2.1	4.3.0
4.3.1	4.3.2	4.3.3	4.3.4	4.3.5	
CDMA					
4.2.5	4.2.6	4.2.7	4.2.8	4.2.9	4.2.10
GSM and CDMA					
5.0	5.0.1	5.1			

Confidential , not for distribution © Cellebrite

mobile data secured

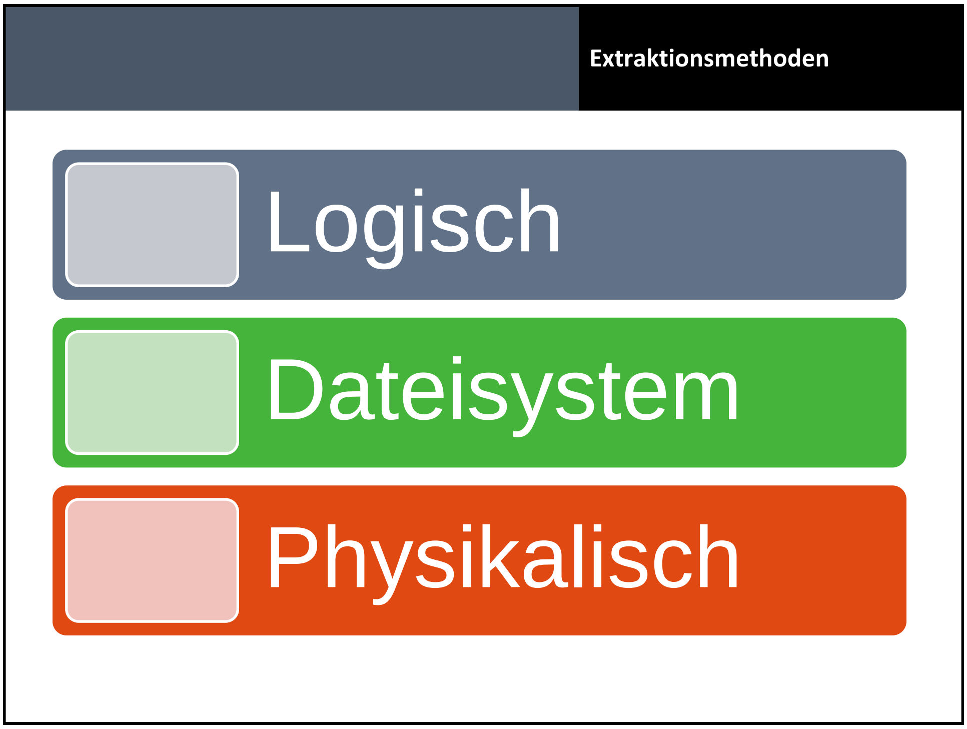
Android Versions



Platform	Distribution	Cellebrite Supported
Android 1.5	0.6%	✓
Android 1.6	1.0%	✓
Android 2.1	7.6%	✓
Android 2.2	27.8%	✓
Android 2.3 - Android 2.3.2	0.5%	✓
Android 2.3.3 - Android 2.3.7	58.1%	✓
Android 3.0	0.1%	✓
Android 3.1	1.4%	✓
Android 3.2	1.9%	✓
Android 4.0 -Android 4.0.2	0.3%	✓
Android 4.0.3	0.7%	✓

*Source: http://developer.android.com/resources/dashboard/platform-versions.html

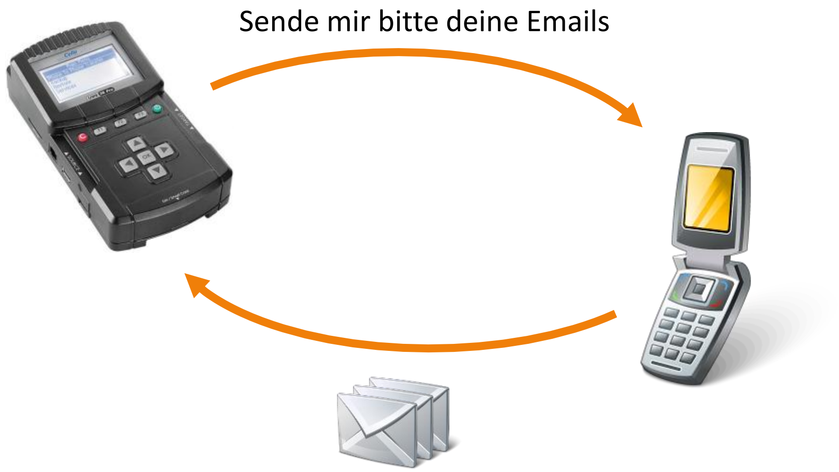
#4 – Daten Extraktion

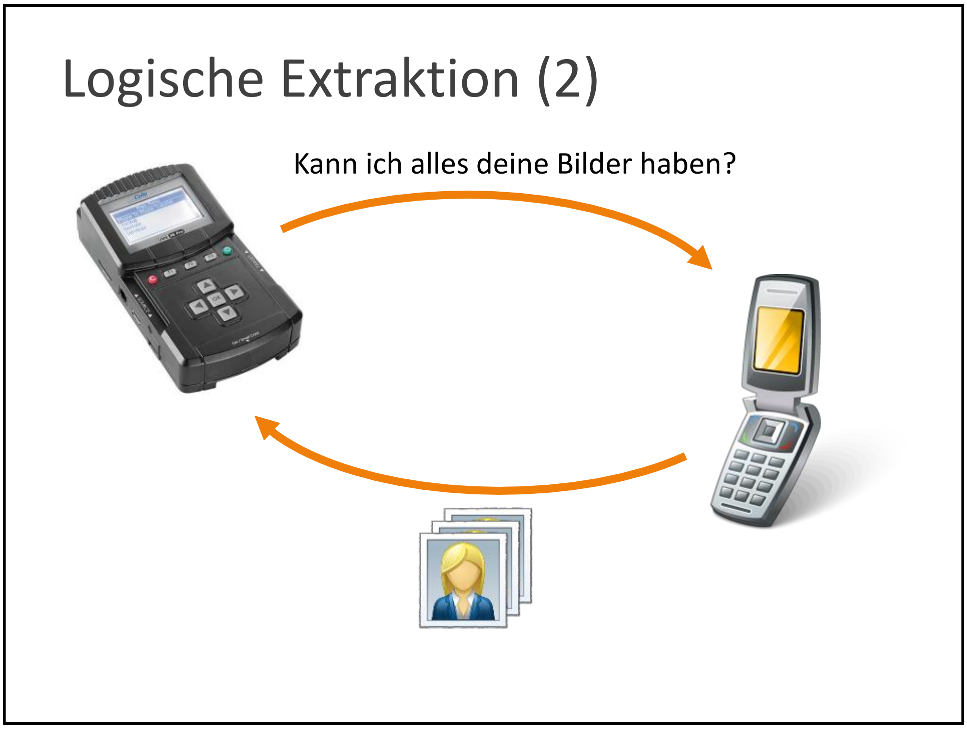


Extraktionsmethoden

- Logisch
- Dateisystem
- Physikalisch

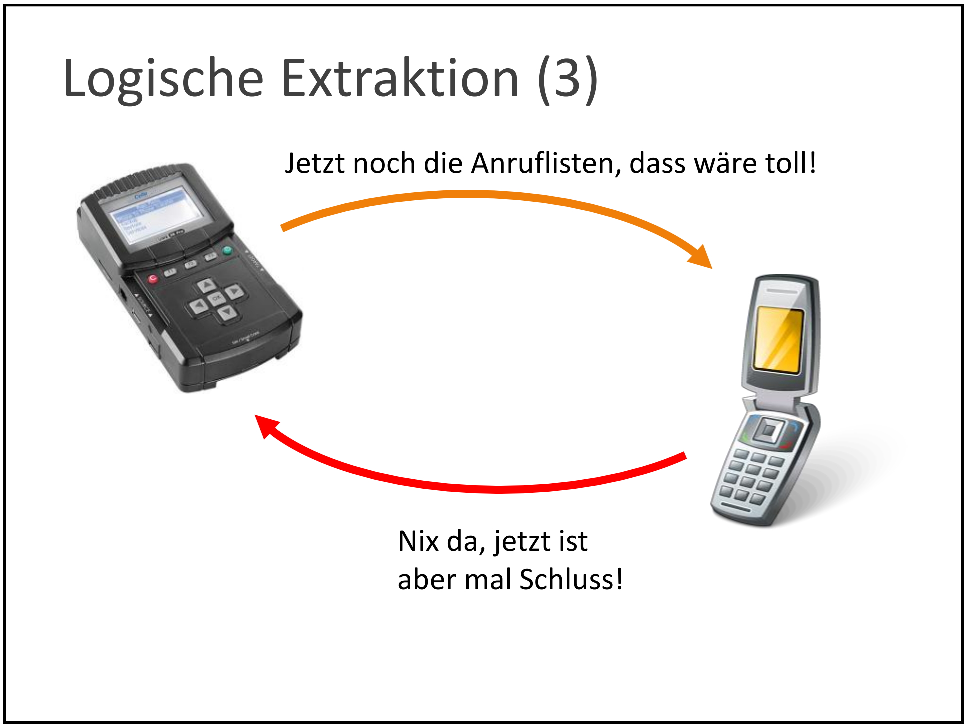
Logische Extraktion





Logische Extraktion (2)

Kann ich alles deine Bilder haben?

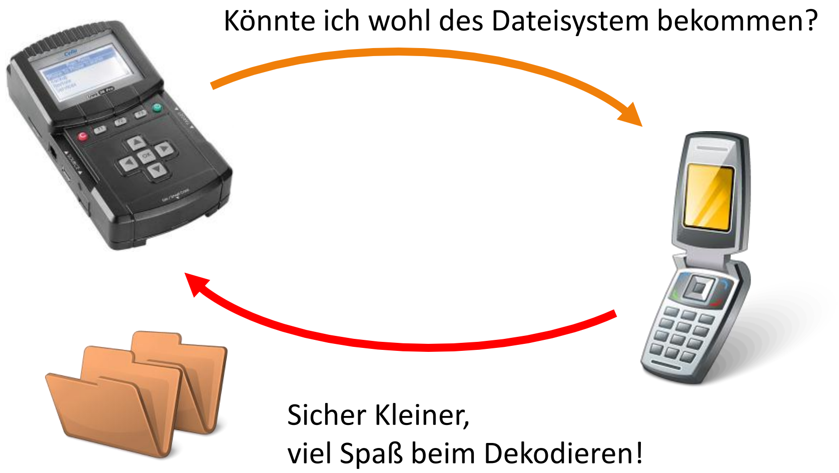


Logische Extraktion (3)

Jetzt noch die Anruflisten, dass wäre toll!

Nix da, jetzt ist
aber mal Schluss!

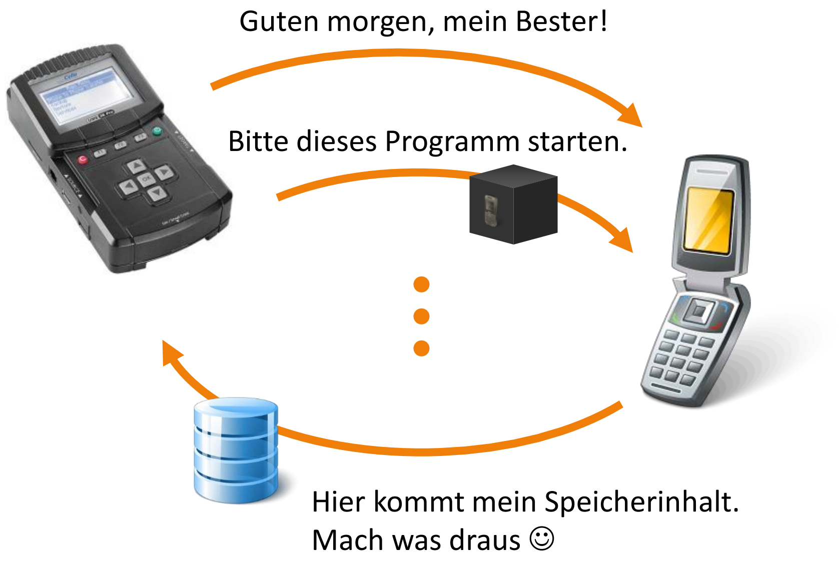
Dateisystem-Extraktion



Könnte ich wohl des Dateisystem bekommen?

Sicher Kleiner,
viel Spaß beim Dekodieren!

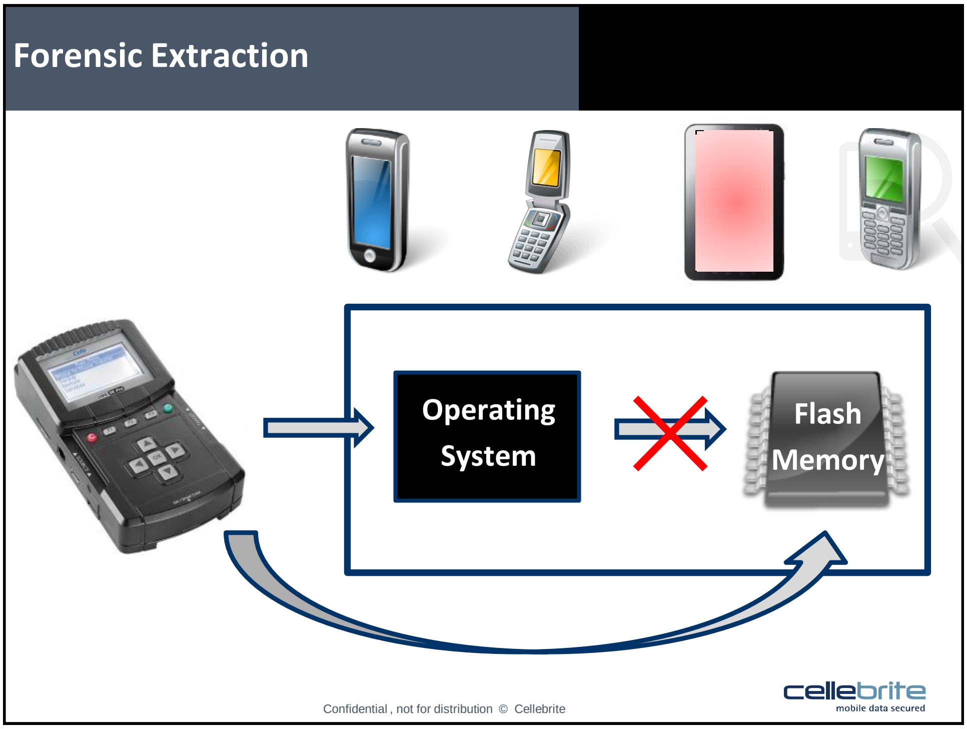
Physikalische Extraktion



Guten morgen, mein Bester!

Bitte dieses Programm starten.

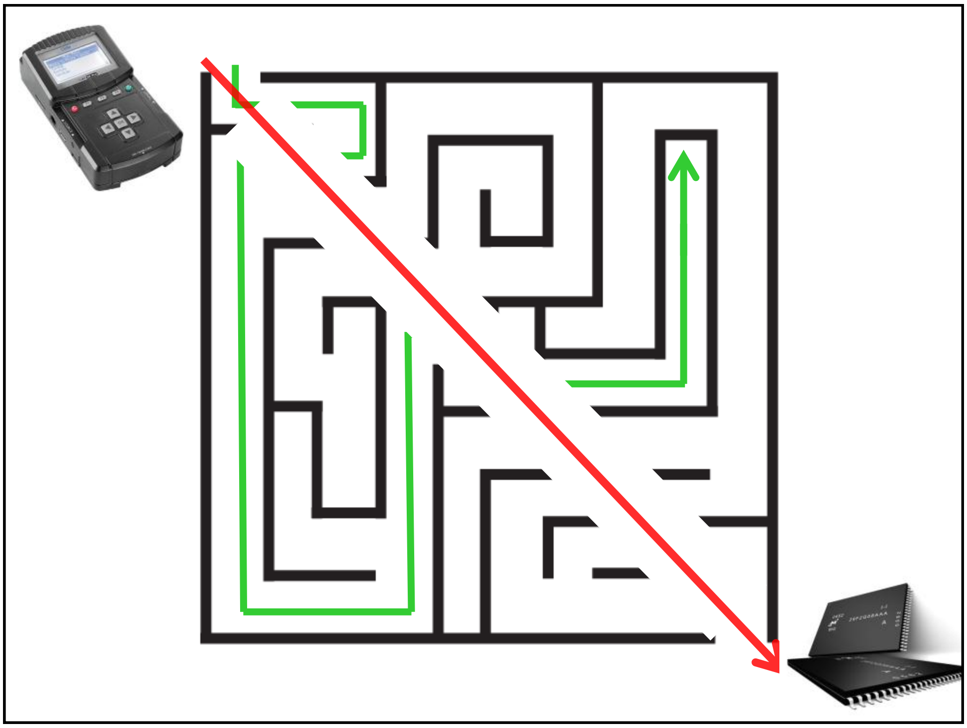
Hier kommt mein Speicherinhalt.
Mach was draus ☺



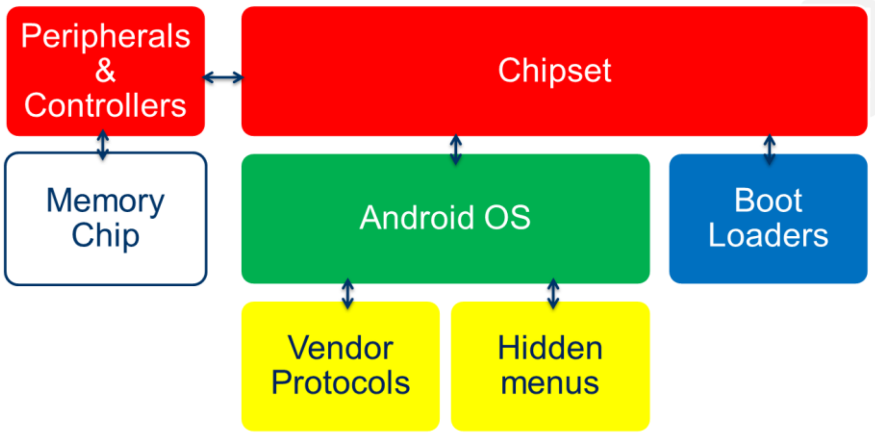
Forensic Extraction

Operating System

Flash Memory



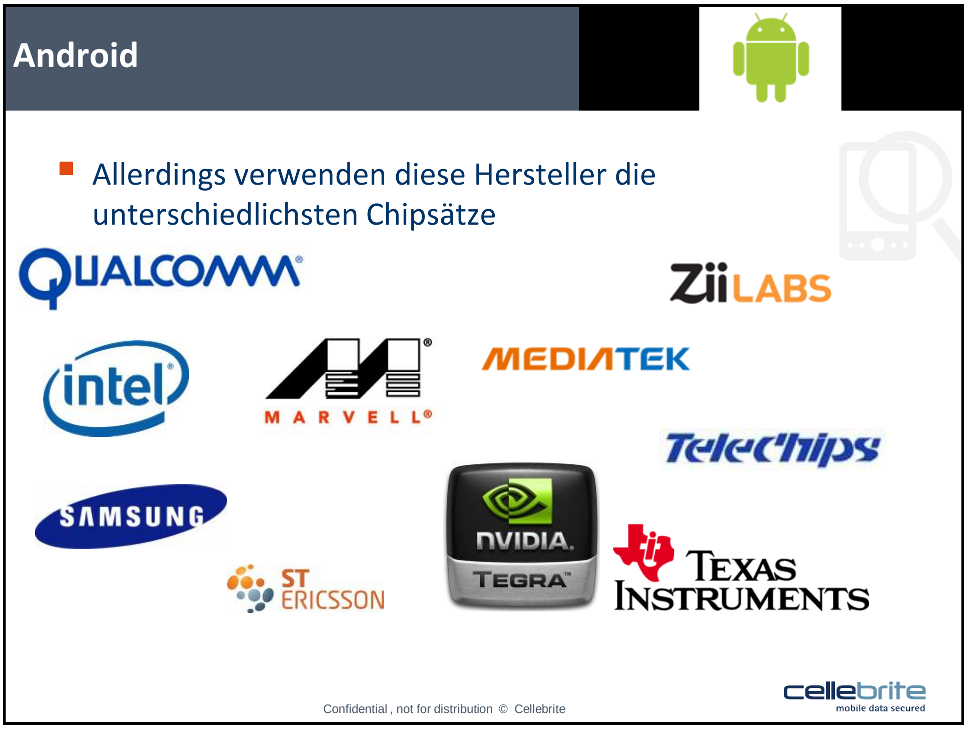
Architektur



Android

- Hersteller

Sony Ericsson
SAMSUNG
LG
hTC
acer
ASUS
ALCATEL
mobile phones
HUAWEI
SANYO
DELL
CREATIVE
MOTOROLA
ARCHOS
GARMIN
ZTE中兴
lenovo
TOSHIBA
ViewSonic
PANTECH



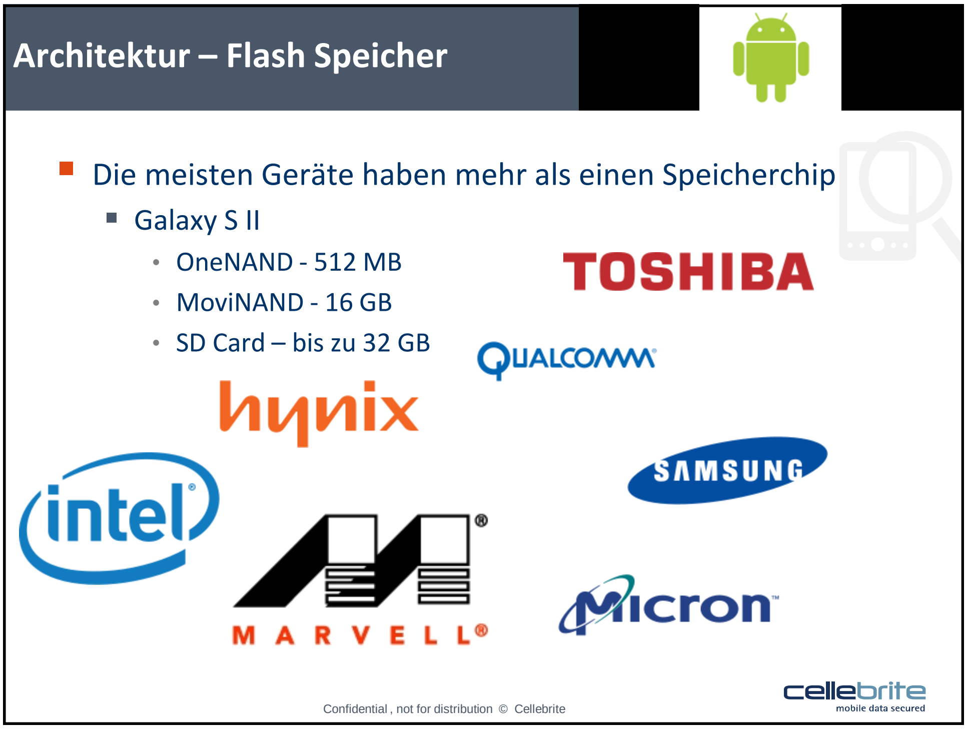
Android

- Allerdings verwenden diese Hersteller die unterschiedlichsten Chipsätze

QUALCOMM
ZiiLABS
intel
MARVELL
MEDIATEK
Telechips
SAMSUNG
NVIDIA TEGRA
ST ERICSSON
TEXAS INSTRUMENTS

Confidential , not for distribution © Cellebrite

cellebrite mobile data secured



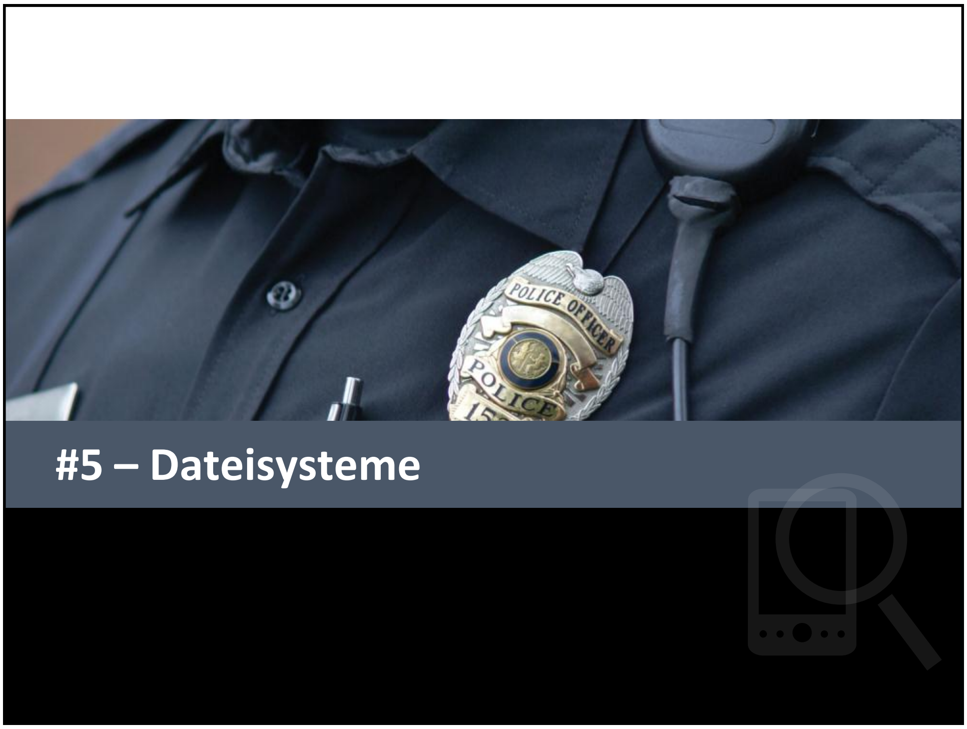
Architektur – Flash Speicher

- Die meisten Geräte haben mehr als einen Speicherchip
  - Galaxy S II
    - OneNAND - 512 MB
    - MoviNAND - 16 GB
    - SD Card – bis zu 32 GB

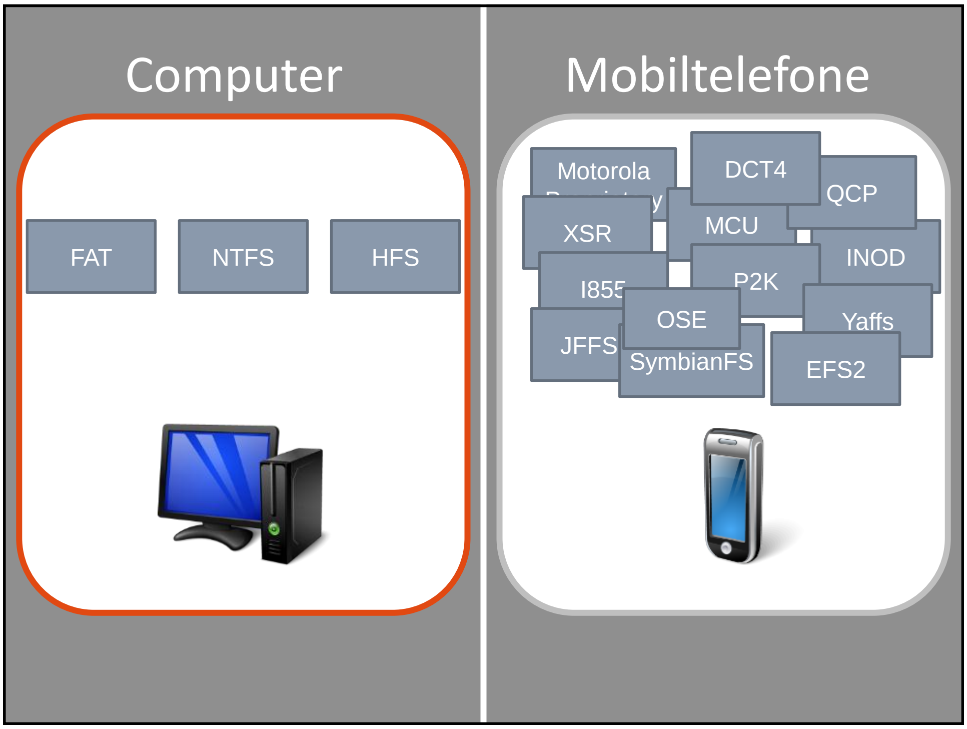
TOSHIBA
QUALCOMM
hynix
SAMSUNG
intel
MARVELL
Micron

Confidential , not for distribution © Cellebrite

cellebrite mobile data secured



#5 – Dateisysteme



Computer

FAT

NTFS

HFS

Mobiltelefone

Motorola

DCT4

QCP

XSR

MCU

INOD

I855

P2K

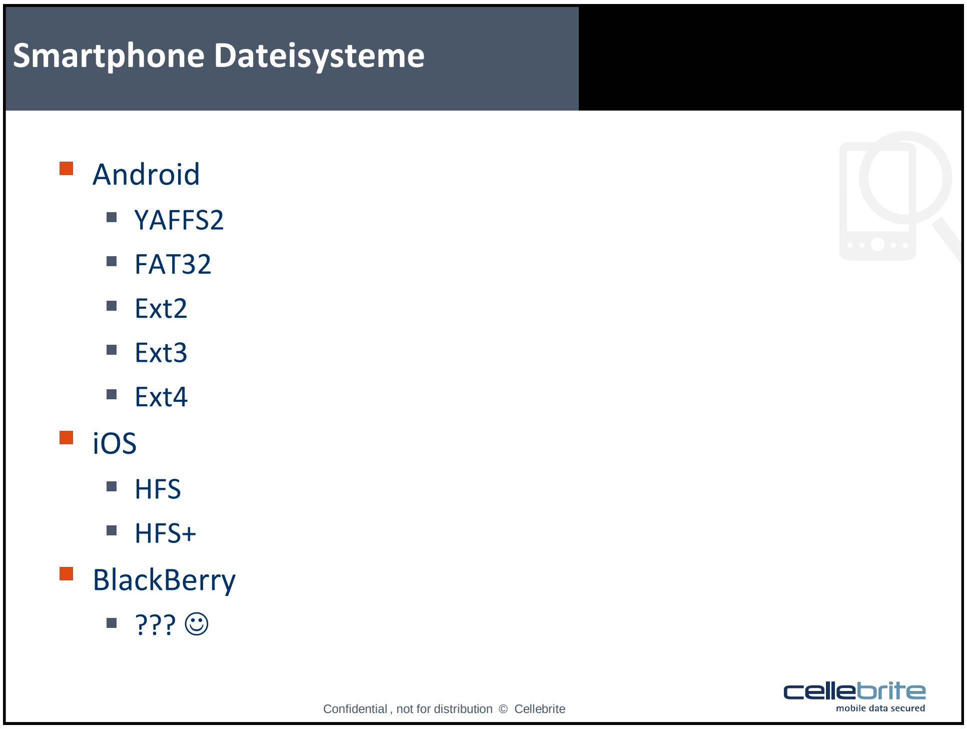
OSE

Yaffs

JFFS

SymbianFS

EFS2

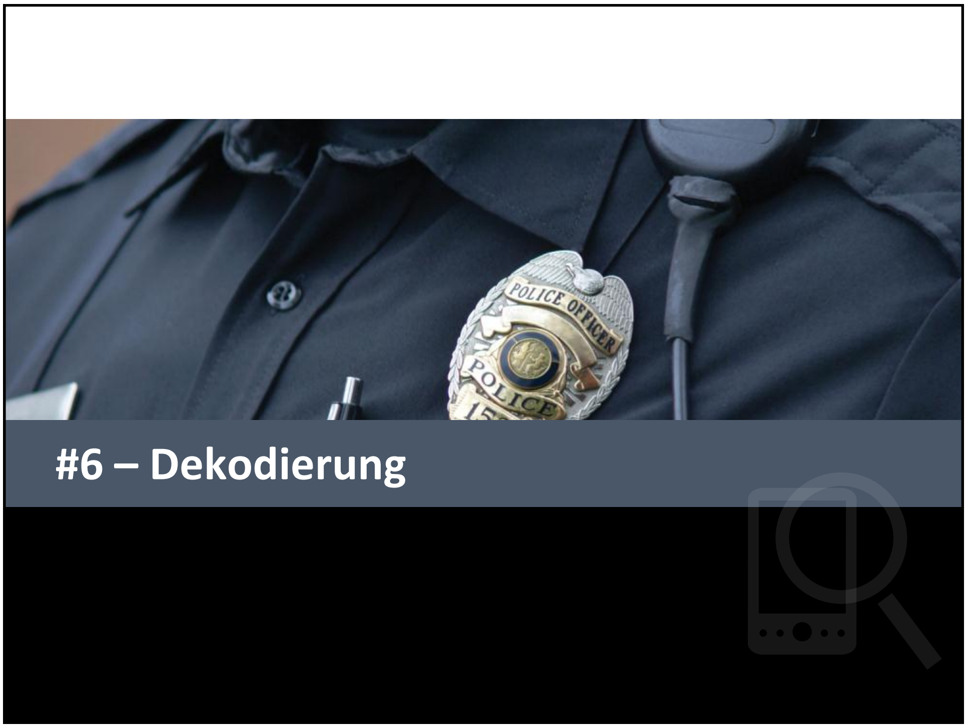


Smartphone Dateisysteme

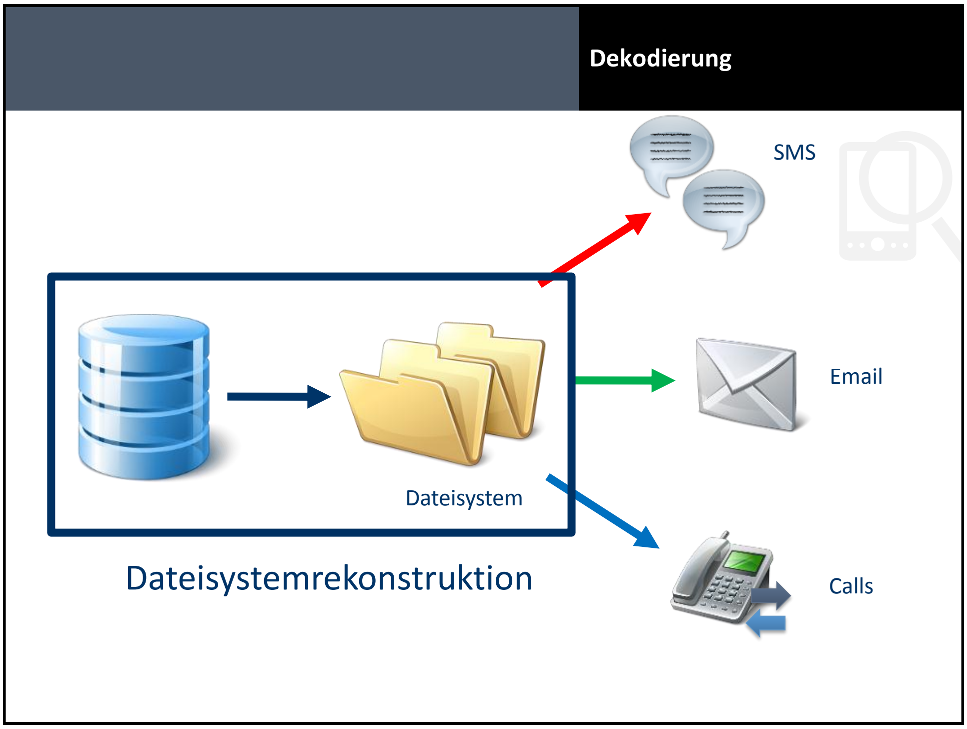
- Android
  - YAFFS2
  - FAT32
  - Ext2
  - Ext3
  - Ext4
- iOS
  - HFS
  - HFS+
- BlackBerry
  - ??? ☺

Confidential , not for distribution © Cellebrite

cellebrite
mobile data secured



#6 – Dekodierung



Dekodierung

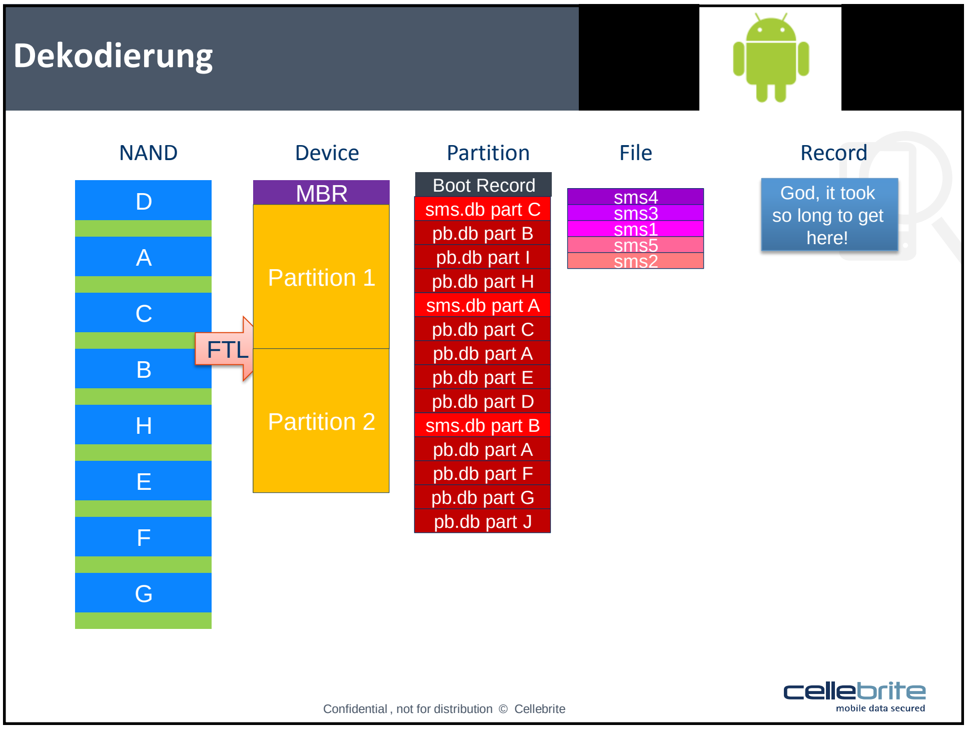
SMS

Email

Calls

Dateisystem

Dateisystemrekonstruktion



Dekodierung

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

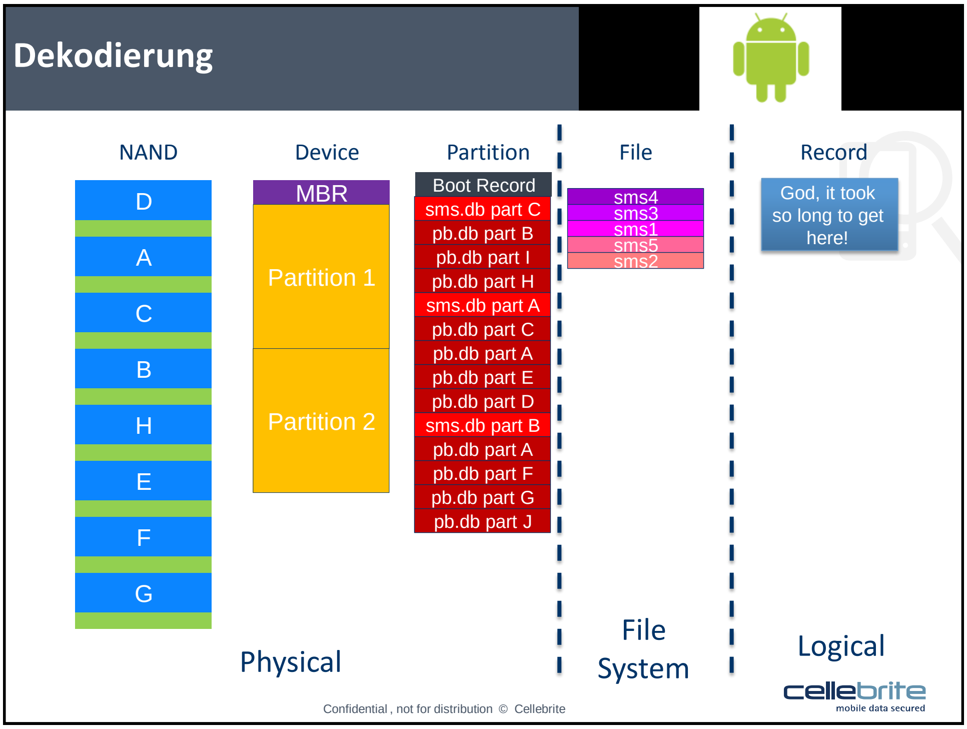
sms4
sms3
sms1
sms5
sms2

Record

God, it took so long to get here!

Confidential , not for distribution © Cellebrite

cellebrite mobile data secured



Dekodierung

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

File System

Logical

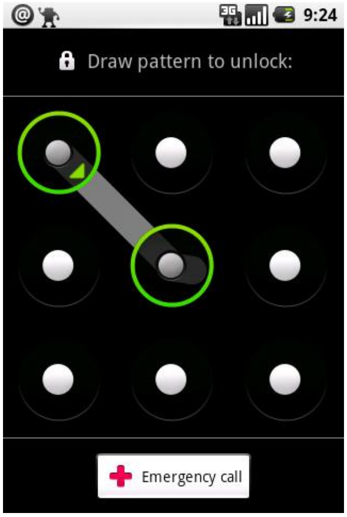
Confidential , not for distribution © Cellebrite

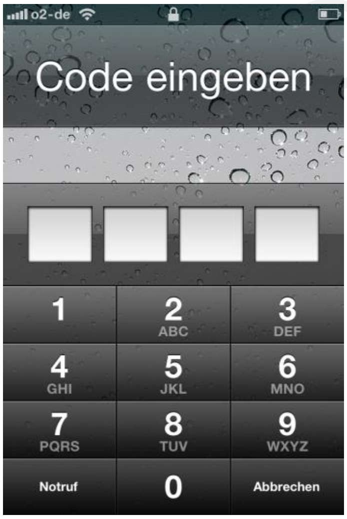
cellebrite mobile data secured

cellebrite
mobile data secured

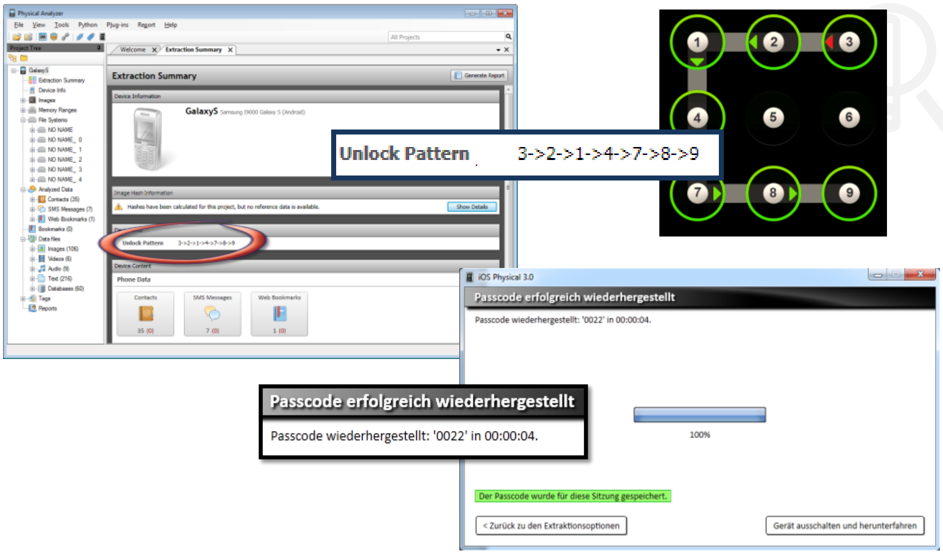
#7 – Gerätesperre

Sperrcodes





Wiederherstellung



Extraction Summary

GalaxyS Samsung I9000 Galaxy S (Android)

Hashes have been calculated for this project, but no reference data is available.

Unlock Pattern 3->2->1->4->7->8->9

Unlock Pattern 3->2->1->4->7->8->9

Passcode erfolgreich wiederhergestellt

Passcode wiederhergestellt: '0022' in 00:00:04.

Der Passcode wurde für diese Sitzung gespeichert.

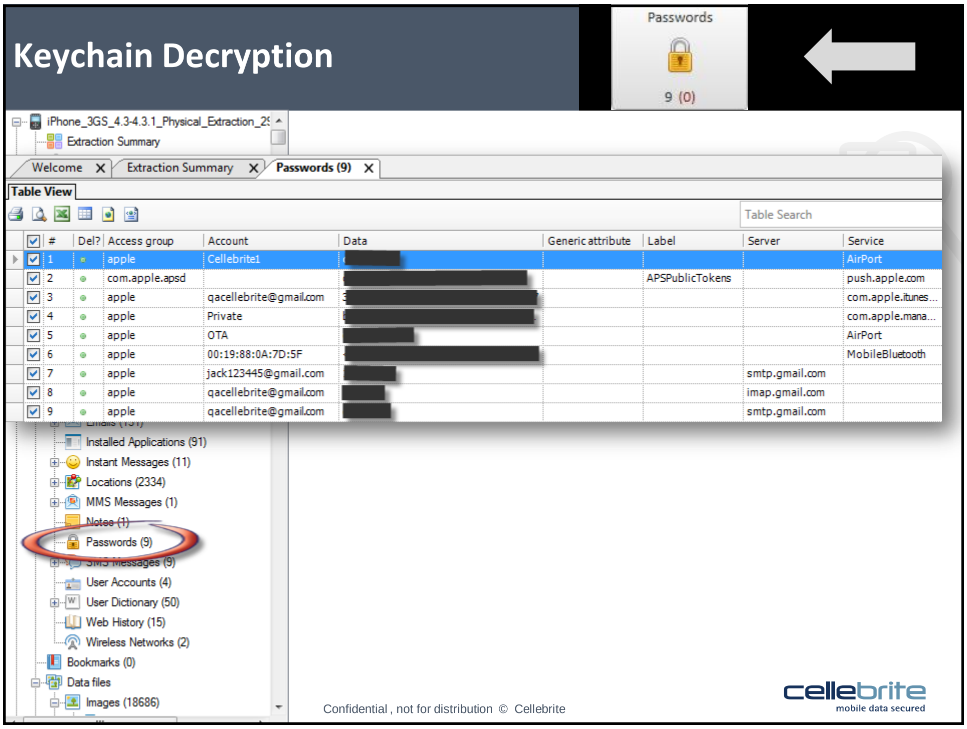
Passcode erfolgreich wiederhergestellt

Passcode wiederhergestellt: '0022' in 00:00:04.

cellebrite
mobile data secured

#8 – Verschlüsselung

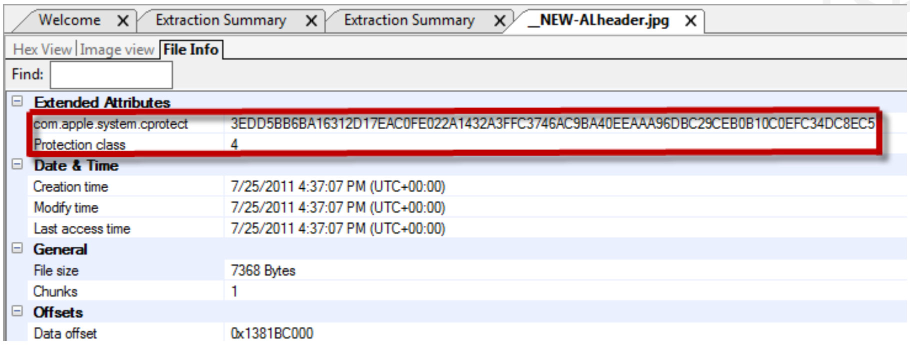
Keychain Decryption



☑	#	Del?	Access group	Account	Data	Generic attribute	Label	Server	Service
☑	1	●	apple	Cellebrite1	[redacted]				AirPort
☑	2	●	com.apple.apsd		[redacted]		APSPublicTokens		push.apple.com
☑	3	●	apple	qacellebrite@gmail.com	[redacted]				com.apple.itunes...
☑	4	●	apple	Private	[redacted]				com.apple.mana...
☑	5	●	apple	OTA	[redacted]				AirPort
☑	6	●	apple	00:19:88:0A:7D:5F	[redacted]				MobileBluetooth
☑	7	●	apple	jack123445@gmail.com	[redacted]			smtp.gmail.com	
☑	8	●	apple	qacellebrite@gmail.com	[redacted]			imap.gmail.com	
☑	9	●	apple	qacellebrite@gmail.com	[redacted]			smtp.gmail.com	

cellebrite
mobile data secured

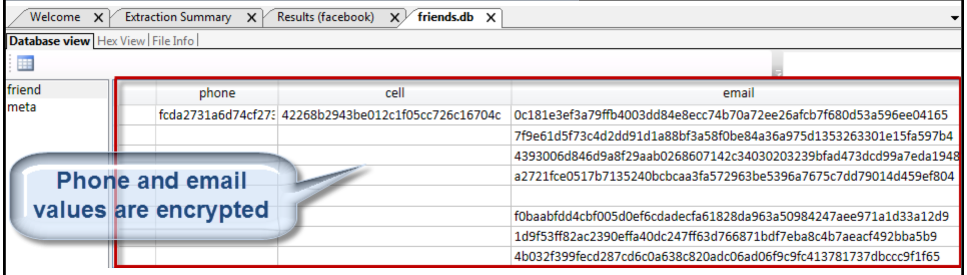
Decryption of iOS File System



Extended Attributes	
com.apple.system.cprotect	3EDD5BB6BA16312D17EAC0FE022A1432A3FFC3746AC9BA40EEAAA96DBC29CEB0B10C0EFC34DC8EC5
Protection class	4
Date & Time	
Creation time	7/25/2011 4:37:07 PM (UTC+00:00)
Modify time	7/25/2011 4:37:07 PM (UTC+00:00)
Last access time	7/25/2011 4:37:07 PM (UTC+00:00)
General	
File size	7368 Bytes
Chunks	1
Offsets	
Data offset	0x1381BC000

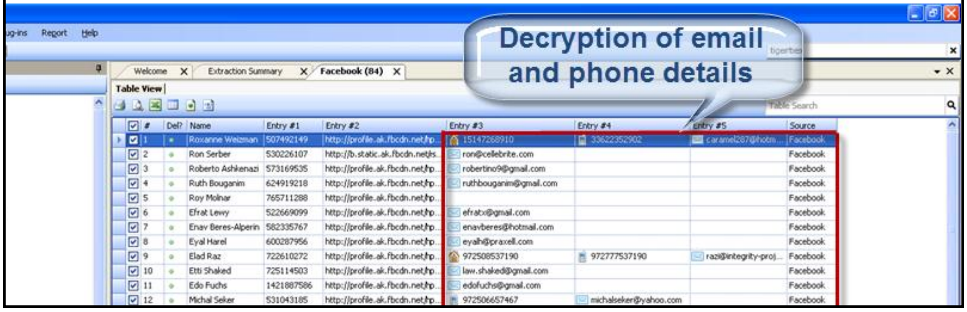
cellebrite
mobile data secured

Facebook Decryption



phone	cell	email
fcda2731a6d74cf27:	42268b2943be012c1f05cc726c16704c	0c181e3ef3a79ffb4003dd84e8ecc74b70a72ee26afcb7f680d53a596ee04165
		7f9e61d5f73c4d2dd91d1a88bf3a58f0be84a36a975d1353263301e15fa597b4
		4393006d846d9a8f29aab0268607142c34030203239bfad473dcd99a7eda1948
		a2721fce0517b7135240bcbcaa3fa572963be5396a7675c7dd79014d459ef804
		f0baabfdd4cbf005d0ef6cdadecfa61828da963a50984247aee971a1d33a12d9
		1d9f53ff82ac2390effa40dc247ff63d766871bdf7eba8c4b7aeacf492bba5b9
		4b032f399fecd287cd6c0a638c820adc06ad06f9c9fc413781737dbccc9f1f65

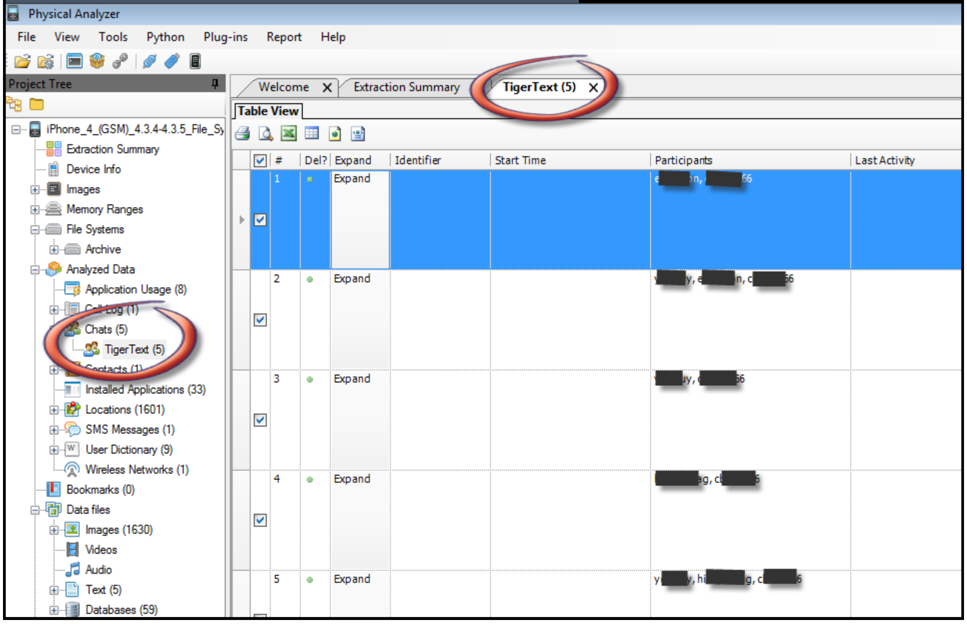
Phone and email values are encrypted



☑	#	Del?	Name	Entry #1	Entry #2	Entry #3	Entry #4	Entry #5	Source
☑	1	●	Roxanne Weizman	507492149	http://profile.ak.fbcdn.net/hp...	15147268910	33622352902	caramel287@hotm...	Facebook
☑	2	●	Ron Serber	530226107	http://b.static.ak.fbcdn.net/rs...	ron@cellebrite.com			Facebook
☑	3	●	Roberto Ashkenazi	573169535	http://profile.ak.fbcdn.net/hp...	robertino9@gmail.com			Facebook
☑	4	●	Ruth Bouganim	624919218	http://profile.ak.fbcdn.net/hp...	ruthbouganim@gmail.com			Facebook
☑	5	●	Roy Molnar	765711288	http://profile.ak.fbcdn.net/hp...				Facebook
☑	6	●	Efrat Lewy	522669099	http://profile.ak.fbcdn.net/hp...	efratx@gmail.com			Facebook
☑	7	●	Enav Beres-Alperin	582335767	http://profile.ak.fbcdn.net/hp...	enavberes@hotmail.com			Facebook
☑	8	●	Eyal Harel	600287956	http://profile.ak.fbcdn.net/hp...	eyalh@praxell.com			Facebook
☑	9	●	Elad Raz	722610272	http://profile.ak.fbcdn.net/hp...	972508537190	972777537190	razi@integrity-proj...	Facebook
☑	10	●	Etti Shaked	725114503	http://profile.ak.fbcdn.net/hp...	law.shaked@gmail.com			Facebook
☑	11	●	Edo Fuchs	1421887586	http://profile.ak.fbcdn.net/hp...	edofuchs@gmail.com			Facebook
☑	12	●	Michal Seker	531043185	http://profile.ak.fbcdn.net/hp...	972506657467	michalseker@yahoo.com		Facebook

Decryption of email and phone details

Tiger Text Decryption

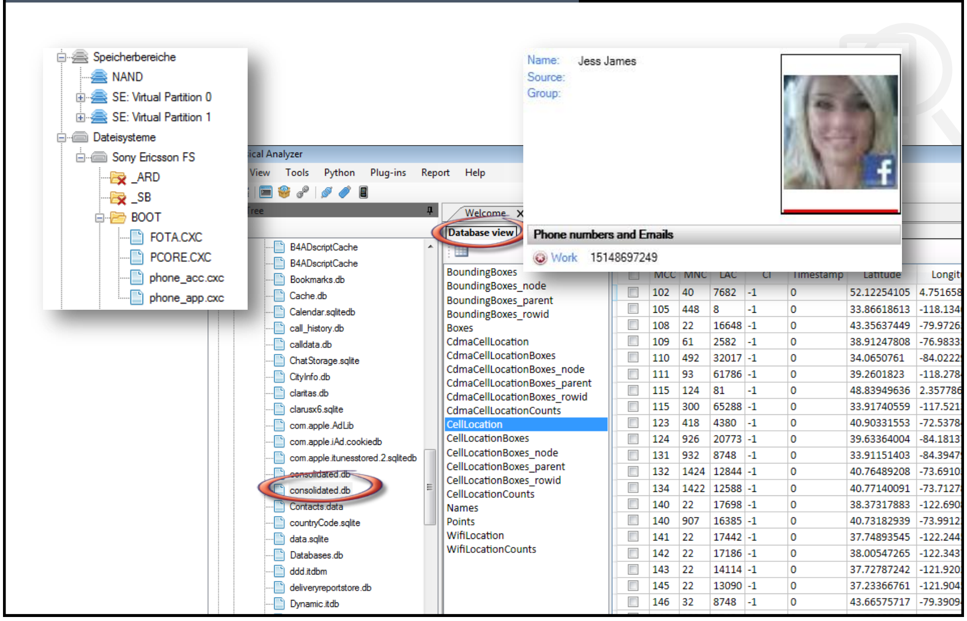


☑	#	Del?	Expand	Identifier	Start Time	Participants	Last Activity
☑	1	●	Expand			[redacted]	
☑	2	●	Expand			[redacted]	
☑	3	●	Expand			[redacted]	
☑	4	●	Expand			[redacted]	
	5	●	Expand			[redacted]	

cellebrite
mobile data secured

#9 – Gelöschte Daten

Gelöschte Daten



- Speicherbereiche
  - NAND
  - SE: Virtual Partition 0
  - SE: Virtual Partition 1
- Dateisysteme
  - Sony Ericsson FS
    - _ARD
    - _SB
    - BOOT
      - FOTA.CXC
      - PCORE.CXC
      - phone_acc.cxc
      - phone_app.cxc

B4ADscriptCache
B4ADscriptCache
Bookmarks.db
Cache.db
Calendar.sqlitedb
call_history.db
calldata.db
ChatStorage.sqlite
CityInfo.db
claritas.db
clarusx6.sqlite
com.apple.AdLib
com.apple.iAd.cookiedb
com.apple.itunesstored.2.sqlitedb
consolidated.db
consolidated.db
Contacts.data
countryCode.sqlite
data.sqlite
Databases.db
ddd.itdbm
deliveryreportstore.db
Dynamic.itdb

BoundingBoxes
BoundingBoxes_node
BoundingBoxes_parent
BoundingBoxes_rowid
Boxes
CdmaCellLocation
CdmaCellLocationBoxes
CdmaCellLocationBoxes_node
CdmaCellLocationBoxes_parent
CdmaCellLocationBoxes_rowid
CdmaCellLocationCounts
CellLocation
CellLocationBoxes
CellLocationBoxes_node
CellLocationBoxes_parent
CellLocationBoxes_rowid
CellLocationCounts
Names
Points
WifiLocation
WifiLocationCounts

Name: Jess James
Source:
Group:

Phone numbers and Emails

Work 15148697249

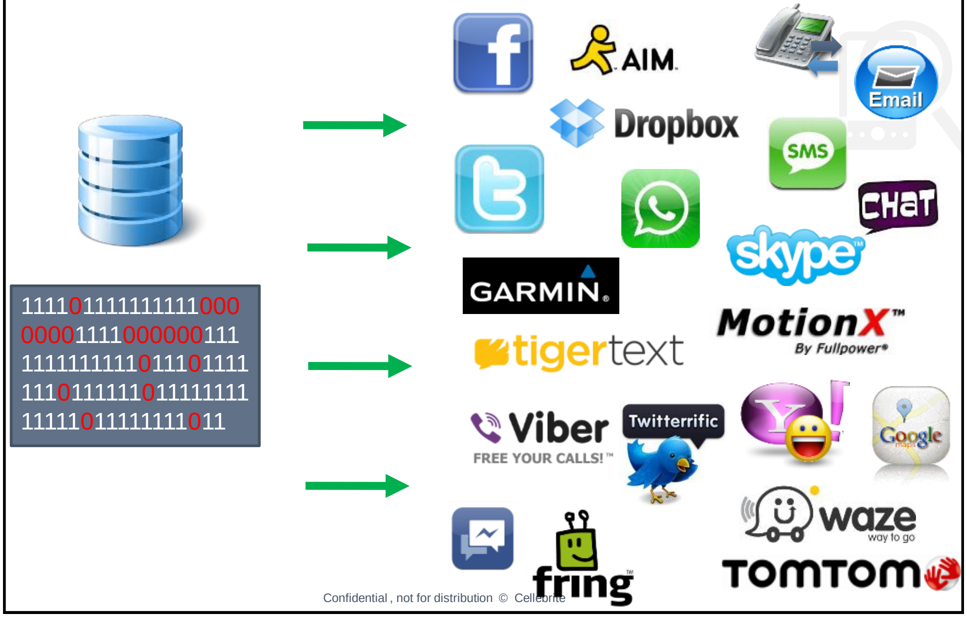
□	MCC	MNC	LAC	CI	Timestamp	Latitude	Longit
□	102	40	7682	-1	0	52.12254105	4.751658
□	105	448	8	-1	0	33.86618613	-118.134
□	108	22	16648	-1	0	43.35637449	-79.9726
□	109	61	2582	-1	0	38.91247808	-76.9833
□	110	492	32017	-1	0	34.0650761	-84.0222
□	111	93	61786	-1	0	39.2601823	-118.278
□	115	124	81	-1	0	48.83949636	2.357786
□	115	300	65288	-1	0	33.91740559	-117.521
□	123	418	4380	-1	0	40.90331553	-72.5378
□	124	926	20773	-1	0	39.63364004	-84.1813
□	131	932	8748	-1	0	33.91151403	-84.3947
□	132	1424	12844	-1	0	40.76489208	-73.6910
□	134	1422	12588	-1	0	40.77140091	-73.7127
□	140	22	17698	-1	0	38.37317883	-122.690
□	140	907	16385	-1	0	40.73182939	-73.9912
□	141	22	17442	-1	0	37.74893545	-122.244
□	142	22	17186	-1	0	38.00547265	-122.343
□	143	22	14114	-1	0	37.72787242	-121.920
□	145	22	13090	-1	0	37.23366761	-121.904
□	146	32	8748	-1	0	43.66575717	-79.3909

cellebrite
mobile data secured

#9 – App‘s, App‘s, App‘s…

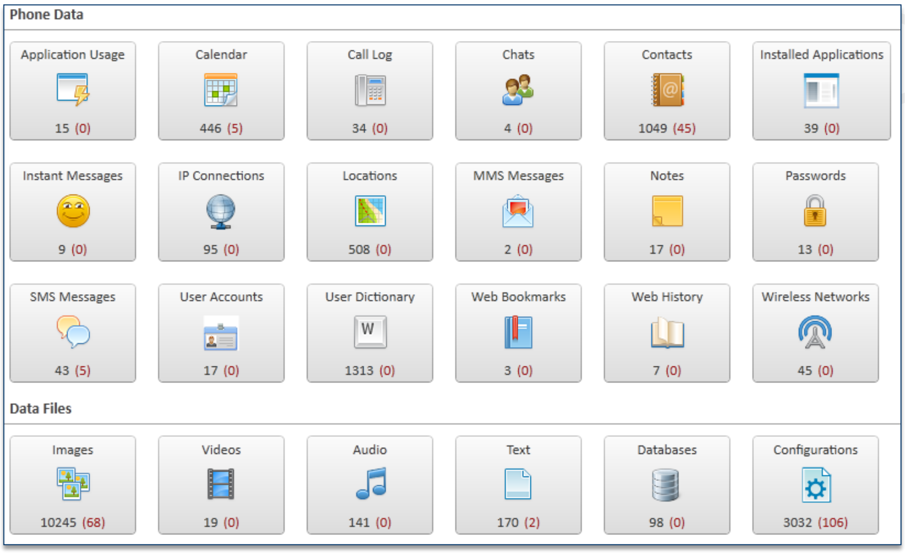
Decoding

DECODE



11110111111111111000
00001111000000111
1111111111011101111
1110111111011111111
1111101111111111011

Decoding



Phone Data

Application Usage 15 (0)	Calendar 446 (5)	Call Log 34 (0)	Chats 4 (0)	Contacts 1049 (45)	Installed Applications 39 (0)
Instant Messages 9 (0)	IP Connections 95 (0)	Locations 508 (0)	MMS Messages 2 (0)	Notes 17 (0)	Passwords 13 (0)
SMS Messages 43 (5)	User Accounts 17 (0)	User Dictionary 1313 (0)	Web Bookmarks 3 (0)	Web History 7 (0)	Wireless Networks 45 (0)

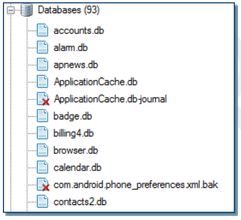
Data Files

Images 10245 (68)	Videos 19 (0)	Audio 141 (0)	Text 170 (2)	Databases 98 (0)	Configurations 3032 (106)

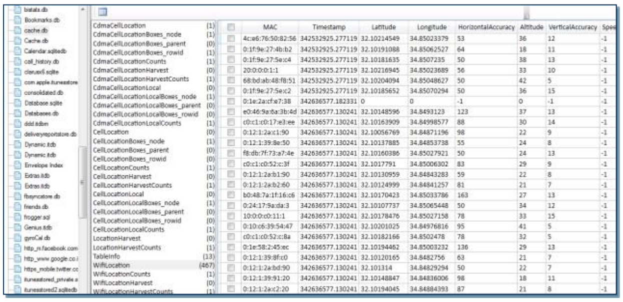
cellebrite
mobile data secured

SQLite Database

- Great sources for information
- Available and deleted databases
- Deleted entries from a database
- Ability to view tables and content
- Search



Databases (93)
- accounts.db
- alarm.db
- apnews.db
- ApplicationCache.db
- ApplicationCache.db-journal
- badge.db
- billing4.db
- browser.db
- calendar.db
- com.android.phone_preferences.xml.bak
- contacts2.db



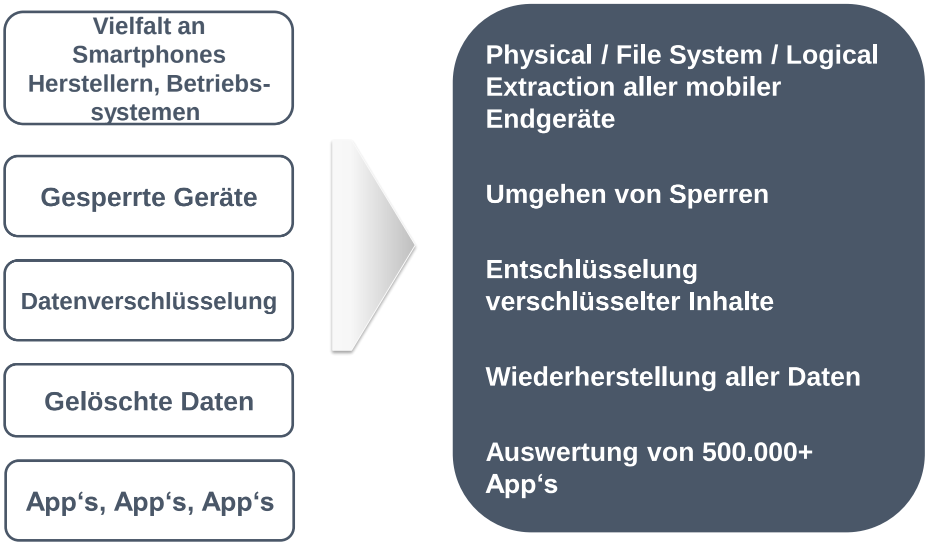
- bistats.db
- Bookmarks.db
- cache.db
- Cache.db
- Calendar.sqlitedb
- call_history.db
- clarus6.sqlite
- com.apple.itunesstore
- consolidated.db
- Database.sqlite
- Databases.db
- ddd.itdbm
- deliveryreportstore.db
- Dynamic.itdb
- Dynamic.itdb
- Envelope Index
- Extras.itdb
- Extras.itdb
- fbsyncstore.db
- friends.db
- frogger.sql
- Genius.itdb
- gyroCal.db
- http_m.facebook.com
- http_www.google.co.i
- https_mobile.twitter.cc
- itunesstored_private.s
- itunesstored2.sqlitedb

CdmaCellLocation	(1)
CdmaCellLocationBoxes_node	(1)
CdmaCellLocationBoxes_parent	(0)
CdmaCellLocationBoxes_rowid	(1)
CdmaCellLocationCounts	(1)
CdmaCellLocationHarvest	(0)
CdmaCellLocationHarvestCounts	(1)
CdmaCellLocationLocal	(0)
CdmaCellLocationLocalBoxes_node	(1)
CdmaCellLocationLocalBoxes_parent	(0)
CdmaCellLocationLocalBoxes_rowid	(0)
CdmaCellLocationLocalCounts	(1)
CellLocation	(0)
CellLocationBoxes_node	(1)
CellLocationBoxes_parent	(0)
CellLocationBoxes_rowid	(0)
CellLocationCounts	(1)
CellLocationHarvest	(0)
CellLocationHarvestCounts	(1)
CellLocationLocal	(0)
CellLocationLocalBoxes_node	(1)
CellLocationLocalBoxes_parent	(0)
CellLocationLocalBoxes_rowid	(0)
CellLocationLocalCounts	(1)
LocationHarvest	(0)
LocationHarvestCounts	(1)
TableInfo	(13)
WifiLocation	(467)
WifiLocationCounts	(1)
WifiLocationHarvest	(0)
WifiLocationHarvestCounts	(1)

□	MAC	Timestamp	Latitude	Longitude	HorizontalAccuracy	Altitude	VerticalAccuracy	Spe
□	4c:e6:76:50:82:56	342532925.277119	32.10214549	34.85023379	53	36	12	-1
□	0:1f:9e:27:4b:b2	342532925.277119	32.10191088	34.85062527	64	18	11	-1
□	0:1f:9e:27:5e:c4	342532925.277119	32.10181635	34.8507235	50	38	13	-1
□	20:0:0:0:1:1	342532925.277119	32.10216945	34.85023689	56	33	10	-1
□	68:bd:ab:48:f8:51	342532925.277119	32.10204094	34.85048627	50	42	5	-1
□	0:1f:9e:27:5e:c2	342532925.277119	32.10185652	34.85070294	50	36	15	-1
□	0:1e:2a:cf:e7:38	342636577.182331	0	0	-1	0	-1	-1
□	e0:46:9a:6a:3b:4d	342636577.130241	32.10148596	34.8493123	123	37	13	-1
□	c0:c1:c0:17:e3:ee	342636577.130241	32.10163909	34.84998577	88	30	14	-1
□	0:12:1:2a:c1:90	342636577.130241	32.10056769	34.84871196	98	22	9	-1
□	0:12:1:39:8e:50	342636577.130241	32.10137885	34.84853738	55	24	8	-1
□	f8:db:7f:73:a7:4e	342636577.130241	32.10160386	34.85027921	50	24	13	-1
□	c0:c1:c0:52:c:3f	342636577.130241	32.1017791	34.85006302	83	29	9	-1
□	0:12:1:2a:b1:90	342636577.130241	32.10130959	34.84843283	59	22	8	-1
□	0:12:1:2a:b2:60	342636577.130241	32.10124999	34.84841257	81	21	7	-1
□	b0:48:7a:1f:16:c6	342636577.130241	32.10170423	34.85033786	163	27	13	-1
□	0:24:17:9a:da:3	342636577.130241	32.10107737	34.85065448	50	34	12	-1
□	10:0:0:c0:11:1	342636577.130241	32.10178476	34.85027158	78	33	15	-1
□	0:10:c6:39:54:47	342636577.130241	32.10201025	34.84976816	95	41	5	-1
□	c0:c1:c0:52:c:8a	342636577.130241	32.10182166	34.8502478	78	32	5	-1
□	0:1e:58:2:45:ec	342636577.130241	32.10194462	34.85003232	136	29	13	-1
□	0:12:1:39:8f:c0	342636577.130241	32.10120165	34.8482756	63	21	7	-1
□	0:12:1:2a:bd:90	342636577.130241	32.101314	34.84829294	50	22	7	-1
□	0:12:1:39:91:20	342636577.130241	32.10148847	34.84836006	98	18	11	-1
□	0:12:1:2a:c2:20	342636577.130241	32.10194045	34.84884393	87	21	8	-1

Easily search for additional vital information

Herausforderungen



Vielfalt an Smartphones Herstellern, Betriebs-systemen

Gesperrte Geräte

Datenverschlüsselung

Gelöschte Daten

App‘s, App‘s, App‘s

Physical / File System / Logical Extraction aller mobiler Endgeräte

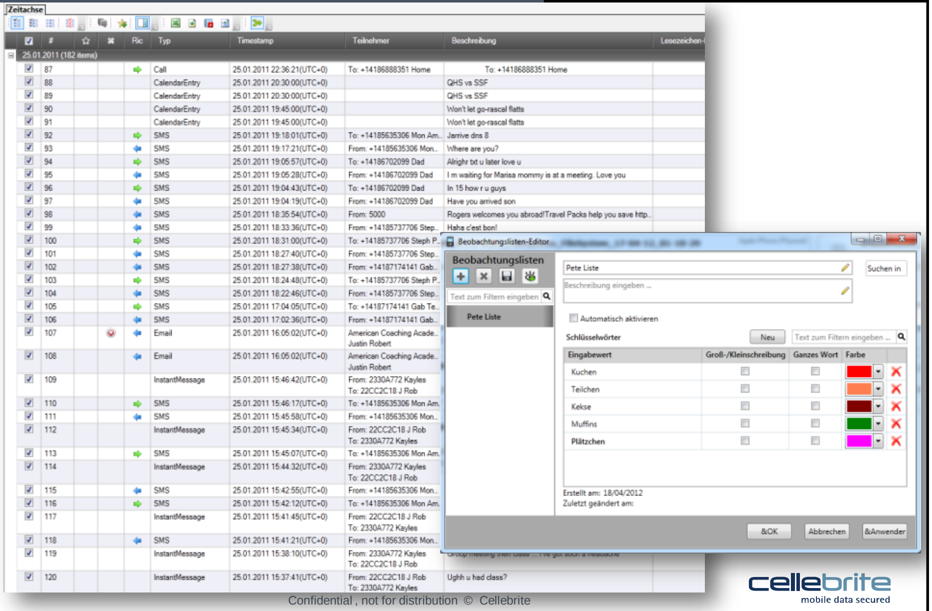
Umgehen von Sperren

Entschlüsselung verschlüsselter Inhalte

Wiederherstellung aller Daten

Auswertung von 500.000+ App‘s

Auswertung



Zeitachse

☑	#	☆	✖	Ric	Typ	Timestamp	Teilnehmer	Beschreibung	Lesezeichen-
25.01.2011 (182 items)									
☑	87			→	Call	25.01.2011 22:36:21(UTC+0)	To: +14186888351 Home	To: +14186888351 Home	
☑	88				CalendarEntry	25.01.2011 20:30:00(UTC+0)		QHS vs SSF	
☑	89				CalendarEntry	25.01.2011 20:30:00(UTC+0)		QHS vs SSF	
☑	90				CalendarEntry	25.01.2011 19:45:00(UTC+0)		Won't let go-rascal flatts	
☑	91				CalendarEntry	25.01.2011 19:45:00(UTC+0)		Won't let go-rascal flatts	
☑	92			→	SMS	25.01.2011 19:18:01(UTC+0)	To: +14185635306 Mon Am...	Jarrive dns 8	
☑	93			←	SMS	25.01.2011 19:17:21(UTC+0)	From: +14185635306 Mon...	Where are you?	
☑	94			→	SMS	25.01.2011 19:06:57(UTC+0)	To: +14186702099 Dad	Alrighr txt u later love u	
☑	95			←	SMS	25.01.2011 19:05:28(UTC+0)	From: +14186702099 Dad	I m waiting for Marisa mommy is at a meeting. Love you	
☑	96			→	SMS	25.01.2011 19:04:43(UTC+0)	To: +14186702099 Dad	In 15 how r u guys	
☑	97			←	SMS	25.01.2011 19:04:19(UTC+0)	From: +14186702099 Dad	Have you arrived son	
☑	98			←	SMS	25.01.2011 18:35:54(UTC+0)	From: 5000	Rogers welcomes you abroad!Travel Packs help you save http...	
☑	99			←	SMS	25.01.2011 18:33:36(UTC+0)	From: +14185737706 Step...	Haha c'est bon!	
☑	100			→	SMS	25.01.2011 18:31:00(UTC+0)	To: +14185737706 Steph P...		
☑	101			←	SMS	25.01.2011 18:27:40(UTC+0)	From: +14185737706 Step...		
☑	102			←	SMS	25.01.2011 18:27:38(UTC+0)	From: +14187174141 Gab...		
☑	103			→	SMS	25.01.2011 18:24:48(UTC+0)	To: +14185737706 Steph P...		
☑	104			←	SMS	25.01.2011 18:22:46(UTC+0)	From: +14185737706 Step...		
☑	105			→	SMS	25.01.2011 17:04:05(UTC+0)	To: +14187174141 Gab Te...		
☑	106			←	SMS	25.01.2011 17:02:36(UTC+0)	From: +14187174141 Gab...		
☑	107		●	←	Email	25.01.2011 16:05:02(UTC+0)	American Coaching Acade... Justin Robert		
☑	108			←	Email	25.01.2011 16:05:02(UTC+0)	American Coaching Acade... Justin Robert		
☑	109				InstantMessage	25.01.2011 15:46:42(UTC+0)	From: 2330A772 Kayles To: 22CC2C18 J Rob		
☑	110			→	SMS	25.01.2011 15:46:17(UTC+0)	To: +14185635306 Mon Am...		
☑	111			←	SMS	25.01.2011 15:45:58(UTC+0)	From: +14185635306 Mon...		
☑	112				InstantMessage	25.01.2011 15:45:34(UTC+0)	From: 22CC2C18 J Rob To: 2330A772 Kayles		
☑	113			→	SMS	25.01.2011 15:45:07(UTC+0)	To: +14185635306 Mon Am...		
☑	114				InstantMessage	25.01.2011 15:44:32(UTC+0)	From: 2330A772 Kayles To: 22CC2C18 J Rob		
☑	115			←	SMS	25.01.2011 15:42:55(UTC+0)	From: +14185635306 Mon...		
☑	116			→	SMS	25.01.2011 15:42:12(UTC+0)	To: +14185635306 Mon Am...		
☑	117				InstantMessage	25.01.2011 15:41:45(UTC+0)	From: 22CC2C18 J Rob To: 2330A772 Kayles		
☑	118			←	SMS	25.01.2011 15:41:21(UTC+0)	From: +14185635306 Mon...		
☑	119				InstantMessage	25.01.2011 15:38:10(UTC+0)	From: 2330A772 Kayles To: 22CC2C18 J Rob	Group meeting then class ... I've got such a headache	
☑	120				InstantMessage	25.01.2011 15:37:41(UTC+0)	From: 22CC2C18 J Rob To: 2330A772 Kayles	Ughh u had class?	

Beobachtungslisten-Editor

Beobachtungslisten

Text zum Filtern eingeben

Pete Liste

Pete Liste

Beschreibung eingeben ...

Suchen in

□ Automatisch aktivieren

Schlüsselwörter

Neu

Text zum Filtern eingeben ...

Eingabewert	Groß-/Kleinschreibung	Ganzes Wort	Farbe	
Kuchen	□	□	🟥	✖
Teilchen	□	□	🟧	✖
Kekse	□	□	🟫	✖
Muffins	□	□	🟩	✖
Plätzchen	□	□	🟪	✖

Erstellt am: 18/04/2012
Zuletzt geändert am:

&OK Abbrechen &Anwender

cellebrite
mobile data secured

cellebrite
mobile data secured

www.cellebrite.com