



Ermittlungen durch Datenauswertung von Smartphones

Marko Rogge

Head of Forensic Discovery

1 Milliarde Nutzer von mobilen Geräten

Vielfalt

Handys, Tablet-Computer, Phablets, **Smartphones** sammeln Unmengen an Daten, nicht nur Kontaktdaten

Ermittlungen

Daraus entsteht der wachsende Fokus der **Ermittlungen** von Strafverfolgungsbehörden im mobilen Bereich.

Straftat

Immer mehr Straftaten unter Nutzung mobiler Geräte z.B. Drogenhandel.

1 Mrd. Smartphones heute!
Prognose: 2 Mrd. bis 2015

Strafverfolgung: Stand der Dinge

Ermittlungen

Bei 84% aller abgeschlossenen Ermittlungen war zur Aufklärung eine Auswertung von mobilen Endgeräten essentiell.

*(Quelle: CONTURN AIG)



**1.Quartal 2013: 70,7 Millionen Samsung Smartphones
37,4 Millionen iPhones. (Zahlen IDC)**

Beispiel

**Datengewinnung aus einem iPhone 5 mit iOS7
&
Analyse der Verbindungsdaten**

Ausgangslage

Tatverdacht: Drogenhandel

Staatsanwaltschaft und Ermittlungsbehörden vermuten verfahrensrelevante Daten auf Computern, sonst. Datenträgern sowie mobilen Endgeräten.

Abwicklung der Geschäfte via Smartphones.

Durchsuchungsmaßnahme der Objekte

Beschlagnahme u.a. EDV und mobile Endgeräte



Sicherstellung EDV Hardware

Bei Hauptbeschuldigten:

- Intel Computer Dell Vision 2000 Srn. Nr. xxxx
- Apple MacBook 15" Srn. Nr. xxxx
- **iPhone 5** IMEI xxxxxxxx
- ... uvm.

Bei weiteren Beschuldigten:

- Weitere Computer
- Weitere Smartphones
- SD-Karten

iPhone 5 – iOS 7

The screenshot shows the 'Info' page of an iPhone 5. At the top, the status bar displays 'Telekom.de LTE 11:58' and '99 %' battery. Below the status bar, there are navigation options: a blue back arrow labeled 'Allgemein' and the word 'Info'. The main content is a list of device specifications:

Name	Victim >
Netzwerk	Telekom.de
Anschluss	Telekom.de
Titel	241
Videos	0
Fotos	43
Kapazität	13,3 GB
Verfügbar	10,6 GB
Version	7.0 (11A465)
Netzbetreiber	Telekom.de 15.0

Apple iPhone – Versionen Vielzahl



GSM

Version 1.0.0, 1.0.1, 1.0.2, 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
... **7.x**

CDMA

Version 4.2.5, 4.2.6, 4.2.7,
4.2.8, 4.2.9, 4.2.10, ...

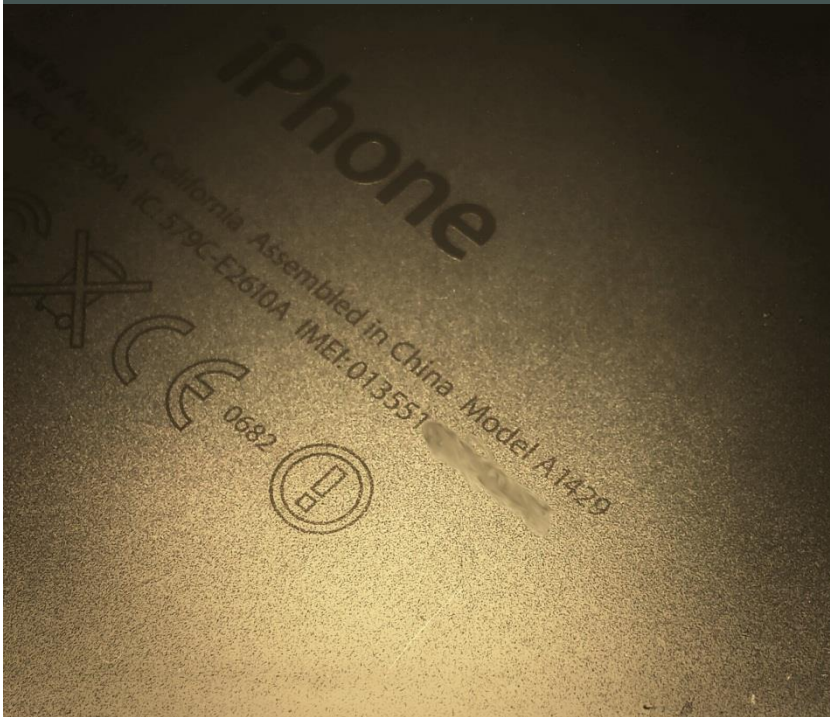
Unified

Version 5.0, 5.0.1, 5.1, ... ,
6.0, ...

Viele unterschiedliche Softwareversionen am Beispiel Apple iPhone & iOS

Identifikation iPhone5

Model Nummer A 1429



Webseite Apple

support.apple.com/kb/HT3939?viewlocale=de_at&locale=de_at

iPhone 5



Year introduced: 2012

Capacity: 16, 32, and 64 GB

- Model number on the back cover:
 - A1428: iPhone 5 (GSM model)
 - A1429: iPhone 5 (GSM and CDMA model)
 - A1442: iPhone 5 (CDMA model, China)
- Front: flat and made of glass.
- Back: anodized aluminum.
- Colors: black and white.
- There is a SIM tray on the right side that holds a "fourth form factor" (4FF) or "nano-SIM" card.
- The IMEI is etched on the back housing.

Hilfe dazu: Rückseite des iPhone5 [support.apple.com/kb/](https://support.apple.com/kb/HT3939)

Challenge

Extraktion der Kommunikationsdaten

Erweiterte logische Extraktion – ohne Passwort

The screenshot shows the CONTURN software interface with the 'Extraktionsübersicht' (Extraction Overview) window open. The window displays the following information:

- Geräteinformationen:** AppleDevice_AdvancedLogical (Apple iPhone Logical), Verbindungstyp: Cable, Extraktionsart: Logical.
- Bild-Hash-Information:** Für dieses Projekt stehen keine Referenz-Hash-Informationen zur Verfügung. (Hashes berechnen)
- Geräte-Info:**

Victim			
IMEI	013551007169	ICCID	89490200
Serial Number	F17KV07	Product Type	iPhone5,2
Product Version	7.0	Is Encrypted	True
Device Name	Victim	Display Name	Victim
- Geräteinhalt:**
 - Telefondaten:**
 - Installierte Anwendungen: 9 (0)
 - Datendateien:**
 - Bilder: 89 (0)
 - Konfigurationen: 149 (0)

Wenige Daten als Ergebnis ☹️

Erweiterte logische Extraktion – herkömmliche Tools

The screenshot shows the EnCase Forensic interface. On the left, a tree view displays the file system structure of an iPhone5, including folders like 'Raw Data', 'CameraRollDomain', 'AppDomain', and 'HomeDomain'. The 'Library' folder is expanded, showing sub-folders such as 'SMS', 'SMSes', 'SpringBoard', 'Keyboard', 'TCC', 'Voicemail', 'Mail', 'com.apple.itunesstored', 'Accounts', 'Notes', 'BackBoard', 'Safari', 'Caches', 'com.apple.WebAppCache', 'SystemPreferencesDomain', 'SystemConfiguration', 'WirelessDomain', and 'Databases'.

The main pane displays a table of files. The selected file is 'sms.db', which is a database file with a logical size of 213,008 bytes. The table columns include Name, Tag, File Ext, Logical Size, Item Type, Category, Signature Analysis, File Type, File Type Tag, Protected, Protection complexity, and Last Accessed.

Name	Tag	File Ext	Logical Size	Item Type	Category	Signature Analysis	File Type	File Type Tag	Protected	Protection complexity	Last Accessed
1 sms.db		db	213.008	Document	Database	Match	Paradox Database	db1			25/09/13 09:12:59

At the bottom, a detailed view of the selected file 'sms.db' is shown, including its file extension, logical size, item type, category, signature analysis, file type, file type tag, last accessed time, file creation time, MD5 hash, primary device, and item path.

```

Name: sms.db
File Ext: db
Logical Size: 213.008
Item Type: Document
Category: Database
Signature Analysis: Match
File Type: Paradox Database
File Type Tag: db1
Last Accessed: 25/09/13 09:12:59 (+2:00 Mitteleuropäische Sommerzeit)
File Created: 10/06/13 19:35:25 (+2:00 Mitteleuropäische Sommerzeit)
MD5: d73fe4440e7e11e4374372bf1410bbdf
Primary Device: iphone5
Item Path: iphone5\Raw Data\HomeDomain\Library\SMS\sms.db
    
```

Fast alle Daten: Keine Dekodierung ☹️

Was bringt z.B. der „iPhone Backup Extractor“?





































The screenshot shows the iPhone Backup Extractor application window. The 'Select backup' section displays a dropdown menu with the value '01.01.0001: 7274919f0e809b4dc'. Below this, it states '1 backups were found in your default folder. If your backups are not stored in this folder, you can select another backup folder.' The 'Backup details' section shows: Device: Unknown type, Time: 00:00:00, Serial: [redacted], IMEI: [redacted], Firmware: 4.0, Status: Complete and encrypted, Folder: 7274919f0e809b4dc. The 'Available data' section lists: Photos: Extract 43..., Videos: None, Contacts: Extract 127..., Voicemail: None, Calendar: None, Notes: None, SMS: Extract 155..., Call history: Extract 100..., Recordings: None, Location data: None, and WhatsApp: None. An 'Expert mode' button is visible at the bottom.

← ICCID?
← IMEI?

ROWID	address	date	duration	flags	id	name	country_code	network_code	read	assisted	face_time_data	originalAddress
1	+491516...	1378709424	351	4	-1		262	01	1	0	{null}	
2	+49173...	1378711819	3	5	141		262	01	1	0	{null}	
3		1378725010	215	8	-1		262	01	1	0	{null}	
4	+491512...	1378731435	0	4	-1		262	01	1	0	{null}	
5	+491512...	1378736115	0	4	-1		262	01	1	0	{null}	
6	+491763...	1378743534	495	5	126		262	01	1	0	{null}	
7	+491516...	1378745160	270	5	149		262	01	1	0	{null}	
8	+49172...	1378748596	4	5	92		262	01	1	0	{null}	
9	01762...	1378748616	591	5	150		262	01	1	0	{null}	
10	+49172...	1378751122	356	4	-1		262	01	1	0	{null}	

Schwaches Ergebnis

Erweiterte logische Extraktion

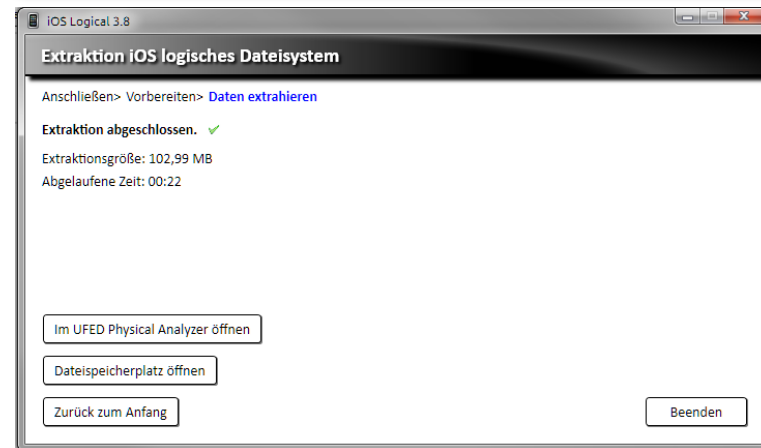
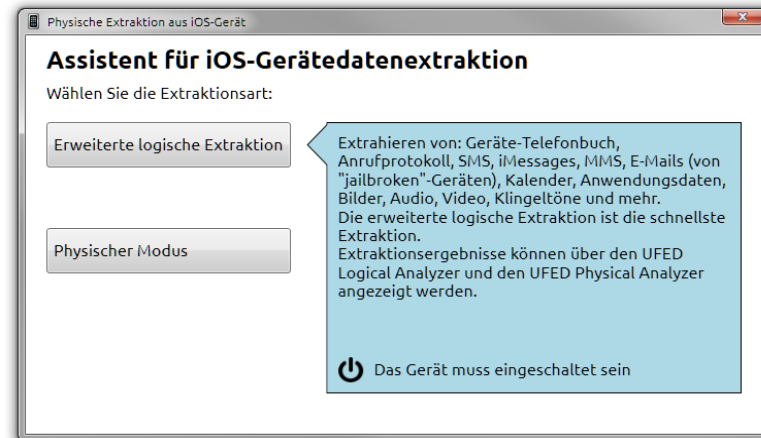
	Logical	File System	Advanced Logical Extraction	Physical
SMS/MMS				
Kontakte				
Anrufliste				
Kalender				
Audio/Video				
Dateien				
Versteckte Dateien				
Gelöschte Daten				
Applikationen				

Zugriffsrechte ermöglichen den erweiterten Zugriff

Erweiterte logische Extraktion!

Was braucht man?

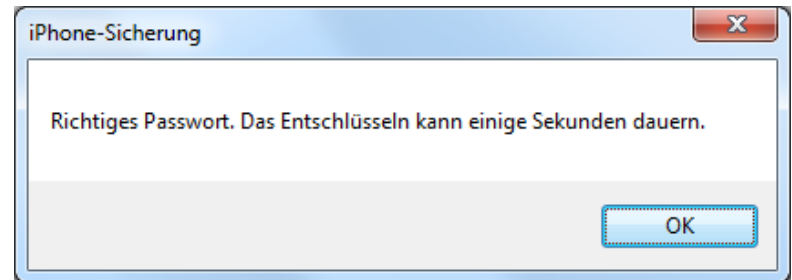
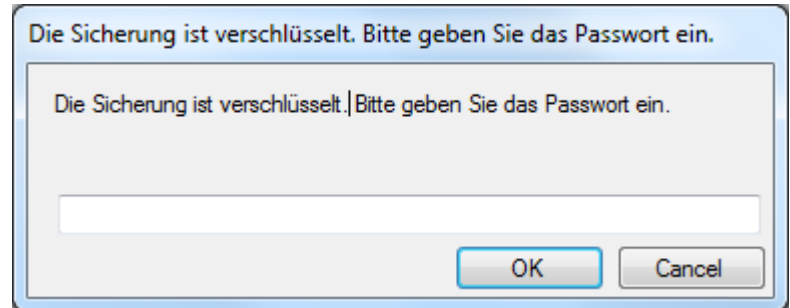
- Forensik Hardware; Cellebrite UFED Physical Analyzer (iOS Adv. Logical)
- iTunes Backup & PW des Beschuldigten
- Etwas Zeit ...



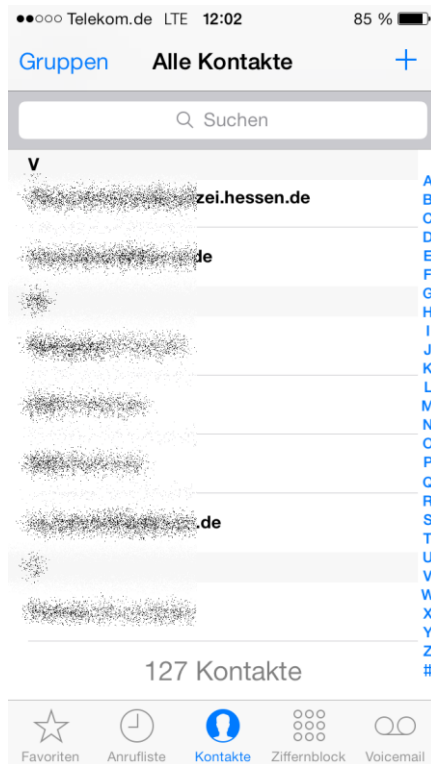
Gelöschte Daten

Woher kommen die Daten?

- iTunes „Flag“ zum iPhone; Backup vorhanden | encrypted
- Passwort des Beschuldigten durch Vernehmung
- iPhone5 erweiterte logische Extraktion (Backup vom iPhone: Yes!)
- Gelöschte Kommunikation!



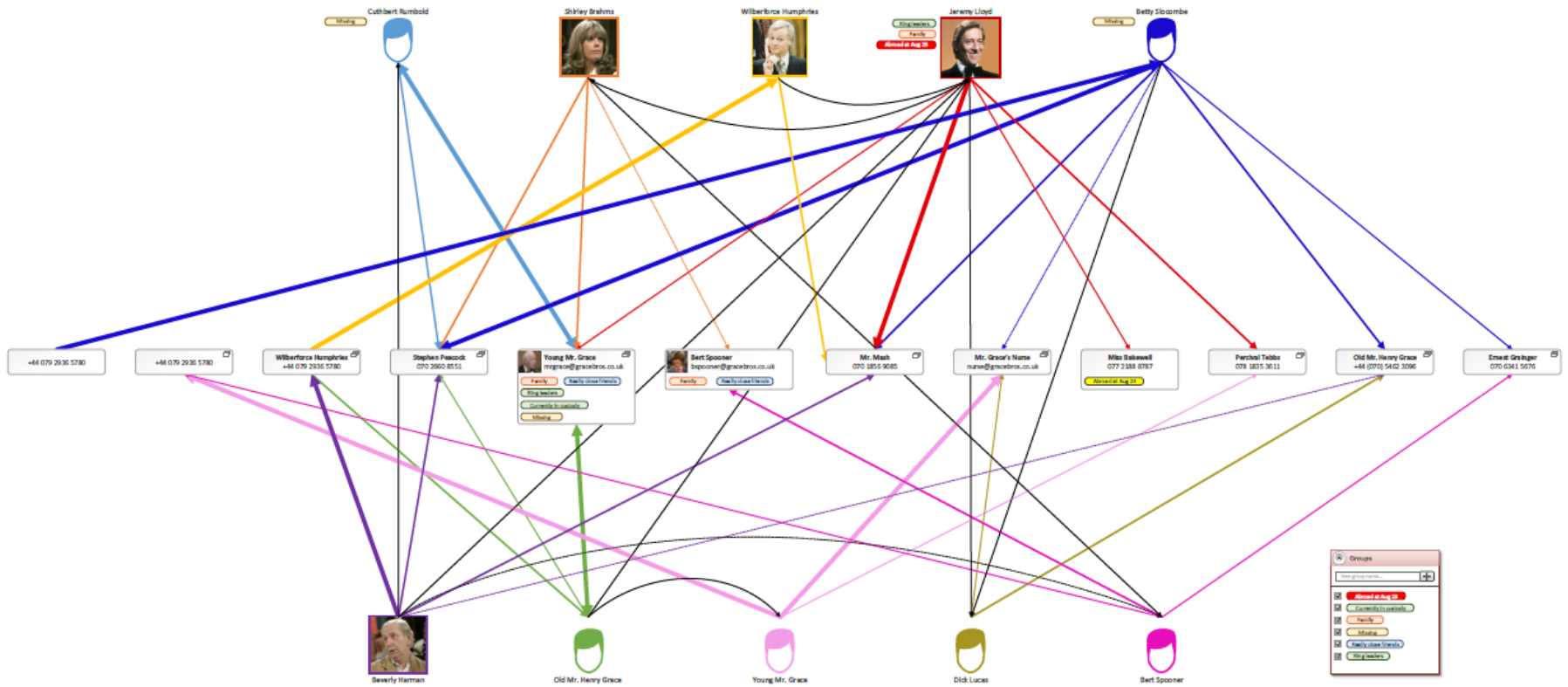
Mobile Forensik: Klare Darstellung für Ermittler



✓	178			+	+49173		05.07.2013 08:10:07(UTC+0)	00:07:37	Incoming	262	01
✓	179				017788		05.07.2013 07:54:24(UTC+0)	00:03:21	Outgoing	262	01
✓	180				017723		04.07.2013 20:17:59(UTC+0)	00:00:00	Outgoing	262	01
✓	181				017723		04.07.2013 20:09:50(UTC+0)	00:00:05	Outgoing	262	01
✓	182				017224		04.07.2013 19:24:45(UTC+0)	00:00:02	Outgoing	262	01
✓	183				061518		04.07.2013 13:03:03(UTC+0)	00:00:57	Outgoing	262	01
✓	184				+49176		04.07.2013 10:24:35(UTC+0)	00:00:14	Outgoing	262	01
✓	185				+49178		04.07.2013 08:44:40(UTC+0)	00:00:00	Missed	262	01
✓	186				017825		04.07.2013 08:41:43(UTC+0)	00:00:00	Outgoing	262	01
✓	187				017883		04.07.2013 08:38:35(UTC+0)	00:00:00	Outgoing	262	01
✓	188				+49176		04.07.2013 07:51:18(UTC+0)	00:08:58	Outgoing	262	01
✓	189				+49699	Guido Kerbsties	04.07.2013 07:35:14(UTC+0)	00:00:32	Outgoing	262	01
✓	190				+49699	Guido Kerbsties	04.07.2013 07:33:06(UTC+0)	00:01:48	Outgoing	262	01
✓	191				+491621		04.07.2013 06:52:02(UTC+0)	00:01:16	Outgoing	262	01
✓	192				0699799		03.07.2013 17:15:24(UTC+0)	00:01:14	Outgoing	262	01
✓	193				+491763	Peter Warnke	03.07.2013 14:26:57(UTC+0)	00:00:08	Outgoing	262	01
✓	194				+491763	Peter Warnke	03.07.2013 14:18:31(UTC+0)	00:00:00	Outgoing	262	01
✓	195				0699795		03.07.2013 13:37:41(UTC+0)	00:00:00	Outgoing		
✓	196				+417975		06.09.2013 09:28:55(UTC+0)	00:03:55	Incoming	F	
✓	197				+49170		10.07.2013 13:25:13(UTC+0)	00:00:04	Outgoing	620	1'
✓	198				0699799		10.07.2013 07:37:18(UTC+0)	00:00:03	Outgoing	262	01
✓	199				+491783		09.07.2013 20:50:54(UTC+0)	00:00:00	Outgoing	262	01
✓	200				+49170		09.07.2013 13:45:34(UTC+0)	00:00:10	Incoming		
✓	201				+491783		09.07.2013 20:48:00(UTC+0)	00:00:00	Missed		
✓	202						26.08.2013 07:13:04(UTC+0)	00:00:43	Incoming		
✓	203				+417975		06.09.2013 09:28:55(UTC+0)	00:03:55	Incoming	262	01
✓	204				+495251		06.09.2013 10:33:06(UTC+0)	00:06:38	Outgoing	262	01
✓	205				+49170		06.09.2013 12:51:37(UTC+0)	00:00:00	Missed	262	01
✓	206				0697555		06.09.2013 13:47:39(UTC+0)	00:00:00	Outgoing	262	01
✓	207						06.09.2013 13:50:29(UTC+0)	00:07:18	Incoming	262	01
✓	208				+491763	Peter Warnke	06.09.2013 14:52:16(UTC+0)	00:22:41	Outgoing	262	01
✓	209				0179216		06.09.2013 16:32:23(UTC+0)	00:08:08	Outgoing	262	01
✓	210				+49170		06.09.2013 19:08:51(UTC+0)	00:01:20	Incoming	262	01
✓	211				+49170		07.09.2013 16:50:29(UTC+0)	00:00:00	Outgoing	262	01
✓	212				+49170		07.09.2013 16:54:32(UTC+0)	00:02:31	Incoming	262	01
✓	213						08.09.2013 20:06:29(UTC+0)	00:00:00	Missed	262	01

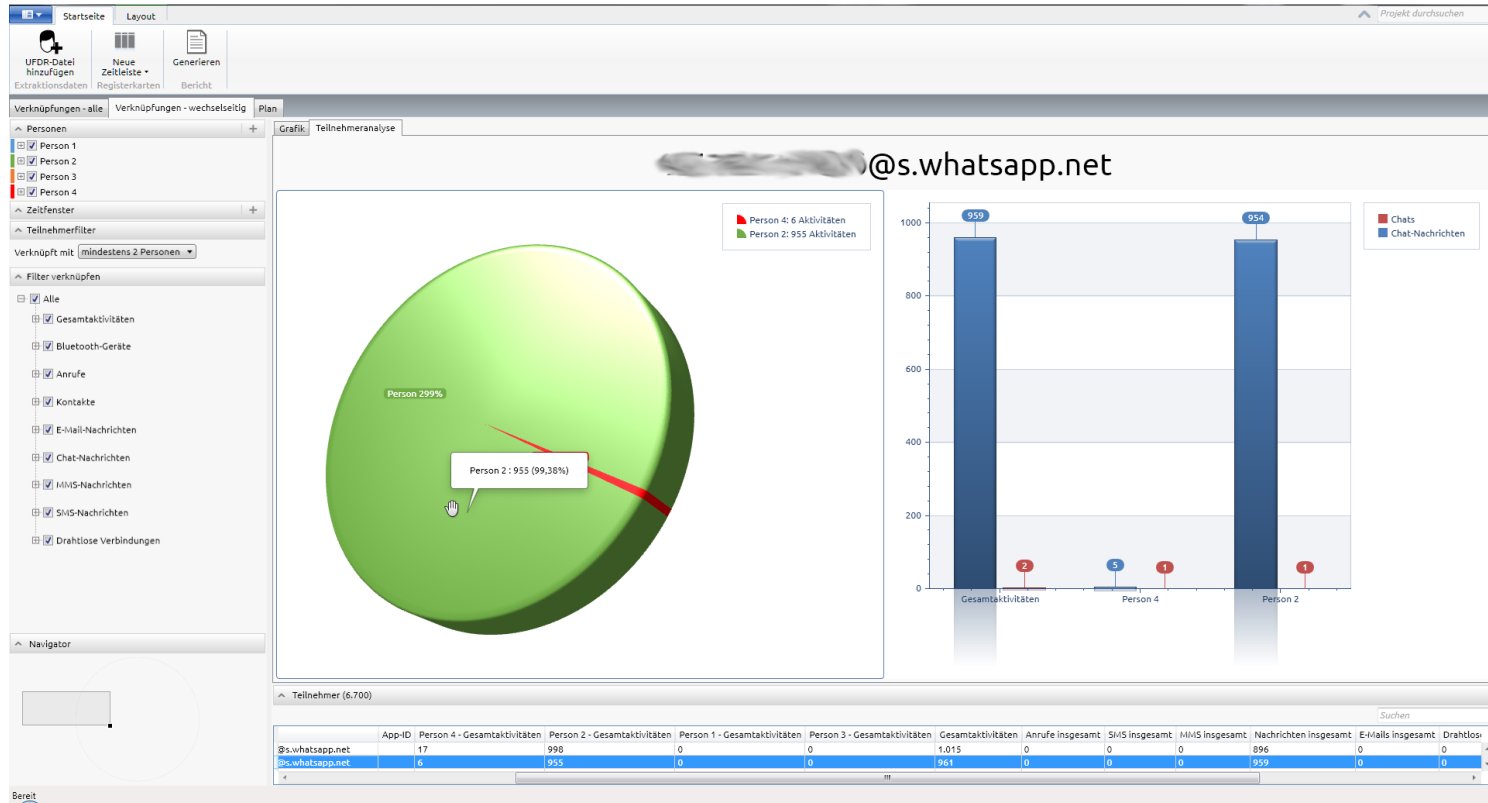
Rufnummernabfrage: Prepaid = 0 Chance!

Wer mit wem? Die Analyse mit Link Analysis



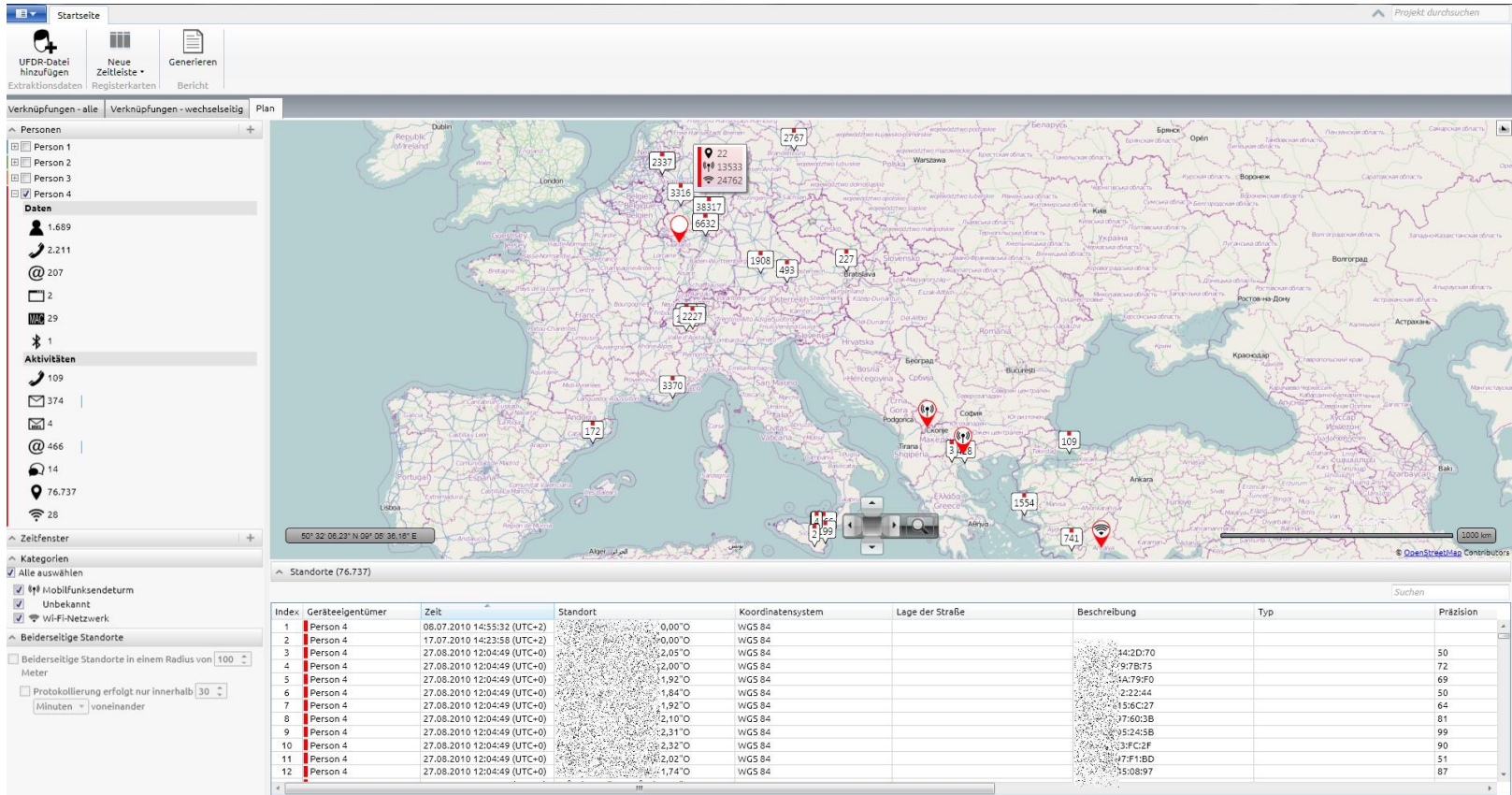
Analyse von Beziehungen und Kommunikation

Link Analysis: Kommunikationsdaten auswerten



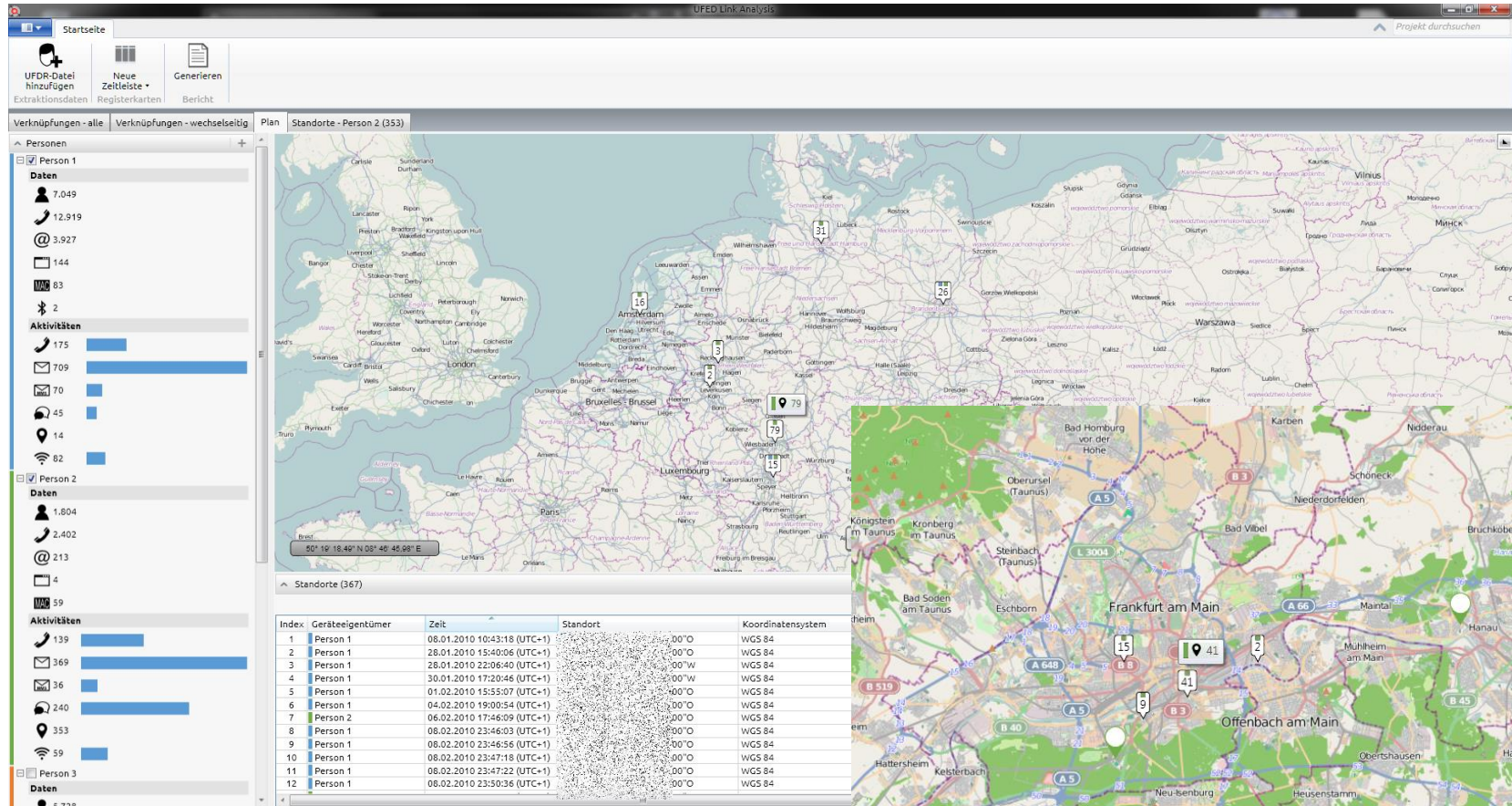
Beziehungen zwischen WhatsApp Partnern

Link Analysis: Standortdaten mit techn. Details



Reiseroute der Person 4

Link Analysis: Noch mehr Details – Zoom in



Reiseroute der Person 1 – mehr Details bitte!

Link Analysis: Klares Reporting für Ermittler

The screenshot displays a software interface for link analysis. On the left, a sidebar lists 'Personen' (Person 1-4) and 'Daten' (1.65, 2.2, 207, 2, 29, 1, 109, 374, 4, 466, 14, 76.7, 28). The main area shows a map with a travel route for 'Person 4' highlighted in blue. A dialog box titled 'Bericht erstellen' (Create Report) is open, showing report configuration options and a table of coordinates.

Bericht erstellen

Berichtsdaten Berichtlayout

Personenzusammenfassung

Ansichten

Verknüpfungen - alle

Verknüpfungen - wechselseitig

Zusätzliche Felder

Name des Ermittlers: Rogge, Marko Ermittler-ID: 832201

Abteilungsname: KM/F-33 Standort: Deutschland

Fall-Nummer: 111 Fall-Name: Imelner

Zurücksetzen

Dateiname: Report

Speichern auf: F:\

Unterverzeichnis erstellen: LinkAnalysisReport_260913_173430

Generieren Abbrechen

Standort	Koordinatensystem	Lage der Straße
01	60°O	WGS 84
02	36°O	WGS 84
03	06°O	WGS 84
04	59°O	WGS 84
05	84°O	WGS 84
06	23°O	WGS 84
07	65°O	WGS 84
08	14°O	WGS 84
09	53°O	WGS 84
10	01°O	WGS 84
11	32°O	WGS 84
12	46°O	WGS 84

Reiseroute der Person 4 – Alle Details übersichtlich im Report!

Zusammenfassung

- ↻ Vielseitige Möglichkeiten der Datengewinnung
- ↻ Geo Daten mit zunehmender Bedeutung
 - Tatort Bestimmungen etc.
- ↻ Analyse von Kommunikationsdaten
- ↻ Gelöschte Daten zurück gewinnen
- ↻ Einfachere Bewertung der Daten für Ermittler
- ↻ Sehr detaillierte Datengewinnung insb. Geo Daten oder Verbindungsdaten
- ↻ ...

Fragen? Fragen!



Vielen Dank!

Kontakt:

CONTURN
Analytical Intelligence Group GmbH

Hamburger Allee 45
60486 Frankfurt am Main

Telefon: +49 (0)69 979 959 20
Telefax: +49 (0)69 979 959 264

Email: infoservice@conturn.com
www.conturn.com

