POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

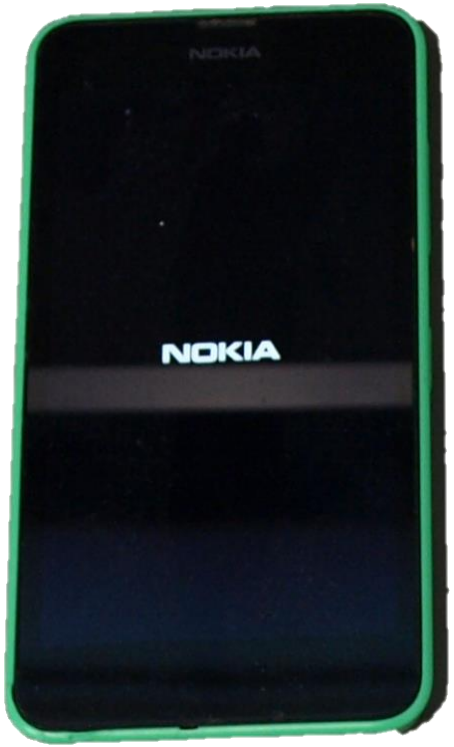
bürgerorientiert · professionell · rechtsstaatlich

Polizeiliche F&E in der mobilen Forensik

Entwicklung einer Software zur Auswertung von Windows Mobile (10) Handys

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Windows Mobile 10



Handys mit Windows Mobile

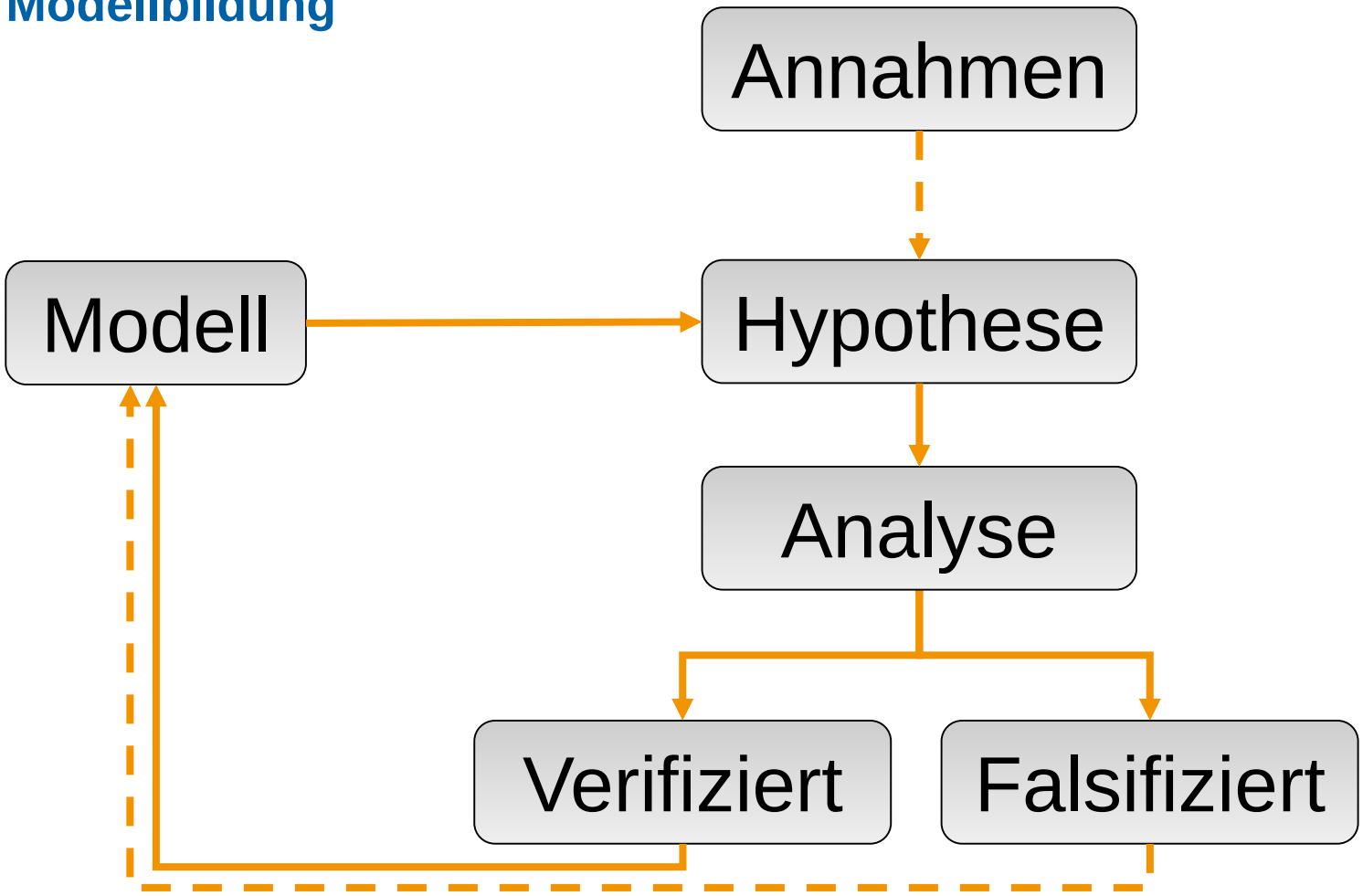
- Insgesamt rund 111 Mio. Geräte verkauft (Quelle: Wikipedia)
- Marktanteil zu Hochzeiten unter 5 % (Quelle: Statista.com)
- Dennoch für polizeiliche Untersuchungen relevant
- „Reiten toter Pferde“

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

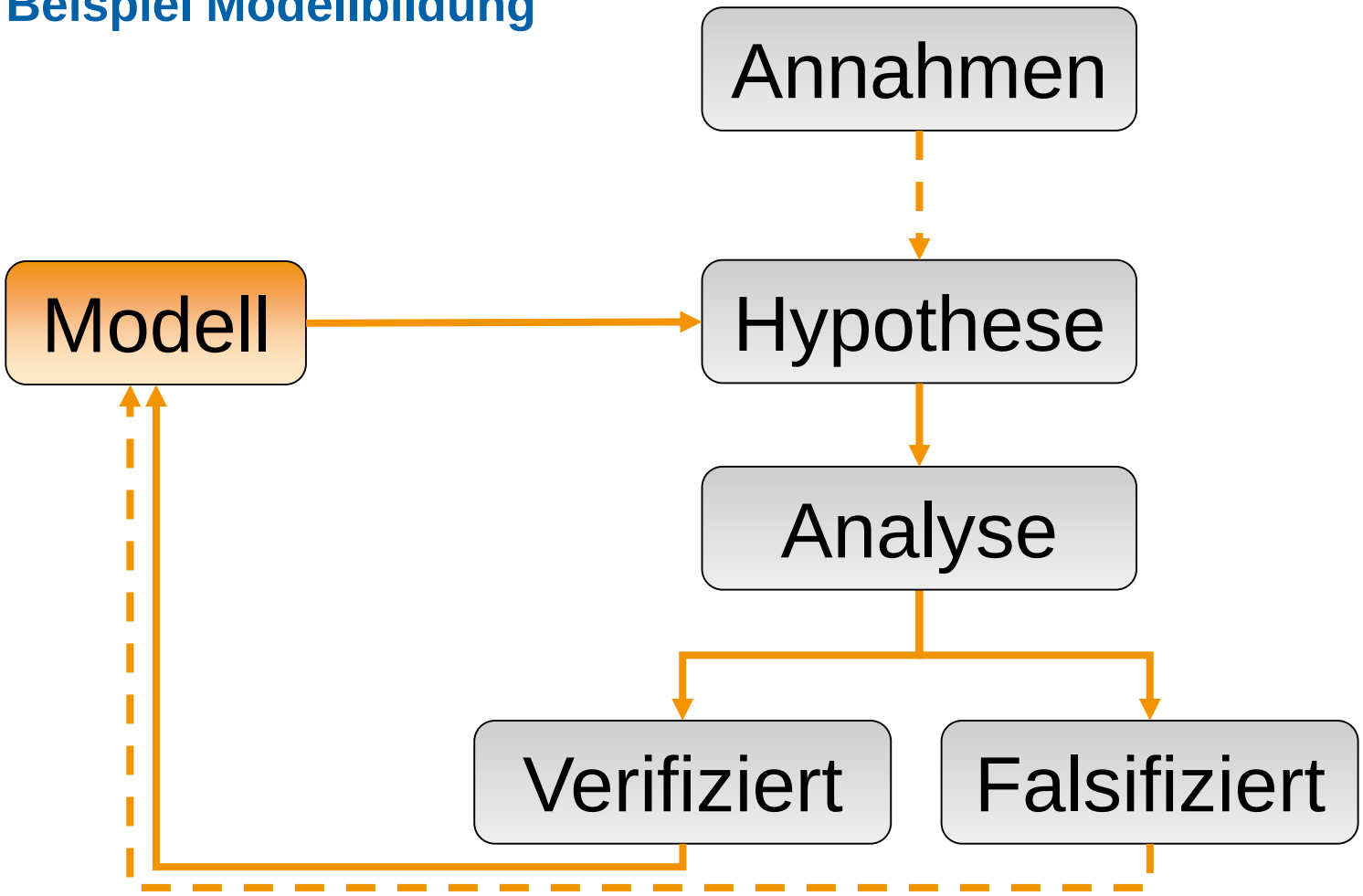
Überblick

- Grundlegendes Vorgehen
  - Modell, Hypothese, Analyse
  - Beispiel
- Analysetechniken
  - Der Weg zum Image
  - Die eigene Mobilfunkzelle
  - Dotnet-Decompiler
- Zusammenfassung

Modellbildung



Beispiel Modellbildung

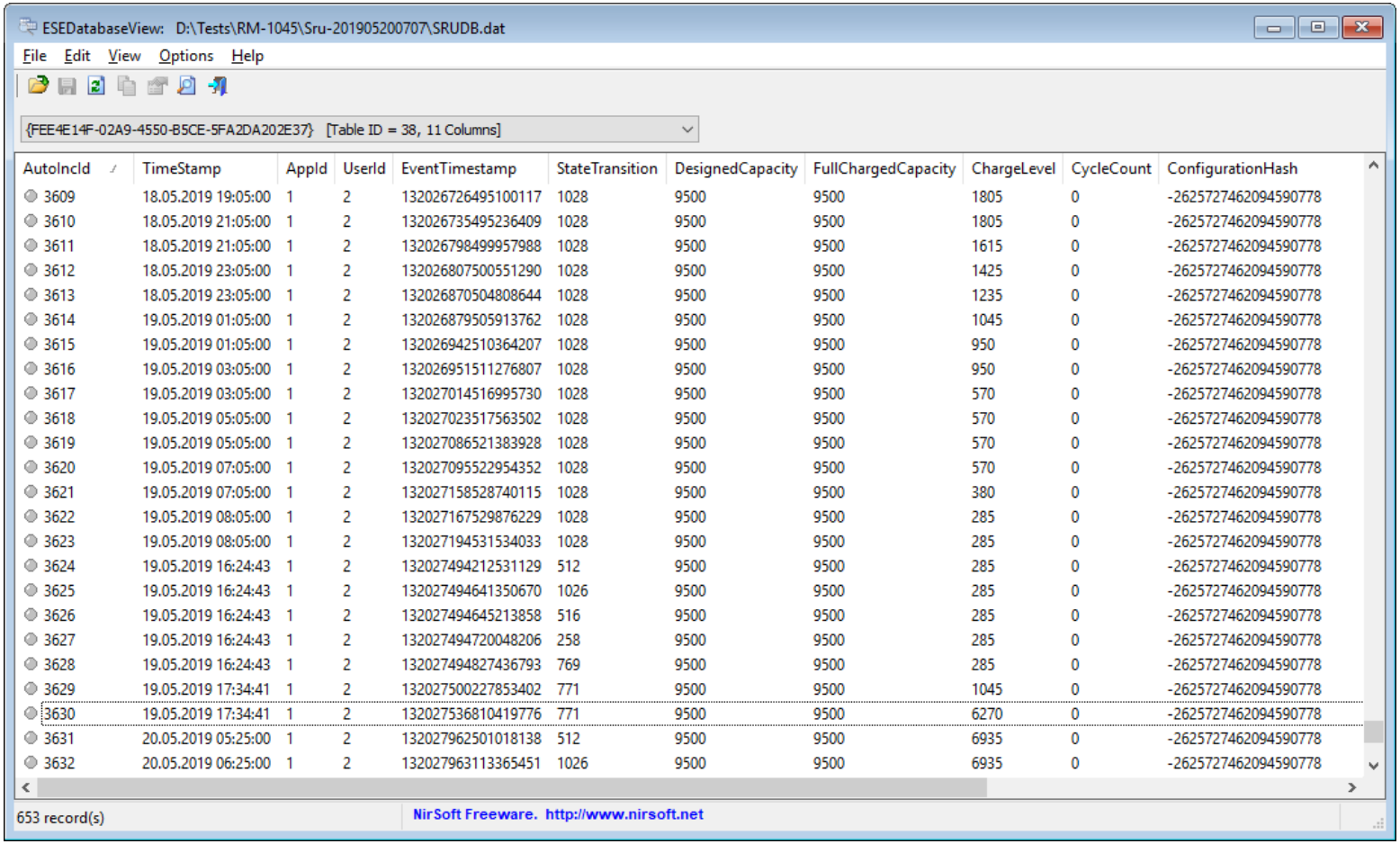


Modell

- System Resource Usage Monitor (SRUM)
  - Windows ESE-Datenbank (Extensible Storage Engine)
  - Netzwerk, laufende Programme, Energieverbrauch
- Tabelle {FEE4E14F-02A9-4550-B5CE-5FA2DA202E37}
  - Energy Usage Provider (energyprov.dll)
- Bekannte Spalten:
  - AutoIncId, TimeStamp, EventTimestamp, DesignedCapacity, FullChargedCapacity, ChargeLevel

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Beispiel

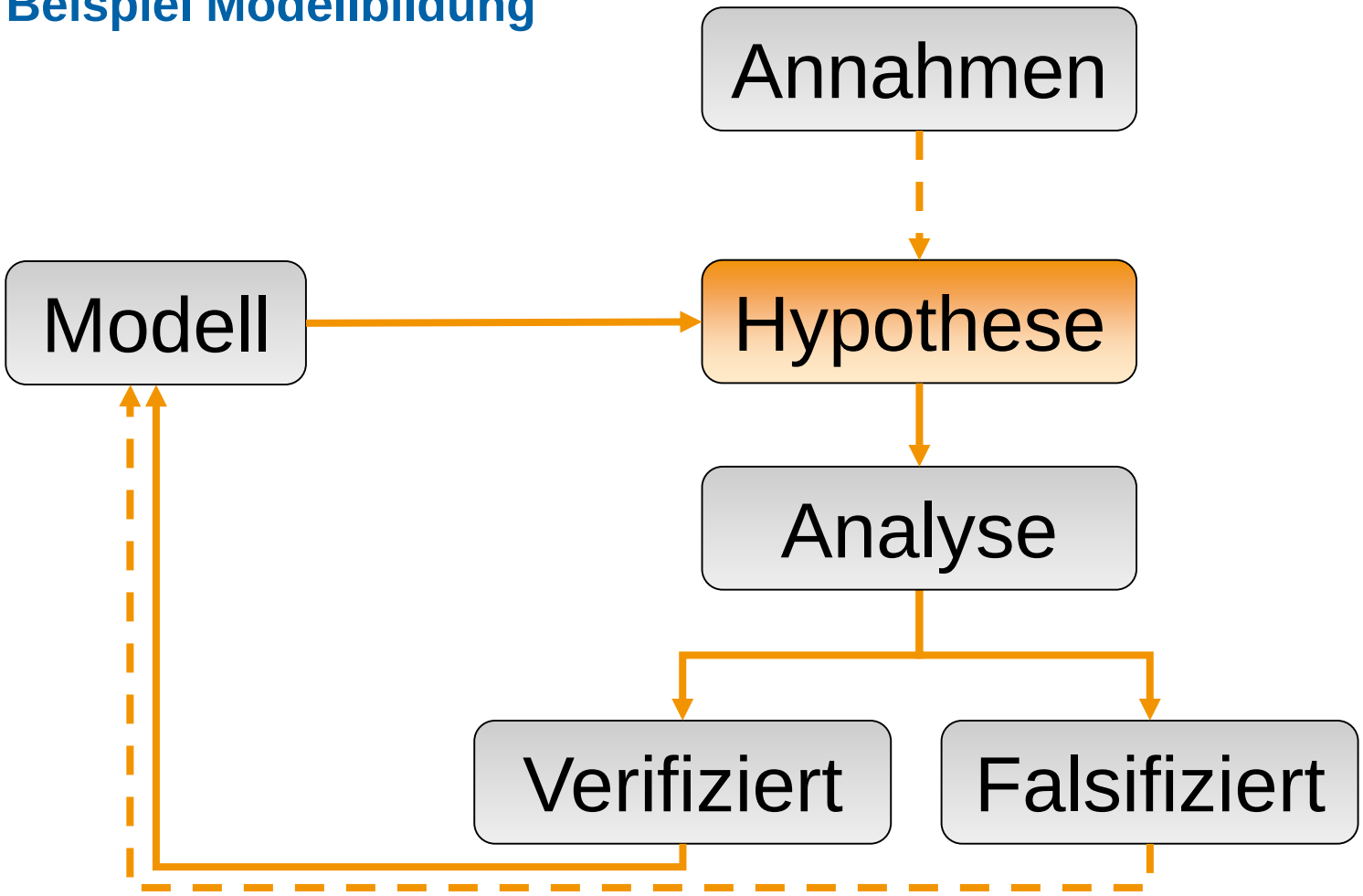


AutoIncId	TimeStamp	AppId	UserId	EventTimestamp	StateTransition	DesignedCapacity	FullChargedCapacity	ChargeLevel	CycleCount	ConfigurationHash
3609	18.05.2019 19:05:00	1	2	132026726495100117	1028	9500	9500	1805	0	-2625727462094590778
3610	18.05.2019 21:05:00	1	2	132026735495236409	1028	9500	9500	1805	0	-2625727462094590778
3611	18.05.2019 21:05:00	1	2	132026798499957988	1028	9500	9500	1615	0	-2625727462094590778
3612	18.05.2019 23:05:00	1	2	132026807500551290	1028	9500	9500	1425	0	-2625727462094590778
3613	18.05.2019 23:05:00	1	2	132026870504808644	1028	9500	9500	1235	0	-2625727462094590778
3614	19.05.2019 01:05:00	1	2	132026879505913762	1028	9500	9500	1045	0	-2625727462094590778
3615	19.05.2019 01:05:00	1	2	132026942510364207	1028	9500	9500	950	0	-2625727462094590778
3616	19.05.2019 03:05:00	1	2	132026951511276807	1028	9500	9500	950	0	-2625727462094590778
3617	19.05.2019 03:05:00	1	2	132027014516995730	1028	9500	9500	570	0	-2625727462094590778
3618	19.05.2019 05:05:00	1	2	132027023517563502	1028	9500	9500	570	0	-2625727462094590778
3619	19.05.2019 05:05:00	1	2	132027086521383928	1028	9500	9500	570	0	-2625727462094590778
3620	19.05.2019 07:05:00	1	2	132027095522954352	1028	9500	9500	570	0	-2625727462094590778
3621	19.05.2019 07:05:00	1	2	132027158528740115	1028	9500	9500	380	0	-2625727462094590778
3622	19.05.2019 08:05:00	1	2	132027167529876229	1028	9500	9500	285	0	-2625727462094590778
3623	19.05.2019 08:05:00	1	2	132027194531534033	1028	9500	9500	285	0	-2625727462094590778
3624	19.05.2019 16:24:43	1	2	132027494212531129	512	9500	9500	285	0	-2625727462094590778
3625	19.05.2019 16:24:43	1	2	132027494641350670	1026	9500	9500	285	0	-2625727462094590778
3626	19.05.2019 16:24:43	1	2	132027494645213858	516	9500	9500	285	0	-2625727462094590778
3627	19.05.2019 16:24:43	1	2	132027494720048206	258	9500	9500	285	0	-2625727462094590778
3628	19.05.2019 16:24:43	1	2	132027494827436793	769	9500	9500	285	0	-2625727462094590778
3629	19.05.2019 17:34:41	1	2	132027500227853402	771	9500	9500	1045	0	-2625727462094590778
3630	19.05.2019 17:34:41	1	2	132027536810419776	771	9500	9500	6270	0	-2625727462094590778
3631	20.05.2019 05:25:00	1	2	132027962501018138	512	9500	9500	6935	0	-2625727462094590778
3632	20.05.2019 06:25:00	1	2	132027963113365451	1026	9500	9500	6935	0	-2625727462094590778

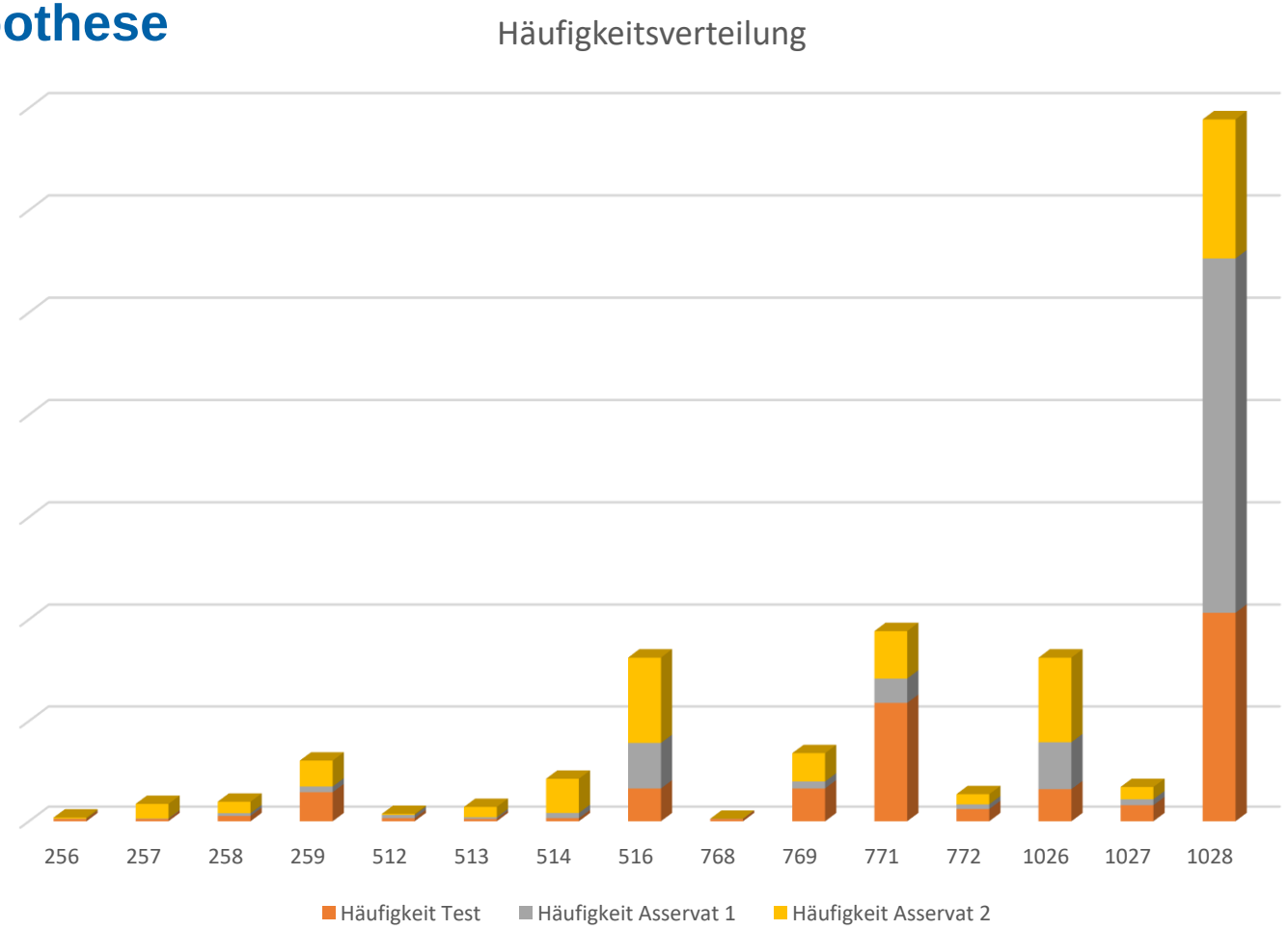
Beispiel

AutoIncId	TimeStamp	AppId	UserId	EventTimestamp	StateTransition	DesignedCapacity	FullChargedCapacity	ChargeLevel	CycleCount	ConfigurationHash
3627	19.05.2019 16:24:43	1	2	132027494720048206	258	9500	9500	285	0	-2625727462094590778
3628	19.05.2019 16:24:43	1	2	132027494827436793	769	9500	9500	285	0	-2625727462094590778
3629	19.05.2019 17:34:41	1	2	132027500227853402	771	9500	9500	1045	0	-2625727462094590778
3630	19.05.2019 17:34:41	1	2	132027536810419776	771	9500	9500	6270	0	-2625727462094590778
3631	20.05.2019 05:25:00	1	2	132027962501018138	512	9500	9500	6935	0	-2625727462094590778
3632	20.05.2019 06:25:00	1	2	132027963113365451	1026	9500	9500	6935	0	-2625727462094590778
3633	20.05.2019 06:25:00	1	2	132027998462517367	1028	9500	9500	6840	0	-2625727462094590778
3634	20.05.2019 06:28:00	1	2	132028000766858553	516	9500	9500	6840	0	-2625727462094590778
3635	20.05.2019 06:28:17	1	2	132028000975539748	1026	9500	9500	6745	0	-2625727462094590778
3636	20.05.2019 06:28:22	1	2	132028001027861465	772	9500	9500	6745	0	-2625727462094590778
3637	20.05.2019 06:28:34	1	2	132028001031729336	259	9500	9500	6745	0	-2625727462094590778

Beispiel Modellbildung



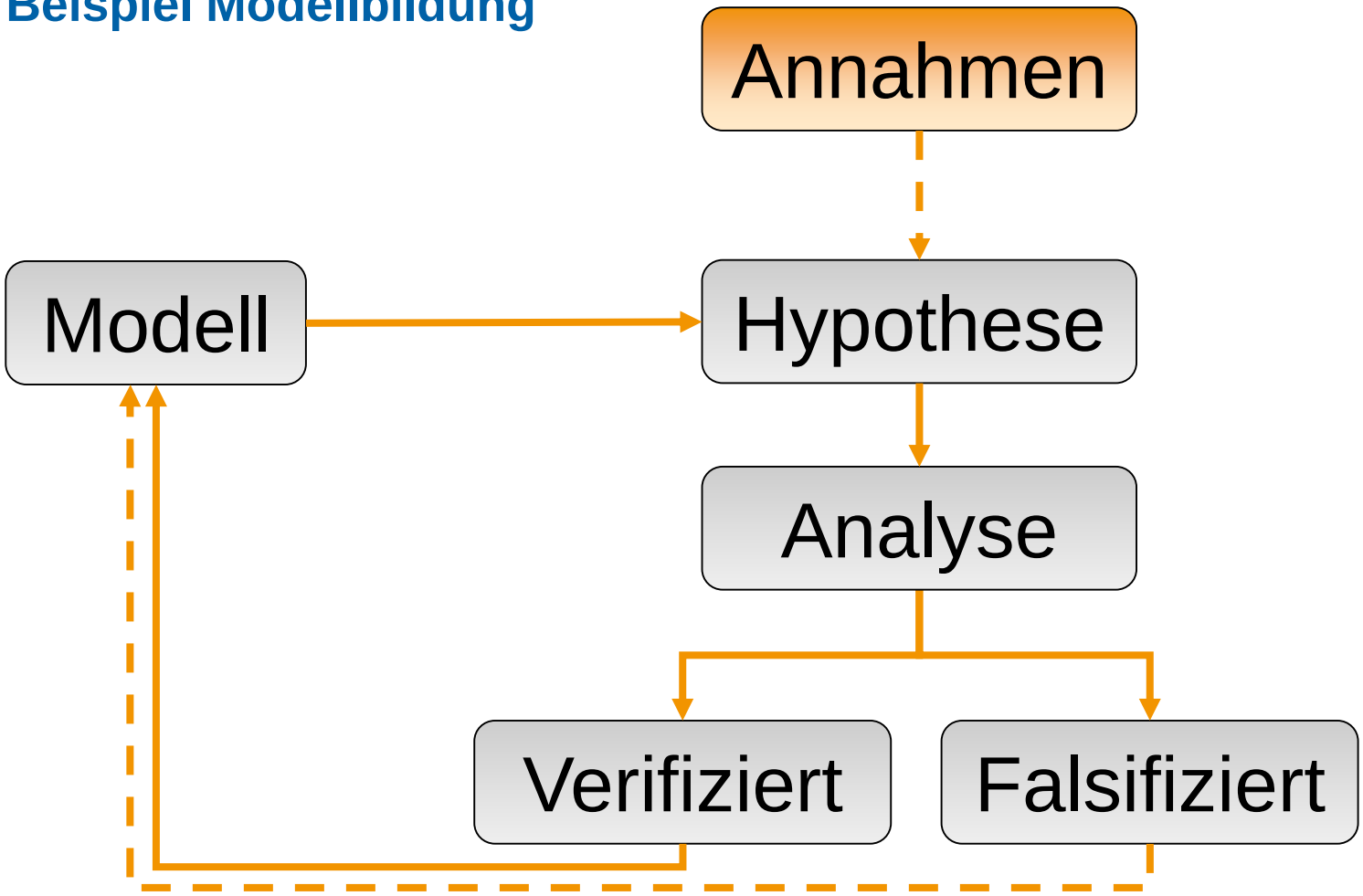
Hypothese


Häufigkeitsverteilung
256
257
258
259
512
513
514
516
768
769
771
772
1026
1027
1028
Häufigkeit Test
Häufigkeit Asservat 1
Häufigkeit Asservat 2

Hypothese

- Anhaltspunkt
  - Spaltenname StateTransition (Zustandsübergang)
  - Tabelle Energy Provider
- Geringe Anzahl an Zustandsübergängen
- Hypothese: Bestimmte Ereignisse triggern einen Zustandsübergang
  - Ladestrom an-/ausschalten
  - Display
  - Netzwerk
  - Mobile Daten
  - Flugmodus, Kamera, Bluetooth, usw.
- Hypothese: Die bitweise Darstellung trägt Information (Bitmaske)

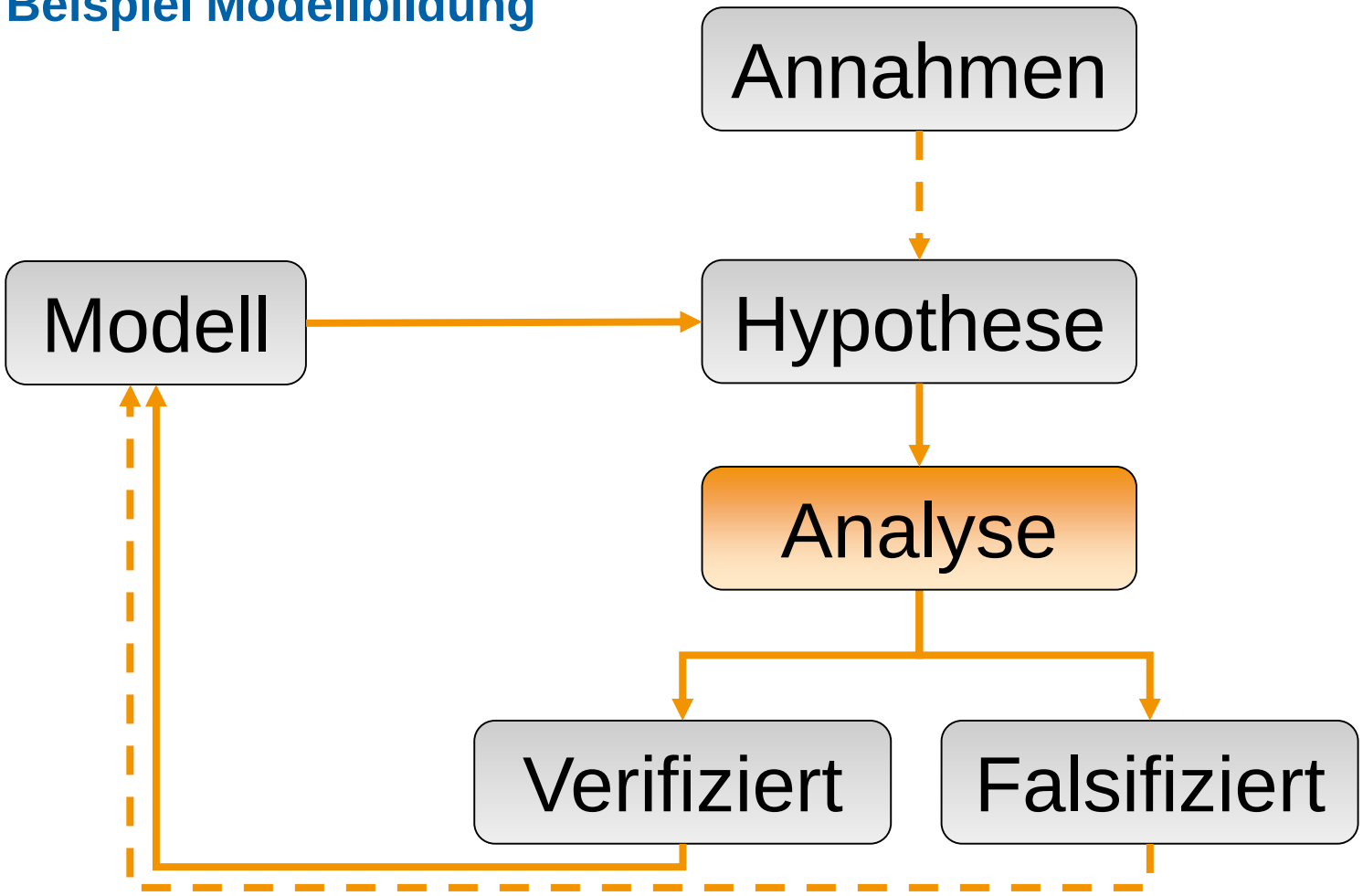
Beispiel Modellbildung



Annahmen

- Einzelne, unabhängige Ereignisse (Unbewusste Annahme)
- Bitmaske durch Zweierpotenzreihe inspiriert (Bias) 1, 2, 4, 8, 16, 32, 64, 128 265, 512, 1024

Beispiel Modellbildung



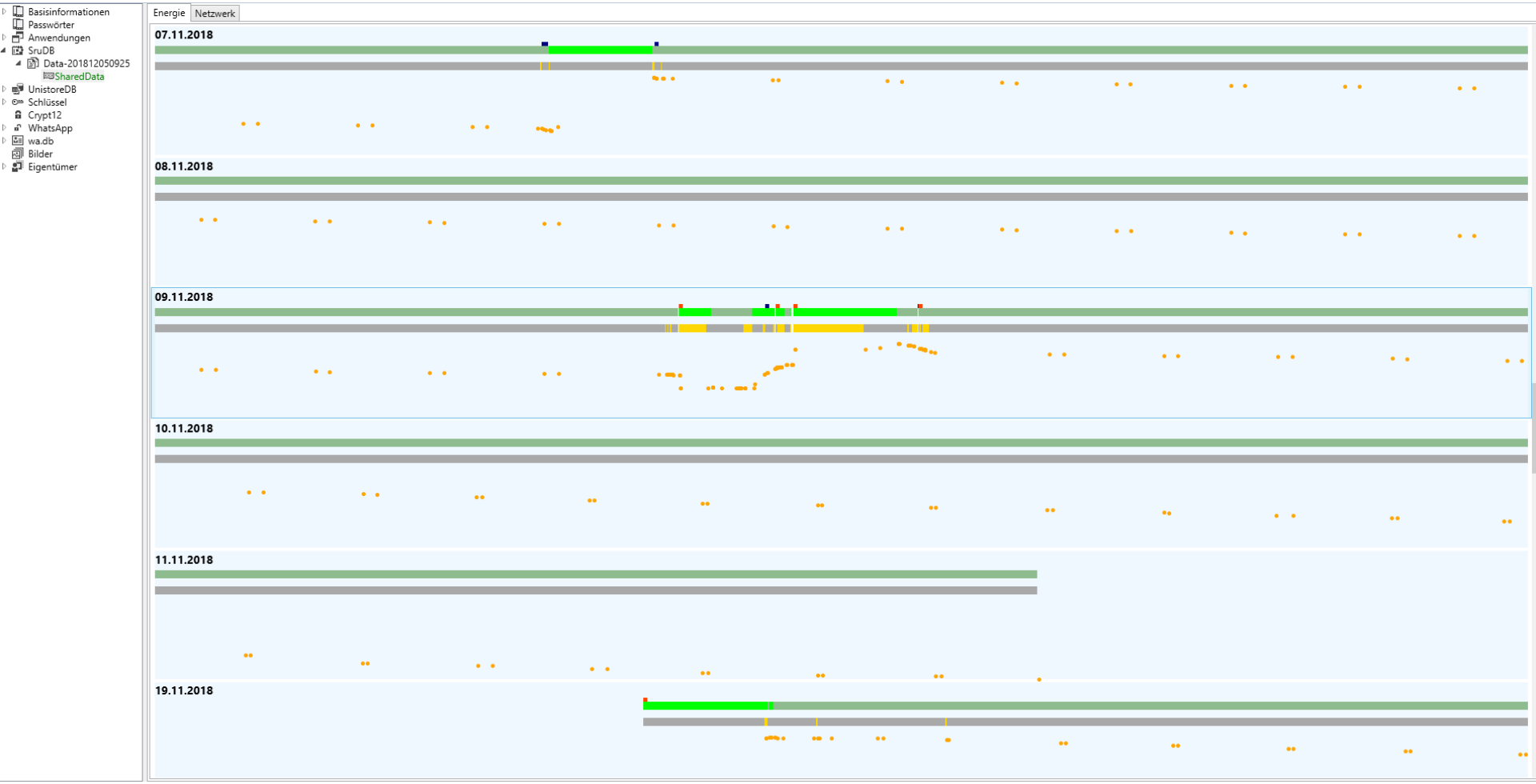
Analyse

Wert (dezimal)	Binärdarstellung			Bedeutung
256	0001	0000	0000	
257	0001	0000	0001	
258	0001	0000	0010	
259	0001	0000	0011	
512	0010	0000	0000	
513	0010	0000	0001	
514	0010	0000	0010	
516	0010	0000	0100	
768	0011	0000	0000	
769	0011	0000	0001	
771	0011	0000	0011	
772	0011	0000	0100	
1026	0100	0000	0010	
1027	0100	0000	0011	
1028	0100	0000	0100	

Analyse

Wert (dezimal)	Binärdarstellung			Bedeutung
256	0001	0000	0000	Einschalten (Gerät am Ladestrom)
257	0001	0000	0001	GSM-Ereignis (Gerät am Ladestrom)
258	0001	0000	0010	Ladestrom anschalten (Display ist an)
259	0001	0000	0011	Display anschalten (Gerät am Ladestrom)
512	0010	0000	0000	Einschalten (Kein Ladestrom)
513	0010	0000	0001	Ladestrom ausschalten (Display ist an)
514	0010	0000	0010	GSM-Ereignis (Kein Ladestrom)
516	0010	0000	0100	Display anschalten (Kein Ladestrom)
768	0011	0000	0000	Einschalten leerer Akku (Gerät am Ladestrom)
769	0011	0000	0001	Display ausschalten (Gerät am Ladestrom)
771	0011	0000	0011	Leerlauf (Gerät am Ladestrom)
772	0011	0000	0100	Ladestrom anschalten (Display ist aus)
1026	0100	0000	0010	Display ausschalten (Kein Ladestrom)
1027	0100	0000	0011	Ladestrom ausschalten (Display ist aus)
1028	0100	0000	0100	Leerlauf (Kein Ladestrom)

Analyse


Basisinformationen
Passwörter
Anwendungen
SruDB
Data-201812050925
SharedData
UnistoreDB
Schlüssel
Crypt12
WhatsApp
wa.db
Bilder
Eigentümer
Energie
Netzwerk
07.11.2018
08.11.2018
09.11.2018
10.11.2018
11.11.2018
19.11.2018

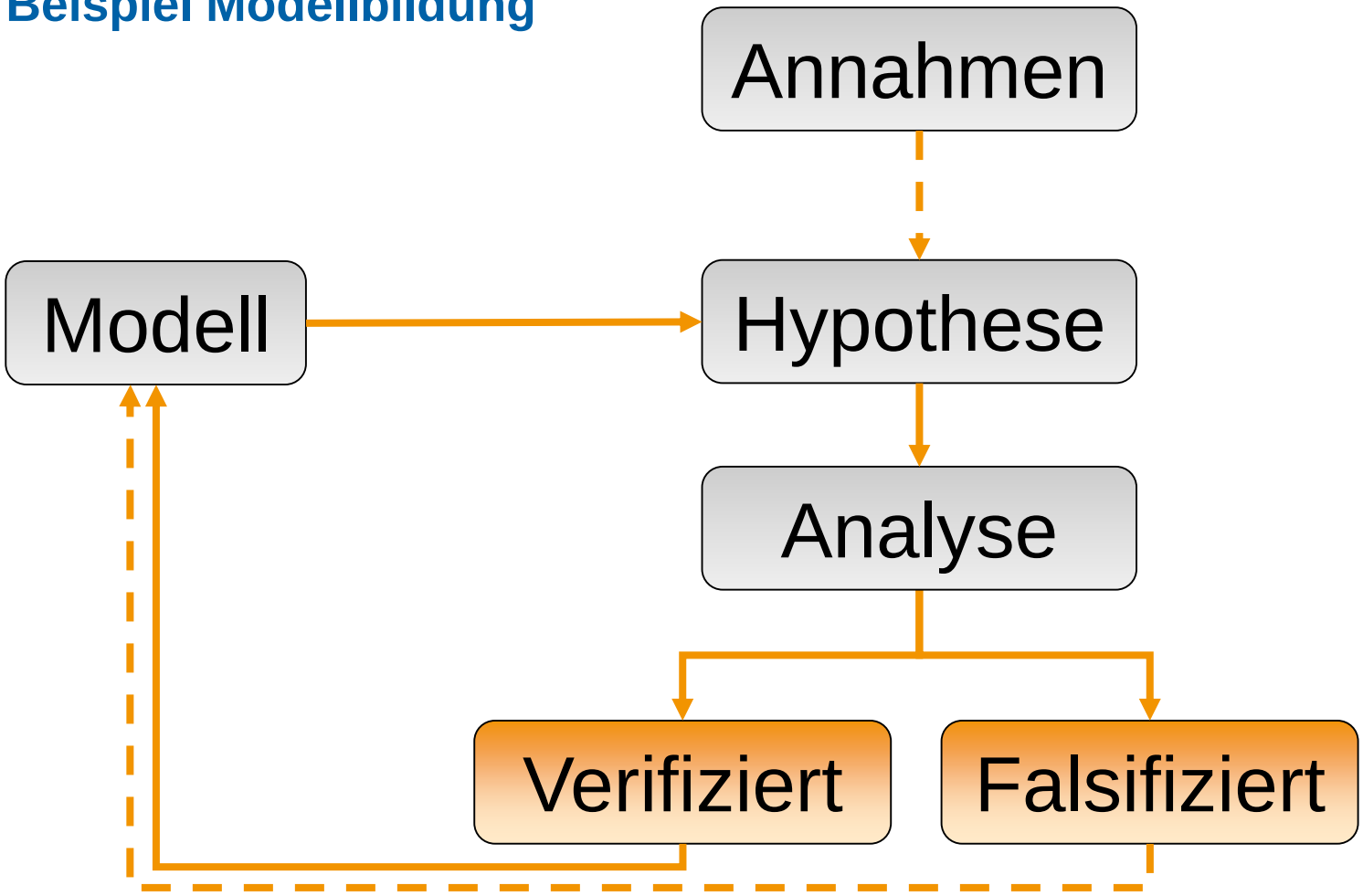
Analyse

Wert (dezimal)	Binärdarstellung			Bedeutung
256	0001	0000	0000	Einschalten (Gerät am Ladestrom)
257	0001	0000	0001	GSM-Ereignis (Gerät am Ladestrom)
258	0001	0000	0010	Ladestrom anschalten (Display ist an)
259	0001	0000	0011	Display anschalten (Gerät am Ladestrom)
512	0010	0000	0000	Einschalten (Kein Ladestrom)
513	0010	0000	0001	Ladestrom ausschalten (Display ist an)
514	0010	0000	0010	GSM-Ereignis (Kein Ladestrom)
516	0010	0000	0100	Display anschalten (Kein Ladestrom)
768	0011	0000	0000	Einschalten leerer Akku (Gerät am Ladestrom)
769	0011	0000	0001	Display ausschalten (Gerät am Ladestrom)
771	0011	0000	0011	Leerlauf (Gerät am Ladestrom)
772	0011	0000	0100	Ladestrom anschalten (Display ist aus)
1026	0100	0000	0010	Display ausschalten (Kein Ladestrom)
1027	0100	0000	0011	Ladestrom ausschalten (Display ist aus)
1028	0100	0000	0100	Leerlauf (Kein Ladestrom)

Analyse

Wert (dezimal)	Binärdarstellung			Bedeutung
256	0001	0000	0000	Einschalten (Gerät am Ladestrom)
257	0001	0000	0001	GSM-Ereignis (Gerät am Ladestrom)
258	0001	0000	0010	Ladestrom anschalten (Display ist an)
259	0001	0000	0011	Display anschalten (Gerät am Ladestrom)
512	0010	0000	0000	Einschalten (Kein Ladestrom)
513	0010	0000	0001	Ladestrom ausschalten (Display ist an)
514	0010	0000	0010	GSM-Ereignis (Kein Ladestrom)
516	0010	0000	0100	Display anschalten (Kein Ladestrom)
768	0011	0000	0000	Einschalten leerer Akku (Gerät am Ladestrom)
769	0011	0000	0001	Display ausschalten (Gerät am Ladestrom)
771	0011	0000	0011	Leerlauf (Gerät am Ladestrom)
772	0011	0000	0100	Ladestrom anschalten (Display ist aus)
1026	0100	0000	0010	Display ausschalten (Kein Ladestrom)
1027	0100	0000	0011	Ladestrom ausschalten (Display ist aus)
1028	0100	0000	0100	Leerlauf (Kein Ladestrom)

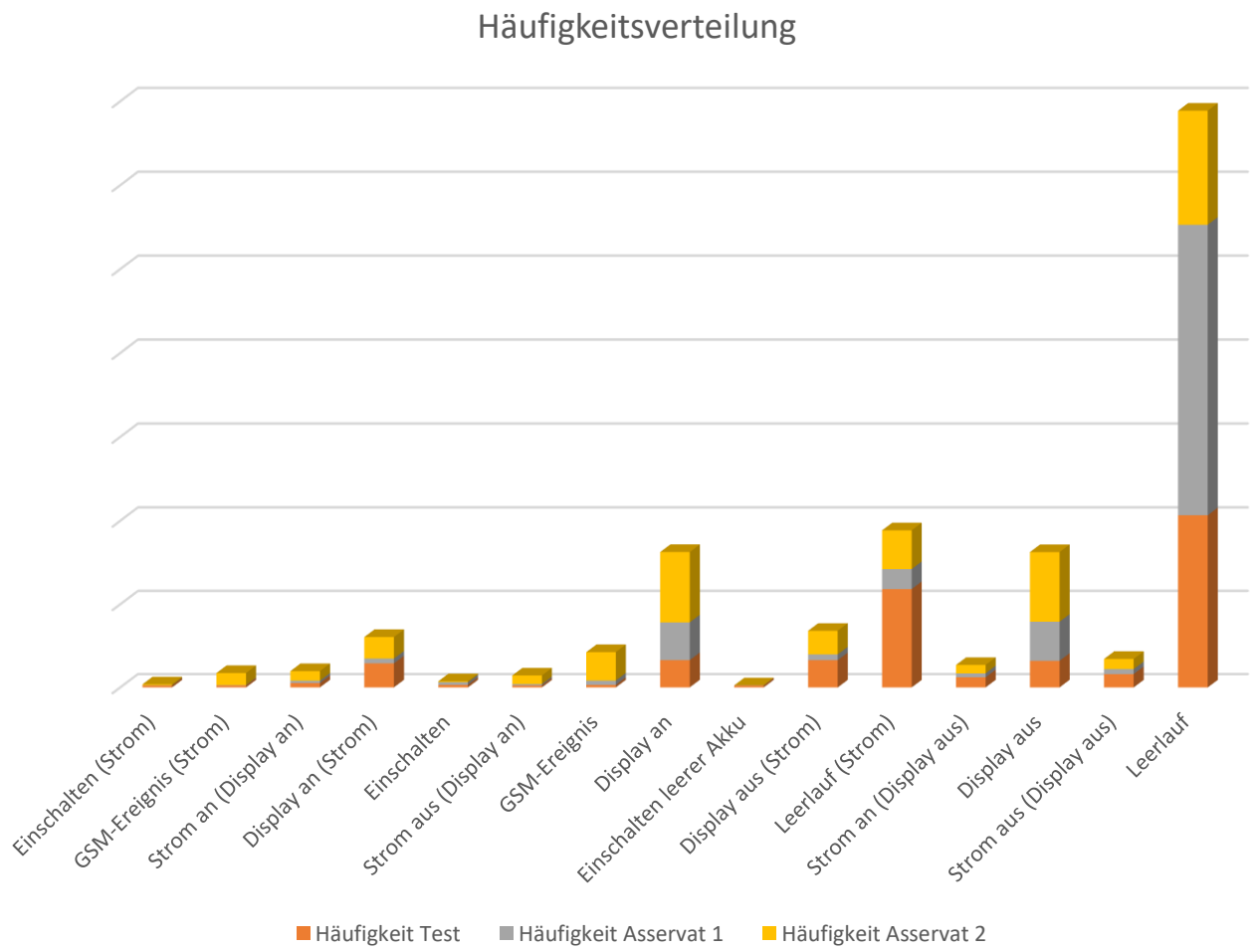
Beispiel Modellbildung



Verifikation und Falsifizierung

- Verifikation
  - Ein-/Ausschalten
  - Display Ein/Aus
  - Es gibt ein GSM-Ereignis
  - Bits haben eine Bedeutung
- Falsifizierung
  - Bluetooth, Kamera, Netzwert, Mobile Daten usw. spielen keine Rolle
  - Keine Bitmaske

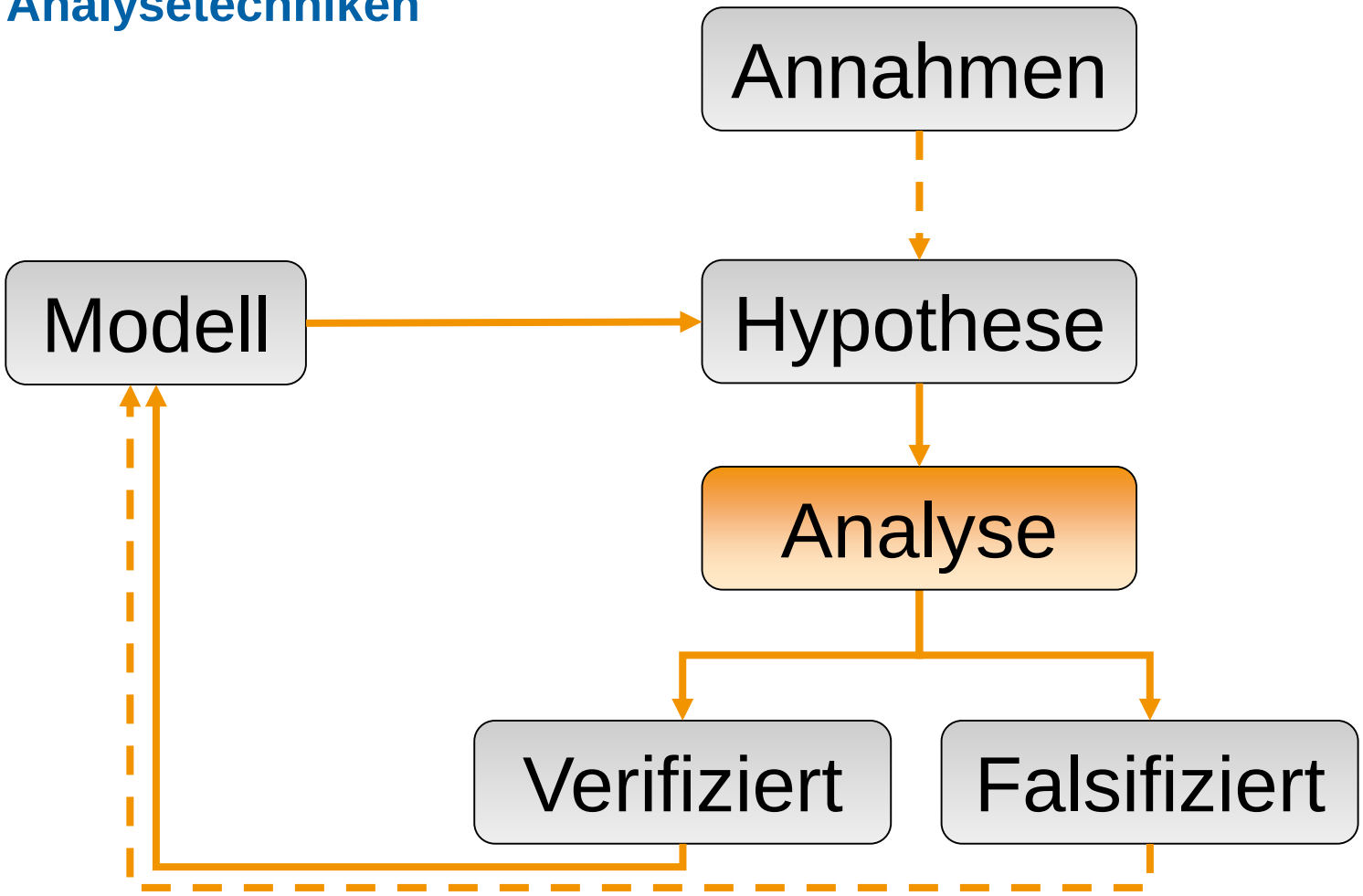
Plausibilitätsprüfung



Überblick

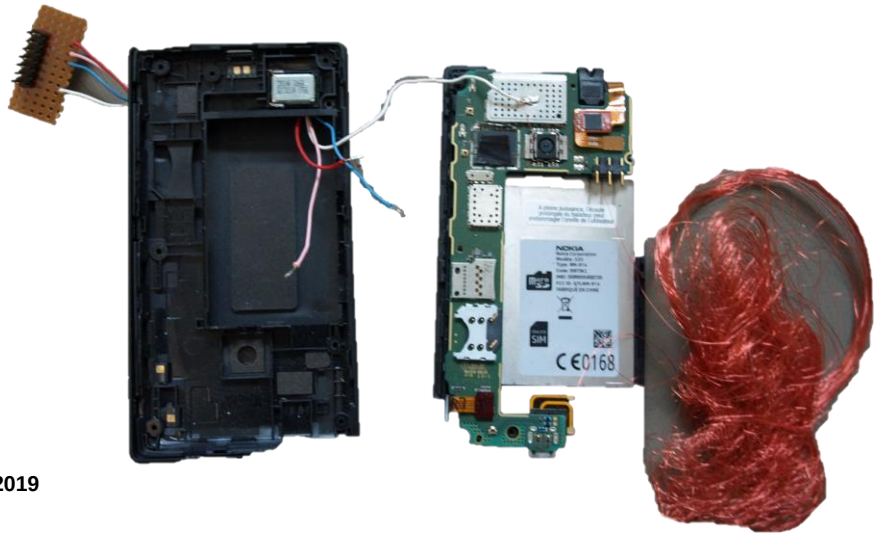
- Grundlegendes Vorgehen
  - Modell, Hypothese, Analyse
  - Beispiel
- Analysetechniken
  - Der Weg zum Image
  - Die eigene Mobilfunkzelle
  - Dotnet-Decompiler
- Zusammenfassung

Analysetechniken



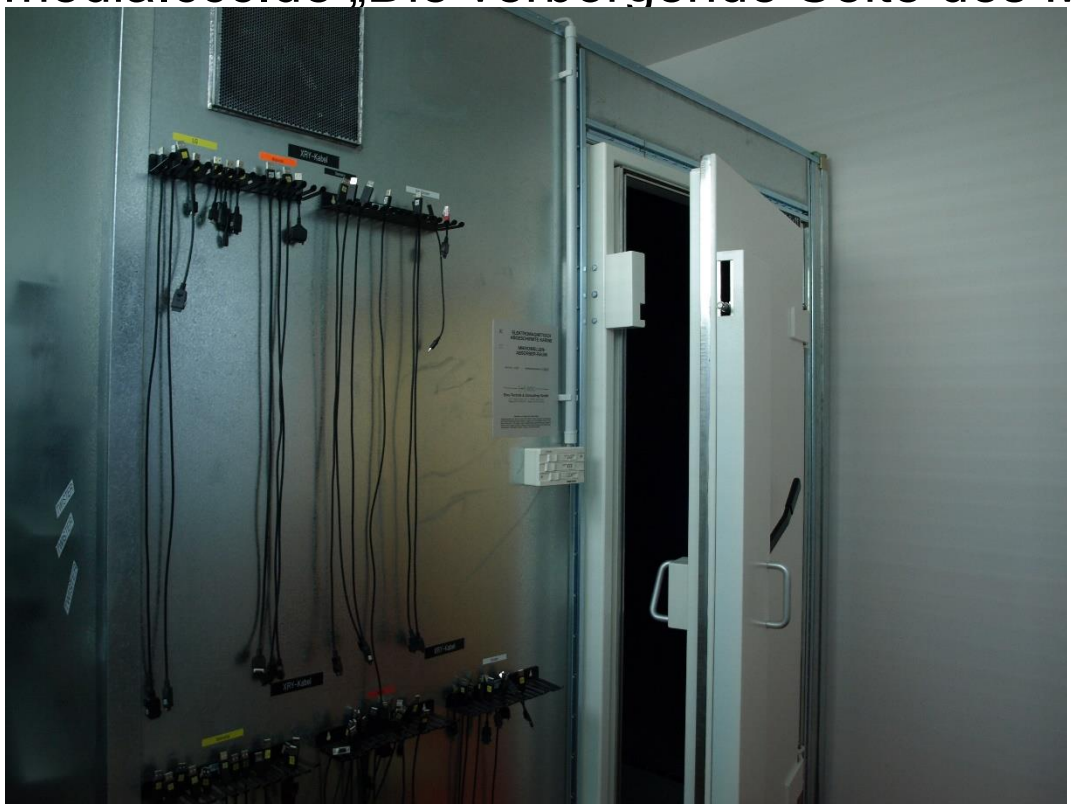
Datensicherung

- Beim Asservat, häufig Chipoff
- Vergleichsgerät ISP (In System Programming)
- Backups per Software
  - Windows Phone Internals (www.wpinternals.net)
  - Image kann dann mit OSFMount (www.passmark.com) als Laufwerk genutzt werden oder in UFED Physical Analyzer importiert werden



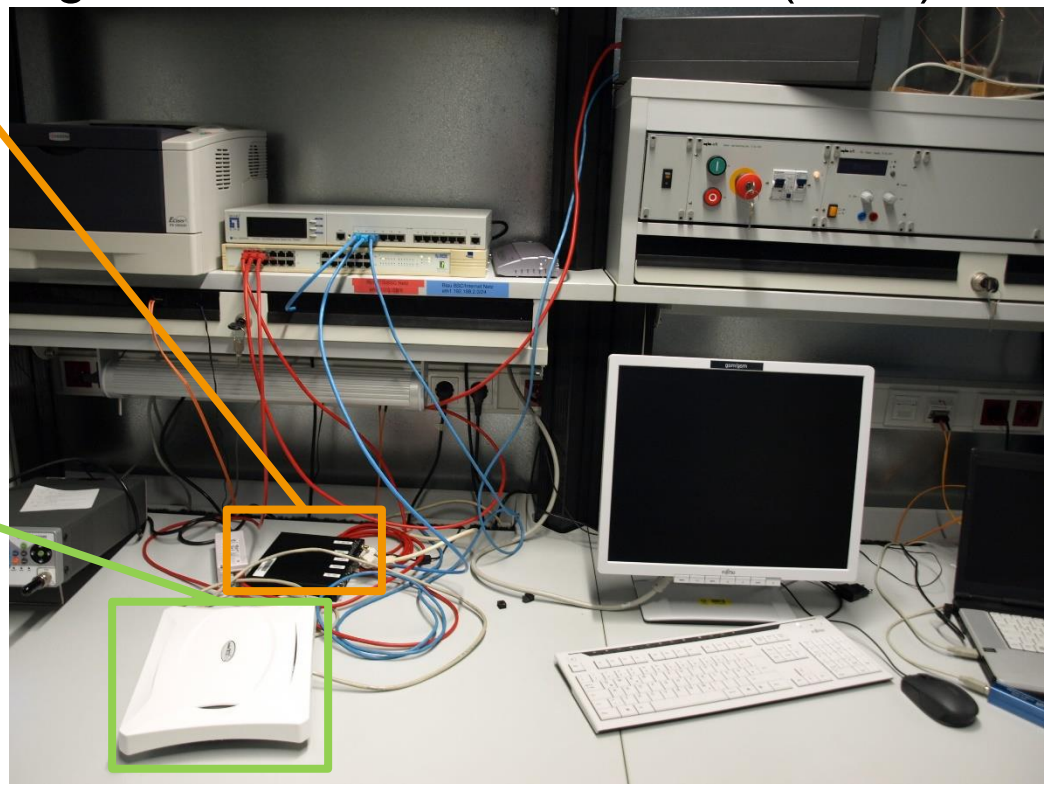
Die eigene Funkzelle

- Bitte nicht nachmachen
  - ➢ media.ccc.de „Die verborgende Seite des Mobilfunks“ (35c3)



Die eigene Funkzelle

- Bitte nicht nachmachen
  - ➢ media.ccc.de „Die verborgende Seite des Mobilfunks“ (35c3)
- Base Station Controller
  - ➢ Zentrale Steuereinheit
  - ➢ Vereinfachtes Setup
  - ➢ Viele weitere Komponenten, wie SMS-Center
- Base Transceiver Station
  - ➢ Senden und Empfangen inkl. Verschlüsselung



Unistore.db

- ESE-Datenbank und Ordner im Dateisystem
  - Anruflisten
  - SMS
  - Email
  - Kalender
  - Kontakte
- Spaltenüberschriften
  - 8-stellige Hex-Werte z.B. 857b0013
- Sehr viele Spalten
  - Tabelle Message: 275, Appointment 52, Contact 161
  - Spalten kommen und gehen auch innerhalb von Windows 10

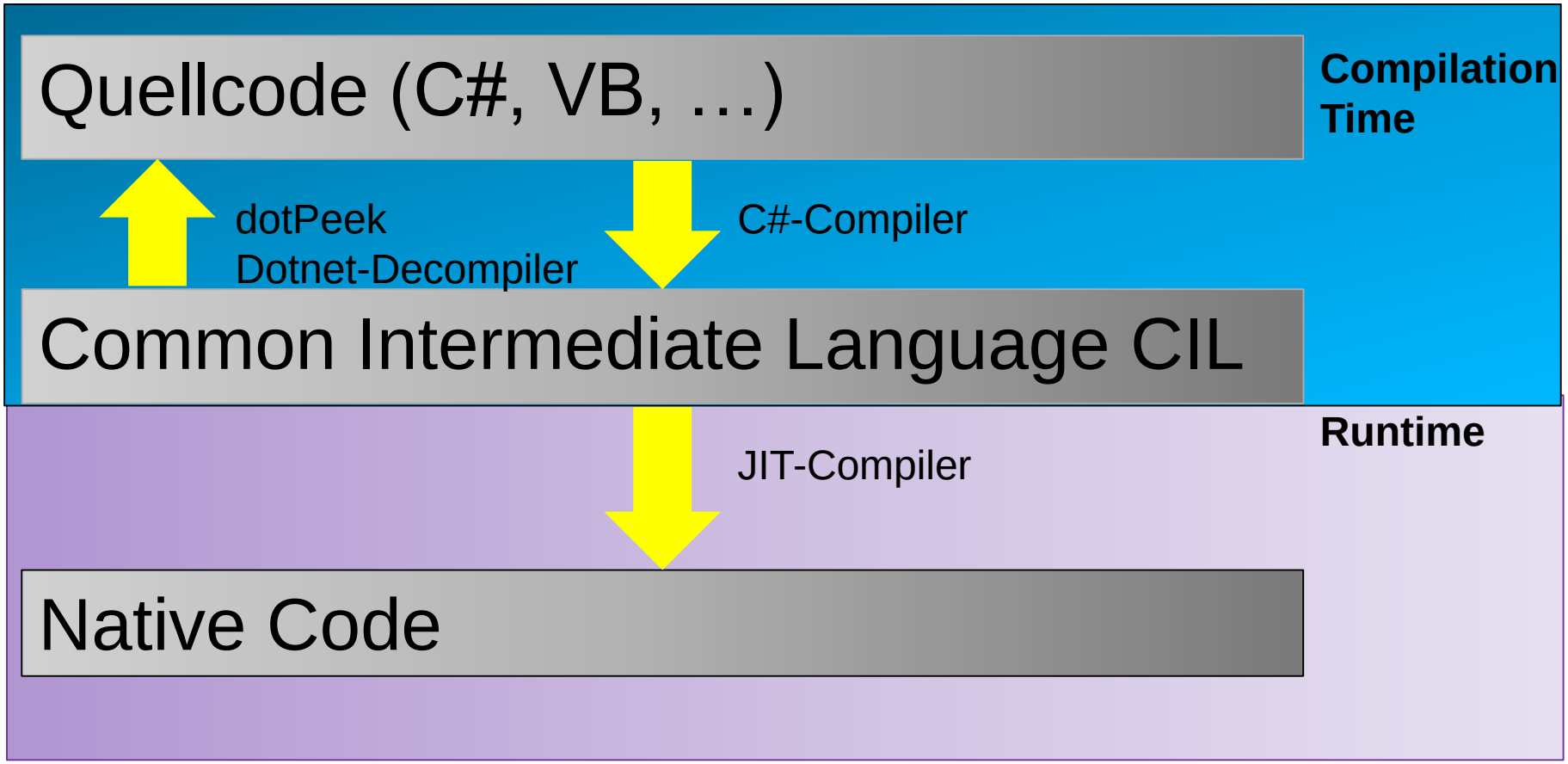
Unistore.db

- Werte können auch Null sein, das geht aber auch anders:

Wert (dezimal)	Wert (hex)	Interpretiert als String
42	2a	*
10794	2a2a	**
707406378	2a2a2a2a	****
3038287259199220266	2a2a2a2a2a2a2a2a	********

- Hexadezimal sieht das schon viel sinnvoller aus
- 2a ist der ASCII-Wert von *
- Es werden auch Werte außerhalb der aktuellen Zeile geändert

Dotnet-Decompiler



WhatsApp

- Gute Zusammenarbeit, insbesondere in großen Projekten ist wichtig
- Android
  - Verschlüsselung AES
  - IV und Salt binär codiert
  - Nachrichten und Anrufe in einer Tabelle
- Windows Mobile
  - Verschlüsselung RC4
  - IV und Salt als JSON codiert
  - Nachrichten und Anrufe in getrennten Tabellen
- Herausforderungen bei der Softwareentwicklung

WhatsApp

```
public enum WhatsAppNachrichtenStatus {
        UnsentOld = 0,
        Uploading = 1,
        Uploaded = 2,
        SentByClient = 3,
        ReceivedByServer = 4,
        ReceivedByTarget = 5,
        NeverSend = 6,
        ServerBounce = 7,
        Undefined = 8,
        Unsent = 9,
        Error = 10, // 0x0000000A
        PlayedByTarget = 11, // 0x0000000B
        ObsoletePlayedByTargetAcked = 12, // 0x0000000C
        Canceled = 14, // 0x0000000E
        Relay = 15, // 0x0000000F
        UploadingCustomHash = 16, // 0x00000010
        Downloading = 17, // 0x00000011
        ReadByTarget = 18, // 0x00000012
        ObsoleteReadByTargetAcked = 19, // 0x00000013
        Pending = 20, // 0x00000014
    }
```

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

Überblick

- Grundlegendes Vorgehen
  - Modell, Hypothese, Analyse
  - Beispiel
- Analysetechniken
  - Der Weg zum Image
  - Die eigene Mobilfunkzelle
  - Dotnet-Decompiler
- Zusammenfassung

Zusammenfassung

- Auswertesoftware für Windows Mobile (10, zum Teil auch 8)
  - SRUM
    - Energieverbrauch
    - Netzwerkaktivität, Laufende Prozesse und Anwendungen
  - Unistore.db
    - Anruflisten, Kontakte, Kalender, Mails, SMS, MMS
  - WhatsApp
    - Chats (Aktuell und Backup)
  - Basisdaten
    - Modell, IMEI, Installierte Software, …
  - PIN und Passwörter
    - PIN (nur Windows 8), WLAN-Passwörter, und vieles mehr

Vielen Dank für Ihre Aufmerksamkeit.