FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Automobil-Forensik mit Berla iVe

Jens Born, B.Sc.

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

Gliederung

- Einleitung
- Über Berla und iVe
- Infotainmentsysteme
- Datenerfassung
- Datenanalyse
- Zusammenfassung

Einleitung

- Welche Daten sind in einem Infotainmentsystem enthalten?
- Wie können die Daten ausgelesen werden?
- Können die Daten gelöscht werden?

Über Berla und iVe

- 2008 gegründet
- Firmensitz in Maryland, USA
- Spezialisiert auf digitale Forensik

- Erstes Produkt: Blackthorn
  - 2009 veröffentlicht
  - Luft- und Seefahrt GPS-Geräte
  - Für mobile GPS Geräte
    - Garmin, TomTom etc.

Über Berla

- Zweites Produkt: iVe
- Forensische Untersuchungen von Infotainmentsystemen
  - BMW, Chevrolet, Chrysler, Fiat, Ford, Jeep, Maserati, Pontiac, Toyota, Volkswagen, etc.
- Auslesen von Daten
- Analysieren der Daten
  - Kontakte, Rufnummern, SMS-Nachrichten
  - Navigationsdaten

Infotainmentsysteme

- BMW Car Information Computer (CIC)
  - Einführung Mitte 2008
  - QNX Neutrino Betriebssystem
  - Unix ähnliches Echtzeitbetriebssystem
- Ford SYNC (Generation) 2
  - Verbaut ab 2010
  - Windows Embedded Automotive

Infotainmentsysteme

- Toyota Touch&Go
  - QNX Neutrino Betriebssystem

- Volkswagen RNS 510
  - VxWorks von Wind River Systems
  - Echtzeitbetriebssystem
  - Mit Java Frontend

Datenerfassung

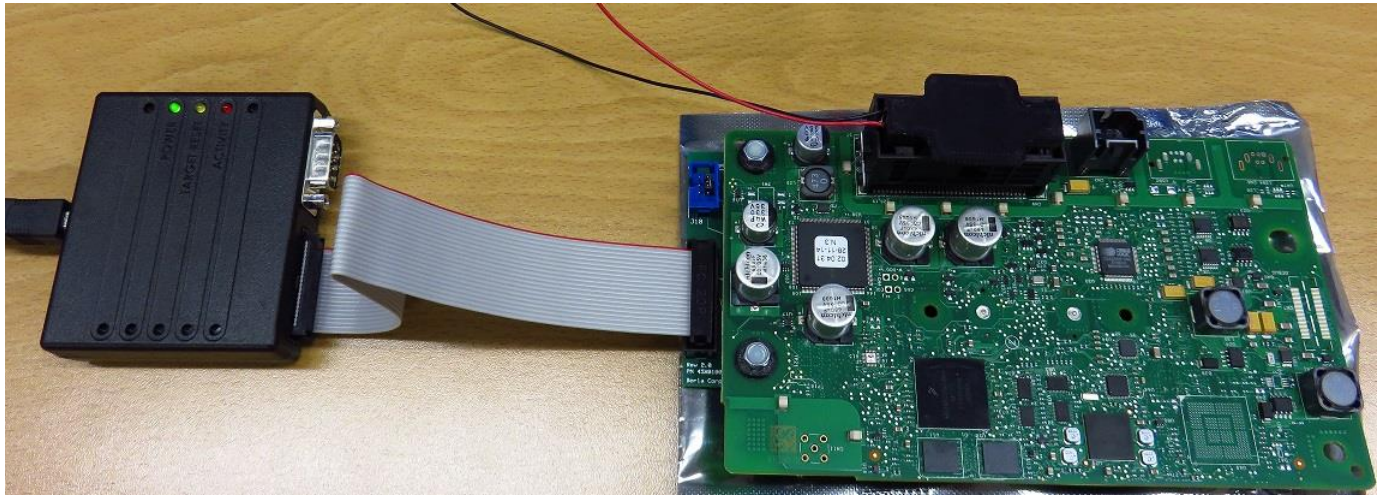
- Assistent zum Durchführen des Auslesevorgangs
- Verbindung zum System testen
  - Erst bei erfolgreichem Test, kann fortgefahren werden
- Eingabe weiterer Daten zur Protokollierung
  - Fallname, -nummer
  - Welches Auto? Welches System?
  - Ortsangabe
  - Weitere Details

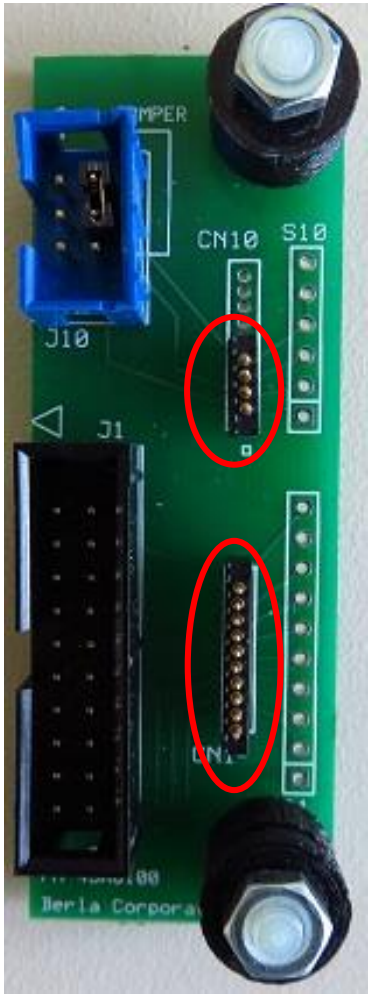
Datenerfassung

- BMW CIC und Toyota Touch&Go
- Verbindung über USB-Ethernet-Adapter

Datenerfassung

- Ford SYNC 2
  - Kompletter Ausbau der Haupteinheit
  - Verbinden mit einer zusätzlichen Platine
  - Verbindung zum Notebook über einen weiteren Adapter





Datenerfassung

- Art und Dauer unterschiedlich
  - USB
  - JTAG
- 10 Minuten bis 5 Stunden
  - Toyota Touch&Go: ca. 10 Min.
  - Ford SYNC 2: ca. 5 Stunden

Datenanalyse

- Mitlesen der Datenverbindung (Wireshark)
- BMW CIC: Verbindung zu einem FTP-Server

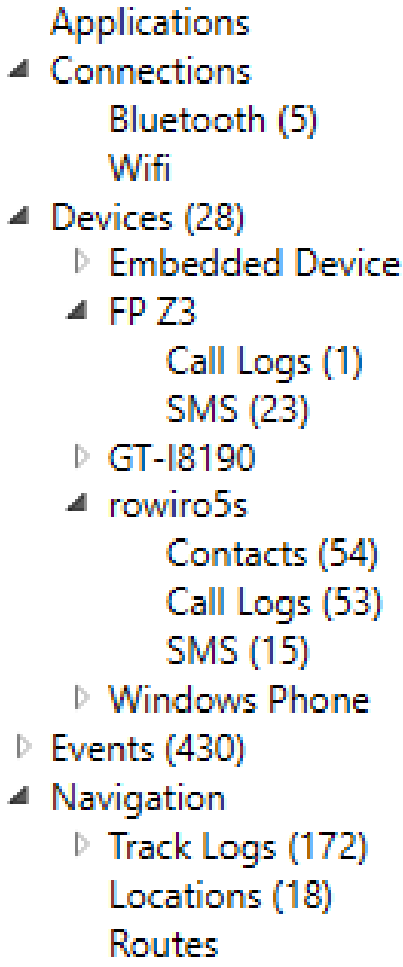
No.	Time	Source	Destination	Protocol	Lengt	Info
612	137.94…	160.48.199.99	160.48.199.10	FTP	91	Response: 220 160.48.199.99 FTP server ready.
613	137.95…	160.48.199.10	160.48.199.99	FTP	65	Request: USER root
614	137.95…	160.48.199.99	160.48.199.10	FTP	87	Response: 331 Password required for root.
615	137.95…	160.48.199.10	160.48.199.99	FTP	68	Request: PASS [redacted]
616	137.96…	160.48.199.99	160.48.199.10	FTP	80	Response: 230 User root logged in.

- Toyota Touch&Go: Telnet Session

```
QNX Neutrino (localhost) (ttyp1)
login: ...root
Password:[redacted]
```

Ermittelte Daten

- iVe listet Ergebnisse auf
  - Applications
  - Connections
  - Devices
  - Events
  - Navigation
- Übersichtlich
- Eigenes Durchschauen der Daten sinnvoll



Ermittelte Daten

- Abhängig vom Infotainmentsystem
- Abhängig von der Benutzung

- Informationen aus dem Multimediasystem
  - Abgespielte CD‘s, MP3‘s
  - ID3-Tag‘s

Ermittelte Daten

- Verbindungsdaten von Smartphones
  - Bluetooth Adresse
  - Gerätename, -hersteller

Tag	Device Name	Device Type(int	Device Type	Unique Number	Unique Number Type	Manufacturer
⊞	Thomas	Phone	Phone	EC88	Bluetooth Address	UNDEFINED
⊞	Marc	Phone	Phone	1030	Bluetooth Address	SAMSUNG
⊞	Xperia S	Phone	Phone	3039	Bluetooth Address	UNDEFINED
⊞	Xperia Active	Phone	Phone	1C45	Bluetooth Address	UNDEFINED
⊟	J B (Galaxy S4 Active)	Phone	Phone	00E3	Bluetooth Address	UNDEFINED

Key	Value
mediafs2wire	00:E3
mssname	mediafs2wire
Last Seen	05.02.2016 12:38:10
Phone Version	UNDEFINED
TimezoneOffset	+01:00

Abbildung: Toyota Touch&Go

Ermittelte Daten - Kontaktdaten

- BMW CIC
  - Gespeichert in „contactbook_<DATUM>.db“
  - Enthält Kontaktdaten, Rufnummern, E-Mail-Adressen
  - Keine SMS, Anrufliste
  - BT_Adresse zur Zuweisung des Smartphones in „contactbook“

Ermittelte Daten - Kontaktdaten

- Ford SYNC 2
  - Speichert verbundene Geräte in „devices.sqlite“
  - Kontakte, Anrufliste gespeichert in „PhoneBook_<BT_Adresse>.sqlite“
  - Nachrichten in „SMS_<BT_Adresse>.db“

Tag	First Name	Last Name	Work Number	Home Number	Mobile Number
☐	F	Kr	053		0178
☐	F	We	060	49163	0160
☐	F	No	+329		+324

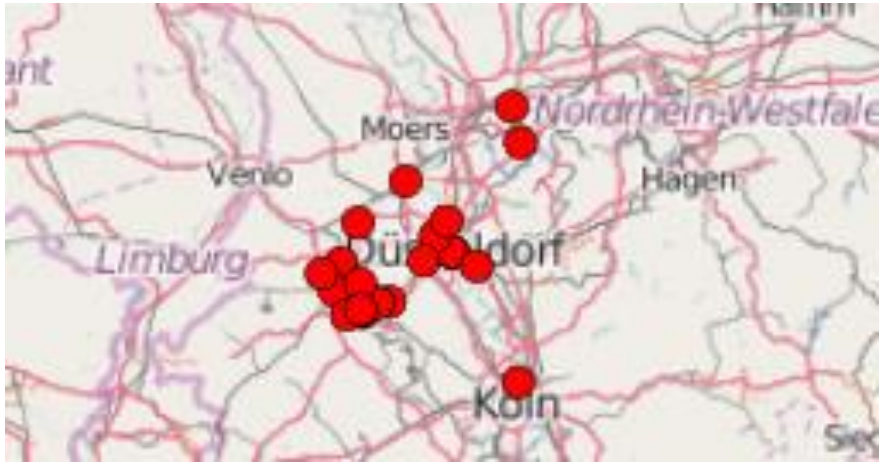
Ermittelte Daten - Kontaktdaten

- Toyota Touch&Go
  - Geräte gespeichert in „PimMgr.dbf“
  - Legt Datenbanken für verschiedene Funktionen an
  - „pmX0000XX.dbf“
    - „pm10000XX.dbf“: Kontakte
    - „pm20000XX.dbf“: Kalender
    - „pm80000XX.dbf“: Anrufliste

TIMESTAMP	PIM_OBJECT_TYPE	FILENAME
05.02.2016 13:38:05	2	pm2000029
05.02.2016 13:38:05	3	pm3000030
05.02.2016 13:38:06	1	pm1000031
05.02.2016 13:38:06	5	pm5000032
05.02.2016 13:38:06	7	pm7000033
05.02.2016 13:38:06	4	pm4000034
05.02.2016 13:38:06	8	pm8000035

Ermittelte Daten – BMW CIC

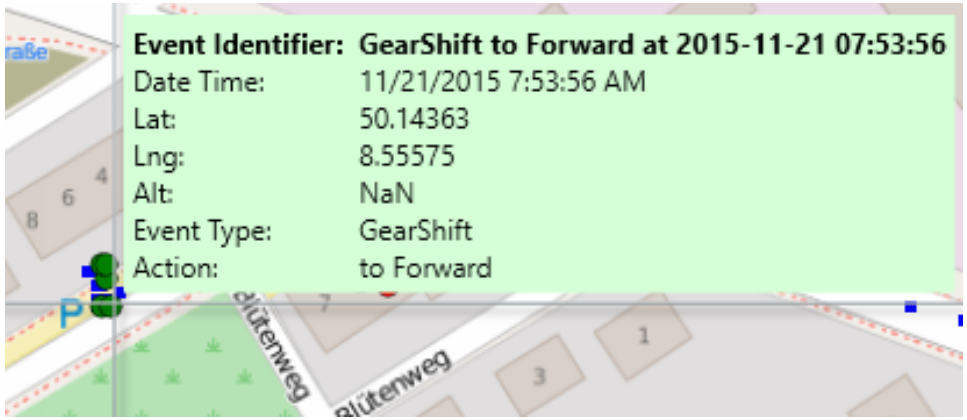
- Ereignisse (Events) beschränken sich auf verbundene Geräte und abgespielte Medien
  - Zeitstempel nicht immer korrekt
- Navigation: Letzte Ziele, Favoriten



Ermittelte Daten – Ford SYNC 2

- Speicherung diverser Events
  - In einer Log-Datei (MsgLog1.txt)
  - Öffnen, Schließen der Fahrer-, Beifahrertür
  - Schaltvorgänge (GearShift to Forward)
  - Verbindungen von Geräten (Bluetooth, USB)
  - Zeitsynchronisationen über GPS

- Alle Ereignisse mit Geo-Tag



Ermittelte Daten – Ford SYNC 2

- Navigation: Letzte Ziele, Favoriten
- Auch abgefahrene Routen
  - Zeitstempel nicht immer korrekt

Date/Time	Bearing	TrackName	Distance	Latitude	Longitude
21.11.2015 07:54:00	18°	Recovered0057	5,65 m	50,143650000	8,555770000
21.11.2015 07:54:01	18°	Recovered0057	11,31 m	50,143670000	8,555830000
21.11.2015 07:54:02	26°	Recovered0057	11,98 m	50,143700000	8,555890000
21.11.2015 07:54:03	23°	Recovered0057	13,61 m	50,143730000	8,555960000

Ermittelte Daten – Toyota T&G

- Navigation: Letzte Ziele, Favoriten
- Ereignisse
  - Abgespielte Medien
  - Verbundene Geräte
    - Auch die Verbindung des Notebooks

Tag	Device Name	Device Type(int	Device Type	Unique Number	Unique Number Type
⊟ ☐	INTERNET			/dev/socket	Internet Socket

Key	Value
mssname	internet
Last Seen	05.02.2016 12:49:59

Löschen der Daten – BMW CIC

- Navigationsziele können gelöscht werden

- Löschen der Smartphone Daten erfolgreich
  - „contactbook_<DATUM>.db“ wird gelöscht
  - Altes Telefonbuch im Dateisystem gefunden
    - Nicht für den Benutzer sichtbar
    - Vermutlich Rückstände einer alten Version

- Über iVe nicht mehr auffindbar

Löschen der Daten – Ford SYNC 2

- Navigationsziele können gelöscht werden
- Löschen der Smartphone Daten erfolgreich
  - Keine Kontakte, Nachrichten, Anruflisten
- Über iVe nicht mehr auffindbar

Löschen der Daten – Toyota T&G

- Navigationsziele können gelöscht werden

- Löschen der Smartphone Daten nicht erfolgreich
- Einträge in „PimMgr.dbf“ entfernt
  - „pmX0000XX.dbf“ immer noch im System vorhanden
  - Zuweisung zum richtigen Smartphone fehlt
  - Daten immer noch im System vorhanden

Datenanalyse

- Volkswagen RNS 510

- Datenanalyse nicht erfolgreich
- Zu viele Fehler aufgetreten
  - Datenbank für Telefonbuch nicht lesbar
  - Datenbank für Nachrichten nicht lesbar
  - Keine Navigationsdaten

Zusammenfassung

- Informationsgehalt ist groß
- Zum Teil einfacher Zugang zu den Daten
- Viele verschiedene Systeme, schwer alle zu unterstützen
- QNX bei Herstellern beliebt
  - Ford SYNC 3 mit QNX

Viele Dank für Ihre Aufmerksamkeit!

Kontakt:

jens.born@alumni.fh-aachen.de