Möglichkeiten und Grenzen der digitalen Forensik

Kriminalistisches Institut, Wintersemester 2015

Forensisches Institut Zürich
Eine Organisation der Kantonspolizei und Stadtpolizei Zürich

Jörg Arnold dipl. phys. ETHZ
Fachbereichsleiter Unfälle/Technik
Andreas Leu, Automobil-Ing. FH
Experte Unfallanalytik

Möglichkeiten und Grenzen der digitalen Forensik

Kriminalistisches Institut, Wintersemester 2015

Zeit/Ort:	Dienstag, 20. Januar 2015, Freitag, 23. Januar 2015, Theatersaal, Universität Irchel
Referent:	Steffen Görlich, MSc Computer Forensics, DC TEU-ICT

Kanton Zürich
Direktion der Justiz und des Innern
Strafverfolgung Erwachsene

Möglichkeiten und Grenzen der digitalen Forensik

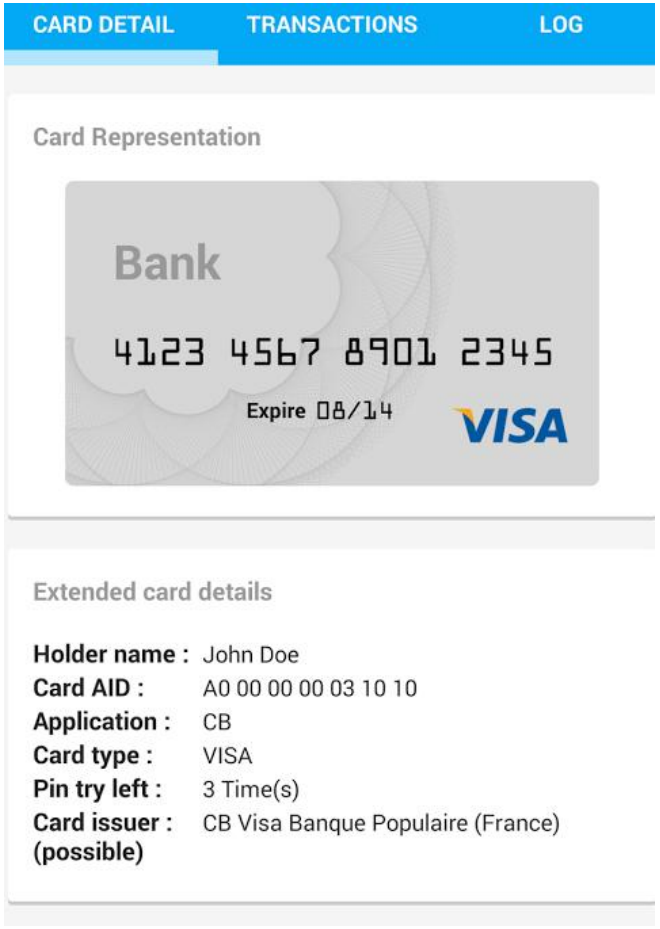
Kriminalistisches Institut, Wintersemester 2015

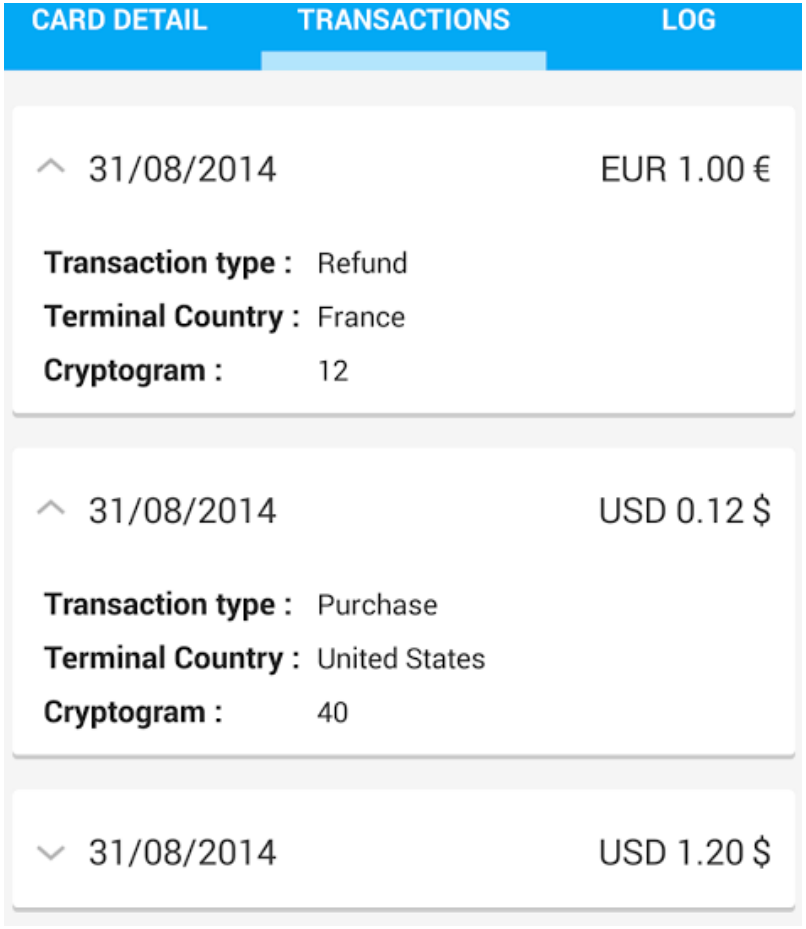
Zeit/Ort:	Dienstag, 20. Januar 2015, Freitag, 23. Januar 2015, Theatersaal, Universität Irchel
Referent:	STA lic.iur. St. Walder, STA II, Abt. D

❶ NFC - Near Field Communication

❶ NFC - Near Field Communication

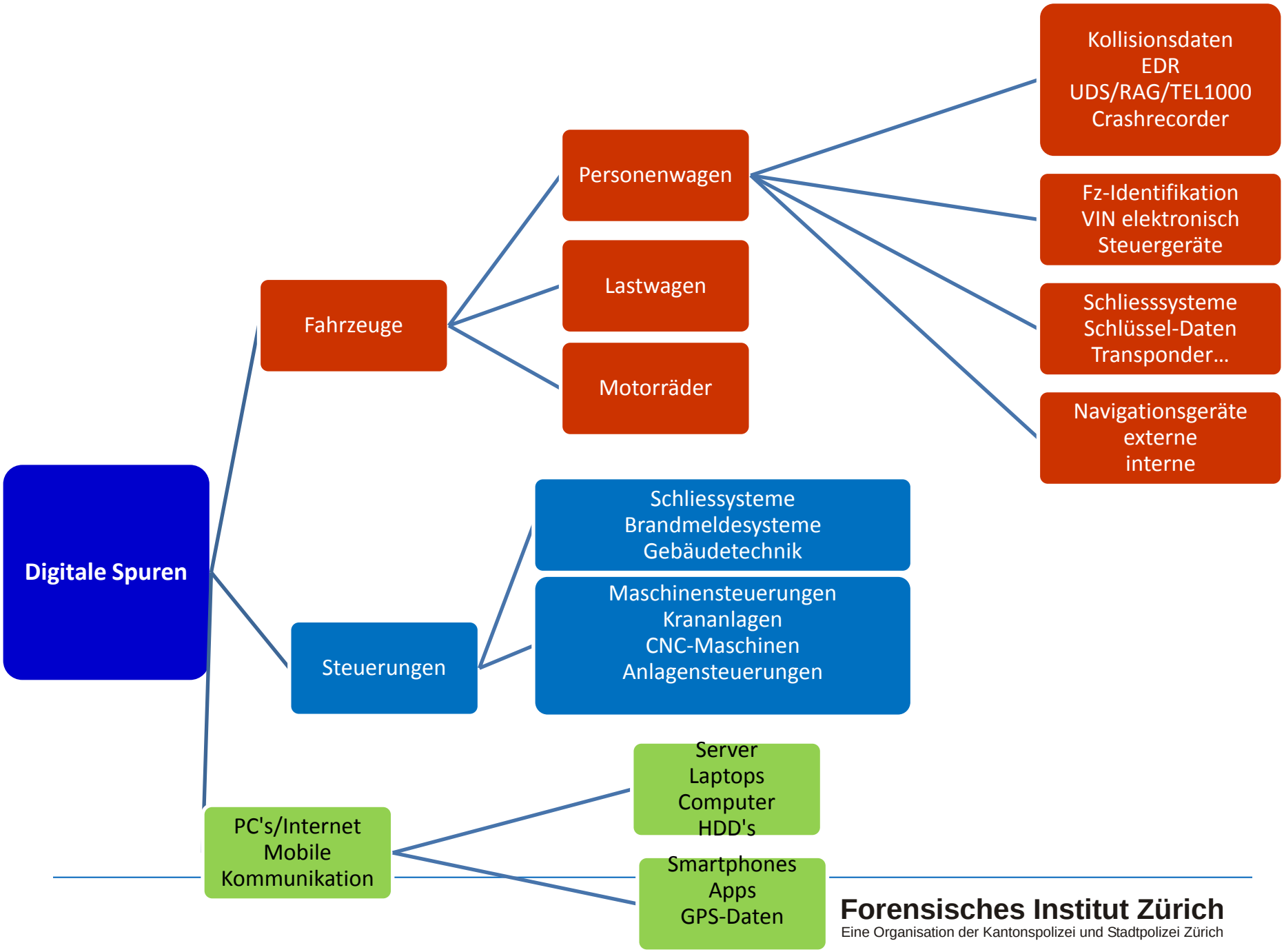
▶ App Banking Card Reader





Digitale Spuren ← → Aufzeichnungen

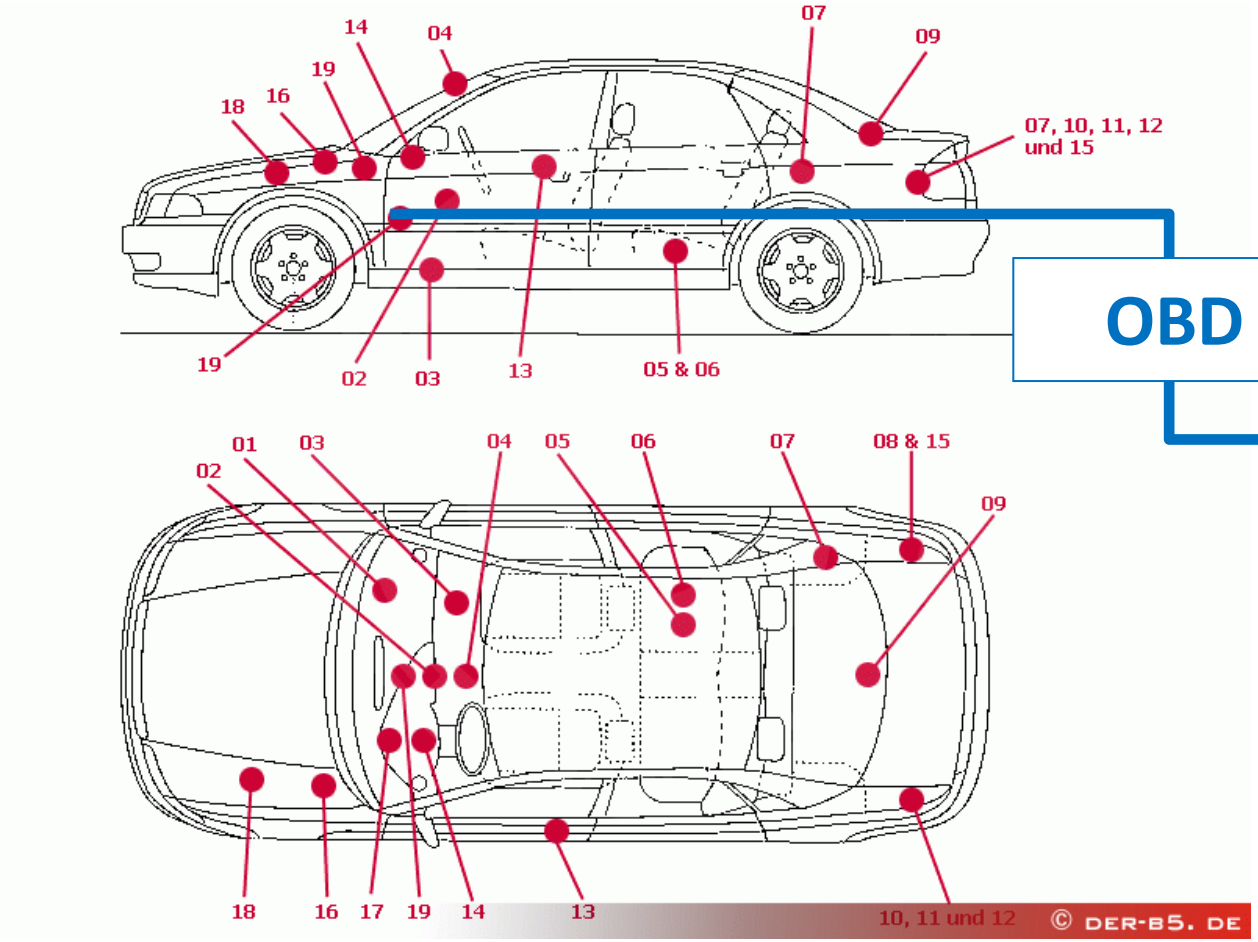
- Digitale Spuren in Fahrzeugen
- Aufzeichnungsgeräte (DFS, RAG, UDS, TEL1000, Jupiter, …… VTS Art. 100 und Art. 102)
- Videoaufzeichnungen (SatSpeed, Semista, Tunnels, Gebäude, DashCams, z. B. 2014 Corvette C7, ……)
- EDR (EventDataRecorders) und CDR-Kit
- Seitenblick in die StPO


Digitale Spuren
Fahrzeuge
Personenwagen
Lastwagen
Motorräder
Kollisionsdaten
EDR
UDS/RAG/TEL1000
Crashrecorder
Fz-Identifikation
VIN elektronisch
Steuergeräte
Schliesssysteme
Schlüssel-Daten
Transponder…
Navigationsgeräte
externe
interne
Steuerungen
Schliessysteme
Brandmeldesysteme
Gebäudetechnik
Maschinensteuerungen
Krananlagen
CNC-Maschinen
Anlagensteuerungen
PC's/Internet
Mobile
Kommunikation
Server
Laptops
Computer
HDD's
Smartphones
Apps
GPS-Daten

Datenspeicherung in Fahrzeugen

- Digitale Spuren in Steuergeräten
  - Daten des Steuergerätes (VIN-Nummer, Seriennummer, Produktion etc.)
  - Fehlercodes mit Umgebungsdaten
  - Schlüssel und Schliessdaten
  - Servicedaten
- Navigationsdaten
- etc., etc.

Steuergeräte / Spuren sichern



OBD II Schnittstelle

EDR-Daten in Pw's (NHTSA 49 CFR part 563)

- **Ab 01.01.2013 USA/Kanada:**
  Alle neuen und neu importierten Fahrzeuge (inkl. aus Asien und Europa), die über EDR verfügen, **müssen** diesem Gesetz entsprechen

- **EDR: Event Data Recorder**
  Baustein im ACM (Airbag Control Module) vorhanden ➔ Kostet ca. 2 $
  Enthält vorkollisionäre Daten aus dem Airbag Modul nach einem "Crash" oder einem „Beinahe-Crash“

CDR-Kit (BOSCH Crash Data Retrival Kit)

Auslesen über OBDII Schnittstelle (intakte Fahrzeugelektrik)

Bei stark beschädigten Fahrzeugen kann das Steuergerät direkt ausgelesen werden

Dashcams in Fahrzeugen

Spurensicherung ab dem Fahrzeug

- **Nur gemeinsam mit dem Hersteller:**
- Zeitfaktor: Man sollte **sofort** …….!!!
- Digitale Spuren in Steuergeräten
  - Daten des Steuergerätes (VIN-Nummer, Seriennummer, Produktion etc.)
  - Fehlercodes mit Umgebungsdaten?
  - Schlüssel und Schliessdaten?
  - Servicedaten
- Navigationsdaten ???

Interpretation der Spuren

- **Basiert auf den mit dem Hersteller zusammen gesicherten digitalen Spuren!**
- Digitale Spuren in Steuergeräten
  - Daten des Steuergerätes: Verändert?
  - Fehlercodes mit Umgebungsdaten: Kriterien?
  - Schlüssel und Schliessdaten: Kriterien?
  - Servicedaten: Verändert?
- Navigationsdaten ??? Zeitliche Zuordnung?
  Nur geplant oder gefahren?

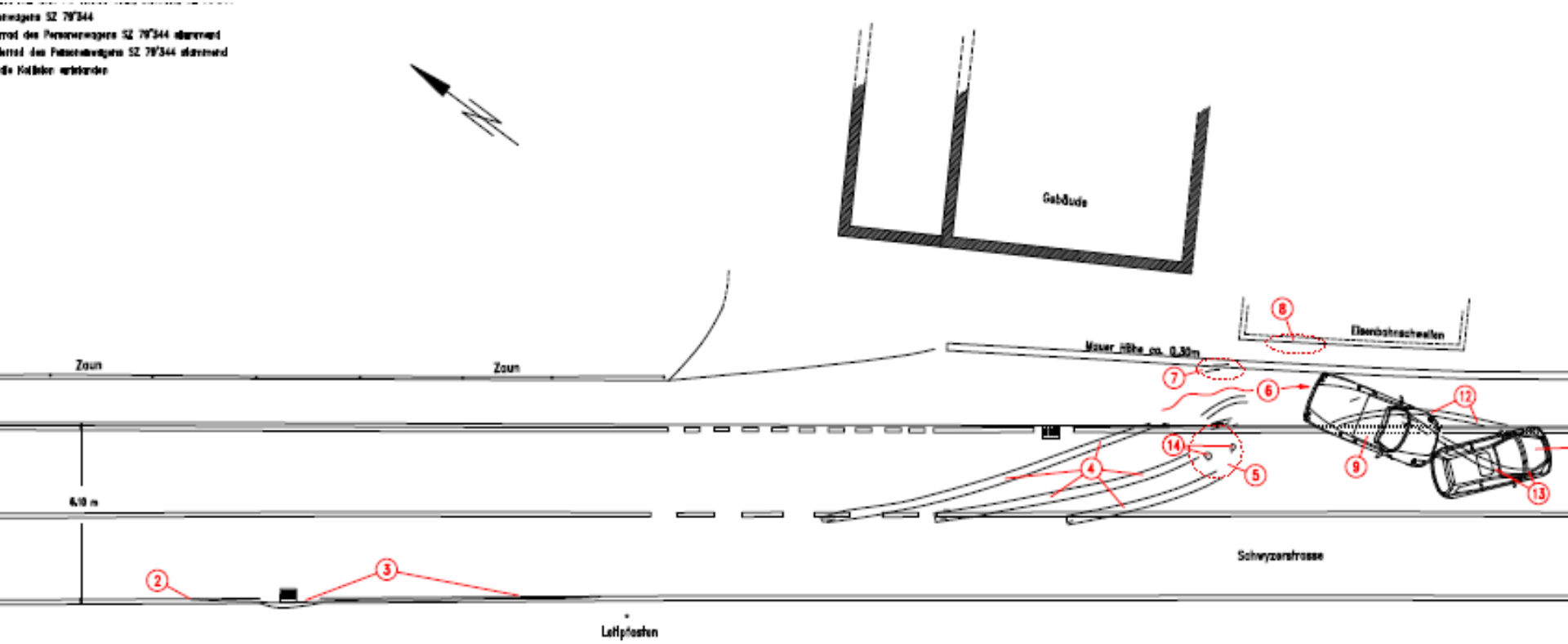
Aktuelle Situation / Fälle?

- **Wie sehen die Bedürfnisse von Polizei und Staatsanwaltschaft oder Gericht aus!**
- Wer löst solche Fälle aktuell mit wem?
- Navigationsdaten ???
- Personelle Ressourcenplanung?
- Prozessuale Fragen: Sicherung
  Durchsuchung
  Auswertung …

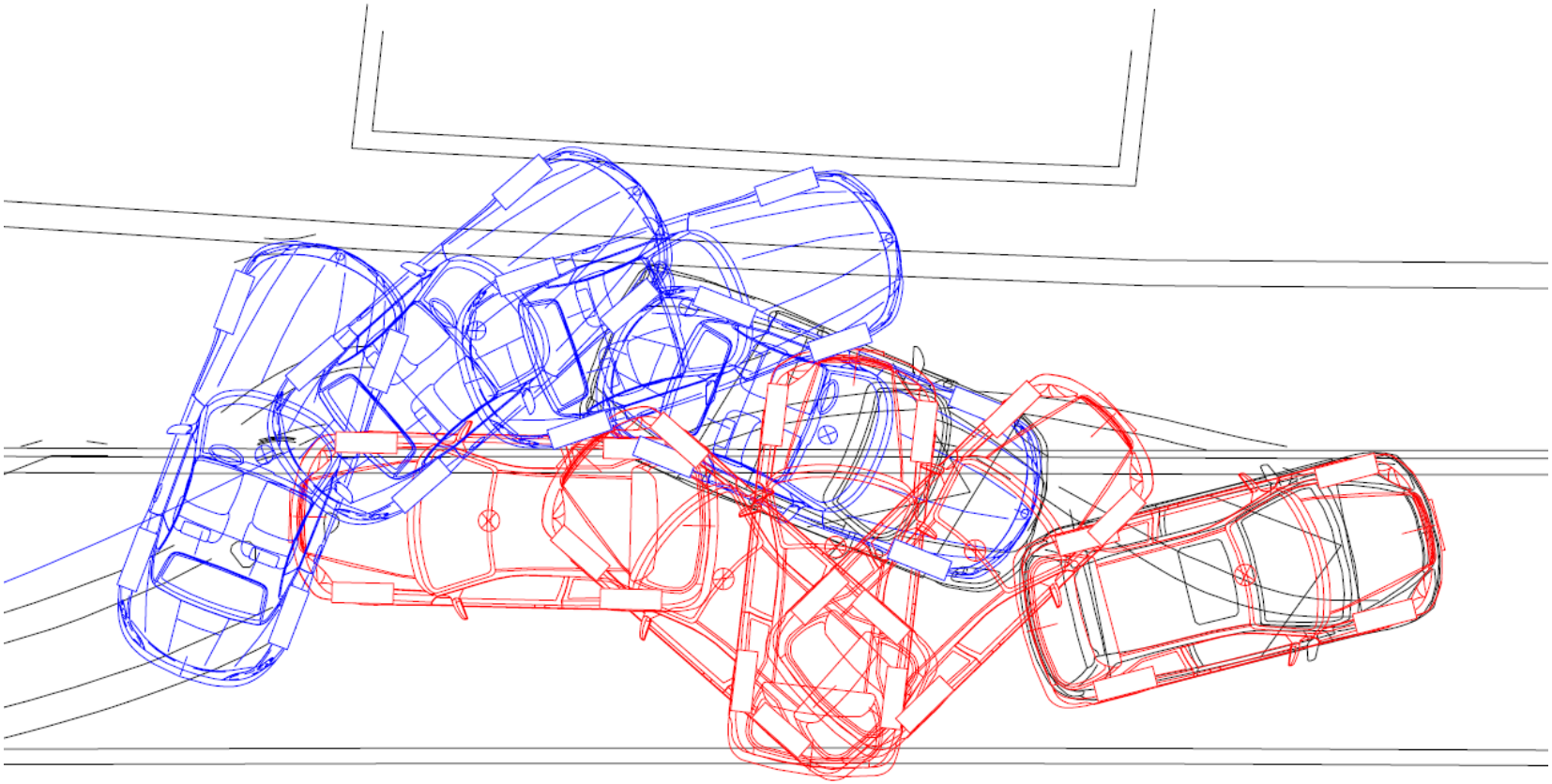
Fallbeispiel: "Corvette Schwyz"

"Corvette Schwyz"

"Corvette Schwyz"



"Corvette Schwyz"



"Corvette Schwyz"

Verfügbare CDR Daten:

BOSCH

CDR CRASH DATA RETRIEVAL

IMPORTANT NOTICE: Robert Bosch LLC and the manufacturers whose vehicles are accessible using the CDR System urge end users to use the latest production release of the Crash Data Retrieval system software when viewing, printing or exporting any retrieved data from within the CDR program. Using the latest version of the CDR software is the best way to ensure that retrieved data has been translated using the most current information provided by the manufacturers of the vehicles supported by this product.

CDR File Information

User Entered VIN	1G1YY26EX65118958
User	Andreas Leu
Case Number	VU Steinen Schwyzerstrasse
EDR Data Imaging Date	08.17.2012
Crash Date	07/21/2012
Filename	1G1YY26EX65118958_ACM.CDRX
Saved on	Freitag, August 17 2012 at 10:44:54
Collected with CDR version	Crash Data Retrieval Tool 6.0
Reported with CDR version	Crash Data Retrieval Tool 6.0
EDR Device Type	Airbag Control Module
Event(s) recovered	Deployment Non-Deployment

Comments

No comments entered.

Data Limitations

Recorded Crash Events:

There are two types of Recorded Crash Events. The first is the Non-Deployment Event. A Non-Deployment Event records data but does not deploy the air bag(s). It contains Pre-Crash and Crash data. The SDM can store up to one Non-Deployment Event. This event can be overwritten by an event that has a greater SDM recorded vehicle longitudinal velocity change. This event will be cleared by the SDM, after approximately 250 ignition cycles. This event can be overwritten by a second Deployment Event, referred to as a Deployment Level Event, if the Non-Deployment Event is not locked. The data in the Non-Deployment Event file will be locked, if the Non-Deployment Event occurred within five seconds before a Deployment Event. A locked Non Deployment Event cannot be overwritten or cleared by the SDM.

The second type of SDM recorded crash event is the Deployment Event. It also contains Pre-Crash and Crash data. The SDM can store up to two different Deployment Events, if they occur within five seconds of one another. If multiple Non-Deployment Events occur within five seconds prior to a Deployment Event, then the most severe Non-Deployment Event will be recorded and locked. If multiple Non-Deployment Events precede a Deployment Event, and occur within five seconds of each other (but not necessarily all within five seconds of the Deployment Event), then the most severe of these Non-Deployment Events (which may have occurred more than five seconds prior to the Deployment Event) will be recorded and locked. If a Deployment Level Event occurs within five seconds after the Deployment Event, the Deployment Level Event will overwrite any non-locked Non-Deployment Event. If multiple Non-Deployment Events occur within five seconds prior to a Deployment Event, and one or more of those events was a Pretensioner Deployment Event, then the most recent Pretensioner Deployment Event will be recorded and locked. Deployment Events cannot be overwritten or cleared by the SDM. Once the SDM has deployed an air bag, the SDM must be replaced.

Data:

-SDM Recorded Vehicle Longitudinal Velocity Change reflects the change in longitudinal velocity that the sensing system experienced during the recorded portion of the event. SDM Recorded Vehicle Longitudinal Velocity Change is the change in velocity during the recording time and is not the speed the vehicle was traveling before the event, and is also not the Barrier Equivalent Velocity. For Deployment Events, the SDM will record 100 milliseconds of data after Deployment criteria is met and up to 50 milliseconds before Deployment criteria is met. For Non-Deployment Events, the SDM can record up to the first 150 milliseconds of data after algorithm enable. Velocity Change data is displayed in SAE sign convention.

-Event Recording Complete will indicate if data from the recorded event has been fully written to the SDM memory or if it has been interrupted and not fully written.

-SDM Recorded Vehicle Speed accuracy can be affected by various factors, including but not limited to the following:

- -Significant changes in the tire's rolling radius
- -Final drive axle ratio changes
- -Wheel lockup and wheel slip

-Brake Switch Circuit Status indicates the open/closed state of the brake switch circuit.

-Pre-Crash data is recorded asynchronously.

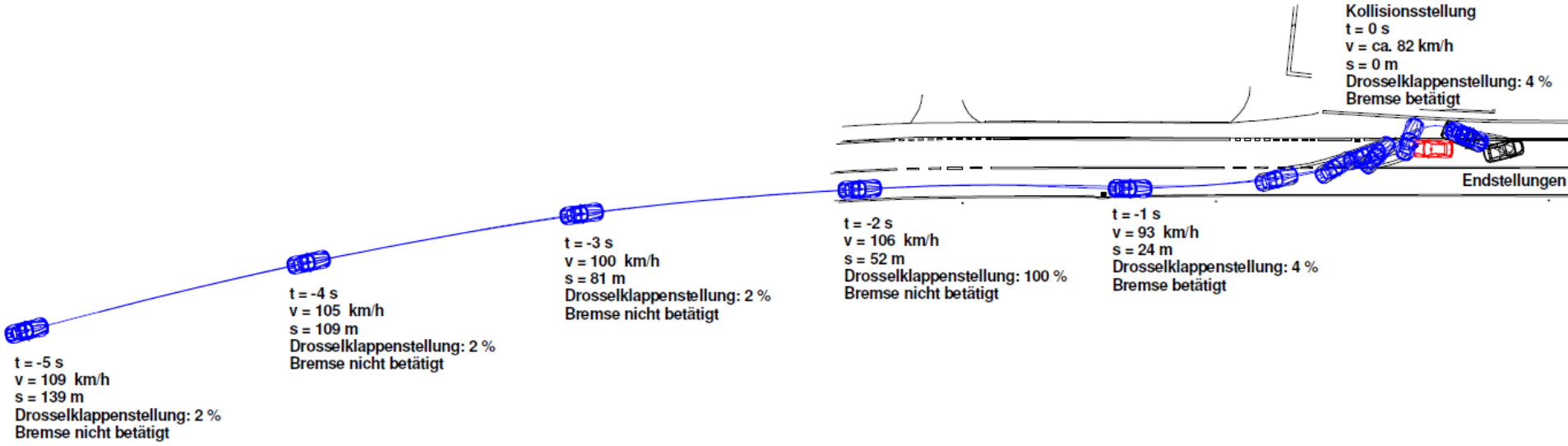
-Pre-Crash Electronic Data Validity Check Status indicates "Data Invalid" if:

- -The SDM receives a message with an "invalid" flag from the module sending the pre-crash data
- -No data is received from the module sending the pre-crash data
- -No module present to send the pre-crash data

-Engine Speed is reported at two times the actual value in the following vehicles, if the vehicle is equipped with a 6.6L Duramax diesel engine (RPO LB7, LBZ, LLY, or LMM):

- -2001-2006 Chevrolet Silverado
- -2007 Chevrolet Silverado Classic
- -2001-2006 GMC Sierra
- -2007 GMC Sierra Classic
- -2006-2007 Chevrolet Express
- -2006-2007 GMC Savana

"Corvette Schwyz"

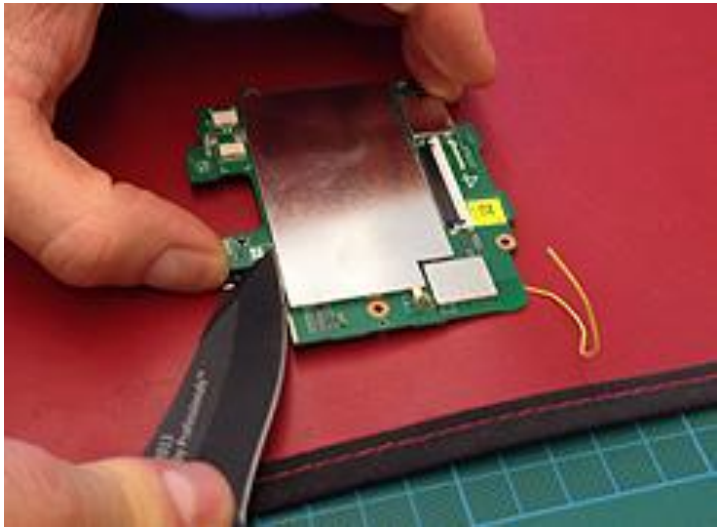


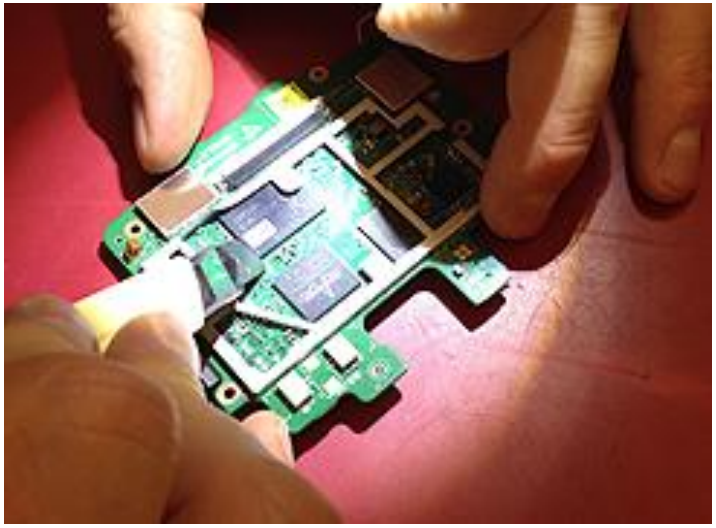
❷ JTAG - Navigationsgerät

- Mobile Navigationsgeräte
- Eingegebene Ziele
- Gefahrene Routen | Triplogs
- Datum und Uhrzeit

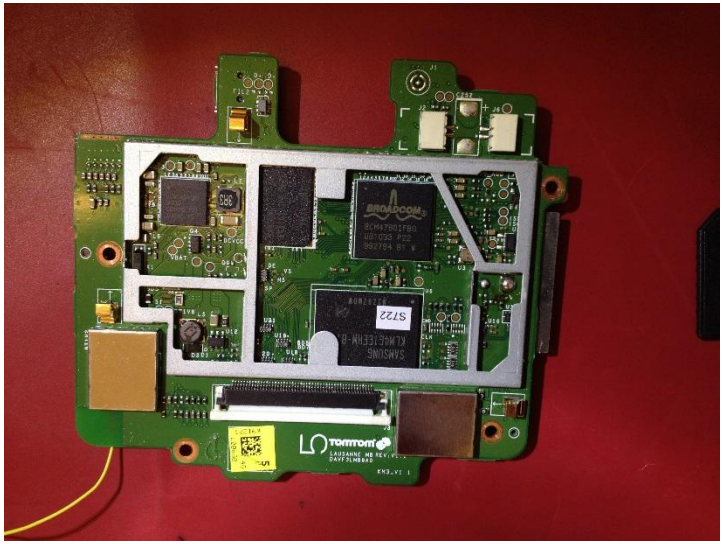
- Keine Schnittstelle
- Kein Massenspeicher

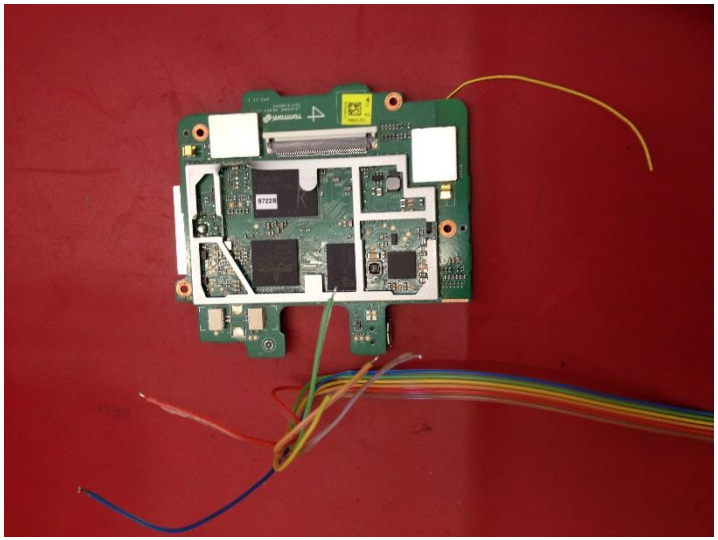
❷ JTAG - Navigationsgerät

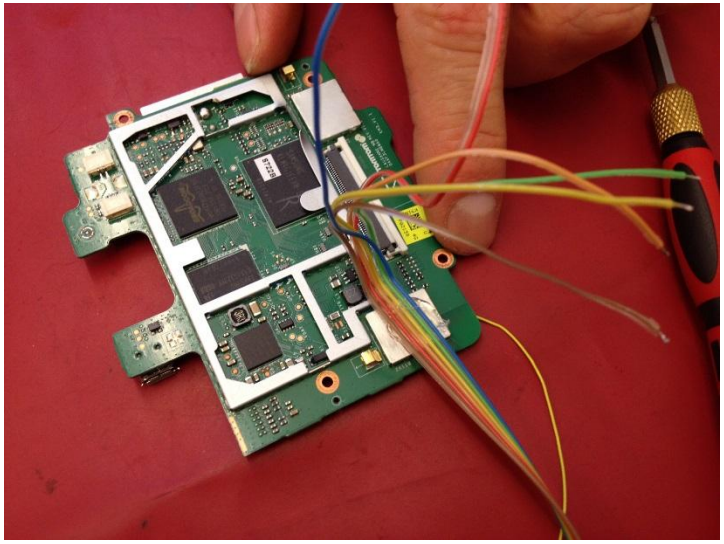


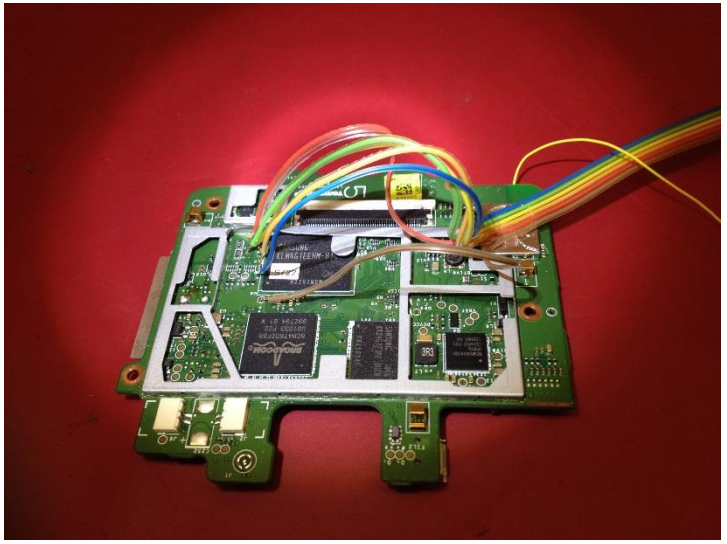


❷ JTAG - Navigationsgerät

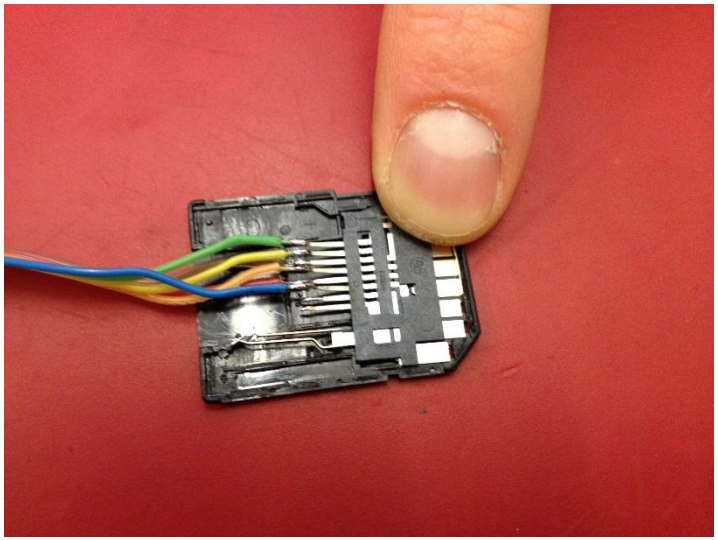


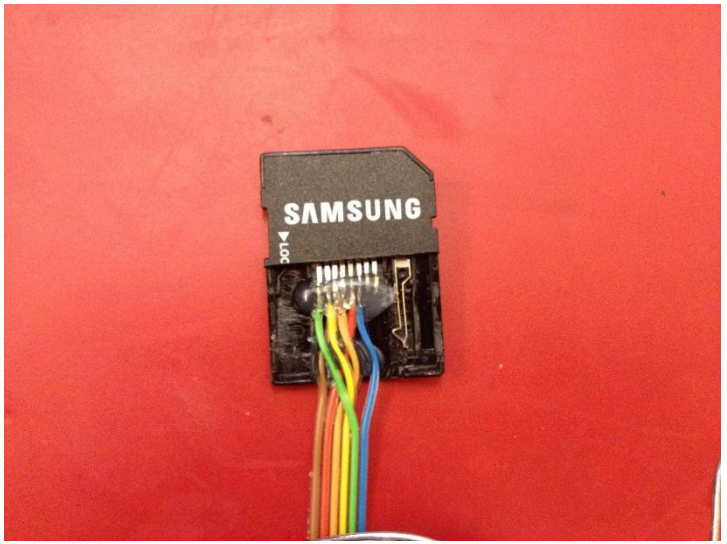


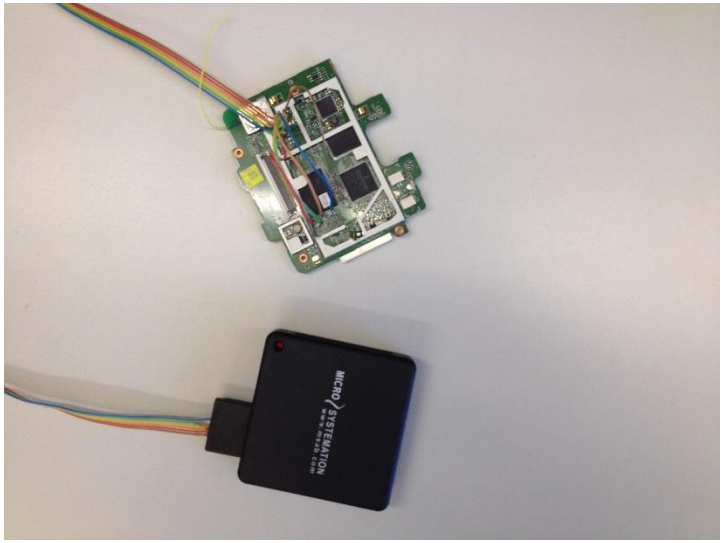


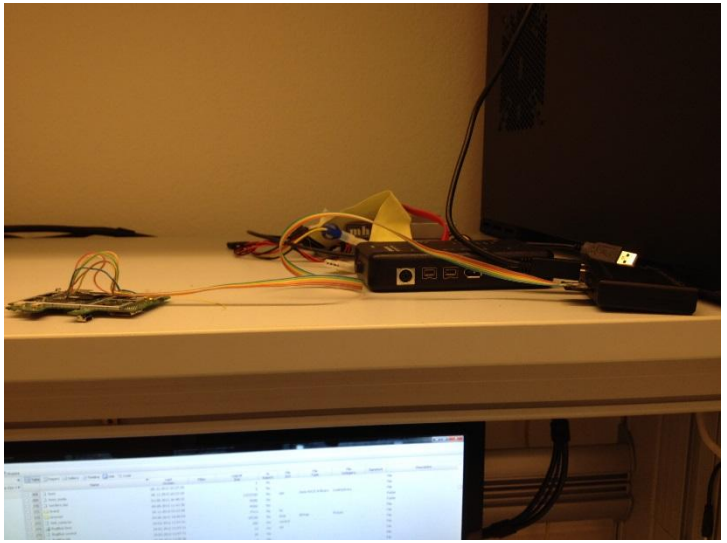


❷ JTAG - Navigationsgerät









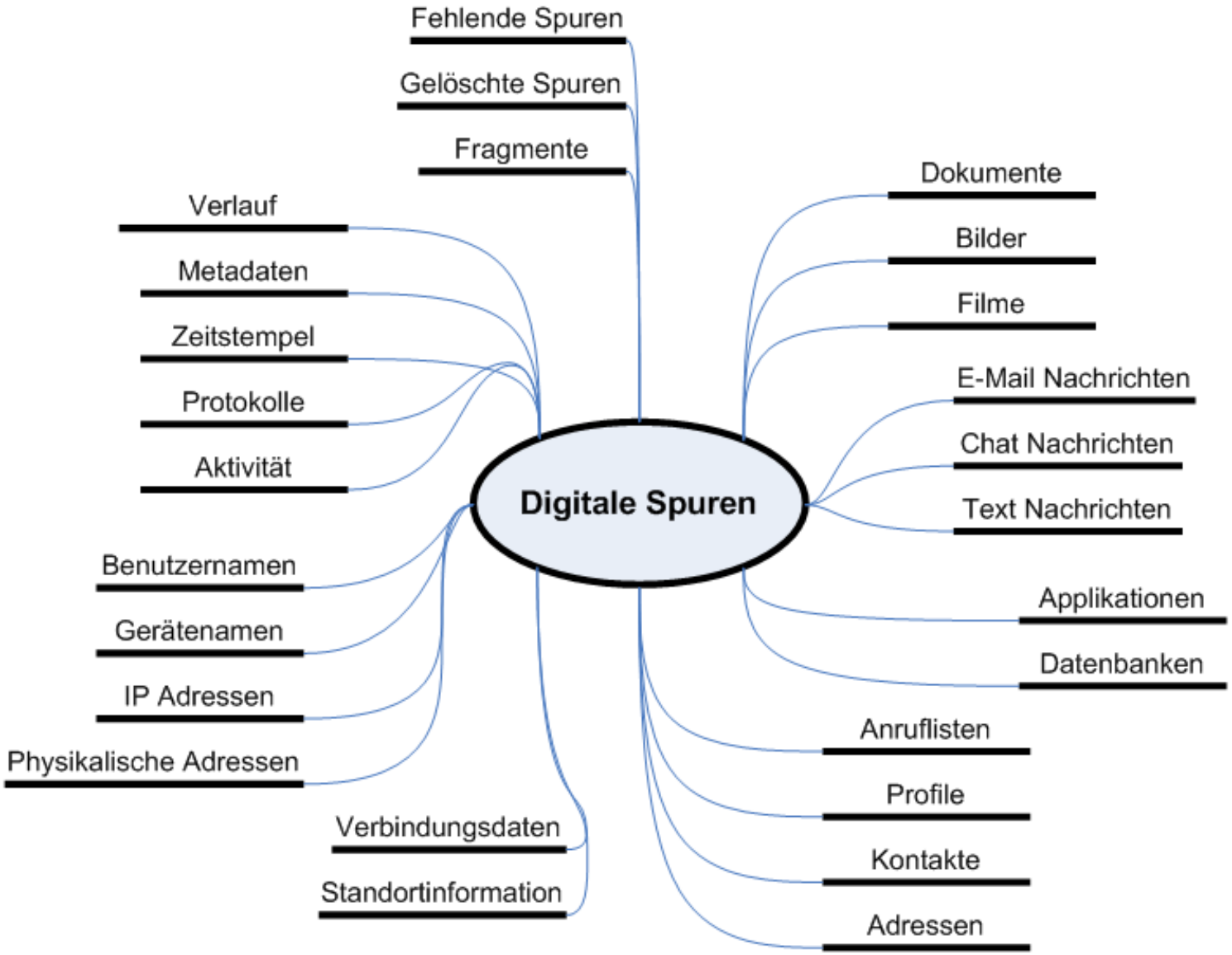
❷ JTAG - Navigationsgerät

- Daten nicht interpretierbar
- proprietäres Datenformat
- teilweise verschlüsselt

- Unterstützung Hersteller
- kostenlos

- Rechtshilfeersuchen

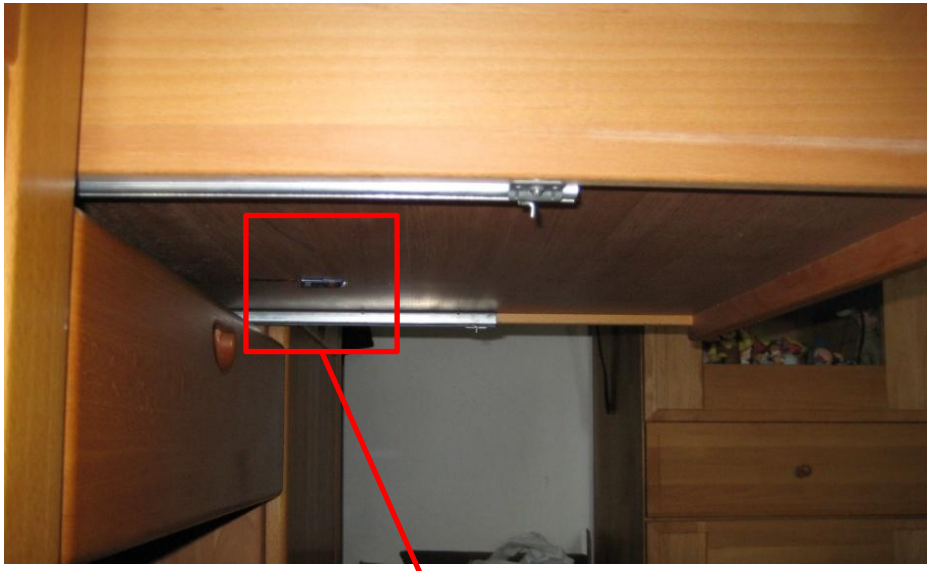
❸ Digitale Spuren - Arten



❸ Digitale Spurenträger - Arten

❸ Digitale Datenträger - Arten

❸ Versteckte Datenträger



❸ Identifikation - Daten

Betreiber RZ | Kunde Housing | Kunde Colocation

Digitale Spuren

Inhalt
Wer?
Wann?
Wo?
Was?
Wie?
Warum?

Malware

- Speicherort beim Hersteller
- Verbreitung über Internet
- Einsatz mittels Botnet
- Command- und Control-Server

Kommunikationsdaten (Mail/Messages/Voice)

- Inhaltsdaten und Randdaten
- Aufzeichnungen / Protokolle / Skripte
- Data in storage, Data in Traffic
- Datenspeicher / Cloud-Speicher

Geldfluss

- Währungsart (Konventionell oder Internetwährung)
- Kontodaten / Wallet-Data
- Kontoinhaber / Wallet-Owner
- Paper -Trail

Data in Storage / in Traffic?

Inhalt

Wer?

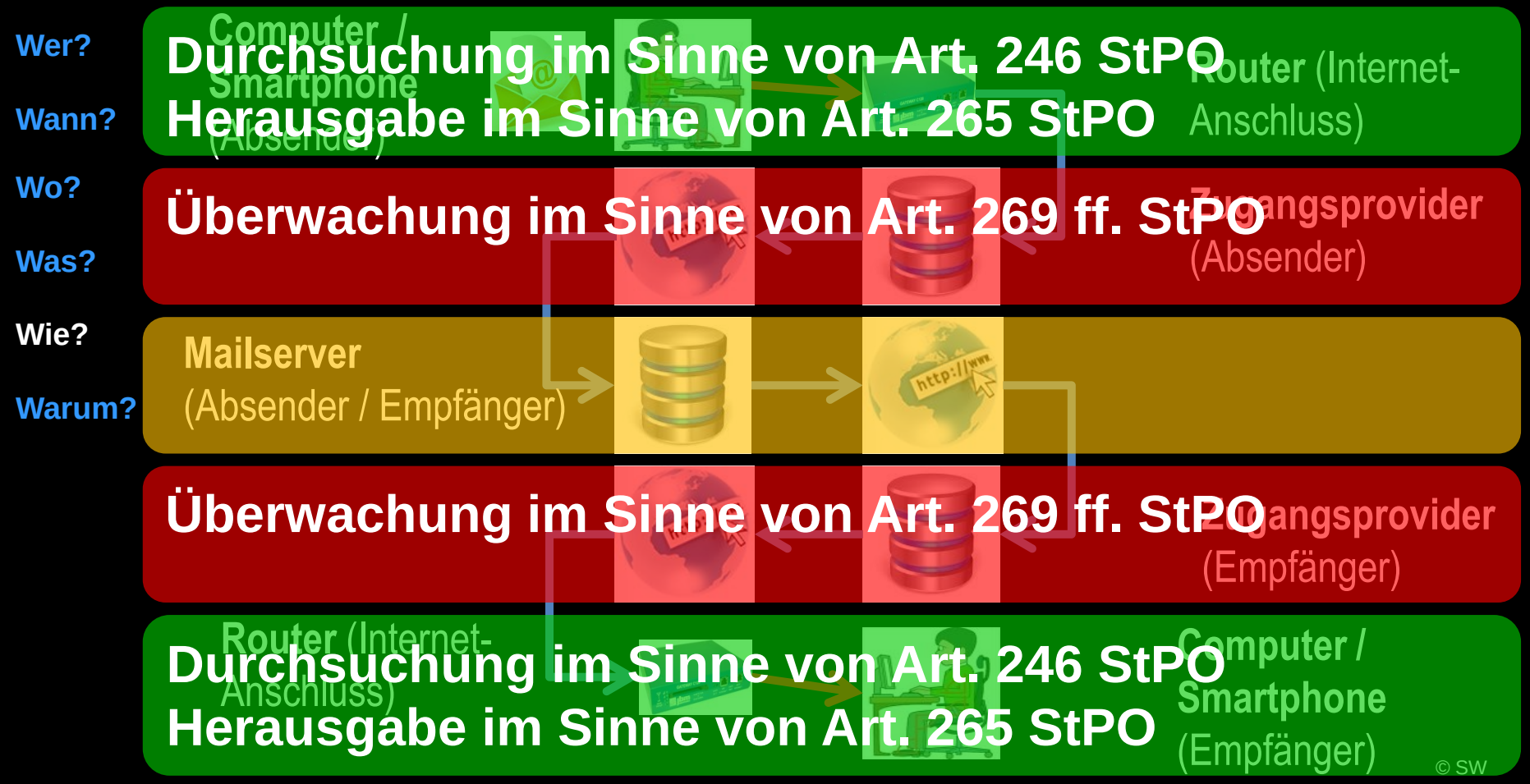
Wann?

Wo?

Was?

Wie?

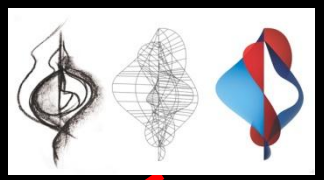
Warum?



Data in Storage / in Traffic?

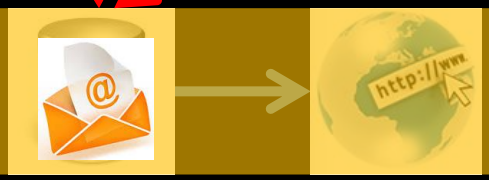
Inhalt
Wer?
Wann?
Wo?
Was?
Wie?
Warum?

Zugang vom Computer / Smartphone mittels Username/Password
- Briefkastenschlüssel?



Zugang über Mail-Server beim Mail-Provider
- Überwachung
- WLAN-Ports 21d!

Mailserver
(Absender / Empfänger)



Rückwirkender Mailverkehr:
- **Randdaten (RTI 6M)**
- **Inhaltsdaten?**

DIGITALE SPUREN WORDLWIDE

Inhalt

Wer?

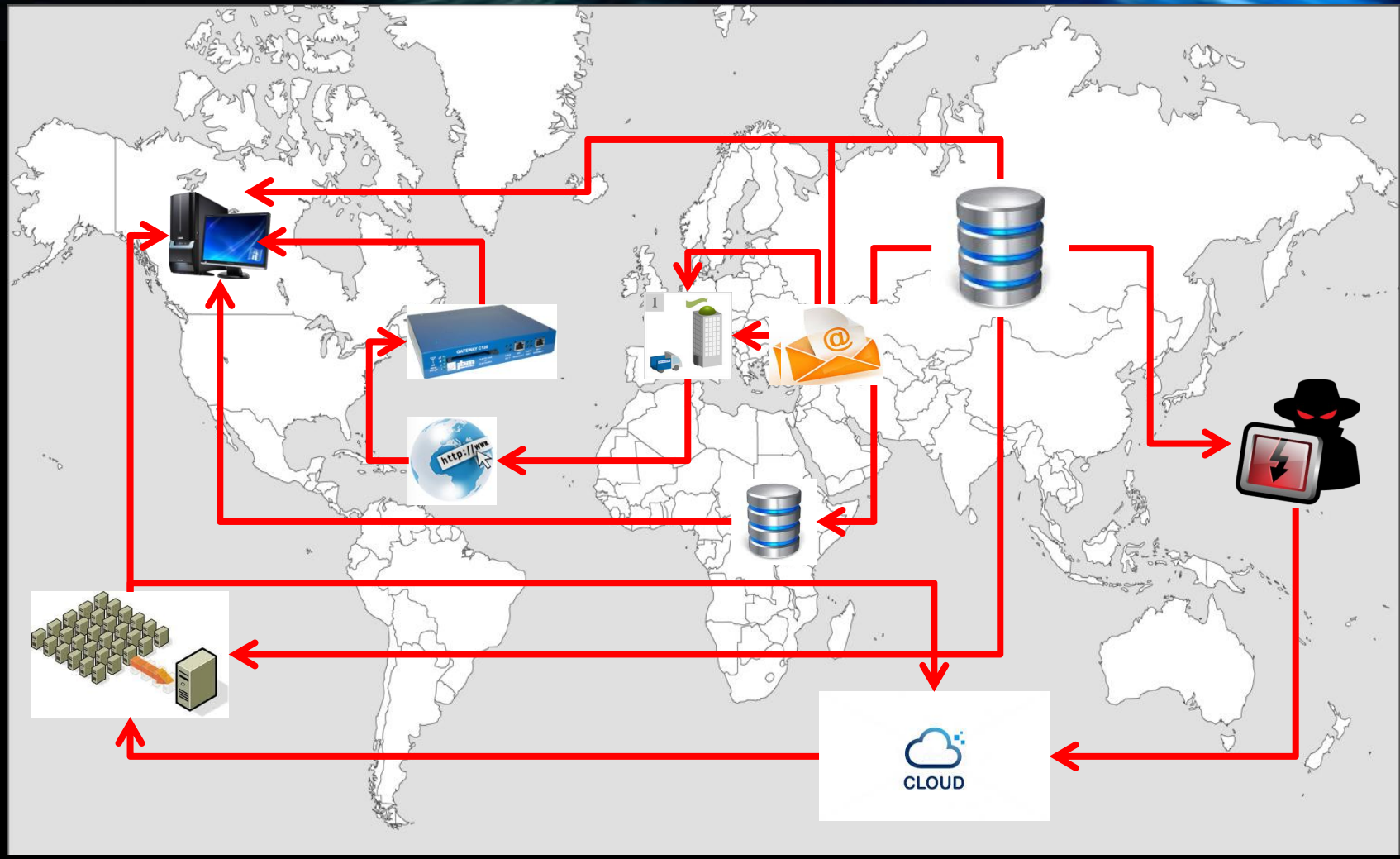
Wann?

Wo?

Was?

Wie?

Warum?

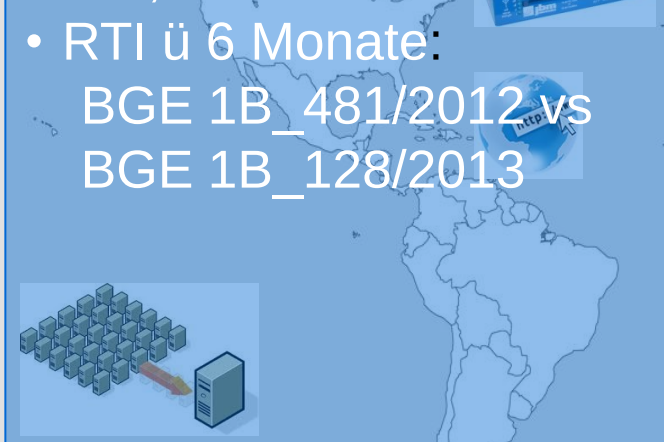


„MLAT“ / NATIONAL

Inhalt
Wer?
Wann?
Wo?
Was?
Wie?
Warum?

ISP: Internet-Service-Provider CH

- Sitz CH
- Provider gemäss FMG/BÜPF
- RTI, Echtzeit etc.
- RTI ü 6 Monate:
  BGE 1B_481/2012 vs
  BGE 1B_128/2013



Benutzer; GES:

- Anschluss CH
- Edition
- Auswertung HD
- Profilübernahme
- VF/VE
- RTI/Echtzeit

MLAT / INT. / EU

Inhalt
Wer?
Wann?
Wo?
Was?
Wie?
Warum?

ISP: Internet-Service-Provider EU

- Preservation Requests gemäss Art. 18 und 29, 32 CCC direkt beim Provider,
- Rechtshilfe (31 CCC) nach Staats-V/ IRSG (Bsp. D: Vertrag zwischen CH und der D über die Ergänzung des Europäischen Übereinkommens über die Rechtshilfe in Strafsachen vom 20. April 1959 und die Erleichterung seiner Anwendung: Direkter Verkehr)

Cybercrime Convention ; Grundregel
Artikel 29 Umgehende Sicherung gespeicherter Computerdaten
1 Eine Vertragspartei kann eine andere Vertragspartei um **Anordnung oder anderweitige Bewirkung der umgehenden Sicherung von Daten** ersuchen, die mittels eines Computersystems gespeichert sind, das sich im Hoheitsgebiet der anderen Vertragspartei befindet, und derentwegen die ersuchende Vertragspartei beabsichtigt,

Titel 2 – Rechtshilfe in Bezug auf Ermittlungsbefugnisse
Art. 31 CCC **Rechtshilfe** beim Zugriff auf gespeicherte Computerdaten
1 Eine Vertragspartei kann eine andere Vertragspartei um **Durchsuchung oder ähnlichen Zugriff, um Beschlagnahme oder ähnliche Sicherstellung und um Weitergabe von Daten** ersuchen, die mittels eines Computersystems gespeichert sind, das sich im Hoheitsgebiet der er-suchten Vertragspartei befindet, einschließlich Daten, die nach Artikel 29 gesichert worden sind.

MLAT / INT. / USA

Inhalt
Wer?
Wann?
Wo?
Was?
Wie?
Warum?

ISP USA:

- Preservation Requests nach Art. 18 und 32 CCC Anfragen über Mail, LERS-Portale

ISP, Enduser USA:

- Staatsvertrag mit den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen (BG-RVUS, SR 351.93
- Bundesgesetz zum Staatsvertrag mit den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen (SR 351.93)
- Beweiserhebungen: Dauer 3-18M
- Über Zentralstelle USA des BJ

PR / INT. / NON GOV. FRIENDLY

Inhalt
Wer?
Wann?
Wo?
Was?
Wie?
Warum?

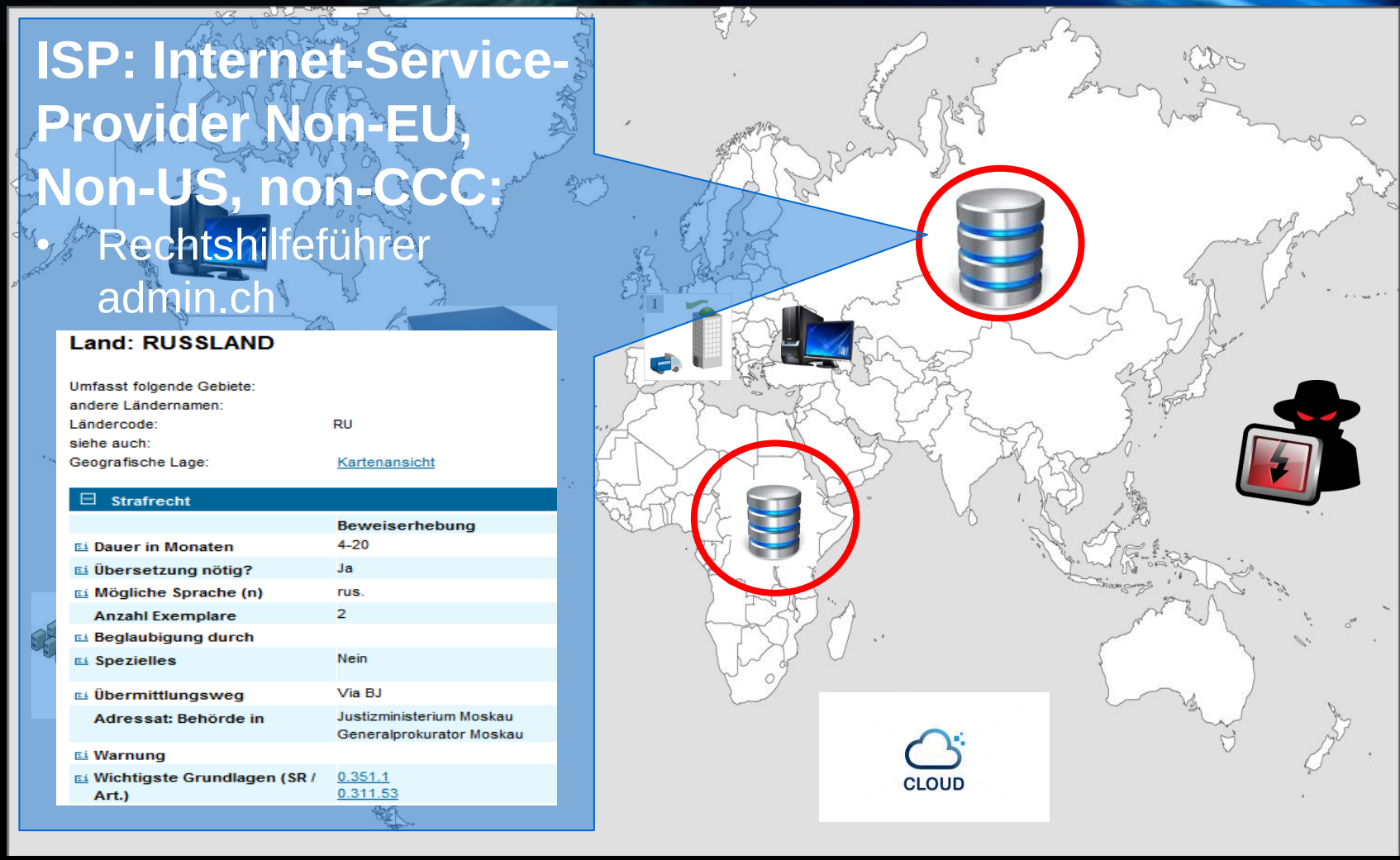
ISP: Internet-Service-Provider Non-EU, Non-US, non-CCC:

- Rechtshilfeführer admin.ch

Land: RUSSLAND

Umfasst folgende Gebiete:
andere Ländernamen:
Ländercode: RU
siehe auch:
Geografische Lage: Kartenansicht

Strafrecht	
	Beweiserhebung
Dauer in Monaten	4-20
Übersetzung nötig?	Ja
Mögliche Sprache (n)	rus.
Anzahl Exemplare	2
Beglaubigung durch	
Spezielles	Nein
Übermittlungsweg	Via BJ
Adressat: Behörde in	Justizministerium Moskau Generalprokurator Moskau
Warnung	
Wichtigste Grundlagen (SR / Art.)	0.351.1 0.311.53

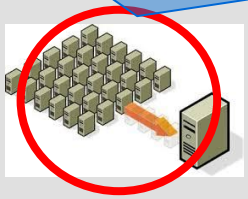


PR / Off-Shore / Cloud

Inhalt
Wer?
Wann?
Wo?
Was?
Wie?
Warum?

Dynamic Off-Shore Serverfarmen

- Keine Staatsverträge
- Keine Datenspeicherfristen
- Keine Gegenseitigkeit nach IRSG

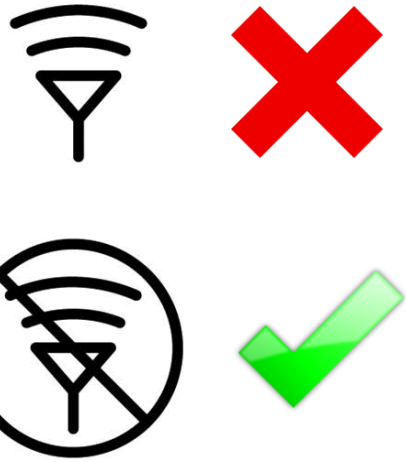


Cloud-Speicher

- Kein „Serverstandort“
- Keine physisch isolierbaren Rechner
- Keine Server am allfälligen Firmensitz
- Keine Lokalisation der Daten(-Fragmente) möglich

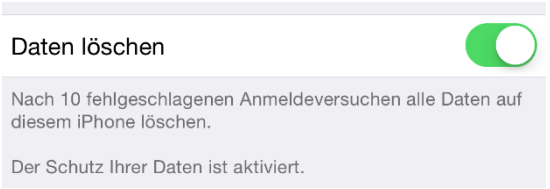
❹ Apple iOS-Geräte - Fernlöschung

- Spurenschutz!
- Flug- | Offlinemodus aktivieren
- Stromversorgung sicherstellen

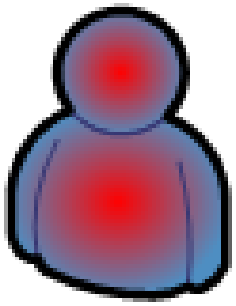


❹ Apple iOS-Geräte

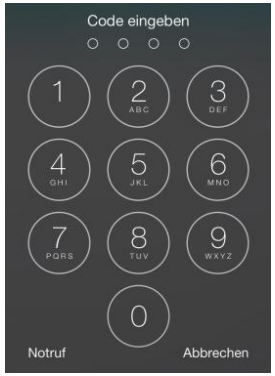
- Brute-Force Attacke
- Einfacher Gerätesperrcode
- Version iOS 7 | (iOS 8)
- Löschung nach 10 Falscheingaben



❹ Apple iOS-Geräte - Gerätesperrcode

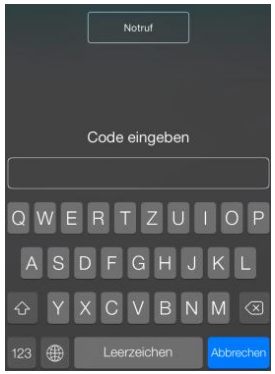


- Kooperation
- Ermittlung



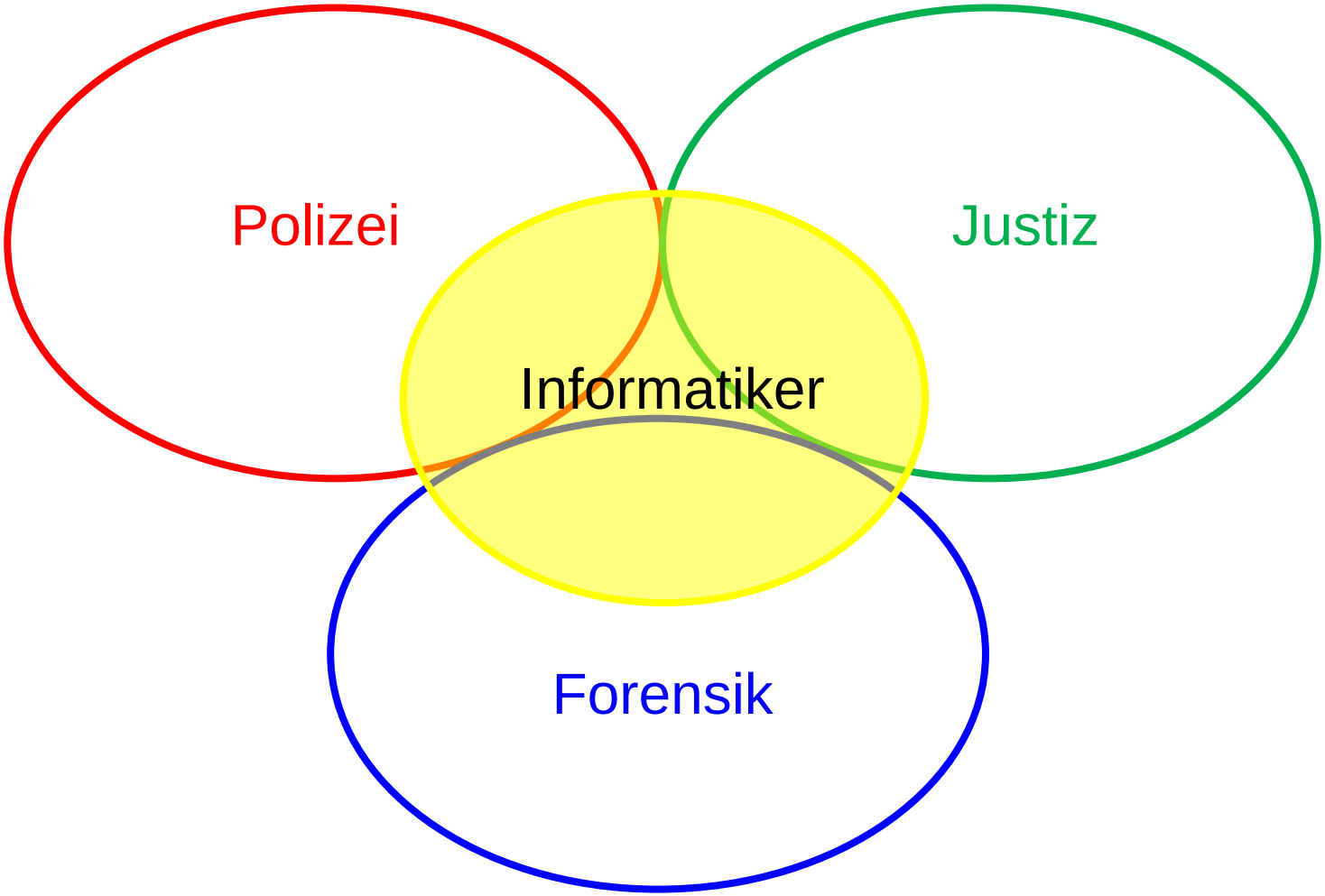
- <= iOS 7
- >= iOS 8

- Einfacher Code
- <= iOS 7 | (iOS 8)
- 10 Falscheingaben



- Apple ID
- Passwort

Lösungsansatz für digitale Spuren?



Polizeiliches Ermittlungsverfahren
Art. 306 StPO: Aufgaben der Polizei

- [1] Die Polizei stellt im Ermittlungsverfahren auf der Grundlage von Anzeigen, Anweisungen der Staatsanwaltschaft oder eigenen Feststellungen den für eine Straftat relevanten **Sachverhalt** fest.
- [2] Sie hat namentlich:
  a. **Spuren und Beweise sicherzustellen und auszuwerten;**
  b. geschädigte und tatverdächtige Personen zu **ermitteln** und zu **befragen**;
  c. tatverdächtige Personen nötigenfalls **anzuhalten** und **festzunehmen** oder nach ihnen zu **fahnden**.

Art. 139 ff in der StPO: Beweismittel

Art. 139: Grundsätze

[1] Die Strafbehörden setzen zur Wahrheitsfindung **alle nach dem Stand von Wissenschaft und Erfahrung geeigneten Beweismittel** ein, die **rechtlich zulässig** sind.

- Was heisst **alle geeigneten** Beweismittel?
- Diverse weiteren Artikel regeln, was rechtlich **nicht** zulässig ist oder wann Beweismittel **nicht verwertet** werden können!

Weisse Flecken in der StPO

- Art. 306 Abs. 2 lit. a
  … Die Polizei hat namentlich …
- Art. 139
  … zur Wahrheitsfindung **alle** …

- Umfang?
- Qualität?
- Methoden?
- Beizug von Spezialisten?

Polizei ←→ Staatsanwalt

Beschlagnahme
Art. 263 StPO: Grundsatz

[1] Gegenstände und Vermögenswerte einer beschuldigten Person oder einer Drittperson können beschlagnahmt werden, wenn die Gegenstände und Vermögenswerte voraussichtlich:

a. als **Beweismittel** gebraucht werden; …

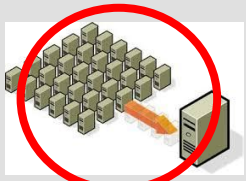
[3] Ist **Gefahr im Verzug**, so können die Polizei oder Private … … vorläufig sicherstellen.

PR / OFF-SHORE / CLOUD

Inhalt
Wer?
Wann?
Wo?
Was?
Wie?
Warum?

Off-Shore Serverfarmen/Cloud-Speicher

Problem:
Anknüpfungspunkt am „Serverstandort“



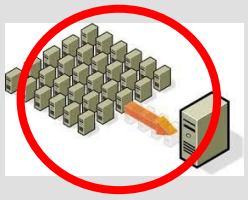
PR / Off-Shore / Cloud

Inhalt
Wer?
Wann?
Wo?
Was?
Wie?
Warum?

Off-Shore Serverfarmen/Cloud-Speicher

Lösung:
Anknüpfungspunkt am Ort der Verfügbarkeit der Daten, nämlich

- auf durchsuchtem Rechner mittels Zugangsdaten
- am Sitz der Unternehmung in der Schweiz
- am Sitz der Niederlassung in der Schweiz



INTERNATIONALER ENTSCHEID

- Urteil des District Court Southern New York vom 25. April 2014

Inhalt

Wer?

Wann?

Wo?

Was?

Wie?

Warum?

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION	:	13 Mag. 2814 MEMORANDUM AND ORDER

Conclusion

Even when applied to information that is stored in servers abroad, an SCA Warrant does not violate the presumption against extraterritorial application of American law. Accordingly, Microsoft's motion to quash in part the warrant at issue is denied.

SO ORDERED.

and Borders -- The Rise of Law in Cyberspace, 48 Stan. L. Rev. 1367, 1375 (1996). In this case I must consider the circumstances under which law enforcement agents in the United States may obtain digital information from abroad. Microsoft Corporation

NATIONALE PRAXIS?

Inhalt
Wer?
Wann?
Wo?
Was?
Wie?
Warum?

☹ **Problem: Erhebung am Speicherort**

☺ **Lösung: Erhebung am CH-Sitz oder -Niederlassung**

Facebook Switzerland Sàrl *in* Vernier, C

Google Switzerland GmbH *in* Zürich, Gr

Microsoft Schweiz GmbH *in* Wallisellen

Apple Switzerland AG *in* Zürich, AG, ++

Yahoo! Sàrl *in* Rolle, GmbH, +++, CHE-

Artikel 18 – Anordnung der Herausgabe

1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen anzuordnen,

a dass eine Person in ihrem Hoheitsgebiet bestimmte Computerdaten, die sich in ih-rem Besitz oder unter ihrer Kontrolle befinden und die in einem Computersys-tem oder auf einem Computerdatenträger gespeichert sind, vorzulegen hat und

b **dass ein Diensteanbieter, der seine Dienste im Hoheitsgebiet der Vertragspartei anbietet, Bestandsdaten in Zusammenhang mit diesen Diensten, die sich in seinem Besitz oder unter seiner Kontrolle befinden, vorzulegen hat**.

Ansatz Schweingruber*

Inhalt
Wer?
Wann?
Wo?
Was?
Wie?
Warum?

- Artikel 18 CCC (Cybercrime Convention)
  Anordnung der Herausgabe
- 1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen anzuordnen,
- a dass eine Person in ihrem Hoheitsgebiet bestimmte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden und die in einem Computersys-tem oder auf einem Computerdatenträger gespeichert sind, **vorzulegen** hat und
- b dass ein Diensteanbieter, der seine Dienste im Hoheitsgebiet der Vertragspartei anbietet, **Bestandsdaten** in Zusammenhang mit diesen Diensten, die sich in sei-nem Besitz oder unter seiner Kontrolle befinden, **vorzulegen** hat.

*STA lic.iur. Sandra Schweingruber, Jusletter vom 10. November 2014

Ansatz Schweingruber*

Inhalt
Wer?
Wann?
Wo?
Was?
Wie?
Warum?

www.jusletter.ch

Sandra Schweingruber

Cybercrime-Strafverfolgung im Konflikt mit dem Territorialitätsprinzip

Im Cyberspace existieren keine staatlichen Grenzen. Cybercrime ist deshalb nahezu immer international, sodass Strafverfolger fast immer auf Daten angewiesen sind, die im Ausland liegen. Aufgrund des Territorialitätsprinzips ist dazu der Rechtshilfeweg nötig; doch bis ein Ersuchen im angefragten Staat bearbeitet ist, sind die Daten oft nicht mehr vorhanden. Mit dem Übereinkommen über Computerkriminalität wurden erste Instrumente geschaffen, die einen Zugriff auf ausländische Daten ohne Rechtshilfeverfahren ermöglichen. Dieser Artikel setzt sich mit dessen Umsetzung auseinander und will Denkanstösse für eine pragmatische Interpretation liefern.

Beitragsarten: Beiträge
Rechtsgebiete: Strafrecht im Informatikrecht; Strafprozessrecht; Internationale Rechtshilfe

Direkte „Edition“?

Inhalt
Wer?
Wann?
Wo?
Was?
Wie?
Warum?

Artikel 32 CCC (Cybercrime Convention)
Grenzüberschreitender Zugriff auf gespeicherte Computerdaten mit Zustimmung oder wenn diese öffentlich zugänglich sind

- Eine Vertragspartei darf ohne die Genehmigung einer anderen Vertragspartei

  a auf **öffentlich zugängliche gespeicherte Computerdaten** (offene Quellen) zugreifen, **gleichviel, wo sich die Daten geographisch befinden**, oder

  b auf **gespeicherte Computerdaten**, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden, mittels eines Computersystems in ihrem Hoheitsgebiet zugreifen oder diese Daten empfangen, wenn sie **die rechtmäßige und freiwillige Zustimmung der Person einholt, die rechtmäßig befugt ist, die Daten mittels dieses Computersystems an sie weiterzugeben**.

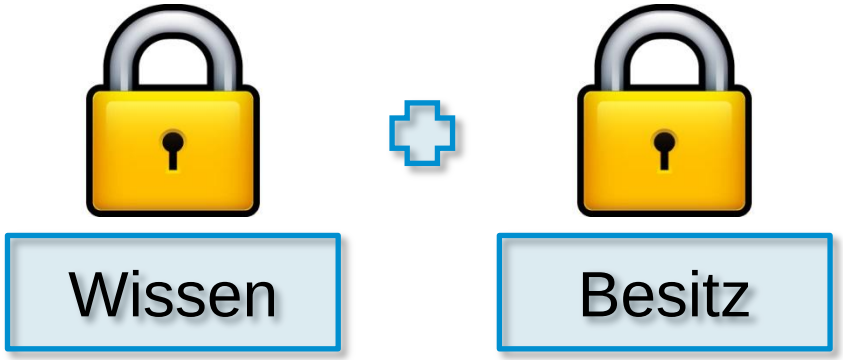
Fallstudie

Inhalt
Wer?
Wann?
Wo?
Was?
Wie?
Warum?

1. Rassendiskriminierungen via **Facebook** Accounts
2. **Preservation Request** bei Facebook
3. Facebook verlangt **„richterlichen Entscheid“** für die freiwillige Herausgabe im Sinne von **Art. 32 CCC**
4. **Nicht-Genehmigung** bzw. -Eintreten durch ZMG, da kein **Art. 32 CCC Anwendungsfall** (Datenherrin, Freiwilligkeit)
5. **Beschwerde ans BGER**
   - Anwendungsfall von Art. 32 CCC, weil Daten gemäss AGB bei Upload Facebook in den Besitz von Facebook übergehen.
   - Art. 273 StPO anwendbar, da RTI-Daten (IP-History und Zeitstempel Eruierung Anschlussinhaber ermöglicht)
   - Keine rückwirkende Rekonstruktion von Inhaltsdaten mittels URL

❺ Zwei-Faktor Authentifizierung (2FA)

- Zusätzliche Sicherheit ⇨ Identitätsnachweis



- Geldautomat ⇨ PIN ✚ Bankkarte
- Arbeitsplatz ⇨ Passwort ✚ Smartcard
- e-Banking ⇨ Vertragsnummer ✚ Kartenleser

❺ Zwei-Faktor Authentifizierung (2FA)

- The Fappening | #Celebgate

Neue Zürcher Zeitung

Aufregung um Nacktbilder im Netz

Henning Steier 1.9.2014, 07:19 Uhr

Stars wie Jennifer Lawrence, Kate Upton und Rihanna sollen Opfer von Cyberkriminellen geworden sein. Offenbar wurden simple Sicherheitsregeln missachtet. Apple prüft die Vorwürfe.

❺ Zwei-Faktor Authentifizierung (2FA)

- Google Konto | Google Mail

- Passwort

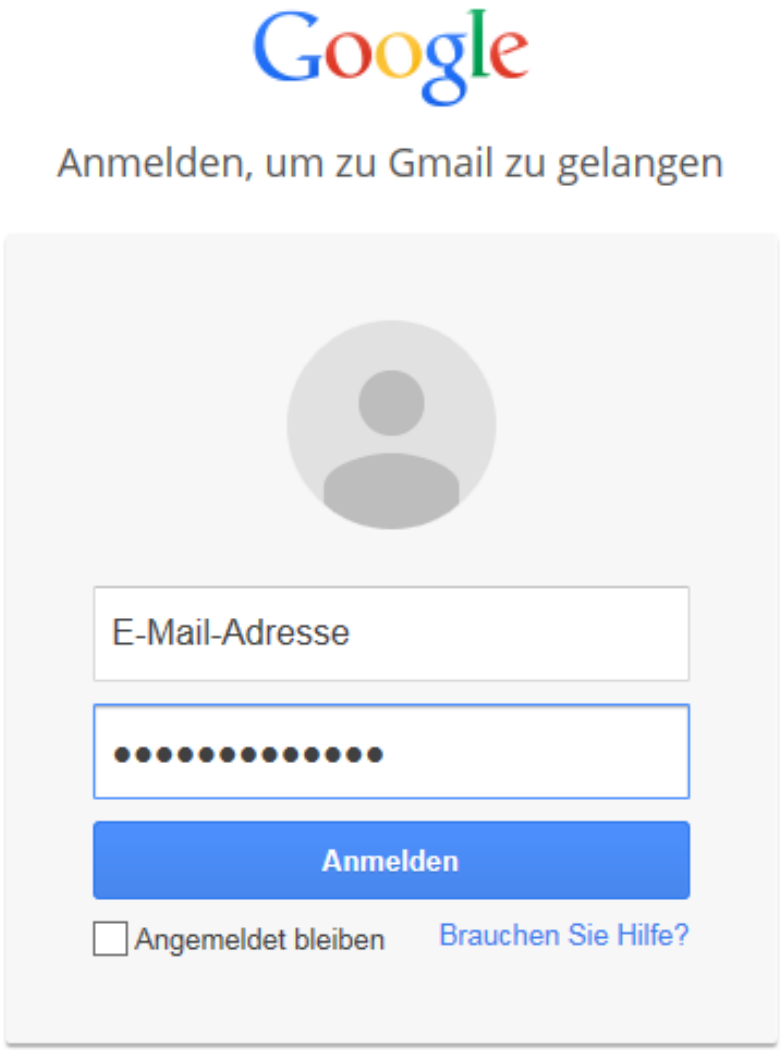
- SMS

- Anruf

- Google Authenticator

- Sicherheitsschlüssel

❺ Zwei-Faktor Authentifizierung (2FA)



❺ Zwei-Faktor Authentifizierung (2FA)

Google

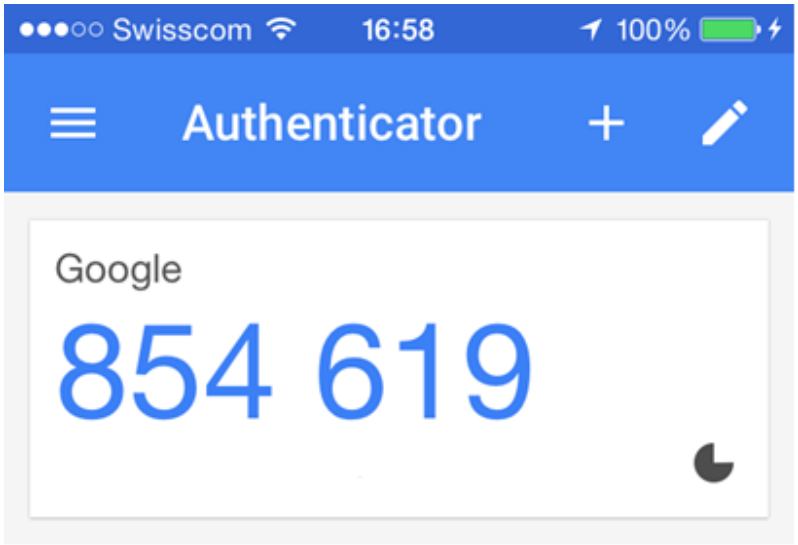
Bestätigung in zwei Schritten

Geben Sie den von Ihrer mobilen Anwendung generierten Bestätigungscode ein.

854619

Bestätigen

Auf diesem Computer nicht mehr nach Codes fragen



PHISHING „CLASSIC“

Inhalt

Wer?

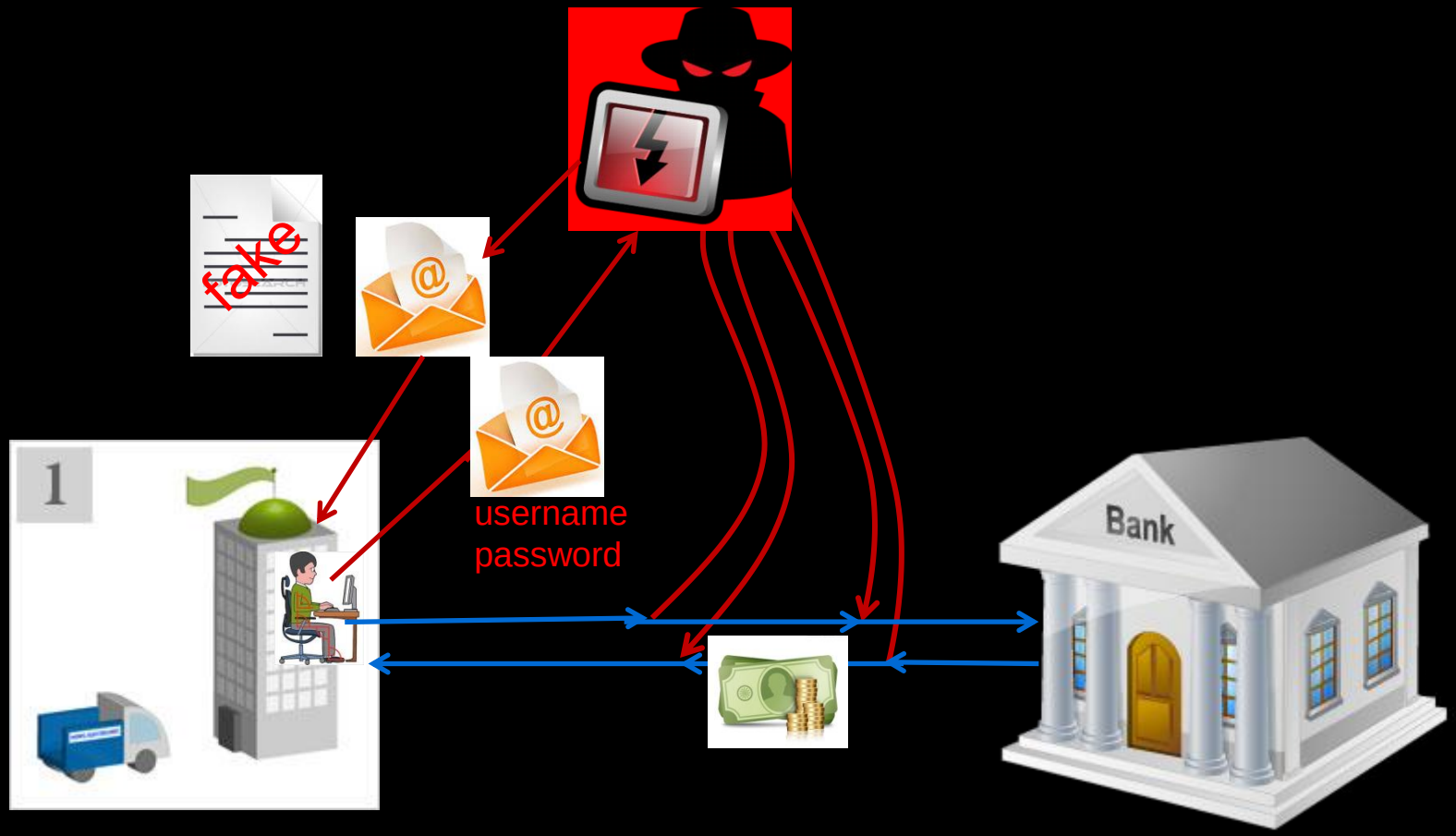
Wann?

Wo?

Was?

Wie?

Warum?



PHISHING „TODAY“

Inhalt

Wer?

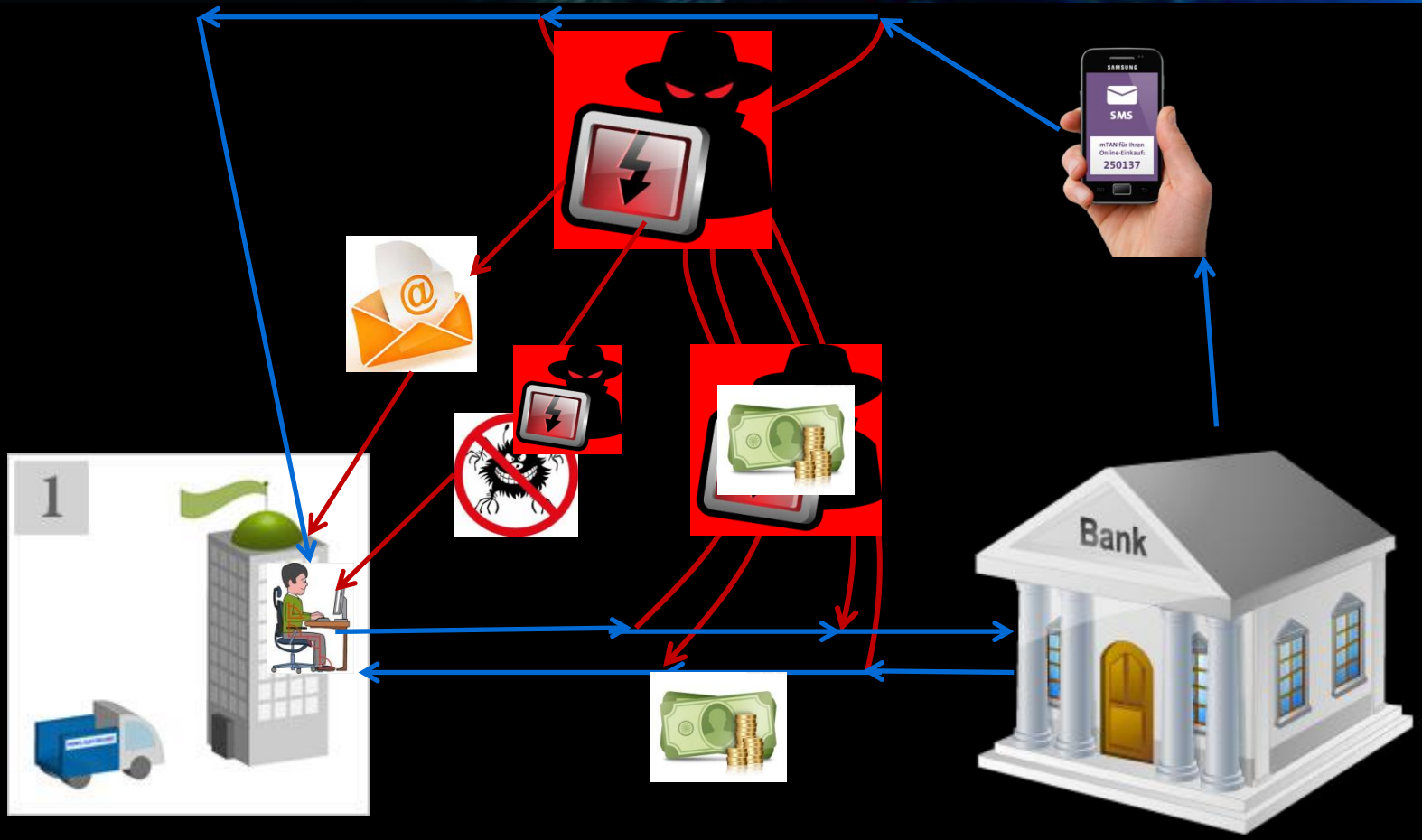
Wann?

Wo?

Was?

Wie?

Warum?



PHISHING „TODAY“

Inhalt

Wer?

Wann?

Wo?

Was?

Wie?

Warum?

„Hintermann“

- Sender der E-Mails,
- Koordinator ; Empfänger des Geldes
- Zuständigkeit BA bei Hintermännern im Ausland

„Malware-Distributor“

- Versendet Malware
- Kann Tor-Exit-Node oder Botnet sein
- Zuständigkeit am Tatort/Wohnort

„Money Mule“

- Stellt eigenes Konto zur Verf.
- Leitet Gelder auf Anweisung weiter
- Ist von „Firma“ angestellt
- Zuständigkeit am Tatort/Wohnort

❻ Verschlüsselung

WHO WATCHES THE WATCHMEN?

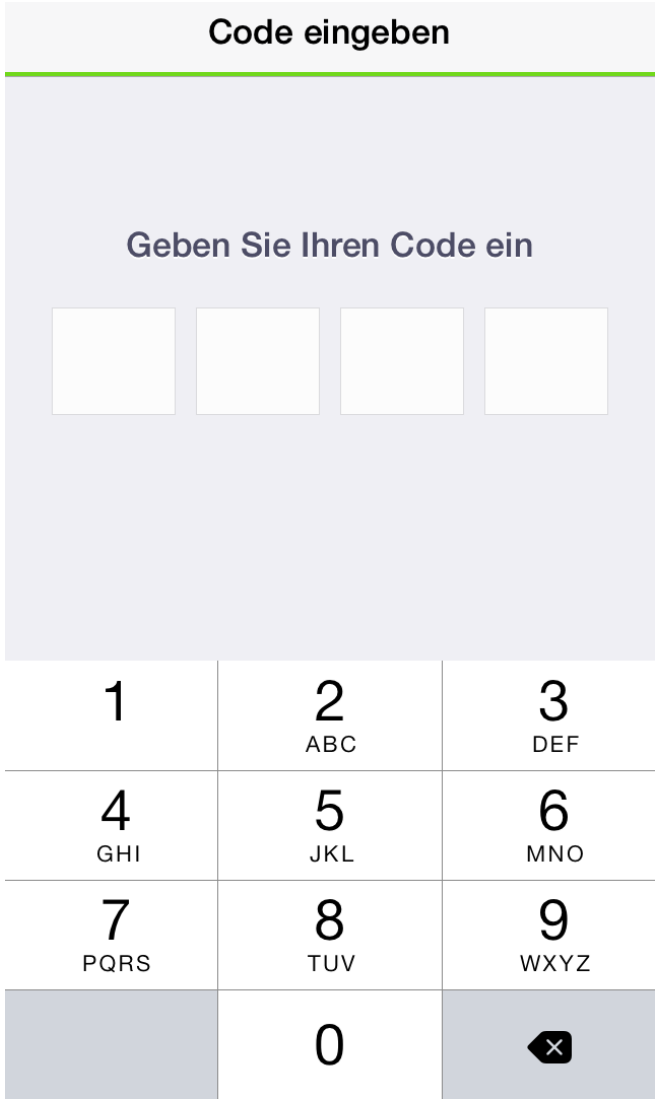
❻ Verschlüsselung

- BitLocker
- File Vault 2
- dm-crypt/LUKS

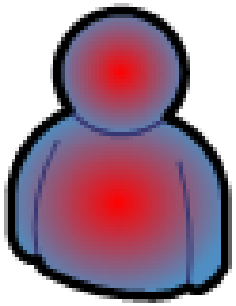
- Apple iOS 8
- Android 5

❻ Verschlüsselung - Kommunikation

- Skype
- WhatsApp
- Threema



❻ Verschlüsselung



- Kooperation
- Ermittlung

?

- Schwachstellen
- Dictionary Attack
- Brute-Force Attack

?

- 
- Verschlüsselung

- GovWare

(Government Software)

?

ÜBERWACHUNG?

Inhalt

Wer?

Wann?

Wo?

Was?

Wie?

Warum?

☹ Mil. Nachrichtendienst
☹ Lagebild
☹ Bedrohungen
☹ gesetzliche Grundlage

☺ Strafverfolgung
☺ Beweiserhebung
☺ Katalogtaten
☺ Verhältnismässigkeit (Tatschwere)
☺ Dringender Tatverdacht
☺ Proportionalität
☺ Susidiarität
☺ Genehmigung Zwangsmassnahmengericht
☺ Mitteilungspflicht
☺ Zufallsfunde
☺ Verwertbarkeit

ÜBERWACHUNG „CLASSIC“

Inhalt

Wer?

Wann?

Wo?

Was?

Wie?

Warum?

Internetzugangsanbieterin
ISP

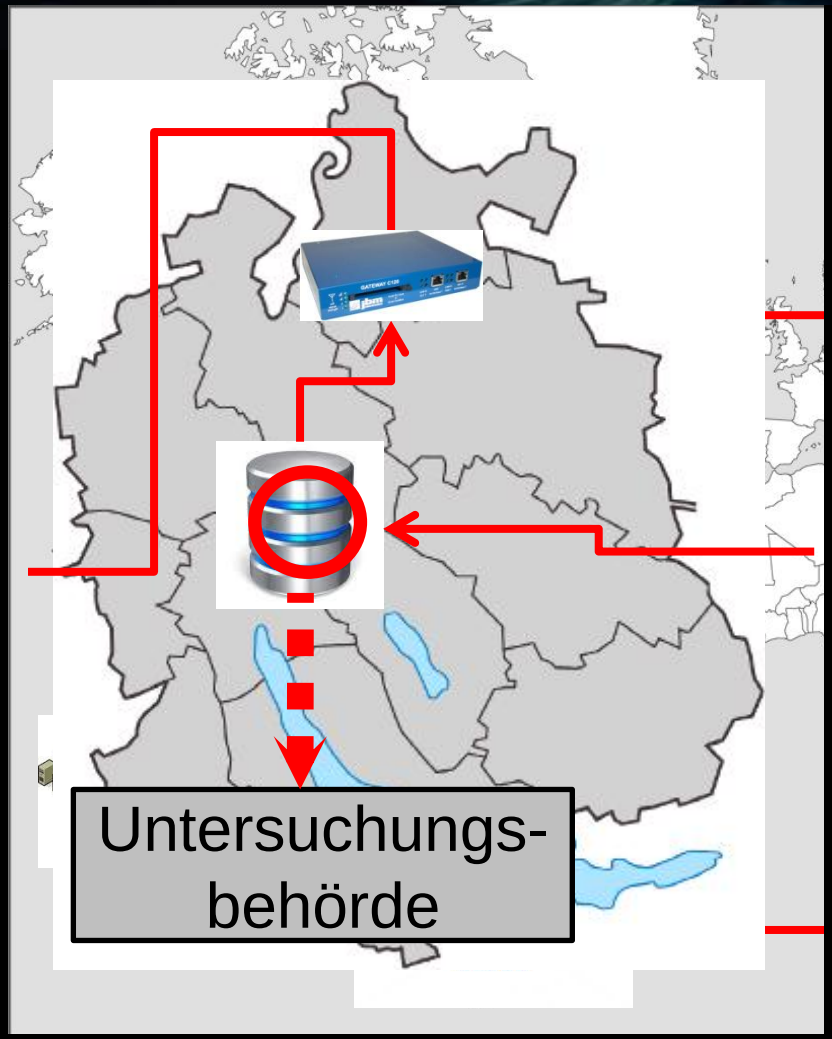
☹ **Packet-Loss**
☹ **LIS/ISS, ISC ÜPF**
☹ **Unverschlüsselt**

Ausleitung einer Kopie des Ein- und Ausgehenden Datenverkehrs

Untersuchungsbehörde

Überwachung Server

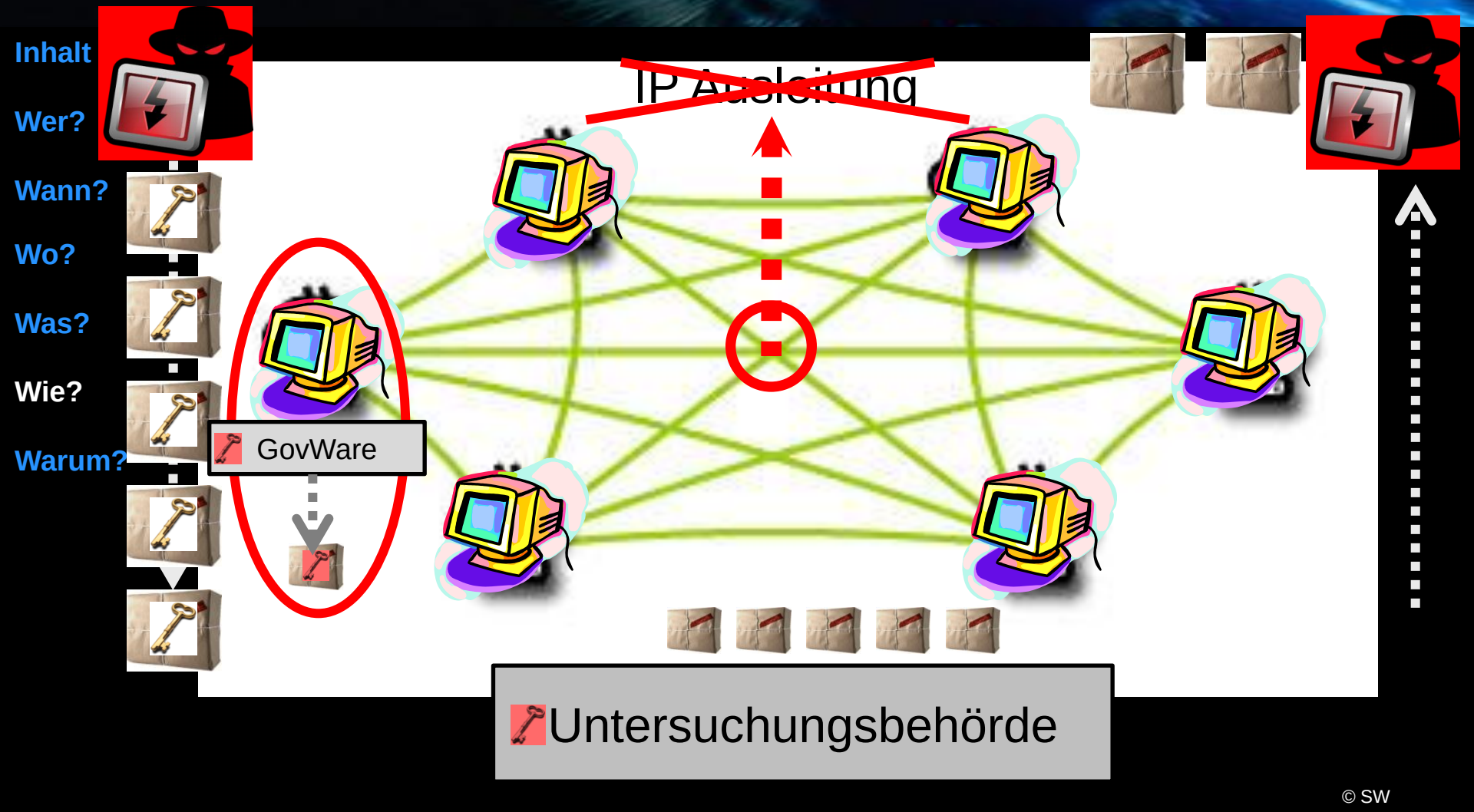
Inhalt
Wer?
Wann?
Wo?
Was?
Wie?
Warum?



- ☺ Echtzeitüberwachung im Sinne von Art. 269ff StPO
- ☺ Genehmigungsfähig (ZMG OG ZH)
- ☺ Nicht über ISC-EJPD, Dienst ÜPF
- ☺ Direkt beim Provider
- ☺ Ausleitung auf Server
- ☺ Man in the middle
- ☺ kostenschonend

- ☺ Nur bei intakter PPP
- ☺ keine Verschlüsselung

ÜBERWACHUNG GOVWARE



Kanton Zürich
Direktion der Justiz und des Innern
Strafverfolgung Erwachsene

Überwachung NoGovWare

Inhalt

Wer?

Wann?

Wo?

Was?

Wie?

Warum?

Untersuchungsbehörde

Kanton Zürich
Direktion der Justiz und des Innern
Strafverfolgung Erwachsene

FRAGEN?

Vielen Dank für

Fragen?

Ihre Aufmerksamkeit

Fragen?

und Ihr Interesse!

Forensisches Institut Zürich
Eine Organisation der Kantonspolizei und Stadtpolizei Zürich

Kantonspolizei Zürich