

Handysicherheit

Für Endanwender

Christoph Weinandt
IT-Stammtisch Darmstadt

Handysicherheit

Profil

Christoph Weinandt

IT-Stammtisch Darmstadt

•Skills:

- CCSA
- CNA
- IT-Sicherheit
- Forensic
- Penetration Testing
- Networking
- ITILv3



Handysicherheit



Agenda

- × Verwendung von Smartphones im Alltag
- × Gefährdungslage
- × Anforderungen an die Handsicherheit
- × Empfehlungen und Tools
- × LiveDemos

Agenda

Verwendung von Smartphones im Alltag

1994...

• Telefonieren



2011



- Email
- Chat
- Soziale Netzwerke
- Online Bezahlen
- Online Banking
- Internet Radio
- Internet TV
- SMS
- Adressen und Termine
- Cloud Computing
- Telefonieren

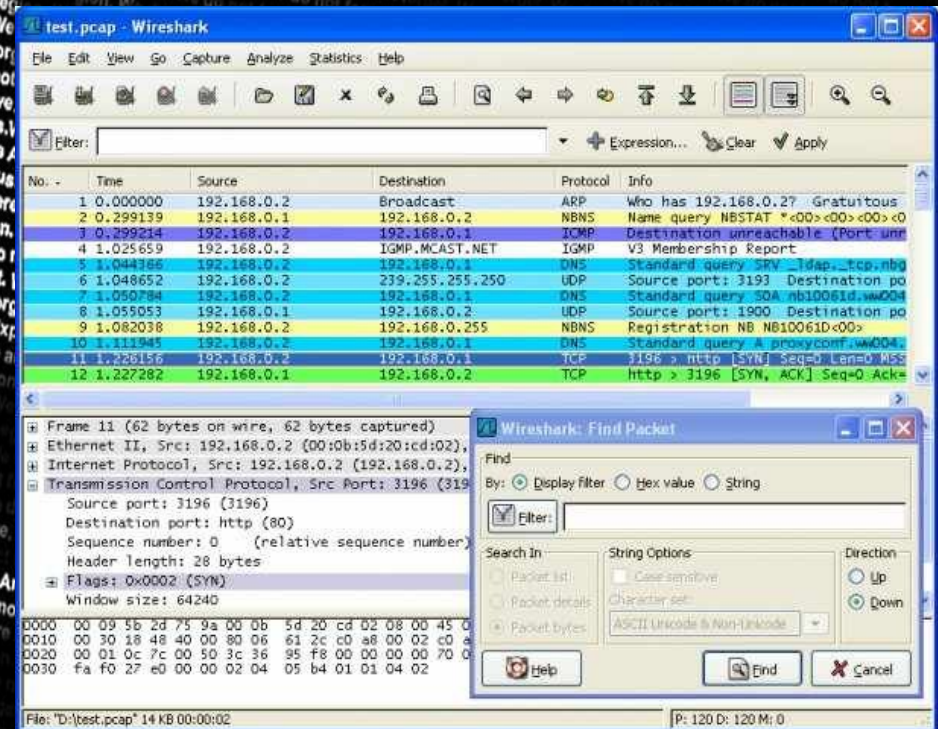
Agenda

Gefährdungslage

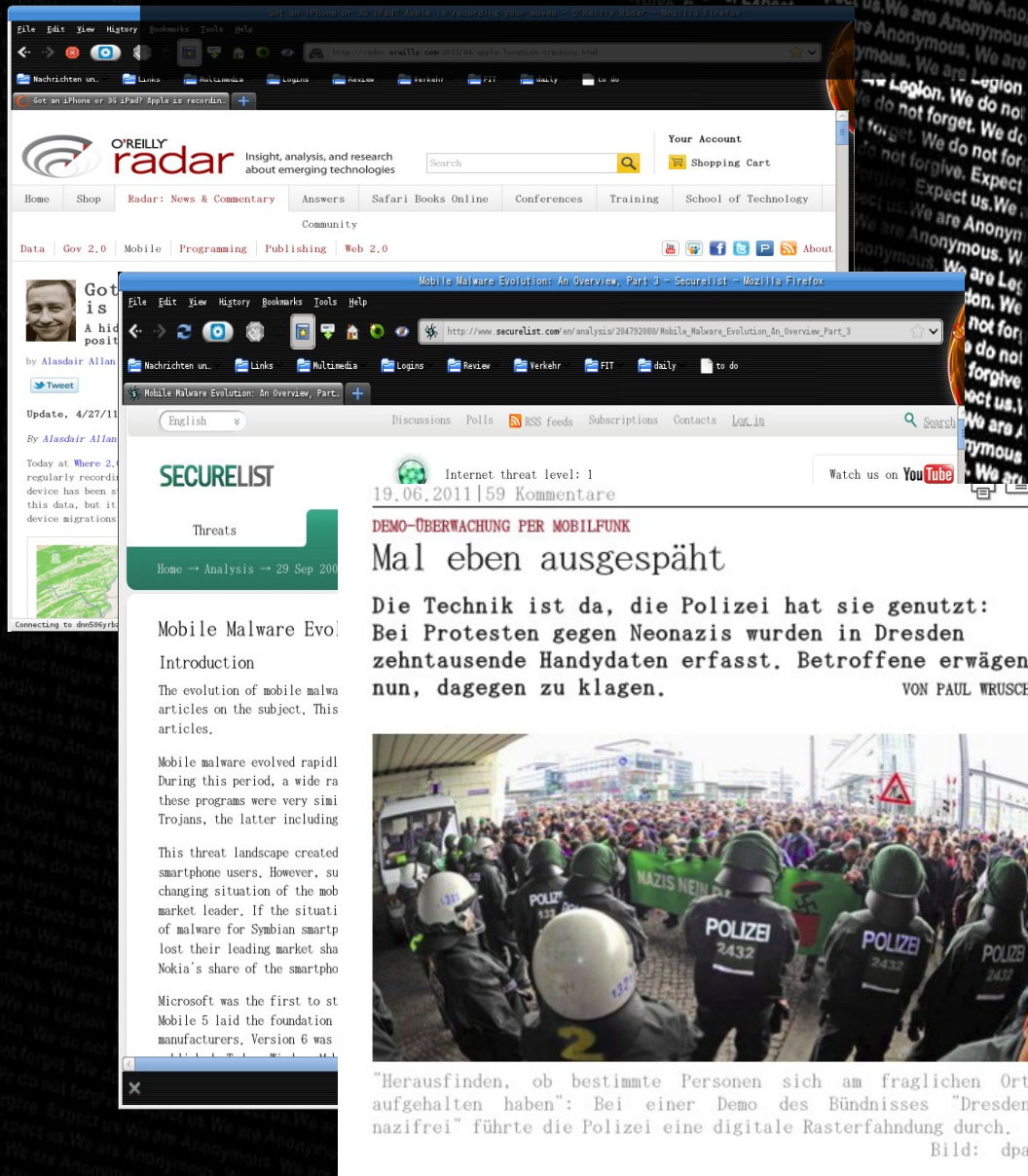
Internet

- Verschlüsselung?
- Privatsphäre?
- Datensicherheit?

Fehlanzeige!



Gefährdungslage



• „Locationgate“
Apple Iphone / Android

• Malware

• Berechtigungen

• Anwendungen von
Drittanbietern

• Trojaner
Zeus

• Custom Firmware

• (Un-)Locked Bootloader

• Abofallen

• Dresden:
„Polizei erfasst Tausende Handydaten“

Gefährdungslage

• Ziele:

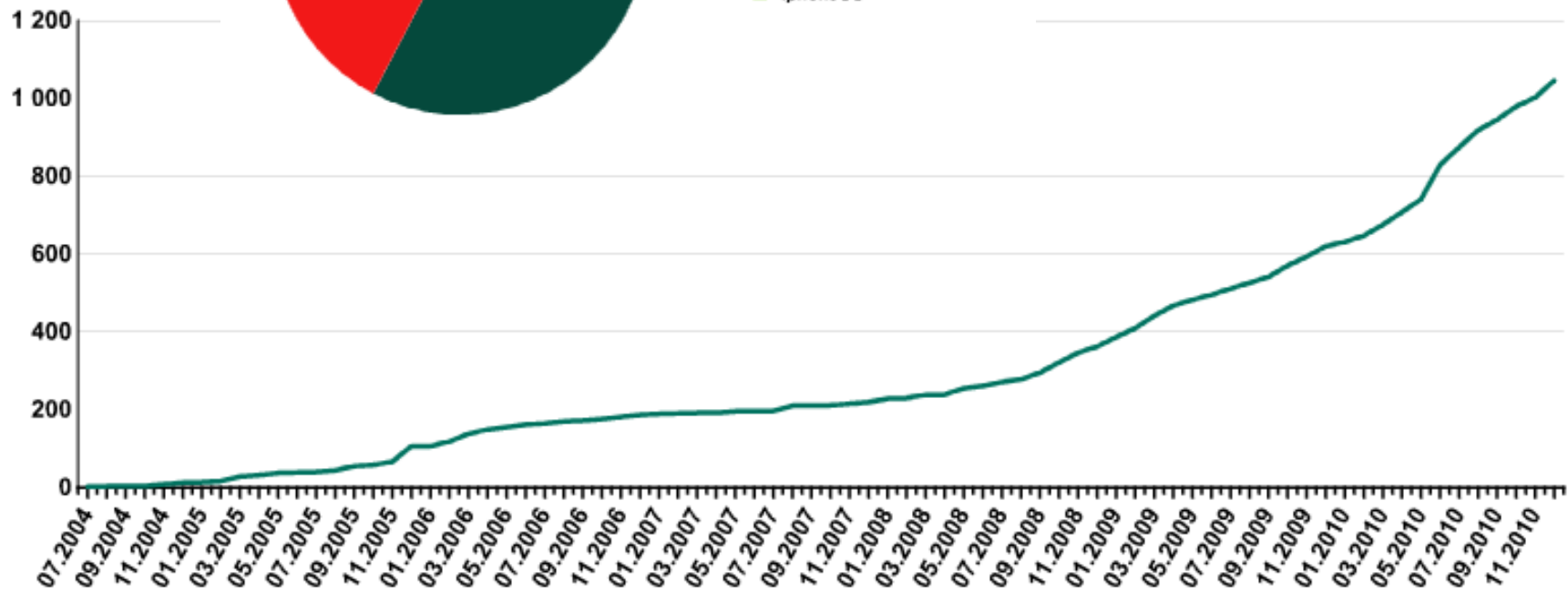
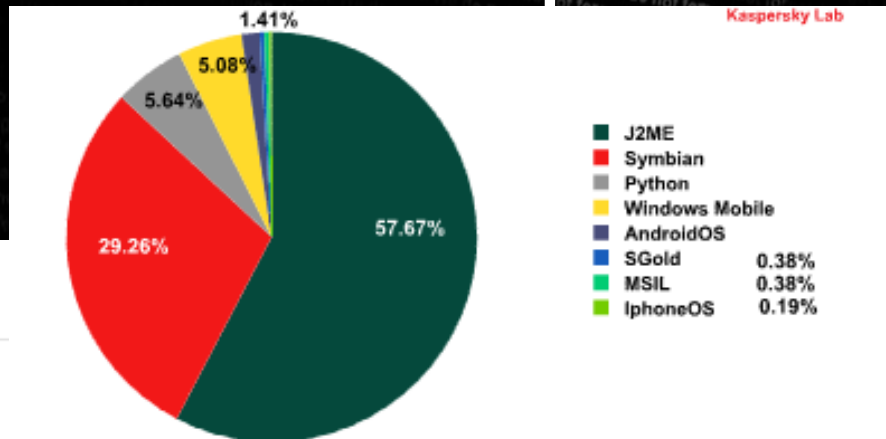
- mTAN/Banking
- Ihre Daten

• Malware ist ein lukrativer Markt

- Botnetze
- Profiling
- Tracking



Mal ein paar Zahlen



http://www.securelist.com/en/analysis/204792168/Mobile_Malware_Evolution_An_Overview_Part_4#14

Achtung – Wichtig!

- Software (Apps)
- Diebstahl und Verlust
- Tracking
- Datensammelwut
- Anwendungs-berechtigungen
- Jailbreak/Rooting
- Dropbox
- Abofallen

Data counter widget

Roy Solberg



★★★★★ (5,302)

INSTALLIEREN

Mehr vom Entwickler



kor.im Phone Locator

ROY SOLBERG

★★★★★ (298)

Kostenlos

Data counter pro

ÜBERSICHT

ERFAHRUNGSBERICHTE (1337)

Berechtigungen

DIESE APP KANN AUF FOLGENDES ZUGREIFEN:

SPEICHER

INHALT DES USB-SPEICHERS UND DER SD-KARTE ÄNDERN/LÖSCHEN

Ermöglicht einer App das Schreiben in den USB-Speicher

SYSTEM-TOOLS

STANDBY-MODUS DEAKTIVIEREN

Ermöglicht einer App, den Standby-Modus des Geräts zu deaktivieren

☑ Alle anzeigen

- MobileSpy
- jamba

Ihre Daten

Bundesnetzagentur
Postfach 80 01
53105 Bonn
Fax 0228 - 14 8872

22.09.11

Anzeige wegen ordnungswidriger Speicherung von Telekommunikations-Verkehrsdaten

Sehr geehrte Damen und Herren,

hiermit bringe ich zur Anzeige, dass die folgenden Unternehmen eine mit einer Geldbuße bis zu dreihunderttausend Euro zu ahndende Ordnungswidrigkeit begehen, indem sie entgegen § 96 Abs. 1 Satz 3 und § 97 Abs. 3 Satz 2 TKG Telekommunikationsverkehrsdaten nicht rechtzeitig löschen:

1. BT (Germany) GmbH & Co. OHG,
2. E-Plus Service GmbH & Co. KG,
3. M-net Telekommunikations GmbH,
4. Telefónica Germany GmbH & Co. OHG,
5. Telekom Deutschland GmbH,
6. Vodafone D2 GmbH.

1. BT (Germany) GmbH & Co. OHG

Nach Erkenntnissen des bayerischen Landeskriminalamts (<http://cryptome.org/isp-spy/munich-spy.pdf>) speichert die BT (Germany) GmbH & Co. OHG 180 Tage lang netzübergreifend Verbindungsdaten sämtlicher ein- und ausgehender Verbindungen ihrer Kunden.

- Werden genutzt für Werbung
- Werden genutzt für Statistiken und Auswertungen Ihres Verhalten
- Werden genutzt für Bewegungsprofile
- Werden 90 – 180 Tage lang gespeichert (obwohl dies rechtswidrig ist, TKG)
- Werden „mitgelesen“
- Stehen Staatsanwaltschaft und Urheberrechteinhabern zur Verfügung
- Sind in der Regel unverschlüsselt und Dritten zugänglich

Handyortung

Einsatzszenarien der Handyortung - Handyortung, info - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.handyortung

Nachrichten un... Links Multimedia Logins Review Verkehr FIT daily to do

Einsatzszenarien der Handyortung - Handyort...

Navigation

- Startseite
- Nachrichten
- Funktionsweise
- Handydiebstahl
- Einsatzszenarien**
- GPS-Ortung
- Laptop Security
- Partnerprogramm
- Onlineshop

Handy-Ortung

Login-Name

Passwort

[Noch keinen Login-Namen](#)

[Passwort vergessen](#)

Verschiedene Einsatzszenarien der Handyortung

Es gibt vielfältige Einsatzmöglichkeiten der Handyortung. Auch Ihnen fallen bestimmt auf Anhieb einige ein. Aber seien Sie ehrlich: Wären Sie darauf gekommen, dass die Handyortung Ihnen nach einem Unfall mit dem Fahrrad im Gelände hilfreich sein kann?

Die Handyortung ist sowohl für private wie gewerbliche Zwecke nutzbar!



Baumaschinen



LKWs, Container und Frachtgut



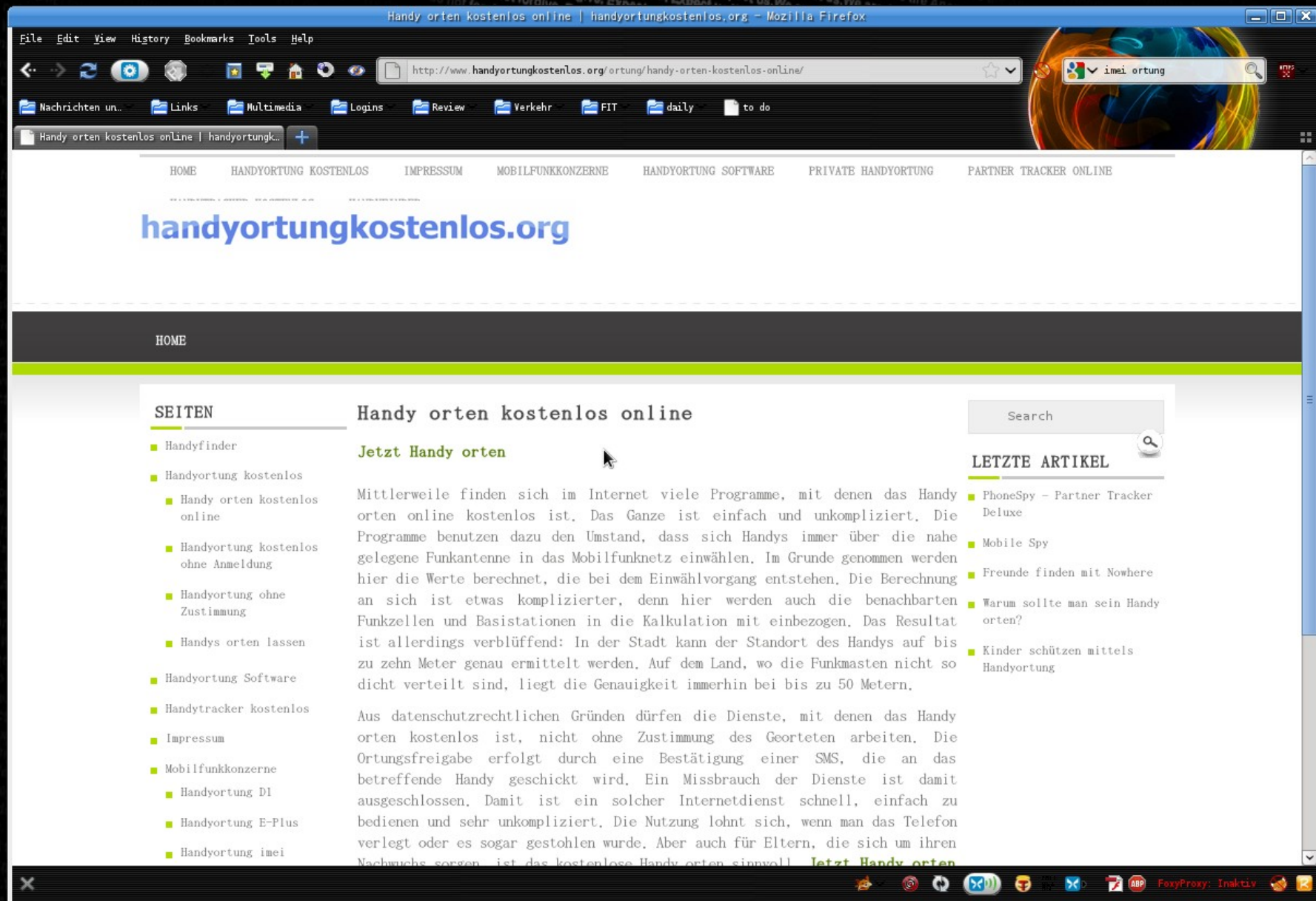
Sport- und Freizeitaktivitäten



Kinder







Handyortung

Orte die Handys deiner Freunde!

Handyortungskostenlos.org

Impressum

Impressum

Guerilla Mobile Berlin GmbH
Pfuelstrasse 5
10997 Berlin

Support: [hier klicken](#)

Telefon: 01805 035318 (0,14 EUR/Min, Festnetz 42Cent/min Mobilfunk)
Fax: 01805 035319 (0,14 EUR/Min, Festnetz 42Cent/min Mobilfunk)

Geschäftsführung: Oliver Thiel, Maurice Reimer

Registergericht: Berlin

Registernummer: HRB 11666 7B

Umsatzsteuer-Identifikationsnummer gemäß 27a UStG: DE 264719846

Beauftragter für Datenschutz und Jugendschutz: Stephan Becker

Mobile Spy



Copyright 2003-2011 © Mobile Spy | IMPRESSUM | AGB

Handyortung

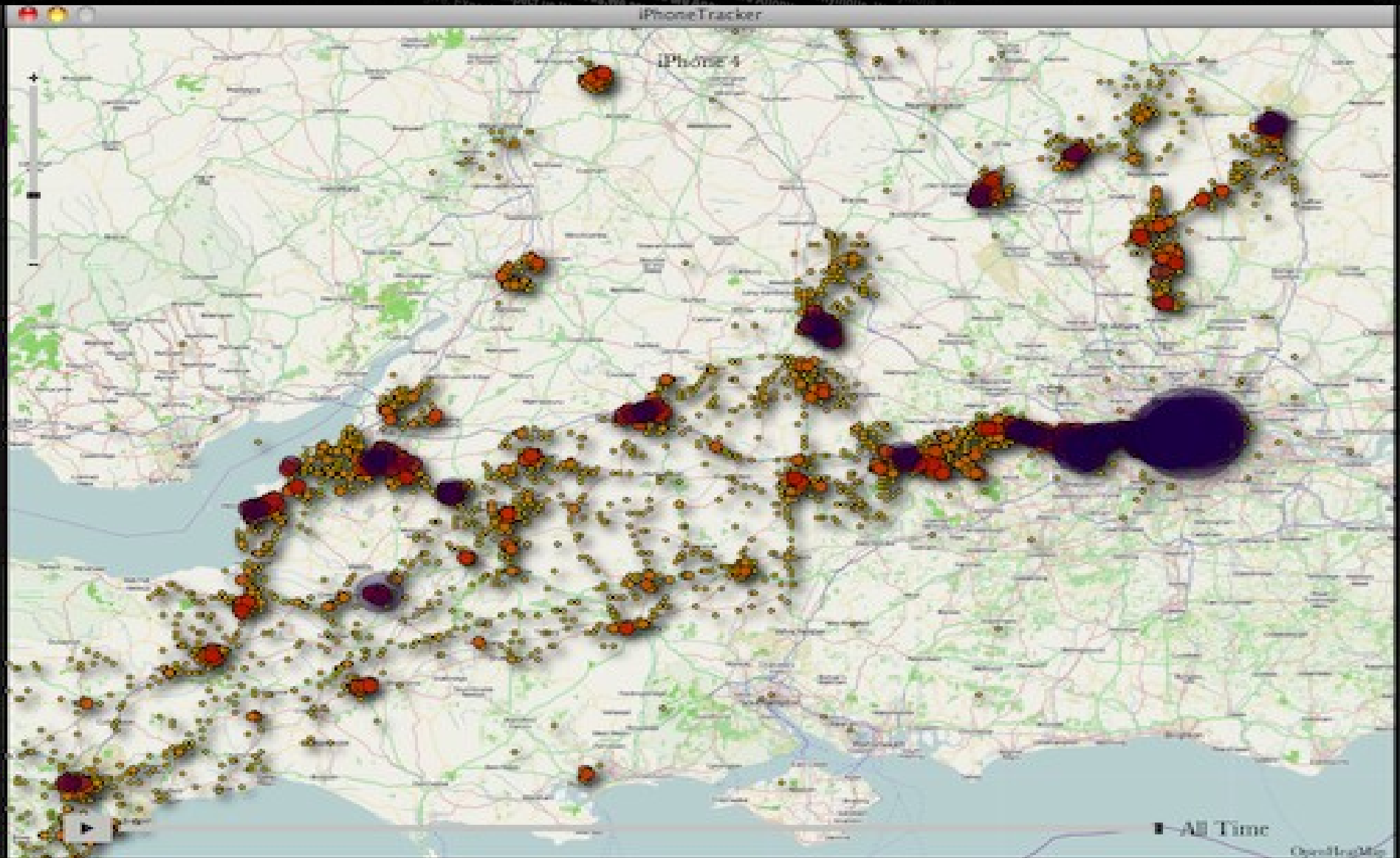
• Handyortungskostenlos.org

– Ortung gibts keine!

– Abofalle!

Bekannte Abofalle!

So schnell geht das!



Handyortung

• Ortung

auch mit deaktiviertem GPS
und Mobilfunknetz:

CID

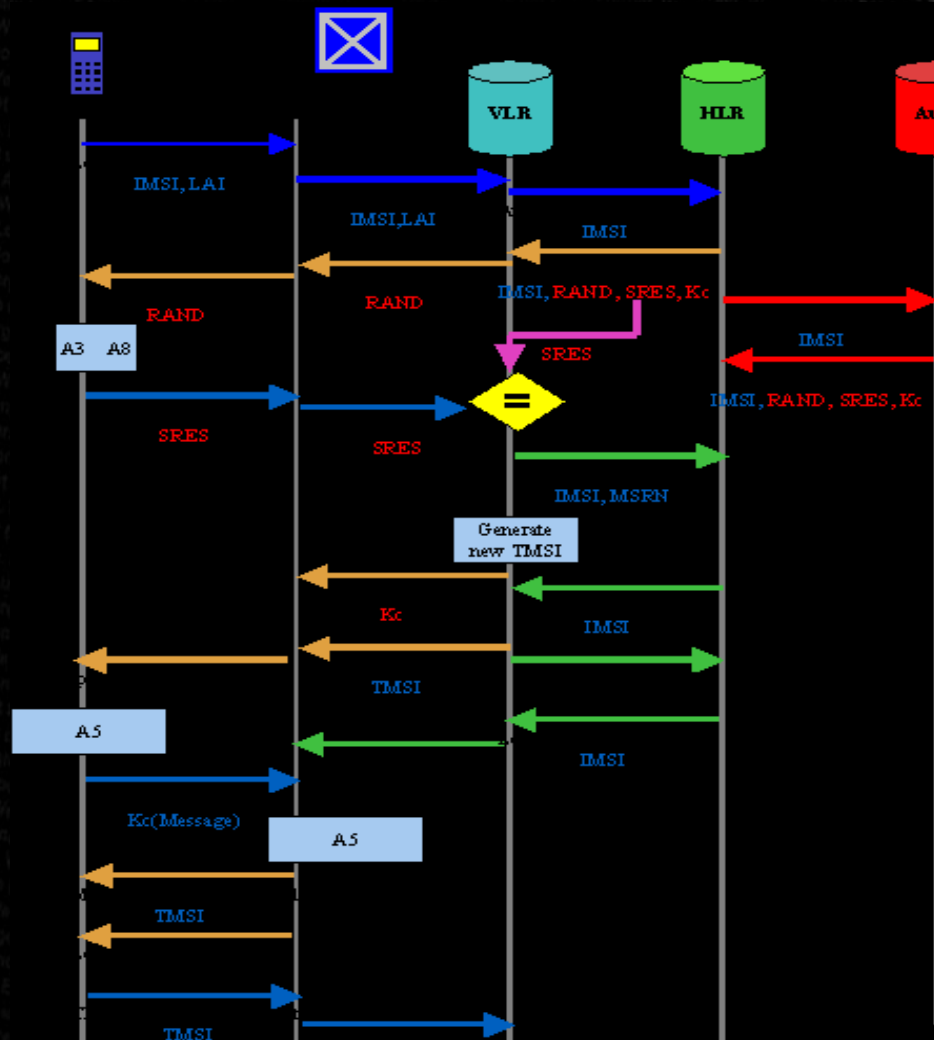
– LAC

– (Ungenau) Ortung jederzeit
möglich -> GSM Funkzelle

– <http://www.umtslink.at>



Handyortung



• GSM Anmeldung

Einbuchung in Providernetz:

– CID, LAC, IMSI

– Location Registration

– Location Update

– Ortung des Standorts ist unbedingt notwendig für Telefonfunktion

Speicherung:

– CID

– Uhrzeit

Bis zu 180 Tage

– IP Adresse

– IMSI

Handyortung

Telekommunikationsgesetz

Teil 7 - Fernmeldegeheimnis, Datenschutz, Öffentliche Sicherheit (§§ 88 - 115)

Abschnitt 2 - Datenschutz (§§ 91 - 107)

§ 96 Verkehrsdaten

(1) Der Diensteanbieter darf folgende Verkehrsdaten erheben, soweit dies für die in diesem Abschnitt oder in § 2 oder § 4 des Zugangsschwerungsgesetzes genannten Zwecke erforderlich ist:

1. die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten,
2. den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
3. den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,
4. die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
5. sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten,

Diese Verkehrsdaten dürfen nur verwendet werden, soweit dies für die in Satz 1 genannten oder durch andere gesetzliche Vorschriften begründeten Zwecke oder zum Aufbau weiterer Verbindungen erforderlich ist. Im Übrigen sind Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen,

(2) Eine über Absatz 1 hinausgehende Erhebung oder Verwendung der Verkehrsdaten ist unzulässig.

• Rechtsgrundlage

TKG, TDDSG, TDSV,
BDSG

• TKG

§ 96 und 97 regelt die
Speicherung der sog.
„Verkehrsdaten“ zu
Abrechnungszwecken

• Verstoß =
Ordnungswidrigkeit

• Max. € 50.000,-

<http://www.itrechtler.de>

Handyortung

• TKG

§ 98 regelt die Speicherung von Standortdaten

Nur nach Einwilligung

- Nur Anonymisiert
- Zustimmungspflichtig im Einzelfall (> 5 Ortungen)
- Widerspruchsmöglichkeit
- Verpflichtung zur Ortung bei Notrufnummern

Abschnitt 2 - Datenschutz (§§ 91 - 107)

§ 98 Standortdaten

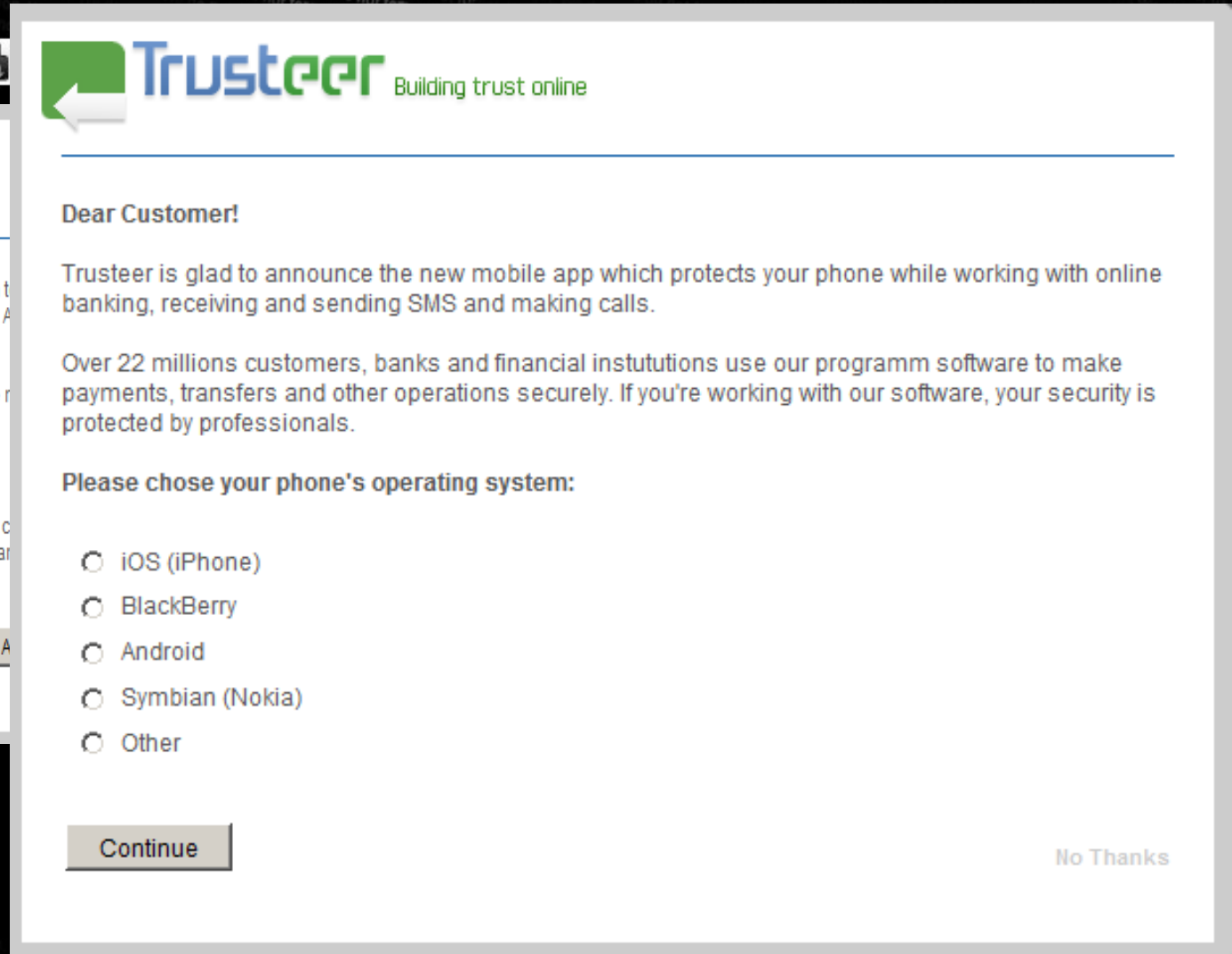
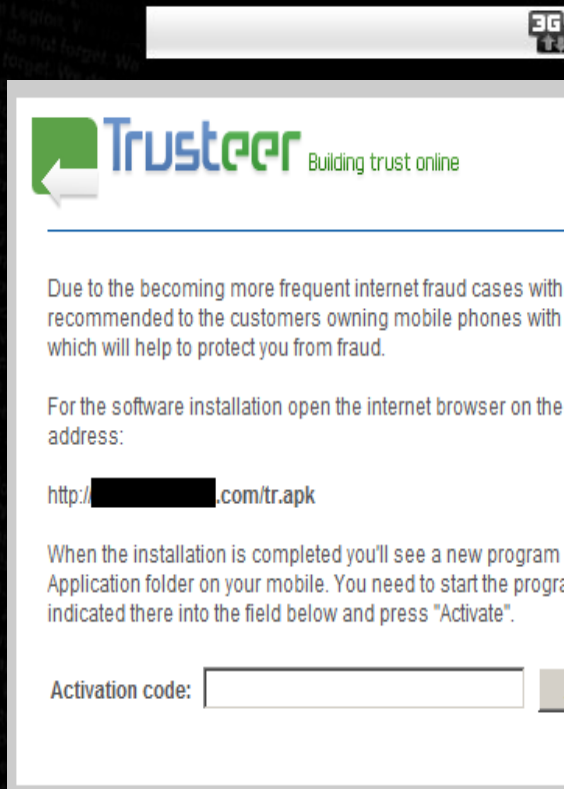
(1) Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder Telekommunikationsdiensten für die Öffentlichkeit verwendet werden, dürfen nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer seine Einwilligung erteilt hat. Werden die Standortdaten für einen Dienst mit Zusatznutzen verarbeitet, der die Übermittlung von Standortdaten eines Mobilfunkendgerätes an einen anderen Teilnehmer oder Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen sind, zum Gegenstand hat, muss der Teilnehmer abweichend von § 94 seine Einwilligung ausdrücklich, gesondert und schriftlich erteilen. In diesen Fällen hat der Diensteanbieter den Teilnehmer nach höchstens fünfmaliger Feststellung des Standortes des Mobilfunkendgerätes über die Anzahl der erfolgten Standortfeststellungen mit einer Textmitteilung zu informieren, es sei denn, der Teilnehmer hat gemäß § 95 Abs. 2 Satz 2 widersprochen. Der Teilnehmer muss Mitbenutzer über eine erteilte Einwilligung unterrichten. Eine Einwilligung kann jederzeit widerrufen werden.

(2) Haben die Teilnehmer ihre Einwilligung zur Verarbeitung von Standortdaten gegeben, müssen sie auch weiterhin die Möglichkeit haben, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und unentgeltlich zeitweise zu untersagen.

(3) Bei Verbindungen zu Anschlüssen mit der Rufnummer 112, den in der Rechtsverordnung nach § 108 Abs. 2 festgelegten Rufnummern oder der Rufnummer 124 124, hat der Diensteanbieter sicherzustellen, dass nicht im Einzelfall oder dauernd die Übermittlung von Standortdaten ausgeschlossen wird.

(4) Die Verarbeitung von Standortdaten nach den Absätzen 1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers des öffentlichen Telekommunikationsnetzes oder öffentlich zugänglichen Telekommunikationsdienstes oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln.

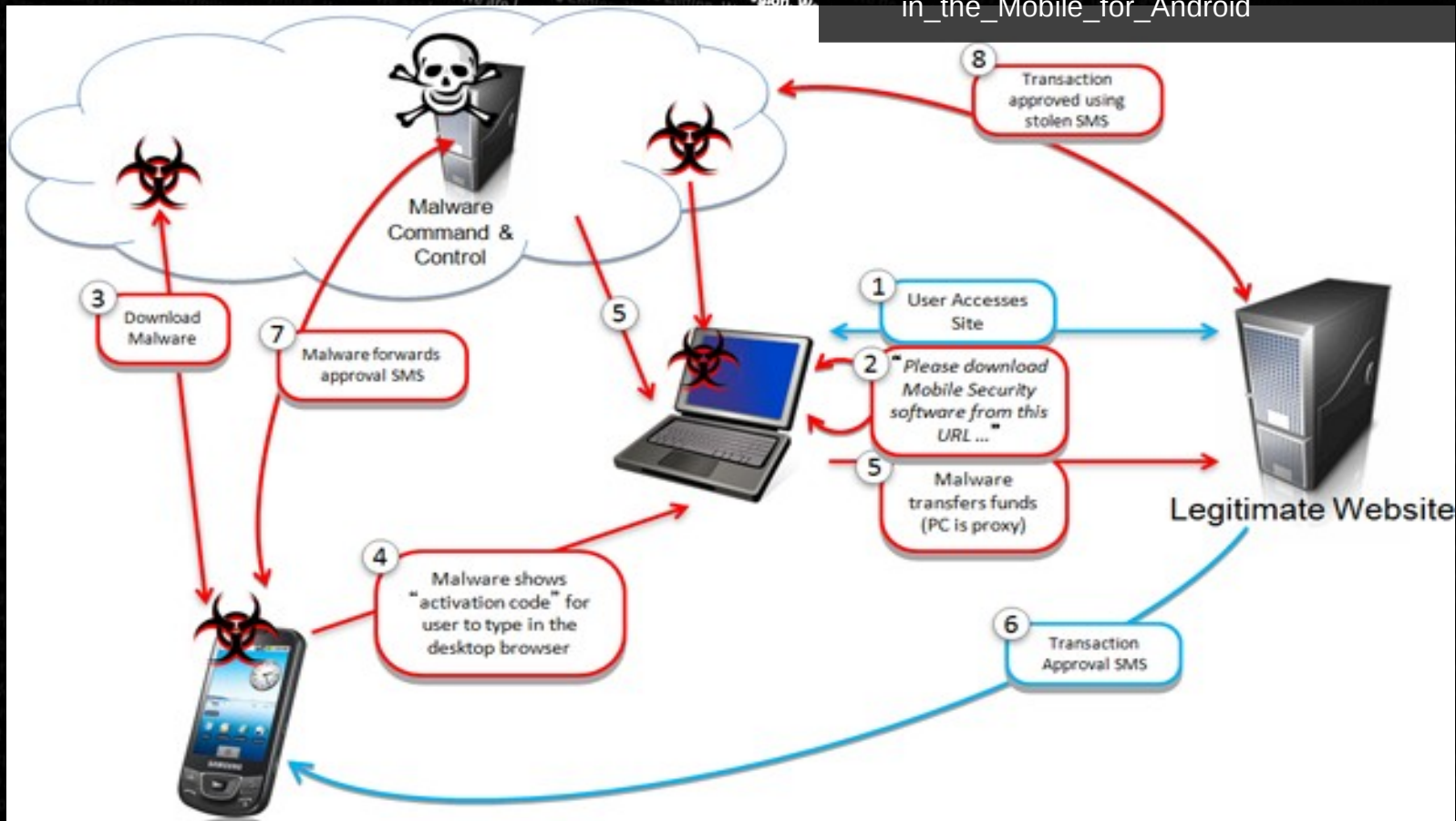
Malware



Malware

- Beispiel:

http://www.securelist.com/en/blog/208193029/ZeuS_in_the_Mobile_for_Android



„Ich bin root, ich darf das...!“

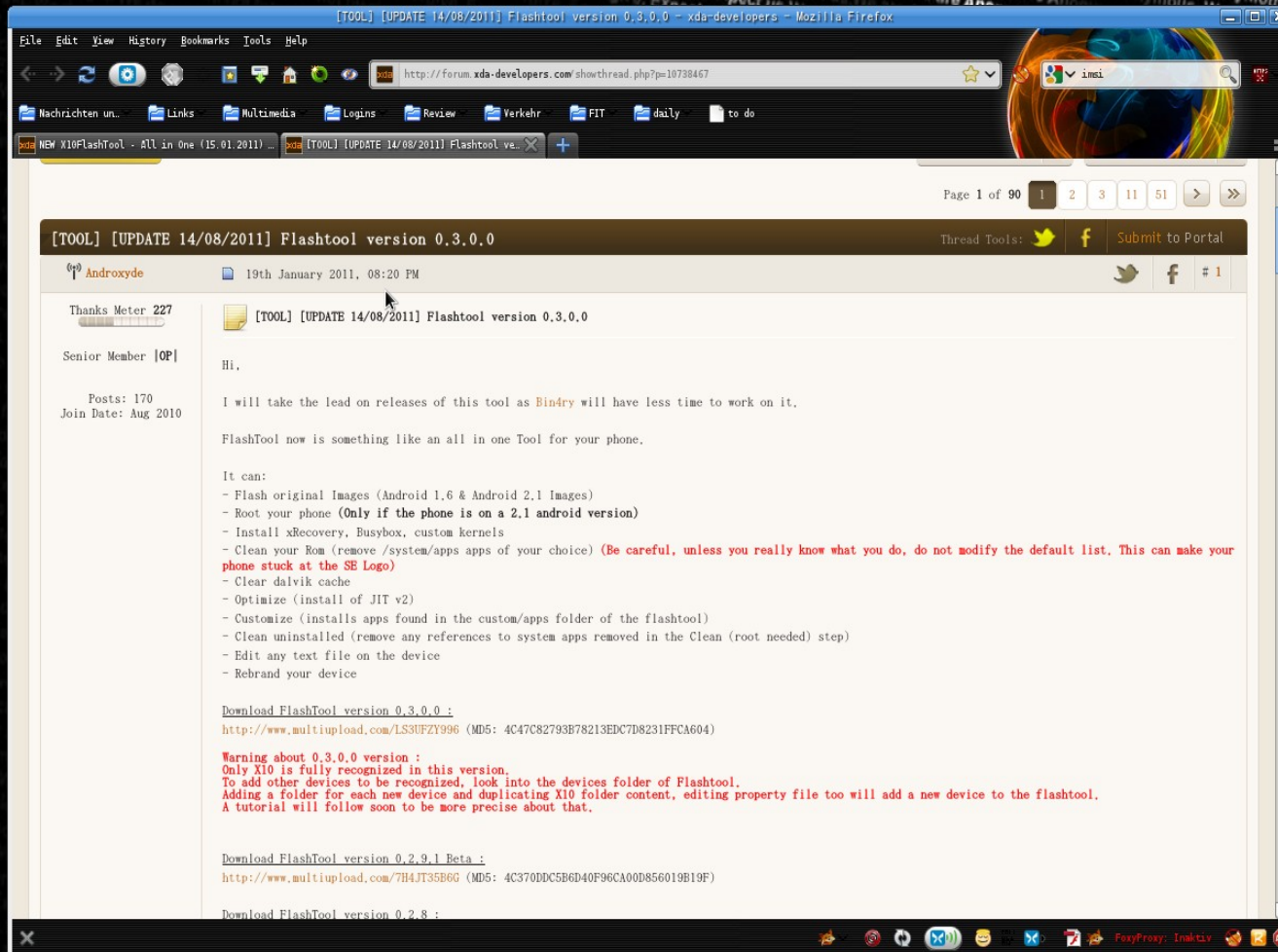
- Root Exploit
- Custom Firmware
- Tethering
- Unlock Bootloader
- Custom Software
 - Terminal
 - SSH
 - WebKey
 - APG
 - File Manager
- Configs



„Ich bin root, ich darf das...!“

- Root Exploit
- Custom Firmware
- Unlock Bootloader
- Custom Software
- Configs

xda-developers.com



Innenansichten



• Nutzungsstatistiken

– Zeit

– Startzähler

Anwendung

– 10080 anonymous usage statistics

• Wifi

– Status

– Configs

Agenda

Anforderungen an die Handsicherheit

Antworten

- Distribution von
 - Firmware
 - Applikationen
- Berechtigungskonzept
 - „weniger ist mehr“
- Locked Bootloader
- User Rights Management
- DRM
- Digitale Signaturen
- Verschlüsselung
- Datenschutz



Antworten

Benutzer Akzeptanz ?????

- Distribution von
- Applikationen
- Berechtigungskonzept
- „weniger ist mehr“
- Locked Bootloader
- User Rights Management

Marktanteile

Umsatz

- Digitale Signaturen
- Verschlüsselung
- Datenschutz

Shareholder Value

Antworten

Tun Sie selbst etwas !

Agenda

Empfehlungen und Tools

Empfehlungen

News

Home Newsticker 7-Tage-News News-Archiv Leser
heise online > News > 2011 > KW 41 > iPhone 4S: Nutzer

16.10.2011 12:14

iPhone 4S: Nutzer melden Probleme mit UPDATE

vorlesen / MP3-Download

In Userforen melden derzeit einige Käufer des iPhone Probleme mit der Netzverbindung. Die Nutzer berichten dabei von abgebrochenen Telefonaten, fehlender Netzverbindung, nicht erkannter SIM-Karten und verzögertem SMS-Versand. Wieviele Anwender davon tatsächlich betroffen sind und ob das Problem an der SIM-Karte, der Hardware, iOS 5 oder an der Kombination der drei Faktoren liegt, ist unklar. Vor allem Kunden Deutschen Telekom melden sich in den Foren zu Wort, scheinen auch andere Netzbetreiber betroffen zu sein. Mitarbeiter der Telekom sprach in einem T-Online-Forum von "keinem providerabhängigem Phänomen".

[Update] Mittlerweile hat die Telekom die Probleme dem iPhone 4S bestätigt. Das Problem trete auf, wer "eine bereits aktivierte Micro-SIM Karte (z.B. aus iPhone 4), die mit einer PIN geschützt ist, in das iPhone 4S gelegt wird". Es trete bei allen Netz-Problem auf. Als provisorische Problembeseitigung empfiehlt die Deaktivierung der PIN-Abfrage (Anleitung als PDF-Datei) so die Telekom, gebe es Probleme beim Update älterer bei der Aktivierung des iPhone 4S. Grund hierfür sei Überlastung der Apple-Server. [/Update]



Anleitung zur Deaktivierung der PIN-Abfrage der Micro-SIM

Als provisorische Lösung der Probleme mit dem neuen iPhone 4S schlagen wir vor, die PIN-Abfrage der Micro-SIM vor dem Einsetzen in das neue iPhone 4S auszuschalten. Diese Lösung schafft in den meisten Fällen Abhilfe.

Benutzen Sie ein anderes Micro-SIM fähiges Gerät, z.B. ein iPhone 4, und führen Sie die folgenden Schritte aus:

1. Wählen Sie vom Startbildschirm „Einstellungen“ und dann „Telefon“



2. Wählen Sie im Menü „SIM-PIN“



3. Stellen Sie den Schieberegler auf aus (0)



empfehl

age

ren

Empfehlungen



• Einstellungen ändern:

- PIN Abfrage einschalten
- Passwörter unsichtbar
- Display-Sperre einschalten
- SIM Sperre einschalten
- Anmeldeinformationspeicher mit Passwort schützen
- Standortdaten und GPS deaktivieren

Empfehlungen

- Einstellungen ändern:
 - Drahtlos & Netzwerke



Einstellungen



- Dienste abschalten

- GPS

- Bluetooth

- Data

- Funkzellenortung

- UMTS/GPRS

und nur einschalten, wenn man sie nutzt!

- Vorteil

- Schont den Akku

- Erhöht die Sicherheit

Einstellungen

13:49
cwemail:Posteingang (6) (Nächster Abruf @ 1...

Re: update

»Cosima [IT-Stammtisch Darmst... 8:06

Ticket Sales for Wyrd Sisters.

ESOC Theatre Group 13.10.2011

C246144540 Ihr Anliegen zur Bandb...

Einstellungen

Ordner-einstellungen

Kontoeinstellungen

Globale Ein...

13:55
Private Schlüssel verwalten

Christoph Weinandt (new, feb 2011)

<mail@christoph-weinandt.de>

Christoph Weinandt (temp schlüssel T410)

<weinandt@wiwi.uni-frankfurt.de>

LinkedIn Timescape™

Kryptographie

OpenPGP Provider

APG

Auto-sign

Email Adresse des Kontos verwenden um Signaturschlüssel zu schützen.

- Email

- TLS

- SSL

- IMAP

- PGP

Aktivieren!

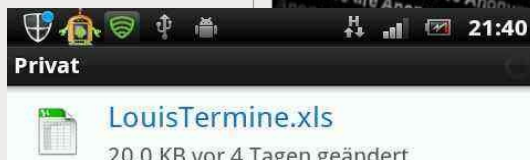
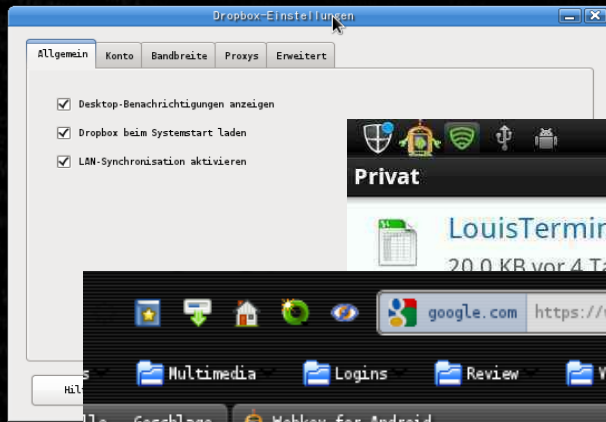
- Vorteil

- Verschlüsselung der Emails

- Tool

- APG, K9 Mail

Einstellungen



- Cloud Computing
- Backup
- Filesharing



Leiablage

information is transferred and becomes subject to a different privacy policy.

Information security

We take appropriate security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data. These include internal reviews of our data collection, storage and processing practices and security measures, including appropriate encryption and physical security measures to guard against unauthorized access to systems where we store personal data.

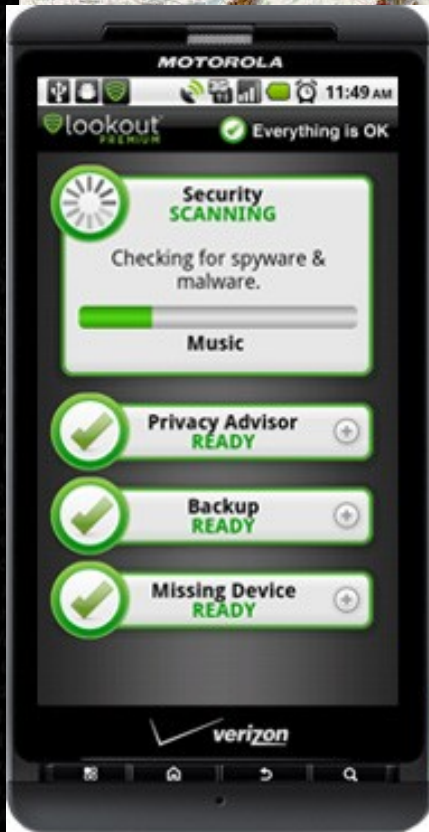
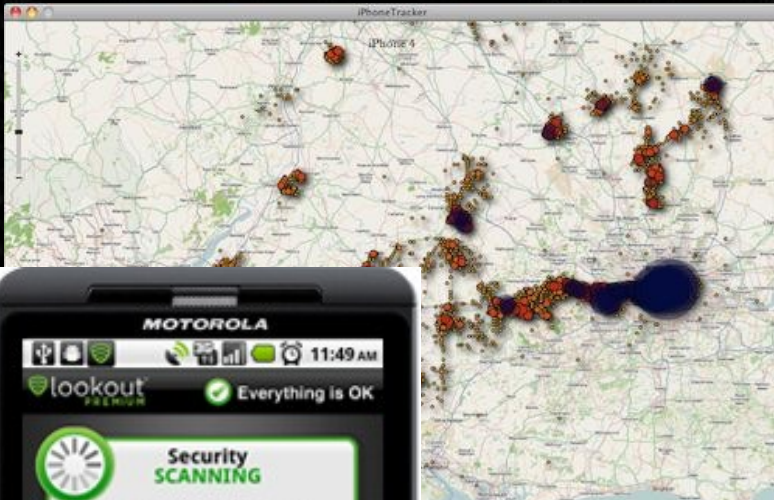
We restrict access to personal information to Google employees, contractors and agents who need to know that information in order to process it on our behalf. These individuals are bound by confidentiality obligations and may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations.

sselt nutzen

- Nicht empfohlen:
- Nutzungsbedingungen
- Keine Verschlüsselungsmöglichkeit

Tools

- Onlinebanking
 - StarMoney
- Android Firewall
- SSH
- VPN
- Schutz vor Verlust
 - Iphone Tracker
 - Lookout
- Überwachung der Datennutzung
 - Data counter widget



Tools

- Lookout „standard“

- Malware Scanner gegen Trojaner

- Backup zur automatisierten Datensicherung

- Missing Device zum wiederfinden eines verlorenen oder gestohlenen Handys

- Lookout „premium“

- Privacy advisor zum Schutz der eigenen Daten

- Safe Browsing zum Schutz vor Malwareseiten beim Surfen

- Remote Lock zum Sperren und Löschen eines verlorenen Handys

\$ 2,99/monat oder \$ 29,99/jahr



Tools

• Lookout

Lookout Mobile Security :: Home - Mozilla Firefox

History Bookmarks Tools Help

mylookout.com https://www.mylookout.com/home

Links Multimedia Logins Review Verkehr FIT daily

iPhone 4S: Nutzer melden Problem Webkey for Android

lookout MOBILE SECURITY

Android 17 [Edit] Connected

Add New Device

Dashboard Security Back

Everything is OK!

Security PROTECTED

Your last security scan was 9 days ago.

Security Activity

Recent Activity

TODAY October 16

- You updated your settings.
- You successfully updated your settings.
- Your first sync was started.
- Your device was successfully activated.

October 10

lookout

Stop Screaming

Found less than a minute ago
11:02 pm
Sunday, October 16, 2011
Open in Google Maps
Notify your friends: [Facebook icon] [Twitter icon]
Can't get to your phone?
Lock or Wipe to keep your data secure.

Location History

Location Settings Delete All

Tools

Android Firewall

- Zeigt versteckte Prozesse
- Blockieren oder Erlauben eines Prozesses

Iptables Syntax

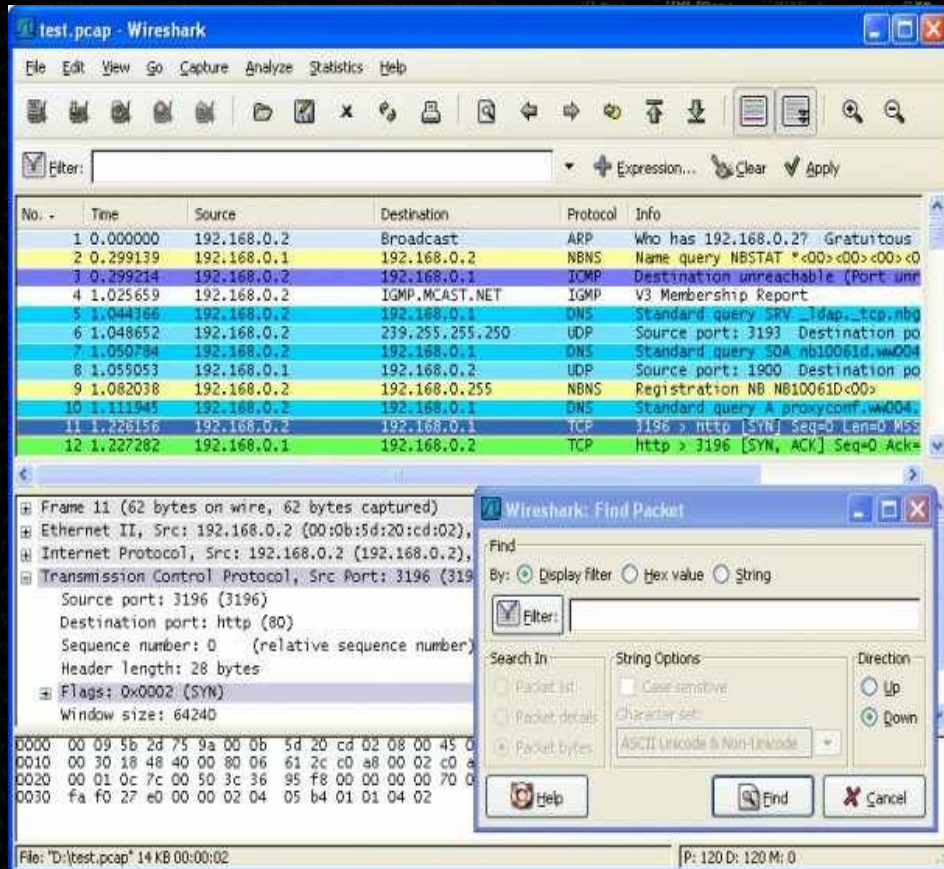
- Iptables kommt von Linux wie Android auch



Agenda

LiveDemos

Live Demo „Verkehrsdaten“



- Mitschnitt Handynutzung

- Freiwillige vor!

- Pop3 Passwort

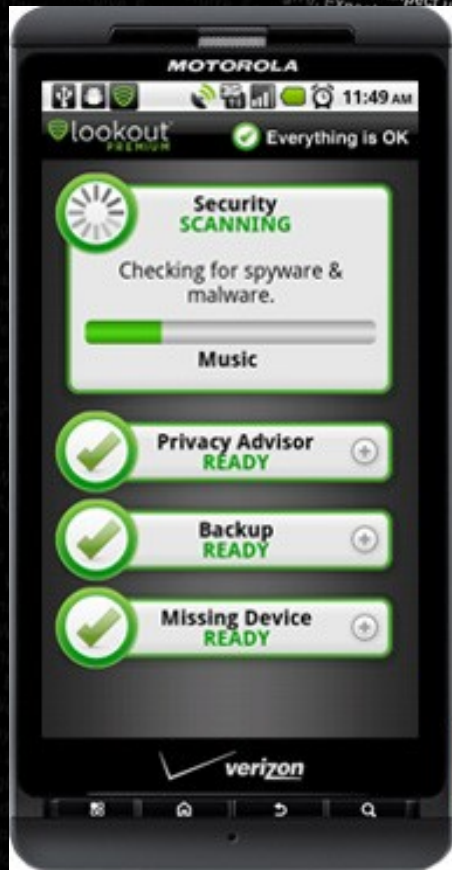
- Login

- Emailadresse

LiveDemo „Lookout“

- Features

- × Malware scanner
- × Privacy advisor
- × Online Backup
- × Missing Device



LiveDemo „DroidWall“

• Features

x Paketfilter

x Eingehend/Ausgehend

x Block/allow Policy

x ROOT notwendig

x Logging

x Abschaltbar



Agenda

Vielen Dank für Ihre Aufmerksamkeit !

Vortragsfolien in Kürze unter

www.it-stammtisch-darmstadt.de



Herzlich willkommen

Dieser Vortrag beschäftigt sich mit dem Thema „Handysicherheit“.



Ein paar Worte vorweg zu mir:

Ich bin Fachinformatiker der Fachrichtung „Systemintegration“ und habe mich vor 10 Jahren während meiner langjährigen Tätigkeit als IT-Berater auf „IT-Sicherheit“ spezialisiert.

Neben einigen Zertifizierungen im Bereich von Systemen zur Netzwerkabsicherung und Netzwerkbetrieb habe ich viele Projekte in diesem Bereich durchgeführt.

Da ich mein Hobby zum Beruf gemacht habe, sind die teilweise unüblichen Arbeitszeiten nicht das Problem und ansonsten ist das Ganze erstaunlich familienkompatibel.

Seit 2 Jahren arbeite ich für die Freudenberg IT in Weinheim im Bereich „Managed Network Services“ und „IT-Sicherheit“. Dort betreue ich hauptsächlich Netzwerke im Banken- und Grosskundenumfeld. Meine Aufgaben sind neben dem Design auch der Betrieb sicherer Netzwerke.

Handysicherheit



19.10.2011

IT-Stammtisch Darmstadt

3/ 48

5/ 48

Danke für Ihre Aufmerksamkeit –
wenn Sie Fragen haben oder wenn
Sie ein paar Sachen gezeigt
bekommen wollen, stehe ich Ihnen
gerne zur Verfügung

1994...

• Telefonieren

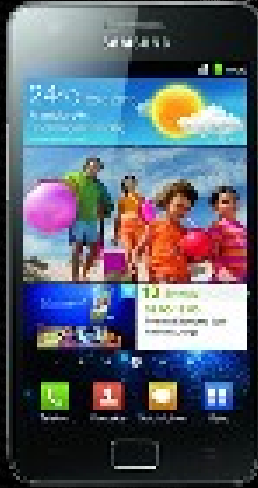


19.10.2011

IT-Stammtisch Darmstadt

6/ 48

2011



- Email
- Chat
- Soziale Netzwerke
- Online Bezahlen
- Online Banking
- Internet Radio
- Internet TV
- SMS
- Adressen und Termine
- Cloud Computing
- Telefonieren

19.10.2011

IT-Stammtisch Darmstadt

7/ 48

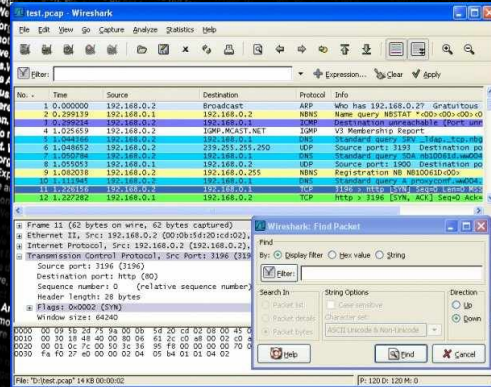


Danke für Ihre Aufmerksamkeit – wenn Sie Fragen haben oder wenn Sie ein paar Sachen gezeigt bekommen wollen, stehe ich Ihnen gerne zur Verfügung

Internet

- Verschlüsselung?
- Privatsphäre?
- Datensicherheit?

Fehlanzeige!



Gefährdungslage

- „Locationgate“
Apple Iphone / Android
- Malware
- Berechtigungen
- Anwendungen von
Drittanbietern
- Trojaner
Zeus
- Custom Firmware
- (Un-)Locked Bootloader
- Abofallen
- Dresden:
„Polizei erfasst Tausende Handydaten“



Gefährdungslage

• Ziele:

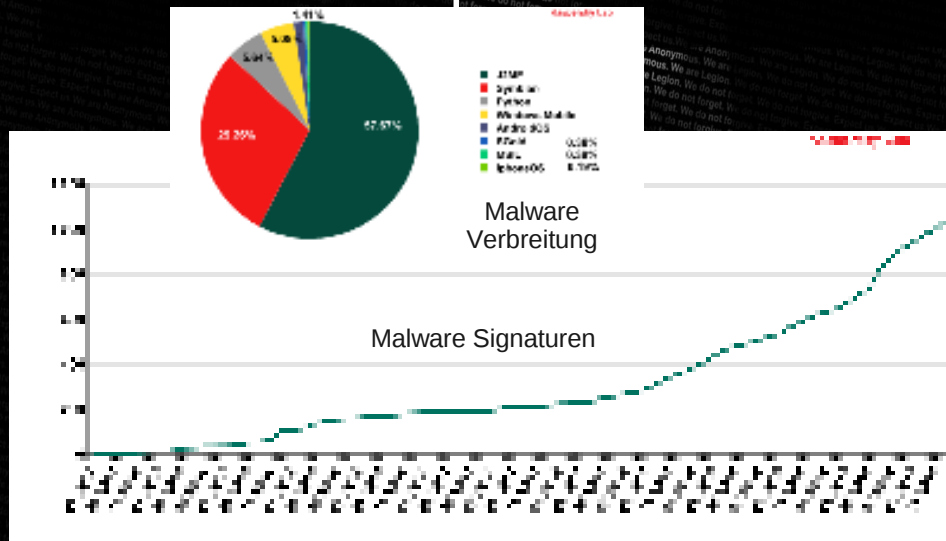
- mTAN/Banking
- Ihre Daten

• Malware ist ein lukrativer Markt

- Botnetze
- Profiling
- Tracking

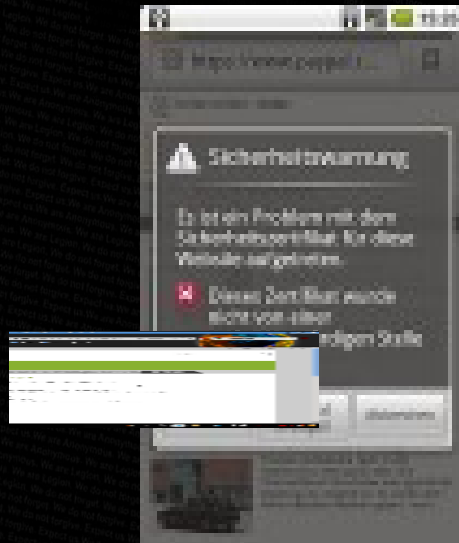


Mal ein paar Zahlen



http://www.securelist.com/en/analysts/204793168/Mobile_Malware_Evolution_An_Overview_Part_4#14

Achtung – Wichtig!



- Software (Apps)
- Diebstahl und Verlust
- Tracking
- Datensammelwut
- Anwendungsberechtigungen
- Jailbreak/Rooting
- Dropbox
- Abfallen

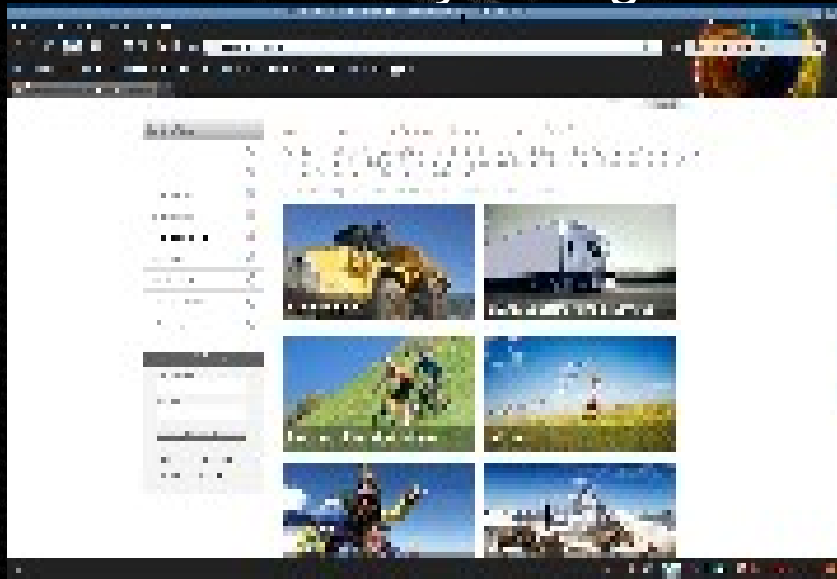
- MobileSpy
- jamba

Ihre Daten



- Werden genutzt für Werbung
- Werden genutzt für Statistiken und Auswertungen Ihres Verhalten
- Werden genutzt für Bewegungsprofile
- Werden 90 – 180 Tage lang gespeichert (obwohl dies rechtswidrig ist, TKG)
- Werden „mitgelesen“
- Stehen Staatsanwaltschaft und Urheberrechtinhabern zur Verfügung
- Sind in der Regel unverschlüsselt und Dritten zugänglich

Handyortung



19.10.2011

IT-Stammtisch Darmstadt

15/ 48



Handyortung

- Handyortungskostenlos.org

- Ortung gibts **keine!**

- Weiterleitung auf:

- Mobilespy.de

Bekannte Abofalle!

Handyortung

• Handyortungskostenlos.org

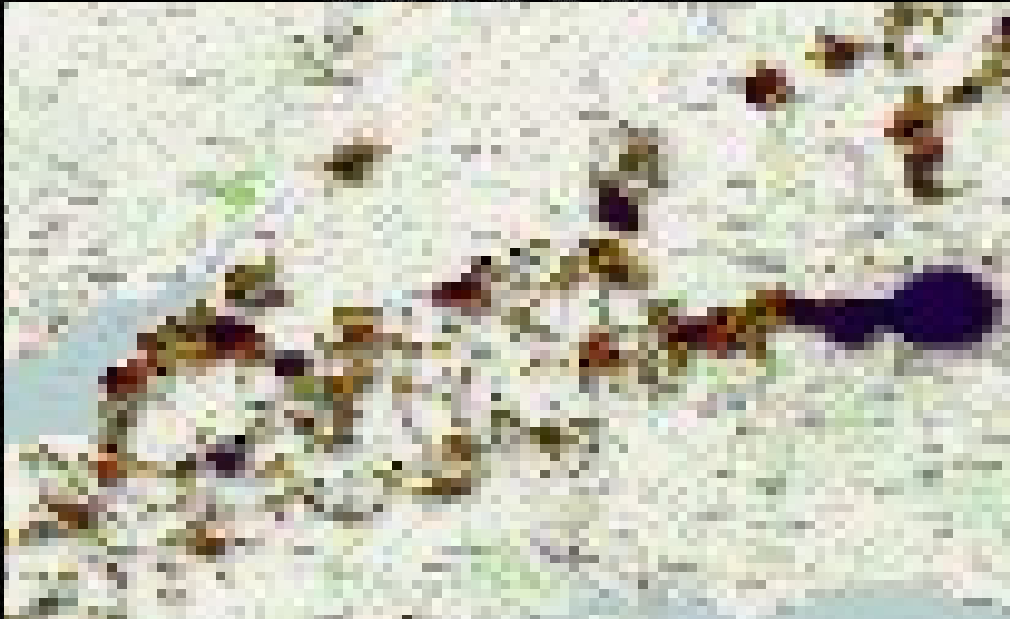
Ortung gibts keine!

Abofalle!

le

Bekannte Abofalle!

So schnell geht das!



19.10.2011

IT-Stammtisch Darmstadt

19/ 48

Handyortung

- Ortung

auch mit deaktiviertem GPS
und Mobilfunknetz:

CID
LAC

- (Ungenaue) Ortung jederzeit möglich -> GSM Funkzelle

- <http://www.umtslink.at>



19.10.2011

IT-Stammtisch Darmstadt

20/ 48

Handyortung

- GSM Anmeldung

Einbuchung in Providernetz:

CID, LAC, IMSI

Location Registration

Location Update

- Ortung des Standorts ist unbedingt notwendig für Telefonfunktion

Speicherung:

- CID

- Uhrzeit

- IP Adresse

- IMSI

Bis zu 180 Tage

Handyortung

- **Rechtsgrundlage**

TKG, TDDSG, TDSV,
BDSG

- **TKG**

§ 96 und 97 regelt die
Speicherung der sog.
„Verkehrsdaten“ zu
Abrechnungszwecken

- Verstoß =
Ordnungswidrigkeit
- Max. € 50.000,-

<http://www.itrechtler.de>

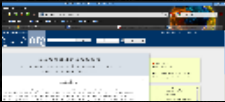


Handyortung

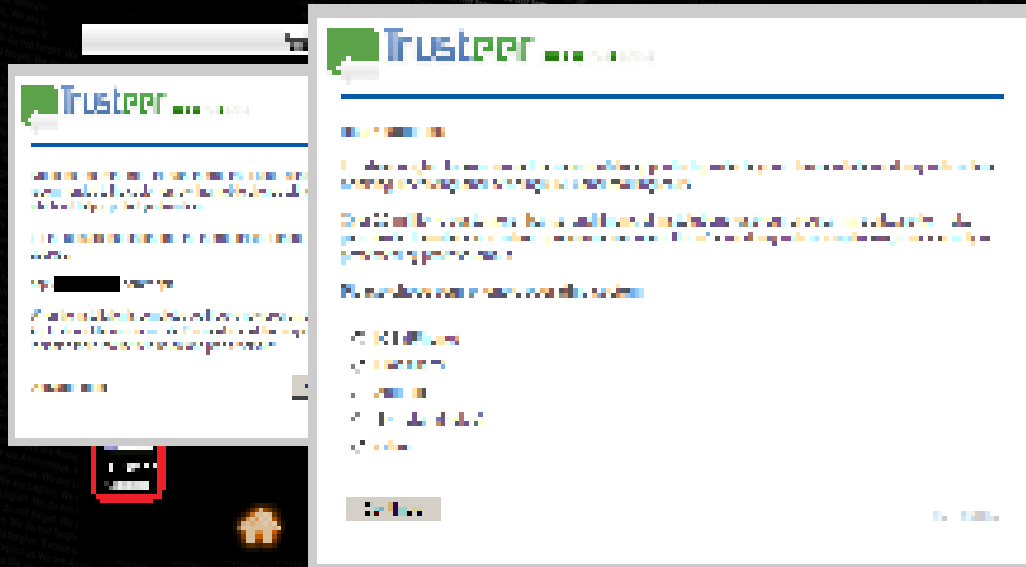
• TKG

§ 98 regelt die
Speicherung von
Standortdaten

- Nur nach Einwilligung
- Nur Anonymisiert
- Zustimmungspflichtig im
Einzelfall
(> 5 Orten)
- Widerspruchsmöglichkeit
- Verpflichtung zur Ortung
bei Notrufnummern



Malware

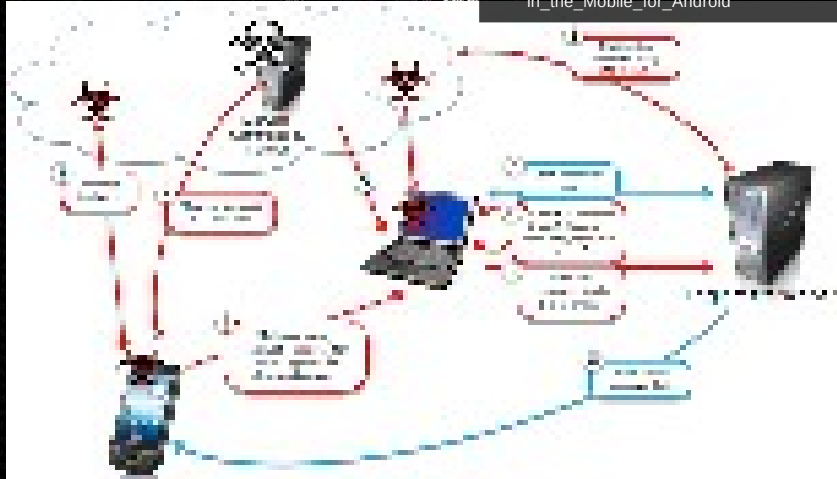


19.10.2011

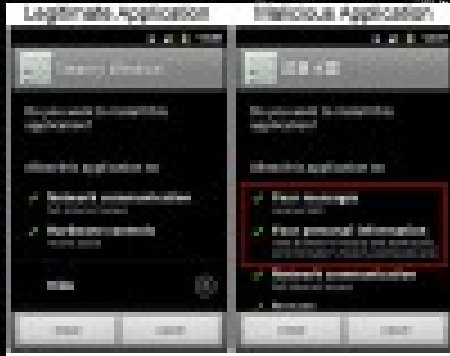
IT-Stammtisch Darmstadt

24/ 48

http://www.securelist.com/en/blog/208193029/ZeuS_in_the_Mobile_for_Android

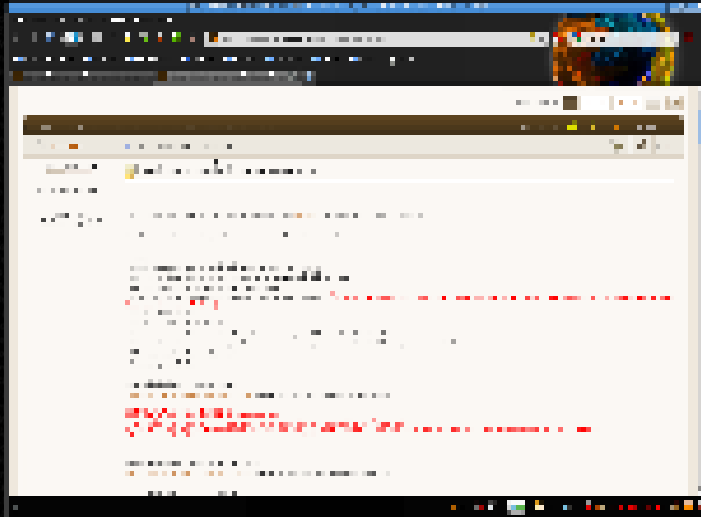


„Ich bin root, ich darf das...!“



- Root Exploit
- Custom Firmware
- Tethering
- Unlock Bootloader
- Custom Software
 - Terminal
 - SSH
 - WebKey
 - APG
 - File Manager
- Configs

„Ich bin root, ich darf das...!“



- Root Exploit
- Custom Firmware
- Unlock Bootloader
- Custom Software
- Configs

xda-developers.com

Innenansichten

- Nutzungsstatistiken

- Zeit

- Startzähler

- Anwendung

- 10080 anonymous usage statistics

- Wifi

- Status

- Configs

Agenda

Anforderungen an die Handysicherheit

19.10.2011

IT-Stammtisch Darmstadt

29/ 48

Danke für Ihre Aufmerksamkeit – wenn Sie Fragen haben oder wenn Sie ein paar Sachen gezeigt bekommen wollen, stehe ich Ihnen gerne zur Verfügung

Antworten

- Distribution von
 - Firmware
 - Applikationen
- Berechtigungskonzept
 - „weniger ist mehr“
- Locked Bootloader
- User Rights Management
- DRM
- Digitale Signaturen
- Verschlüsselung
- Datenschutz



- 31/ 48

Antworten

Tun Sie selbst etwas !

Agenda

Empfehlungen und Tools

19.10.2011

IT-Stammtisch Darmstadt

33/ 48

Agenda

Empfehlungen und Tools

19.10.2011

IT-Stammtisch Darmstadt

33/ 48

19.10.2011

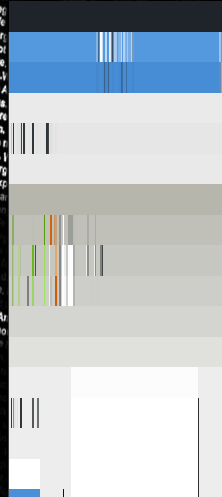
19.10.2011 IT-Stammtisch Darmstadt

19.10.2011 IT-Stammtisch Darmstadt 33/ 48

Danke für Ihre Aufmerksamkeit – wenn Sie Fragen haben oder wenn Sie ein paar Sachen gezeigt bekommen wollen, stehe ich Ihnen gerne zur Verfügung

Empfehlungen

- Ihr Provider empfiehlt



Abfrage

aktivieren

Empfehlungen

• Einstellungen ändern:

- PIN Abfrage einschalten
- Passwörter unsichtbar
- Display-Sperre einschalten
- SIM Sperre einschalten
- Anmeldeinformationspeicher mit Passwort schützen
- Standortdaten und GPS deaktivieren

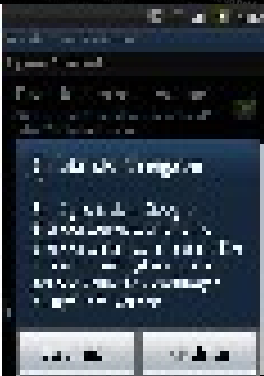


Empfehlungen

- Einstellungen ändern:
 - Drahtlos & Netzwerke



Einstellungen



• Dienste abschalten

- GPS
- Bluetooth
- Data
- Funkzellenortung
- UMTS/GPRS

und nur einschalten, wenn man sie nutzt!

• Vorteil

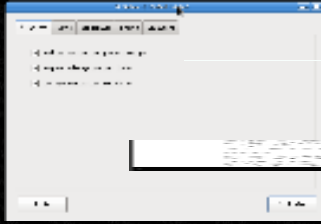
- Schont den Akku
- Erhöht die Sicherheit

Einstellungen



- Email
 - TLS
 - SSL
 - IMAP
 - PGP
- Aktivieren!
- Vorteil
 - Verschlüsselung der Emails
- Tool
 - APG, K9 Mail

Einstellungen



- Cloud Computing

- Backup

- Filesharing

- Lokale Dateiablage

- Streaming

Tools:

- Dropbox

- NUR verschlüsselt nutzen

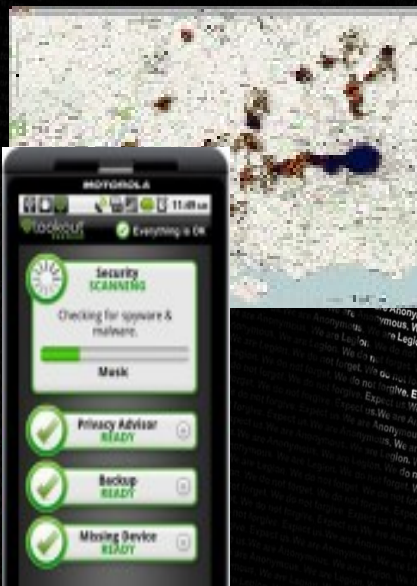
- Google Docs

- Nicht empfohlen:

- Nutzungsbedingungen

- Keine Verschlüsselungsmöglichkeit

Tools



19.10.2011

IT-Stammtisch Darmstadt

- Onlinebanking
- StarMoney
- Android Firewall
- VPN
- Schutz vor Verlust
- iPhone Tracker
- Lookout
- Überwachung der Datennutzung
- Data counter widget

40/ 48

Tools



• Lookout „standard“

– Malware Scanner gegen Trojaner

– Backup zur automatisierten Sicherung

– Find my Device zum wiederfinden verlorenen oder gestohlenen Handys

• Lookout „premium“

– Privacy advisor zum Schutz der eigenen Daten

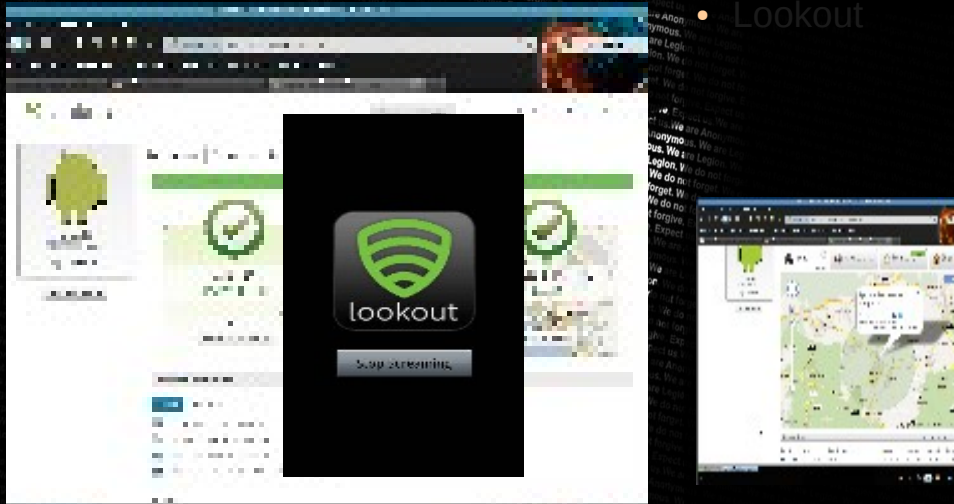
– Safe Browsing zum Schutz vor Malwareseiten beim Surfen

– Remote Lock zum Sperren und Löschen eines verlorenen Handys

\$ 2,99/monat oder \$ 29,99/jahr

Tools

- Lookout



Tools

Android Firewall

- Zeigt versteckte Prozesse
- Blockieren oder Erlauben eines
- Syntax
- Iptables kommt von Linux wie
- Android auch

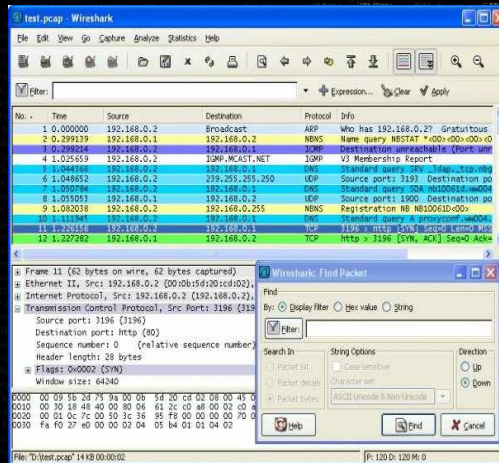




Danke für Ihre Aufmerksamkeit – wenn Sie Fragen haben oder wenn Sie ein paar Sachen gezeigt bekommen wollen, stehe ich Ihnen gerne zur Verfügung

Live Demo „Verkehrsdaten“

- Mitschnitt Handynutzung
- Freiwillige vor!
 - Pop3 Passwort
 - Login
 - Emailadresse



LiveDemo „Lookout“

• Features

Malware scanner

Privacy advisor

Online Backup

Missing Device



LiveDemo „DroidWall“

• Features

Paketfilter

Eingehend/Ausgehend

Block/allow Policy

ROOT notwendig

Logging

Abschaltbar



19.10.2011

IT-Stammtisch Darmstadt

47/ 48

Agenda

Vielen Dank für Ihre Aufmerksamkeit !

Vortragsfolien in Kürze unter
www.it-stammtisch-darmstadt.de

19.10.2011

IT-Stammtisch Darmstadt

48/ 48

Danke für Ihre Aufmerksamkeit – wenn Sie Fragen haben oder wenn Sie ein paar Sachen gezeigt bekommen wollen, stehe ich Ihnen gerne zur Verfügung