



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Was ist eigentlich das Darknet?

Matteo Cagnazzo

cagnazzo@internet-sicherheit.de

 @montimonte

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
<http://www.internet-sicherheit.de>

if(is)
internet-sicherheit.



- Wir werden über fragwürdige Inhalte sprechen
- Ich kann nicht versprechen, dass Sie sich nicht angegriffen fühlen
- Inhalte die wir entdecken könnten:
 - Drogen
 - Pornographie
 - Auftragsmörder
 - Geldwäsche
 - Hacking/Cracking
 - Etc.

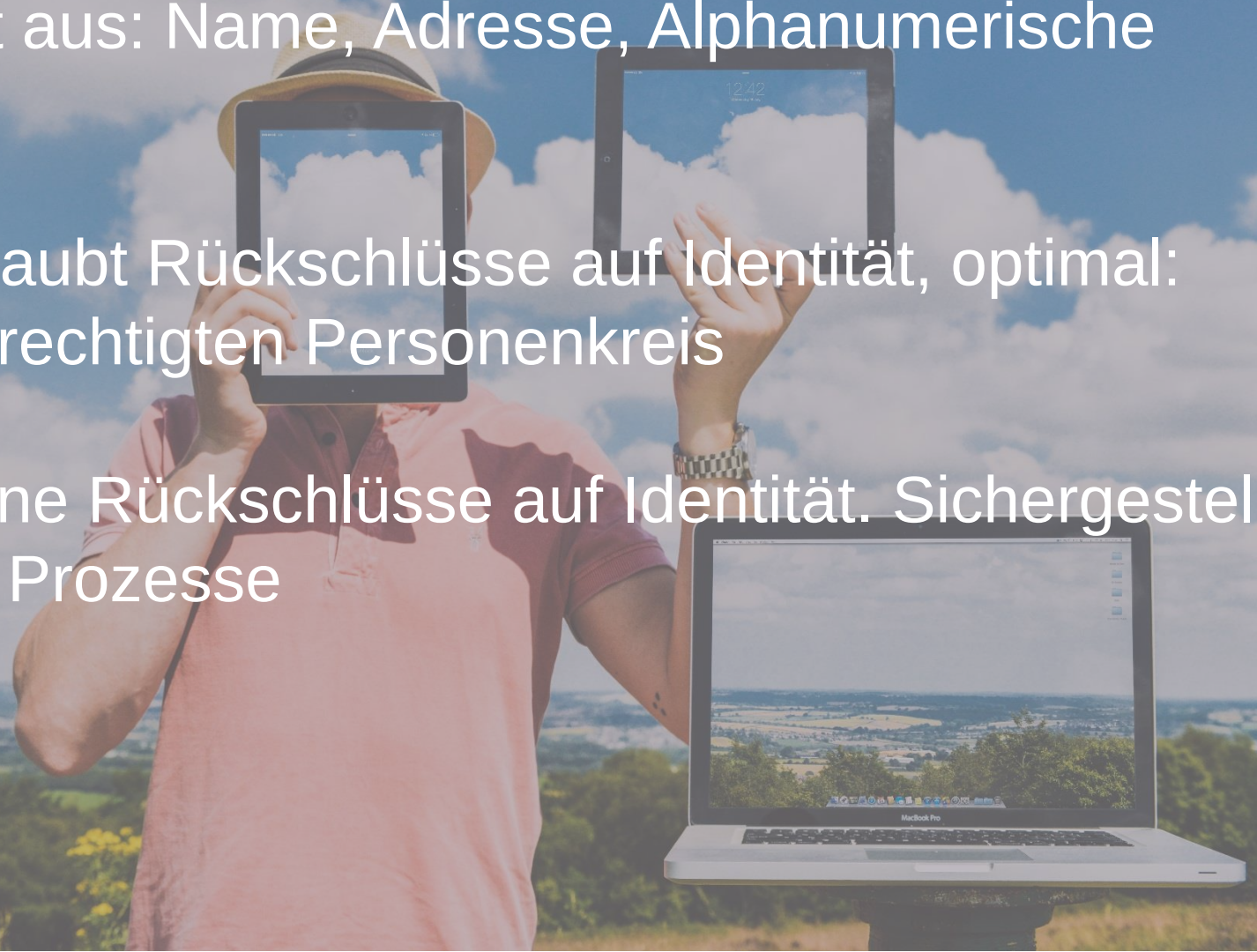


Identitäten, Pseudonyme und Anonymität

Identität besteht aus: Name, Adresse, Alphanumerische Ketten

Pseudonym: Erlaubt Rückschlüsse auf Identität, optimal: nur für einen berechtigten Personenkreis

Anonymität: Keine Rückschlüsse auf Identität. Sichergestellt durch anonyme Prozesse

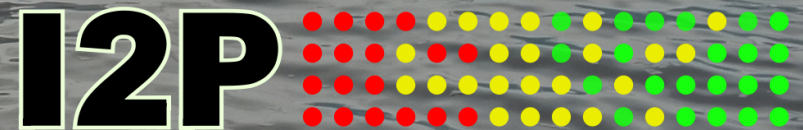
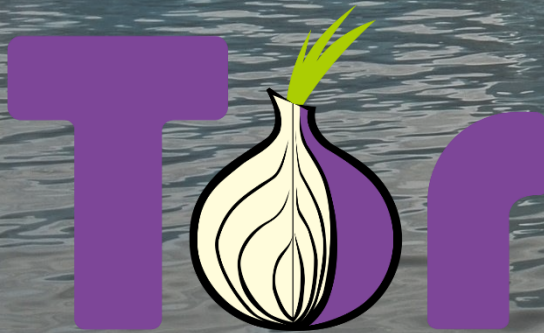


Abgrenzung zum normalen Netz

Surface Web: Alles was über Standardsuchmaschinen auffindbar ist

Deep Web: Universitätsdatenbanken, Foren mit Zugangsbeschränkung

Dark Web: Nicht auffindbar mit Suchmaschinen, spezielle Software wird benötigt



Wie kann ich Tor bekommen?

Viele potentielle Möglichkeiten

Out of the Box:

Herunterladen des Clients und .exe ausführen

Optimal: Kombination mit Virtualbox, Tails oder anderen Anonymitätsfördernden bzw. virtuellen Betriebssystemen

Was ist Tails*?

Linux Live System

Zwingt ab Installation sämtlichen Traffic durch Tor

Schreibt keine Daten auf die Festplatte

Vorinstallierte Software mit Privatheits- und Sicherheitsmechanismen

- Https everywhere

- OpenPGP

- Pidgin OTR

- Keepass



*Suche nach Tails klassifiziert Sie als Extremist

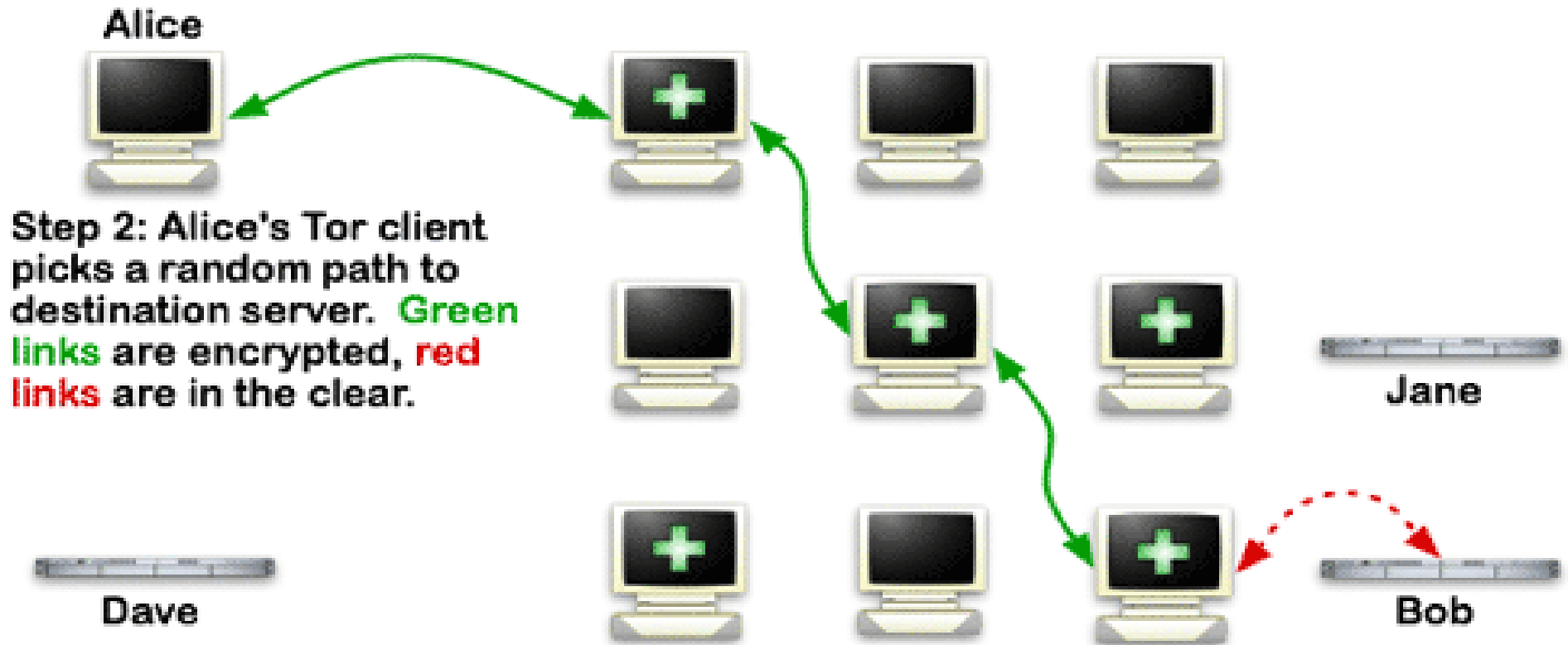
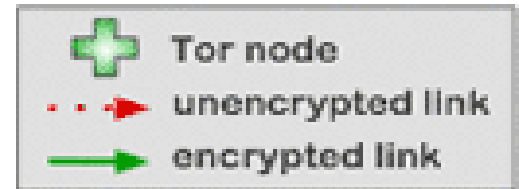
Wie funktioniert Tor?

How Tor Works: 1



Wie funktioniert Tor?

How Tor Works: 2



Hidden Services

Seiten die nur im Tor Netzwerk „leben“

.onion als Top Level Domain

Hidden Services nutzen Rendez-vous Punkte zur
Wahrung von Anonymität und Privatsphäre*

* Ziemlich Komplex, genauer: <https://www.torproject.org/docs/hidden-services.html.en>

Demotime



Government control starts between your ears when you tell yourself what your masters told you.

offers Feld

THOSE WHO SACRIFICE FREEDOM & SECURITY DESERVE NEITHER

Ich w...
Was...
nach...
YES WE SCAN

Die NSA wusste schon vorher, was für ein Schild ich malen würde.
fuck #PRISM

CRIME!
HAVE ST...
LIT...
ED + EDUC...
PEOPLE INSTEAD

1984 IS NOW

You are the first Afro PRESIDENT need to also censored for the SYSTEM?

YES WE CAN SCAN

TRANSPARENTER STAAT
STATT GLÄSERNER BÜRGER!
change.org/prism

Wer nutzt Tor

**„Tor wird nur von
Kriminellen genutzt“**





Warsaw Chopin Airp...

Folgen

Gefällt 16 Mal

4Std.

mysweetime #businesstrip #firststop
#boardingpass #boarding #airport #plane
#byplane #takeoff #lufthansa #delegacja
#poczatekpodrozy #warsaw #munich
#warsawairport #lecimy #waytogo

Melde dich an, um mit „Gefällt mir“ zu
markieren oder zu kommentieren.

...



Lufthansa

Nonstop you

[Buchen & Planen](#)

[Top-Angebote](#)

[Info & Service](#)

[Miles & More](#)

[Meine Buchungen](#)

[→ Hilfe & Kontakt](#)

[→ Miles & More](#)

Meine Buchungen

Athen

[Buchung ändern](#) ▼

Di, 31 Januar – Sa, 4 Februar 2017

Hin- und Rückflug

Buchungscode: [REDACTED]

Nicht auf LH.com gebucht



Warschau (WAW) – Athen (ATH)
über MUC

Economy Classic

Passagier

[→ Flugdetails](#)



Buchungsnummer: [REDACTED]

[→ Versicherungsdetails](#)

Unsere Empfehlung für Ihre Reise

Wer nutzt Tor wirklich?

Journalisten nutzen Tor

Aktivisten nutzen Tor

Das Militär nutzt Tor

Aktivisten nutzen Tor

Unternehmen nutzen Tor

Bürger mit Privatheitsbedenken nutzen Tor

Warum nutzen diese Gruppen Tor?



Gezielte Überwachung von einzelnen Mitgliedern der zivilen Gesellschaft

Trends ins Gesetzgebung, Politik und Technologie sind Bedrohung für Privatheit und Freiheit im Internet

Meinungs- und Pressefreiheit wird aktiv beeinträchtigt

Was können Unternehmen im Darknet tun?

Nutzung als Veröffentlichungsplattform für Sicherheitsvorfälle

Proaktives Whistleblowing

Mitbewerber sehen, wie der Markt Sie sieht

Strategien vertraulich halten

Verantwortlichkeiten übernehmen

Was können IT-Verantwortliche im Darknet tun?

Verifikation von IP-basierten Firewalls

Umgehen von eigenen Sicherheitssystemen

Umgehen von ISP-Ausfällen

Aktuelle Sicherheitslücken und 0-days

Worte der Vorsicht

Innerhalb von Tor kursieren Viren, Ransomware etc.

Minimum: Tor in virtueller Maschine laufen lassen

Optimal: Diese VM ist nicht an das Produktionsnetzwerk angeschlossen sondern verfügt über ein eigenes Netzwerk

Sonst: Heruntergeladene Dateien nie öffnen, wenn mit dem Internet verbunden

Tor kann auch Identität nicht zu 100% schützen

Korrelationsangriffe: Eingangs und Ausgangsknoten beobachten

Browser Exploits: XSS, Pingbacks etc.

Zusätzliche Worte der Vorsicht

Up2Date bleiben über den Tor Blog oder Subreddit

Tor/Tor Browser updaten!

Betriebssystem aktuell halten

Virtuelle Maschine oder dedizierte Hardware nutzen

Nicht in soziale Netze einloggen

Zusammenfassung

Es gibt im anonymen Netz nicht nur Kriminalität

Privatheit und Anonymität als Business Enabler sind möglich

Gefahren gibt es im anonymen Netz ebenso wie im normalen Internet

Bewegt man sich umsichtig, kann man im anonymen Netz einiges an Informationen gewinnen

008

C'thulhu

Email: BM-2cVbNcn18dhfcefbaX73USLq4dYtAxW7U@bitmessage.ch

Solutions to Common Problems! We are an organized criminal group, former soldiers and mercenaries from the FFL, highly-skilled, with military experience of more than five years. We can perform hits all around the world.

If you're asking yourself "Why someone would need to hire a killer online?", we'll tell you: simply because it is anonymous. You can always find examples of contractors who collaborated with cops (when they were facing 20 years of prison), and you (the buyer) could end up in the prison because of that. On the other hand, you can also find examples where police found who had the interest to put out a contract, and they can come to you and you can give your testimony (which would put the hitman in jail).



So, it is of mutual interest to make everything anonymous. This website is hosted on a series of anonymous servers, with access to the Internet through the Tor network. You can access this site anonymously only through the Tor network, and we upload files to the server through the Tor network. You can make payments with an anonymous digital currency, either Bitcoins. It means we don't know you and you don't know us. We can't send you to prison, and you can't send us to prison. Of course you must take a risk when you pay in advance, but there is no interest. With risk comes reward. You take a risk, and someone can always cheat you. As we said, many criminals have the balls to do things to other people, but when they face 20 years of prison they begin to talk with the police. Risks about prison and money are always present. If you are not ready to take a risk, don't contact this kind of organizations. And know, we are only one, real contractor there. Any other will try cheat

you. — Contract Killer © 2011.



No fish too big, no job too small - HITMAN does it all!

Q & A!

Can I see proofs of your last work?

No! Every contract is Private, and all data is purged after elimination proof is sent to the customer. It is mandatory for customer's privacy and our safety!

Can You give me contact to previos customers?

No! Every contract is Private! Without Exceptions! And we will never store such info.

Where to find feedback about your succeeded work?

None of our happy customers take time on forums, to post feedbacks. All comments was written directly to our mail, only. And none of them will show any proof if we'll post it on our own page. Even if you'll find an feedback on any page, Good or Bad it was write by an random person, who don't have with as any business.

We don't take any prepayments. We are only asking for your wallet number to see that you really hold the amount, to arrange full escrow on trusted for both third party service.

We should probably get started if your budget is at least:

Murder Types	Low Rank	Medium Rank	High Rank and Political
Regular	\$45,000	\$90,000	\$180,000
Missing in action	\$60,000	\$120,000	\$240,000
Death in accident	\$75,000	\$150,000	\$300,000

Funny/Weird Stuff 2

Hallo zusammen.

Ich bin im Besitz einer vollstaendigen Datenbank eines deutschen Anlageunternehmens mit mehr als 10000 Kunden. Das heißt im Klartext man hat Einsicht in alle Kontostaende, mehr als 1000 Ausweisdokumente, Mailadressen etc.

Kleiner Auszug:

[REDACTED]

Gesucht wird:

- Zusammenarbeit
- oder Abnehmer der gesamten DB

Von Klein bis Großanleger ist alles dabei. Ich wuerde das gesamte angelegte Kapital auf etwa 2 Mil. € schaeetzen.

Was der Abnehmer mit der DB macht ist ihm selbst überlassen. Ob Erpressung; Trojaner; Auscashen => es gibt einige Möglichkeiten.

Angebote und Kontaktaufnahme nur via Bitmessage & PGP.

Grüße

Funny/Weird Stuff 3

BYPASS for Audi Skoda Seat VW VAG ECU Unlock Immob

Vendor [REDACTED]
Price \$0.2855 (€200)
Ships to Worldwide, Worldwide
Ships from england
Escrow Yes



Product description

USE: Thanks to Bypass, you can remove immo through OBD diagnostic plug. You can use it multiple number of times. Once plugged in, the tool would send a request to the ecu to start communication. It recognizes ECU type automatically. Then, once communication has been established the tool checks to see if immo off procedure has been conducted correctly.

Test on Drives:

0281011XXX
K-Line
0281011145 VW Passat B5 2.0 Tdi mechanical igniton switch
0281011258 VW Tourareg 2.5 Tdi
0281011364 A3 1.9Tdi 2004
0281011383
0281011385
0281011568 VW T5 2.5 Tdi 2006/2007
0281011843 Golf5 2.0 Tdi 2004
0281011844 VW Touran 2.0 Tdi 2004
0281011855 VW T5 1.9 Tdi 2003
0281011856 VW T5 1.9 Tdi 2005
0281044882 VW Caddy 1.9 Tdi 2006
0281011883 Skoda Octavia 1.9 Tdi 2004-2010
0281011900
0281011945
0281011946 Touran 1.9 Tdi 2006
0281011907 Touran 2.0 Tdi

0281012XXX
K-Line
0281012220 VW GOLF5 1.9 Tdi 2005
0281012390 VW Caddy 1.9 Tdi 2003-2010
0281012696 Seat Alhambra, VW Sharan 2.0 Tdi 2005-2010
0281012698 Skoda Super B 2.0 Tdi 2006
0281012762 VW T5 1.9 Tdi 2006-2010
0281012792

CAN
0281012113 Audi A4 2.0 Tdi 2008
0281012545 AUDI 1.9 Tdi 2007
0281012546 Audi 1.9 Tdi 2006
0281012654 Audi 2.0 Tdi 2005

0281013XXX
K-Line
0281013228 VW Jetta 2.0 Tdi 2007
0281013299 Skoda Octavia2 2.0 Tdi 2005-2011
0281013302 VW Touareg 2.5 Tdi 2005-2010
0281013311 VW Passat 2.0 Tdi 2005-2009
0281013440 VW Passat C 2.0 Tdi 2005-2009
0281013606 VW Golf5 1.9 Tdi 2006

CAN
0281013177 A6 2.7 Tdi 2007

0281014XXX
K-Line
0281014004
0281014044 VW Touran 1.9 Tdi 2006-2010
0281014049 T5 2.5 Tdi 2007
0281014064 VW Golf 1.9 Tdi 2006-2008
0281014128 Tauran 1.9 Tdi 2006-2010
0281014136 Skoda Octavia II 1.9 Tdi 2006-2010
0281014891 T5 2.5 Tdi 2009

Funny/Weird Stuff 4

CUSTOM SELFIES HOLDING ID + UB



฿0.2636

WW → WW

Order



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Was ist eigentlich das Darknet

Das Darknet bietet viele Chancen, Möglichkeiten und Risiken, wie das normale Internet auch

Matteo Cagnazzo

cagnazzo@internet-sicherheit.de

 @montimonte

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
<http://www.internet-sicherheit.de>

if(is)
internet-sicherheit.

Hat Sie das Thema gepackt? Hören Sie unseren Cybärcast



Jeden letzten Freitag
im Monat

Diverse Experten aus
Wirtschaft und
Forschung

Sie haben Interesse
mit uns zu diskutieren?

 @cybaercast

 cybaercast@protonmail.com