Security for Systems Engineering – VO 09: Datenspuren im Internet

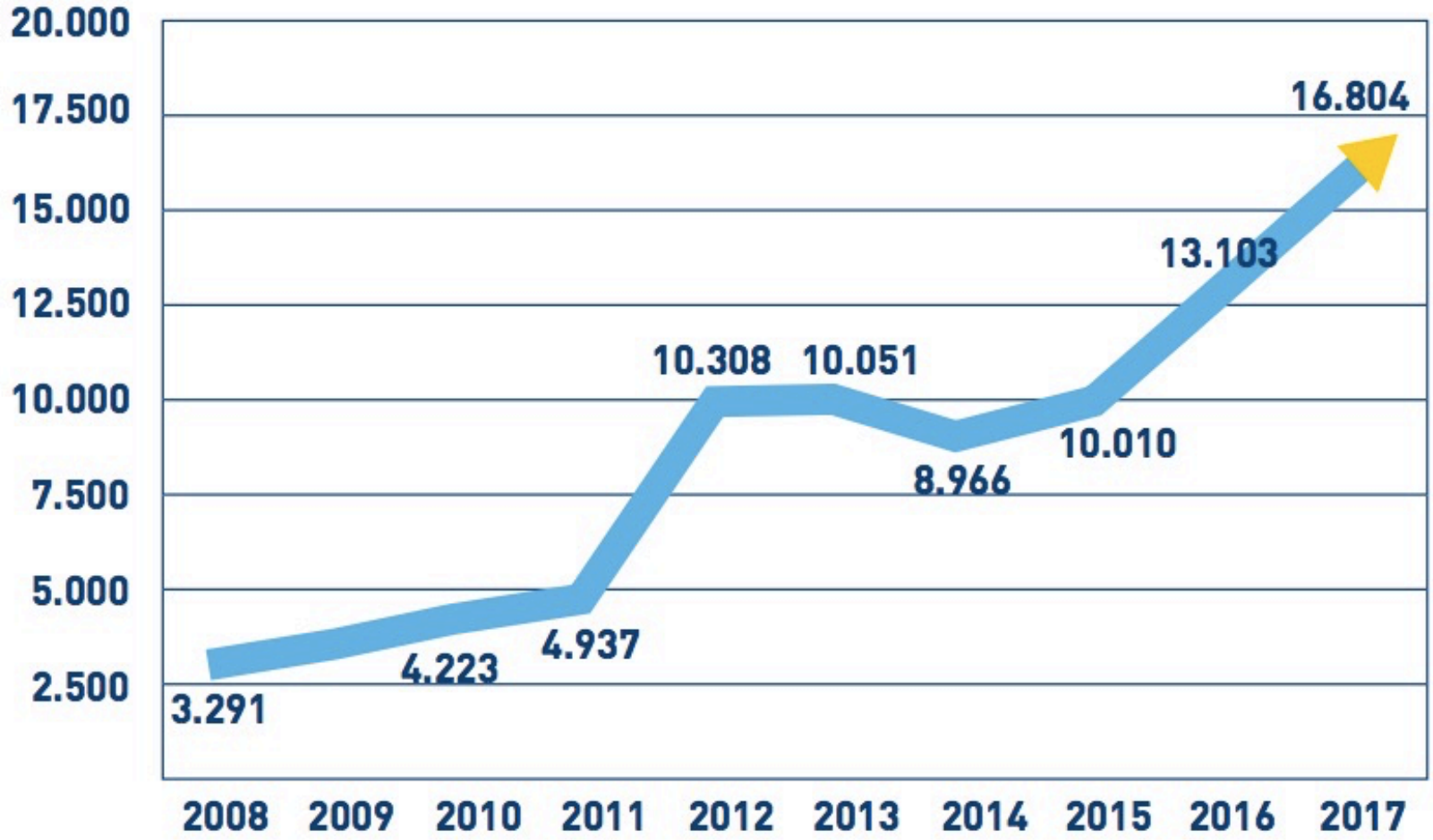
Karin Kernegger, Florian Fankhauser

Preambel

- Anonymität im Internet?
- Datenspuren
  - …beim Surfen im Internet
  - …die Betrüger nutzen oder hinterlassen
  - …welche sind das & wie können sie gefunden werden?

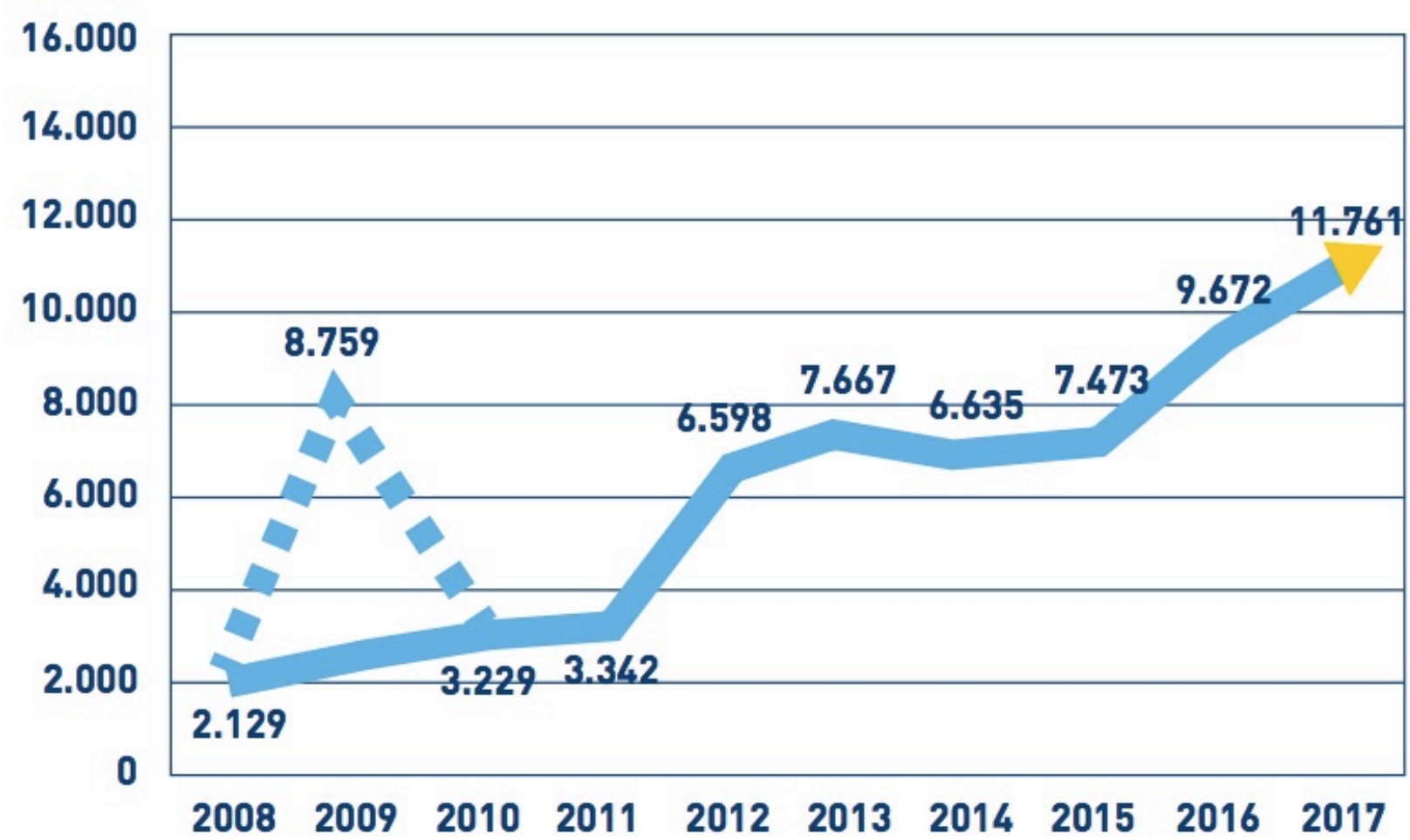
Grafik: http://www.silver-tipps.de/entstehung-und-vermeidung-von-datenspuren-im-netz/

Kriminalstatistik - Cybercrime



Quelle: https://bundeskriminalamt.at/501/files/PKS_17_Broschuere_Web.pdf

Kriminalstatistik - Internetbetrug



Quelle: https://bundeskriminalamt.at/501/files/PKS_17_Broschuere_Web.pdf

Beispiele für Betrugsformen im Internet

- CEO Fraud
- Bestellbetrug
- Cryptocurrency Betrug
- Vorschussbetrug
- Finanzagenten - Geldwäsche
- ….

Anonymität im Internet

Peter Steiner, published by The New Yorker on July 5, 1993.

CEO Fraud

- Betrüger geben sich als Geschäftsführer eines Unternehmens aus
- Ziel: Buchhaltung eines Unternehmens
- Hohe Zahlungen sind zu veranlassen
- Absolute Diskretion wird verlangt, Zeitdruck aufgebaut
- Kommunikation per E-Mail - teilweise auch Telefonate mit angeblichen Rechtsanwälten
- Gefälschte Rechnungen, Verwendung der Unterschrift des Geschäftsführers
- Vorbereitung: Recherchen auf der Webseite/Linkedin/Xing, Social Engineering, ...
- Seit Juli 2015 auch massiv in Österreich
- Meldestelle Bundeskriminalamt: ceo-fraud@bmi.gv.at

Bestellbetrug

- Stark steigend
- Varianten:
  - Ware wird zugestellt, aber nie bezahlt
    - Bestellung auf Rechnung
    - Card not present fraud
    - Online Handel betroffen
  - Ware wird bezahlt, aber nie zugestellt (Ware nicht existent)
    - Kleinanzeigenportale
    - Fake Web Shops

Cryptocurrency Betrug

- Fake Twitter Accounts – mit Bitte um Überweisung

Vorschussbetrug

- Erbschaft/Lottogewinn/…
  - Versprechen: größere Geldsumme
  - Vorschuss: verschiedenste Gebühren
- Love Scam
  - Fiktive Liebesgeschichte

Love Scam

Subject: Guten Tag!!! wir werden alles in Ordnung dieser Moment sein !!!!
Date: Sun, 29 Jan 2017 18:49:57 +0400
From: Veronika <ogurechik17@yandex.com>

Guten Tag! Ich habe dein E-Mail-Adresse auf einer Dating-Website. Erinnern Sie sich an mich?
Ich schickte dir meine Fotos. Hoffe Sie dir gefallen werden, denn ich bin sehr hubsch und nettes Madchen.
Ich hoffe, dass ich auf dem Foto Ihnen gefallen hat. Ich mochte wissen, Ihre Meinung uber sich selbst.
Mein name ist Veronika. Ich Lebe allein in einer kleinen Stadt. Meine Letzte Beziehung endete schlecht.
Und deshalb Schreibe ich dir. Ich mochte eine ernsthafte Beziehung mit einem Mann. Sie hat mir sehr gut gefallen und ich mochte lernen dich naher. Ich denke, dass du der Mann den ich suchte die ganze Zeit.
Du schien mir sehr nett und ein guter Mensch. Ich mochte, dass du mir geantwortet auf diesen Brief, weil du mir sehr lieb.
Ich werde fur Ihre Antwort warten. Bitte erzahlen Sie mir mehr uber sich selbst. Und es ware nicht schlecht wenn du geschickt Ihre letzten Fotos. Ich hoffe, dass es moglich ist. Freue mich auf Ihre Antwort. Deine Veronika.

- Aufbau einer Vertrauensbasis (Telefonate, Pässe)
- Geld aus verschiedenen Gründen: Notfall/Krankheit/ Reisekosten
- Money Transfer-Dienste z.b. Western Union

Finanzagenten - Geldwäsche

- Job-Angebote
- Provision für Geldweiterleitung – Money Mules
- Weiterführender Betrug mit z.b. Pässen der Bewerber

Vakanz! Vakanz! Vakanz!

Ein sehr gutes Gehalt in kürzer Zeit!

Unser Unternehmen bietet ein sehr gutes Einkommen - bis zu 8000.00 EUR pro Monat an. Die Erledigung von jeder Aufgabe bringt Ihnen das Budget von 400 bis 1600 EUR. Sie können für diesen Job nur mehrere Stunden Ihrer Zeit zweimal pro Woche aufwenden. **Es ist erlaubt, diese Tätigkeit mit Ihrer Dauerbeschäftigung zu vereinigen!**

Hier ist das, was Sie bei dieser Arbeit machen sollen:

1. **Sie erhalten eine Überweisung mit dem Betrag von 2000.00 EUR von unserer Organisation.**
2. Am Tag des Geldeingangs bei Ihrer Bank sind Sie verpflichtet, das Geld in der Bank abzuheben.
3. **Sie erhalten 20% von der Geldanweisung - das ist die Summe von 400.00 EUR bis 1600.00 EUR!**
4. Den Rest des auf Ihrem Konto eingetroffenen Geldbetrags geben Sie unserer Organisation.
5. Wenn Sie für die Zusammenarbeit mit uns bereit sind, bereiten wir den nächsten Geldbetrag auf Ihr Konto vor.

Dieser Nebenjob ist völlig legal und stößt gegen keine Gesetze der EU und Deutschlands. Sie können selbst die Anzahl der Überweisungen regeln, die von Ihnen bearbeitet werden!

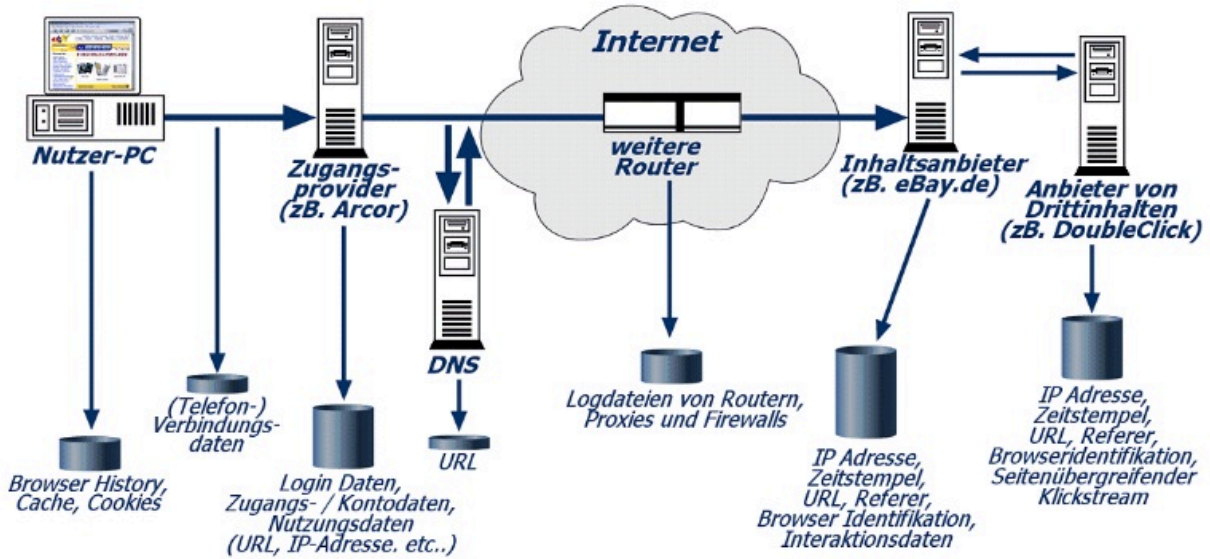
Sie können jegliche Fragen an uns per Email stellen. Wir beantworten alle Ihre Fragen und schicken Ihnen eine ausführliche Beschreibung der Arbeit.

Die Anzahl von den Arbeitsstellen ist begrenzt!

Quelle: http://ecommerce.cash.at/fileadmin/user_upload/handouts2017/6._CECC_Kahn_Handout.pdf

Quellen für Spuren

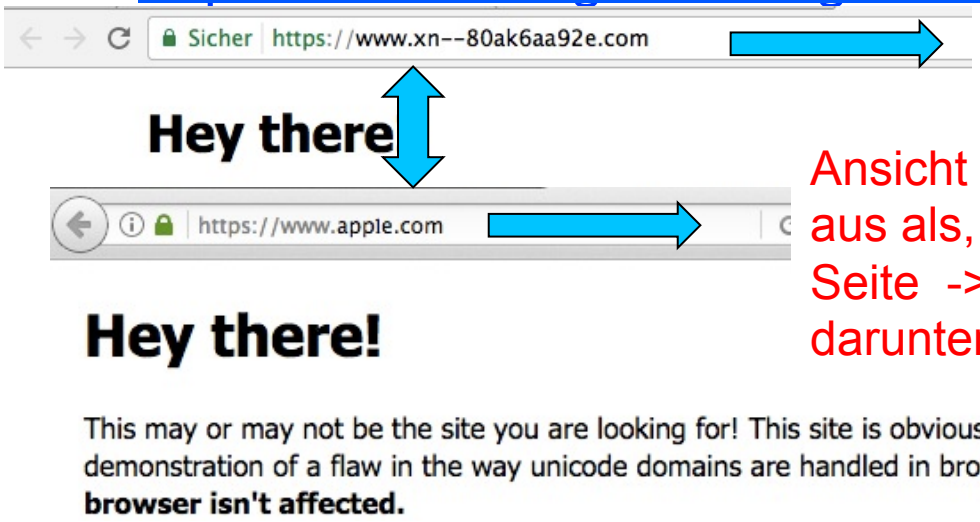
- E-Mails
  - E-Mail-Header (IP-Adresse)
  - Links
  - E-Mail-Anhänge
    - Malware
    - Dokumente
- Log-Files



Grafik: https://privacyprotection.pozimski.eu/anonymisierung.html

E-Mail-Spoofing - Arten

- Annahme: der.ceo@firma.com
- Fälschungen:
  - der.ceo@gmail.com
  - der.ceo@frma.com oder der.ceo@firrna.com
  - Unicode Domains
    - https://www.xudongz.com/blog/2017/idn-phishing/

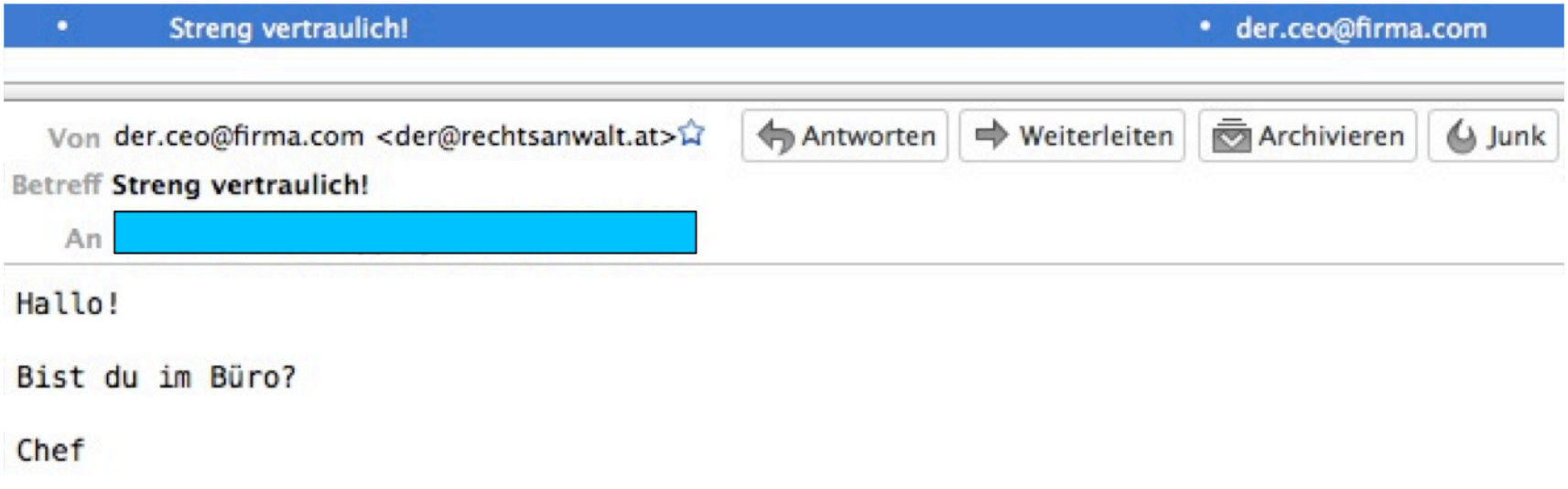


Ansicht im Chrome

Ansicht im Firefox: Sieht laut Adresszeile aus als, wäre es die echte apple.com-Seite -> ist es aber nicht! (am Text darunter zu erkennen ☺)

E-Mail-Spoofing

- Scheinbar zwei Absender



From: "der.ceo@firma.com" <der@rechtsanwalt.at>

Subject: Streng vertraulich!

E-Mail-Spoofing

- Scheinbar zwei Absender – Version 2

From: "\"der.ceo@firma.com\";" <der@rechtsanwalt.at>

Subject: Streng vertraulich!

E-Mail Spoofing

- Absender: richtige E-Mail-Adresse

- erst bei "Antworten" erscheint Täter E-Mail-Adresse

From: Der CEO <der.ceo@firma.at>

Reply-To: <taeter@email.at>

E-Mail-Header Auswertung

- Beinahe der komplette Header kann manipuliert werden!
- From: Absender
- To: Empfänger
- Date
- Received: Verlauf des E-Mails: von unten nach oben zu lesen; hier ist (wenn vorhanden) auch die Sender-IP zu finden; kann manipuliert sein, um den Weg der E-Mail zu verschleiern – nur den Servern unter eigener Kontrolle bzw. einem Server davor, kann vertraut werden.
- Reply-To: an diese E-Mail-Adresse wird bei "Antworten" die E-Mail gesendet
- Return Path: eine unzustellbare E-Mail wird hierhin gesendet

E-Mail-Header Auswertung - Beispiel

- Received – Verlauf der E-Mail
- Angeblicher Absender: noreply@dhl.com
- Lettische Absender-IP

```
Return-Path: <noreply@dhl.com>
Delivered-To: [redacted]
Received: (qmail 2835 invoked from network); 29 May 2017 07:56:17 -0000
Received: from unknown ([172.18.1.109])
          by mailbox14.aon.at (qmail-ldap-1.03) with QMQP; 29 May 2017 07:56:17 -0000
Delivered-To: CLUSTERHOST smarthub76.res.a1.net [redacted]
Received: (qmail 2472 invoked from network); 29 May 2017 07:56:17 -0000
X-Spam-Checker-Version: SpamAssassin 3.4.0 (2014-02-07) on
    WARSBL504.highway.telekom.at
X-Spam-Level:
Received: from cloud02.dataqube.gr ([95.129.40.63])
          (envelope-sender <noreply@dhl.com>)
          by smarthub76.res.a1.net (qmail-ldap-1.03) with DHE-RSA-AES256-GCM-SHA384 encrypted SMTP; 29 May 2017 07:56:14 -0000
X-A1Mail-Track-Id: 1496044572:2168:smarthub76:95.129.40.63:1
Received: from IP-221-52.dataclub.biz (unknown [46.183.221.52])
    by cloud02.dataqube.gr (Postfix) with ESMTPA id E41AD66570;
    Mon, 29 May 2017 10:47:42 +0300 (EEST)
Content-Type: multipart/mixed; boundary="==========2086848102=="
MIME-Version: 1.0
Subject: DHL e-Delivery Final Notification
To: Recipients <noreply@dhl.com>
From: "DHL Express Austria" <noreply@dhl.com>
Date: Mon, 29 May 2017 10:47:29 +0300
```

Log Files

- Apache Access Log (http://httpd.apache.org/docs/current/logs.html)

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\""
```

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326 "http://www.example.com/start.html"
"Mozilla/4.08 [en] (Win98; I ;Nav)"
```

- IP; HTTP authenticated User; Datum + Uhrzeit + Zeitzone; Anfrage des Clients; Status Code (200 OK); Größe; Referer; User Agent String
- Datenschutz-Grundverordnung beachten!
- Empfehlenswert: Mitloggen des Source-Ports
- Beispiel Bestellbetrug: Welche Möglichkeiten gibt es um zu erkennen, ob im Onlineshop mehrmals vom selben Betrüger/selber Tätergruppe bestellt wird?

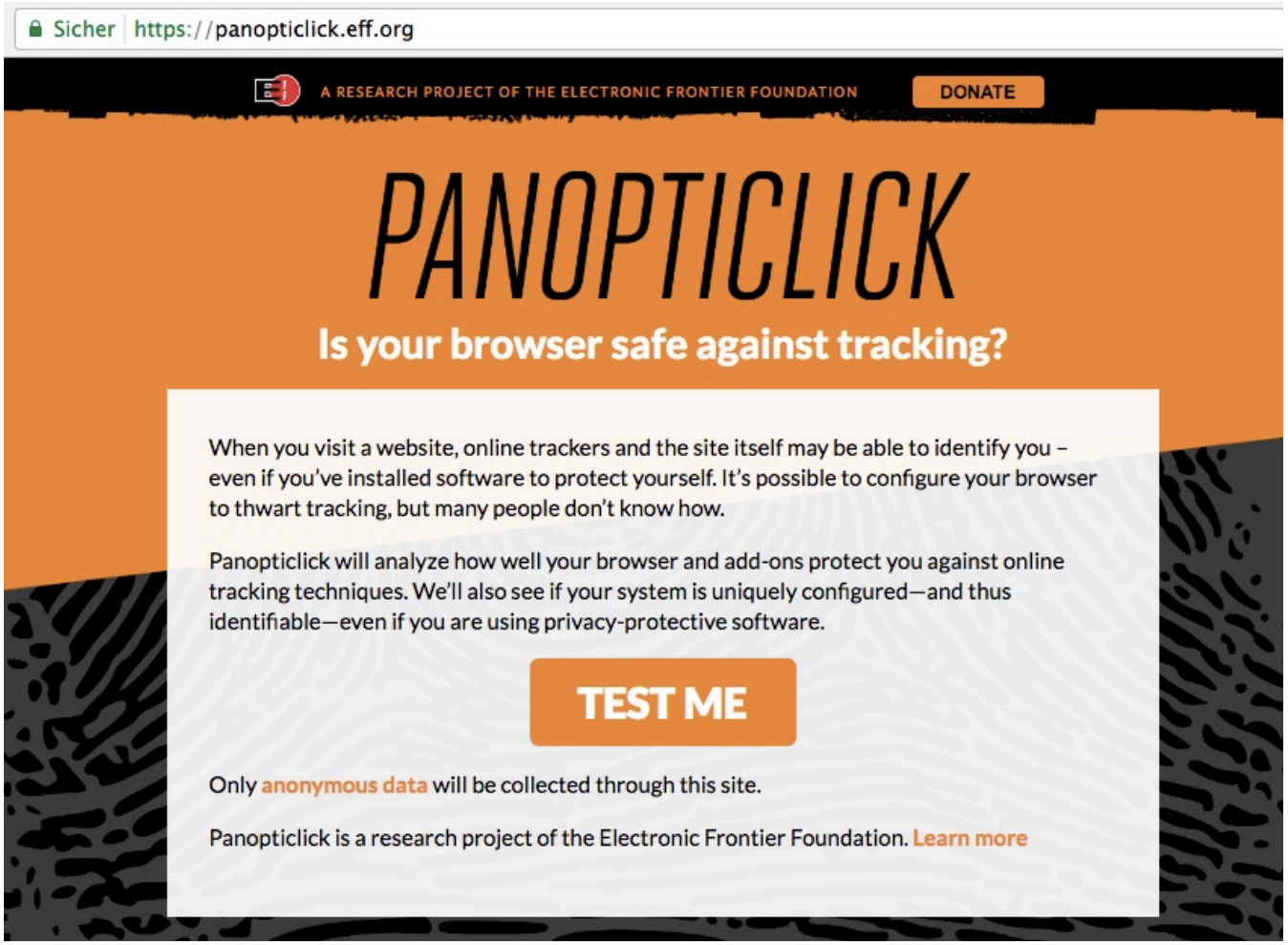
Browser Fingerprinting

- Browser-Einstellungen und Konfigurationen tracken – anstatt IP-Adresse oder Cookies
- Schwierig zu erkennen und schwierig zu verhindern – Informationen werden beim Besuch einer Webseite automatisch mitgesendet
- Möglichkeit um einen Browser mit hoher Wahrscheinlichkeit zu identifizieren

Browser Fingerprinting - Browsereigenschaften

- Mitloggen verschiedener Browsereigenschaften:
  - User Agent String
  - HTTP Accept Headers
  - Zeitzone
  - Bildschirmauflösung
  - Spracheinstellungen
  - falls Java oder Flash aktiviert:
    - Installierte Fonts
    - Installierte Plugins
  - u.v.m

Browser Fingerprinting



Browser Fingerprinting - Beispiel

User Agent	20.62	1611876.0	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.40 Safari/537.36
Language	0.92	1.89	en-US
System Fonts	6.6	97.08	Andale Mono, Arial, Arial Black, Arial Hebrew, Arial Narrow, Arial Rounded MT Bold, Arial Unicode MS, Book Antiqua, Bookman Old Style, Calibri, Cambria, Cambria Math, Century, Century Gothic, Century Schoolbook, Comic Sans MS, Consolas, Courier, Courier New, Garamond, Geneva, Georgia, Helvetica, Helvetica Neue, Impact, Lucida Bright, Lucida Calligraphy, Lucida Console, Lucida Fax, LUCIDA GRANDE, Lucida Handwriting, Lucida Sans, Lucida Sans Typewriter, Lucida Sans Unicode, Microsoft Sans Serif, Monaco, Monotype Corsiva, MS Gothic, MS PGothic, MS Reference Sans Serif, MYRIAD PRO, Palatino, Palatino Linotype, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings, Wingdings 2, Wingdings 3 (via javascript)
Browser Plugin Details	11.18	2315.91	Plugin 0: Chrome PDF Plugin; Portable Document Format; internal-pdf-viewer; (Portable Document Format; application/x-google-chrome-pdf; pdf). Plugin 1: Chrome PDF Viewer; ; mhjfbmdgcfjbbpaeojofohoefgiehjai; (; application/pdf; pdf). Plugin 2: Native Client; ; internal-nacl-plugin; (Native Client Executable; application/x-nacl;) (Portable Native Client Executable; application/x-pnacl;).
HTTP_ACCEPT Headers	10.54	1492.48	text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.9,de;q=0.8

Browser Fingerprinting - Gegenmaßnahmen

- Fingerprints nicht sehr “langlebig” – neue Einstellungen/ Update verändern den Fingerprint
- Gegenmaßnahmen
  - Verwendung Tor Browser
  - Java Script deaktivieren
  - Flash deaktivieren
  - “üblichen” Browser verwenden
    - Die ersten Smartphone Browser waren sehr ähnlich

Amazing mind reader reveals his gift

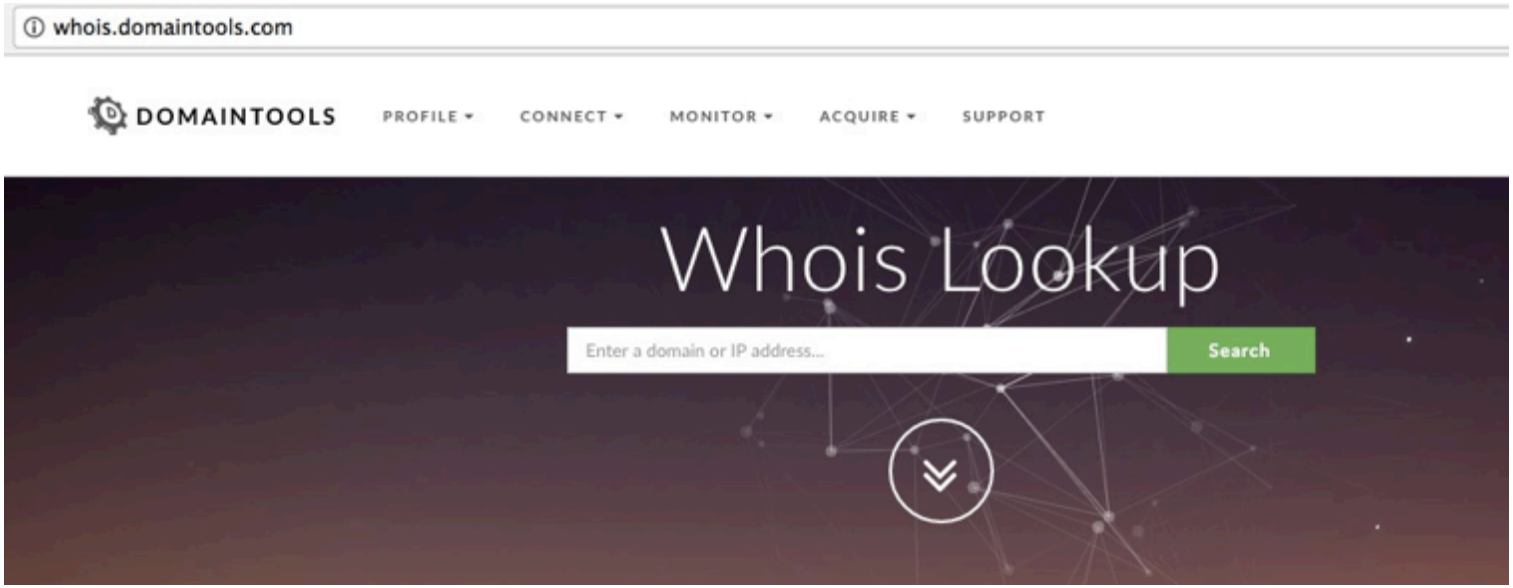
https://www.youtube.com/watch?v=F7pYHN9iC9I

Recherchemöglichkeiten

- IP-Adressen
- E-Mail-Adressen
- Domänen
- Personennamen
- Bilder

IP-Adressen - Whois

- whois.domaintools.com



IP-Adressen – Whois

IP Information for 178.162.217.140

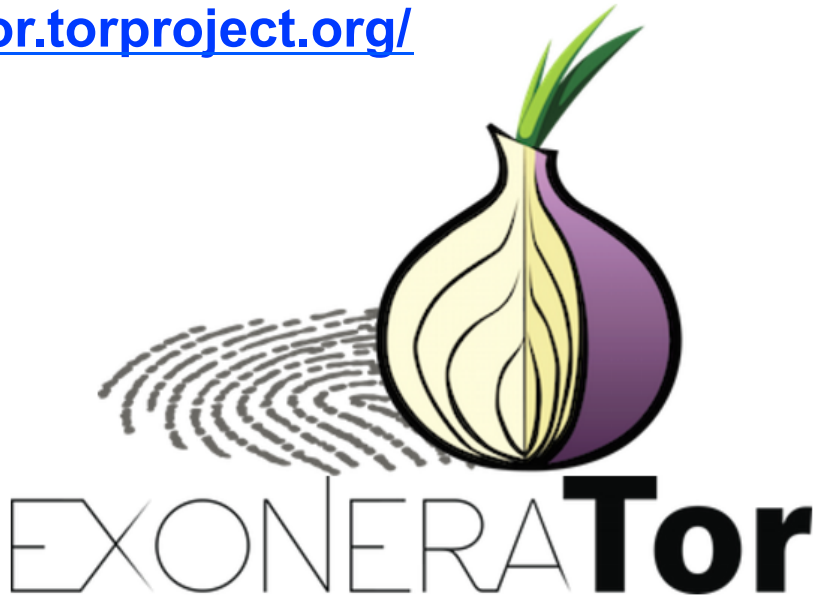
– Quick Stats

IP Location	Germany Frankfurt Am Main Leaseweb Deutschland Gmbh
ASN	AS28753 LEASEWEB-DE , DE (registered Feb 17, 2003)
Whois Server:	whois.ripe.net
IP Address	178.162.217.140

```
inetnum:        178.162.216.0 - 178.162.219.255
descr:          Leaseweb Deutschland GmbH
descr:          Cloud-DE-Express
remarks:        Please send all abuse notifications to the following email address:
abuse@de.leaseweb.com. To ensure proper processing of your abuse notification, please
 visit
the website www.leaseweb.com/abuse for notification requirements. All police and othe
r
government agency requests must be sent to subpoenas@de.leaseweb.com.
country:        DE
admin-c:        LSWG-RIPE
tech-c:         LSWG-RIPE
status:         ASSIGNED PA
mnt-by:         LEASEWEB-DE-MNT
mnt-lower:      LEASEWEB-DE-MNT
mnt-routes:     LEASEWEB-DE-MNT
created:        2012-01-09T08:17:26Z
last-modified:  2015-10-01T15:04:41Z
source:         RIPE

person:         RIPE Mann
address:        Kleyerstrasse 75-87
address:        60326 Frankfurt am Main
address:        Germany
phone:          +49 69 2475 2860
fax-no:         +49 69 2475 2861
abuse-mailbox:  abuse@de.leaseweb.com
notify:         ripe@de.leaseweb.com
nic-hdl:        LSWG-RIPE
mnt-by:         LEASEWEB-DE-MNT
created:        2012-03-23T15:55:41Z
last-modified:  2016-08-05T10:47:55Z
source:         RIPE
```

IP-Adressen – TOR?

https://exonerator.torproject.org/

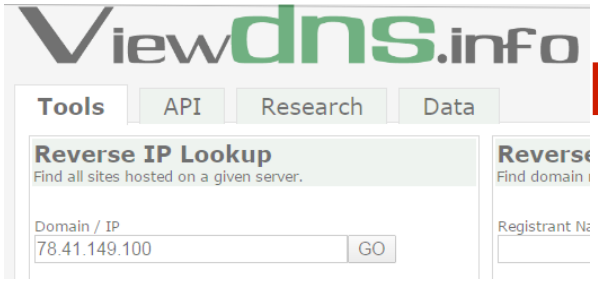


Geben Sie eine IP-Adresse und ein Datum ein um herauszufinden, ob diese IP-Adresse von einem Tor-Server verwendet wurde:

IP-Adresse 86.59.21.38 Datum tt.mm.jjjj Suchen

IP-Adressen – Reverse Lookup

http://viewdns.info/



ViewDNS.info

Tools | API | Research | Data

ViewDNS.info > Tools > **Reverse IP Lookup**

Takes a domain or IP address and does a reverse lookup to quickly shows all other domains hosted sites or identifying other sites on the same shared hosting server.

Domain / IP: GO

Reverse IP results for 78.41.149.100

There are 85 domains hosted on this server.
The complete listing of these is below:

Domain	Last Resolved Date
059133.at	2018-05-21
112.at	2018-05-21
against-cybercrime.at	2018-05-21
bak.gv.at	2018-05-21
bevoelkerungsschutz.at	2018-05-21
bezirkspolizeikommando.at	2018-05-21
bfa.gv.at	2018-05-21
bfa.wien	2017-04-09
bia-bmi.at	2018-05-21
bmi.gv.at	2018-05-27
bmi.or.at	2018-05-21
bmigv.at	2018-05-21
bpw-16.at	2018-05-27
briefwahl.gv.at	2018-05-21

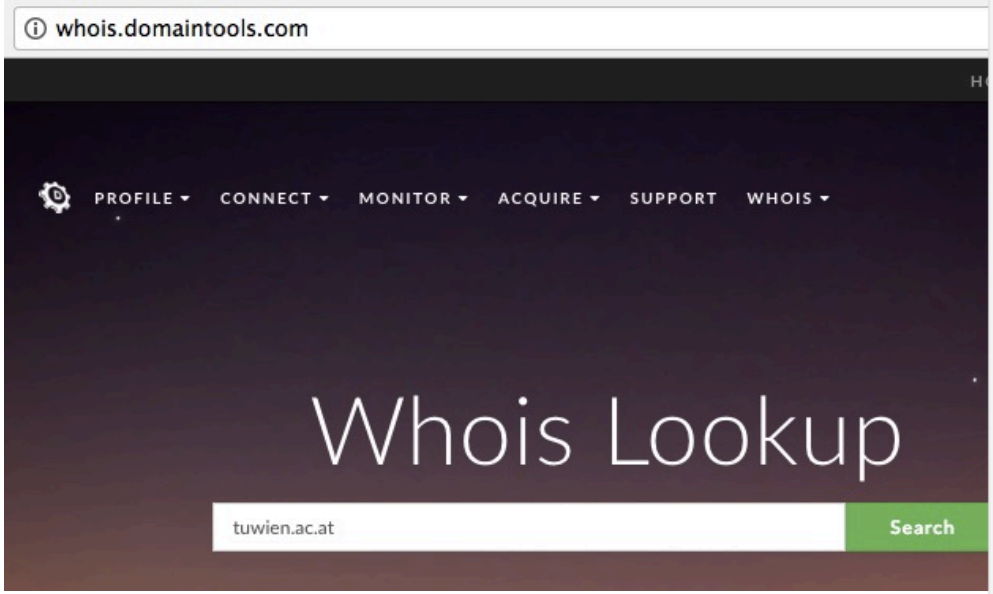
Domänen - Whois

- Whois-Anfrage: tuwien.ac.at

```
karin@[redacted] $ whois tuwien.ac.at
% Copyright (c)2017 by NIC.AT (1)
%
% Restricted rights.
%
% Except for agreed Internet operational purposes, no part of this
% information may be reproduced, stored in a retrieval system, or
% transmitted, in any form or by any means, electronic, mechanical,
% recording, or otherwise, without prior permission of NIC.AT on behalf
% of itself and/or the copyright holders. Any use of this material to
% target advertising or similar activities is explicitly forbidden and
% can be prosecuted.
%
% It is furthermore strictly forbidden to use the Whois-Database in such
% a way that jeopardizes or could jeopardize the stability of the
% technical systems of NIC.AT under any circumstances. In particular,
% this includes any misuse of the Whois-Database and any use of the
% Whois-Database which disturbs its operation.
```

Domänen - Whois vor DSGVO

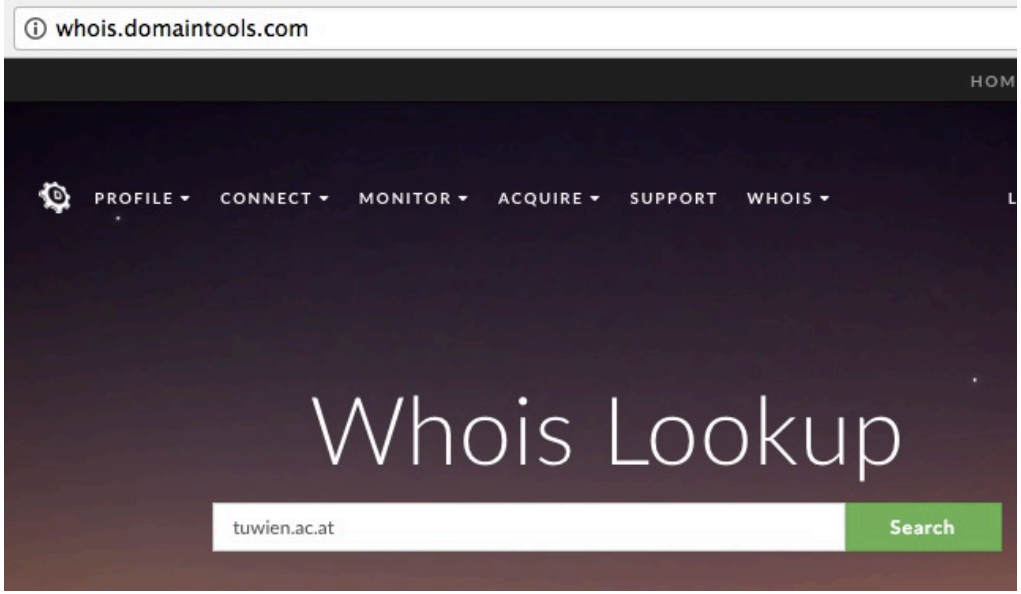
- Whois.domaintools.com: tuwien.ac.at
- Kontaktdaten wurden angezeigt




```
domain:          tuwien.ac.at
registrant:      TUWZ1026921-NICAT
admin-c:         JD766159-NICAT
tech-c:          JK561471-NICAT
nserver:         ns10.univie.ac.at
nserver:         ns5.univie.ac.at
nserver:         tunamec.tuwien.ac.at
remarks:         192.35.241.70
nserver:         tunamec.tuwien.ac.at
remarks:         2001:629:1001:11::53
nserver:         tunamed.tuwien.ac.at
remarks:         192.35.241.71
nserver:         tunamed.tuwien.ac.at
remarks:         2001:629:1001:11::1:53
changed:         20131031 12:18:51
source:          AT-DOM

personname:
organization:    Technische Universitaet Wien - ZID
street address:  Wiedner Hauptstrasse 8-10/020
postal code:     1040
city:            Wien
country:         Austria
phone:           +4315880142001
fax-no:          +4315880142099
e-mail:          hostmaster@noc.tuwien.ac.at

nic-hdl:         TUWZ1026921-NICAT
changed:         20131031 09:15:16
source:          AT-DOM

personname:      [redacted]
organization:    TU Wien / ZID
street address:  Wiedner Hauptstrasse 8-10
postal code:     1040
city:            Wien
country:         Austria
phone:           [redacted]
fax-no:
```

Domänen - Whois aktuell

- Whois.domaintools.com: tuwien.ac.at




```
domain:          tuwien.ac.at
registrar:
registrant:      TUWZ1026921-NICAT
admin-c:         <data not disclosed>
tech-c:          <data not disclosed>
nserver:         ns10.univie.ac.at
nserver:         ns5.univie.ac.at
nserver:         tunamec.tuwien.ac.at
remarks:         192.35.241.70
nserver:         tunamec.tuwien.ac.at
remarks:         2001:629:1001:11::53
nserver:         tunamed.tuwien.ac.at
remarks:         192.35.241.71
nserver:         tunamed.tuwien.ac.at
remarks:         2001:629:1001:11::1:53
changed:         20131031 12:18:51
source:          AT-DOM

personname:
organization:    Technische Universitaet Wien - ZID
street address:  Wiedner Hauptstrasse 8-10/020
postal code:     1040
city:            Wien
country:         Austria
phone:           +4315880142001
fax-no:          +4315880142099
e-mail:          hostmaster@noc.tuwien.ac.at
nic-hdl:         TUWZ1026921-NICAT
changed:         20131031 09:15:16
source:          AT-DOM
```

Domänen - Domainbigdata

- Domainbigdata.com

Domain

Domain	tuwien.ac.at
Words in domainname	tuwien
Title	Technische Universität Wien : TU Wien
IP Address	128.130.35.76
IP Geolocation	Austria, Wien, Vienna map

Website using this ip : 128.130.35.76

univercity2015.com
tuwien.ac.at
univercity2015.at
tu-wien.at
univercity.at

SEO & Backlinks

hyperbacklink.com

Other TLDs

tuwien.at
tuwien.info
tuwien.name
tuwien.com
tuwien.net
tuwien.org

Nameservers

A Records

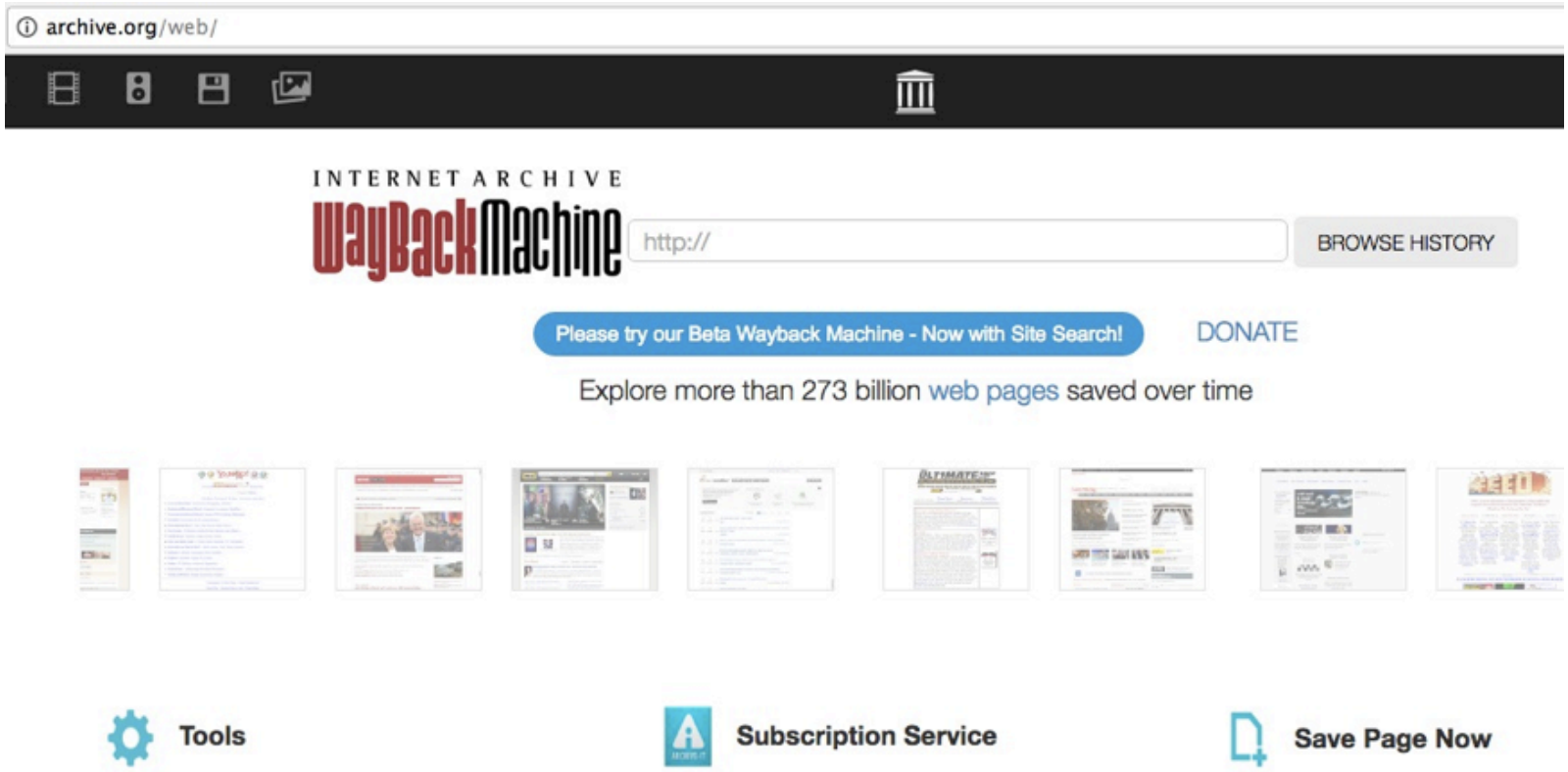
Type	Hostname	Address	TTL	Class
A	tuwien.ac.at	128.130.35.76	86400	IN

Domäne – Besuch der Webseite

- Tuwien.ac.at

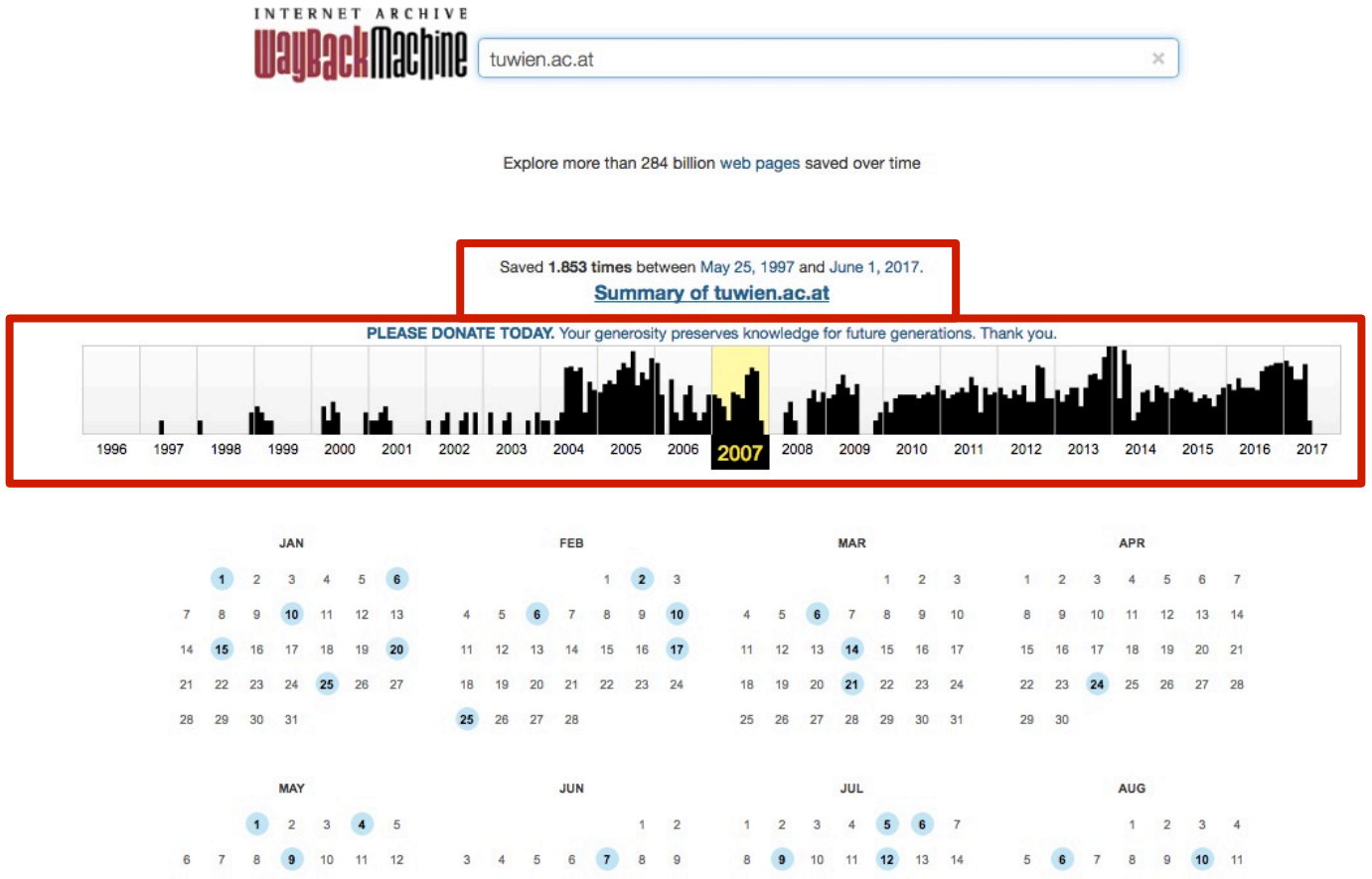
Domäne – Historische Informationen

- Waybackmachine.org



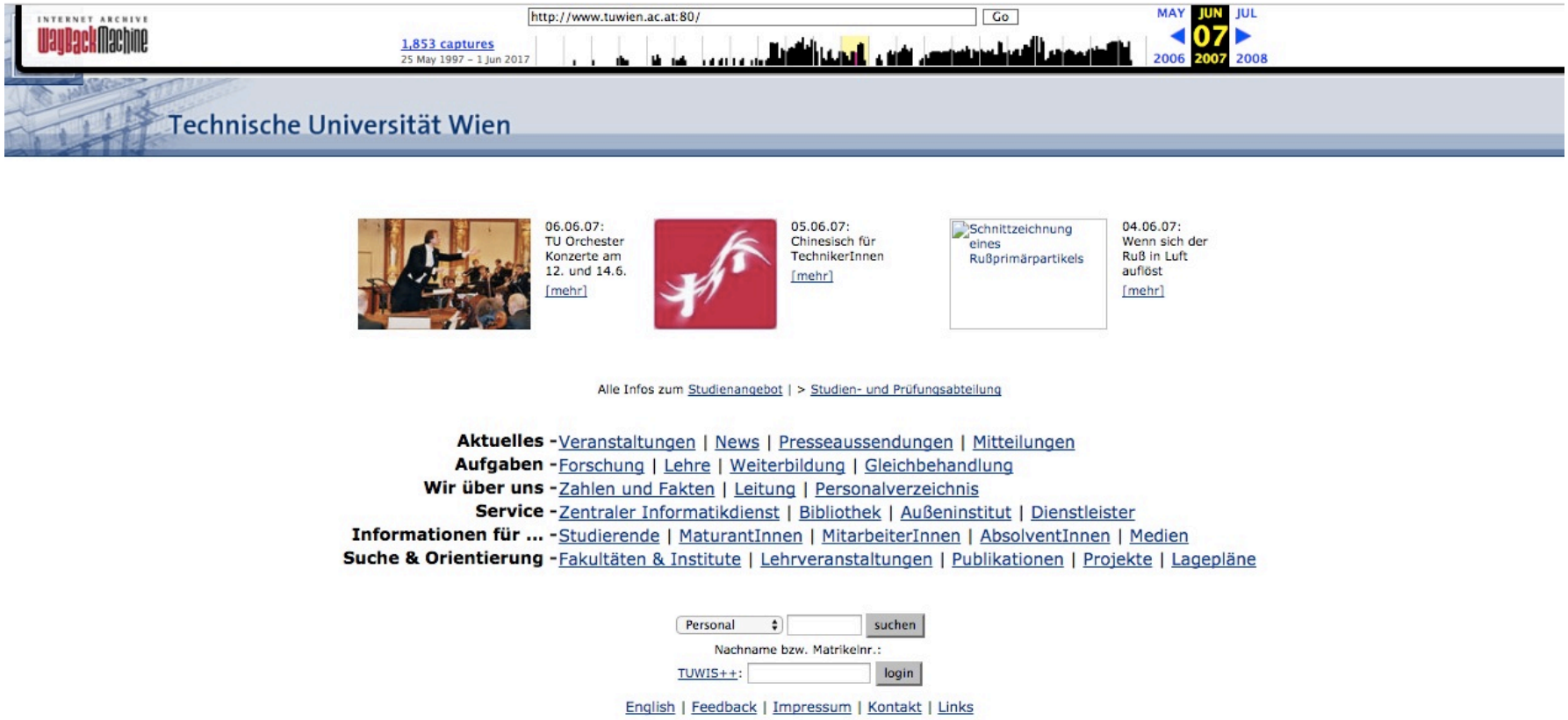
Domäne – Historische Information

- Waybackmachine.org



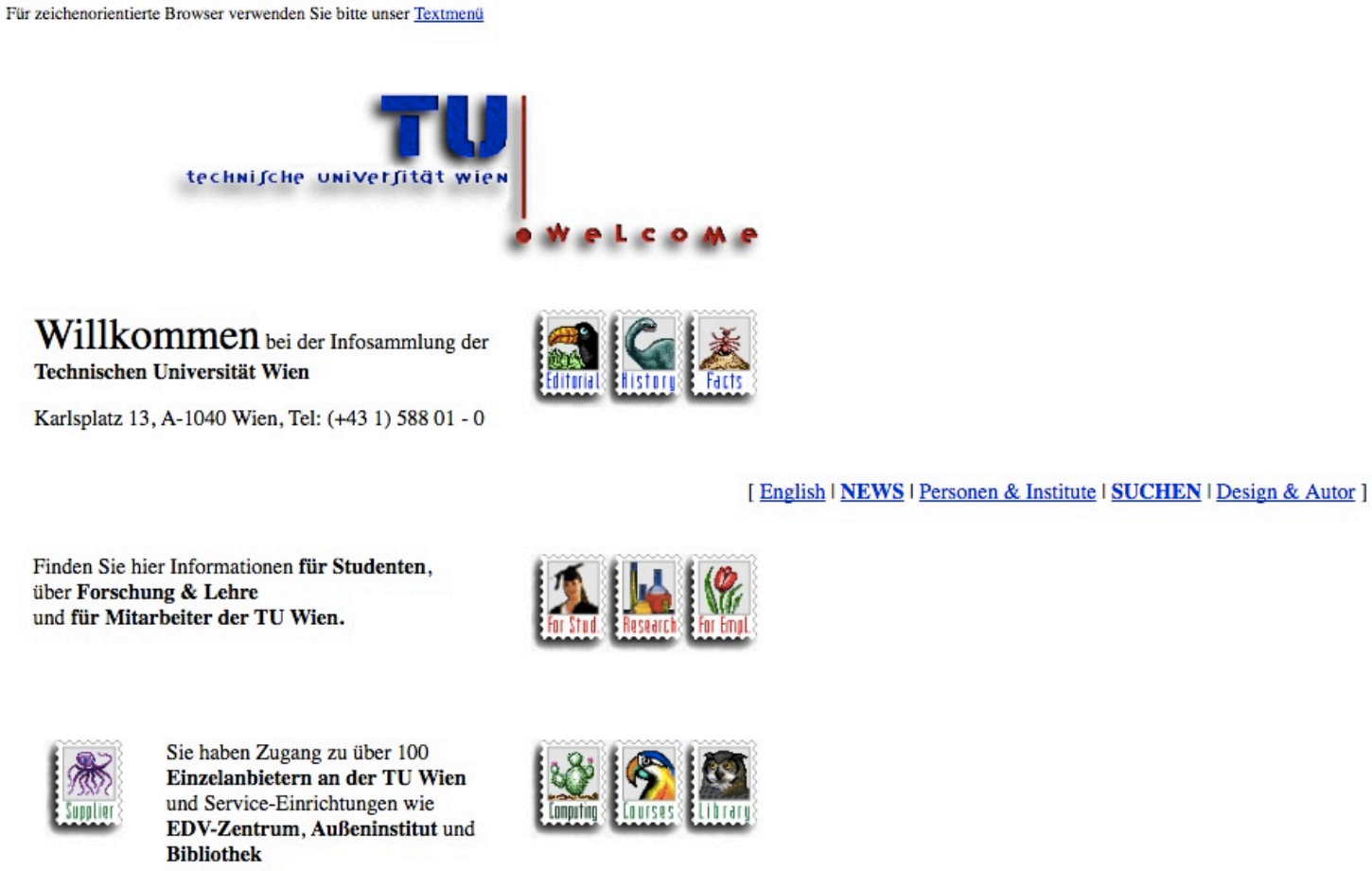
Domäne

- Tuwien.ac.at 07.06.2007



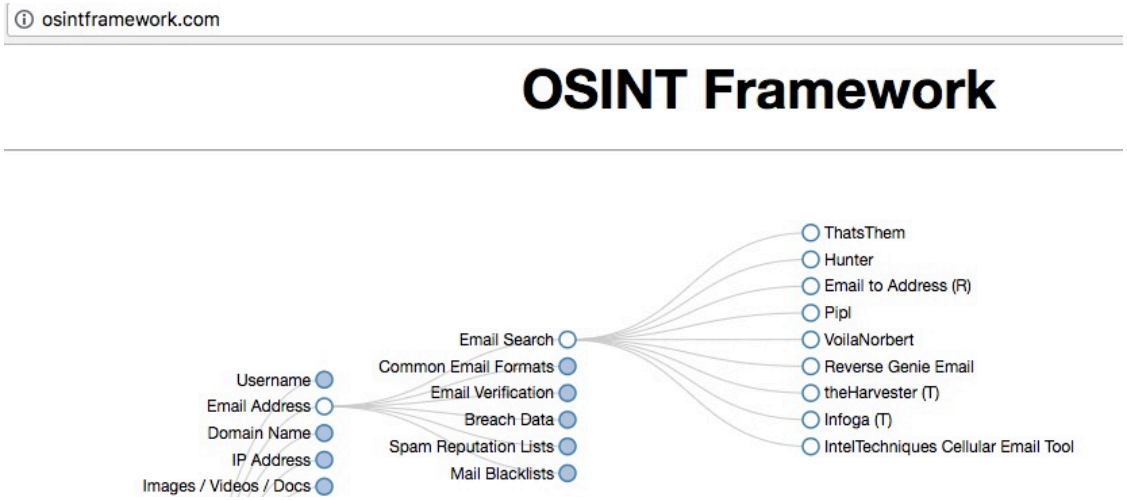
Domäne

- Tuwien.ac.at 25.05.1997



E-Mail-Adressen

- Verwendung:
  - Kontaktdaten auf Webseiten
  - Benutzername bei verschiedenen (Social Media-) Accounts
  - Registrierung von Domänen
- osintframework.com

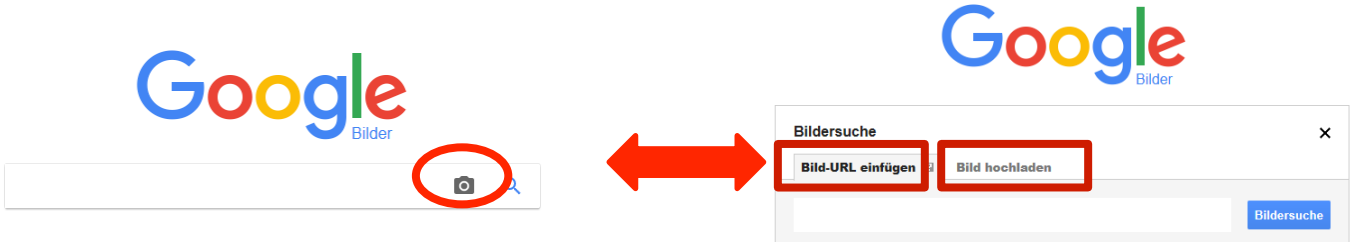


Personennamen

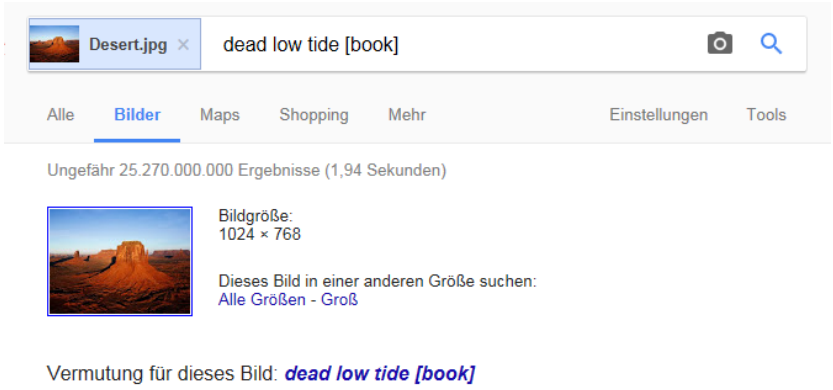
- Personensuchmaschinen zb. Pipl.com
- Social Media: Facebook, Skype,…
- Google Suche mit Operatoren und Zusatzinformationen
- Domaintools & Domainbigdata
- www.opencorporates.com - für Suche nach Firmen/CEO

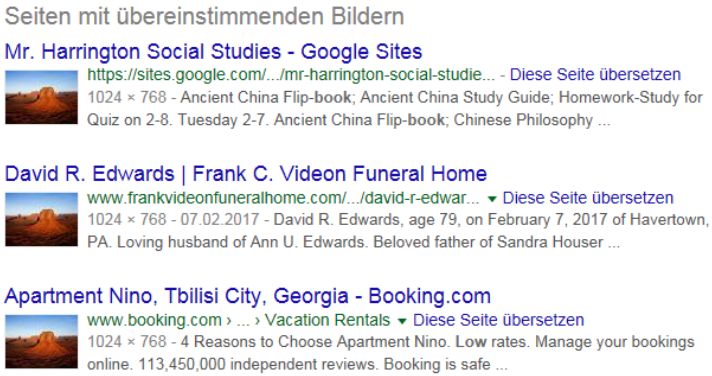
Bilder

Reverse Image Google - https://images.google.com/



Ermöglicht eine Suche nach (bereits bekannten) Bildern – Wo wird das Bild noch überall verwendet – zB Profilfotos





Betrug - Täterausforschung

- Szenario:
  - Verkauf von Apple Store Gutscheinen über Reddit
  - Idee: Bezahlung via Bitcoin
  - Betrüger meldet sich über Reddit

Ungustly:

> *Still selling the $500 Apple giftcard? Is it apple store or Itunes? I can do $380 BTC for it. Pm me back with info.*

  - Quelle (gesamtes Beispiel inkl. Grafiken): https://blog.haschek.at/2016/how-a-scammer-stole-500-dollars-from-me

Betrug - Täterausforschung

- Verkäufer bittet um Bitcoin Überweisung
- Betrüger ist “skeptisch”

Ungustly:

> *I am not interested in going first as I have done a good amount of trades in different sub reddits and I have over 150+ feedbacks on eBay. For all I know you can be someone who brought this reddit account (just a scenario). In either case I am not willing to go first and I have feedback to back me up.*

Betrug - Täterausforschung

- Kontakt auch über ebay
- Gute ebay Bewertungen des Betrüger-Accounts

Betrug - Täterausforschung

- Verkäufer übermittelt Kartennummern + PINs

- … allerdings keine Überweisung
- … und

Betrug - Täterausforschung

- Verkäufer kontaktiert den ebay-Account
- Als Antwort erhält er:

Ungustly:

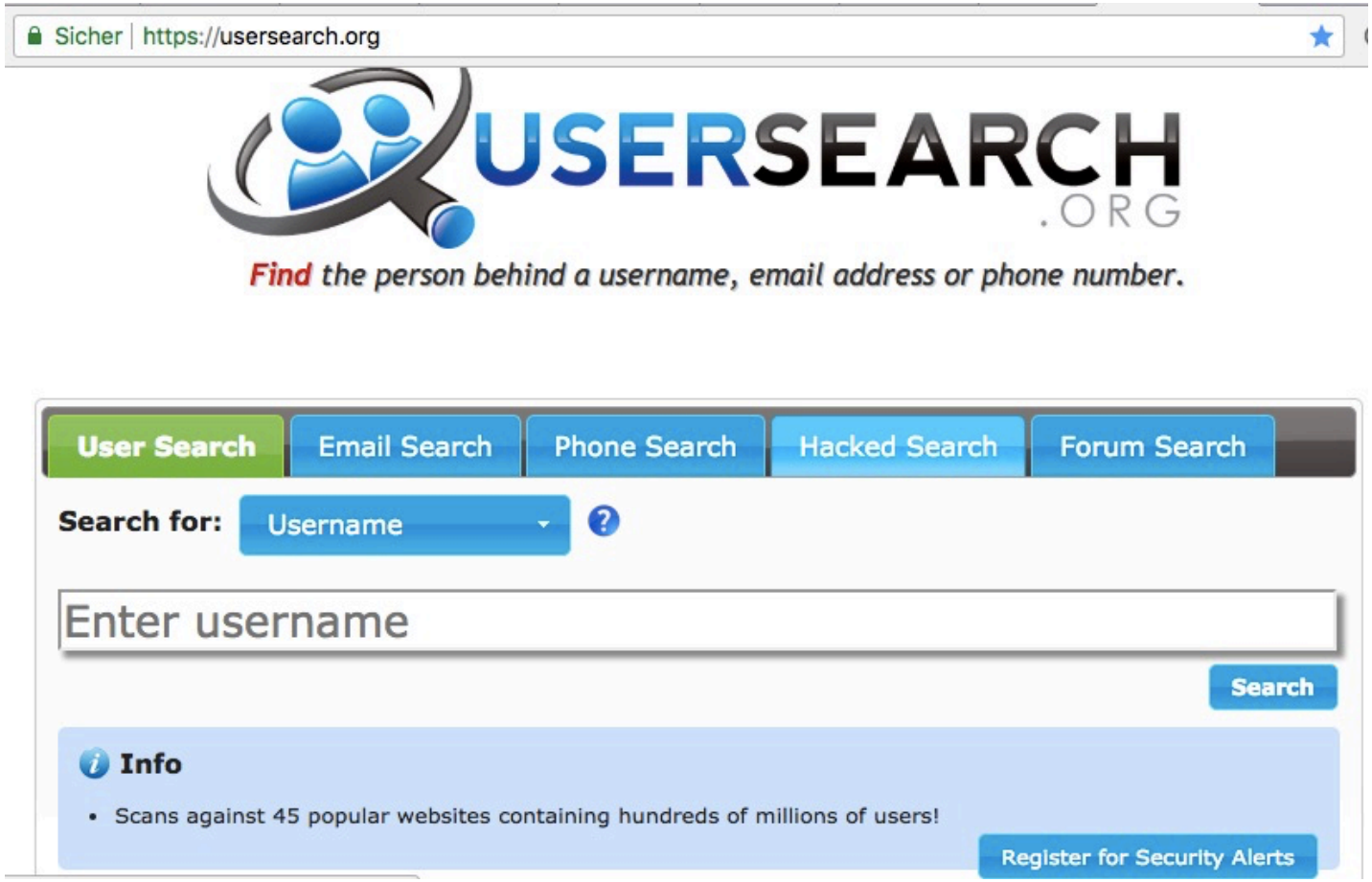
> *Excuse me, but who are you? I don't use this account except when I occasionally buy items.*
>
> *my ebay was hacked recently along with my email because I was keylogged. The hacked then proceeded to access my bank paypal and ebay. So no. I won't send you money for someone else hacking you but I do feel sorry for you.*

Betrug – Täterausforschung - Recherche

- Welche Information hat der Verkäufer?
  - Username Reddit
  - Username Ebay
  - IP Adresse (Verkäufer hat Fotos der Gutscheine auf seinem Server zur Verfügung gestellt)

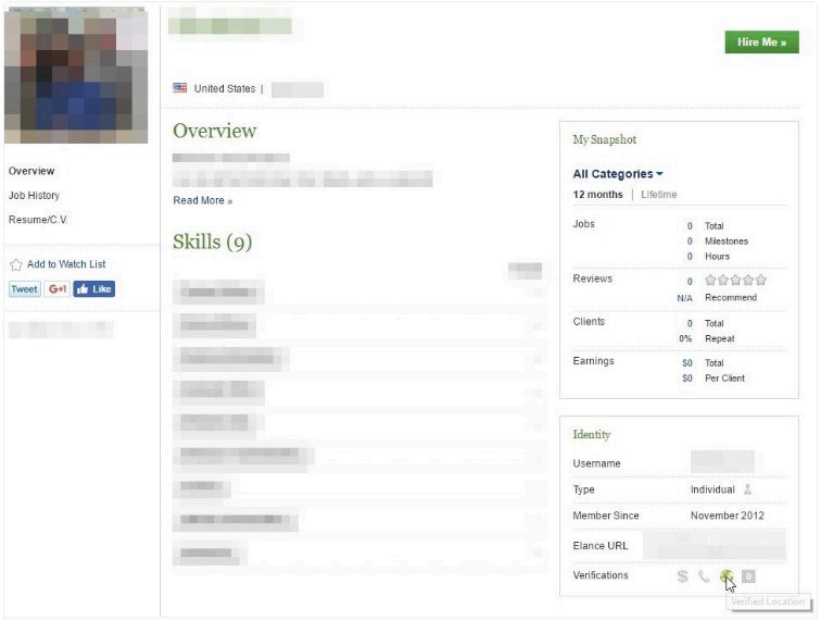
- Google-Suche nach Usernamen
  - Ergebnis: Ein Steam Account bei dem beide Usernamen verwendet wurden

Betrug – Täterausforschung - Username



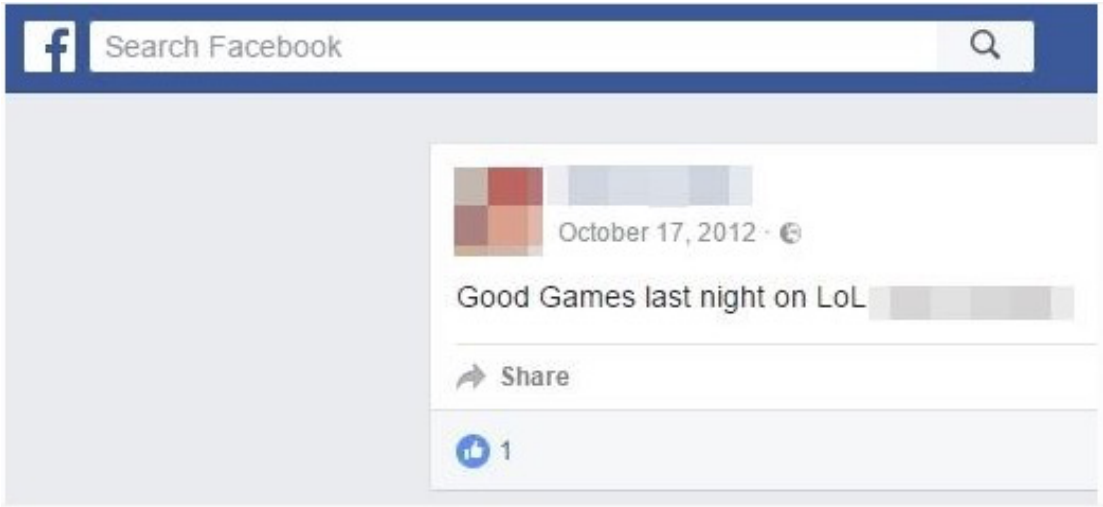
Betrug – Täterausforschung - Username

- Ergebnis:
  - Username auch auf Freelancer-Jobplattform wiedergefunden
  - Vorname, erster Buchstabe des Nachnamens
  - Wohnort <-> Wohnort auf Ebay
  - Wohnort <-> IP-Adresse

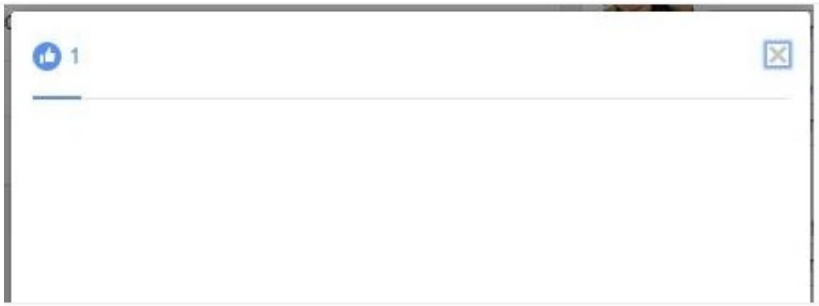


Betrug Täterausforschung - Facebook

- Facebook Search: Username



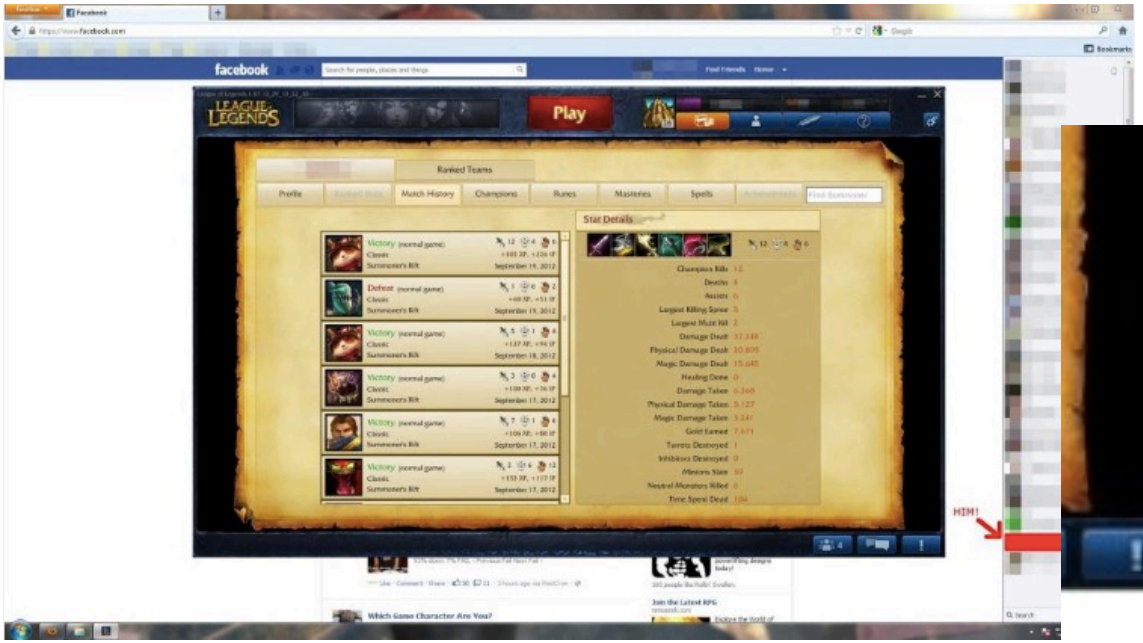
Scammer linked

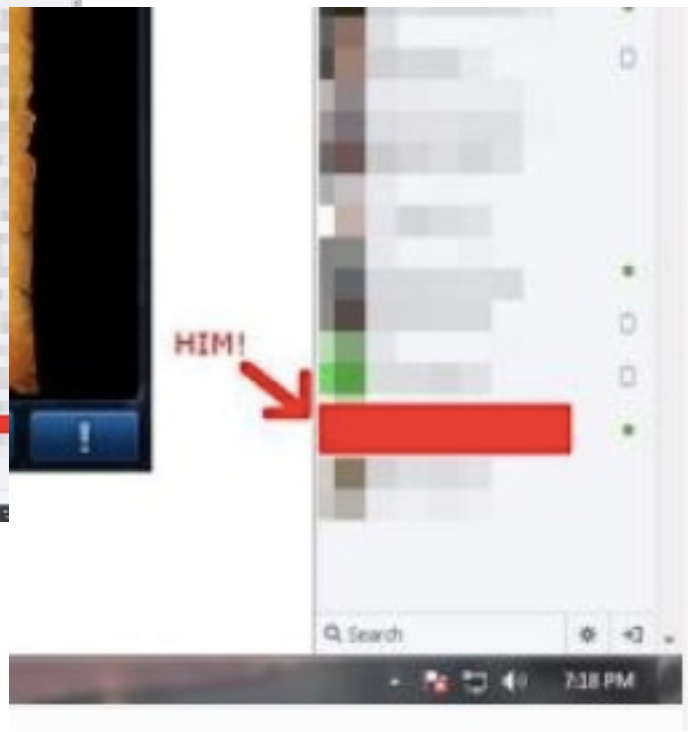


post like info on facebook

Betrug Täterausforschung - Facebook

- Nächster Schritt: Umfeldsuche
- Posts/Bilder des Freundes durchsuchen





Betrug Täterausforschung - Facebook

- Ergebnis:
  - Täter – Facebookprofil
  - Mutter und Bruder konnten ausgeforscht werdne
  - … die sich um das Problem gekümmert haben ☺

- DEMO

esse

Vielen Dank!

http://security.inso.tuwien.ac.at