Selbstkritik bei deutschen Journalisten unbekannt

MediaACT: „Criticism – unknown to German journalists“.

„More than one-third of the questioned German journalists never or hardly ever criticize their peers; two-thirds are never or hardly ever criticized even by their supervisors. Conclusion: Although German journalists regularly attack politicians and managers, they lack the experience of turning a critical view on themselves. This is a key result of an international study“.

„The project ‚Media Accountability and Transparency in Europe‘ is a comparative research effort on media accountability systems (MAS) in EU member states as indicators for media pluralism in Europe.“

---

10 Jahre Second Life

Happy birthday! Ich bin fast jeden Tag ein paar Stunden dort….

Kapitalismus – die Neurose der Menschheit

„Eine der größten Errungenschaften des Kapitalismus ist gerade, dass sich selbst der proletarische Sklave wie ein Meister fühlt. Dass selbst er glaubt, er habe die Wahl, sein Leben zu ändern. (…) Kapitalismus ist die Neurose der Menschheit.“ (Renate Saleci, Philosophin, für das deutsche Wikipedia zu irrelevant)

Spiegel online entblödet sich nicht, den Kapitalismus zu einer anthropologischen Konstante zu erklären: „Am Ende reflektiert Kapitalismus doch nur die menschliche Natur.“ Hätten Sie’s gewusst? Die Sklavenhaltergesellschaft oder das Lehnswesen sind wider die menschliche Natur, nur der Kapitalismus bringt uns Glück, Wohlstand und Freiheit für alle und erfüllt die Vorgaben der Evolution.

Merke: Nur Philosopen, schräge Vögel oder andere Spinner dürfen in Mainstream-Medien das Wort „Kapitalismus“ sagen. „Volkswirtschaftler“ aka Angehörige der Glaubensgemeinschaft Freier Markt(TM) jedoch nicht. Deren religiöse Weltanschauung zwingt sie, affirmativ „freie soziale Marktwirtschaft“ zu stammeln.

Durchschnittliche Wähler

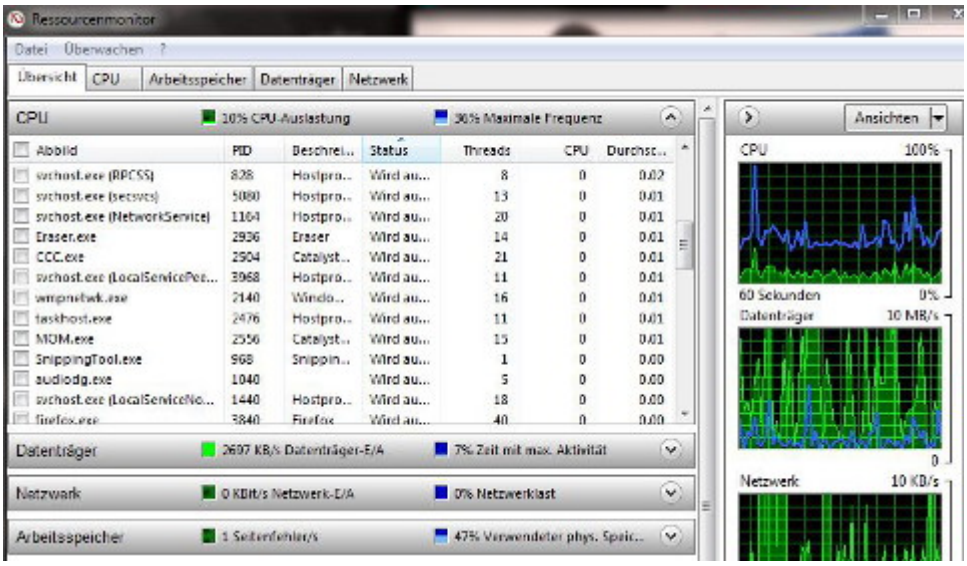
„The best argument against democracy is a five-minute conversation with the average voter.“ (Winston Churchill)

Ouito, revisited

Aus gegebenem Anlass ein Blick auf die Altstadt von Quito, der Hauptstadt Ecuadors – das Foto habe ich 1979 gemacht. Heute sieht es da natürlich ein bisschen anders aus.

Die Online-Durchsuchung live

beobachten



Kleiner Tipp am Rande für Windows(7)-Nutzer: Unter *Start | alle Programme | Zubehör | Systemprogramme | Ressourcenmonitor*
kann man sich alle laufenden Prozesse des Rechners anzeigen lassen.

Fall jemand eine unverschlüsselte E-Mail bekommen hat mit dem Betreff „Wir tun alles für Ihre Sicherheit!“ und das Attachment angeklickt hat und
die Frage *bundestrojaner_skype.exe is an unknown application – install anyway?* mit „ja“ beantwortet, kann dann live beobachten, was geschieht. Für Unix gibt es übrigens z.B. Monit.

Tweet of the Day 63

@ioerror: „A patriot must always be ready to defend his country against his government.“ (Edward Abbey)

Sollen die Idioten doch in ihr Unglück rennen

Aus einem Posting im Heise-Forum:
„Das Ausmaß und die Tatsache der Schnüffelei ist schon recht heftig – was mich aber an der ganzen Sache am meisten ankotzt, ist die Tatsache, wievielen Menschen das absolut egal ist oder sogar von ihnen befürwortet wird. Man hat ja nichts zu verbergen und so.

Das nervte mich schon immer, aber ich dachte: hey, wenn irgendwann rauskommt wie sehr wir überwacht werden, wachen die Leute auf. Falsch gedacht. Viele befürworten ja die Überwachung und freuen sich, daß dadurch total viele Terroranschläge auf ihre Nachbarschaft verhindert werden. Ja ne ist klar.

Ich habe keine Lust mehr. (…) Ich habe keinen Bock mehr den Leuten zu erklären, daß Zensur und Überwachung niemals gut ist. Sollen doch die Millionen Facebook-Idioten und Stasi-Befürworter in ihr Unglück rennen.“

Not Trusting Google is Good Idea

Herbert Snorrason (anarchism.is) (via Fefe):

I. Information to be disclosed by Google, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Inc., Google, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, deleted e-mails, emails preserved pursuant to a request made under 18 U.S.C. § 2703(f), the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files, and including any deleted information and any information preserved pursuant to a request made under 18 U.S.C. § 2703(f);

Noch Fragen? Will mir noch jemand eine unverschlüsselte E-Mail per GMail senden? Echt?

Landgericht Hamburg ab nach Regensburg? [Update]

Der Fall Mollath wird jetzt richtig spannend: Das Bundesverfassungsgericht hat sich eingeschaltet und will prüfen, ob es noch verhältnismäßig ist, dass jemand wegen Körperverletzung und Sachbeschädigung in der Psychiatrie sitzt.

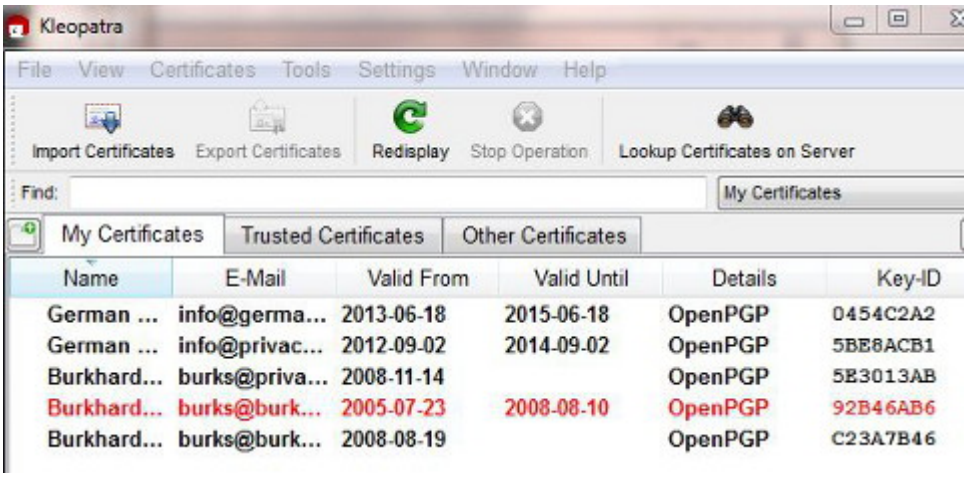
Ich wäre ja dafür, die Pressekammer des Landgerichts Hamburg nach Regensburg zu verlegen. Dessen Entscheidungen sind ja ähnlich „originell“. Würde also passen.

[Update] Vgl. Thomas Stadler | Internet-Law: „Mollath-Verteidiger legt nach“, Wolfgang Michal | Carta: „Die Taktik der Bayerischen Staatsregierung im Fall Mollath“, und Markus Kloeckner | Telepolis: „Fall Mollath: Abgehörte Telefonate beschäftigen Rechtsanwaltskammern“.

Was macht eigentlich der DJV?

Ein kleiner Beitrag von mir auf meinem Recherchegruppe-Blog über die Konsequenzen, die Journalistenverbände aus den aktuellen Abhör-Skandalen (nicht) ziehen.

Kleopatra sei Dank!



Hurra, nach stundenlangem Dröseln und Rätseln habe ich mein APG-Problem gelöst und kann jetzt auch E-Mails auf meinem Android-Smartphone verschlüsseln. Es gab zwei Probleme:

Erstens: Wie einige kundige Leser schon vermuteten, ist das Format, das Enigmail (das OpenPGP-Add-on für Thunderbird) zum Export der Schlüssel benutzt, offenbar nicht kompatibel mit der Dateiverwaltung von Android, obwohl der Schlüssel korrekt im ASCII-Format erscheint. Da muss man erst mal drauf kommen. Also genau das, was hier ~~in Klingonisch~~ erwähnt wird:
APG cannot import keys in .asc files terminated with CR/LF (PC-style): it requires LF only (UNIX style). If your PC editor offers you a choice (e.g., TextPad does) save the file as UNIX text.

Ich habe es also mit Kleopatra versucht und damit die öffentlichen und meine geheimen Schlüssel exportiert und auf das Smartphone gebeamt.

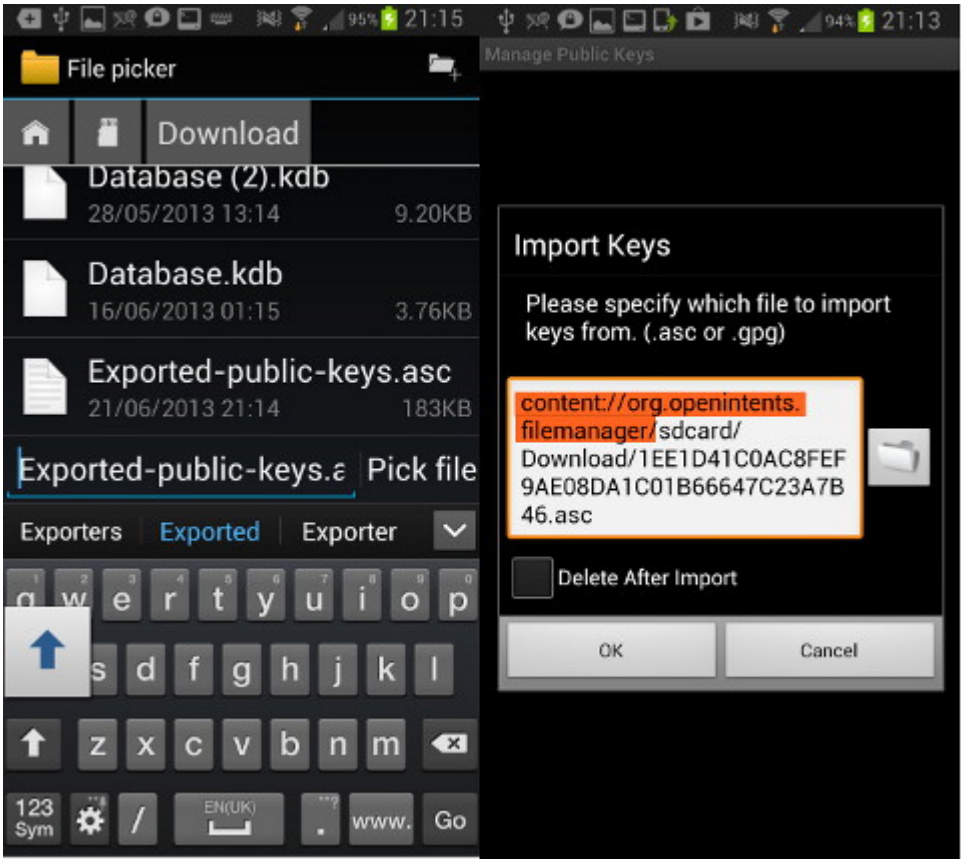
Nun zu uns, Programmierer! Wir sind ja alle dankbar, dass ihr uns das Schöne, Gute und Wahre Open Source und gratis usw. zusammendröselt und zum Downlad anbietet. Ihr habt aber trotzdem einen Knall: Welche Pappnase denkt sich für jeden Softwareschnipsel einen anderen Namen aus? Kleopatra, „ist der bevorzugte Zertifikatsmanager in Gpg4win“. Geht’s noch? Sind

wir hier im Gallischen Krieg oder beim großen Latinum? Und das nur, weil ihr Leute abschrecken wollt, das auch zu nutzen?

Was kriegt der Laie in den ersten fünf Minuten alles zu sehen: PGP, OpenPGP, GnuPG, Gpg4Win, GPG, OpenPGP & S/MIME, Algorithmenstärken, öffentliche und private Schlüssel, und jetzt auch noch Kleopatra – glaubt ihr denn, auch nur ein wohlwollender Nutzer und eine geneigte Nutzerin hat da noch Lust, überhaupt anzufangen? Und welche Knalltüte nennt die Schlüssel bei Kleopatra „Zertifikate“? Sogar ich musste erst überlegen und probieren, und ich verschlüssele meine E-Mails seit 1995.

Ich glaube, ich sollte mich mal selbst hinsetzen, der breiten Masse aufs Maul schauen und die Angelegenheit volkstümlich formulieren. So wird das nix.

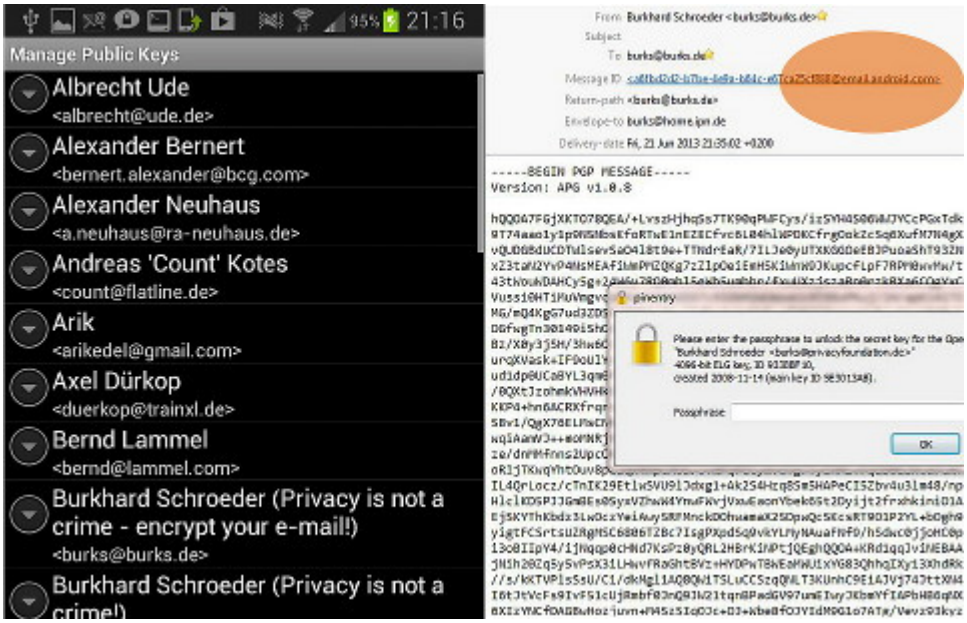
Wie sagte Paulus über das erfolgreiche Missionieren ganz richtig: „Den Juden bin ich geworden wie ein Jude, auf daß ich die Juden gewinne. Denen, die unter dem Gesetz sind, bin ich geworden wie unter dem Gesetz, auf daß ich die, so unter dem Gesetz sind, gewinne. Denen, die ohne Gesetz sind, bin ich wie ohne Gesetz geworden , auf daß ich die, so ohne Gesetz sind, gewinne. Den Schwachen bin ich geworden wie ein Schwacher, auf daß ich die Schwachen gewinne. Ich bin jedermann allerlei geworden, auf daß ich allenthalben ja etliche selig mache. Den DAUS bin ich geworden ein Dau, auf daß sie ihre E-Mails verschlüsseln lernen und ich sie selig mache.“



Zweitens: Auch der Dateimanager (ich nutze den OI File Manager) zickt herum.

Auf der linken Seite des oberen Screenshots sind die verschiedenen Dateien im Download-Verzeichnis zur Auswahl zu sehen. Wenn man eine ausgesucht hat und auf „pick file“ drückt, erscheint eben dieselbe, was auf der rechten Seite deutlich wird – hier will ich eine .asc-Datei (so hat Kleopatra meinen öffentlichen Schlüssel genannt) importieren. Niemand sagte mir aber, dass man per Hand (!) zunächst den vorderen Teil des Pfades (alles, was rot markiert ist), eliminieren muss, ansonsten kommt wieder die Meldung „file not found“.

Ich hatte nur so eine vage Ahnung, nachdem ich praktisch alle Forenbeiträge zum Thema der letzten drei Jahre gelesen habe. Das sind gar nicht so viele, und alle natürlich in Englisch. Ich habe einfach herumprobiert. Das kann man niemandem, der das lernen will, zumuten.



Der Verschlüsseln ist auch nicht einfach, und APG stürzt manchmal ab, warum, werde ich herausfinden. Aber immerhin habe ich alle öffentlichen Schlüssel importiert und es geschafft, mir selbst eine verschlüsselte E-Mail zu schicken, die ich mit einem meiner Rechner dann lesen konnte (MessageID email.android.com, oben rechts rot markiert)

Die nächste Aufgabe ist herauszufinden, wo APG die Schlüssel speichert. Ich habe mir für den Fall der Fälle, dass ich sie verstecken will, EDS installiert.

Time will remember this music

The best epic music ever… falls jemand meinen Musikgeschmack noch nicht kennt. Kann ich drei Stunden am Stück hören und auch noch über den Titel nachdenken.

Netzpolitik.org im #Neuland

Netzpolitik.org: „Dan Goodin betont diesen Punkt auf Ars Technica nochmal: Wer Anonymisierung wie Tor verwendet, wird gespeichert, egal ob US-Bürger oder nicht, weil man damit nicht nachweist, wo man ist. Und wer seine Kommunikation verschlüsselt wie mit OTR oder OpenPGP, dessen Kommunikation ist verdächtig und wird so lange gespeichert, bis die NSA sie entschlüsseln kann.“

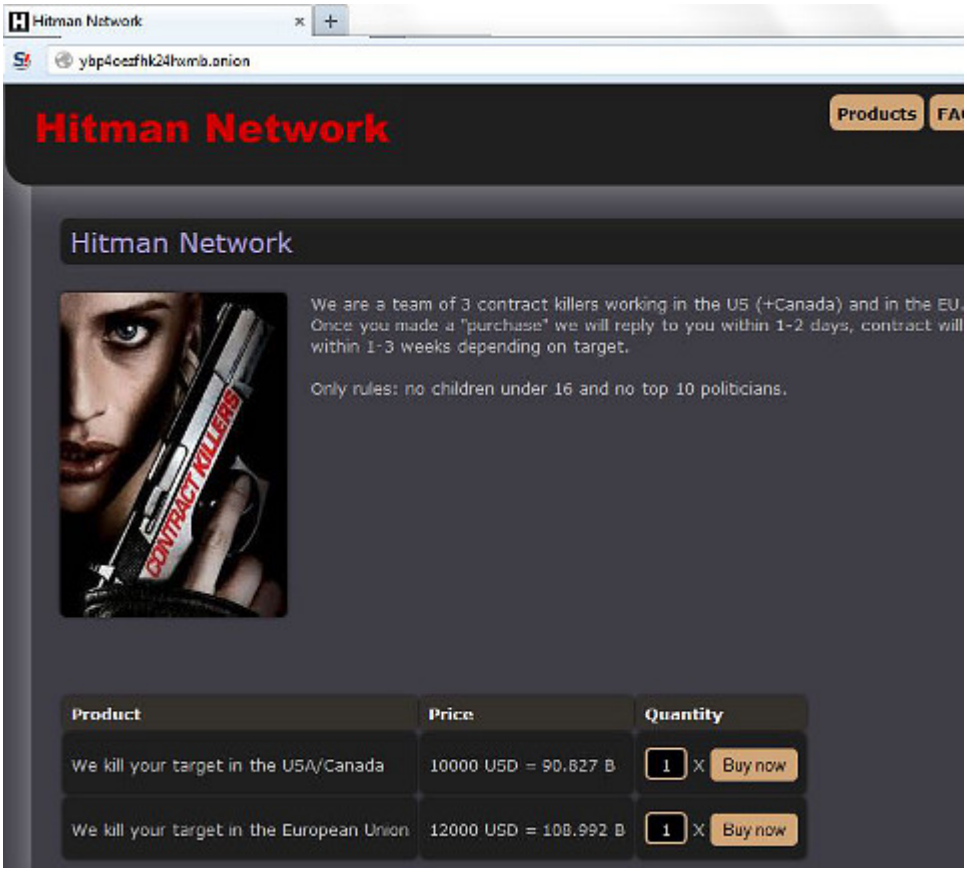
Ach ja? Die NSA kann OpenPGP entschlüsseln? Was für ein gequirlter Quatsch ist das denn? Und wie will man speichern, wer Tor benutzt? Selten so eine dämliche Verschwörungstheorie gelesen.

Der Autor Andre Meister „begleitet diverse netzpolitische Zusammenhänge“. Dann kann ja nichts mehr schief gehen. Wieder jemand, der mich von nun an ignorieren wird. In der Attitude der beleidigten Leberwurst braucht man keine Argumente mehr. Das kenn ich aus dem DJV.

[Update] An den Kommentaren bei netzpolitik.org kann man das Niveau der „Argumentation“ wunderbar verfolgen. Ich habe übrigens *nie* behauptet, dass es keinen „Staatstrojaner“ gebe, sondern dass der so, wie die Medien sich das vorstellten, nicht funktioniert, nur, wenn das „Opfer“ denkbar bescheuert ist. Und „Abfallprodukte“ von Skype sind ja wohl etwas anderes. Aber ich füttere auch keine Trolle.

Deepsearch im Darknet

[Update]



In den letzten Tagen habe ich mich aus Recherchegründen mehrfach im Darknet herumgetrieben. Ausserdem konnte ich mir nicht erklären, warum Deepsearch, eine Suchmaschine für diesen – verborgenen – Teil des Internet, auf einigen Rechnern und ausgerechnet während meines Seminars zum Thema einfach nicht aufrufbar war.

Wie naiv muss man eigentlich sein, um eine „Contract Killer“-Seite ernst zu nehmen, womöglich mit Vorkasse? 10.000 Dollar pro Kopf – „Quantity: 1“ – „in den Einkaufskorb legen“? LOLWUT?

Das Hiddenwiki (im Darknet erreichbar nur via Tor-Browser) erklärt die Technik und worum es geht: „We all know of the dark underground world of drug dealing, arm dealing and other criminal activities offline. What most of us don’t know is that the same world exists online.“

Der Kollege Andreas Winterer hatte auf Hyperland schon vor zwei Jahren einen sehr informativen Artikel verfasst – „Das unbekannte Schatten-Internet“ – und auf ein Statement der Hacker-Gruppe *Anonymous* (jeder kann sich diesen Namen zulegen, auch die NSA) hingewiesen, die versucht hatte, in der „#OpDarknet“ mehrere Serverm auf denen besonders ekelhaften Dinge angeboten wurden, lahmzulegen. Das ist wohl nicht wirklich gelungen.
The ‚darknet‘ sites of TOR, I2P, and Freenode peaked our interest. We were aware that, TOR and I2P where originally designed to protect individuals from the oppressive governments of China, Iran and protect Free Speech. (…) What we discovered was quite the opposite. An growing and large of community of pedophiles was abusing such systems for personal profit.“

Anonymous behauptet, die Identität einiger krimineller Nutzer aufgedeckt zu haben; ohne konkrete Beweise bleibt das für mich bloße Denunziation. In der Official Release – 10/15/2011 wird sogar auf Nutzer hingewiesen, deren einschlägige Youtube-Channel auch noch nach zwei Jahren vorhanden sind. Entweder ist also an den Vorwürfen nichts dran, oder es handelt sich um Lockspitzel-Angebote der US-amerikanischen Strafverfolger (denen ist so etwas erlaubt). Ich glaube nicht, dass ein Channel nach dem Hinweis „pädaphile Angebote bei Youtube“ auch nur zehn Minuten online wäre – Youtube hätte das sofort abgeschaltet. Bei Sven Slootweg ist noch ein Statement zu sehen, das sich offenbar auf die „#OpDarknet“ bezieht.

Interessant ist, wie *anonymous* versucht hat, Teile des Darknets anzugreifen:
The WWW started to ask about our tools called ‚The Legion‘, ‚THOR‘ aka ‚Chris Hansen‘. The best way to describe them is to refer at the US patents #5,621,671 and #6,947,978. Many asked if were simply „script kiddies“. No we specifically developed the tools ‚The Legion‘, ‚THOR‘, ‚Chris Hansen‘ in protest of Lolita City, Freedom Hosting, and the Hidden Wiki.

Aus der Patentbeschreibung für 5,621,671:
Method for geolocating logical network addresses on electronically switched dynamic communications networks, such as the Internet, using the time latency of communications to and from the logical network address to determine its location. Minimum round-trip communications latency is measured between numerous stations on the network and known network addressed equipment to form a network latency topology map. Minimum round-trip communications latency is also measured between the stations and the logical network address to be geolocated. The resulting set of minimum round-trip communications latencies is then correlated with the network latency topology map to determine the location of the network address to be geolocated.

Fazit: Natürlich nutzen Kriminelle auch die gängige Technik, im Internet anonym zu bleiben. Bankräuber nutzen auch die Technik der Fahrzeugkonstruktion, um Fluchtwagen zu benutzen. Das ist der Preis, den man für die Freiheit bezahlen muss. *Anonymous* hingegen schreibt:
One thing is clear, #OpDarknet did reveal that the benevolent community used to uphold Free Speech against the oppressive governments of Iran and China. It is now corrupted by the underground of trading and sale of Child Pornography aka „kiddie porn“.

Das halte ich für waschechtes Agent-provocateur-Sprech. Erstens ist diese Tatsache schon so lange bekannt, wie es Tor und das Darknet gibt, also keine Überraschung, und zweitens ist das ein mehr als durchsichtiger Versuch, die Anonymisierungs-Netze insgesamt zu diskreditieren, was für Leute, die sich „Hacker“ nennen und anonym bleiben wollen, eher eine *contradicio in adiecto* ist.

How to remain anonymous – Always watch your back

Bitte versucht nicht ohne das dementsprechende Wissen, wie man einen Browser „abdichtet“ und wie man vermeidet, Datenspuren

zu hinterlassen, in den dunklen Ecken des Internet herumzusurfen. Das ist gefährlich:
„Bei Sicherheitsbehörden aber bedeutet Inkompetenz gefährliche Unberechenbarkeit, wegen der auch das Argument ‚Wer nichts zu verbergen hat…' nicht zieht. Das Risiko, in einer Antiterrordatei zu landen, ohne dass man die geringste Ahnung hat, warum, ist sehr real geworden – mit allen Konsequenzen von Einreiseverboten bis hin zum nächtlichen Besuch eines Sonderkommandos." (Herbert Braun, Computerzeitschrift c't, Leitartikel 7/2013)

Update: Vgl. torrorists: „Tor network mostly contains legal content".

Troll, troller, am Trollsten

Nur mal so kurz zwischendurch die Hinweis auf die „besten" deutschsprachigen Websites aller Zeiten: die „Dr. Gernot Hochbürder Stiftung – Institut zur Bekämpfung der psycho-medizinischen Computerkriminalität" (danke, Ruedi!) und natürlich der Klassiker Ingenfeld.

Gute Gründe zum Mitlesen

„Wenn überhaupt, dann liest die Regierung Ihre E-Mails oder lauscht Ihren Telefongespräche mit einem guten Grund.“ (Ein Vertreter des indischen „Telekommunikationsministeriums“ laut Heise).

Warum ist unserer Totalüberwachungs- und Vorratsdatenspeicherungslobby dieser Satz noch nicht eingefallen? Bosbach (CDU) und Hartmann (SPD), übernehmen Sie!

APG für Android

Mein Problem mit APG ist immer noch nicht gelöst. Der Entwickler reagiert nicht.

Zum Beispiel 1:
Importing works when I specify the full path to the key manually and not over the OI file manager.
Ausprobiert, geht trotzdem nicht.

Selecting the file with the OI file manager leads to the path „content://org.openintents.filemanager/mnt/sdcard/…“.
All before /mnt should not be included in the path.
Ausprobiert, geht trotzdem nicht (ausserdem ist der Pfad bei mir anders.)

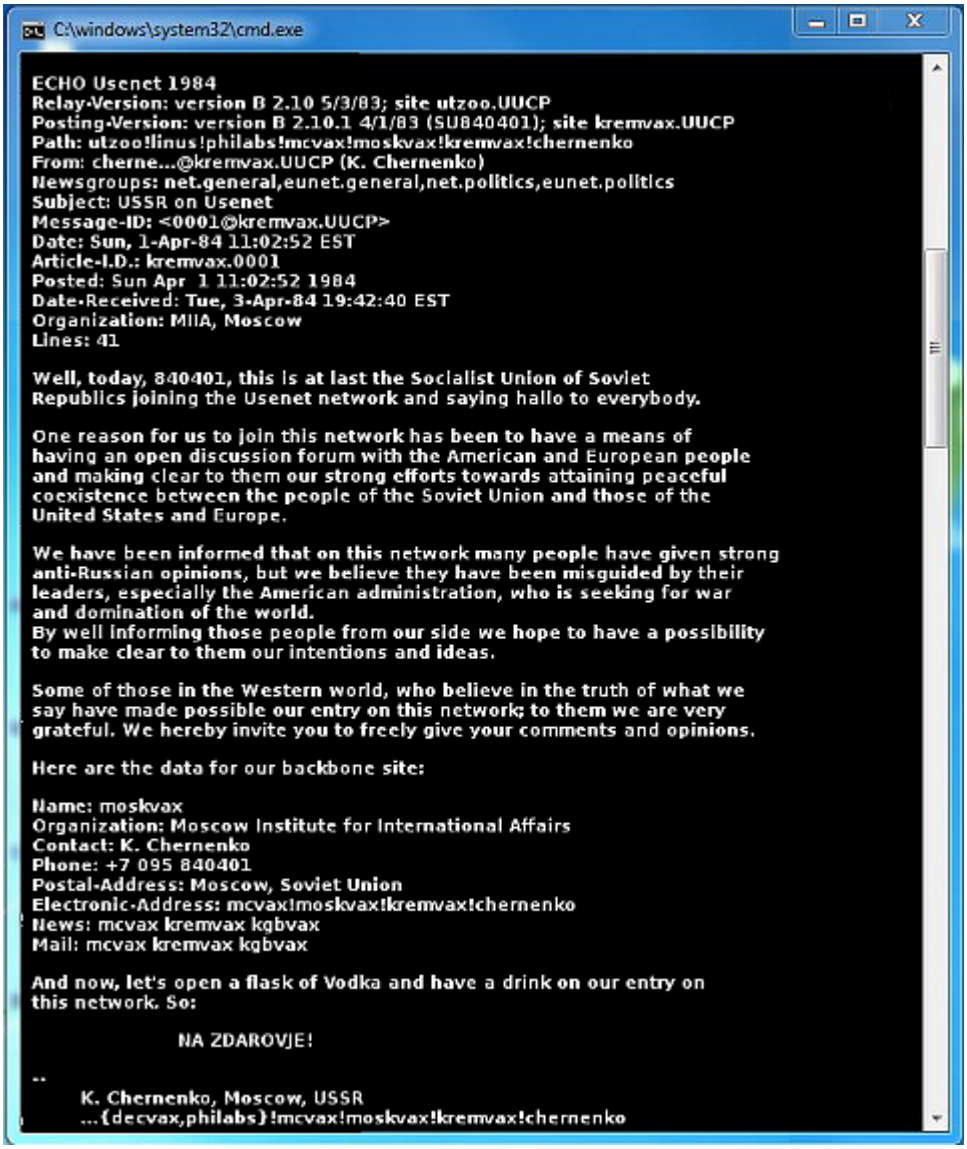
I had to add the .asc file extension to ASTRO to get my keys imported.
War bei mir eh schon so.

Zum Beispiel 2:
APG cannot import keys in .asc files terminated with CR/LF (PC-style): it requires LF only (UNIX style). If your PC editor offers you a choice (e.g., TextPad does) save the file as UNIX text.
Könnte es das sein? aber die keys sind doch im ASCII-Format. direkt aus dem Keymanager von Enigmail (Thunderbird) exportiert. (Das wird hier auch empfohlen.)

Copy the .asc files on your phone (e.g. via USB), the location does not matter.
Offensichtlich doch.

Bin ich der einzige Mensch auf der Welt, der seine E-Mails auch auf dem Smartphone verschlüsseln will? Verdammt!

Neulich in Neuland

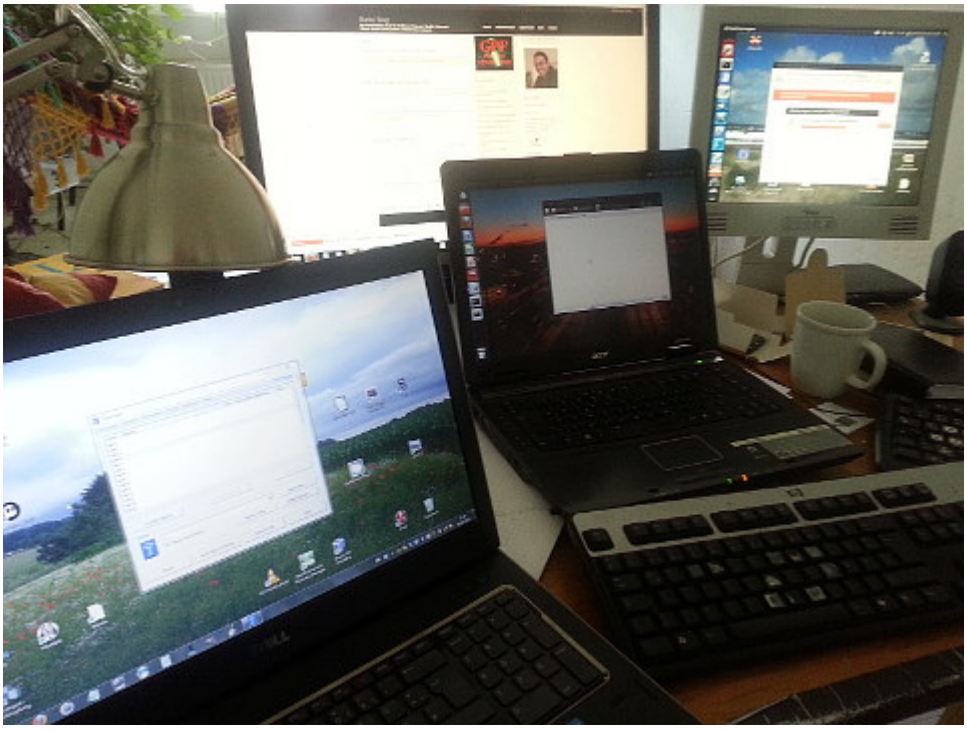


Focus online: „Das World Wide Web mag 23 Jahre alt sein, sein Vorgänger noch älter. Das Internet hat sich in diesen 23 Jahren allerdings so sehr entwickelt, das es kaum wiederzuerkennen ist.“

Seit 23 Jahren – jetzt muss ich rechnen… Wir befinden uns also im Jahr 1990. „Sein Vorgänger“? Hatte das WWW „einen“ Vorgänger? Echt jetzt?

Unendliche digitale Weiten. Seit ~~einem Jahr~~ vielen Jahren kreuzt ~~die Enterprise nun durch die Galaxis~~ Crosspoint durch das Internet. Da begegnete mir etwas Seltsames, was ich hier dokumentiere…

Im Maschinenraum



Heute, nach dem Frühstück, habe ich mich auf eine (noch) ungedrosselte Pirsch nach Neuland begeben…