# Datenspuren 2008

----------<<<//>>----------

Workshop Browsersicherheit

# Über mich

----------<<</>>----------

- Verehrer der Privatsphäre
- Wohne seit 07 in DD
- Erste Datenspuren
- Blog: http://kopfueber.wordpress.com
- Spaß am Dinge erlernen, basteln und bauen

# Gliederung

----------<<<//>>----------

- 1. Teil: Sicherheit
  - Aufbau von HTTP
  - HTTPS: HTTP mit SSL
  - Aktive Inhalte (JavaScript & Flash)
  - Browser im ganzen

# Gliederung

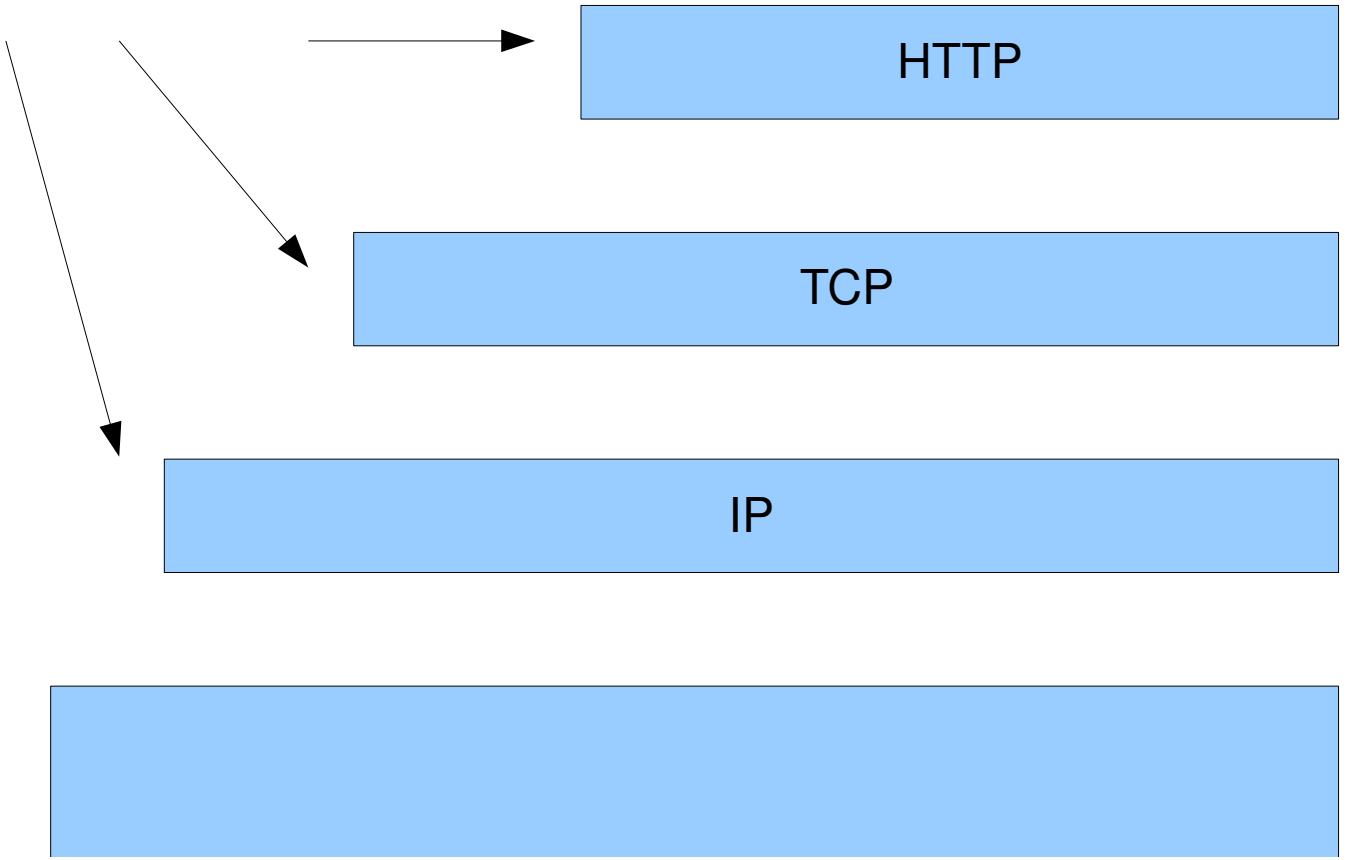
----------<<</>>----------

- 2. Teil: Praxis - Wie kann ich mich schützen?
  - Welcher Browser?
  - Plugins
  - Benutzung dieser
  - Und was gibt’s sonst? Proxies, Sandboxes

# Senden/Empfangen von Daten

----------<<</>>----------

Pro Layer, mehr Daten dazu!



# IP, DNS

----------<<</>>----------

- Jeder Rechner wird über IP-Adresse angesprochen
  - z.B. 123.456.789.100
- Da man sich lange Nummern schlecht merken kann -> Namen (www.beispiel.de)
- Werden durch sog. DNS Server verwaltet, funktionieren wie Telefonbuch

# DNS

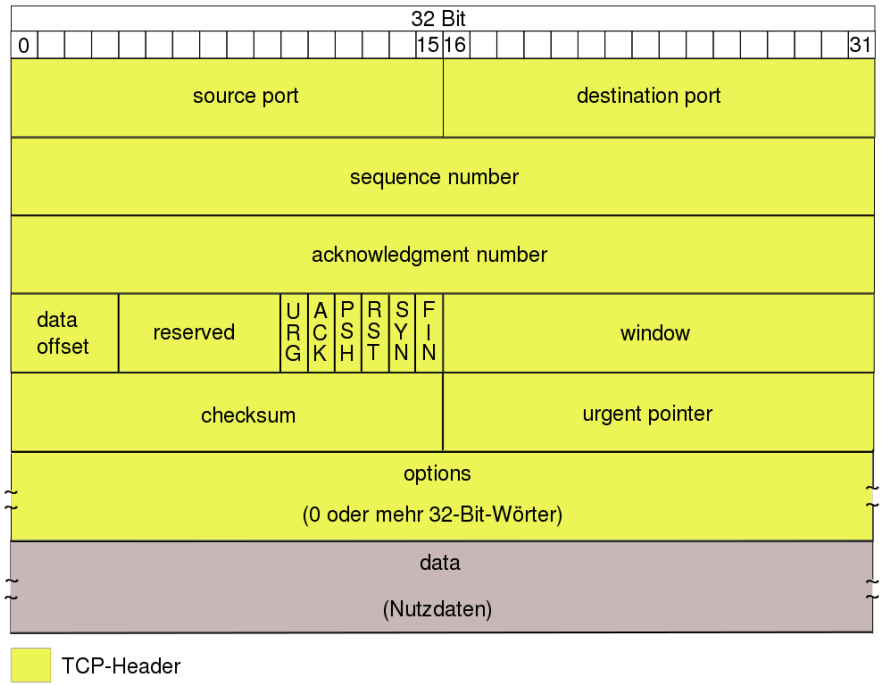
----------<<<//>>----------

- Problem: Wenn IP-Adresse nicht mit Name-Record übereinstimmt
  - Beispiel: **beispiel.de** hat IP 123.456.789.100
  - Angreifer verändert IP zu 001.987.654.321
  - Name wird falsch aufgelöst, Benutzer landet auf 001.987.654.321 anstatt auf 123.456.789.100
- Damit ist auch Zensur möglich – Namen die nicht aufgelöst werden können, gibt es nicht
- Der ISP weiß wo man surft (wg. DNS Anfragen)

# TCP/IP

----------<<<//>>----------

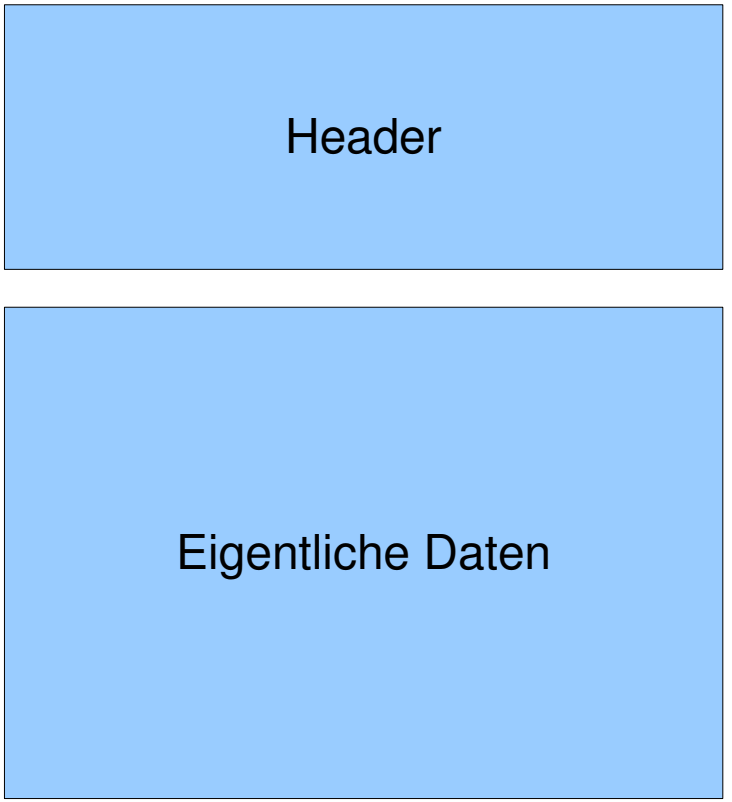
- TCP over IP
- IP: Verbindungsprotokoll
- TCP
  - Transport der Nutzdaten
  - In data: z.B. HTTP



# HTTP

----------<<</>>----------

- HTTP
  - Enthält die eigentlichen Daten
  - Außerdem im Header:
    - Referrer
    - User-Agent
    - Cookies



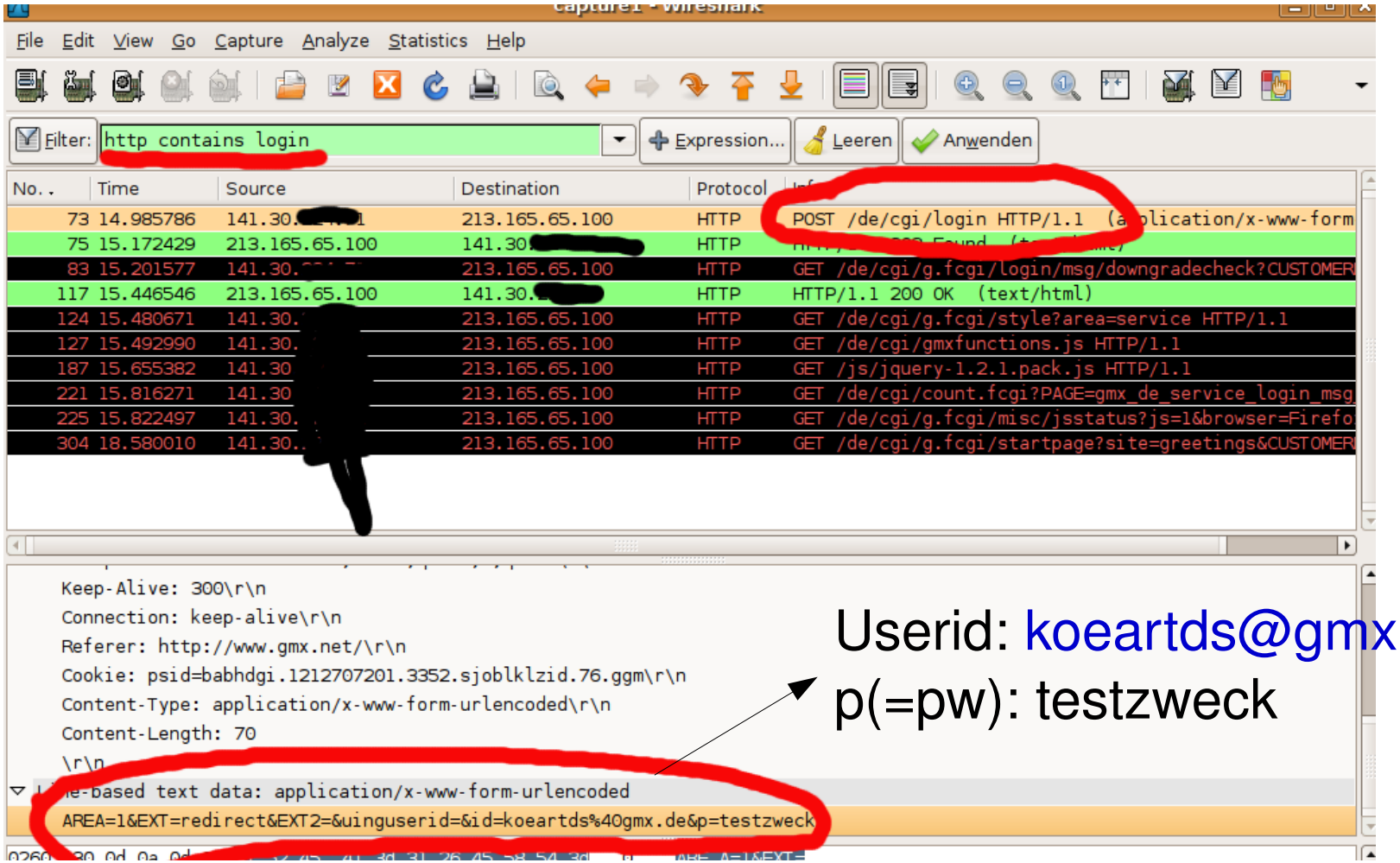
# HTTP

----------<<</>>----------

- Super Sache, oder?
- Header gibt Dinge über User preis (dazu später)
- Sicherheitsproblem: Daten werden im Klartext übertragen!!1!
- Ja, auch Passwörter!

# HTTP: PW lesen!

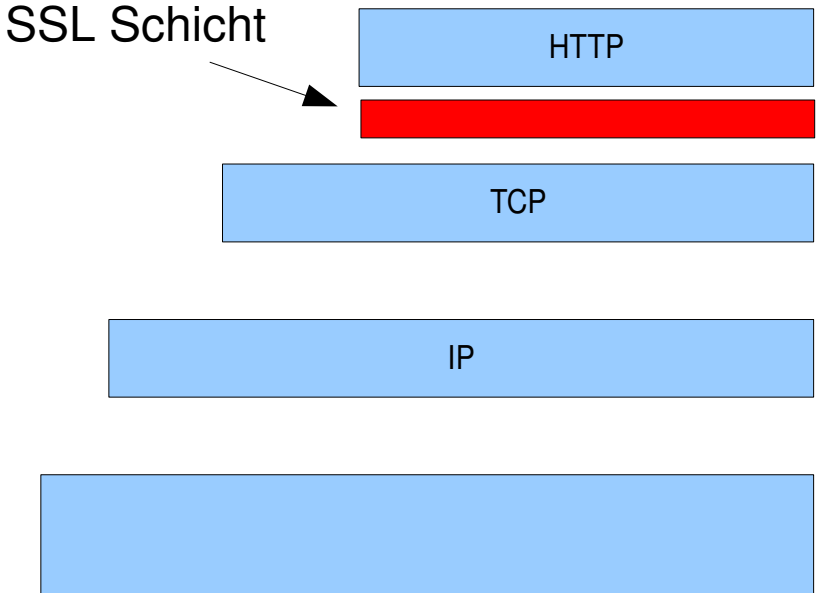
----------<<</>>----------



# HTTPS, HTTP over SSL

----------<<<//>>----------

- Hierbei wird eine sichere Verbindung zwischen Server und Client aufgebaut
- Über diese Verbindung wird HTTP geschickt
- Tipp: anstatt http://gmx https://gmx



# SSL

----------<<</>>----------

- Funktionsweise:
  - Es wird ein gemeinsamer symmetrischer Schlüssel ausgetauscht
  - Mit diesem werden Nutzdaten verschlüsselt
  - Standardport: 443

# SSL - Ablauf

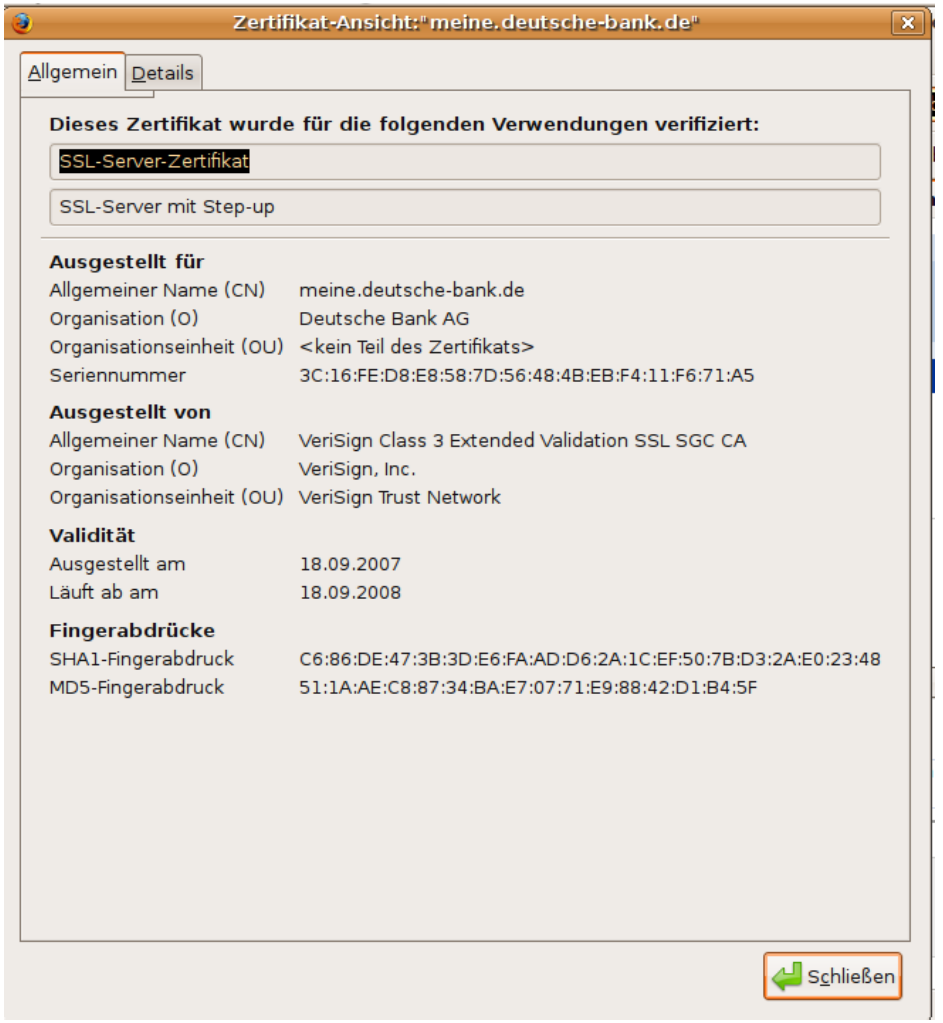
----------<<<//>>----------

- Erster Schritt
  - Client schickt ein client_hello an Server, dieser schickt ein server_hello zurück
  - Es wird eine Zufallszahl übertragen (32 Bit)
  - Mögliche Verschlüsselungsverfahren werden ausgetauscht
  - Es wird Session ID vergeben
- Zweiter Schritt
  - Server schickt Zertifikat (nach X.509 Standard) an Client
- Dritter Schritt
  - Client versucht Zertifikat zu verifizieren
  - Evtl. wird Schlüssel aus Zertifikat übernommen
- Vierter Schritt: Erzeugung des symmetrischen Schlüssels

# X.509 Zertifikat

----------<<<//>>>----------

- Werden z.B. mit OpenSSL erzeugt
- Eigentümer wird von Aussteller überprüft
- Zertifizierungsstellen (Aussteller) sind hierarchisch organisiert ≠ „Web-of-Trust“



# SSL-Schlüssel

----------<<</>>----------

- SSL besteht aus öffentlichem und geheimen Schlüssel
  - Öffentlicher Schlüssel: Verschlüsselung
  - Geheimer Schlüssel: Entschlüsselung
- Wie wird signiert?
  - Aus privatem Schlüssel wird ein „Certificate Sign Request“ erstellt, wird Zertifizierungsstelle geschickt
  - Es kommt (nach Prüfung) das Zertifikat
  - Zertifikat wird als Public Key an Client geschickt

# SSL Zertifikate

----------<<<//>>----------

- Wie überprüft man nun?
  - Häufig: Extended Validation Certificate
  - In Browser wird Zertifikatseigentümer und Eigentümer der Domain angezeigt. Stimmen diese überein ist alles gut
  - Wenn nicht – Finger weg!
  - Ablaufdatum muss in Zukunft liegen (keine abgelaufenen Zertifikate akzeptieren)
- Zertifizierer: z.B. Thawte, VeriSign, CAcert u.a.

# JavaScript, Flash

----------<<</>>----------

- JavaScript/Flash werden Clientseitig ausgeführt
- In Sandbox, können nur auf Browser zugreifen
- ABER: Browser Bugs!!1!!
- JavaScript
  - Kann z.B. Link-Ziele fälschen
- Flash
  - Kann „Flash-Cookies“ anlegen – nicht im Browser sichtbar

# Toolbars, Adware, Spyware

----------<<</>>----------

- Fiese Tools
- Installiert man sich bei kostenlosen Programmen: ICQ, Skype, MSN, KaZaa, etc pp
- Problem: Wenn mit Browser verbandelt, keine Kontrolle mehr durch Firewall, da man Browser ja nicht Internet verbieten kann
- Sehr schwer zu deinstallieren
- Was machen sie wirklich?

# Toolbars, Adware, Spyware

----------<<<</>>>----------

- FINGER WEG!1!

# Teil 2: Anonymität und Praxis

----------<<<//>>----------

- Warum muss man auf Anonymität achten?
- User können (wieder)erkannt und verfolgt werden durch:
  - IP-Adresse
  - Cookies
  - Andere Sachen aus HTTP-Header (User-Agent, Referrer)
- Aber: Header kann man verändern!

# Teil 2: Anonymität und Praxis

----------<<<//>>----------

- Auch nicht gut: Java(Script), Flash
- Mit Java(Script) können Informationen über den Computer abgefragt werden -> Identifizierung TROTZ modifizierter Header
- Werbung oft mit Hilfe von Java(Script) und Flash realisiert
- Leider brauchen einige Seiten JS/Flash (z.B. Youtube) -> Flexibiltät gefordert!

# Plugin: Adblock+

----------<<<</>>>----------

- https://addons.mozilla.org/de/firefox/addon/1865
- Blockiert Werbung
- Man kann selbst Objekte blockieren (grafiken etc)
- Vordefinierte Filterlisten
  - Ich benutze „Dr. Evil“

# Plugin: NoScript

----------<<<//>>----------

- https://addons.mozilla.org/de/firefox/addon/722
- Verhindert das ausführen von Java(Script), Flash etc
- Blacklist, Whitelist, Temporär
- Kann jedem einzelnen Skript Erlaubnis geben/verweigern

# Cookies

----------<<</>>----------

- Werden im HTTP-Header übertragen
  - Aufbau:

| Feld | Beschreibung | Beispiel |
|---|---|---|
| Name | ASCII Name & Wert | gmxsid_de433[...] |
| Expires | Ablaufdatum | Sa 26 Jun 2010 11:04:17 CEST |
| Max-Age | Ablaufzeit in Sek | |
| Domain | Wer darf Cookie sehn? | .gmx.net |
| Path | z.B. ausgewählte Site-Abschnitte | / |
| Comment | Kommentar | |
| Secure | Cookie sicher übertragen? | Nein |

# Cookies

----------<<</>>----------

- Erleichtern einem die Arbeit (angemeldet bleiben etc)
- ABER: Ermöglichen es dem Server User wiederzuerkennen – auch wenn sich deren IP-Adresse geändert hat
- Ablaufdatum: Zum Teil auf max (Jahr 2035)
- Beispiel auf *de.wikipedia.org/wiki/HTTP-Cookie*

# Plugin: CS Lite

----------<<<</>>>----------

- https://addons.mozilla.org/de/firefox/addon/5207
- Cookie-Manager
- Blacklist/Whitelist, temporär etc.
- Man kann Ausnahmen der Sitzung am Ende wieder löschen lassen

# User-Agent

----------<<</>>----------

- Beispiel:
  - Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312461; Irgend-Ein-Name)
- Man kann Rückschlüsse auf:
  - Patchlevel schließen -> Sicherheit
  - Betriebssystem Infos bekommen ->Sicherheit
  - User identifizieren -> Anonymität
- Auch NutzerGRUPPEN erkennbar (Linux-Nutzer)

# User-Agent

----------<<<//>>----------

- Desto einzigartiger man ist (z.B. wenn man sich alles selbst kompiliert), umso mehr hebt man sich aus der Masse hervor
- Wozu braucht man den?
  - Browserweichen zur Darstellung von Webseiten
  - Gute Webseiten sollten auch so funktionieren
- Möglichst zur größten Teilmenge gehören (z.B. Windows XP Nutzer, mit IE 6)
- Kann man verändern

# Plugins: User-Agent Switcher

----------<<<//>>----------

- https://addons.mozilla.org/de/firefox/addon/59
- Verändert den User-Agent
- Damit ist Surfer nicht mehr über User-Agent identifizierbar

# Referrer

----------<<<//>>----------

- Beispiel:
  - 141.xxx.xxx.xxx - - [Da/tum/hier:00:11:59 +0200] "GET /security/email_know_how.htm HTTP/1.1" 200 47407 www.gurusheaven.de "http://www.google.at/search?q=header+von+email+aufbau&ie=UTF-8&hl=de&btnG=Google-Suche&meta=" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; LYCOS r04/02)" "-"
- Man erkennt, wie die Seite gesucht wurde

# Referrer

----------<<<//>>----------

- Nützlich für Webmaster: Woher kommen die Leute? Wie wurde ich gefunden?
- Legt die Interessen der Leute offen
  - Man sucht bei Google nach „Barbie Puppen“
  - Man geht zu Amazon
    - Amazon sieht den Suchstring
    - Kann einen direkt Barbies anbieten

# Plugin: RefControl

----------<<<//>>----------

- https://addons.mozilla.org/de/firefox/addon/953
- Verändert den Referrer
- Sites können nicht mehr nachvollziehen, woher der User kam

# Such-Logs

----------<<<//>>----------

- Suchanfragen verraten viel über Nutzer
- Am 7.8.2006 macht AOL reSearch 20 Millionen ANONYMISIERTE Suchanfragen von 658.086 Nutzern öffentlich (ca. 30 Suchanfragen pro Nutzer)
- Daraus wurde u.a. 62-jährige Thelma Arnold (#4417749) identifiziert

# Such-Logs: Thelma Arnold

----------<<<//>>----------

- Suchanfragen:
  - Medizinischer Rat bei tauben Fingern
  - Landschaftsgärtnern in ihrem Wohnort
  - Vor- und Nachnamen von Verwandten
- Keine speziellen Suchanfragen
- Wer viel sucht, gibt noch mehr über sich Preis!
- Verschiedene Suchmaschinen zur Recherche nutzen

# Plugin: TrackMeNot

----------<<<</>>>----------

- http://mrl.nyu.edu/~dhowe/TrackMeNot/
- Sendet Suchanfragen an Google, AOL, usw
- Damit nicht mehr nachvollziehbar, ob User eine ECHTE Suchanfrage stellt, oder das Tool sucht
- Suche wird breiter gefächert, es wird nach Unsinn gesucht, damit kein eindeutiges Profil von Nutzer mehr erstellbar

# Jenseits des Tellers

----------<<</>>----------

- z.B. Firefox oder Opera statt IE verwenden (mehr Konfigurationsmöglichkeiten)
- Proxies: Können Header etc. filtern, IP verschleiern etc
  - Beispiel: Privoxy (privoxy.org)
- Sandboxes: sperren Browser ein
- Anonymisierungstools/~netzwerke
  - Beispiel: TOR (->Workshop auf DS!; torproject.org)

# Und sonst?

----------<<<//>>----------

- Am unsichersten: Der USER!!1! Überlegen was man installiert, auf Programme verzichten lernen
- OpenSource besser als ClosedSource, man kann einsehn was Programme machen
- Alternativ Programme nutzen (z.b. pidgin anstatt ICQ)
- Andere Fragen, z.B. heute!

# Das wars jetzt aber!

----------<<<//>>----------

Danke für Aufmerksamkeit!
Folien unter
http://www.datenspuren.de/fahrplan/events/2562.de
oder
http://kopfueber.wordpress.com