Surfen - sicher und komfortabel

Computerlabor im KuZeB
computerlabor.kire.ch

12.10.2009

Kire
www.kire.ch

Layout-Template von Chih-Hao Tsai
chtsai.org

Inhaltsverzeichnis

World Wide Web - Hintergründe

- Hypertext-System von Tim Berners-Lee
  - als Projekt 1989 am CERN entstanden
- WWW ≠ Internet

- Kernstandards
  - HTTP (Übertragungsprotokoll)
  - HTML (Seitenbeschreibungssprache)
  - URL (Ressourcenbezeichner)
- Weitere Standards
  - CSS (Trennung von Darstellung und Inhalt in HTML)
  - JavaScript (Clientseitige Skriptsprache)
  - HTTPS (Verschlüsselung & Authentisierung)

World Wide Web - Clients & Server

- Webserver
  - Apache HTTP Server
  - Microsoft Internet Information Services (IIS)
- Webbrowser
  - Windows Internet Explorer
  - Mozilla Firefox
  - Safari, Opera, Google Chrome

World Wide Web - HTTP

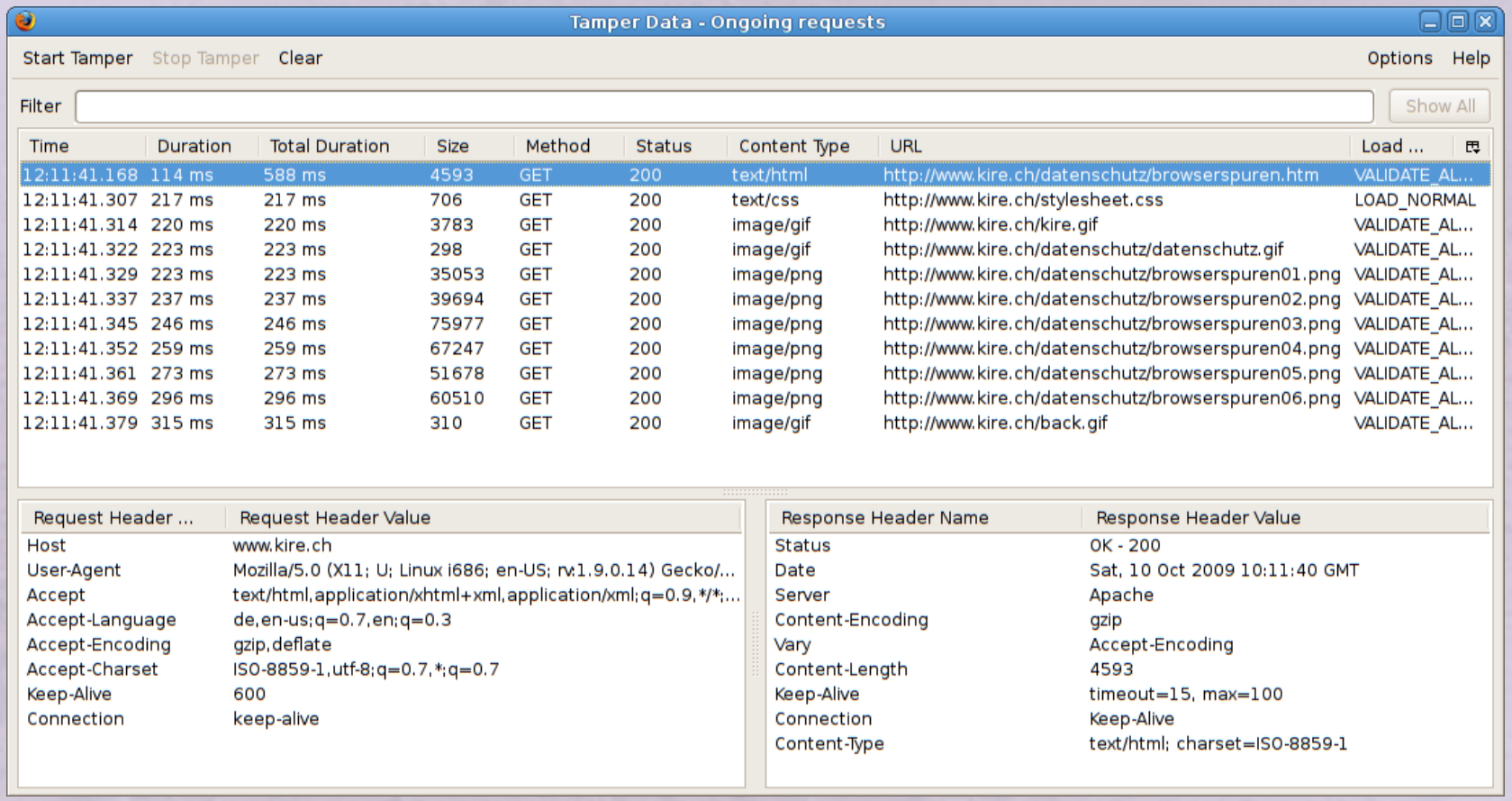
- Hypertext Transfer Protocol
  - Beispiel: HTML-Seite von Server anfordern

    GET /datenschutz/browserspuren.htm HTTP/1.1
    Host: www.kire.ch
  - Antwort vom Server

    HTTP/1.1 200 OK
    Date: Sat, 10 Oct 2009 09:53:55 GMT
    Server: Apache
    Transfer-Encoding: chunked
    Content-Type: text/html; charset=ISO-8859-1

    (und direkt angehängt der Inhalt des HTML-Dokuments)

- Mit Firefox-Erweiterung „Tamper Data“ mitgeschnitten



- Dabei übertragene HTML-Seite

Source of: http://www.kire.ch/datenschutz/browserspuren.htm - Mozilla Firefox

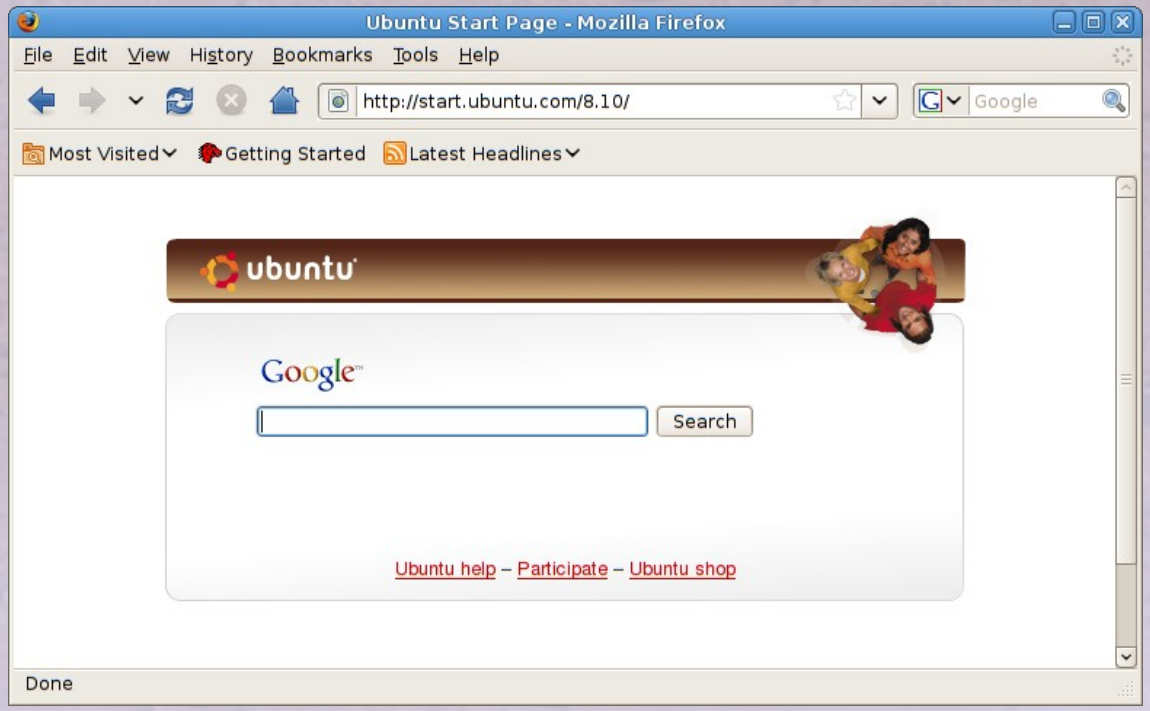
File Edit View Help

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">

<html>

<head>
<title>kire.ch - Datenschutz - Browser-Spuren</title>
<meta name="description" content="kire.ch: Datenschutz und Datensicherheit, Linux, Fotografie, Rollenspiel, Crossgolf">
<meta name="keywords" content="kire.ch, Datenschutz, Datensicherheit, Linux, Fotografie, Rollenspiel, Rollenspiele, Crossgolf,
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link rel="stylesheet" href="../stylesheet.css" type="text/css">
</head>


<body>

<table>

<tr>
<td valign=top rowspan=2>
<a href="../index.htm"><img src="../kire.gif" alt="kire.ch" hspace=20 vspace=15 border="0"></a>
</td>
<td>
<a href="index.htm"><img src="datenschutz.gif" alt="Datenschutz" vspace=15 border="0"></A>
</td>
<td width=50 rowspan=2></td>
</tr>

<tr>
<td>
<center><b>Browser-Spuren - die beim Surfen im Netz hinterlassen werden</b></center><p>
Beim Surfen im World Wide Web hinterlassen wir verschiedenste Spuren. Mit Hilfe von Cookies und anderen Identifikationsmerkmale
Zuerst wird bei einer Seitenanfrage eine weltweit eindeutige IP-Adresse &uuml;bertragen, welche es dem angefragten Server &uuml
Zus&auml;tzlich &uuml;bertr&auml;gt der Browser Informationen &uuml;ber sich selbst und zum verwendeten Betriebssystem. Mit auf
```

Line 69, Col 9

Mozilla Firefox - Hintergründe

- Basiert auf Gecko (ursprünglich von Netscape)
- Open Source Software
- Linux, Max OS X, Windows
- Inoffizielle Portierungen
  - für verschiedenste Plattformen



Mozilla Firefox - Wissenswertes & Grundeinstellungen

- Grundeinstellungen sind ziemlich gut
  - Security → Use a master password
- Wirklich mächtig wird der Browser durch
  - „Suchmaschinen“
  - Add-ons
    - Extensions, Themes, Languages, Plugins
- RSS Feed-Reader bereits integriert
  - Bessere gibt es als Extensions
- Ev. interessant
  - Bookmarks als HTML-Datei exportieren

Mozilla Firefox - Suchmaschinen

- Nicht nur Suchmaschinen im Sinne von Google
- Beziehen von mycroft.mozdev.org
  - eTools.ch (etools.ch)
    - In ~/.mozilla/firefox/*.default/searchplugins/etoolsch.xml unmittelbar an {searchTerms} anhängen:
      - &country=web&language=all
        - Für weltweite Suche als Standard
  - Wikipedia (de) - Artikel (wikipedia-de)
  - Deutscher Wortschatz (wortschatz)
  - LEO de<->en (leo_deen)
  - [map.search.ch] Schweiz (map_search_ch)

Mozilla Firefox - Erweiterungen

- German Dictionary (Switzerland)
- Tab Mix Plus
  - Für komfortable Tab-Steuerung
    - Enable built-in session restore and disable the Tab Mix Session Manager
    - Tab Opening & Tab Closing
      - Einstellungen nach Gusto vornehmen
- Adblock Plus
  - Werbeblocker

Sichere Verbindungen per HTTPS

- Public-Key-Infrastruktur nach X.509-Standard
  - Hierarchisches System von vertrauenswürdigen Zertifizierungsstellen
  - Server weist sich gegenüber dem Browser aus und ermöglicht Verschlüsselung
- Browserhersteller
  - prüft Zertifizierungsstelle (Hardware, Software, Abläufe)
  - und nimmt dessen Root-Zertifikat(e) in den Browser auf

Sichere Verbindungen per HTTPS

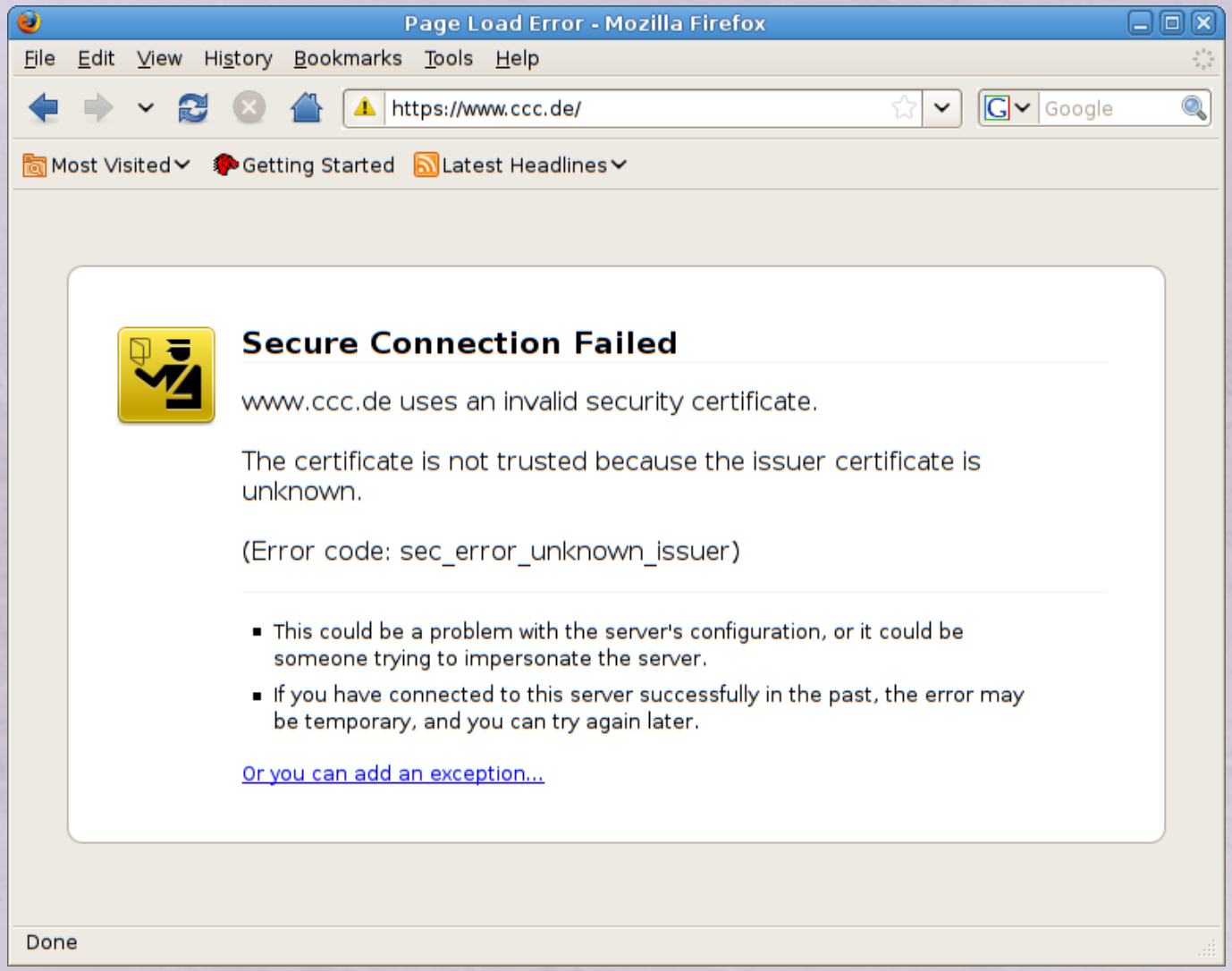
- Zertifizierungsstelle (Certification Authority CA)
  - prüft BesitzerIn einer Domäne
  - stellt Zertifikate für (i.d.R.) Hostnamen
  - und/oder Zwischenzertifizierungsstellen aus
    - welche ihrerseits wiederum Zertifikate ausstellen können
      - Baumhierarchie
  - und pflegt eine Sperrliste
- CAcert
  - Freie Zertifizierungsstelle für Gratis-Zertifikate
  - Identität wird von mindestens zwei voll beglaubigten Mitgliedern geprüft
  - Zertifizierung gegenüber Browserherstellern ist teuer und aufwändig
    - Root-Zertifikate müssen (noch) manuell importiert werden

Sichere Verbindungen per HTTPS

- Webbrowser
  - bezieht beim Verbindungsaufbau zum Server das Zertifikat
  - und prüft, ob
    - sich dieses auf durch eine vertrauenswürdige Zertifizierungsstelle ausgestelltes Zertifikat zurückführen lasst
    - der aufgerufene Hostnamen zum Zertifikat passt
    - das Gültigkeitsdatum nicht abgelaufen ist
    - das Zertifikat nicht gesperrt worden ist
  - Falls die Prüfung fehl schlägt, wird ein Fehler angezeigt
    - der übersteuert werden kann
  - Für bessere Kennzeichnung in Adresszeile
    - about:config → browser.identity.ssl_domain_display = 1

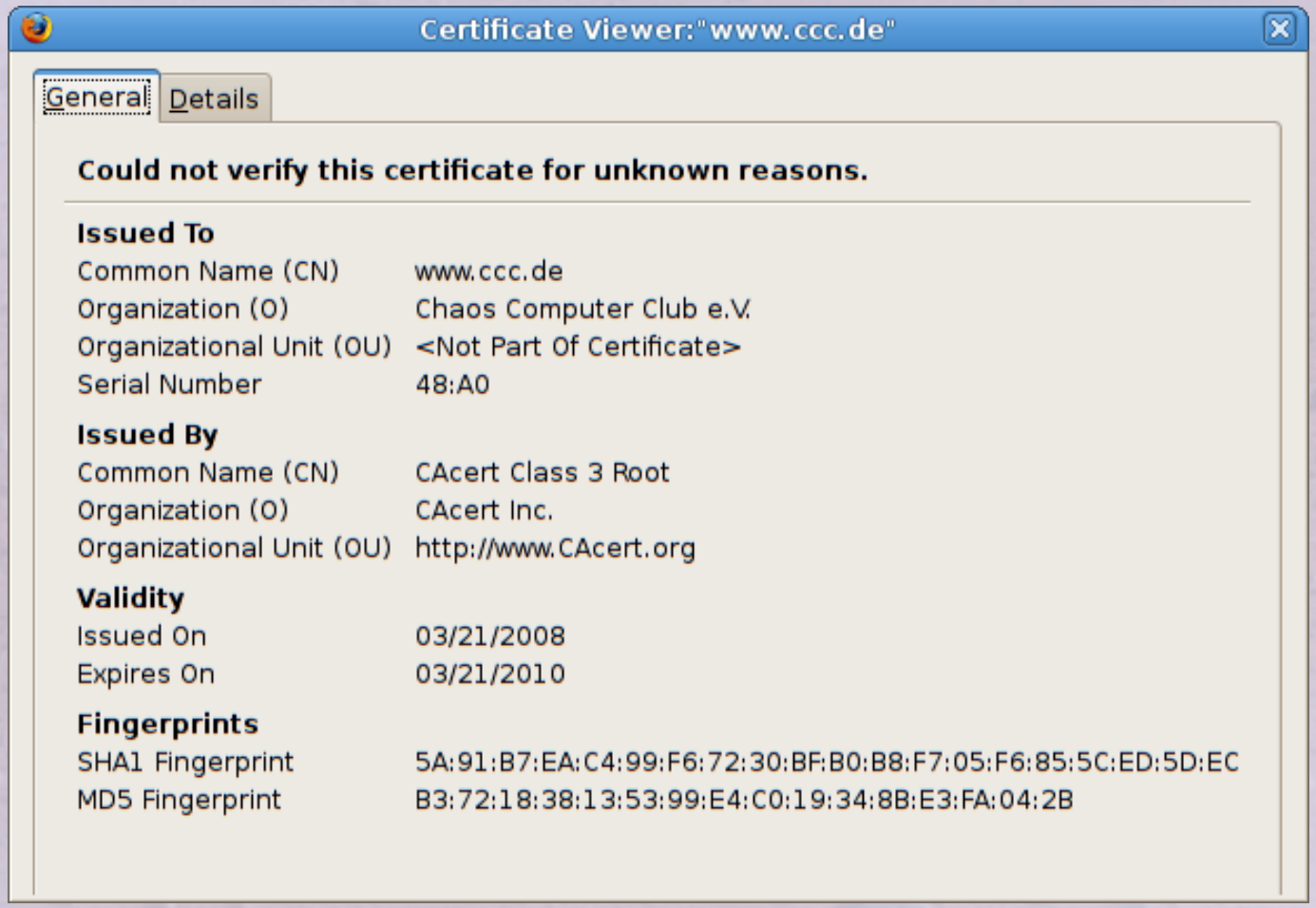
Sichere Verbindungen per HTTPS

- Aussteller-Zertifikat ist unbekannt



Sichere Verbindungen per HTTPS

- Aussteller ist CAcert



Sichere Verbindungen per HTTPS

- Diesem Server-Zertifikat könnte nun vertraut werden
  - Mit „Confirm Security Exception“
    - Besser nicht permanent

Sichere Verbindungen per HTTPS

- Noch besser, das Root-Zertifikat der CA importieren
  - Falls CA vertrauenswürdig
    - Und Root-Zertifikat (und/oder Fingerprint) von vertrauenswürdiger Stelle
      - https://...
  - Für CAcert
    - http://www.cacert.org/index.php?id=3
    - Klick auf Dateien im PEM-Format
      - „Trust this CA to identify web sites“ wählen
      - und vor dem Speichern Fingerprint prüfen
        - CAcert Class 1 PKI Key - SHA1: 13:5C:EC:36:F4:9C:B8:E9:3B:1A: B2:70:CD:80:88:46:76:CE:8F:33
        - CAcert Class 3 PKI Key - SHA1: DB:4C:42:69:07:3F:E9:C2:A3:7D: 89:0A:5C:1B:18:C4:18:4E:2A:2D

Sichere Verbindungen per HTTPS

- Sicherheit
  - HTTPS gilt als sicher
  - Standard-Zertifikate bestätigen, dass der Hostnamen unter der administrativen Kontrolle der beantragenden Person steht
    - Teilweise reicht Prüfung der E-Mail
      - an zu beglaubigende Domain
- Extended-Validation-SSL-Zertifikate
  - Identität der Besitzerin (Person, Unternehmung) einer Domäne wird von CA genau geprüft
  - Adresszeile verfärbt sich grün anstatt blau

Browser-Spuren - technisch & rechtlich

- Server-Logfiles
  - Webserver
    - IP-Adresse, Browser, Betriebssystem, Referrer, Datum
  - Mailserver
  - Nameserver (DNS)
- Aufbewahrungspflicht der IP-Zuordnungen
  - CH: 6 Monate durch Provider
  - EU: 6 - 24 Monate
- Eindeutige Merkmale
  - MAC-Adresse
  - "Einwahl"
  - Cookies & IDs
- lokaler Computer
  - Cache & Browser-History

Browser-Spuren - Browser-Einstellungen

- Cookies
  - Generell alle Cookies annehmen
  - und beim Schliessen des Browsers löschen
- Browserhistory nur einen Tag aufbewahren
  - und Eingaben sowie Downloads nicht merken
- Cache auf 0 MB stellen
- Super-Cookies
  - about:config → dom.storage.enabled = false
  - ~/.mozilla/firefox/*.default/webappsstore.sqlite löschen
- Genauere Beschreibung und Screenshots
  - http://www.kire.ch/datenschutz/browserspuren.htm

Browser-Spuren - Browser-Einstellungen

- Adobe Flash Player
  - http://www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager07.html
- ev. weitere Plugins
  - Google-Toolbar
  - allenfalls (Google) Search Suggestions
  - Adobe Reader
    - mit standardmässig aktiviertem JavaScript
  - RealPlayer

Browser-Spuren - Nützliche Add-ons für Firefox

- User Agent Switcher
  - Browserinformationen ändern
- RefControl
  - Referrer unterdrücken
  - Default-Einstellung auf "<Block> (3rd Party)" stellen
- QuickJava
  - Ein-/Ausschalter für Java & JavaScript
- Flashblock
  - Adobe Flash nicht automatisch ausführen

Browser-Spuren - Nützliche Add-ons für Firefox

- NoScript
  - Anstatt Flashblock und QuickJava
  - Einstellungen pro Site, permanent oder temporär
  - Viele Möglichkeiten und daher auch komplizierter
    - Whitelist ausser (about:*) löschen
    - Unter Plugins "Forbid <IFRAME>" auswählen
    - Unter Notifications ausschalten:
      - Show message about blocked scripts
      - Display the release notes on updates
  - Viele Sites benötigen JavaScript
    - Prüfung von Formulardaten
    - Web 2.0
- Test
  - http://centralops.net/asp/co/BrowserMirror.vbs.asp