

5. Darmstädter Informationsrechtstag

Google Software (Chrome und Android)

Harald Baier

10.07.2009



h_da

HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

fbi

FACHBEREICH INFORMATIK



CASED

Wo kommt es zu einer für den User
nicht-offensichtlichen Kommunikation
zwischen dem Chrome-Browser und
Google bzw. einem anderen Internet-Dienst?

Agenda

- Grundsätzliches zu Chrome
- Funktionen von Chrome (in Version 2.0.172.33)
 - Autovervollständigung von URLs
 - User-ID: Eindeutige Anwendungsnummer für Chrome
 - Sicherheitsfeatures: Safe-Browsing
 - Vorzeitige Auflösung von Links: DNS Prefetching
- Strategie von Google

Agenda

- Grundsätzliches zu Chrome
- Funktionen von Chrome (in Version 2.0.172.33)
 - Autovervollständigung von URLs
 - User-ID: Eindeutige Anwendungsnummer für Chrome
 - Sicherheitsfeatures: Safe-Browsing
 - Vorzeitige Auflösung von Links: DNS Prefetching
- Strategie von Google

Der Browsermarkt in Deutschland

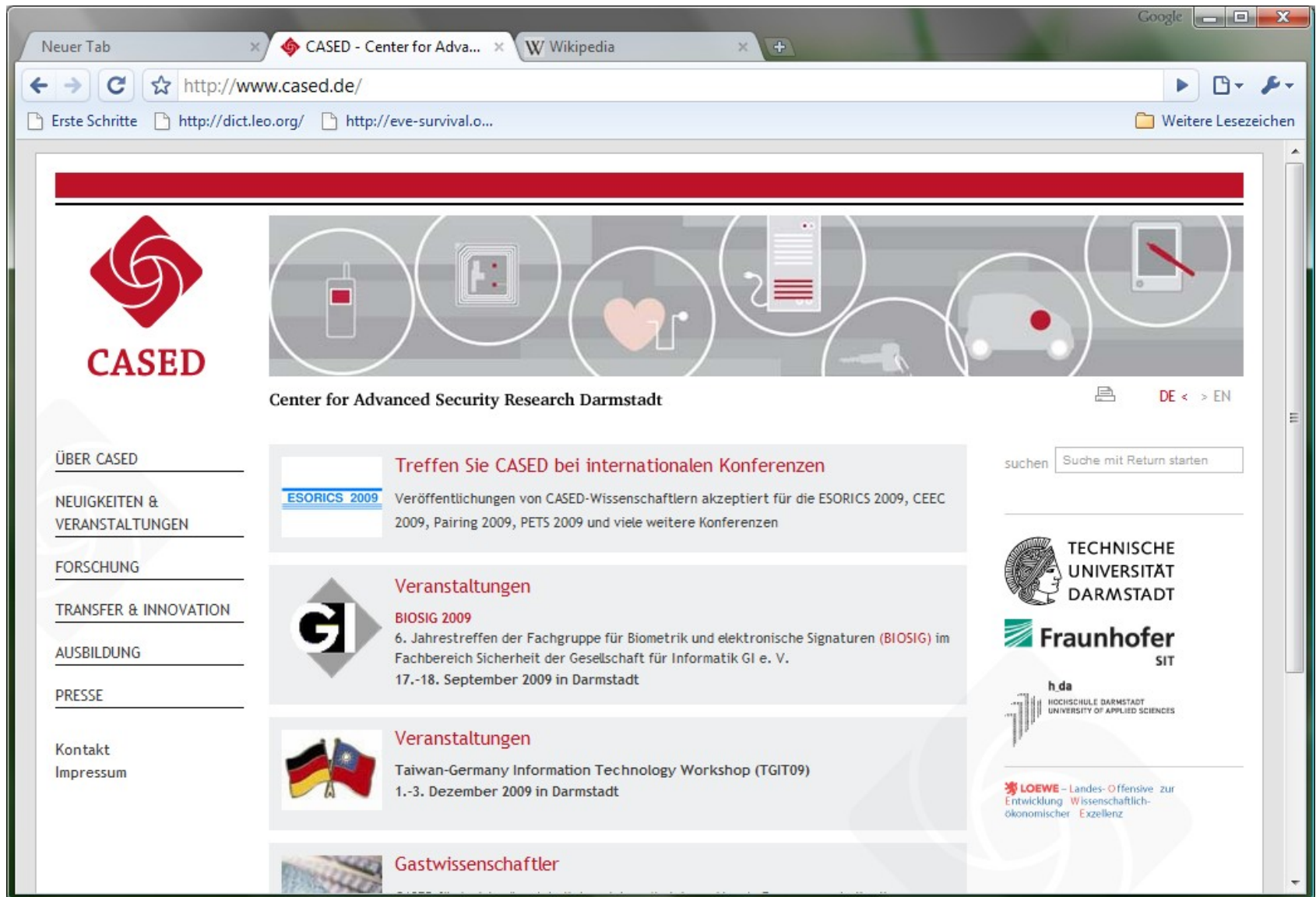
- Noch ein Browser ...

	www.browser-statistik.de 2009-06-29	www.heise.de Mai 2009
Firefox	51.1%	65.8%
Internet Explorer	37.2%	18.9%
Safari	4.6%	4.7%
Opera	3.6%	7.3%
Chrome	1.6%	0.9%

Ziele von Chrome laut Google

- Quelle: Google-Webfilm zu Chrome
- Zentrale Ziele:
 - Weg bereiten für bessere Webanwendungen
 - Usability:
 - ♦ Oberfläche: Einfach und übersichtlich
 - ♦ Vorbild: Design von www.google.de
 - Sicherer Browser:
 - ♦ Open-Source
 - ♦ Eigene System-Prozesse für jedes Browserfenster (Tab)

Aussehen



Position des BSI

- Positionspapier vom 2009-09-09
- Hauptkritik:
 - Vorab-Version von Chrome veröffentlicht
 - Obsolet seit 2009-12-11 mit Chrome-Version 1.0
- Positiv:
 - Förderung des Wettbewerbs bei IT-Sicherheitsprodukten wie Browsern
 - Eigener Prozess pro Webseite (Tabs unabhängig)
 - Open-Source: Jeder kann Quellcode prüfen



Agenda

- Grundsätzliches zu Chrome
- Funktionen von Chrome (in Version 2.0.172.33)
 - Autovervollständigung von URLs
 - User-ID: Eindeutige Anwendungsnummer für Chrome
 - Sicherheitsfeatures: Safe-Browsing
 - Vorzeitige Auflösung von Links: DNS Prefetching
- Strategie von Google

Autovervollständigung der URL

- Aktuelle Eingabe: 'c' für cased.de



Autovervollständigung der URL

- Ziel: Vorschläge für vollständige URL an Anwender
- Bei jedem Tastendruck:
 - Übermittlung einer Vervollständigungs-Anfrage an Google
 - Google-Cookie wird von Chrome an Google mitgesendet
- Antwort von Google:
 - Vorschläge für Vervollständigung
- **Ohne (offensichtliche) Willensbekundung** werden Daten vom Browser zum Server übermittelt.

User-ID

- Version 1.x:
 - Bei Installation vergeben
 - Wesentliche Kritik:
 - Verknüpfung mit personalisiertem Google-Account (z.B. GMail) liefert tatsächliche Anwenderdaten
 - Verknüpfung mit Cookies dessen Aktivitäten
- Version 2.x (ab 2009-05-22)
 - User-ID wird nur erzeugt, falls Option zum Übertragen von Nutzungsstatistiken und Ausfallberichten an Google aktiviert ist
 - Standardeinstellung: Deaktiviert
- Anscheinend hat Google auf Kritik reagiert

User-ID: Datenschutz

The screenshot shows a Google Chrome browser window with the address bar displaying <http://www.google.com/chrome/intl/de/privacy.html?hl=de>. The page title is "Google Chrome - Anmerkung zum Datenschutz". The content is in German and discusses data protection policies for Google Chrome. It mentions that personal information is handled when using Google products and services, and that Google Chrome provides information about its data protection measures. It also states that Google Chrome sends information to Google when used, including IP addresses and cookies. The page includes a list of links on the left side: "Download", "Funktionen", "Warum wir einen Browser konzipiert haben", "Webentwickler", "Datenschutzbestimmungen", and "Open source". The main content area has a heading "Google Chrome - Anmerkung zum Datenschutz" followed by the date "February 18, 2009". The text explains that Google Chrome sends information to Google when used, including IP addresses and cookies. It also mentions that Google Chrome sends information to Google when used, including IP addresses and cookies. The page includes a list of links on the left side: "Download", "Funktionen", "Warum wir einen Browser konzipiert haben", "Webentwickler", "Datenschutzbestimmungen", and "Open source".

Google Chrome - Anmerkung zum Datenschutz

February 18, 2009

In den [Datenschutzbestimmungen von Google](#) wird beschrieben, wie persönliche Informationen behandelt werden, wenn Sie Produkte und Dienste von Google verwenden. Dazu zählen auch bei der Verwendung von Google Chrome bereitgestellte Informationen. Zudem werden im Folgenden unsere spezifischen Datenschutzmaßnahmen für Google Chrome erläutert. Google benachrichtigt Sie über alle erheblichen Änderungen an diesen Bestimmungen und Sie haben immer die Möglichkeit, das Senden von persönlichen Informationen an Google durch entsprechende Browsereinstellungen zu verhindern oder die Verwendung einzustellen.

Bei der Verwendung von Google Chrome an Google gesendete Informationen

Zum Verwenden und Herunterladen von Google Chrome müssen keine persönlichen Informationen angegeben werden. Falls Sie Google Chrome herunterladen oder zum Herstellen einer Verbindung mit den Servern von Google verwenden, empfängt Google nur [standardmäßige Protokollinformationen](#) wie die IP-Adresse Ihres Computers und einige [Cookies](#). Sie können Google Chrome wie [hier](#) erläutert so konfigurieren, dass keine Cookies an Google oder andere Websites gesendet werden.

Darüber hinaus werden von einigen Funktionen von Google Chrome in begrenztem Umfang weitere Informationen an Google gesendet:

- In die Adressleiste eingegebene URLs oder Suchanfragen werden an Google gesendet, damit von der Vorschlagsfunktion automatisch gesuchte Begriffe oder URLs empfohlen werden können. Falls Sie Nutzerstatistiken an Google senden möchten und Sie eine vorgeschlagene Suchanfrage oder URL akzeptieren, sendet Google Chrome diese Information ebenfalls an Google. Sie können diese Funktion wie [hier](#) erläutert deaktivieren.
- Von Ihnen aufgerufene nicht vorhandene URLs werden unter Umständen an Google gesendet, damit wir Ihnen bei der Suche nach der gewünschten URL helfen können. Sie können diese Funktion wie [hier](#) erläutert deaktivieren.
- Die Funktion "Sicheres Durchsuchen" stellt regelmäßig eine Verbindung zu den Servern von Google her, um die aktuellste Liste bekannter Phishing- und Malware-Websites herunterzuladen. Zusätzlich wird, wenn Sie eine Website besuchen, die eine Phishing- oder Malware-Website sein könnte, von Ihrem Browser eine verschlüsselte Kopie eines Teils der URL dieser Website an Google gesendet, sodass wir weitere Informationen über diese potenziell gefährliche URL bereitstellen können. Google kann die tatsächliche URL, die Sie aufrufen, anhand dieser Informationen nicht ermitteln. Weitere Informationen erhalten Sie [hier](#).
- [Ihr Google Chrome-Browser enthält mindestens eine eindeutige Anwendungsnummer](#). Diese Nummern und Informationen zur Installation des Browsers (z. B. Versionsnummer, Sprache) werden bei der erstmaligen Installation und Verwendung der Anwendung und bei der automatischen Update-Prüfung von Google Chrome an Google gesendet. Falls Sie [Nutzungsstatistiken und Ausfallberichte](#) an Google senden, werden uns diese Informationen sowie eine eindeutige Anwendungsnummer vom Browser übermittelt. Ausfallberichte enthalten Informationen aus Dateien, Anwendungen und Diensten, die zum Zeitpunkt eines Problems ausgeführt wurden. Mithilfe von Ausfallberichten können Browserprobleme diagnostiziert und behoben werden.
- Sie können Google mithilfe von Google Chrome als Suchmaschine festlegen und Sie können mit Google Chrome auch auf andere

Sicherheitsfeatures: Safe-Browsing-Funktion

- User wird gewarnt, wenn er 'unsichere' Seite besuchen will:
 - Malware-Schutz
 - Phishing-Schutz
- Vorgehen:
 - Eingeegebene URL mit hinterlegter Vergleichsliste abgeglichen
 - Liste wird regelmäßig von Google heruntergeladen
 - URLs in Vergleichsliste liegen nur als 'Teilwerte' vor
 - Bei Übereinstimmung der 'Teilwerte' wird 'Gesamt-URL-Wert' bei Google online abgefragt
- Interaktion Browser-Google bei verdächtigem 'Teilwert'

DNS Prefetching

- DNS = Domain Name System
 - Zuordnung 'Domain Name' - IP-Adresse
 - Beispiel: www.cased.de - 146.140.212.153
 - Analogie: Telefonauskunft (Auflösung Name - Telefonnummer)
- DNS Prefetching:
 - Chrome lädt gewünschte Webseite (z.B. www.cased.de)
 - Chrome fragt für **alle darin enthaltenen** Links per DNS die IP-Adresse ab
- User erwartet typischerweise nicht, dass Browser im Vorgriff alle Links verarbeitet

Agenda

- Grundsätzliches zu Chrome
- Funktionen von Chrome (in Version 2.0.172.33)
 - Autovervollständigung von URLs
 - User-ID: Eindeutige Anwendungsnummer für Chrome
 - Sicherheitsfeatures: Safe-Browsing
 - Vorzeitige Auflösung von Links: DNS Prefetching
- Strategie von Google

Strategie von Google ?

- Vermutung:
 - User soll nur noch Google-Applikationen einsetzen
 - Cloud Computing
 - Google = Microsoft 2.0 ?
- (Einige) Bausteine:
 - Suchmaschine im WWW
 - Mail-Account und Web-Browser
 - Google-Earth und Google-Map
 - Chrome-Betriebssystem für Netbooks
 - Android-Betriebssystem für mobile Geräte

Vielen Dank für Ihre Aufmerksamkeit !!

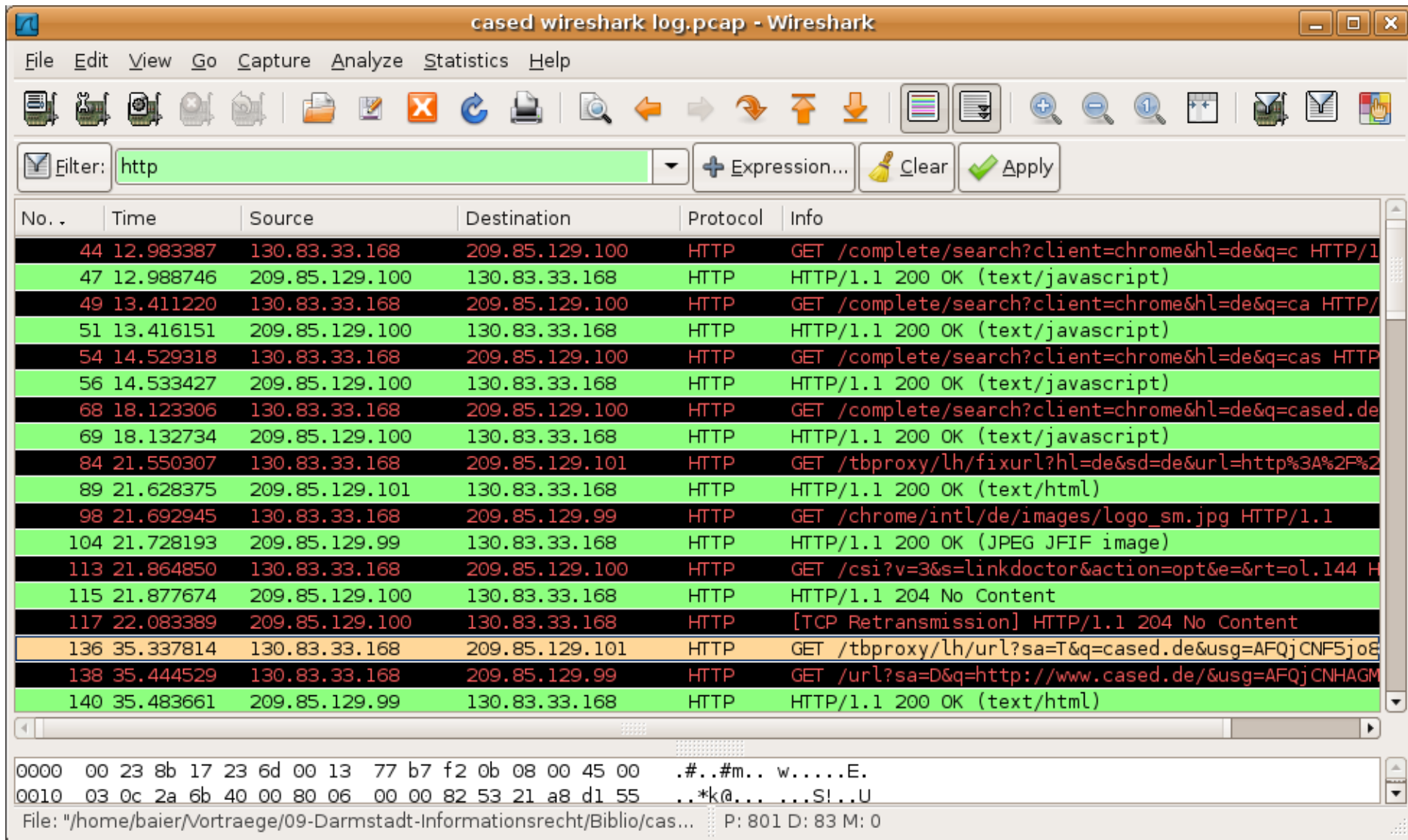
Fragen ?



Kontakt: Harald Baier

E-Mail: h.baier@fbi.h-da.de oder
baier@cased.de

Autovervollständigung: Netzwerkverkehr

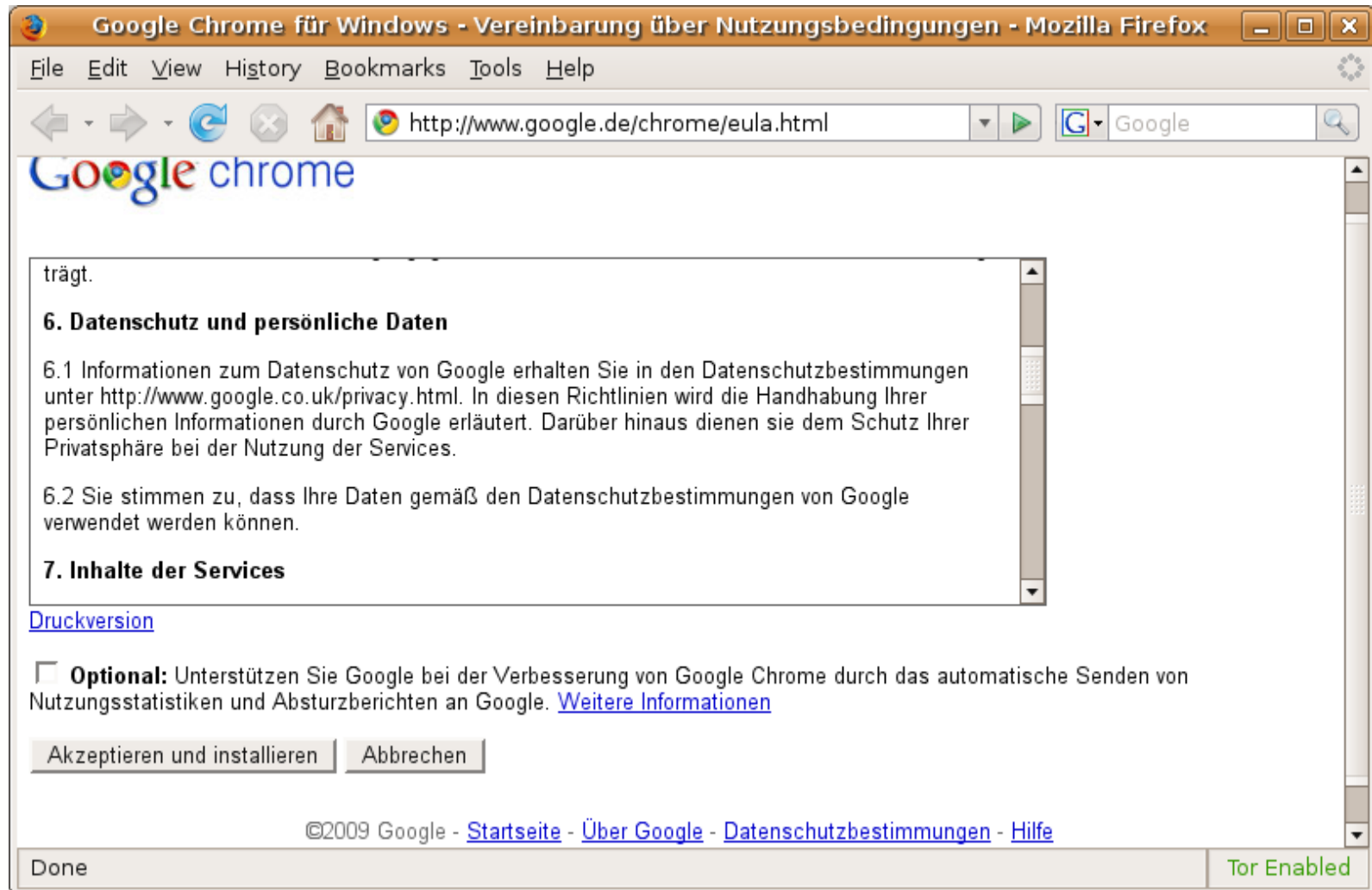


The image shows a Wireshark window titled "cased wireshark log.pcap - Wireshark". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Help), a toolbar with various icons, and a filter bar set to "http". The main display area shows a list of network packets with columns for No., Time, Source, Destination, Protocol, and Info. The packets are filtered to show only HTTP traffic. The bottom status bar displays the current file path and packet statistics.

No.	Time	Source	Destination	Protocol	Info
44	12.983387	130.83.33.168	209.85.129.100	HTTP	GET /complete/search?client=chrome&hl=de&q=c HTTP/1
47	12.988746	209.85.129.100	130.83.33.168	HTTP	HTTP/1.1 200 OK (text/javascript)
49	13.411220	130.83.33.168	209.85.129.100	HTTP	GET /complete/search?client=chrome&hl=de&q=ca HTTP/
51	13.416151	209.85.129.100	130.83.33.168	HTTP	HTTP/1.1 200 OK (text/javascript)
54	14.529318	130.83.33.168	209.85.129.100	HTTP	GET /complete/search?client=chrome&hl=de&q=cas HTTP
56	14.533427	209.85.129.100	130.83.33.168	HTTP	HTTP/1.1 200 OK (text/javascript)
68	18.123306	130.83.33.168	209.85.129.100	HTTP	GET /complete/search?client=chrome&hl=de&q=cased.de
69	18.132734	209.85.129.100	130.83.33.168	HTTP	HTTP/1.1 200 OK (text/javascript)
84	21.550307	130.83.33.168	209.85.129.101	HTTP	GET /tbproxy/lh/fixurl?hl=de&sd=de&url=http%3A%2F%2
89	21.628375	209.85.129.101	130.83.33.168	HTTP	HTTP/1.1 200 OK (text/html)
98	21.692945	130.83.33.168	209.85.129.99	HTTP	GET /chrome/intl/de/images/logo_sm.jpg HTTP/1.1
104	21.728193	209.85.129.99	130.83.33.168	HTTP	HTTP/1.1 200 OK (JPEG JFIF image)
113	21.864850	130.83.33.168	209.85.129.100	HTTP	GET /csi?v=3&s=linkdoctor&action=opt&e=&rt=ol.144 H
115	21.877674	209.85.129.100	130.83.33.168	HTTP	HTTP/1.1 204 No Content
117	22.083389	209.85.129.100	130.83.33.168	HTTP	[TCP Retransmission] HTTP/1.1 204 No Content
136	35.337814	130.83.33.168	209.85.129.101	HTTP	GET /tbproxy/lh/url?sa=T&q=cased.de&usg=AFQjCNF5joE
138	35.444529	130.83.33.168	209.85.129.99	HTTP	GET /url?sa=D&q=http://www.cased.de/&usg=AFQjCNHAGM
140	35.483661	209.85.129.99	130.83.33.168	HTTP	HTTP/1.1 200 OK (text/html)

0000 00 23 8b 17 23 6d 00 13 77 b7 f2 0b 08 00 45 00 .#..#m.. w.....E.
0010 03 0c 2a 6b 40 00 80 06 00 00 82 53 21 a8 d1 55 ..*k@... ..S!...U
File: "/home/baier/Vortraege/09-Darmstadt-Informationsrecht/Biblio/cas... P: 801 D: 83 M: 0

User-ID: Nutzungsbedingungen



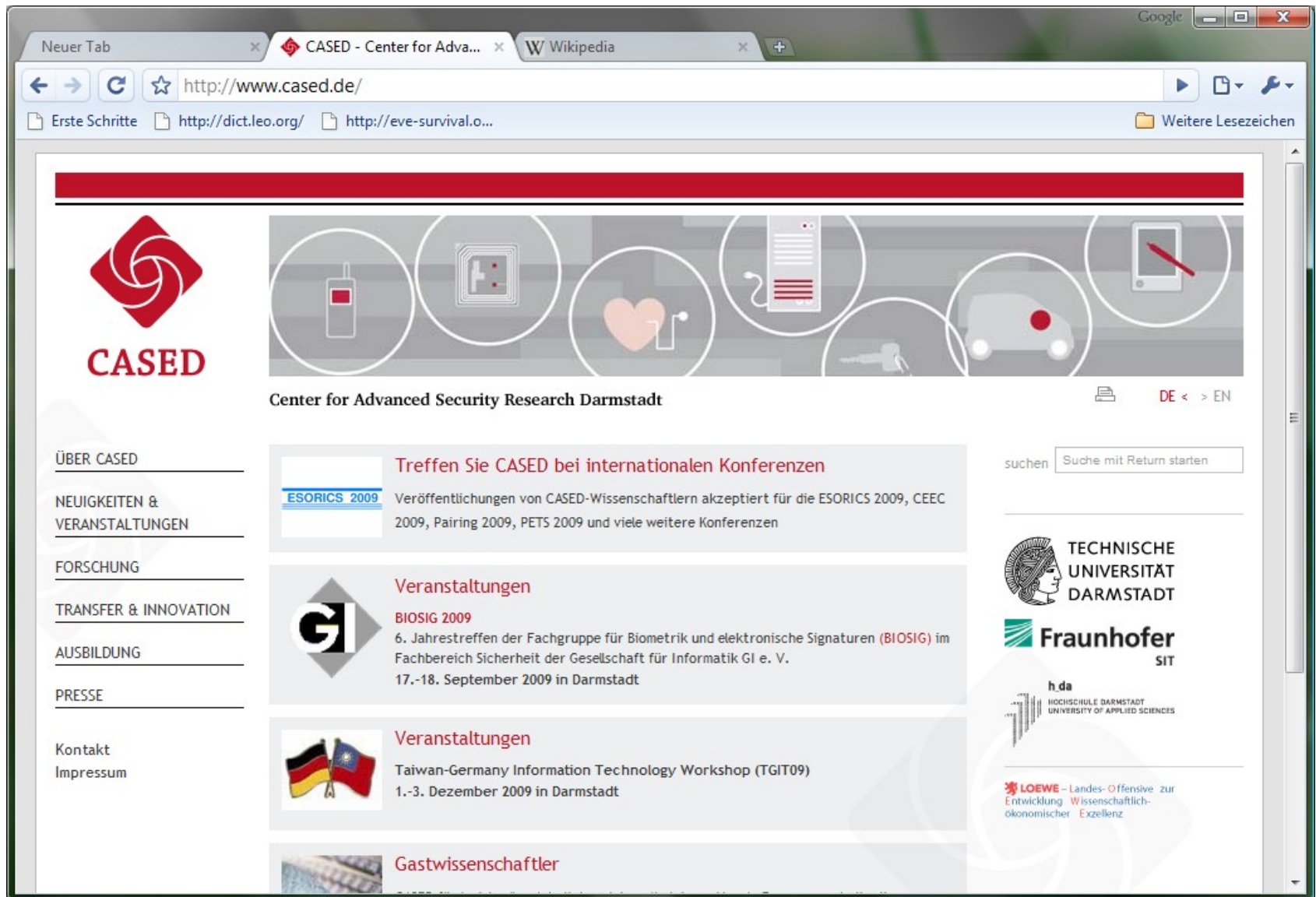
Safe-Browsing-Abfrage

The image shows a Wireshark packet capture window titled "(Untitled) - Wireshark". The filter is set to "http". The packet list shows a series of HTTP requests and responses. The selected packet is packet 21, which is a GET request to `/safebrowsing/rd/goog-malware-shavar_s_12341-12360.12341-12360.:` from 10.0.0.244 to 74.125.104.91. The packet details pane shows the following information:

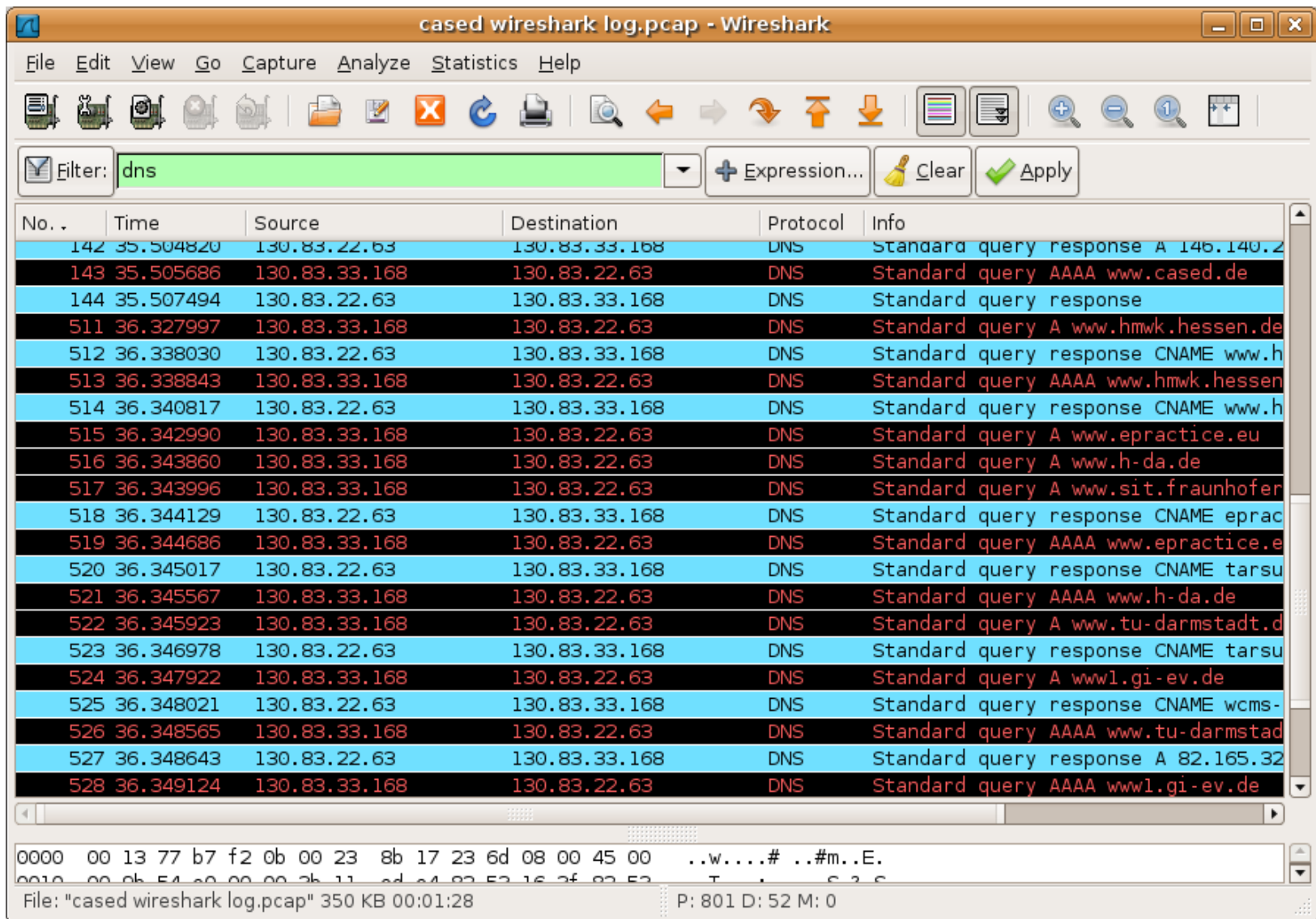
- Frame 21 (551 bytes on wire, 551 bytes captured)
- Ethernet II, Src: IntelCor_72:6f:b0 (00:21:6b:72:6f:b0), Dst: Tecom_5a:e4:e3 (00:03:c9:5a:e4:e3)
- Internet Protocol, Src: 10.0.0.244 (10.0.0.244), Dst: 74.125.104.91 (74.125.104.91)
- Transmission Control Protocol, Src Port: 49169 (49169), Dst Port: http (80), Seq: 1, Ack: 1, Len: 497
- Hypertext Transfer Protocol
 - GET /safebrowsing/rd/goog-malware-shavar_s_12341-12360.12341-12360.: HTTP/1.1\r\n
 - [Expert Info (Chat/Sequence): GET /safebrowsing/rd/goog-malware-shavar_s_12341-12360.12341-12360.: HTTP/1.1\r\n]
 - Request Method: GET
 - Request URI: /safebrowsing/rd/goog-malware-shavar_s_12341-12360.12341-12360.:
 - Request Version: HTTP/1.1
 - Host: safebrowsing-cache.google.com\r\n
 - Connection: keep-alive\r\n
 - User-Agent: Mozilla/5.0 (Windows; U; windows NT 6.0; en-US) AppleWebKit/530.5 (KHTML, like Gecko) Chrome/2.0.172.33 Safari/530.5\r\n
 - Accept-Encoding: gzip,deflate,bzip2,sdch\r\n

The packet bytes pane shows the raw data of the request, including the headers and the body.

DNS Prefetching: Beispiel



DNS Prefetching: Abfragen für www.cased.de



The image shows a Wireshark capture of DNS traffic. The filter is set to 'dns'. The packet list shows a series of DNS queries and responses. The packet details pane shows the structure of a DNS packet, including the header and the question section.

No.	Time	Source	Destination	Protocol	Info
142	35.504820	130.83.22.63	130.83.33.168	DNS	Standard query response A 146.140.2
143	35.505686	130.83.33.168	130.83.22.63	DNS	Standard query AAAA www.cased.de
144	35.507494	130.83.22.63	130.83.33.168	DNS	Standard query response
511	36.327997	130.83.33.168	130.83.22.63	DNS	Standard query A www.hmwk.hessen.de
512	36.338030	130.83.22.63	130.83.33.168	DNS	Standard query response CNAME www.h
513	36.338843	130.83.33.168	130.83.22.63	DNS	Standard query AAAA www.hmwk.hessen
514	36.340817	130.83.22.63	130.83.33.168	DNS	Standard query response CNAME www.h
515	36.342990	130.83.33.168	130.83.22.63	DNS	Standard query A www.epractice.eu
516	36.343860	130.83.33.168	130.83.22.63	DNS	Standard query A www.h-da.de
517	36.343996	130.83.33.168	130.83.22.63	DNS	Standard query A www.sit.fraunhofer
518	36.344129	130.83.22.63	130.83.33.168	DNS	Standard query response CNAME eprac
519	36.344686	130.83.33.168	130.83.22.63	DNS	Standard query AAAA www.epractice.e
520	36.345017	130.83.22.63	130.83.33.168	DNS	Standard query response CNAME tarsu
521	36.345567	130.83.33.168	130.83.22.63	DNS	Standard query AAAA www.h-da.de
522	36.345923	130.83.33.168	130.83.22.63	DNS	Standard query A www.tu-darmstadt.d
523	36.346978	130.83.22.63	130.83.33.168	DNS	Standard query response CNAME tarsu
524	36.347922	130.83.33.168	130.83.22.63	DNS	Standard query A www1.gi-ev.de
525	36.348021	130.83.22.63	130.83.33.168	DNS	Standard query response CNAME wcms-
526	36.348565	130.83.33.168	130.83.22.63	DNS	Standard query AAAA www.tu-darmstad
527	36.348643	130.83.22.63	130.83.33.168	DNS	Standard query response A 82.165.32
528	36.349124	130.83.33.168	130.83.22.63	DNS	Standard query AAAA www1.gi-ev.de

0000 00 13 77 b7 f2 0b 00 23 8b 17 23 6d 08 00 45 00 ..w....#...#m...E.
0010 00 0b 54 c0 00 00 2b 11 ed c4 82 53 16 2f 82 53 T...C...
File: "cased wireshark log.pcap" 350 KB 00:01:28 P: 801 D: 52 M: 0

Linux-Webseite von Google Chrome



Google Chrome - Laden Sie einen neuen Browser herunter - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.google.de/chrome

Google chrome

Select a language

Google Chrome: Ein neuer Webbrowser für Windows

Google Chrome ist ein Browser, der einfache Gestaltung mit fortschrittlicher Technologie kombiniert, um die Nutzung des Internets zu beschleunigen, zu vereinfachen und sicherer zu gestalten.

Weitere Informationen

Weitere Informationen zu Open Source-Entwicklungsprojekten. (Nur in englischer Sprache verfügbar.)

Für Windows Vista/Windows XP SP2

Ausführen einer Suche aus der Adressleiste heraus

Bei Eingabe von Text in die Adressleiste erhalten Sie Vorschläge zu Such- und Webseiten.

Miniaturansichten Ihrer am häufigsten besuchten Websites

Rufen Sie Ihre Lieblingsseiten von jedem neuen Tab aus blitzschnell auf.

Privates Surfen

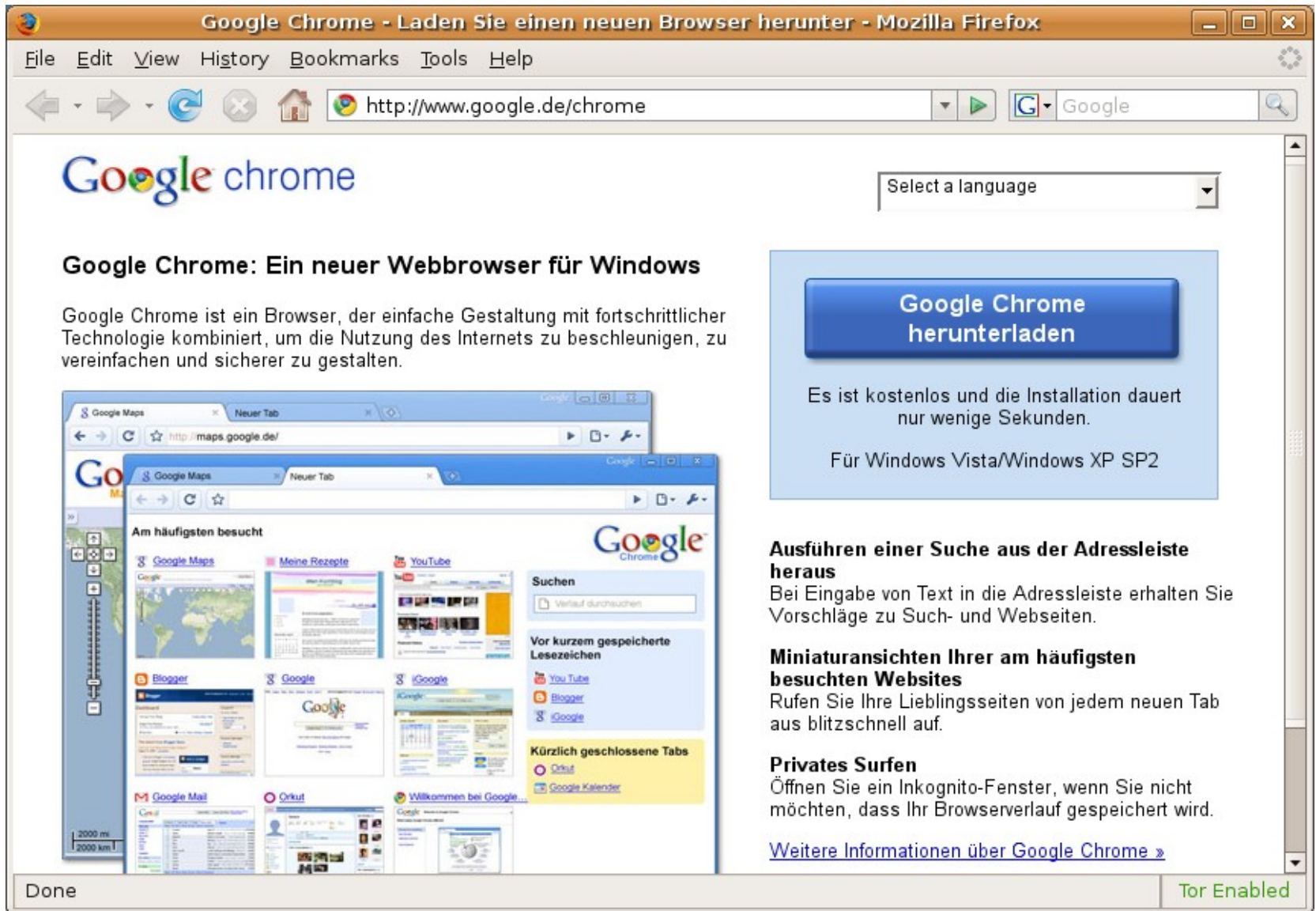
Öffnen Sie ein Inkognito-Fenster, wenn Sie nicht möchten, dass Ihr Browserverlauf gespeichert wird.

[Weitere Informationen über Google Chrome »](#)

Done

Tor Disabled

Windows-Webseite von Google Chrome



Google Chrome - Laden Sie einen neuen Browser herunter - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.google.de/chrome

Google chrome

Select a language

Google Chrome: Ein neuer Webbrowser für Windows

Google Chrome ist ein Browser, der einfache Gestaltung mit fortschrittlicher Technologie kombiniert, um die Nutzung des Internets zu beschleunigen, zu vereinfachen und sicherer zu gestalten.

Google Chrome herunterladen

Es ist kostenlos und die Installation dauert nur wenige Sekunden.

Für Windows Vista/Windows XP SP2

Ausführen einer Suche aus der Adressleiste heraus
Bei Eingabe von Text in die Adressleiste erhalten Sie Vorschläge zu Such- und Webseiten.

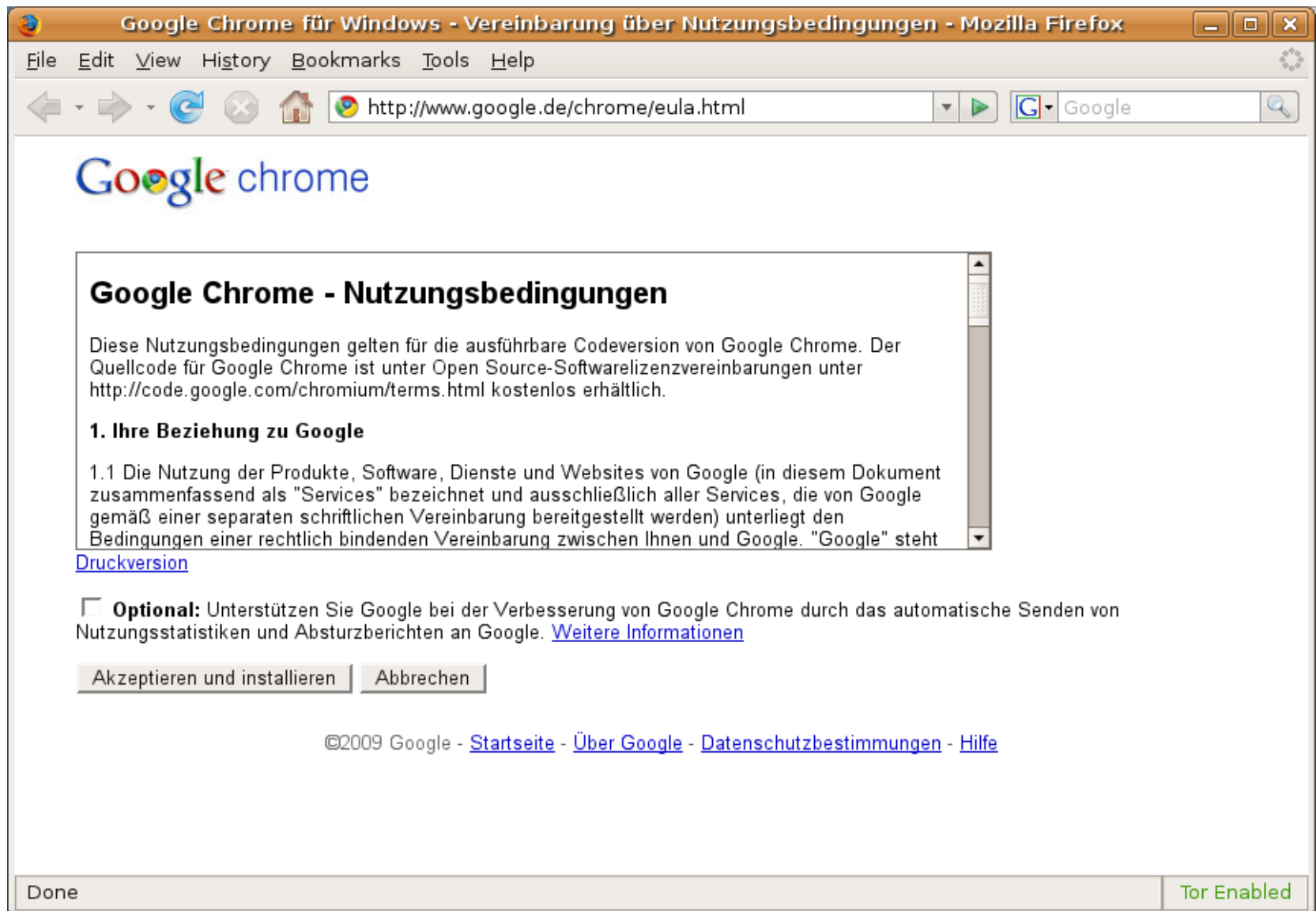
Miniaturansichten Ihrer am häufigsten besuchten Websites
Rufen Sie Ihre Lieblingsseiten von jedem neuen Tab aus blitzschnell auf.

Privates Surfen
Öffnen Sie ein Inkognito-Fenster, wenn Sie nicht möchten, dass Ihr Browserverlauf gespeichert wird.

[Weitere Informationen über Google Chrome »](#)

Done Tor Enabled

Windows-Webseite von Google Chrome (2)



Linux-Webseite von Google Chrome (2)

