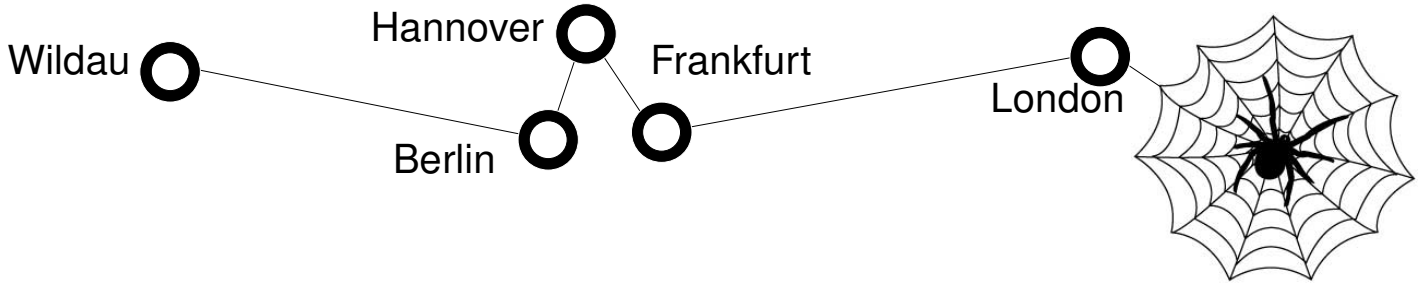
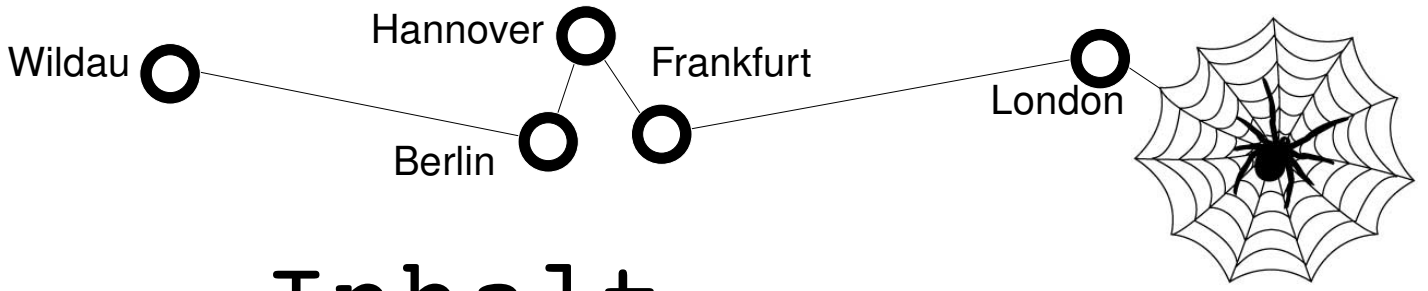


Spuren im Netz

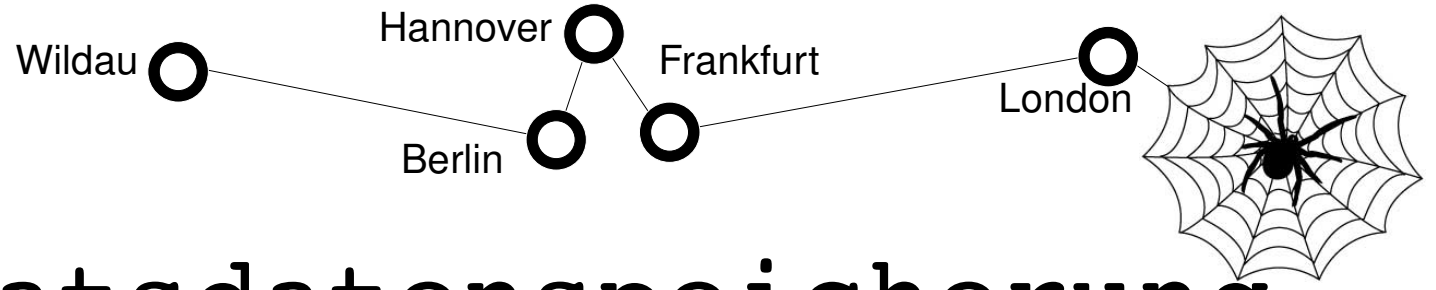
ein Arbeit von

Stefan Dassow



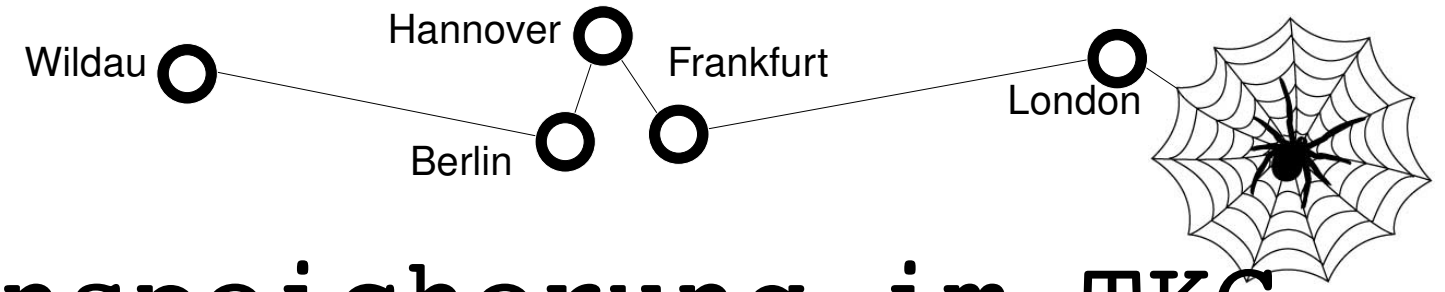
Inhalt

- Gesetzliche Daten-speicherungsregeln
- Datentypen
- Daten einer HTTP-Anfrage
- Daten erzeugt von Dienstleistern
- Cookies als Datenspeicher
- Sessionverfolgung
- Web-Bugs / Banner
- E-mails und News
- IRC & Instant Messenger
- Global Unique Identifier
- Öffentliche Verzeichnisse
- Portscan
- Fazit



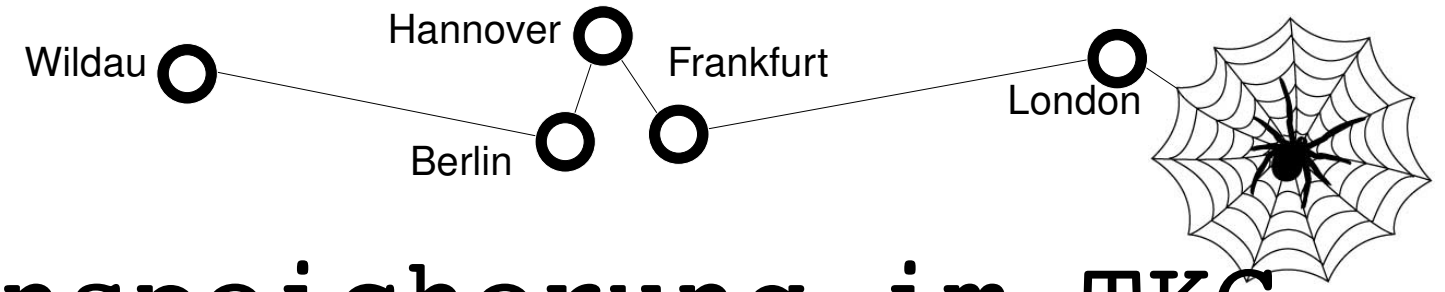
Vorratsdatenspeicherung

- Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Maßnahmen
- Beschluss nach namentlicher Abstimmung durch den deutschen Bundestag am 9.11.2007
- Neuerungen STPO:
  - Standortermittlungen von Mobilfunkendgeräten



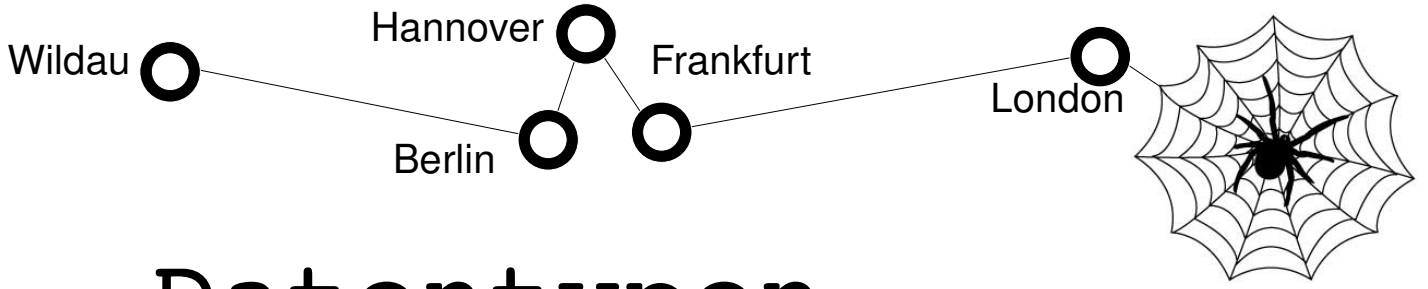
Datenspeicherung im TKG

- Neuerungen TKG:
  - Speichern der Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,
  - Beginn und Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone,



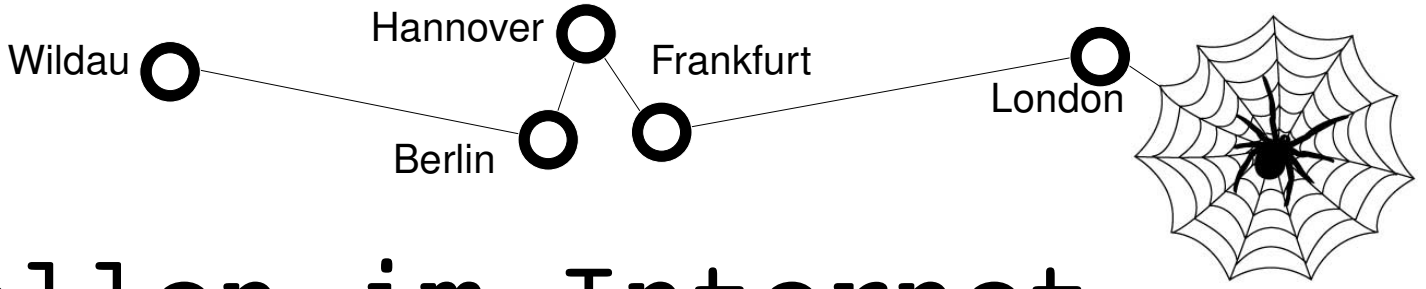
Datenspeicherung im TKG

- in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst,
- Bezeichnung der genutzten Funkzelle (Mobil),
- bei anonymen Diensten die Aktivierungsdaten,
- IP-Adressen bei VoIP,
- bei elektronischer Post der gesamte Weg und das an jeder Stelle (auch IP bei Abruf),
- bei Veränderung von Verkehrsdaten sind die Veränderungen lückenlos zu dokumentieren

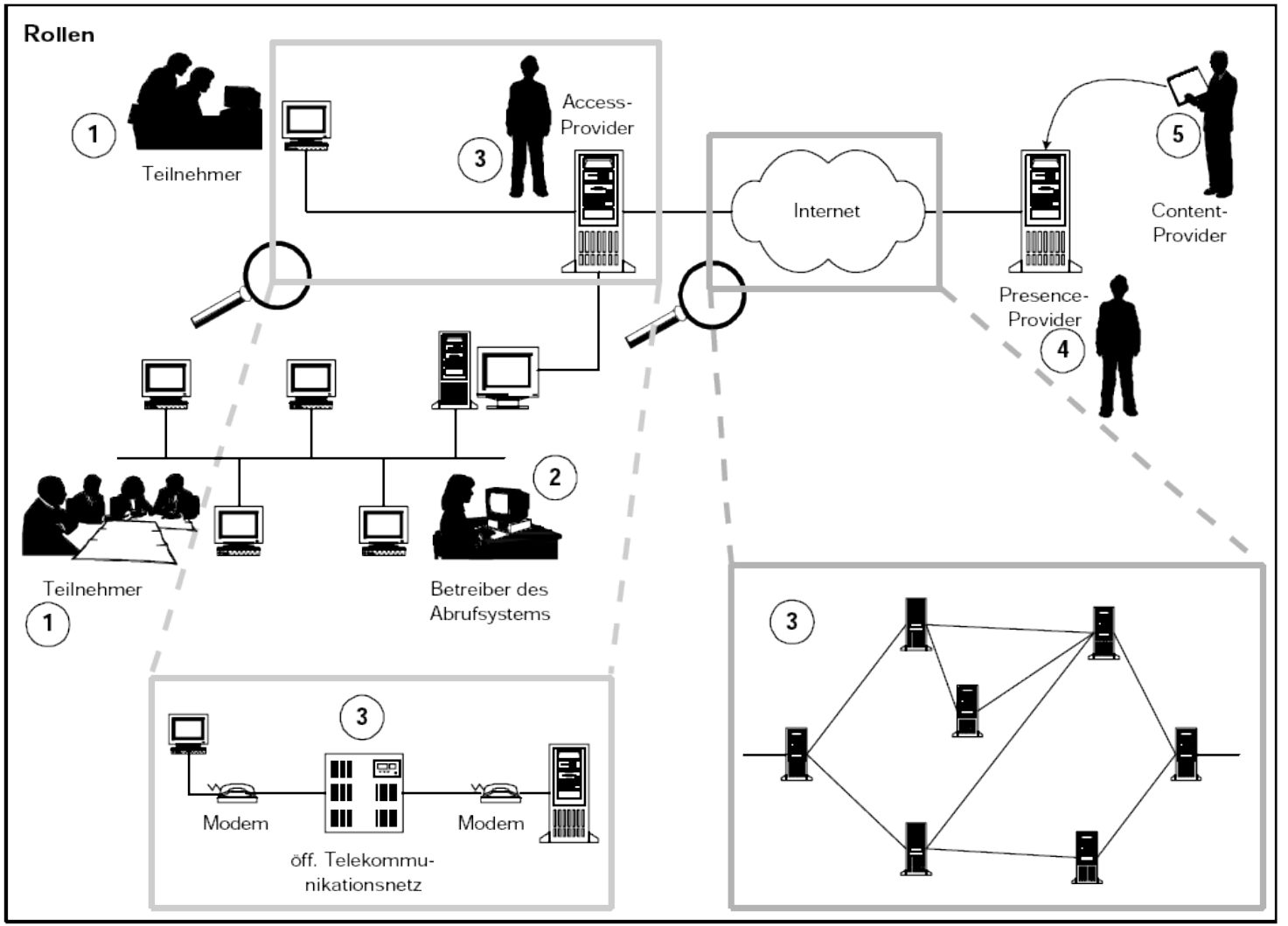


Datentypen

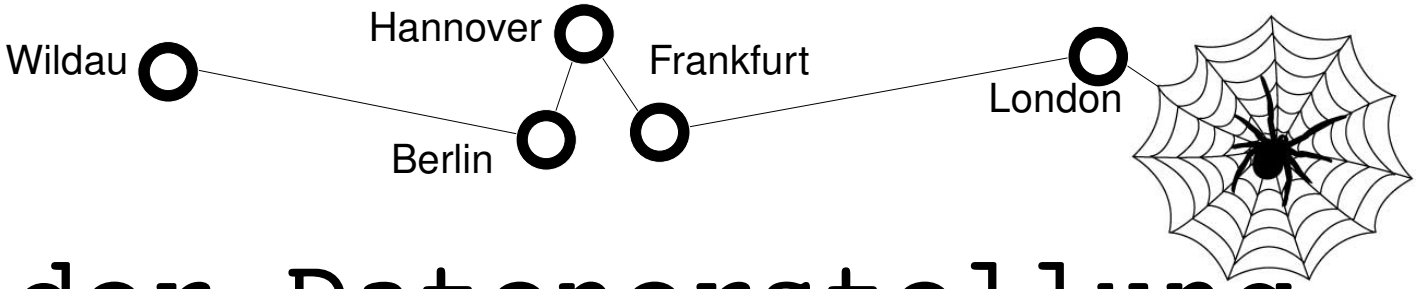
- Bestandsdaten
- Verbindungsdaten
- Inhaltsdaten



Rollen im Internet

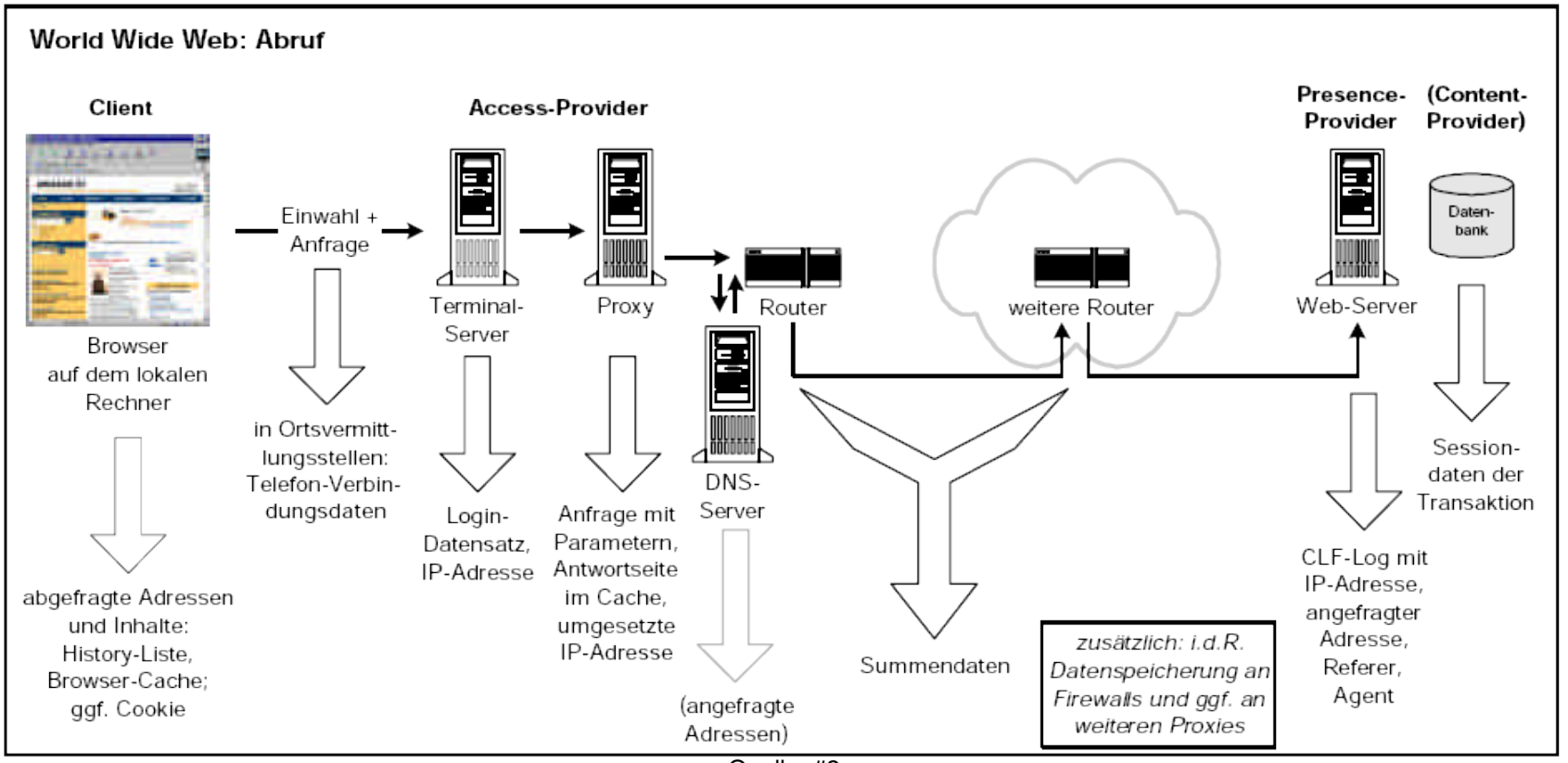


Quelle: #2

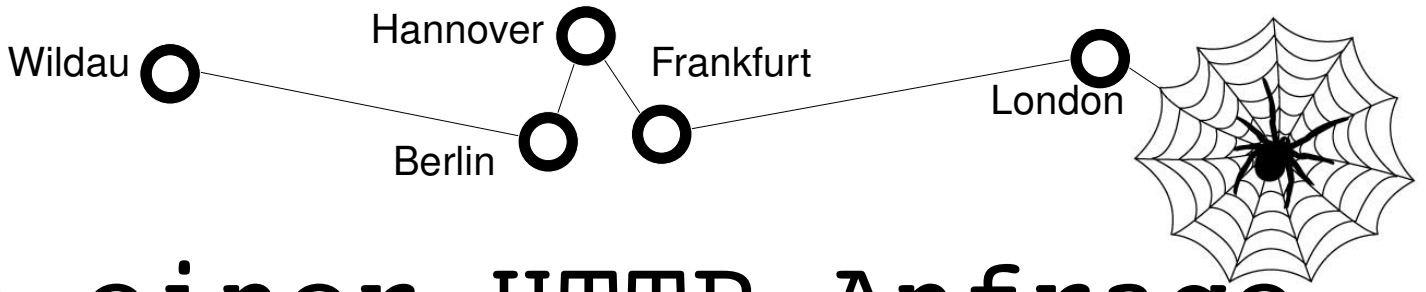


Orte der Datenerstellung

- Daten werden an den unterschiedlichsten Orten erhoben



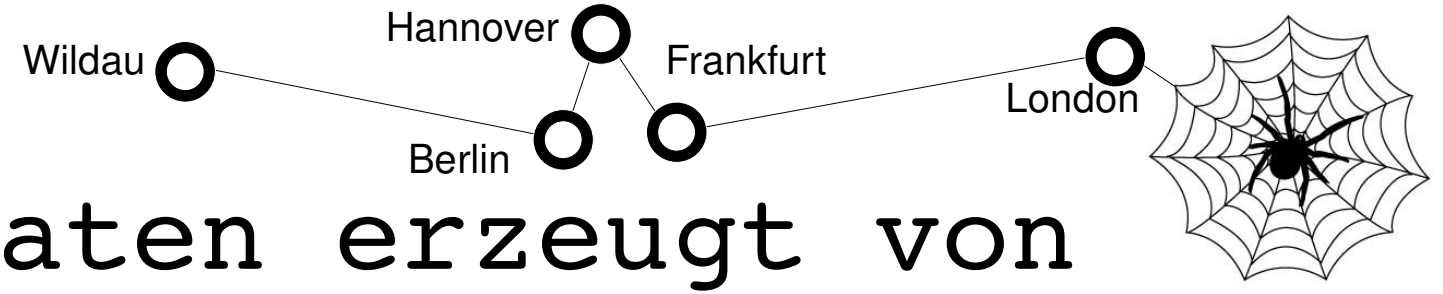
Quelle: #2



Daten einer HTTP-Anfrage

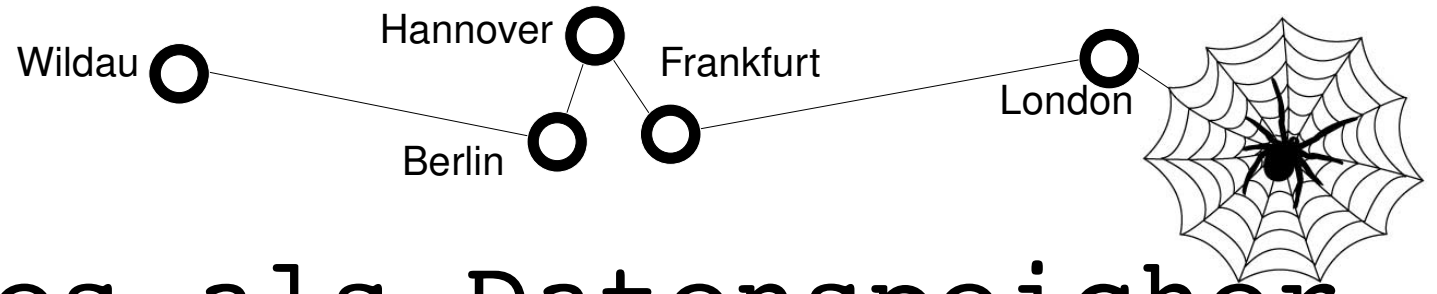
- 89.50.34.79 - - [25/Nov/2007:16:43:40 +0100] "GET /tasklist.php HTTP/1.1" 401 5915 "-" "Opera/9.20 (X11; Linux i686; U; de)"
- 89.50.34.79 - **Administrator** [25/Nov/2007:16:43:48 +0100] "GET /tasklist.php HTTP/1.1" 200 11924 "-" "Opera/9.20 (X11; Linux i686; U; de)"
- 89.50.34.79 - Administrator [25/Nov/2007:16:48:01 +0100] "GET /liga.php**?game=119&task=change&logger=d785f384f6dc086b3a79a708fc26446c&season=21** HTTP/1.1" 200 11930 "-" "Opera/9.20 (X11; Linux i686; U; de)"
- 192.166.53.200 - - [25/Nov/2007:10:16:54 +0100] "GET /index.php?page=3 HTTP/1.1" 200 11240 "**http://www.google.de/search?hl=de&sa=X&oi=spell&resnum=1&ct=result&cd=1&q=H%C3%BCrdenCup+2007&spell=1**" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)"

Quelle: #6



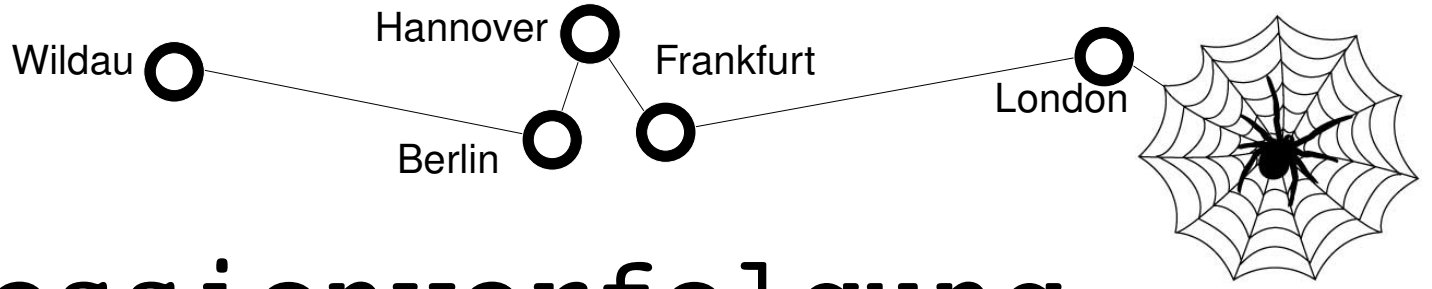
Daten erzeugt von Dienstleistern

- mehrere Möglichkeiten der Speicherung von Nutzerdaten möglich:
  - Cookies
  - Verfolgung mittels serverseitigen Sessions
  - Web-Bugs / Banner



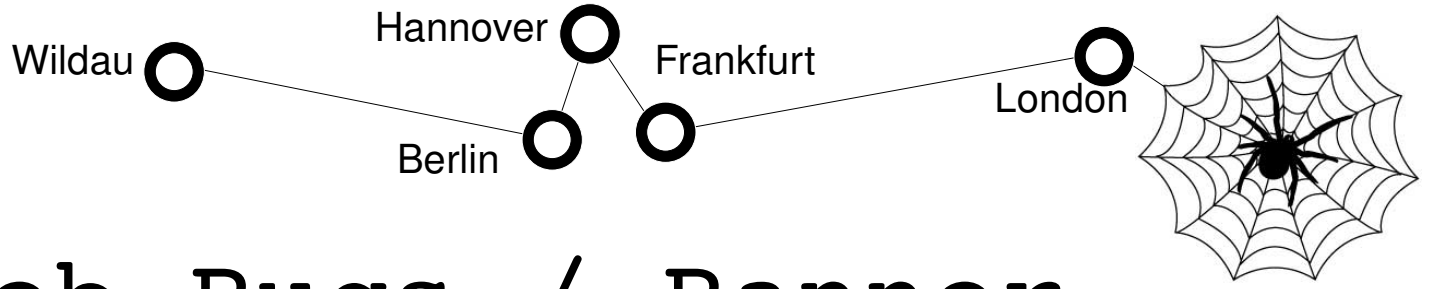
Cookies als Datenspeicher

- Maximalgröße: 4KB
- ein Cookie pro URL
- Mehrere Attribute; wichtigste sind „Name“, „Wert“ und „Ablaufdatum“
- Beispiel Google:
  - PREF=ID=28face613556316eTM=1184620070LM=1184620070S=DkEaab7_F7PtM3ZX (Quelle: #5)
- Neu: DOM-Storage Cookies



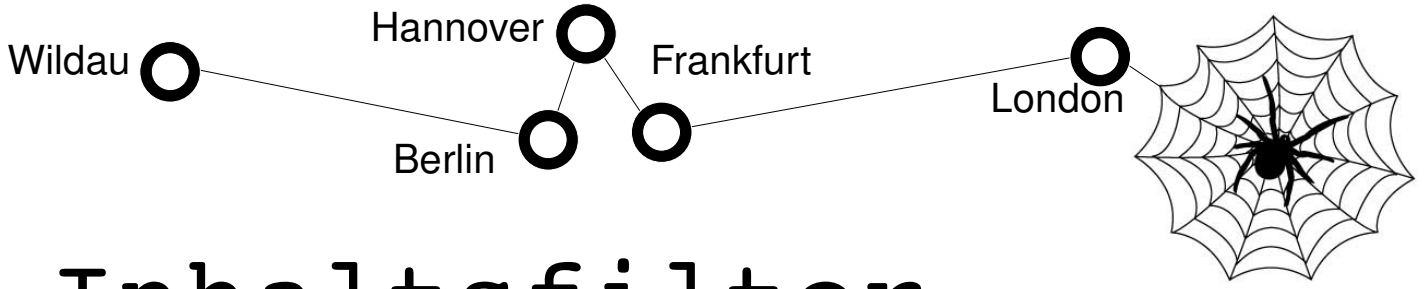
Sessionverfolgung

- Session-ID's dienen der Identifizierung, meist als Ersatz, wenn Cookies abgelehnt werden
- ID's können mit temporären Cookies verglichen werden
- Standardvariablennamen sind bekannt, daher einfacher Identitätsdiebstahl durch „man-in-the-middle“ möglich



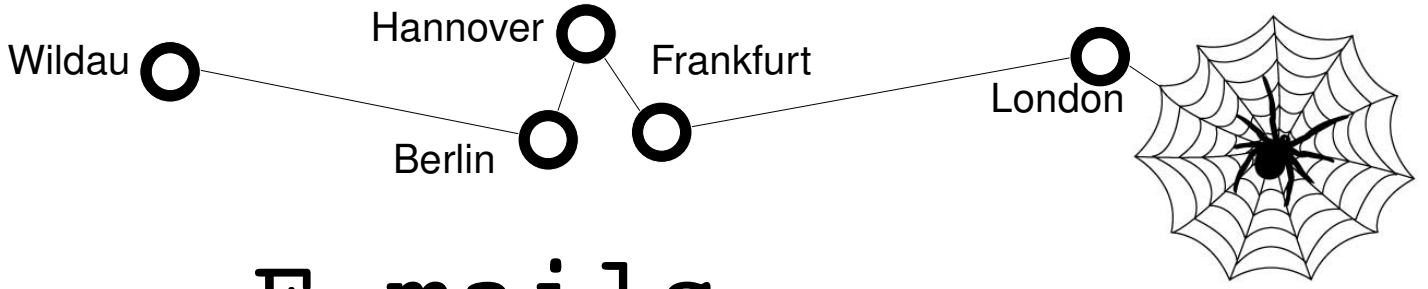
Web-Bugs / Banner

- Web-Bugs sind Bilder der Größe 1x1 Pixel mit transparentem Hintergrund
- Auch in HTML E-mails werden Web-Bugs verwendet
- Bilder können genauso wie HTML-Seiten Cookies setzen



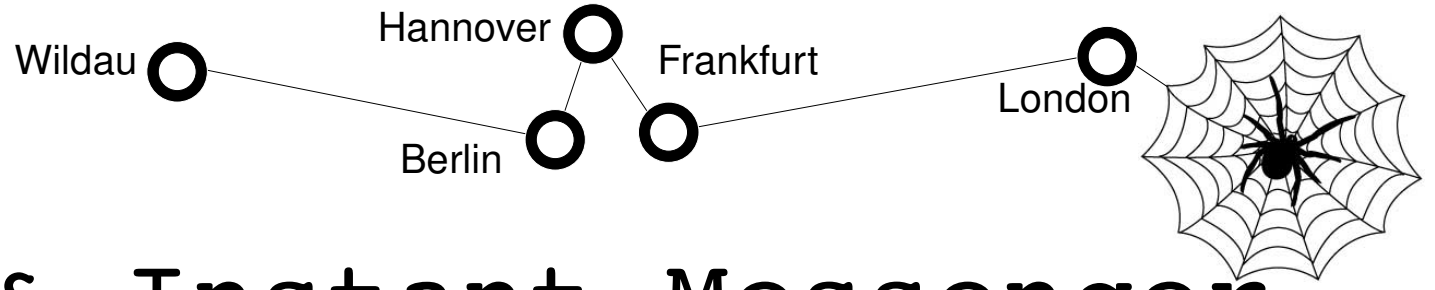
Inhaltsfilter

- Moderne Browser unterstützen die Filterung von Inhalten für den Jugendschutz
- Für Filterung müssen die URL's an einen zentralen Server zur Überprüfung gesendet werden



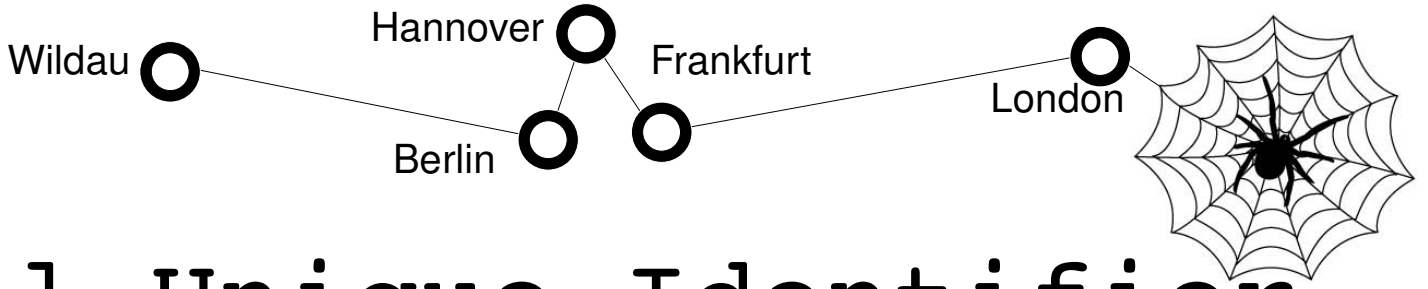
E-mails

- Innerhalb von E-mails werden Zusatzinformationen zum Absender und den E-mail Weg übertragen
- Verwendung von PK-Infrastrukturen lassen Rückschlüsse auf mögliche Kommunikationspartner zu
- E-mail Adressen werden weiterhin in Mailinglists öffentlich bekannt gemacht
- Die Notwendigkeit für Foreneinträge die E-mail Adresse anzugeben führen häufig auch zu einer Veröffentlichung



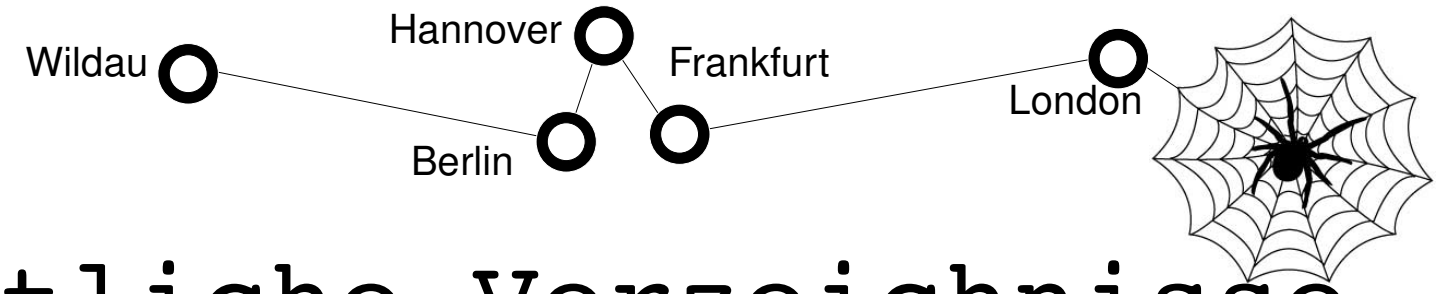
IRC & Instant Messenger

- Über whois-Anfragen sind im IRC IP und Nutzername einsehbar
- Bei einer Verbindung über einen Server sind für den Betreiber die Nachrichten i.A. sichtbar und können je nach Dienst auch mitgeloggt und ausgewertet werden



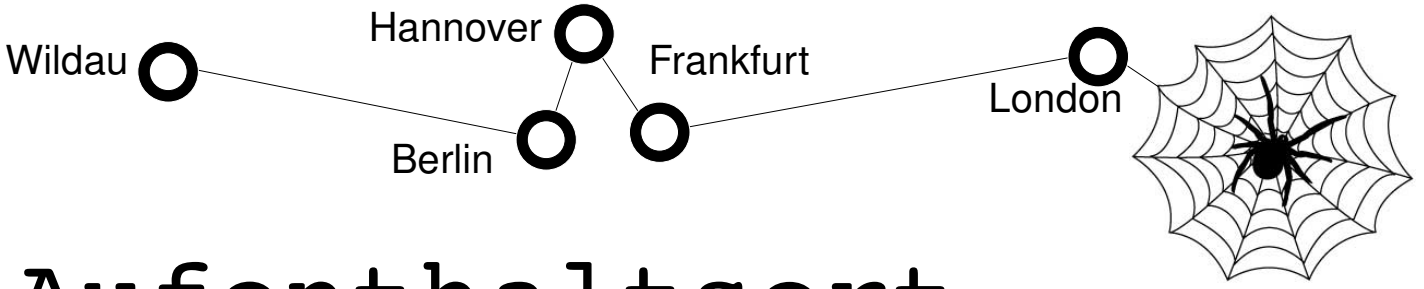
Global Unique Identifier

- Software versucht über GUID Nutzer eindeutig zu identifizieren
- Beispiel:
  - Pentium III enthielt Seriennummer, die über Software auslesbar war



Öffentliche Verzeichnisse

- www.meineip.de Lässt Rückschlüsse auf den Aufenthaltsort zu
- In den whois-Datenbanken der NIC's finden sich die Besitzerdaten von den einzelnen Websites
- Auf Public-Key-Servern finden sich Unmengen von E-mail Adressen stellenweise mit Zuordnung zur Identität
- www.yasni.de sammelt Informationen von Personen über die Indexierung von Websiten

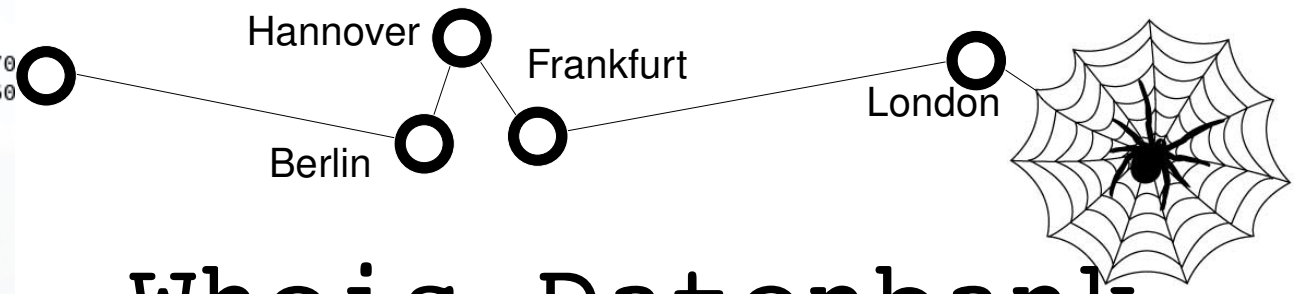


Aufenthaltsort

Details zu Deiner IP Adresse und zu Deinem System

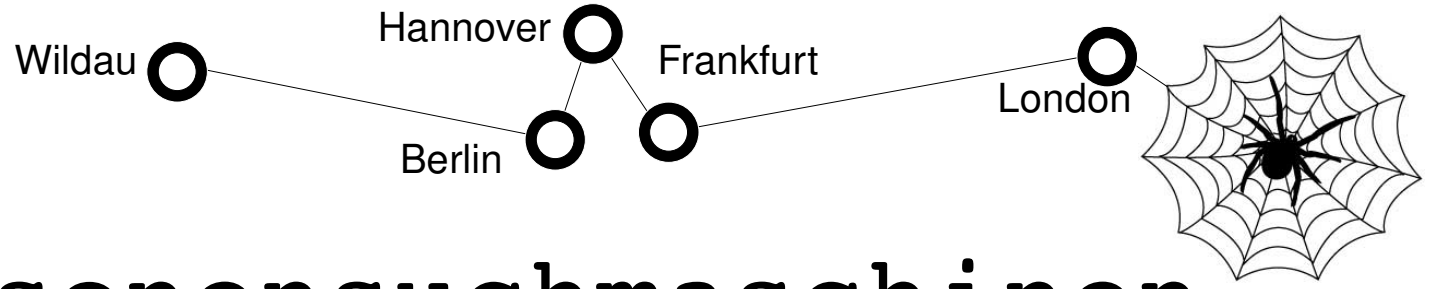
Das ist Deine IP-Adresse	89.50.34.68
Dein Rechnername ist	N2244.n.pppool.de
Du surfst mit diesem Browser	Opera - 9.2
Du hast dieses Betriebssystem	Linux
Dein DSL Anschluss kommt von	freenet Cityline GmbH
Proxy eingeschaltet?	Nein
Dein Netzknoten befindet sich in	Stadt: 16515 Oranienburg Region: Brandenburg Land: Deutschland

```
Domain:      tfh-wildau.de
Domain-Ace:  tfh-wildau.de
Nserver:     fresie.hrz.tfh-wildau.de 193.175.213.170
Nserver:     krokus.hrz.tfh-wildau.de 193.175.213.160
Nserver:     deneb.dfn.de
Status:      connect
Changed:     2007-11-08T11:55:08+01:00

[Holder]
Type:         ORG
Name:         Technische Fachhochschule Wildau
Address:      Friedrich-Engels-Str. 63
Pcode:        15745
City:         Wildau
Country:      DE
Changed:      2006-06-14T23:51:08+02:00

[Admin-C]
Type:         PERSON
Name:         Bernd Heimer
Address:      Technische Fachhochschule Wildau
Address:      Hochschulrechenzentrum
Address:      Bahnhofstr. 1
Pcode:        15745
City:         Wildau
Country:      DE
Changed:      2007-11-08T11:55:16+01:00

[Tech-C]
Type:         PERSON
Name:         Bernd Heimer
Address:      Technische Fachhochschule Wildau
Address:      Hochschulrechenzentrum
Address:      Bahnhofstr. 1
Pcode:        15745
City:         Wildau
Country:      DE
Phone:        +49 3375 508 992
Fax:          +49 3375 508 993
Email:        heimer@hrz.tfh-wildau.de
Changed:      2007-11-08T11:55:16+01:00

[Zone-C]
Type:         PERSON
Name:         Bernd Heimer
Address:      Technische Fachhochschule Wildau
Address:      Hochschulrechenzentrum
Address:      Bahnhofstr. 1
Pcode:        15745
City:         Wildau
Country:      DE
Phone:        +49 3375 508 992
Fax:          +49 3375 508 993
Email:        heimer@hrz.tfh-wildau.de
Changed:      2007-11-08T11:55:16+01:00
```



Whois-Datenbank

- whois-Eintrag enthält:
  - Inhaber
  - Adresse des Name-Server
  - Administrator
  - Technischer Ansprechpartner
  - Zonenverwalter
  - bei allen Datensätzen sind Kontaktdaten mit enthalten



Personensuchmaschinen

yasni.de BETA **Person suchen** | Personen-Profil anlegen | Über uns | FAQ | Login

Bernd Eylert Suchen

Sie sind hier: Person suchen > Bernd Eylert Alle Personen/Namen

0 Personen [?]

yasni Person

Jetzt erstes Personen-Profil anlegen (Vorteile):
Bernd Eylert (Neues Personen-Profil)

Markieren Sie die Ergebnisse, die zu Ihnen gehören. Dann: Zum Personen-Profil

Eigenes Personen-Profil anlegen

0 Ergebnisse [Neu]

Markieren Sie die Suchergebnisse, die zu Ihnen gehören, mit einem Häkchen, und klicken Sie auf "Speichern"! (Vorteile)

Personen-Profil speichern

18 Ergebnisse zum Namen [?] VIP-Rank

Markierte Ergebnisse als Personen-Profil speichern [?]

Google **Dr. Bernd Eylert (UMTS Forum): UMTS / 3. Generation Markt Studie ...**
Der Autor, Dr. Bernd Eylert, präsentiert die Ergebnisse einer Studie, in der die weltweite Nachfrage nach UMTS/3G Dienst ...
www.competence-site.de

Google **MeinProf.de - Prof. Dr. Bernd Eylert**
Dr. Bernd Eylert Hochschule: Technische Fachhochschule Wildau Stadt: Wildau Bundesland: Brandenburg Schwerpunkt: Informa ...
www.meinprof.de

Live Search **Berlin Brandenburg Aerospace Allianz e.V. | BBAA : News**
Bernd Eylert, selbst Pilot, begeisterte das Fachpublikum mit seinen Erläuterungen zu AVIGAL. Zugleich skizzierte er die ...
www.bbaa.de

Live Search **Buchshop Notfallmedizintechnik.de - UMTS**
von Bernd Eylert EUR 87,99: UMTS. Mobile Communications for the Future von Flavio Muratore EUR 81,99: UMTS Basics. Die G ...
astore.amazon.de

Google **CeBIT: Staat soll UMTS fördern | Home - News - Themenüberblick ...**
Nach Ansicht des Vorsitzenden des internationalen UMTS-Forums (London), Bernd Eylert, wird sich UMTS nicht schlagartig m ...
www.tecchannel.de

3 Bilder zum Namen [?]

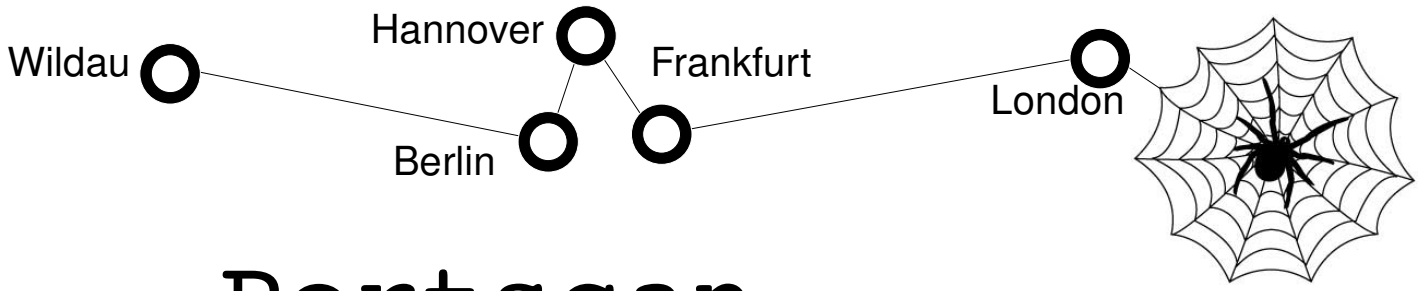
Google Google Google

Suche eingrenzen / erweitern [?]

Begriff eingeben

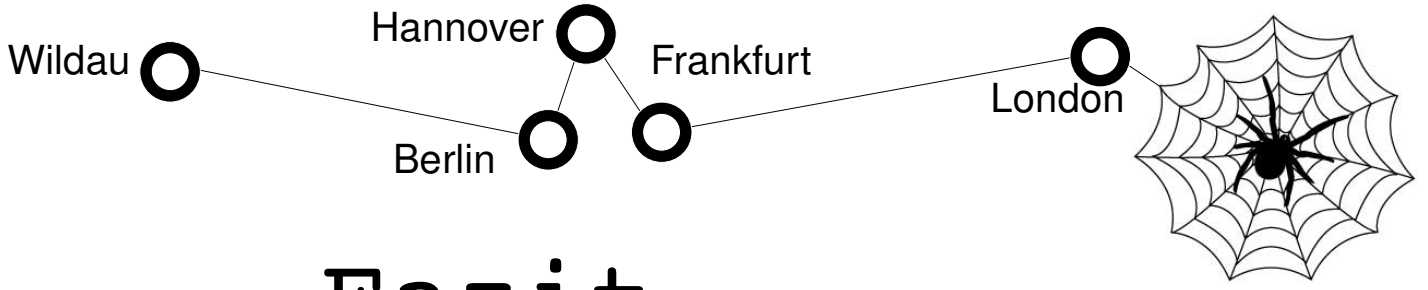
Ok

Aerospace Allianz Ansicht Artikel06 Autor Avigal Bbaa Berlin Brandenburg Buchshop Cebit Chairman Dorothee Erläuterungen Eur Fachhochschule Fachpublikum Friedhelm Future Geres Geschäftsführer Gewinne Gewinnerwartung Gmbh Griese Gsm Hansjörg Hillebrand Jahre Killerapplikation Kompendium Lehmanns London Mathematik Mobile Mobilkommunikation News Numerische Pilot Prof Siemens Technische Umts Umts-forum Umts-forums Vorsitzenden Vorsitzender Wildau Zeitraum Zugleich



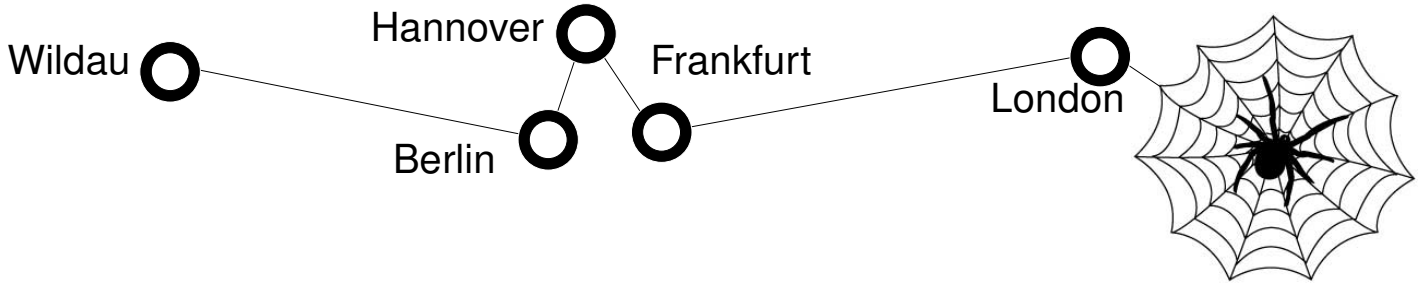
Portscan

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ )
  at 2007-11-27 20:41 CET

Interesting ports on 127.0.0.1:

Not shown: 1675 closed ports

PORT     STATE SERVICE

22/tcp   open  ssh

25/tcp   open  smtp

80/tcp   open  http

443/tcp  open  https

3306/tcp open  mysql

Nmap finished: 1 IP address (1 host up) scanned in
  13.149 seconds
```

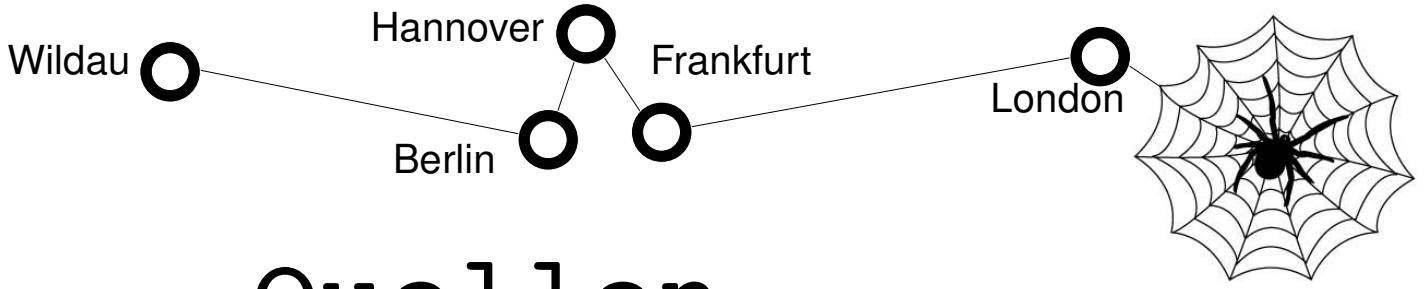


Fazit

- Daten sind generell nichts Schlechtes; aber in den falschen Händen, können sie bisweilen verheerende negative Folgen haben
- In rein deutschen Netzen ist Anonymität mit Beschluss der Vorratsdatenspeicherung nicht mehr möglich
- Wenn man nicht will, dass Inhaltsdaten bekannt werden, darf man sie entweder nicht übertragen oder muss sie vor Einsichtnahme schützen

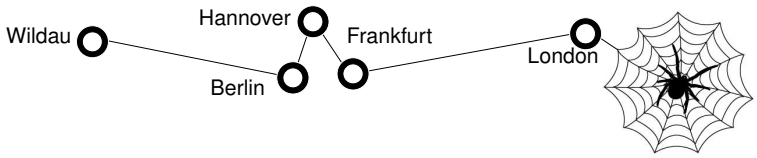


Vielen Dank für die Aufmerksamkeit



Quellen

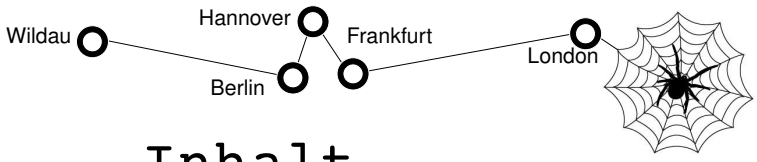
#1		**Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung ...**
		http://www.vorratsdatenspeicherung.de
#2	Köhntopp & Köhntopp	**Datenspuren im Internet**
	4/2001	Computer und Recht
#3	Reischl	**Gefährliche Netze (Wie Datenjäger das Internet missbrauchen)**
	2001	Ueberreuter
#4	Hall & Brown	**Core Web Programming**
	2001	Sun Microsystems Press
#5		**Google's Cookie**
		http://www.google-watch.org/cgi-bin/cookie.htm
#6		**Apache Log-File**
	25.11.07	http://sv-electronic-hn.com



Spuren im Netz

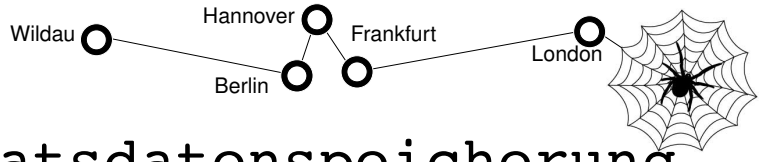
ein Arbeit von

Stefan Dassow



Inhalt

- Gesetzliche Daten-speicherungsregeln
- Datentypen
- Daten einer HTTP-Anfrage
- Daten erzeugt von Dienstleistern
- Cookies als Datenspeicher
- Sessionverfolgung
- Web-Bugs / Banner
- E-mails und News
- IRC & Instant Messenger
- Global Unique Identifier
- Öffentliche Verzeichnisse
- Portscan
- Fazit

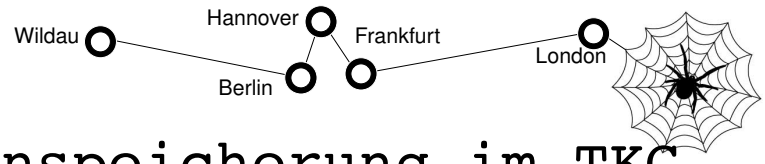


Vorratsdatenspeicherung

- Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Maßnahmen
- Beschluss nach namentlicher Abstimmung durch den deutschen Bundestag am 9.11.2007
- Neuerungen STPO:
  - Standortermittlungen von Mobilfunkendgeräten

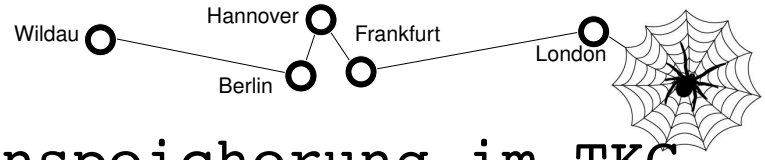
Vielseitige Änderungen an den verschiedensten Gesetzen zur Umsetzung der EG Richtlinie 2006/24/EG

Änderung der Strafprozessordnung wobei in besonderen Fällen die Beauftragung durch Staatsanwaltschaft möglich



Datenspeicherung im TKG

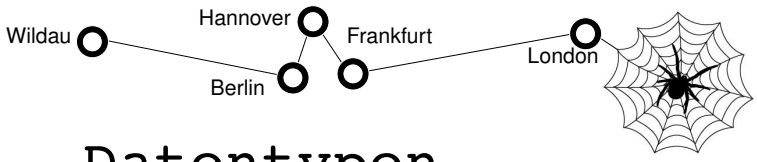
- Neuerungen TKG:
  - Speichern der Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,
  - Beginn und Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone,



Datenspeicherung im TKG

- in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst,
- Bezeichnung der genutzten Funkzelle (Mobil),
- bei anonymen Diensten die Aktivierungsdaten,
- IP-Adressen bei VoIP,
- bei elektronischer Post der gesamte Weg und das an jeder Stelle (auch IP bei Abruf),
- bei Veränderung von Verkehrsdaten sind die Veränderungen lückenlos zu dokumentieren

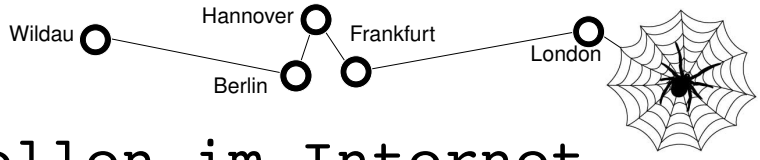
Funkzellenname muss Rückschluss auf Geokoordinaten ermöglichen
Bei Mobilfunk internationale Kennung aller Teilnehmer
Bei Nutzung von anonymen Diensten zusätzlich die erste Aktivierung des Dienstes mit vollem Datensatz
Bei E-mail muss der Absender die IP des Empfängers und der Empfänger die IP des Absenders speichern
Bei Zugriff auf das Postfach die IP des Abrufenden speichern
Alle Datensätze inkl. Datum und Uhrzeit



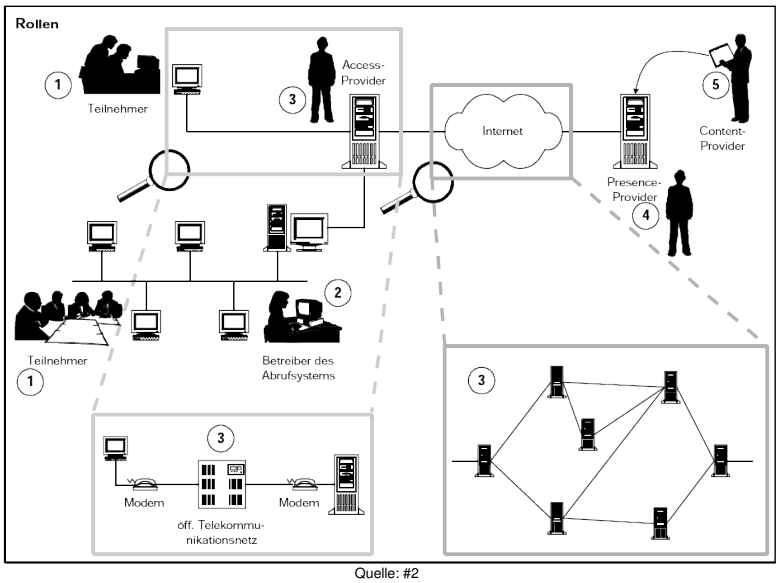
Datentypen

- Bestandsdaten
- Verbindungsdaten
- Inhaltsdaten

- Daten meist aus Vertragsabschlüssen, wie Name, Adresse, Bankverbindung u.ä. - fällt an bei Telekommunikationsanbieter, Access-Provider, Service-Provider)
- Absender, Empfänger, Zeitstempel, Dienst

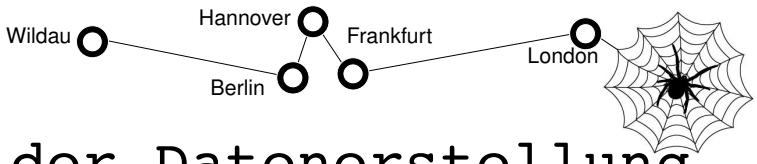


Rollen im Internet



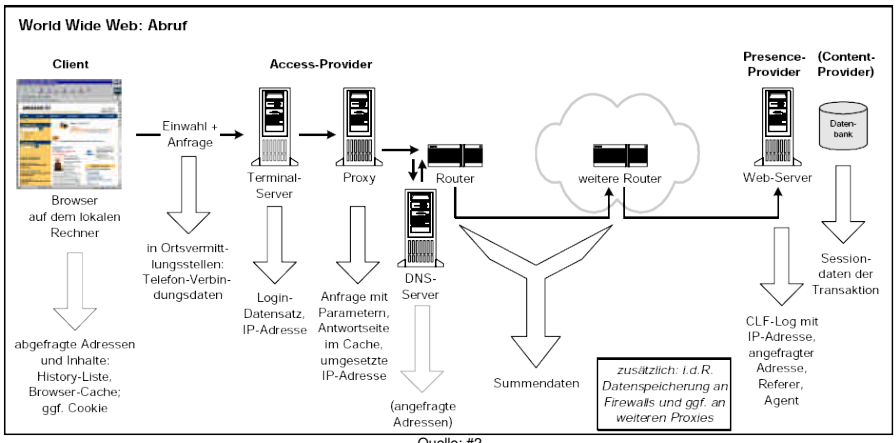
Quelle: #2

Teilnehmer nutzen Dienste/Rezipient (1)
Betreiber eines lokalen Netzwerkes sind außerhalb des Privatbereiches die Regel (2) – Unterscheidung von un-/eingeschränktem Zugang
Zugangsvermittler (3)
Diensteanbieter (4) – VoIP oder FTP-Server, E-mail
Inhaltsanbieter (5) – stellen mit Hilfe der Diensteanbieter Inhalte (Videos, Nachrichten...) zur Verfügung



Orte der Datenerstellung

- Daten werden an den unterschiedlichsten Orten erhoben



Quelle: #2

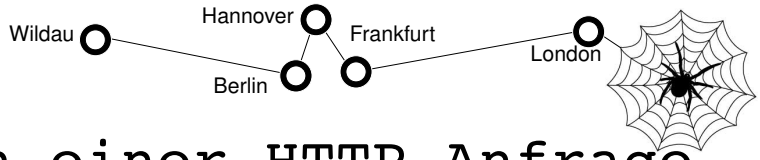
Internet-Browser speichert abgerufene Daten in den Standardeinstellungen für einen bestimmten Zeitraum

Einwahl erzeugt beim TK-Anbieter sowohl Daten zur Nutzung des Dienstes (Zeitstempel, Nummer des Anrufenden, Zielrufnummer) / ISDN und Daten in den Logs des Terminal-Servers (Login, IP, Zeitstempel)

vorhandene Proxy speichern NAT-Datensatz

DNS speichert im Regelfall nur die Zuordnung von IP-Adresse und Domain-Namen (Vergabe von Domainnamen erfolgt auch bei dynamischen IP's)

Router auf dem Weg speichern meist nur Summendaten (Datenvolumen zur Abrechnung)



Daten einer HTTP-Anfrage

- 89.50.34.79 - - [25/Nov/2007:16:43:40 +0100] "GET /tasklist.php HTTP/1.1" 401 5915 "-" "Opera/9.20 (X11; Linux i686; U; de)"
- 89.50.34.79 - **Administrator** [25/Nov/2007:16:43:48 +0100] "GET /tasklist.php HTTP/1.1" 200 11924 "-" "Opera/9.20 (X11; Linux i686; U; de)"
- 89.50.34.79 - Administrator [25/Nov/2007:16:48:01 +0100] "GET /liga.php**?game=119&task=change&logger=d785f384f6dc086b3a79a708fc26446c&season=21** HTTP/1.1" 200 11930 "-" "Opera/9.20 (X11; Linux i686; U; de)"
- 192.166.53.200 - - [25/Nov/2007:10:16:54 +0100] "GET /index.php?page=3 HTTP/1.1" 200 11240 "**http://www.google.de/search?hl=de&sa=X&oi=spell&resnum=1&ct=result&cd=1&q=H%C3%BCrdenCup+2007&spell=1**" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)"

Quelle: #6

Standardabfrage mit Source-IP, Zeitstempel, einfache Anfrage, HTTP-Statuscode (Authentifizierung gefordert), Dateigröße und Browserinfo

Wenn Authentifiziert ist auch noch der Nutzername ersichtlich

Bei GET-Anfrage kann man zusätzlich die Parameter einsehen

Wenn der Referrer mit übertragem wird, kann zusätzlich die vorherige URL eingesehen werden

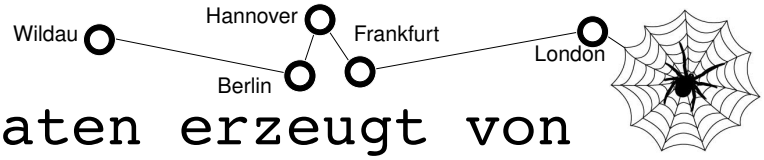
Dieses Apache Log zeigt aber noch nicht alle Daten:

- Unterstützte Mime-Types
- Komprimierungsunterstützung
- Automatische Cookie-Übertragung
- Zusätzlich zur IP den Hostnamen
- Aktualisierungsinformationen

Besonders problematisch ist, wenn in den Informationen Usernamen, Passwörter oder Kreditkarteninformationen übertragen werden

Weiterhin kann es passieren, dass Dateinamen die normalerweise für anonyme Nutzer nicht bekannt sind, über Referer Verbreitung finden

Das Ausschalten des Referers ist nur in den wenigsten Browsern komfortabel möglich



Daten erzeugt von Dienstleistern

- mehrere Möglichkeiten der Speicherung von Nutzerdaten möglich:
  - Cookies
  - Verfolgung mittels serverseitigen Sessions
  - Web-Bugs / Banner

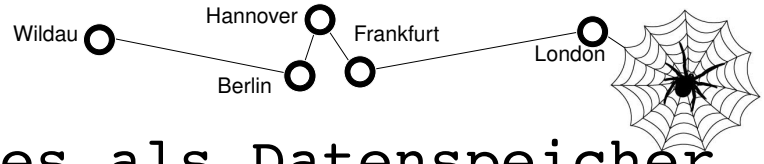
Zusätzlich zu den Daten, die die Dienstleister aus den Zugriffslogs erhalten, können sie mit Hilfe verschiedenster Techniken weitere Daten gewinnen und speichern

Die wohl älteste Form und in Misskredit geratene Variante ist der Cookie

Dann kommt die Verfolgung mittels Sessions

Die hinterlistigste Variante sind die Web-Bugs

Banner sind ähnlich den Web-Bugs, bloß dass der Nutzer weiß worauf er sich einlässt



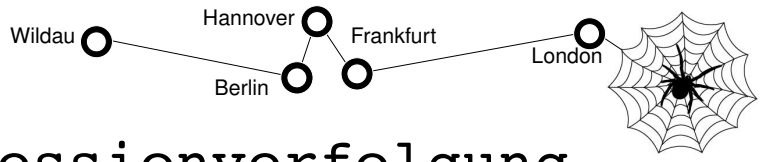
Cookies als Datenspeicher

- Maximalgröße: 4KB
- ein Cookie pro URL
- Mehrere Attribute; wichtigste sind „Name“, „Wert“ und „Ablaufdatum“
- Beispiel Google:
  - PREF=ID=28face613556316eTM=1184620070LM=1184620070S=DkEaab7_F7PtM3ZX (Quelle: #5)
- Neu: DOM-Storage Cookies

Cookies sind nur vom Server Abrufbar, der genau die gleiche URL hat
Die Gesamtgröße ist maximal 4KB
Übertragungsmodus festlegen (http od. Https)
Pfad lässt sich generalisieren (sprich host/ordner/ordner/datei lässt sich auch für host speichern, aber nicht für host/ordner/ornder2)
Daten sind im ASCII – Format (meist zur eindeutigen Nutzeridentifizierung)
Inhalte und Kondierung erfolgt durch den Server
Wenigste Cookies im Klartext lesbar
Beispiel Google:

- ID spricht wohl für sich
- TM = Zeitpunkt des ersten Setzens
- LM = Zeitpunkt der letzten Änderung
- S = Checksumme
- Ablaufdatum häufig so weit weg, dass über die ID eine eindeutige Identifizierung des Suchenden über großen Zeitraum möglich ist

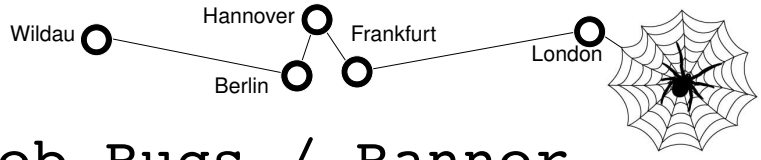
Dom-Storage Cookies können bis zu 5 MB groß sein und ermöglichen auch den Abruf von Seiten die ähnlich klingen
Vorteil: Daten aus Web2.0 Anwendungen müssen nicht mehr zwangsläufig zum Server übertragen werden
Nachteil: unscharfe Suche lässt Missbrauch durch Seiten mit ähnlichem Namen zu



Sessionverfolgung

- Session-ID's dienen der Identifizierung, meist als Ersatz, wenn Cookies abgelehnt werden
- ID's können mit temporären Cookies verglichen werden
- Standardvariablennamen sind bekannt, daher einfacher Identitätsdiebstahl durch „man-in-the-middle“ möglich

Session-Id speichern keine Informationen außer die Zugangsdaten
Häufig sind sie Ersatz für Cookies
Da Session-ID's nur temporär gültig sind, kann man sie mit Cookies vergleichen, die eine kurzfristige Ablaufzeit haben
Auf Grundlage der ID lassen sich Zuordnungen zu den Nutzern machen und in einer DB speichern
Wird die ID erst nach einer Anmeldung erzeugt ist eine eindeutige Nutzeridentifizierung über mehrere Sessions möglich
Da Session-ID's abgefangen werden können, wird bei der Nutzeridentifikation meist noch die IP des aufrufenden Nutzers mit ausgewertet



Web-Bugs / Banner

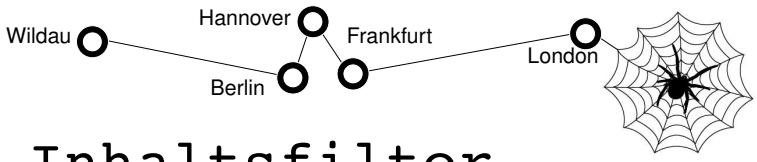
- Web-Bugs sind Bilder der Größe 1x1 Pixel mit transparentem Hintergrund
- Auch in HTML E-mails werden Web-Bugs verwendet
- Bilder können genauso wie HTML-Seiten Cookies setzen

Web-Bugs sind nur schwer zu identifizieren, da sie meist nur im Quelltext als <img>-Tags zu sehen sind

Beim Einsatz in E-mails können sie dazu verwendet werden ob und wann Nachricht eingesehen wurde

Auf Banner trifft das gleiche zu, wie auf Web-Bugs. Sie können Cookies setzen und erzeugen im Web-Server einen vollständigen Eintrag in der Logdatei

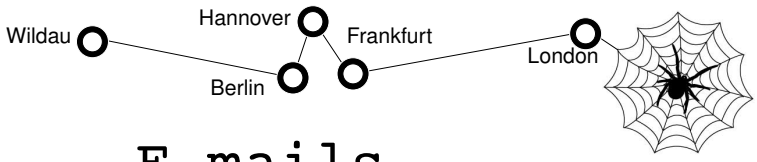
Bestes Beispiel dafür ist DoubleClick, durch das Schalten von Werbung auf Websites sind riesige auswertbare Datenmengen entstanden



Inhaltsfilter

- Moderne Browser unterstützen die Filterung von Inhalten für den Jugendschutz
- Für Filterung müssen die URL's an einen zentralen Server zur Überprüfung gesendet werden

Unter dem Vorwand des Jugendschutzes könnten mit solchen Mechanismen weitere Datenhalden entstehen



E-mails

- Innerhalb von E-mails werden Zusatzinformationen zum Absender und den E-mail Weg übertragen
- Verwendung von PK-Infrastrukturen lassen Rückschlüsse auf mögliche Kommunikationspartner zu
- E-mail Adressen werden weiterhin in Mailinglists öffentlich bekannt gemacht
- Die Notwendigkeit für Foreneinträge die E-mail Adresse anzugeben führen häufig auch zu einer Veröffentlichung

Zusätzlich zu den eigentlichen Inhaltsdaten werden noch übertragen:

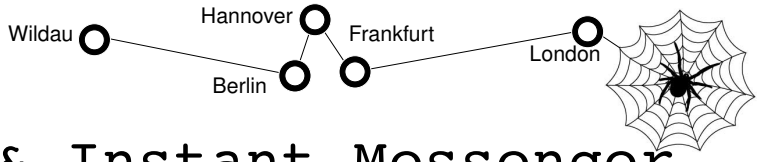
- User-Agent
- Sämtliche Adressaten, sofern sie nicht als BCC aufgeführt waren
- Verwendung von X-Schlüssel für nicht standardisierte Werte (X-Enigmail-Version, Daten zur Virenprüfung u.Ä.)

Anonymisierung von E-mail Adressen ist genauso wie beim HTTP über Dienstleister möglich

News werden nicht zielgerichtet weitergeleitet sondern auf Servern zum Abruf vorgehalten bzw. an verschiedenste weitere Newsserver verteilt

News und somit auch die E-mail Adresse werden meistens um 30 Tage öffentlich vorgehalten

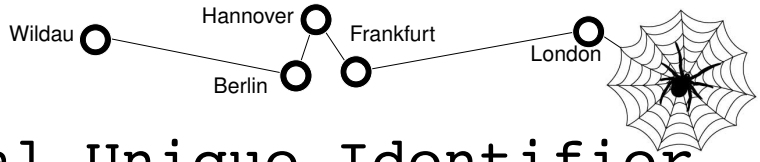
News werden trotzdem häufig archiviert, eine „Netiquett“ verhindert aber die Archivierung „X-No-Archive: Yes“



IRC & Instant Messenger

- Über whois-Anfragen sind im IRC IP und Nutzername einsehbar
- Bei einer Verbindung über einen Server sind für den Betreiber die Nachrichten i.A. sichtbar und können je nach Dienst auch mitgeloggt und ausgewertet werden

Daten aus den WHOIS-Anfragen sind nicht immer authentisch, da z.B. durch Proxies oder Webinterfaces die Daten verfäscht werden können

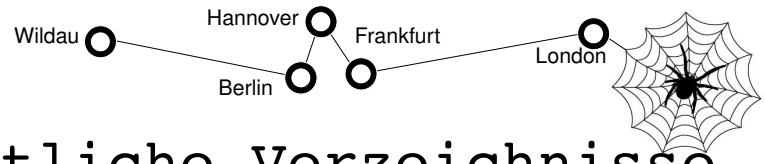


Global Unique Identifier

- Software versucht über GUID Nutzer eindeutig zu identifizieren
- Beispiel:
  - Pentium III enthielt Seriennummer, die über Software auslesbar war

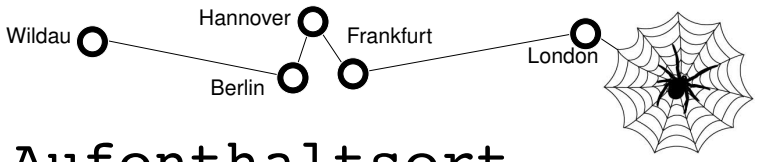
Wenn solche Nummern ohne Wissen des Nutzers gespeichert werden, bedeutet das bei Bekanntwerden einen großen Vertrauensverlust

Quellen behaupten, dass im IPv6-Protokoll die Mac-Adresse in jedem Paket mitgesendet werden soll, eine Bestätigung für diese Behauptung war nicht auffindbar



Öffentliche Verzeichnisse

- www.meineip.de Lässt Rückschlüsse auf den Aufenthaltsort zu
- In den whois-Datenbanken der NIC's finden sich die Besitzerdaten von den einzelnen Websites
- Auf Public-Key-Servern finden sich Unmengen von E-mail Adressen stellenweise mit Zuordnung zur Identität
- www.yasni.de sammelt Informationen von Personen über die Indexierung von Websiten



Aufenthaltsort

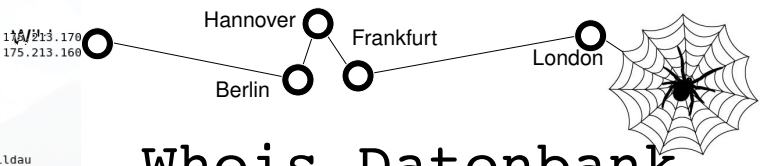
Details zu Deiner IP Adresse und zu Deinem System

Das ist Deine IP-Adresse	89.50.34.68
Dein Rechnername ist	N2244.n.pppool.de
Du surfst mit diesem Browser	Opera - 9.2
Du hast dieses Betriebssystem	Linux
Dein DSL Anschluss kommt von	freenet Cityline GmbH
Proxy eingeschaltet?	Nein
Dein Netzknoten befindet sich in	Stadt: 16515 Oranienburg Region: Brandenburg Land: Deutschland

Aufenthaltsort wird auf Grundlage des Weges zu der IP ermittelt. Die letzte öffentlich zugängliche Stelle wird als Zugang angegeben

Zu sehen sind auch noch einmal Teile der Daten, die der Browser mit übermittelt

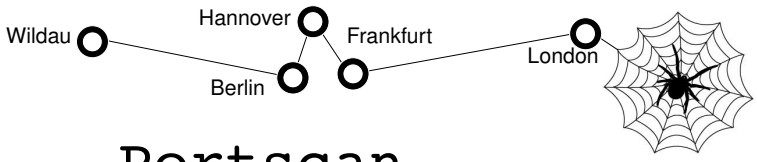
```
Domain:      tfh-wildau.de
Domain-Ace:  tfh-wildau.de
Nserver:     fresie.hrz.tfh-wildau.de 193.175.213.170
Nserver:     krokus.hrz.tfh-wildau.de 193.175.213.160
Nserver:     deneb.dfn.de
Status:      connect
Changed:     2007-11-08T11:55:08+01:00

[Holder]
Type:         ORG
Name:         Technische Fachhochschule Wildau
Address:      Friedrich-Engels-Str. 63
Pcode:        15745
City:         Wildau
Country:      DE
Changed:      2006-06-14T23:51:08+02:00

[Admin-C]
Type:         PERSON
Name:         Bernd Heimer
Address:      Technische Fachhochschule Wildau
Address:      Hochschulrechenzentrum
Address:      Bahnhofstr. 1
Pcode:        15745
City:         Wildau
Country:      DE
Changed:      2007-11-08T11:55:16+01:00

[Tech-C]
Type:         PERSON
Name:         Bernd Heimer
Address:      Technische Fachhochschule Wildau
Address:      Hochschulrechenzentrum
Address:      Bahnhofstr. 1
Pcode:        15745
City:         Wildau
Country:      DE
Phone:        +49 3375 508 992
Fax:          +49 3375 508 993
Email:        heimer@hrz.tfh-wildau.de
Changed:      2007-11-08T11:55:16+01:00

[Zone-C]
Type:         PERSON
Name:         Bernd Heimer
Address:      Technische Fachhochschule Wildau
Address:      Hochschulrechenzentrum
Address:      Bahnhofstr. 1
Pcode:        15745
City:         Wildau
Country:      DE
Phone:        +49 3375 508 992
Fax:          +49 3375 508 993
Email:        heimer@hrz.tfh-wildau.de
Changed:      2007-11-08T11:55:16+01:00
```



Whois-Datenbank

- whois-Eintrag enthält:
  - Inhaber
  - Adresse des Name-Server
  - Administrator
  - Technischer Ansprechpartner
  - Zonenverwalter
  - bei allen Datensätzen sind Kontaktdaten mit enthalten

Personensuchmaschinen als erstes in den USA aufgetaucht
Über Indexierung von Internetseiten werden die Daten gesammelt
Durch das Anlegen von Profilen wird die Suche schärfer
Größtenteils Metasuche bei anderen Suchmaschinen mit Spezialisierung auf Personeninformationen
Suchmaschinen können meist nur auf öffentliche Datensätze zugreifen, außer sie haben spezielle Abkommen mit Social-Networks-Betreibern

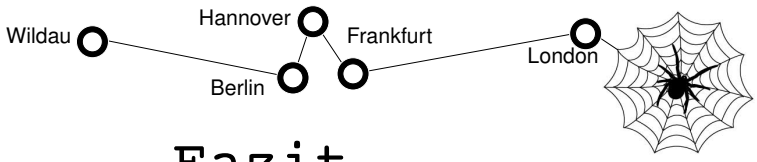


Portscan

```
Starting Nmap 4.11 ( http://www.insecure.org/nmap/ )
  at 2007-11-27 20:41 CET
Interesting ports on 127.0.0.1:
Not shown: 1675 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql
Nmap finished: 1 IP address (1 host up) scanned in
  13.149 seconds
```

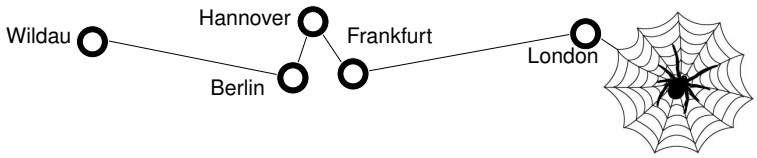

PortScans geben Aufschluss über von Außen erreichbare Dienste des Computers

Aufgrund der Liste lassen sich Angriffsszenarios für dies Dienste erstellen

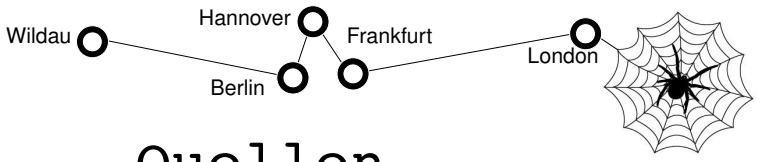


Fazit

- Daten sind generell nichts Schlechtes; aber in den falschen Händen, können sie bisweilen verheerende negative Folgen haben
- In rein deutschen Netzen ist Anonymität mit Beschluss der Vorratsdatenspeicherung nicht mehr möglich
- Wenn man nicht will, dass Inhaltsdaten bekannt werden, darf man sie entweder nicht übertragen oder muss sie vor Einsichtnahme schützen



Vielen Dank für die Aufmerksamkeit



Quellen

#1		**Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung ...**
		http://www.vorratsdatenspeicherung.de
#2	Köhntopp & Köhntopp	**Datenspuren im Internet**
	4/2001	Computer und Recht
#3	Reischl	**Gefährliche Netze (Wie Datenjäger das Internet missbrauchen)**
	2001	Ueberreuter
#4	Hall & Brown	**Core Web Programming**
	2001	Sun Microsystems Press
#5		**Google's Cookie**
		http://www.google-watch.org/cgi-bin/cookie.htm
#6		**Apache Log-File**
	25.11.07	http://sv-electronic-hn.com