



E-mail and Internet investigations

E-mail forensics
Web browser forensics
Internet forensics

E-mail klient undersökningar

- Lagarna är lite olika från land till land
 - Tex. vad gäller sändning av spam
 - Rätten att kontrollera arbetstagares email osv.
- Många brott och överträdelser mot policys sker via email
 - Trakasserier
 - Bedrägerier
 - Förföljelse/obehörig övervakning (computer stalking)
 - Utpressning
 - Malware (trojaner etc.)
 - Osv... listan kan göras väldigt lång

E-mail klienter och servrar

- Många olika E-mail program finns
 - Lista på säkra: www.bretschneider.net.de/tips/secmua.html
 - Outlook (Express) och Windows Mail (ej med i 7 men Windows Live Mail ingår i live essentials) är de mest använda i Windows
- E-mail servrar - MTA (Mail/Message Transfer Agent)
 - MS Exchange Server, SendMail, Postfix, etc.
 - IMAP (Internet Message Access Protocol) eller POP (Post Office Protocol), SMTP (Simple Mail Transfer Protocol)
- De populäraste webb-baserade lösningarna, vissa tillåter lokal lagring (off-line) av email
 - Gmail, Yahoo! Mail, Windows Live Hotmail
- Andra email lösningar
 - Apple Mail, Outlook Web App, MDaemon, RoundCube, etc.

http://en.wikipedia.org/wiki/Comparison_of_webmail_providers

Analys av E-mail

- Forensisk analys av mail
 - Göra en image av alla mailkomponenter
 - Leta igenom text, bifogade filer och e-mail headers i den fil eller filer som mailen lagras i
 - Vissa klienter kan kryptera mail (PGP/GPG, etc.), adressbok samt konfigurationsfiler (tex. TheBat! via eToken)
- Outlook familjen lagrar e-mailed i olika foldrar i en .PST (Personal Storage Table) fil
 - New, Read, Deleted, Draft plus egendefinierade foldrar
 - Lokal vs. server .PST fil?
 - .ost - Offline Storage Table, .pab - Personal Address Book file mm., se mer: <http://en.wikipedia.org/wiki/.pst>
- Mer information som kan finnas i E-mail klienter
 - Adressbok och kontaktinformation
 - Kalender med tid och datum för aktiviteter
 - Tasks – saker man planerar att göra

Analys av E-mail headern

- Var/vem kommer E-posten ifrån och vem skulle potentiellt motta mailet?
- RFC 821 (SMTP) Simple Mail Transfer Protocol
 - <http://www.ietf.org/rfc/rfc0821.txt>
- RFC 822 (Standard för meddelandeformat)
 - <http://www.ietf.org/rfc/rfc0822.txt>
- Krypterad server förbindelse via SSL/TLS, RFC 5246
 - STARTTLS - RFC 2595 (IMAP/POP), RFC 3207 (SMTP), ...
- Kom ihåg att varje del i mailet kan vara spoofat (förfalskat)
 - Sändaradress, e-mail server och olika identifierare
 - Headern kan ej krypteras!
- Utnyttja verktyg för att validera innehållet
 - <http://www.validateemailaddress.org/>

MIME (Multipurpose Internet Mail Extensions)

- Internet Standard för formatet på e-post, kallas ibland för SMTP/MIME
- e-post sänds med protokollet SMTP som endast stödjer 7-bits ASCII
 - Det finns en 8BITMIME SMTP extension standard
 - <http://en.wikipedia.org/wiki/8BITMIME>
- MIME definierar mekanismer för att sända e-post med andra språk och inkluderade bilagor av olika slag
- Används också för att kunna sända viss data inbäddat i andra protokoll, tex. HTTP (Webbserverns MIME types) och MMS
- "Transfer encodings" definierar hur man representerar 8-bits binär data med 7-bits ASCII
- "Content-type" ger meddelandets typ, tex. text/plain
- "Multipart messages" hanterar flera content types

RFC 822 headern 1

Return-Path: <tkv@du.se>

1. Retur adress

Received: from delta.du.se ([unix socket])
by delta (Cyrus v2.2.12) with LMTPA;
Mon, 16 Apr 2007 07:55:16 +0200

X-Sieve: CMU Sieve 2.2

Received: from tuna.du.se (tuna.du.se [130.243.57.133])
by delta.du.se (8.12.11/8.12.11) with ESMTP id I3G5tGrr029985
for <hjo@du.se>; Mon, 16 Apr 2007 07:55:16 +0200 (CEST)

Received: from localhost (localhost.localdomain [127.0.0.1])
by tuna.du.se (8.13.4/8.12.10) with ESMTP id I3G5tGMe020657
for <hjo@du.se>; Mon, 16 Apr 2007 07:55:16 +0200

2. Hops via e-mail server och deras IP-adress

Received: from tuna.du.se ([127.0.0.1])
by localhost (tuna.du.se [127.0.0.1]) (amavisd-new, port 10024)
with LMTP id 20079-08 for <hjo@du.se>;
Mon, 16 Apr 2007 07:55:15 +0200 (CEST)

Received: from PCTKV2 (pc-tkv2.du.se [130.243.36.173])
by tuna.du.se (8.13.4/8.13.3) with SMTP id I3G5sfTF020586
for <hjo@du.se>; Mon, 16 Apr 2007 07:54:41 +0200

3. Från IP nr Datum och tid

Message-ID: <000901c77feb\$be1de1e0\$ad24f382@ad.du.se>

From: "Thomas Kvist" <tkv@du.se>

To: "Hans Jones" <hjo@du.se>

4. Till

RFC 822 headern 2

References: <009b01c77db8\$9373c200\$ad24f382@ad.du.se>
<18510541690.20070413144858@du.se>

Subject: Re: Exjobb ITsäkerhetsplan

Date: Mon, 16 Apr 2007 07:54:43 +0200

MIME-Version: 1.0

Content-Type: multipart/alternative;
boundary="-----=_NextPart_000_0006_01C77FFC.7EBB2AB0"

X-Priority: 3

X-MSMail-Priority: Normal

X-Mailer: Microsoft Outlook Express 6.00.2900.3028

X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3028

X-Greylist: Sender IP whitelisted, not delayed by milter-greylist-2.0.2 (tuna.du.se
[130.243.57.133]); Mon, 16 Apr 2007 07:54:41
+0200 (CEST)

X-Virus-Scanned: by amavisd-new at du.se

X-Amavis-Alert: BAD HEADER Non-encoded 8-bit data (char E4 hex) in message header
'Subject'

Subject: Re: Exjobb ITs\344kerhetsplan\n ^

Hej Hans! Bla, bla, bla...

5. Ämnet

6. Datum och tid

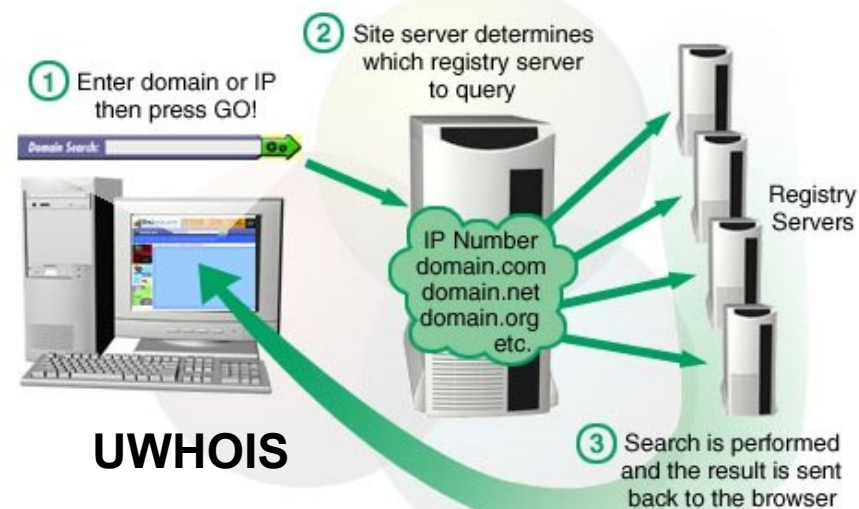
7. Typ text/html
text/plain
multipart/mixed
osv.

8. IP-adress på servern
som skickade mailet

9. Body

Whois databaser

- Registrerare för domäner – lista: www.internic.com
- Vem äger en specifik domän?
 - Vilken WHOIS-tjänst som helst i princip
 - www.uwhois.com för landsspecifika .ru .se .uk etc. (universal)
 - Namn, telefonnummer, mail, postadress, reg. data, namn servrar
- Vem "äger" ett specifikt IP nummer?
 - Underhåller WHOIS databas
 - Mapper IP-adress till FQDN (Fully Qualified Domain Name) samt ger info om FQDN mm.
 - Är dock ofta ISP:ns information
 - www.ripe.net (Europa)
 - www.arin.net (USA)
 - www.apnic.net (Asien)
 - www.lacnic.net (Sydamerika)
 - www.afrinic.net (Afrika)



Validera e-mail headers innehåll och Webb-baserade resurser för validering

- Fungerar reverse DNS?
 - Baklänges uppslag, leder ofta till ISP (ägaren av IP-adresserna)
- Webb-baserade och lokala verktyg i OS
- Sam Spade (<http://samspade.org/d/>) spade114.exe
- Ping – ICMP paket
- PingPlotter/(Win)MTR eller TraceRT/Visual Trace Route tool (www)
 - Visar hops mellan eget IP och FQDN
 - Windows -> tracert
 - GNU/Linux, Unix -> traceroute
- Få tag på telefonnummer och kontaktinfo till personal på FQDN
 - Ofta fel i whois databasen
 - www.google.com eller annan sökmotor
 - Gula och vita sidorna för respektive land
 - Kostar oftast pengar
- Bra resurs! http://www.sans.org/reading_room/



Exempel 2

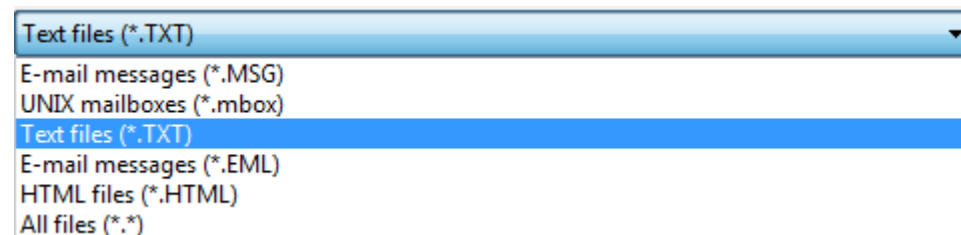
- thepiratebay.org DNS uppslag på <http://www.robtex.com>
- thepiratebay.org is a domain controlled by four nameservers at thepiratebay.org themselves. All of them are on different IP networks. Incoming mail for thepiratebay.org is handled by one mailserver also at thepiratebay.org. thepiratebay.org has one IP record. bayimg.net, bayimg.com, suprbay.net, suprbay.com, suprbay.org and at least seven other hosts share nameservers with this domain. piratebay.se, piratebay.net, thepiratebay.se, thepiratebay.net and thepiratebay.com share mailservers with this domain. ww.thepiratebay.org, mx.thepiratebay.org, ns1.thepiratebay.org, ns2.thepiratebay.org, www.thepiratebay.org and at least ten other hosts are subdomains to this hostname. org is a domain controlled by six nameservers. All of them are on different IP networks.

| base | record | name | ip | reverse | route | as |
|------------------------------|--------|-----------------------------------|--|------------------------------------|------------------------------------|---|
| | a | | 91.191.138.15 | lighttpd | (none) | 91.191.128.0/20 DCS.net AS21202 DCSnet-AS DCS.net Stockholm, Sweden |
| | | ns0.thepiratebay.org 1 hour old | 91.191.138.21 ? | (none) | | |
| | | ns1.thepiratebay.org 3 days old | 194.71.107.1 | SWEDEN | 194.71.107.0/24 Anycast DNS | AS13214 DCP-AS DCP Networks |
| thepiratebay.org 4 hours old | ns | ns2.thepiratebay.org 5 days old | 85.17.40.33 | dns Stockholm SWEDEN | ge0.anycast1.ams LEASEWEB | AS16265 LeaseWeb AS Amsterdam, Netherlands |
| | | ns3.thepiratebay.org 3 days old | 217.75.120.120 Apache/2.0.55 (Unix) PHP/5.2.5 SWEDEN | (none) | 217.75.120.0/21 STL-Port80, Sweden | AS39369 PORT80 AB, Sweden Bix Telecom AB, Sweden |
| | mx | 10 mx.thepiratebay.org 5 days old | 213.63.222.20 | lighttpd Postfix ESMTP NETHERLANDS | tfr.org | 213.63.192.0/19 SpaceDump Networks aggregated route AS30880 SPACEDUMP-AS SpaceDump Networks. This ASN is located on STLIX at Tulegatan Stokab And also on STLIX at Tulegatan Stokab For peering issues contact ripe@spacedump.net |

Server side undersökningar

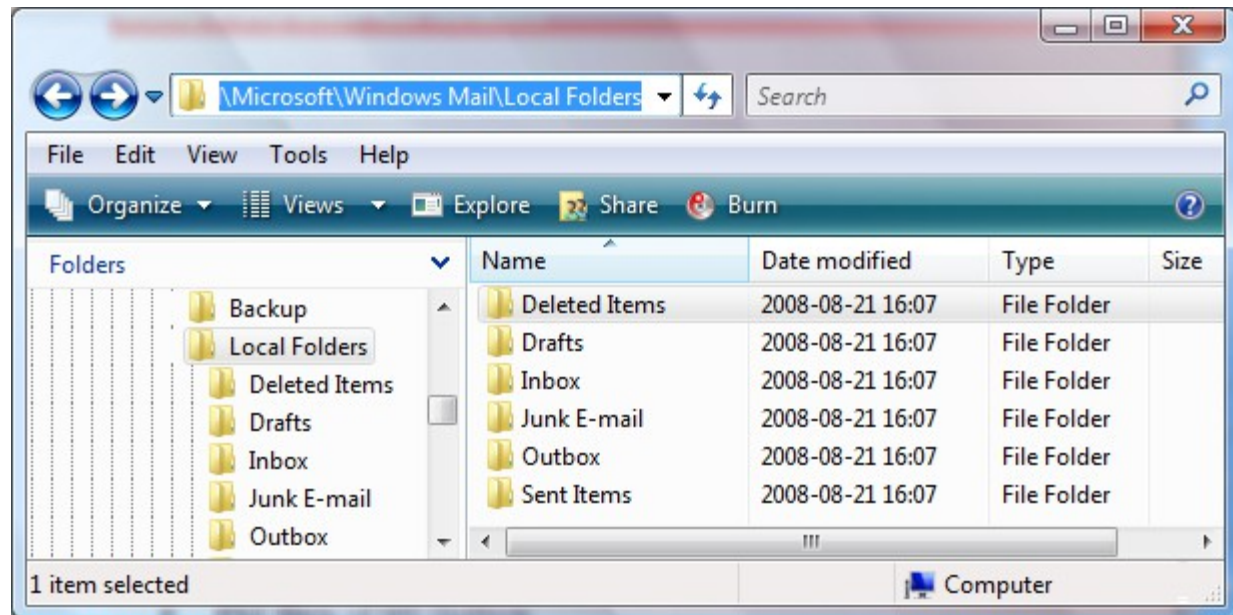
- Raderade mail i klienten kan fortfarande vara tillgängliga på e-mailservern
- Loggar över sända e-mail kan finnas kvar
 - Kan även validera klientens sända mail och därmed förbättra bevisen i caset
- Specialprogram eller kompetens kan behövas
- Exportera till .PST, .MSG fil eller annat lämpligt format
- Undersökningar på en organisations e-mailserver kan vara kritisk vad gäller uptime
- Forska! Enron Email data set (<http://www.cs.cmu.edu/~enron/>)
[server]\training_forensics_networkanalysis\Enron Email Dataset
- Slutligen, kom ihåg att det finns anonyma e-mail tjänster som tex. <http://www.sendanonymousemail.net/>

TheBat! Save Message As...



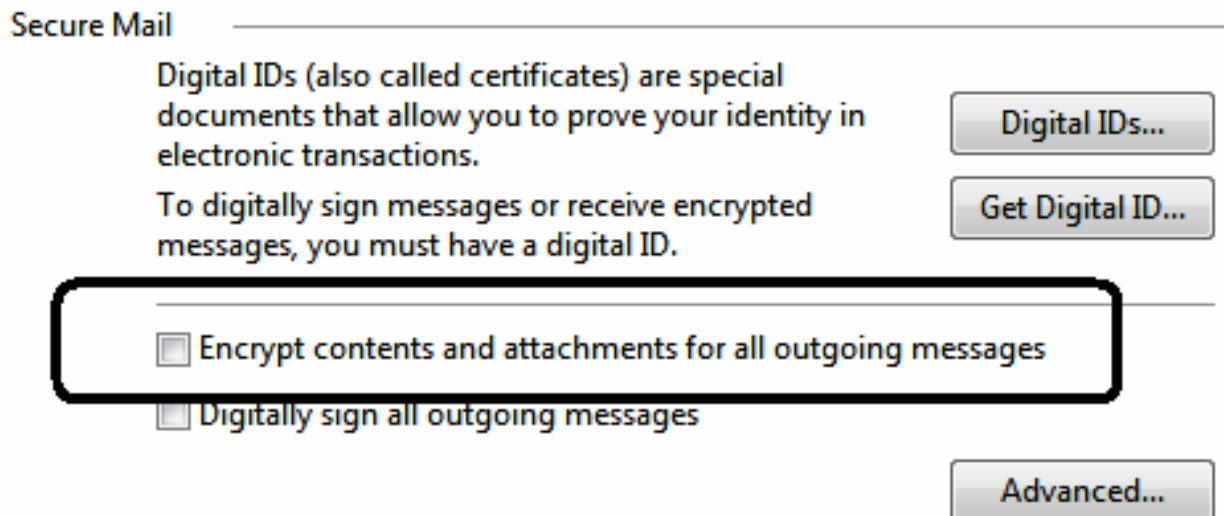
Windows Vista Mail 1

- Mail is no longer stored in a DBX volume and it is instead stored in simple plain text EML files.
 - http://en.wikipedia.org/wiki/Email#Filename_extensions
- The mail is stored under the user's profile in the following location
 - C:\Users\\AppData\Local\Microsoft\WindowsMail\Local Folders\



Windows Vista Mail 2

- One thing to note is that Windows Mail now has the ability to use encryption and digital signatures
 - Free secure email certificates (S/MIME) are available for download and can be used to encrypt email messages (comodo.com, thawte.com etc.)
- Email messages that are sent with the encryption flag set are encrypted before being placed in the outbox, so an examiner may find an email message in the Outbox where the body is encrypted and unreadable
 - The message headers though would be in plaintext



Windows 7 Live Mail

- With Windows 7 Microsoft made a change in policy - they did not included a desktop email program
- They do offer the option though to install - for free - **Windows Live Essentials**, which includes **Windows Live Mail**
 - <http://windows.microsoft.com/en-us/windows7/products/features/windows-live-essentials>
- Windows Live Mail has been made to look like a desktop mail program, but it isn't one
- Windows Live Mail is taken “into the cloud” - that means it is a web based application
- Sent, concepts and received emails are stored on a Microsoft server, **NOT ON THE COMPUTER!**
- In Windows 8 a more integrated solution will be available
 - Hotmail + Skydrive + Messenger + ...

Internet undersökning

Webbläsare

- Webbläsare är designade för att visa och köra
 - HTML, XML, FTP, Java Script och plugins som Java Applets, ActiveX kontroller, Adobe Flash mm.
- De innehåller
 - En cache av webbsidor och URL:er som besökts
 - Temporära Internet filer som skall öka hastigheten
 - X.509 digitala certifikat för att etablera säkra Internet förbindelser - PKI (Public Key Infrastructure)
 - Typiska användningen är att endast servern är autentiserad (dvs. dess identitet verifierad) medan klienten är icke-autentiserad
 - Stöd för krypterade kommunikationsprotokoll
 - SSL (Secure Socket Layer, Netscape), HTTPS, port 443
 - TLS (Transport Layer Security, nyare version av SSL)

PKI (Public Key Infrastructure)

http://en.wikipedia.org/wiki/Public_key_infrastructure

- Grundläggande funktion för all certifikathantering är att rätt objekt (användare, nätverksenheter eller programvaror) har ett korrekt utfärdat certifikat för en viss funktion
- Utfärdandeprocessen handhas av en CA (Certificate Authority) som är betrodd
 - För egna tillämpningar kan man låta egna företaget vara det
- Certifikat typer
 - Mjuka – lagringen sker i en fil på datorn
 - Hårda – lagringen sker på ett aktivt kort (smartcard etc.)
- CA internationellt: Verisign, Thawte osv.
- Exempel på CA i Sverige: Posten, Telia (hårda och mjuka), banker (BankID) osv.

Webbläsar-statistik

<http://www.w3schools.com/browsers/default.asp>

- Market share med äldre siffror (se nästa slide)

– <http://marketshare.hitslink.com/report.aspx?qprid=0>

- Webbläsar statistik per månad



– **Firefox** kommer från Mozilla projektet vilket i sin tur härstammar från Netscape



– **Safari** (Webkit baserad) utvecklas av Apple, används i Mac OS X och iOS



– **Opera** är Norsk, satsar mycket på små enheter

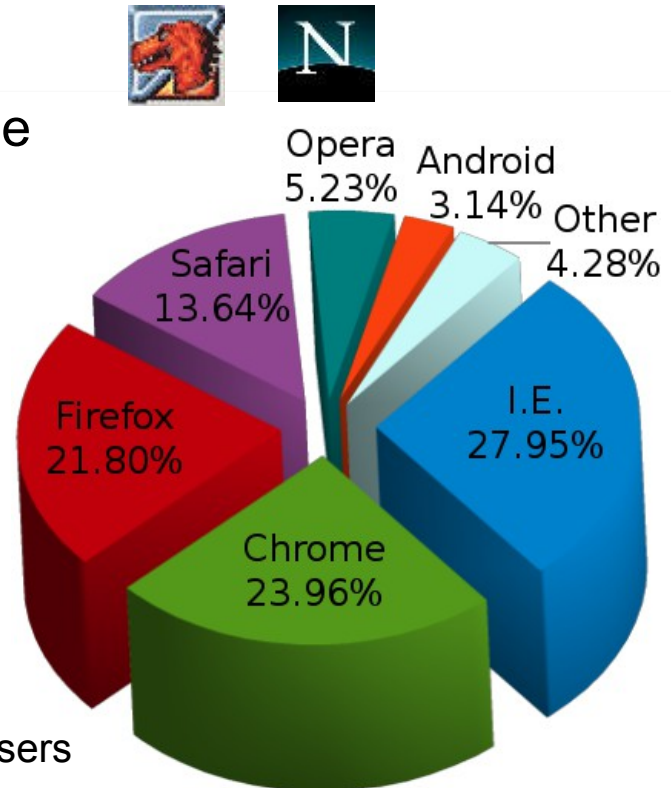


– **Chrome** (Webkit baserad) är Googles webbläsare



– **IE** (Internet Explorer) - Microsoft

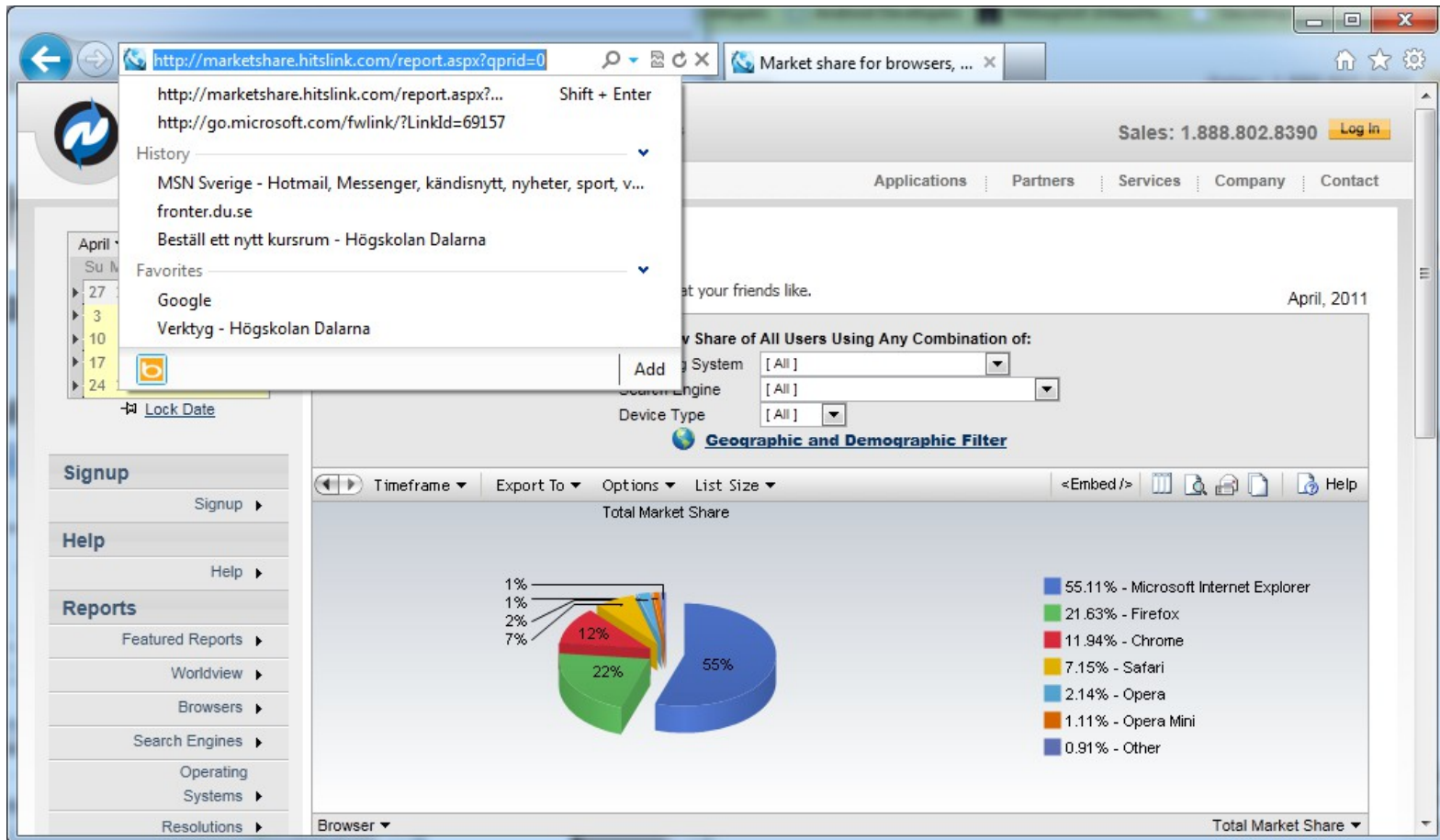
http://en.wikipedia.org/wiki/Usage_share_of_web_browsers



**Browser usage on Wikimedia
March 2012**

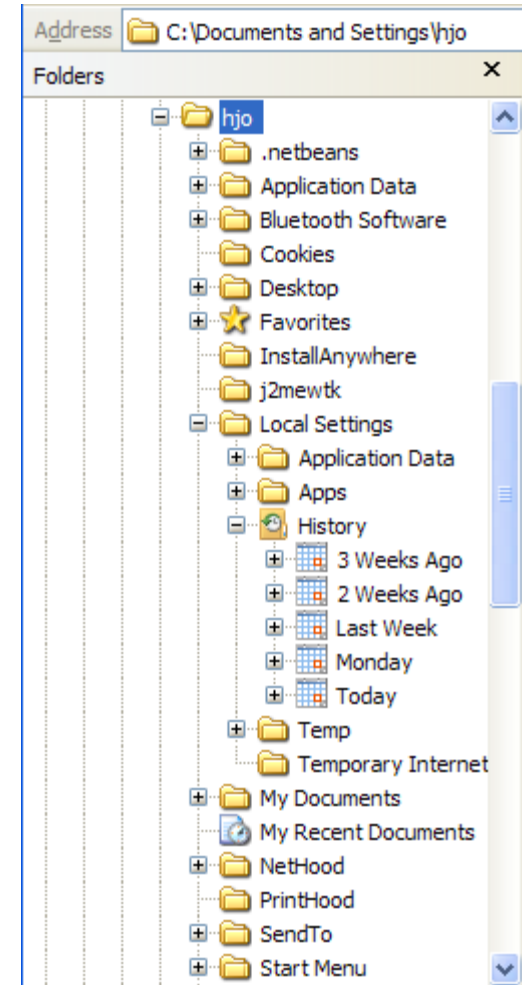
Webbläsare history 1

- De URL:er som användaren knappat in syns i applikationens adress fält
 - Adresser man klickat på syns *vanligen* inte i listan



Webbläsare history 2

- Webbläsar historyn lagras vanligen i användarprofilen
- Notera att förekomsten av en URL i en history mapp inte behöver betyda att användaren besökt sidan
 - Webbläsaren kan ha öppnas från "remote" för att misstänkliggöra användaren
 - Någon kan ha varit på datorn när användaren tillfälligt var borta
 - En länk/script på en webbsida kan öppna nya fönster eller sända användaren till en ny sida utan tillstånd
- Non IE history → SQLite DB file



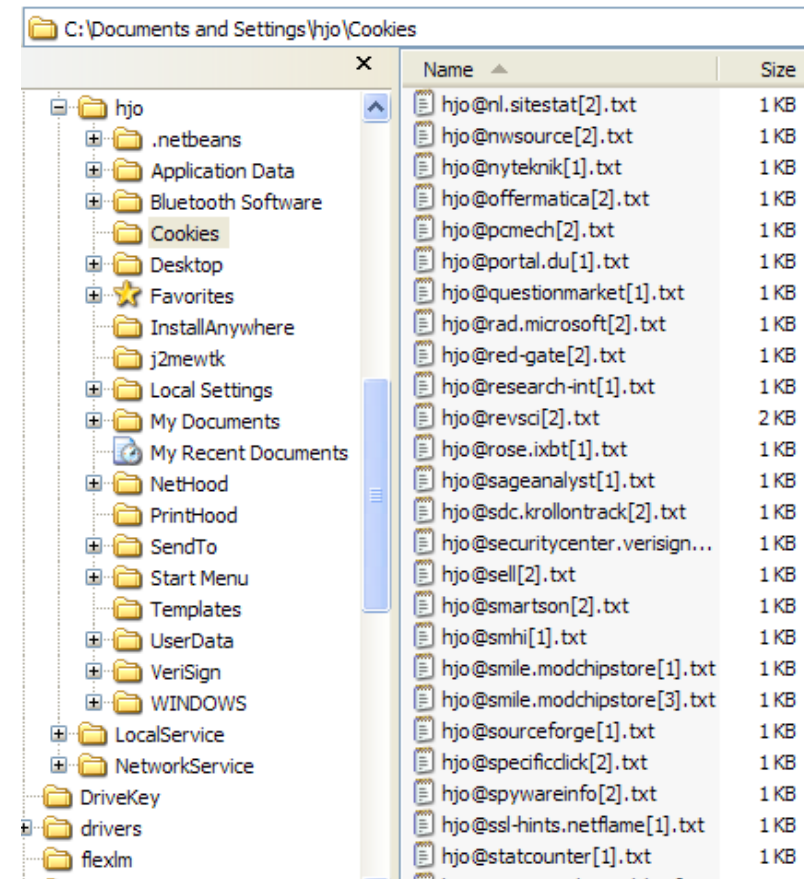
Chrome: C:\Users\<<user name>\AppData\Local\Google\Chrome\User Data\Default

Firefox: C:\Users\<<user name>\AppData\Roaming\Mozilla\Firefox\Profiles\<<profile folder>

IE Vista/7: c:\users\<<user name>\AppData\Local\Microsoft\Windows\History

Webbläsare cookies (IE)

- Cookies är små textfiler som vissa webbservrar lägger på datorn
 - För att identifiera dig
 - För att göra framtida besök mer anpassade
- Två typer finns
 - Tillfällig, finns bara under sessionen
 - Beständig, skrivs till fil på lokala datorn
- HTTP är ett tillståndslöst protokoll!!
- Ny lag om cookies 2011-07-01
- Non IE cookies → SQLite DB file



Chrome: C:\Users\\AppData\Local\Google\Chrome\User Data\Default

Firefox: C:\Users\\AppData\Roaming\Mozilla\Firefox\Profiles\

IE Vista/7: c:\users\\AppData\Roaming\Microsoft\Windows\Cookies

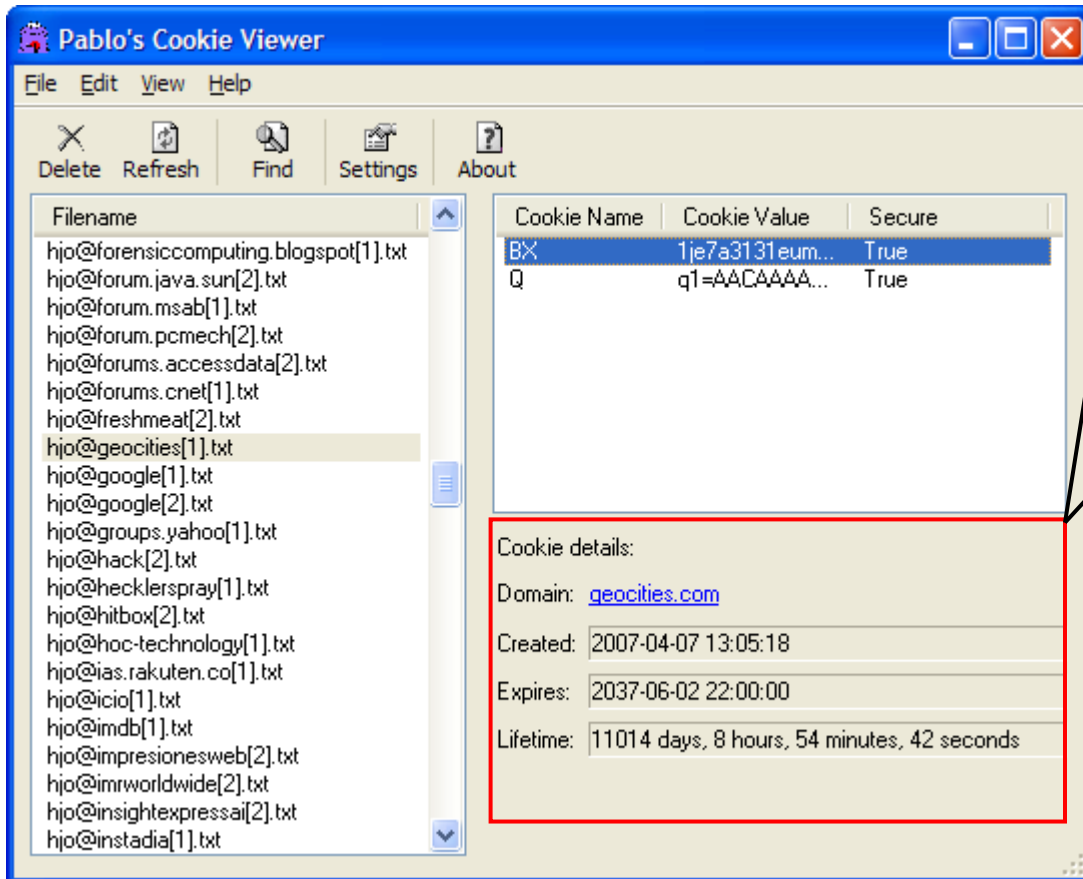
Vad finns det i en cookie?

- Precis som kakor bakas enligt ett specifikt recept - så fungerar även (beständiga) Internet cookies
- Följande värden kan man minst förvänta sig att finna i en cookie:
 - **Name:** Namnet på cookien
 - **Value:** Informationen cookien lagrar
 - **Expiration Date:** "Bäst före" datumet för informationen i cookien
 - **Domain:** Namnet på domänen som gett ut cookien
 - **Path:** Anger tillsammans med domain var cookiens information gäller
 - **Secure connection:** Denna inställning avgör om webbläsaren måste kommunicera med siten över en säker anslutning som tex. HTTPS
- Se ODESSA "Forensic analysis of MS IE Cookie Files"

Mer om cookies

- Cookie filerna är små (≤ 4 kB) och följer ett visst format
- Verktyg – Pablo's CV, Karen's CV, Galleta (ODESSA)

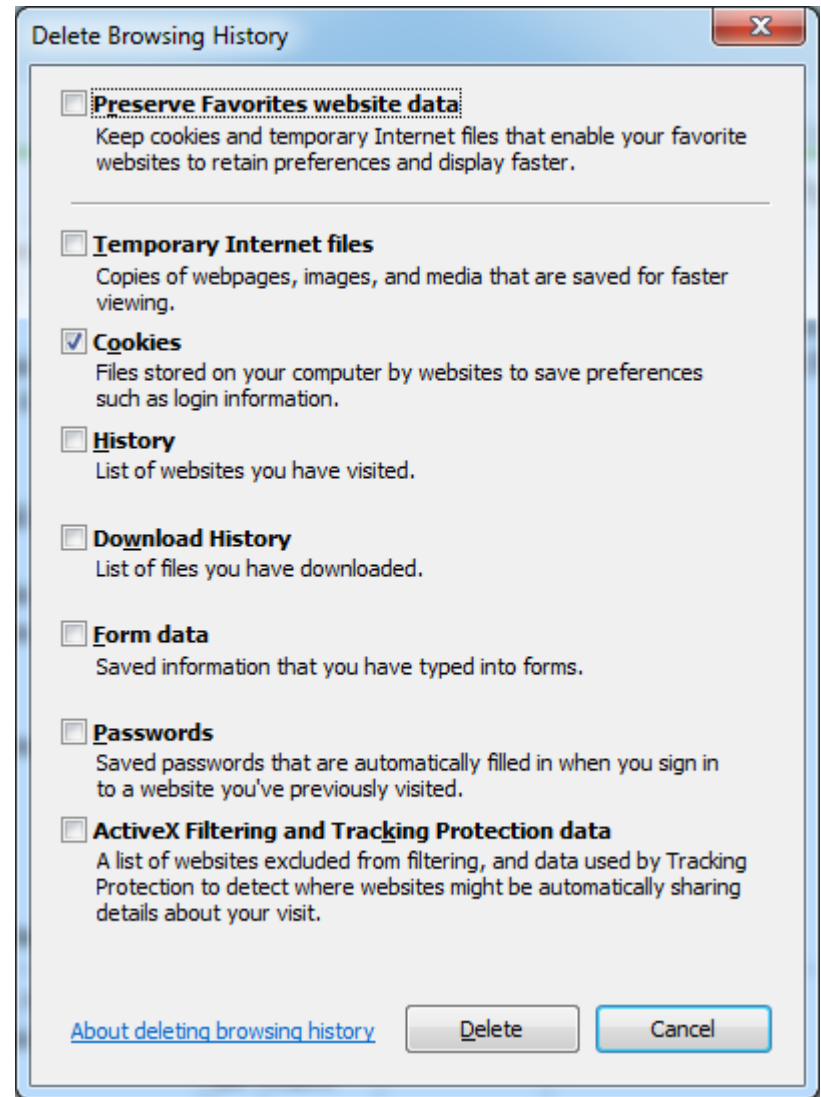
Cookie filen



```
BX
1je7a3131eumu&b=3&s=8l
geocities.com/
1024
342532096
32065574
2692891440
29849860
*
Q
q1=AAACAAAAA--&q2=RheYag--
geocities.com/
1088
3632617472
30584718
2718021440
29849860
*
```


Radera surf-historik

- Temporary Internet files == cachan för hemtagna webbsidor
- Olika slags historik och användardata kan raderas för att dölja vilka sidor som besökts
- InPrivate/Incognito/Private Browsing stöd?
- Firefox, Chrome etc. har liknande funktioner för radering av historik som IE
- Location på disk för cachan



Chrome: C:\Users\\AppData\Local\Google\Chrome\User Data\Default\Cache

Firefox: C:\Users\\AppData\Local\Mozilla\Firefox\Profiles\\Cache

IE Vista/7: C:\Users\\AppData\Local\Microsoft\Windows\Temporary Internet Files

Testa att skriva in "about:cache" i adressfältet för Firefox och Chrome

Webbläsare loggning

- Görs bäst via proxy eller firewall etc. i nätverket
 - Används mest för att blockera vissa domäner etc.
- Med spion programvaror som tex. BlazingTools Stealth Web Page Recorder eller Perfect Keylogger
 - <http://www.blazingtools.com/>
 - Visar besökt URL med hyperlänk
 - Datum och tid för besök
- Interaktiv monitoring av webbläsare aktivitet kan vara nödvändigt i speciella fall
 - Användaren clearar history, cookies, cachen mm.
 - Incongnito mode, InPrivate/Private browsing etc.

IE index.dat filer

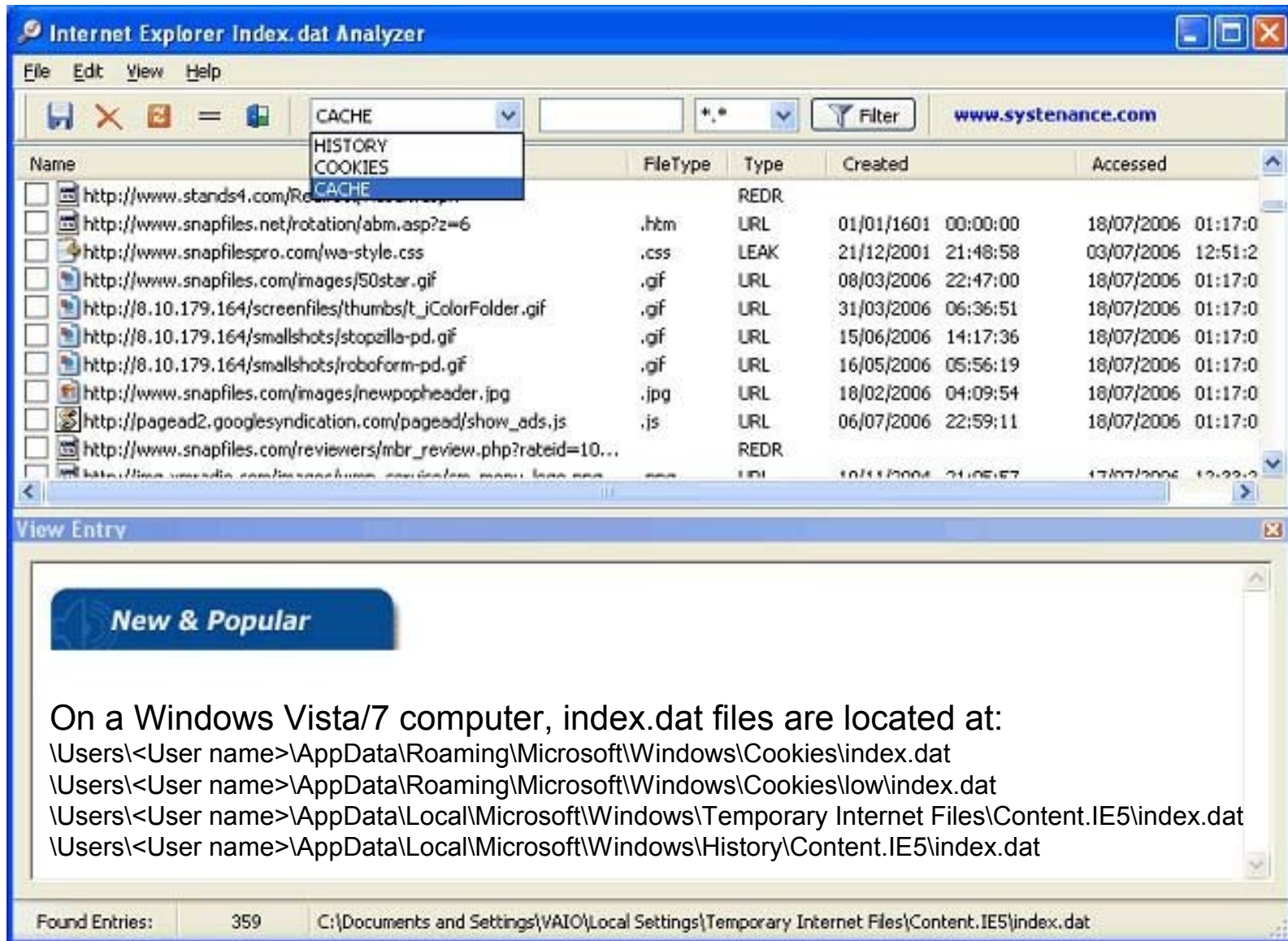
- Binära **gömda** proprietära systemfiler som i princip håller reda på all internetaktivitet för Internet Explorer, finns för:
 - Cache, cookies, och history (mest intressant)
- **Index.dat filerna** raderas inte när history, cache etc. clearas
 - Är flaggad som "in use" av OS
 - **Sökvägarna varierar mellan olika Win OS och IE versioner!**
 - Mer info: http://www.acesoft.net/delete_index.dat_files.htm
- **Index.dat filer** visar tex.
 - History på besökta (eller redirectade) URLer med hyperlänk
 - Datum och tid för besök
 - Om cachen har blivit clearad
 - Antalet gånger sidan har besökts
- De flesta användare vet inte om att denna information kan återskapas!
- Crap Cleaner är ett freeware program rensar det mesta, även index.dat filer: <http://www.piriform.com/ccleaner>



Webbläsare och forensics

- Internet Explorer, Chrome och Firefox
 - Mängder med verktyg förutom FTK och andra CF verktyg
 - **Index.dat Analyzer**, **Mandiant Web historian**, Pasco, mfl.
 - I cachan finns det mesta kvar, tex. dina webbmail (komprimerat?)
 - Cache view, Netanalysis mfl.
 - De flesta webbläsare förutom IE använder **SQLite databaser** (.db filer) för att lagra information
 - Ett webb case finns beskrivet på securityfocus webbsida www.securityfocus.com/infocus/1832
 - Part 1 och part 2 (finns även under /forensics/docs/web browser forensics)
- Bra!:** <http://aggressivevirusdefense.wordpress.com/2009/10/07/web-browser-forensics/>
- ODESSA (Open Digital Evidence Search and Seizure Architecture) - <http://sourceforge.net/projects/odessa/>
 - A cross-platform framework for performing Computer Forensics and Incident Response
 - White paper: "Forensic Analysis of Internet Explorer Activity Files"

Index.dat Analyzer



Internet Explorer Index.dat Analyzer

File Edit View Help

SAVE X COPY PASTE = FILTER www.systemance.com

CACHE HISTORY COOKIES CACHE

| Name | FileType | Type | Created | Accessed |
|--|----------|------|---------------------|--------------------|
| http://www.stands4.com/Re... | | REDR | | |
| http://www.snapfiles.net/rotation/abm.asp?z=6 | .htm | URL | 01/01/1601 00:00:00 | 18/07/2006 01:17:0 |
| http://www.snapfilespro.com/wa-style.css | .css | LEAK | 21/12/2001 21:48:58 | 03/07/2006 12:51:2 |
| http://www.snapfiles.com/images/50star.gif | .gif | URL | 08/03/2006 22:47:00 | 18/07/2006 01:17:0 |
| http://8.10.179.164/screenfiles/thumbs/t_jColorFolder.gif | .gif | URL | 31/03/2006 06:36:51 | 18/07/2006 01:17:0 |
| http://8.10.179.164/smallshots/stopzilla-pd.gif | .gif | URL | 15/06/2006 14:17:36 | 18/07/2006 01:17:0 |
| http://8.10.179.164/smallshots/roboform-pd.gif | .gif | URL | 16/05/2006 05:56:19 | 18/07/2006 01:17:0 |
| http://www.snapfiles.com/images/newpopheader.jpg | .jpg | URL | 18/02/2006 04:09:54 | 18/07/2006 01:17:0 |
| http://pagead2.googleadsyndication.com/pagead/show_ads.js | .js | URL | 06/07/2006 22:59:11 | 18/07/2006 01:17:0 |
| http://www.snapfiles.com/reviewers/mbr_review.php?rateid=10... | | REDR | | |
| http://www.snapfiles.com/reviewers/mbr_review.php?rateid=10... | | REDR | | |

View Entry

New & Popular

On a Windows Vista/7 computer, index.dat files are located at:
\\Users\\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
\\Users\\AppData\Roaming\Microsoft\Windows\Cookies\low\index.dat
\\Users\\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
\\Users\\AppData\Local\Microsoft\Windows\History\Content.IE5\index.dat

Found Entries: 359 C:\Documents and Settings\VAIO\Local Settings\Temporary Internet Files\Content.IE5\index.dat

Mandiant Web Historian

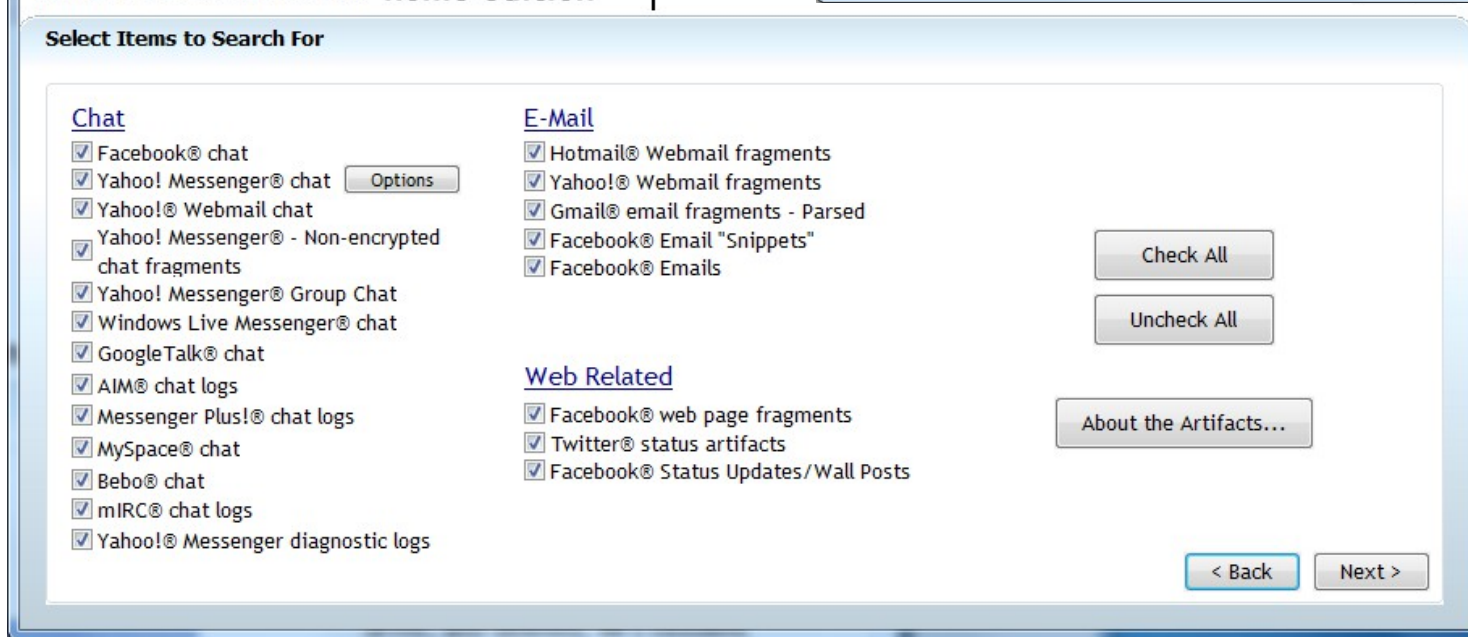
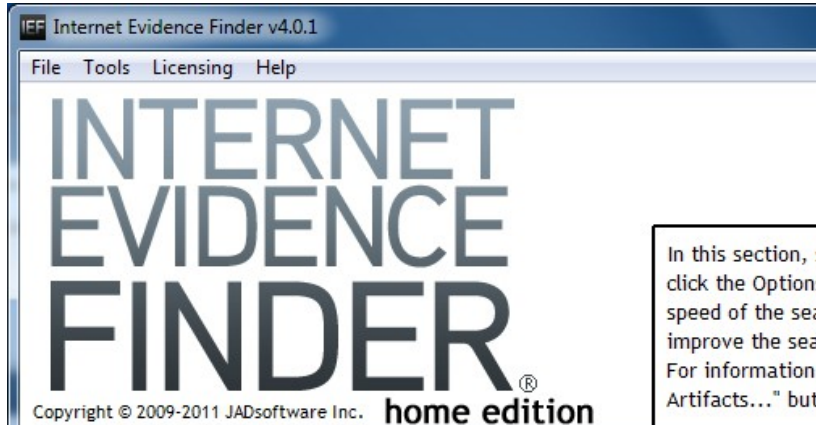
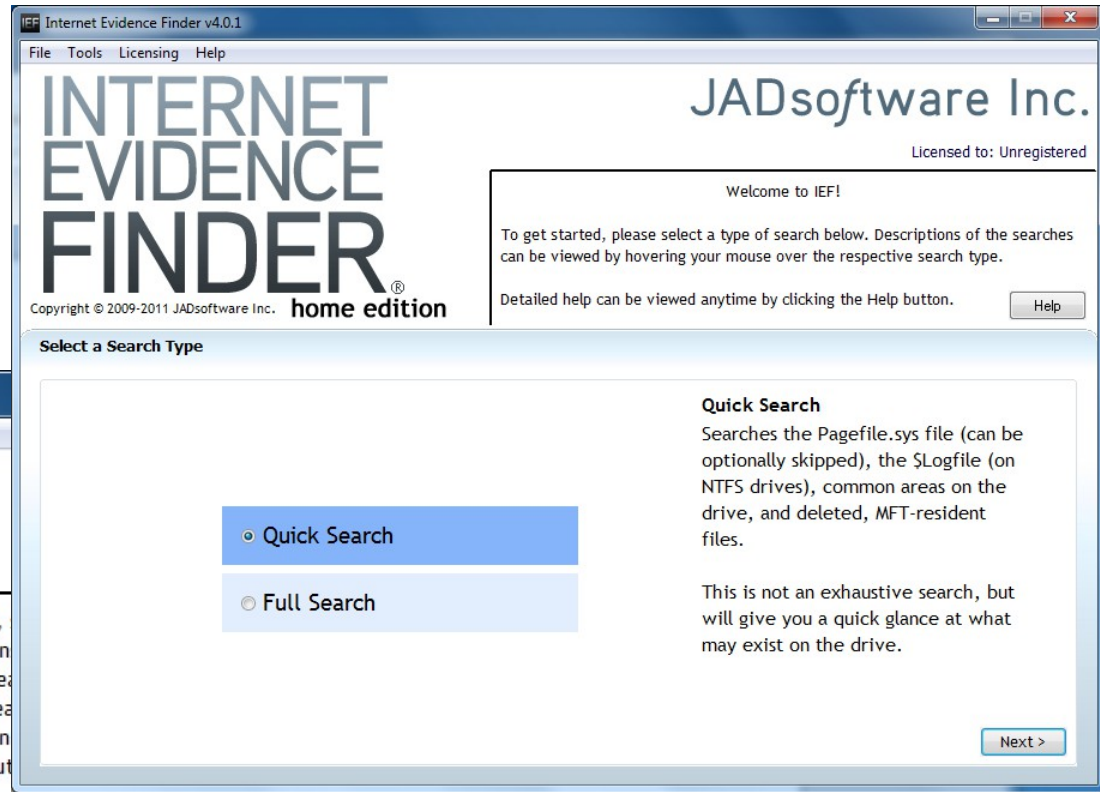
The screenshot displays the Mandiant Web Historian application interface. At the top, there is a menu bar (File, Edit, View, Tools, Help) and a search bar. Below the menu is a toolbar with icons for various functions. A navigation bar shows 'Web History', 'Cookie History', 'Download History', and 'Form History' tabs. The main area contains a table of scan results with columns for Profile, BrowserName, BrowserVersion, Username, DownloadType, FileName, TargetDirectory, SourceURL, StartDate, and State. The first row is highlighted in blue.

| Profile | BrowserName | BrowserVersion | Username | DownloadType | FileName | TargetDirectory | SourceURL | StartDate | State |
|---------|-------------|----------------|----------|--------------|--------------|-------------------|--------------------|--------------------|----------|
| Default | Chrome | 11.0.696.60 | hjo | Manual | GenuineCheck | \Users\hjo\Dow... | http://download... | 1970-01-01T00:2... | Finished |
| Default | Chrome | 11.0.696.60 | hjo | Manual | | | | | |
| Default | Chrome | 11.0.696.60 | hjo | Manual | | | | | |
| Default | Chrome | 11.0.696.60 | hjo | Manual | | | | | |
| Default | Chrome | 11.0.696.60 | hjo | Manual | | | | | |
| Default | Chrome | 11.0.696.60 | hjo | Manual | | | | | |
| Default | Chrome | 11.0.696.60 | hjo | Manual | | | | | |
| Default | Chrome | 11.0.696.60 | hjo | Manual | | | | | |

An 'Export Results' dialog is open in the bottom-left corner, showing options to select history data (Web history, Cookie history, File download history, Form history) and an output format (HTML). It also has radio buttons for 'Export all data' and 'Export only data shown in current gridviews (filtered)', and a 'Browse...' button for the export location.

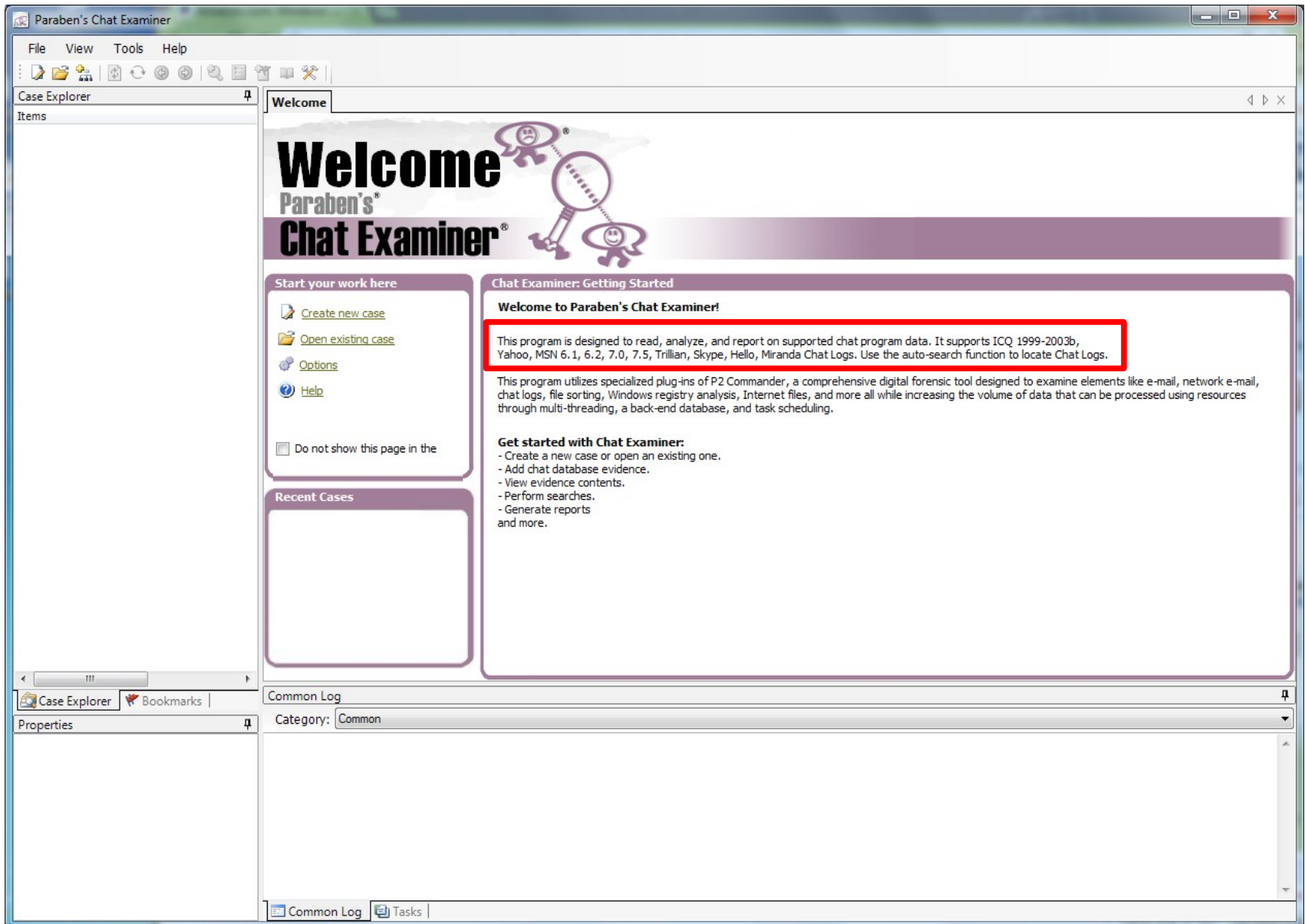
A 'Web History Scan' dialog is open in the bottom-right corner, showing a 'Start' button and a 'Scan ready. Click 'Start' to begin' message. It has tabs for 'Agent Output', 'Settings', and 'Advanced'. The 'Settings' tab is active, showing options for where to look for web history (Scan my local system, Profile folder, History file) and what data to collect (Browsers: Firefox, Chrome, Chrome Frame, Internet Explorer, Safari; Collect history: Website history, Cookie History, Retrieve Chrome website thumbnails, Retrieve Chrome indexed page content, File Download History, Form History, System Information).

IM (Instant Message) chats and other internet artifacts



IEF

Paraben Chat Examiner



Maltego

Maltego v2.0.2CE

File Edit View Navigate Tools Window Help

Speed/Accuracy # Results

Palette

New Graph (1) * x

Infrastructure

- AS
- DNS Name
- Domain
- IP Address
- Netblock
- Website

Pen Testing

- Banner
- Port
- Service
- Vuln
- Webdir
- Webtitle

Personal

- Email Address
- Location
- Person
- Phone Number
- Phrase

Mining View Centrality View Edge Weighted View

100 retomeier

1100 neier.kirchberg@gmail.com

100 RT @HeathrowAirport: T5 has been partially evacuat...

100 @retomeier Any idea why?

100 @retomeier #androidPL OMG! Button! (https://market...

300

300

100

Satellite View

Properties

Entity properties

| | |
|-------------------------|------------------------------|
| Entity type | AffiliationTwitter |
| Value | Reto Meier |
| Weight | 100 |
| Unique identifier [key] | retomeier |
| Network [key] | Twitter |
| Profile URL | http://twitter.com/retomeier |

Detail View

| | | |
|-----------|---|----------------------|
| Source | RT @HeathrowAirport: partially evacuat... | (Twit) |
| Transform | To Twitter Affiliation [Convert] | |
| Result | Reto Meier | (AffiliationTwitter) |
| Gen_date | 2011-3-10 14:54 | |

Author info

| | |
|---------|------------------------|
| Icon | |
| Profile | retomeier (Reto Meier) |

Output - Transform execution

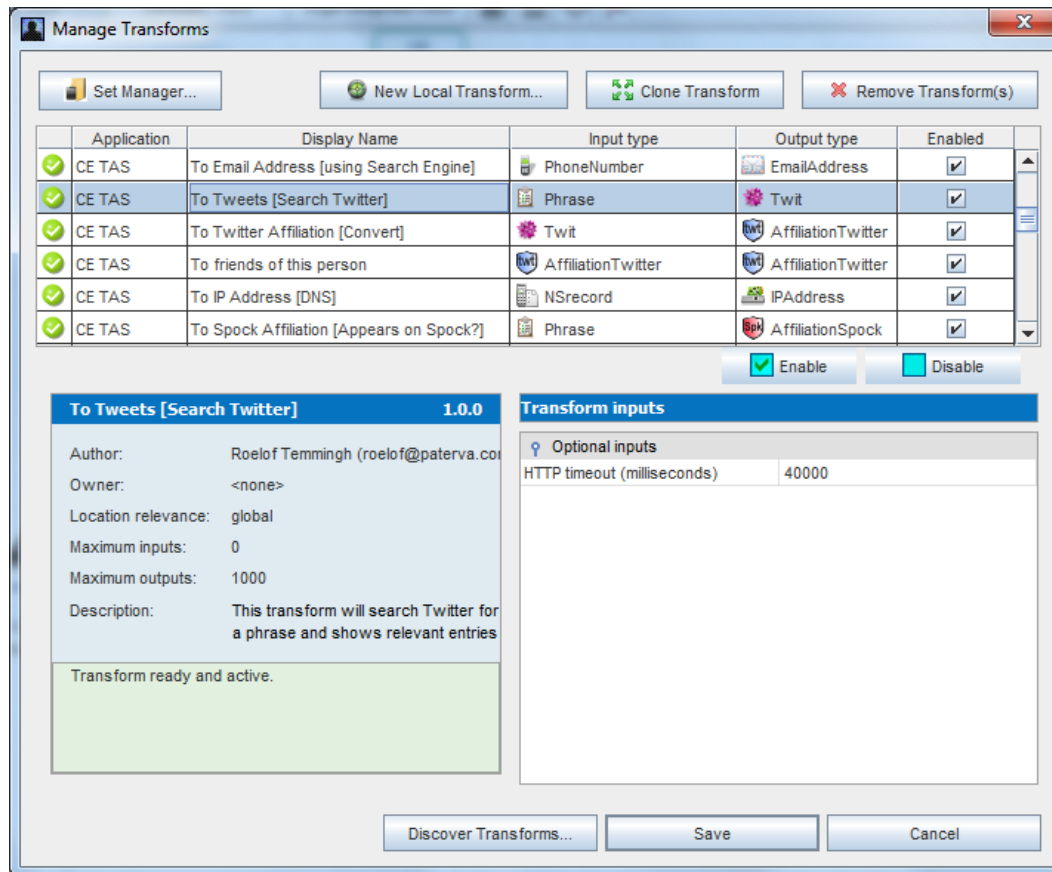
```
Transform "To URLs [show Search Engine results]" completed with 0 results
- No URLs were found on this node...
Transform 'Mirror: External links found' cancelled by user.
Transform 'Mirror: Email addresses found' cancelled by user.
Transform "To friends of this person" completed with 12 results
```

What is Maltego?

- Maltego is an information gathering tool that allows you to visually see relationships. Maltego allows you to enumerate network and domain information like
 - Domain Names, Whois Information, DNS Names
 - Netblocks, IP Addresses
- Maltego also allows you to enumerate People information like
 - Email addresses associated with a person's name
 - Web sites associated with a person's name
 - Phone numbers associated with a person's name
 - Social groups that are associated with a person's name
 - Companies and organizations associated with a person's name
- Maltego also allows you to
 - Do simple verification of email addresses
 - Search blogs for tags and phrases
 - Identify incoming links for websites
 - Extract metadata from files from target domains

Maltego transforms

- All the information gathering "processes" that Maltego does are called "Transforms," and unfortunately not all of them are documented. But different transforms query different types of information. The full list is here:
 - <http://ctas.paterva.com/view/Category:Transforms>



Maltego resources

- Maltego Part I - Intro and Personal Recon
 - <http://www.ethicalhacker.net/content/view/202/24/>
- Maltego Part II - Infrastructure Enumeration
 - <http://www.ethicalhacker.net/content/view/251/24/>
- Data Mining Tony Hawk's Twitter Hunt with Maltego
 - <http://www.securityg33k.com/blog/?p=180>
- Maltego: Transform & Correlate
 - <https://www.issa.org/Library/Journals/2009/December/McRee-toolsmith.pdf>
- Maltego
 - <http://www.paterva.com>



WebSite-Watcher 1

- Automatically check web pages for updates and changes
- Automate your daily routine, boost your productivity
- Features
 - Monitor web pages
 - Monitor password protected pages
 - Monitor forums for new postings and replies
 - Monitor RSS feeds, newsgroups and local files
 - Highlight changes in a page
 - Powerful filter system to ignore unwanted content
 - Many more features to stay up-to-date!
 - <http://aignes.net/>

WebSite-Watcher 2

WebSite-Watcher 2010

| Name | URL | Last change | Status | Last check |
|--------------------------|--------------------|---------------------|------------------|----------------|
| DIR wswatch | D:\wswatch | 2010-04-01 12:58:05 | OK | 2010-04-01 ... |
| news://asp.members.te... | news://asp.me... | 2010-04-01 09:51:17 | OK | 2010-04-01 ... |
| WebSite-Watcher - Dow... | http://www.ai... | 2010-04-01 12:45:54 | OK | 2010-04-01 ... |
| WebSite-Watcher - Sup... | http://www.ai... | 2010-04-01 12:46:46 | OK, phpBB2 Pl... | 2010-04-01 ... |
| WSW Forum RSS | http://www.ai... | 2010-04-01 11:03:53 | OK | 2010-04-01 ... |
| www.website-watcher.c... | http://www.ai... | 2010-04-01 12:52:48 | OK | 2010-04-01 ... |
| www.website-watcher.c... | http://aignes.c... | 2006-07-08 15:12:59 | OK | 2006-07-08 ... |

WebSite-Watcher 2010 (10.0) - 02-Feb-2010

Download (7.8 MB) Mirror (7.8 MB)

System: 2000, XP, Vista, 7, Server 2003/2008
Version History

If you install a new version, do not uninstall your existing copy of WebSite-Watcher - just install the new version over the old one!

Download our other products

Local Website Archive 3.1.1
Archive web pages for future reference 3 MB Download Mirror More Info...

Bookmarks: 95 [4]

Forum Feature Request

| Thread Title | Replies | User | Date |
|--|---------|---------------------|---------------------------|
| Time and date as email variables | 2 | watchdog | Wed Apr 14, 2010 5:46 am |
| alert when a bookmark does not update for some time | 1 | pinoweb | Tue Apr 13, 2010 12:26 pm |
| show name of URL in delete window dialog | 1 | ringo | Wed Apr 07, 2010 12:37 pm |
| Send by email only the text extracted between 2 filters ? | 3 | ifen | Wed Apr 07, 2010 12:20 pm |
| Autowatch check at specific intervals in minutes. | 2 | Imennuti | Thu Mar 25, 2010 2:51 pm |
| Minimum number of... | 80 | mkscomputing | Thu Mar 25, 2010 2:11 pm |
| Indicator to scroll d... | 250 | catallhood | Tue Mar 23, 2010 2:11 pm |
| Shortcut for Manual... | 100 | Vidado | Tue Mar 16, 2010 10:57 am |
| Double check a link... | 128 | Martin Aignasberger | Mon Mar 15, 2010 10:41 am |
| Will there be an update for the Firefox 3.0 Add-On? | 4 | ringo | Mon Mar 08, 2010 1:05 pm |
| Wishlist | 5 | gelite | Tue Feb 23, 2010 9:43 am |
| Searching for keywords according to the language of the page | 5 | hertel | Wed Feb 17, 2010 12:57 pm |

Bookmarks: 96 [4]