*

Safe(r) Searching

Workshop at the VOGIN IP conference

Arno H.P. Reuser
a@reuser.biz
+31 6 3812 7715

Reuser's Information Services
Leiden, The Netherlands

Leiden, The Netherlands

Reuser's Information Services

Monday 4th March, 2013

Print and typeset using LaTeX 2_ε
Published by *Reuser's Information Services*

Edited February 2013
Print Monday 4th March, 2013

This handbook was created in support of the Safe(r) Searching workshop at the VOGIN IP Lezingen conference, conducted on the 28th February 2013, by Reuser's Information Services. It constitutes the presentations and additional explanations and material.

De Wetstraat 16
2332 XT
Leiden
The Netherlands

Reuser's Information Services http://www.reuser.biz

Contents

List of Figures

List of Tables

1 Validation of Information

1.1 Check the URL

Take a good look at the address bar or URL.

1. The national bank of France (Banque de France)
   (a) `http://www.banquefrance.fr`
   (b) `https://www.banquedefrance.com`
   (c) `https://NationalBankOfFrance.tw/login.asp`
2. Hiding, obscuring the URL
   (a) `http://banquedefrance.fr` [1]
   (b) `http://193.45.22.7/secure/login`
   (c) `http://www-ebay-com.login.com/secure/`
   (d) `Latest Bond Movie` [2] `garantueed free!`
   (e) `Banque de France` [3] , can you see the entire URL on your (very) tiny phone screen?
   (f) `Banque de France` [4] `official website.`
   (g) `Banque de France, or ...` [5]

   Older techniques like replacing ASCII characters with their dWord value, hexadecimal value or even octaal values won't work anymore. Browsers are too smart for that.
3. A heritage. Just call the bank of quadronia
   (a) `"dr Mike Shukwuweta" chukwuweta@aol.co.uk`
4. Protocol What protocol is used? HTTP? HTTPS?
   Websites with sensitive data (banks, databases) use SSL protocols to be safe(r).
5. Executable or HTML page? Is the object being referred to a webpage, or, an executable program?
   (a) `http://www.banqdefrance.fr/clients/login.asp`
   (b) `http://www.banqdefrance.fr/clients/login.com`
   (c) `http://www.banqdefrance.fr/clients/login.exe`

   (See figure ~1)

[1] http://clickme.and.get.hacked/stupid!
[2] http://tinyurl.com/7nyshvd
[3] http://www.banquedefrance.fr.reuser.biz
[4] http://www.banquedefrance.fr:secure_login_clients@www.reuser.biz
[5] http://www.banquedefrance.fr@213.73.89.122

Figure 1: Certificate of OSC

6. Certificates

   Secure websites use certificates to identify themselves. A bank website without a certificate is ...interesting.

   Watch out for Diginotar certificates. Remove them from your system.

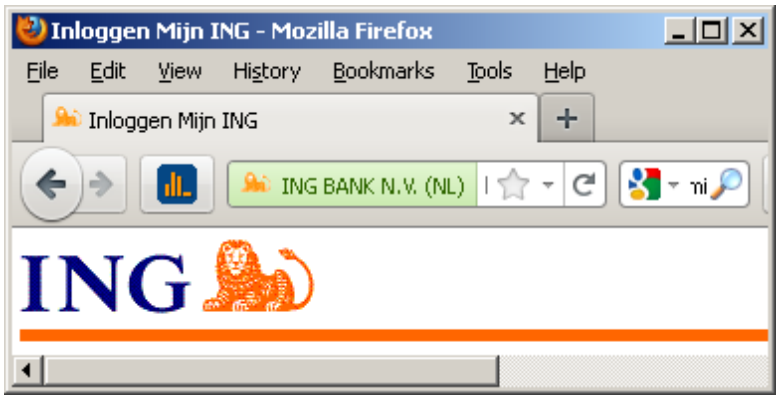


Figure 2: Certificate of ING Bank

   (See figure ~2)

7. Private? `http://www.demon.co.uk/~BBCNews.html`

And off course you dit LOOKUP the IP address and you also try to find out WHOIS behind a website, and a TRACERT to identify the route to the target.

2 Cyber weapons

2.1 People

Best cyberweapon of all: human beings

Or, their attitude of nonchalance, indifference, ignorance, not caring, not believing, security not taken seriously and general lack of awareness, can be used by hackers as a weapon.

People in general:

1. Don't care
2. Don't know
3. Are ignorant

Typical remarks by people

1. "There is nothing of interest on my PC/laptop" Dream on. Ever heard of BotNet, or identity theft
2. "I have nothing to hide"

   Really? What about: taxes, finance, sexlife, pincodes (of bank cards, of phones), secret lovers, failures, fibs.

   Remember the News of the World phone scandal?

Figure 3: Hacking starts early

(See figure ~3)

3. ”My children don’t do things like that”

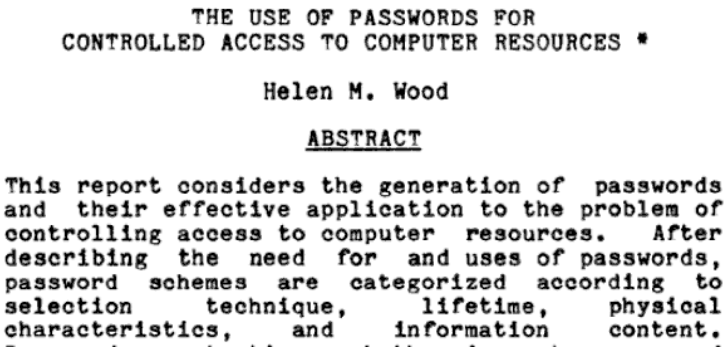
   Dream on. Children are much more capable of doing things than you think. Remember the kid who run a brothel from the classroom via mobile phone?

4. ”My child is too young for such things”

   Absolutely. It’s all the others isn’t it?

Who cares about security?

1. Helft kantoorpersoneel omzeilt beveiliging [6] om te kunnen werken (”more than 50% of office workers ignore security rules in order to be able to work properly”)
2. ”Just 4% follow the password policies of their companies”. (Report [7])



THE USE OF PASSWORDS FOR
CONTROLLED ACCESS TO COMPUTER RESOURCES *

Helen M. Wood

ABSTRACT

This report considers the generation of passwords and their effective application to the problem of controlling access to computer resources. After describing the need for and uses of passwords, password schemes are categorized according to selection technique, lifetime, physical characteristics, and information content.

Figure 4: The use of passwords for controlled access to computer systems / Helen M. Wood. - 1977

(See figure ˜4)

2.2 Intercepting and cracking

Intercepting passwords on a network is not too difficult.

A password sniffer

”Listen carefully, I shall say this, only once”

1. With ’password sniffers’ one can sniff or listen for logonid’s and passwords
2. Listening utility loaded on 10.0.0.61, sniffing machine 10.0.0.51
3. Finds remote address, logon ID, password

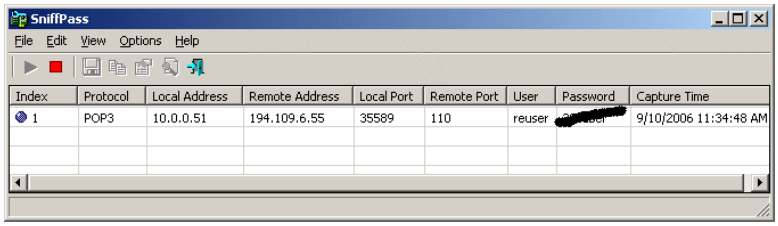


Figure 5: A password sniffer

(See figure ˜5)

HTTP sniffer

A sniffer, sniffs, everything

1. The entire session is interceptedt
2. All pages are stored
3. Finds search behaviour, passwords
4. Only for HTTP protocols, not for HTTPS

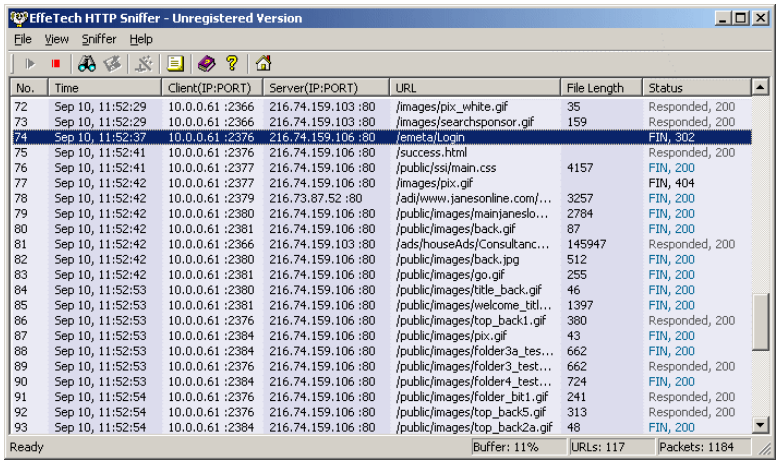


Figure 6: Intercepting full HTTP traffic

(See figure ˜6)

(See figure ˜7)

Protected storage passwords

Very safely stored by Microsoft on your disc.

[6] Beveiligingsbeleid.txt
[7] PasswordAuthenticationfromaHumanFactorsPerspective.pdf

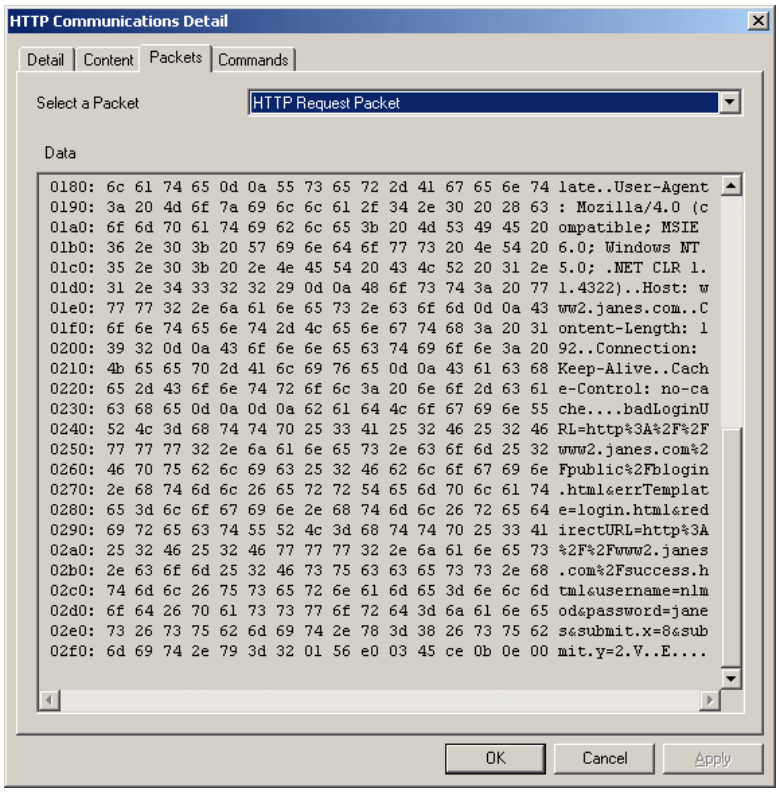


Figure 7: Finding the password while intercepting HTTP traffic

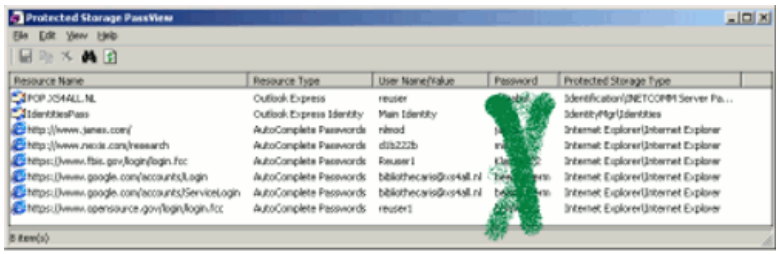


Figure 8: Protected Storage Passview

(See figure ˜8)

Do you ever check you public libraries PC's? Can visitors plug in flash memory drives?

3 Identity fraud

3.1 Faking identities

On the internet, many simply fake complete identities making it difficult to establish true authorship.

Ein Lichtbildausweis

Dutch journalist Brenno de Winter created a fake ID card that gave him access to all kinds of official institutes for nine months [8] [9] [10]

Figure 9: journalist Brenno de Winter fake ID

(See figure ˜9)

Got access to, amongst others:

1. Ministries of General Affairs, Home office, Security and Justice, Health, Infrastructure
2. National Cyber Security Center, Houses of Parliament.
3. Nationale Police corps, Police The Hague, Royal Military Police
4. Also accepted as legal ID to vote for parliament

Robin Sage

Robin Sage, an example of a fake, new identity.

(See figure ˜10)

[8] Winter – ID bewijzen slecht gecontroleerd / Brenno de Winter. - NU.nl, 24 September 2012
[9] RTL – RTL Nieuws 24 september 012
[10] NRC – Minister Spies belooft betere controle identiteitsbewijs Marije Willems. - NRC Handelsblad, 25 September 2012

Figure 10: Robin Sage

1. 25-year-old "cyber threat analyst"
2. Naval Network Warfare Command in Norfolk, Virginia
3. Graduated from MIT
4. 10 years of work experience
5. offered several high-ranking positions with a.o. Google, Lockheed Martin
6. Gained access to email and bank accounts; to personal documents; learning the location of secret military units based on Facebook photos of soldiers and connections between different people and organizations.
7. Got offers to speak at several conferences.

The truth? Robin Sage is a military exercise. The girl on the photograph is a porn star. Robin Sage was invented by Thomas Ryan (The Guardian, 24 july 2010).

3.2 Giving away identities

Facebook

Loosing your identity in Facebook.

A case of a Dutch diplomatic who is updating her status in Facebook:

(See figure ˜11)

Facebook 'friends' giving friendly advice :

(See figure ˜12)

(See figure ˜13)

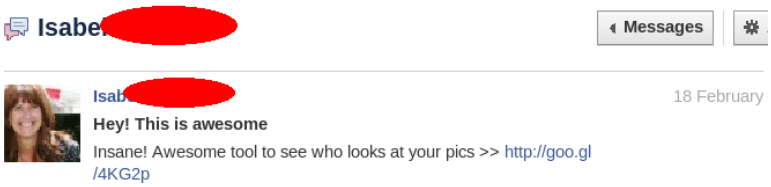


Figure 11: A 'lost' account in Facebook

Figure 12: Facebook sponsored 'likes'

Twitter

Loosing your identity in Twitter.

(See figure ~14)

(See figure ~15)

Twitter 'friends' giving friendly advice:

Friendly advice about my 'Blue Screen of Death'. Here is the original Tweet published by me on 20 Feb 2012 in the night somewere, and further down the responses.

(See figure ~16)

(See figure ~17)

Figure 13: Facebook sponsored 'likes' 2

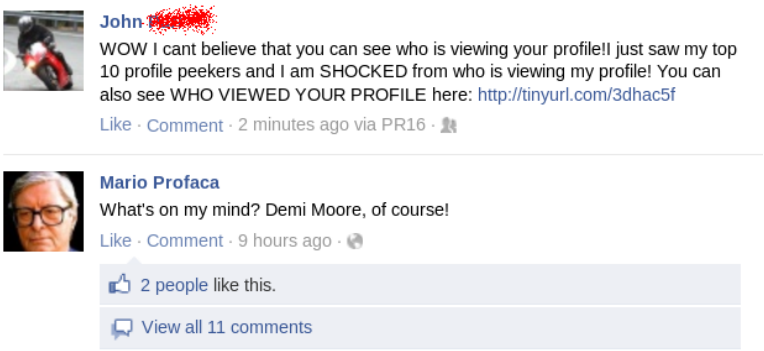


Figure 14: Advice from a friend, or not?

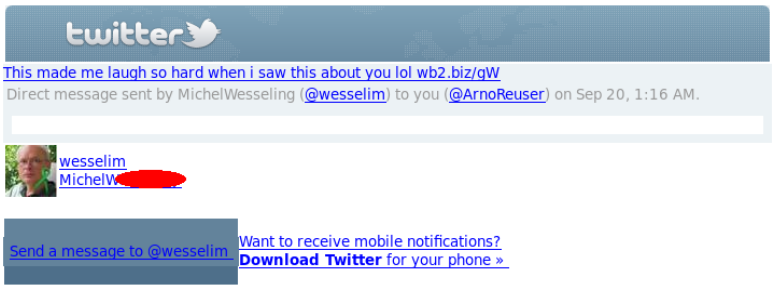


Figure 15: Another 'lost' or 'stolen' account

Figure 16: BSOD Tweet by Reuser

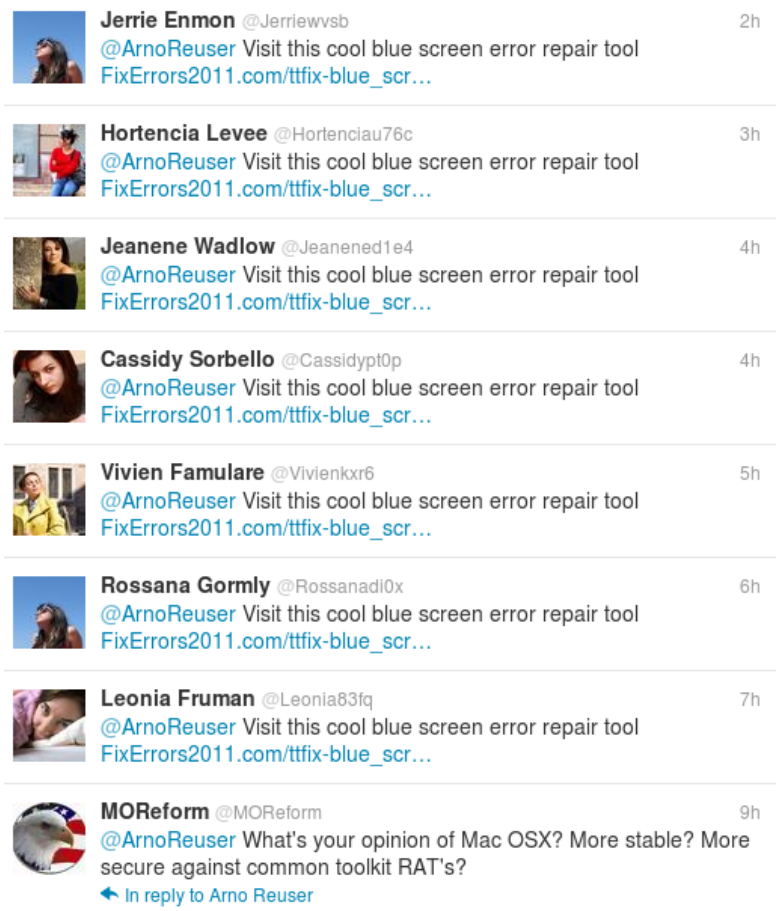


Figure 17: Twitter abused identities

4 Internet

4.1 IP numbering system

How do computers on a TCP/IP network 'find' eachother?

IP Numbers

Each and every device connected to the Internet has an IP number. A IP number consists of four 8 -bit integers connected by dots.

Examples:

```
193.10.14.71  - IP address
213.84.242.64    - IP address of your teacher
```

Addresses to remember

(See table˜1)

Table 1: Reserved IP numbers

IP address	Description
192.168.0.0	Start of a Class C private range. By convention used for Intranet and other private networks.
10.0.0.0	Same.
127.0.0.1	Loopback device (i.e., your own machine)
0.0.0.0	Reserved. Used when there is no connection to the Net. Also used for messages with unknown origin.

And more. See IANA

The organisation of IP addresses

The organisation and issuing of IP adresses needs to be carefully controlled.

There is one single organization responsible for the entire system, with five subordinate organizations.

(See figure ˜18)

Figure 18: Five Internet registries

(See table˜2)

Table 2: A hierarchy

Top	Regional registries	top level domains	ISP's
IANA	IP nos.	Domain names	
	ARIN		
	APNIC	.AF: Ministry of Communications and IT [11] .CN: Computer Network Information Center, Chinese Academy of Sciences [12] .PK: Star Joint Venture Company [13]	
	RIPE NCC	.IR: Institute for Research in Fundamental Sciences [14] .IT: ITT-CNR [15] .NL: SIDN [16] .UK: NomiNet UK [17]	
	LACNIC		
	AfriNIC		

IANA

IANA holds the IPv4 address space registry, the allocation of IP address space to various registries.

See: www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

Listing of Regional Registries [18] with list of countries of each.

[11] http://www.nic.af/
[12] http://www.cnnic.cn/
[13] http://www.star.co.kp/
[14] http://www.nic.ir/
[15] http://www.nic.it
[16] http://www.domain-registry.nl/
[17] http://www.nic.uk/
[18] http://www.iana.org/numbers/rirs.html

4.2 You and the Internet

Introduction

There are (many) other computers, nodes, WIFIs etc between your machine and the machine that you wish to go to. They all make a copy of your message(s).

Network topology may be represented by a Pyramid, like below.

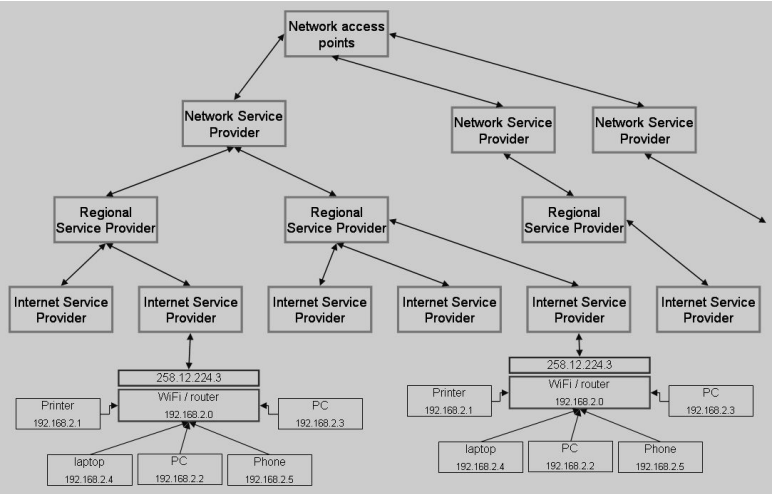


Figure 19: An Internet Pyramid

(See figure ˜19)

4.3 Traceroute

A tool that may come in handy sometimes

What does traceroute do?

1. Tool to display the root between the source computer (you) and the final destination
2. Lists all machine in between, names and IP addresses
3. Useful for validation purposes
4. Useful for reliability checks.

How to use?

1. Win7/XP: start - all programs - accessories - (DOS) command prompt

2. Type in: `tracert www.whitehouse.gov` [enter]
3. Linux: start a console and type in: `traceroute www.whitehouse.gov`

```
>tracert www.afghan.com

Tracing route to www.afghan.net [209.123.16.9]
over a maximum of 30 hops:

  1     *      841 ms   972 ms  e0.dr1.s340.xs4all.net [194.109.30.11]
  2   952 ms  1161 ms   972 ms  11.ge-0-2-0.xr1.s340.xs4all.net [194.109.30.1]
  3  1132 ms   971 ms   972 ms  0.ge-0-3-0.xr1.d12.xs4all.net [194.109.5.25]
  4   941 ms   962 ms   971 ms  0.so-6-0-0.xr1.tc2.xs4all.net [194.109.5.10]
  5  1131 ms   972 ms  1161 ms  amsix1.telecomplete.net [195.69.144.178]
  6  1171 ms   982 ms   961 ms  e0-44-r3.thn.telecomplete.net [193.0.255.1]
  7   981 ms   972 ms   971 ms  v100-r2.thn.telecomplete.net [213.160.96.54]
  8   952 ms   971 ms  1162 ms  267.ge-0-0-0.gbr1.ltn.nac.net [213.160.97.146]
  9  1192 ms   971 ms  1162 ms  0.ge-6-0-0.gbr2.oct.nac.net [209.123.11.50]
 10  1001 ms   981 ms  1172 ms  signature.visual.com [209.123.16.9]

Trace complete.
```

Figure 20: traceroute

(See figure ˜21)

4.4 Ping

A tool that may come in handy sometimes

What does Ping do?

1. Tool to send a 'ping' to a destination and get a reply back
2. To find out if you have a working Internet connection
3. To find out if a destination is online
4. To find a IP address for a DNS

How to use?

1. Win7/XP: start - all programs - accessories - (DOS) command prompt
2. Type in: `ping www.whitehouse.gov` [enter]
3. Linux: start a console and type in: `ping www.whitehouse.gov`

(See figure ˜21)

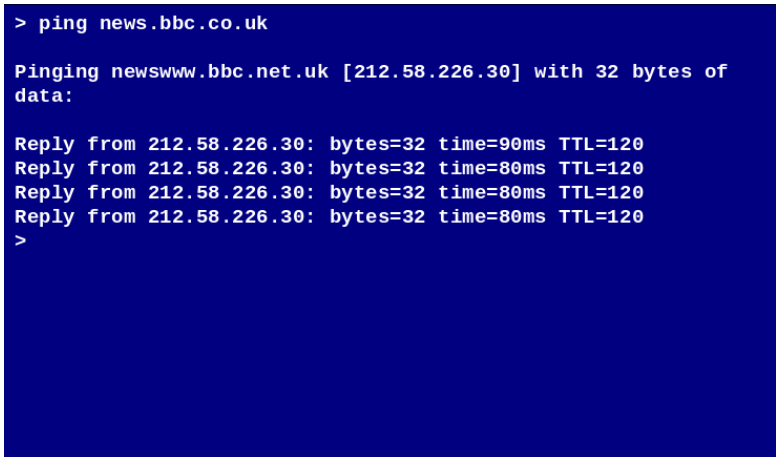


Figure 21: traceroute

5 Privacy anonymity

5.1 You own your own data

Who is the owner of your data? You?

AT&T

AT&T [19] owns all your data (offline [20]). Have a look at a anouncement about a change in privacy policy.

While your Account Information may be personal to you, these records constitute business records that are owned by AT&T. As such, AT&T may disclose such records to protect its legitimate business interests, safeguard others, or respond to legal process. Specifically, AT&T provides Account Information to collection agencies and/or credit bureaus. We may disclose your information in response to subpoenas, court orders, or other legal process, or to establish or exercise our legal rights or defend against legal claims. We may also use your information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of Service Terms or the Acceptable Use Policy, or as otherwise required or permitted by law. SecurityFocus 2006-06-30.pdf

LinkedIn

Here are a few extracts:

You grant LinkedIn a nonexclusive, irrevocable, worldwide, perpetual, unlimited, assignable, sublicenseable, fully paid up and royalty-free right to us to copy, prepare derivative works of, improve, distribute, publish, remove, retain, add, process, analyze, use and commercialize, in any way now known or in the future discovered, any information you provide, directly or indirectly to LinkedIn, including, but not limited to, any user generated content, ideas, concepts, techniques or data to the services, you submit to LinkedIn, without any further consent, notice and/or compensation to you or to any third parties. LinkedIn user agreement, section 2B, 2013

We use the information you provide to: [...] create and distribute advertising relevant to your or your network8217;s LinkedIn experience. If you share your interactions on LinkedIn, for example, when you recommend a product, follow a company, establish or update your profile, join a Group, etc., LinkedIn may use these actions to create social ads for your network on LinkedIn using your profile photo and name. LinkedIn Privacy Policy Highlights 2013

Twitter

"You retain your rights to any Content you submit, post or display on or through the Services. By submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt,

[19] AT&T: http://www.securityfocus.com/news/11398
[20] SecurityFocus2006-06-30.pdf

modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed)."

"You agree that this license includes the right for Twitter to provide, promote, and improve the Services and to make Content submitted to or through the Services available to other companies, organizations or individuals who partner with Twitter for the syndication, broadcast, distribution or publication of such Content on other media and services, subject to our terms and conditions for such Content use."

"Such additional uses by Twitter, or other companies, organizations or individuals who partner with Twitter, may be made with no compensation paid to you with respect to the Content that you submit, post, transmit or otherwise make available through the Services."

"We may modify or adapt your Content in order to transmit, display or distribute it over computer networks and in various media and/or make changes to your Content as are necessary to conform and adapt that Content to any requirements or limitations of any networks, devices, services or media."

(See Twitter Terms of Service, [chapter] 5 Your Rights, jan 2013

Facebook

Some want access to your name and picture to use on their behalf.

Friends Around the World

Figure 22: Facebook app Get Friend Map

(See figure ˜22)

Request for permission: post to Facebook as me: Get Friend Map may post status messages, notes, photos and videos on my behalf Page.me

Using Facebook and Skype

Here is the price you pay if you want to use Facebook via skype:

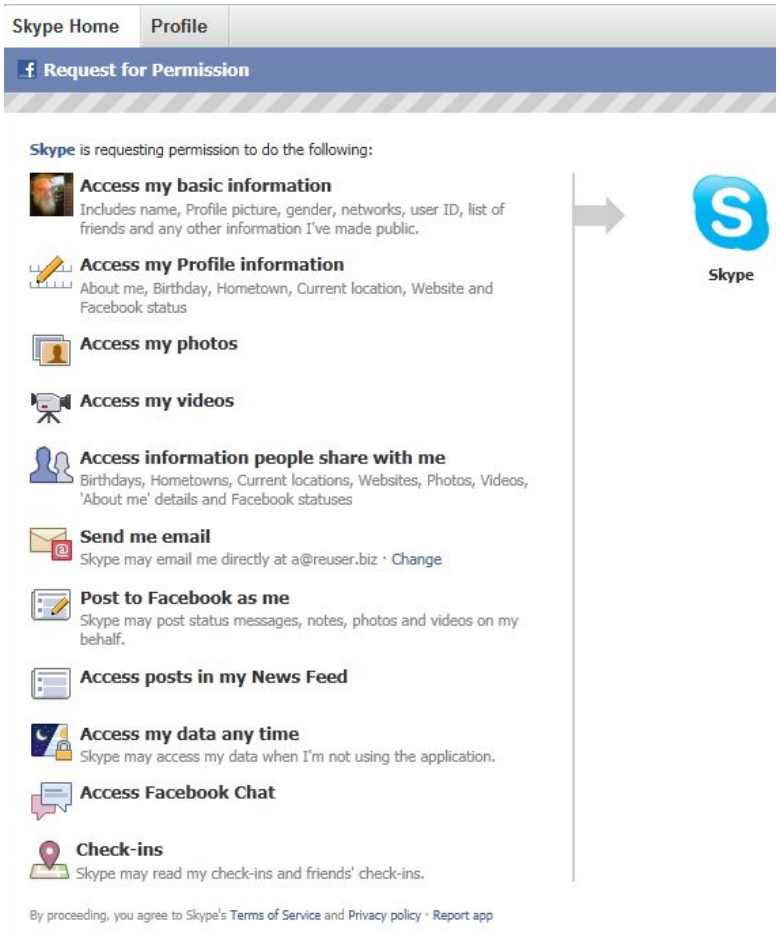


Figure 23: Using Facebook via Skype

(See figure ˜23)

6 Safe(r) searching

6.1 Prepare your machine

Get ready for searching by preparing your machine in order to get organised for research and to prevent leaving behind too many traces while searching the Net.

Organize your machine

1. Create a separate partition on your hard disk to hold all your data. Keep the partition with the operating system as clean as possible
2. Turn on automatic updates

   For your operating system as well as your software. This has its disadvantages (some providers are suspect of pushing all kinds of Beta software to their clients this way as a cheap means of advertising) but in general you are much safer this way.
3. Create a directory on your data partition called "All Downloads". Use this directory to 'dump' everything you download for later processing
4. In 'services', turn off all software or services that you do not need anyway (like bluetooth?)

'Cleaner' software

Download, install and use on a daily basis software to clean your machine from traces left behind while searching.

Such as: CCleaner [21] (Piriform).

Turn 'off' your machine

Turn your machine off once a day (prevent the 'sleep' mode) to allow the operating system to install patches and security updates.

Providers

Use multiple providers and change regularly. Do not always make use of the same one.

Email adresses

In addition to your normal email account, create a few extra email accounts, some with regular providers, some with free providers.

[21] CCleaner: http://www.piriform.com/ccleaner/download/standard

Create a bunch of aliases for some of the email adresses

Example:

1. a@reuser.biz : official address of Arno H.P. Reuser
2. harewood@xs4all.nl : address used by Arno to register with hotels, buy tickets, reserve accomodation, buy subscriptions, temporary access, etc.
3. nedbib@reuser.biz : used by Arno to administer the NEDBIB Listserv discussion list
4. dead.bishop@xs4all.nl : used by Arno for online games, other crap, silly things
5. (and many more)

Prepare the browser

Preferred browser: Mozilla Firefox. Worst browser: Microsoft Internet Explorer

1. Find, and turn on, the Browsers bookmark toolbar. Remove links you do not need from the toolbar
2. Make some bookmarks to often used website. Put some of these bookmarks on your bookmark toolbar for quick access
3. Turn the statusbar on
4. Install important add-ons, plug-ins, etc.
5. Turn the 'Download Directory' of your browser to the download directory you just created.

Recommended Add-on's for browsers

(See figure ˜24)

For Mozilla Firefox, use the following for author verification purposes:

1. Active Whois plugin for Firefox 3.0
2. DT Whois 1.7
3. FlagFox 4.1.13
4. Site Information Tool
5. WhoisDomain - All in One Site Lookup 3.0
6. WorldIP 2.2.0
7. Ghostery

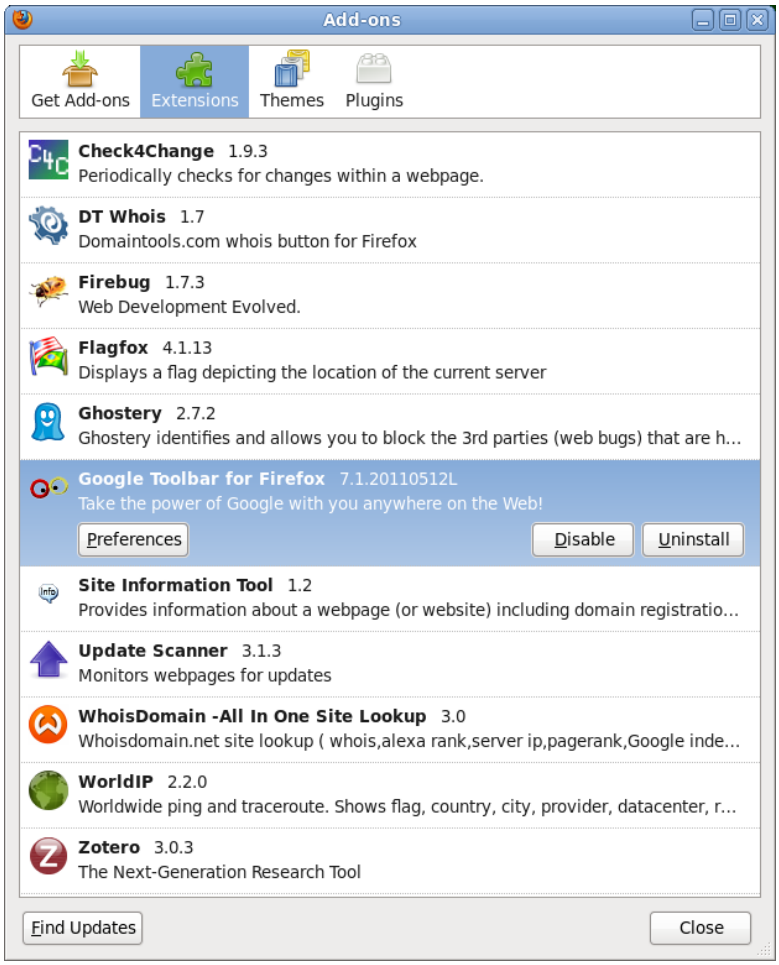


Figure 24: Mozilla Firefox Add-on's

Save your work

Use Reuser's Methods and management techniques to save your queries for future reference and forensic evidence.

Consider extra tools to save the webpages you have visited (also for evidence)

1. Scrapbook 1.5.5 [22]

   "ScrapBook is a Firefox extension, which helps you to save Web pages and easily manage collections. Key features are lightness, speed, accuracy and multi-language support. Major features are: * Save Web page * Save snippet of Web page * Save Web site * Organize the collection in the same way as Bookmarks * Full text search and quick filtering search of the collection * Editing of the collected Web page"

   In Mozilla Firefox, install Scrapbook from the Add-ons.

   (a) Scrapbook Plus 1.9.23.40

[22] Scrapbook 1.5.5: https://addons.mozilla.org/en-US/firefox/addon/scrapbook/

(b) Scrapbook AutoSave Improved 1.4.0

2. Zotero [23]

"Zotero is like a personal research assistant, inside your browser. It includes the following features, among others: Automatic capture of citation information from web pages ; Storage of PDFs, files, images, links, and whole web pages ; Flexible notetaking with autosave ; Fast, as-you-type search through your materials ; Playlist-like library organization ; Formatted citation export with thousands of popular publisher and journal styles available ; Tight integration with Microsoft Word and LibreOffice/OpenOffice via plugins ; Synchronize and back up your research library to zotero.org ; Create and share public or private research groups to collaborate with other Zotero users ; Automatically extract and identify metadata from PDFs ; Automatic support for library and other institutional proxy servers"

Privacy settings browsers

Browsers offer settings to safeguard your privacy

Figure 25: Mozilla Firefox Ghostery

(See figure ~25)

Mail signatures

Never use mail signatures.

Turn OFF the option to automatically decode and open attachments.

CD ROM / DVD

To experiment in a safe(r) way, do the following

1. Load and run your laptop with an operating system from DVD/CD

[23] Zotero: https://addons.mozilla.org/en-US/firefox/addon/zotero/?src=search

2. Use your laptop in a public place with a public WIFI
3. Or even, remove the hard disc

6.2 Where does an e-mail really come from?

By opening up the source of an email and examining the headers, one can identify the originating IP address. If lucky, this can be traced back to the originator by using some simple tools. It is called reverse IP engineering. Here's how.

An email, we won!

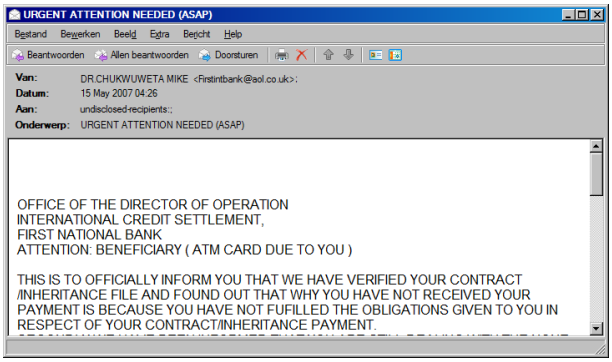


Figure 26: Phishing : first national bank

(See figure ˜26)

Open up the source file

Also called 'headers', or just 'source'. Differs per client, but in MS Outlook 2003 right click on the message title, then choose Options.

The website WHO@ [24] (WHOA, Working to Halt Online Abuse), has a list of about 30 email clients with for each client, how to get the headers.

(See figure ˜27)

which results in :

(See figure ˜28)

The headers

The e-mail headers look like the following:

[24] WHO@: http://haltabuse.org/help/headers/

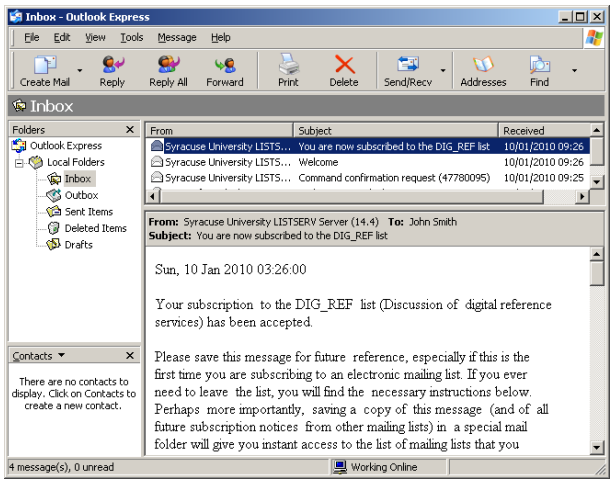


Figure 27: MS Outlook Express

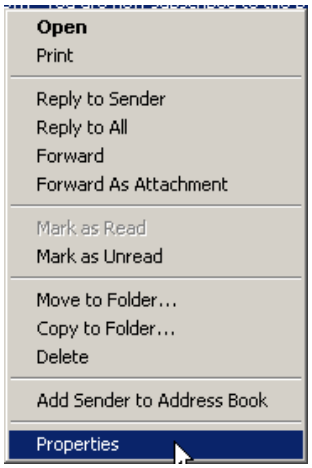


Figure 28: Clicking the right hand side mouse button

```
Return-Path: Firstintbank@aol.co.uk
Received: from Conwy.ReuserNET.nl (localhost.localdomain [127.0.0.1]) by
   localhost.localdomain (8.13.8/8.13.8) with ESMTP id l4FA0HSX003147
   for $<$reuser@localhost$>$; Tue, 15 May 2007 12:04:46 +0200
Received: from pop.xs4all.nl [194.109.6.55] by Conwy.ReuserNET.nl with
   POP3 (fetchmail-6.3.6) for $<$reuser@localhost$>$ (single-drop);
   Tue, 15 May 2007 12:04:46 +0200 (CEST)
Received: from mercury.worldispnetwork.com (mercury.worldispnetwork.com
   [216.219.94.71]) by mxdrop28.xs4all.nl (8.13.8/8.13.8) with SMTP id
   l4F2anB9014134 for $<$bibliothecaris@xs4all.nl$>$ Tue, 15 May 2007
   04:36:51 +0200 (CEST) (envelope-from Firstintbank@aol.co.uk)
Received: (qmail 83117 invoked by uid 398); 15 May 2007 02:26:35 -0000
Received: from 208.70.7.41 ([208.70.7.41]) by 216.219.94.71 (Horde MIME
   library) with HTTP; Mon, 14 May 2007 19:26:31 -0700
Message-ID: 20070514192631.l468c15vs4ks4g4c@216.219.94.71
```

```
Date: Mon, 14 May 2007 19:26:31 -0700
From: "DR.CHUKWUWETA MIKE " Firstintbank@aol.co.uk
Reply-to: ptroom23401@yahoo.com
To: undisclosed-recipients: ;
Subject: URGENT ATTENTION NEEDED (ASAP)
```

Reverse IP engineering

Use some publicly available tool such as Network tools [25] .

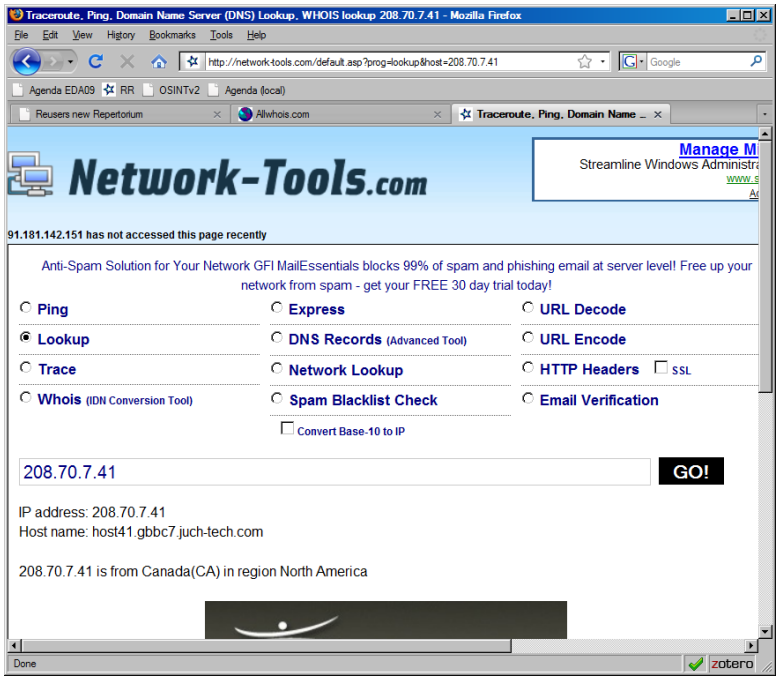


Figure 29: Network Tools for reverse IP engineering

(See figure ~29)

ARIN

At least you found the main region (Canada). Let go to the Regional Internet Registry of that region and try their WHOIS database to find more data. (offline) [26] (offline html [27]).

[25] Network tools: network-tools.com/
[26] ChukwuwetaARINoutput.pdf
[27] ARIN.html

6.3 Identifying Website owners/registrants

A domain name (and hence a website) must be registered via a local provider. The data registered is in the public domain in so called WHOIS services.

Why?

Consider http://www.washingtonmonument.com

It is strongly recommended to do a WHOIS check on every domain unknown to you.

1. To validate the data
2. To judge reliability
3. To identify hoax websites or fraud.

Required is some knowledge of the domain name system.

Example

Who is the registrant of http://www.reuser.biz?

(See figure ˜30)

WHOIS services

Plenty. Each Regional Internet Registry has one, each national registry has one for each country. In addition, there are many 'free' services offering WHOIS (or Domain Research). Have a look at Reuser's New Repertorium at the category of Internet tools [28] .

[28] Internet tools: http://rr.reuser.biz/internet tools

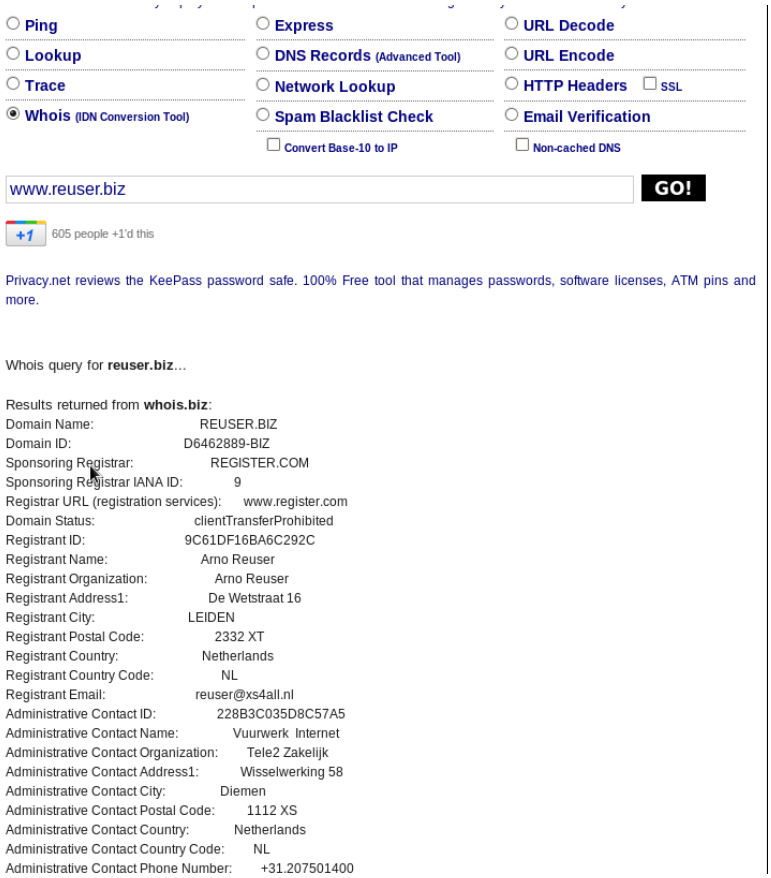


Figure 30: WHOIS Reuser

7 Searcher's behaviour

7.1 What happened to the Facebook login?

1. A website publishes an article about the cooperation between Facebook and AOL Instant Messenger
2. Users can use both services with a single login
3. The page ranks number one on Google when searching for "facebook login"
4. Hundreds of users mix up the article with Facebook Login page, and are most confused

Facebook wants to be your one true login [29] / Mike Melanson. - ReadWriteWeb, 10 February 2010.

(live link [30]) (Offline [31])

[29] FacebookLoginRWW.pdf
[30] http://www.readwriteweb.com/archives/facebook_wants_to_be_your_one_true_login.php
[31] facebook_wants_to_be_your_one_true_login.php.html

8 A little warning

8.1 A law

When to publish something online? (mail, queries, documents, ...)

A safe(r) publication law

IF: anything you publish can be retrieved:

1. By everybody and anybody
2. All over the world
3. For many, many years

AND: you consider the risc that the information you publish can hurt you is very low

THEN publish

ELSE wait OR stop OR end