



Velkommen til

# Sikkerhed - snifning på netværket

Flemming Jacobsen fj@batmule.dk  
Thomas Rasmussen thomas@gibfest.dk  
Henrik Lund Kramshøj hlk@kramse.org

**THECAMP.DK** - 7 open source days

# Plan for foredraget



Hvorfor? Sidste år :- ) - idag er det kun teknikken

BackTrack 5 Wireshark til primære demo

Sniffe - demoer POP3, FTP, m.v.

Løsninger og demoer: POP3S, SSL/TLS, IMAPS, SMTP over TLS osv.

Mere avanceret: OpenSSH tunnel med Open Source

VPN og SSL VPN - generelt, eksempel med OpenVPN,

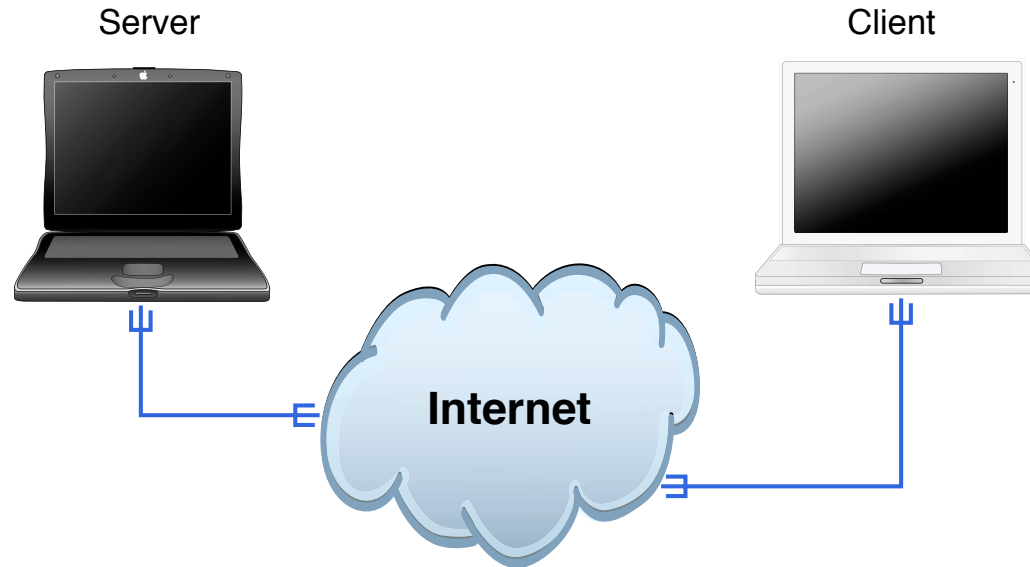
FileZilla

Advanced sniffing:

Tcpdump wizardry

Kismet demo

# Internet today

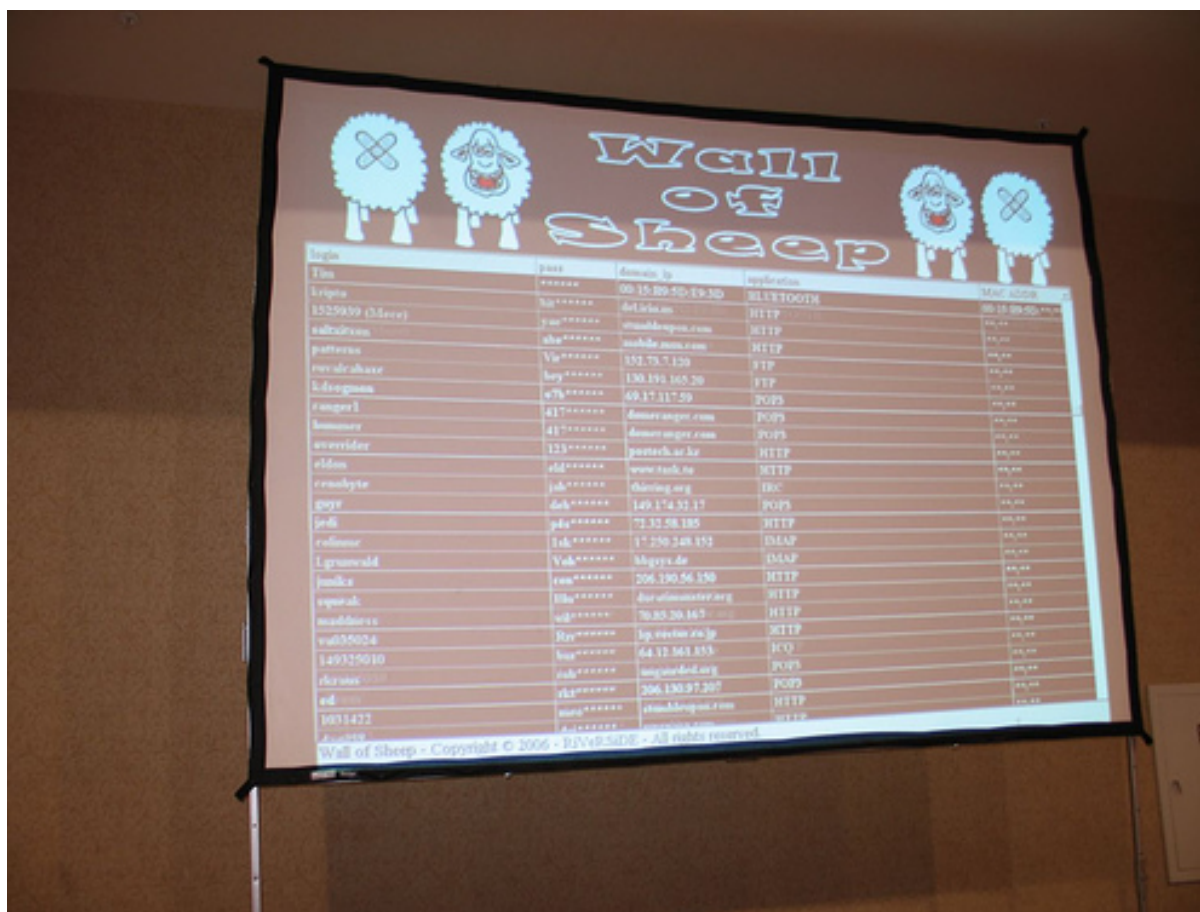


Clients and servers

Rooted in academic networks

Protocols which are more than 20 years old, moved to TCP/IP in 1981

# Hvorfor? Sidste års problemer :-)



login	pass	domain_ip	application	MAC address
Tim	*****	00-15-89-5D-E9-3D	BLUETOOTH	00-15-89-5D-E9-3D
krigen	kr*****	defcon.no	HTTP	00-15-89-5D-E9-3D
1325959 (3days)	kr*****	defcon.no	HTTP	00-15-89-5D-E9-3D
saltdescom	shp*****	saltdescom.com	HTTP	00-15-89-5D-E9-3D
patterns	Via*****	152.75.7.130	FTP	00-15-89-5D-E9-3D
revsdrakke	boy*****	130.193.165.20	FTP	00-15-89-5D-E9-3D
lidsognom	o7*****	49.17.117.59	POP3	00-15-89-5D-E9-3D
camper1	417*****	camperanger.com	POP3	00-15-89-5D-E9-3D
hammer	417*****	camperanger.com	POP3	00-15-89-5D-E9-3D
anovider	123*****	postech.ac.kr	HTTP	00-15-89-5D-E9-3D
elldon	elld*****	www.rack.se	HTTP	00-15-89-5D-E9-3D
crashbyte	jak*****	thawing.org	IRC	00-15-89-5D-E9-3D
goye	dak*****	149.174.32.17	POP3	00-15-89-5D-E9-3D
jedi	jak*****	72.32.58.185	HTTP	00-15-89-5D-E9-3D
collinsc	jak*****	17.230.248.151	IMAP	00-15-89-5D-E9-3D
lgrunwald	Vak*****	ldgoye.de	IMAP	00-15-89-5D-E9-3D
janika	ram*****	206.190.56.150	HTTP	00-15-89-5D-E9-3D
spatalk	lhu*****	lhu*****	HTTP	00-15-89-5D-E9-3D
madhorec	sig*****	70.85.20.167	HTTP	00-15-89-5D-E9-3D
vall36024	Ryz*****	lg.richmon.jp	HTTP	00-15-89-5D-E9-3D
149325010	huy*****	44.12.363.153	ICQ	00-15-89-5D-E9-3D
chrisus	zsh*****	angusdefcon.org	POP3	00-15-89-5D-E9-3D
ed	akl*****	206.190.97.207	POP3	00-15-89-5D-E9-3D
1031422	mar*****	camperanger.com	HTTP	00-15-89-5D-E9-3D

Wall of Sheep - Copyright © 2006 - RIV4R54DE - All rights reserved

## Defcon Wall of Sheep

Husk nu at vi er venner her! - idag er det kun teknikken



File Transfer Protocol - filoverførsler

Trivial File Transfer Protocol - uautentificerede filoverførsler

De bruges især til:

- FTP - drivere, dokumenter, rettelser - Windows Update? er enten HTTP eller FTP
- TFTP bruges til boot af netværksklienter uden egen harddisk

FTP sender i klartekst

**USER brugernavn** og

**PASS hemmeligt-kodeord**

# POP3 - e-mail i Danmark



POP3 sender brugernavn og kodeord i klartekst - ligesom FTP  
bruges dagligt af næsten alle privatkunder  
alle internetudbydere og postudbydere tilbyder POP3  
der findes en variant, POP3 over SSL/TLS

# BackTrack 5 og sniffer programmer



Wireshark - <http://www.wireshark.org> avanceret netværkssniffer  
bruger vi til at sniffe, vi bruger Wireshark til primære demo, nævner Ettercap osv.

BackTrack <http://www.backtrack-linux.org/>

# alle: Sniffe - demoer



Vi starter en sniffer

hvordan man henter post med POP3 og en FTP server

update af webhotel scenarier - vi bruger thecamp netværket





en sniffer til mange usikre protokoller

inkluderer **arpspoof**

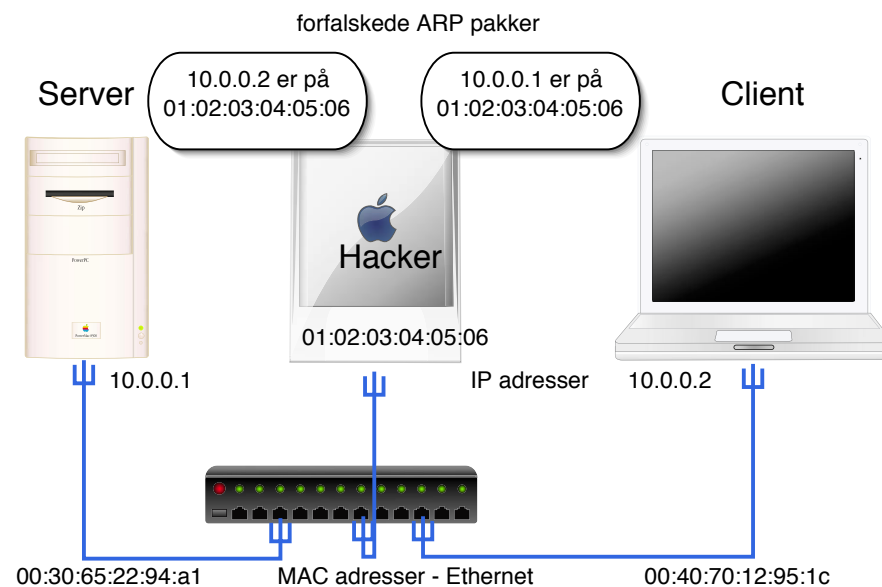
Lavet af Dug Song, [dugsong@monkey.org](mailto:dugsong@monkey.org)

dsniff is a password sniffer which handles FTP, Telnet, SMTP, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, PPTP MS-CHAP, NFS, VRRP, YP/NIS, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix ICA, Symantec pcAnywhere, NAI Sniffer, Microsoft SMB, Oracle SQL\*Net, Sybase and Microsoft SQL protocols.



Der er visse forudsætninger der skal være opfyldt

- Man skal have trafikken
- Det kan gøres gennem arp spoofing eller ved at hacke ind i et system/router på netværksvejen



# Kommenteret dsniff

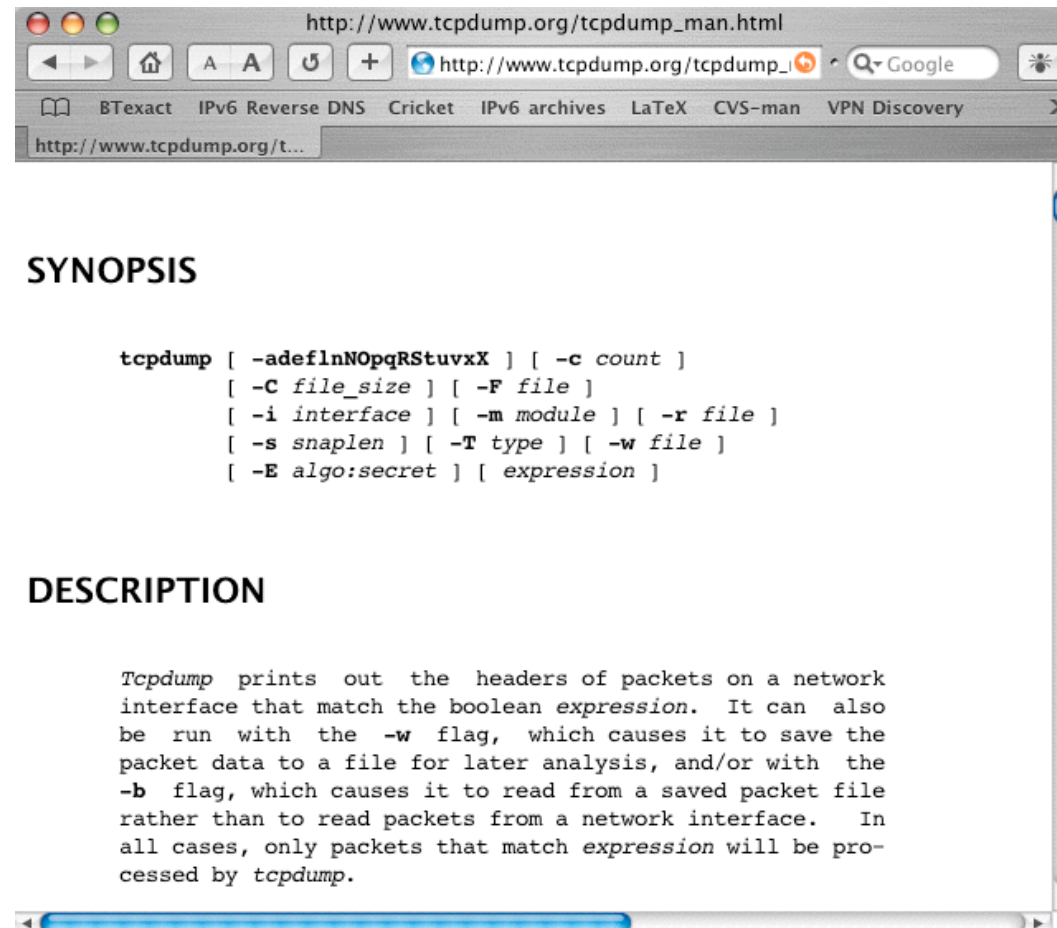


```
root@hlk: /home/hlk
[root@hlk hlk]# dsniff
dsniff: listening on fxp0
-----
05/20/03 08:53:38 tcp client.49154 -> server.110 (pop)
USER hlk
PASS secr3t!
-----
05/20/03 08:54:11 tcp client.49155 -> server.23 (telnet)
[poppe]

hlk
secr3t!
ls
exit
-----
05/20/03 08:55:33 tcp client.49156 -> server.23 (telnet)
[poppe]

an ja
anjnaan ja
an ja
```

# TCPDUMP - protokolanalyse pakkesniffer



<http://www.tcpdump.org> - både til Windows og UNIX

# tcpdump - normal brug



- tekstmode
- kan gemme netværkspakker i filer
- kan læse netværkspakker fra filer
- er de-facto standarden for at gemme netværksdata i filer

```
[root@otto hlk]# tcpdump -i en0
tcpdump: listening on en0
13:29:39.947037 fe80::210:a7ff:fe0b:8a5c > ff02::1: icmp6: router advertisement
13:29:40.442920 10.0.0.200.49165 > dns1.cybercity.dk.domain: 1189+[|domain]
13:29:40.487150 dns1.cybercity.dk.domain > 10.0.0.200.49165: 1189 NXDomain*+[|domain]
13:29:40.514494 10.0.0.200.49165 > dns1.cybercity.dk.domain: 24765+[|domain]
13:29:40.563788 dns1.cybercity.dk.domain > 10.0.0.200.49165: 24765 NXDomain*+[|domain]
13:29:40.602892 10.0.0.200.49165 > dns1.cybercity.dk.domain: 36485+[|domain]
13:29:40.648288 dns1.cybercity.dk.domain > 10.0.0.200.49165: 36485 NXDomain*+[|domain]
13:29:40.650596 10.0.0.200.49165 > dns1.cybercity.dk.domain: 4101+[|domain]
13:29:40.694868 dns1.cybercity.dk.domain > 10.0.0.200.49165: 4101 NXDomain*+[|domain]
13:29:40.805160 10.0.0.200 > mail: icmp: echo request
13:29:40.805670 mail > 10.0.0.200: icmp: echo reply
...
```

# TCPDUMP syntaks - udtryk



filtre til husbehov

- type - host, net og port
- src pakker med afsender IP eller afsender port
- dst pakker med modtager IP eller modtager port
- host - afsender eller modtager
- proto - protokol: ether, fddi, tr, ip, ip6, arp, rarp, decnet, tcp og udp

IP adresser kan angives som dotted-decimal eller navne

porte kan angives med numre eller navne

komplekse udtryk opbygges med logisk and, or, not

# tcpdump udtryk eksempler



Host 10.1.2.3

Alle pakker hvor afsender eller modtager er 10.1.2.3

host 10.2.3.4 and not host 10.3.4.5


Alle pakker til/fra 10.2.3.4 undtagen dem til/fra 10.3.4.5

- meget praktisk hvis man er logget ind på 10.2.3.4 via netværk fra 10.3.4.5

host foo and not port ftp and not port ftp-data

trafik til/fra maskine *foo* undtagen hvis det er FTP trafik

# Wireshark - grafisk pakkesniffer



The screenshot shows the Wireshark website homepage. At the top is a blue banner with the 'WIRESHARK' logo, which features a shark fin above the text. To the right of the logo is an image of a shark swimming in blue water. Below the banner is a navigation bar with links: HOME, ABOUT, WHAT'S NEW, DOWNLOAD, and FAQ. The main content area is divided into several sections. On the left is a sidebar with links under categories: 'Get It' (Download), 'Get Help' (FAQs, Documentation, Mailing Lists, Wiki, Bug tracker), 'Develop' (Developer Info), and 'Products' (AirPcap, Network Toolkit, OEM WinPcap). The central part of the page has a section titled 'Sniffing Problems A Mile Away' with text about the software's history and features, accompanied by a small screenshot of the Wireshark interface. To the right of this is a 'Download Now' box showing version '0.99.3'. Below the central text is a 'News' section titled 'Wireshark 0.99.3 Released' dated 'Aug 23, 2006', mentioning security fixes. On the far right is a Q&A section with a question about capturing 802.11 traffic and an answer, with the 'AirPcap' logo at the bottom.

**WIRESHARK**

HOME ABOUT WHAT'S NEW DOWNLOAD FAQ

**Get It**  
[Download](#)

**Get Help**  
[FAQs](#)  
[Documentation](#)  
[Mailing Lists](#)  
[Wiki](#)  
[Bug tracker](#)

**Develop**  
[Developer Info](#)

**Products**  
[AirPcap](#)  
[Network Toolkit](#)  
[OEM WinPcap](#)

**Sniffing Problems A Mile Away**

The Ethernet network protocol analyzer has changed its name to Wireshark.

The name might be new, but the software is the same. Wireshark's powerful features make it the tool of choice for network troubleshooting, protocol development, and education worldwide.

Wireshark was written by networking experts around the world, and is an example of the power of open source. It runs on Windows, Linux, UNIX, and other platforms.

**Download Now**  
0.99.3

**Q:**  
How do I capture 802.11 traffic on Windows?

**A:**

**News**  
**Wireshark 0.99.3 Released**  
Aug 23, 2006

Wireshark 0.99.3 has been released. Security-related vulnerabilities in the SCSI, DHCP, ESP, and Q.2931 dissectors have been fixed. See the [advisory](#) for details.

**AirPcap**

<http://www.wireshark.org>  
både til Windows og UNIX, tidligere kendt som Ethernet



# Programhygiejne!



Download, installer - kør! - farligt!

Sådan gøres det:

- download program OG signaturfil/MD5
- verificer signatur eller MD5
- installer
- brug programmet
- hold programmet opdateret!

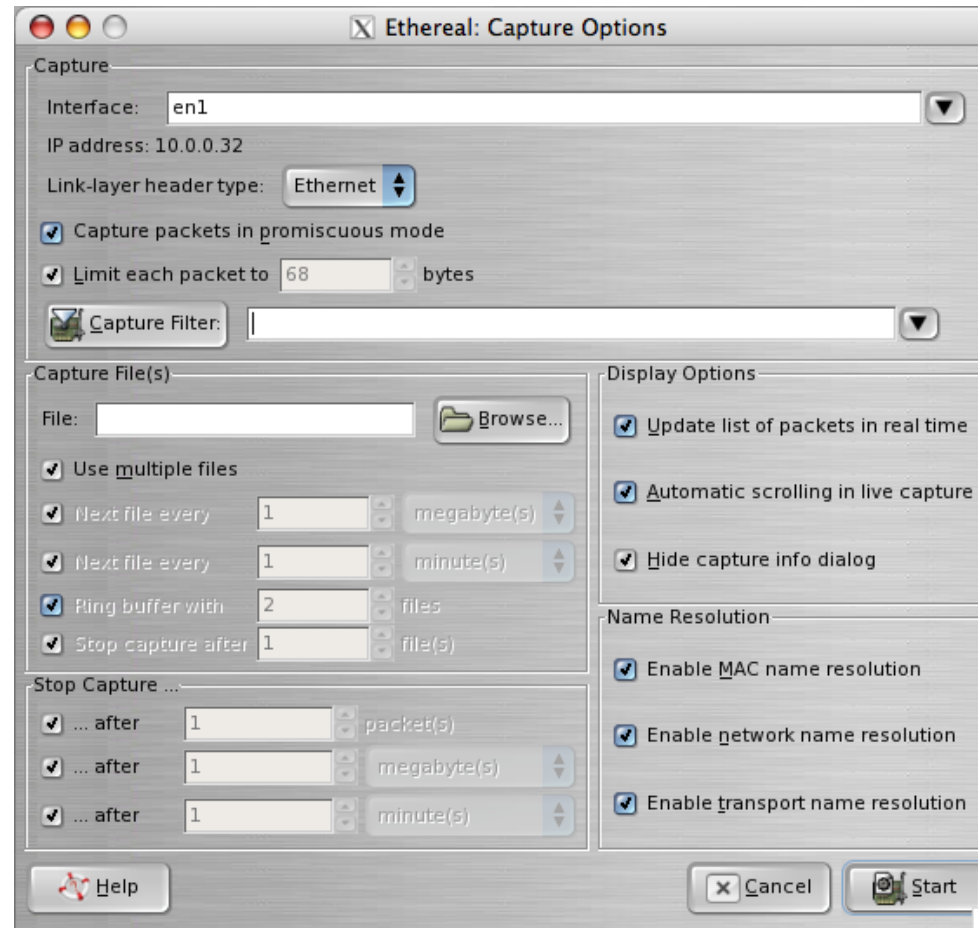
Se eksempelvis teksten på hjemmesiden:

*Wireshark 0.99.2 has been released. Several security-related vulnerabilities have been fixed and several new features have been added.*

NB: ikke alle programmer har signaturer :(

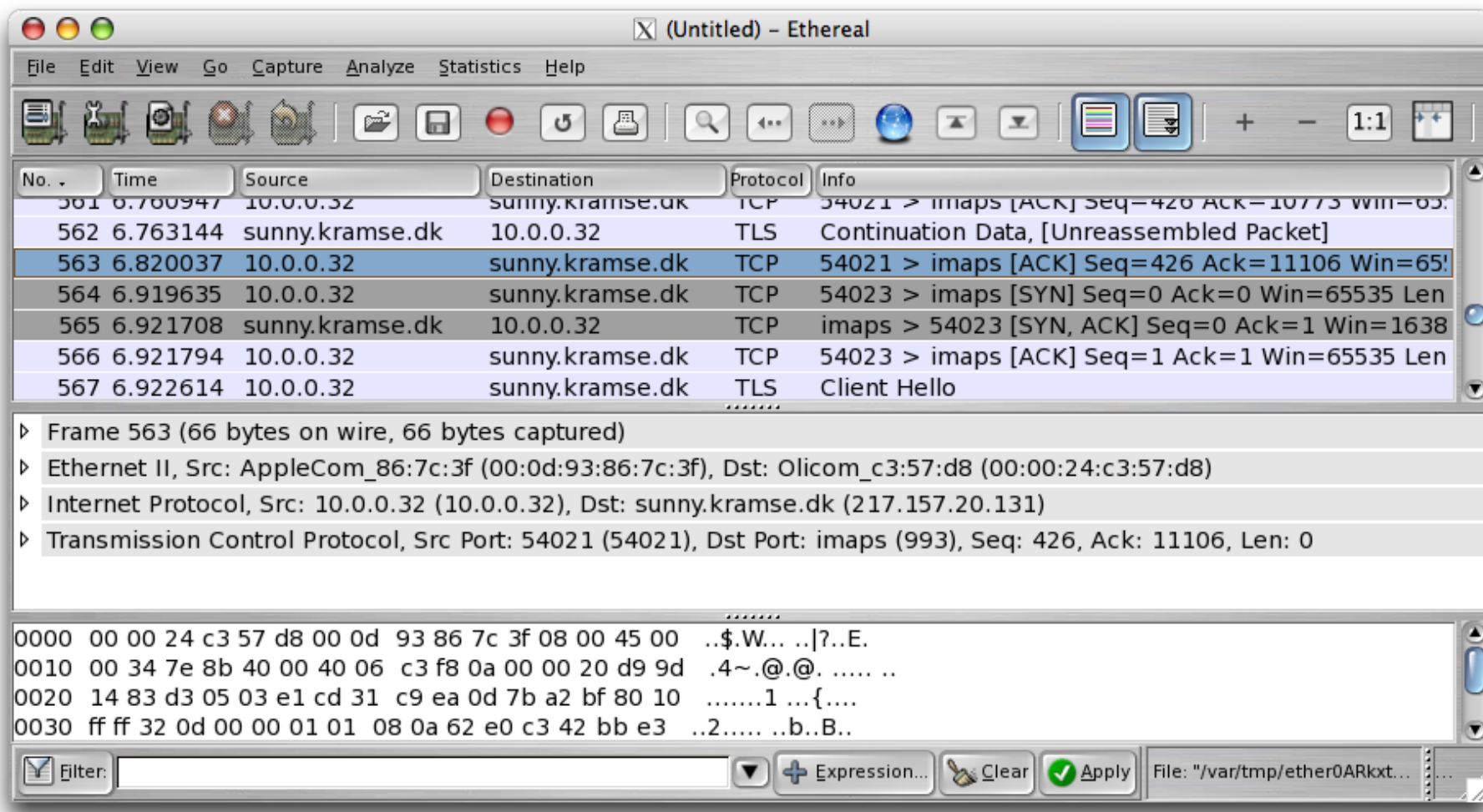
MD5 er en envejs hash algoritme - mere om det senere

# Brug af Wireshark

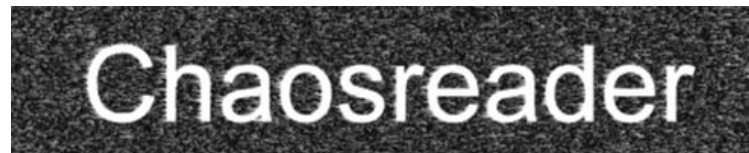


Man starter med Capture - Options

# Brug af Wireshark



Læg mærke til filtermulighederne



## Chaosreader Report

Created at: Sun Nov 16 21:04:18 2003, Type: snoop

[Image Report](#) - Click here for a report on captured images.

[GET/POST Report](#) (Empty) - Click here for a report on HTTP GETs and POSTs.

[HTTP Proxy Log](#) - Click here for a generated proxy style HTTP log.

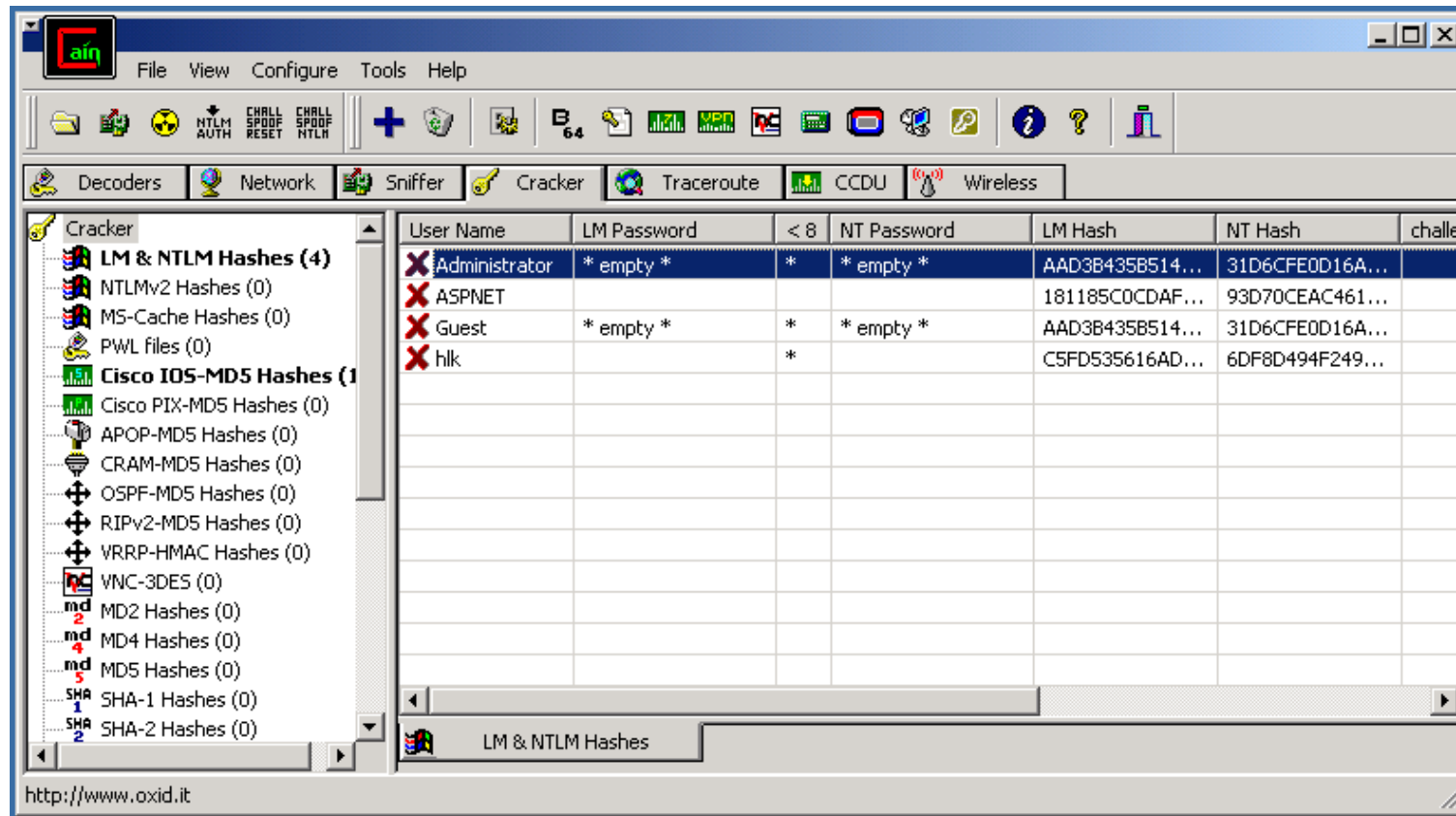
### TCP/UDP/... Sessions

1.	Sun Nov 16 20:38:22 2003	30 s	192.168.1.3:1368 <-> 192.77.84.99:80	web	383 bytes	• <a href="#">as_html</a>
2.	Sun Nov 16 20:38:22 2003	29 s	192.168.1.3:1366 <-> 192.77.84.99:80	web	381 bytes	• <a href="#">as_html</a>

Med adgang til et netværksdump kan man læse det med chaosreader

Output er HTML med oversigter over sessioner, billeder fra datastrømmen osv.

<http://chaosreader.sourceforge.net/>



Cain og Abel anbefales ofte istedet for l0phtcrack <http://www.oxid.it>

# Demo: løsninger



# kryptering, PGP og SSL/TLS



kryptering er den eneste måde at sikre:

- fortrolighed
- autenticitet

kryptering består af:

- Algoritmer - eksempelvis RSA
- *protokoller* - måden de bruges på
- programmer - eksempelvis PGP

fejl eller sårbarheder i en af komponenterne kan formindske sikkerheden

PGP = mail sikkerhed, se eksempelvis Enigmail plugin til Mozilla Thunderbird

Secure Sockets Layer SSL / Transport Layer Services TLS = webservere og klienter

# DES, Triple DES og AES/Rijndael



DES kryptering baseret på den IBM udviklede Lucifer algoritme har været benyttet gennem mange år.

Der er vedtaget en ny standard algoritme Advanced Encryption Standard (AES) som afløser Data Encryption Standard (DES)

Algoritmen hedder Rijndael og er udviklet af Joan Daemen og Vincent Rijmen.

**Kilder:** <http://csrc.nist.gov/encryption/aes/> - AES Homepage

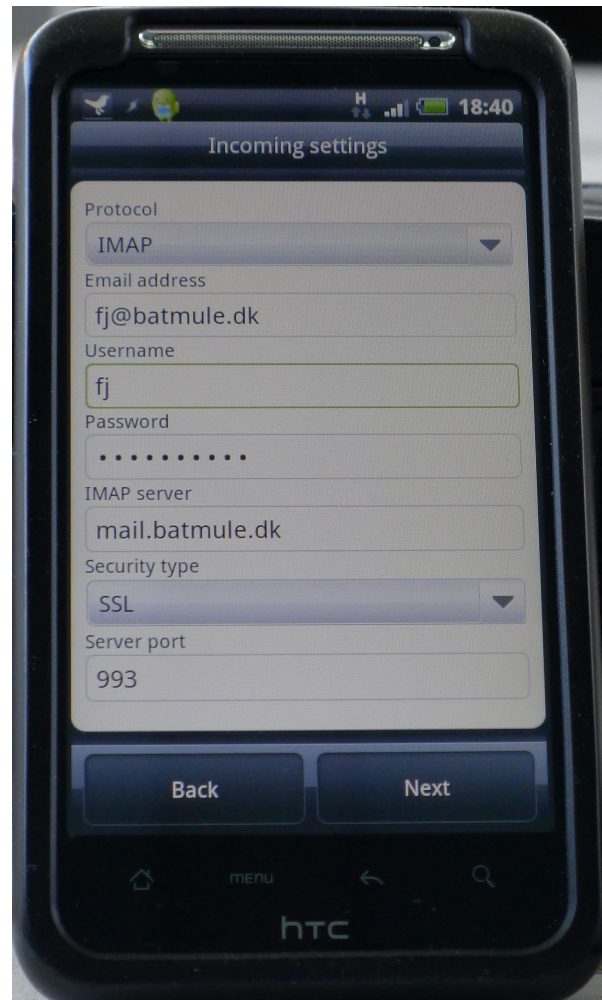
<http://www.esat.kuleuven.ac.be/~rijmen/rijndael/> - The Rijndael Page



# SSL/TLS (1)



Istedet for POP3 brug POP3s, Istedet for IMAP brug IMAPs



# Server, Dovecot

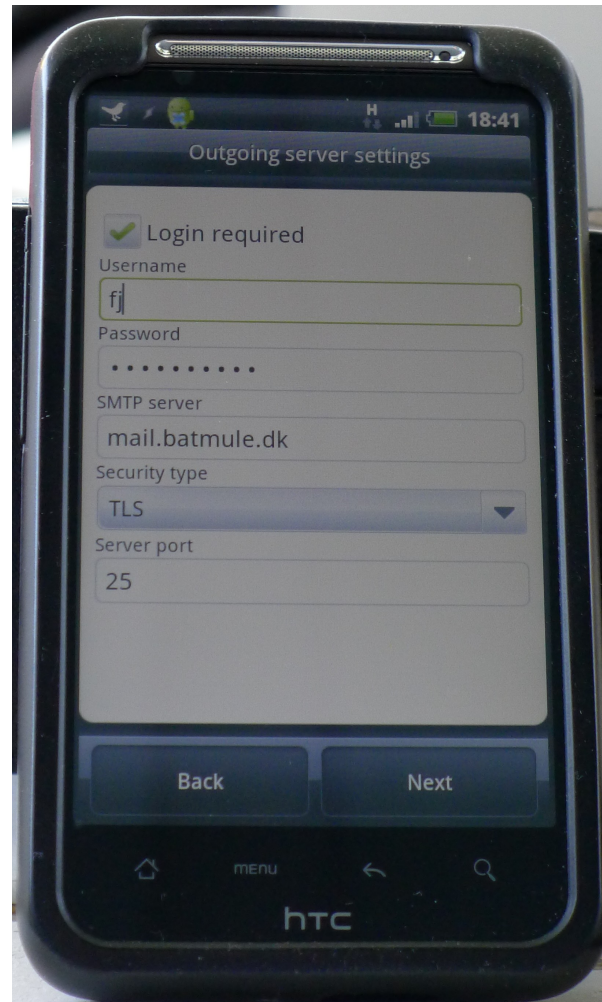


```
protocols = imaps pop3s          # Kun tillade crypt
listen = *, [::]                 # Også IPv6
disable_plaintext_auth = yes     # Ingen auth uden crypt
ssl_cert_file = /config/etc/Dovecot/cert.pem
ssl_key_file = /config/etc/Dovecot/cert.pem
auth default {
    passdb passwd-file {
        args = /config/etc/Dovecot/dovecot.passwd
    }
    userdb passwd-file {
        args = username_format=%n /config/etc/Dovecot/dovecot.passwd
    }
    user = nobody
    socket listen {              # Socket Postfix bruger for auth
        client {
            path = /var/spool/postfix/private/auth # modsvarer postfix conf
            mode = 0660
            user = postfix
            group = postfix
        }
    }
}
```

## SSL/TLS (2)



SMTP kan erstattes med SMTP+TLS



# Config til Server



Server, brug TLS hvis afsender supporterer det (Postfix):

```
# TLS settings
smtpd_tls_CAcert_file = /config/etc/Dovecot/ca.crt      # Certifikater,
smtpd_tls_cert_file = /config/etc/Dovecot/cert.pem     # hjemmelavede er fine
smtpd_tls_key_file = /config/etc/Dovecot/cert.pem
smtpd_tls_auth_only = yes                             # Tillad kun auth over TLS
smtpd_tls_received_header = yes                       # Log crypto i Recieved: header
smtpd_tls_security_level = may                        # Opportunistic TLS
smtpd_tls_loglevel = 1                                # Log i almindelige detaljer
```

Server, tillad relay hvis afsender er kendt (Postfix bruger Dovecot for auth info):

```
# SASL settings
smtpd_sasl_type = dovecot                             # Auth type
smtpd_sasl_path = private/auth                        # Modsvarer Dovecot conf.
smtpd_sasl_auth_enable = yes                          # Tillad relay, hvis bruger er auth'et
smtpd_sasl_authenticated_header = yes                 # Vis auth'et bruger navn i Recieved:
```

# Mere avanceret





SSH afløser en række protokoller som er usikre:

- Telnet til terminal adgang
- r\* programmerne, rsh, rcp, rlogin, ...
- FTP med brugernavn/passord

# SSH - de nye kommandoer er



kommandoerne er:

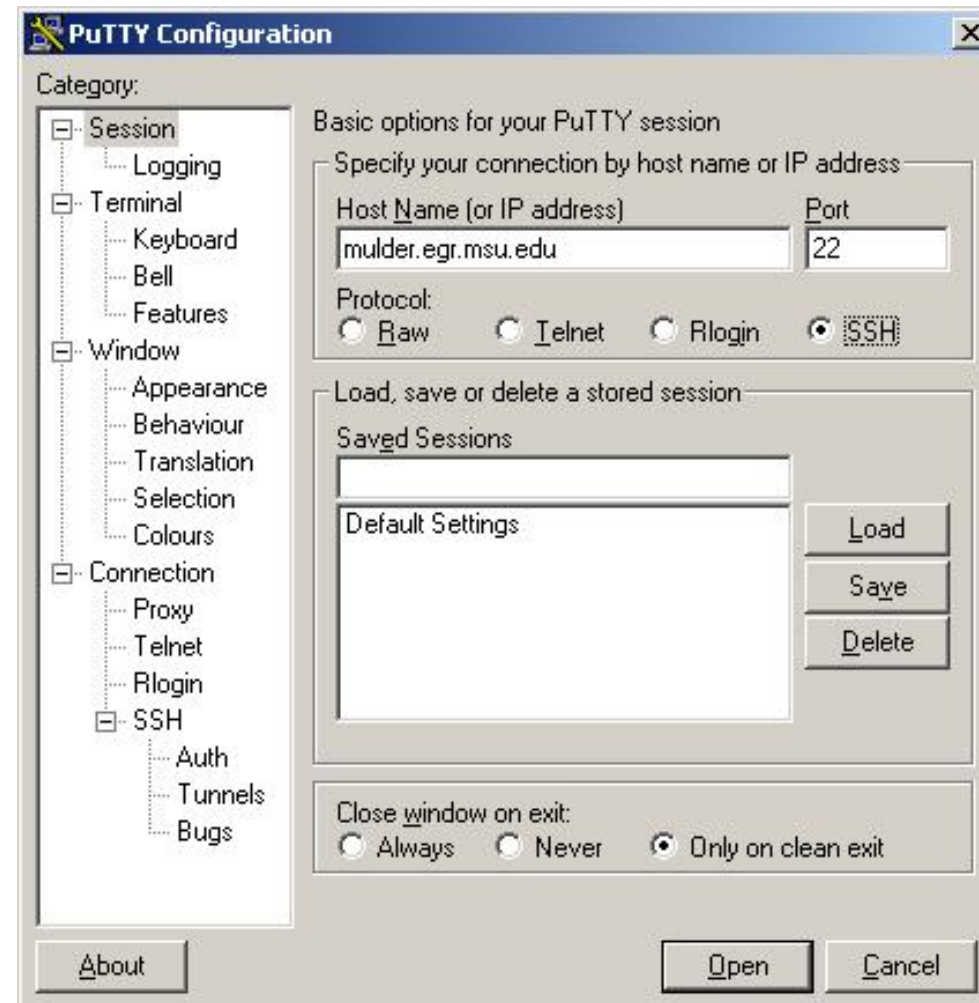
- ssh - Secure Shell
- scp - Secure Copy
- sftp - secure FTP

Husk: SSH er både navnet på protokollerne - version 1 og 2 samt programmet `ssh` til at logge ind på andre systemer

SSH tillader også port-forward, tunnel til usikre protokoller, eksempelvis X protokollen til UNIX grafiske vinduer

**NB: Man bør idag bruge SSH protokol version 2!**

# Putty en SSH til Windows



Login skærmen til Putty terminal programmet



# Putty terminaladgang



```
edu.muhos.fi - PuTTY
login as: wtestaaaj
Sent username "wtestaaaj"
wtestaaaj@edu.muhos.fi's password:
Last login: Thu Apr 18 11:55:44 2002 from yalu117164.muhos
[17.12.2001]
    Käyttäkää telnet- ja ftp-yhteyksien sijasta SSH:ta tietoturvallisuuden
    vuoksi. Lisätietoja http://edu.muhos.fi/opas/ssh

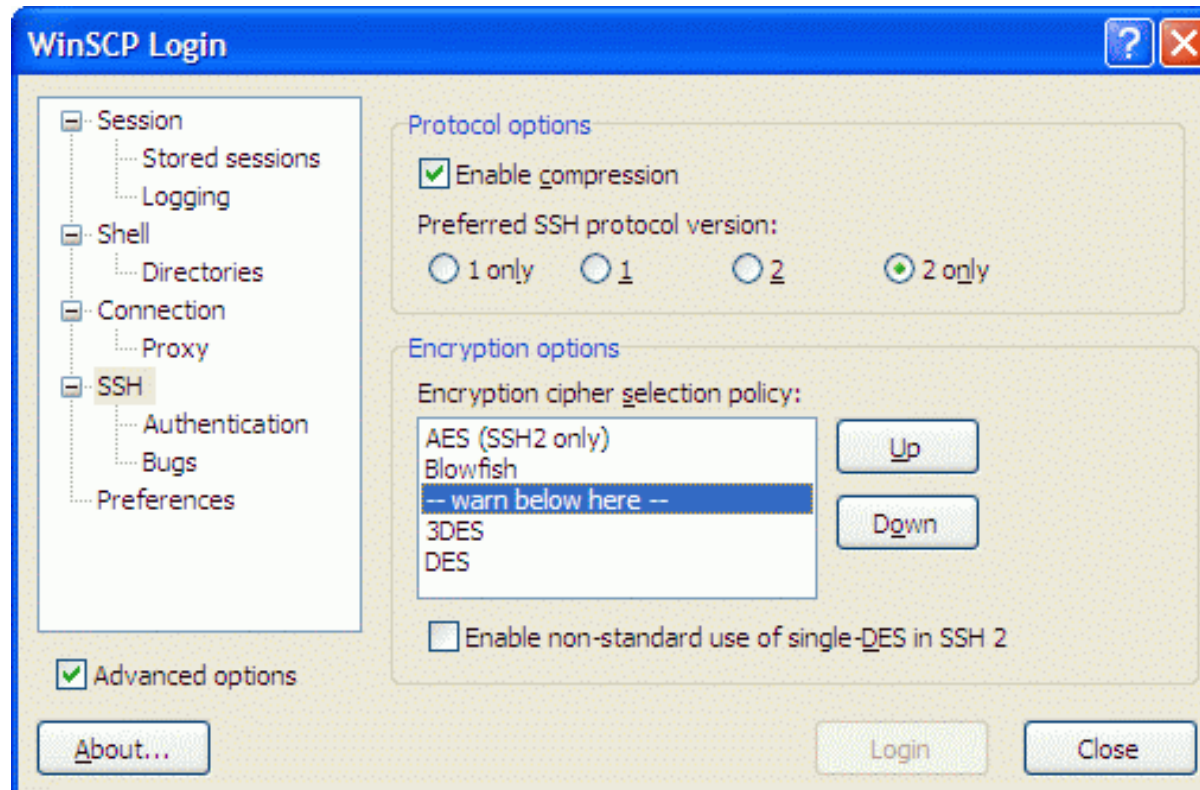
[15.01.2002]
    Salasanaa ei saa vaihtaa passwd-komennolla! Käyttäkää salasanan vaihtoon
    WWW-selainta osoitteessa https://edu.muhos.fi/salasana

[28.01.2002]
    VIRUSVAROITUS!! Älkää avatko sähköpostiviestiä, jonka otsikkona on:
    "new photos from my party!"

    Lisätietoa viruksesta:
    http://www.f-secure.fi/fin/support-page\_2002012800.shtml

Disk quotas for user wtestaaaj (uid 587):
   Filesystem  blocks   quota  limit  grace  files   quota  limit  grace
   /dev/sda10    56   60000 240000      0     11      0      0      0
[wtestaaaj@edu ~]$
```

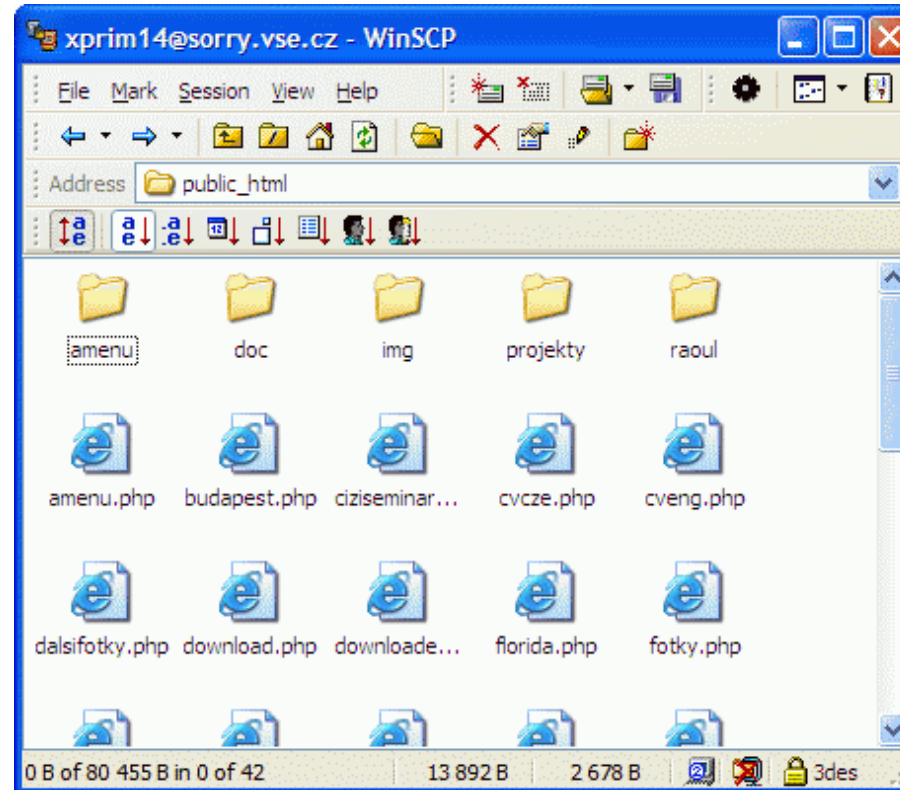
Billede fra <http://edu.muhos.fi/opas/ssh/putty-ohje.htm>



screenshot fra

<http://winscp.vse.cz/eng/screenshots/large/advanced.gif>

# Grafisk Secure Copy - WinSCP



screenshot fra

<http://winscp.vse.cz/eng/screenshots/large/explorer.gif>

# OpenSSH tunnel



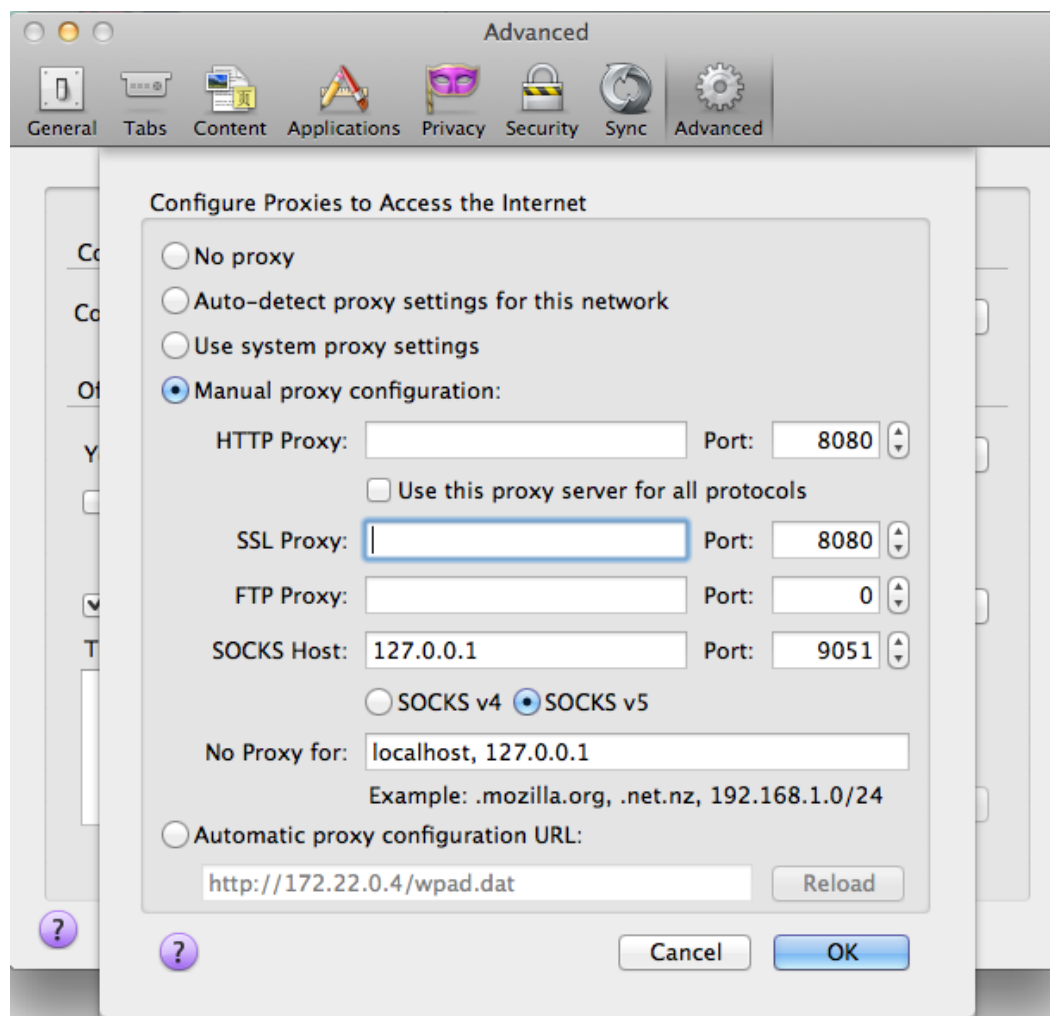
Nemt (når man har en server)

Sikkert, samme kryptering som SSH

Kræver at programmet understøtter socks 5 proxy

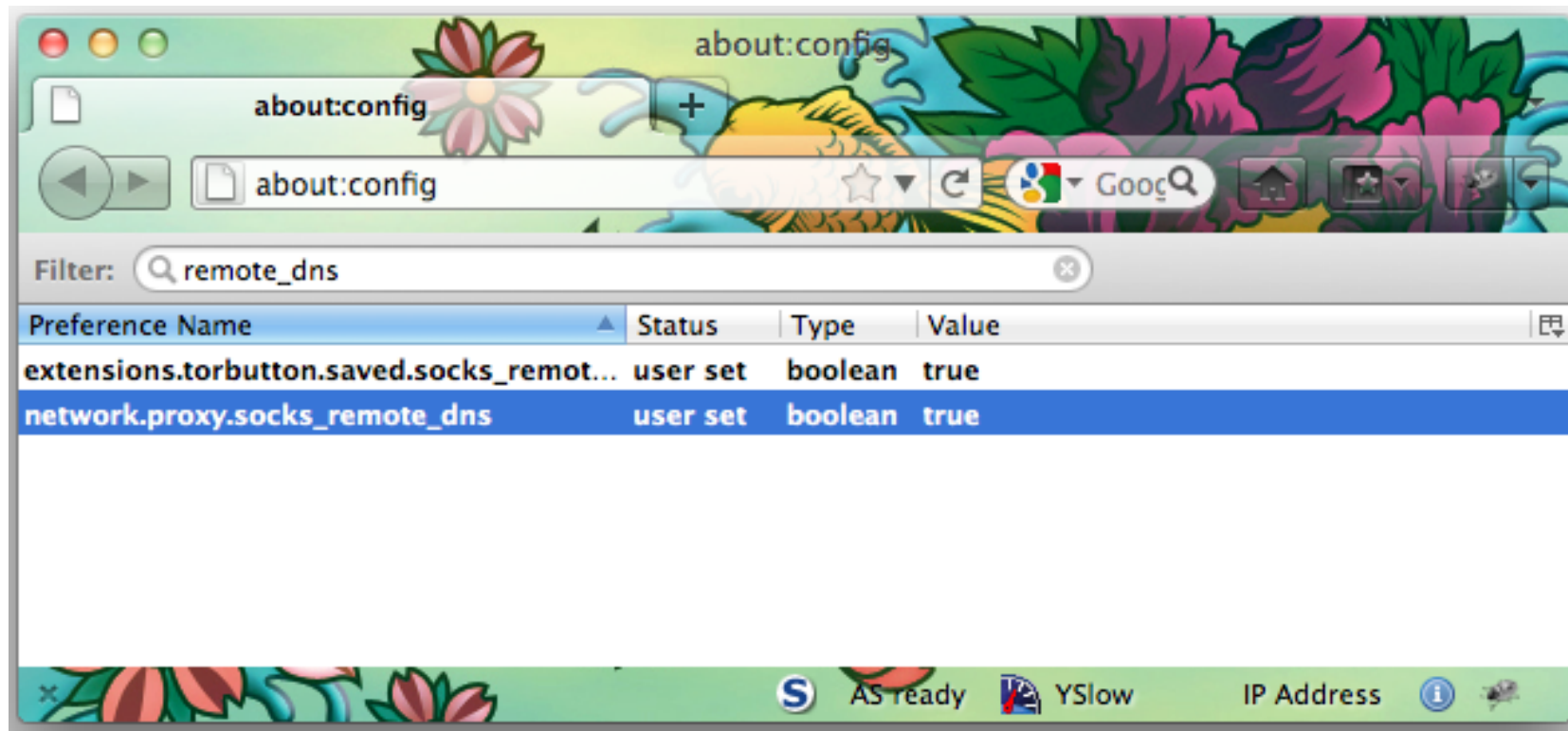
ssh -D 8080

# OpenSSH tunnel - Firefox konfig



Bemærk: F.eks. Thunderbird og Filezilla understøtter også socks 5 proxy

# OpenSSH tunnel - husk Firefox DNS konfig



er ikke default på alle platforme

# OpenSSH VPN



Lidt mere omstændigt at sætte op, men mere fleksibelt

Kræver ikke support fra hvert enkelt program

Kræver root på serveren der SSHes til (p.g.a. ifconfig)

`ssh -w 0`

# OpenSSH VPN - ifconfig



Direkte fra man ssh(1):

On the client:

```
# ssh -f -w 0:1 192.168.1.15 true
# ifconfig tun0 10.1.1.1 10.1.1.2 netmask 255.255.255.252
# route add 10.0.99.0/24 10.1.1.2
```

On the server:

```
# ifconfig tun1 10.1.1.2 10.1.1.1 netmask 255.255.255.252
# route add 10.0.50.0/24 10.1.1.1
```





VPN [http://en.wikipedia.org/wiki/Virtual\\_private\\_network](http://en.wikipedia.org/wiki/Virtual_private_network)

SSL/TLS VPN - Generelt koncept. Adskillige leverandører: Cisco, Juniper, F5 Big IP

De snakker ikke ret godt sammen på tværs. Brug IPSec for dette.

IPsec er desværre blokeret mange steder og man skal bruge en klient  
(I praksis bruger SSL VPN ofte en klient, men den downloades fra web)

Open source variant: OpenVPN

# OpenVPN server config



Server konfiguration:

```
port 4500                                # Port der lyttes på.
                                           # Kun een ad gangen er supporteret :-(
proto udp                                # TCP i TCP er ikke godt
ca keys/ca.crt                           # CA public key. Denne har signeret alle
                                           # klienters cert og serverens.
cert keys/server.crt                     # Server cert, public key
key keys/server.key                       # Server cert, private key
server 10.1.13.0 255.255.255.0            # Det net VPN klienter får IP på
push "route 10.1.0.0 255.255.0.0"        # Mit interne netværk
[Resten default]
```

# OpenVPN server status



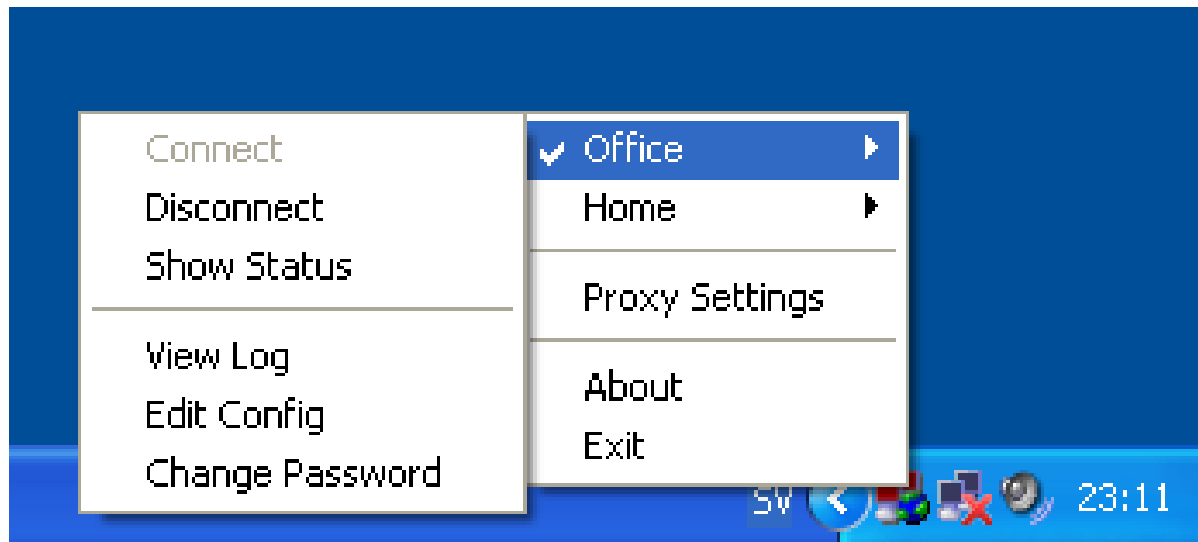
```
# cat openvpn-status.log
OpenVPN CLIENT LIST
Updated,Tue Jul 26 12:57:13 2011
Common Name,Real Address,Bytes Received,Bytes Sent,Connected Since
heartofgold,80.160.242.134:25313,1146127,1358645,Sun Jul 24 12:32:38 2011
guide2,80.160.242.134:52650,464241,509289,Mon Jul 25 17:07:22 2011
ROUTING TABLE
Virtual Address,Common Name,Real Address,Last Ref
10.1.13.6,heartofgold,80.160.242.134:25313,Tue Jul 26 10:40:51 2011
10.1.13.10,guide2,80.160.242.134:52650,Tue Jul 26 09:12:44 2011
GLOBAL STATS
Max bcast/mcast queue length,0
END
#
```

# OpenVPN client config



Klient konfiguration:

```
remote aftern.batmule.dk 4500      # Server og port
proto udp
ca ca.crt                          # Cert stuff (tilsvarende server)
cert guide2.crt
key guide2.key
[Resten default]
```



OpenVPN GUI on Windows



## FileZilla Features

### ◆ Overview

FileZilla Client is a fast and reliable cross-platform FTP, FTPS and SFTP client with lots of useful features

### ◆ Features

Among others, the features of FileZilla include the following:

- Easy to use
- Supports FTP, FTP over SSL/TLS (FTPS) and SSH File Transfer Protocol (SFTP)
- Cross-platform. Runs on Windows, Linux, \*BSD, Mac OS X and more
- IPv6 support
- Available in many languages
- Supports resume and transfer of large files >4GB
- Tabbed user interface
- Powerful Site Manager and transfer queue
- Bookmarks
- Drag & drop support
- Configurable transfer speed limits

<http://filezilla-project.org/>

# Advanced sniffing - Tcpdump / windump



tcpdump(1) har en lang række "primitives" som bruges til filtrere, se man pcap-filter(7) for mange flere:

src, dst, host, ether, net, port, icmp, tcp, udp, ip, arp, broadcast

tcpdump(1) understøtter også bit-matching i pakker:

For at vise pakker hvor bit 5 i byte 11 er 0 (binært 00001000):

```
tcpdump 'udp[11] & 8 = 0'
```

Eksempel fra wiki.tyk.nu som kun matcher dynamic DNS update queries:

```
tcpdump port 53 and 'udp[10] & 128 = 0' and 'udp[10]  
& 64 = 0' and 'udp[10] & 32 = 32' and 'udp[10]  
& 16 = 0' and 'udp[10] & 8 = 8'
```

# Trådløse teknologier 802.11



802.11 er arbejdsgruppen under IEEE

De mest kendte standarder idag indenfor trådløse teknologier:

- 802.11b 11Mbps versionen
- 802.11g 54Mbps versionen
- 802.11n endnu hurtigere, og draft
- 802.11i Security enhancements

Der er proprietære versioner 22Mbps og den slags

- det anbefales IKKE at benytte disse da det giver vendor lock-in - man bliver låst fast

Kilde: <http://grouper.ieee.org/groups/802/11/index.html>

# Kismet - wireless sniffing



Fra man-siden: Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic.

Kismet kan for eksempel anvendes når man vil finde en wlan kanal hvor der er lidt ro

Kismet gemmer som default al trafik på alle kanaler i "tcpdump-format"

Kismet gør det nemt for alle at sniffe på et trådløst netværk

f.eks. Wireshark eller Chaosreader kan bruges til at snage yderligere i trafik opsamlet med Tcpdump / Kismet



# Questions?



Flemming Jacobsen fj@batmule.dk  
Thomas Rasmussen thomas@gibfest.dk  
Henrik Lund Kramshøj hlk@kramse.org

**THECAMP.DK** - 7 open source days