Крипто-вечеринка

dmitri@equalit.ie

6765 11E9 33AC 3F9D 1A4B 0AAC 7110 EACE 6FF1 895D

https://equalit.ie/cp

eQualitie

DIGITAL SECURITY FOR CIVIL SOCIETY

Free. Open Source. Principled.

CENO

DEFLECT

WEB SECURITY

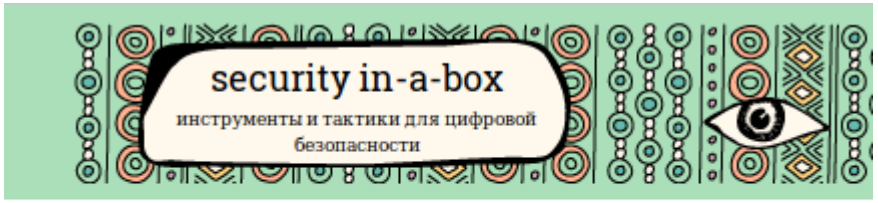
ORGANIZATIONAL SECURITY

SOFTWARE DEVELOPMENT

https://equalit.ie

@equalitie

https://securityinabox.org/ru



Рекомендации Linux Windows

SURVEILLANCE SELF-DEFENSE

СОВЕТЫ, ИНСТРУМЕНТЫ И РУКОВОДСТВА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ОНЛАЙНОВЫХ КОММУНИКАЦИЙ.

ПРОЕКТ ELECTRONIC FRONTIER FOUNDATION

https://ssd.eff.org/ru

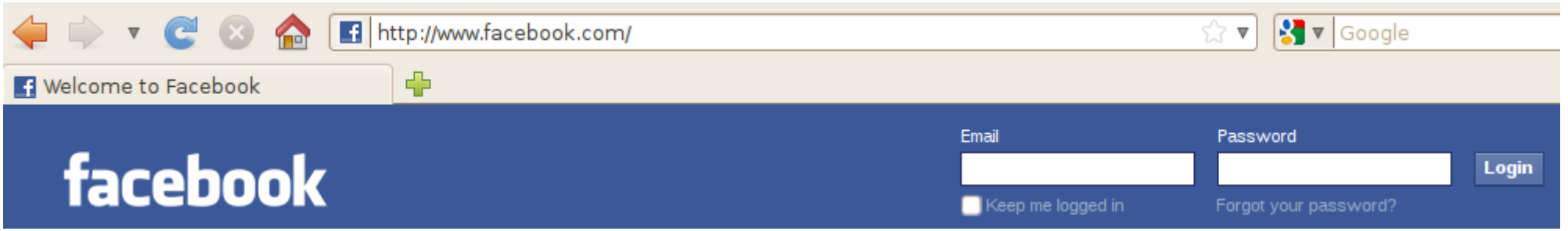
https://safe.roskomsvoboda.org

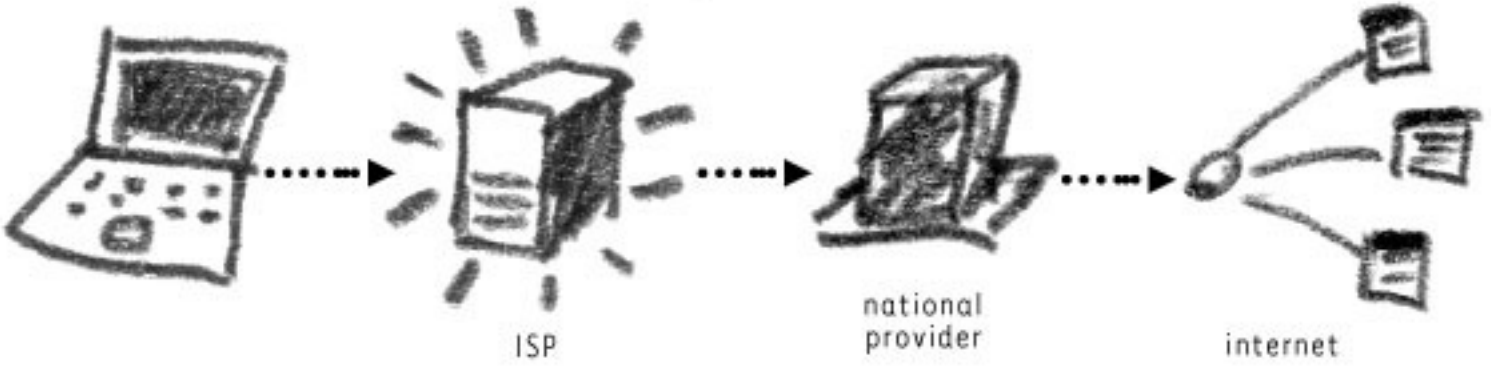
DIGITAL FIRST AID KIT

https://digitalfirstaid.org/ru

PRISM BREAK

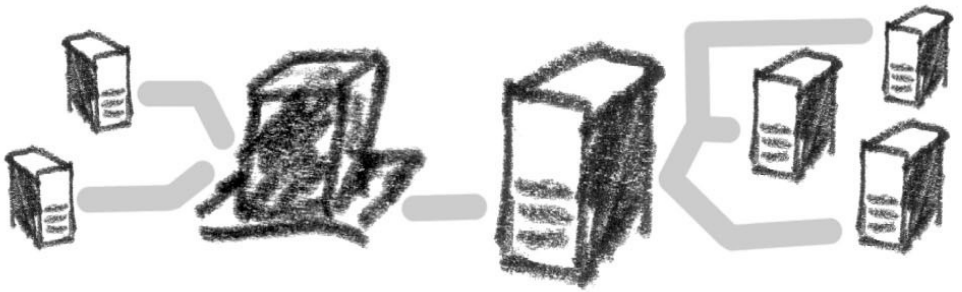
https://prism-break.org/ru





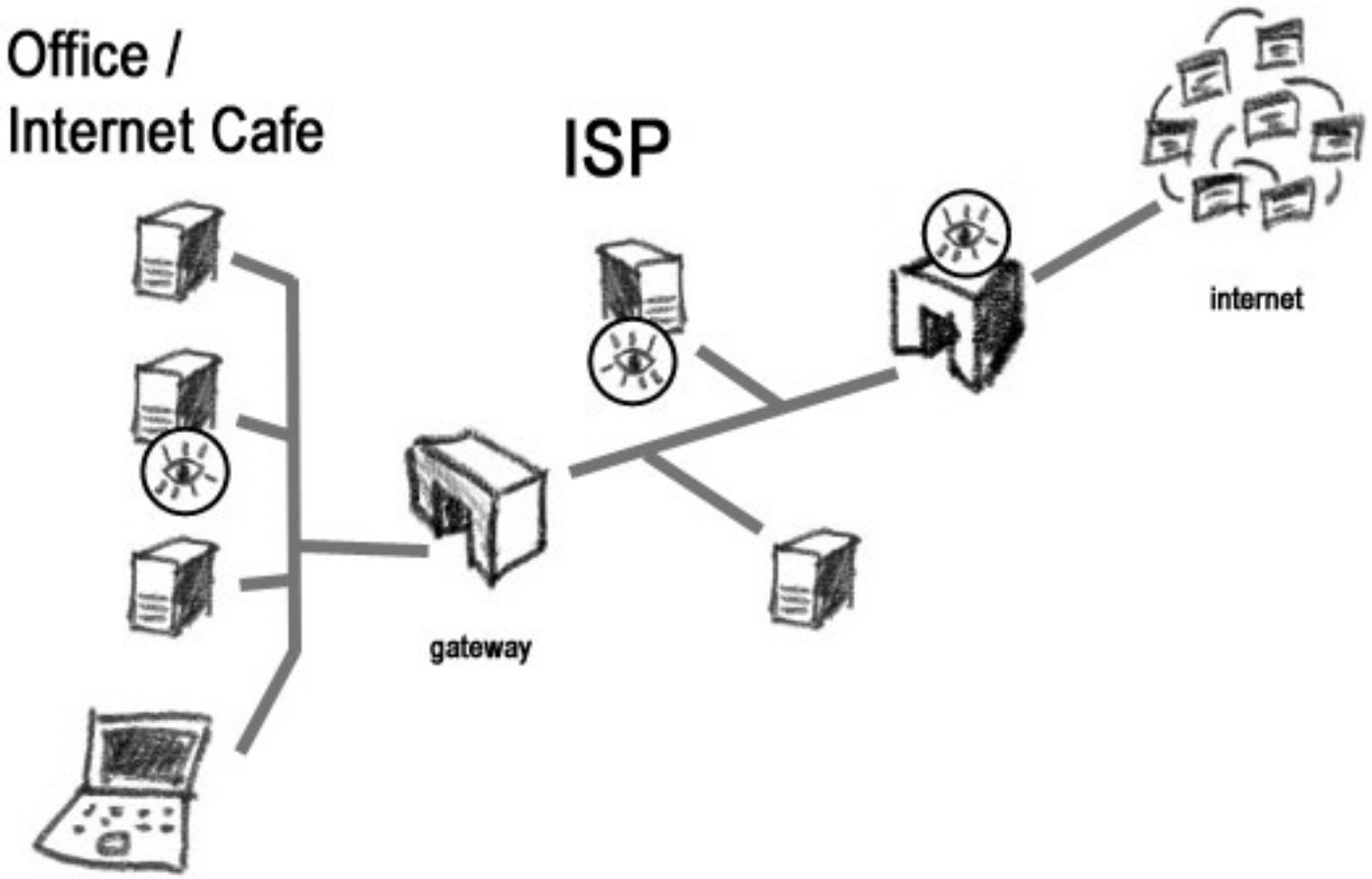
IP ADDRESS = 172.68.50.36

Content and application standards

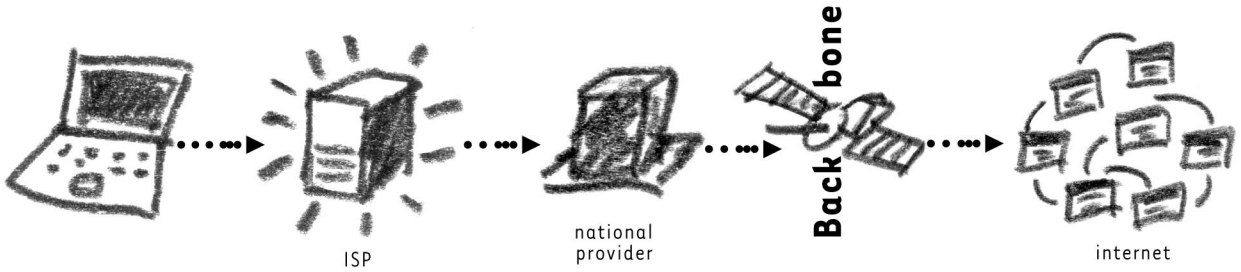


Technical standards (TCP, IP, DNS etc.)

Telecommunication infrastructure



IP ADDRESS = 172.68.50.36



No.	Time	Source	Destination	Protocol	Info
131	46.503857	192.168.1.11	euroradio.fm	HTTP	POST /admin/do_login.php HTTP/1.1 (application/x-w
133	46.796971	euroradio.fm	192.168.1.11	HTTP	HTTP/1.1 302 Found
135	46.953024	192.168.1.11	euroradio.fm	HTTP	GET /admin/index.php HTTP/1.1
230	48.877844	euroradio.fm	192.168.1.11	HTTP	HTTP/1.1 200 OK (text/html)
268	49.850529	192.168.1.11	euroradio.fm	HTTP	GET /javascript/JSCookMenu/ThemeOffice/theme.css HT
275	50.010763	euroradio.fm	192.168.1.11	HTTP	HTTP/1.1 200 OK (text/css)
282	50.488101	192.168.1.11	euroradio.fm	HTTP	GET /css/sign_big3.gif HTTP/1.1
287	50.613311	euroradio.fm	192.168.1.11	HTTP	HTTP/1.1 200 OK (GIF89a)
312	50.954657	192.168.1.11	euroradio.fm	HTTP	GET /css/tol.gif HTTP/1.1
328	51.070983	euroradio.fm	192.168.1.11	HTTP	HTTP/1.1 200 OK (GIF89a)
329	51.073215	192.168.1.11	euroradio.fm	HTTP	GET /css/logout.png HTTP/1.1
350	51.292112	euroradio.fm	192.168.1.11	HTTP	HTTP/1.1 200 OK (PNG)
126	46.334935	192.168.1.11	euroradio.fm	TCP	hb-engine > http [SYN] Seq=0 Win=65535 Len=0 MSS=14
127	46.381720	euroradio.fm	192.168.1.11	TCP	http > hb-engine [SYN, ACK] Seq=0 Ack=1 Win=5840 Le
128	46.382226	192.168.1.11	euroradio.fm	TCP	hb-engine > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
129	46.382661	192.168.1.11	euroradio.fm	TCP	[TCP segment of a reassembled PDU]
130	46.503694	euroradio.fm	192.168.1.11	TCP	http > hb-engine [ACK] Seq=1 Ack=594 Win=6523 Len=0

Follow TCP Stream

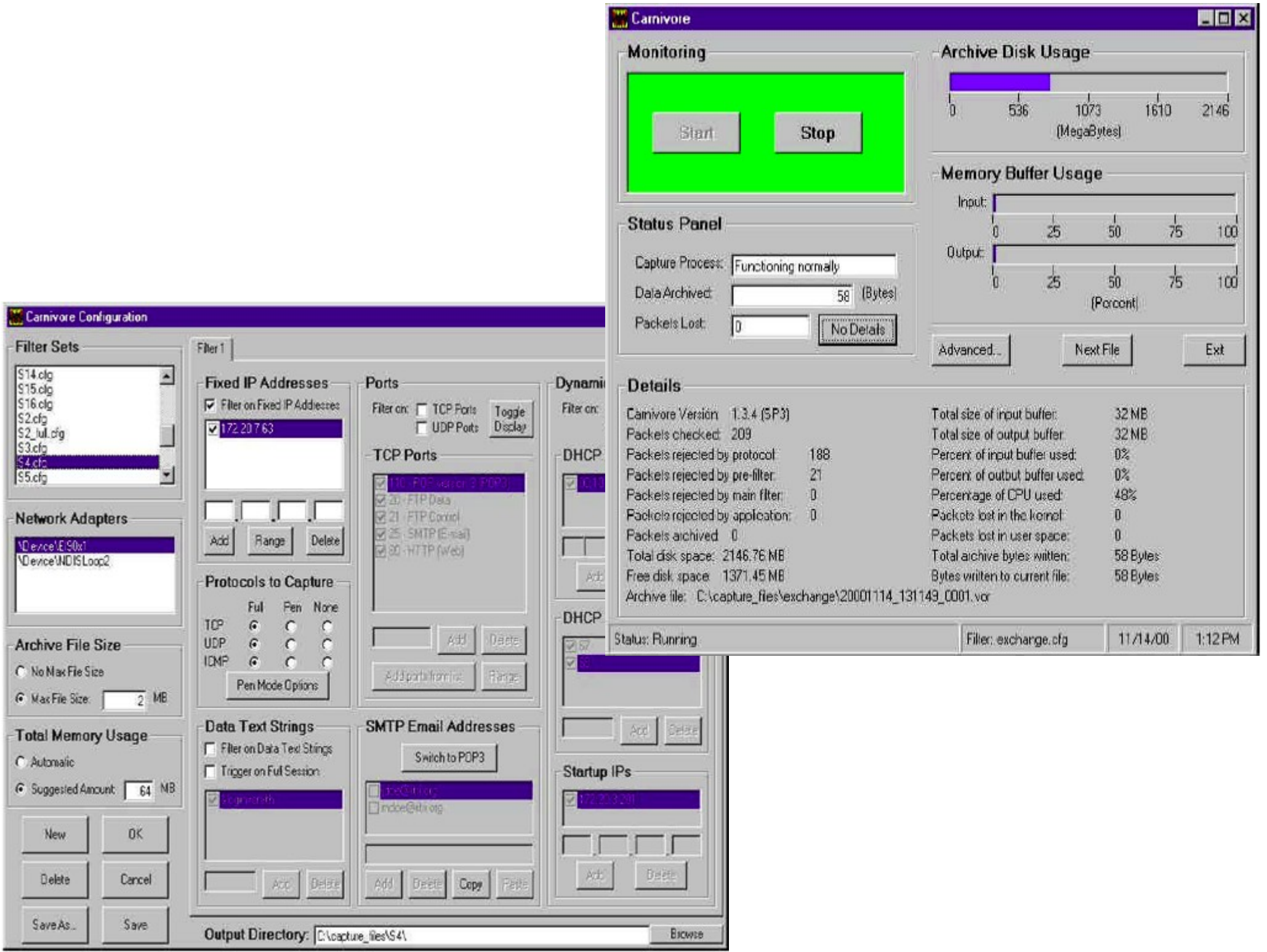
Stream Content

```
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://euroradio.fm/admin/login.php
Cookie: PHPSESSID=48e3ed080d2e50510271cca2131f7334
Content-Type: application/x-www-form-urlencoded
Content-Length: 170

f_is_encrypted=1&f_user_name=dmvit&f_password=KyFzt8fOfkGGeeU0fc&f_login_language=en&Login=Login&f_xkoery=f14314bf4d4a1b
302 Found
Date: Mon, 14 Jul 2008 08:04:59 GMT
Server: Apache/2.0.55 (Ubuntu) PHP/5.1.2
X-Powered-By: PHP/5.1.2
Set-Cookie: PHPSESSID=48e3ed080d2e50510271cca2131f7334; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

Find | Save As | Print | Entire conversation (103685 bytes) | ASCII | EBCDIC | Hex Dump | C Arrays | Raw

Help | Close | Filter Out This Stream


Carnivore
Monitoring
Start
Stop
Archive Disk Usage
0
536
1073
1610
2146
(MegaBytes)
Memory Buffer Usage
Input:
Output:
0
25
50
75
100
(Percent)
Status Panel
Capture Process:
Functioning normally
Data Archived:
58
(Bytes)
Packets Lost:
0
No Details
Advanced...
Next File
Exit
Details
Carnivore Version: 1.3.4 (SP3)
Packets checked: 209
Packets rejected by protocol: 188
Packets rejected by pre-filter: 21
Packets rejected by main filter: 0
Packets rejected by application: 0
Packets archived: 0
Total disk space: 2146.76 MB
Free disk space: 1371.45 MB
Total size of input buffer: 32 MB
Total size of output buffer: 32 MB
Percent of input buffer used: 0%
Percent of output buffer used: 0%
Percentage of CPU used: 48%
Packets lost in the kernel: 0
Packets lost in user space: 0
Total archive bytes written: 58 Bytes
Bytes written to current file: 58 Bytes
Archive file: C:\capture_files\exchange\20001114_131149_0001.vor
Status: Running
Filter: exchange.cfg
11/14/00
1:12 PM
Carnivore Configuration
Filter Sets
S14.cfg
S15.cfg
S16.cfg
S2.cfg
S2_lul.cfg
S3.cfg
S4.cfg
S5.cfg
Network Adapters
\Device\E90x1
\Device\NDISLoop2
Archive File Size
No Max File Size
Max File Size: 2 MB
Total Memory Usage
Automatic
Suggested Amount: 64 MB
New
OK
Delete
Cancel
Save As...
Save
Filter 1
Fixed IP Addresses
Filter on Fixed IP Addresses
172.20.7.63
Add
Range
Delete
Protocols to Capture
Full
Pen
None
TCP
UDP
ICMP
Pen Mode Options
Ports
Filter on: TCP Ports
UDP Ports
Toggle Display
TCP Ports
20 - FTP Data
21 - FTP Control
25 - SMTP (E-mail)
80 - HTTP (Web)
Add
Delete
Add ports from list
Range
Data Text Strings
Filter on Data Text Strings
Trigger on Full Session
Add
Delete
SMTP Email Addresses
Switch to POP3
Add
Delete
Copy
Paste
Dynami
Filter on:
DHCP
Add
Delete
DHCP
Add
Delete
Startup IPs
Add
Delete
Output Directory: C:\capture_files\S4\
Browse

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Tasking Process

ONYX

CARNIVORE

ECHELON

Titan

ECHELON intercept station at Menwith Hill, England

Project 6

SORM-2

Golden shield

NATGRID

PRISM +

XKeyscore

Frenchelon

MUSCULAR

TEMPORA

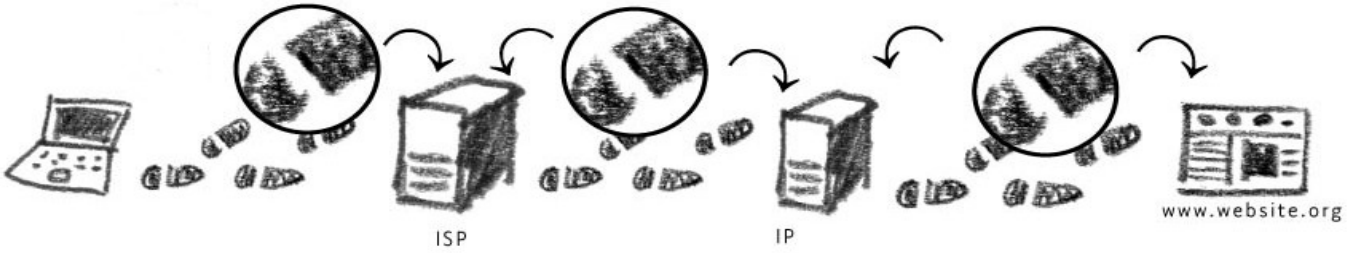
Mystic

Цифровая личность

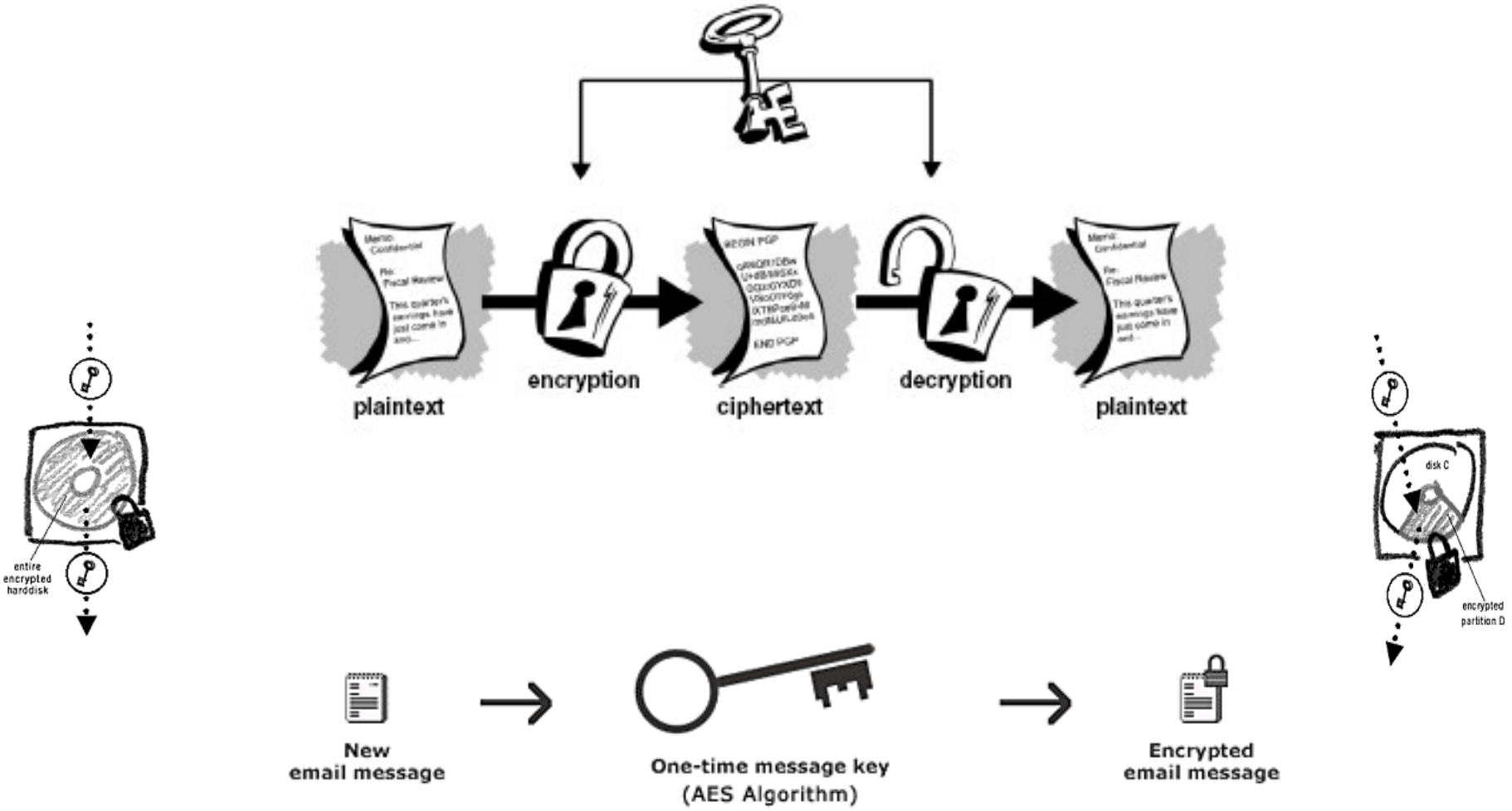
- Данные *
- Мета – данные
- IP
- Тайм стэмп
- Device ID
- MAC

- SIM
- IMEI
- IMSI
- GPS

Социальная граффа



Симметричное шифрование - требует передачи зашифрованного сообщения и ключа для его расшифровки.



Merkle Helman Diffie


CRYPTO WARS
How the NSA Is Making Us All Less Safe


Mykotronx
MYK78T
20513
Crypto Museum

шифрование с открытым ключом

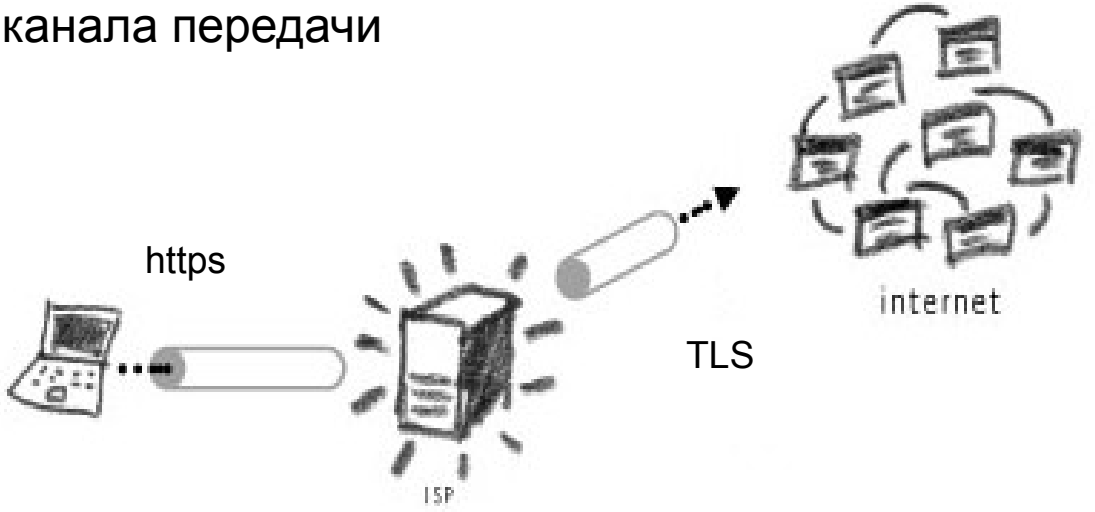
Step 1: Give your public key to the sender

Step 2: Sender uses your public key to encrypt the plaintext

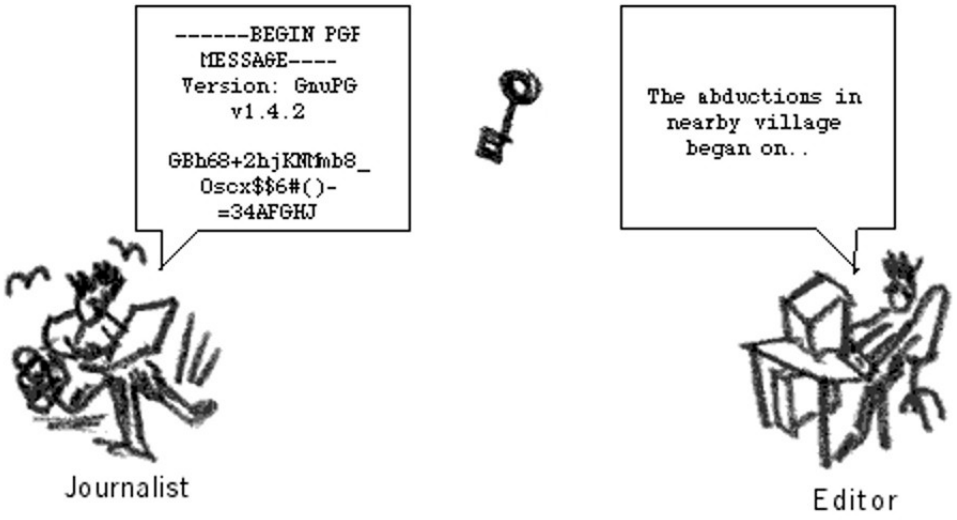
Step 3: Sender gives the ciphertext to you

Step 4: Use your private key (and passphrase) to decrypt the ciphertext

Шифрование канала передачи



Шифрование данных



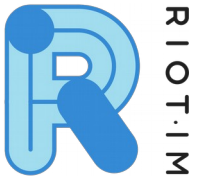
Чат

pidgin

adium

jitsi

conversation



OTR

OMEMO

MATRIX

SIGNAL

MTProto

ZRTP

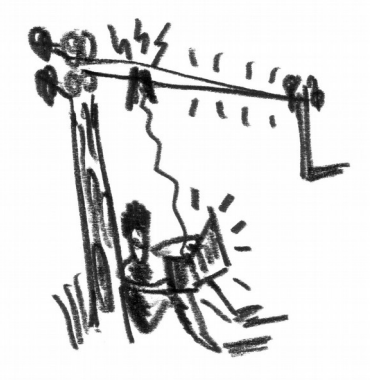
npIsec

PGP

Мессенджеры

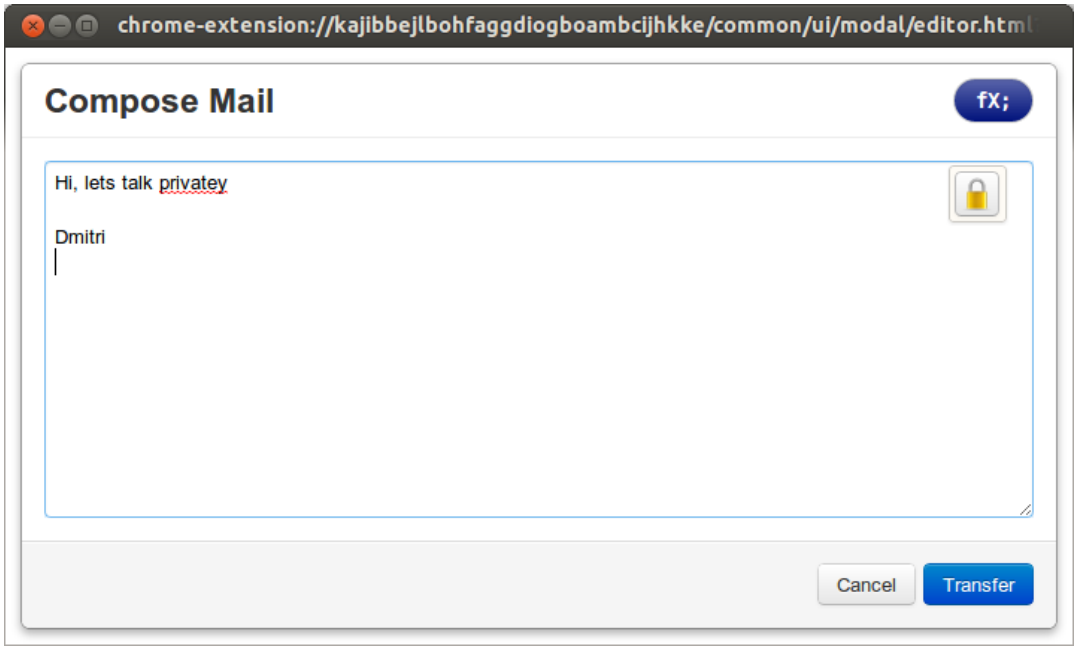
Почта и файлы

конфиденциальность

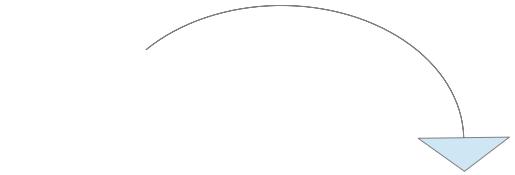


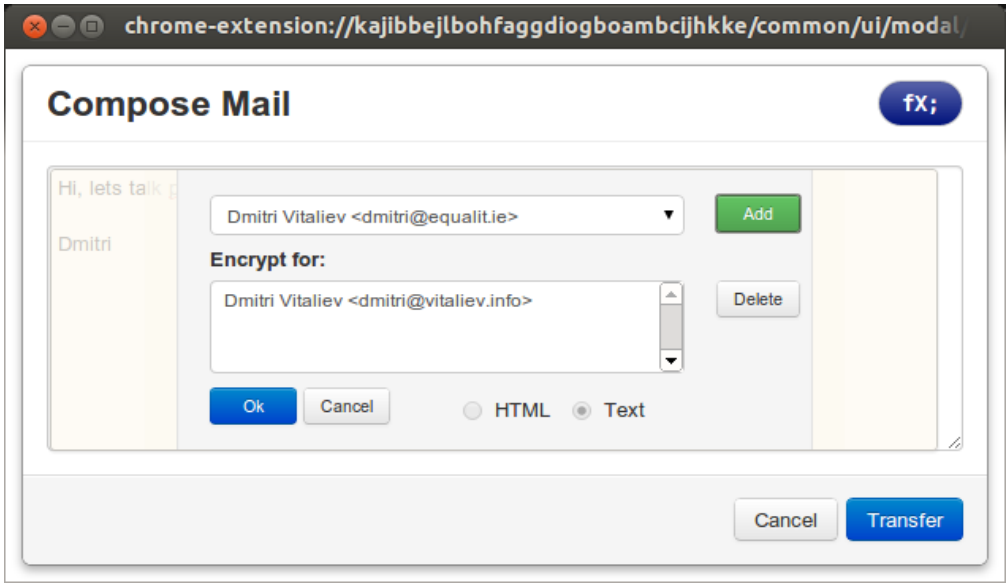
≠

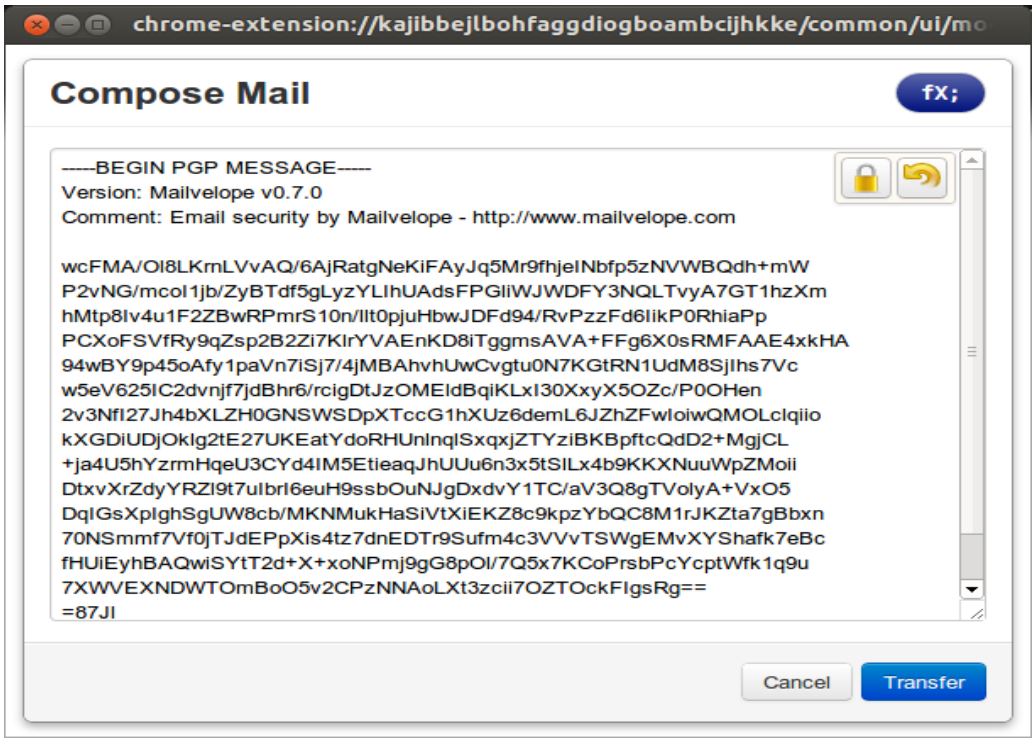
подлинность



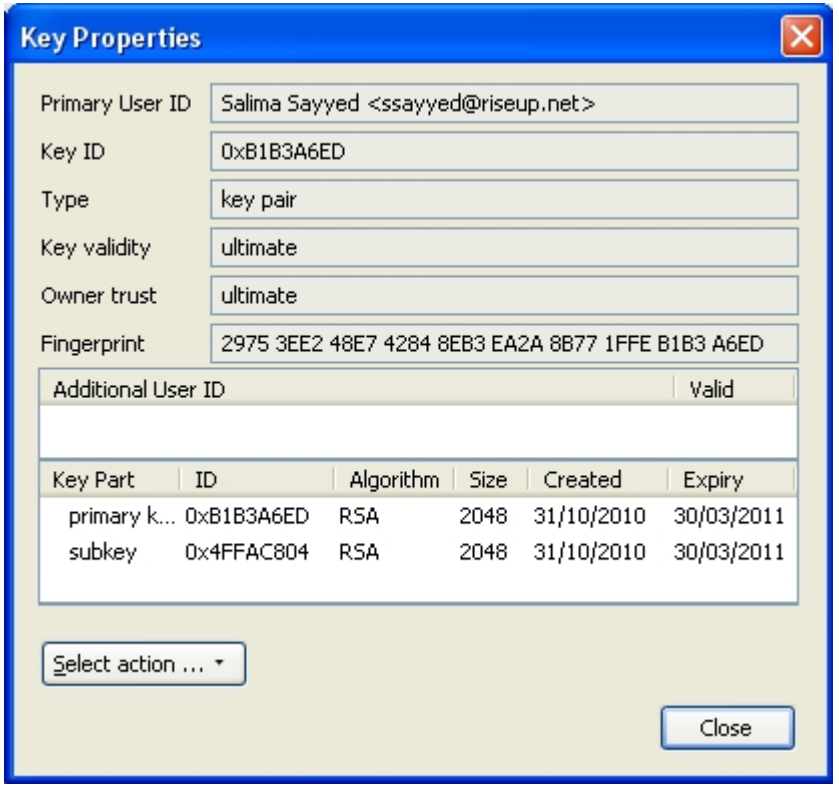
mailvelope.com

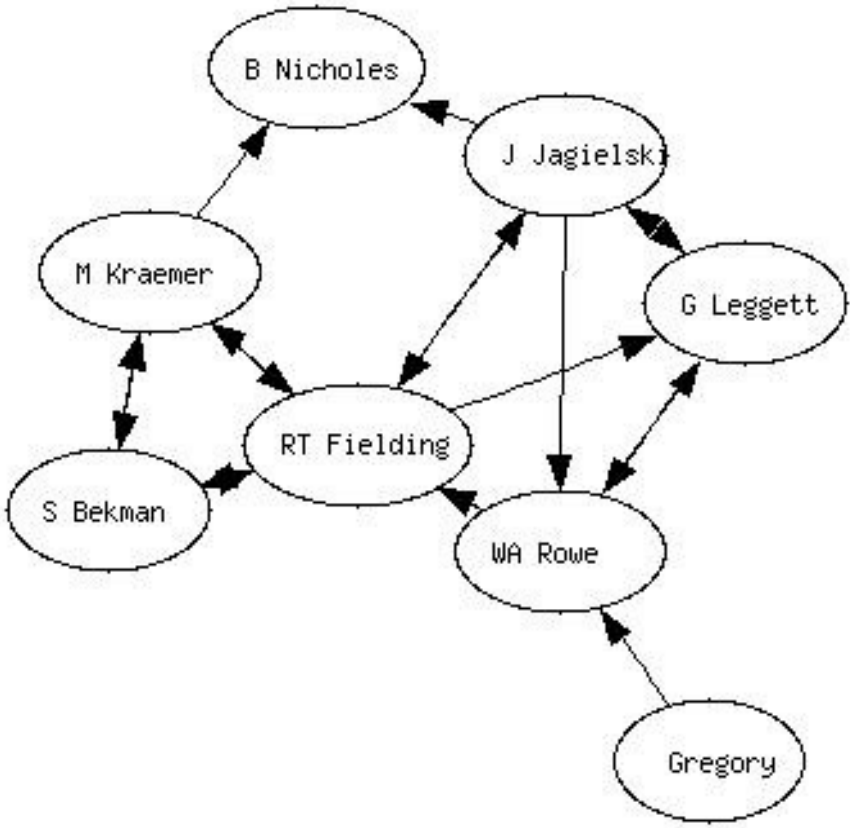






Public Key Servers





Without strong encryption, you will be spied on systematically by lots of people.

Whitfield Diffie