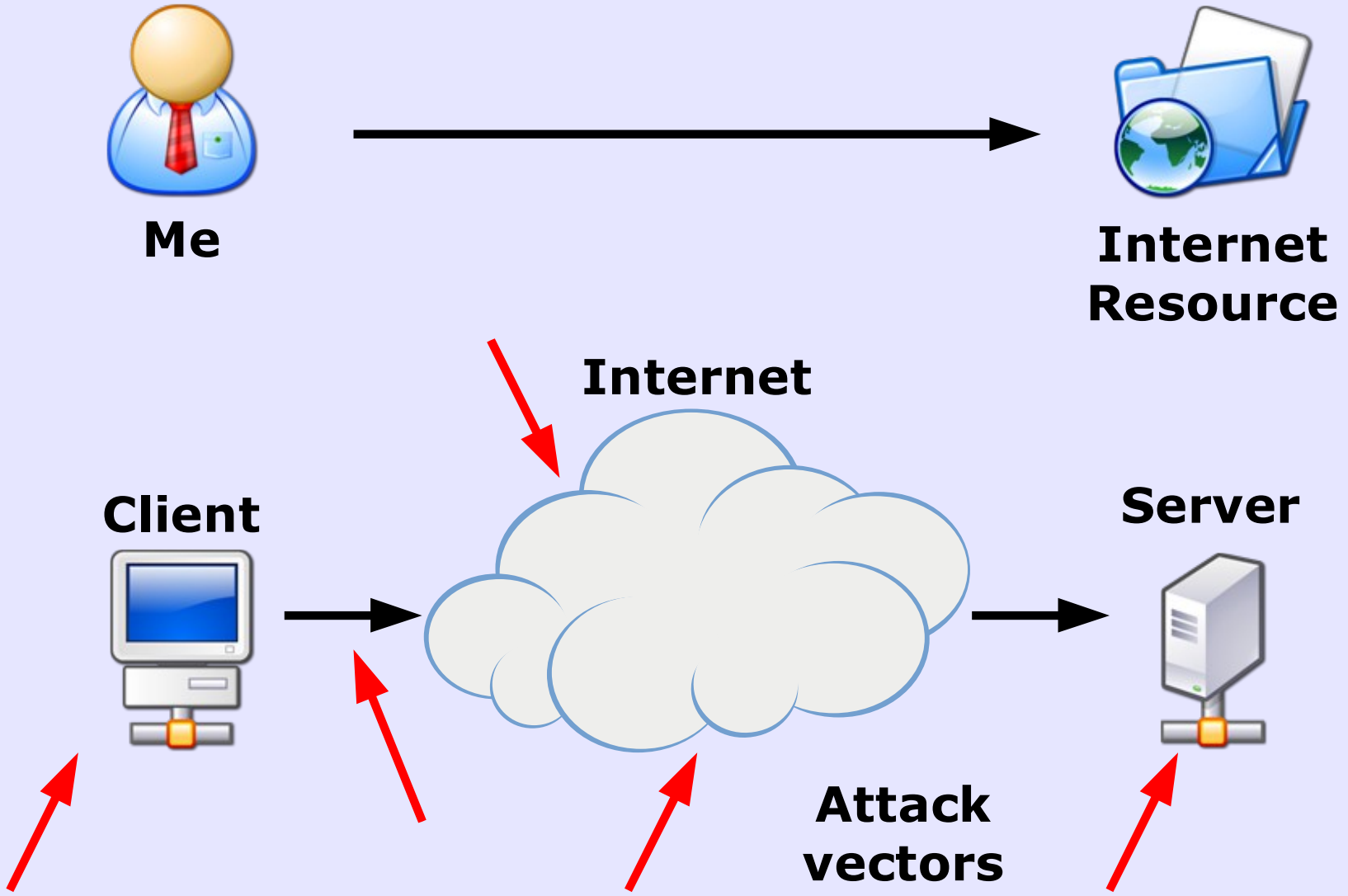
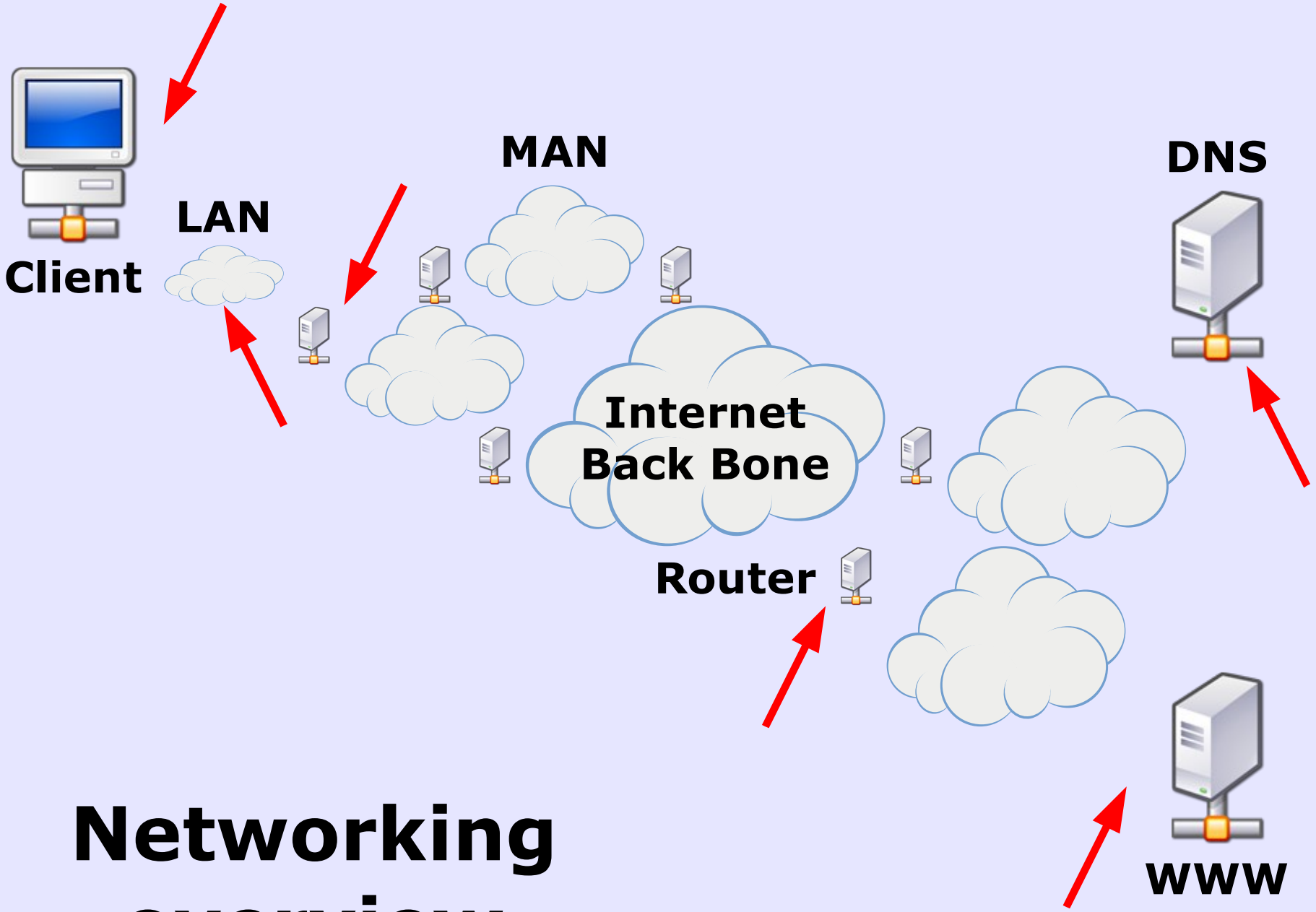
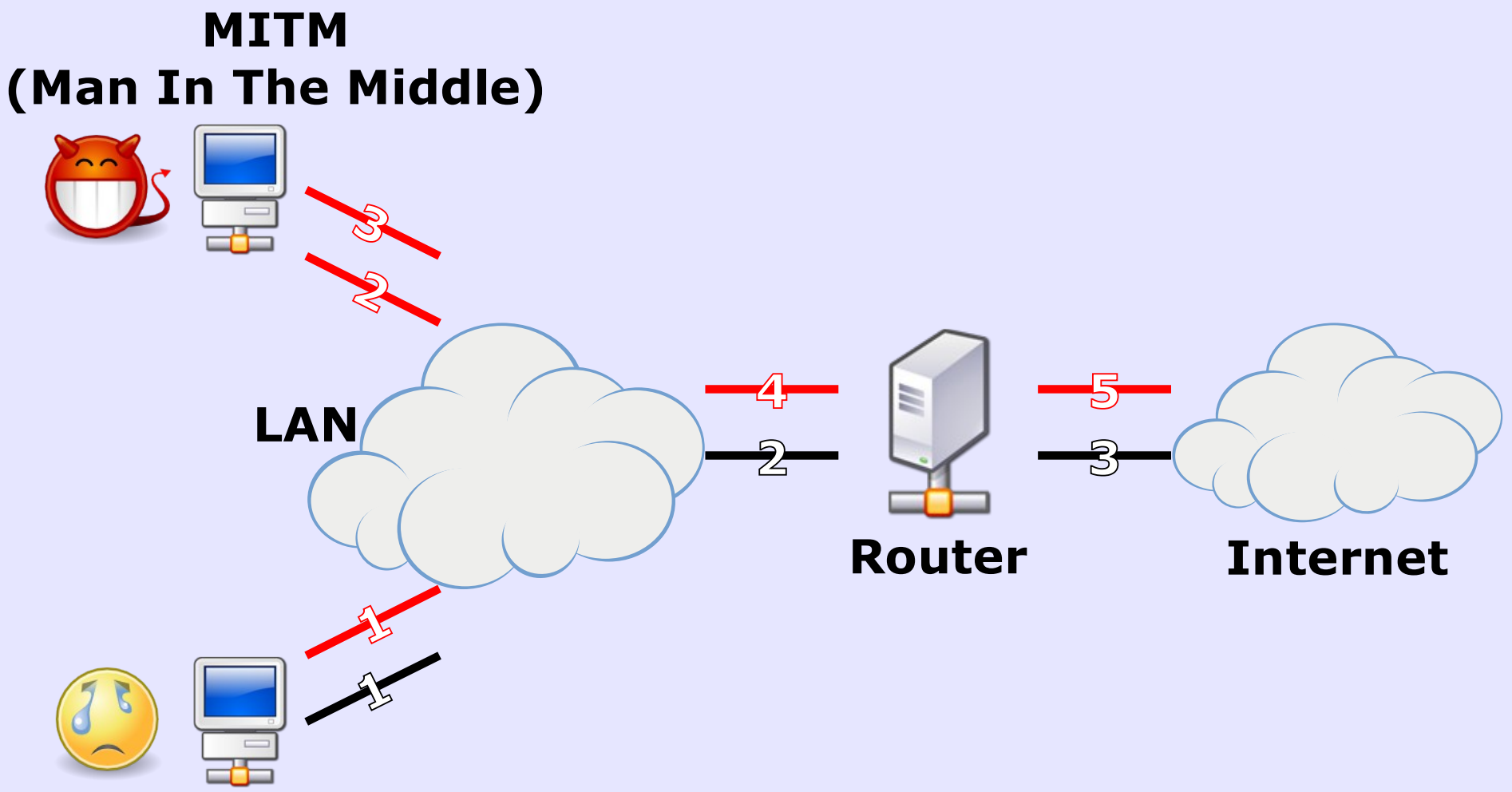
Communication security over the Internet

The big picture

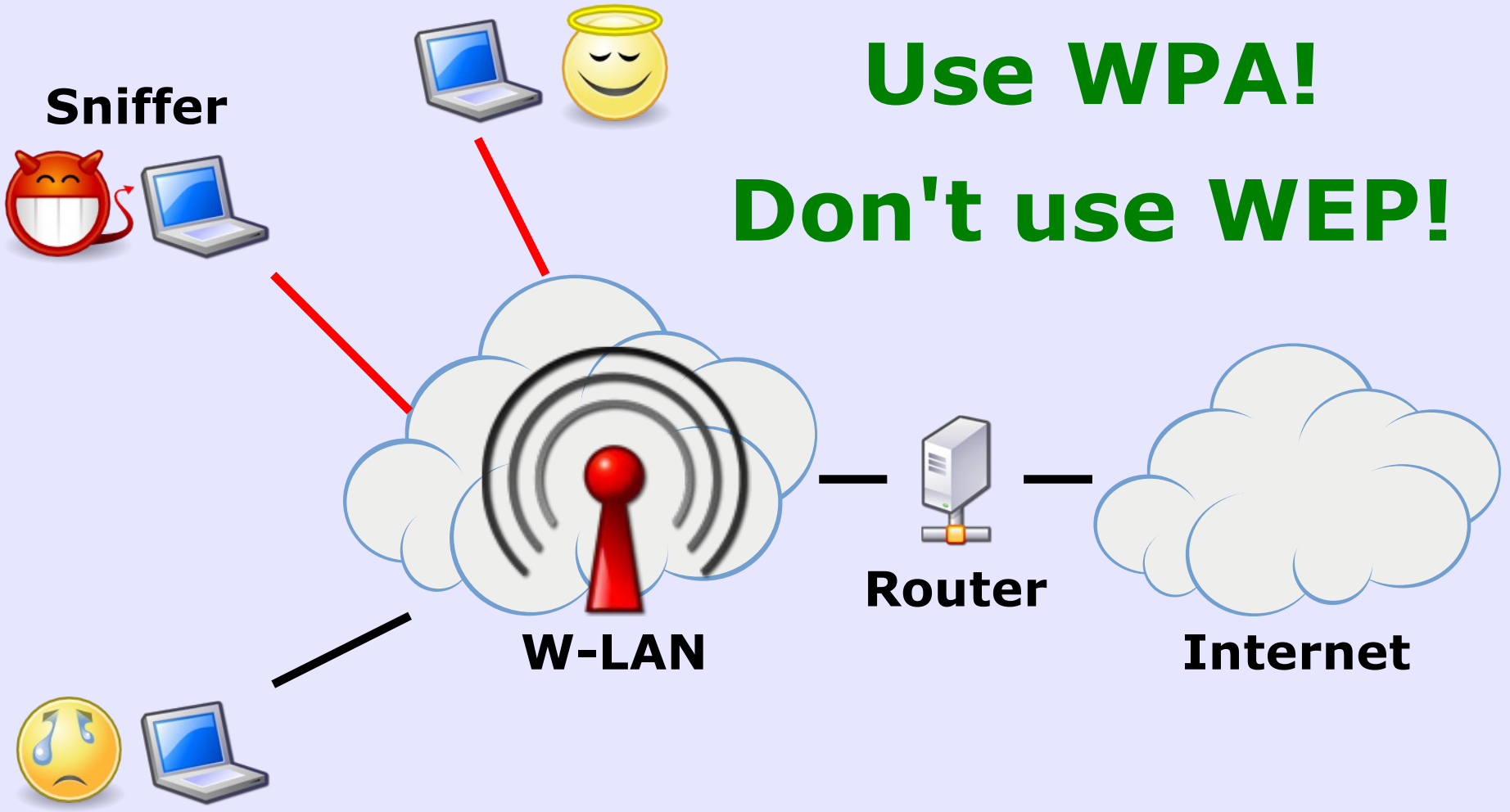




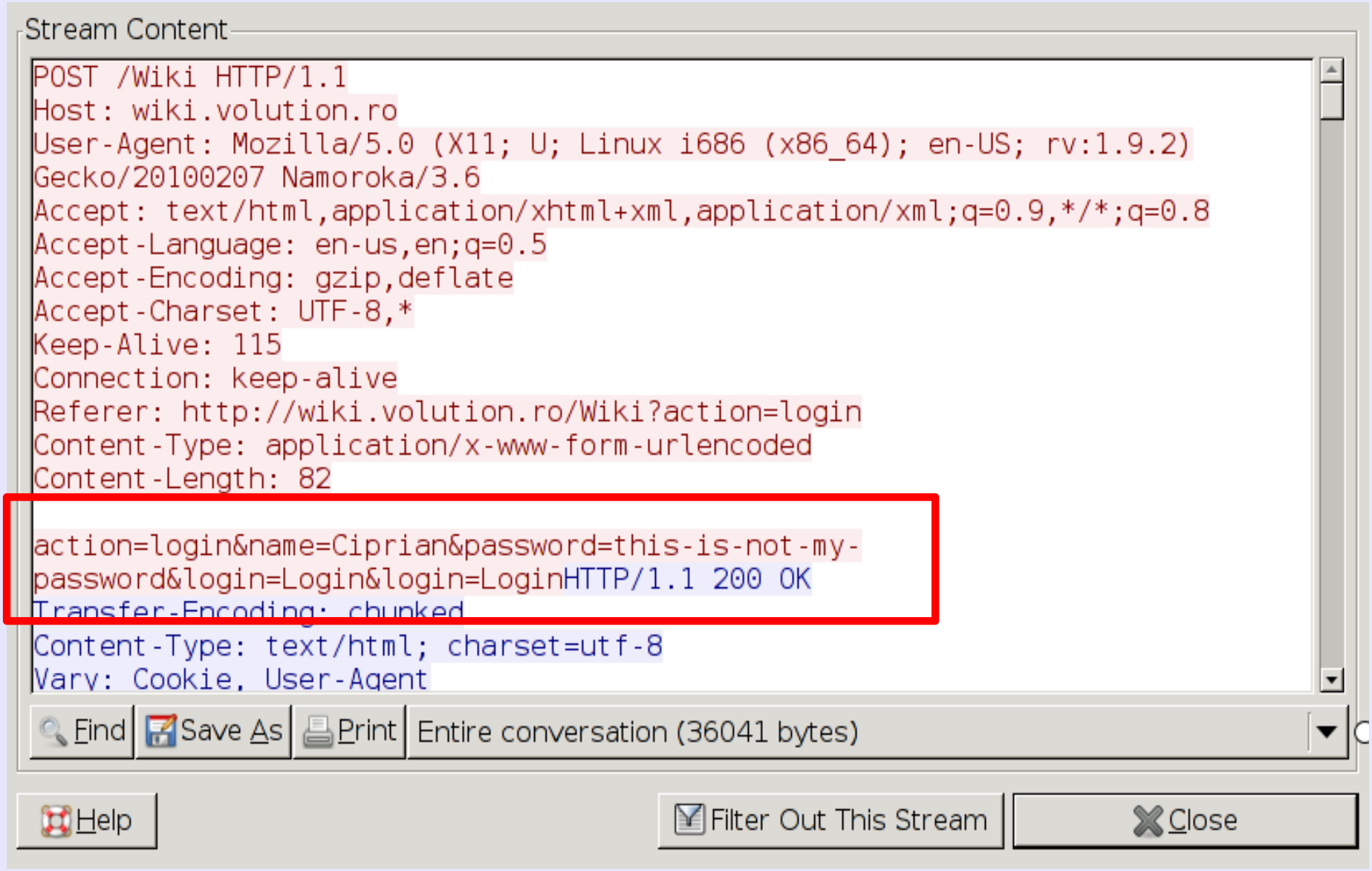
Networking overview



AV: Spoofing



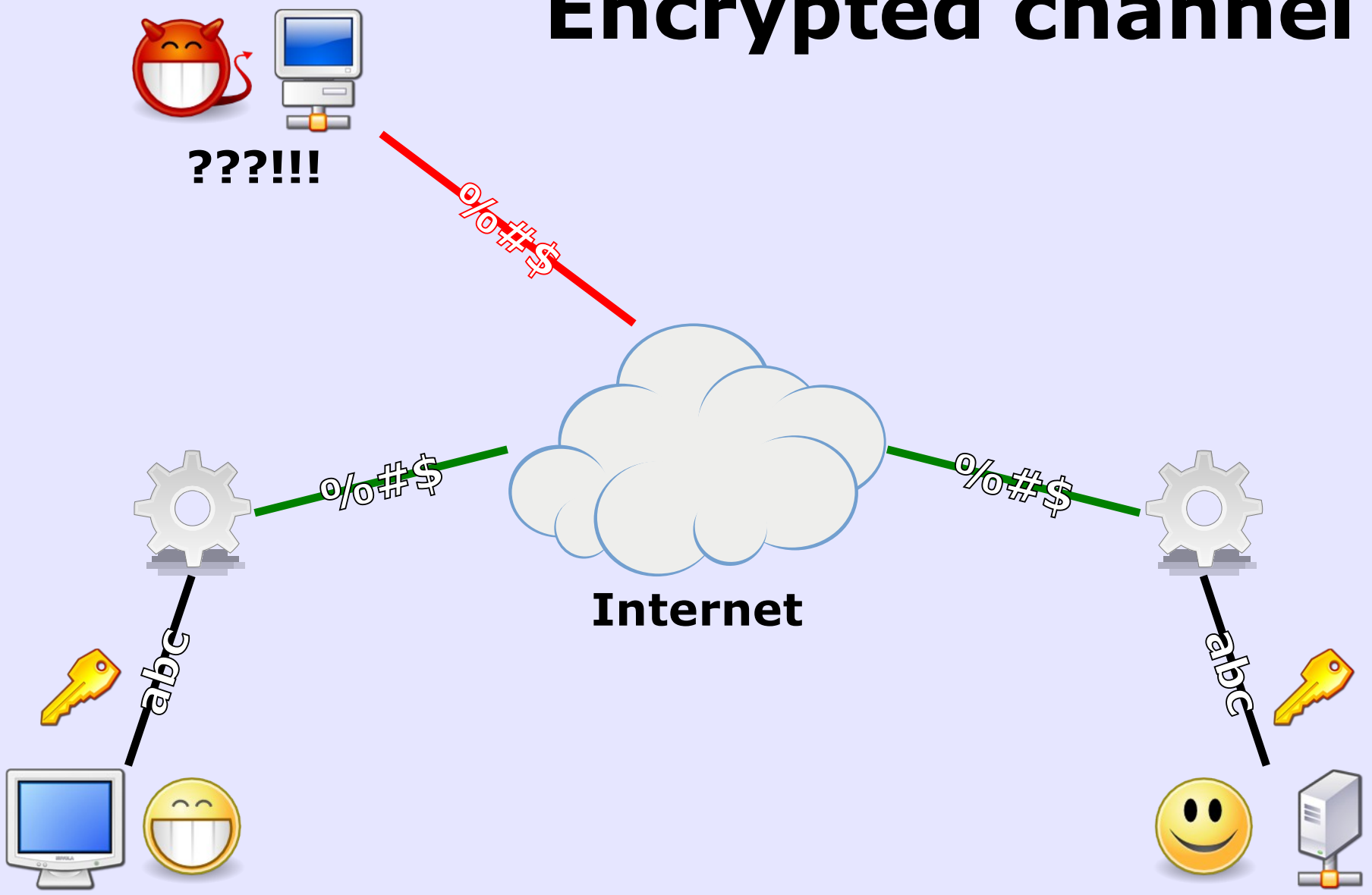
AV: Sniffing

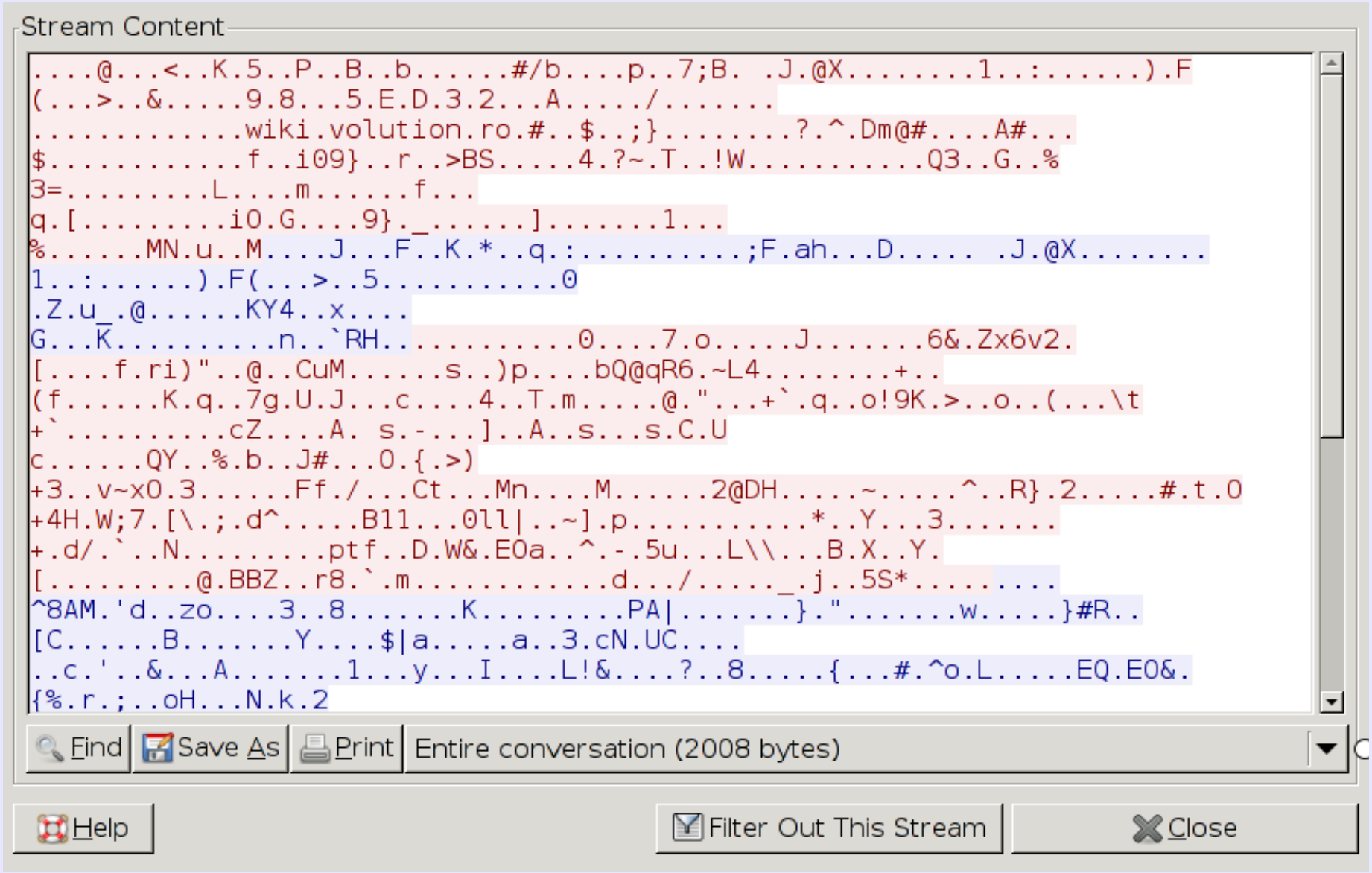


HTTP network capture

Encryption

Encrypted channel

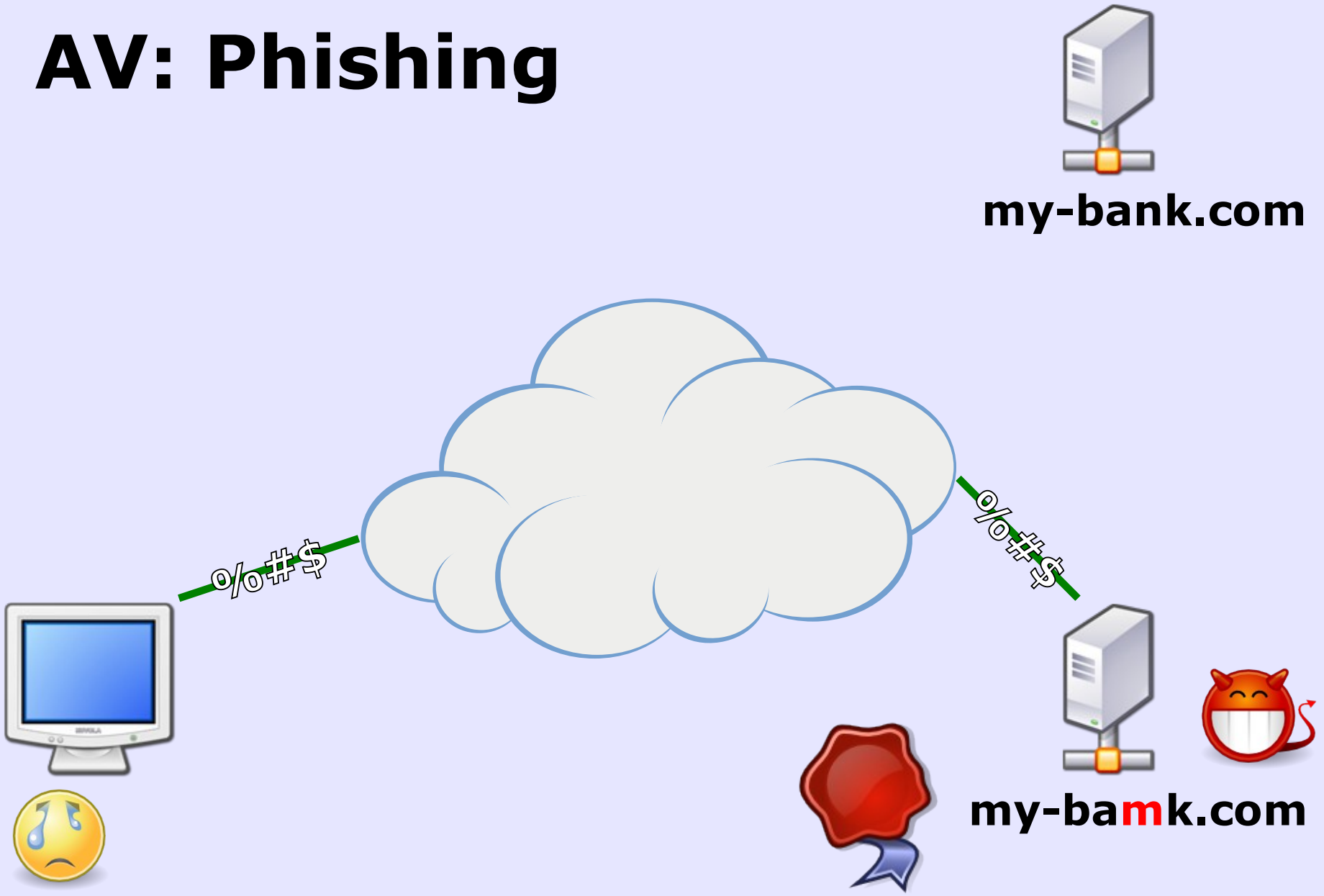


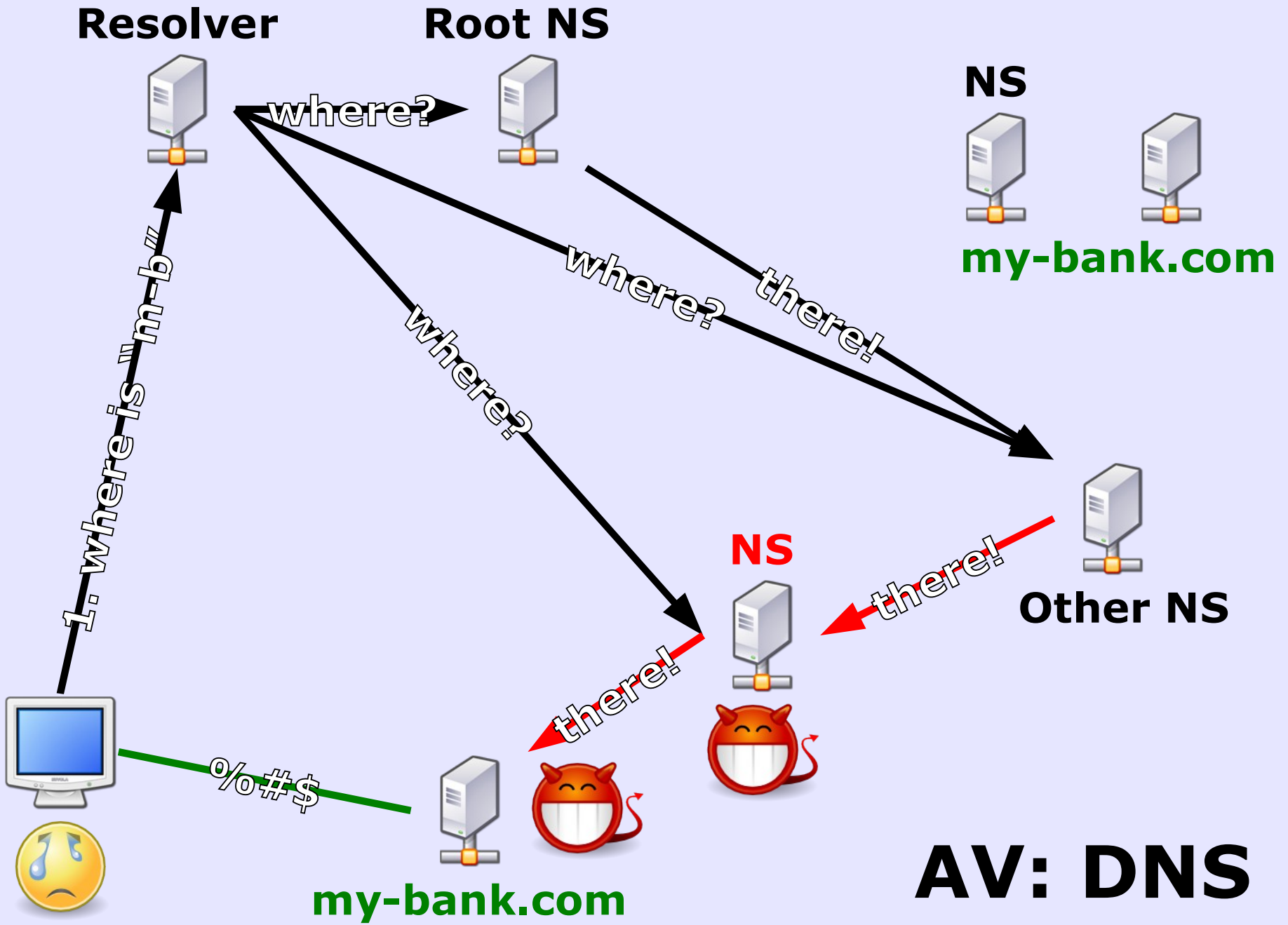


HTTPS Capture

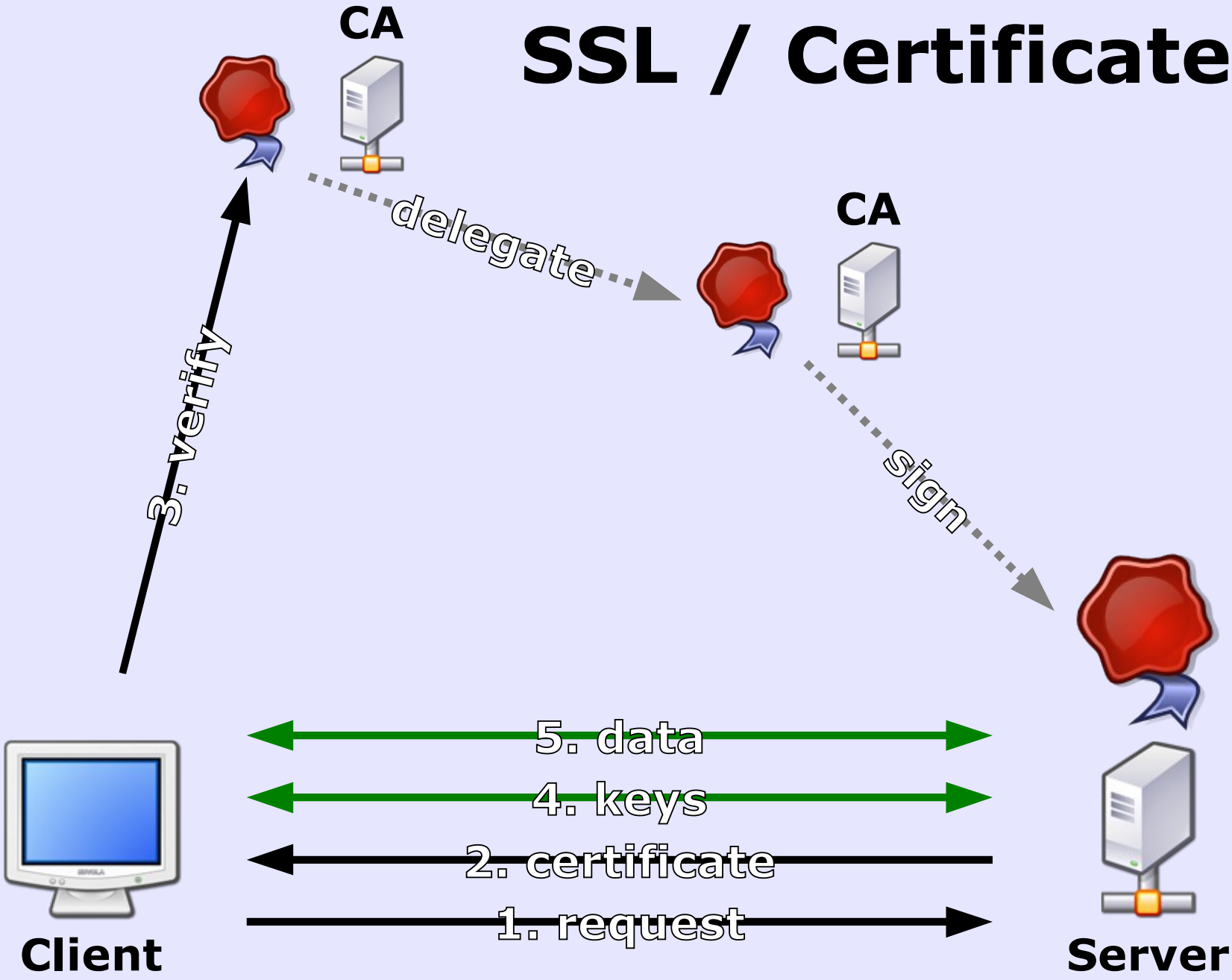
HTTPS (TLS/SSL)

AV: Phishing




Resolver
Root NS
NS
where?
where?
where?
there!
my-bank.com
1. where is "m-b"
NS
there!
Other NS
there!
there!
%o#$
my-bank.com
AV: DNS

SSL / Certificates



SSL in action (1)

SSL in action (2)

Web Site Identity

Web site: **www.raiffeisenonline.ro**

Owner: **This web site does not supply ownership information.**

Verified by: **VeriSign Trust Network**

View Certificate

Privacy & History

Have I visited this web site before today? **No**

Is this web site storing information (cookies) on my computer? **Yes** View Cookies

Have I saved any passwords for this web site? **No** View Saved Passwords

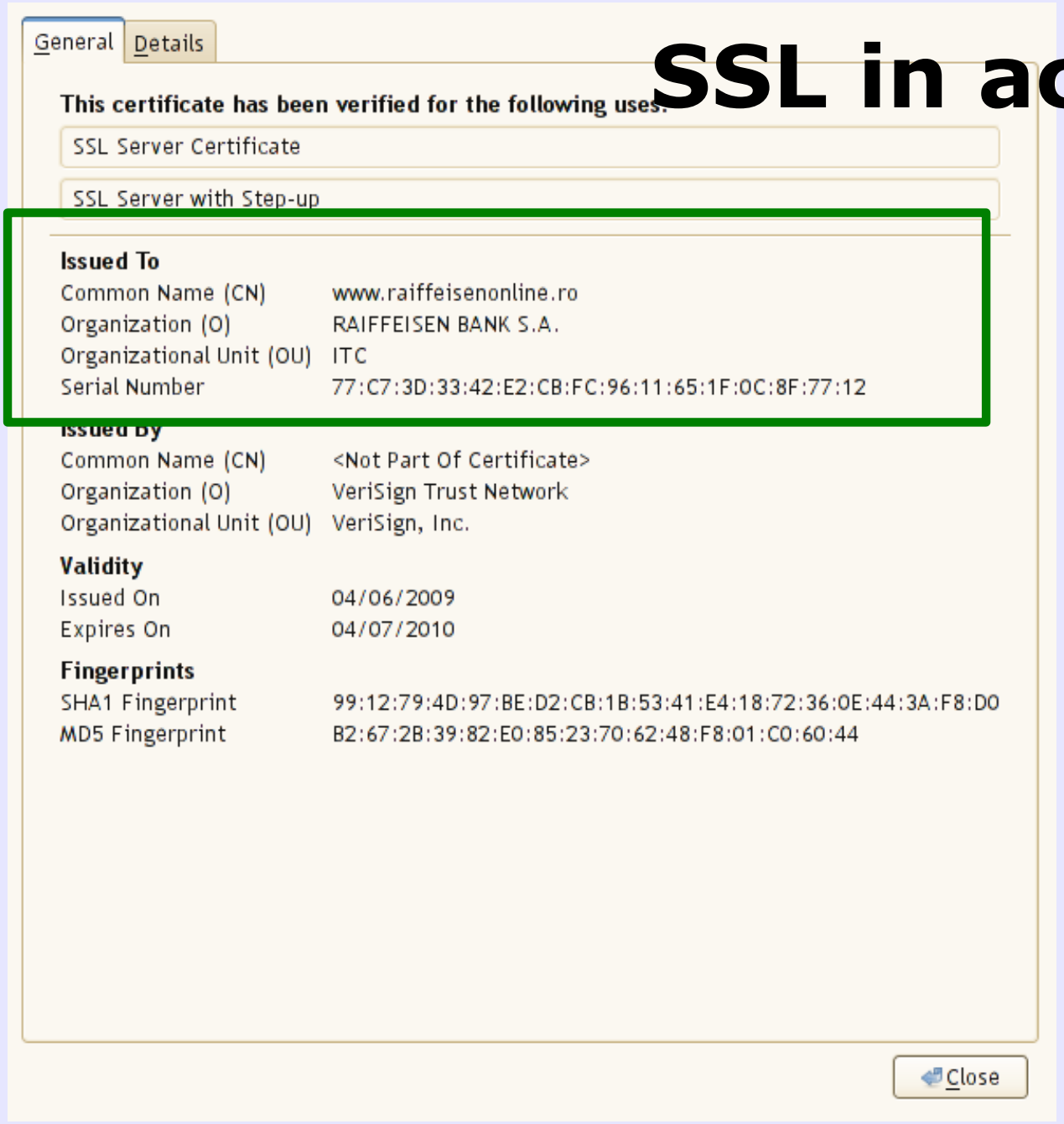
Technical Details

Connection Encrypted: High-grade Encryption (3DES-EDE-CBC 168 bit)

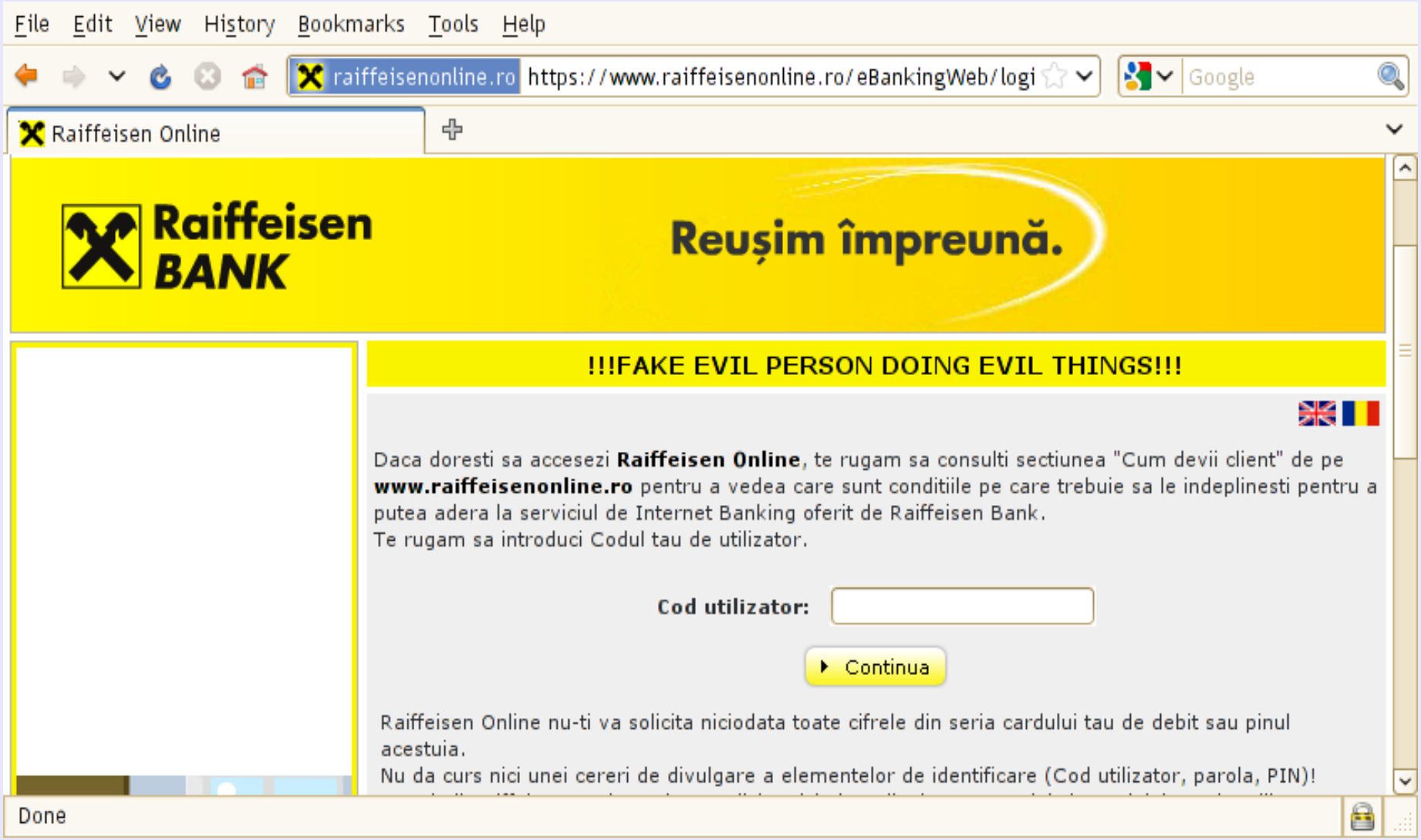
The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

SSL in action (3)



SSL in action (4)



SSL missing in action ???!!!

File Edit View History Bookmarks Tools Help

raiffeisenonline.ro https://www.raiffeisenonline.ro/eBankingWeb/logi

Google

Raiffeisen Online

Raiffeisen BANK

Reușim împreună.

!!!FAKE EVIL PERSON DOING EVIL THINGS!!!

Daca doresti sa accesezi **Raiffeisen Online**, te rugam sa consulti sectiunea "Cum devii client" de pe **www.raiffeisenonline.ro** pentru a vedea care sunt conditiile pe care trebuie sa le indeplinesti pentru a putea adera la serviciul de Internet Banking oferit de Raiffeisen Bank.
Te rugam sa introduci Codul tau de utilizator.

Cod utilizator:

Continua

Raiffeisen Online nu-ti va solicita niciodata toate cifrele din seria cardului tau de debit sau pinul acestuia.
Nu da curs nici unei cereri de divulgare a elementelor de identificare (Cod utilizator, parola, PIN !

Done

General | Media | Permissions | Security

Web Site Identity

Web site: **www.raiffeisenonline.ro**

Owner: **This web site does not supply ownership information.**

Verified by: **Evil Person**

View Certificate

Privacy & History

Have I visited this web site before today?

Is this web site storing information (cookies) on my computer?

View Cookies

Have I saved any passwords for this web site? **No**

View Saved Passwords

??? Huh ???

Technical Details

Connection Encrypted: High-grade Encryption (AES-256 256 bit)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

Check “SHA1 Fingerprint”!!!

General Details

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	www.raiffeisenonline.ro
Organization (O)	FAKE RAIFFEISEN
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	01

Issued By

Common Name (CN)	My Evil CA
Organization (O)	Evil Person
Organizational Unit (OU)	<Not Part Of Certificate>

Validity

Issued On	03/18/2010
Expires On	[illegible]

Fingerprints

SHA1 Fingerprint	DB:2B:A4:DA:B4:35:0F:41:C7:8C:D3:A0:9F:C0:51:8E:1A:34:1A:B1
MD5 Fingerprint	F5:1C:C0:91:B6:0D:69:AA:F7:19:61:48:6D:57:A9:E0

Cl[illegible]

Don't rely on “MD5 Fingerprint”!!!

The explanation!

Your Certificates | People | Servers | Authorities | Others

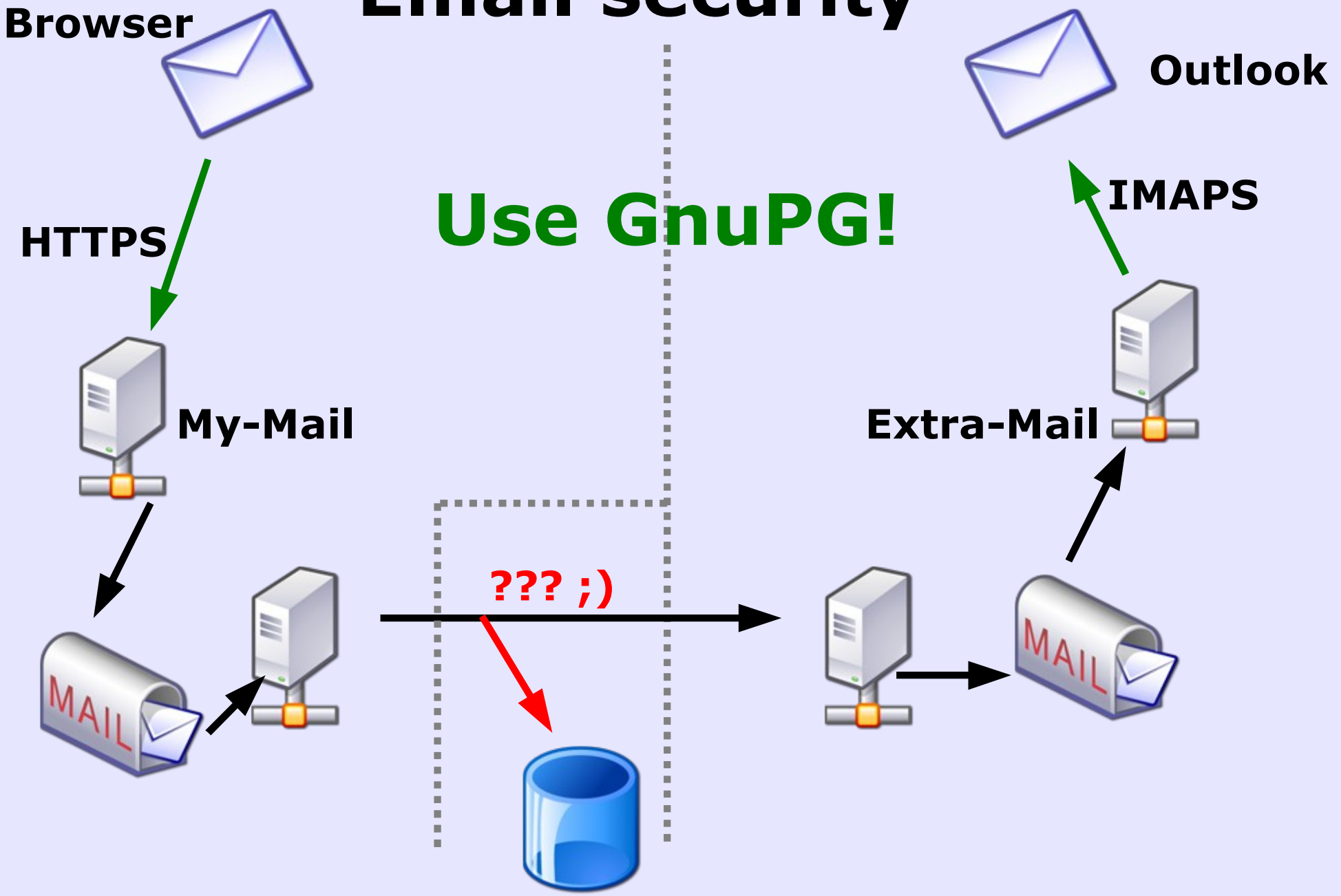
You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
Equifax Secure Global eBusiness CA-1	Builtin Object Token
Equifax Secure eBusiness CA-1	Builtin Object Token
Evil Person	
My Evil CA	Software Security Device
GeoTrust Inc.	
GeoTrust Primary Certification Authority	Builtin Object Token
GeoTrust Global CA	Builtin Object Token
GeoTrust Global CA 2	Builtin Object Token
GeoTrust Universal CA	Builtin Object Token
GeoTrust Universal CA 2	Builtin Object Token

View... | Edit... | Import... | Export... | Delete...

OK

Email security



Keep focus!