$ whoami

- attività professionale:
  - analisi delle vulnerabilità e penetration testing
  - security consulting
  - formazione
- altro:
  - sikurezza.org
  - (F|Er|bz)lug

free advertising >

Agenda

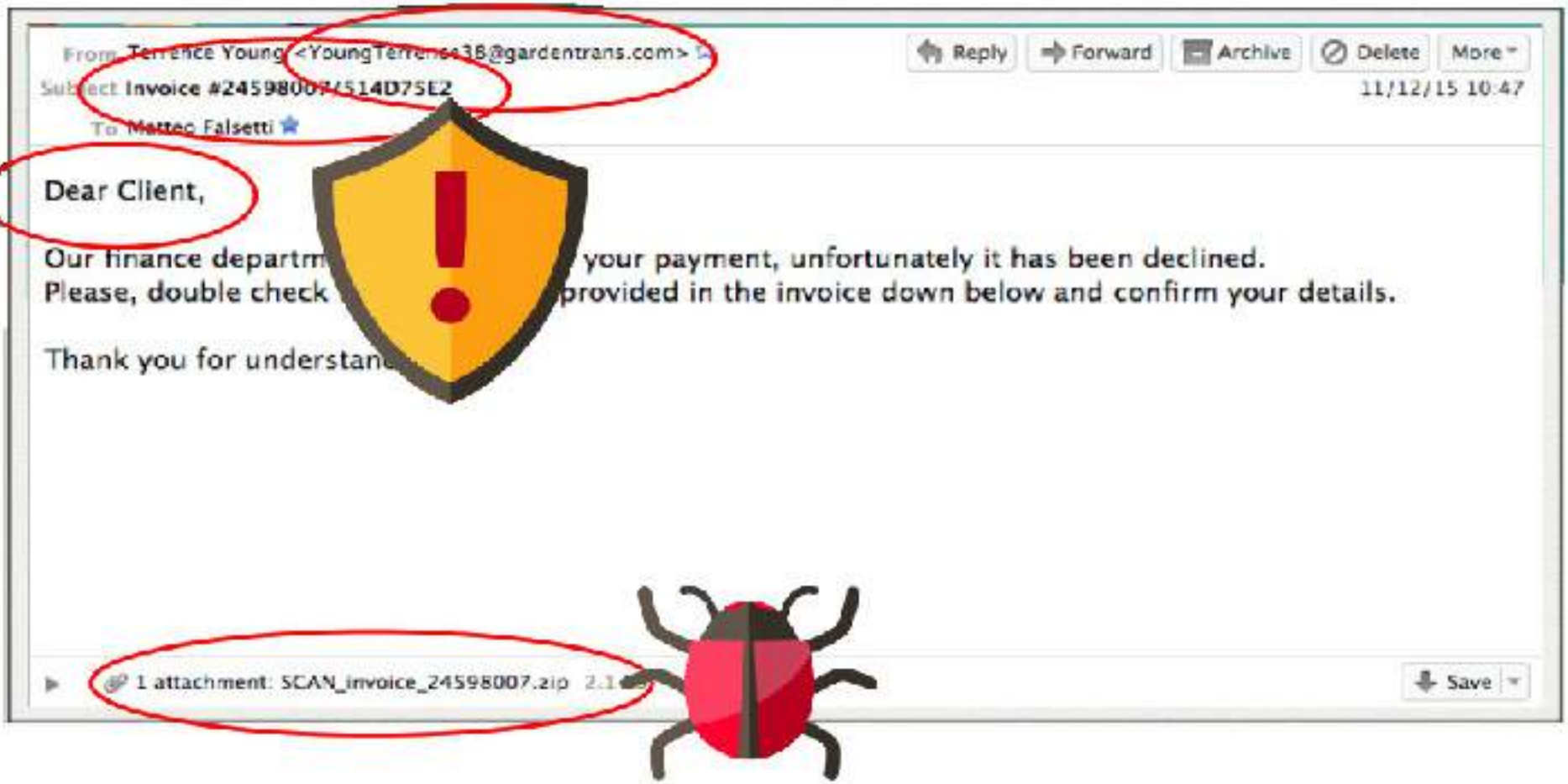
src: https://www.facebook.com/worldeconomicforum/posts/10152578793381479

Scenario 1: utenti

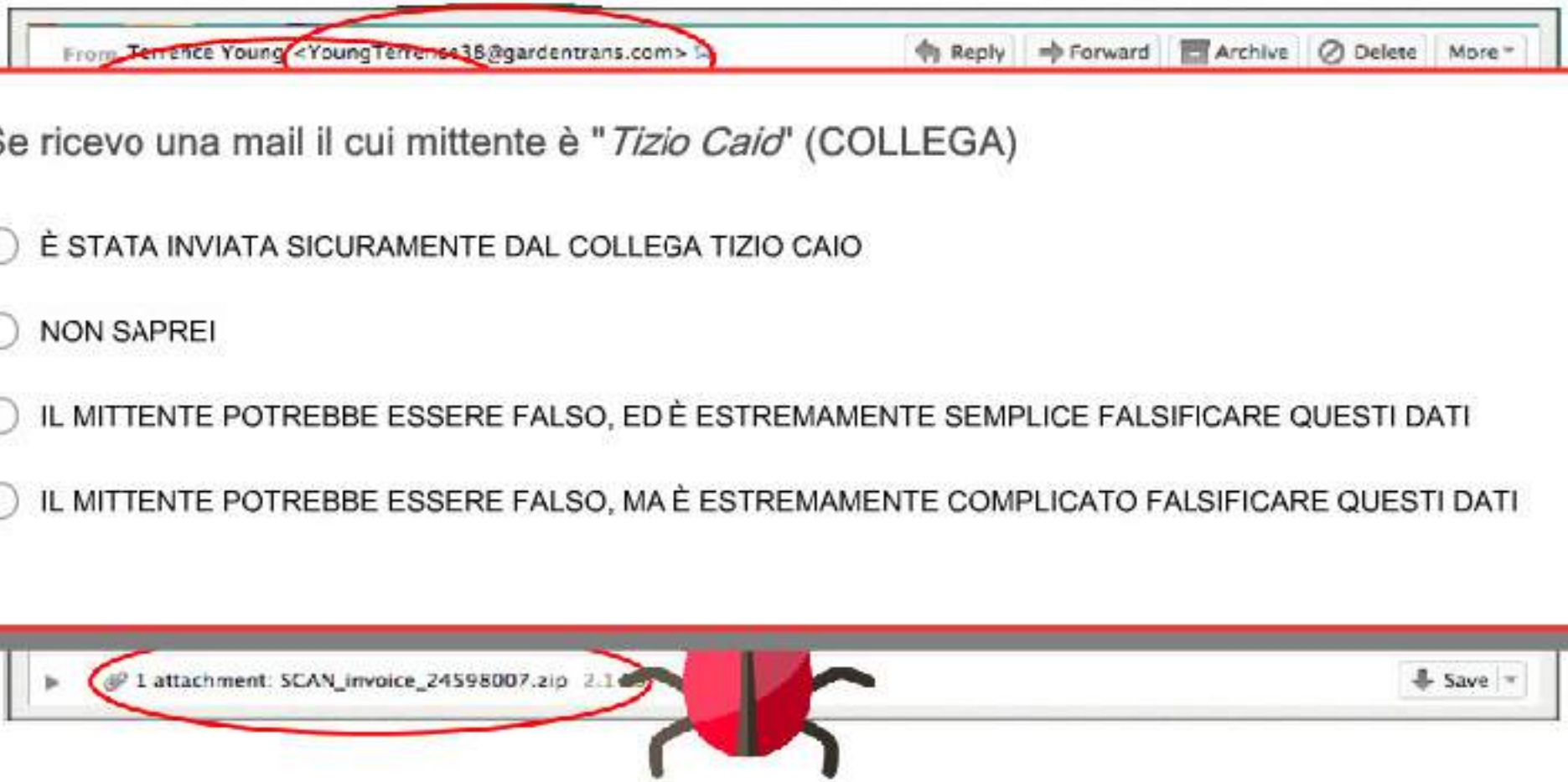
malware

Scenario 1: utenti

malware



Quiz 1: mittente

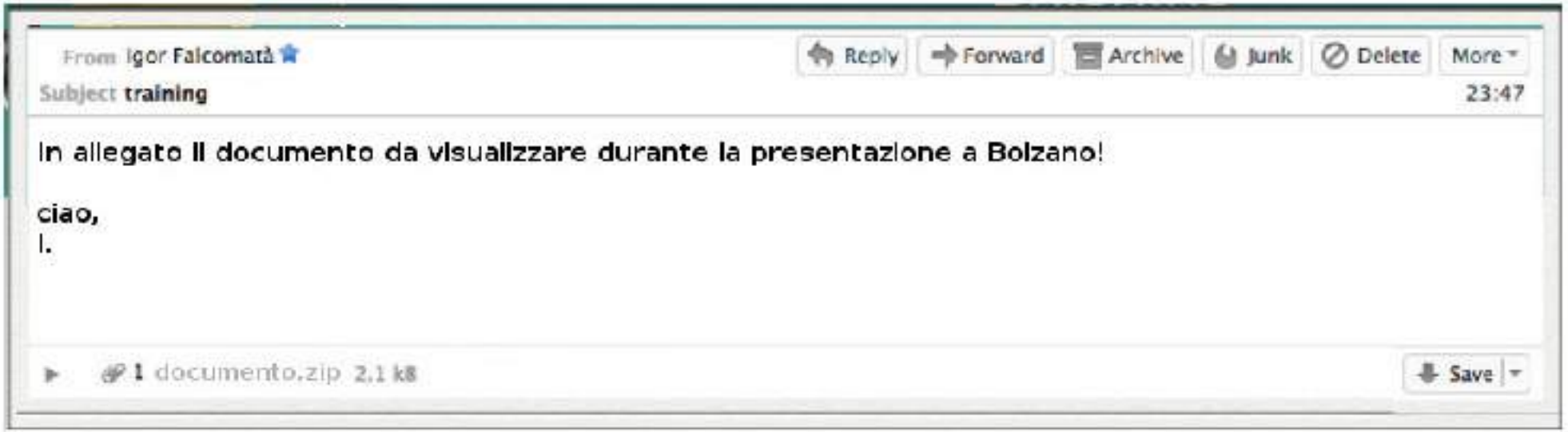


Se ricevo una mail il cui mittente è "*Tizio Caid*" (COLLEGA)

- ◯ È STATA INVIATA SICURAMENTE DAL COLLEGA TIZIO CAIO
- ◯ NON SAPREI
- ◯ IL MITTENTE POTREBBE ESSERE FALSO, ED È ESTREMAMENTE SEMPLICE FALSIFICARE QUESTI DATI
- ◯ IL MITTENTE POTREBBE ESSERE FALSO, MA È ESTREMAMENTE COMPLICATO FALSIFICARE QUESTI DATI

Scenario 1: utenti

malware

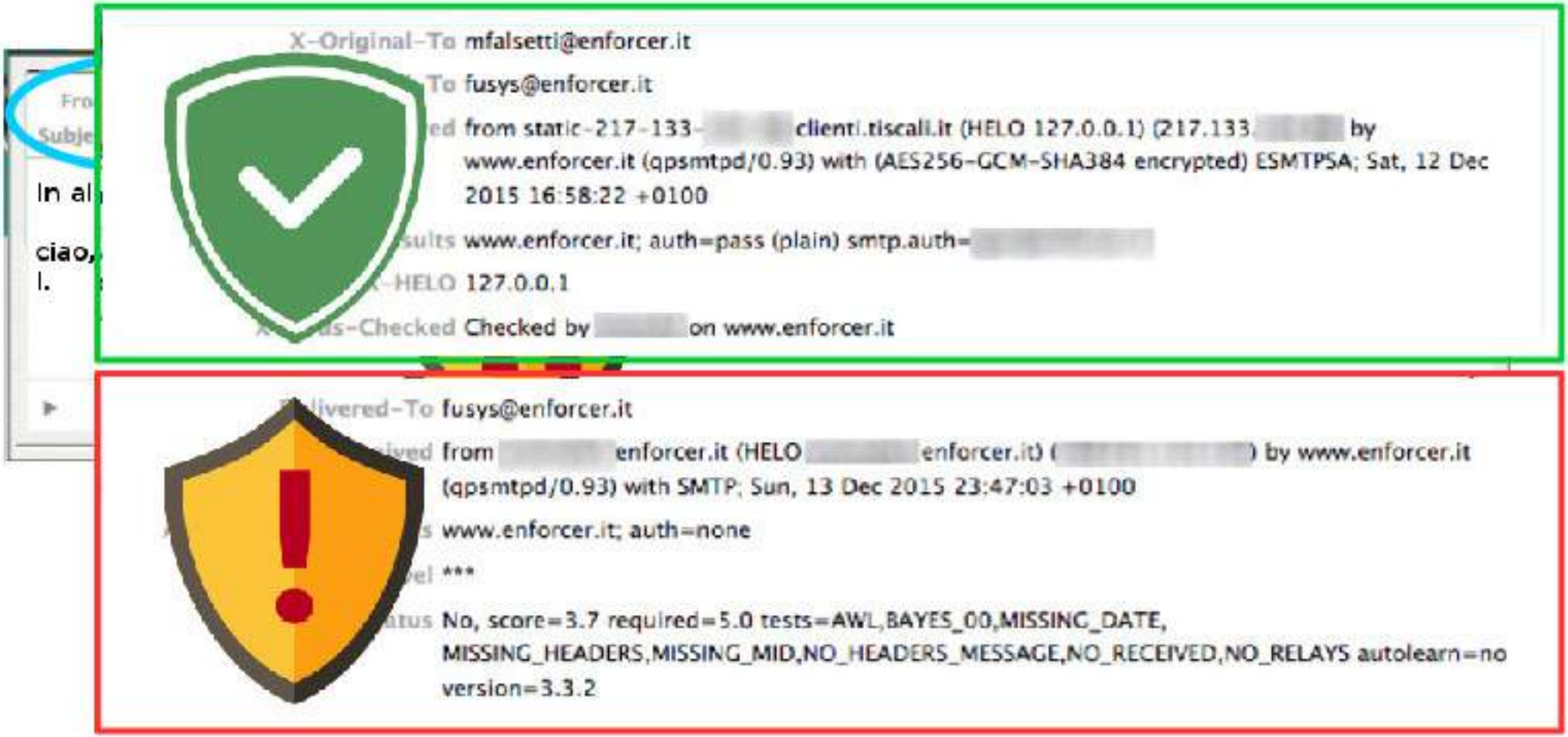


Scenario 1: utenti

malware

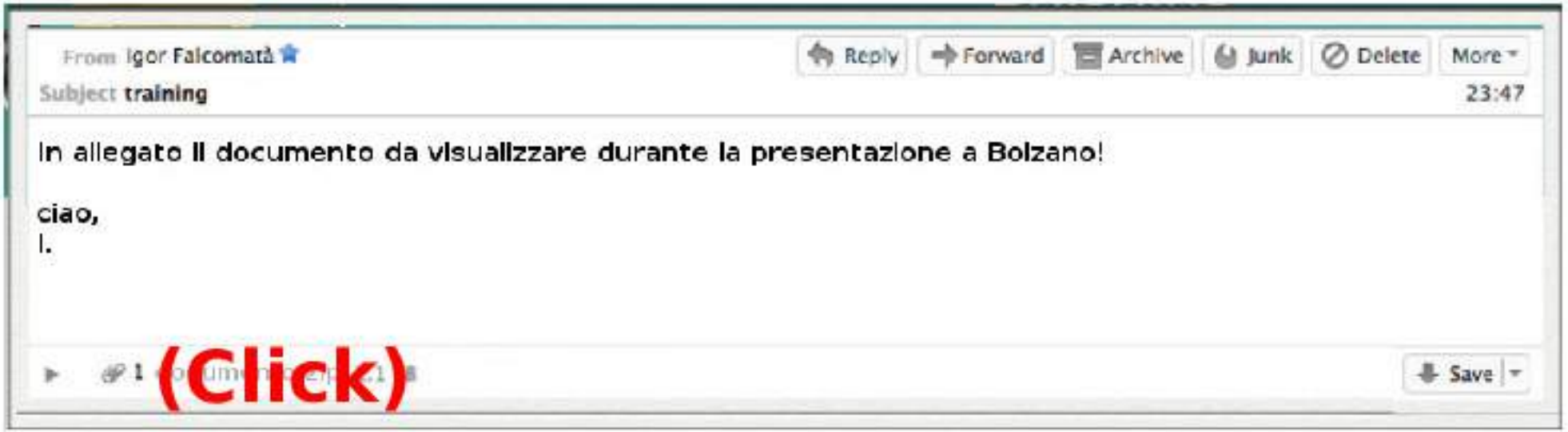
Scenario 1: utenti

malware



Scenario 1: utenti

malware



CryptoLocker

Your Personal files are encrypted!

Private key will be destroyed on

1/6/2015 1:11:17 PM

Time left

71:55:27

Checking wallet..

Received: 0.00 BTC

Your personal files **encryption** produced on this computer: photos, videos, documents, etc. Encryption was produced using a **unique** public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **1.00 bitcoin** (~291 USD).

You can easily delete this software, but know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

For more information on how to buy and send bitcoins, click "Pay with Bitcoin"
To open a list of encoded files, click "Show files"

Do not delete this list, it will be used for decryption. And do not move your files.

Show files

Pay with Bitcoin

Quiz 2: go fishing?

Il *phishing* è

- ○ NON SAPREI
- ○ È UNA TECNICA DI ALLENAMENTO (GINNASTICA)
- ○ È UNA TECNICA DI PESCA (CON LA "MOSCA")
- ○ È UNA TECNICA DI ATTACCO INFORMATICO

Scenario 2: utenti

phishing

src: https://en.wikipedia.org/wiki/Phishing

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

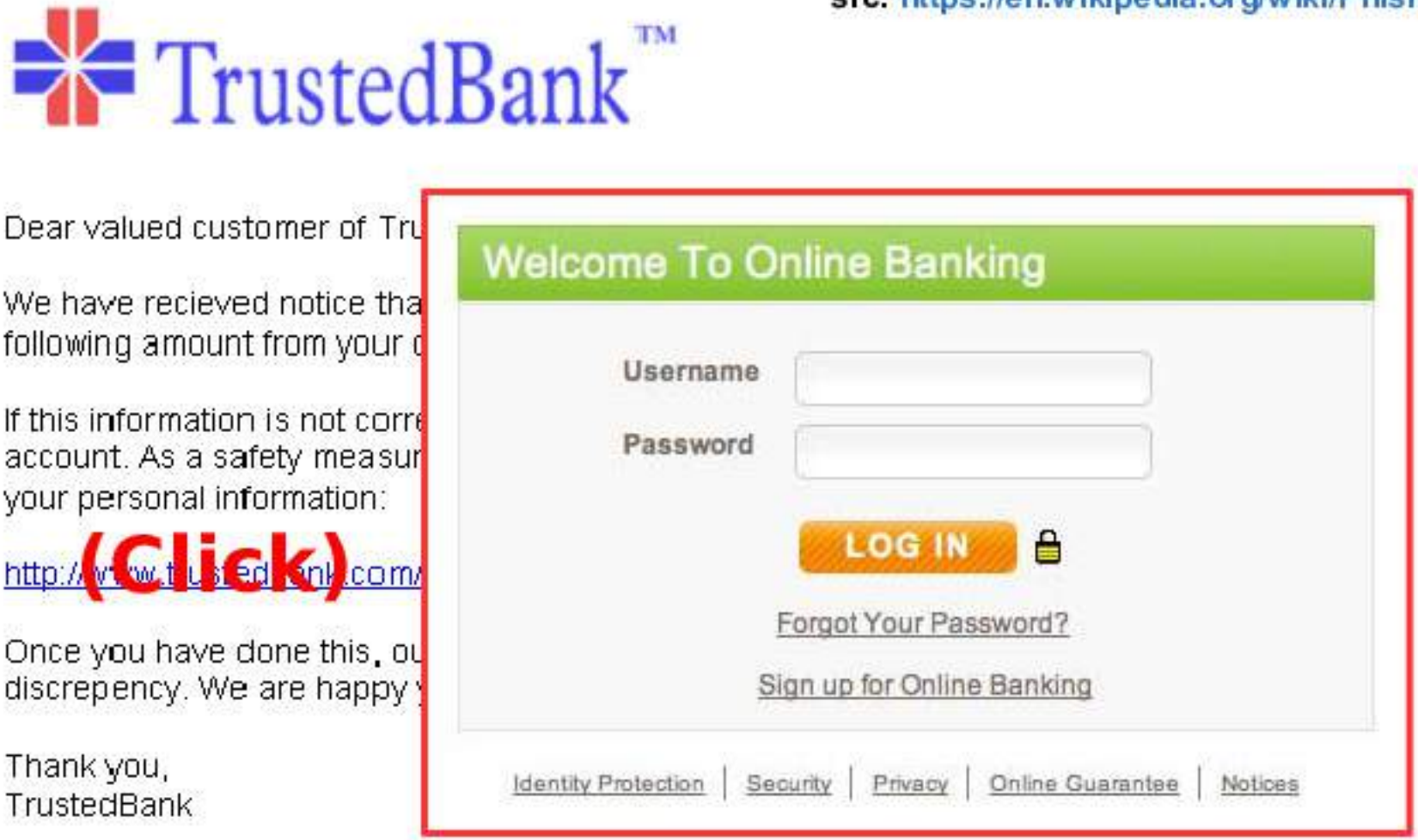
Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Scenario 2: utenti

phishing

src: https://en.wikipedia.org/wiki/Phishing

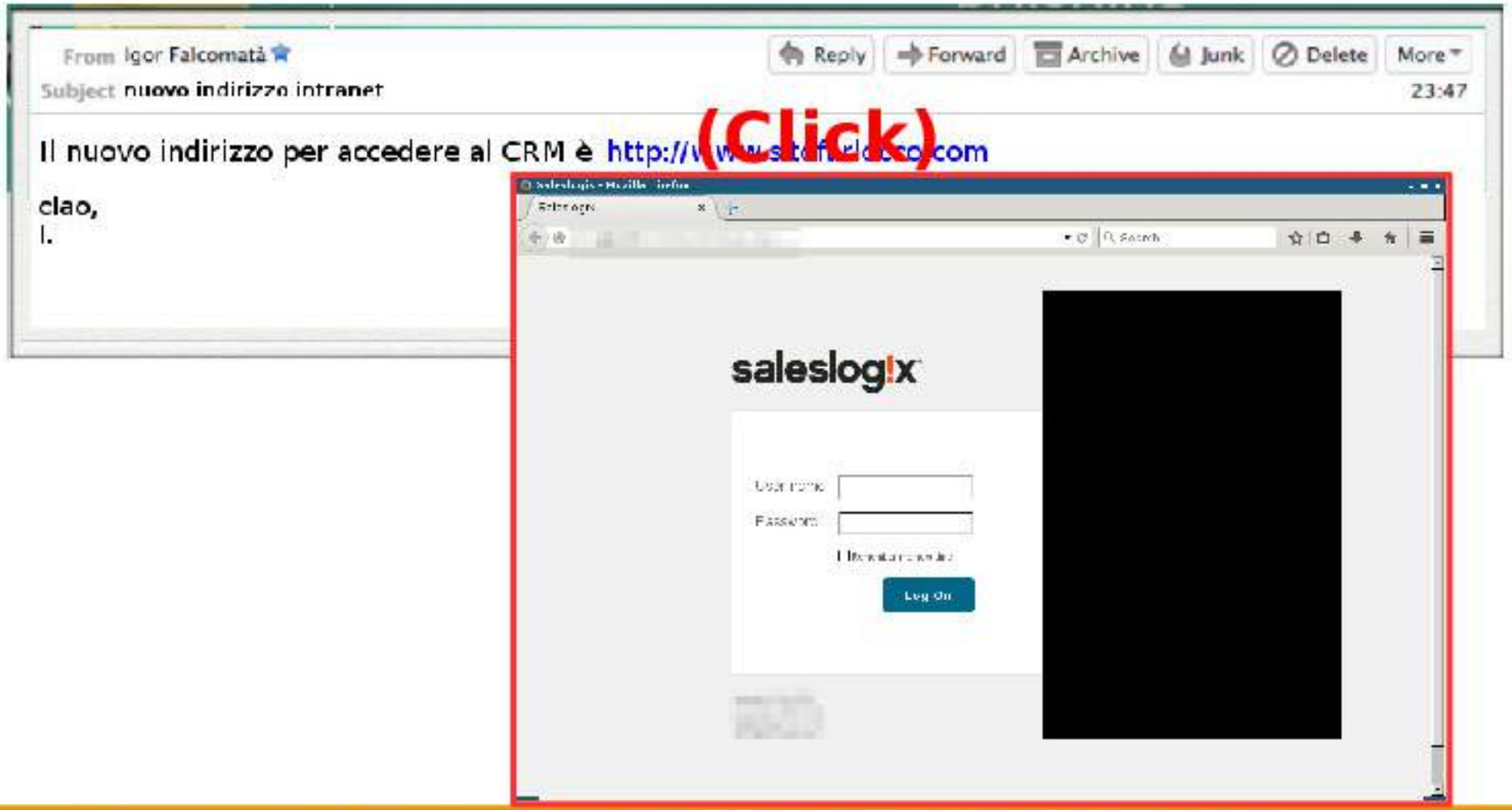


Scenario 2: utenti

phishing

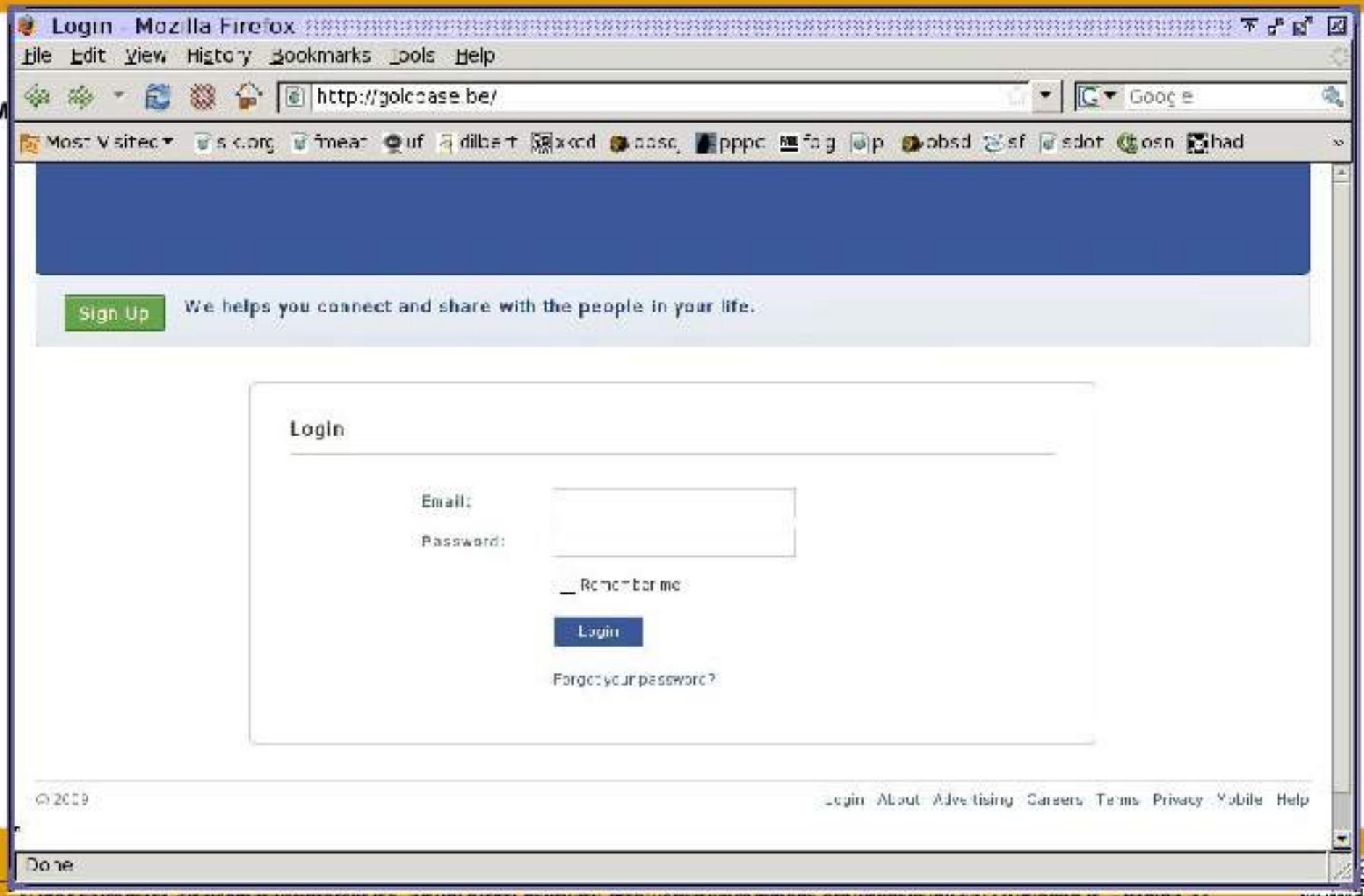
Scenario 2: utenti

phishing



Phishing

...non solo verso siti di banking



Prima di Internet

1960..

- phreaking
- social engineering (telefono, persona)
- malware (virus, trojan)
- X25 / itapac / videotel
- RAS / BBS
- 1-800-... / green
- Layer 1 (Physical)

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC)

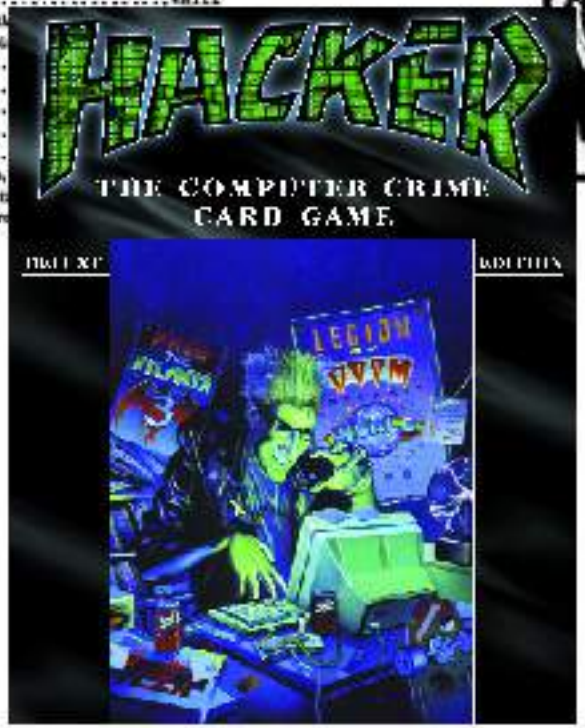
United States Marshals Service NCIC wanted number: (NIC/ W214609211)

NAME: .....MITNICK, KEVIN DAVID

AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: .....MALE
Race: .....WHITE



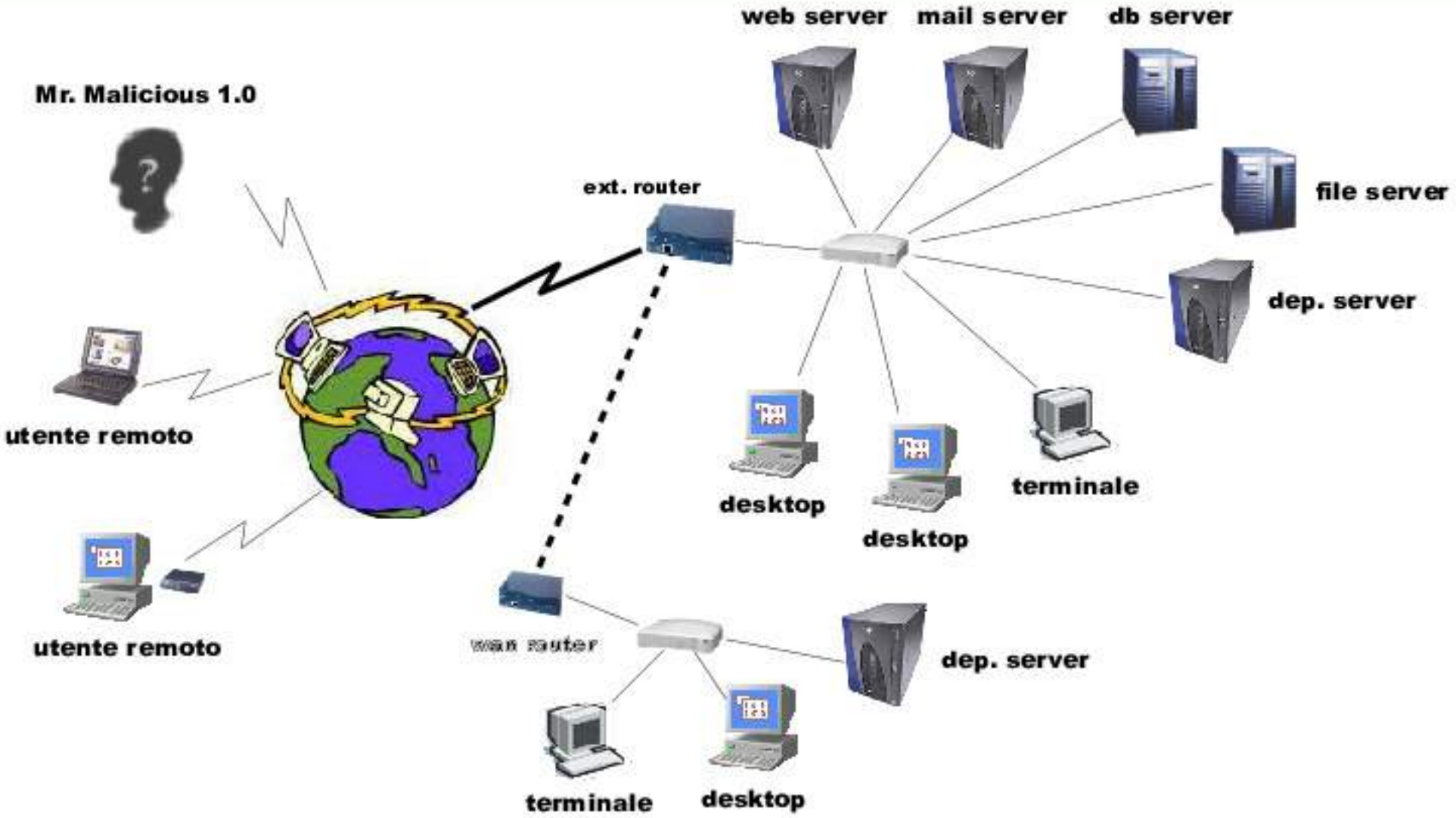
Internet 1.0

1980..

- social engineering (mail)
- malware (worm, dialer)
- attacchi client/server
  - basso numero di sistemi
  - nessun firewall
  - scarsa conoscenza tecniche di attacco
- DOS (Denial of Service)

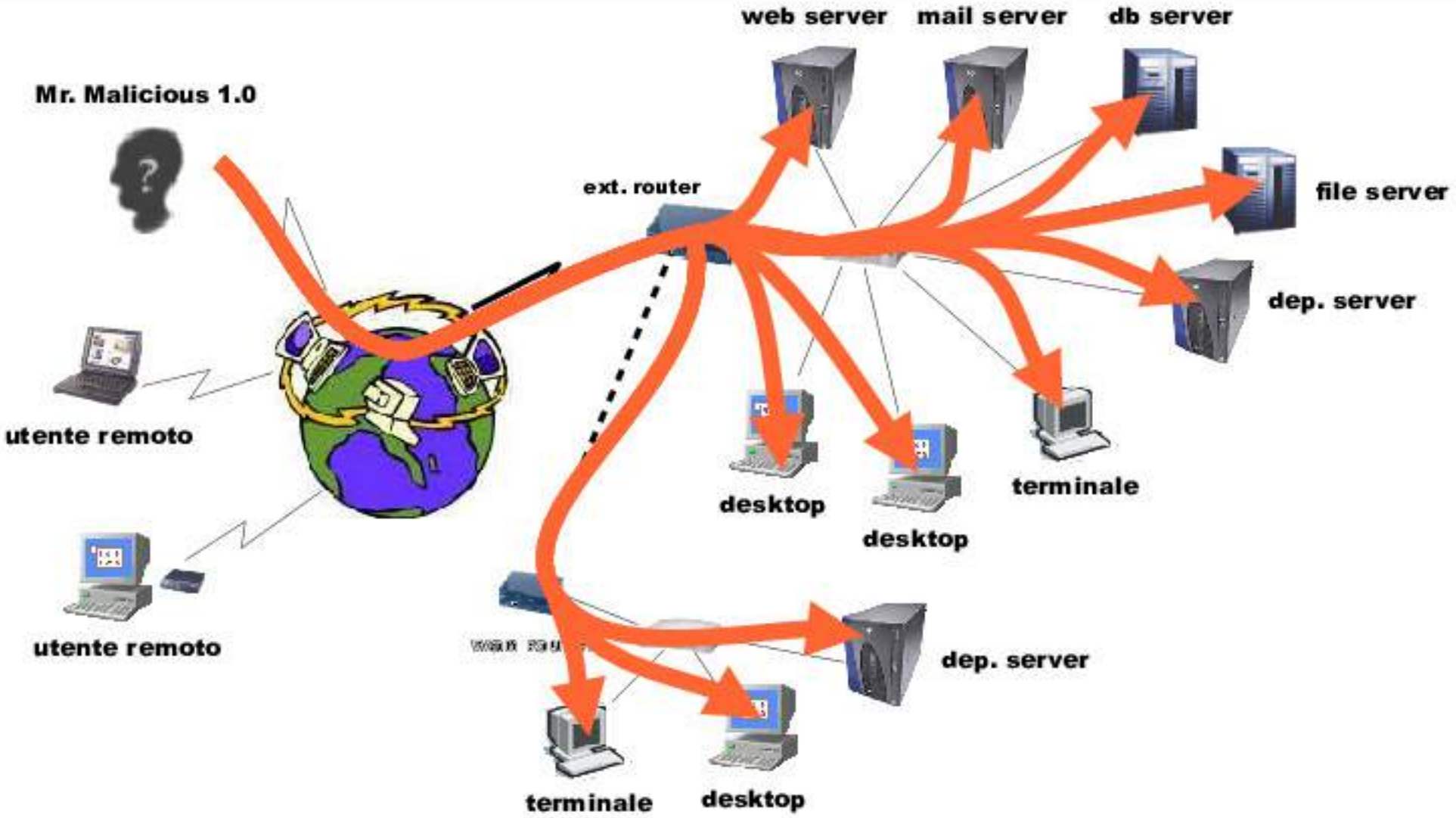
Own1ng the Enterprise 1.0

in una Internet remota, molti anni fa ..



Discovery...

Own1ng the Enterprise 1.0

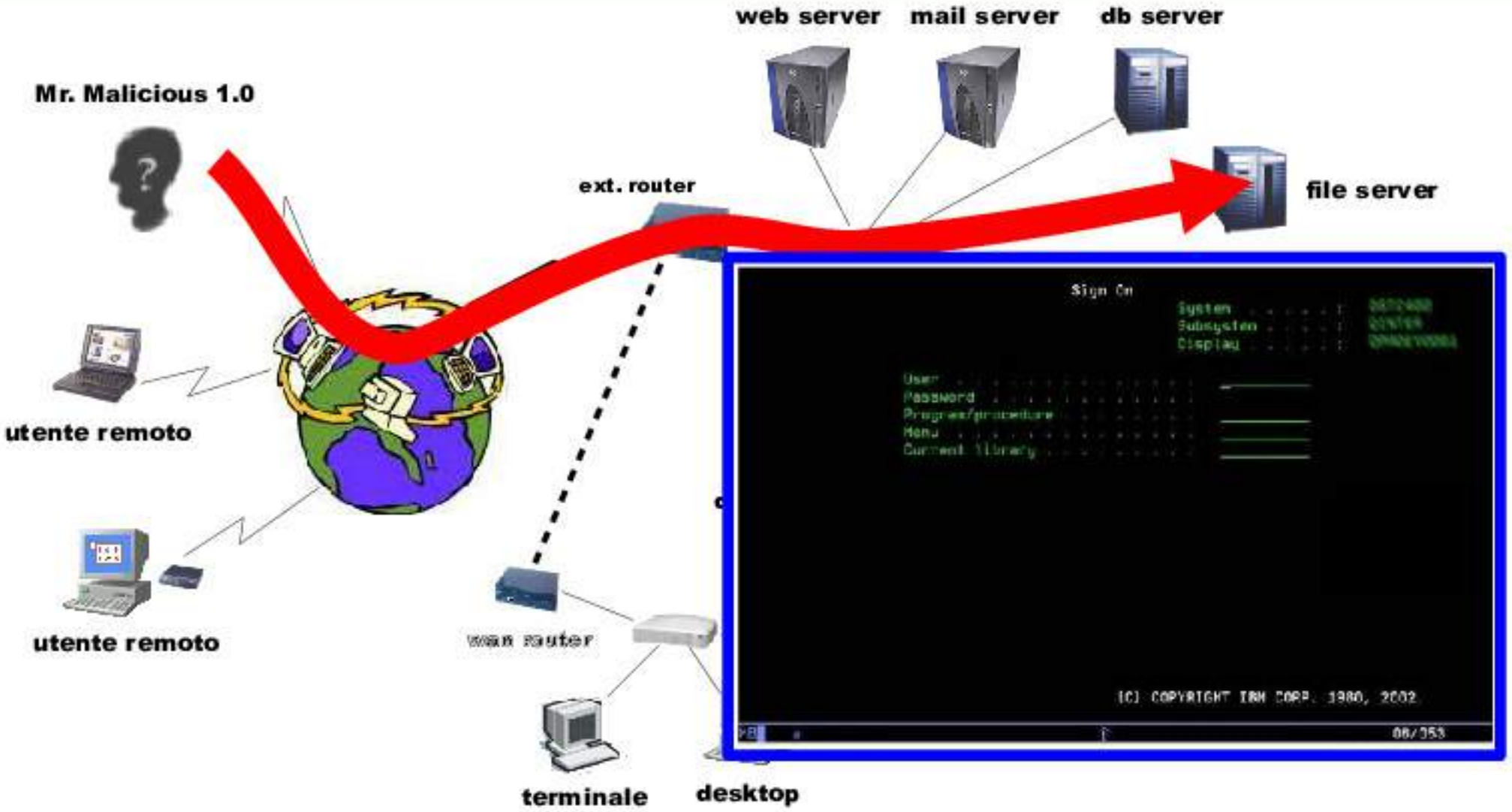


Discovery...

```
1.2.3.1:
          23/tcp       telnet  router

1.2.3.3:
           7/tcp       echo
           9/tcp       discard?
          13/tcp       daytime
          19/tcp       chargen
          21/tcp       ftp     10.x ftpd 4.1 (Tue May 15 16:38:46 CDT 2001)
          23/tcp       telnet  telnetd
          25/tcp       smtp    8.9.3/8.9.3 (AIX 4.3)
          37/tcp       time    bits)
          53/tcp       domain  Bind 8.X
         512/tcp       exec    rexecd
         513/tcp       rlogin
        1002/tcp       status  (rpc #100024)
        1521/tcp       oracle-tns      TNS Listener

1.2.3.11:
        1080/tcp       socks5  authentication required
        8080/tcp       http-proxy      webproxy 2.4.STABLE1

1.2.3.12:
          80/tcp       http    IIS webserver 4.0
         135/tcp       msrpc   Windows RPC
         139/tcp       netbios-ssn
        5900/tcp       vnc     (protocol 3.1)
```

Exploiting...

0wn1ng the Enterprise 1.0



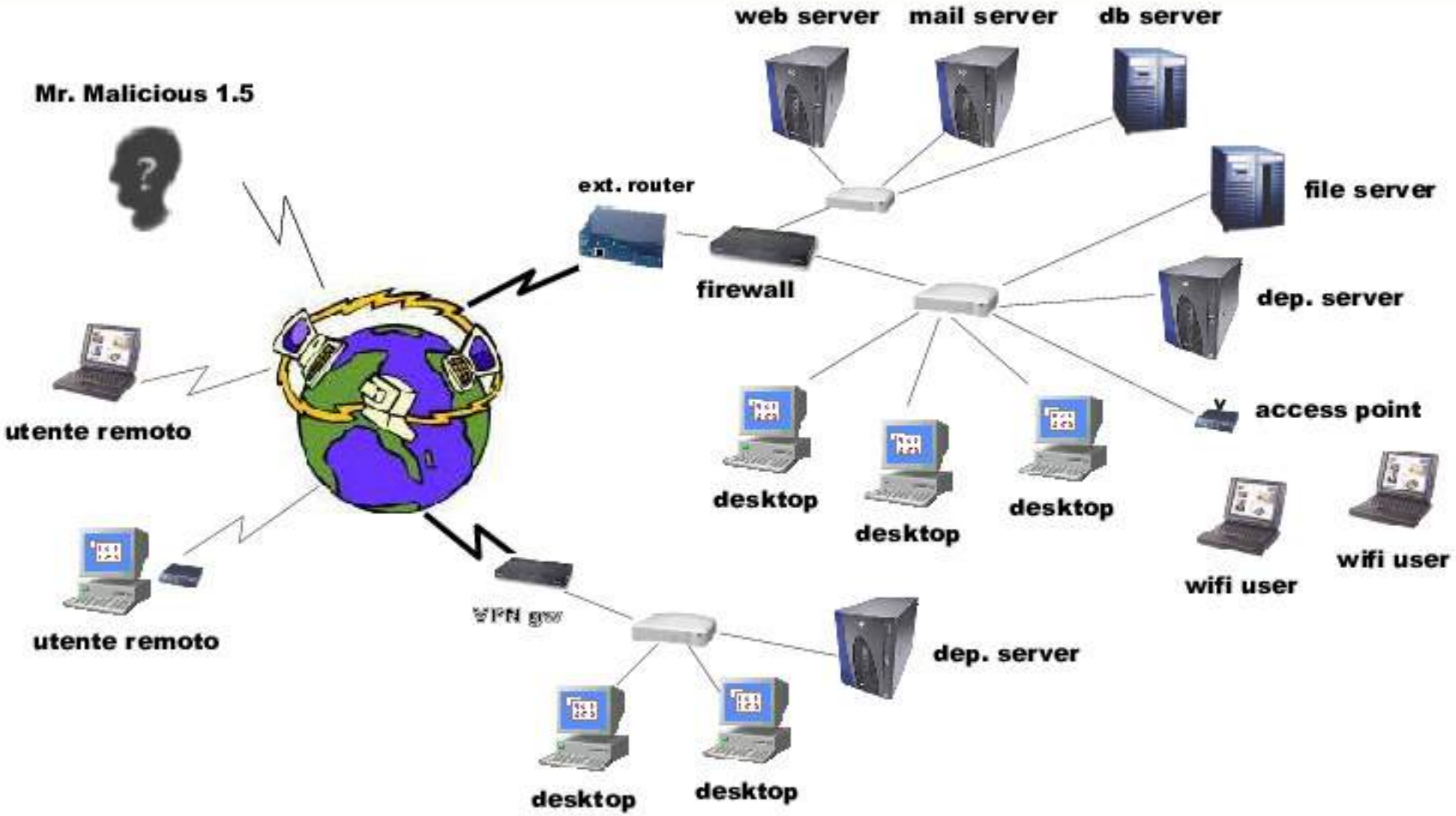
Internet 1.5

2000..

- **social engineering** (fake web / phishing)
- **malware**
  - spyware
  - keylogger
  - bank-aware
- **applicazioni web**
- **wireless** (wardriving, no encryption, WEP, ..)
- **DDOS** (Distributed Denial of Service)

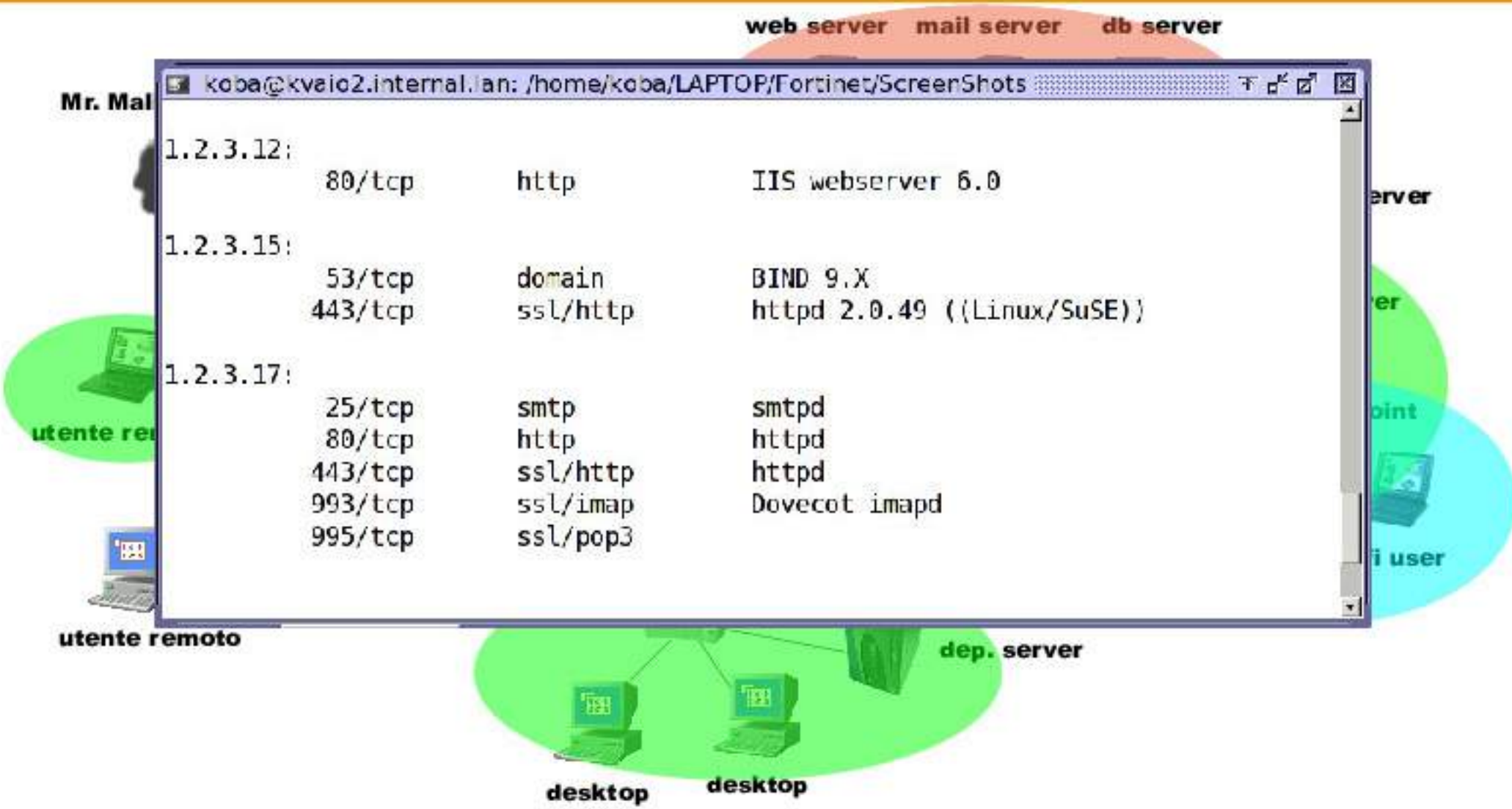
Discovery...

Own1ng the Enterprise 1.5



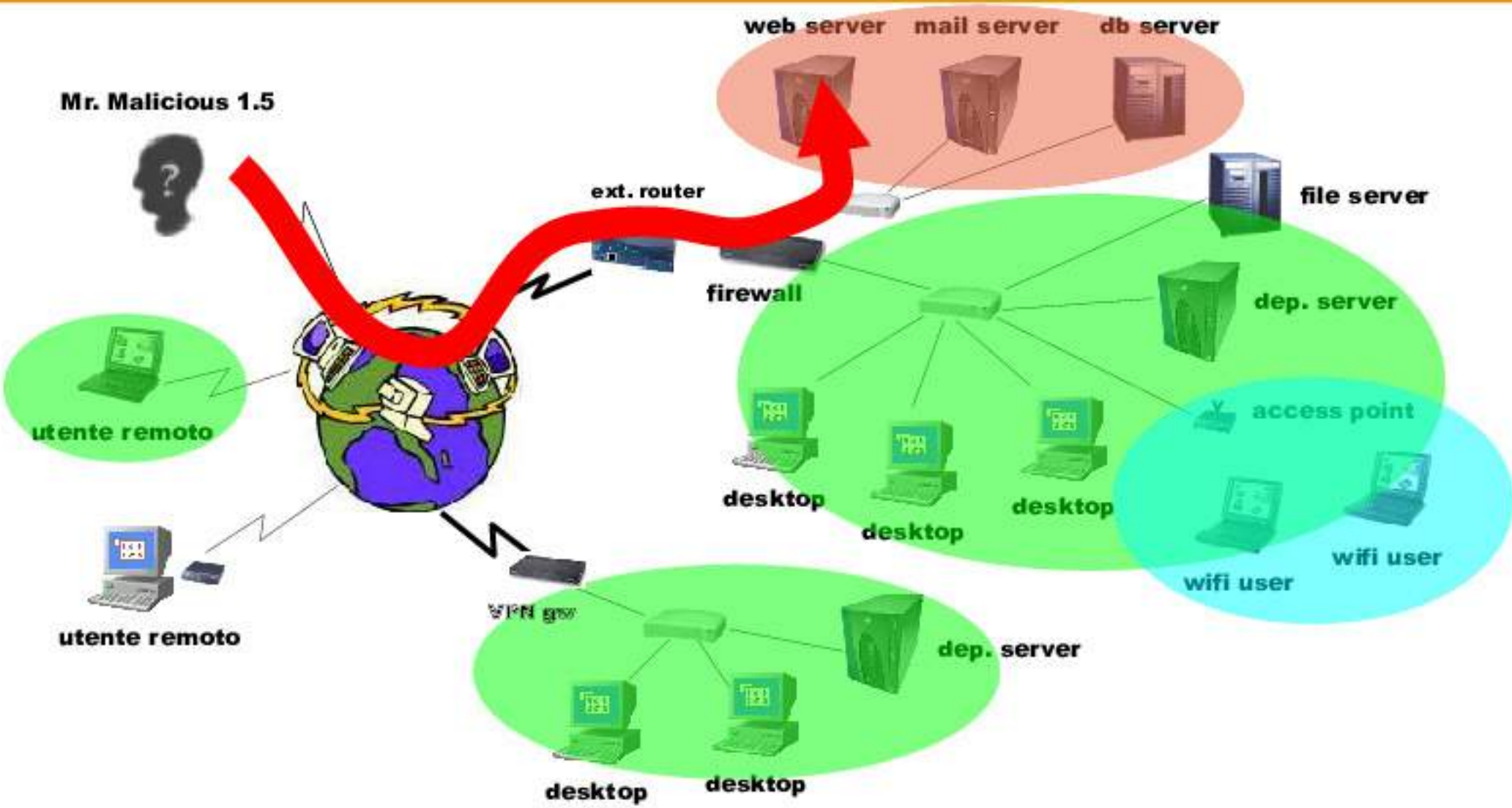
Discovery...

Own1ng the Enterprise 1.5



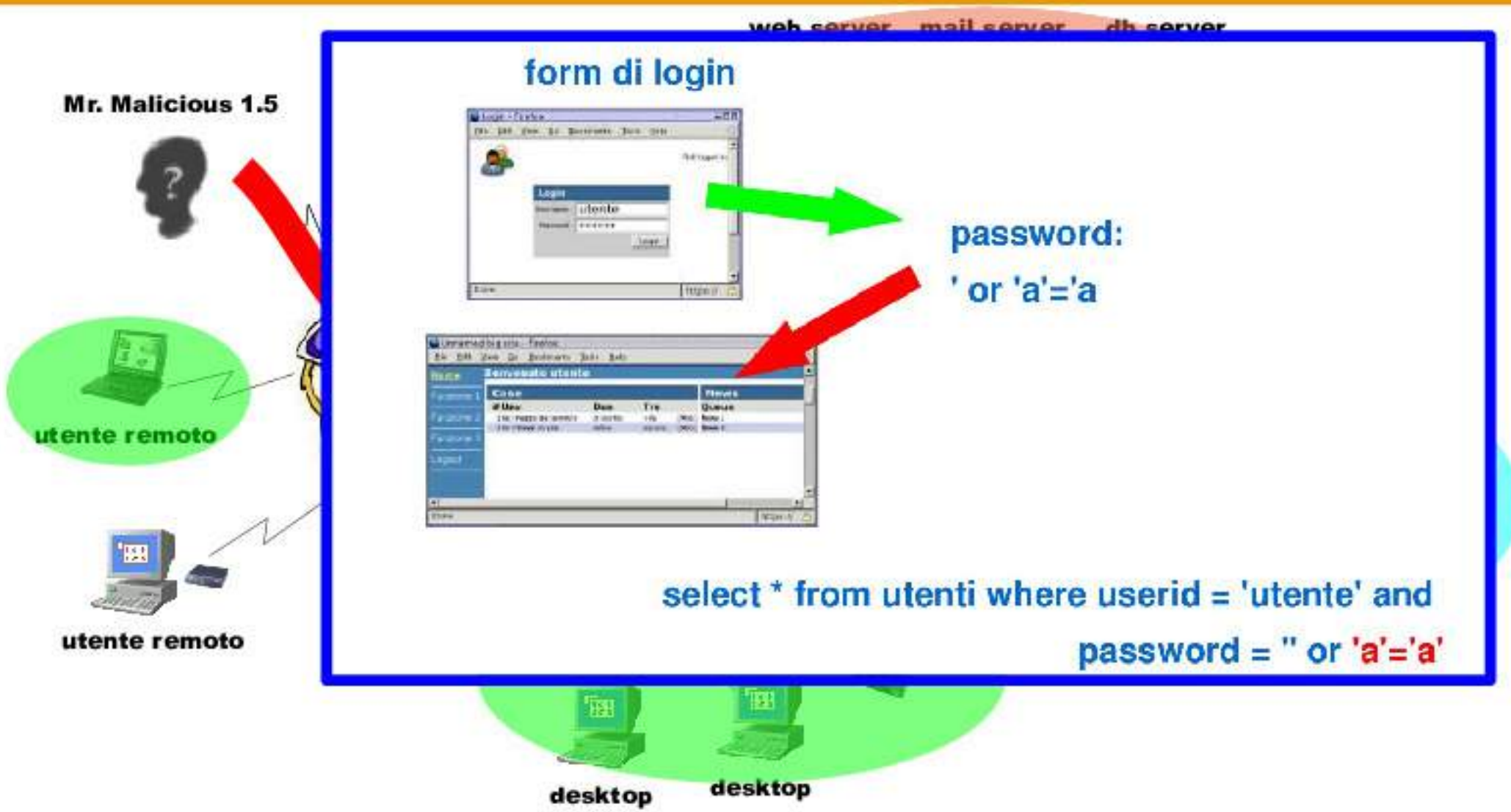
Exploiting...

0wn1ng the Enterprise 1.5



Exploiting...

Own1ng the Enterprise 1.5



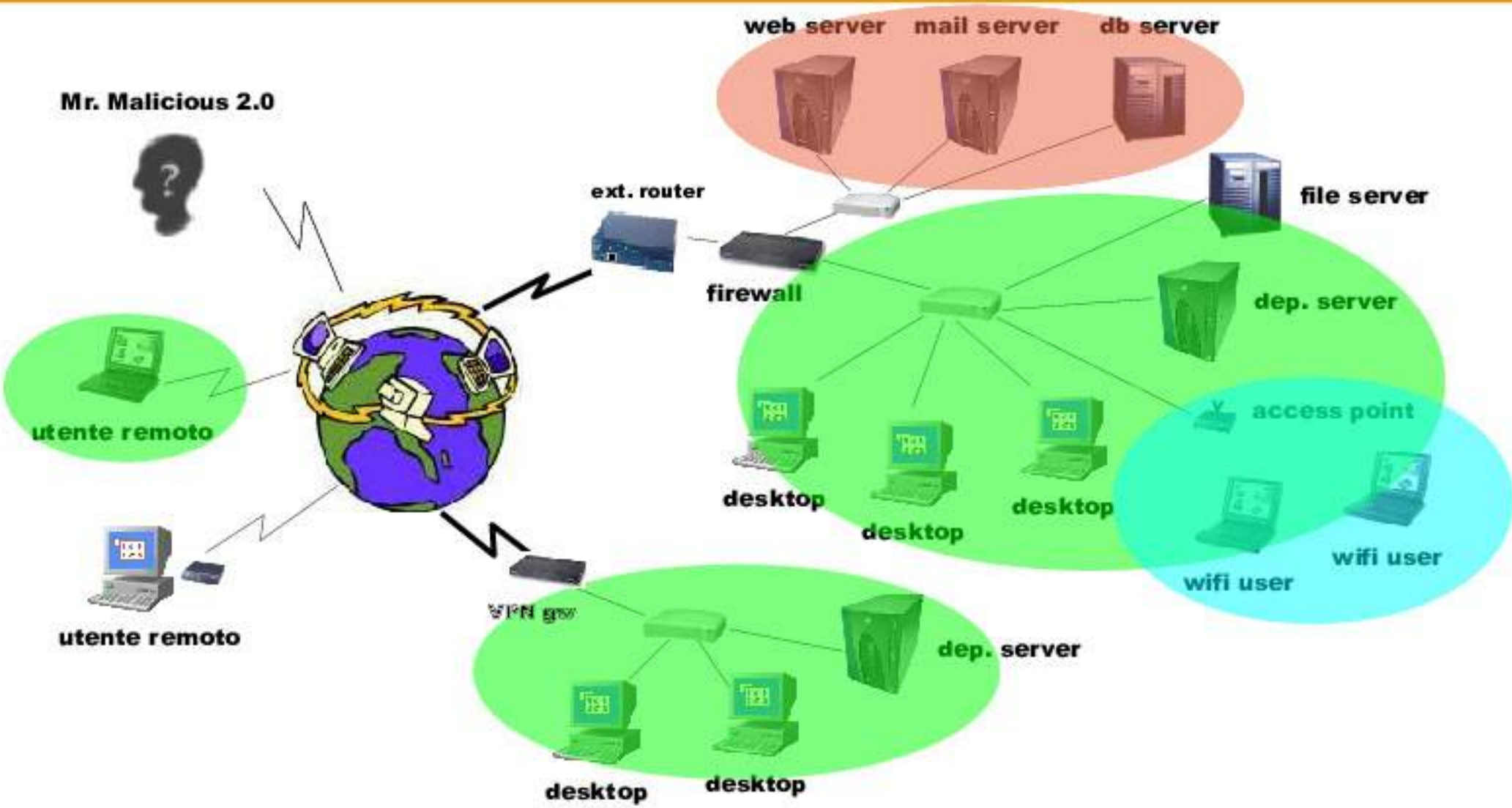
Internet 2.0

2005..

- social engineering
  - social network / messenger
- client-side attack
  - Cross Site Scripting & Co.
  - exploit applicazioni “client” -> LAN
  - mobile
- cloud lifestyle (Single Sign Own)

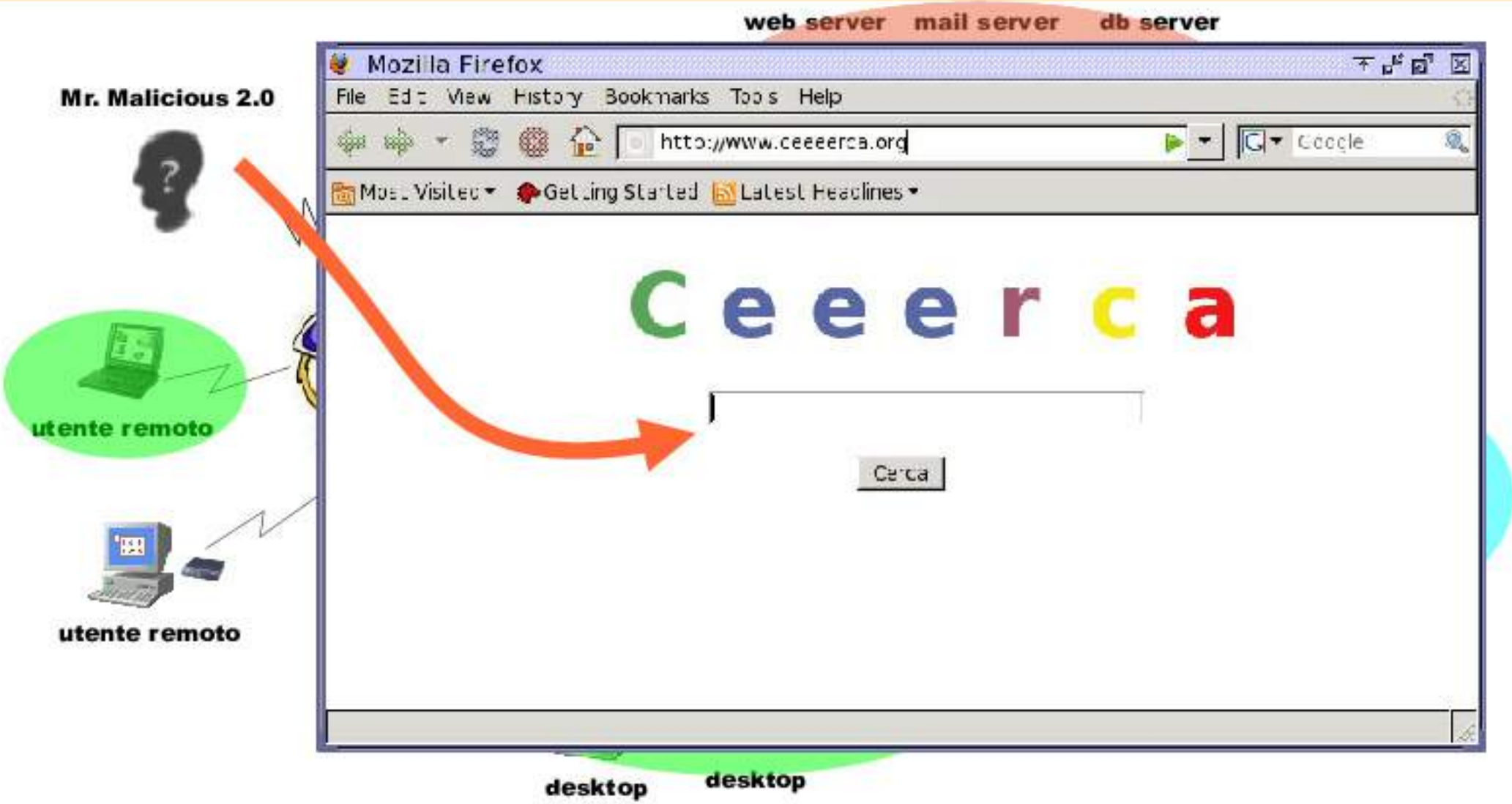
Discovery...

0wn1ng the Enterprise 2.0



Discovery...

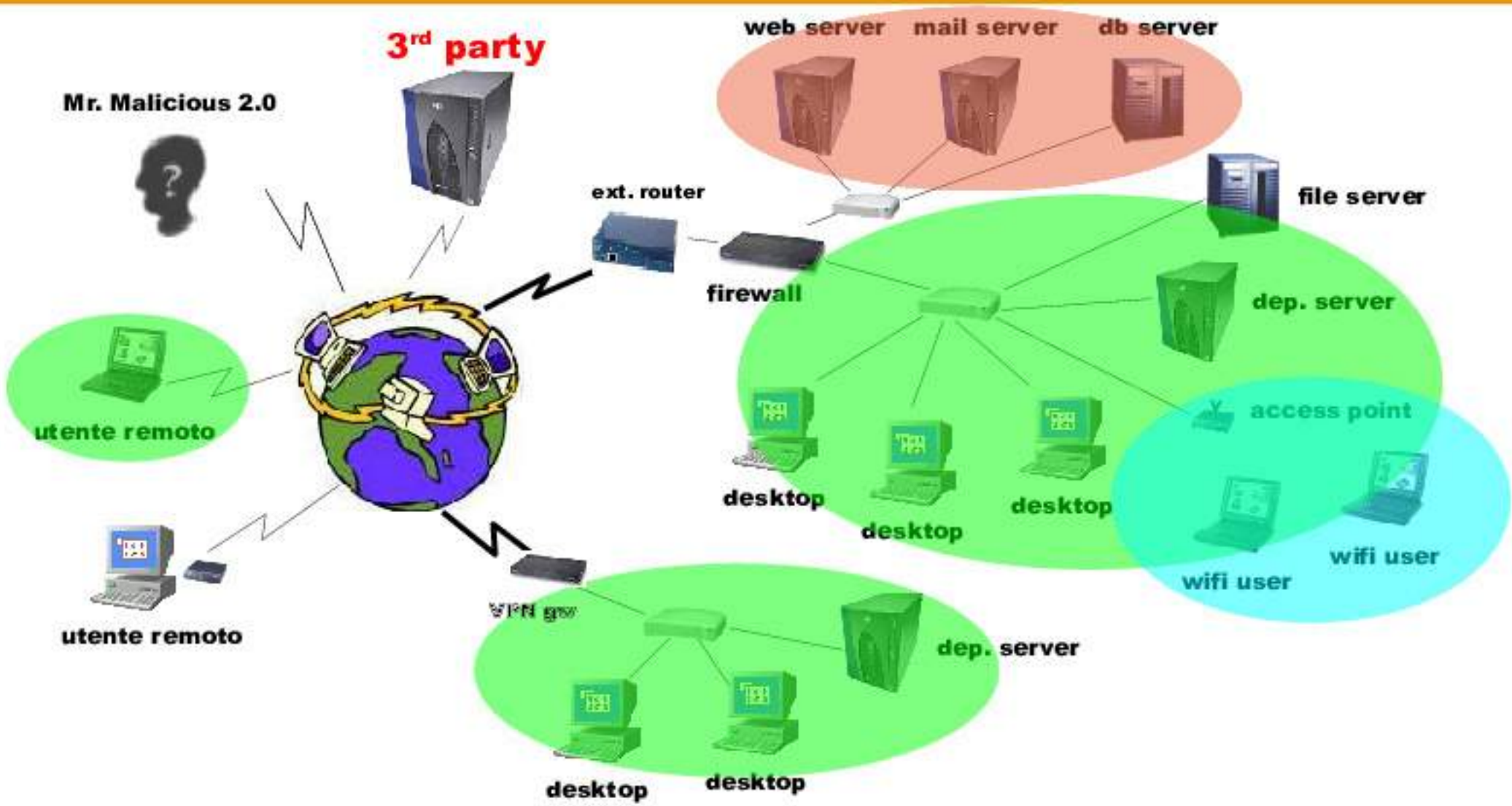
0wn1ng the Enterprise 2.0



Discovery...

Exploiting...

0wn1ng the Enterprise 2.0



Exploiting...

0wn1ng the Enterprise 2.0

Il presente..

2010(*)..

- **malware**
  - **targetted spyware**
  - **SCADA (Stuxnet, ..)**
  - **mobile**
  - **mass exploiter**
- **VoIP phreaking**
- **SCADA (Smart cities, Internet of things, ..)**
- **“App” (e back-end)**

Riassumendo..

Social engineering 2.0

img src: http://bits.blogs.nytimes.com/2007/10/30/bill-gates-has-joined-facebook-he-has-friends/

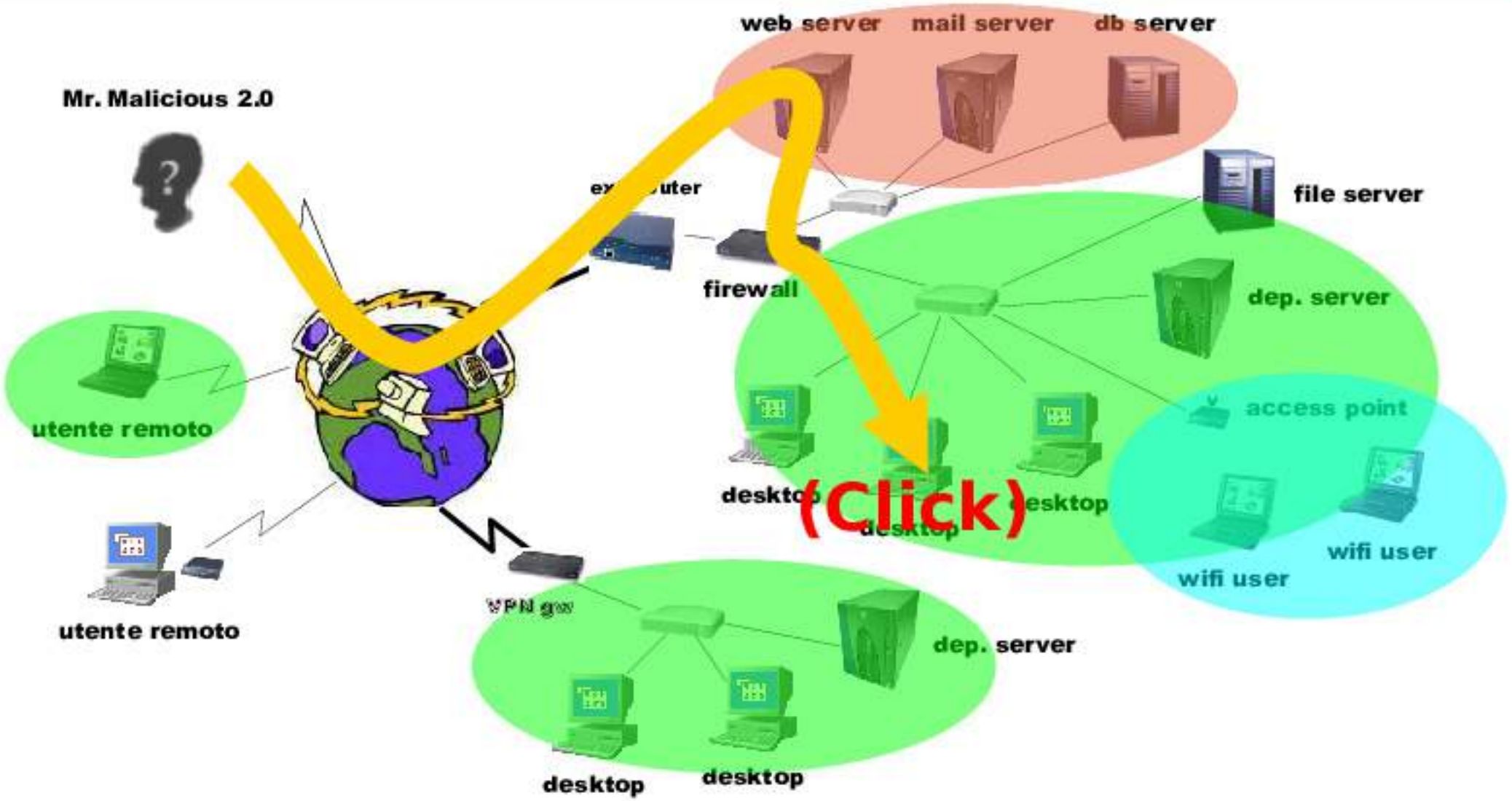
Hey, sono Bill, il collega di Canicattì... ti ricordi?

Hey Bill.. come va?
sei ancora al marketing?

...

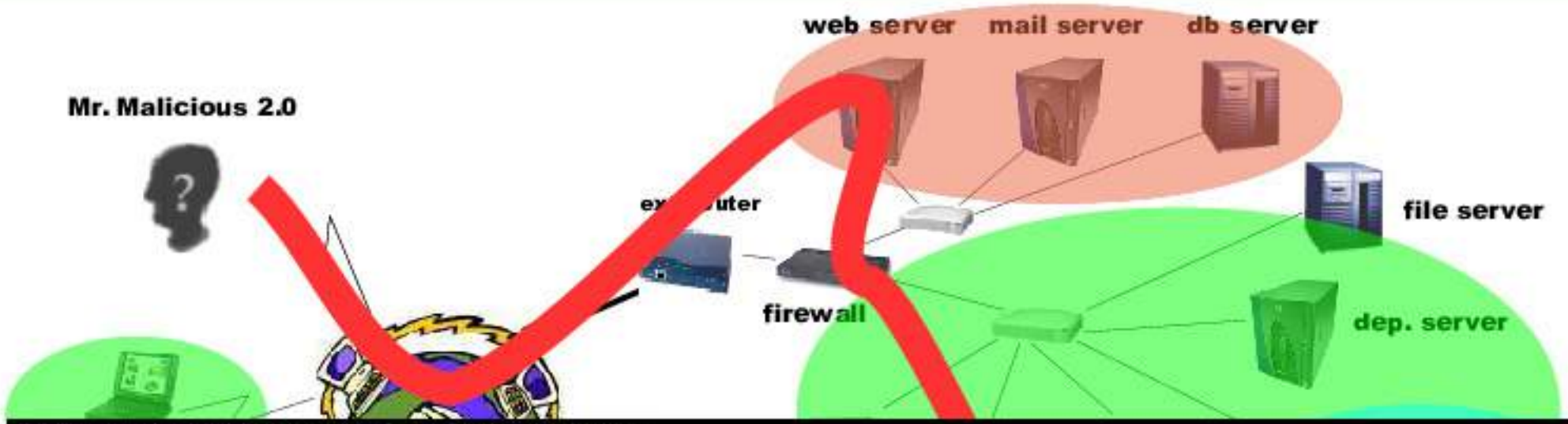
Scenario 1: utenti

malware



Scenario 1: utenti

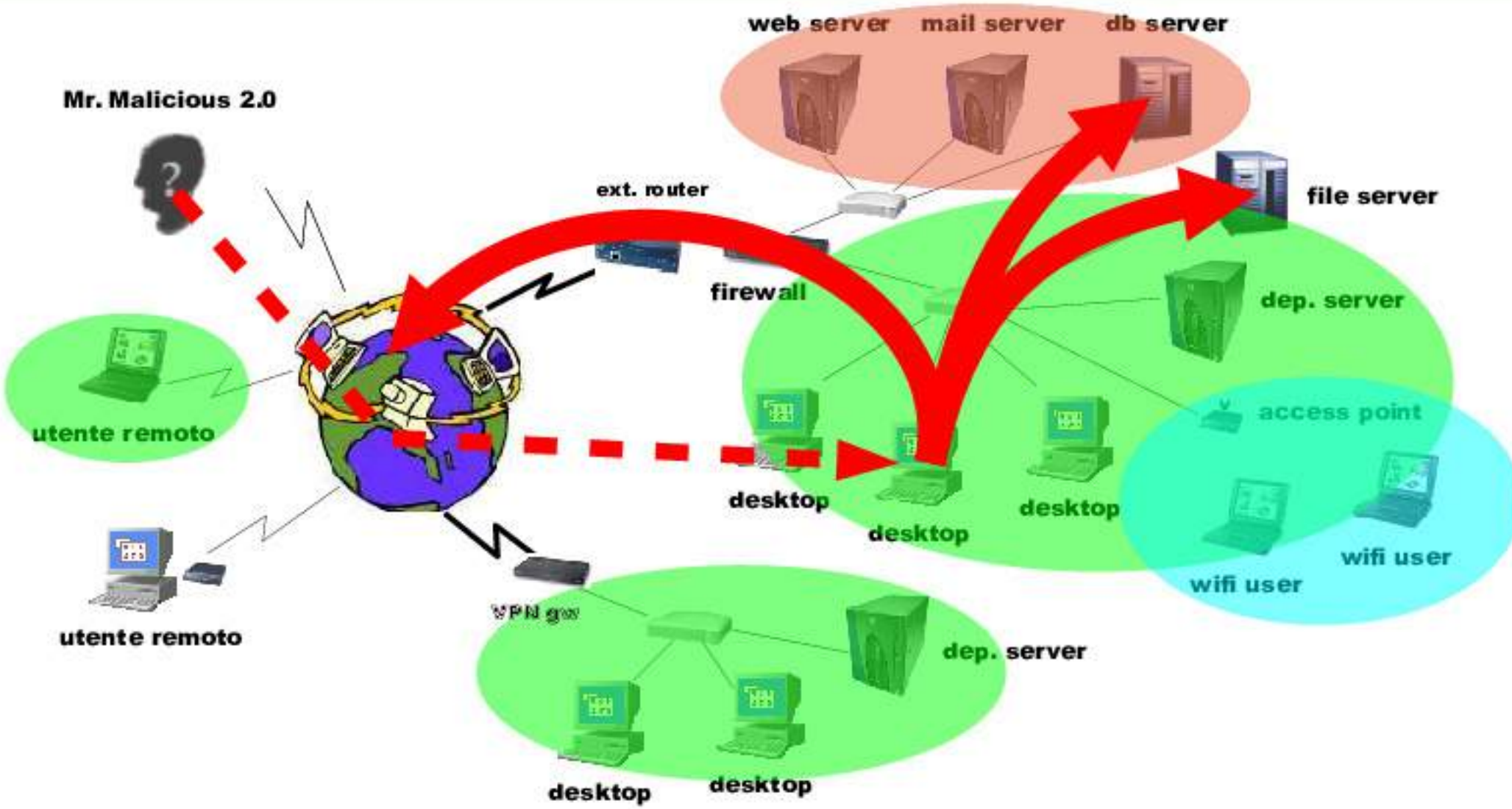
malware




```
C:\Documents and Settings\baltar\Desktop>dir C:\
dir C:\
 Il volume nell'unità C non ha etichetta.
 Numero di serie del volume: 6813-B985

 Directory di C:\

21/10/2010  14.54                 0 AUTOEXEC.BAT
21/10/2010  14.54                 0 CONFIG.SYS
21/10/2010  15.11    <DIR>          Documents and Settings
21/10/2010  15.11    <DIR>          Programmi
21/10/2010  15.11    <DIR>          WINDOWS
               2 File                0 byte
               3 Directory   8.961.507.328 byte disponibili

C:\Documents and Settings\baltar\Desktop>
```

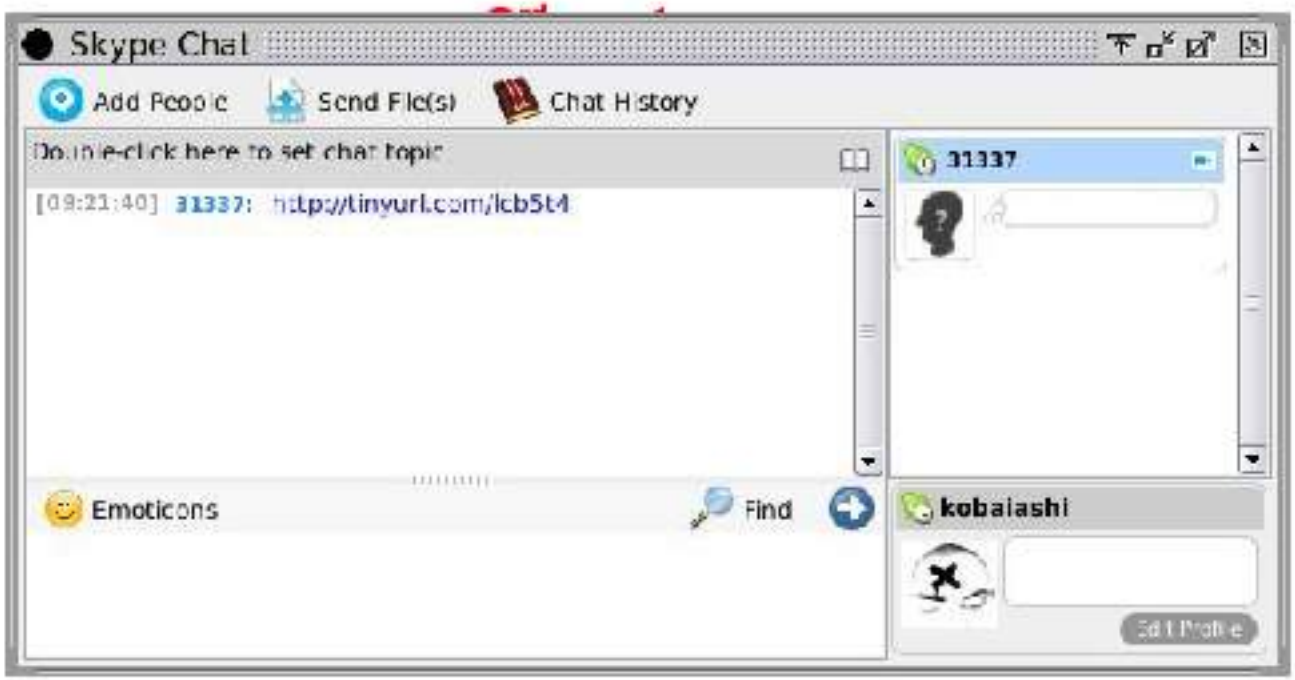

Scenario 1: utenti

malware



URL “shortener”

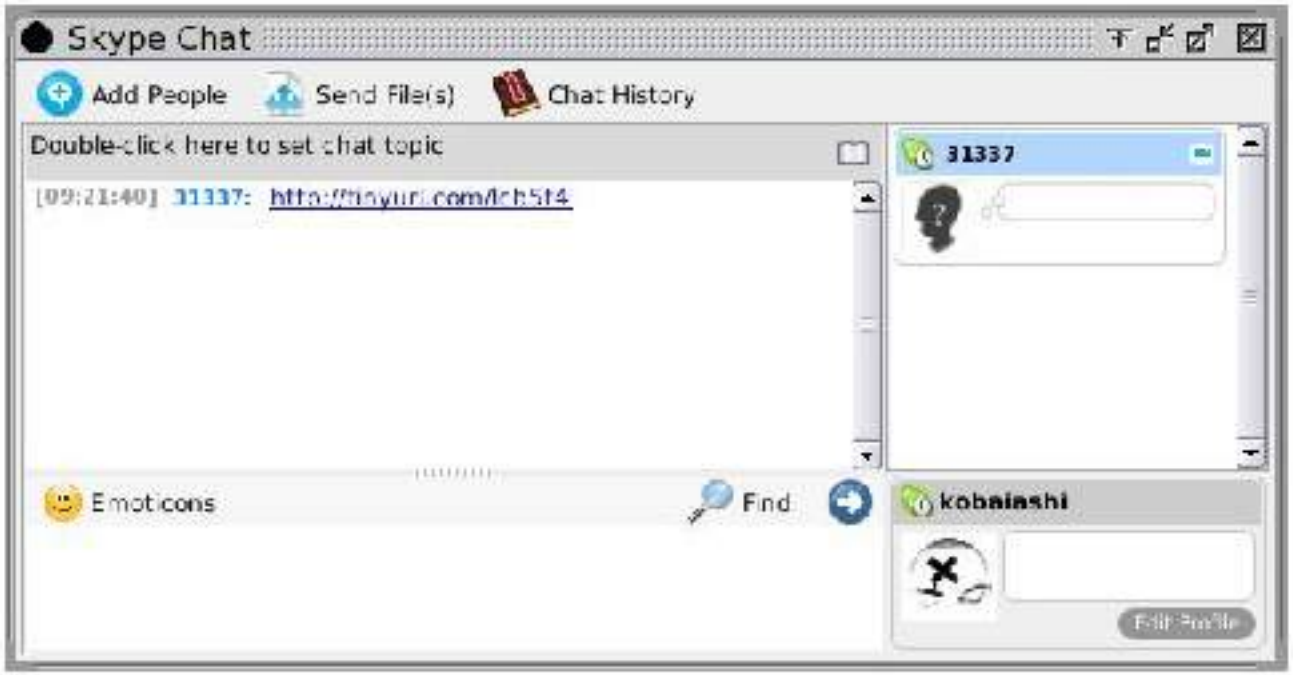
..come offuscare un link con un semplice click



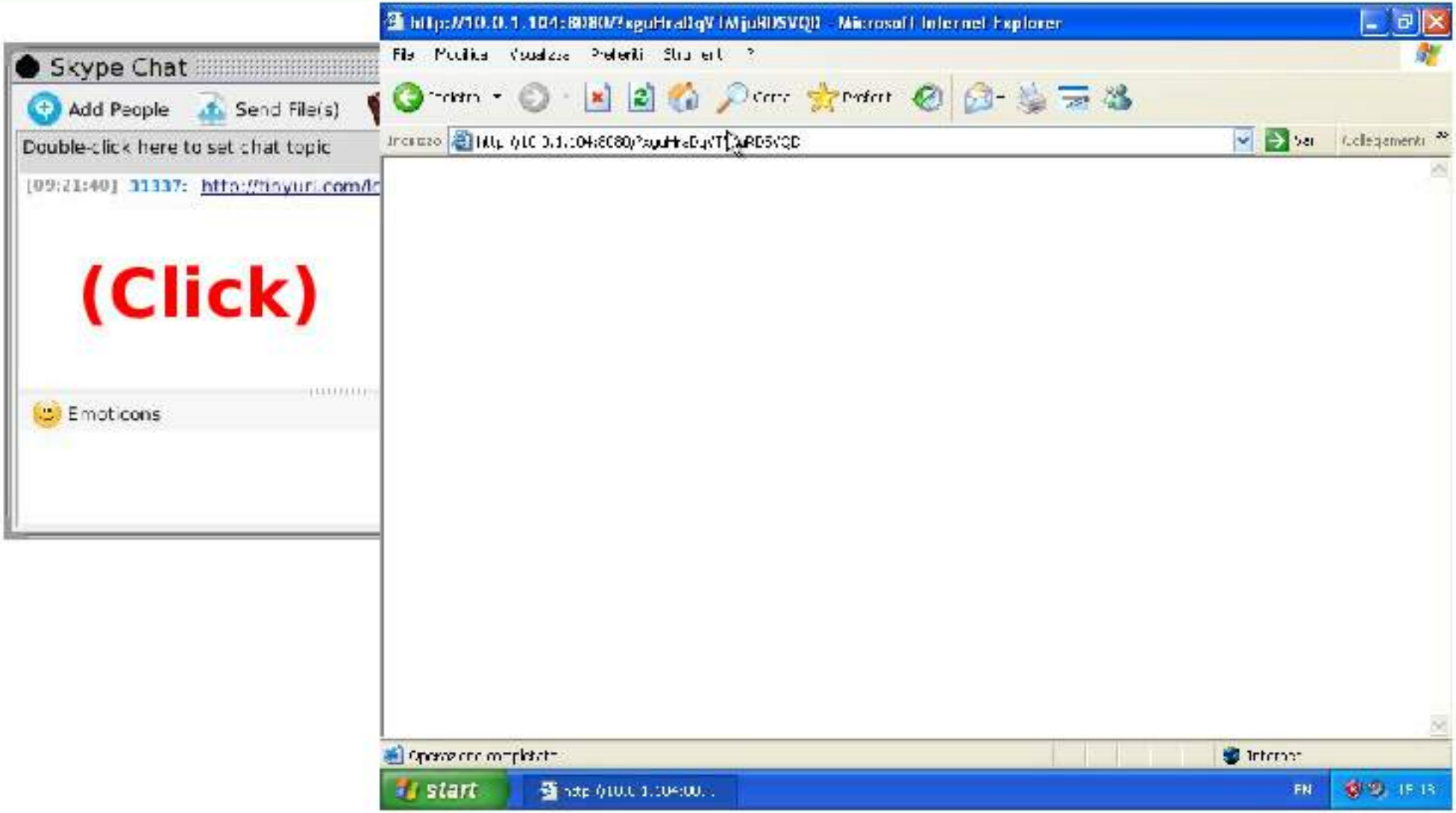
URL “shortener”

..come offuscare un link con un semplice click

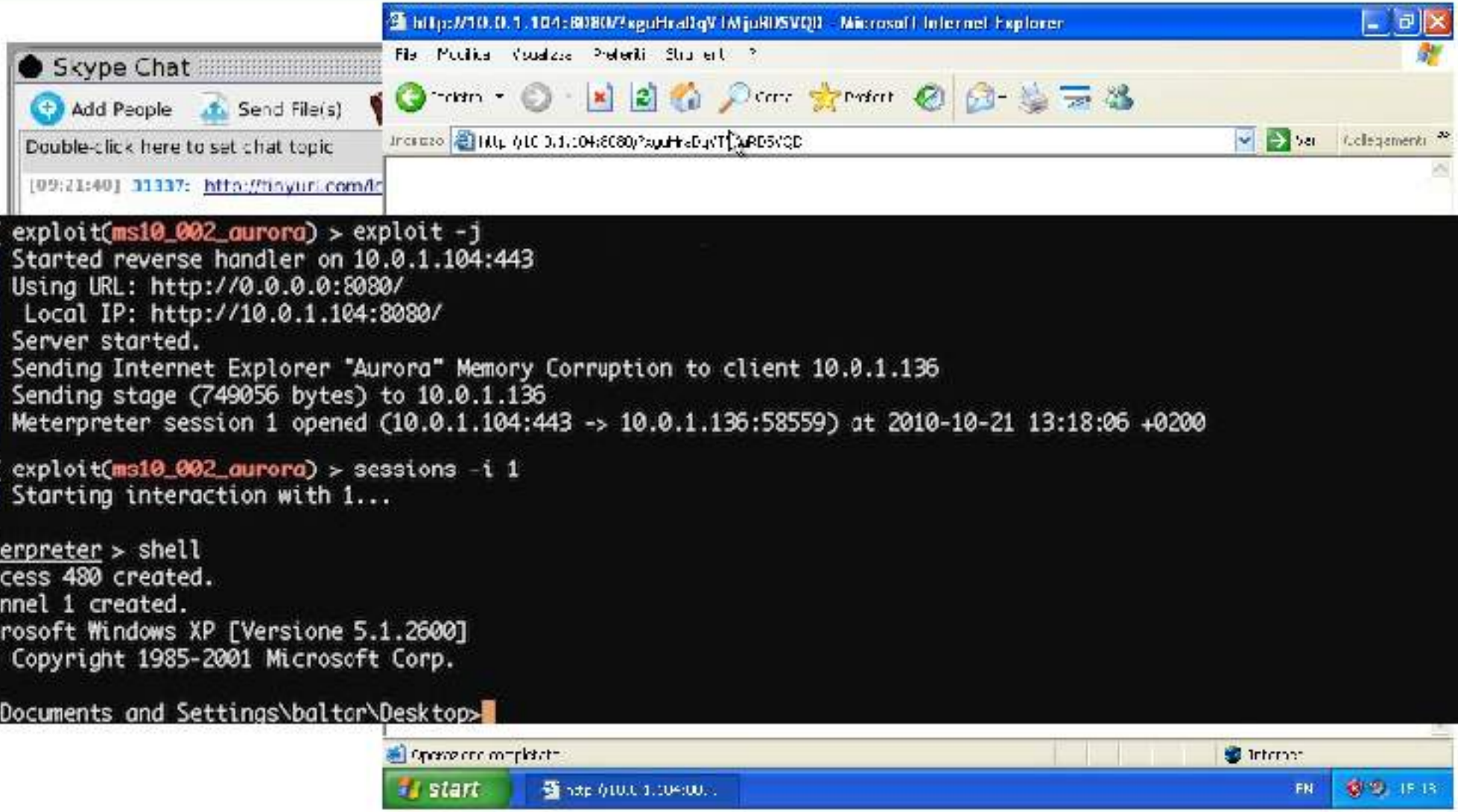
Client-side attack..



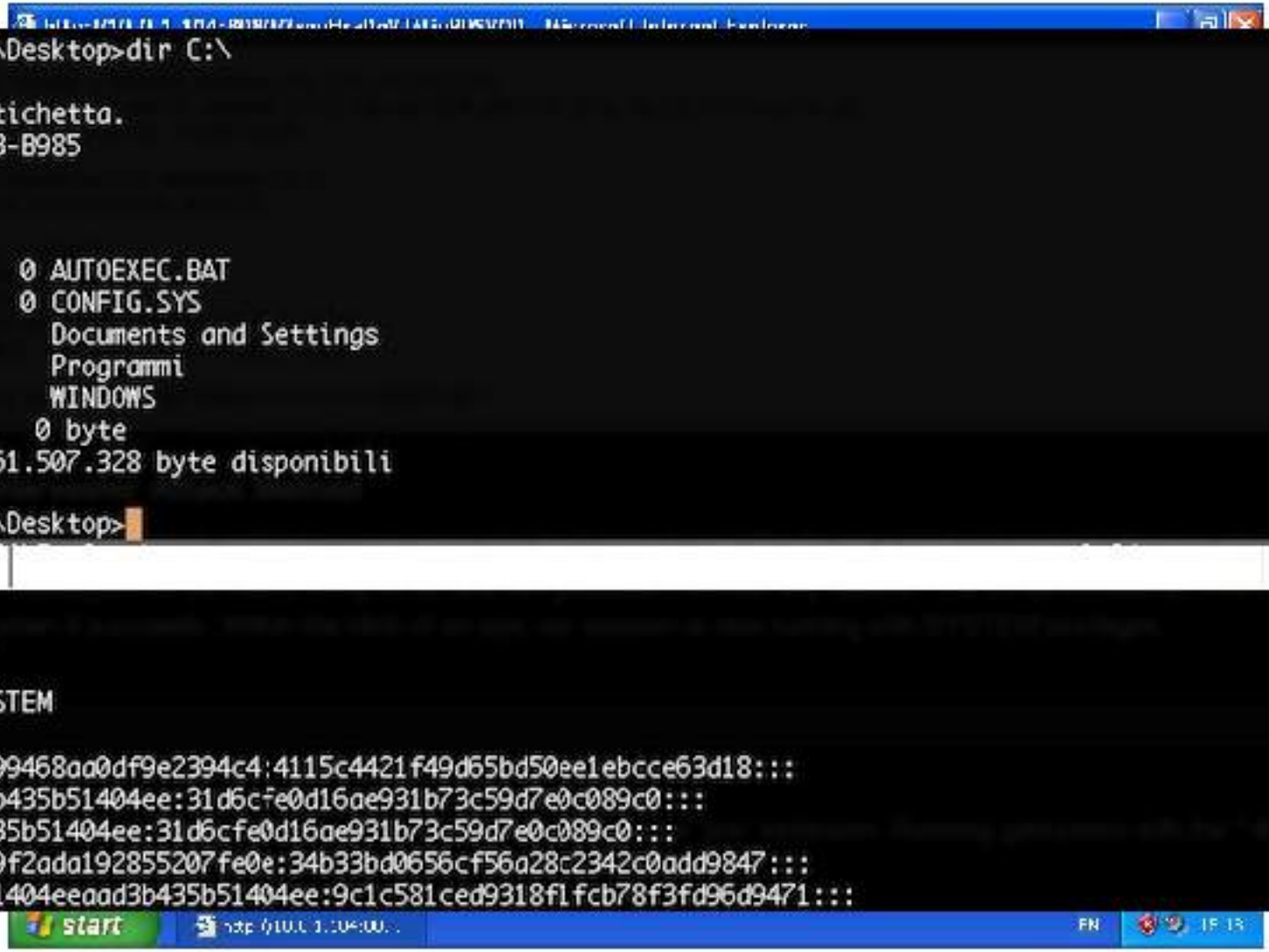
..un click per..



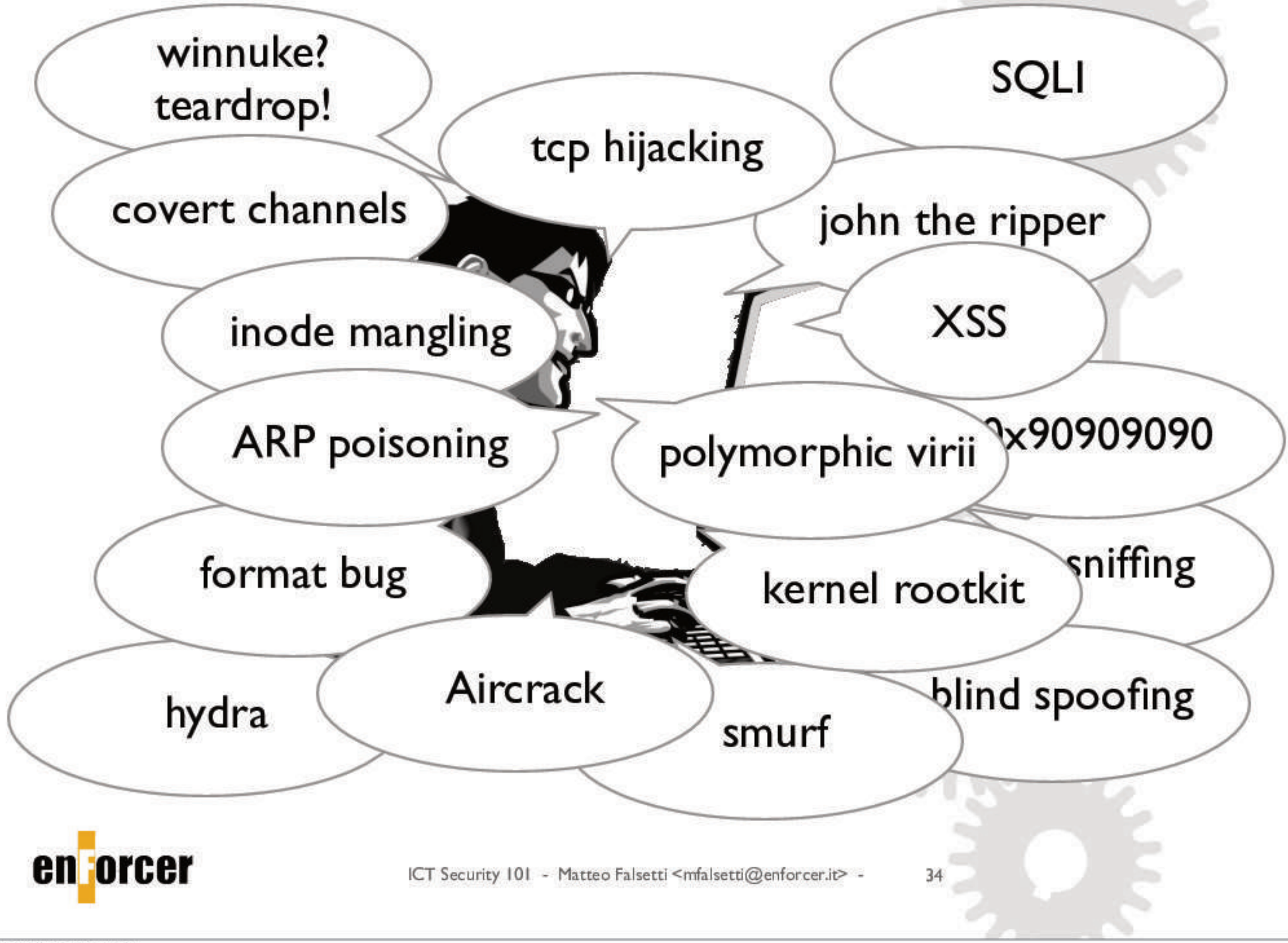
..avere la stazione compromessa



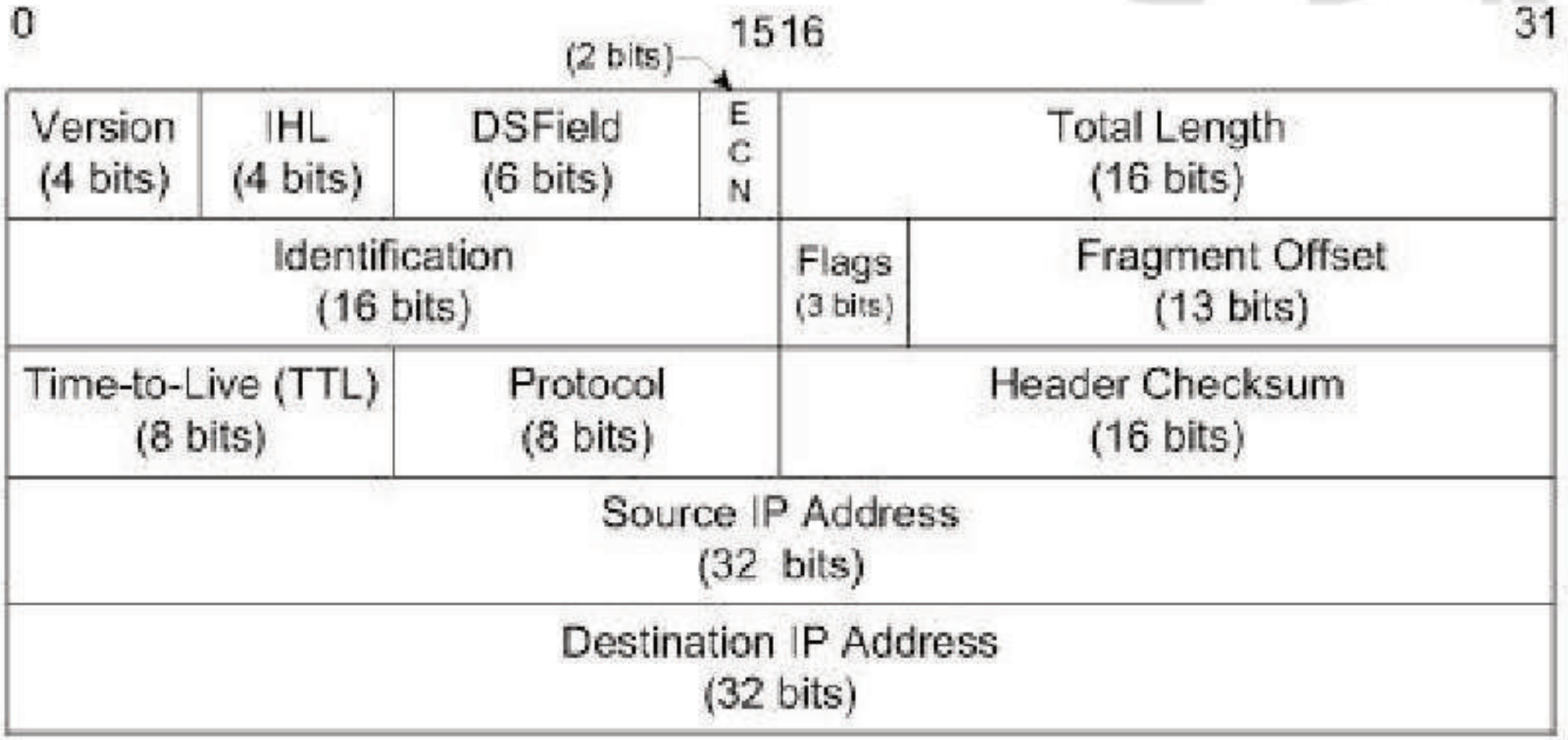
..avere la stazione compromessa



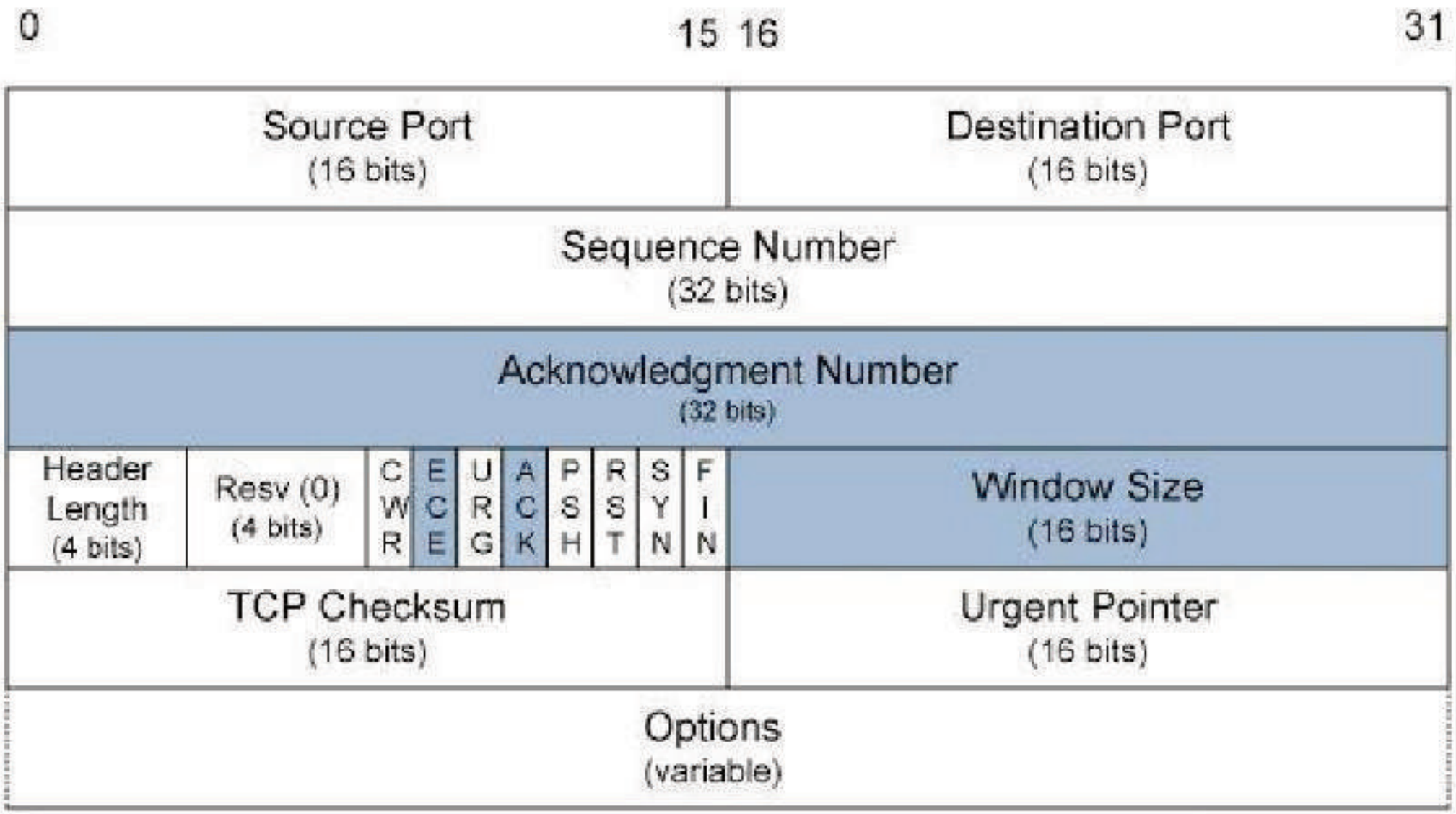
"Pivoting"


winnuke?
teardrop!
tcp hijacking
SQLI
covert channels
john the ripper
inode mangling
XSS
ARP poisoning
polymorphic virii
0x90909090
format bug
kernel rootkit
sniffing
hydra
Aircrack
smurf
blind spoofing

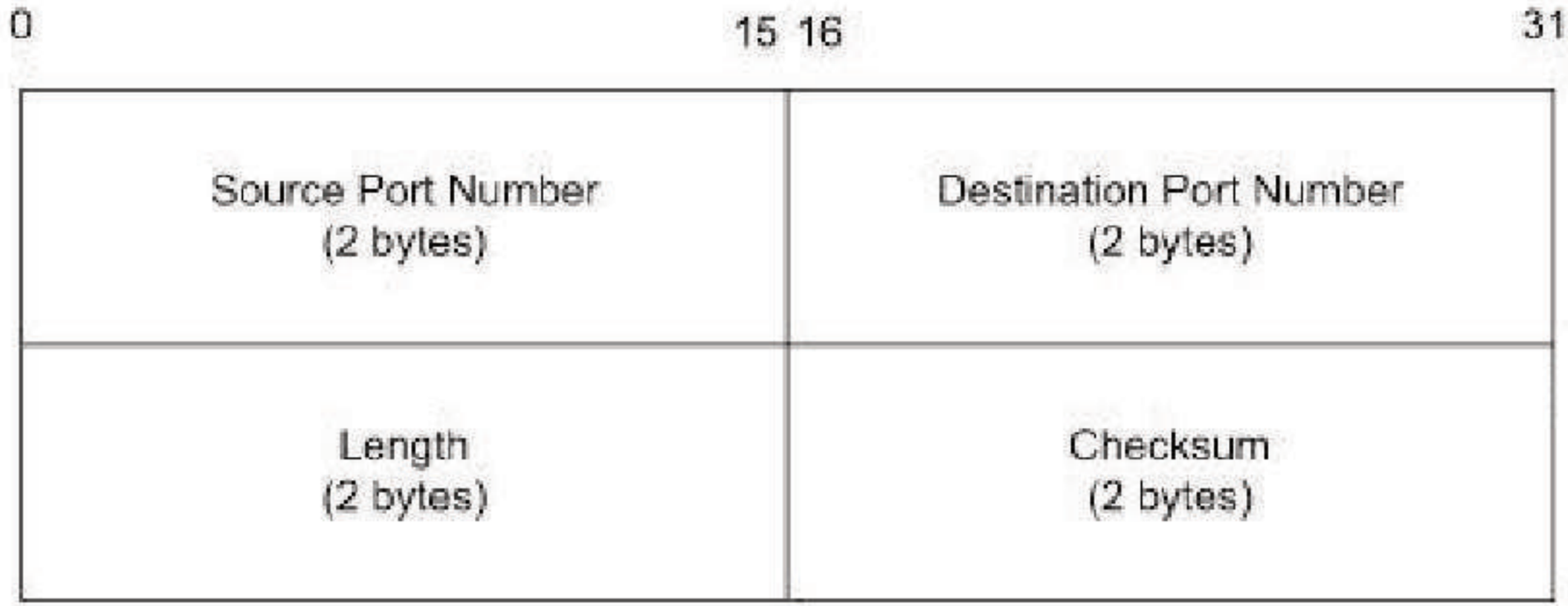
IPv4 header


0
15 16
31
(2 bits)
Version (4 bits)
IHL (4 bits)
DSField (6 bits)
ECN
Total Length (16 bits)
Identification (16 bits)
Flags (3 bits)
Fragment Offset (13 bits)
Time-to-Live (TTL) (8 bits)
Protocol (8 bits)
Header Checksum (16 bits)
Source IP Address (32 bits)
Destination IP Address (32 bits)

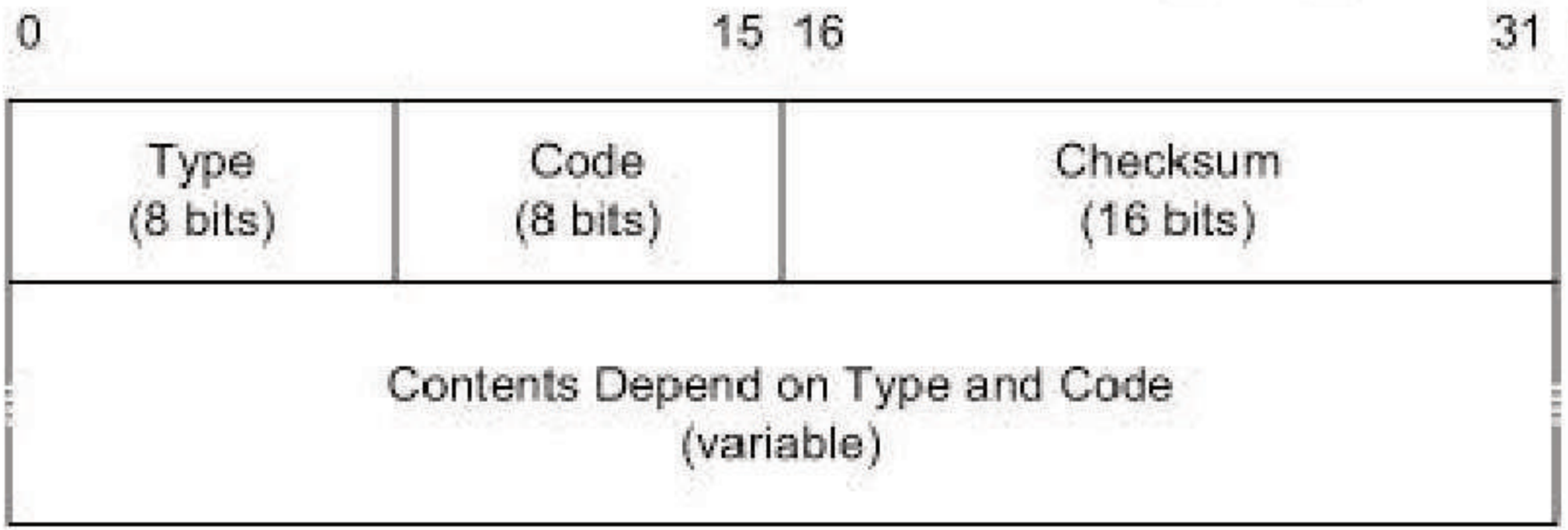
TCP header


0
15 16
31
Source Port
(16 bits)
Destination Port
(16 bits)
Sequence Number
(32 bits)
Acknowledgment Number
(32 bits)
Header Length
(4 bits)
Resv (0)
(4 bits)
CWR
ECE
URG
ACK
PSH
RST
SYN
FIN
Window Size
(16 bits)
TCP Checksum
(16 bits)
Urgent Pointer
(16 bits)
Options
(variable)

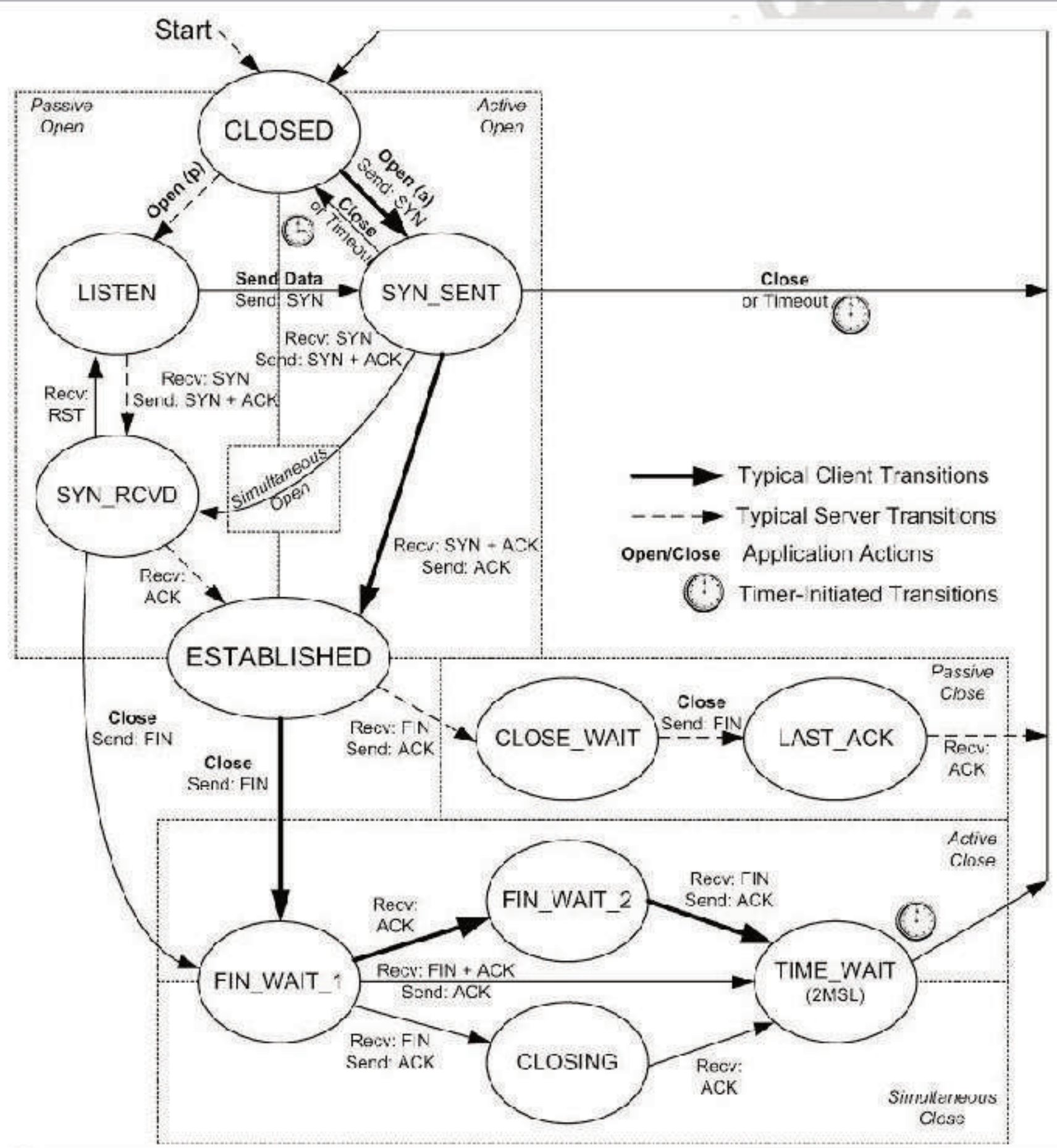
UDP header


0
15 16
31
Source Port Number
(2 bytes)
Destination Port Number
(2 bytes)
Length
(2 bytes)
Checksum
(2 bytes)

ICMP header


0
15
16
31
Type
(8 bits)
Code
(8 bits)
Checksum
(16 bits)
Contents Depend on Type and Code
(variable)

tcp/ip 101



enforcer

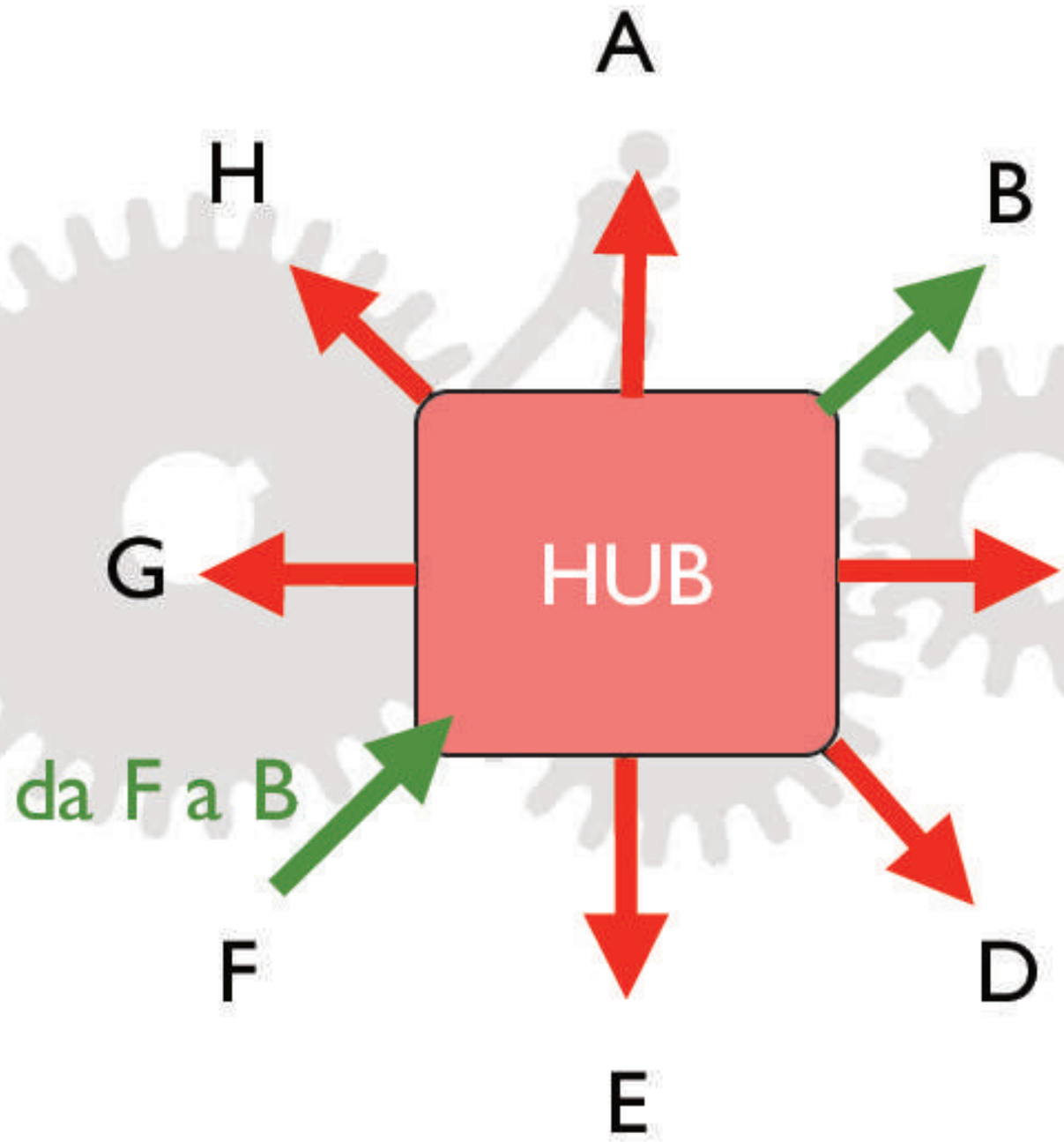
sniffing

Si definisce sniffing l'attività di intercettazione passiva dei dati che transitano in una rete telematica.

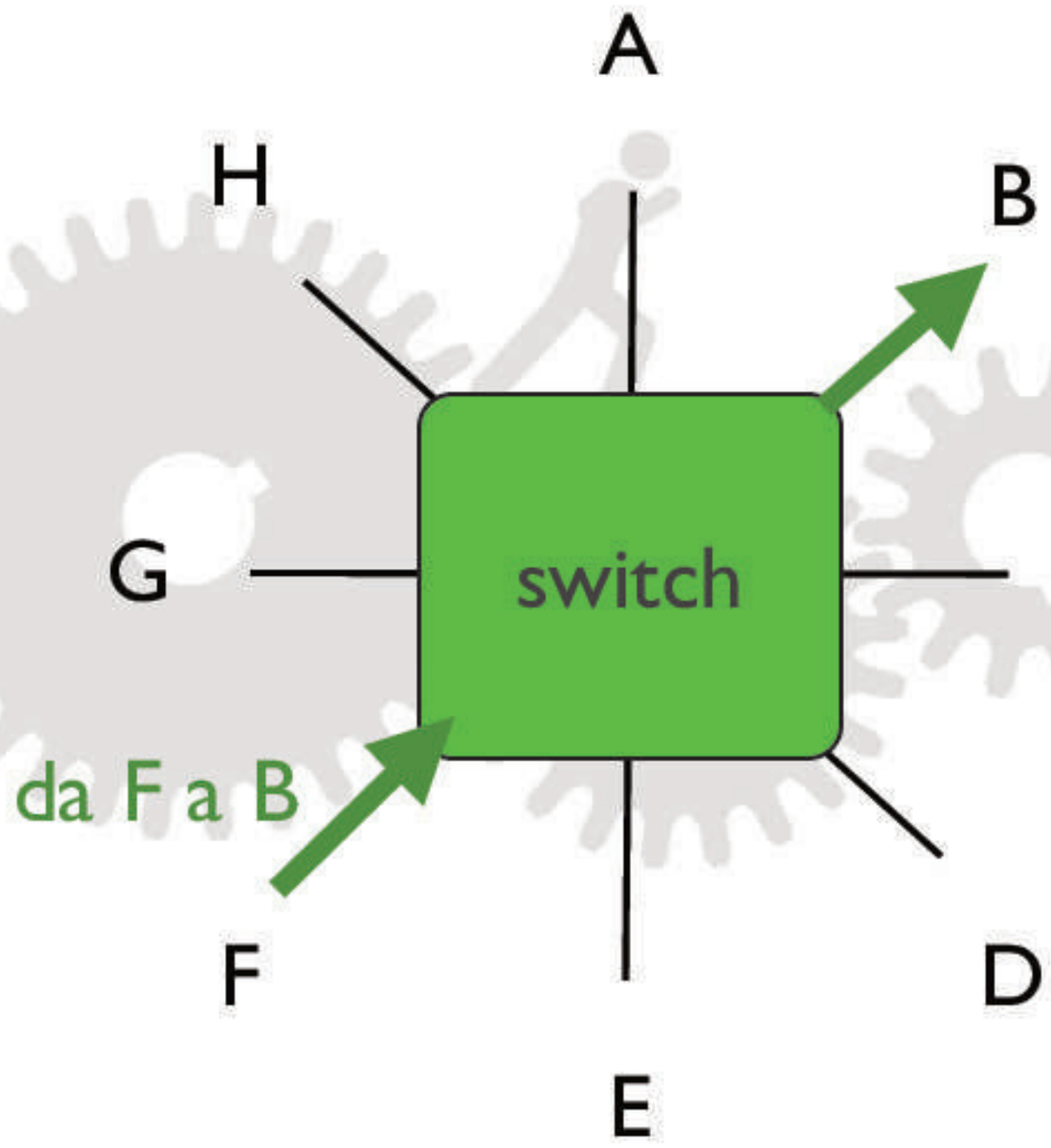
Gli sniffer intercettano i singoli pacchetti, decodificando le varie intestazioni di livello datalink, rete, trasporto, applicativo.

sniffing

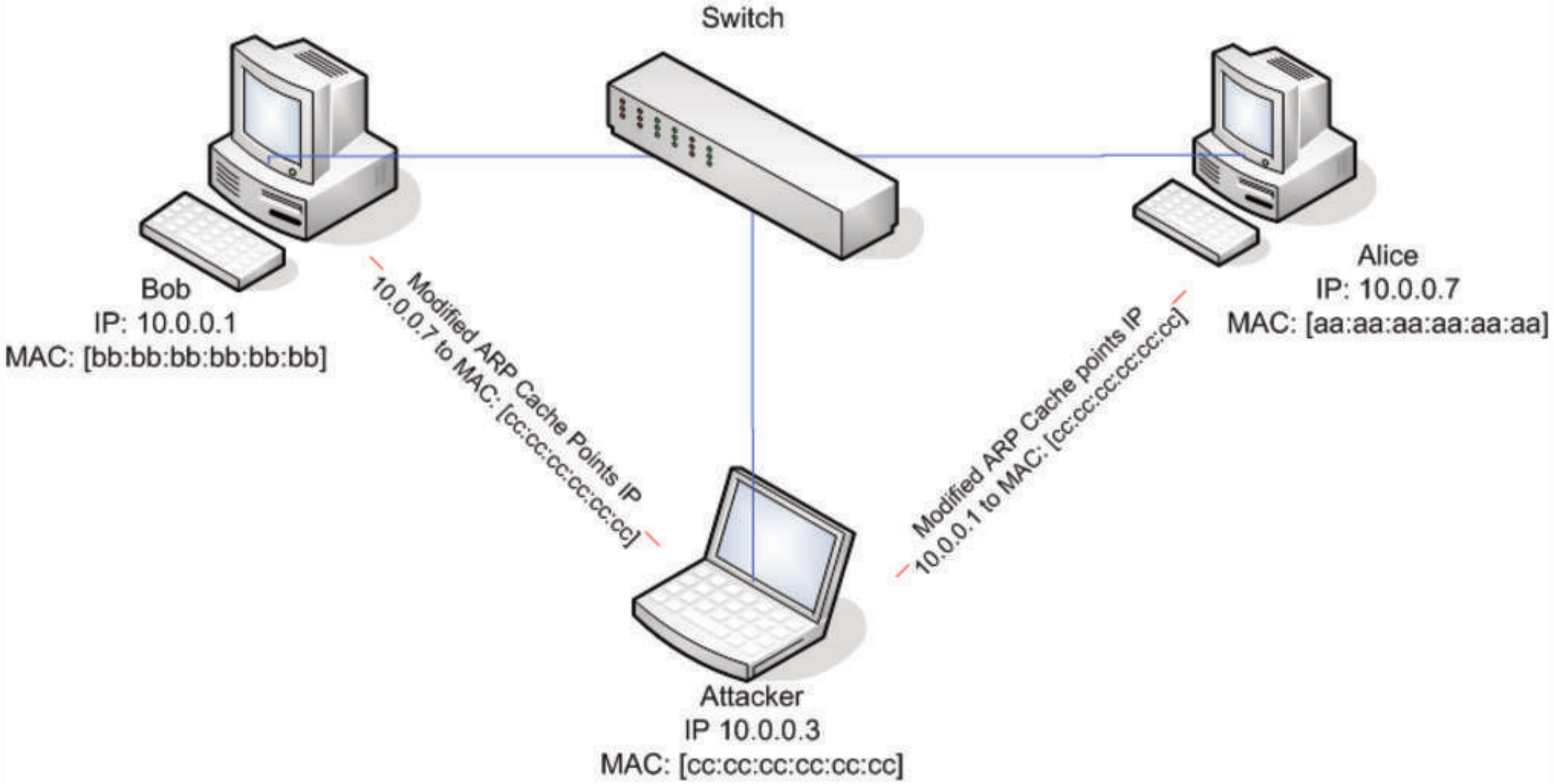
sniffing



sniffing



sniffing


Switch
Bob
IP: 10.0.0.1
MAC: [bb:bb:bb:bb:bb:bb]
Alice
IP: 10.0.0.7
MAC: [aa:aa:aa:aa:aa:aa]
Modified ARP Cache
10.0.0.7 to MAC: [cc
Cache Points IP
AC: [cc:cc:cc:cc:cc:cc]
Cache points IP
:cc:cc:cc:cc:cc]
Modified ARP Cache
10.0.0.1 to MAC: [cc:cc:cc
Attacker
IP 10.0.0.3
MAC: [cc:cc:cc:cc:cc:cc]

network attacks

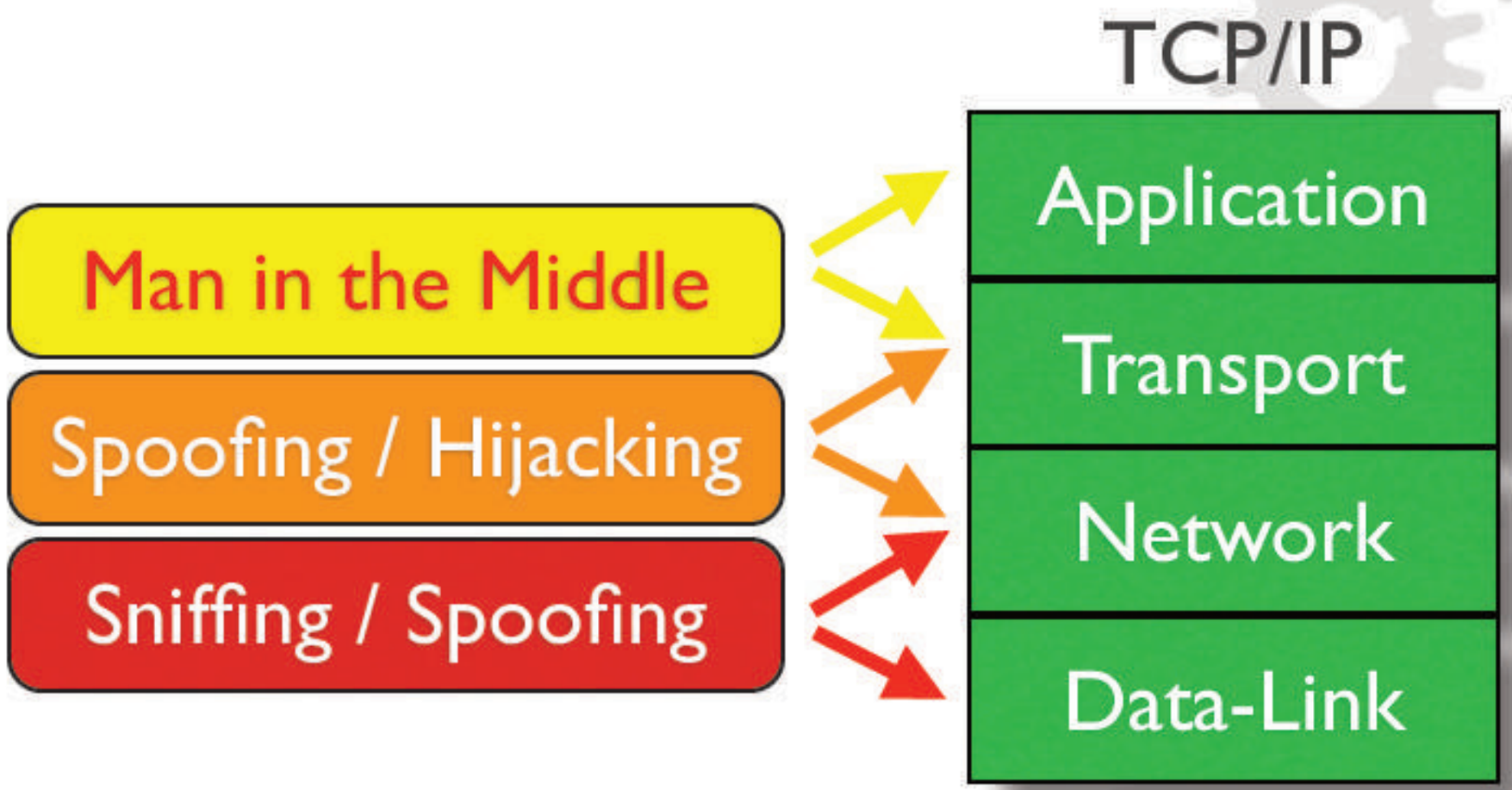
ISO/OSI

- Application
- Presentation
- Session
- Transport
- Network
- Data-Link
- Physical

TCP/IP

- Application
- Transport
- Network
- Data-Link

network attacks



network attacks

telnet	SSH	IPSec	Crypt NIC
clear	crypted	clear/crypted	clear/crypted
clear	clear	crypted	clear/crypted
clear	clear	clear	crypted

Application

Transport

Network

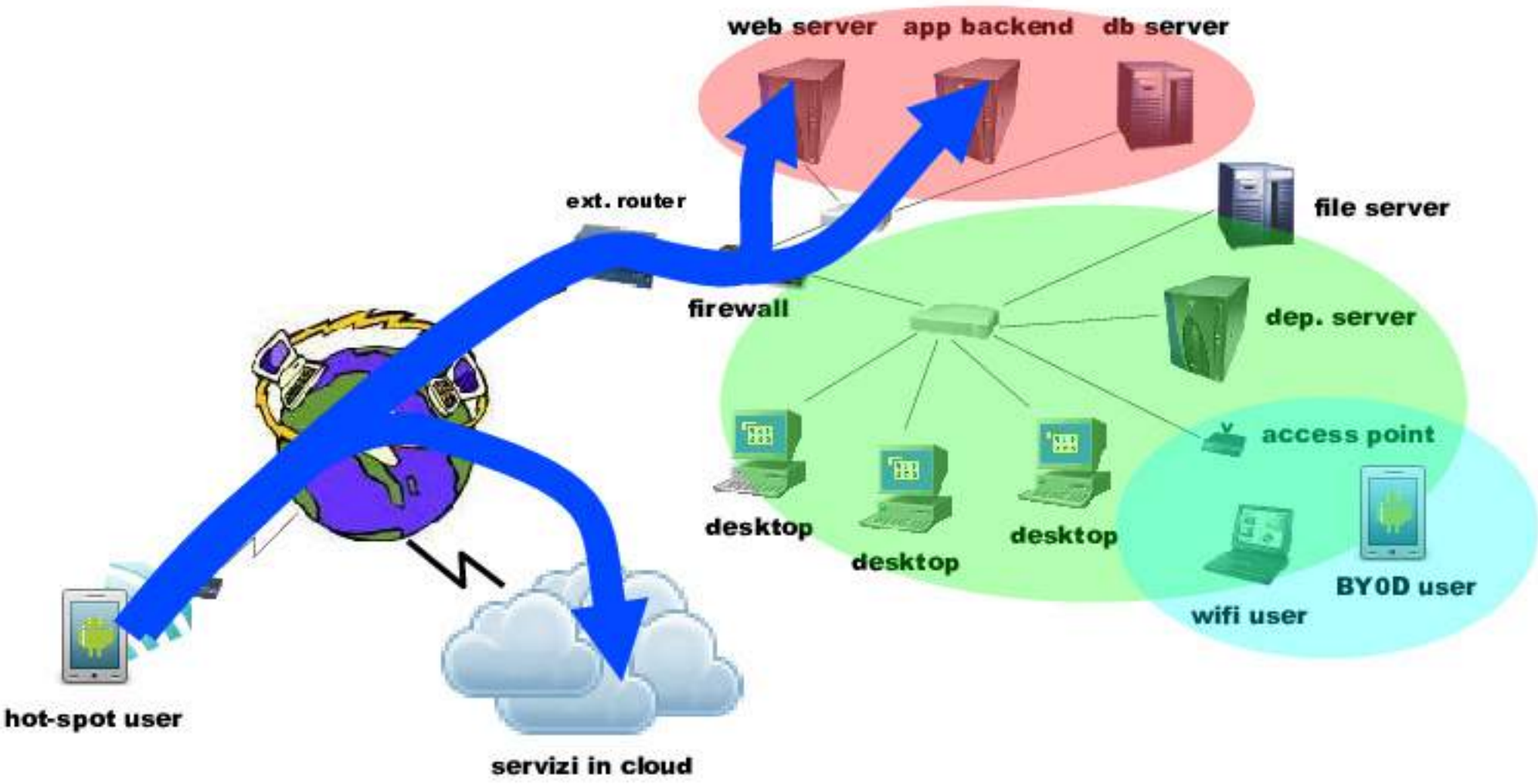
Data-Link

sniffing TCP mangling routing DoS HW tamper

enforcer

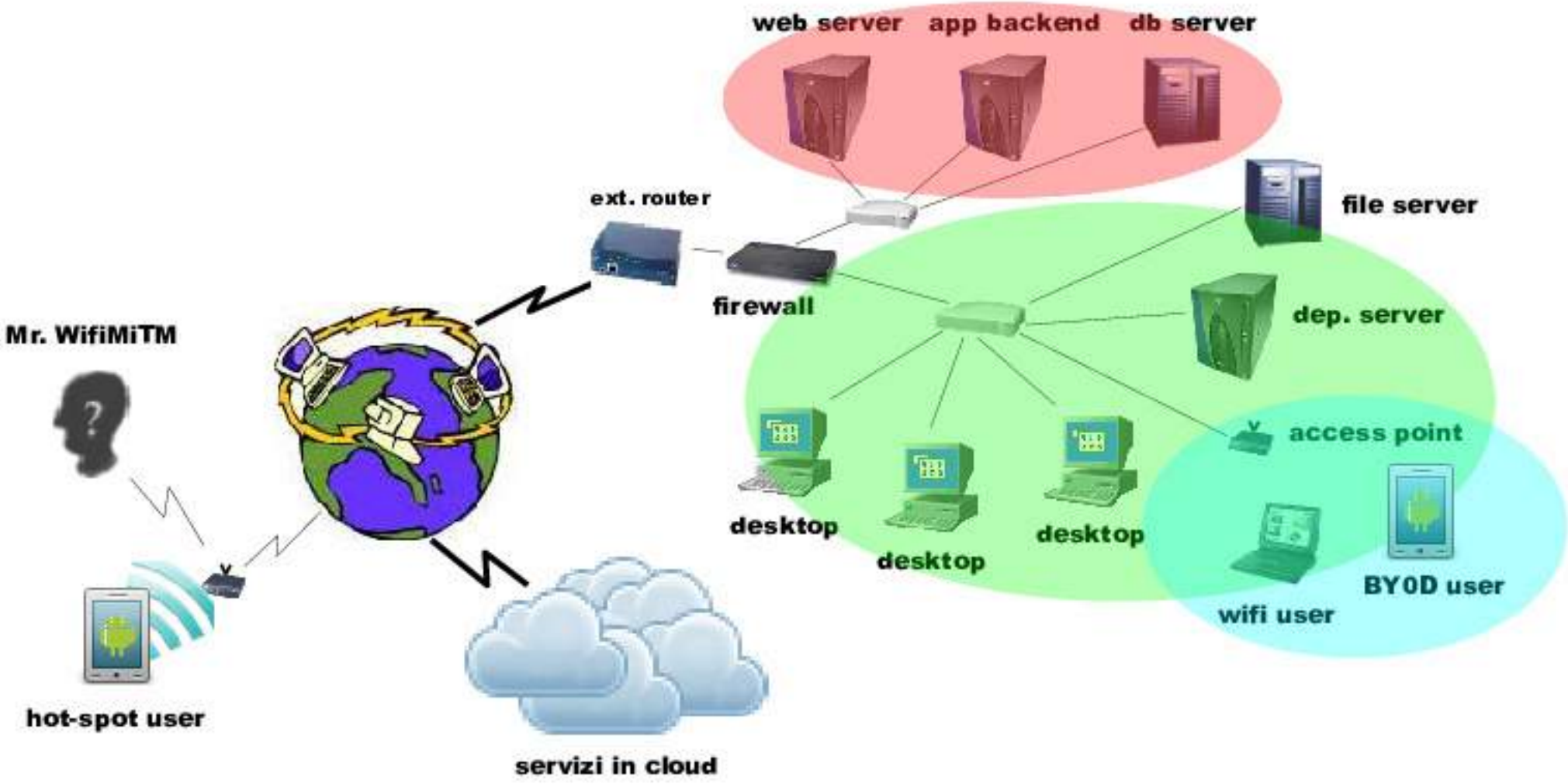
Scenario 3: utenti

Man In The Middle



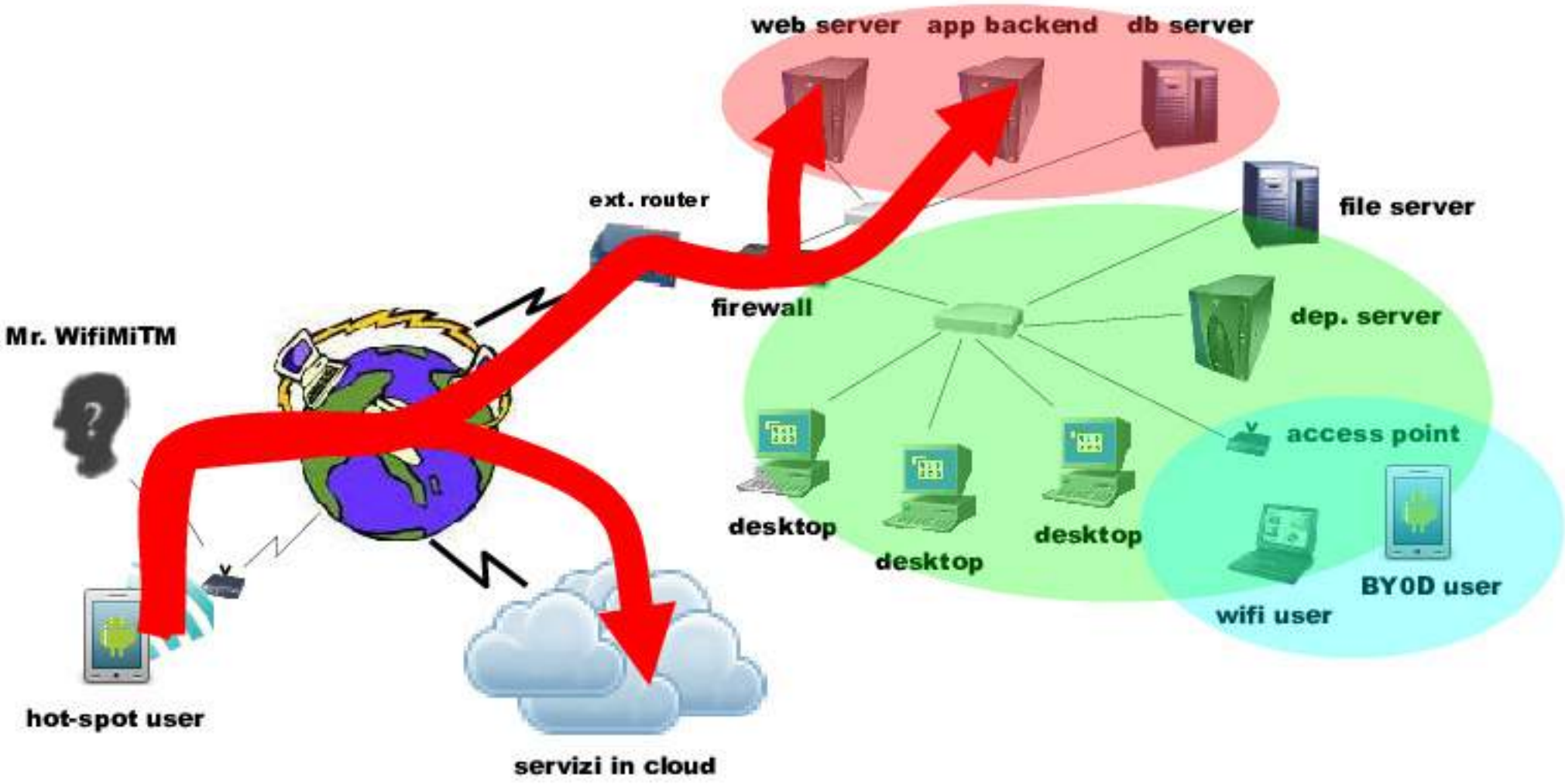
Scenario 3: utenti

Man In The Middle



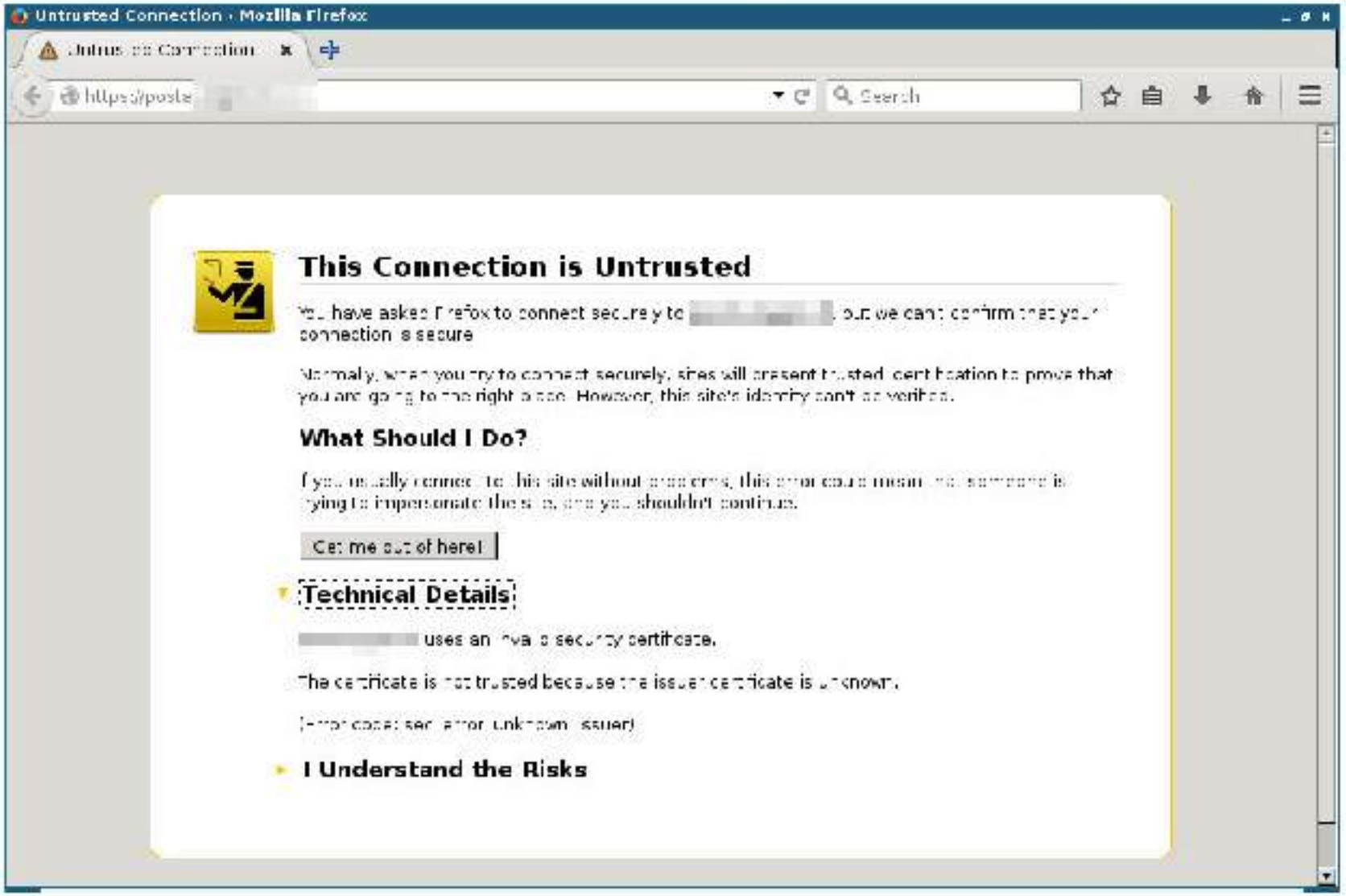
Scenario 3: utenti

Man In The Middle



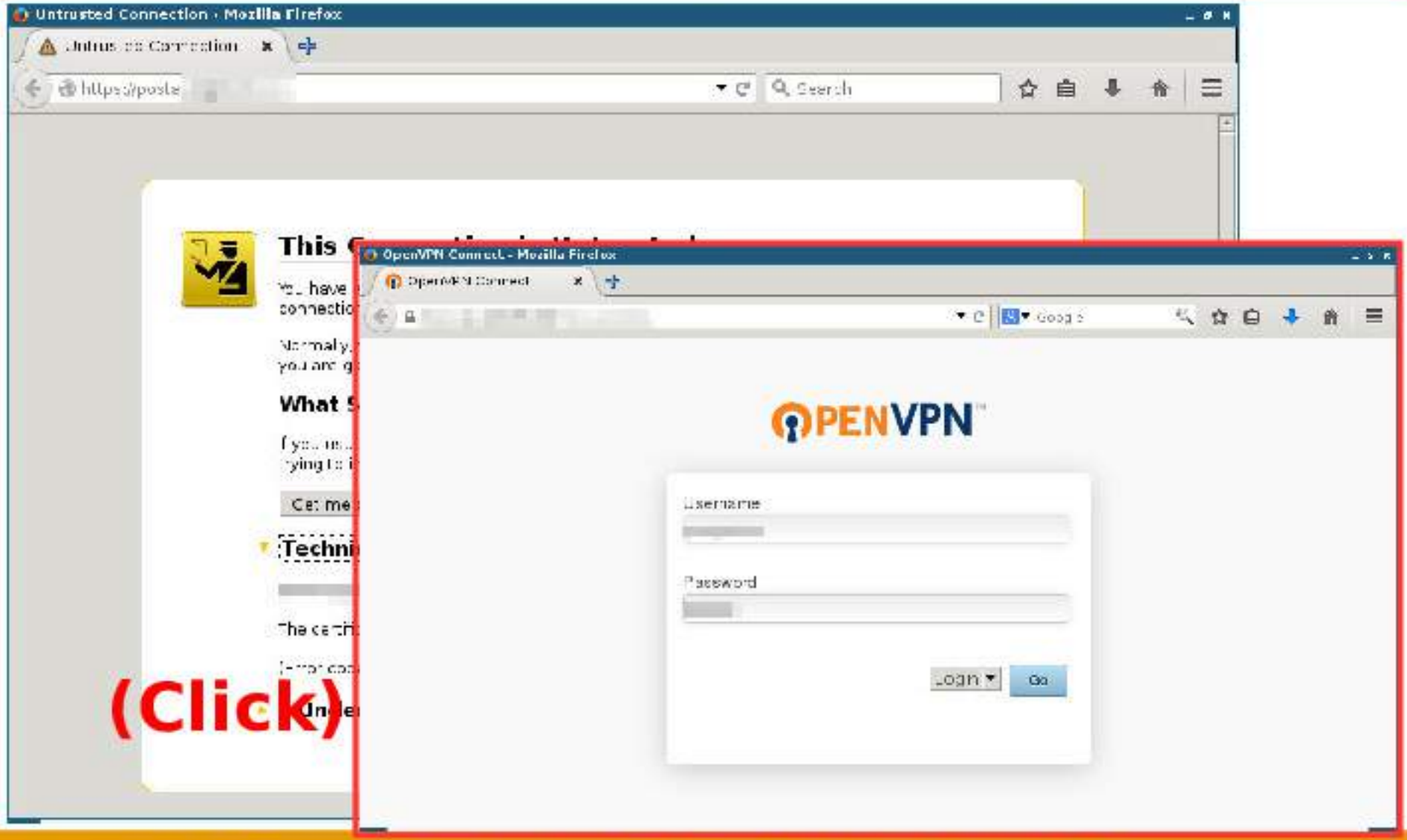
Scenario 3: utenti

Man In The Middle

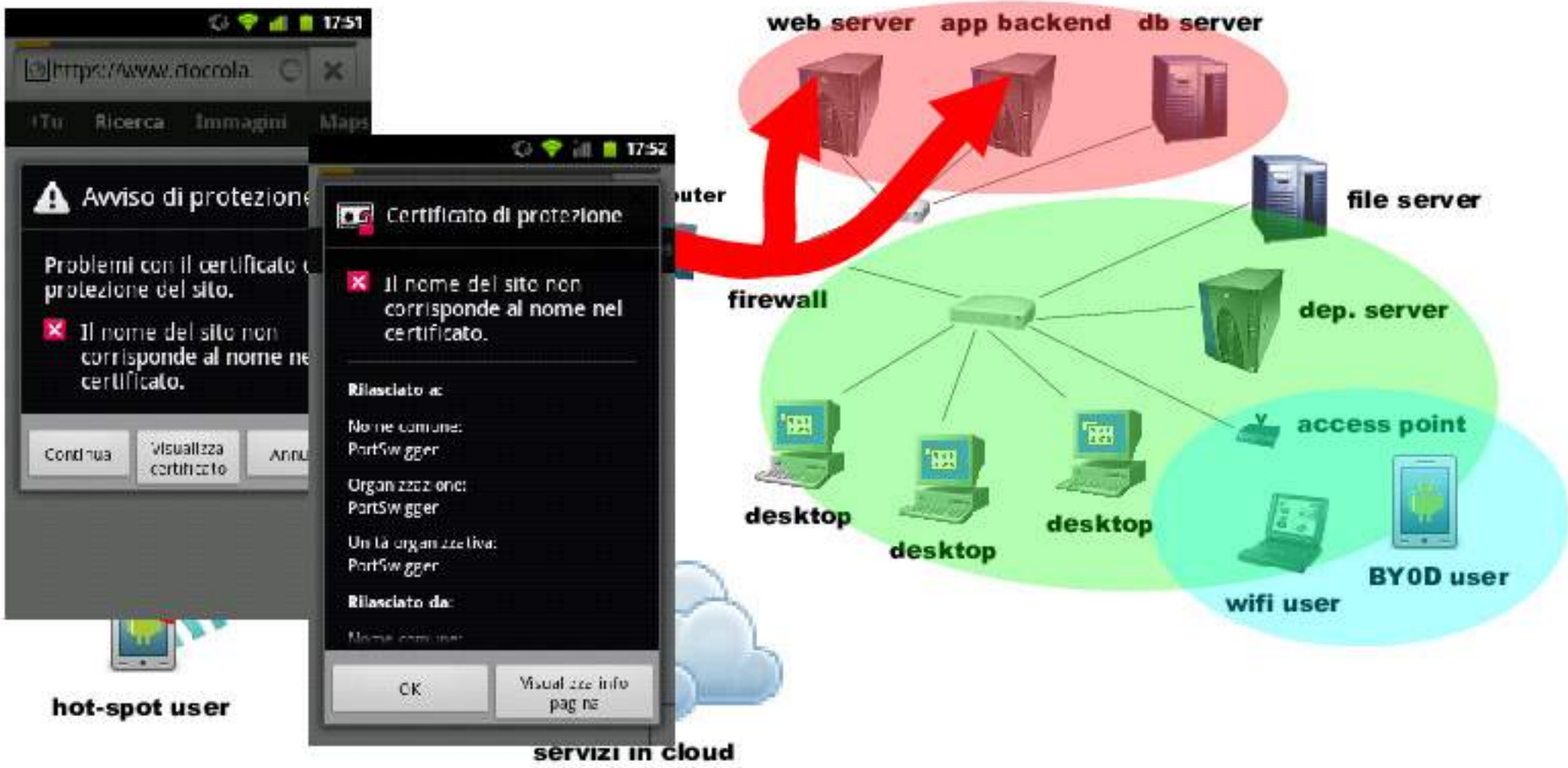


Scenario 3: utenti

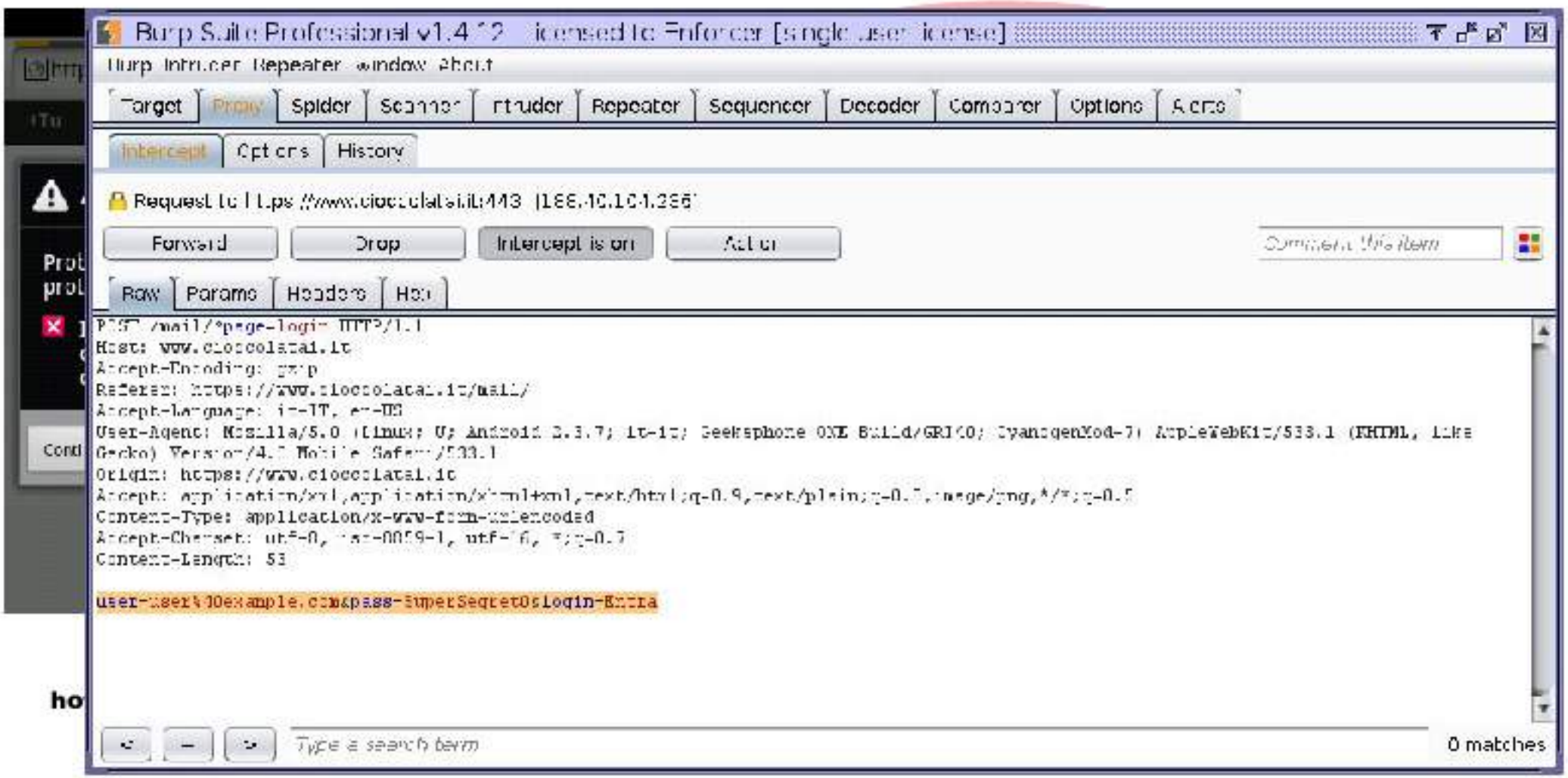
Man In The Middle

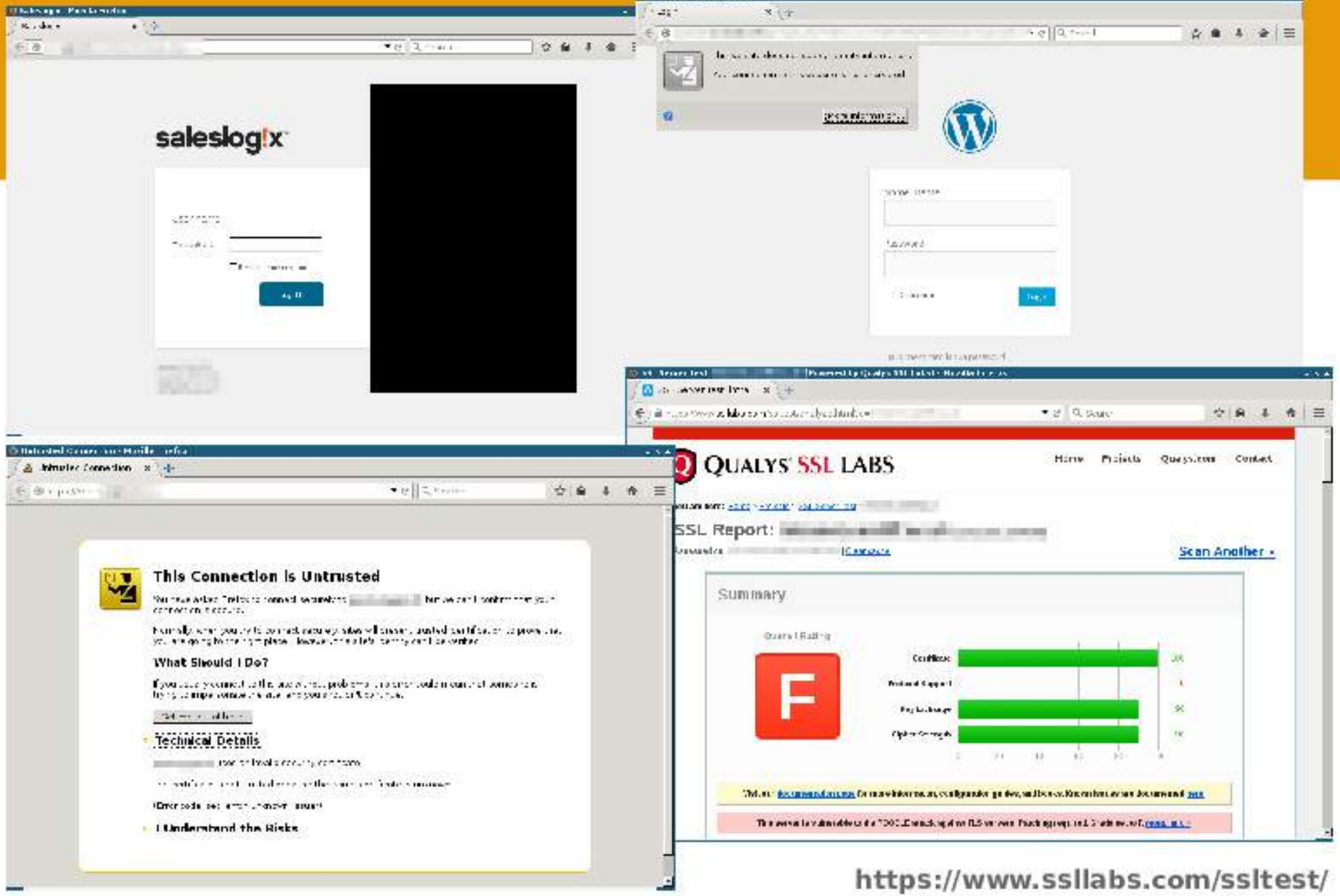


HTTPS?



“Man in The Middle”





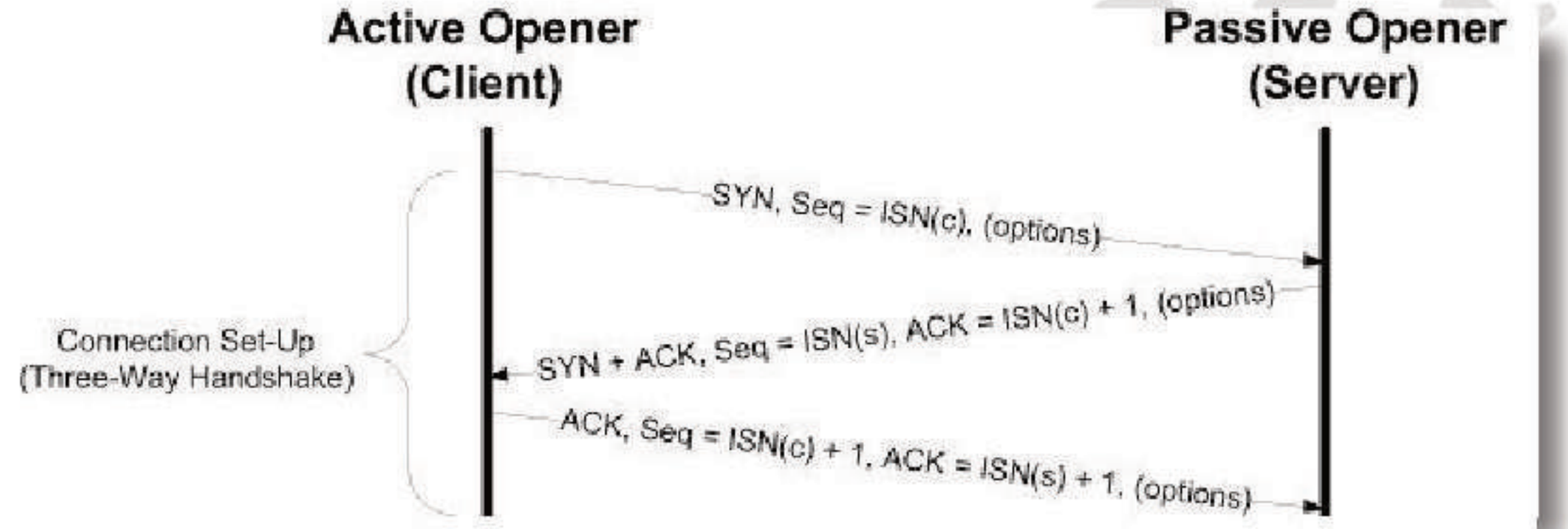
https://www.ssllabs.com/ssltest/

portscan

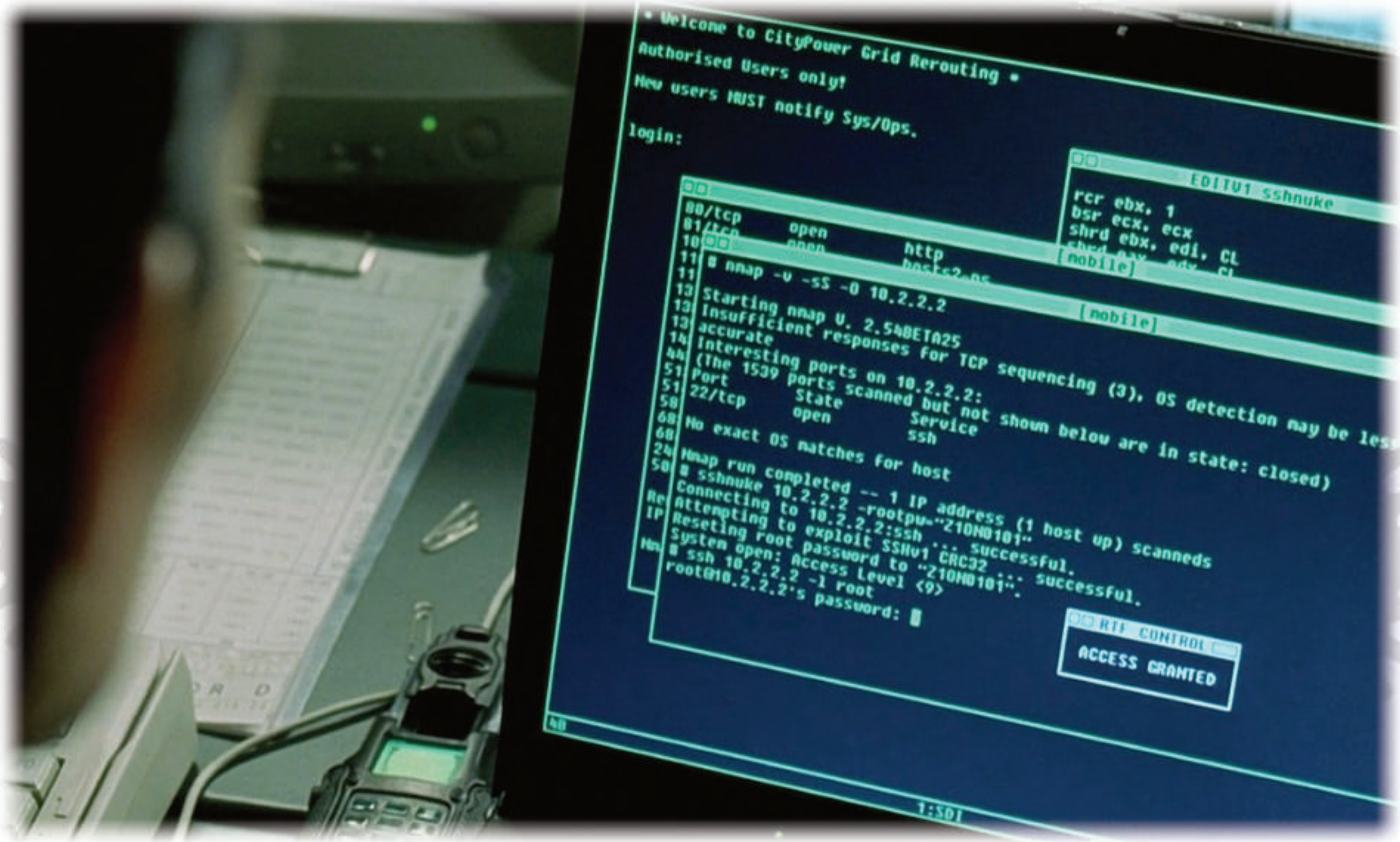
Si definisce portscan la tecnica informatica utilizzata per raccogliere informazioni su un computer connesso ad una rete stabilendo quali porte siano in ascolto su una macchina.

Letteralmente significa "scansione delle porte": inviando richieste di connessione al computer bersaglio (soprattutto pacchetti TCP, UDP e ICMP creati ad arte) ed elaborando le risposte è possibile stabilire quali servizi di rete siano attivi su quel computer. Una porta si dice "in ascolto" ("listening") o "aperta" quando vi è un servizio, programma o processo che la usa.

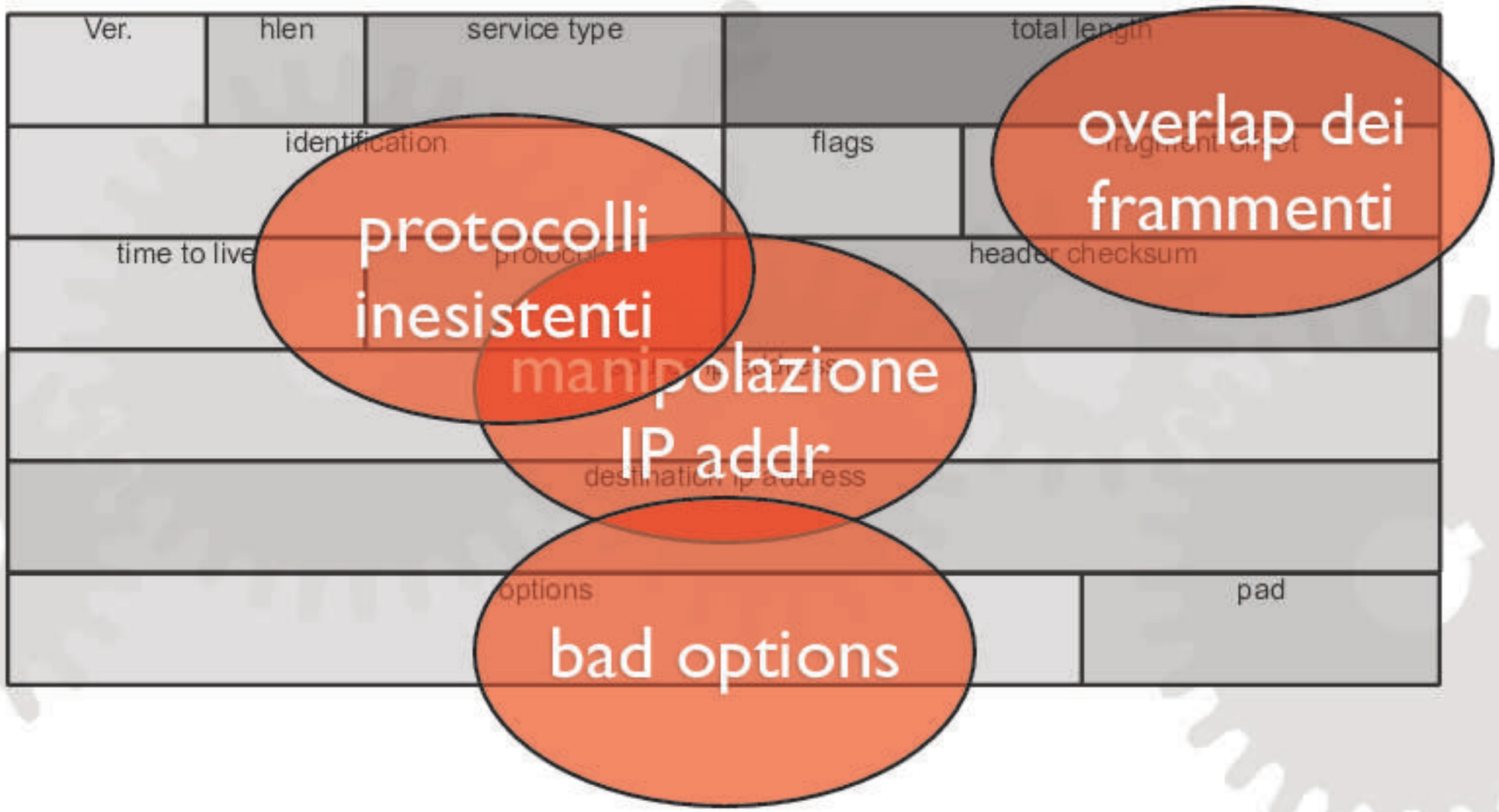
TCP 3way handshake



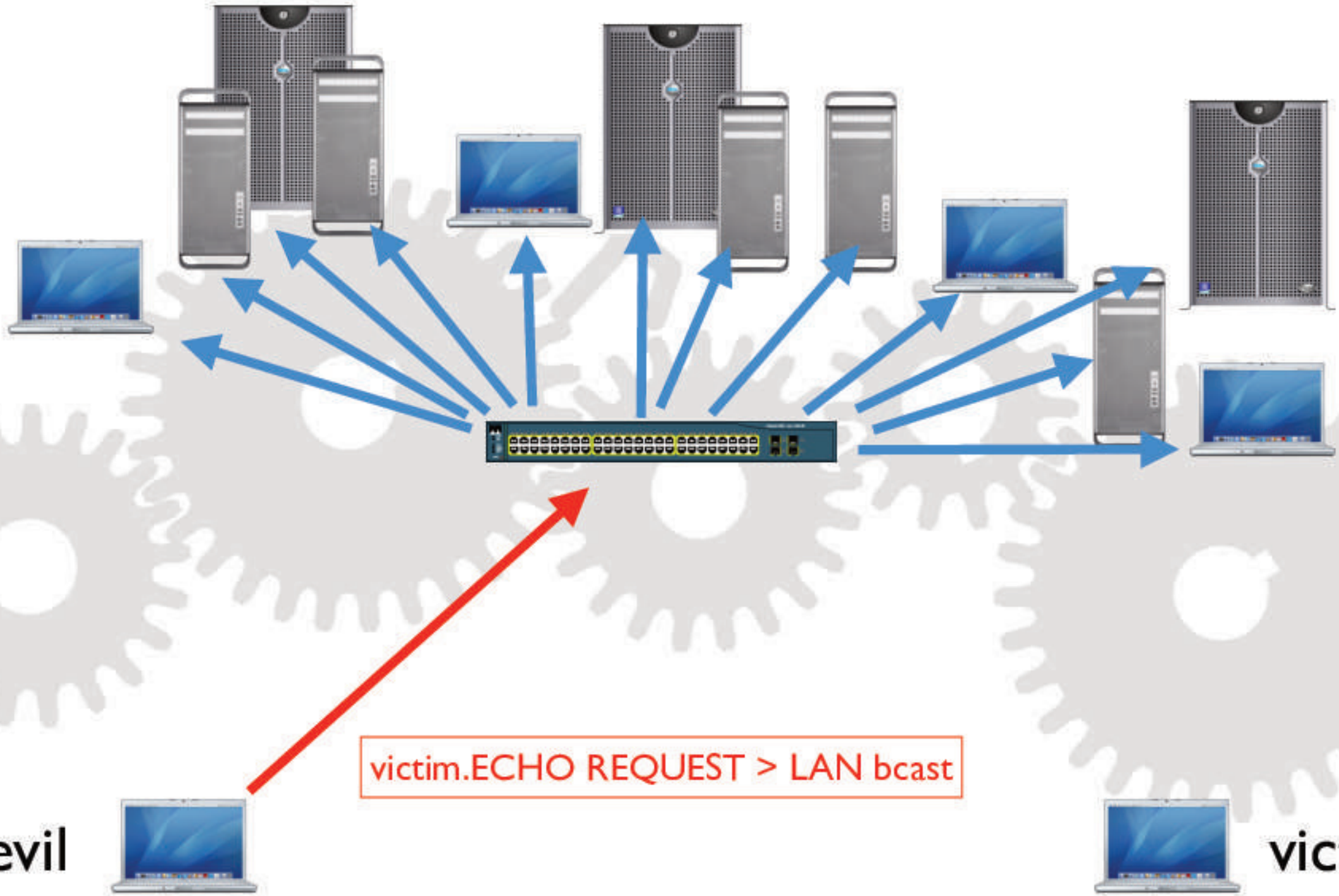
portscan


Welcome to CityPower Grid Rerouting
Authorised Users only!
New users MUST notify Sys/Ops.
login:
80/tcp open http
nmap -v -sS -O 10.2.2.2
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection may be less accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: closed)
Port State Service
22/tcp open ssh
No exact OS matches for host
Nmap run completed -- 1 IP address (1 host up) scanned
sshnuke 10.2.2.2 -rootpw="Z1ON0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z1ON0101".
System open: Access Level (9)
ssh 10.2.2.2 -l root
root@10.2.2.2's password:
rcr ebx, 1
bsr ecx, ecx
shrd ebx, edi, CL
[nobile]
RTI CONTROL
ACCESS GRANTED
1:501

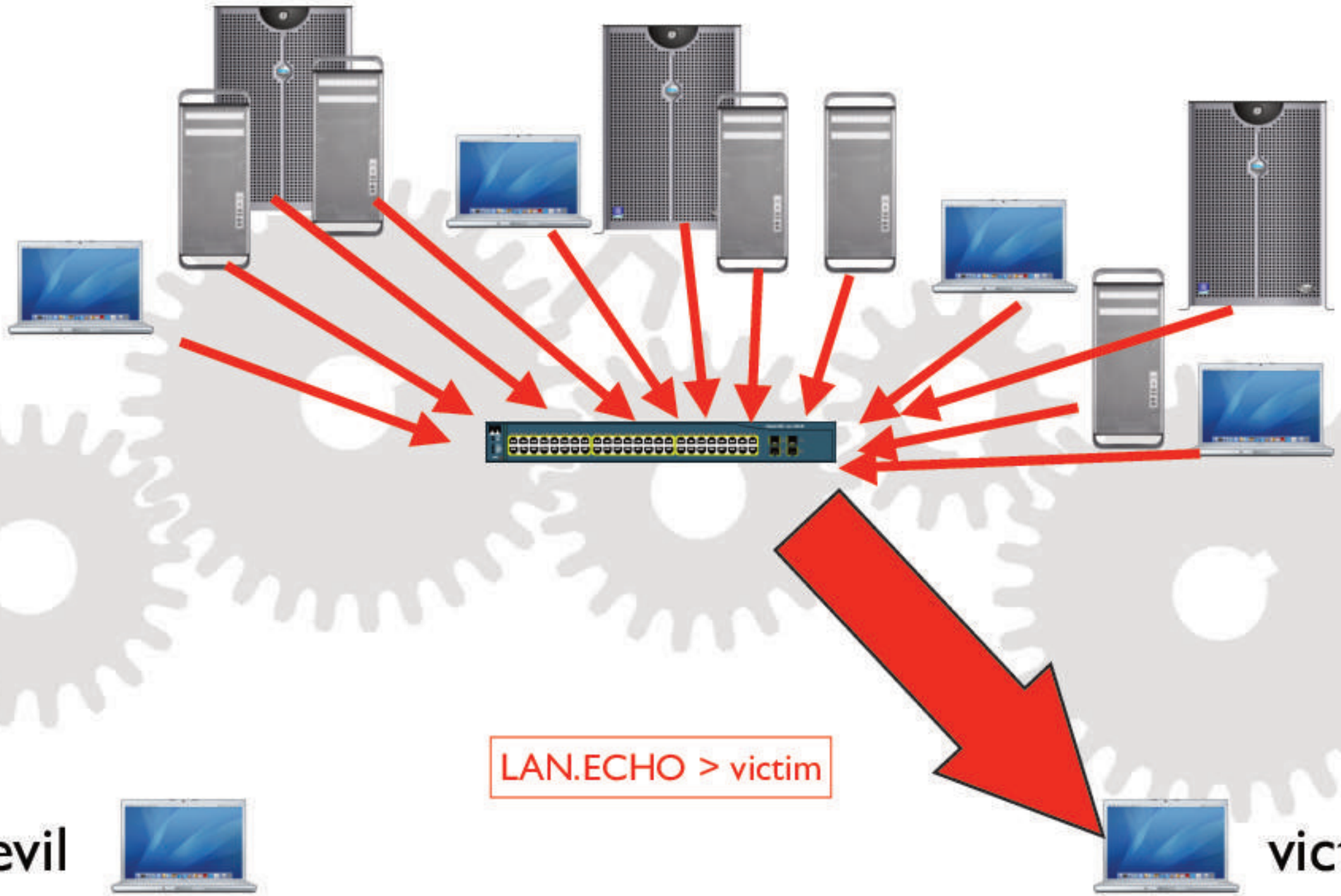
Denial of Service - TCP/IP stack



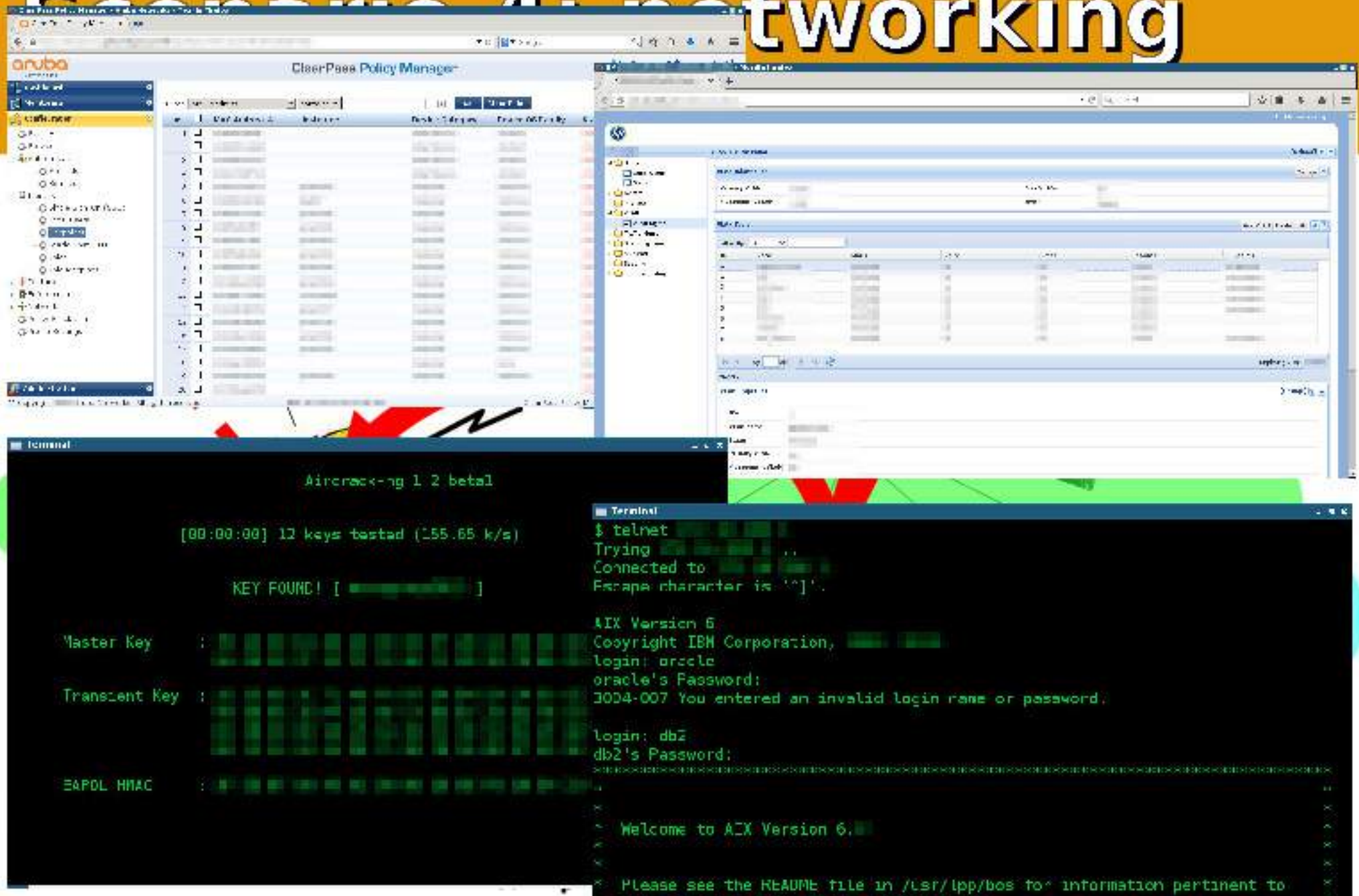
Denial of Service - TCP/IP protocols



Denial of Service - TCP/IP protocols



Scenario 4: networking



Scenario 4: networking

segmentazione reti