

Dimmi il tuo numero
e ti dirò dove sei



HELLER
Tracing

\$whoami

Lordscinawa

- lordscinawa [at] {olografix, autistici} [dot] org
- Università degli studi di Milano - Sicurezza delle Reti e dei Sistemi Informatici
- Supporta/Membro di:
E-quipe: <http://noname.webgui.ws>



\$whoami

Epto (A)

- epto [at] tramaci [dot] org / epto [at] usa [dot] com
- Università C'a foscari, Venezia - Informatica
- Attivista hacker Veneziano
(Secondo il giornale L'unità)
- Supporta membro di:



Epto (A)
LordScinawa



Pronto! Con.. quanti parlo?

Da la Domenica del Corriere, citato in Selezione dal Reader's
Digest, febbraio 1974.

No!





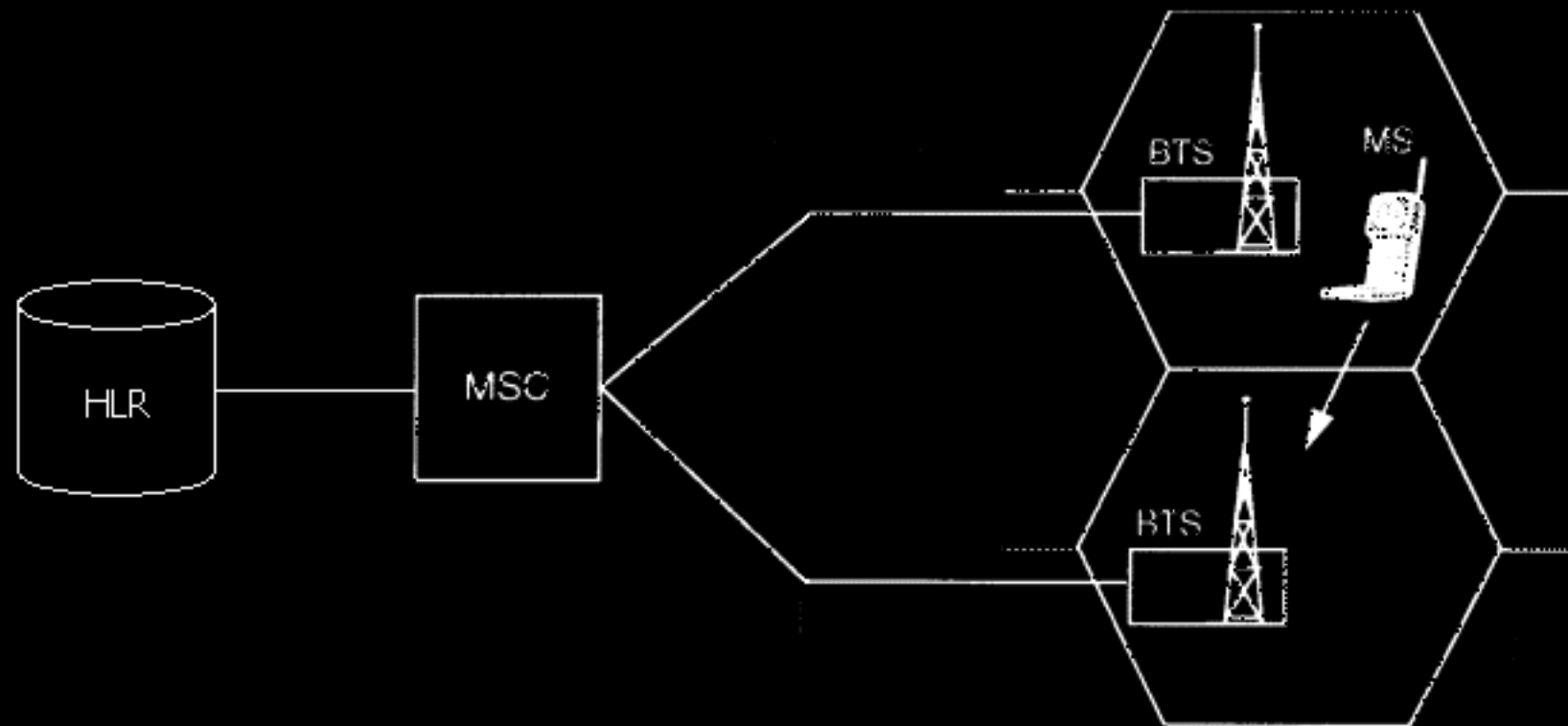
La nostra posizione...

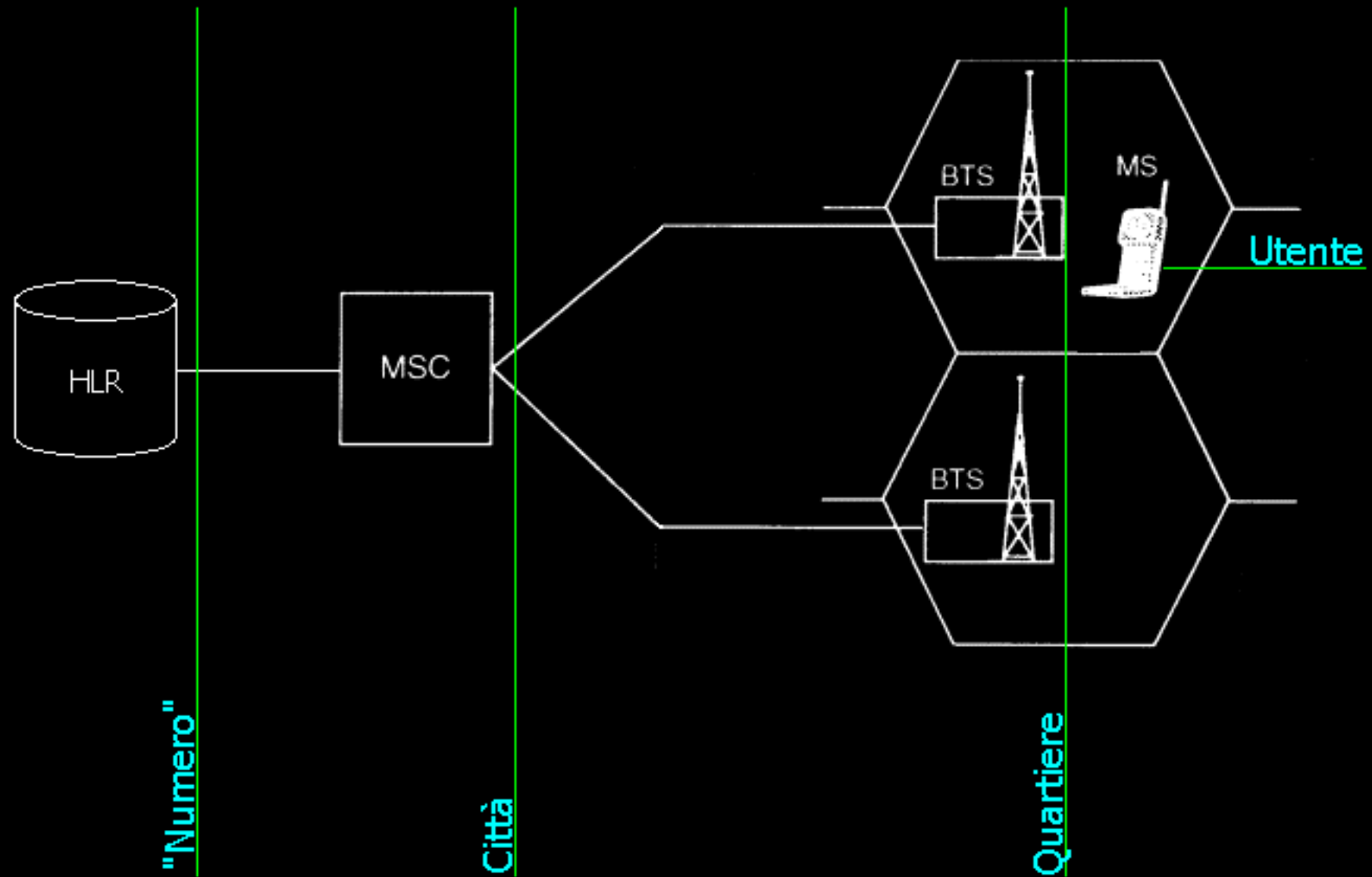
...e' un dato
personale?

Qualcuno voleva
vederci chiaro...



Breve presentazione del sistema mobile:





PSTN vs. GSM/UMTS



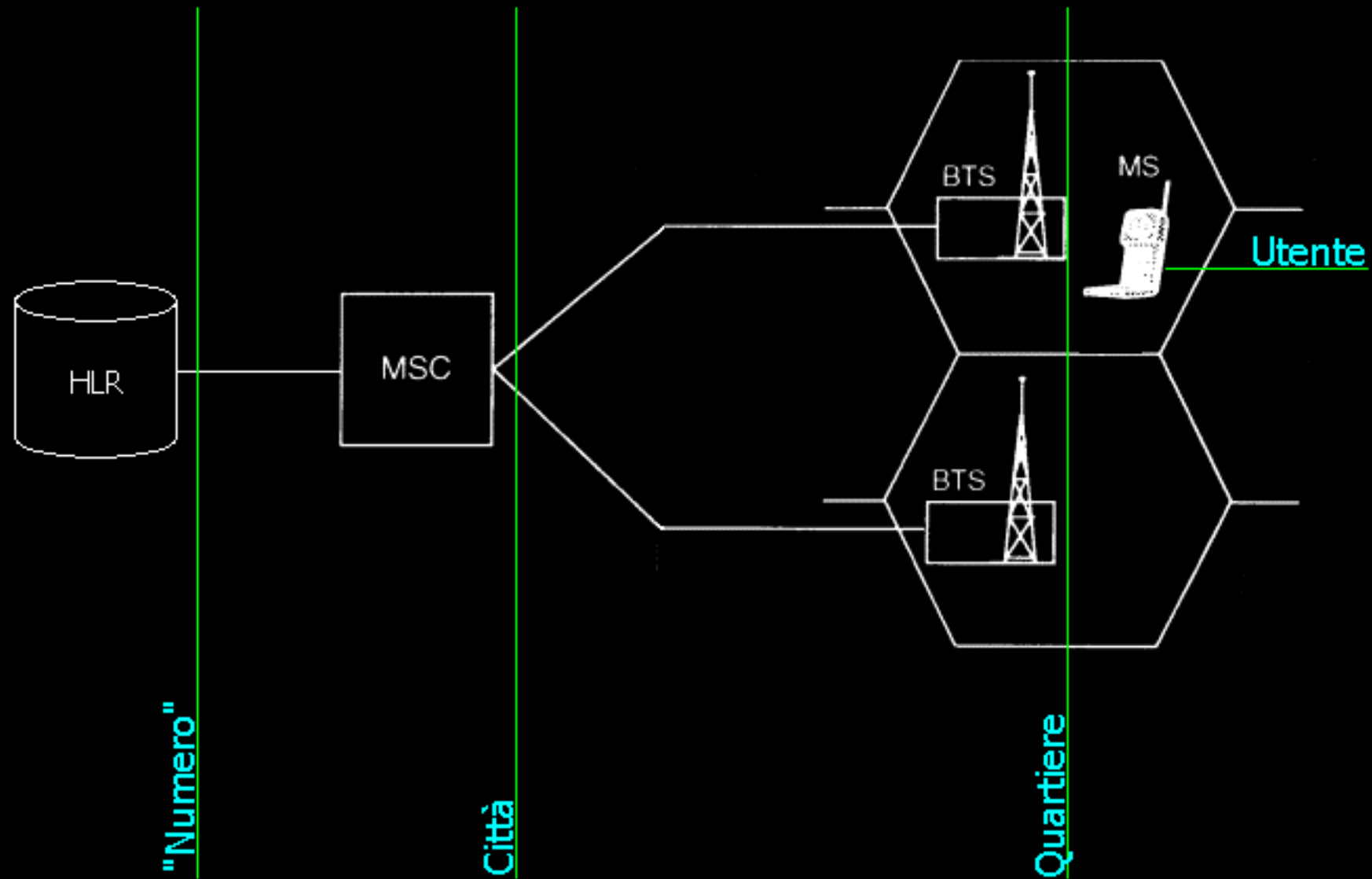
C'è qualche analogia?
(nei due sistemi?)

Nella vecchia rete
fissa, ogni località
ha un prefisso
telefonico

- 06 - 907080 (Roma)
- 02 - 907080 (Milano)
- 0432 - 907080 (Udine)
- 049 - 907080 (Padova)
- ...
- ...

Ma per la rete
GSM?

The Hack



Posso sapere la
posizione di un
telefonino avendo solo il
numero di telefono?

The Hack

Si...

Come?!

Ma gli MSC hanno
un numero di
telefono!

Useremo lo stesso
metodo con cui la rete
telefonica trova la
posizione dei telefonini

Le Query

We did it for the
lulz

Una storia simpatica..

We did it for the
lulz

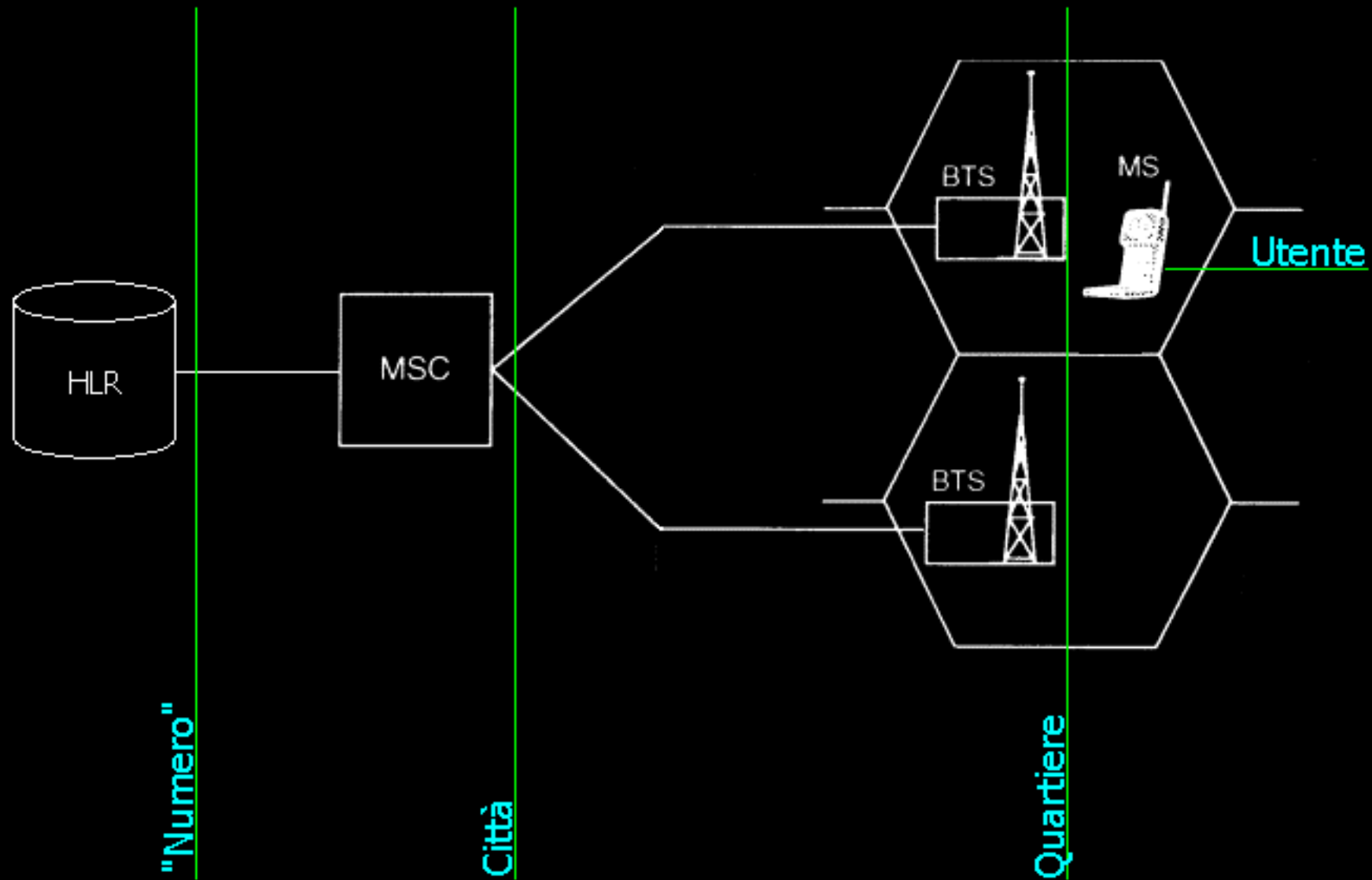
Admin

We did it for the
lulz

OR $I = I$

$=)$

Query
HLR
“?”

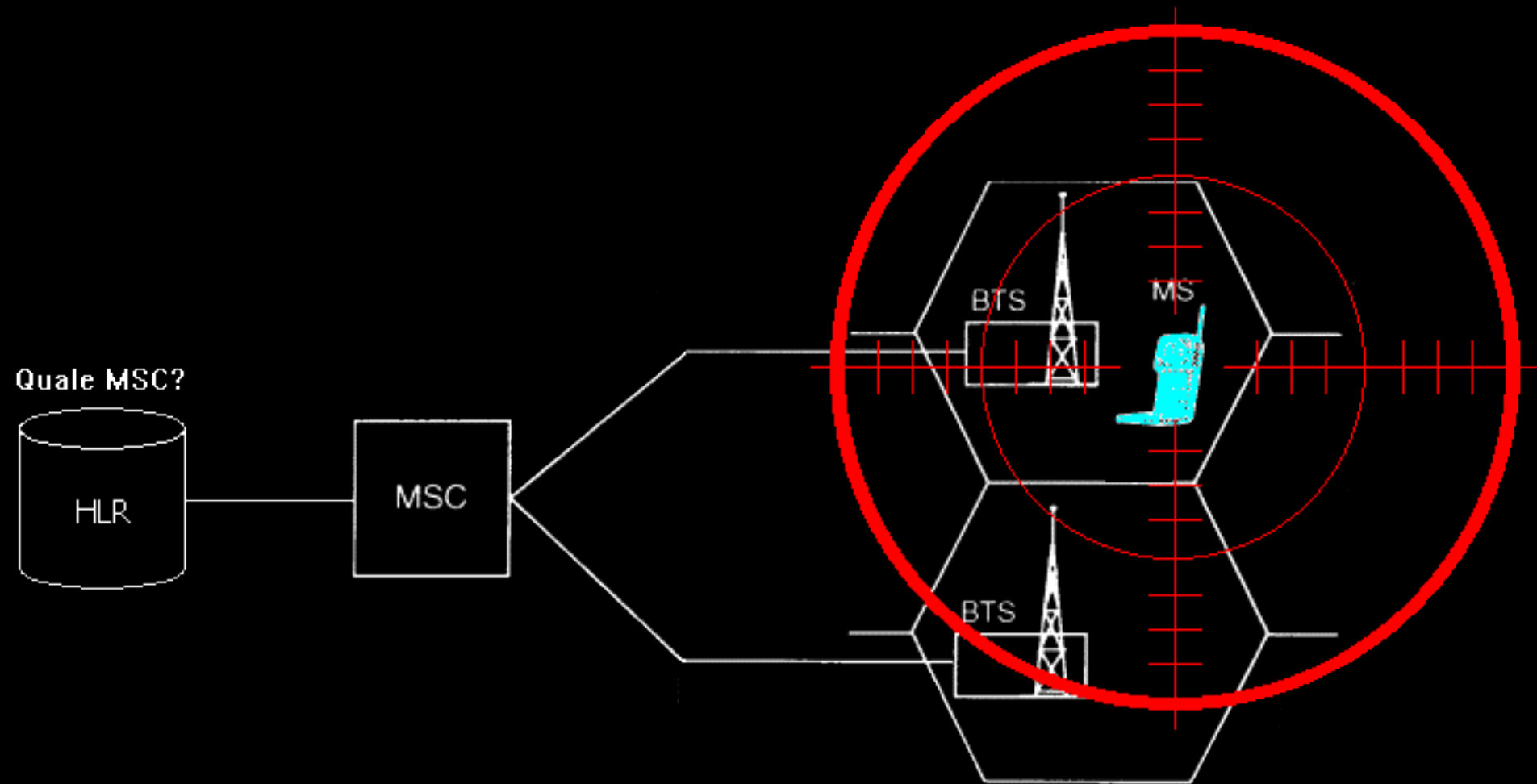


Come si correlano i numeri degli MSC alle città?

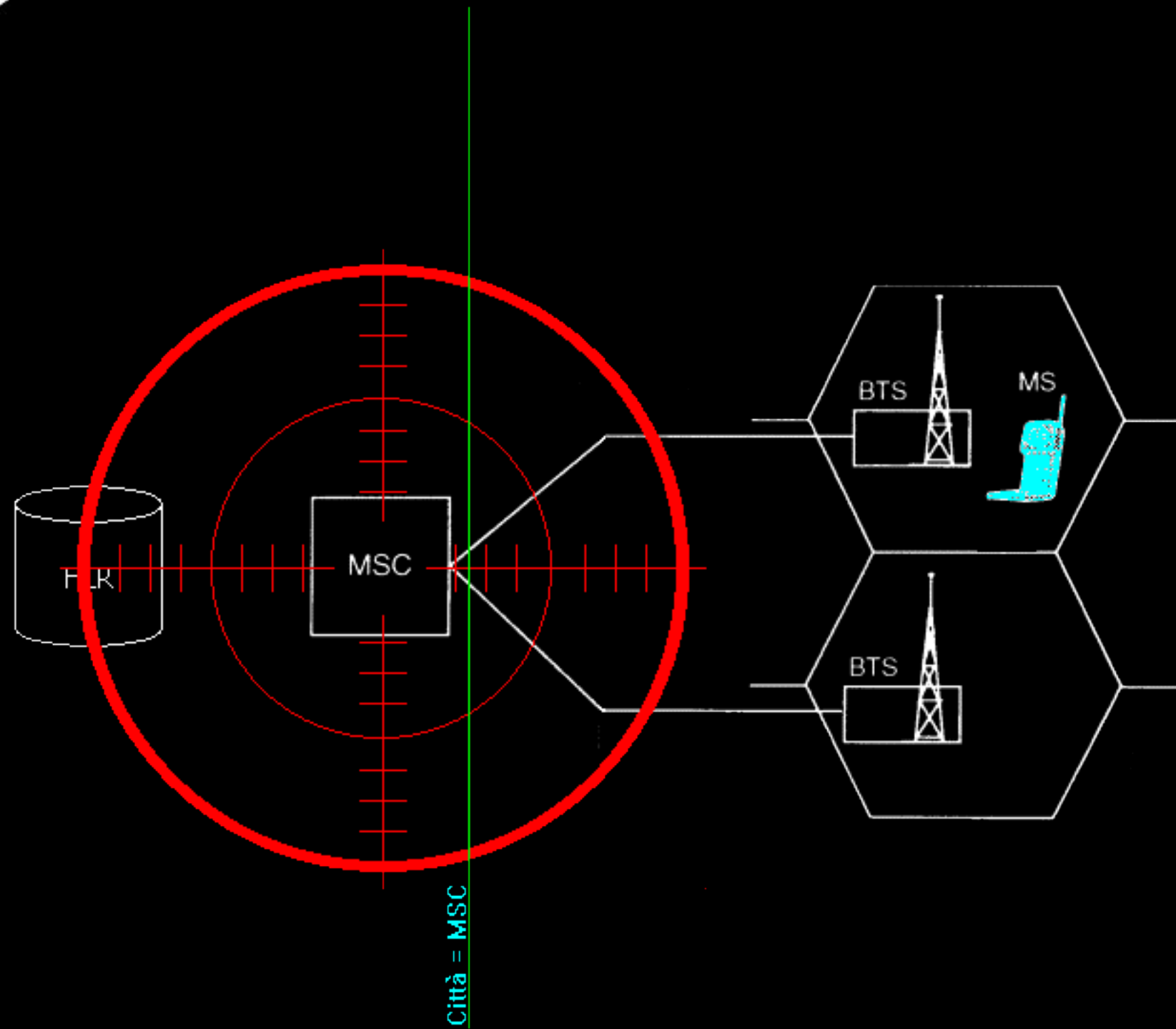
Procedendo all'inverso

Ancora!!!

The Hack



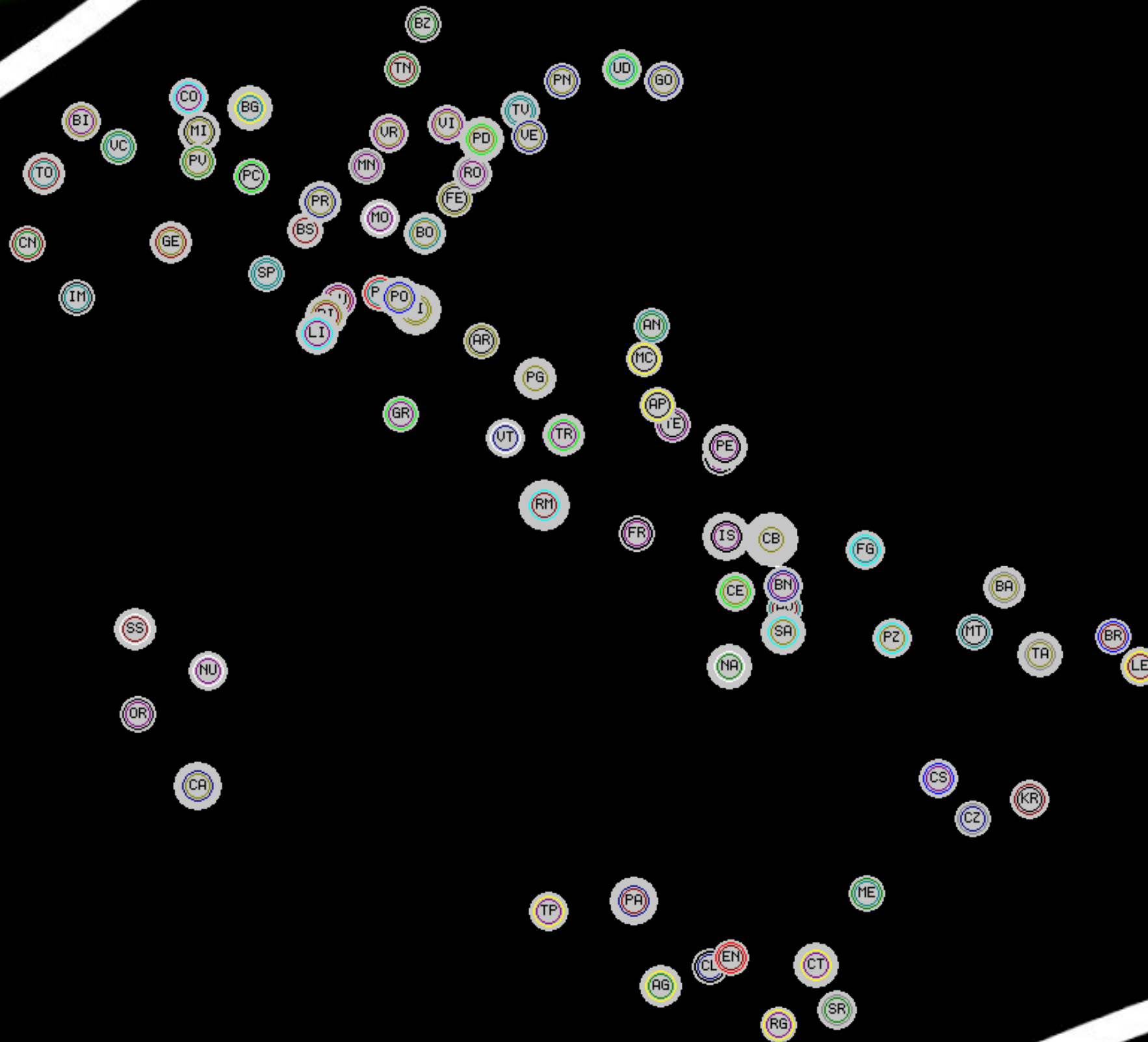
The Hack



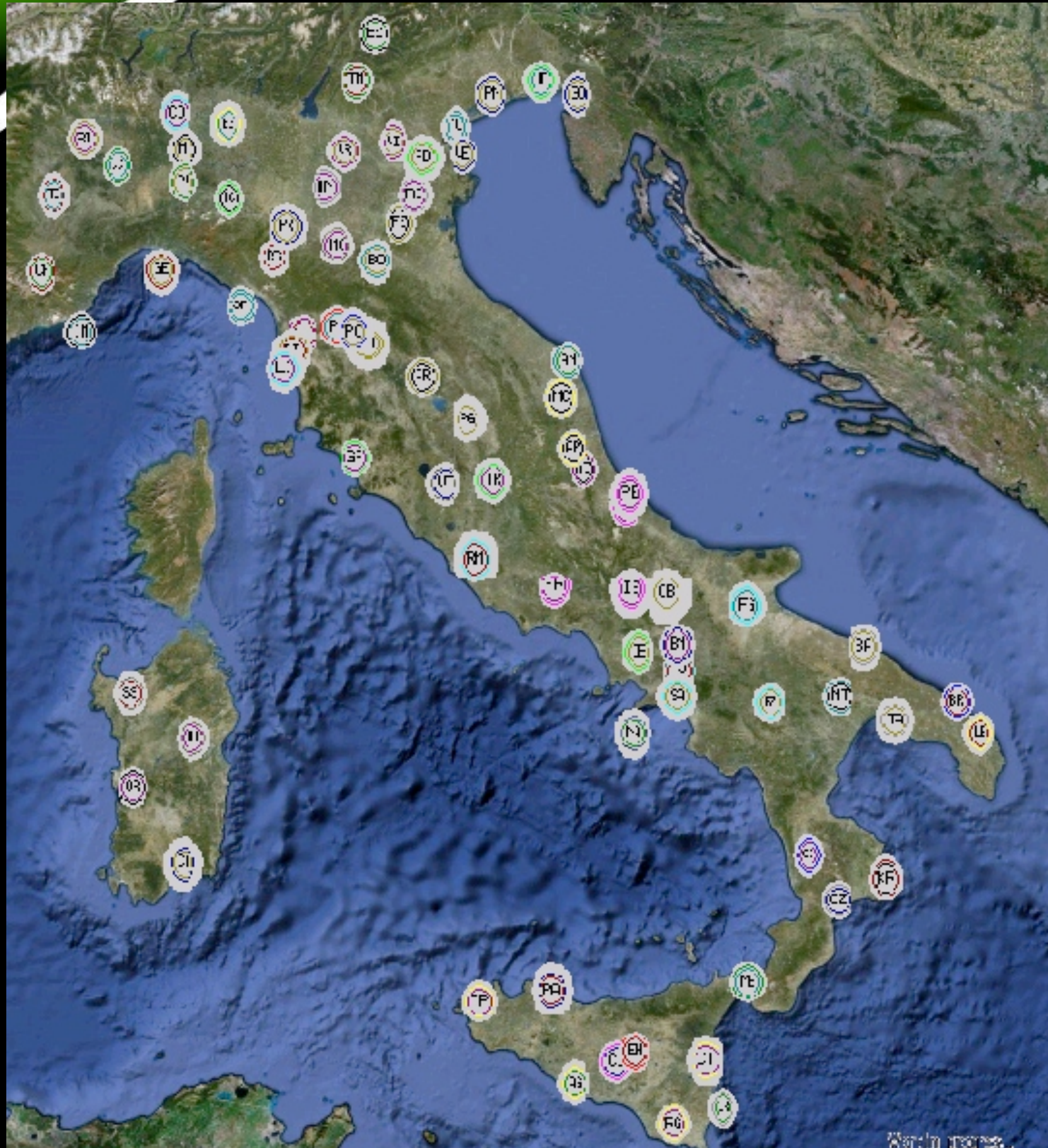
Città == MSC!
:)



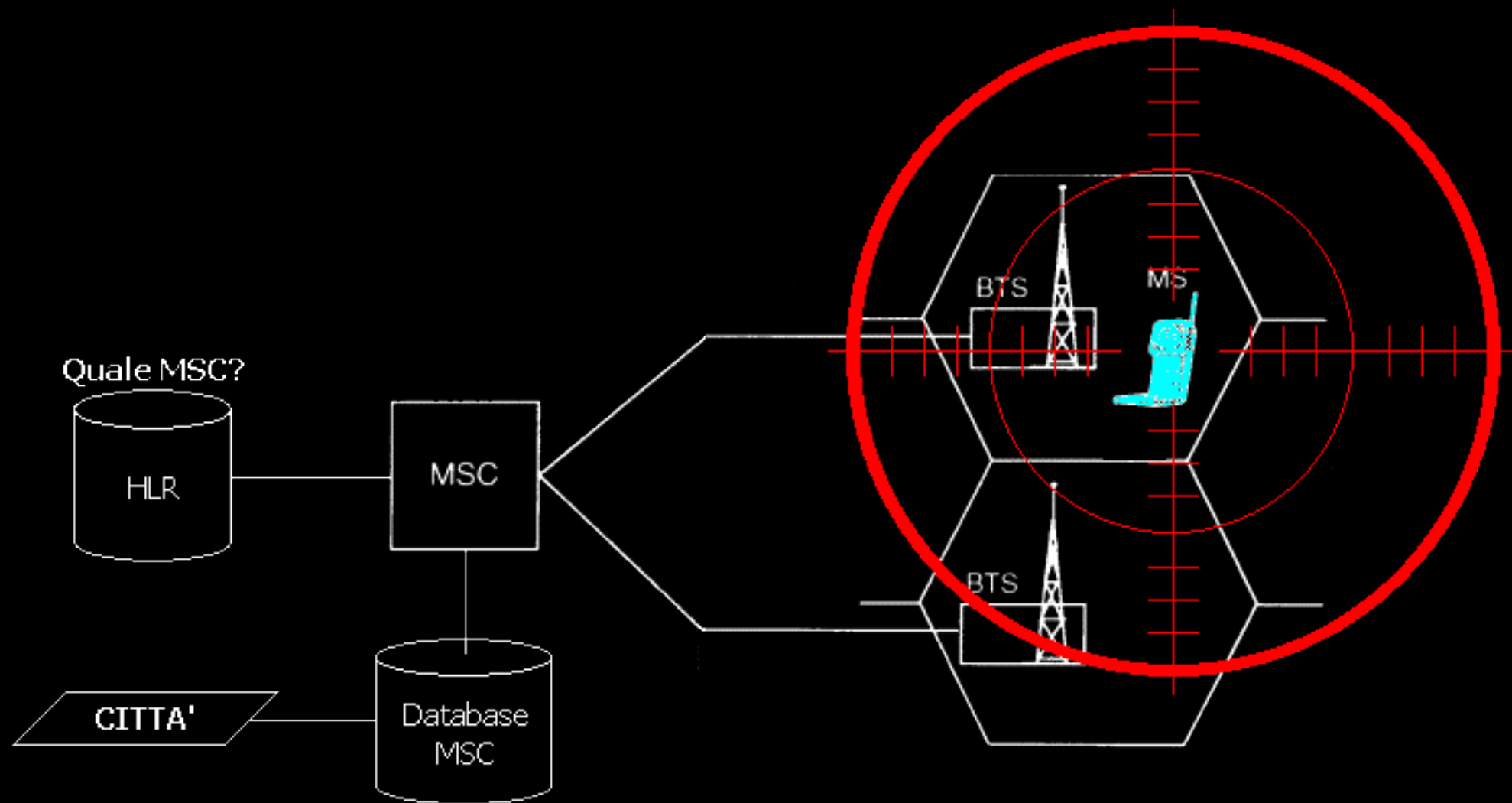
Some results



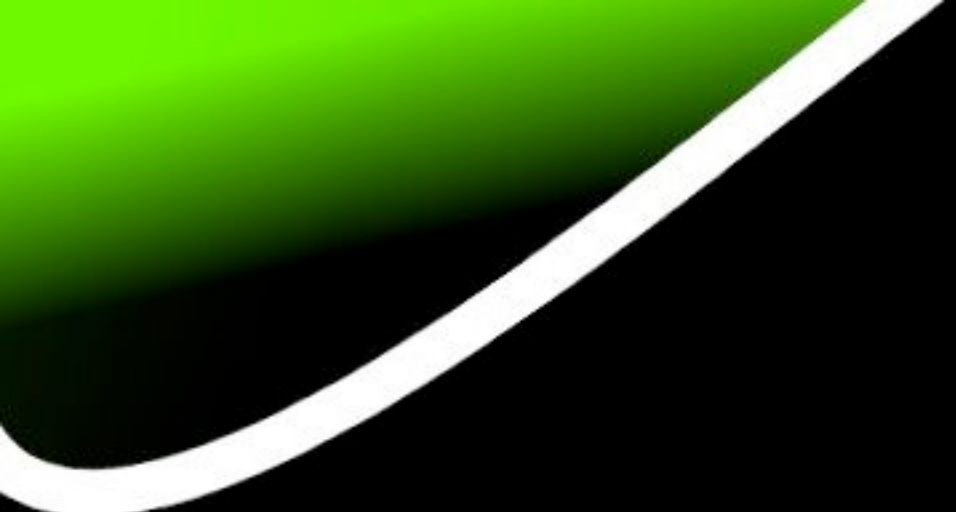
Some results



Epto (A)
LordScinawa

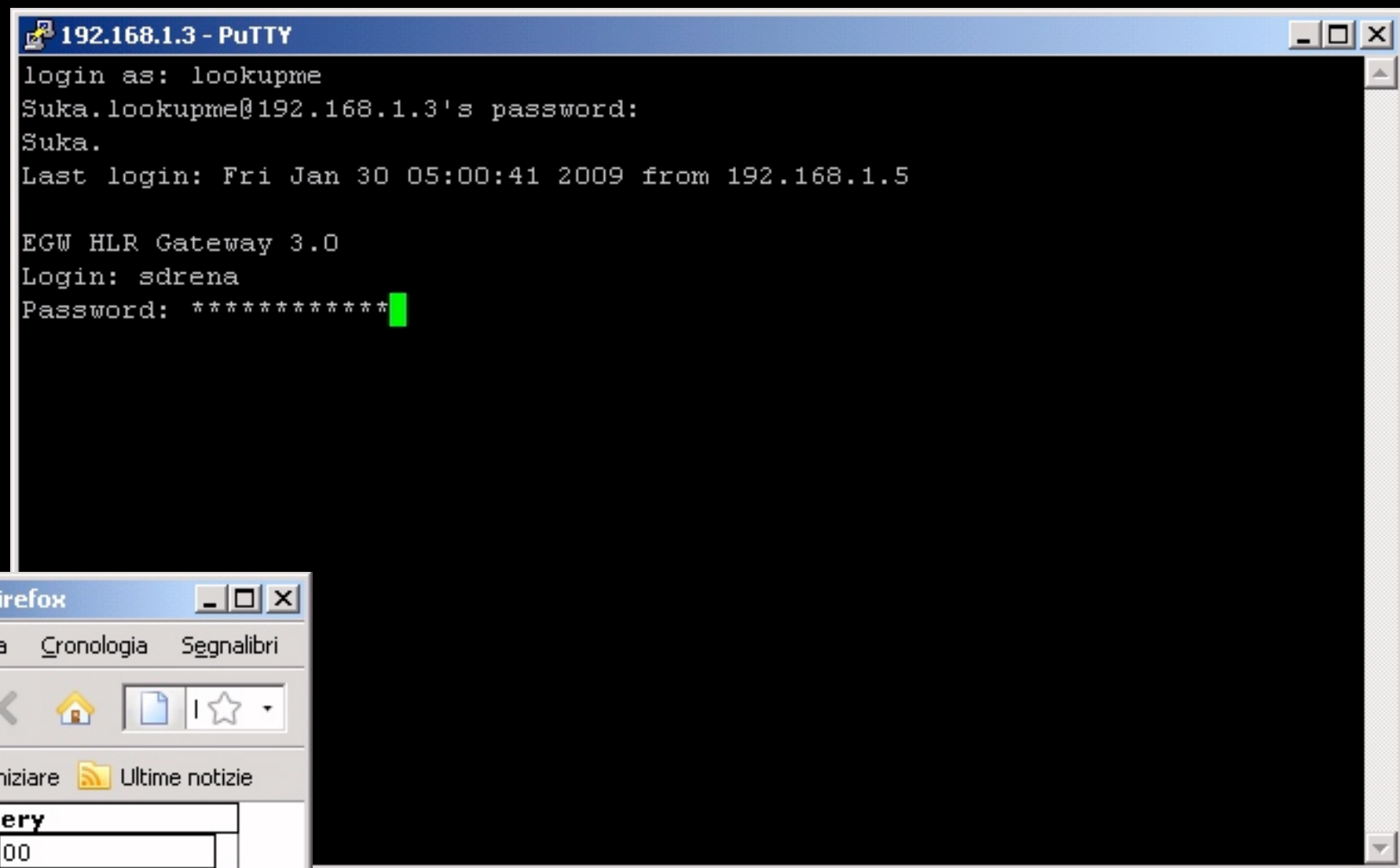


Dimmi il tuo
MSISDN e ti dirò
l'MSISDN del tuo
MSC!



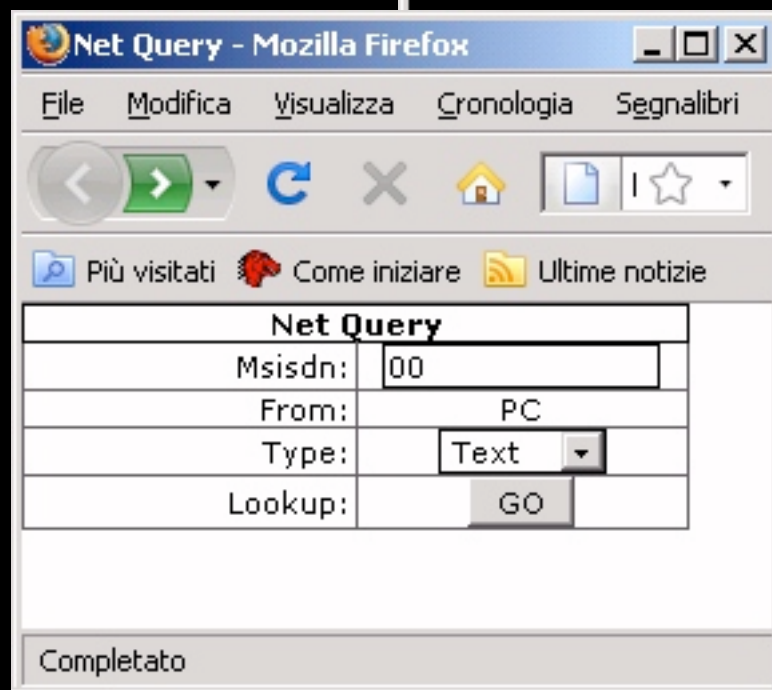
Volete qualche esempio?

Some example



```
192.168.1.3 - PuTTY
login as: lookupme
Suka.lookupme@192.168.1.3's password:
Suka.
Last login: Fri Jan 30 05:00:41 2009 from 192.168.1.5

EGW HLR Gateway 3.0
Login: sdrena
Password: *****
```



Net Query	
Msisdn:	00
From:	PC
Type:	Text
Lookup:	GO

Completato

Some example

192.168.1.3 - PuTTY

```
{
  [id] => 266
  [networkcode] => 22299
  [mcc] => 222
  [mnc] => 99
  [country] => Italy
  [operator] => Hi3G
}

[position] => Array
(
  [0] => Array
  (
    [city] => bergamo
    [subcity] => sorisole
    [r-id] => 891
    [prov] => BG
    [regione] => Lombardia
    [x] => 45.7000
    [y] => 09.6667
    [ct_id] => 39
  )

  [1] => Array
```

Epto (A)
LordScinawa

Hlr Lookup - Mozilla Firefox

FileModificaVisualizzaCronologiaSegnalibriStrumenti?

http://192.168.1.3/hlr/index.php

Più visitatiCome iniziareUltime notizie

Response		
Msisdn:	+00	
Mcc:	222	
Mnc:	10	
Networkcode:	22210	
Network {	Id:	114
	Networkcode:	22210
	Mcc:	222
	Mnc:	10
	Country:	Italy
	Operator:	Omnitel Pronto
Lnetwork {	Id:	114
	Networkcode:	22210
	Mcc:	222
	Mnc:	10
	Country:	Italy
	Operator:	Omnitel Pronto
City {	Id:	90
	Msc:	393492001153
	Ido:	155 156 160 180
	City:	milano
	Subcity:	
	Networkcode:	22210
	Operator:	Vodafone (Omnitel Pronto)
	Errorcode:	
	E:	1
	P:	4
	Pro:	0
	Typ:	UMTS
	Sup:	1
Introaming:	0	
Type:	UMTS	
Sup:	2	
Retcode:	200	
Status:	Ok	
Regione:		
Citta {	milano	
	pavia	

Completato

Some example

Response		
Msisdn:	+0039 [REDACTED]	
Mcc:	222	
Mnc:	01	
Networkcode:	22201	
Network {	Mcc:	222
	Mnc:	1
Lnetwork {	Mcc:	222
	Mnc:	1
City:	TRUE	
Introaming:	0	
Retcode:	200	
Status:	Ok	
Regione:	Toscana	
Citta {	firenze	

Bug fix?

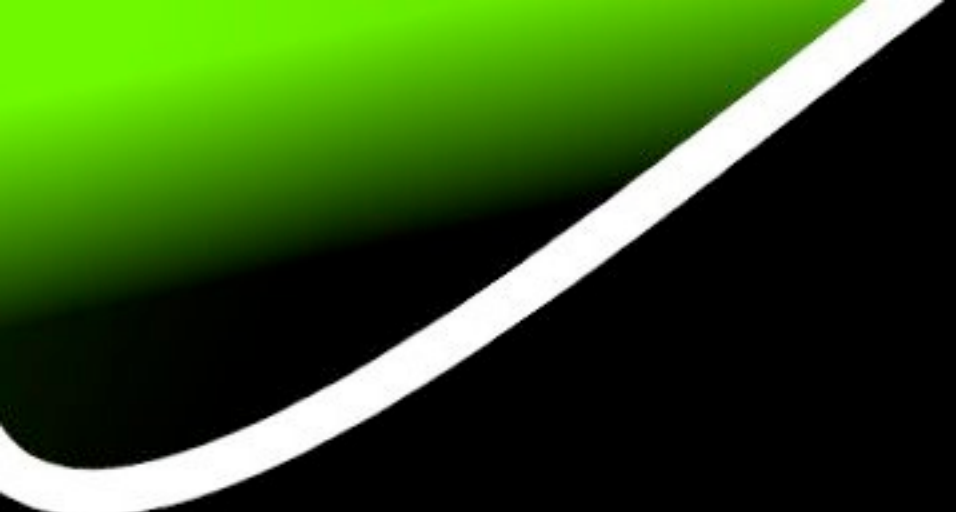
Ci si può
proteggere?

Link interessanti..

- ◇ http://bork.informatik.uni-erlangen.de/pub/ccc/25c3/video_h264_720x576/25c3-2997-en-locating_mobile_phones_using_ss7.mp4

Domande?





Grazie per l'attenzione!