immi il tuo numero
ti dirò dove sei

Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

$whoami

Enzo Epto (A) Anci
nci

- 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

Dimmi il tuo numero
e ti dirò dove sei

$whoami

Alessandro Lordscinawa Luongo
uongo
-lordscinawa [at] {olografix, autistici} [dot] org

-Università degli studi di Milano - Sicurezza delle Reti e dei Sistemi Informatici

- Supporta/Membro di:

Perl.it

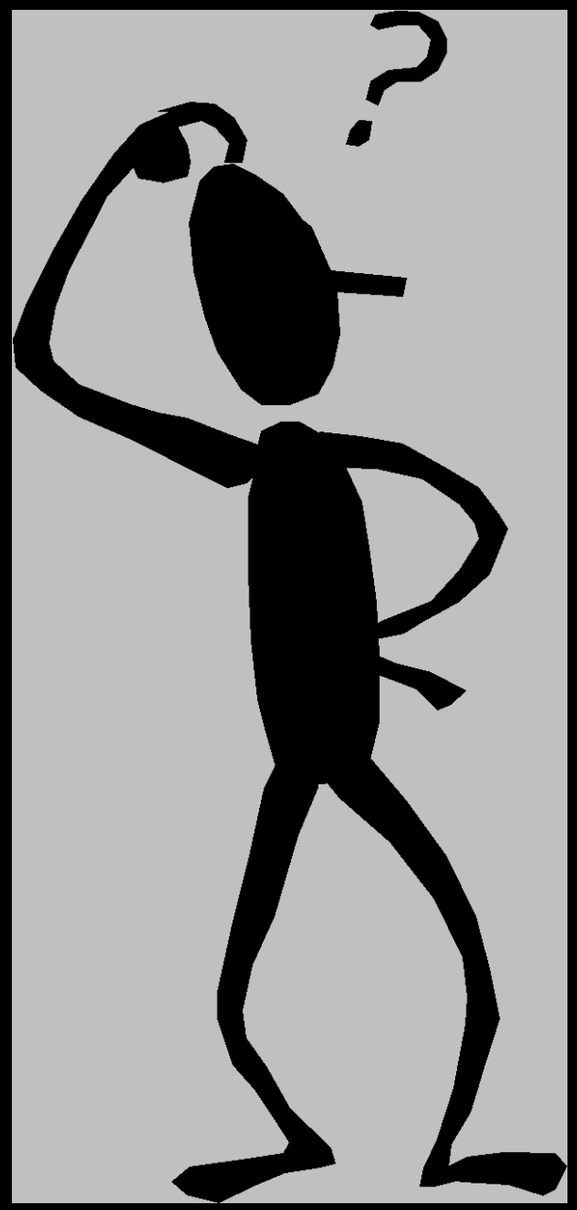
immi il tuo numero
ti dirò dove sei

Pronto! Con.. quanti parlo?

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

Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei



Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

No!

Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

Quindi?

Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

La nostra posizione...

Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

...e' un dato personale?

Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

Un’ attimo di riflessione

Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

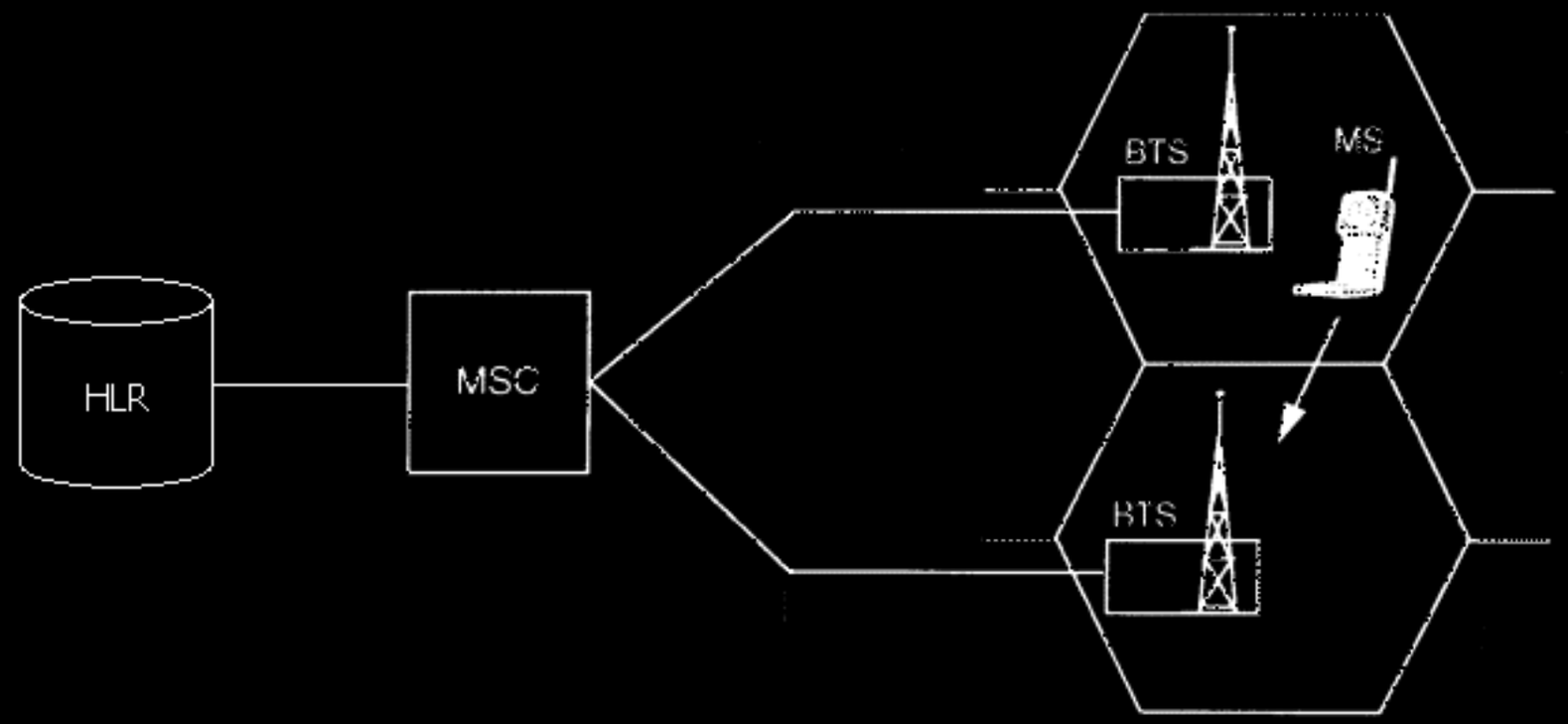
Qualcuno voleva vederci chiaro...

Epto (A)
LordScinawa

Introduzione al sistema di telefonia mobile

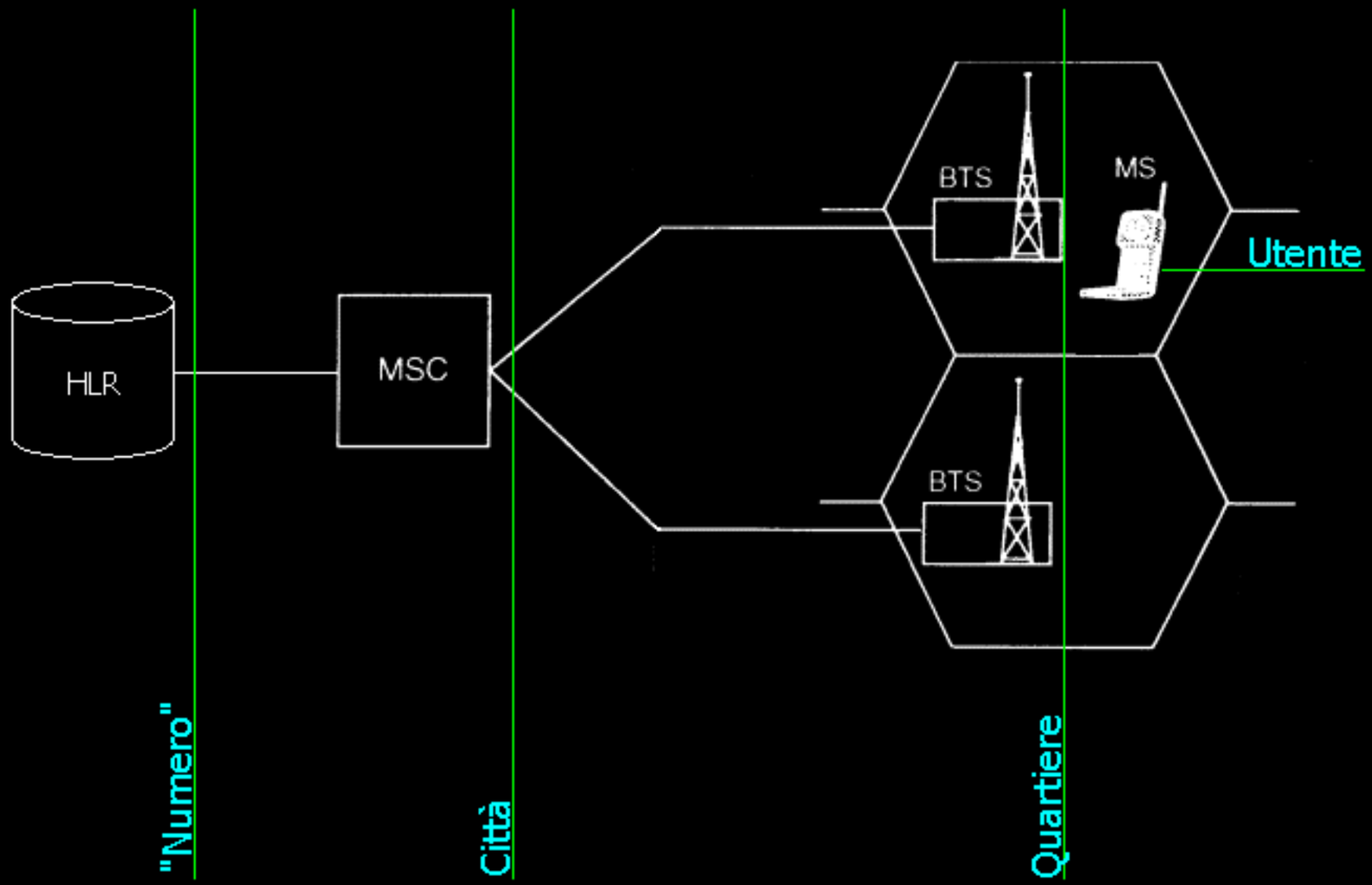
Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei



Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei



Epto (A)
LordScinawa

Dimmi il tuo numero
e ti dirò dove sei

PSTN vs. GSM/UMTS

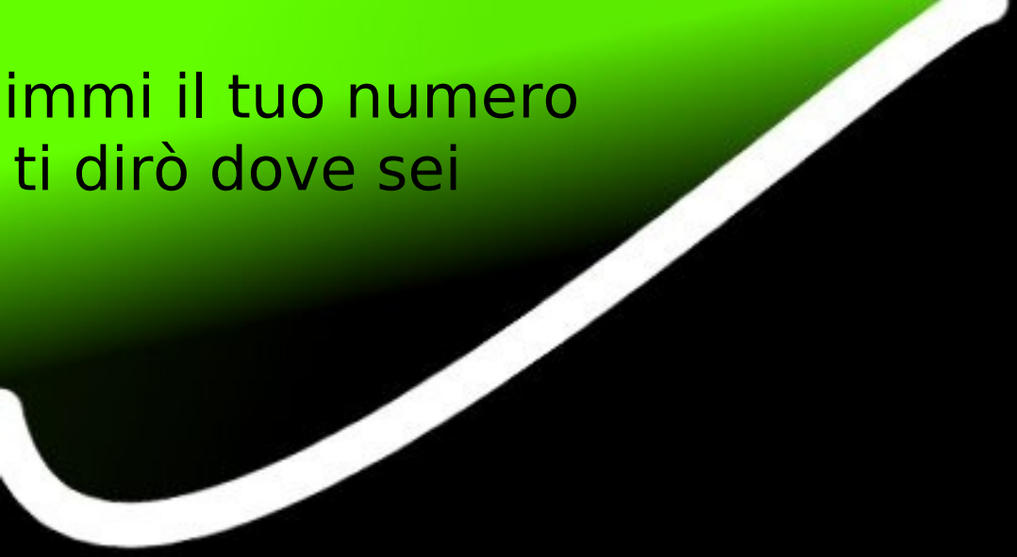
C’è qualche analogia?
(nei due sistemi?)

Dimmi il tuo numero
e ti dirò dove sei

Nella vecchia rete fissa, ogni località ha un prefisso telefonico

Dimmi il tuo numero
e ti dirò dove sei

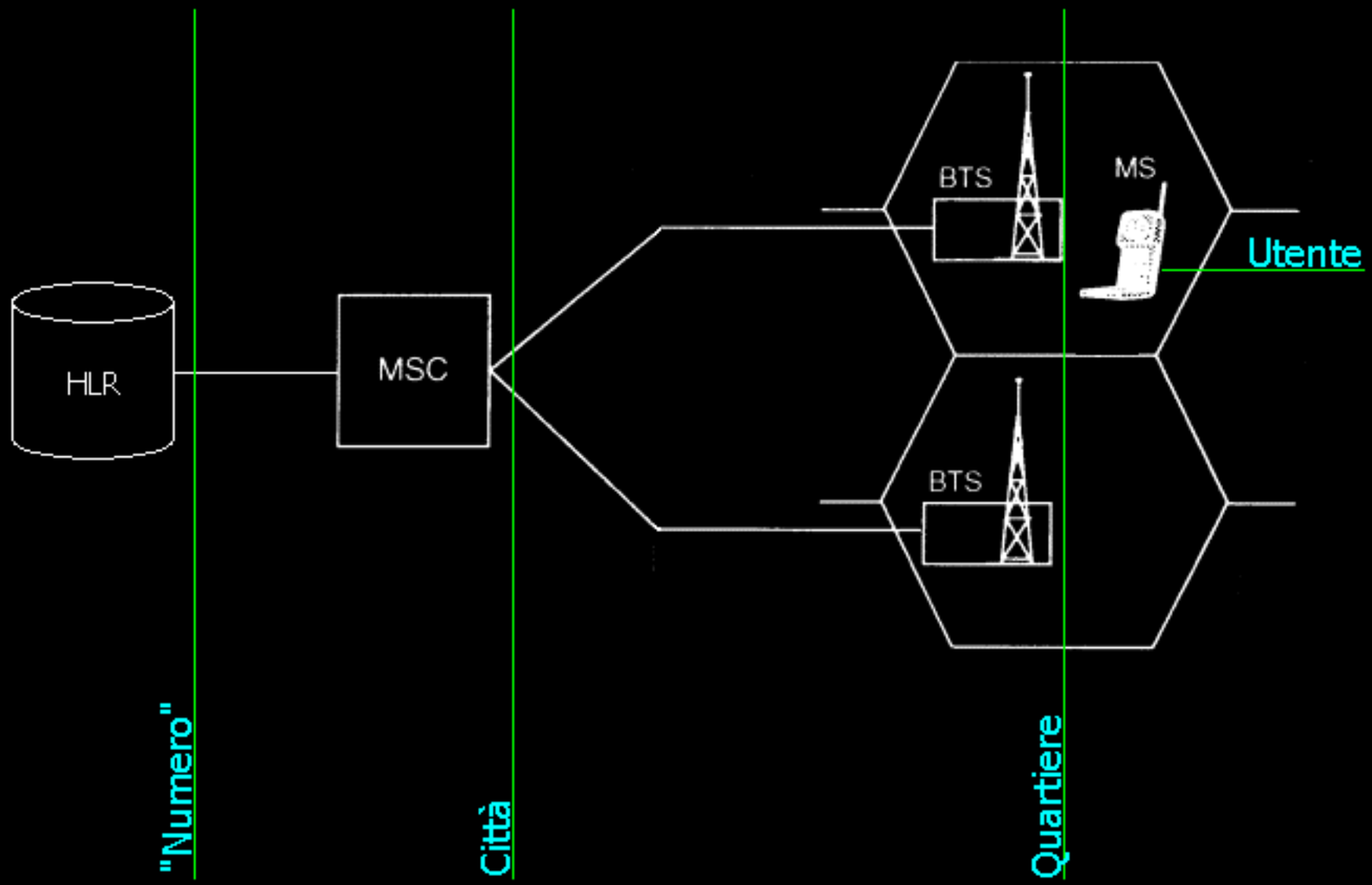
- 06 - 907080 (Roma)
- 02 - 907080 (Milano)
- 0432 - 907080 (Udine)
- 049 - 907080 (Padova)
- ...
- ...



Ma per la rete GSM?

Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei



Epto (A)
LordScinawa

Gli MSC hanno un numero di telefono?

Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

Si...

Epto (A)
LordScinawa

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

Epto (A)
LordScinawa

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

Epto (A)
LordScinawa

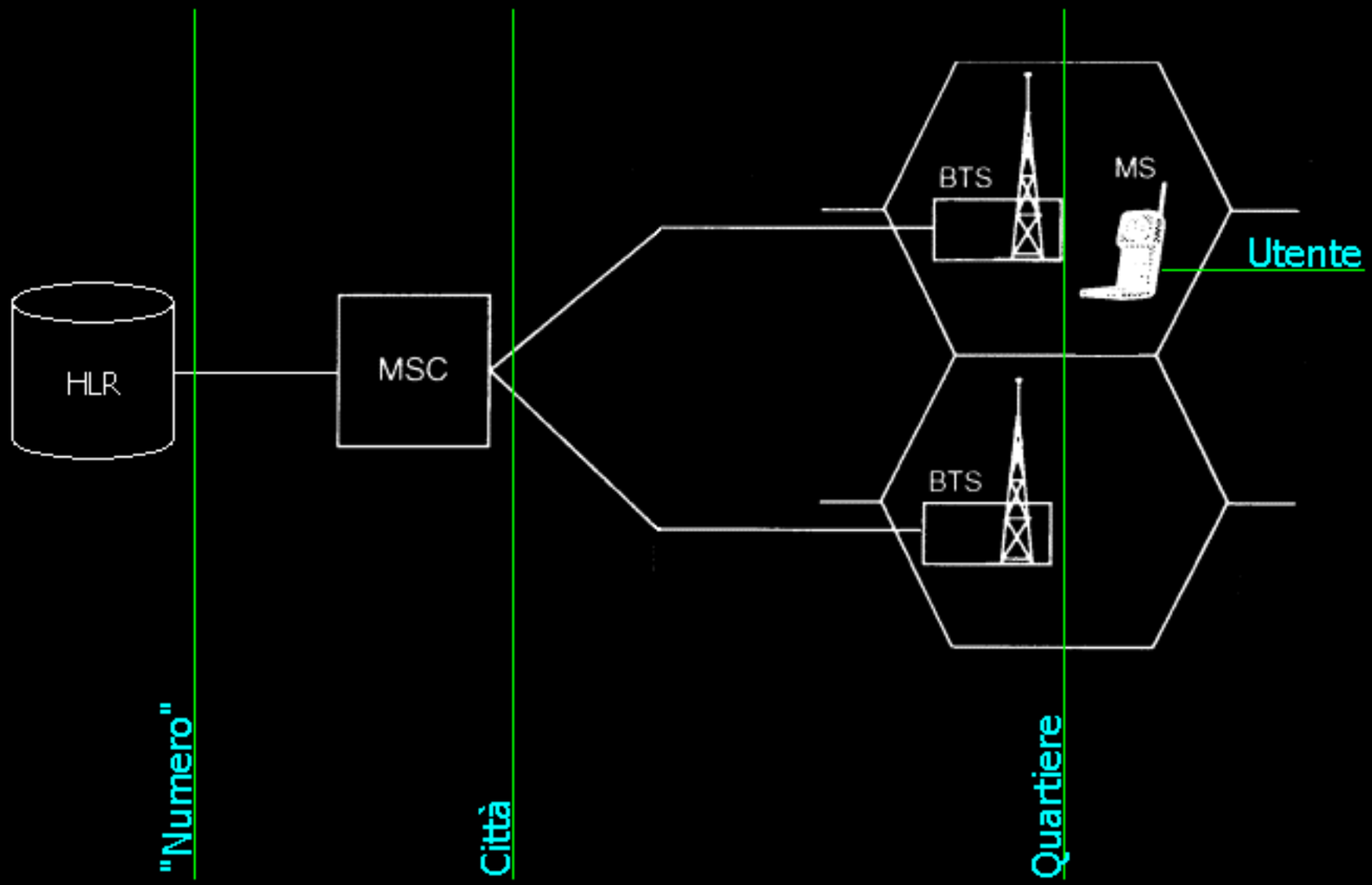
immi il tuo numero
ti dirò dove sei

Le Query

Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

Query HLR “?”



Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

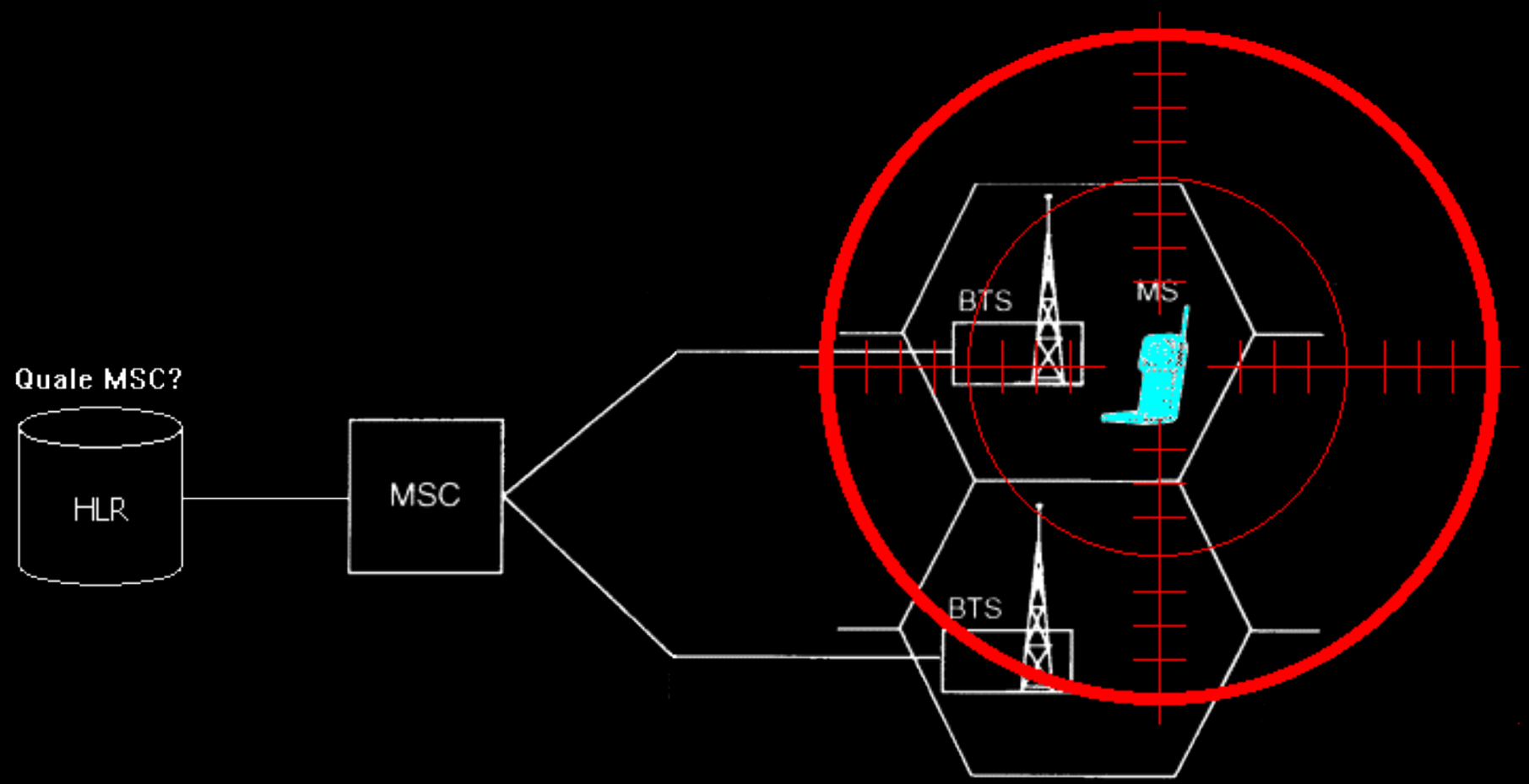
Come si correlano i numeri degli MSC alle città?

Epto (A)
LordScinawa

Procedendo all’inverso

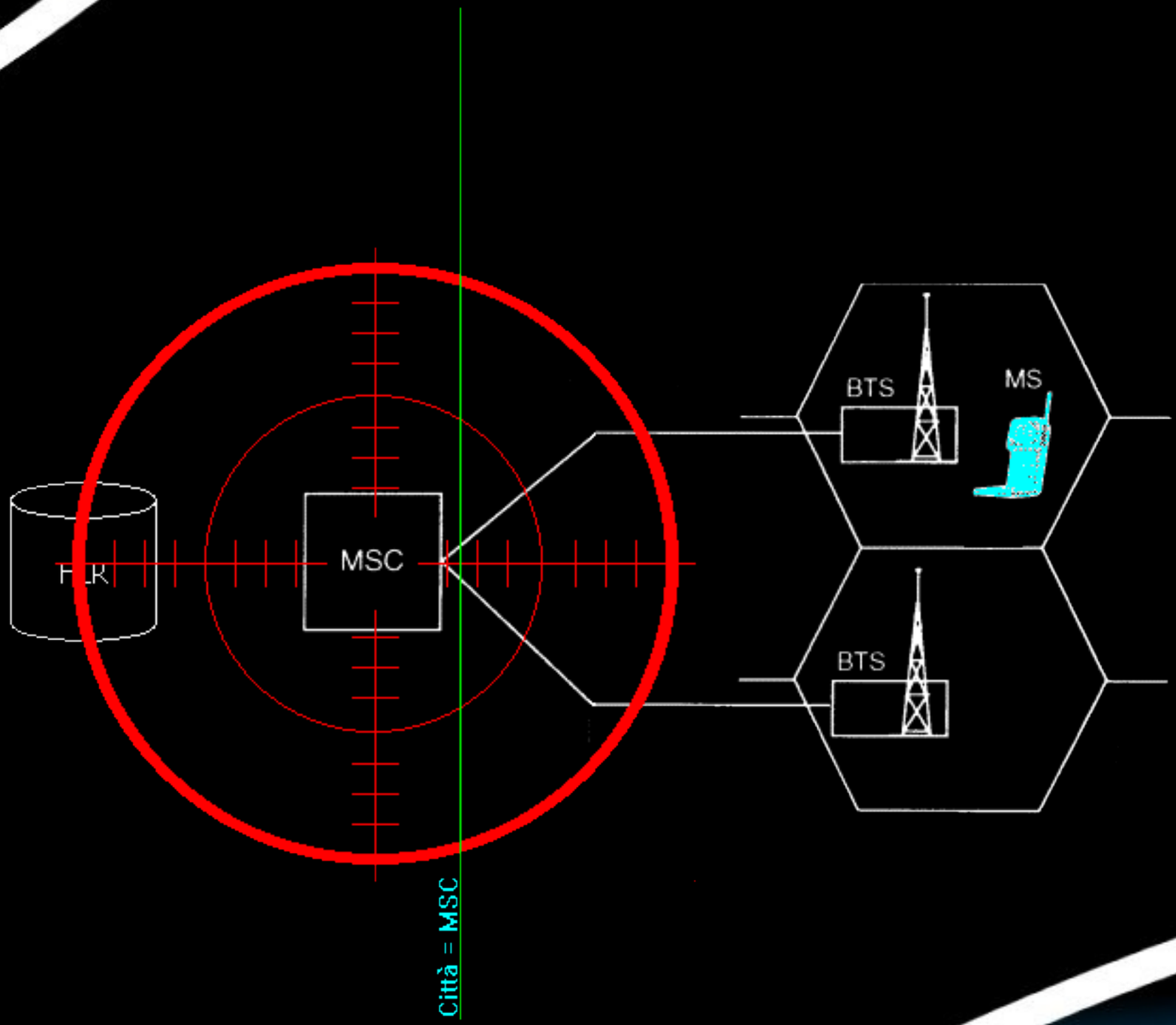
Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei



Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei



Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

Città == MSC!

:)

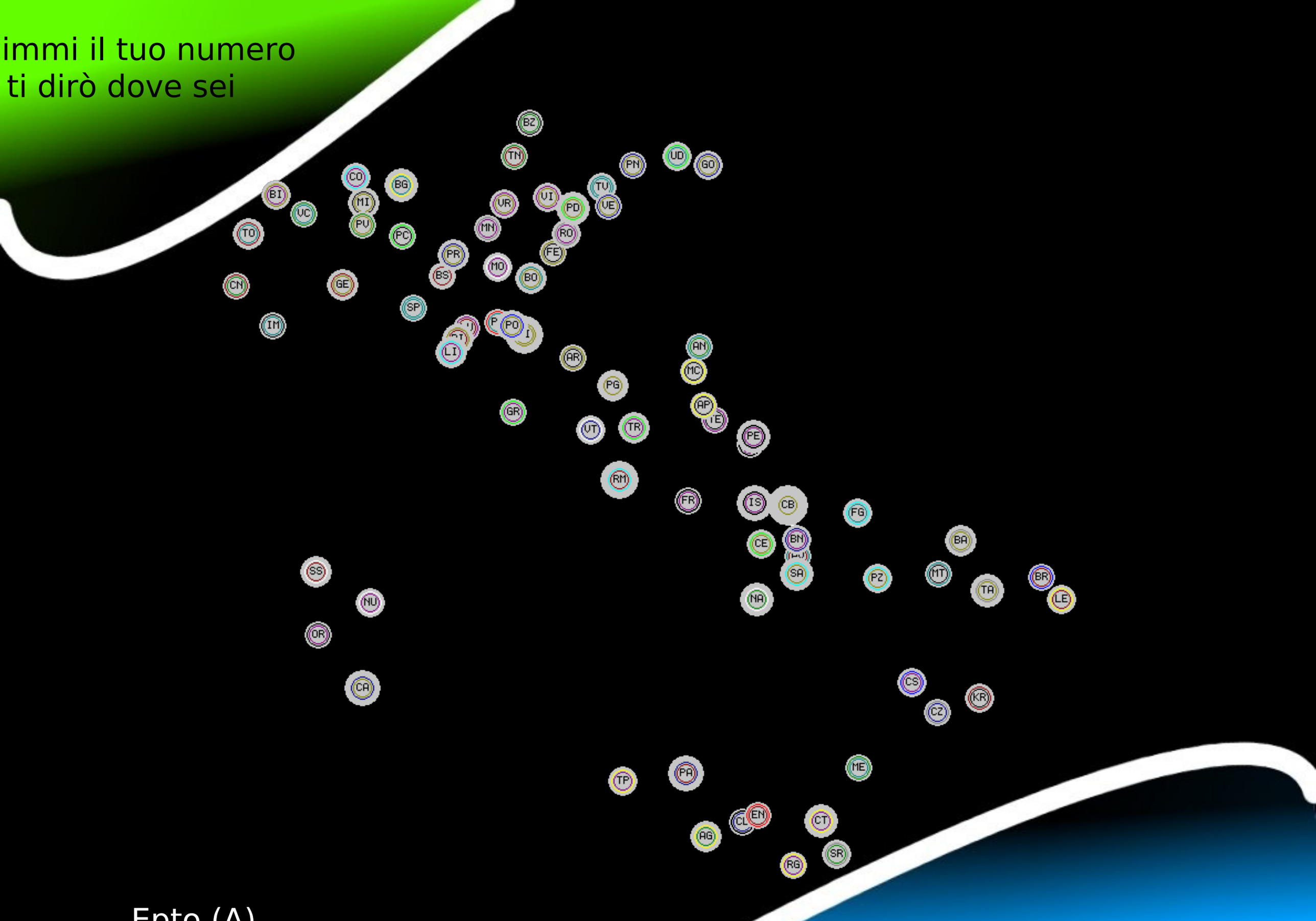
:)

Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

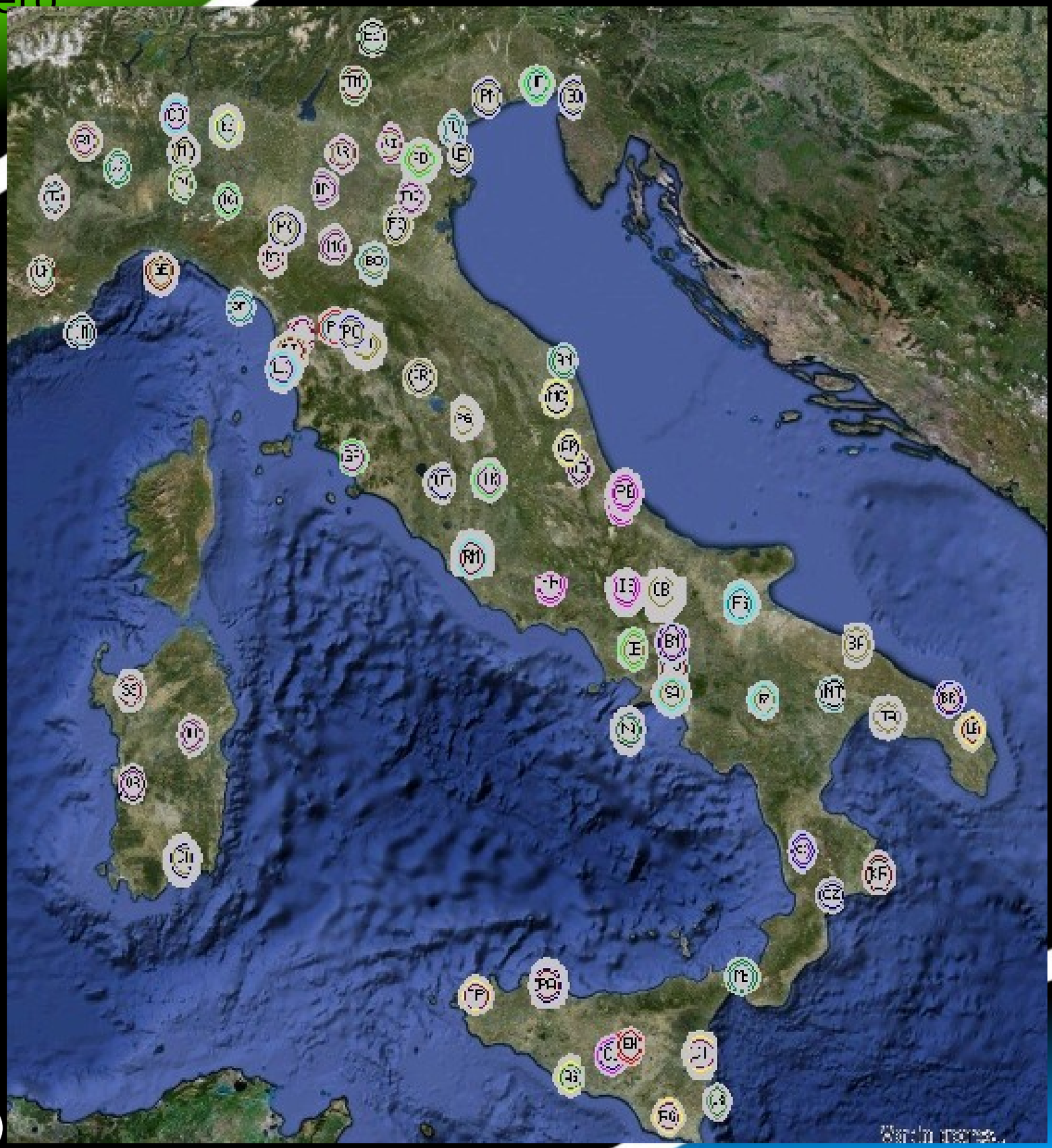
Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei



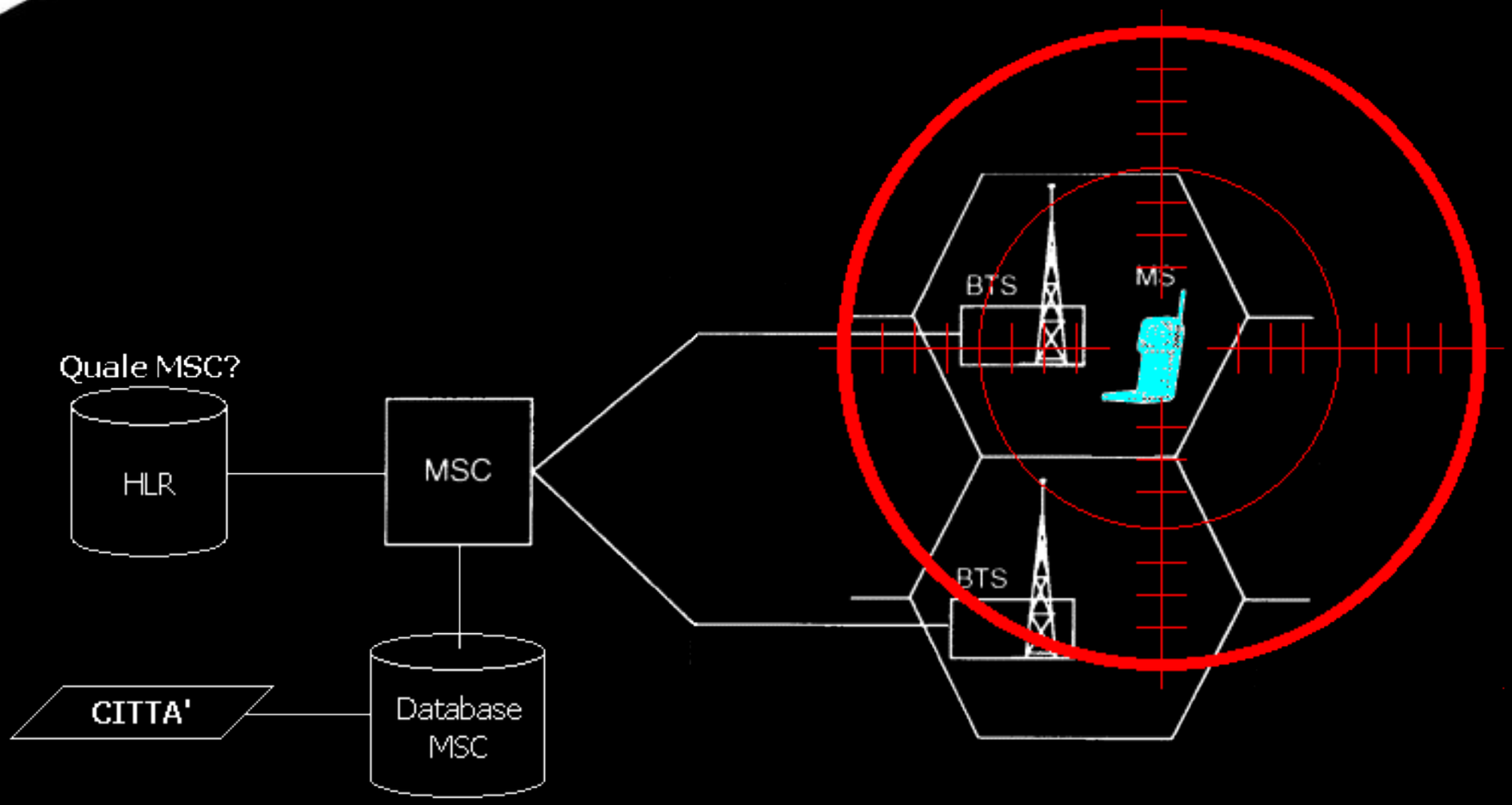
Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei



Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei



Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

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

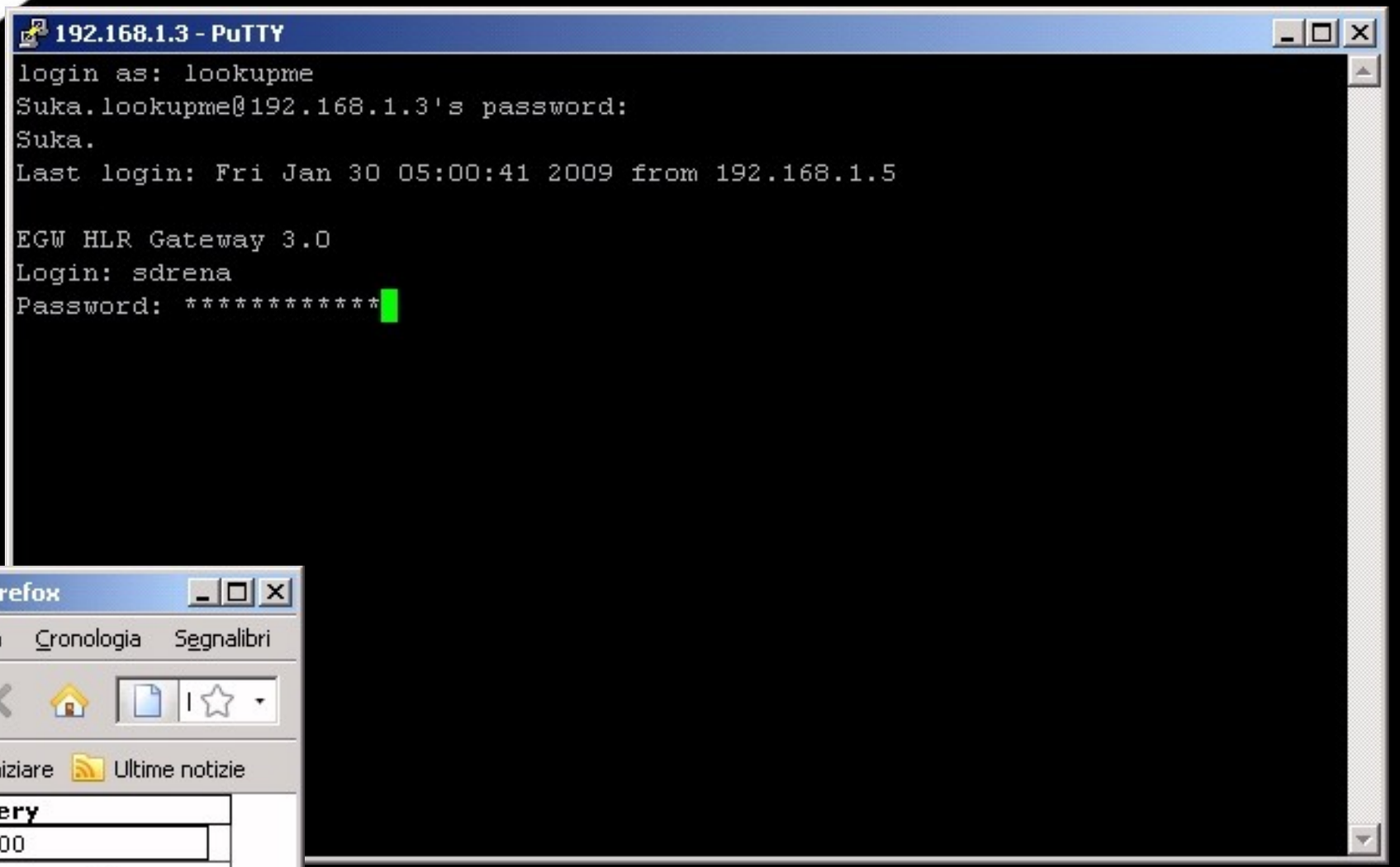
Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

Volete qualche esempio?

Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei



Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

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
```

Hlr Lookup - Mozilla Firefox

File Modifica Visualizza Cronologia Segnalibri Strumenti ?

http://192.168.1.3/hlr/index.php

Più visitati Come iniziare Ultime notizie

Response		
Msisdn:	+00[redacted]	
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

Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

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	

Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

Ci si può proteggere?

Epto (A)
LordScinawa

immi il tuo numero
ti dirò dove sei

Link interessanti..

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

Epto (A)
LordScinawa

Dimmi il tuo numero
e ti dirò dove sei

Domande?

immi il tuo numero
ti dirò dove sei

Grazie per l’attenzione!

Epto (A)
LordScinawa