

# Off line Whois as an IRT query tool

Gilles André/CERTA












# Why would we want to do whois off line ?

- incident involving a huge number of victims
  - e.g. codeded,
  - scan log left by intruder,
- on line queries are slooooooow ;
- too many queries and you are banned ;
- incident regarding sensitive victims

# the database exists

## Index of ftp://ftp.ripe.net/ripe/dbase/split/

[Up to higher level directory](#)

 <a href="#">RIGHTS</a>			1/07/03 0:00:00
 <a href="#">ripe.db.as-block.gz</a>	8 KB	21/09/04 1:29:00	
 <a href="#">ripe.db.as-set.gz</a>	444 KB	21/09/04 1:29:00	
 <a href="#">ripe.db.aut-num.gz</a>	2467 KB	21/09/04 1:29:00	
 <a href="#">ripe.db.domain.gz</a>	5072 KB	21/09/04 1:30:00	
 <a href="#">ripe.db.filter-set.gz</a>	4 KB	21/09/04 1:30:00	
 <a href="#">ripe.db.inet-rtr.gz</a>	12 KB	21/09/04 1:30:00	
 <a href="#">ripe.db.inet6num.gz</a>	276 KB	21/09/04 1:30:00	
 <a href="#">ripe.db.inetnum.gz</a>	61142 KB	21/09/04 1:32:00	
 <a href="#">ripe.db.key-cert.gz</a>	2902 KB	21/09/04 1:32:00	
 <a href="#">...</a>	17 KB	21/09/04 1:32:00	

# the database is structured

```
inetnum: 195.6.202.0 - 195.6.202.255
netname: FR-MINISTERE-DU-TRAVAIL
descr: MINISTERE DU TRAVAIL
country: FR
admin-c: JB13346-RIPE
tech-c: JB13346-RIPE
status: ASSIGNED PA
remarks: travail.gouv.fr
notify: addr-reg@rain.fr
mnt-by: RAIN-TRANSPAC
changed: ingo@rain.fr 20000724
source: RIPE
```

# the database is structured

```
inetnum: 212.201.51.0 - 212.201.63.255
netname: SLUBNET
descr: Saechsische Landesbibliothek -
descr: Staats- und Universitaetsbibliothek
admin-c: AK115-RIPE
tech-c: RT1374-RIPE
country: DE
status: ASSIGNED PA
mnt-by: DEFN-LIR-MNT
mnt-irt: IRT-DFN-CERT
changed: polidi@dfn.de 20010705
changed: polidi@dfn.de 20031008
source: RIPE
```

# olwi off line whois tool

- parse the whois databases
  - RIPE
  - APNIC
  - takes a couple of minutes
- listens to queries
  - each query is an IP address
- answers very fast

```
$ wc -l iplist.txt
```

```
14527
```

```
$ head -1 iplist.txt
```

```
213.56.176.2
```

```
$ cat iplist.txt | time -v olwi ripe.db.inetnum > res
```

```
Elapsed (wall clock) time (h:mm:ss or m:ss): 1:18.22
```

# Results

🔍 **find victims in your constituency:**

```
$ grep :FR: result.txt
217.128.48.218:217.128.0.0 - 217.128.255.255:ALLOCATED PA:FR-TELECOM-20010115 :FR:
217.128.48.218:217.128.48.0 - 217.128.48.255:ASSIGNED PA:IP2000-ADSL-BAS :FR:
217.128.49.223:217.128.0.0 - 217.128.255.255:ALLOCATED PA:FR-TELECOM-20010115 :FR:
217.128.49.223:217.128.49.0 - 217.128.49.255:ASSIGNED PA:IP2000-ADSL-BAS :FR:
$ grep IRT-IRIS-CERT result.txt
193.144.74.65:193.144.64.0 - 193.144.95.255:ASSIGNED PA:USC:ES :IRT-IRIS-CERT
193.144.75.196:193.144.64.0 - 193.144.95.255:ASSIGNED PA:USC:ES :IRT-IRIS-CERT
```

# Requirements

- licence:
  - olwi is GPL
  - databases have their own copyrights
  - please read the databases licences
  - check if they are compatible with what you want to do with olwi
- olwi is based on:
  - very recent version of glib2
  - tested on linux
- olwi needs memory:
  - add swap

# Conclusion

- olwi is still in early developpement
- comments are welcome
- olwi can be used to share information on a need to know basis
  - rather than sending the whole list of IP to everybody, just send the IP to the right IRT

# Questions and answers

