Marco Bagnaschi
m.bagnaschi@icloud.com

Nell’esercizio di oggi lo studente effettuerà una simulazione di fase di raccolta informazioni utilizzando dati pubblici su un target a scelta. Lo scopo di questo esercizio è più che altro familiarizzare con i tool principali della fase di information gathering, quali: Google, per la raccolta passiva delle info dmirty Recon-ng Maltego

Dmitry:

```
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Writing output to '***'

HostIP:***
HostName:***

Gathered Inet-whois information for ***
---------------------------------



inetnum:       ***
netname:       ARUBA-NET
descr:         Aruba S.p.A. - Cloud Services Farm2
country:       IT
admin-c:       SS936-RIPE
tech-c:        AN3450-RIPE
status:        ASSIGNED PA
remarks:       INFRA-AW
mnt-by:        ARUBA-MNT
created:       2014-12-11T16:16:20Z
last-modified:  2014-12-11T16:16:20Z
source:        RIPE

role:          ARUBA Network
address:       Aruba S.p.A.
address:       via S.Clemente 53
address:       24036 Ponte San Pietro (BG)
address:       Italy
abuse-mailbox:  abuse@staff.aruba.it
admin-c:       SC279-RIPE
admin-c:       AC68-RIPE
tech-c:        LR8449-RIPE
tech-c:        PL14025-RIPE
```

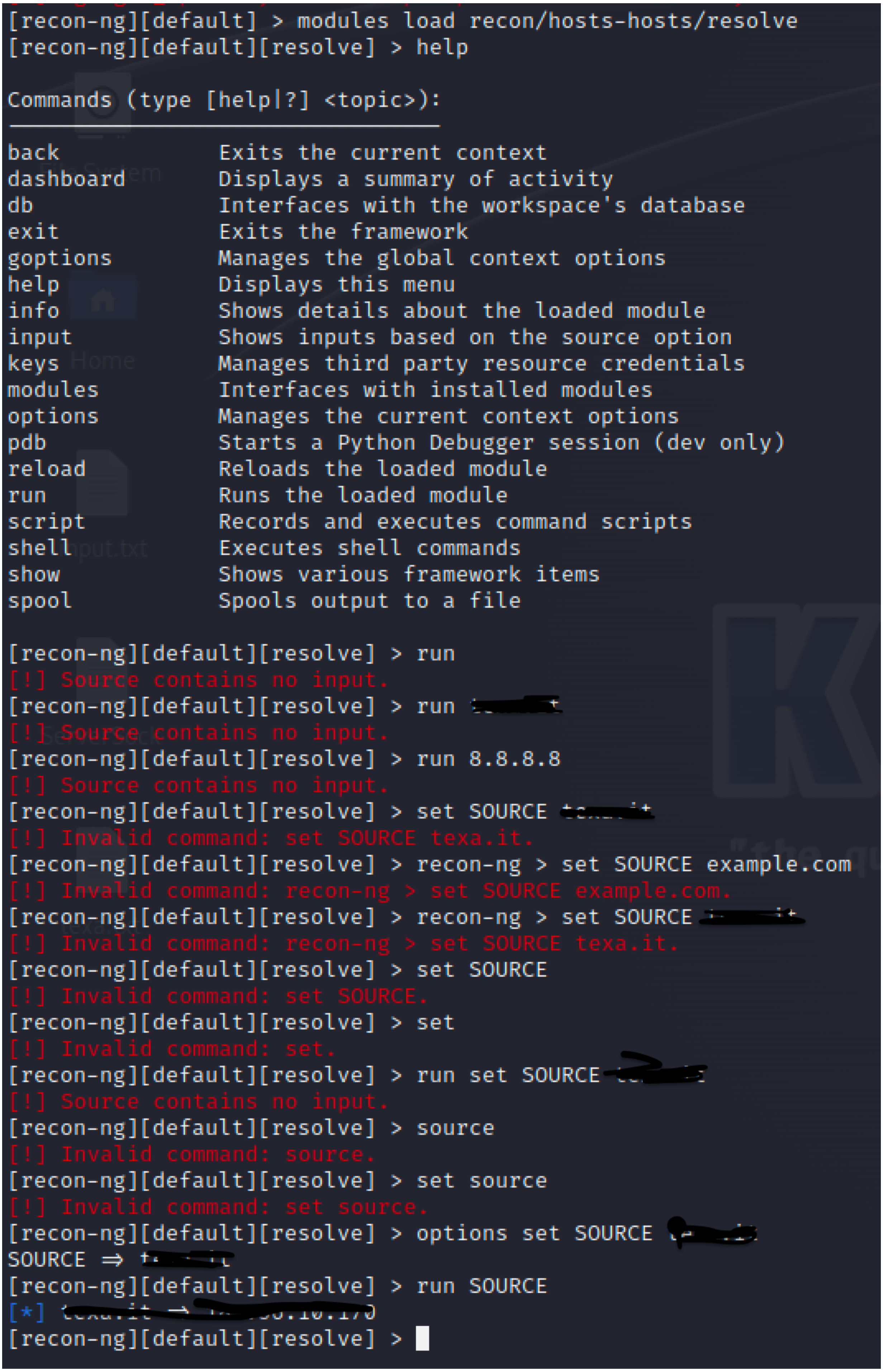
```
tech-c:        MP36509-RIPE
tech-c:        RADA-RIPE
nic-hdl:       AN3450-RIPE
mnt-by:        ARUBA-MNT
created:       2008-11-19T19:02:34Z
last-modified: 2021-09-03T15:23:40Z
source:        RIPE # Filtered

person:        ***
address:       Aruba S.p.A.
address:       Via S.Clemente, 53
address:       24036 Ponte San Pietro (BG)
phone:         +39 ***
fax-no:        +39 ***
nic-hdl:       SS936-RIPE
mnt-by:        ARUBA-MNT
created:       1970-01-01T00:00:00Z
last-modified: 2017-11-15T08:14:40Z
source:        RIPE # Filtered

% Information related to '***/22AS31034'

route:         ***/22
descr:         ARUBA.IT Network
origin:        AS31034
mnt-by:        ARUBA-MNT
created:       2014-05-26T09:16:46Z
last-modified: 2014-05-26T09:16:46Z
source:        RIPE

% This query was served by the RIPE Database Query Service version 1.109.1 (BUSA)



Gathered Inic-whois information for ***
---------------------------------

Domain:             ***
Status:             ok
Signed:             no
Created:            1997-09-24 00:00:00
Last Update:        2023-09-27 00:51:18
Expire Date:        2024-09-11

Registrant
  Organization:     ***
  Address:          via ***
```

```
            IT
  Created:        2007-09-11 12:51:11
  Last Update:    2010-11-29 12:23:53

Admin Contact
  Name:           ***
  Organization:   ***
  Address:        ***
            ***



  Created:        2007-09-11 12:51:11
  Last Update:    2010-11-29 12:23:53

Technical Contacts
  Name:           Technical Support
  Organization:   Register SpA
  Address:        Via Zanchi 22
            Bergamo
            24126
            BG
            IT
  Created:        2009-09-28 11:01:09
  Last Update:    2020-12-09 16:18:25

Registrar
  Organization:   Register S.p.a.
  Name:           REGISTER-REG
  Web:            https://www.register.it
  DNSSEC:         yes

Gathered Netcraft information for ***
---------------------------------

Retrieving Netcraft.com information for ***
Netcraft.com Information gathered

Gathered Subdomain information for ***
---------------------------------
Searching Google.com:80...
HostName:***
HostIP:***
HostName:***
HostIP:127.0.0.1
HostName:***
```

```
HostIP:127.0.0.1
Searching Altavista.com:80...
Found 3 possible subdomain(s) for host ***, Searched 0 pages containing 0 results

Gathered E-Mail information for ***
---------------------------------
Searching Google.com:80...
Searching Altavista.com:80...
Found 0 E-Mail(s) for host ***, Searched 0 pages containing 0 results

Gathered TCP Port information for ***
---------------------------------

 Port      State

21/tcp      open
25/tcp      open
80/tcp      open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed

Error: Unable to close file stream writing to ***
```

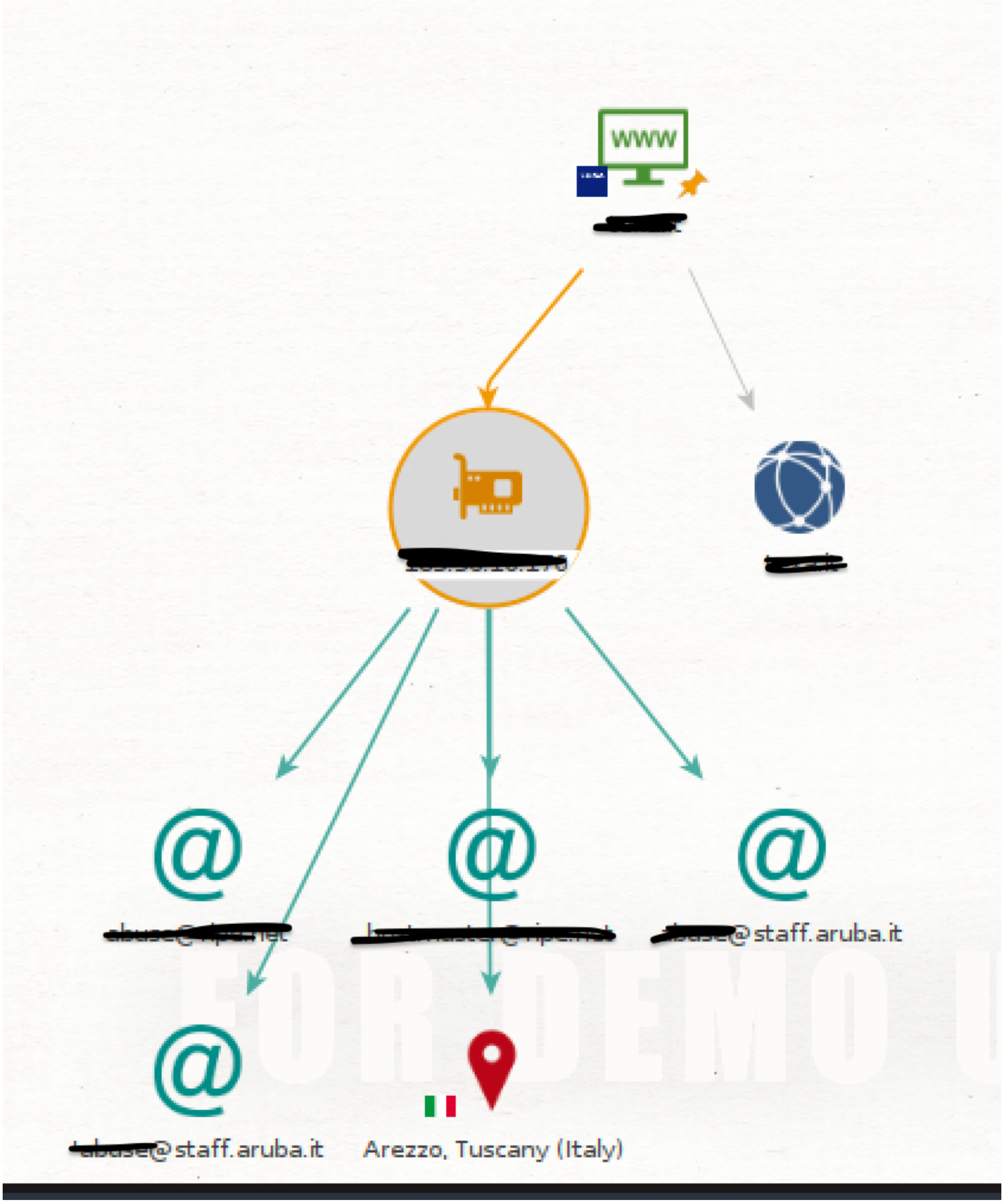
Recon-ng:

Con il modulo di recon che si vede in figura andiamo a verificare la veridicità dell'ip del target trovato con il precedente tool



```
[recon-ng][default] > modules load recon/hosts-hosts/resolve
[recon-ng][default][resolve] > help

Commands (type [help|?] <topic>):
_________________________________
back              Exits the current context
dashboard         Displays a summary of activity
db                Interfaces with the workspace's database
exit              Exits the framework
goptions          Manages the global context options
help              Displays this menu
info              Shows details about the loaded module
input             Shows inputs based on the source option
keys              Manages third party resource credentials
modules           Interfaces with installed modules
options           Manages the current context options
pdb               Starts a Python Debugger session (dev only)
reload            Reloads the loaded module
run               Runs the loaded module
script            Records and executes command scripts
shell             Executes shell commands
show              Shows various framework items
spool             Spools output to a file

[recon-ng][default][resolve] > run
[!] Source contains no input.
[recon-ng][default][resolve] > run [redacted]
[!] Source contains no input.
[recon-ng][default][resolve] > run 8.8.8.8
[!] Source contains no input.
[recon-ng][default][resolve] > set SOURCE [redacted]
[!] Invalid command: set SOURCE texa.it.
[recon-ng][default][resolve] > recon-ng > set SOURCE example.com
[!] Invalid command: recon-ng > set SOURCE example.com.
[recon-ng][default][resolve] > recon-ng > set SOURCE [redacted]
[!] Invalid command: recon-ng > set SOURCE texa.it.
[recon-ng][default][resolve] > set SOURCE
[!] Invalid command: set SOURCE.
[recon-ng][default][resolve] > set
[!] Invalid command: set.
[recon-ng][default][resolve] > run set SOURCE [redacted]
[!] Source contains no input.
[recon-ng][default][resolve] > source
[!] Invalid command: source.
[recon-ng][default][resolve] > set source
[!] Invalid command: set source.
[recon-ng][default][resolve] > options set SOURCE [redacted]
SOURCE ⇒ [redacted]
[recon-ng][default][resolve] > run SOURCE
[*] [redacted]
[recon-ng][default][resolve] > █
```

Maltego:



Fatta esclusione per la località geografica, tutti gli altri dati vengono confermati rispetto ai tool precedenti.