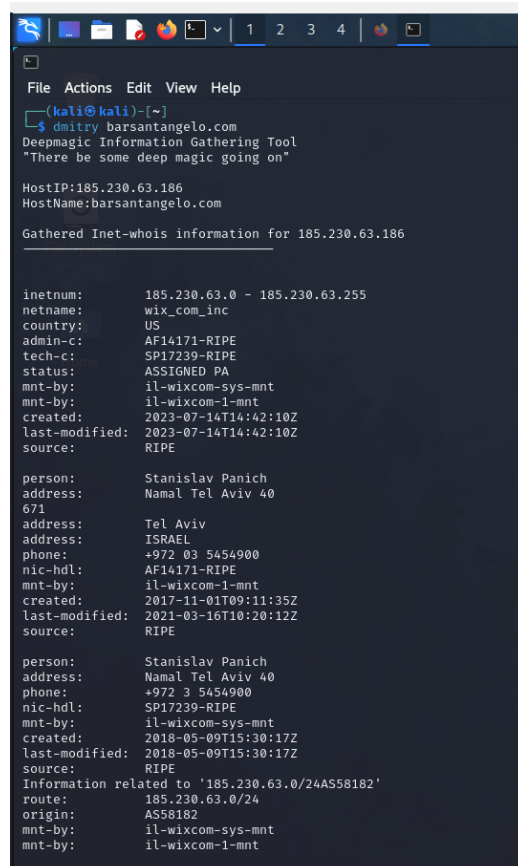


ESERCIZIO W10D1 PRATICA 2

DMITRY:



```
File Actions Edit View Help
~(kali@kali)-[~]
└─$ dmitry barsantangelo.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:185.230.63.186
HostName:barsantangelo.com

Gathered Inet-whois information for 185.230.63.186

inetnum:        185.230.63.0 - 185.230.63.255
netname:        wix_com_inc
country:        US
admin-c:        AF14171-RIPE
tech-c:         SP17239-RIPE
status:         ASSIGNED PA
mnt-by:         il-wixcom-sys-mnt
mnt-by:         il-wixcom-l-mnt
created:        2023-07-14T14:42:10Z
last-modified:  2023-07-14T14:42:10Z
source:         RIPE

person:         Stanislav Panich
address:        Namal Tel Aviv 40
671
address:        Tel Aviv
address:        ISRAEL
phone:          +972 03 5454900
nic-hdl:        AF14171-RIPE
mnt-by:         il-wixcom-l-mnt
created:        2017-11-01T09:11:35Z
last-modified:  2021-03-16T10:20:12Z
source:         RIPE

person:         Stanislav Panich
address:        Namal Tel Aviv 40
phone:          +972 3 5454900
nic-hdl:        SP17239-RIPE
mnt-by:         il-wixcom-sys-mnt
created:        2018-05-09T15:30:17Z
last-modified:  2018-05-09T15:30:17Z
source:         RIPE
Information related to '185.230.63.0/24AS58182'
route:          185.230.63.0/24
origin:         AS58182
mnt-by:         il-wixcom-sys-mnt
mnt-by:         il-wixcom-l-mnt
```

Ecco alcune informazioni raccolte utilizzando lo strumento Dmirty e alcune ricerche:

Informazioni WHOIS sul dominio barsantangelo.com:

Il sito barsantangelo.com è registrato presso il registrar Wix.com Ltd.

Il dominio è stato registrato il 15 giugno 2021 e scadrà il 15 giugno 2024.

I server dei nomi sono NS4.WIXDNS.NET e NS5.WIXDNS.NET.

Informazioni WHOIS sull'indirizzo IP del sito (185.230.63.186):

L'indirizzo IP è assegnato a wix_com_inc negli Stati Uniti.

La persona di contatto è Stanislav Panich.

Informazioni Netcraft:

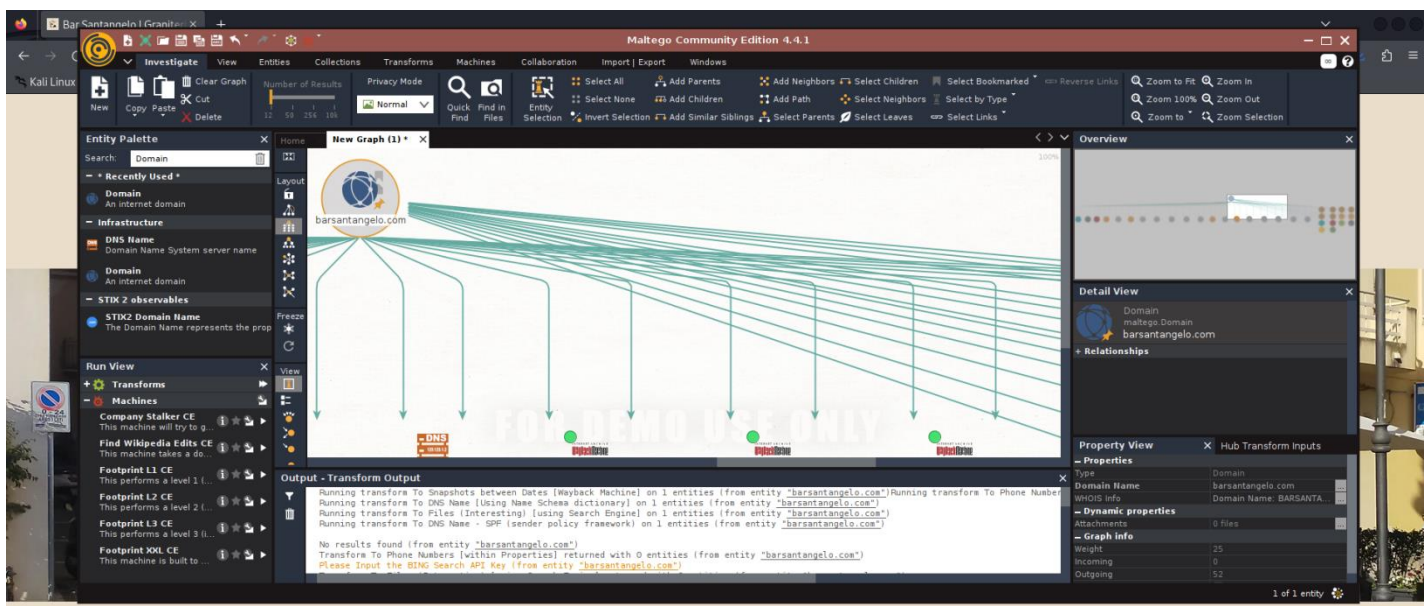
Il sito non sembra avere informazioni rilevanti in Netcraft.

Informazioni sui sottodomini:

Il sottodominio "www.barsantangelo.com" è associato all'indirizzo IP 34.149.87.45.

Informazioni sulle porte aperte: Le porte 80 e 82 sono aperte sull'indirizzo IP 185.230.63.186.

MALTEGO



Ecco un report sulle trasformazioni eseguite per il dominio "barsantangelo.com":

Trasformazione per ottenere URL dalle proprietà: Questa trasformazione non ha restituito alcun risultato. Potrebbe significare che non sono stati trovati URL all'interno delle proprietà del dominio.

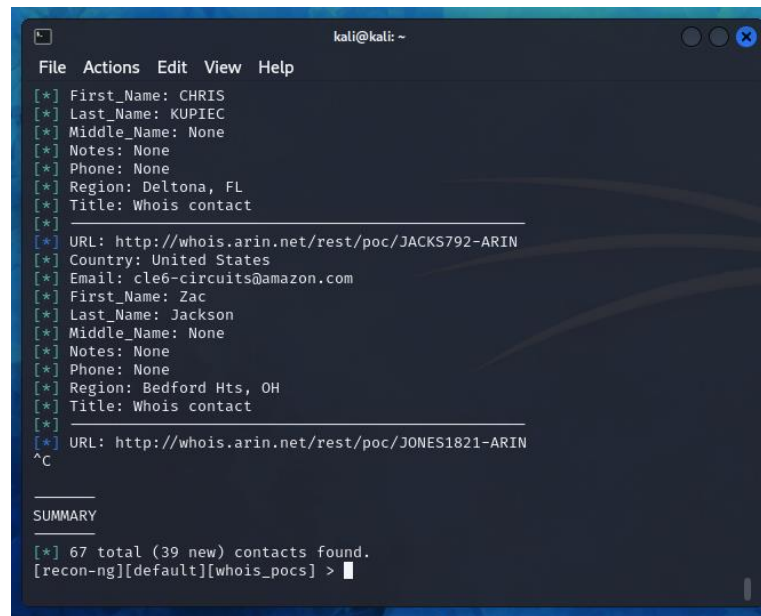
Trasformazione per estrarre gli indirizzi email dalle informazioni WHOIS: Questa trasformazione ha restituito un indirizzo email associato al dominio "barsantangelo.com".

Trasformazione per trovare snapshot contenenti una frase specifica tramite Wayback Machine: Questa trasformazione ha restituito un snapshot contenente la frase specifica associata al dominio "barsantangelo.com".

Trasformazione per ottenere informazioni WHOIS tramite IBM Watson: Questa trasformazione ha restituito 12 entità di informazioni WHOIS correlate al dominio "barsantangelo.com".

Trasformazione per trovare nomi DNS interessanti tramite SecurityTrails: Questa trasformazione non ha restituito alcun risultato. Potrebbe significare che non sono stati trovati nomi DNS interessanti correlati al dominio.

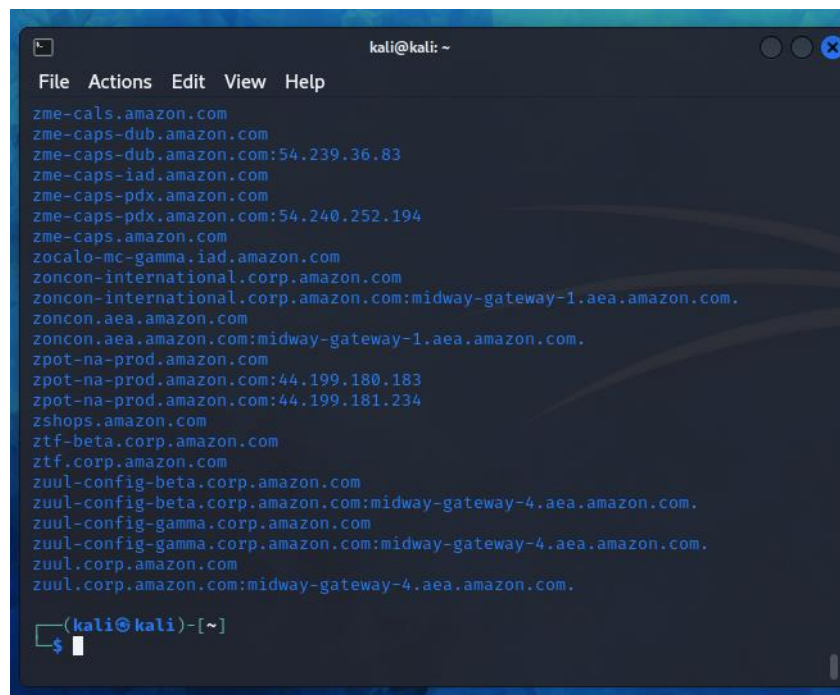
RECON-NG



```
kali@kali: ~  
File Actions Edit View Help  
[*] First_Name: CHRIS  
[*] Last_Name: KUPIEC  
[*] Middle_Name: None  
[*] Notes: None  
[*] Phone: None  
[*] Region: Deltona, FL  
[*] Title: Whois contact  
[*]  
[*] URL: http://whois.arin.net/rest/poc/JACKS792-ARIN  
[*] Country: United States  
[*] Email: cle6-circuits@amazon.com  
[*] First_Name: Zac  
[*] Last_Name: Jackson  
[*] Middle_Name: None  
[*] Notes: None  
[*] Phone: None  
[*] Region: Bedford Hts, OH  
[*] Title: Whois contact  
[*]  
[*] URL: http://whois.arin.net/rest/poc/JONES1821-ARIN  
^C  
  
SUMMARY  
[*] 67 total (39 new) contacts found.  
[recon-ng][default][whois_pocs] > 
```

Con la funziona **whois-pocs** ho ottenuto informazioni sui contatti associati ad Amazon.com, inclusi nomi, email, regioni e titoli. In particolare, ho individuato Kevin Chivington come una figura ricorrente in diverse località, insieme ad altri contatti legati all'azienda.

The Harvester



```
kali@kali: ~  
File Actions Edit View Help  
zme-cals.amazon.com  
zme-caps-dub.amazon.com  
zme-caps-dub.amazon.com:54.239.36.83  
zme-caps-iad.amazon.com  
zme-caps-pdx.amazon.com  
zme-caps-pdx.amazon.com:54.240.252.194  
zme-caps.amazon.com  
zocalo-mc-gamma.iad.amazon.com  
zoncon-international.corp.amazon.com  
zoncon-international.corp.amazon.com:midway-gateway-1.aea.amazon.com.  
zoncon.aea.amazon.com  
zoncon.aea.amazon.com:midway-gateway-1.aea.amazon.com.  
zpot-na-prod.amazon.com  
zpot-na-prod.amazon.com:44.199.180.183  
zpot-na-prod.amazon.com:44.199.181.234  
zshops.amazon.com  
ztf-beta.corp.amazon.com  
ztf.corp.amazon.com  
zuul-config-beta.corp.amazon.com  
zuul-config-beta.corp.amazon.com:midway-gateway-4.aea.amazon.com.  
zuul-config-gamma.corp.amazon.com  
zuul-config-gamma.corp.amazon.com:midway-gateway-4.aea.amazon.com.  
zuul.corp.amazon.com  
zuul.corp.amazon.com:midway-gateway-4.aea.amazon.com.  
  
$ 
```

Ho ottenuto una lista di indirizzi e nomi di dominio associati ad Amazon. Questi includono una vasta gamma di subdomini e domini principali utilizzati per vari scopi, come servizi interni,

strumenti di sviluppo, e-commerce e altro ancora. Potrebbero essere utilizzati per l'accesso a piattaforme, applicazioni interne o servizi specifici all'interno dell'ecosistema Amazon.