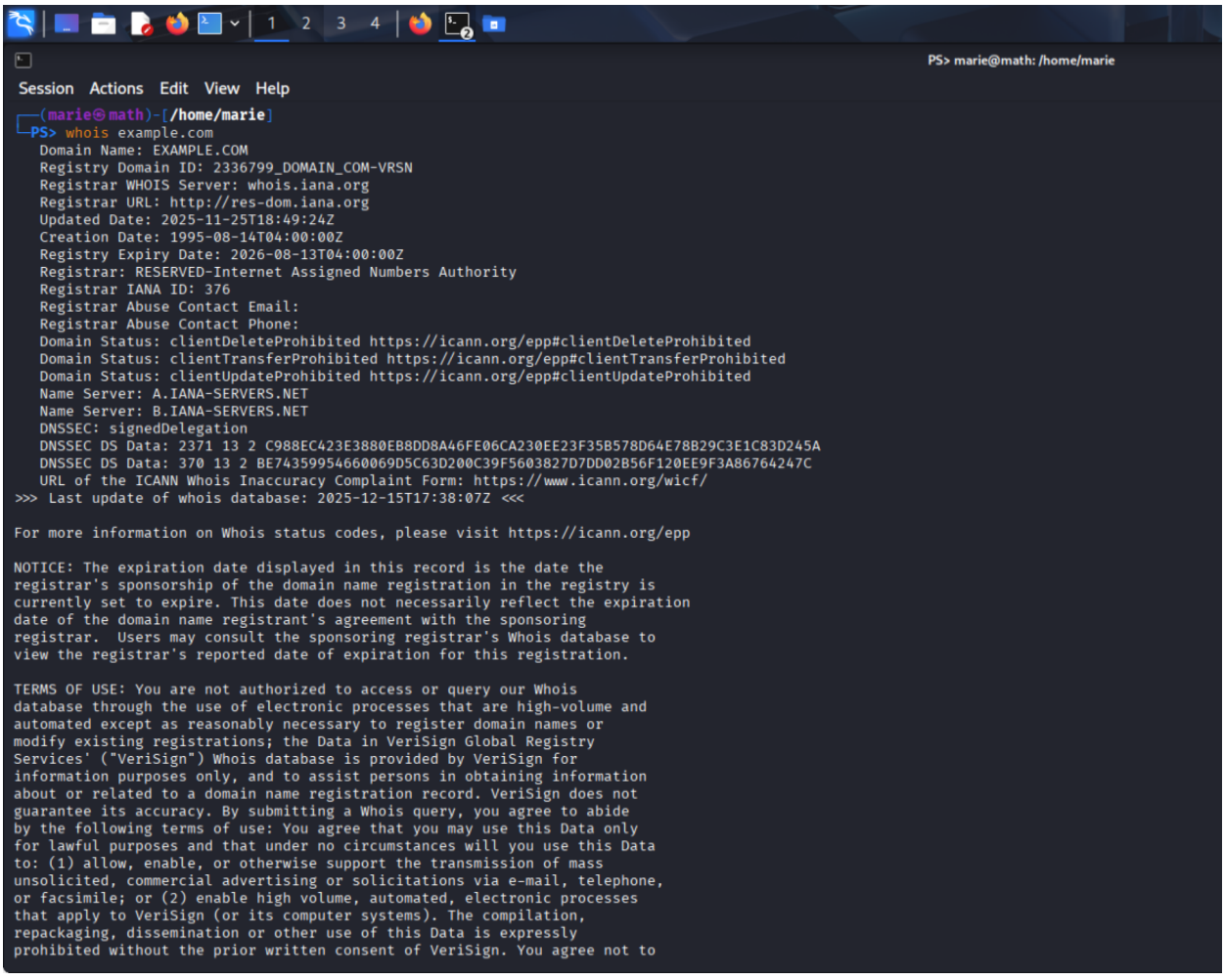
# Passive footprinting & Reconnaissance

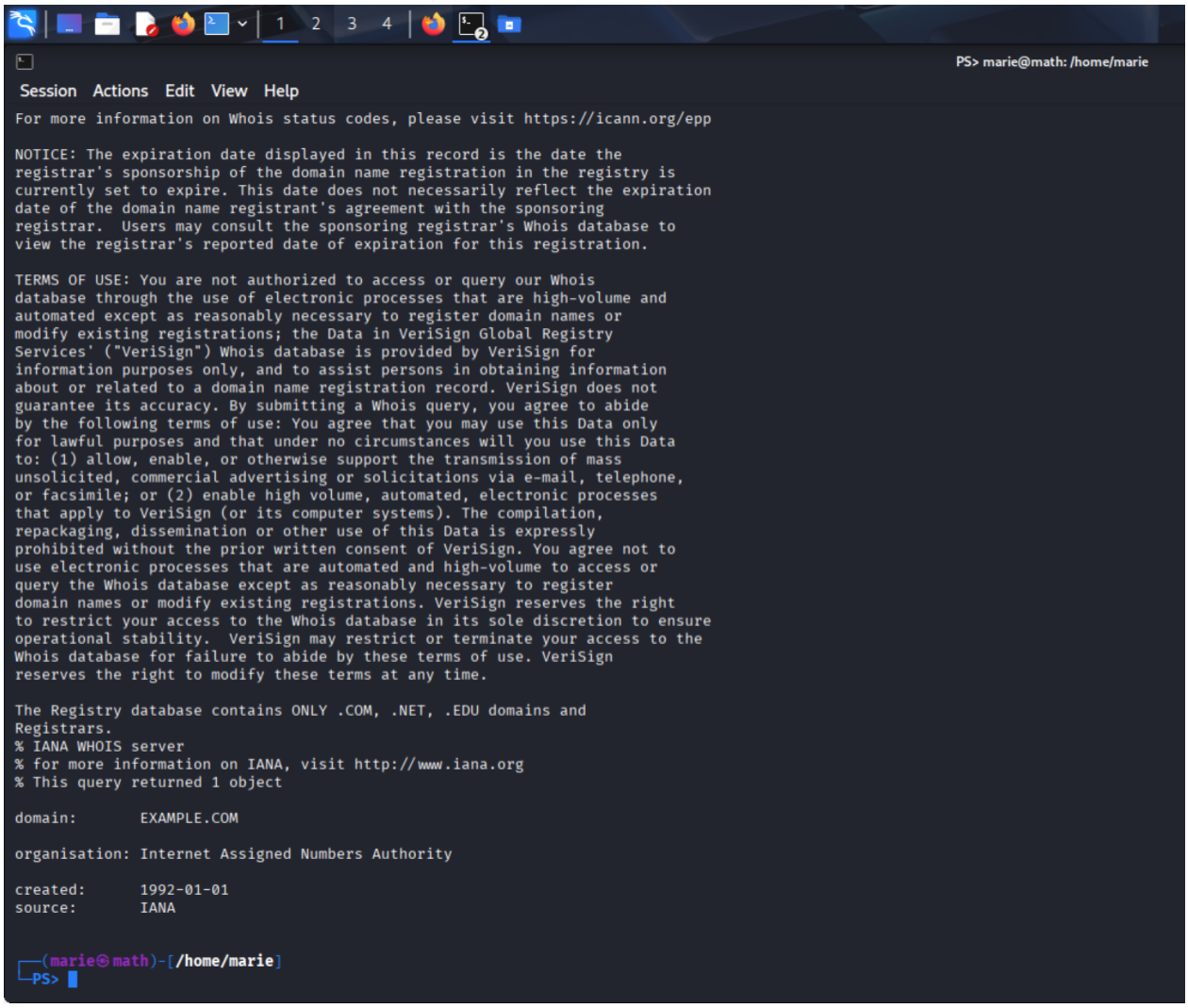
## Step 1: Domain Information Gathering

Domain name chosen-example.com

- Used whois to find domain registration details.
- Used dig or nslookup to identify DNS records.

### Tools: whois, dig, nslookup.

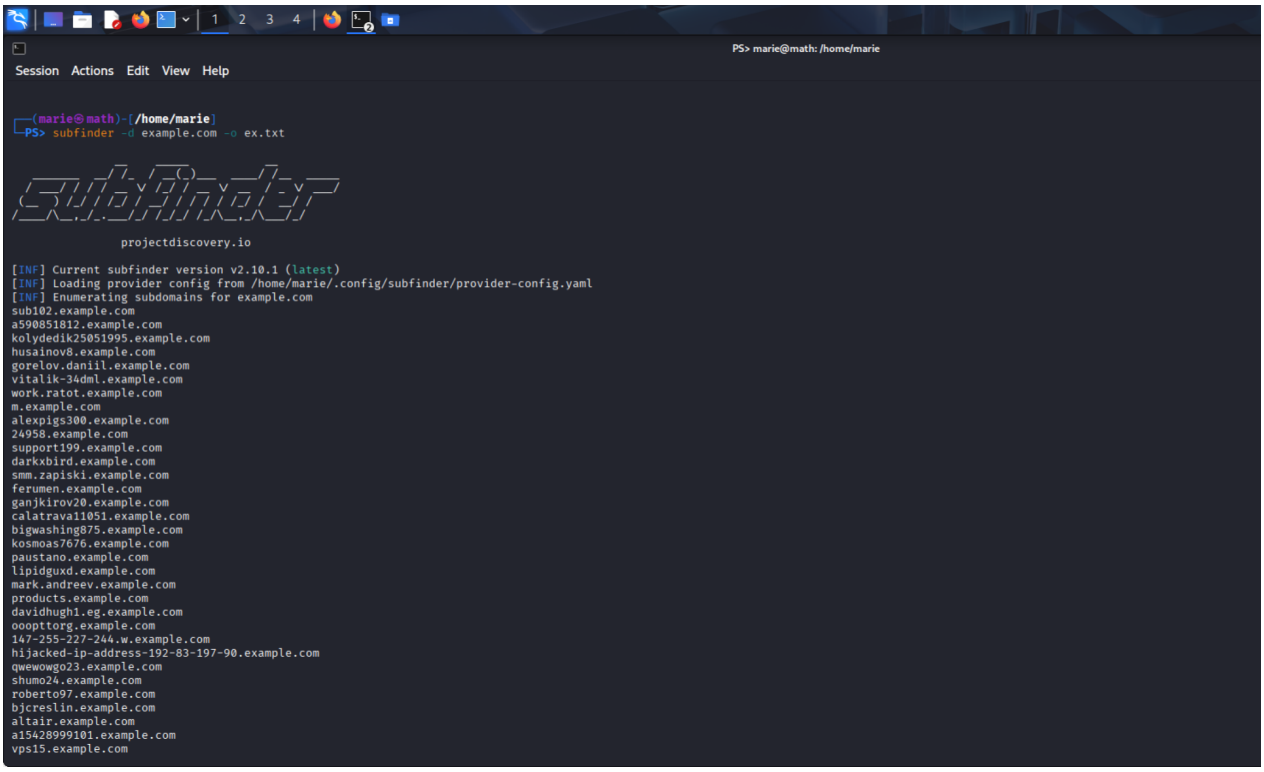





## Step 2: Subdomain Enumeration

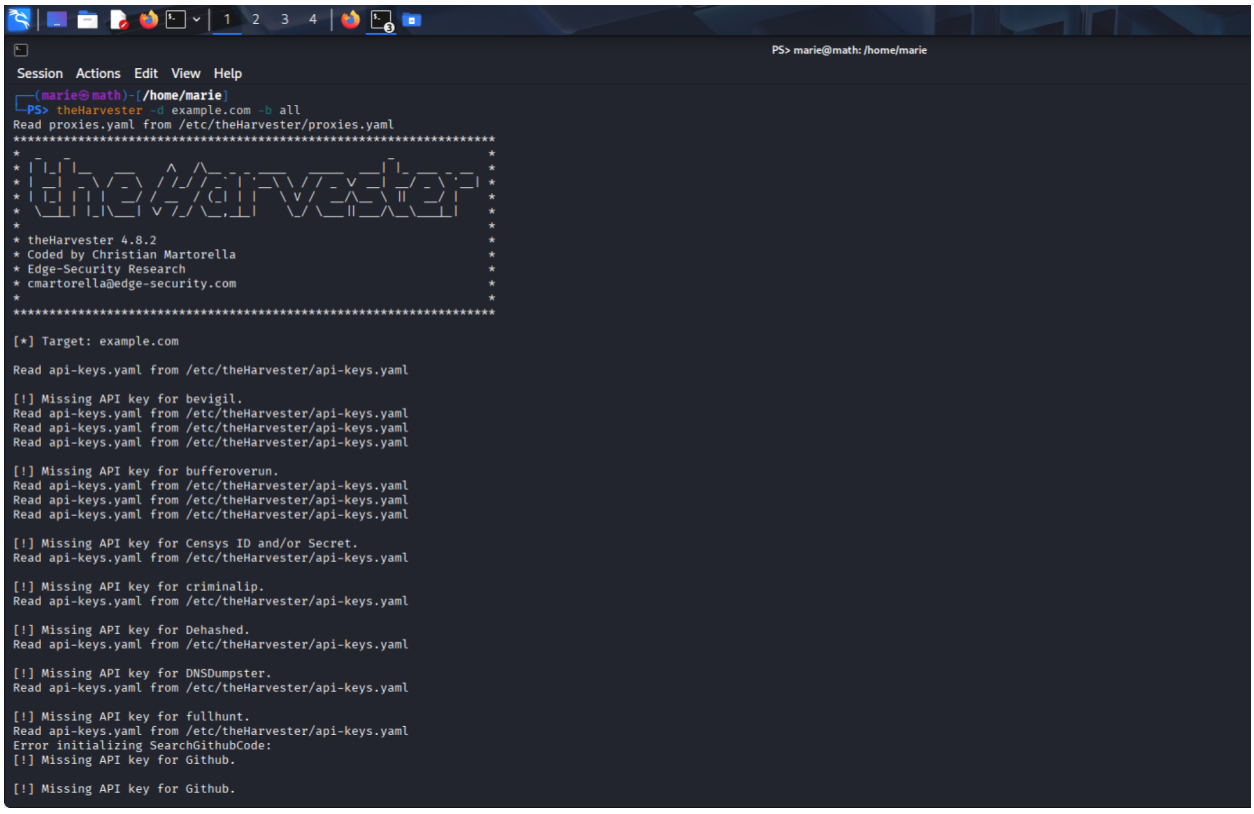
Performed passive subdomain discovery using tools like:

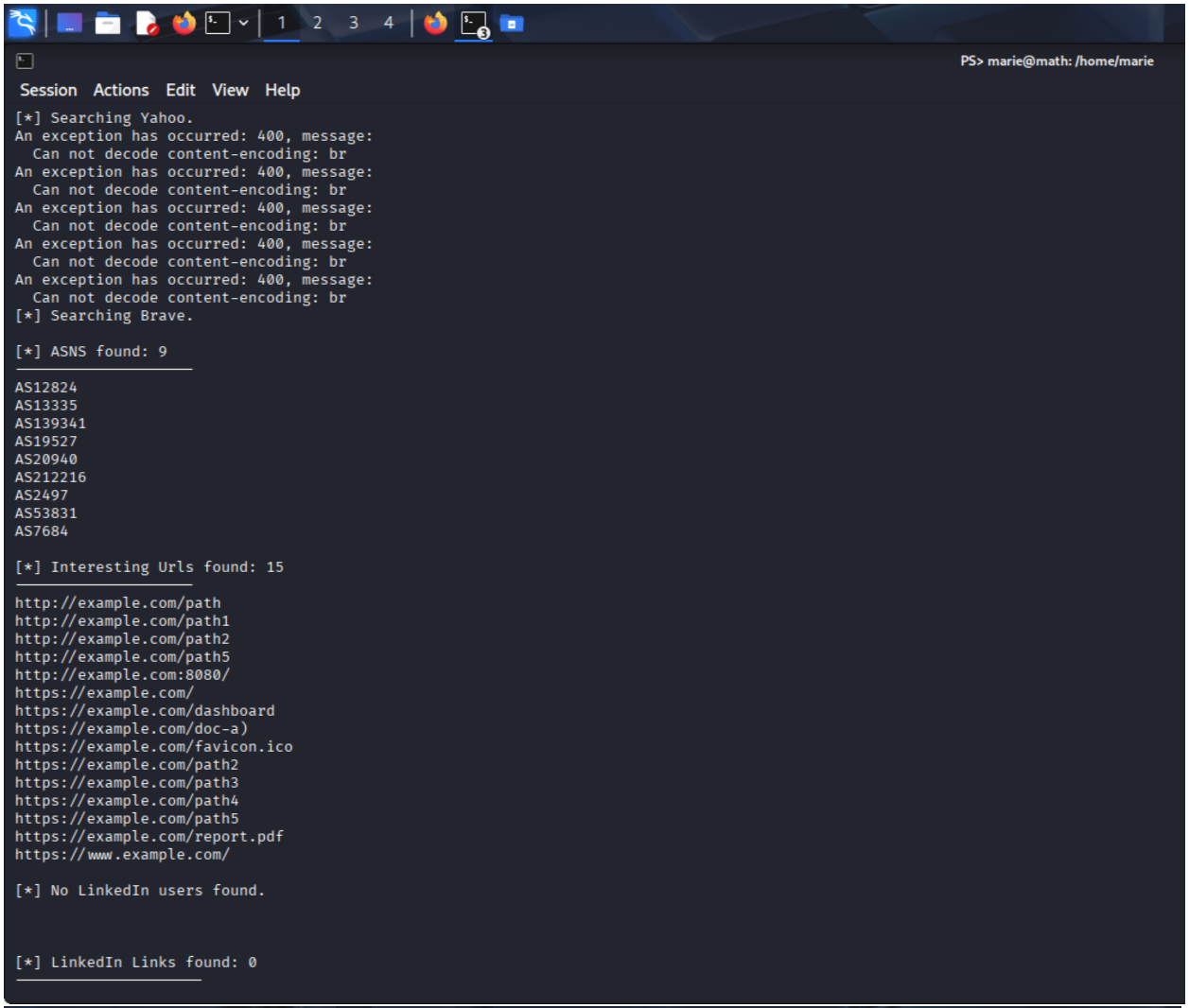
- subfinder
- Assetfinder
- Amass (in passive mode)

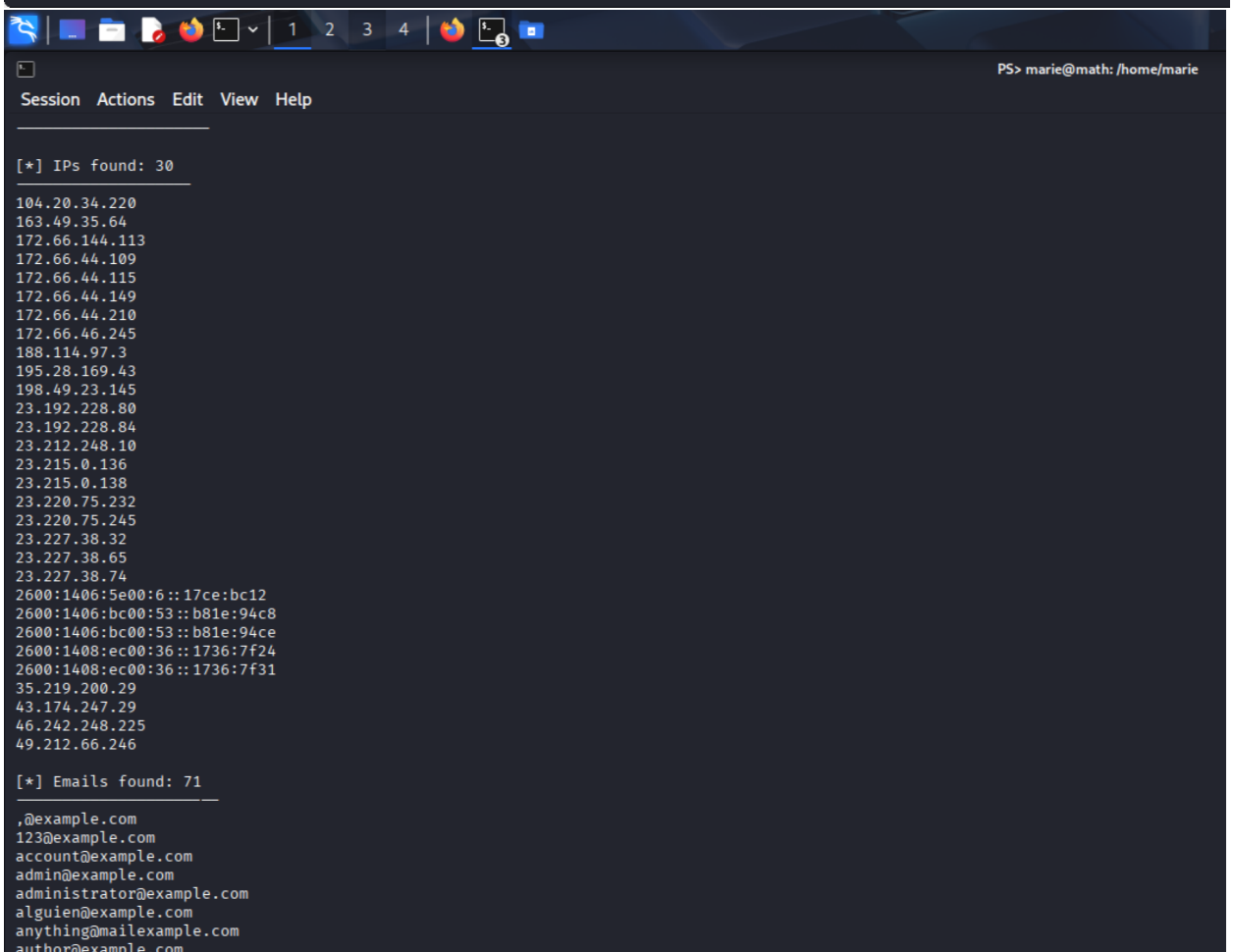


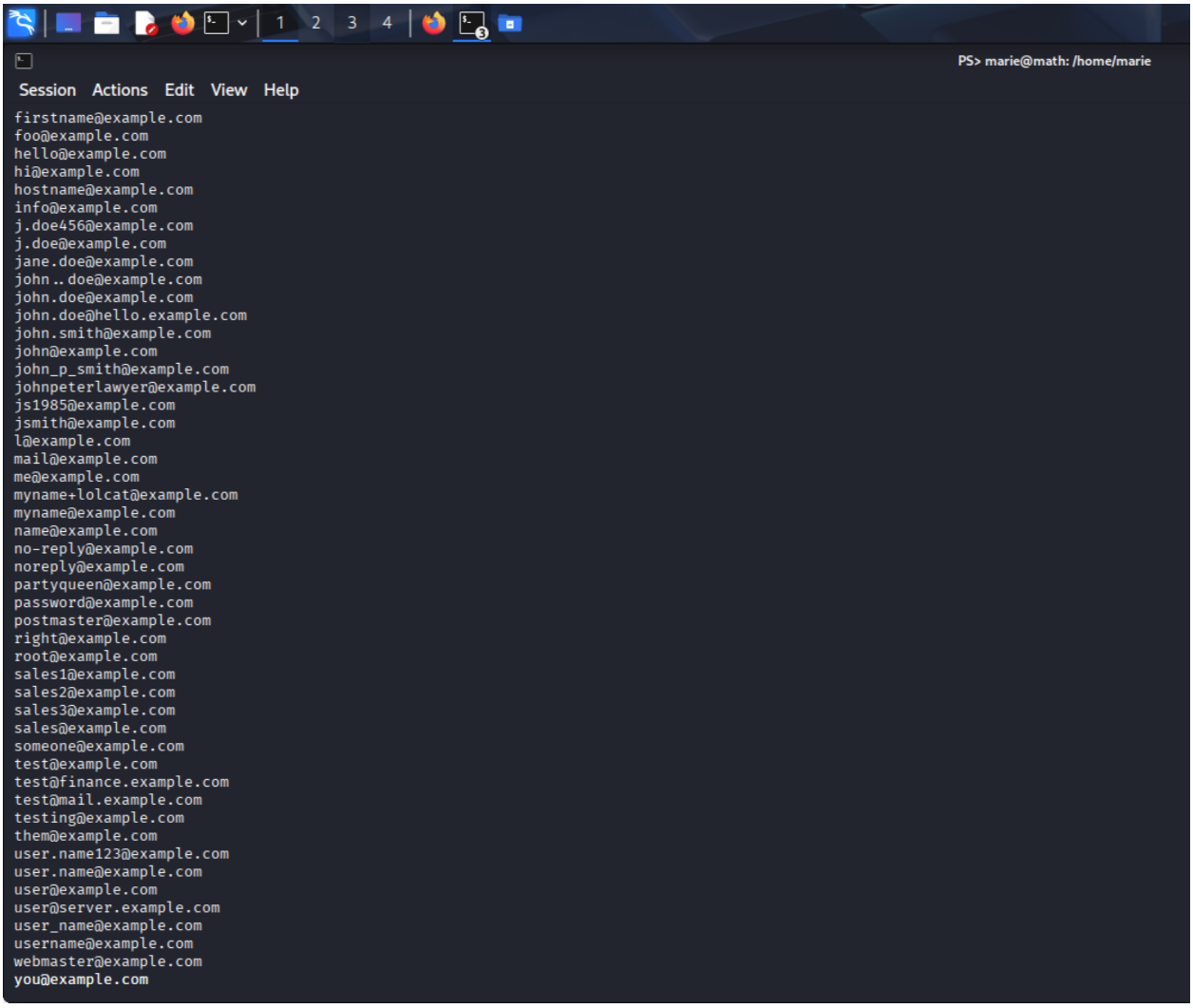

## Step 3: Email & Employee Information

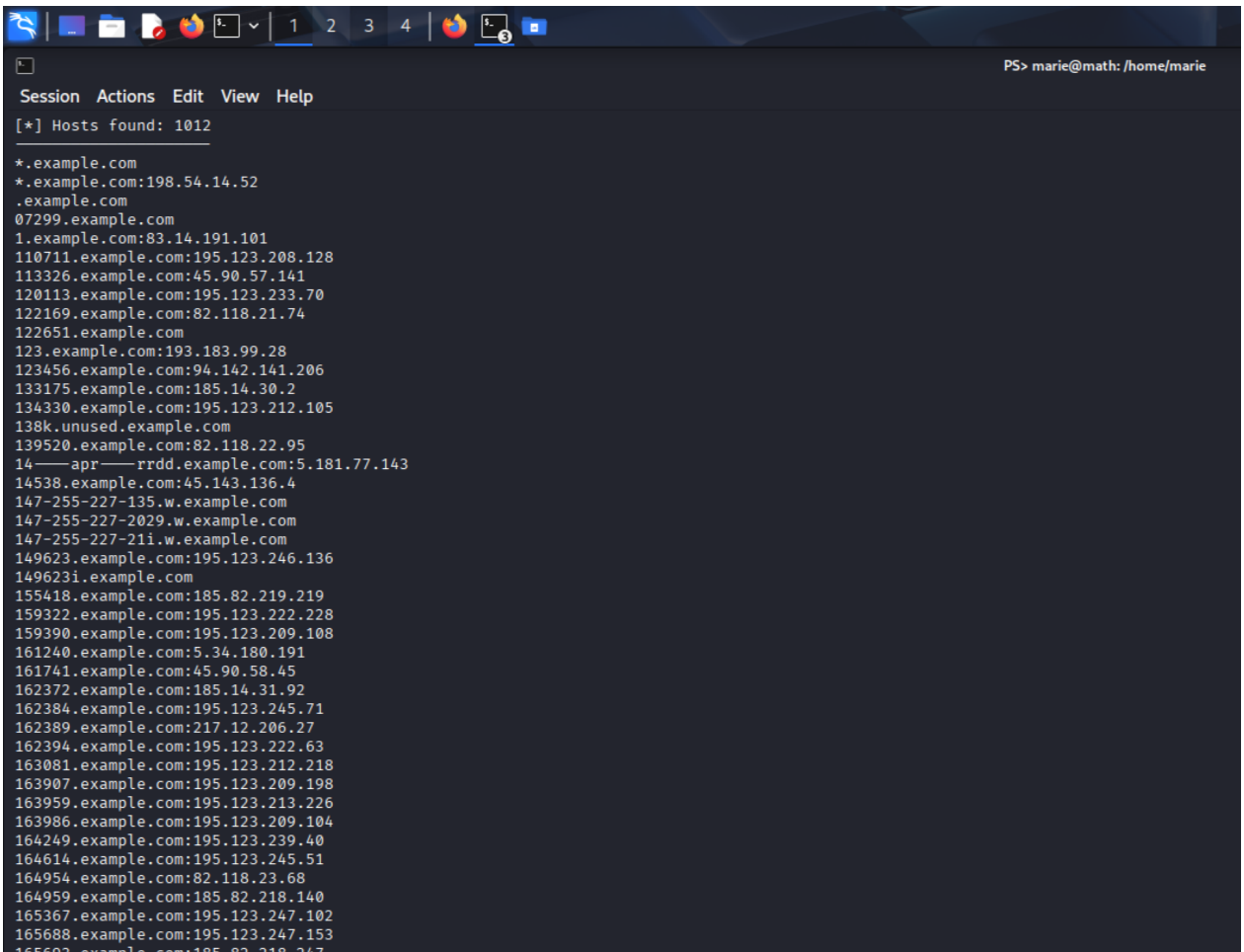
Used theHarvester to gather emails, names, and hosts from public sources (Google, Bing, LinkedIn, etc.).




1 2 3 4
PS> marie@math: /home/marie
Session Actions Edit View Help
[*] Searching Yahoo.
An exception has occurred: 400, message:
Can not decode content-encoding: br
An exception has occurred: 400, message:
Can not decode content-encoding: br
An exception has occurred: 400, message:
Can not decode content-encoding: br
An exception has occurred: 400, message:
Can not decode content-encoding: br
An exception has occurred: 400, message:
Can not decode content-encoding: br
[*] Searching Brave.
[*] ASNS found: 9
AS12824
AS13335
AS139341
AS19527
AS20940
AS212216
AS2497
AS53831
AS7684
[*] Interesting Urls found: 15
http://example.com/path
http://example.com/path1
http://example.com/path2
http://example.com/path5
http://example.com:8080/
https://example.com/
https://example.com/dashboard
https://example.com/doc-a)
https://example.com/favicon.ico
https://example.com/path2
https://example.com/path3
https://example.com/path4
https://example.com/path5
https://example.com/report.pdf
https://www.example.com/
[*] No LinkedIn users found.
[*] LinkedIn Links found: 0


1 2 3 4
PS> marie@math: /home/marie
Session Actions Edit View Help
[*] IPs found: 30
104.20.34.220
163.49.35.64
172.66.144.113
172.66.44.109
172.66.44.115
172.66.44.149
172.66.44.210
172.66.46.245
188.114.97.3
195.28.169.43
198.49.23.145
23.192.228.80
23.192.228.84
23.212.248.10
23.215.0.136
23.215.0.138
23.220.75.232
23.220.75.245
23.227.38.32
23.227.38.65
23.227.38.74
2600:1406:5e00:6::17ce:bc12
2600:1406:bc00:53::b81e:94c8
2600:1406:bc00:53::b81e:94ce
2600:1408:ec00:36::1736:7f24
2600:1408:ec00:36::1736:7f31
35.219.200.29
43.174.247.29
46.242.248.225
49.212.66.246
[*] Emails found: 71
,@example.com
123@example.com
account@example.com
admin@example.com
administrator@example.com
alguien@example.com
anything@mailexample.com
author@example.com


1 2 3 4
PS> marie@math: /home/marie
Session Actions Edit View Help
firstname@example.com
foo@example.com
hello@example.com
hi@example.com
hostname@example.com
info@example.com
j.doe456@example.com
j.doe@example.com
jane.doe@example.com
john..doe@example.com
john.doe@example.com
john.doe@hello.example.com
john.smith@example.com
john@example.com
john_p_smith@example.com
johnpeterlawyer@example.com
js1985@example.com
jsmith@example.com
l@example.com
mail@example.com
me@example.com
myname+lolcat@example.com
myname@example.com
name@example.com
no-reply@example.com
noreply@example.com
partyqueen@example.com
password@example.com
postmaster@example.com
right@example.com
root@example.com
sales1@example.com
sales2@example.com
sales3@example.com
sales@example.com
someone@example.com
test@example.com
test@finance.example.com
test@mail.example.com
testing@example.com
them@example.com
user.name123@example.com
user.name@example.com
user@example.com
user@server.example.com
user_name@example.com
username@example.com
webmaster@example.com
you@example.com


1 2 3 4
PS> marie@math: /home/marie
Session Actions Edit View Help
[*] Hosts found: 1012
*.example.com
*.example.com:198.54.14.52
.example.com
07299.example.com
1.example.com:83.14.191.101
110711.example.com:195.123.208.128
113326.example.com:45.90.57.141
120113.example.com:195.123.233.70
122169.example.com:82.118.21.74
122651.example.com
123.example.com:193.183.99.28
123456.example.com:94.142.141.206
133175.example.com:185.14.30.2
134330.example.com:195.123.212.105
138k.unused.example.com
139520.example.com:82.118.22.95
14———apr———rrdd.example.com:5.181.77.143
14538.example.com:45.143.136.4
147-255-227-135.w.example.com
147-255-227-2029.w.example.com
147-255-227-21i.w.example.com
149623.example.com:195.123.246.136
149623i.example.com
155418.example.com:185.82.219.219
159322.example.com:195.123.222.228
159390.example.com:195.123.209.108
161240.example.com:5.34.180.191
161741.example.com:45.90.58.45
162372.example.com:185.14.31.92
162384.example.com:195.123.245.71
162389.example.com:217.12.206.27
162394.example.com:195.123.222.63
163081.example.com:195.123.212.218
163907.example.com:195.123.209.198
163959.example.com:195.123.213.226
163986.example.com:195.123.209.104
164249.example.com:195.123.239.40
164614.example.com:195.123.245.51
164954.example.com:82.118.23.68
164959.example.com:185.82.218.140
165367.example.com:195.123.247.102
165688.example.com:195.123.247.153

## Step 4: Metadata Extraction

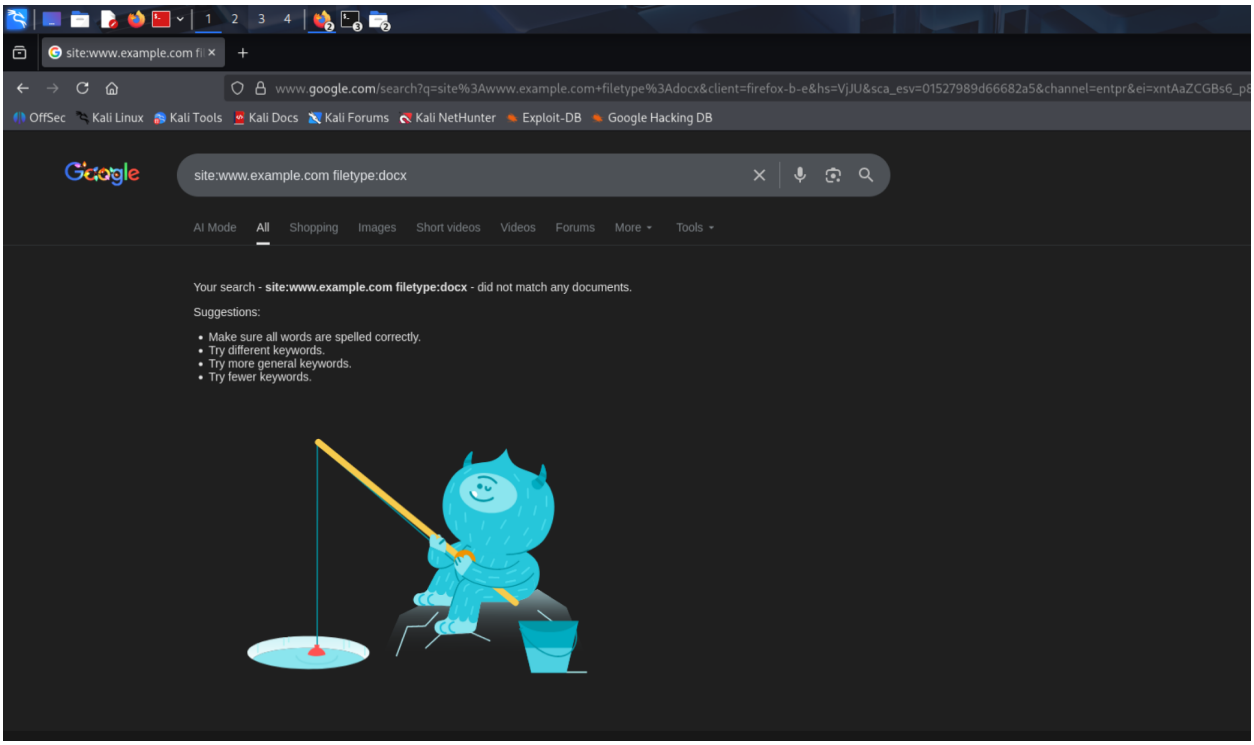
Tried to Download publicly available documents (PDF, DOCX, PPTX) and analyze metadata. Tool: exiftool, strings, metagoofil.

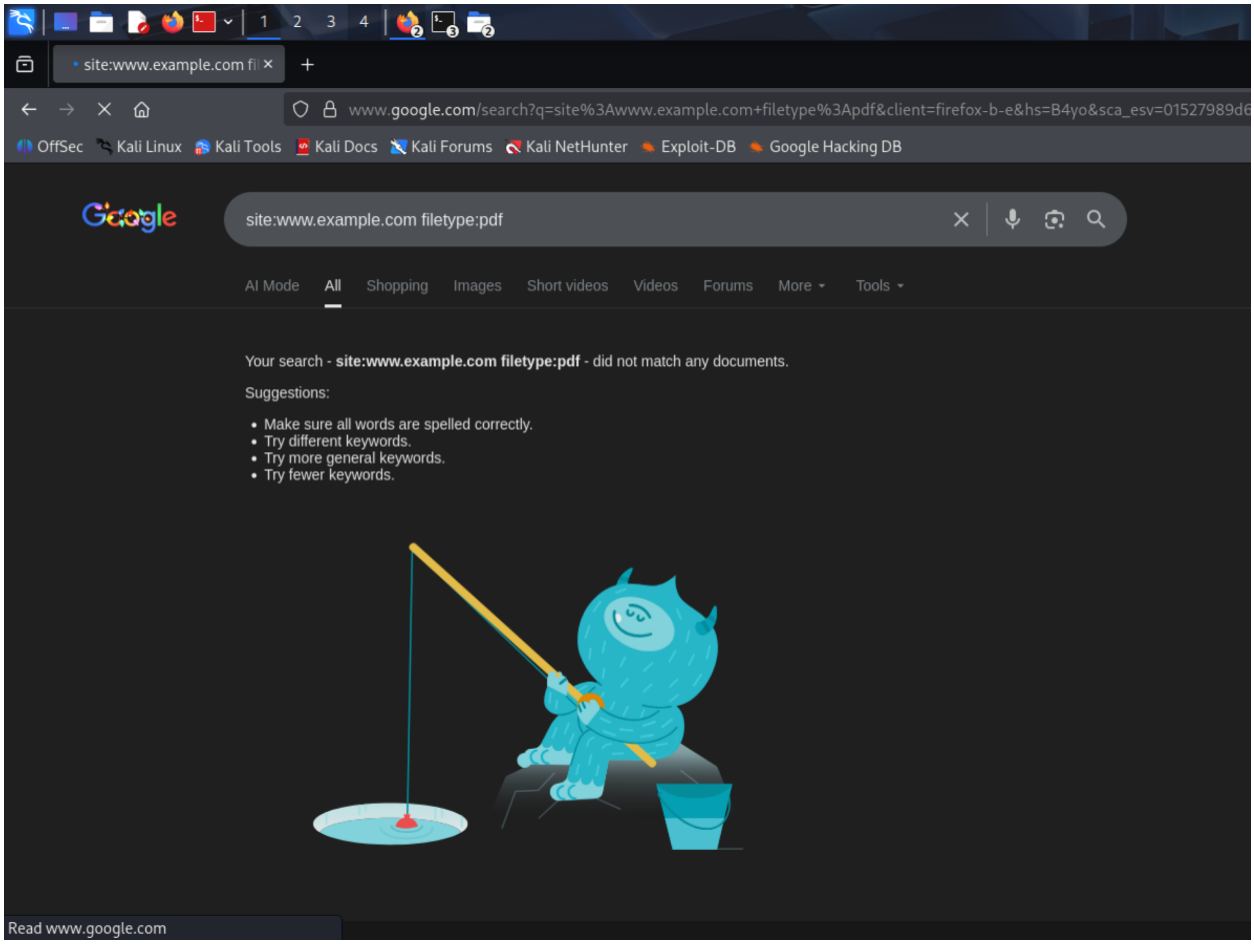
```
┌──(marie㉿math)-[/home/marie]
└─PS> metagoofil -d www.example.com -t pdf,docx,pptx -o exdocs.pdf
[*] Searching for 100 .pdf files and waiting 30.0 seconds between searches
[*] Results: 0 .pdf files found
[*] Searching for 100 .docx files and waiting 30.0 seconds between searches
[*] Results: 0 .docx files found
[*] Searching for 100 .pptx files and waiting 30.0 seconds between searches
[*] Results: 0 .pptx files found
[+] Done!

┌──(marie㉿math)-[/home/marie]
└─PS>
```

## Step 5: Google Dorking

Used Google search queries to find sensitive information.Example:

- site:example.com filetype:pdf
- site:example.com intitle:index of

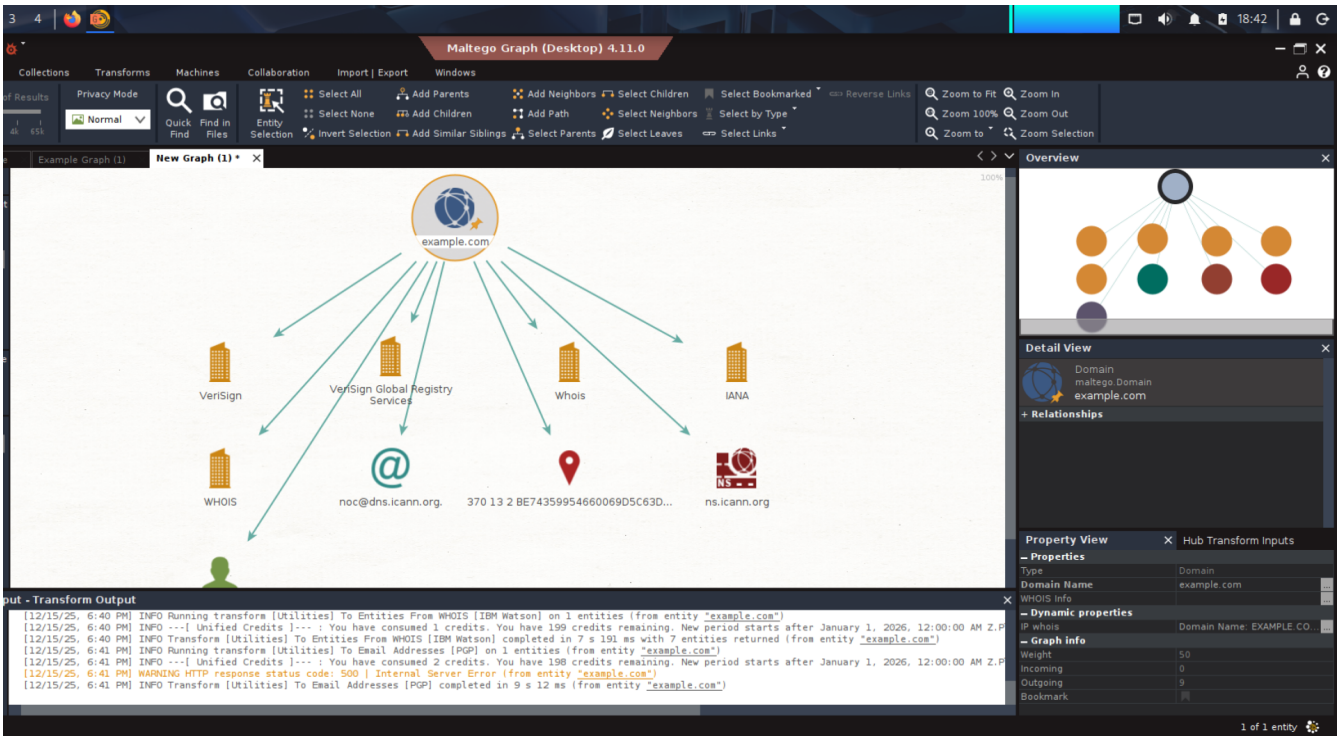


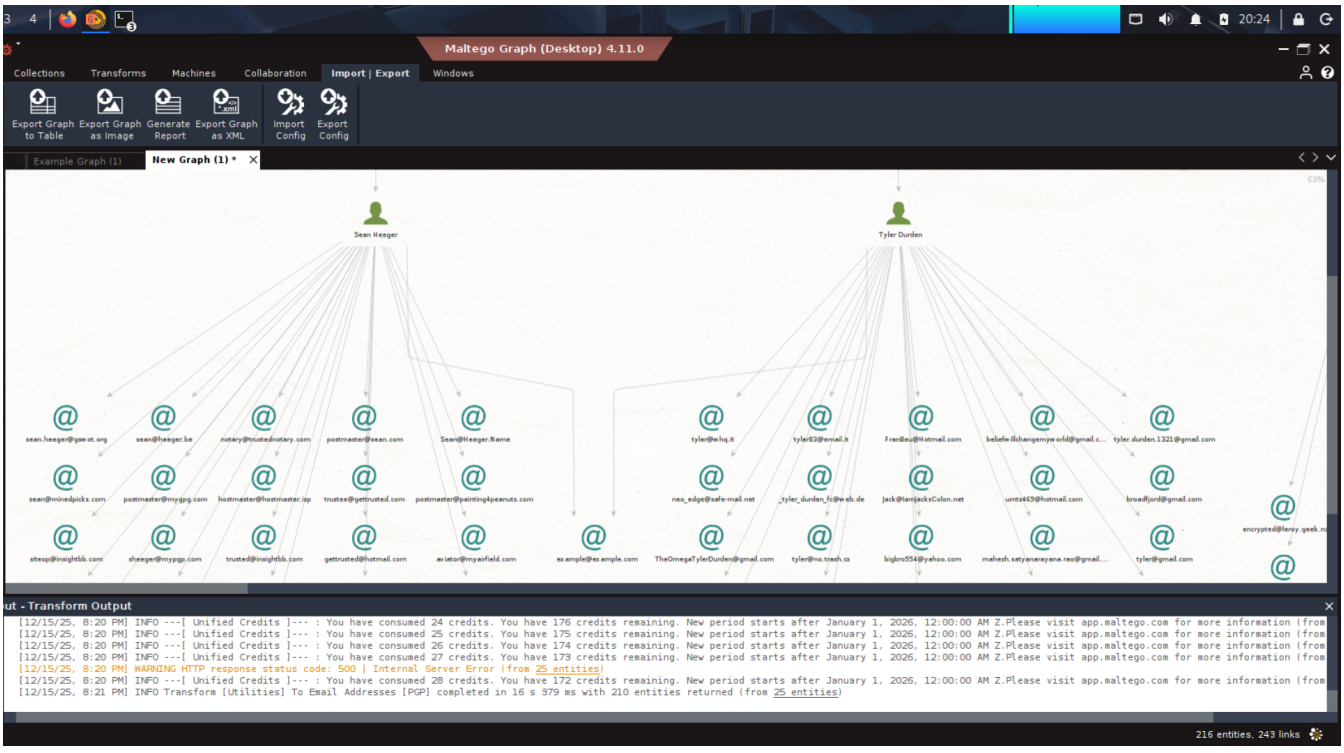

site:www.example.com fi
www.google.com/search?q=site%3Awww.example.com+filetype%3Apdf&client=firefox-b-e&hs=B4yo&sca_esv=01527989d6
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Google
site:www.example.com filetype:pdf
AI Mode
All
Shopping
Images
Short videos
Videos
Forums
More
Tools
Your search - site:www.example.com filetype:pdf - did not match any documents.
Suggestions:
Make sure all words are spelled correctly.
Try different keywords.
Try more general keywords.
Try fewer keywords.
Read www.google.com

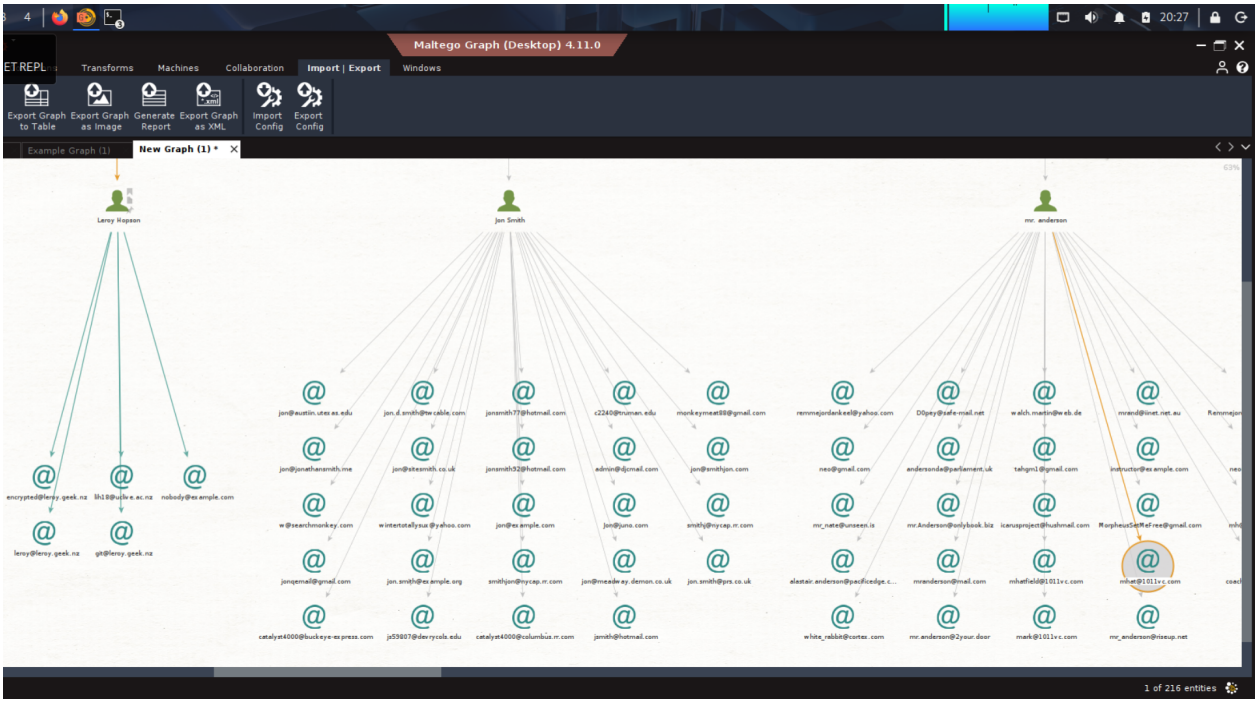
## Step 6: Social Media & Open Source Intelligence (OSINT)

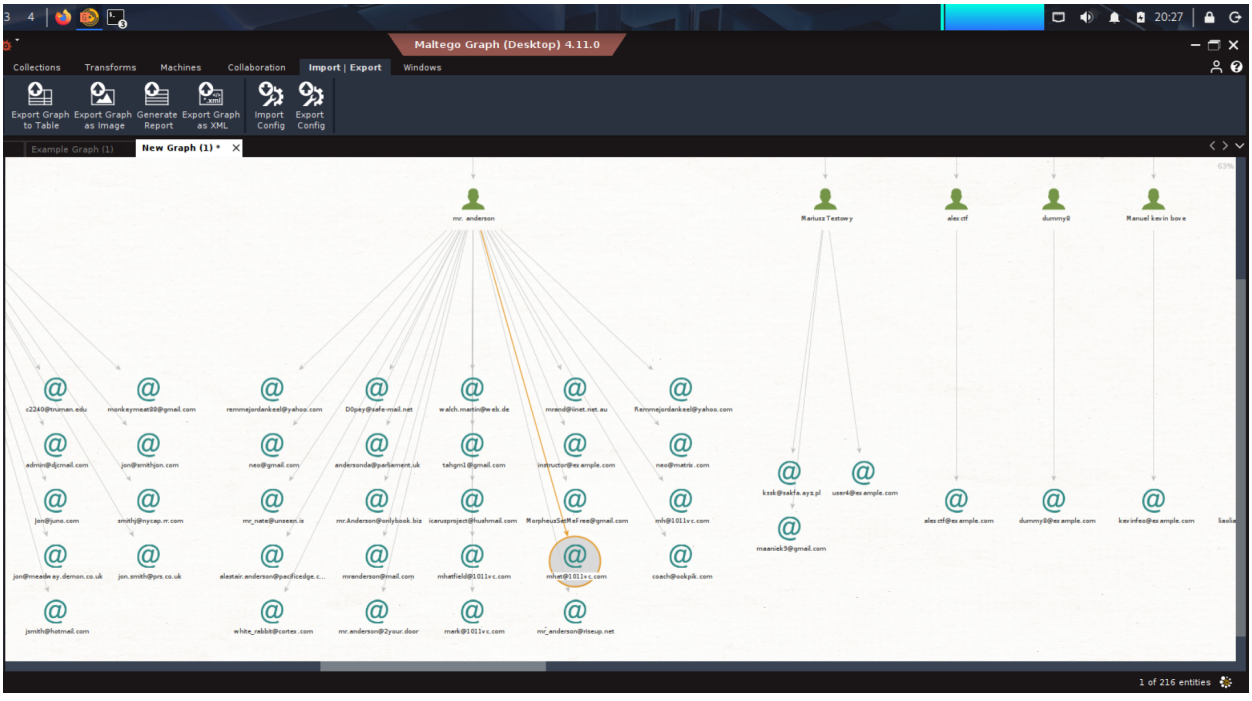
Identified target presence on LinkedIn, Twitter, GitHub, etc.

**Tools: Maltego, SpiderFoot.**



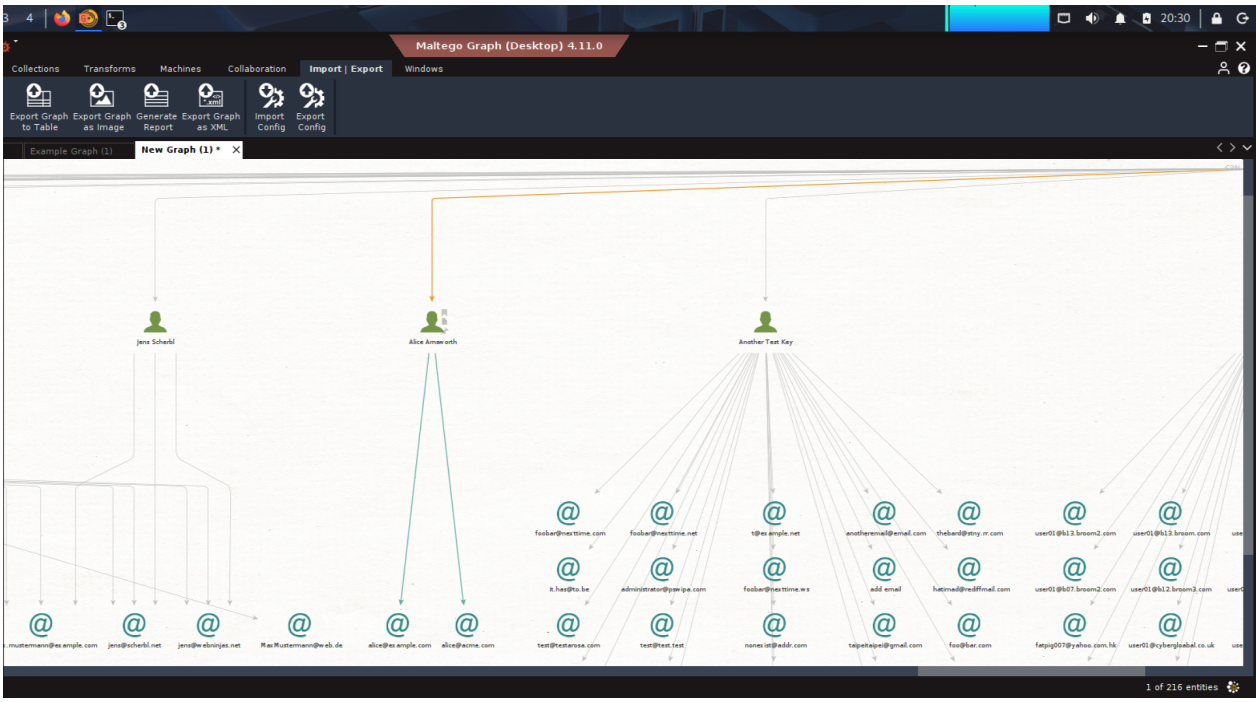



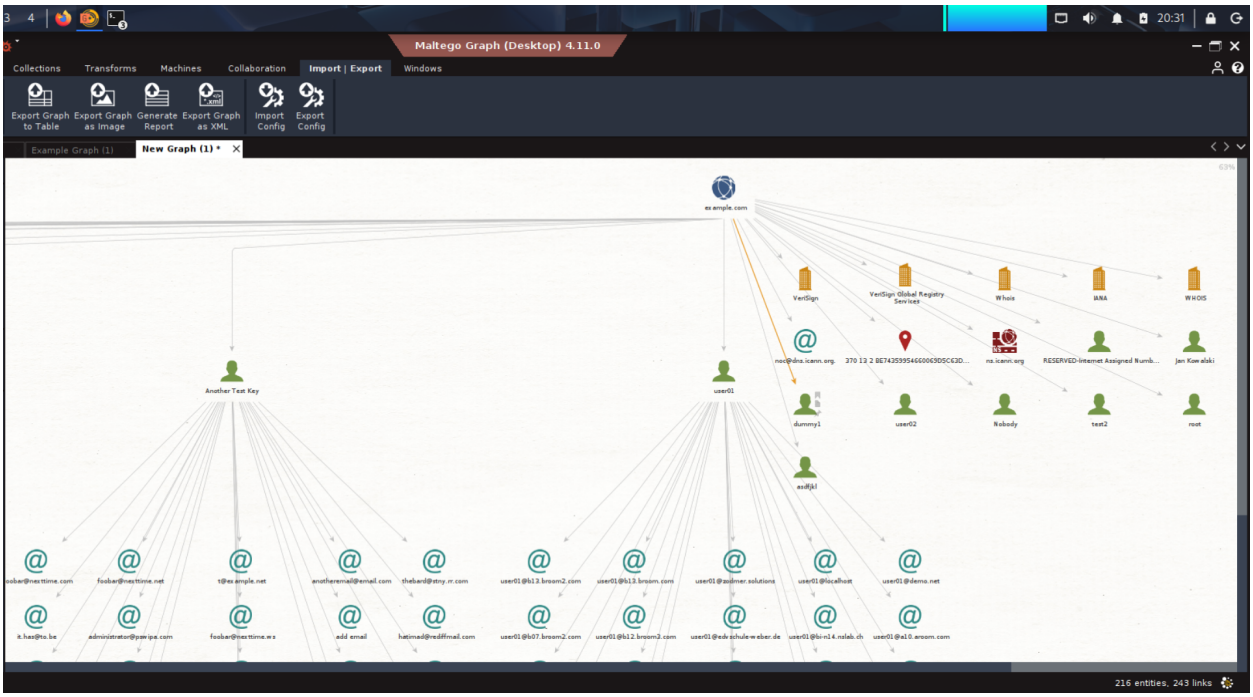

Maltego Graph (Desktop) 4.11.0
Transforms
Machines
Collaboration
Import | Export
Windows
Export Graph to Table
Export Graph as Image
Generate Report
Export Graph as XML
Import Config
Export Config
Example Graph (1)
New Graph (1) *
Leroy Hopson
Jon Smith
mr. anderson
1 of 216 entities


Maltego Graph (Desktop) 4.11.0
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Export Graph to Table
Export Graph as Image
Generate Report
Export Graph as XML
Import Config
Export Config
Example Graph (1)
New Graph (1) *
mr. anderson
Mariusz Testowy
alex ctf
dummy8
Manuel kevin bove
1 of 216 entities


Maltego Graph (Desktop) 4.11.0
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Export Graph to Table
Export Graph as Image
Generate Report
Export Graph as XML
Import Config
Export Config
Example Graph (1)
New Graph (1) *
1 of 216 entities

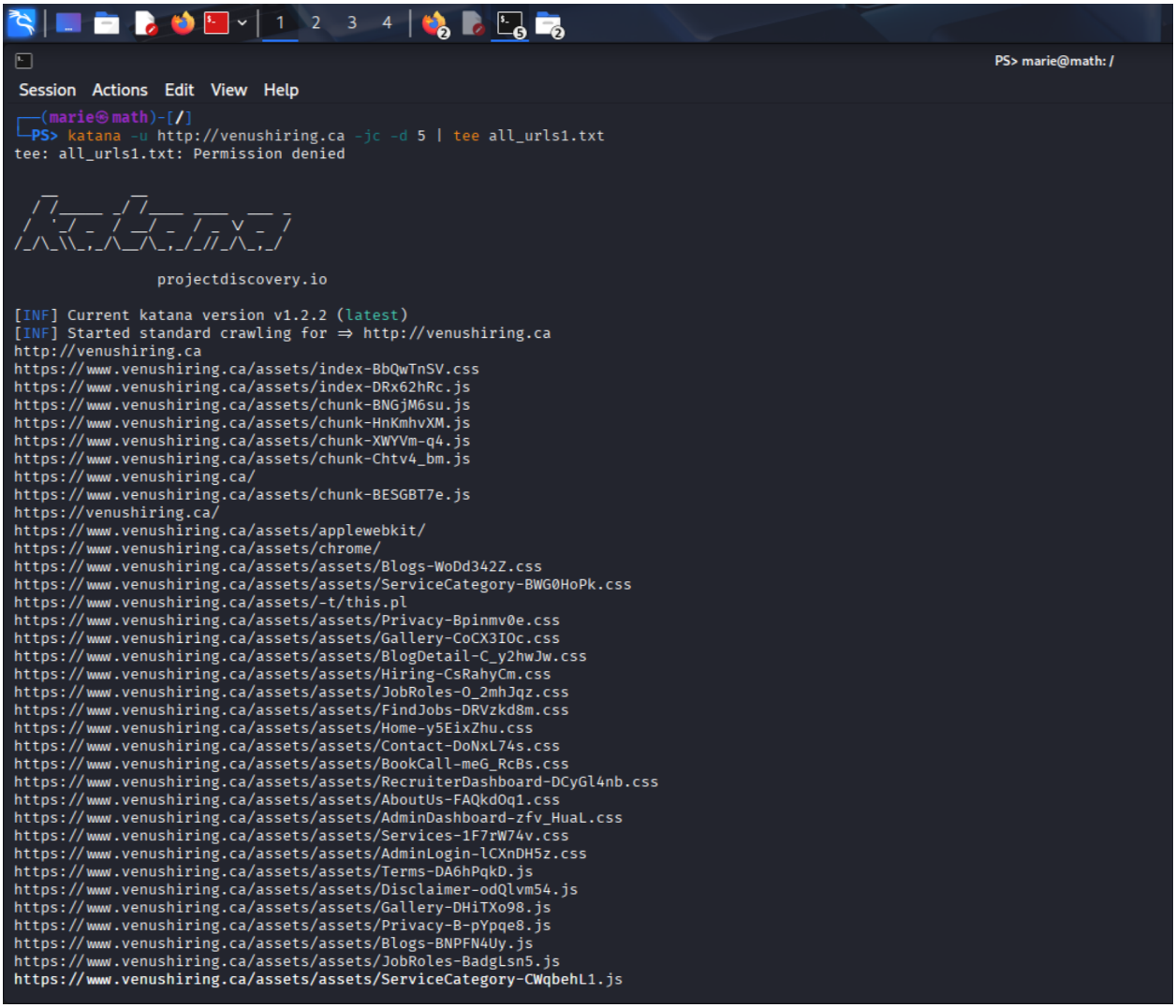

Maltego Graph (Desktop) 4.11.0
Transforms
Machines
Collaboration
Import | Export
Windows
Export Graph to Table
Export Graph as Image
Generate Report
Export Graph as XML
Import Config
Export Config
Example Graph (1)
New Graph (1) *
Max Mustermann
Max Mustermann
1 of 216 entities

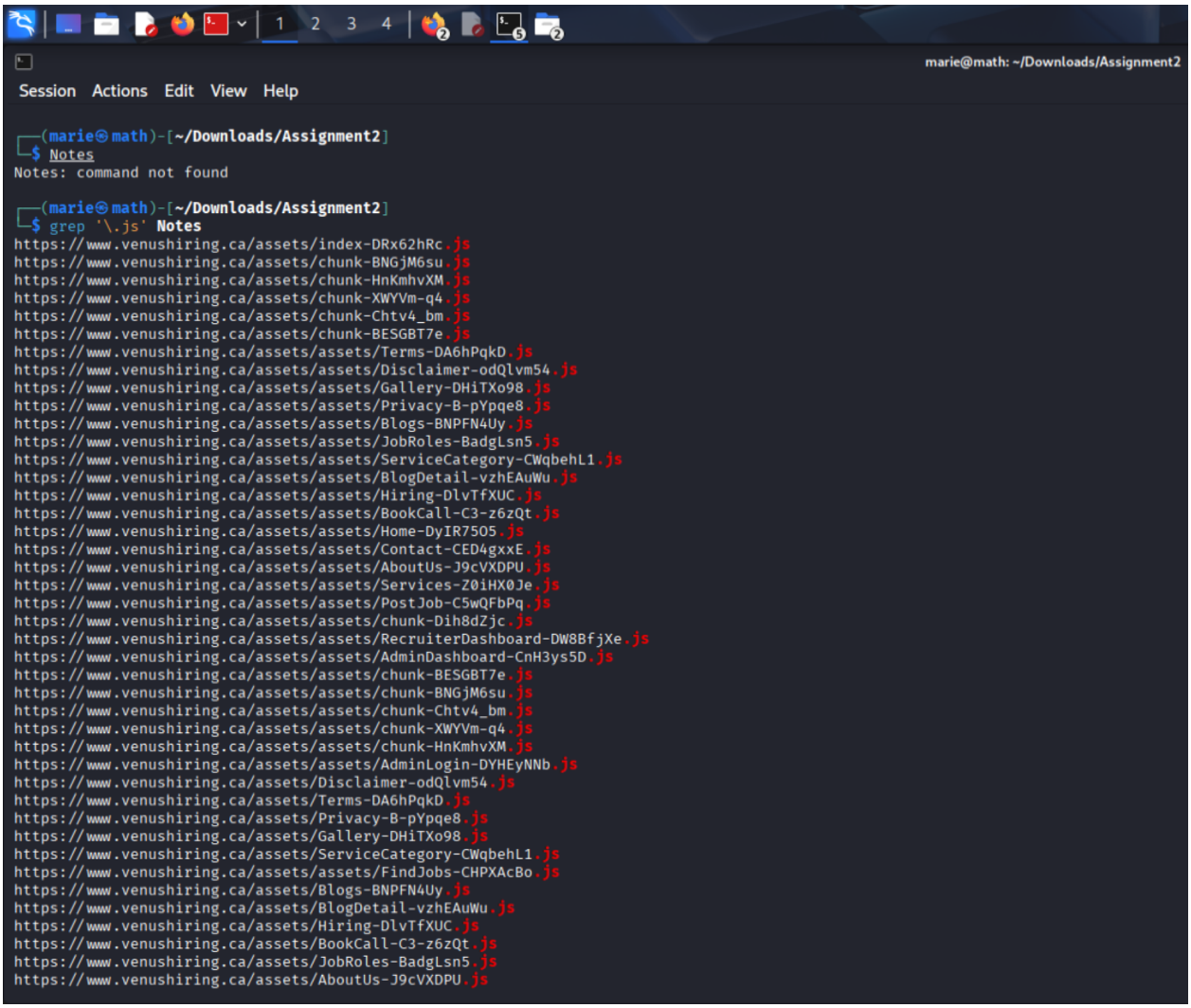

Maltego Graph (Desktop) 4.11.0
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Export Graph to Table
Export Graph as Image
Generate Report
Export Graph as XML
Import Config
Export Config
Example Graph (1)
New Graph (1) *
Jens Scherbl
Alice Amaworth
Another Test Key
1 of 216 entities


Maltego Graph (Desktop) 4.11.0
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Export Graph to Table
Export Graph as Image
Generate Report
Export Graph as XML
Import Config
Export Config
Example Graph (1)
New Graph (1) *
es.ample.com
Another Test Key
user01
VeriSign
Whois
IANA
WHOIS
dummy1
user02
Nobody
test2
root
asdfjkl
216 entities, 243 links

## Step 7 : Collected all the urls of the target & filter JS files

**Tools used for collecting urls**:Katana,GAU,Waybackurls




1 2 3 4
marie@math: ~/Downloads/Assignment2
Session Actions Edit View Help
┌──(marie㉿math)-[~/Downloads/Assignment2]
└─$ Notes
Notes: command not found
┌──(marie㉿math)-[~/Downloads/Assignment2]
└─$ grep '\.js' Notes
https://www.venushiring.ca/assets/index-DRx62hRc.js
https://www.venushiring.ca/assets/chunk-BNGjM6su.js
https://www.venushiring.ca/assets/chunk-HnKmhvXM.js
https://www.venushiring.ca/assets/chunk-XWYVm-q4.js
https://www.venushiring.ca/assets/chunk-Chtv4_bm.js
https://www.venushiring.ca/assets/chunk-BESGBT7e.js
https://www.venushiring.ca/assets/assets/Terms-DA6hPqkD.js
https://www.venushiring.ca/assets/assets/Disclaimer-odQlvm54.js
https://www.venushiring.ca/assets/assets/Gallery-DHiTXo98.js
https://www.venushiring.ca/assets/assets/Privacy-B-pYpqe8.js
https://www.venushiring.ca/assets/assets/Blogs-BNPFN4Uy.js
https://www.venushiring.ca/assets/assets/JobRoles-BadgLsn5.js
https://www.venushiring.ca/assets/assets/ServiceCategory-CWqbehL1.js
https://www.venushiring.ca/assets/assets/BlogDetail-vzhEAuWu.js
https://www.venushiring.ca/assets/assets/Hiring-DlvTfXUC.js
https://www.venushiring.ca/assets/assets/BookCall-C3-z6zQt.js
https://www.venushiring.ca/assets/assets/Home-DyIR75O5.js
https://www.venushiring.ca/assets/assets/Contact-CED4gxxE.js
https://www.venushiring.ca/assets/assets/AboutUs-J9cVXDPU.js
https://www.venushiring.ca/assets/assets/Services-Z0iHX0Je.js
https://www.venushiring.ca/assets/assets/PostJob-C5wQFbPq.js
https://www.venushiring.ca/assets/assets/chunk-Dih8dZjc.js
https://www.venushiring.ca/assets/assets/RecruiterDashboard-DW8BfjXe.js
https://www.venushiring.ca/assets/assets/AdminDashboard-CnH3ys5D.js
https://www.venushiring.ca/assets/assets/chunk-BESGBT7e.js
https://www.venushiring.ca/assets/assets/chunk-BNGjM6su.js
https://www.venushiring.ca/assets/assets/chunk-Chtv4_bm.js
https://www.venushiring.ca/assets/assets/chunk-XWYVm-q4.js
https://www.venushiring.ca/assets/assets/chunk-HnKmhvXM.js
https://www.venushiring.ca/assets/assets/AdminLogin-DYHEyNNb.js
https://www.venushiring.ca/assets/Disclaimer-odQlvm54.js
https://www.venushiring.ca/assets/Terms-DA6hPqkD.js
https://www.venushiring.ca/assets/Privacy-B-pYpqe8.js
https://www.venushiring.ca/assets/Gallery-DHiTXo98.js
https://www.venushiring.ca/assets/ServiceCategory-CWqbehL1.js
https://www.venushiring.ca/assets/assets/FindJobs-CHPXAcBo.js
https://www.venushiring.ca/assets/Blogs-BNPFN4Uy.js
https://www.venushiring.ca/assets/BlogDetail-vzhEAuWu.js
https://www.venushiring.ca/assets/Hiring-DlvTfXUC.js
https://www.venushiring.ca/assets/BookCall-C3-z6zQt.js
https://www.venushiring.ca/assets/JobRoles-BadgLsn5.js
https://www.venushiring.ca/assets/AboutUs-J9cVXDPU.js