

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.

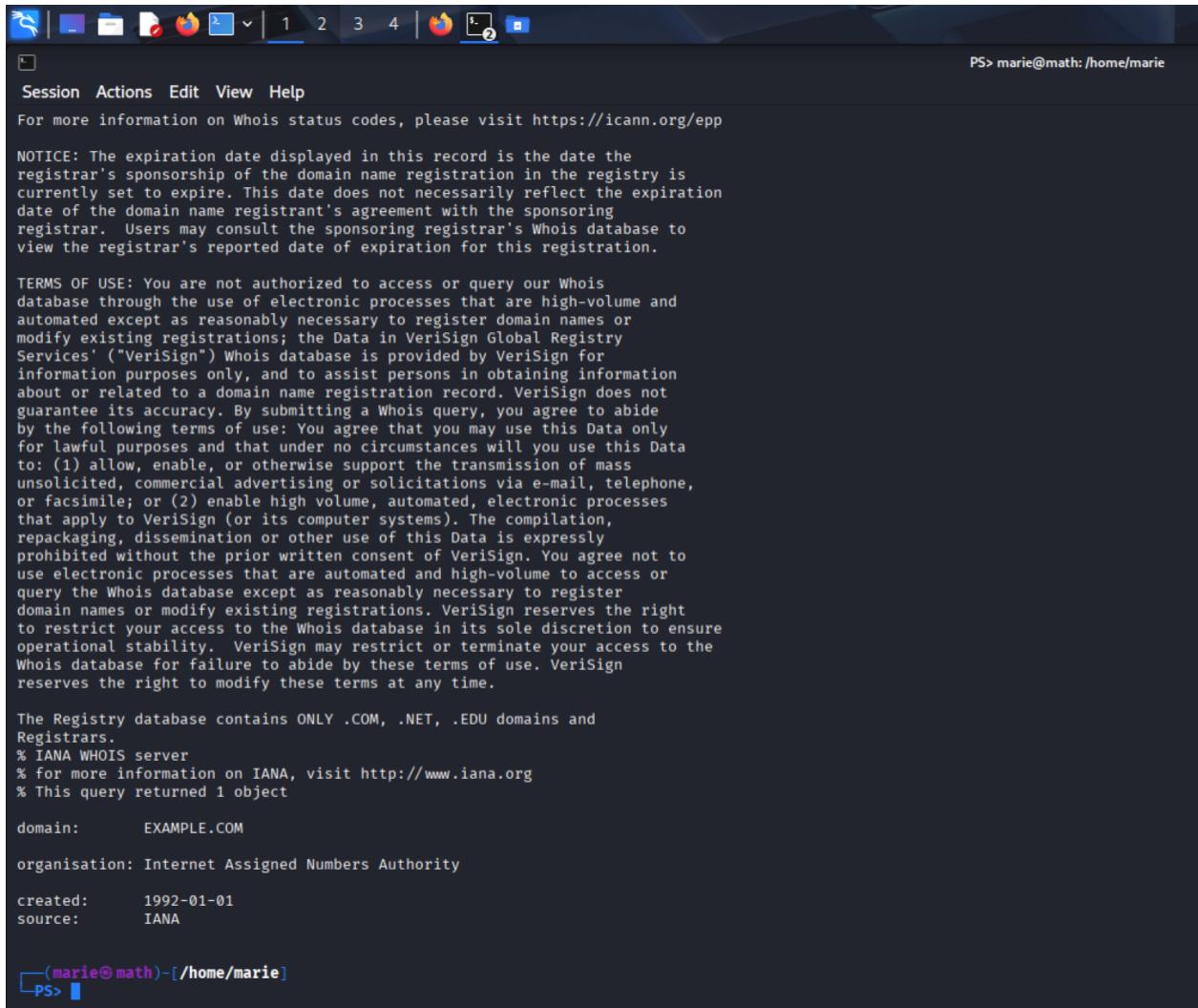
Tools: whois, dig, nslookup.

```
PS> whois example.com
Domain Name: EXAMPLE.COM
Registry Domain ID: 2336799_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.iana.org
Registrar URL: http://res-dom.iana.org
Updated Date: 2025-11-25T18:49:24Z
Creation Date: 1995-08-14T04:00:00Z
Registry Expiry Date: 2026-08-13T04:00:00Z
Registrar: RESERVED-Internet Assigned Numbers Authority
Registrar IANA ID: 376
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: A.IANA-SERVERS.NET
Name Server: B.IANA-SERVERS.NET
DNSSEC: signedDelegation
DNSSEC DS Data: 2371 13 2 C988EC423E3880EB8DD8A46FE06CA230EE23F35B578D64E78B29C3E1C83D245A
DNSSEC DS Data: 370 13 2 BE74359954660069D5C63D200C39F5603827D7D002856F120EE9F3A86764247C
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-12-15T17:38:07Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
```



The screenshot shows a terminal window with a dark background. At the top, there's a toolbar with icons for file operations like copy, paste, and save, followed by tabs labeled 1, 2, 3, 4, and a Firefox icon. The terminal window has a title bar with the text "Session Actions Edit View Help". In the top right corner, it says "PS> marie@math: /home/marie". The main content of the terminal is the WHOIS record for the domain "EXAMPLE.COM". It includes sections for "NOTICE", "TERMS OF USE", and detailed registration information from IANA. The output ends with a prompt "(marie@math)-[/home/marie]" and "PS>".

```
PS> marie@math: /home/marie
Session Actions Edit View Help
For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

domain:      EXAMPLE.COM
organisation: Internet Assigned Numbers Authority
created:     1992-01-01
source:      IANA

---(marie@math)-[/home/marie]
PS>
```

Step 2: Subdomain Enumeration

Performed passive subdomain discovery using tools like:

- subfinder
- Assetfinder
- Amass (in passive mode)

```
Session Actions Edit View Help

PS> subfinder -d example.com -o ex.txt

projectdiscovery.io

[INFO] Current subfinder version v2.10.1 (latest)
[INFO] Loading provider config from /home/marie/.config/subfinder/provider-config.yaml
[INFO] Enumerating subdomains for example.com
sub102.example.com
a590851812.example.com
kolyedik25051995.example.com
husainov8.example.com
gorelov.daniil.example.com
vitalik-34dml.example.com
work.ratot.example.com
m.example.com
alexpiigs300.example.com
24958.example.com
support199.example.com
darkxbird.example.com
smm.zapiski.example.com
ferumen.example.com
ganjikirov20.example.com
calatrava1051.example.com
bigwashingt875.example.com
kosmoas7676.example.com
paustano.example.com
lipidguxd.example.com
mark.andreev.example.com
products.example.com
davidhugh1.eg.example.com
ooopttorg.example.com
147-255-227-244.w.example.com
hijacked-ip-address-192-83-197-90.example.com
qweqwogo23.example.com
shlomo24.example.com
robert097.example.com
bjrcreslin.example.com
altair.example.com
a15428999101.example.com
vps15.example.com
```

Step 3: Email & Employee Information

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

```
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
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

[*] InterestingUrls 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
```

```
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@mail@example.com
author@example.com
```

```
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
```

```
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
147-255-227-211.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
165693.example.com:185.82.218.247
```

Step 4: Metadata Extraction

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

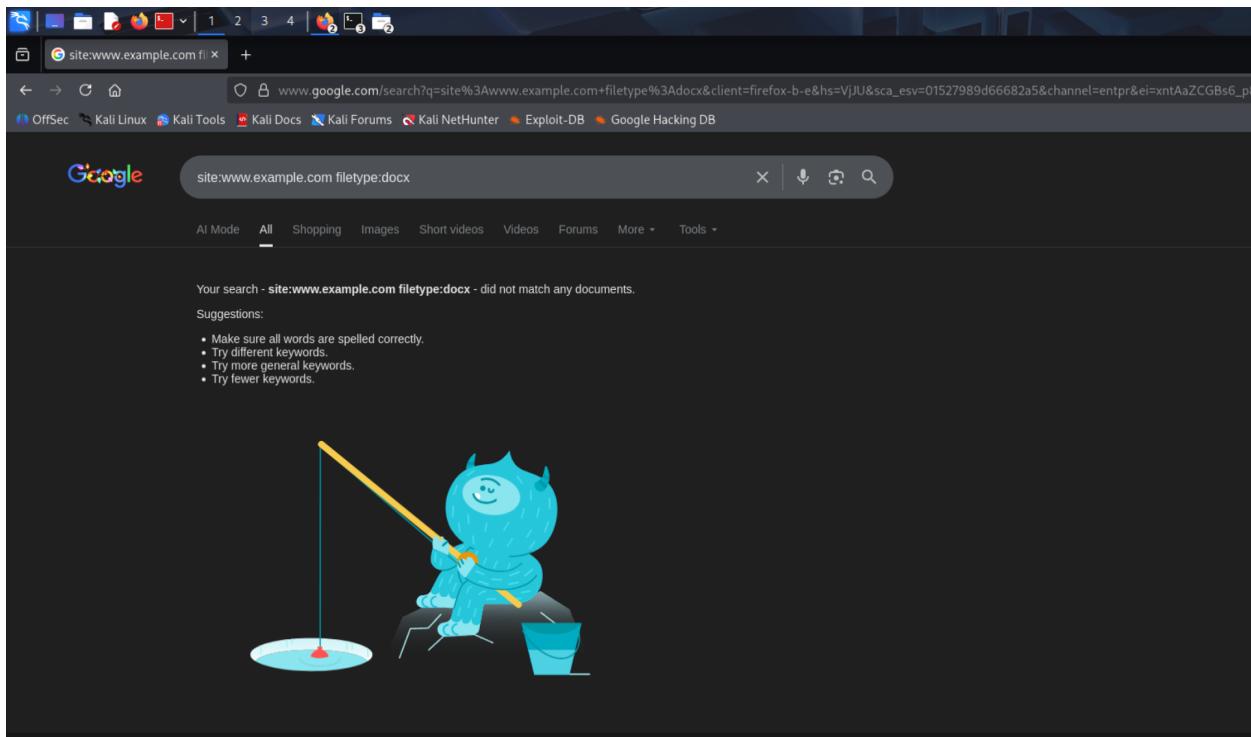
```
└──(marie㉿math)-[~/home/marie]
└─$ metagoofil -d www.example.com -t pdf,docx,pptx -o exdocs.pdf
[*] Searching for 100 .pdf files and waiting 30.0 seconds between searches
[*] Results: 0 .pdf files found
[*] Searching for 100 .docx files and waiting 30.0 seconds between searches
[*] Results: 0 .docx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

└──(marie㉿math)-[~/home/marie]
└─$
```

Step 5: Google Dorking

Used Google search queries to find sensitive information. Example:

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



A screenshot of a Firefox browser window on a Kali Linux desktop. The address bar shows a search for "site:www.example.com filetype:pdf". The results page from Google indicates no matches found, with suggestions to refine the search. A cartoon illustration of a blue monster fishing is displayed below the search results.

site:www.example.com filetype:pdf

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

All Mode All Shopping Images Short videos Videos Forums More Tools

Your search - site:www.example.com filetype:pdf - did not match any documents.

Suggestions:

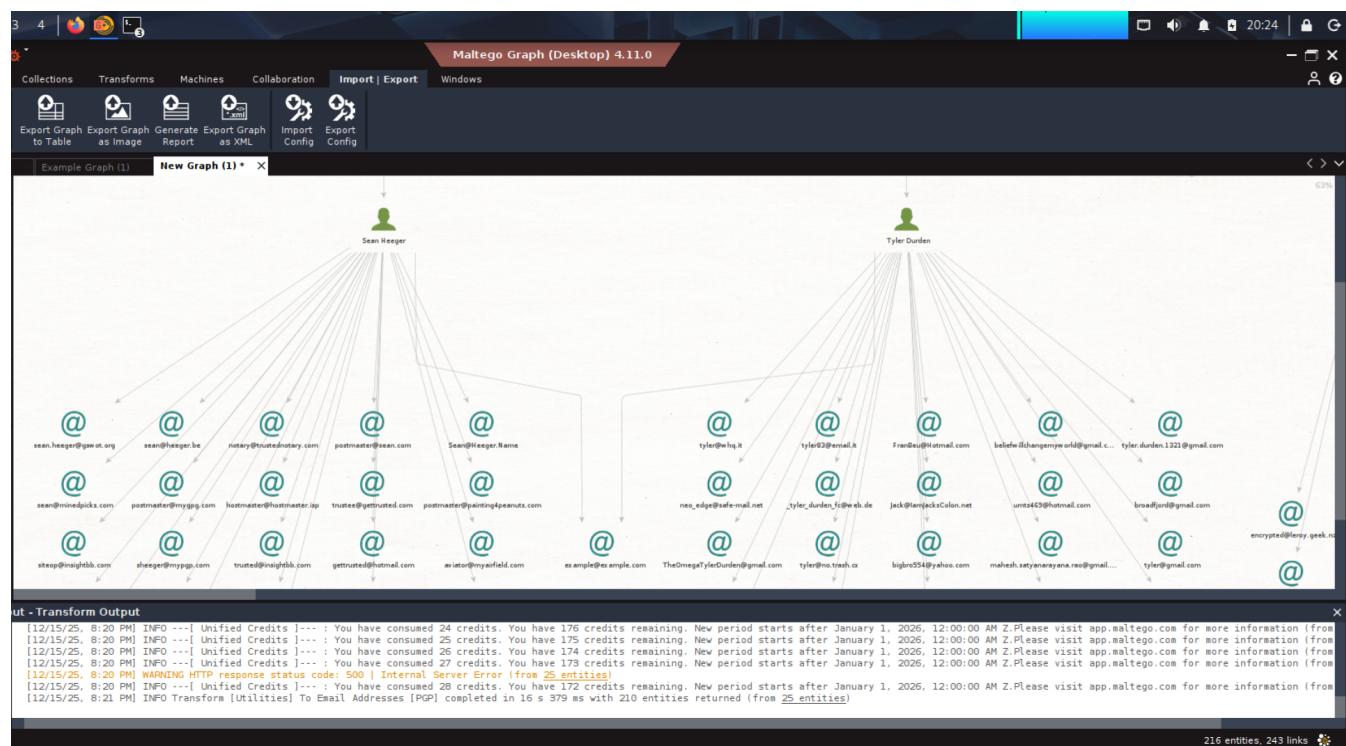
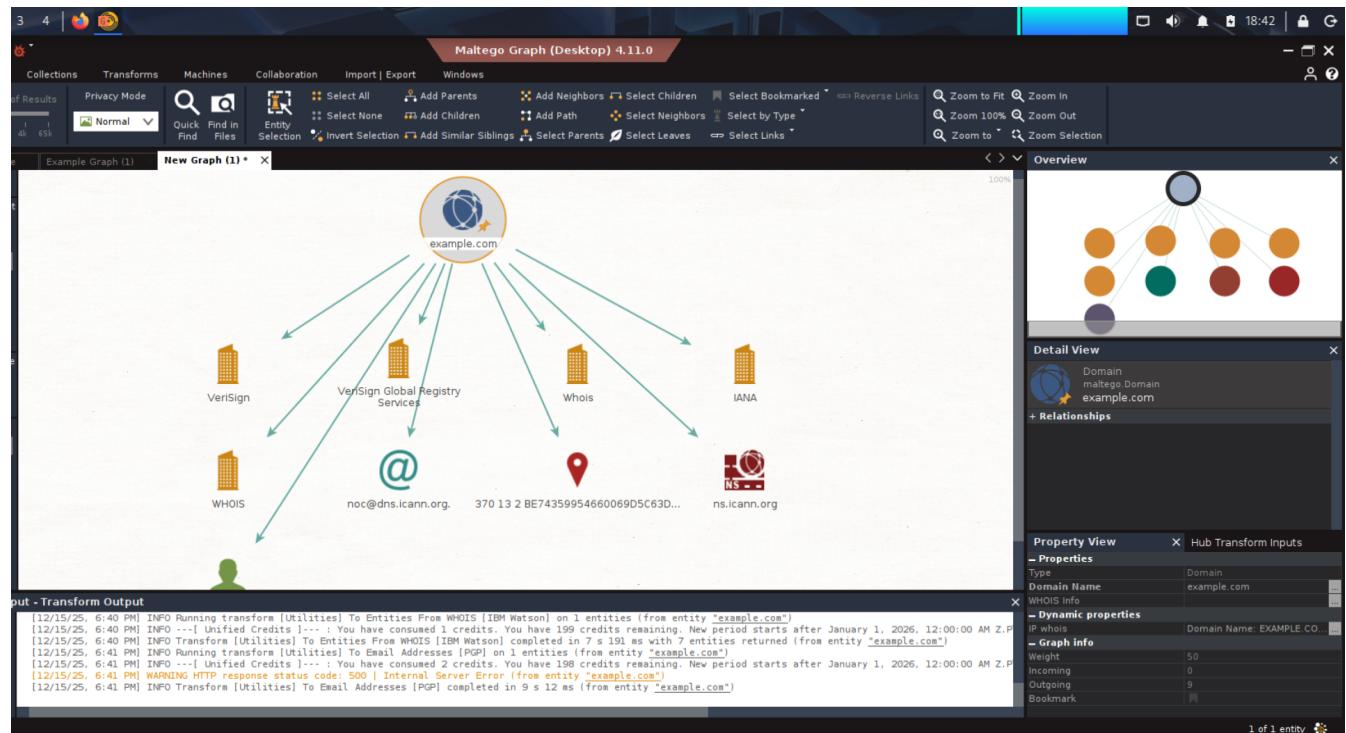
- Make sure all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.

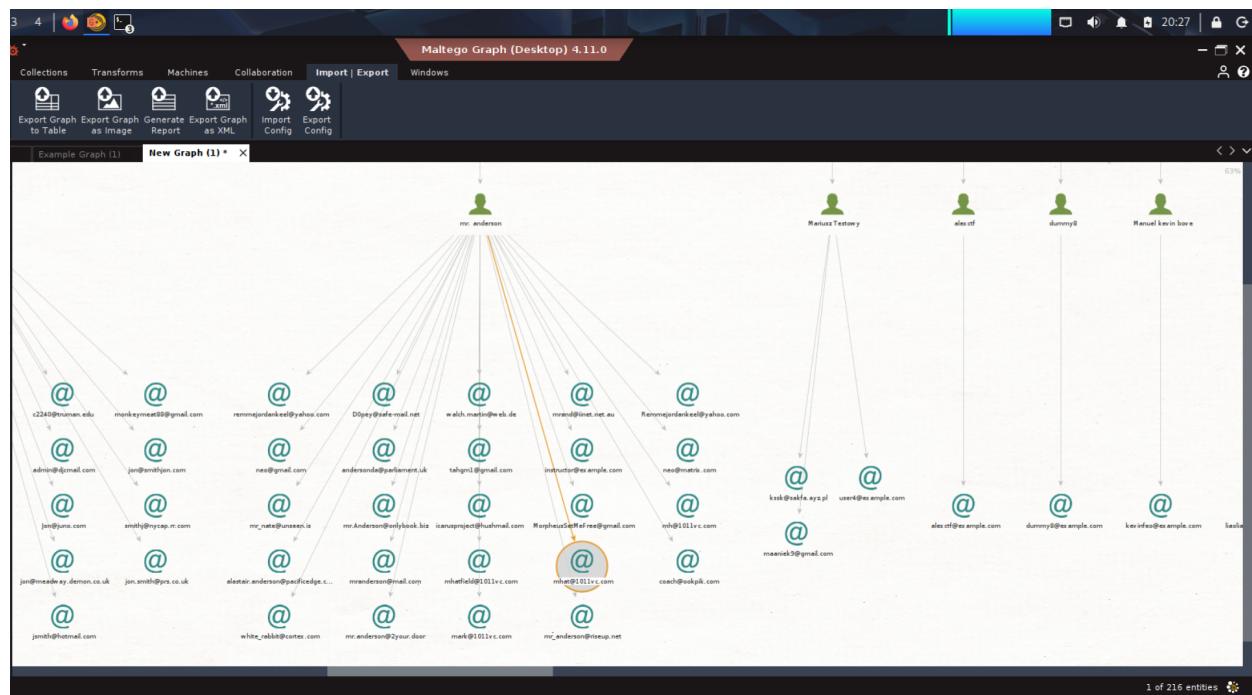
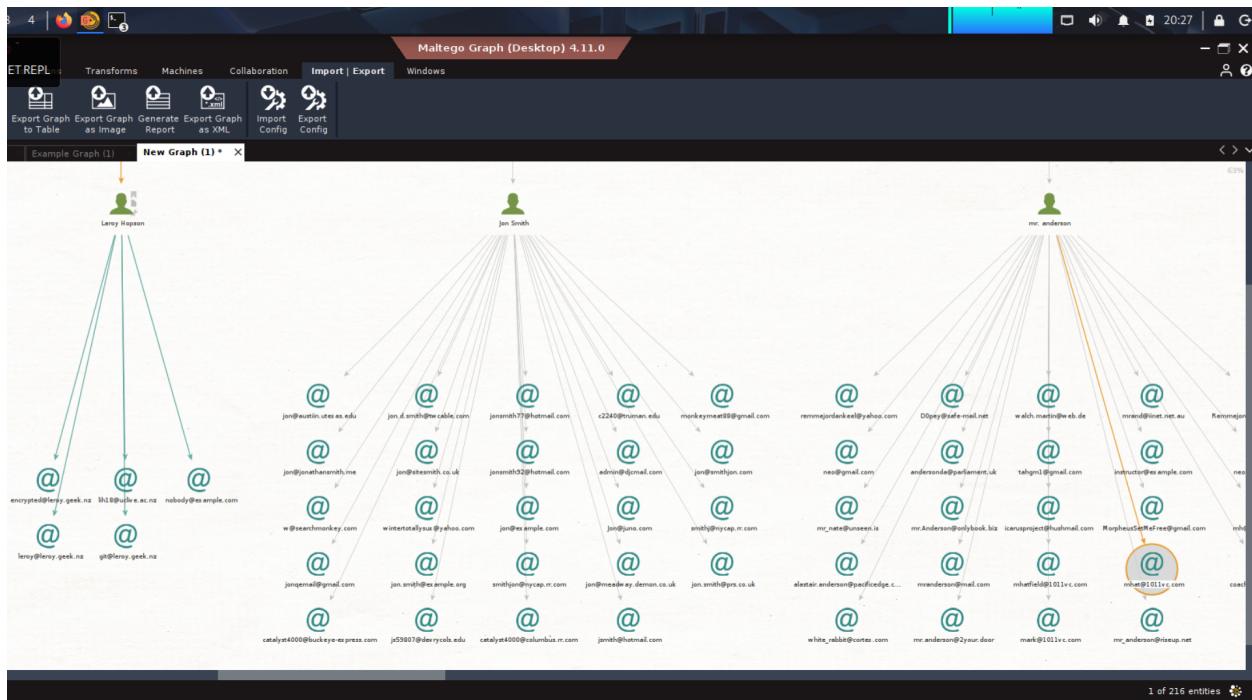
Read www.google.com

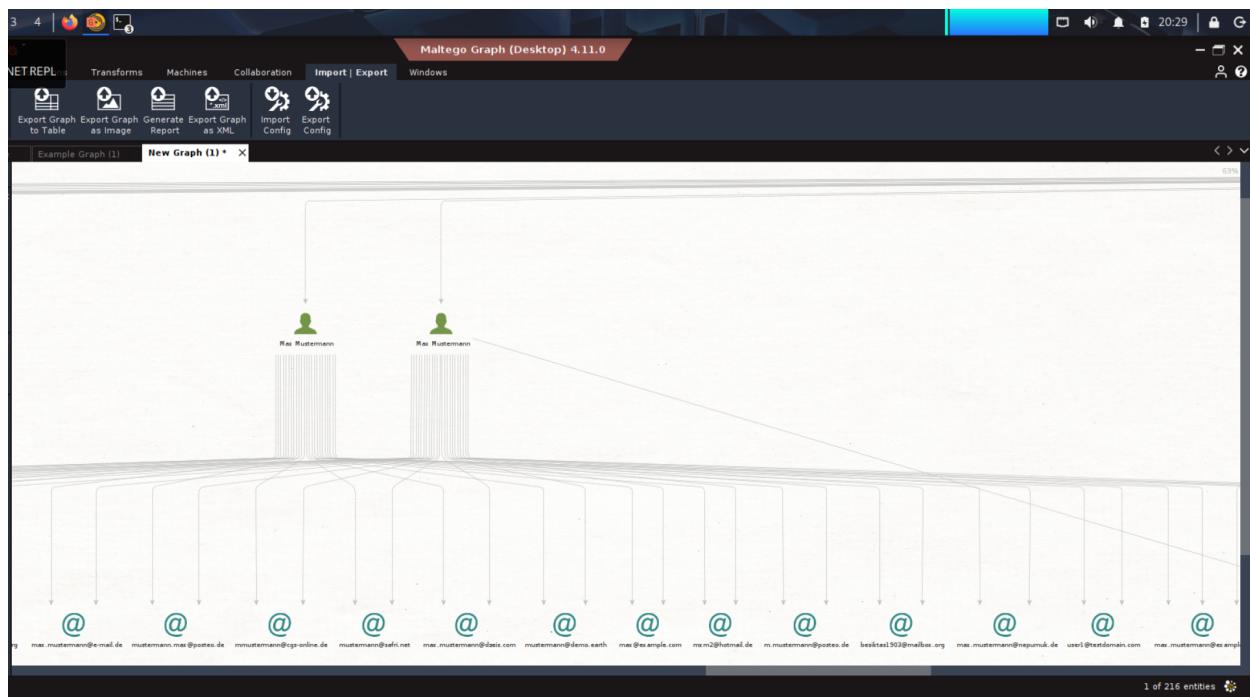
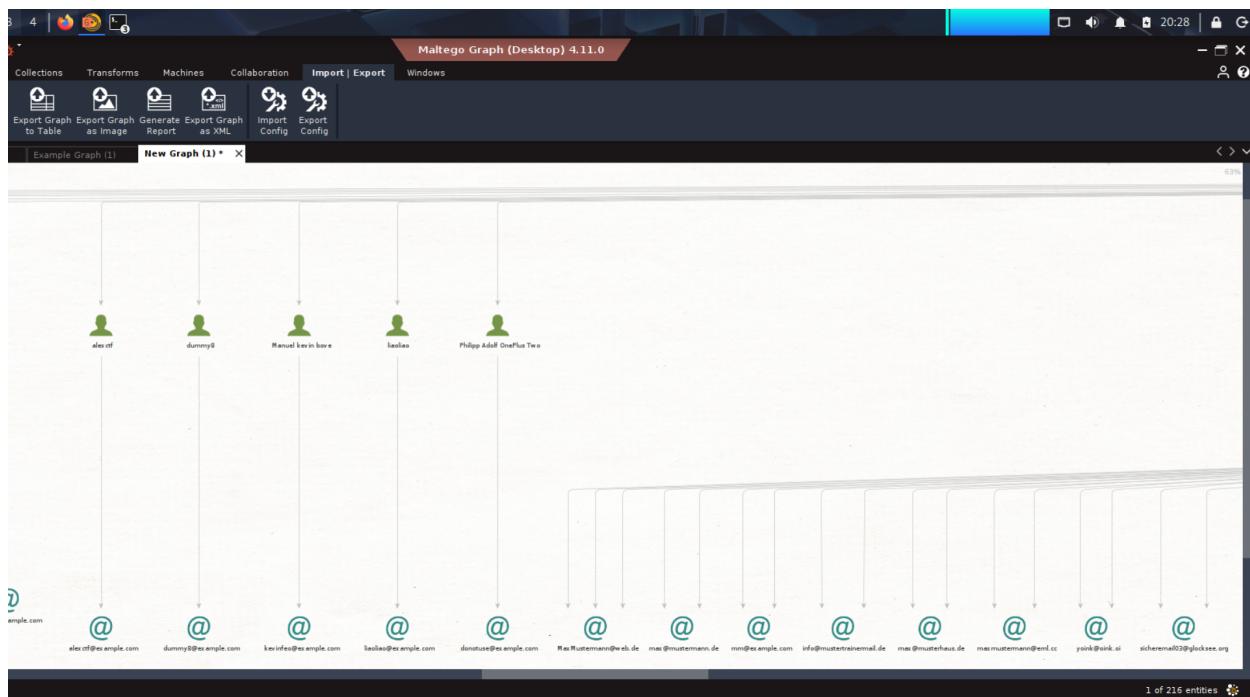
Step 6: Social Media & Open Source Intelligence (OSINT)

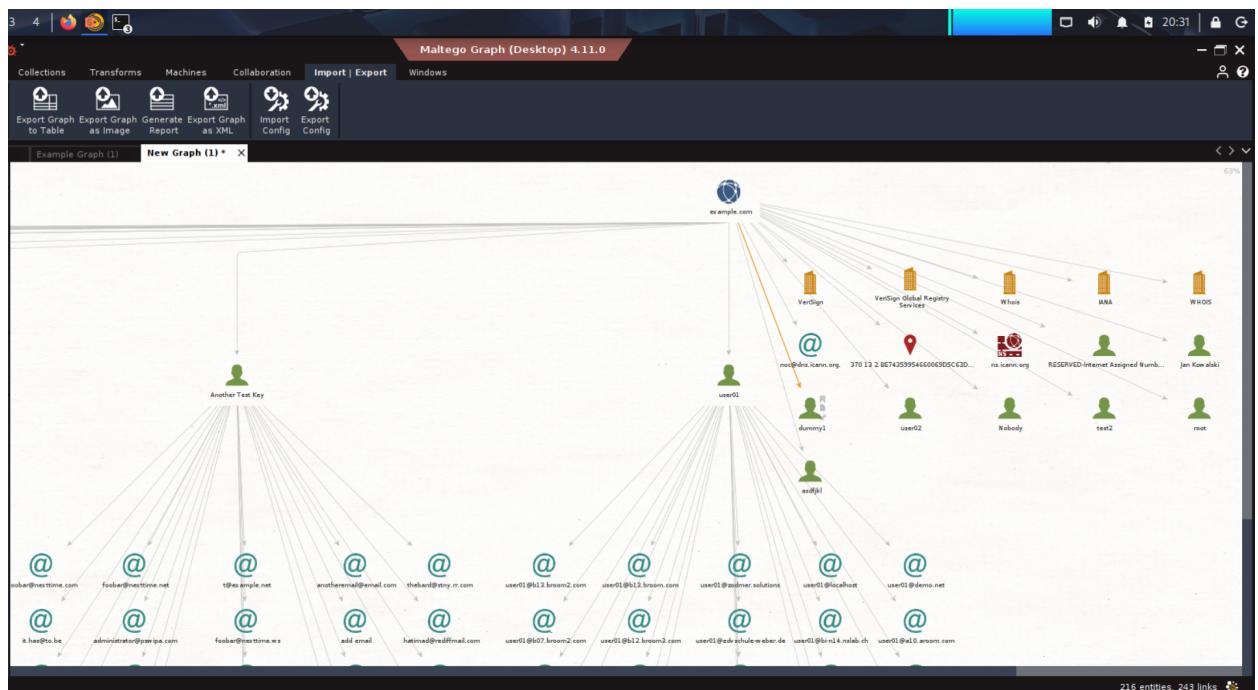
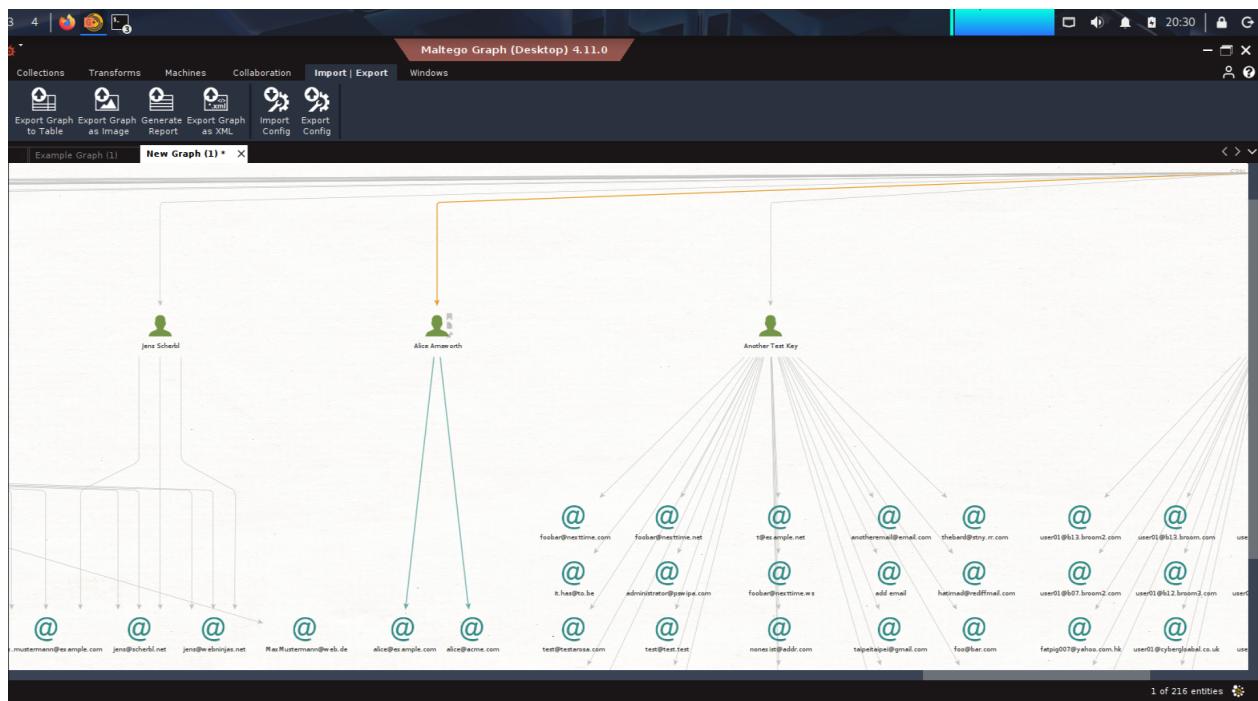
Identified target presence on LinkedIn, Twitter, GitHub, etc.

Tools: Maltego, SpiderFoot.



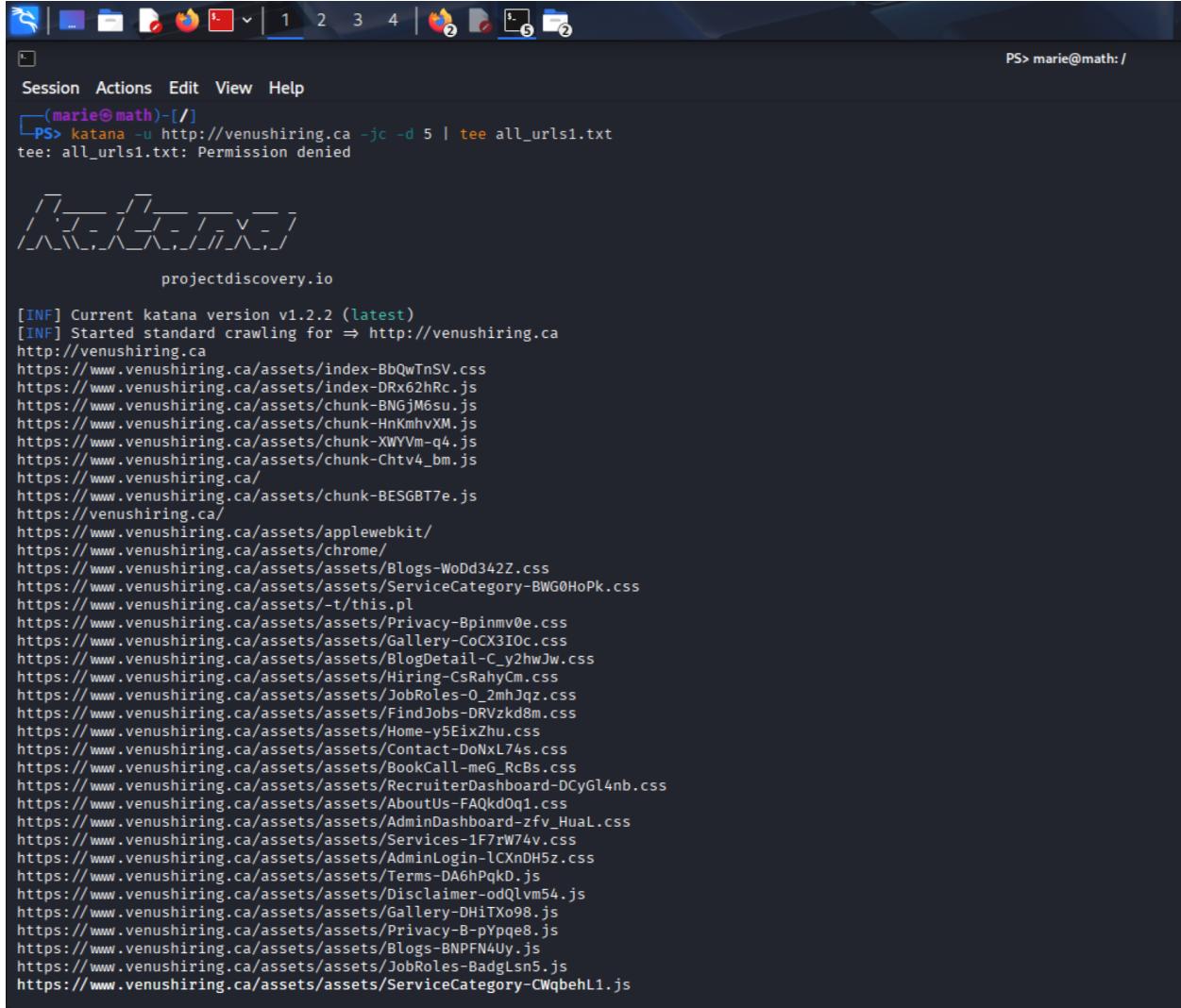






Step 7 : Collected all the urls of the target & filter JS files

Tools used for collecting urls:Katana,GAU,Waybackurls



The screenshot shows a terminal window with a dark blue background. At the top, there's a toolbar with icons for file operations like copy, paste, and save. Below the toolbar, the terminal header shows the session name "(marie@math) [/]" and the prompt "PS>". To the right of the prompt, it says "marie@math:/". The main area of the terminal contains the output of a command:

```
PS> katana -u http://venushiring.ca -jc -d 5 | tee all_urls1.txt
tee: all_urls1.txt: Permission denied
```

Below this, there's some graphical output showing a tree structure of URLs. The root URL is "http://venushiring.ca". Underneath it, there are several sub-directories and files, many of which have been truncated with ellipses (...). Some of the visible URLs include:

- http://www.venushiring.ca/assets/index-BbQwTnSV.css
- http://www.venushiring.ca/assets/index-DRx62hRc.js
- http://www.venushiring.ca/assets/chunk-BNGjM6su.js
- http://www.venushiring.ca/assets/chunk-HnKmhvXM.js
- http://www.venushiring.ca/assets/chunk-XWYVm-q4.js
- http://www.venushiring.ca/assets/chunk-Chtv4_bm.js
- http://www.venushiring.ca/assets/chunk-BESGBT7e.js
- https://www.venushiring.ca/assets/applewebkit/
- https://www.venushiring.ca/assets/chrome/
- https://www.venushiring.ca/assets/assets/Blogs-WoDd34Z2.css
- https://www.venushiring.ca/assets/assets/ServiceCategory-BWG0HoPk.css
- https://www.venushiring.ca/assets/-t/this.pl
- https://www.venushiring.ca/assets/assets/Privacy-8pinmv0e.css
- https://www.venushiring.ca/assets/assets/Gallery-CoCx3IOc.css
- https://www.venushiring.ca/assets/assets/BlogDetail-C_y2hwJw.css
- https://www.venushiring.ca/assets/assets/Hiring-CsRahyCm.css
- https://www.venushiring.ca/assets/assets/JobRoles-0_2mhJqz.css
- https://www.venushiring.ca/assets/assets/FindJobs-DRVZkd8m.css
- https://www.venushiring.ca/assets/assets/Home-y5EixZhu.css
- https://www.venushiring.ca/assets/assets/Contact-DoNxL74s.css
- https://www.venushiring.ca/assets/assets/BookCall-meG_RcBs.css
- https://www.venushiring.ca/assets/assets/RecruiterDashboard-DCyGl4nb.css
- https://www.venushiring.ca/assets/assets/AboutUs-FAQkd0q1.css
- https://www.venushiring.ca/assets/assets/AdminDashboard-zfv_HuaL.css
- https://www.venushiring.ca/assets/assets/Services-1F7rW74v.css
- https://www.venushiring.ca/assets/assets/AdminLogin-lCXnDH5z.css
- 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

The screenshot shows a terminal window with the following details:

- Session Bar:** Shows icons for file operations (copy, paste, move, delete), a terminal icon, and a progress bar.
- Toolbar:** Includes icons for session management (1-4), a terminal icon, and file operations (open, save, copy).
- Text Area:** Displays a command-line session:

```
(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-XWVVm-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-odQlv54.js
https://www.venushiring.ca/assets/assets/Gallery-DH1Tx098.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-DyIR7505.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-ZoiHX0Je.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-DW88FjXe.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-XWVVm-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-odQlv54.js
https://www.venushiring.ca/assets/Terms-DA6hPqkD.js
https://www.venushiring.ca/assets/Privacy-B-pYpqe8.js
https://www.venushiring.ca/assets/Gallery-DHiTx098.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
```
- Status Bar:** Shows the user's name and the current working directory: marie@math: ~/Downloads/Assignment2