OSINT FULL REPORT

1. **Target Primary Email Verification:**

No recover email was found from the primary email.

2. **Extracting the IP address from the email:**

The main location of the email from where it's operating will be get through the IP address.

3. **GEO Location from the IP:**

LOCATION	
City	Riyadh
Region	Riyadh Region (01)
Country	Saudi Arabia (SA)
Continent	Asia (AS)
Coordinates	24.8106436 (lat) / 46.6447161(long)
Time	2023-07-28 18:44:18 (Asia/Riyadh)

NETWORK	
IP address	2.88.2.24
Hostname	2.88.2.24
Provider	Saudi Telecom Company JSC
ASN	25019

4. **The Actual location of the company/or the mail location:**
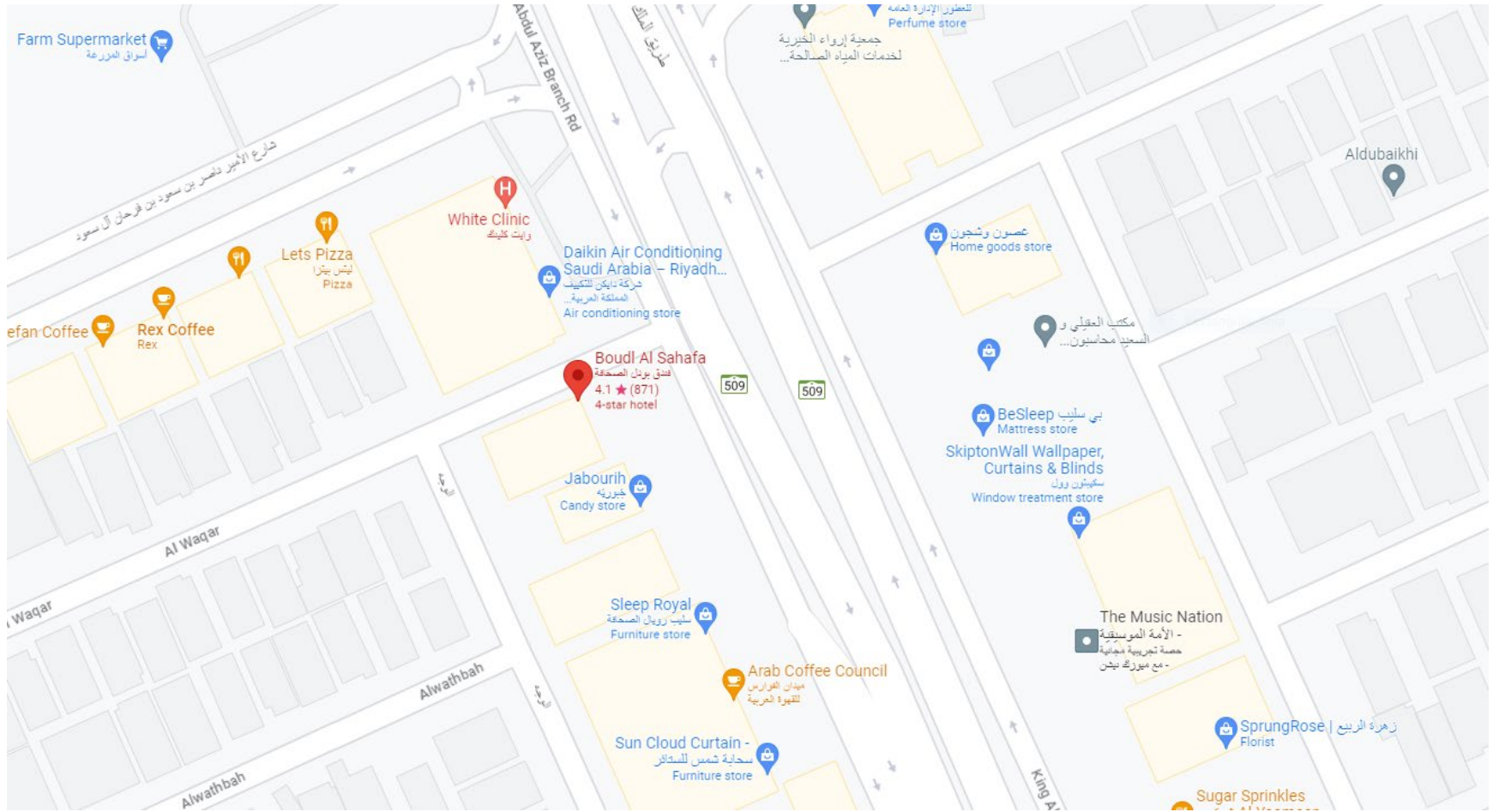
5. **Satelite View:**

Full Address: Boudl Al Sahafa Hotel, Nahr Alnameen, Riyadh, Saudi Arabia

Conclusion: If the business operate from the actual location then the email should be operate from location they put in the website and also the address they sended to you. But after cross checking the location it's remain same at the above location I put. So there location and the website/office location they claiming is mismatched.

Business History Check:

1. **Website Domain History check:**

Domain History:

alriyadhfinance.com - Dark Onion Output

🌐 Domain Information

Domain:	alriyadhfinance.com
Registrar:	NameCheap, Inc.
Registered On:	2023-03-18
Expires On:	2024-03-18
Updated On:	2023-03-18
Status:	clientTransferProhibited
Name Servers:	dns1.namecheaphosting.com dns2.namecheaphosting.com

Business Info:

👤 Business Info

Organization:	Al Riyadh Finance
Street:	Nahr Alnameen
City:	As Sahafah
State:	Riyadh
Postal Code:	13321
Country:	KSA
Phone:	+966 590594636
Email:	

Owner Info:

Owner Info	
First Name	Manoj
Second Name	Sharma
City:	As Sahafah
State:	Riyadh
Postal Code:	13321
Country:	KSA
Phone:	+966 596736522
Email:	

Conclusion: As you can see the information above the business registrated location is same as the IP location. And from the owner information you can see the business is registred with a indian guy who's name is Manoj Sharma. In general if you want to register your business website then it's needed to register with the original owner or with the pepole who is related with the business. But I checked that there is no one called Manoj Sharma who is related with the business.

2. **Phone Number Verification:**

Tracing Dark Web Result for +966596736522

Phone number is valid ☑

Number is not ported ☑

Phone connected to the network ☑

Number information

Name: Manoj Sharma

Country : Saudi Arabia

Country code: +966

Telephone Number: +966596736522

ISO 3166-1 alpha-2 code: SA

Telecom Provider: Zain

Network Type: CDMA / GSM

TimeZone: Asia/Riyadh

Tracing Dark Web Result for +966590594636

Phone number is valid ☑

Number is not ported ☑

Phone connected to the network ☑

Number information

Name: Marie Minalang

Country : Saudi Arabia

Country code: +966

Telephone Number: +966590594636

ISO 3166-1 alpha-2 code: SA

Telecom Provider: Zain

Network Type: CDMA / GSM

TimeZone: Asia/Riyadh

Conclusion: The First number is registered with the Manoj Sharma. And the second number is registerd with the name: Marie Minalang which is a philippines name. But both name are not related to front of the business as we can see the only name Manoj sharma is resgistered with the business.

3. **The Company Domain Black Listed by Local Government Agency:**

Server IP:

```
<!-- www.alriyadhfinance.com--></i>
</div>
</body>
/html>
!--Server Input: 114.198.232.0 Output: 114.198.232.255-->
```

Blacklisted:

🖼 Blacklisted Hosting KSA

.

.

From IP	To IP	Total IPs	Assign Date	Owner
2.88.0.0	2.91.255.255	262144	17/05/10	Saudi Telecom Company JSC
5.41.0.0	5.41.255.255	65536	16/05/12	Saudi Telecom Company JSC
5.42.224.0	5.42.255.255	8192	18/05/12	Integrated Telecom Co. Ltd
5.82.0.0	5.82.255.255	65536	13/06/12	Bayanat Al-Oula For Network Services
5.108.0.0	5.111.255.255	262144	28/06/12	Etihad Etisalat, a joint stock company
5.132.192.0	5.132.255.255	16384	02/07/12	Integrated Telecom Co. Ltd
5.156.0.0	5.156.255.255	65536	19/07/12	Saudi Telecom Company JSC
5.163.0.0	5.163.255.255	65536	30/07/12	Saudi Telecom Company JSC
5.244.0.0	5.247.255.255	262144	11/09/12	Etihad Etisalat, a joint stock company
31.166.0.0	31.167.255.255	131072	01/03/11	Etihad Etisalat, a joint stock company
37.16.32.0	37.16.63.255	8192	16/12/11	Bayanat Al-Oula For Network Services
37.16.128.0	37.16.255.255	32768	16/12/11	Bayanat Al-Oula For Network Services
37.25.0.0	37.25.31.255	8192	23/12/11	Saudi Telecom Company JSC
37.42.0.0	37.43.255.255	131072	04/01/12	Etihad Etisalat, a joint stock company
37.56.0.0	37.56.255.255	65536	13/01/12	Saudi Telecom Company JSC
114.198.232.0	114.198.232.255	255	18/05/23	Al Riyadh Finance
37.99.128.0	37.99.191.255	16384	07/02/12	Etihad Atheeb Telecom Company

Conclusion: If the authority got too many bad feedback or get any scammed alert from the pepole who are victim with the business or the site then in general every country blacklisted the website to make pepole alert. Also for the business there is term to verfication if the owner failed to show the actual office location with video verification then also they can be blacklisted. But as Al Riyadh website created in 18/03/2023 and also get blacklisted in 18/05/2023 that's really suspicous of their validity because within 2 months no valid business should be blacklisted.

4. **Final Recon:**

```
#######################################################################
 Recon succesfully started on https://www.alriyadhfinance.com
#######################################################################


#######################################################################
 Checking installed tools

 [*] jq                         [NO]

 Try running the installer script again ./install.sh
 If it fails for any reason try to install manually the tools missed
 Finally remember to set the $tools variable at the start of this script
 If nothing works and the world is gonna end you can always ping me :D

 Tools check finished
#######################################################################

 Target: https://www.alriyadhfinance.com

#######################################################################
 Searching domain info (whois, registrant name/email domains)

 domain_info Finished in 1 minutes, 8 seconds.
 Results are saved in https://www.alriyadhfinance.com/osint/domain_info_[general/name/email/ip].txt
#######################################################################
#######################################################################
 Searching emails/users/passwords leaks
./reconftw.sh: line 225: jq: command not found
```

```
 Results are saved in https://www.alriyadhfinance.com/osint/[emails/users/h8mail/passwords].txt
#######################################################################

# .git folders (https://www.google.com/search?q=inurl%3A%5C%22%2F.git%5C%22%20https://www.alriyadhfinance.com%20-github)

<urlopen error [Errno -3] Temporary failure in name resolution>

# Backup files (https://www.google.com/search?q=site%3Ahttps://www.alriyadhfinance.com%20ext%3Abkf%20%7C%20ext%3Abkp%20%7C%20ext%3Abak%20%7C%20ext%3Aold%20%7C%20ext%3Abackup)

<urlopen error [Errno -3] Temporary failure in name resolution>

# Exposed documents (https://www.google.com/search?q=site%3Ahttps://www.alriyadhfinance.com%20ext%3Adoc%20%7C%20ext%3Adocx%20%7C%20ext%3Aodt%20%7C%20ext%3Apdf%20%7C%20ext%3Artf%20%7C%20ext%3Asxw%20%7C%20ext%3Apsw%20%7C%20ext%3Appt%20%7C%20ext%3ApptX%20%7C%20ext%3Apps%20%7C%20ext%3Acsv)

<urlopen error [Errno -3] Temporary failure in name resolution>

# Confidential documents (https://www.google.com/search?q=inurl%3Aalriyadhfinance+not+for+distribution+%7C+confidential+%7C+%22employee+only%22+%7C+proprietary+%7C+top+secret+%7C+classified+%7C+trade+secret+%7C+internal+%7C+private+filetype%3Axls+OR+filetype%3Acsv+OR+filetype%3Adoc+OR+filetype%3Apdf)

<urlopen error [Errno -3] Temporary failure in name resolution>

# Config files (https://www.google.com/search?q=site%3Ahttps://www.alriyadhfinance.com%20ext%3Axml%20%7C%20ext%3Aconf%20%7C%20ext%3Acnf%20%7C%20ext%3Areg%20%7C%20ext%3Ainf%20%7C%20ext%3Ardp%20%7C%20ext%3Acfg%20%7C%20ext%3Atxt%20%7C%20ext%3Aora%20%7C%20ext%3Aenv%20%7C%20ext%3Aini)

<urlopen error [Errno -3] Temporary failure in name resolution>

# Database files (https://www.google.com/search?q=site%3Ahttps://www.alriyadhfinance.com%20ext%3Asql%20%7C%20ext%3Adbf%20%7C%20ext%3Amdb)

<urlopen error [Errno -3] Temporary failure in name resolution>

# Other files (https://www.google.com/search?q=site%3Ahttps://www.alriyadhfinance.com%20intitle%3Aindex.of%20%7C%20ext%3Alog%20%7C%20ext%3Aphp%20intitle%3Aphpinfo%20%5C%22published%20by%20the%20PHP%20Group%5C%22%20%7C%20inurl%3Ashell%20%7C%20inurl%3Abackdoor%20%7C%20inurl%3Awso%20%7C%20inurl%3Acmd%20%7C%20shadow%20%7C%20passwd%20%7C%20boot.ini%20%7C%20inurl%3Abackdoor%20%7C%20inurl%3Areadme%20%7C%20inurl%3Alicense%20%7C%20inurl%3Ainstall%20%7C%20inurl%3Asetup%20%7C%20inurl%3Aconfig%20%7C%20inurl%3A%5C%22%2Fphpinfo.php%5C%22%20%7C%20inurl%3A%5C%22.htaccess%5C%22%20%7C%20ext%3Aswf)

<urlopen error [Errno -3] Temporary failure in name resolution>

# SQL errors (https://www.google.com/search?q=site%3Ahttps://www.alriyadhfinance.com%20intext%3A%5C%22sql%20syntax%20near%5C%22%20%7C%20intext%3A%5C%22syntax%20error%20has%20occurred%5C%22%20%7C%20intext%3A%5C%22incorrect%20syntax%20near%5C%22%20%7C%20intext%3A%5C%22unexpected%20end%20of%20SQL%20command%5C%22%20%7C%20intext%3A%5C%22Warning%3A%20mysql_connect()%5C%22%20%7C%20intext%3A%5C%22Warning%3A%20mysql_query()%5C%22%20%7C%20intext%3A%5C%22Warning%3A%20pg_connect()%5C%22)

<urlopen error [Errno -3] Temporary failure in name resolution>

# PHP errors (https://www.google.com/search?q=site%3Ahttps://www.alriyadhfinance.com%20%5C%22PHP%20Parse%20error%5C%22%20%7C%20%5C%22PHP%20Warning%5C%22%20%7C%20%5C%22PHP%20Error%5C%22)

<urlopen error [Errno -3] Temporary failure in name resolution>

# Wordpress files (https://www.google.com/search?q=site%3Ahttps://www.alriyadhfinance.com%20inurl%3Awp-content%20%7C%20inurl%3Awp-includes)

<urlopen error [Errno -3] Temporary failure in name resolution>

# Project management sites (https://www.google.com/search?q=site%3Atrello.com%20%7C%20site%3A*.atlassian.net%20%22alriyadhfinance%22)
```

```
Required file /home/kali/Tools/.github_tokens not exists or empty

github_dorks Finished in 0 seconds.
Results are saved in https://www.alriyadhfinance.com/osint/gitdorks.txt
###################################################################
###################################################################
Github Repos analysis in process

Required file /home/kali/Tools/.github_tokens not exists or empty

github_repos Finished in 0 seconds.
Results are saved in https://www.alriyadhfinance.com/osint/github_company_secrets.json
###################################################################
###################################################################
Scanning metadata in public files

metadata Finished in 9 seconds.
Results are saved in https://www.alriyadhfinance.com/osint/[software/authors/metadata_results].txt
###################################################################
###################################################################
Zone transfer check

zonetransfer Finished in 12 seconds.
Results are saved in https://www.alriyadhfinance.com/subdomains/zonetransfer.txt
###################################################################
###################################################################
Favicon Ip Lookup

favicon Finished in 2 seconds.
Results are saved in hosts/favicontest.txt
###################################################################
###################################################################


Subdomain Enumeration https://www.alriyadhfinance.com


Running : Passive Subdomain Enumeration

0 new subs (passive) in 1 minutes, 34 seconds.

Running : Crtsh Subdomain Enumeration

0 new subs (cert transparency) in 7 seconds.

Running : Active Subdomain Enumeration

0 subs DNS resolved from passive in 13 seconds.

Running : Checking NOERROR DNS response
panic: runtime error: integer divide by zero
```

```
Detected DNSSEC black lies, skipping this technique

Running : Bruteforce Subdomain Enumeration

0 new subs (bruteforce) in 13 seconds.

Running : Permutations Subdomain Enumeration

0 new subs (permutations) in 12 seconds.

Running : Permutations by regex analysis
Traceback (most recent call last):
  File "/home/kali/Tools/regulator/main.py", line 290, in <module>
    main()
  File "/home/kali/Tools/regulator/main.py", line 284, in main
    with open(args['output'], 'w') as handle:
FileNotFoundError: [Errno 2] No such file or directory: '/home/kali/tools/reconftw/Recon/https://www.alriyadhfinance.com/.tmp/https://www.alriyadhfinance.com.rules'
cat: '/home/kali/tools/reconftw/Recon/https://www.alriyadhfinance.com/.tmp/https://www.alriyadhfinance.com.rules': No such file or directory
./make_brute_list.sh: line 4: /home/kali/tools/reconftw/Recon/https://www.alriyadhfinance.com/.tmp/https://www.alriyadhfinance.com.brute: No such file or directory

0 new subs (permutations) in 13 seconds.

sub_recursive_passive skipped in this mode or defined in reconftw.cfg

sub_recursive_brute skipped in this mode or defined in reconftw.cfg

Running : DNS Subdomain Enumeration and PTR search

0 new subs (dns resolution) in 12 seconds.

Running : Source code scraping subdomain search

No subdomains to search (code scraping) in 0 seconds.

Running : Analytics Subdomain Enumeration

0 new subs (analytics relationship) in 0 seconds.

Running : Http probing https://www.alriyadhfinance.com
./reconftw.sh: line 915: jq: command not found
./reconftw.sh: line 915: jq: command not found

0 new websites resolved in 1 seconds.

Total subdomains:


- 0 alive

- 0 new web probed
```

```
nuclei_check Finished in 1 minutes, 22 seconds.
Results are saved in https://www.alriyadhfinance.com/nuclei_output folder
###########################################################################
Web directory fuzzing

fuzz Finished in 0 seconds.
No https://www.alriyadhfinance.com/web/webs.txts file found, fuzzing skipped
###########################################################################
###########################################################################
URL Extraction
###########################################################################
Javascript Scan

jschecks Finished in 0 seconds.
No JS urls found for https://www.alriyadhfinance.com, function skipped
###########################################################################
CMS Scanner

cms_scanner Finished in 0 seconds.
No https://www.alriyadhfinance.com/web/webs.txts file found, cms scanner skipped
###########################################################################
Vulnerable Pattern Search

url_gf Finished in 0 seconds.
Results are saved in https://www.alriyadhfinance.com/gf folder
###########################################################################
Wordlist generation

wordlist_gen Finished in 0 seconds.
Results are saved in https://www.alriyadhfinance.com/webs/dict_[words|paths].txt
###########################################################################
Robots wordlist generation

wordlist_gen_roboxtractor Finished in 0 seconds.
Results are saved in https://www.alriyadhfinance.com/webs/robots_wordlist.txt
###########################################################################
Password dictionary generation

password_dict Finished in 1 seconds.
Results are saved in https://www.alriyadhfinance.com/webs/password_dict.txt
###########################################################################
###########################################################################

Finished Recon on: https://www.alriyadhfinance.com under /home/kali/tools/reconftw/Recon/https://www.alriyadhfinance.com in: 10 minutes, 31 seconds.
###########################################################################
```

```
- 0 alive

- 0 new web probed

Subdomain Enumeration Finished
Results are saved in https://www.alriyadhfinance.com/subdomains/subdomains.txt and webs/webs.txt
###########################################################################

###########################################################################
Http probing non standard ports

Uncommon web ports: 0 new websites

webprobe_full Finished in 0 seconds.
Results are saved in https://www.alriyadhfinance.com/webs/webs_uncommon_ports.txt
###########################################################################

subtakeover skipped in this mode or defined in reconftw.cfg
###########################################################################
AWS S3 buckets search

s3buckets Finished in 56 seconds.
Results are saved in subdomains/s3buckets.txt and subdomains/cloud_assets.txt
###########################################################################
Web Screenshots

screenshot Finished in 0 seconds.
Results are saved in https://www.alriyadhfinance.com/screenshots folder
###########################################################################
CDN provider check

cdnprovider Finished in 0 seconds.
Results are saved in hosts/cdn_providers.txt
###########################################################################
Port scan

Resolved IP addresses (No CDN)

Scanning ports ...

portscan Finished in 0 seconds.
Results are saved in hosts/portscan_[passive|active].txt
###########################################################################
Website's WAF detection

waf_checks Finished in 0 seconds.
```

Conclusion: In general the final recon shows us the employee history about the business owner or pepoles who are related with the business. But in here there is active employee or nothing occurs.

Manual Verification:

So after implementing all the process I though may be I can use one of my client who is really friendly with me and we are working together from last 2 years and he is from saudi arabia also live in Olaya District. So I ask him if he can verify the office which they provided: And here is the conversation with him:

The Final Conclusion: I saw many mismatched with the company information they put in the online. And also the registered name and the info are not matched with the company either, From the name as there is two name one is indian and one is philipines I am suspecting that they made a syndicate to fruad with pepole with their money because if it's a genuine reputated company then there must be few online frootprint with the rating and review but there is nothing with them also there are huge mismatched information with them which can't be found for a normal pepole who are not related into the darker site of internet. Also if you want any authentic sources of their existence then that's a enough proof that one human being who is from saudi arabia visit the place and the find nothing with them.

So the case might look like this: A syndicate using other business policy and location to just making it sure they exist with a website which is also not a corporate builded site just they using it for an marketing policy to show pepole they exist I am suspecting more with company because there is two name related and which is indian and philipines and from my experinces country like india and philipines who belong from them making lots scam nowdays, so their might be chacne of getting scammed or may be you can loss if go for a deal with as there no strong existence of them and also theiris too much mismatched with the company. I would love to recommend you do not go for any financial or business related project with them it can be risky or it can be a huge loss for you, that's all I can suggest you from my experinces and that's kind of scamming going on nowdays on overall the world and the ratio of the scammers are high in india and philipines.

THANK YOU