Task 2 :- Analyze a Phishing Email Sample.

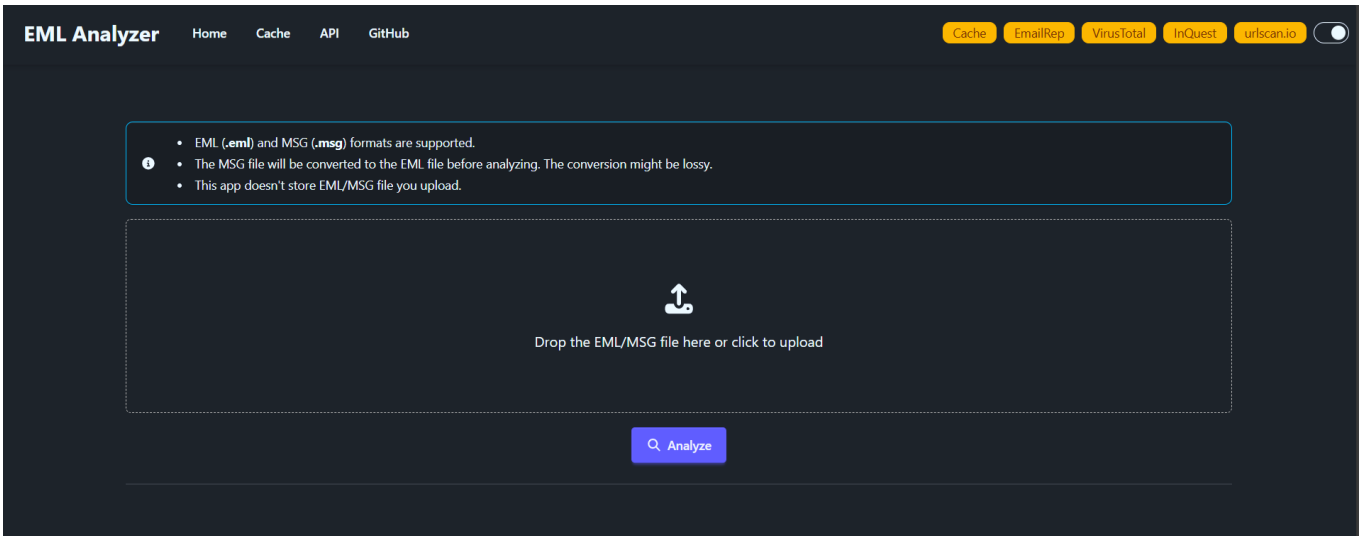
Step 1 :-

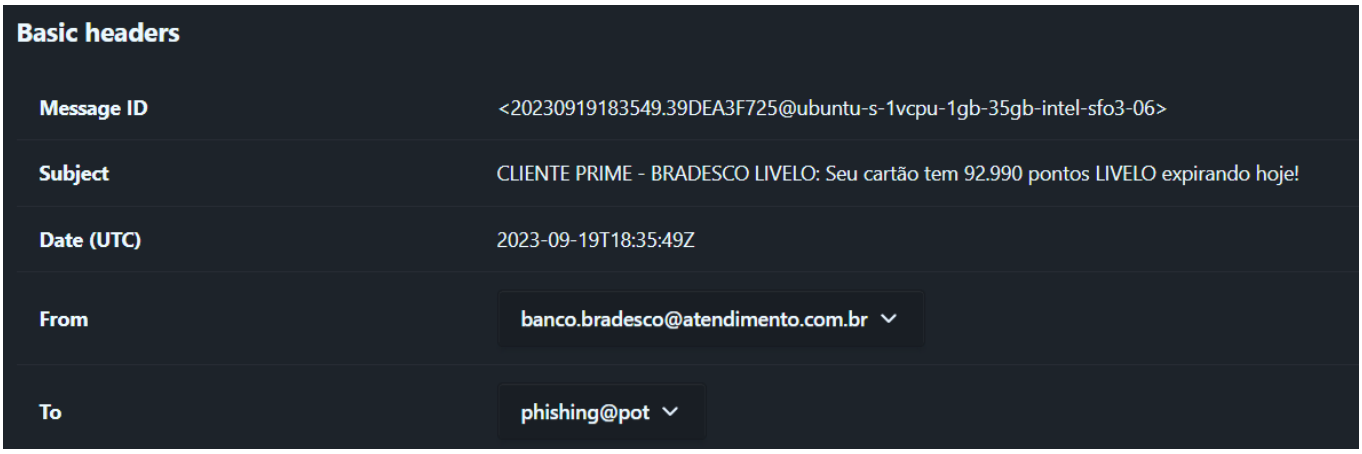
Obtain the phishing email file with .eml extension.

File I got from :- [30-Days-SOC-Challenge-Beginner/Challenge#5/Day#22- Phishing Analysis: Suspicious Lookalike email.md at main · 0xrajneesh/30-Days-SOC-Challenge-Beginner · GitHub](#) .

Step 2 :-

Let's examine the senders email address using EML Analyser.

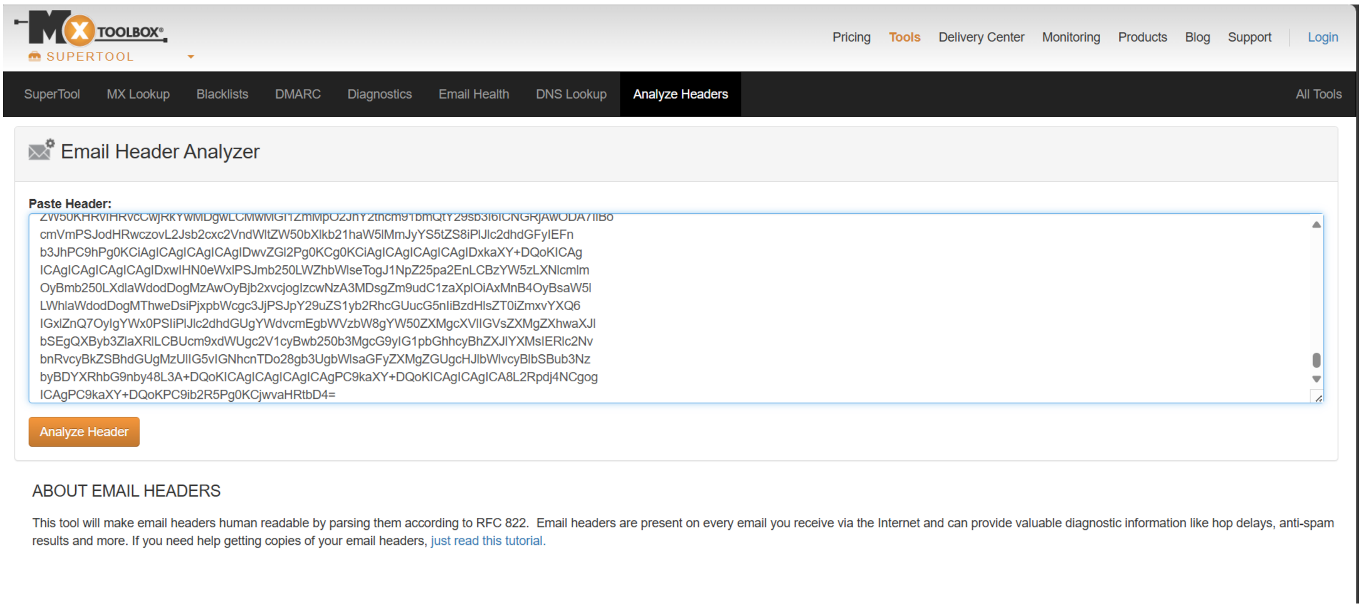


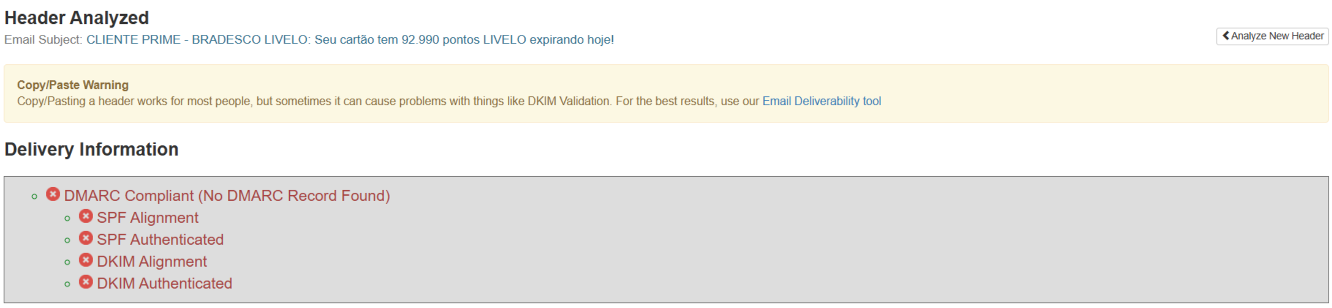


Through this we are able to get the email id of sender and receiver and also to find the ip address through which the mail is been send.

Step 3 :-

Analyze a header of the email using MX Toolbox (it is a multipurpose tool or software but we are going to use it for Header Analyser).





Here we have found the suspicious attachments like :-

1. DMARC Compliant (No DMARC Record Found):

No DMARC record exists; the domain isn't protected from email spoofing.

2. SPF Alignment:

Checks if the "From" domain matches the domain in the SPF record.

3. SPF Authenticated:

Verifies if the sending server is authorized in the SPF record.

4. DKIM Alignment:

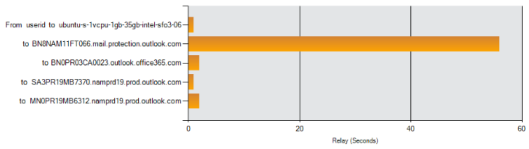
Checks if the domain in the DKIM signature matches the "From" domain.

5. DKIM Authenticated:

Verifies if the DKIM signature is valid and the email wasn't altered.

Relay Information

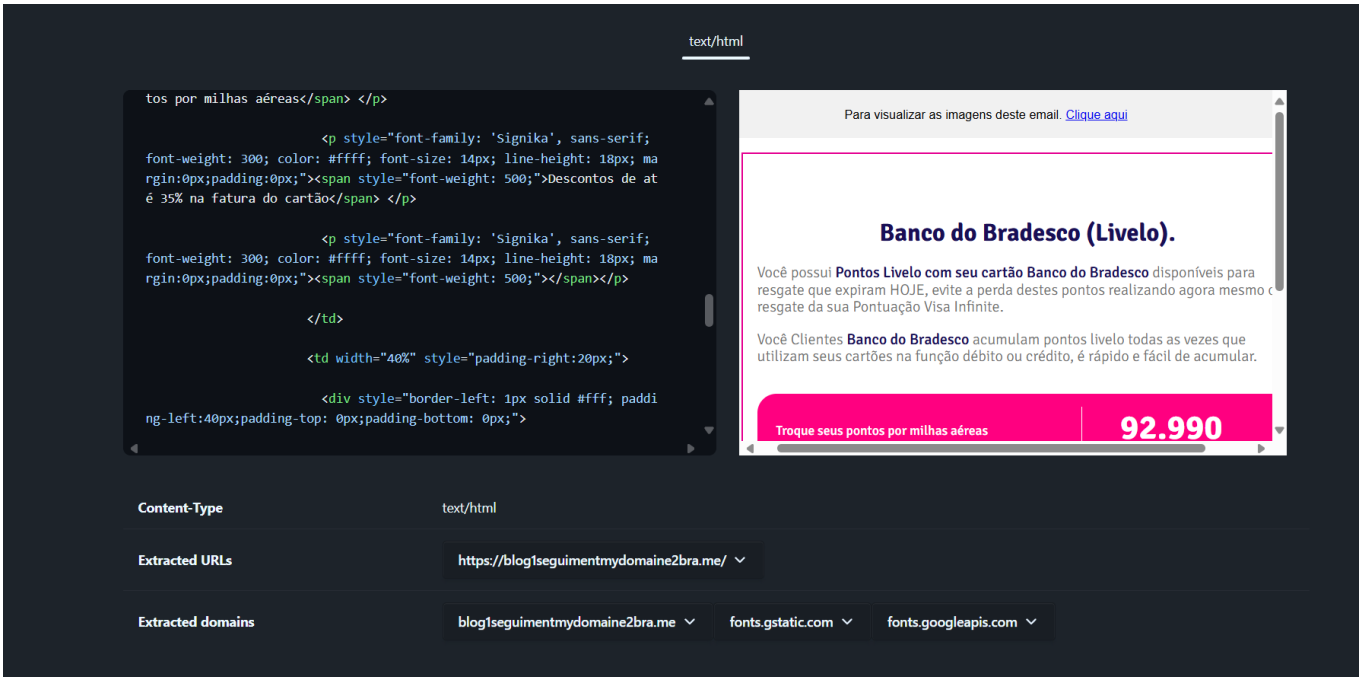
Received Delay:	57 seconds



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	userid	ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06		9/19/2023 6:35:49 PM	
2	55 seconds	ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 137.184.34.4	BN8NAM11FT066.mail.protection.outlook.com 10.13.177.138	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/19/2023 6:36:44 PM	
3	1 Second	BN8NAM11FT066.eop-nam11.prod.protection.outlook.com 2603:10b6:408:e6.cafe::23	BN0PR03CA0023.outlook.office365.com 2603:10b6:408:e6::28	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/19/2023 6:36:45 PM	
4	0 seconds	BN0PR03CA0023.namprd03.prod.outlook.com 2603:10b6:408:e6::28	SA3PR19MB7370.namprd19.prod.outlook.com 2603:10b6:806:317::17	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/19/2023 6:36:45 PM	
5	1 Second	SA3PR19MB7370.namprd19.prod.outlook.com ::1	MN0PR19MB6312.namprd19.prod.outlook.com	HTTPS	9/19/2023 6:36:46 PM	

Step 4 :-

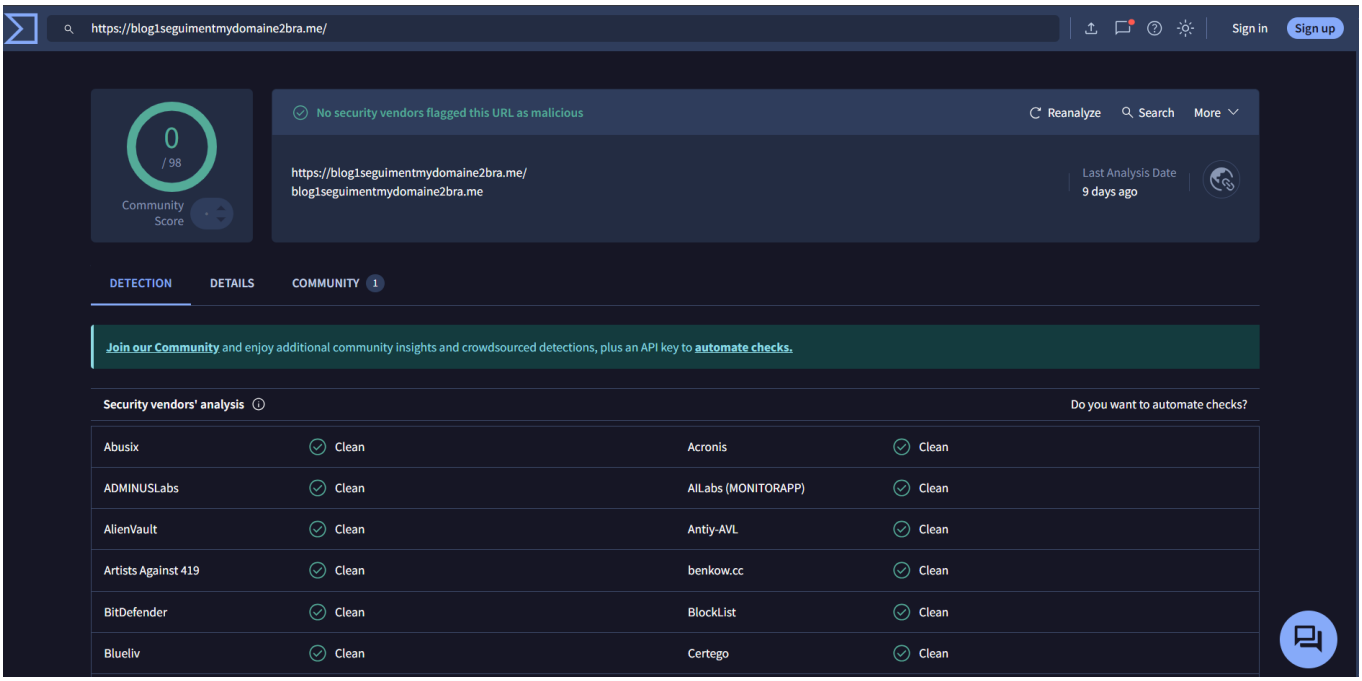
Look for any suspicious links or attachments.



Here we found the suspicious link stating click here (or Clique aqui).

Step 5 :-

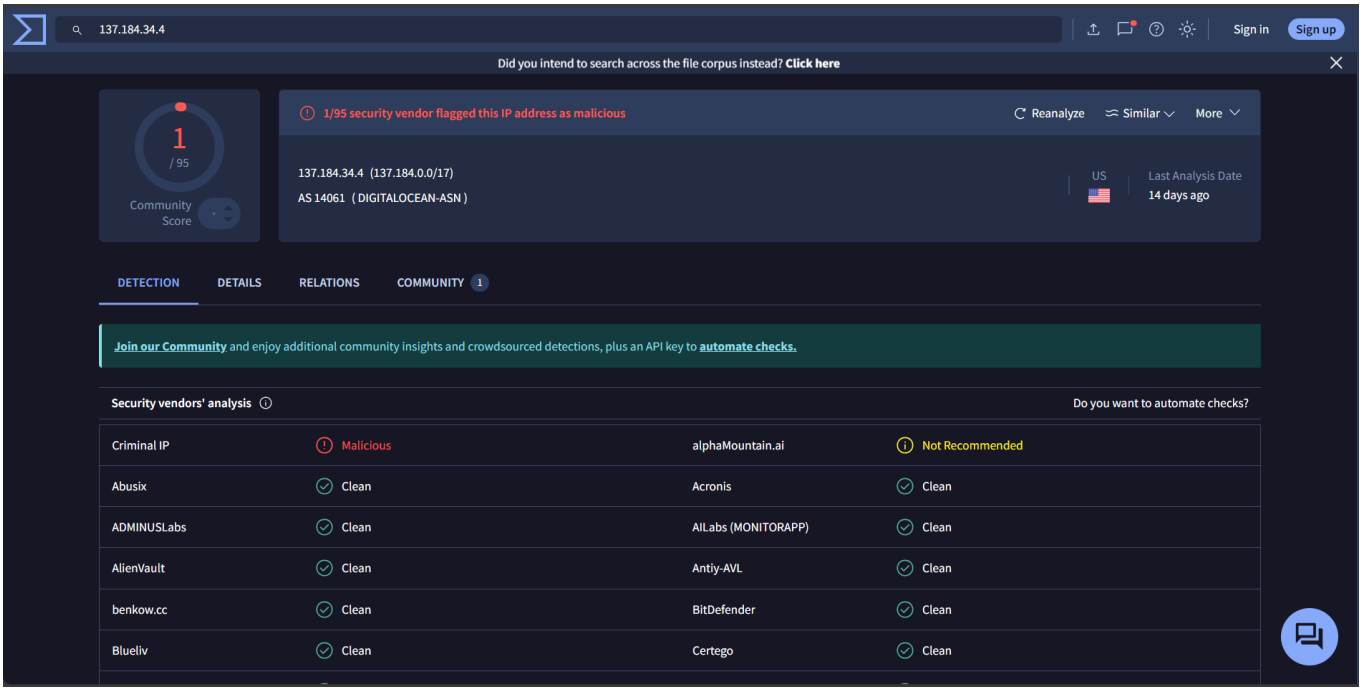
Analyze this links using VirusTool.



Using this software, we are getting clean link but the link is not clean as the software might has the pre-stored lines of code that they analysis and store it as a signature and if few of the lines gets interchange then these signature matching gets' failed and result's us as the non- suspicious link or any files.

Step 5 :-

Let’s search about the ip address that we have found or the senders address.



A malicious link has been discovered.