

Name:	:	Bocobo, Adolf Vincent Padua, Jaymar	Lab No.	:	2
Topic	:	Email Forensics (SMTP)	Group No.	:	20
Subject	:	Cyber Security	Score	:	

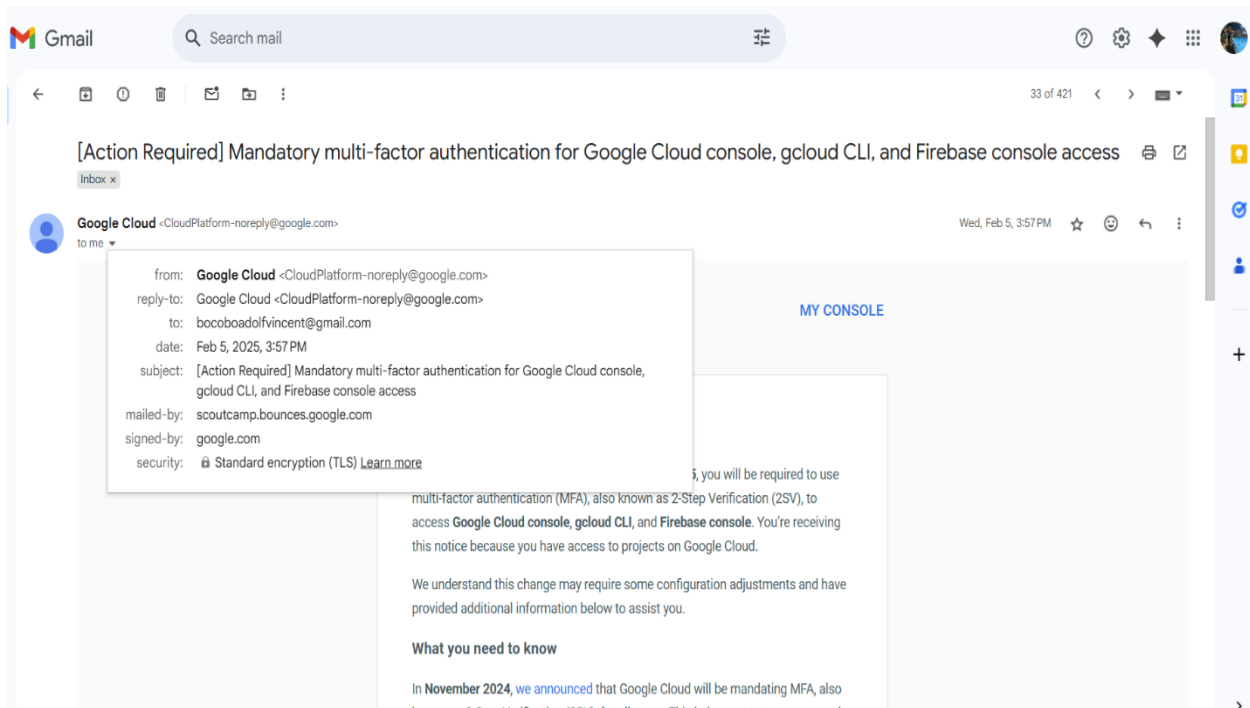
You have recently joined CyberOrg as a Security Analyst, and you have been assigned the task to carry out a forensic investigation of a suspicious email header allegedly received from Facebook.

Carry out a thorough investigation, and respond to the following points:

- Confirm if the email is legitimate or not
- Identify the IP address of the source SMTP server
- Identify the specific country and city where the source SMTP server is located

Procedure/ Algorithm


Step 1: Confirm if the email is legitimate or not



Step 2: Identify the IP address of the source SMTP server

	Blacklist	Reason	TTL	ResponseTime
✓ OK	OSPAM			47
✓ OK	OSPAM RBL			47
✓ OK	Abusix Mail Intelligence Blacklist			0
✓ OK	Abusix Mail Intelligence Domain Blacklist			0
✓ OK	Abusix Mail Intelligence Exploit list			0
✓ OK	Anonmails DNSBL			0
✓ OK	BACKSCATTERER			0
✓ OK	BARRACUDA			16
✓ OK	BLOCKLIST.DE			0
✓ OK	CALIVENT			0
✓ OK	CYMRU BOGONS			0
✓ OK	DAN TOR			188
✓ OK	DRMX			0
✓ OK	DRONE BL			31
✓ OK	FABELSOURCES			16
✓ OK	HIL			0
✓ OK	HIL2			16
✓ OK	Hostkarma Black			141
✓ OK	IBM DNS Blacklist			203
✓ OK	ICMFORBIDDEN			234
✓ OK	IMP SPAM			0
✓ OK	IMP WORM			0

Step 3: Identify the specific country and city where the source SMTP server is located

[Q Search](#)[ABOUT](#)[PRESS](#)[BLOG](#)[SUPPORT](#)

[MY IP](#)[IP LOOKUP](#)[HIDE MY IP](#)[VPNS](#)[TOOLS](#)[LEARN](#)

IP Details For: 209.85.220.69

Decimal: 3512065093

Hostname: mail-sor-f69.google.com

ASN: 15169

ISP: Google LLC

Services: DatacenterLikely [mail server](#)

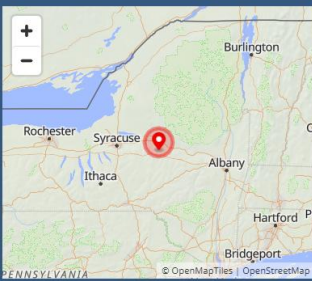
Country: United States

State/Region: New York

City: Utica

Latitude: 43.1013 (43° 6' 4.68" N)

Longitude: -75.2327 (75° 13' 57.57" W)



CLICK TO CHECK BLACKLIST STATUS

Latitude and Longitude are often near the center of population. These values are not precise enough to be used to identify a specific address, individual, or for legal purposes. IP data from [IP2Location](#).

Result and Discussion

Step 1:

After visiting my gmail, I opened some email from google.com. I check the header of the email and it is legit, because the send and the reply are the same.

Step 2:

Source IP address of the origin server to see where it is blacklisted.

Step 3:

For the last step, I Identify the specific country and city where the source SMTP server is located

Conclusion

Through analyzing the email header, we confirmed that the email is legitimate based on matching sender and reply addresses. The source SMTP server's IP address was identified, and its geographic location was successfully traced to a specific country and city, completing the forensic investigation effectively.