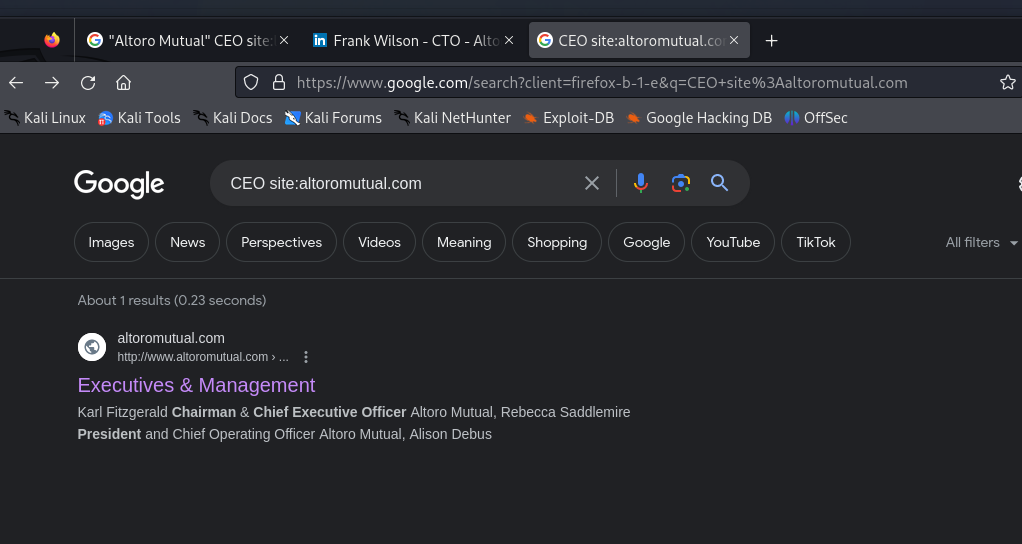
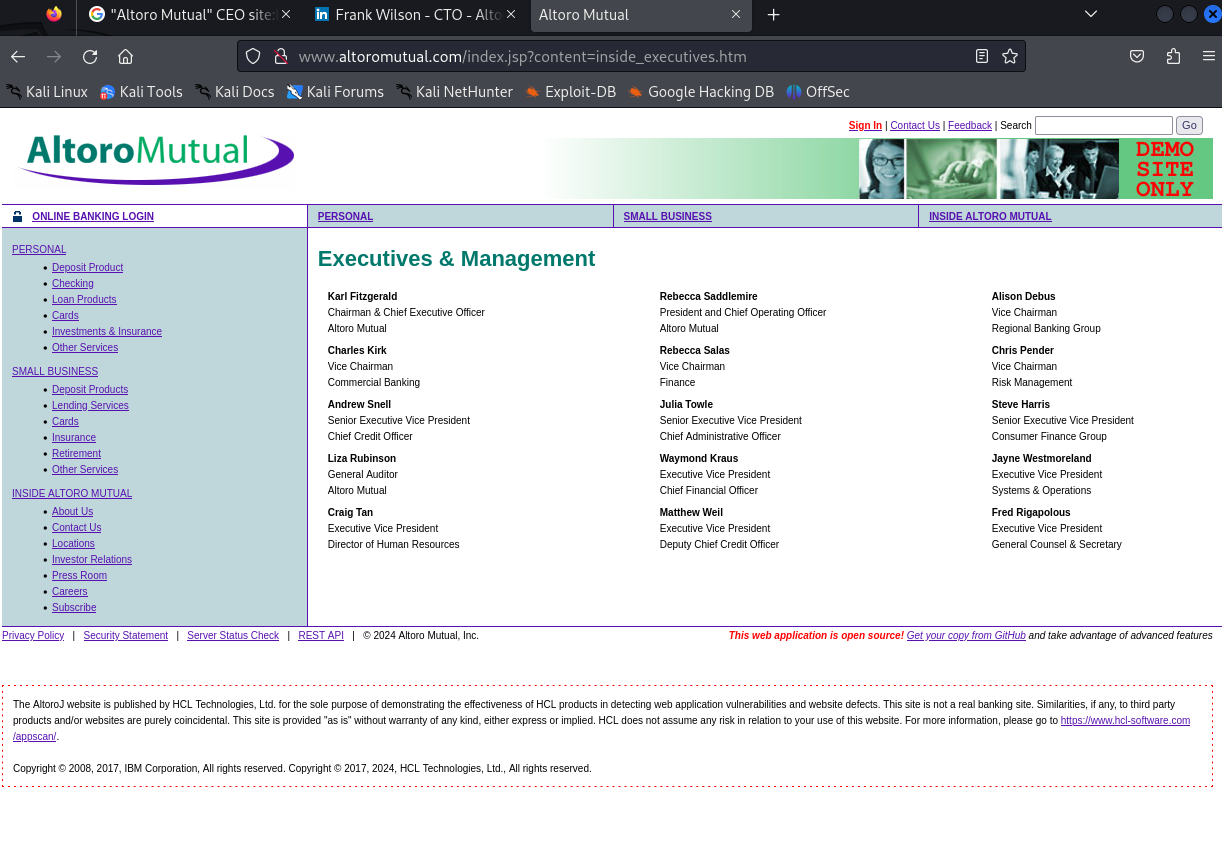
1. Google Dorking

a. Using Google, identify the Chief Executive Officer of Altoro Mutual

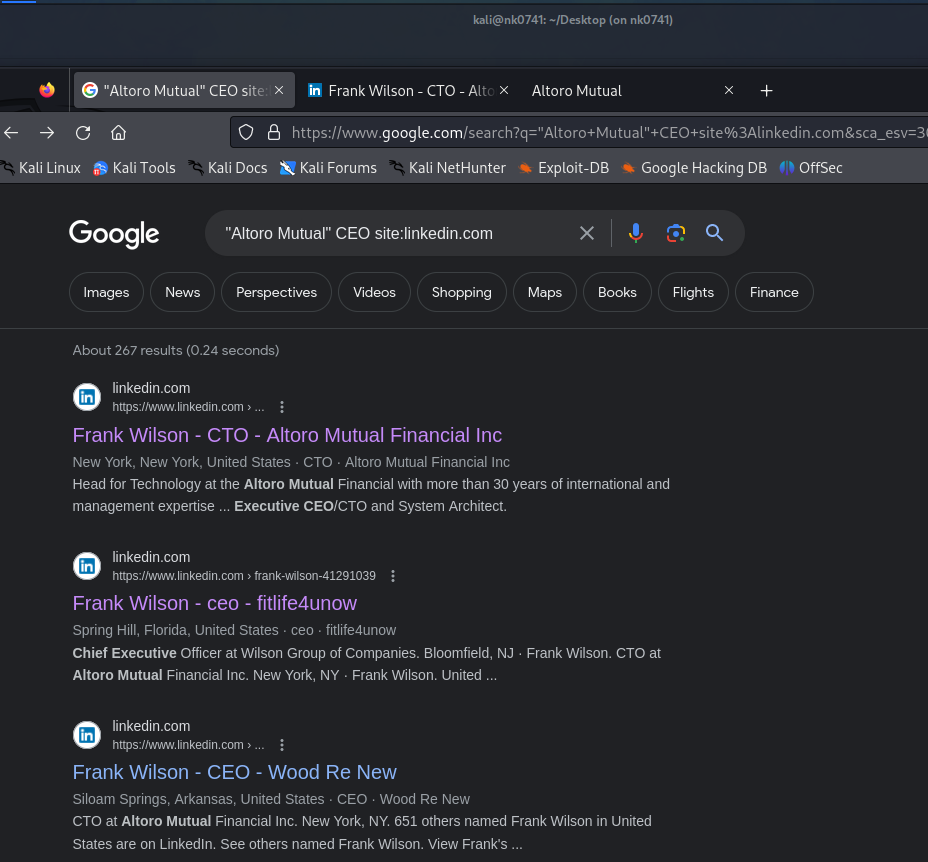
(<http://www.altoromutual.com/>)

From company website: The CEO of Altoro Mutual is Karl Fitzgerald.





Now trying with Linkedin, I couldn’t get the CEO details when I tried using the linkedIn.



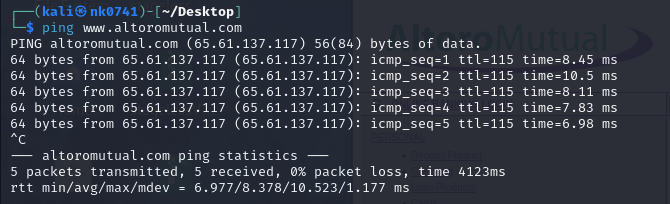
b. How can this information be helpful to an attacker?

The attacker can use this information to spread fall claims about the company damage the image of the company or can trick employee to do things the hacker might need.

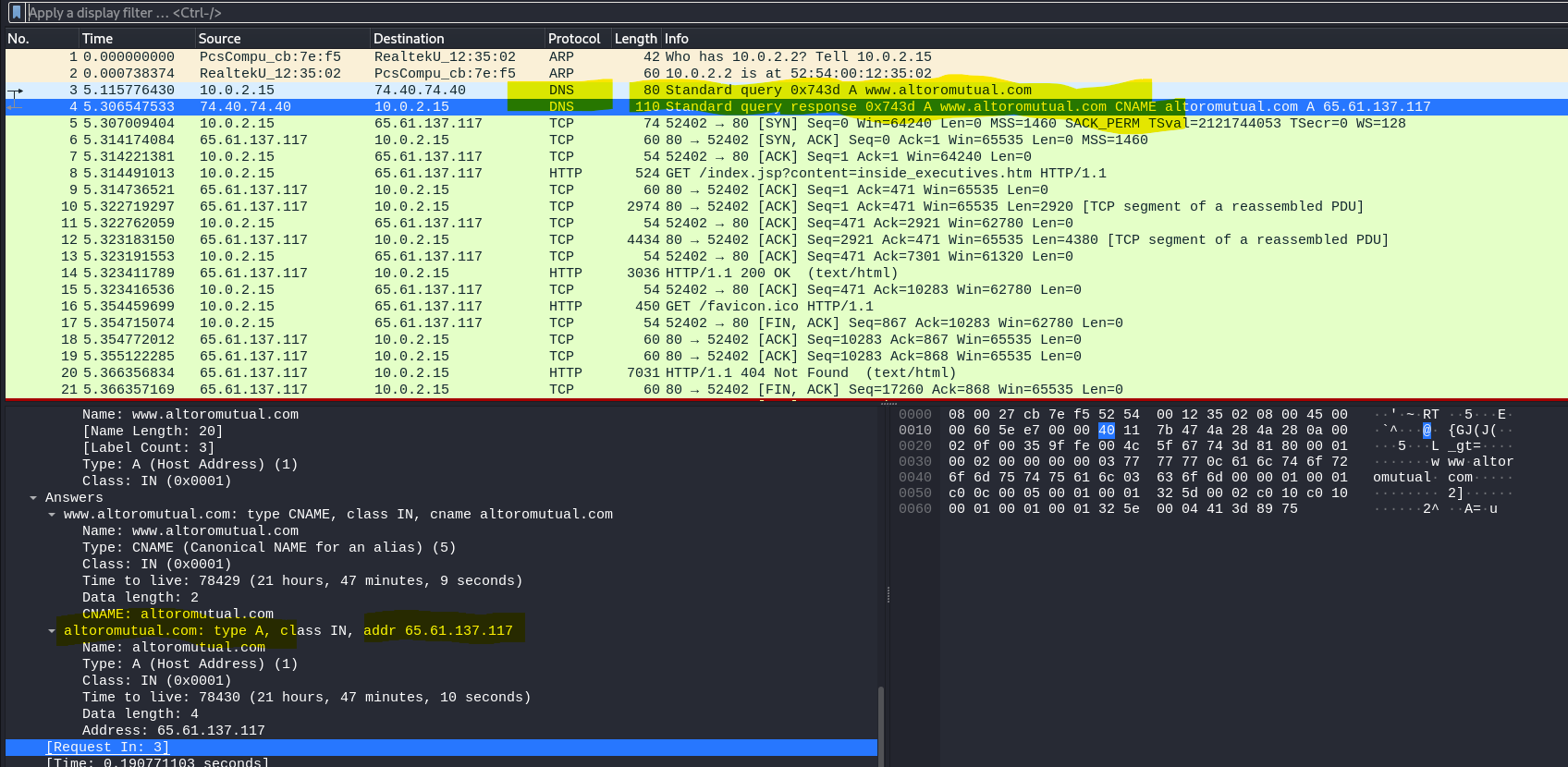
Example: As you can see CEO is not active on Linkedin, the hacker can create fake profile and connect with employees and gather more information and this information can be related to company or employee personal details.

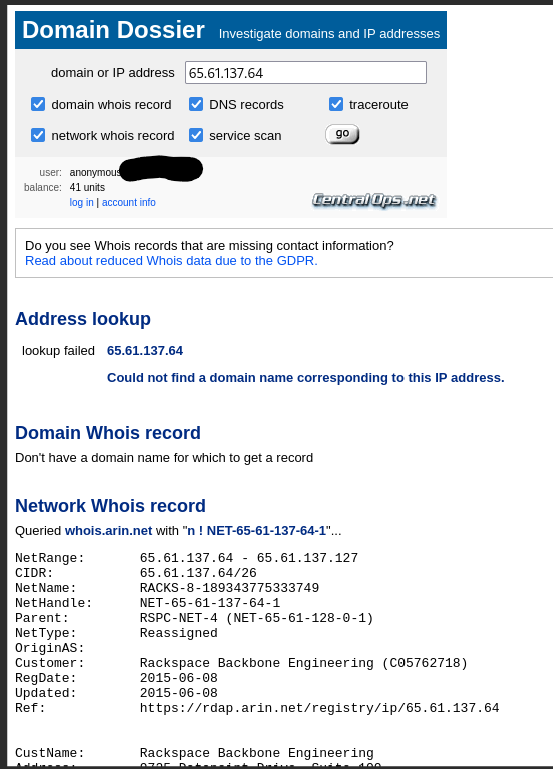
2. What is the IP address for altoromutual.com?

The Ip address I got from ping is 65.61.137.117



Now I used wireshark to get the IP to cross verify the result from ping command. In wireshark, we can see the dns request made by the browser to get the ip of the website and we got the same value in here as well.

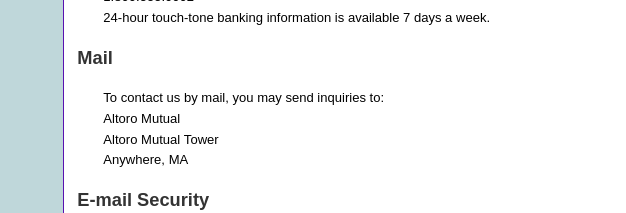




url for above output: <https://centralops.net/co/DomainDossier.aspx?addr=65.61.137.64&dom_whois=true&dom_dns=true&traceroute=true&net_whois=true&svc_scan=true>

i.Where is the company located?

Ans: The information doesn’t provide the location of the company. As the company is fictious we don’t have any real location information. But when we search the website and go through different pages, we can see the company is located in Altoro Mutual tower, Ma.



ii. What NetRange does this hosting environment fall within?

Ans: NetRange: 65.61.137.64 - 65.61.137.127

iii. What company do they use to host their infrastructure and where is it

located?

Ans: Altoro Mutual uses Rackspace to host their infrastructure. Rackspace's location: San Antonio, Texas, United States.

Address: 9725 Datapoint Drive, Suite 100, City: San Antonio, State Prov: TX

3. Shodan

a. Using Shodan (https://www.shodan.io/), what open ports and services are

running on the server hosting altoromutual.com?

Ans:

The ports 80,443,8080 are open on altoromutual.com 