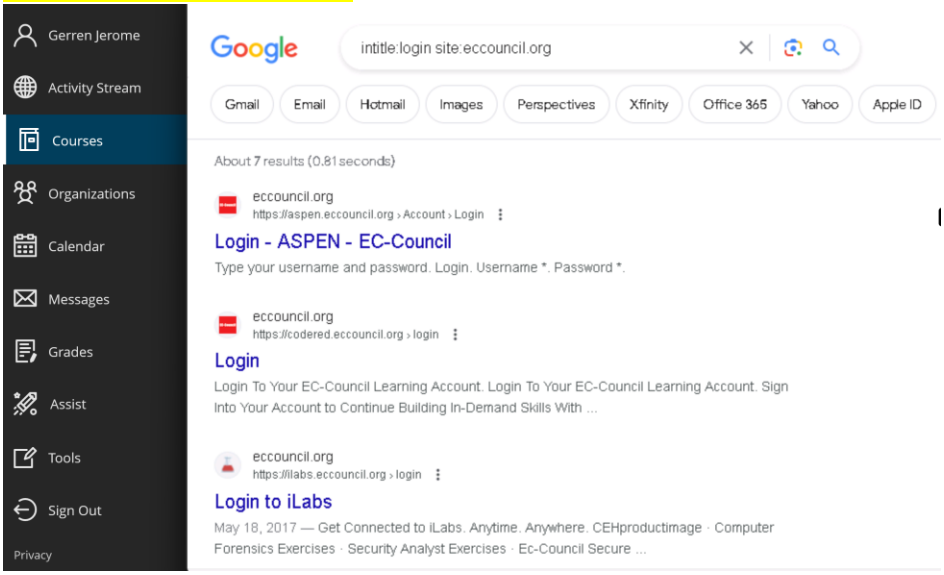
Gerren Jerome

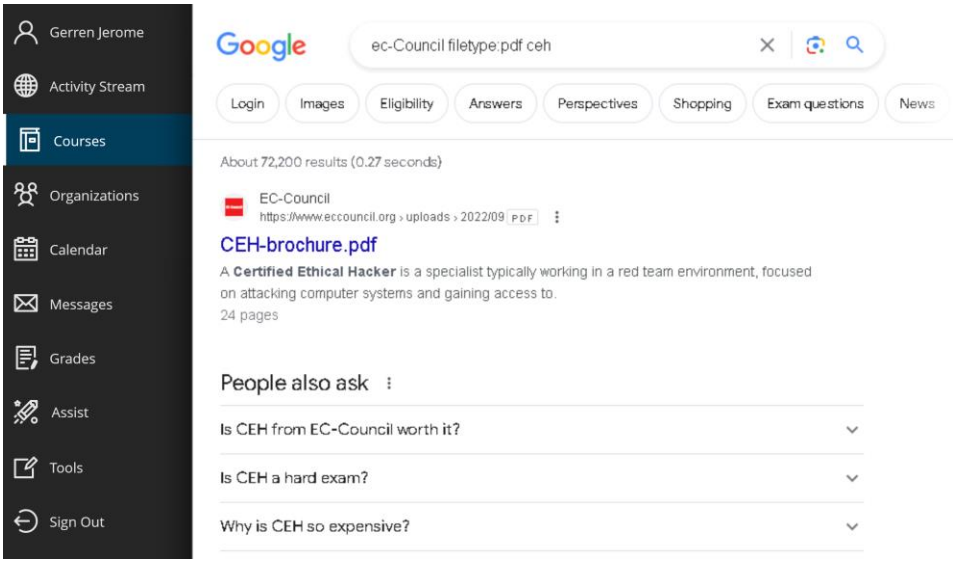
Footprinting and Reconnaissance

Perform footprinting through search engines.
Gather information using advanced Google hacking techniques.

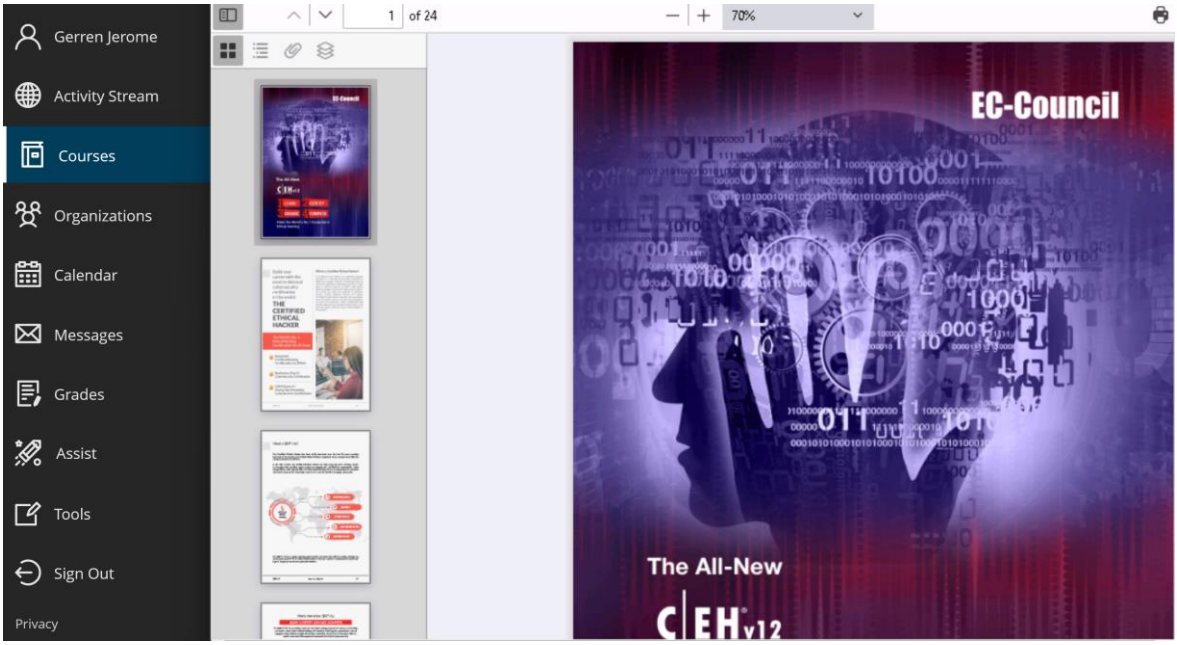
ECCouncil intitle login search



Find ECC pdfs related to the CEH program.



CEH-brochure.pdf

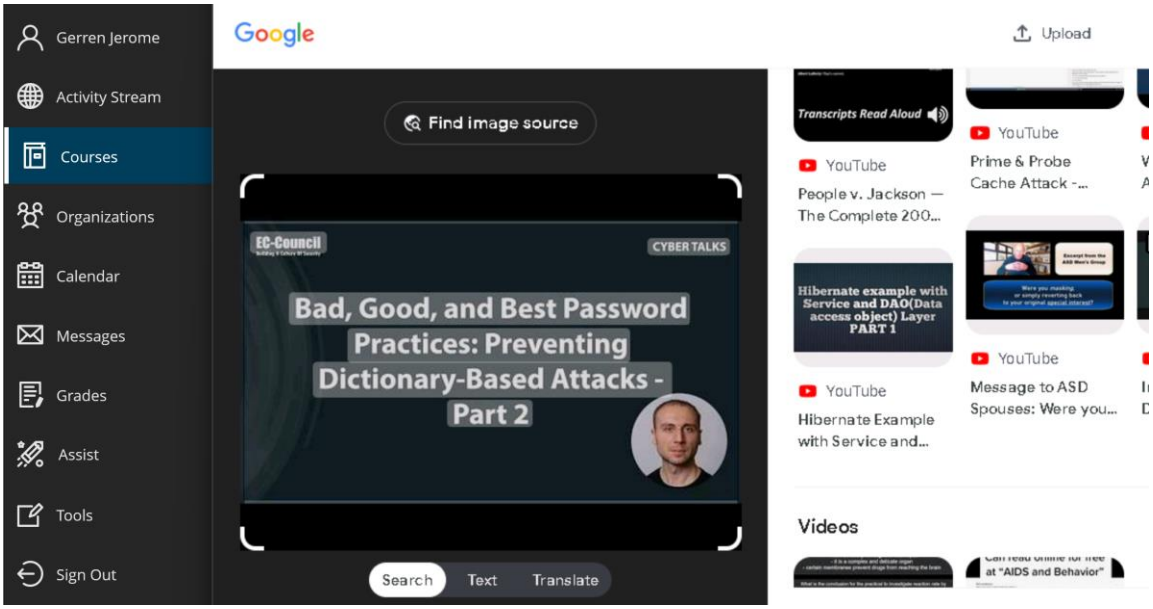


Gather information from video search engines.

http://www.youtube.com/watch?v=f_iVuHgCToA&pp=ygUKZWMtY291bmNpbA%3D%3D

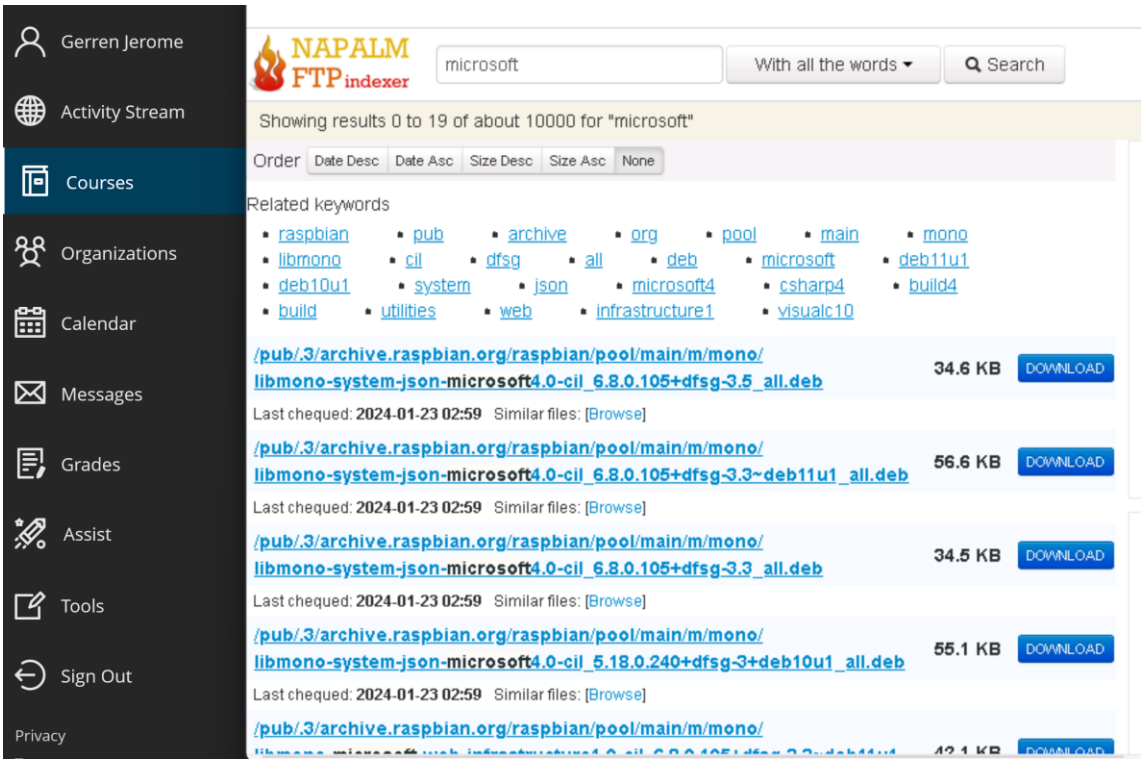
The mattw.io Snippet section

Reverse Image Search



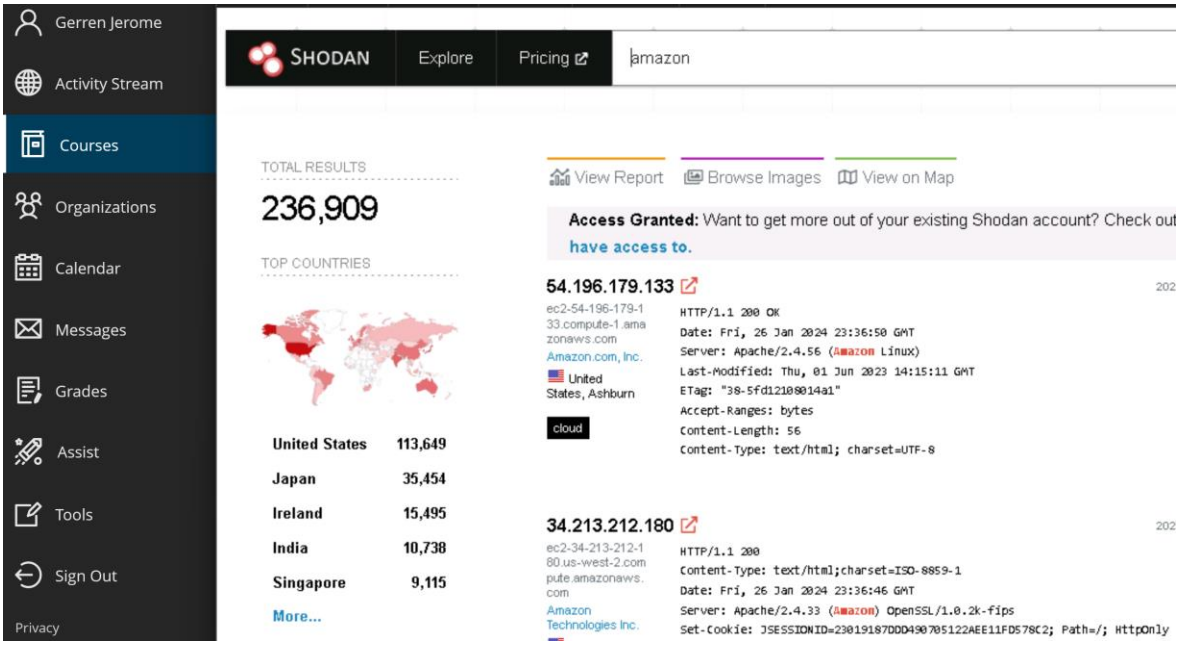
Gather information from FTP search engines.

NAPALM-FTP search results.



Gather information from IoT search engines.

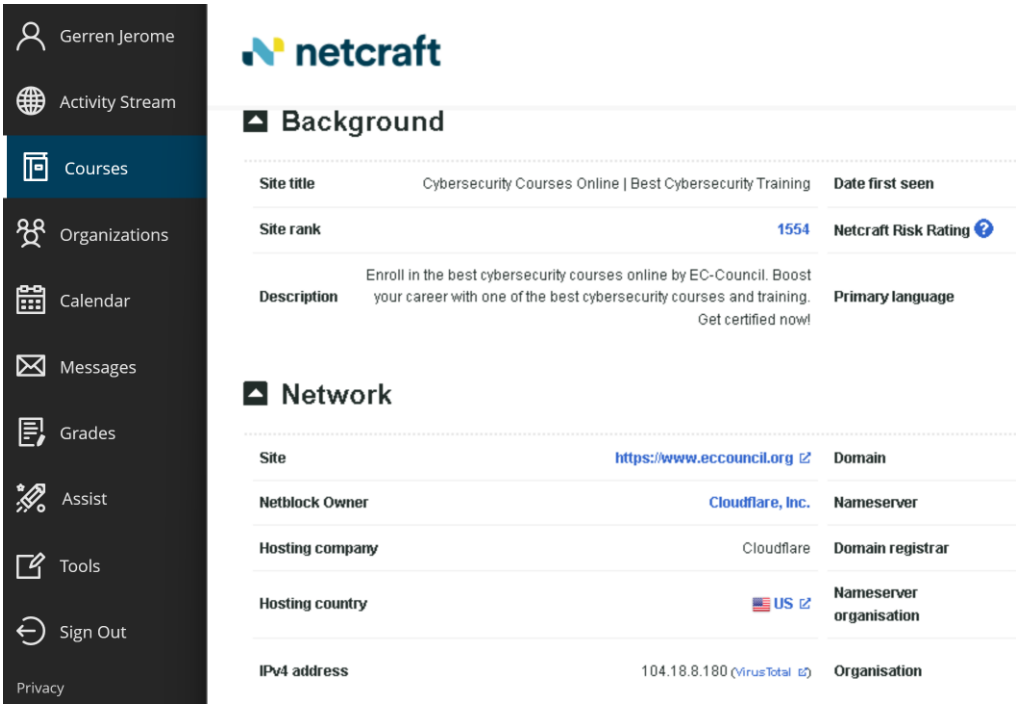
shodan.io search results.



Perform footprinting through web services.

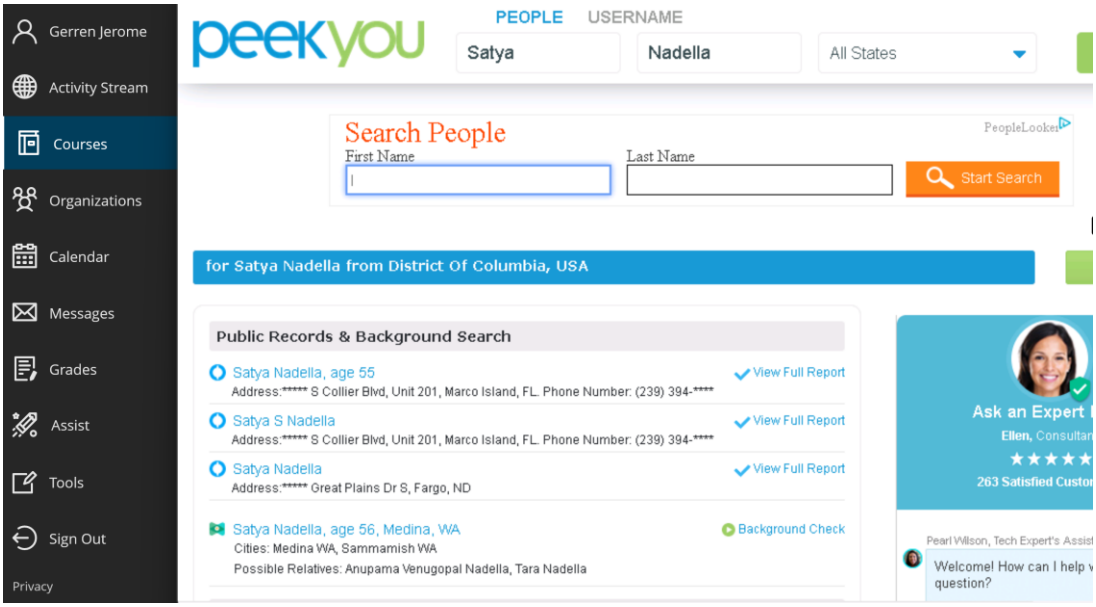
Find the company's domains and sub-domains using Netcraft.

Netcraft site report



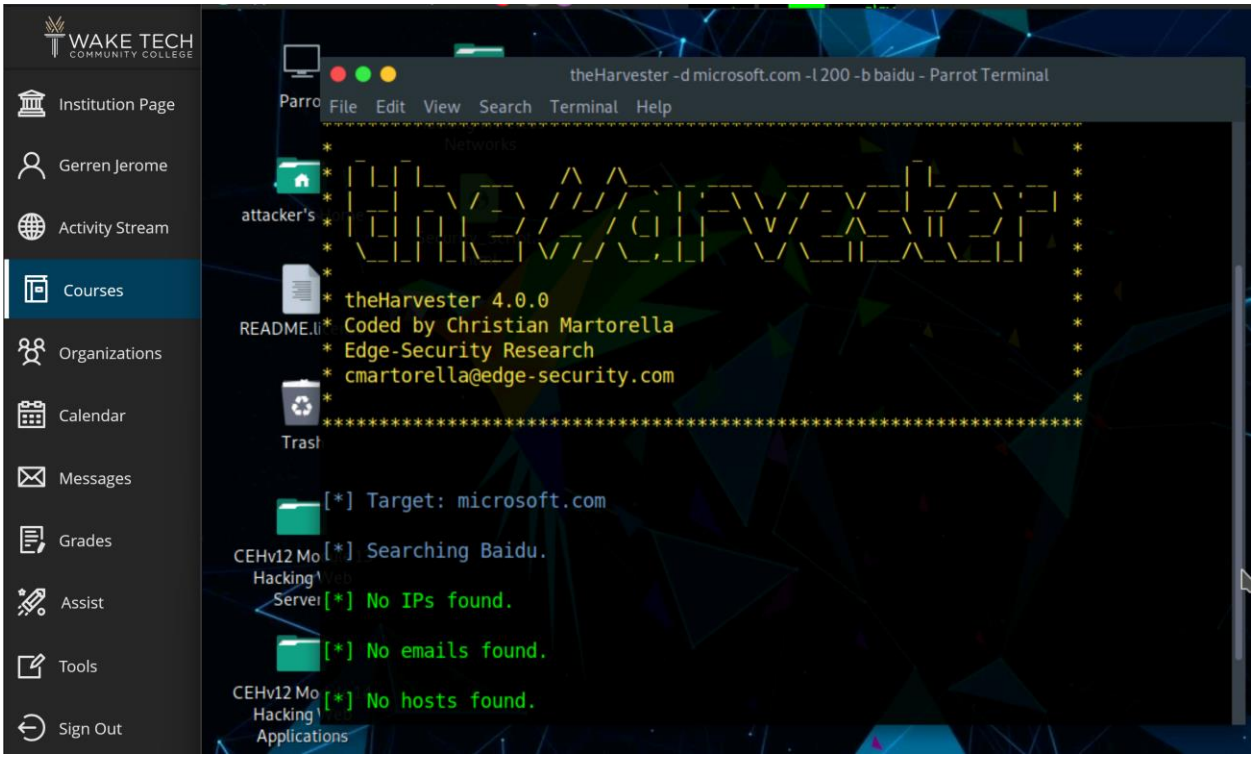
Gather personal information using PeekYou online people search service.

PeekYou search results



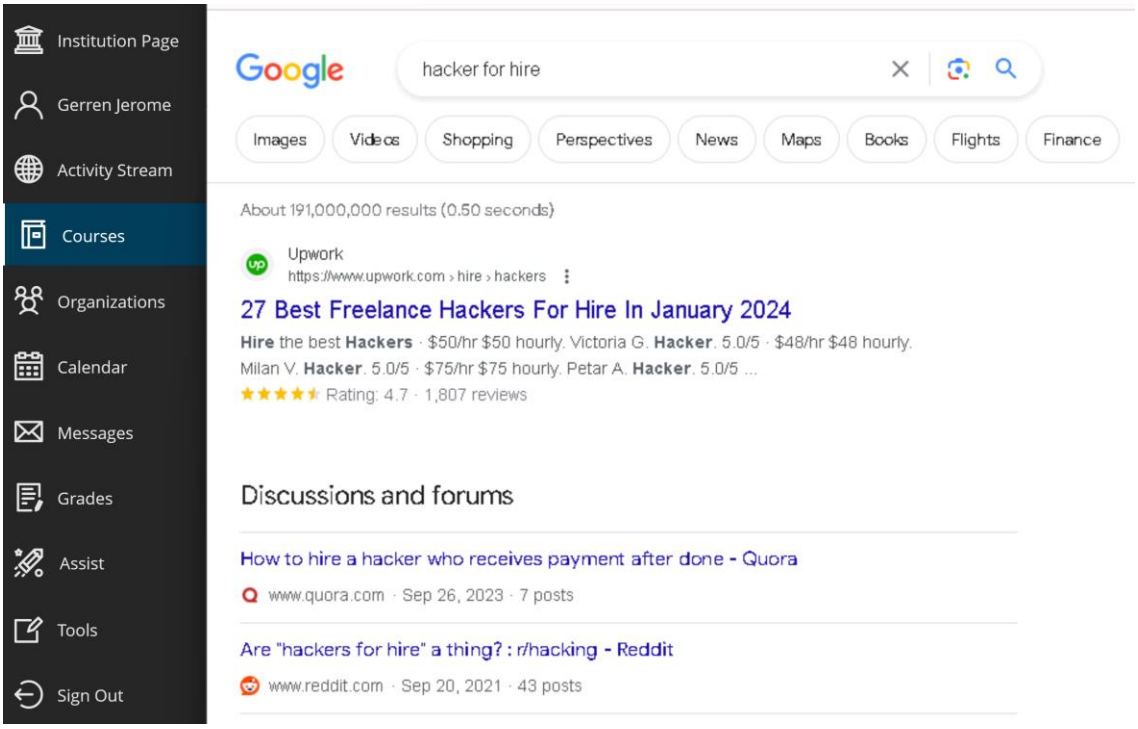
Gather an email list using theHarvester

theHarvester search results



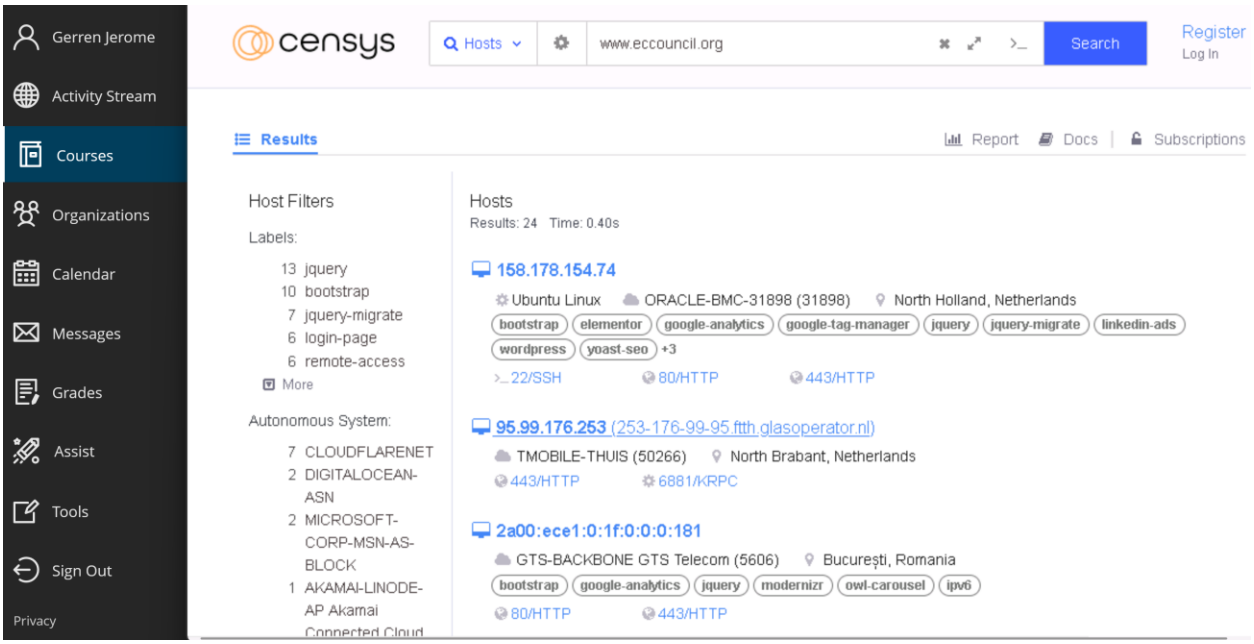
Gather information using deep and dark web searching.

Google search results



Determine target OS through passive footprinting

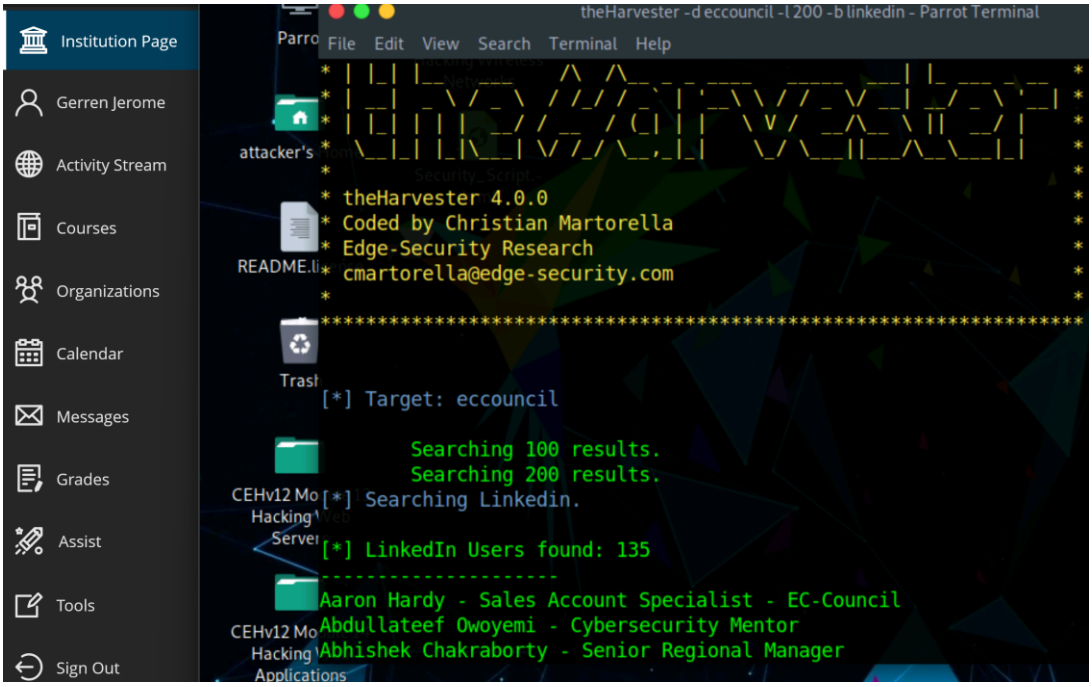
Censys search results



Perform footprinting through social networking sites.

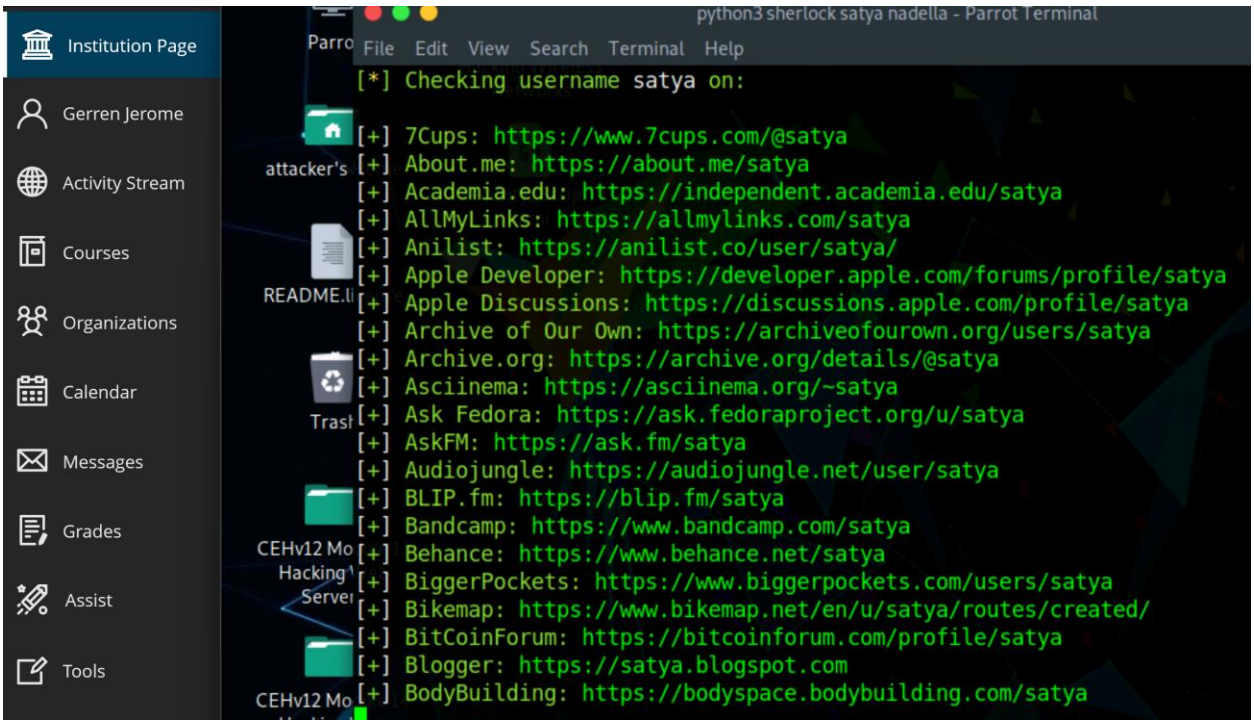
Gather employees' information from LinkedIn using theHarvester

theHarvester search results



Gather personal information from various social networking sites using Sherlock

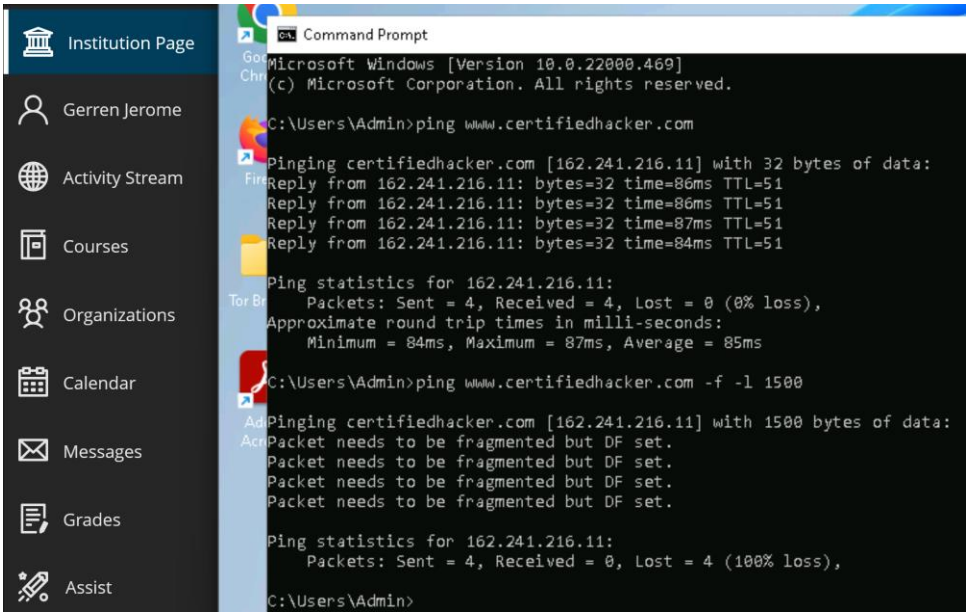
Sherlock search results



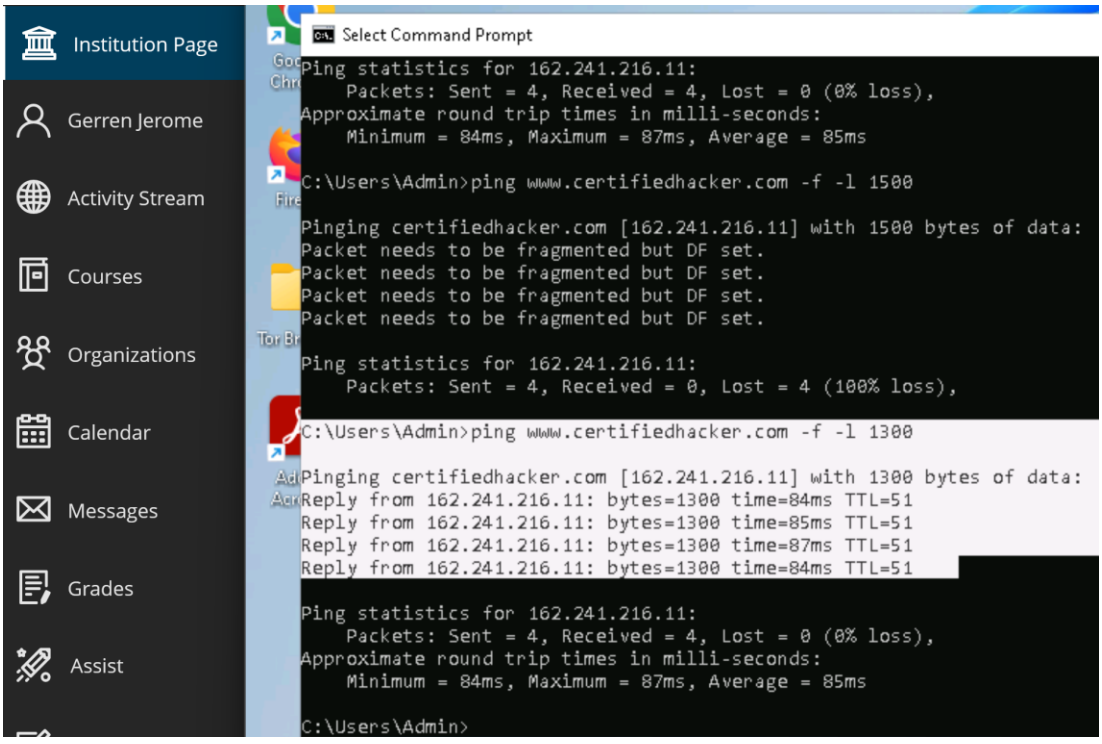
Perform website footprinting

Gather information about a target website using ping command line utility.

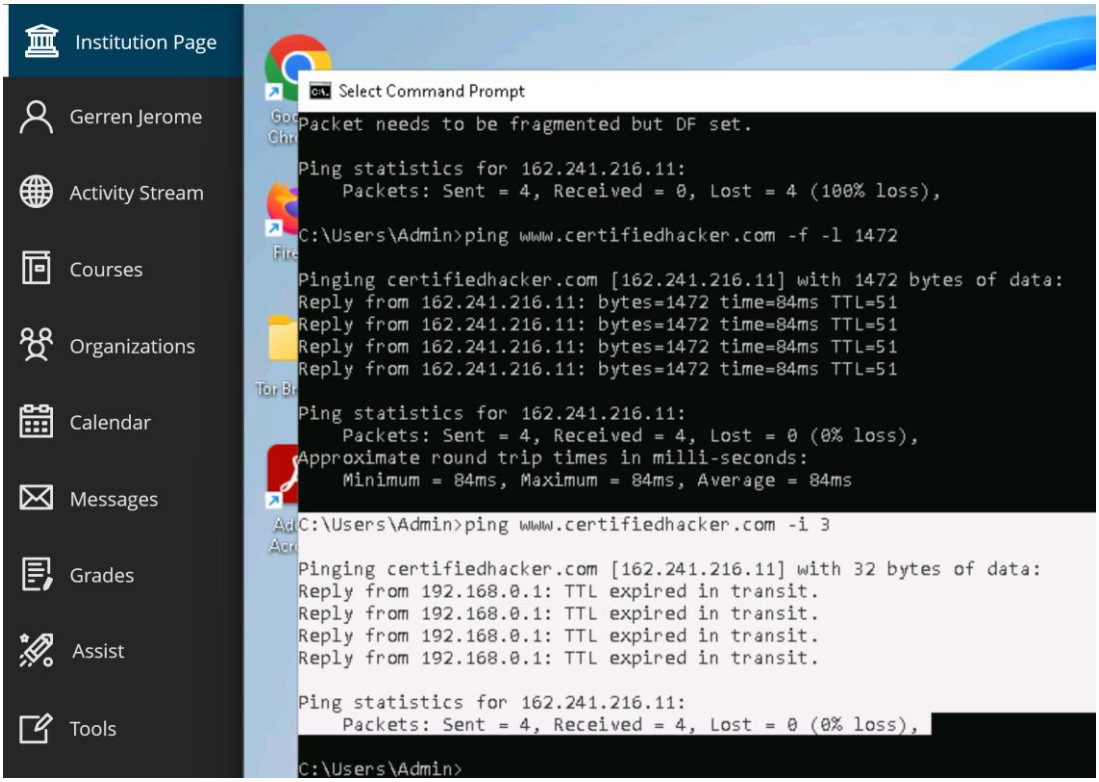
finding the frame limit 1



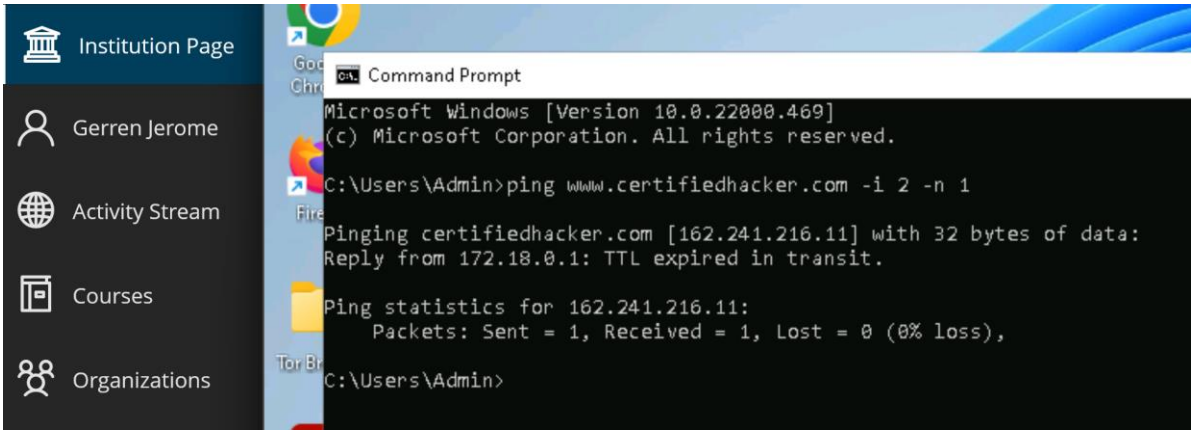
finding the frame limit 2



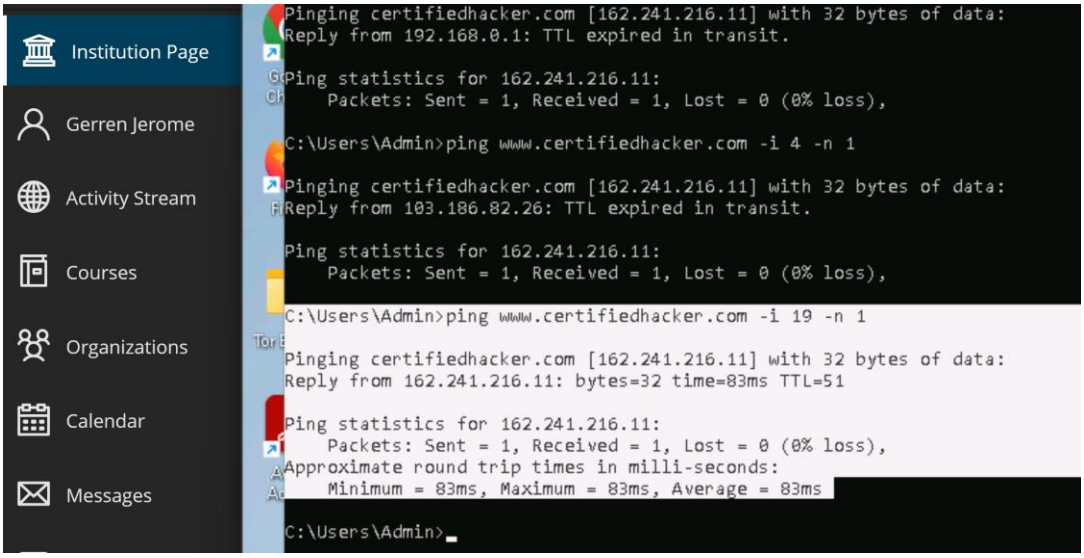
TTL manipulation



ping packet lifespan.

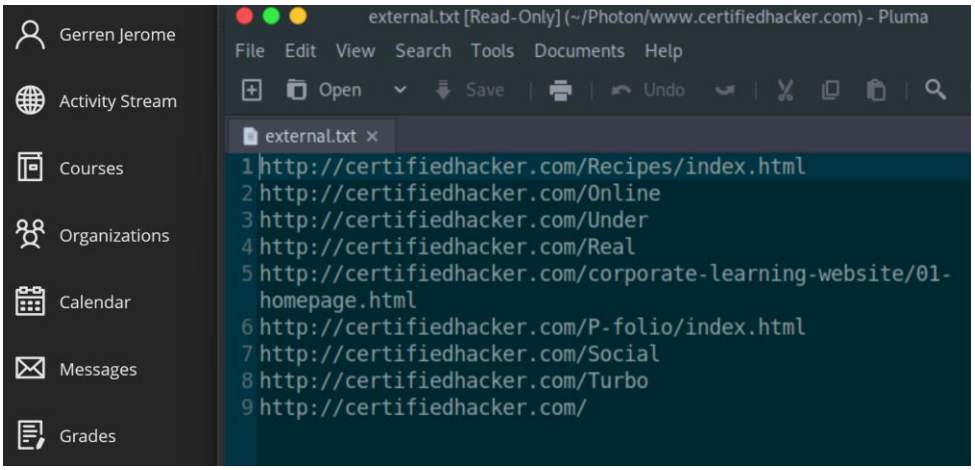


find the hop.

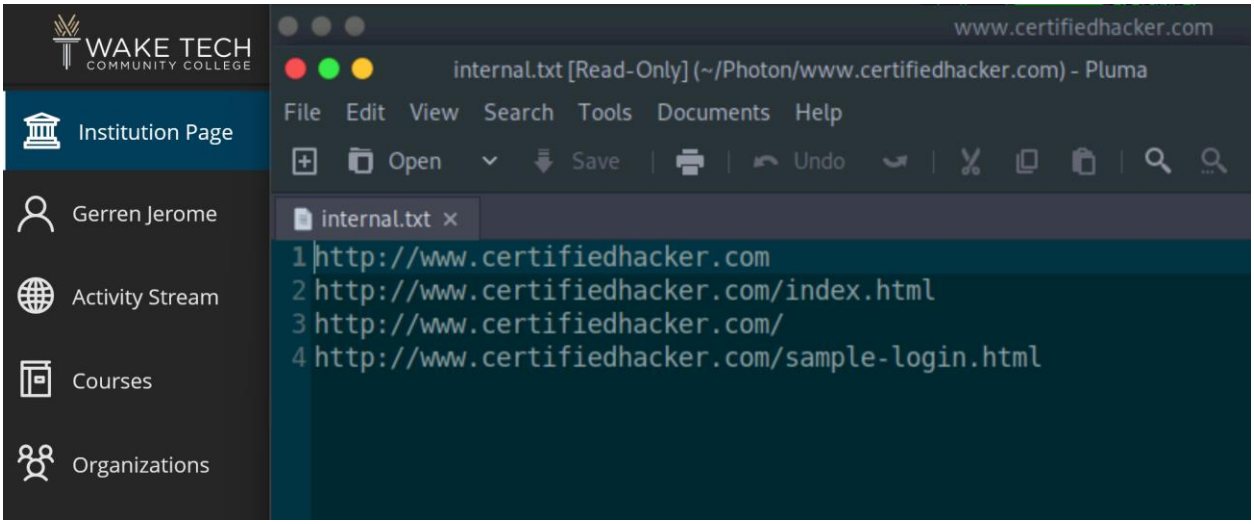


Gather information about a target website using Photon

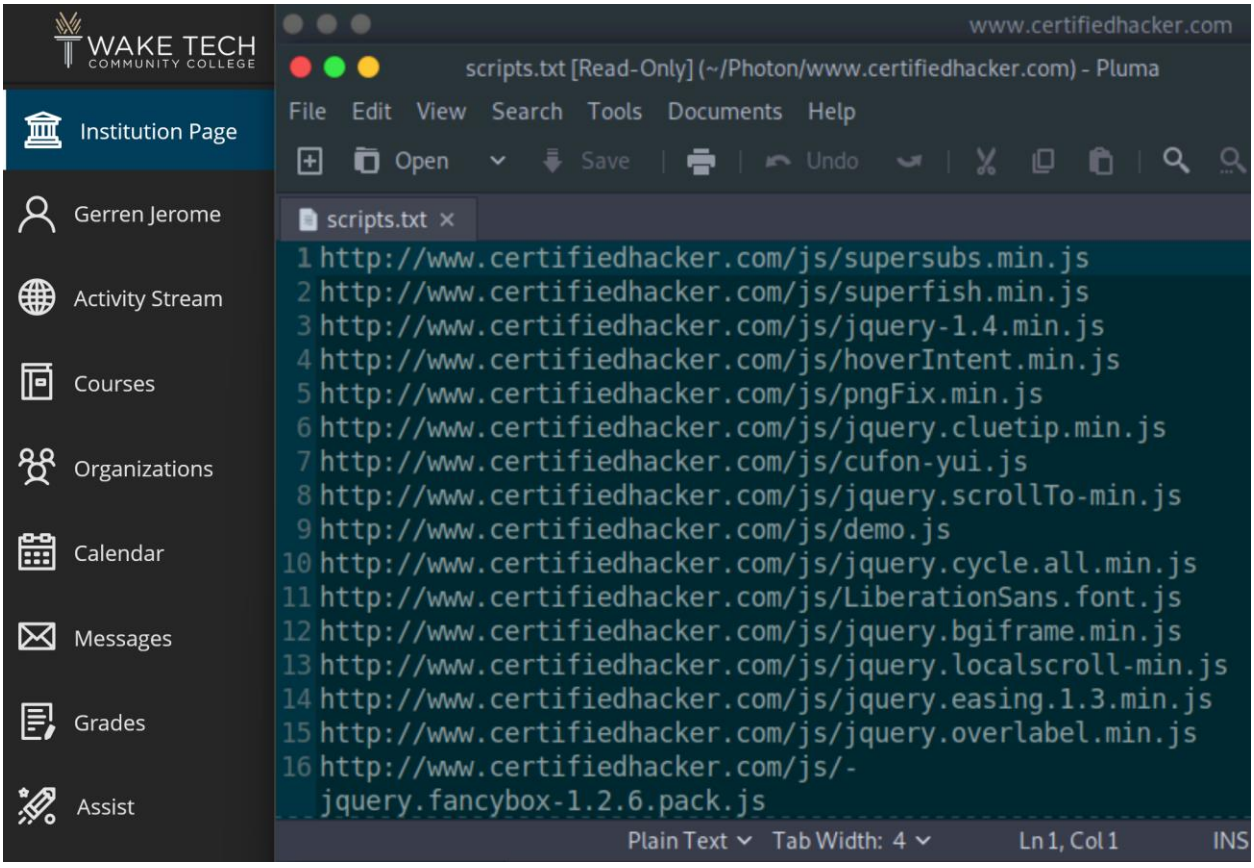
Photon results – external



Photon results – internal

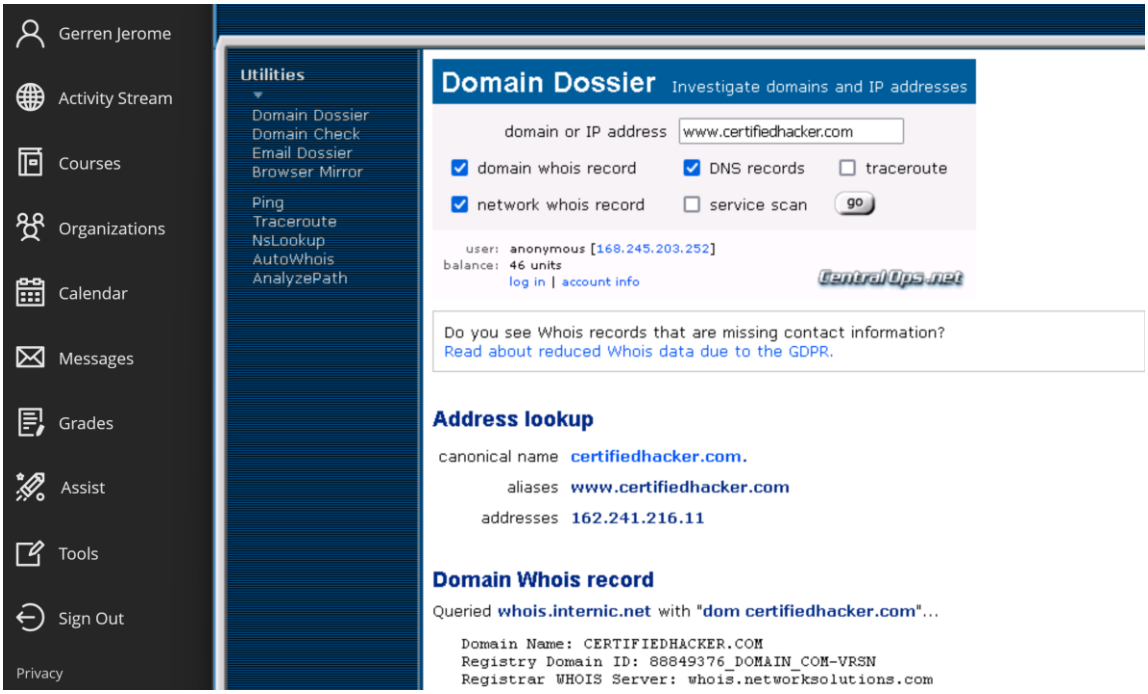


Photon results – scripts



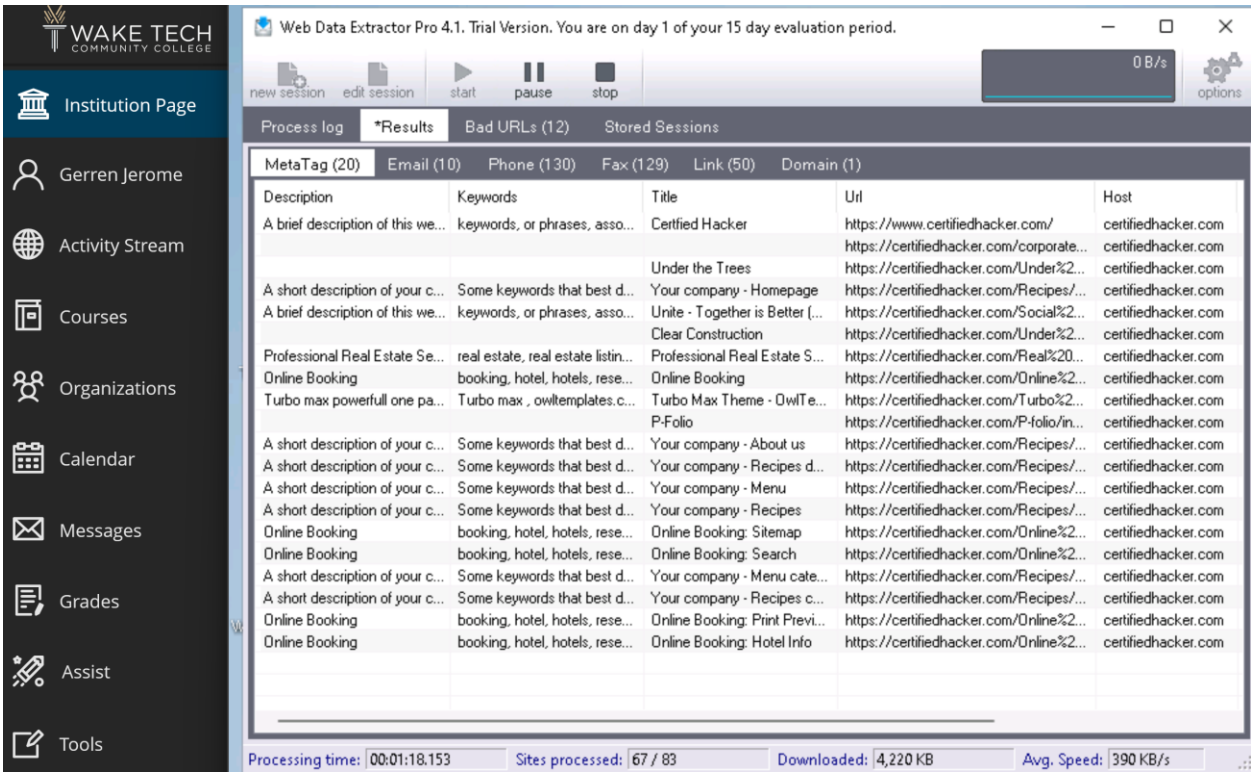
Gather information about a target website using Central Ops

CentralOps results



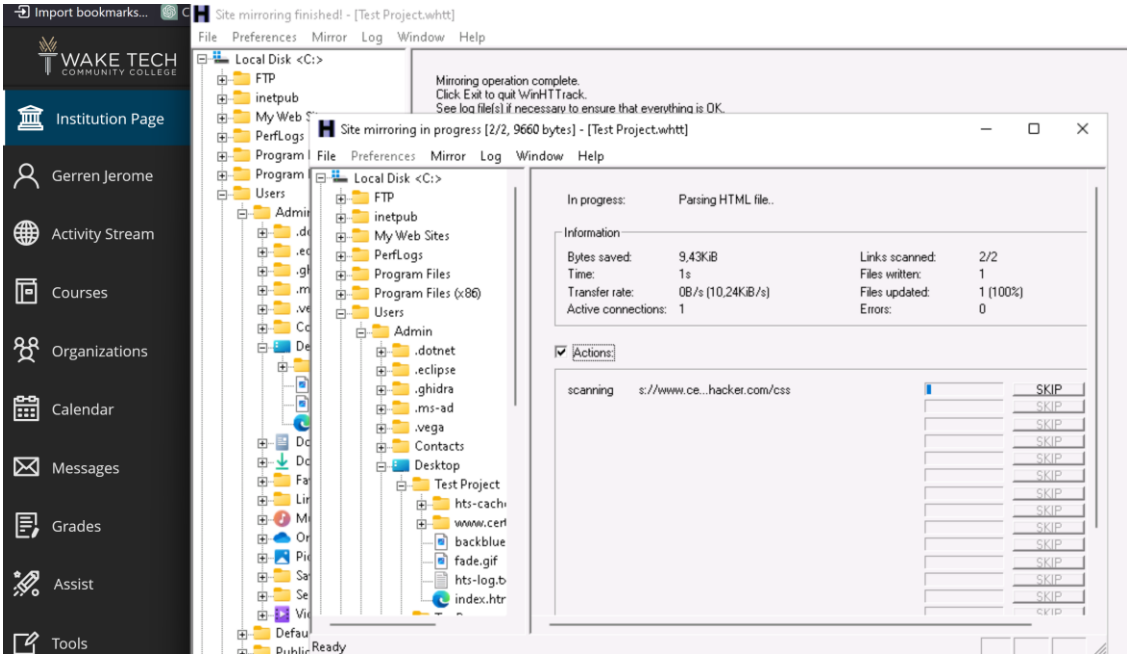
Extract a company's data using Web Data Extractor

WEDPro results

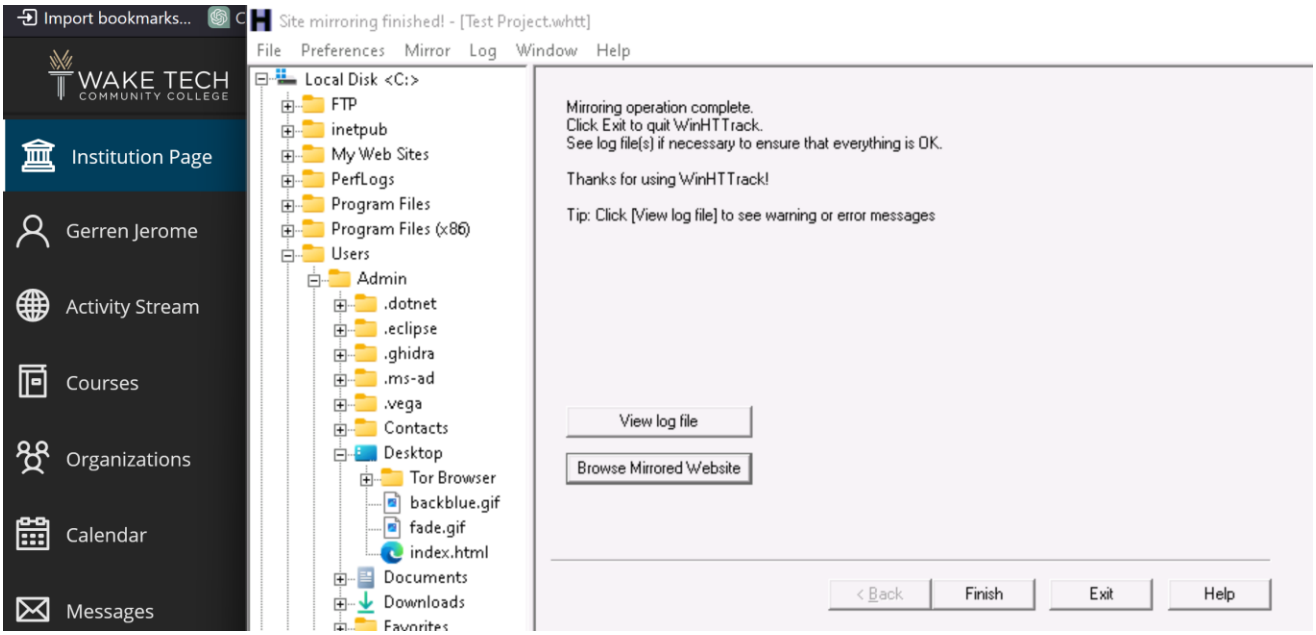


Mirror a target website using HTTrack Web Site Copier

Site mirroring progress

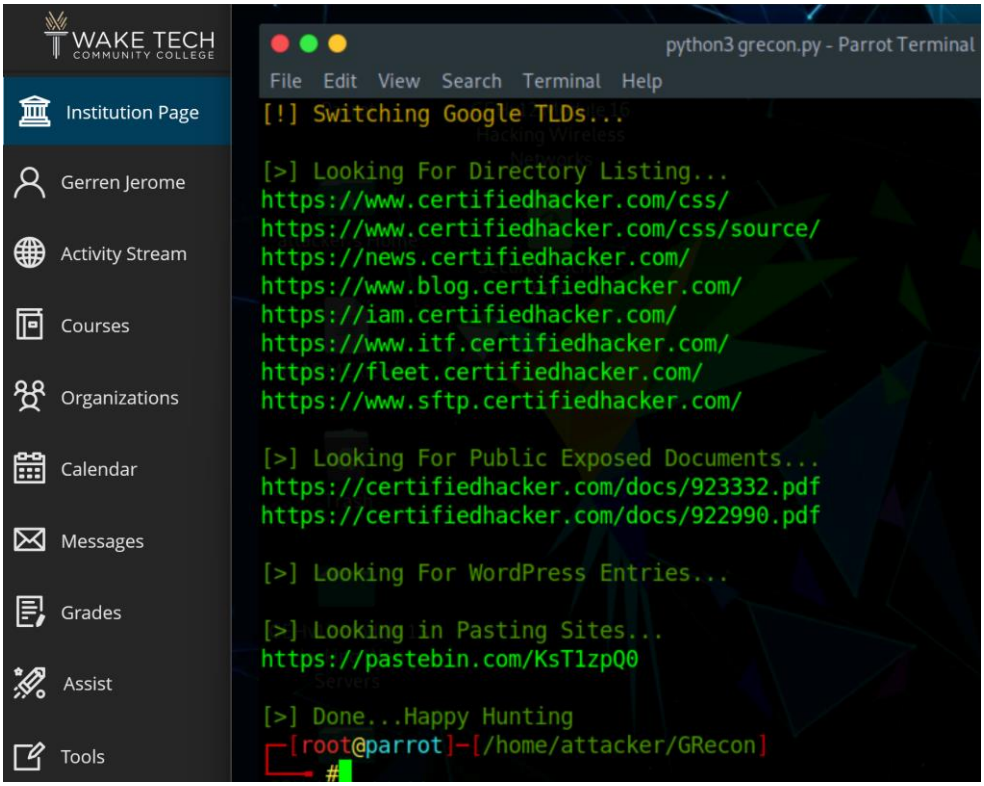


Completed mirroring results.



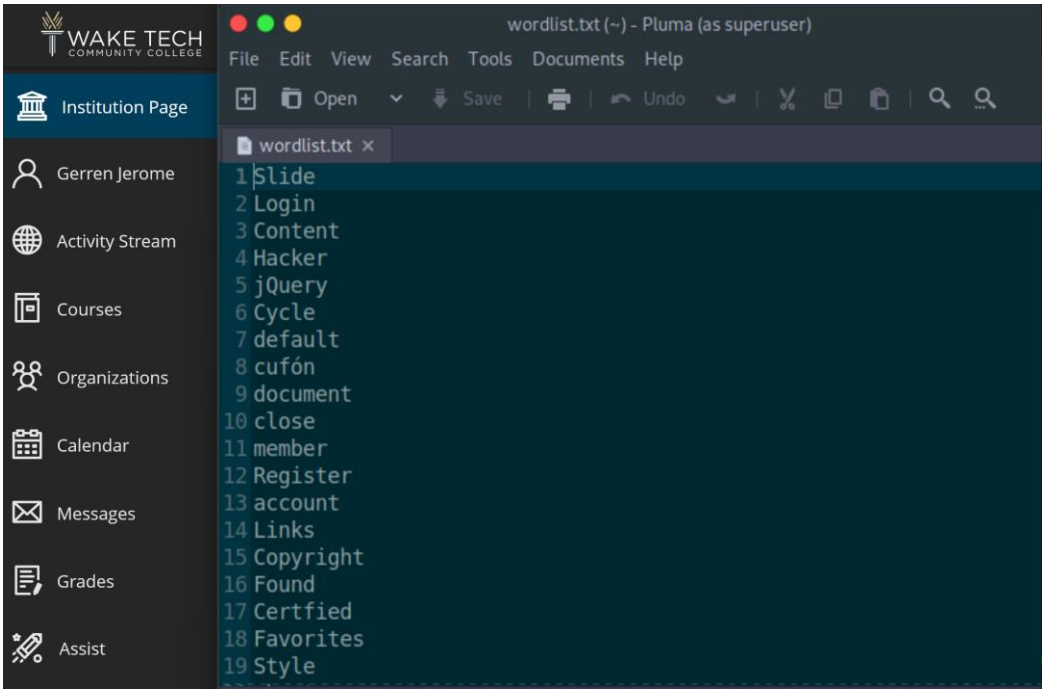
Gather information about a target website using GRecon

GRecon results



Gather a wordlist from the target website using CeWL

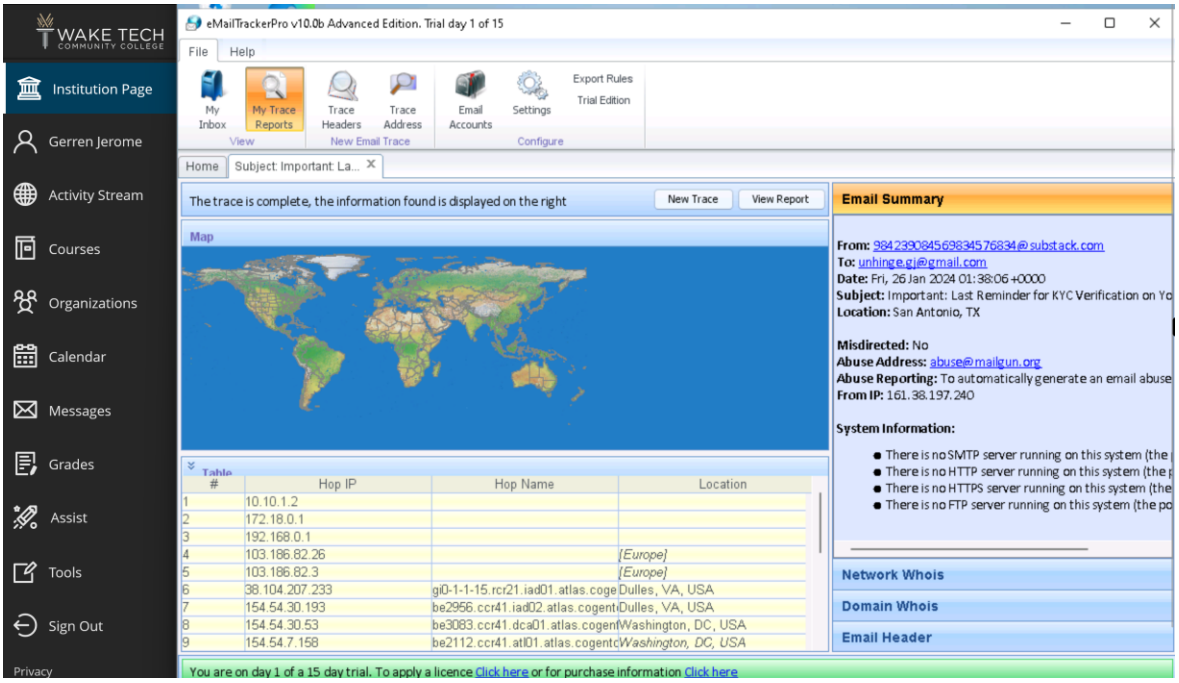
Wordlist output from CeWL



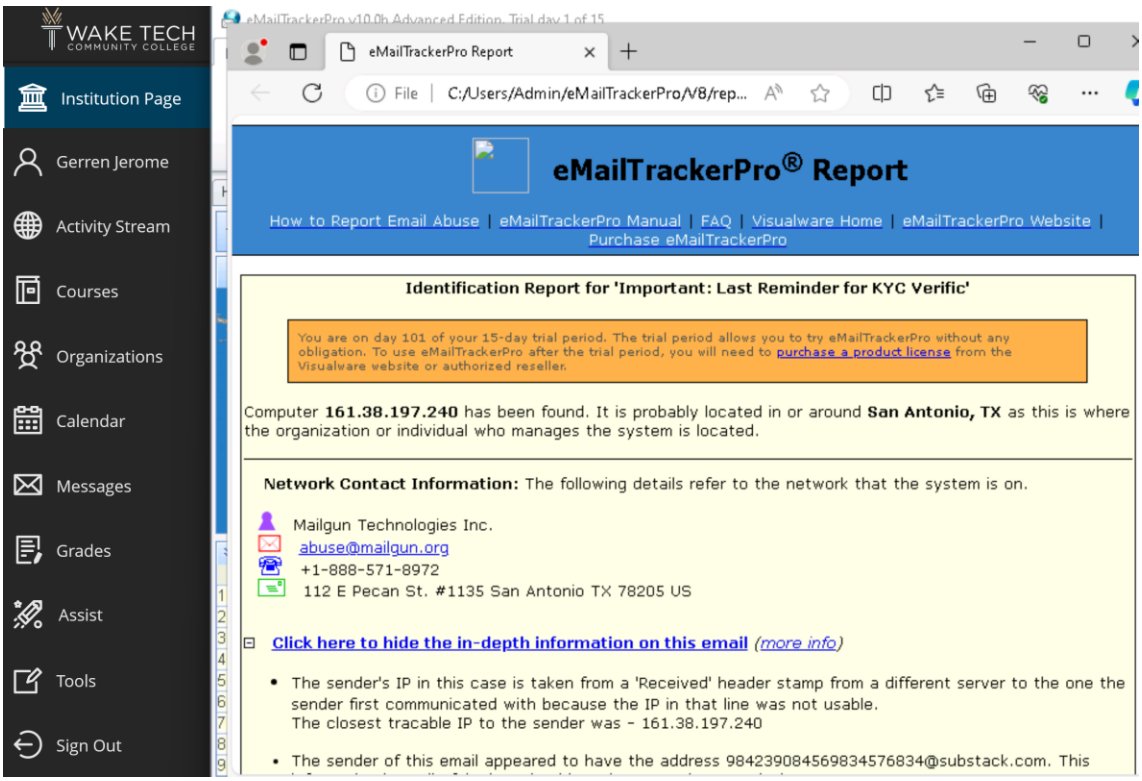
Perform email footprinting

Gather information about a target by tracing emails using eMailTrackerPro

Tracing email header (Map and Summary)



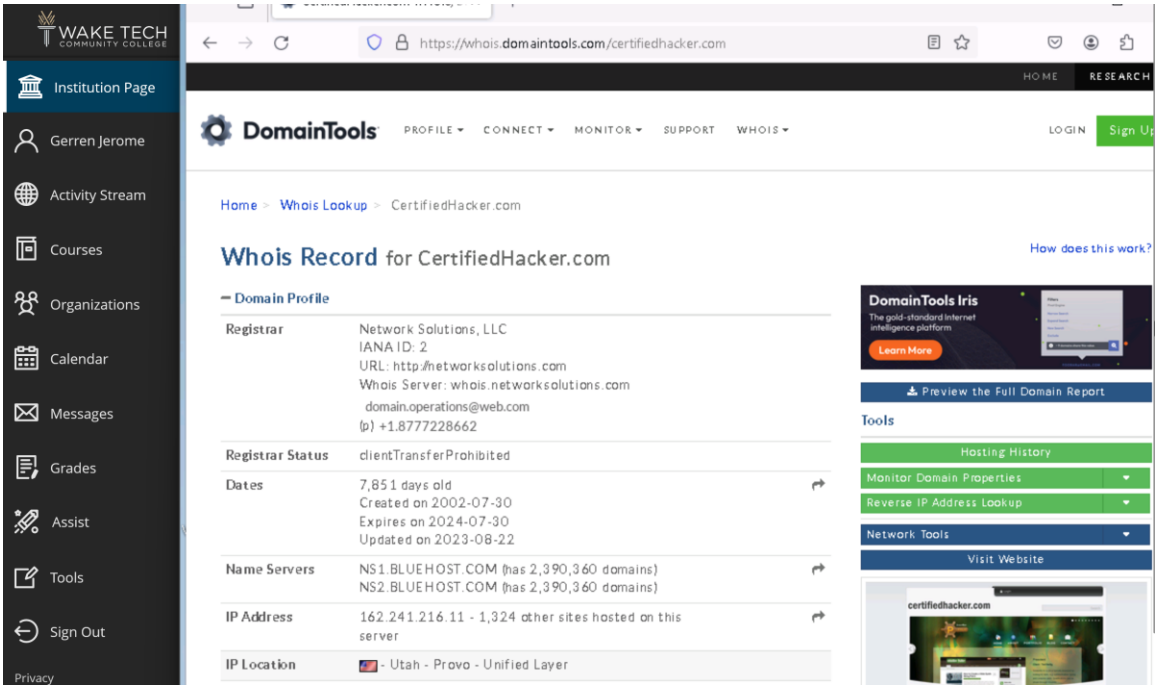
Tracing email header (Report)



Perform Whois footprinting

Perform Whois lookup using DomainTools

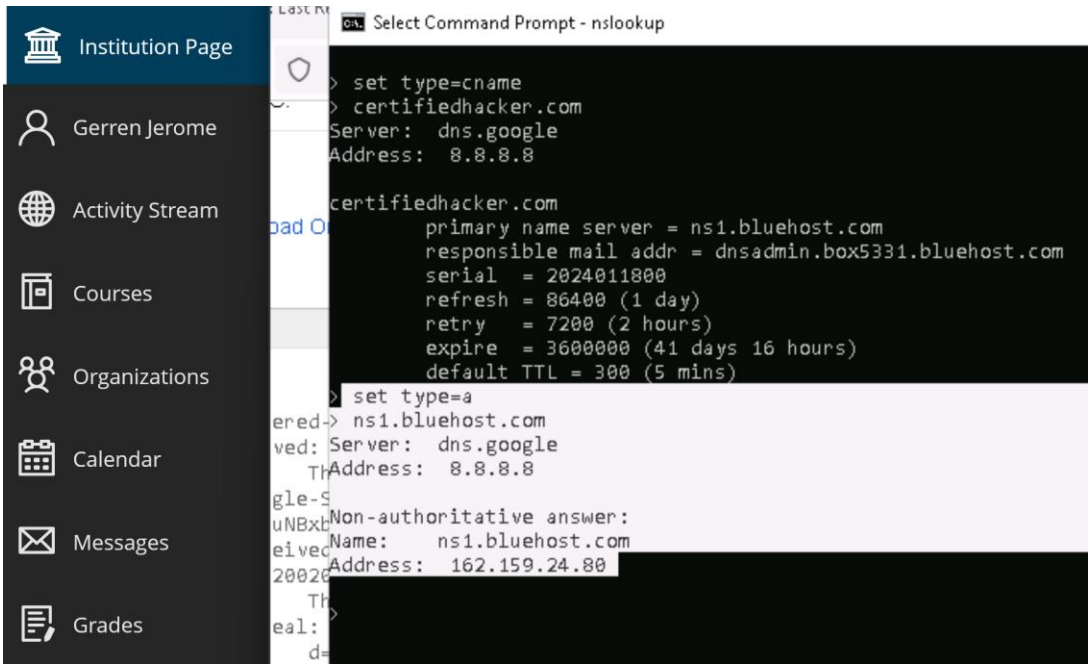
WHOIS Records



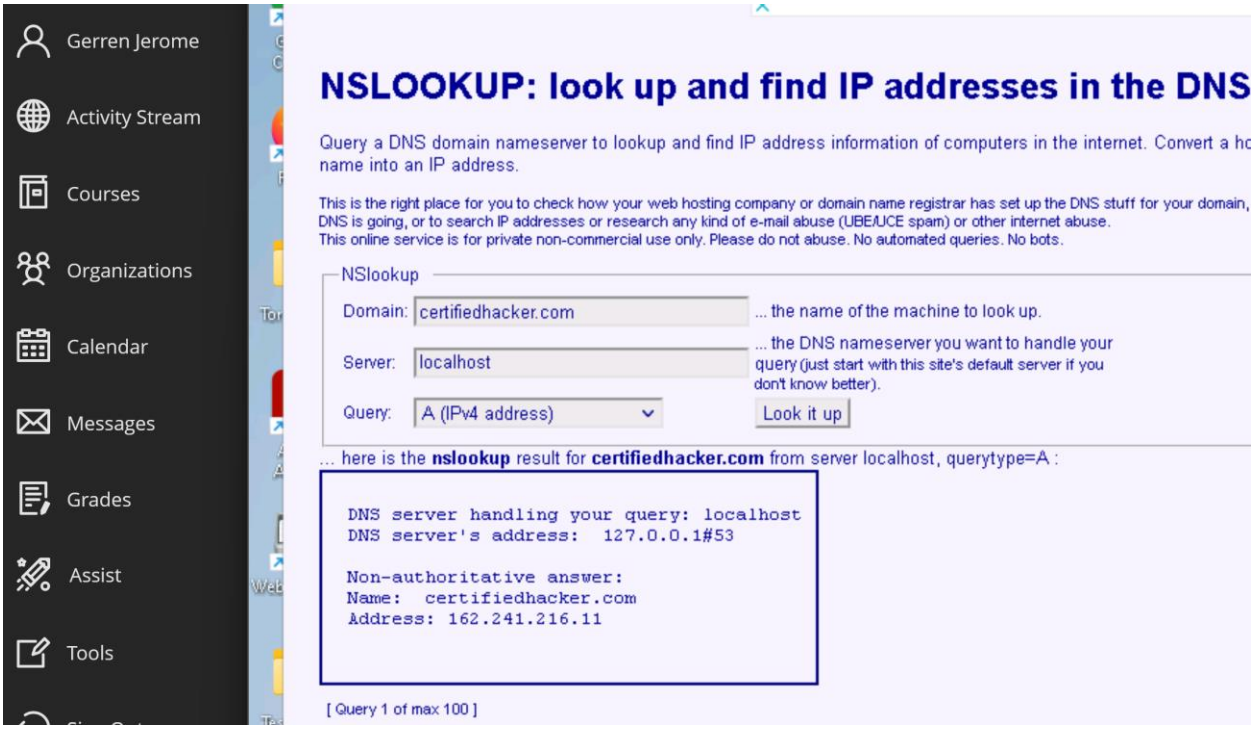
Perform DNS footprinting

Gather DNS information using nslookup command line utility and online tool.

DNS recon with nslookup

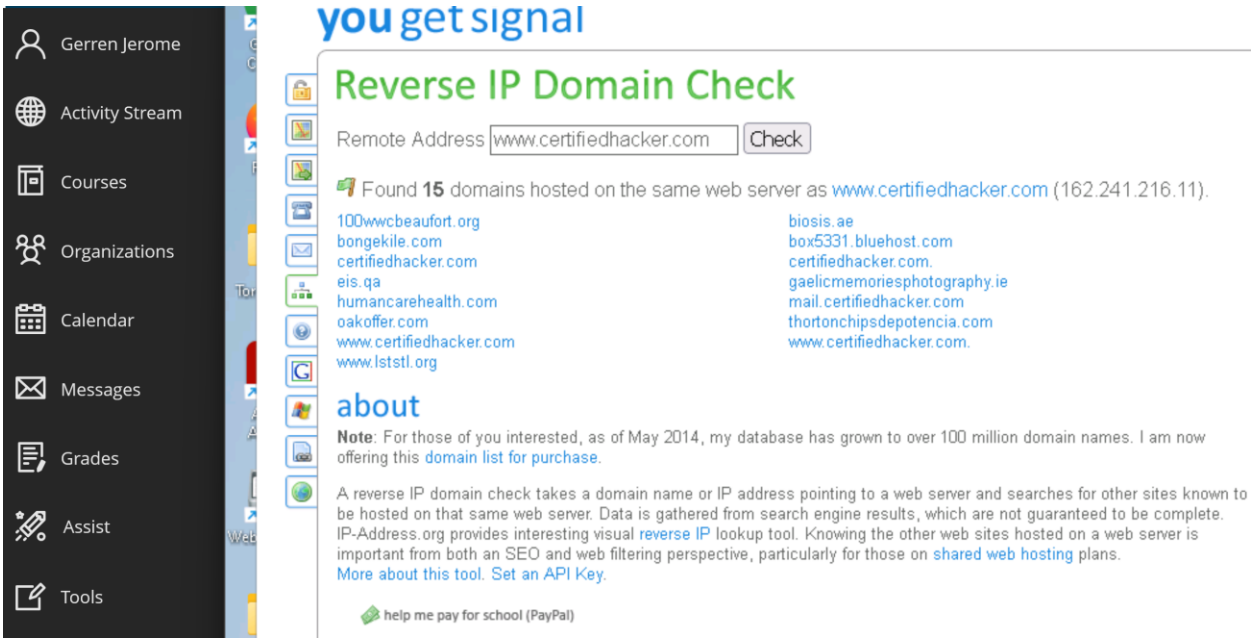


KLOTH.NET results.

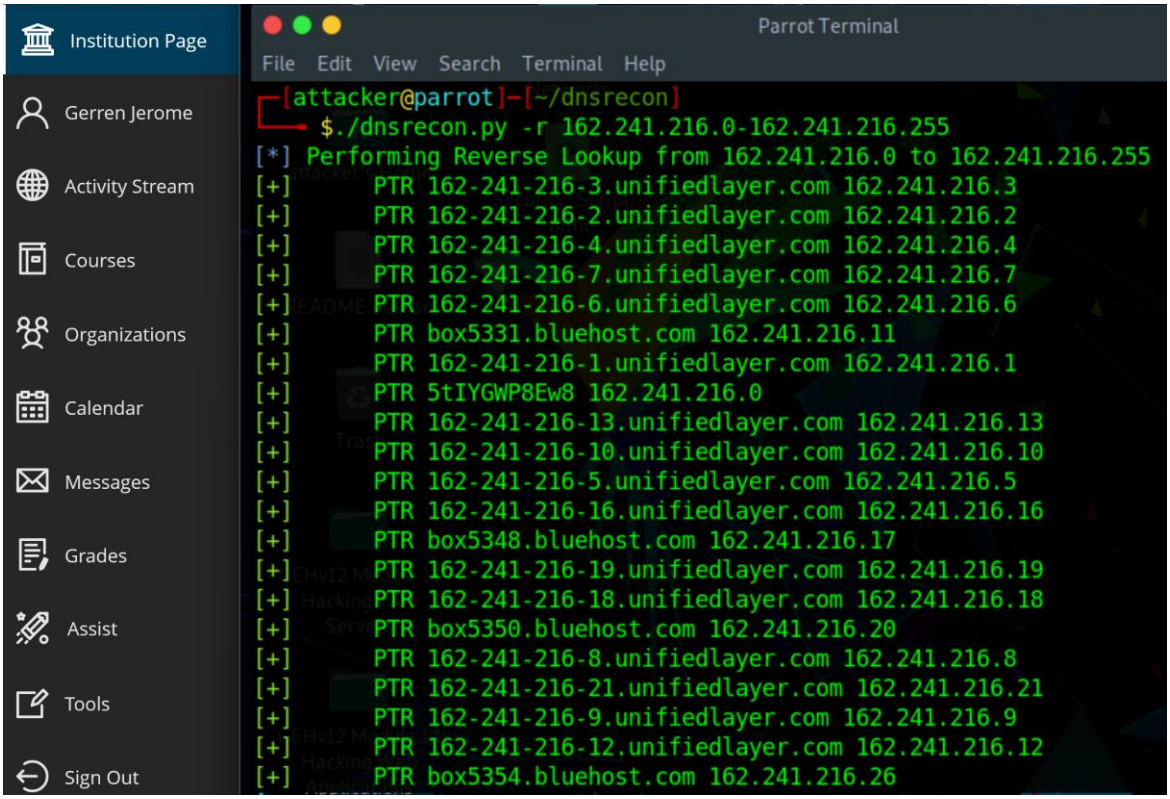


Perform reverse DNS lookup using reverse IP domain check and DNSRecon

yougetsignal.com results.

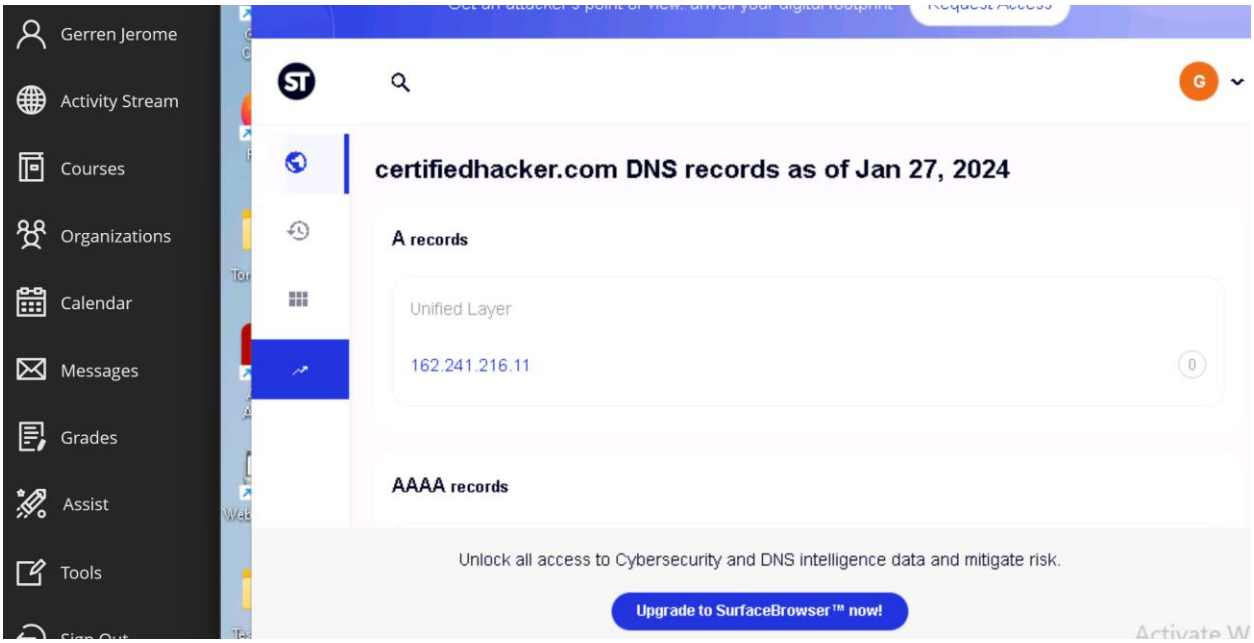


DNSRecon results

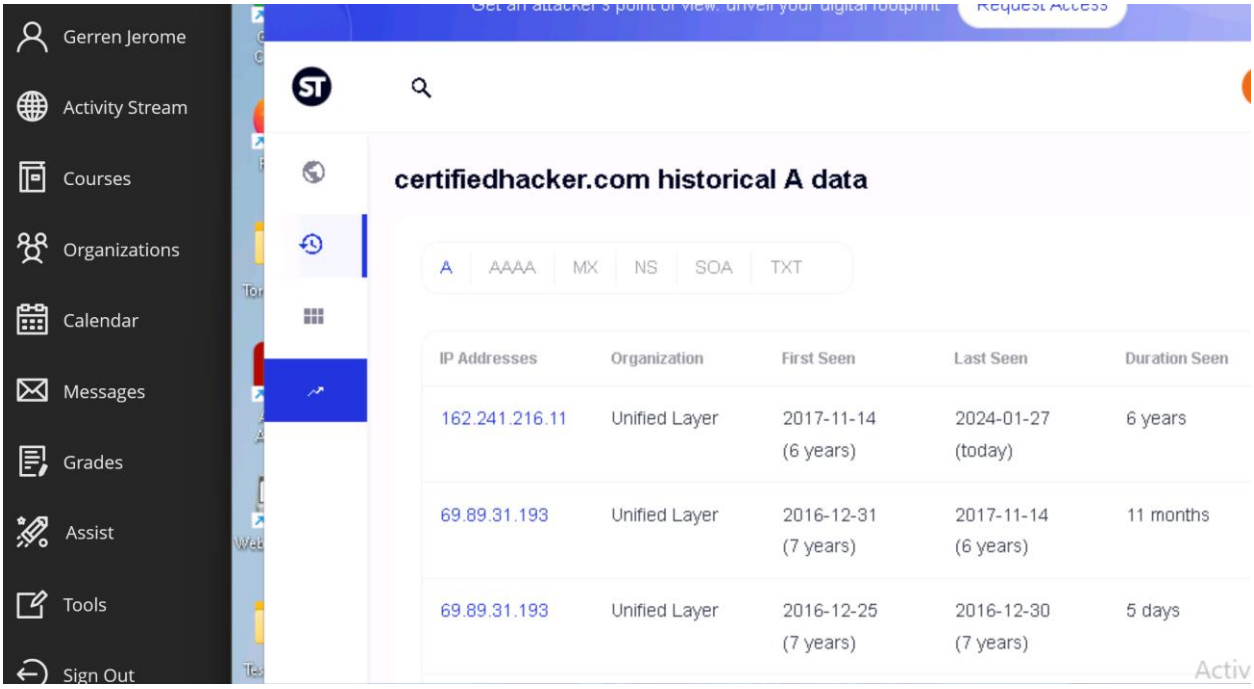


Gather information of subdomain and DNS records using SecurityTrails

SecurityTrails search results



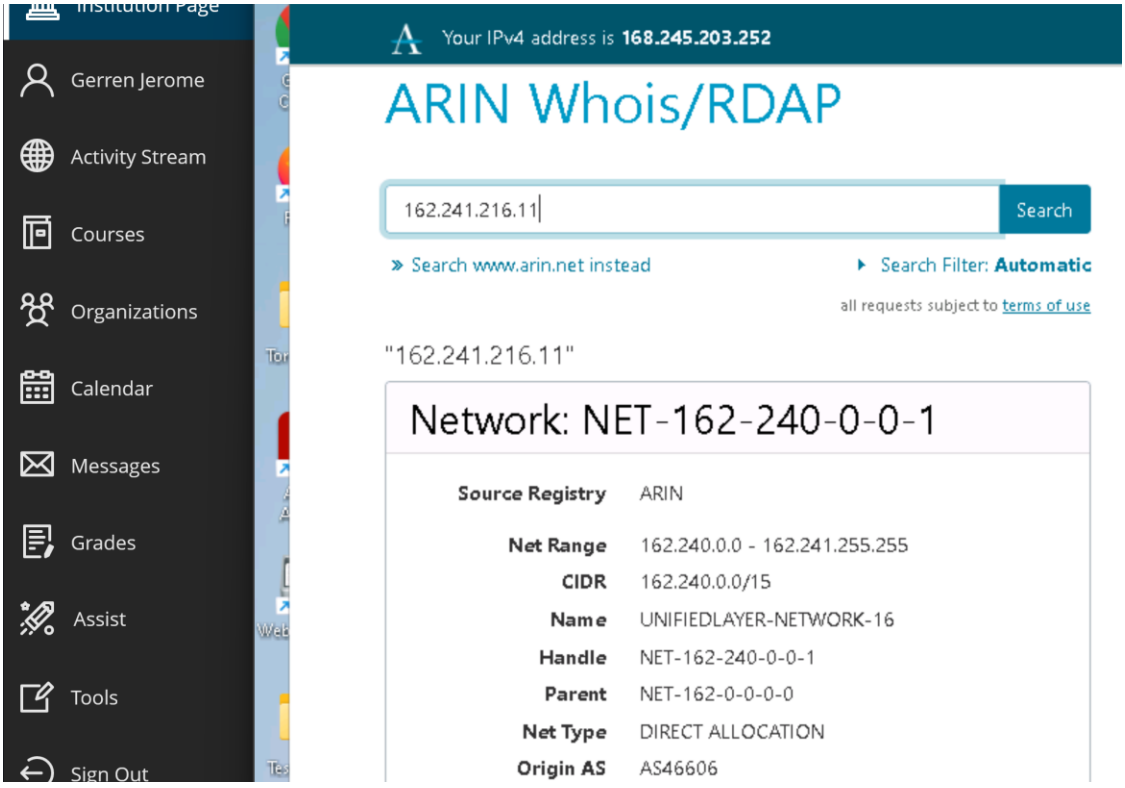
Historical data (A Record)



Perform network footprinting

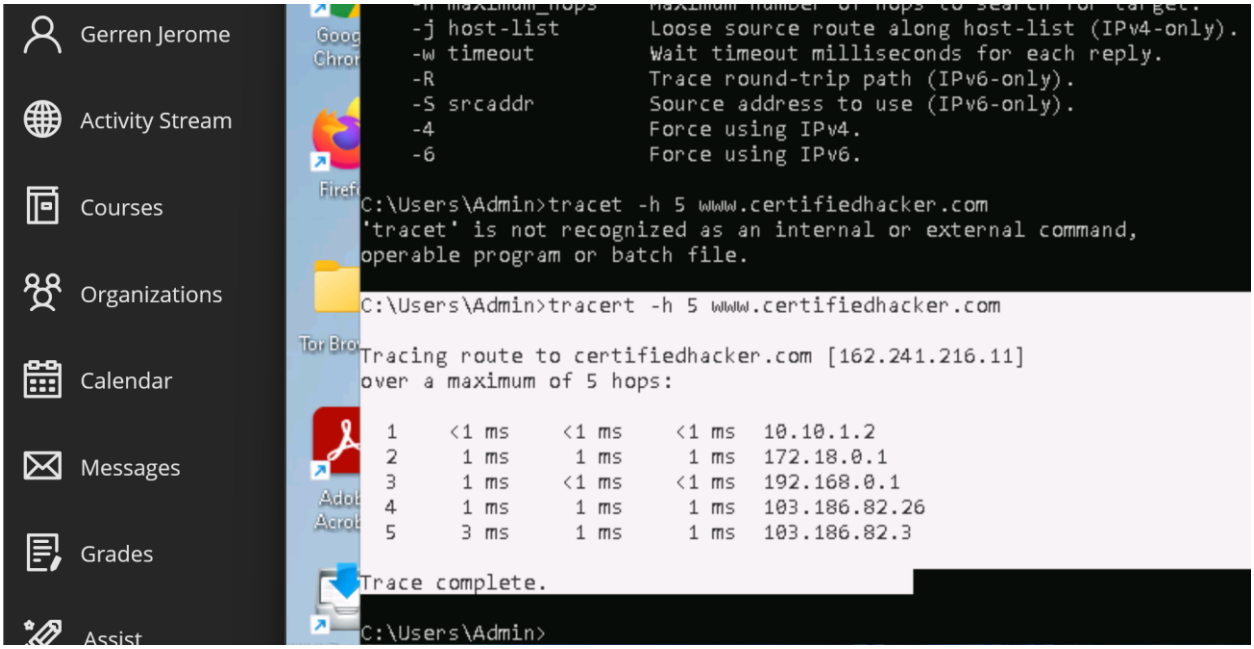
Locate the network range.

ARIN.net search results.

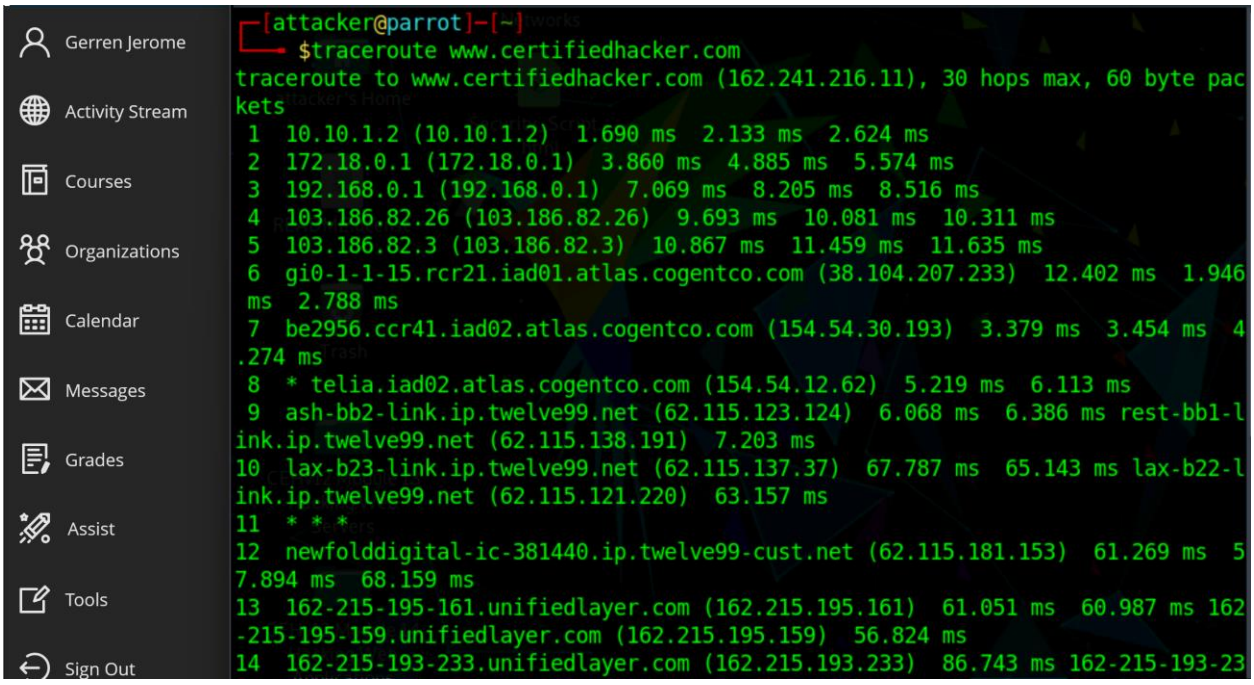


Perform network tracerouting in Windows and Linux Machines

tracert results (WIN)



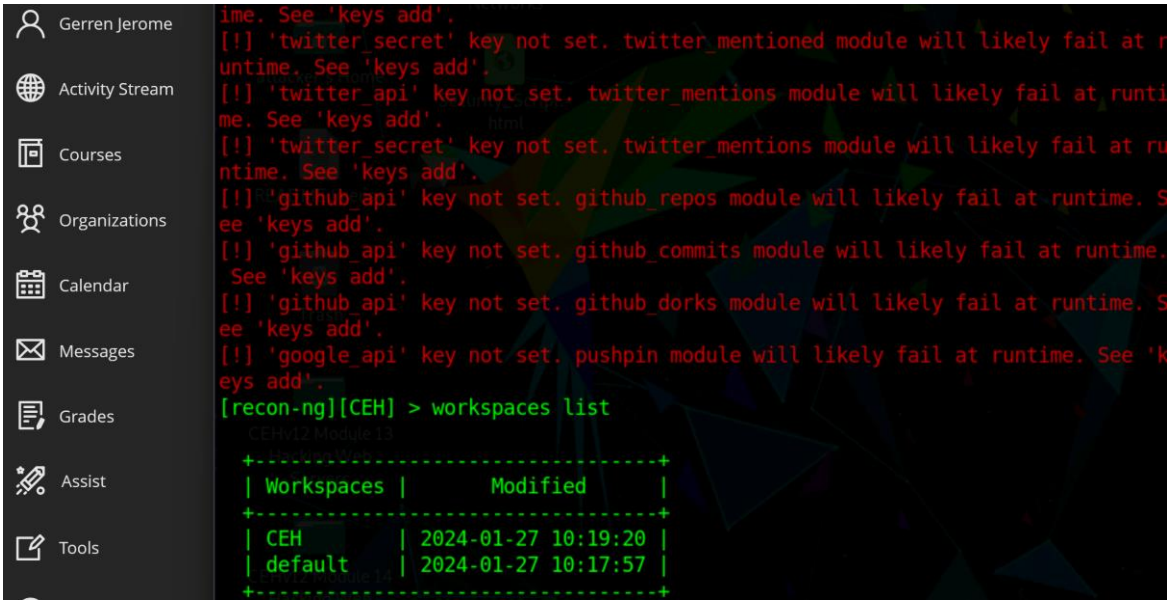
traceroute results (LNX)



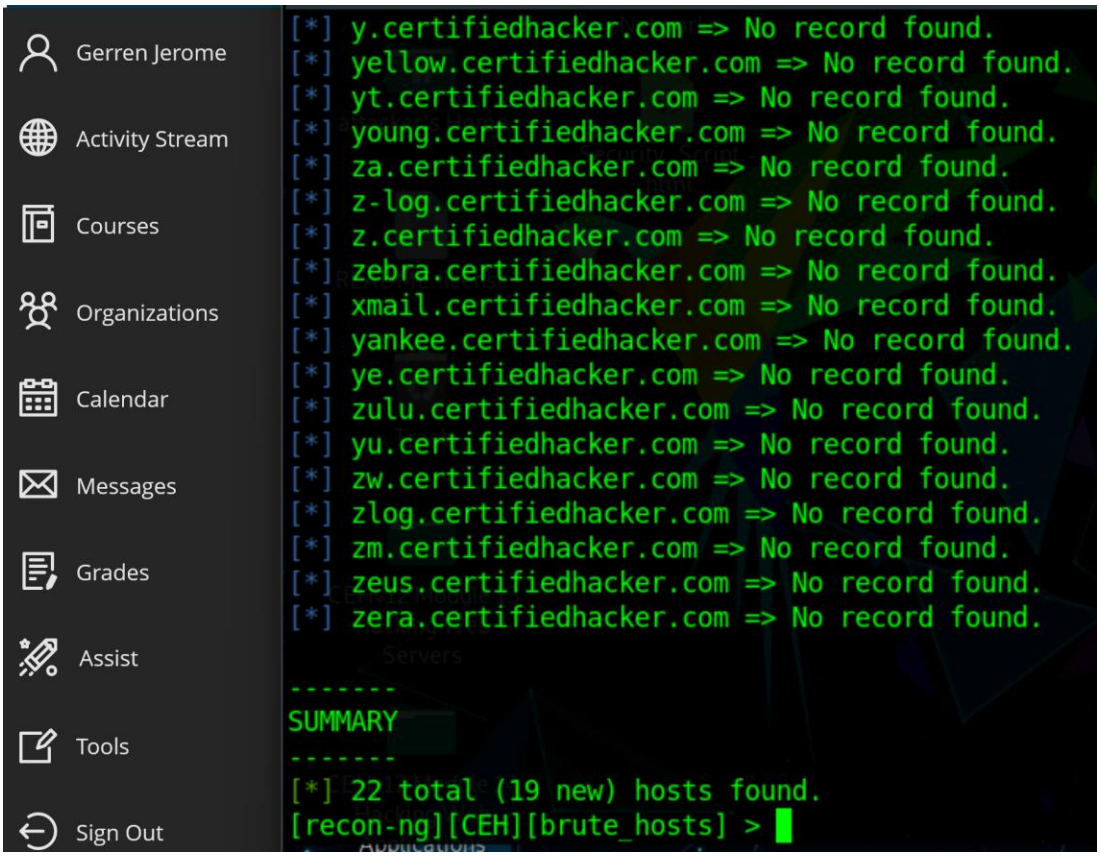
Perform footprinting using various footprinting tools.

Footprinting a target using Recon-ng.

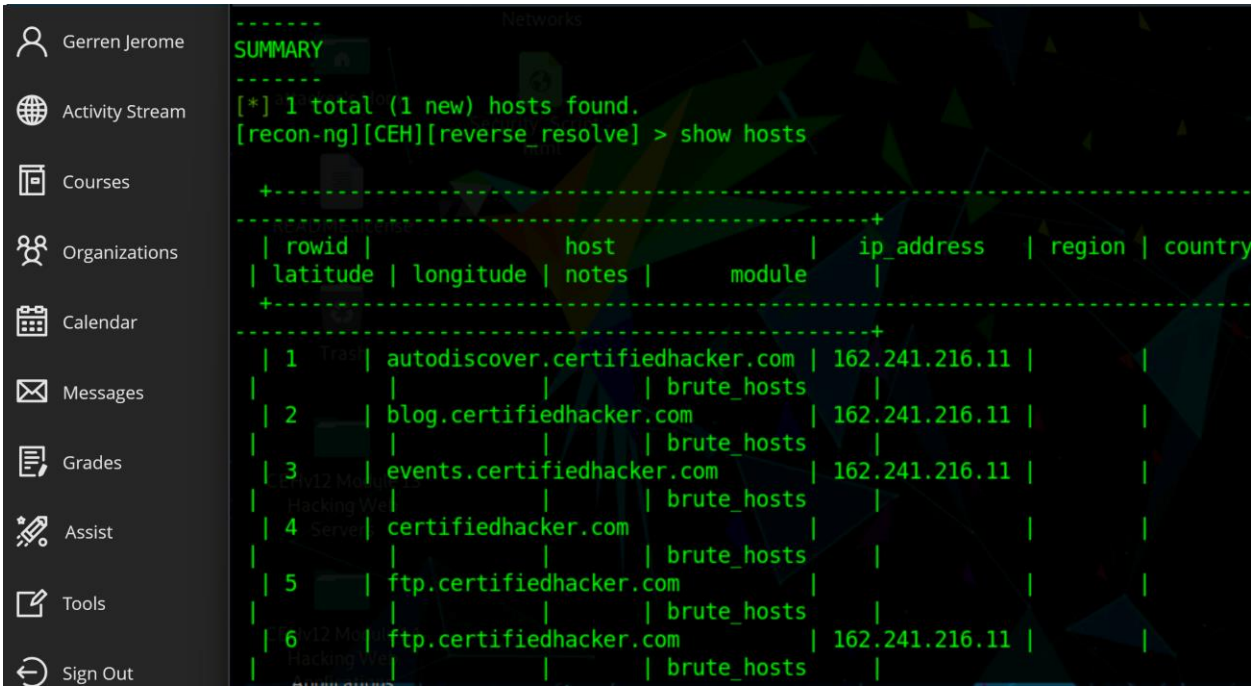
confirm created workspace.



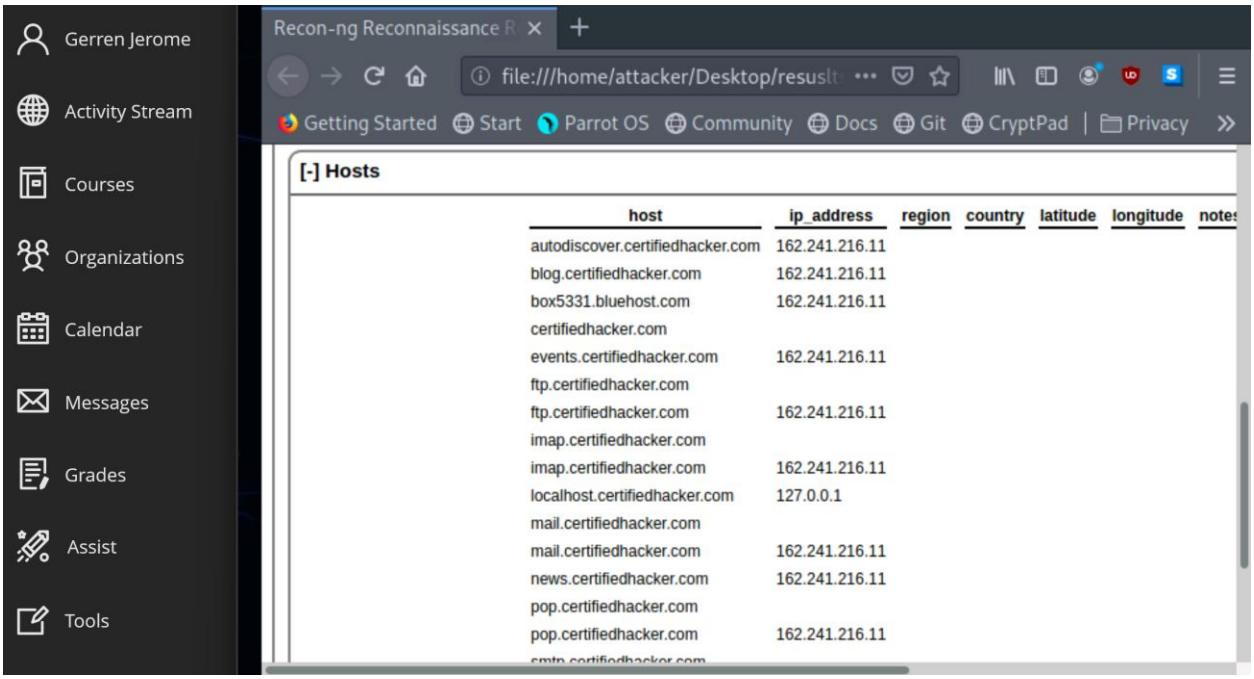
recon-ng results (brute_hosts)



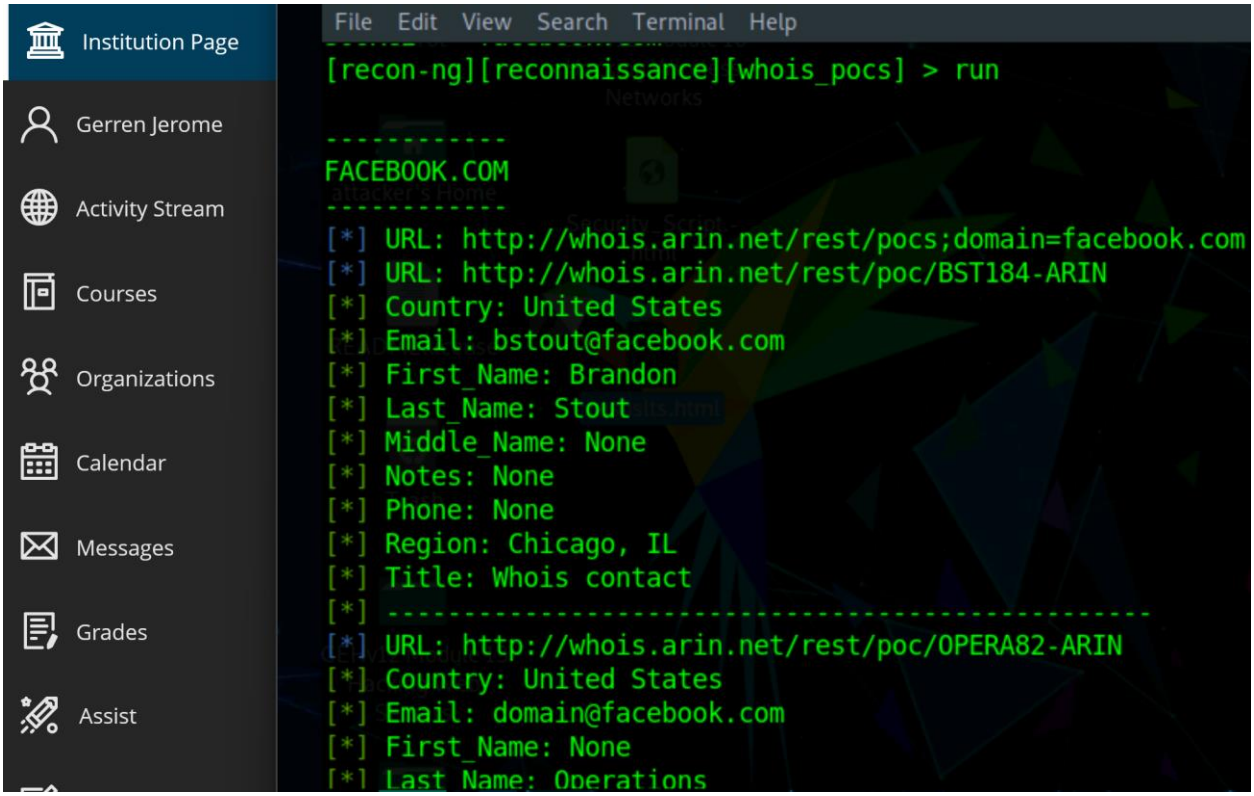
harvested host results (Attacker Window)



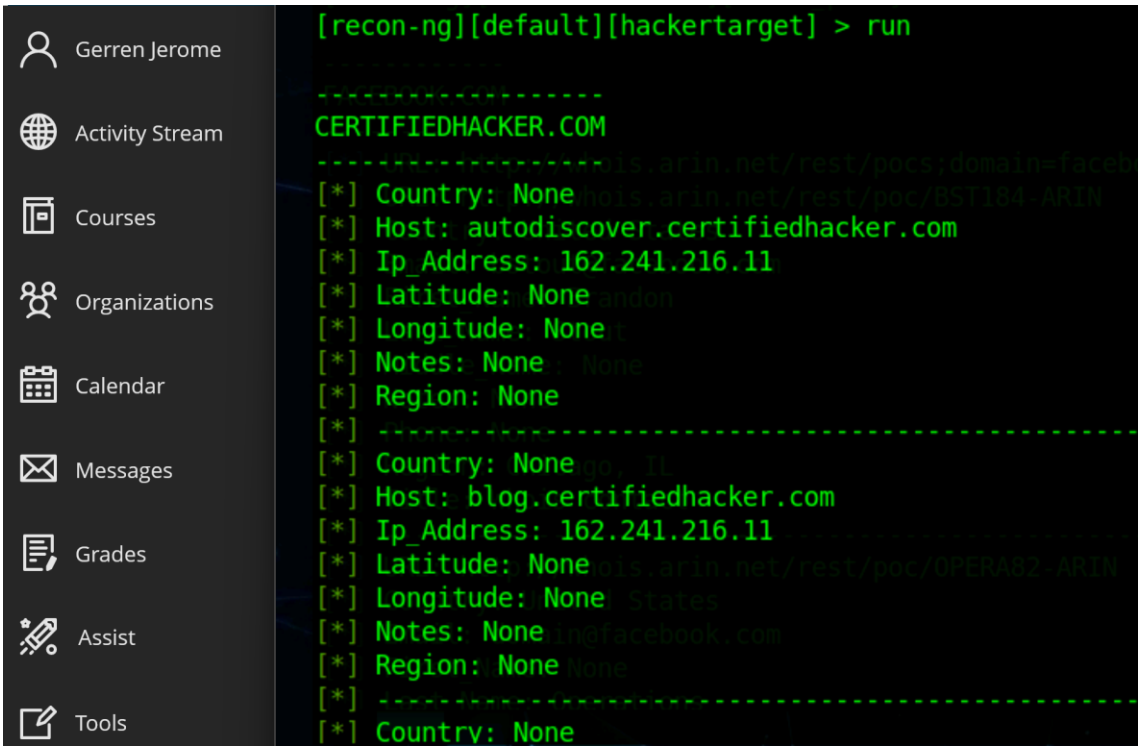
harvested host results (HTML report)



WHOIS_POCS results

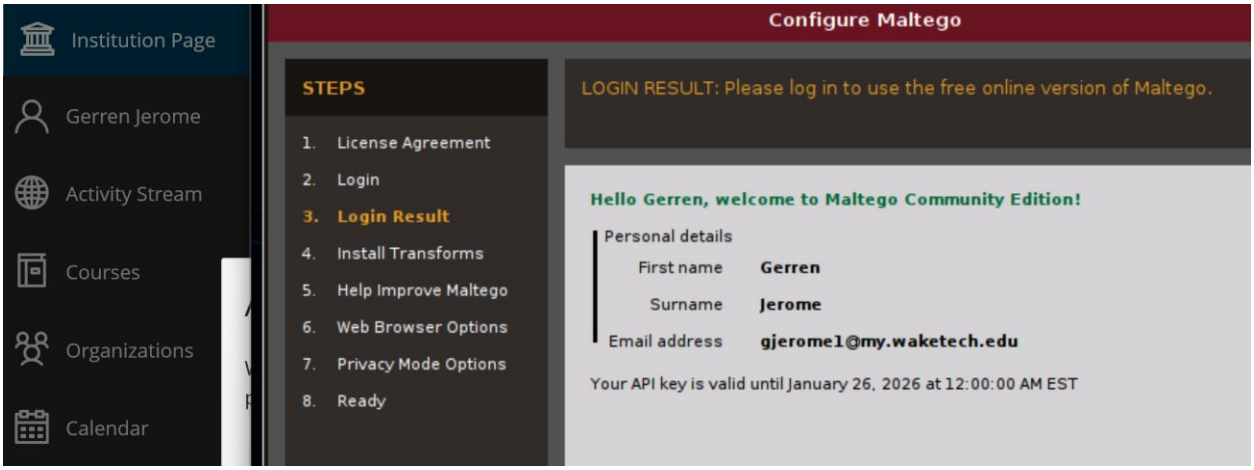


HackerTarget results

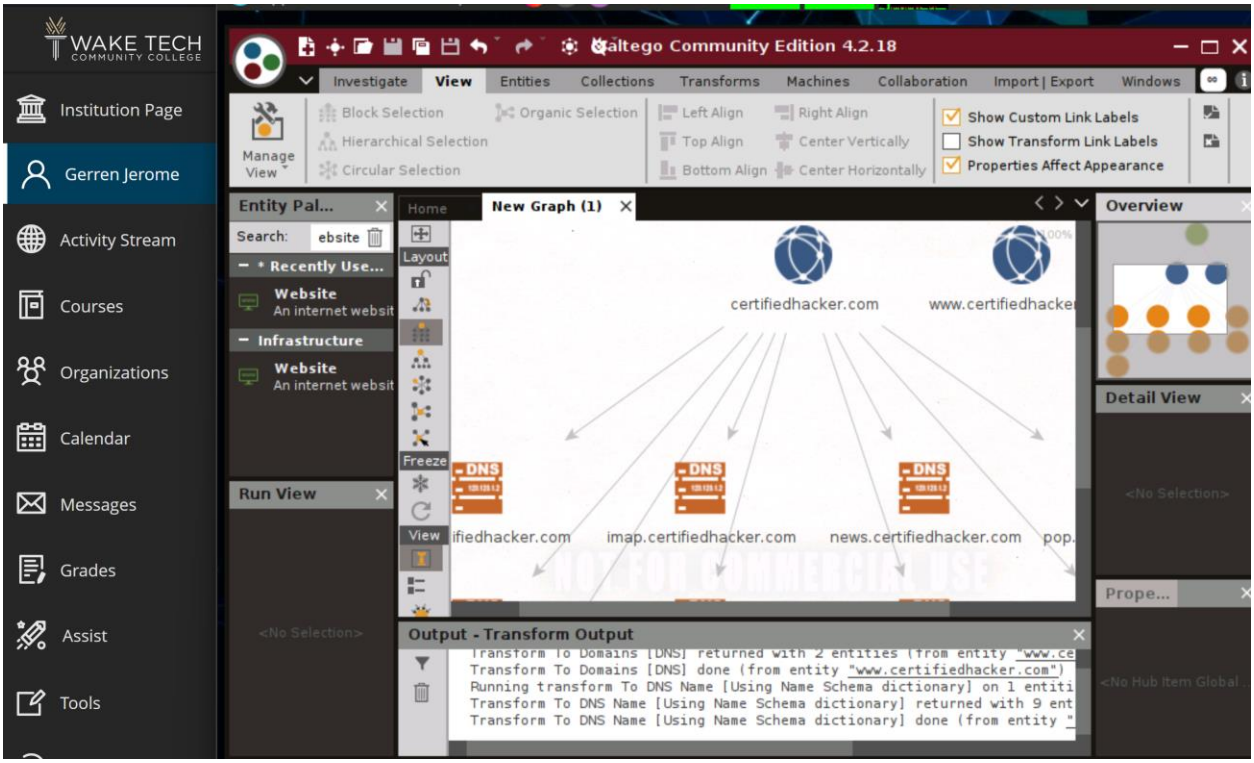


Footprinting a target using Maltego

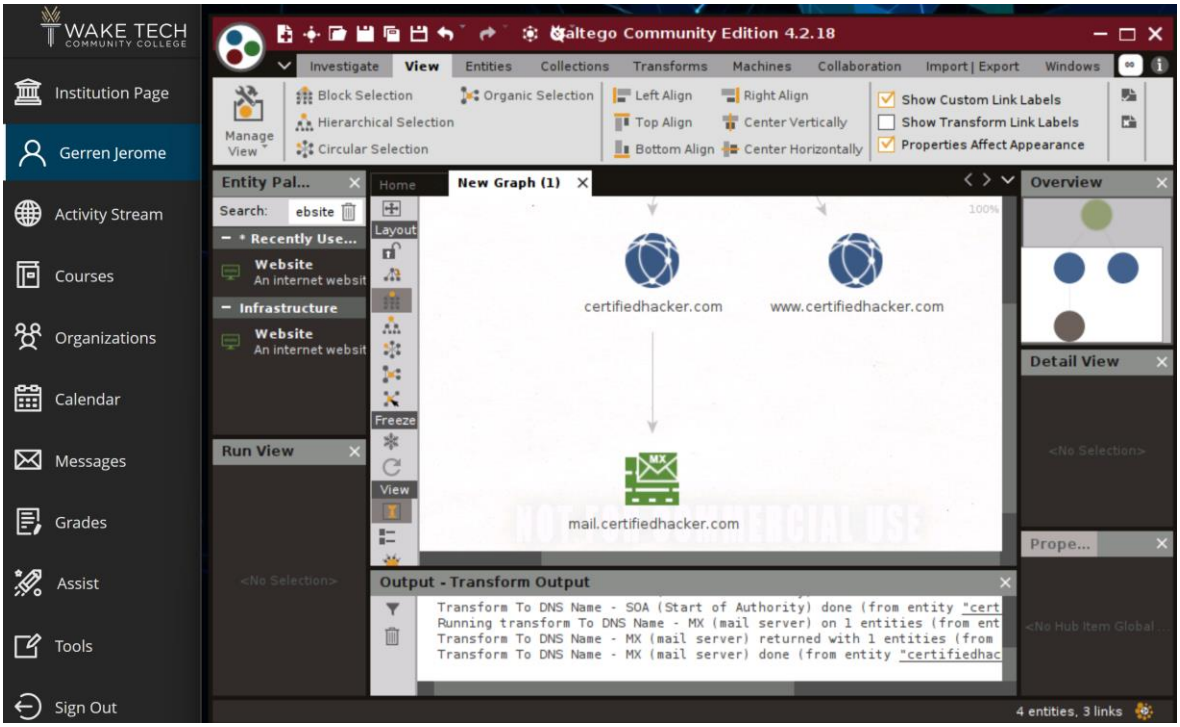
Login Successful



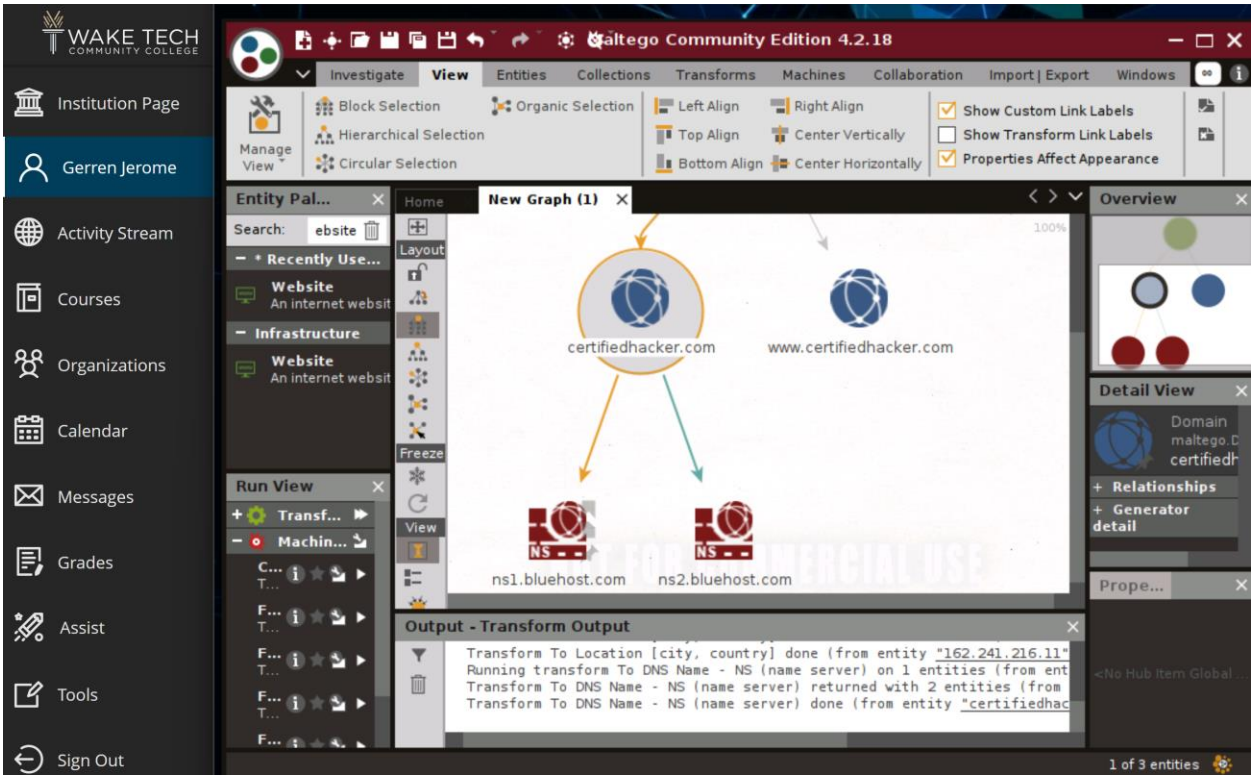
Transform (DNS) – identify and parse.



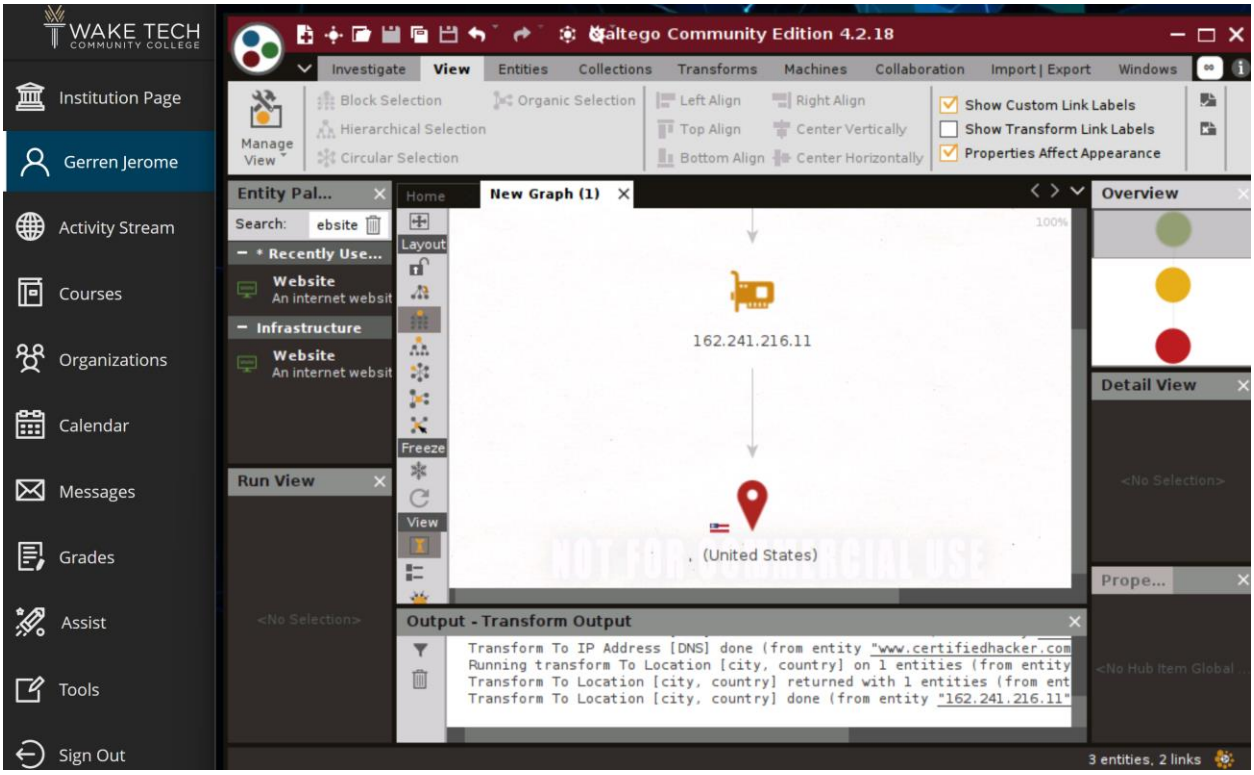
Transform (MX) - identify and parse.



Transform (NS) - identify and parse.

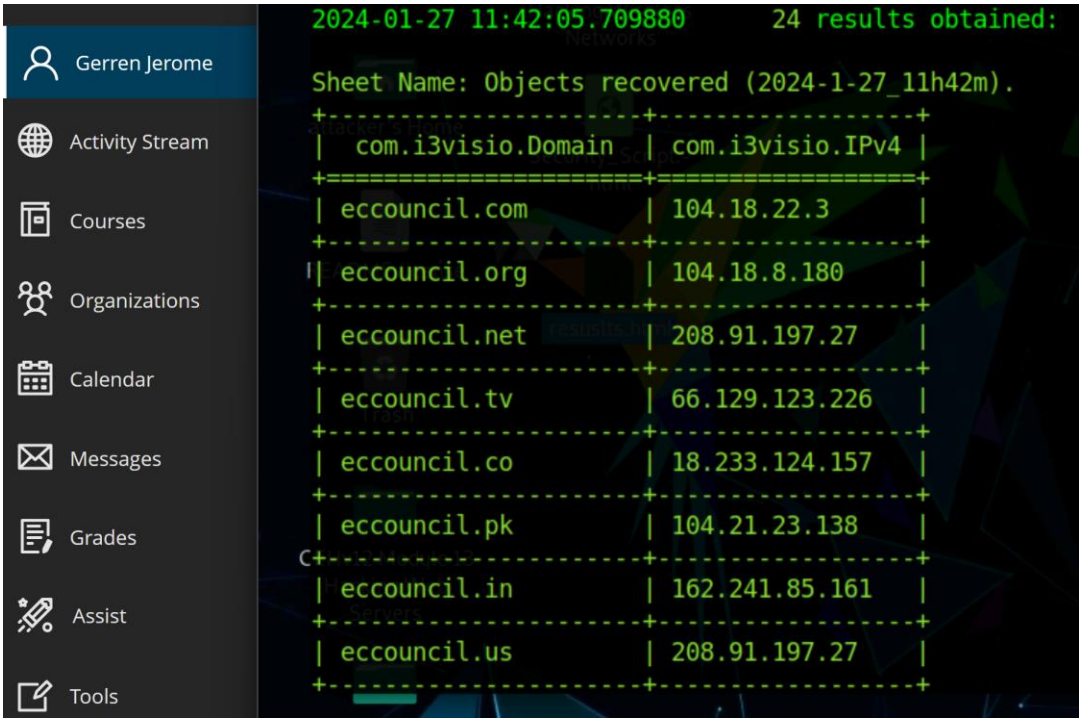


Location (city, country)

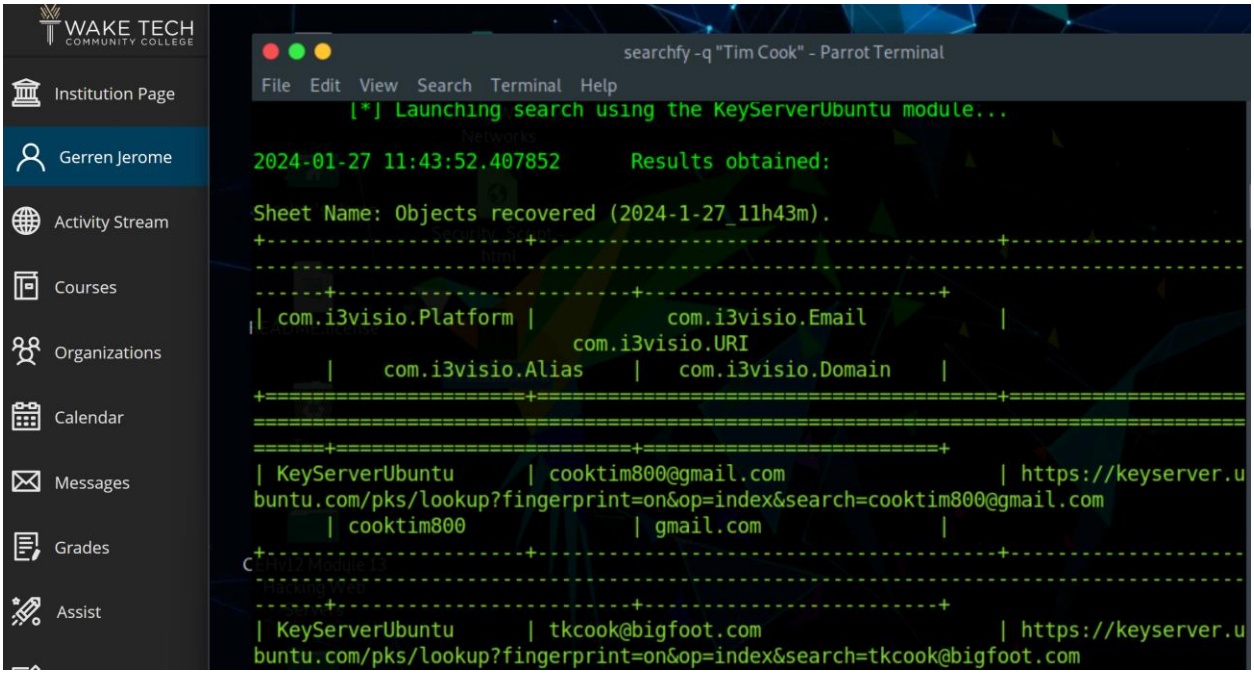


Footprinting a target using OSRFramework

Domainfy results

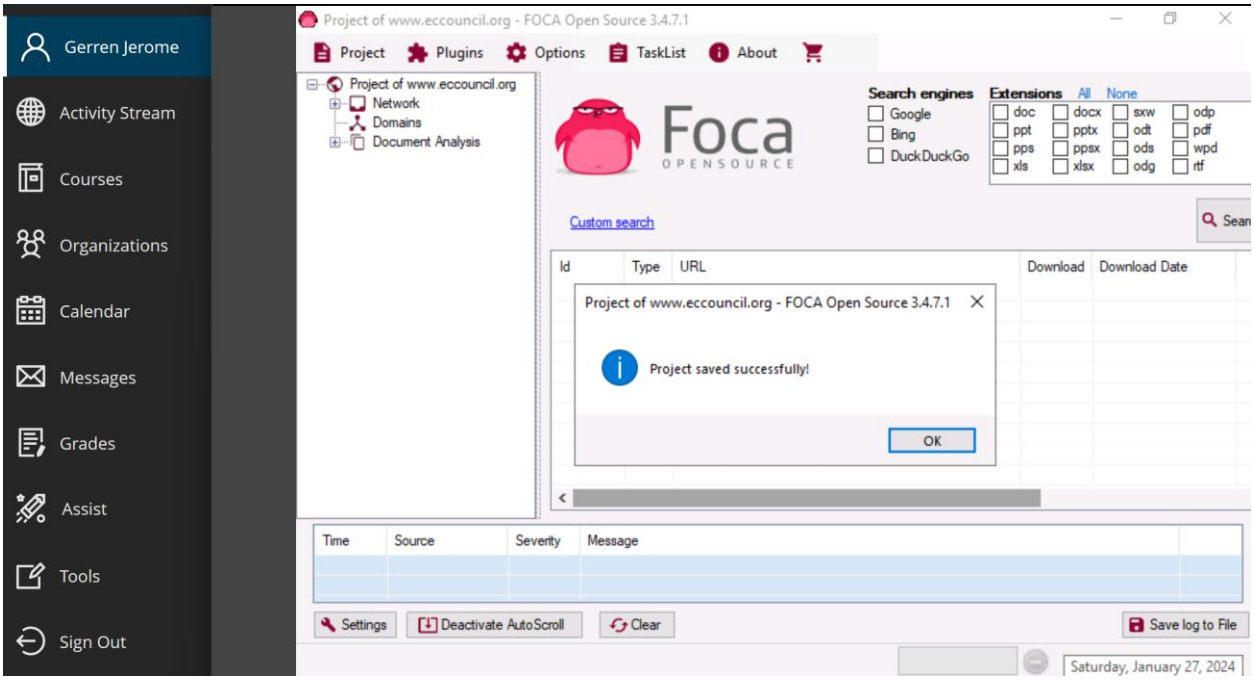


Searchfy results

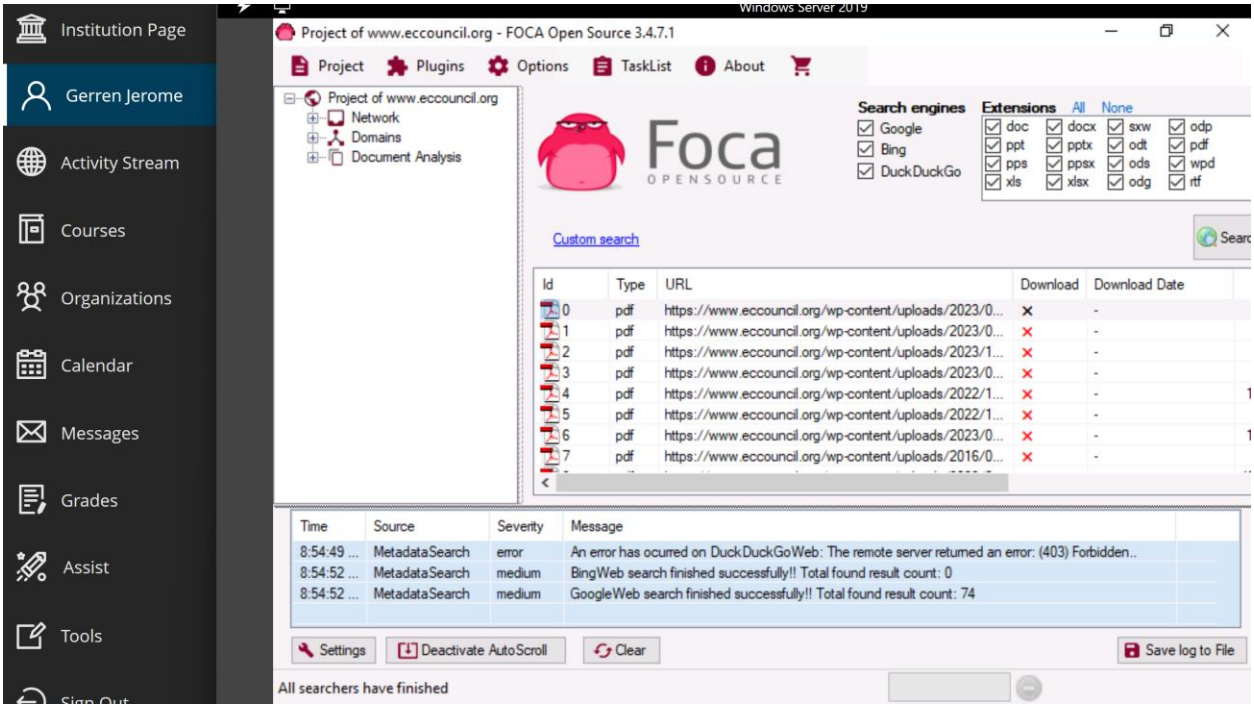


Footprinting a target using FOCA.

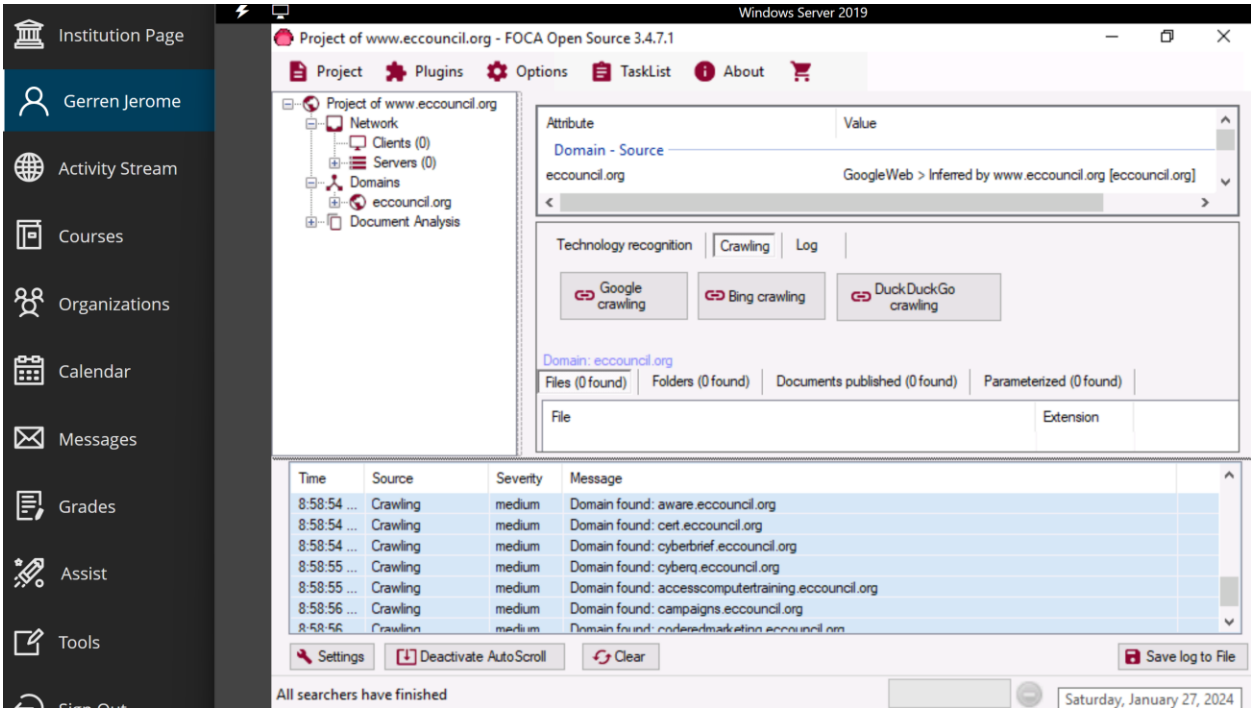
Project saved successfully!



Search All results.

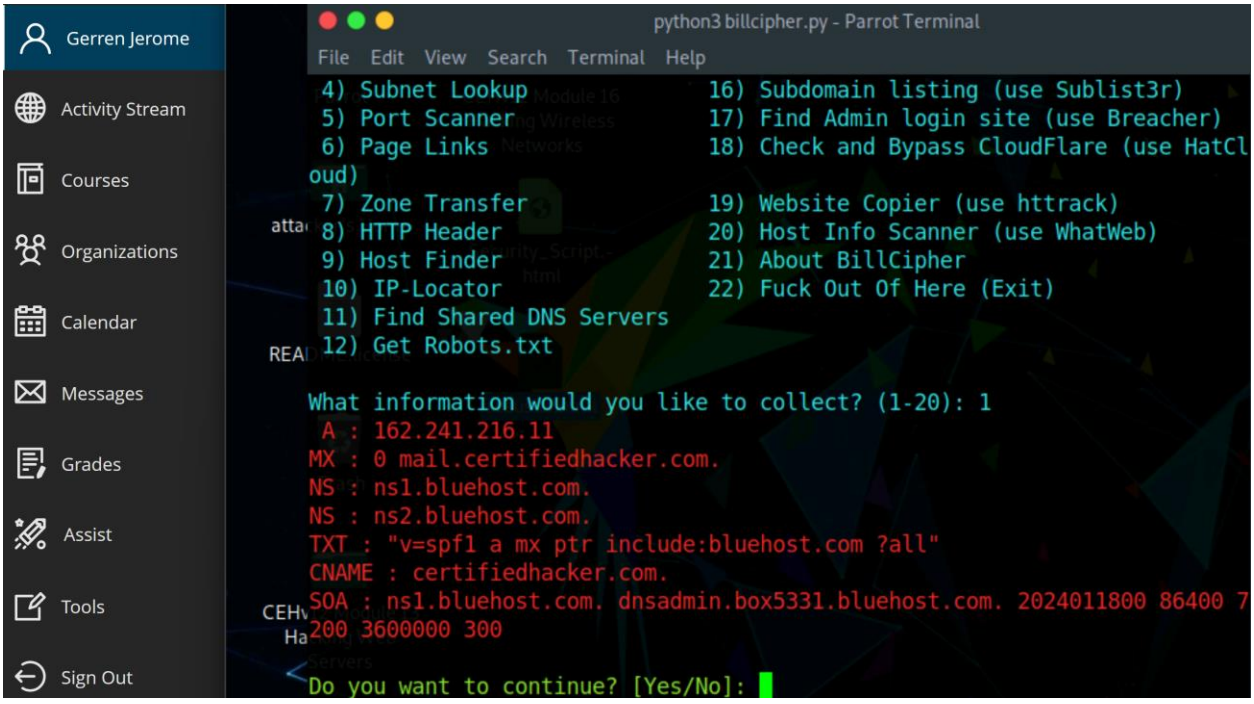


Crawling results

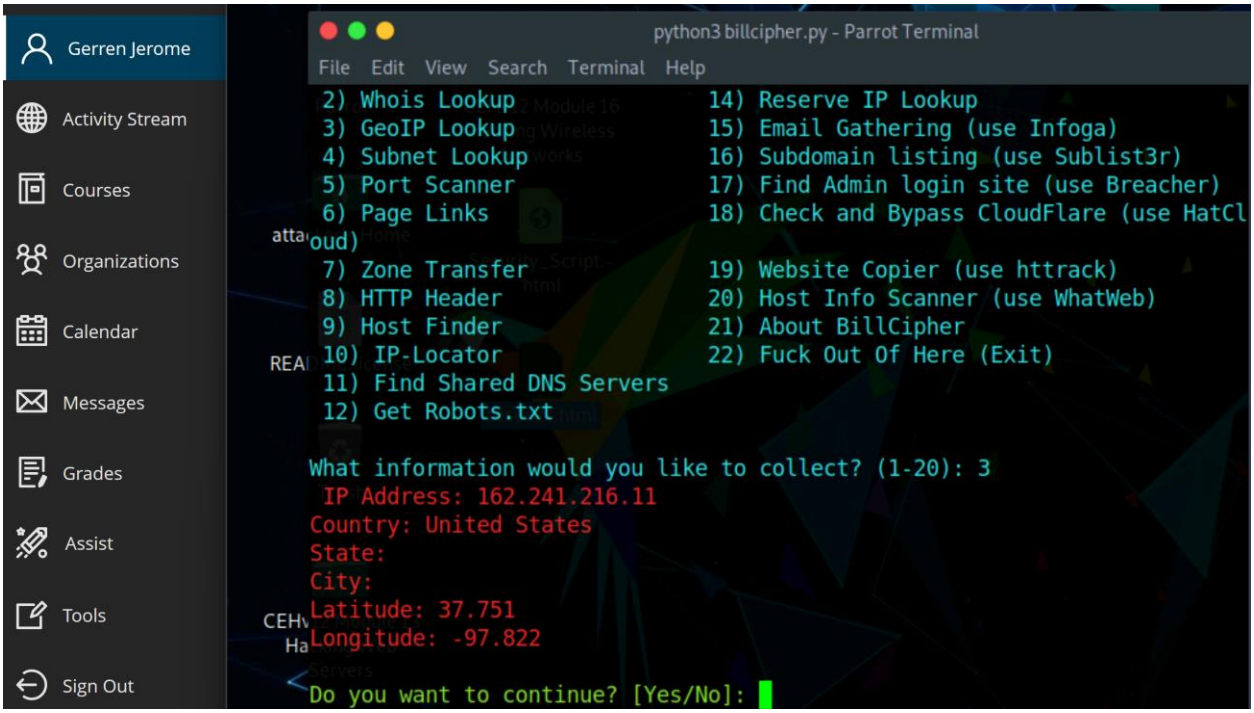


Footprinting a target using BillCipher (NSFW language in the interface)**

Results: DNS Lookup



Results: GeoIP Lookup



Results: Subnet Lookup