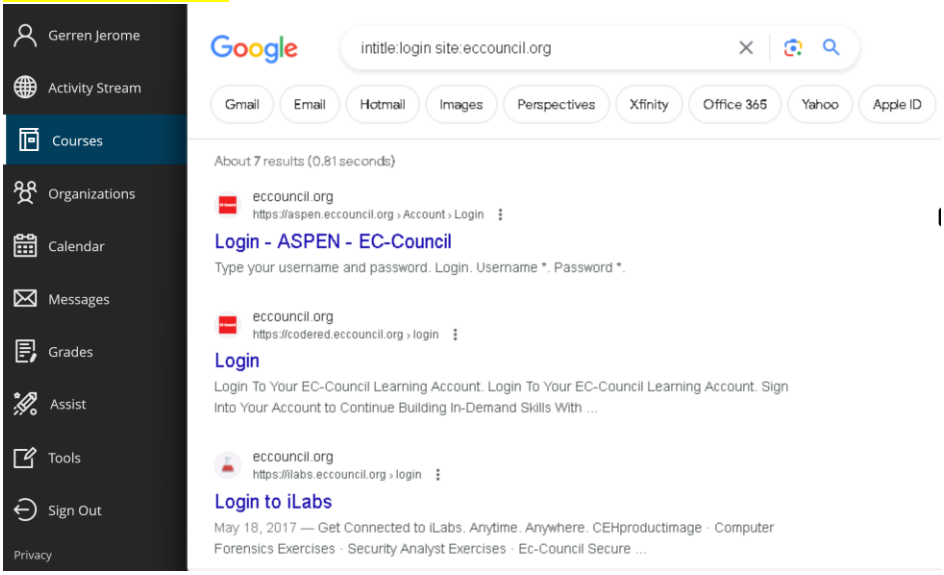
Gerren Jerome

Footprinting and Reconnaissance

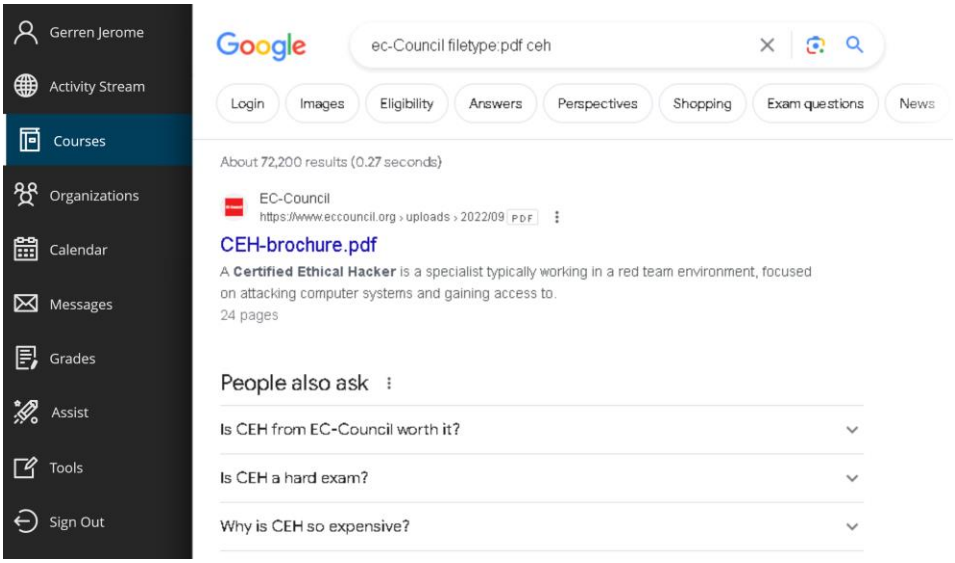
1. Perform footprinting through search engines (8 items)

a) Gather information using advanced Google hacking techniques.

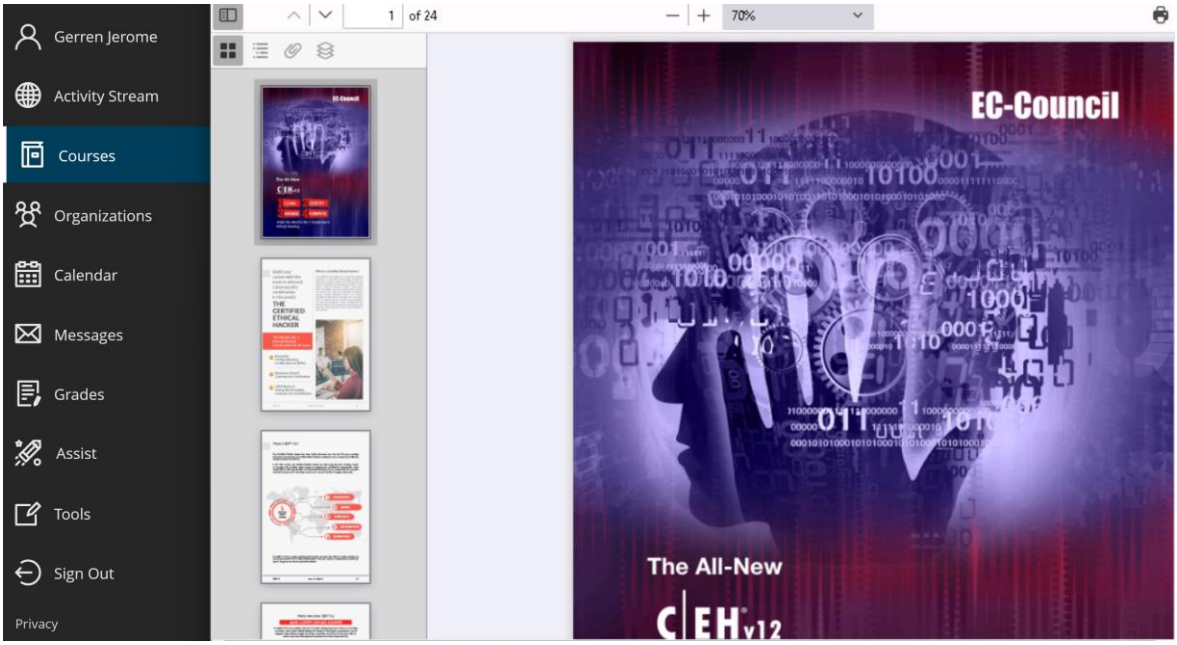
Screengrab: Step 5 – ECCouncil intitle login search



Screengrab: Step 7 – Find ECC pdfs related to the CEH program



Screengrab: Step 9 – CEH-brochure.pdf



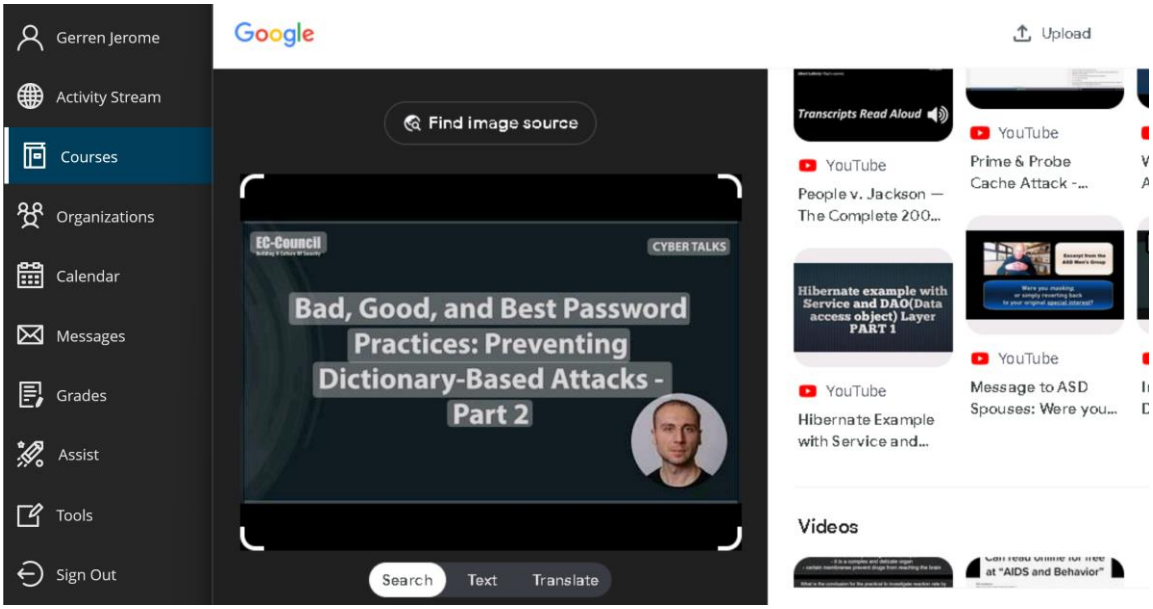
b) Gather information from video search engines.

Text: Step 3 – Paste the link from the video you chose

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

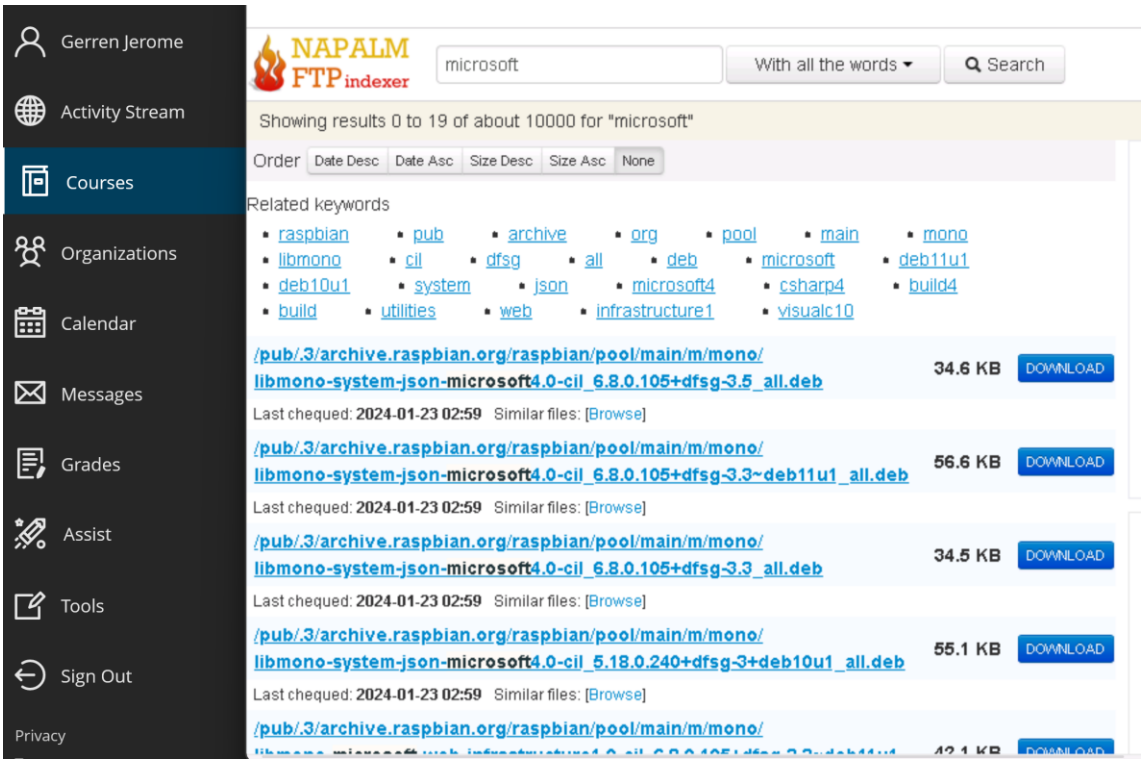
Screengrab: Step 6 – The mattw.io Snippet section

Screengrab: Step 9 – Reverse Image Search



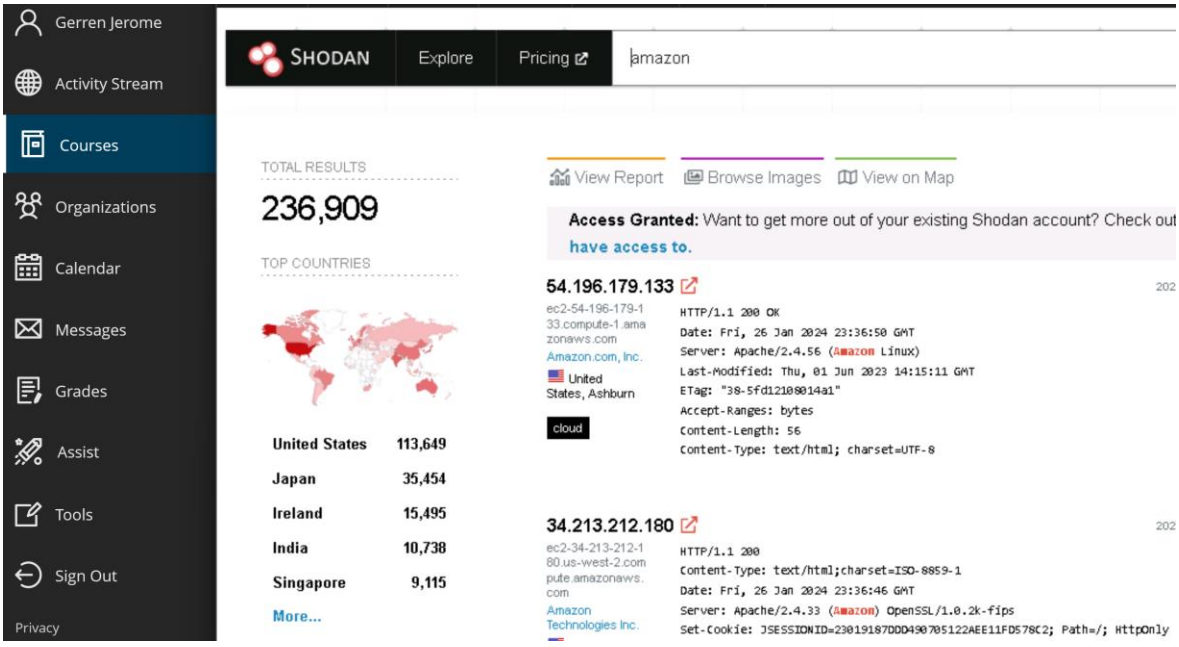
c) Gather information from FTP search engines

Screengrab: Step 4 – NAPALM-FTP search results



d) Gather information from IoT search engines

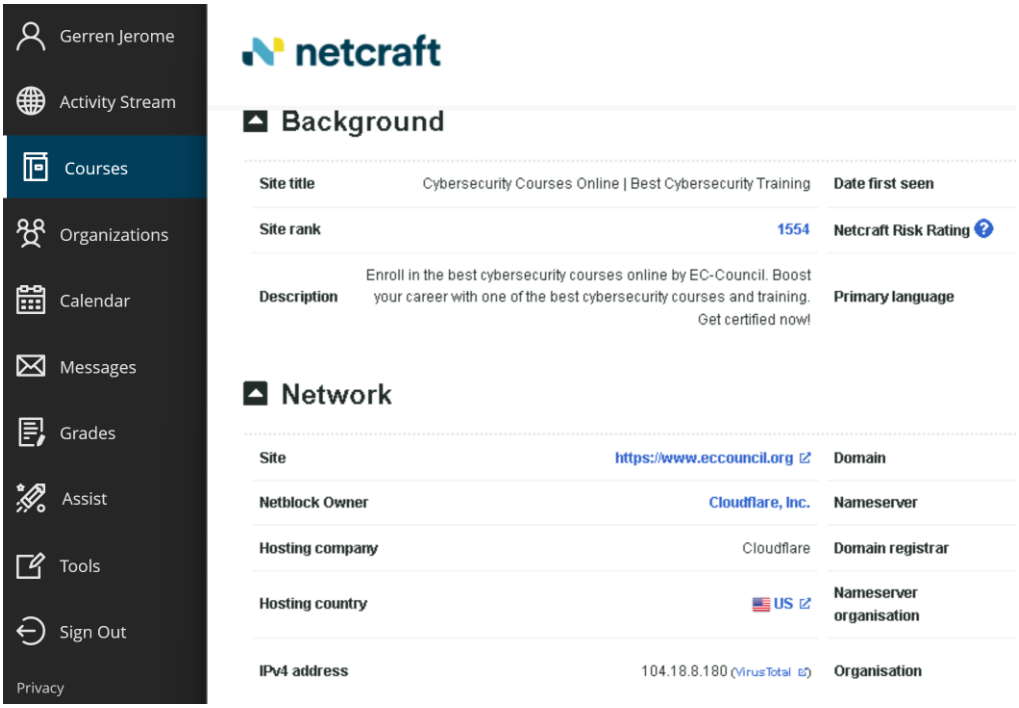
Screengrab: Step 4 – shodan.io search results



2) Perform footprinting through web services (6 items)

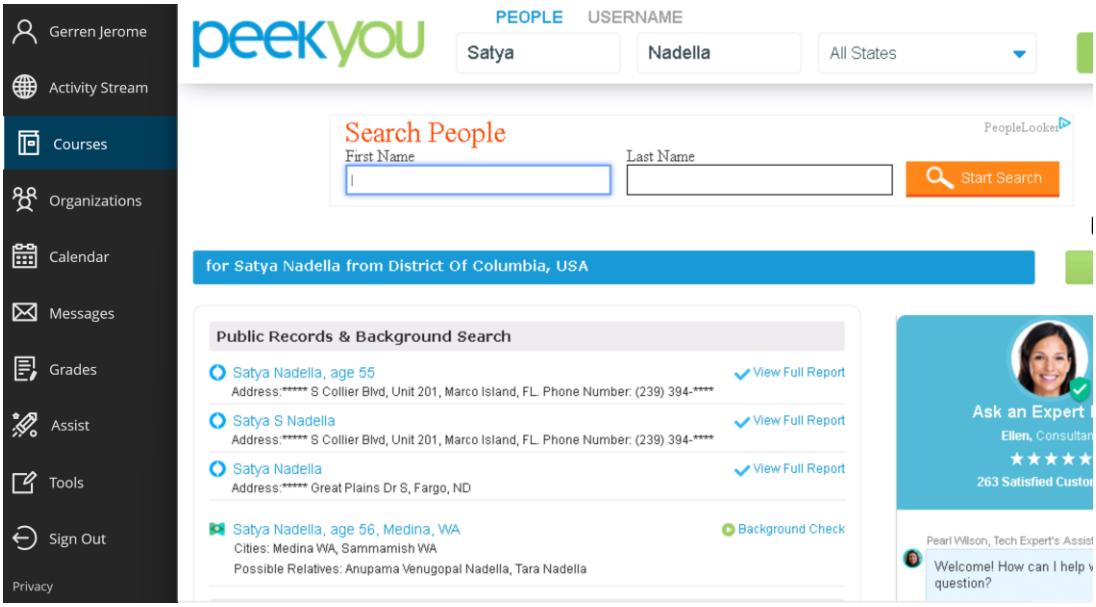
a) Find the company's domains and sub-domains using Netcraft

Screengrab: Step 5 – Netcraft site report



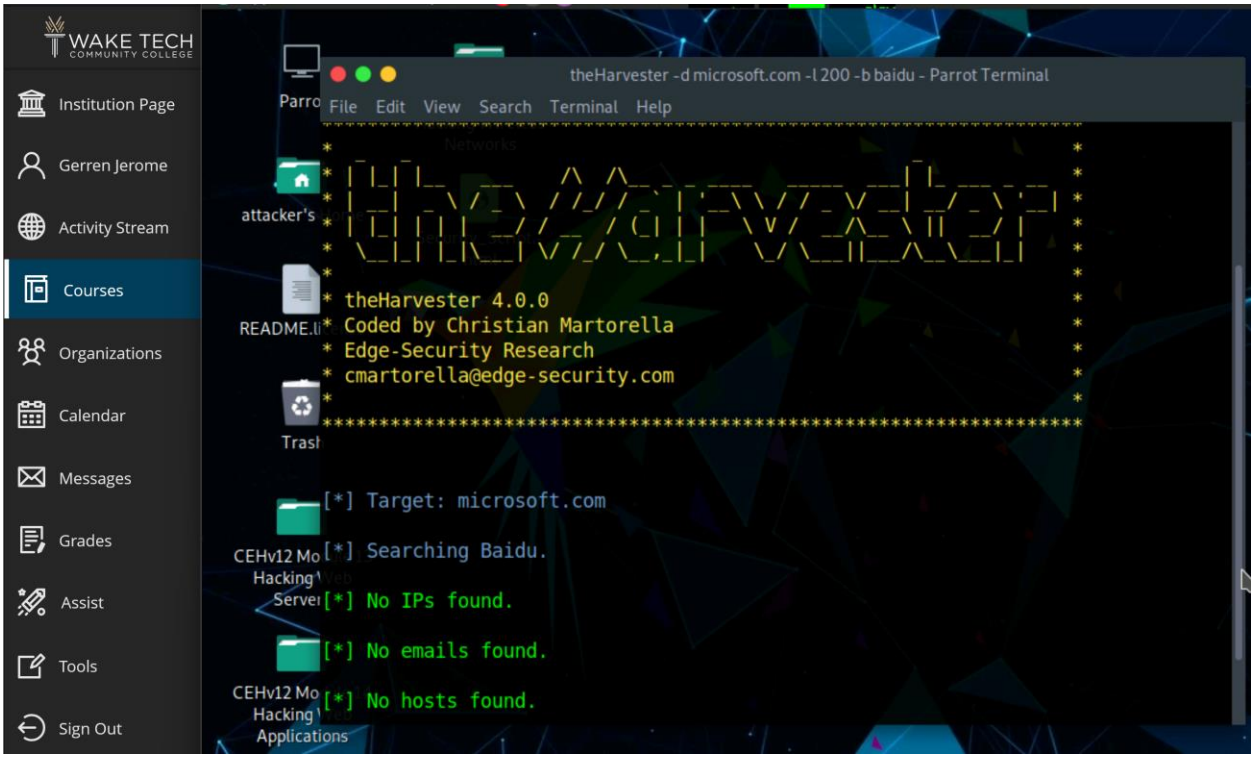
b) Gather personal information using PeekYou online people search service

Screengrab: Step 5 – PeekYou search results



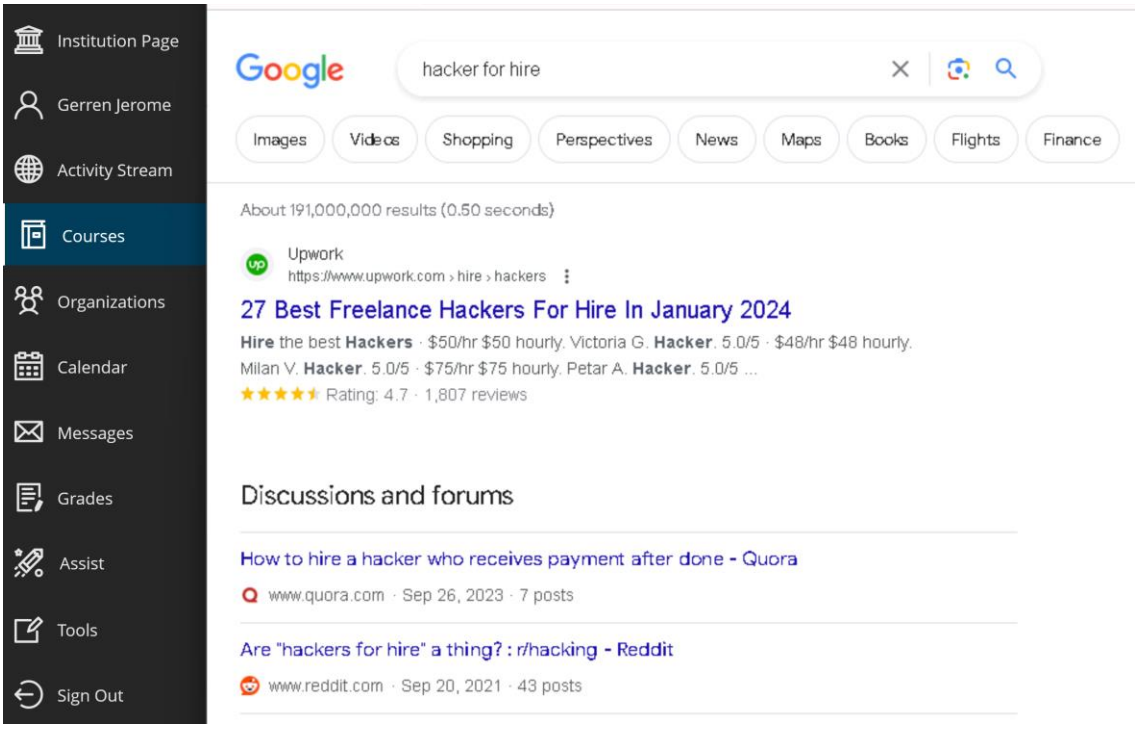
c) Gather an email list using theHarvester

Screengrab: Step 9 – theHarvester search results



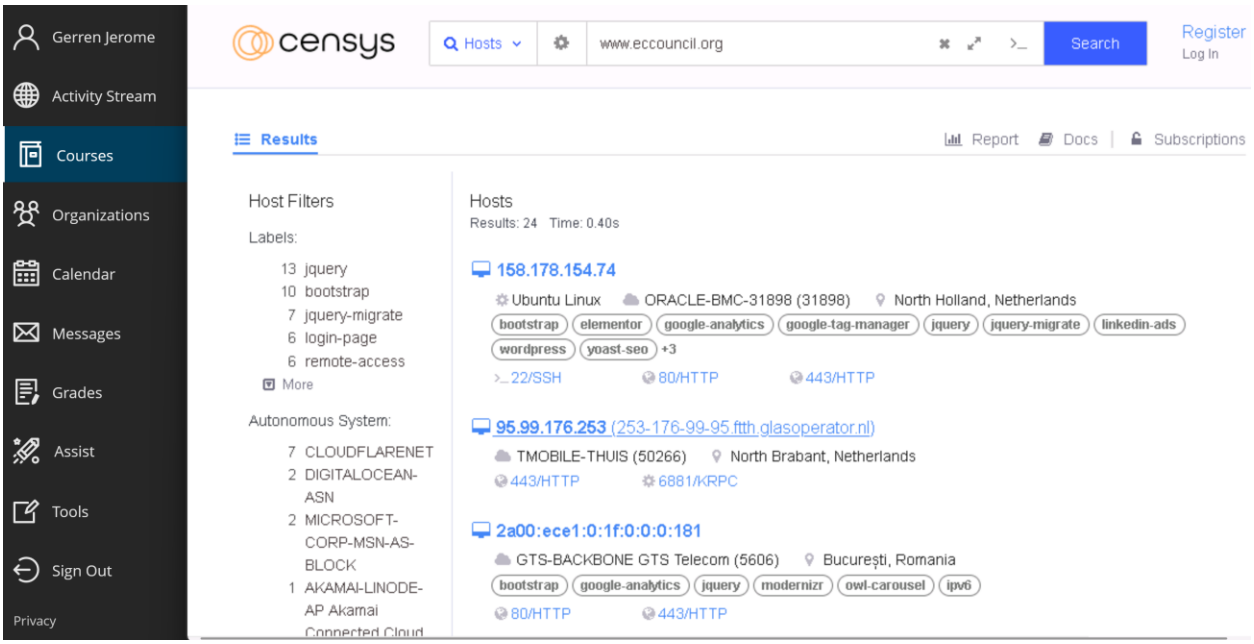
d) Gather information using deep and dark web searching

Screengrab: Step 6 – Google search results



e) Determine target OS through passive footprinting

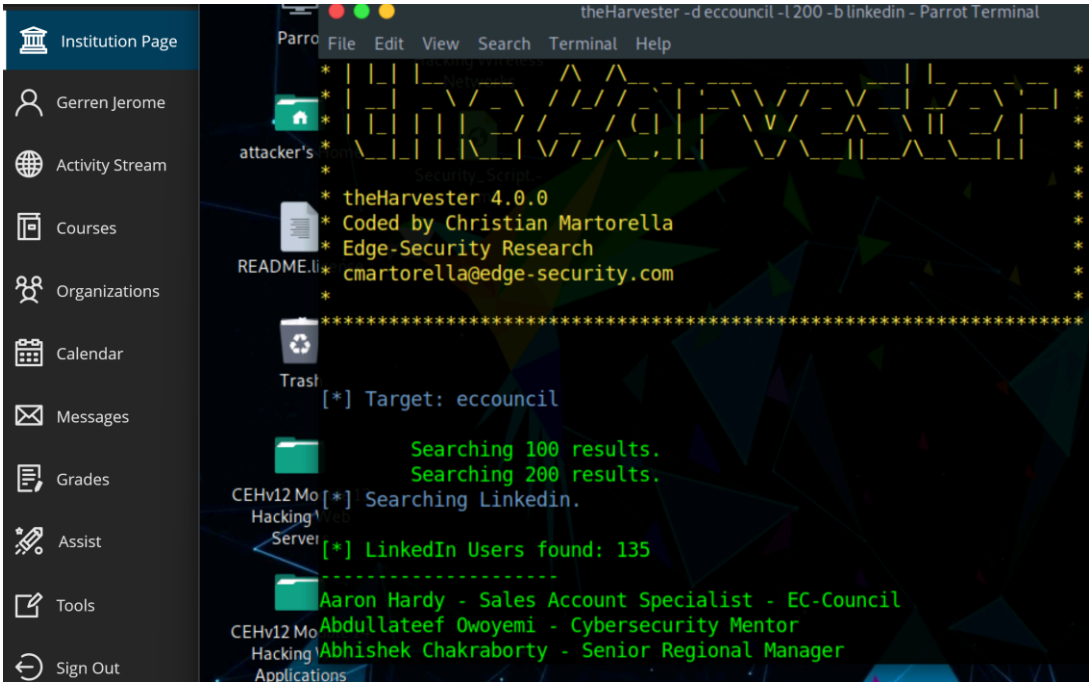
Screengrab: Step 2 – Censys search results



3) Perform footprinting through social networking sites (2 items)

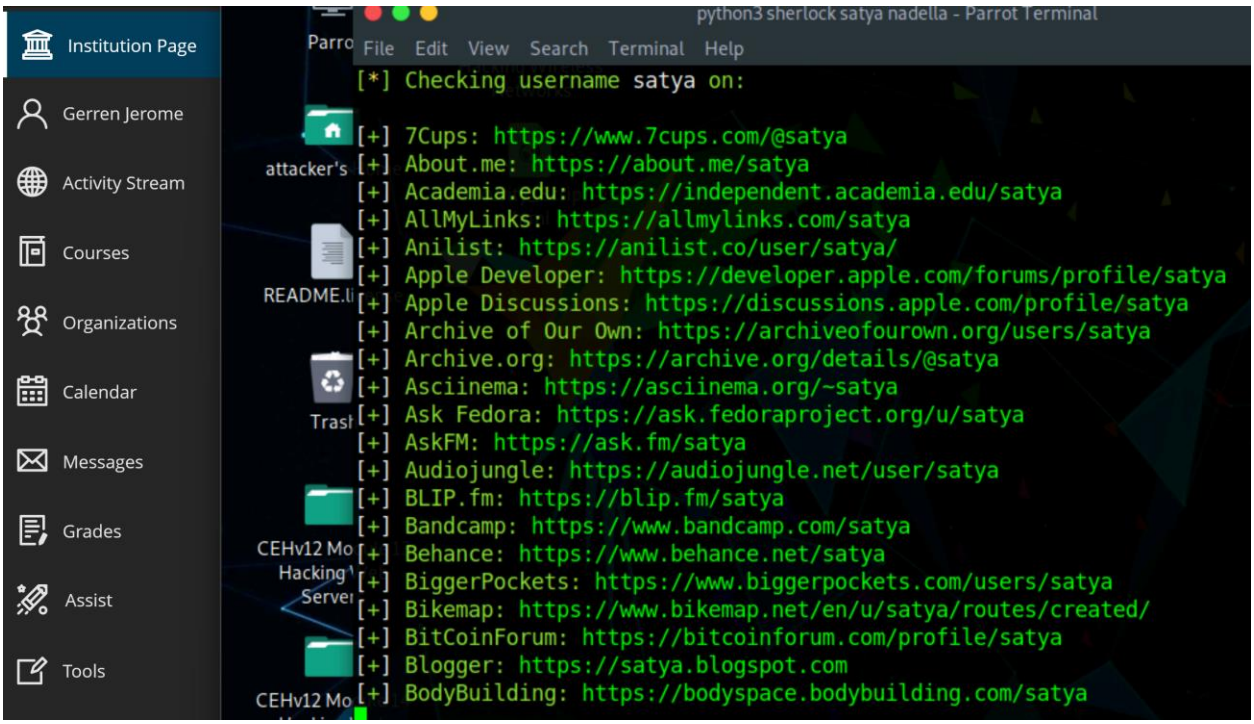
a) Gather employees' information from LinkedIn using theHarvester

Screengrab: Step 6 – theHarvester search results



b) Gather personal information from various social networking sites using Sherlock

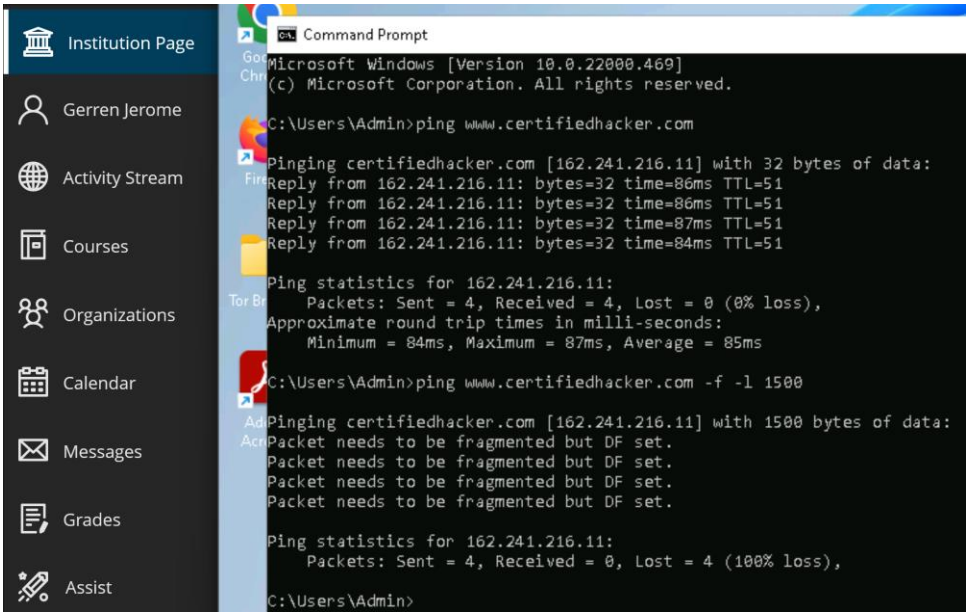
Screengrab: Step 6 – Sherlock search results



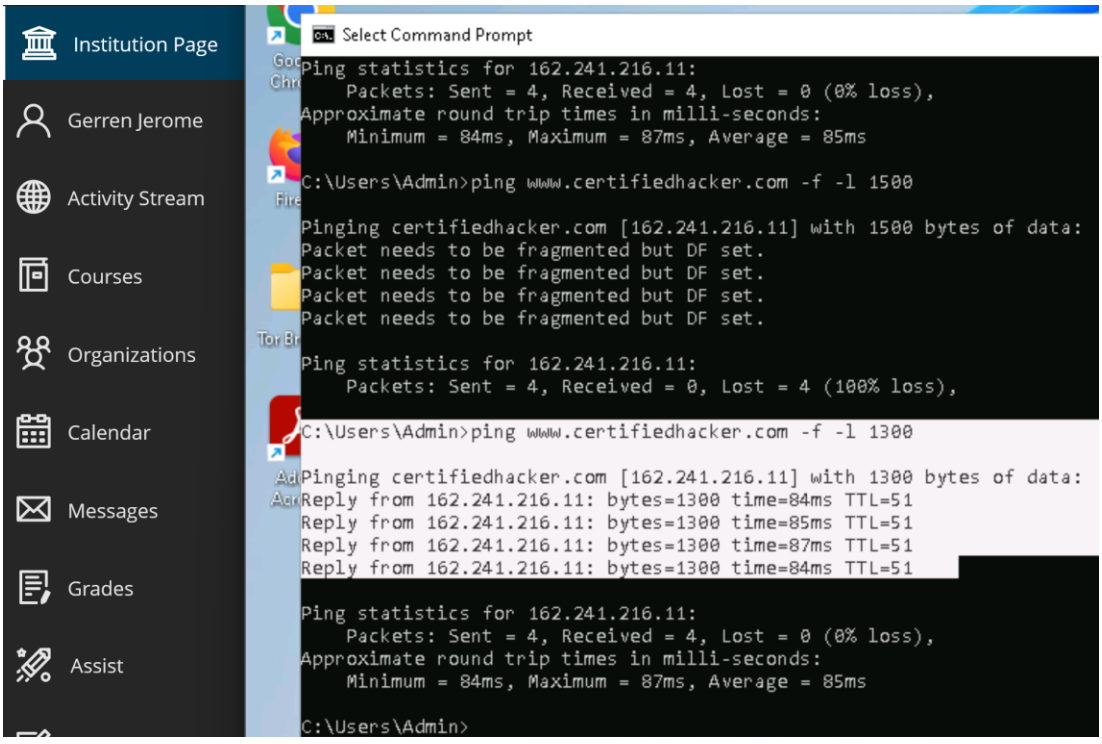
4) Perform website footprinting (14 items)

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

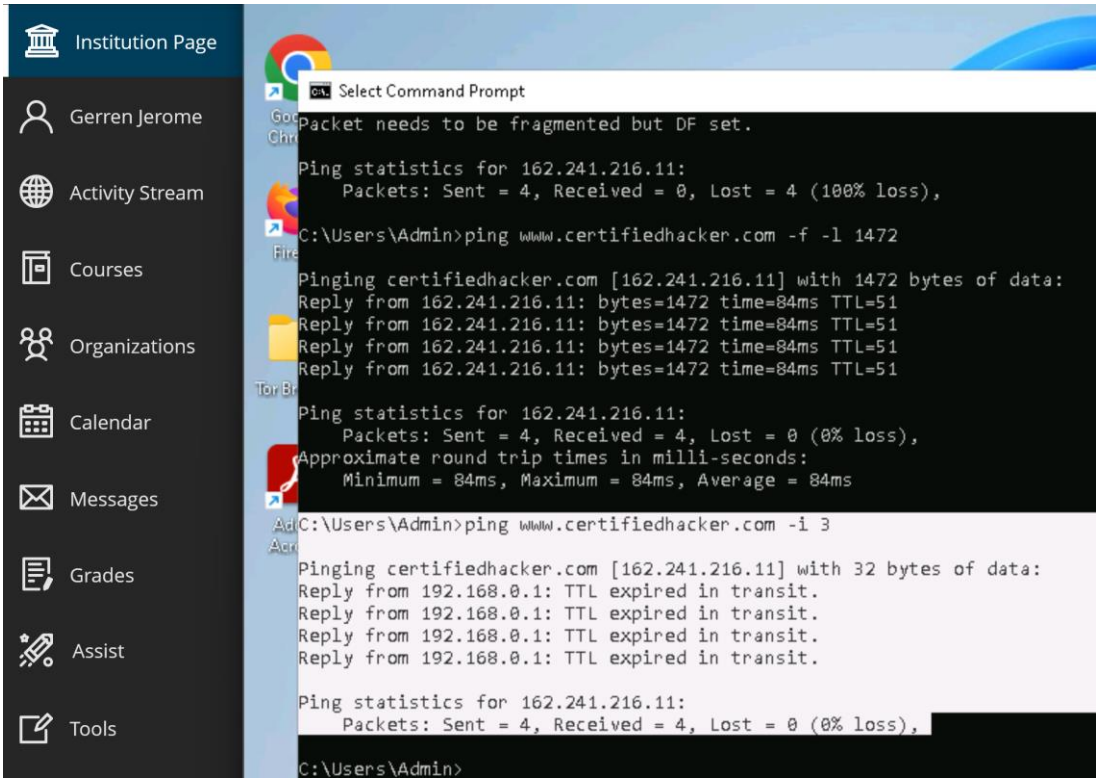
Screengrab: Step 4 - finding the frame limit, part 1



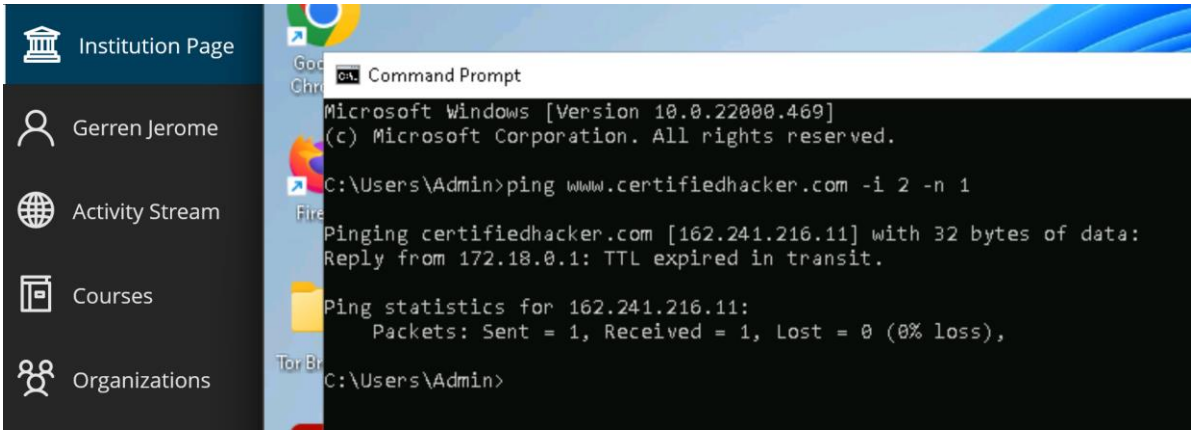
Screengrab: Step 6 – finding the frame limit, part 2



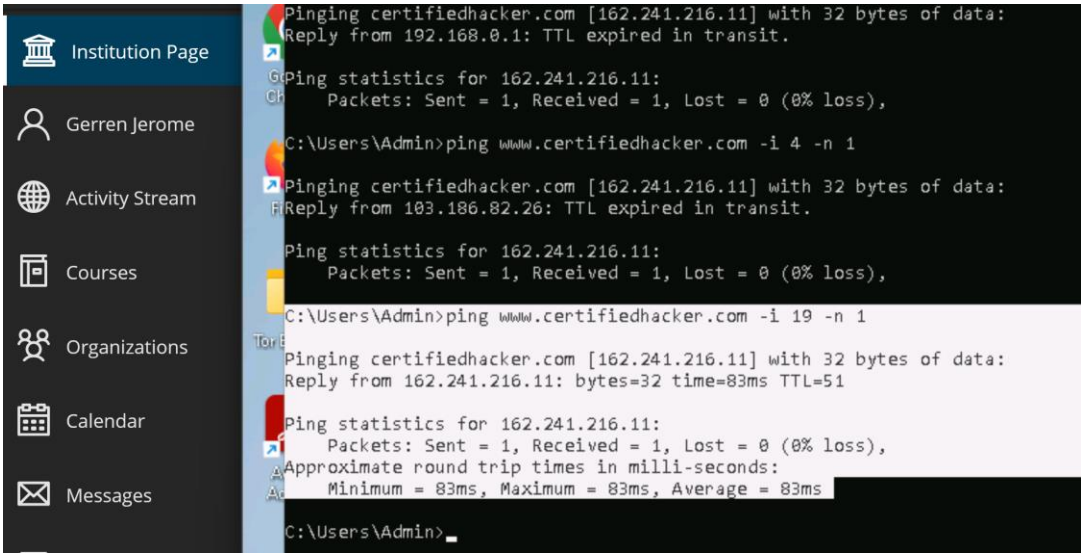
Screengrab: Step 10 – TTL manipulation



Screengrab: Step 12 – ping packet lifespan

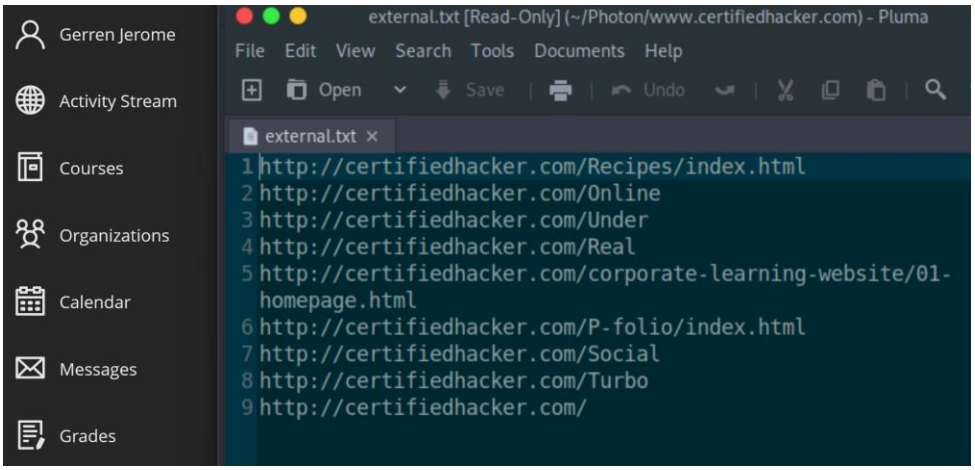


Screengrab: Step 17 – find the hop

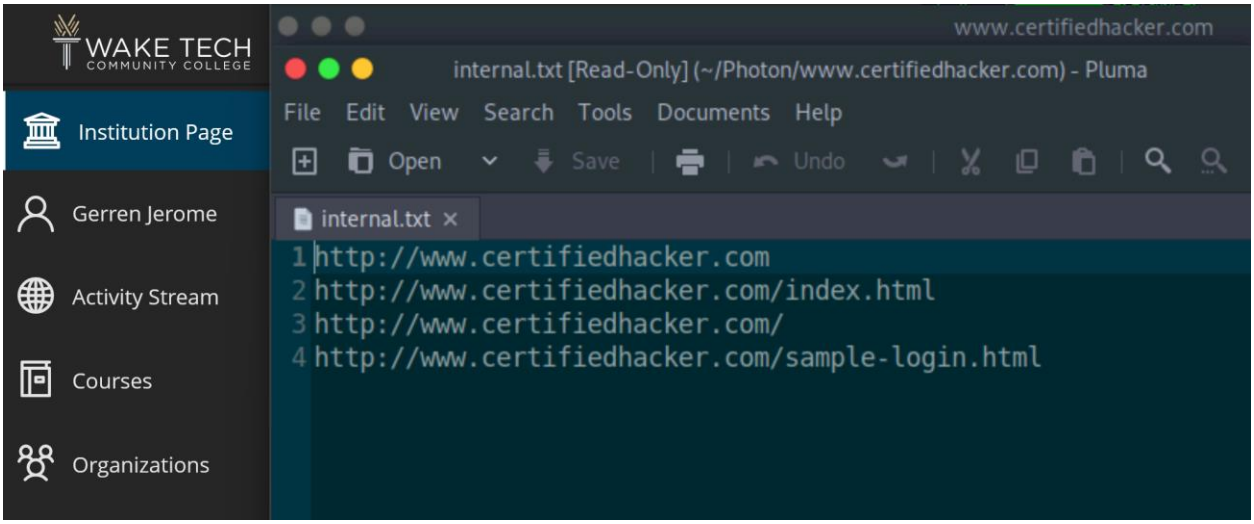


b) Gather information about a target website using Photon

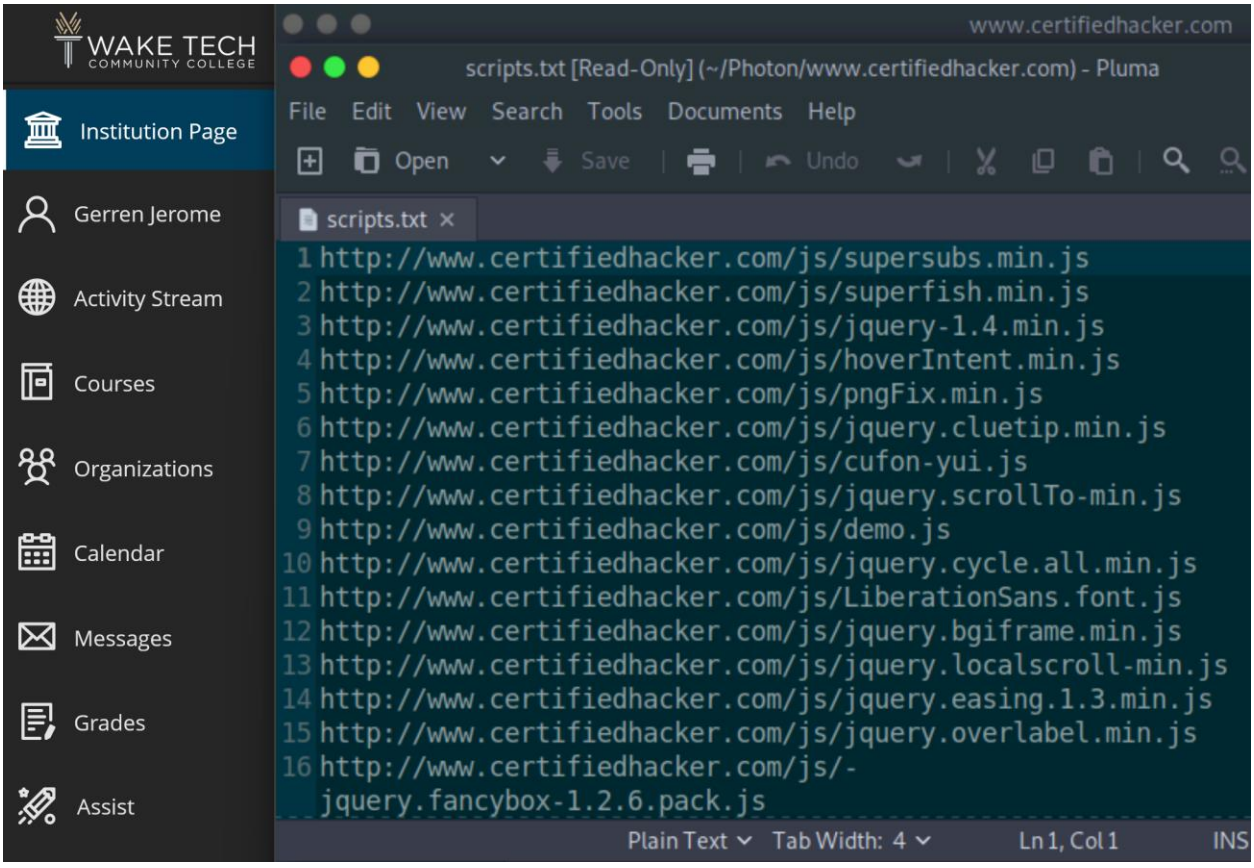
Screengrab: Step 15 – Photon results – external



Screengrab: Step 16 - Photon results – internal

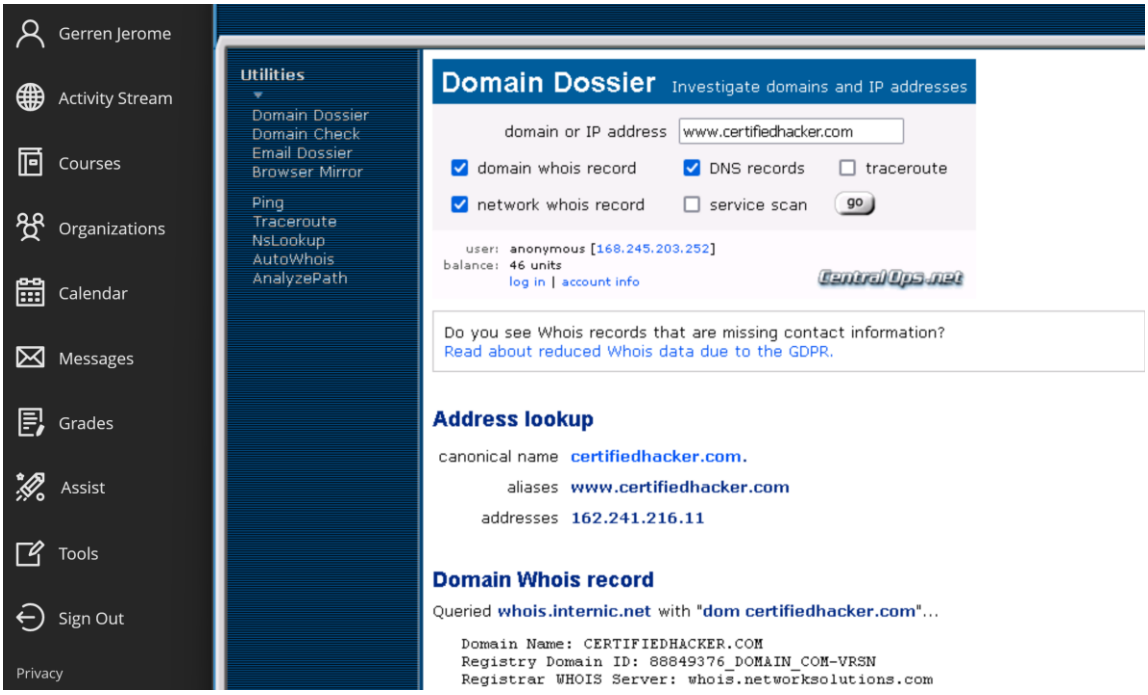


Screengrab: Step 16 - Photon results – scripts



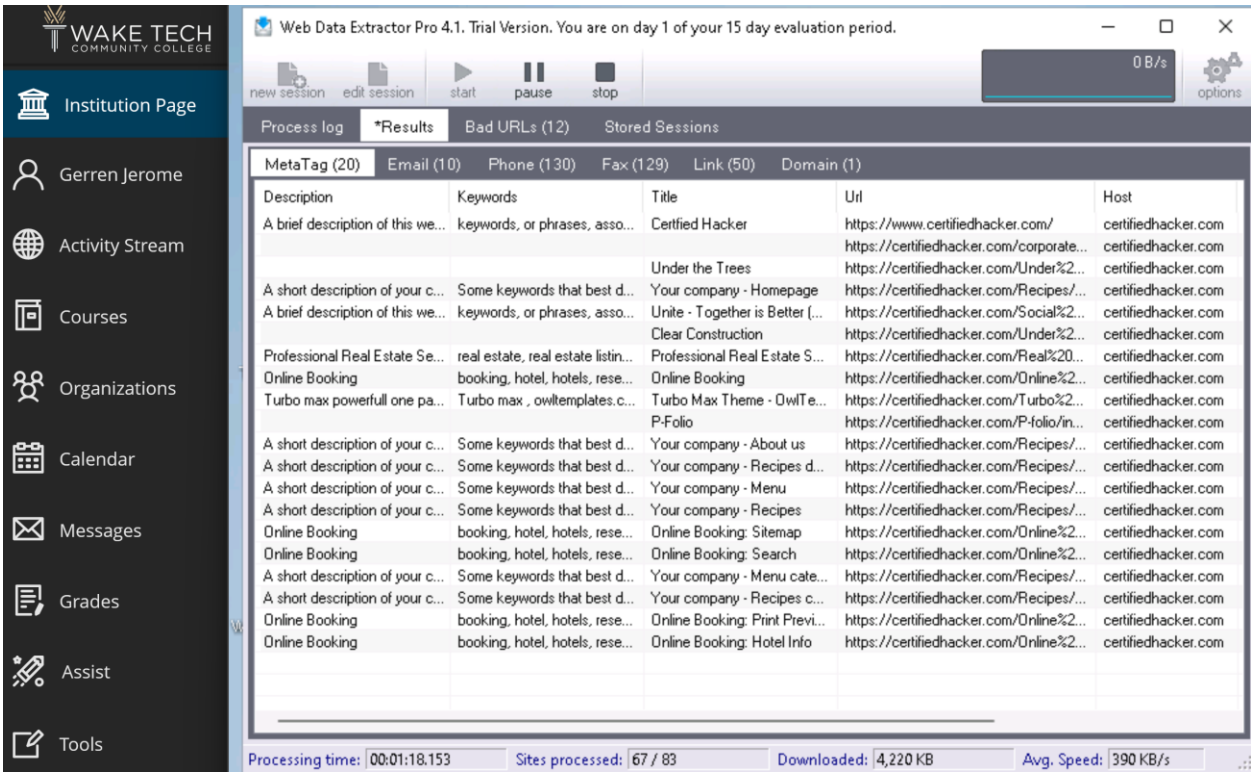
c) Gather information about a target website using Central Ops

Screengrab: Step 3 – CentralOps results



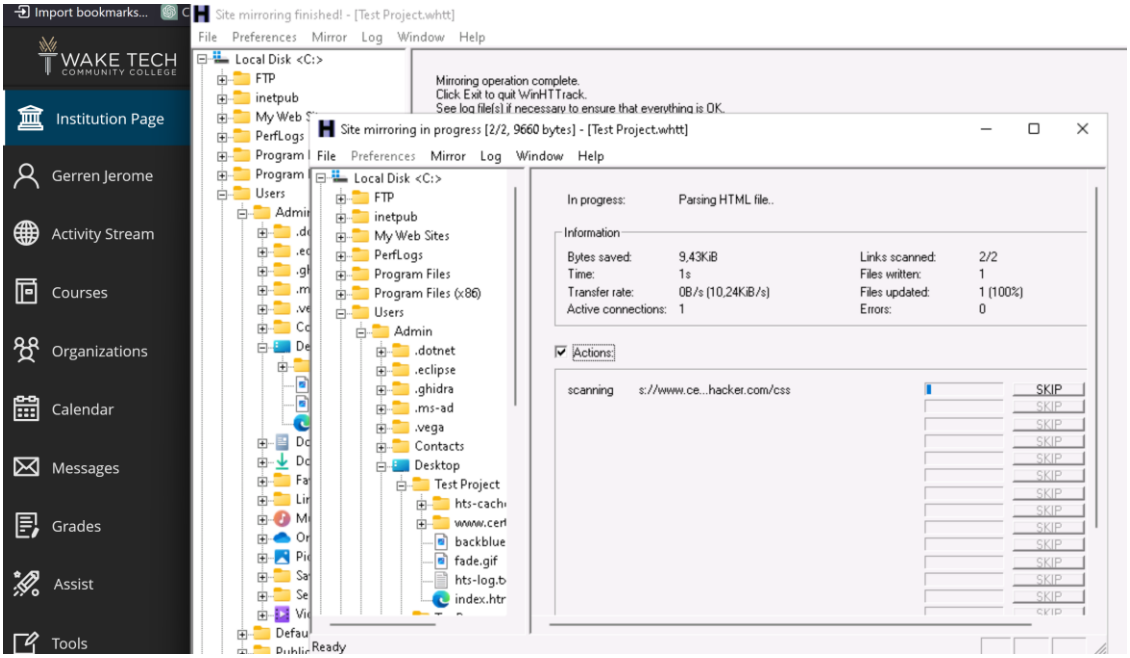
d) Extract a company's data using Web Data Extractor

Screengrab: Step 9 – WEDPro results

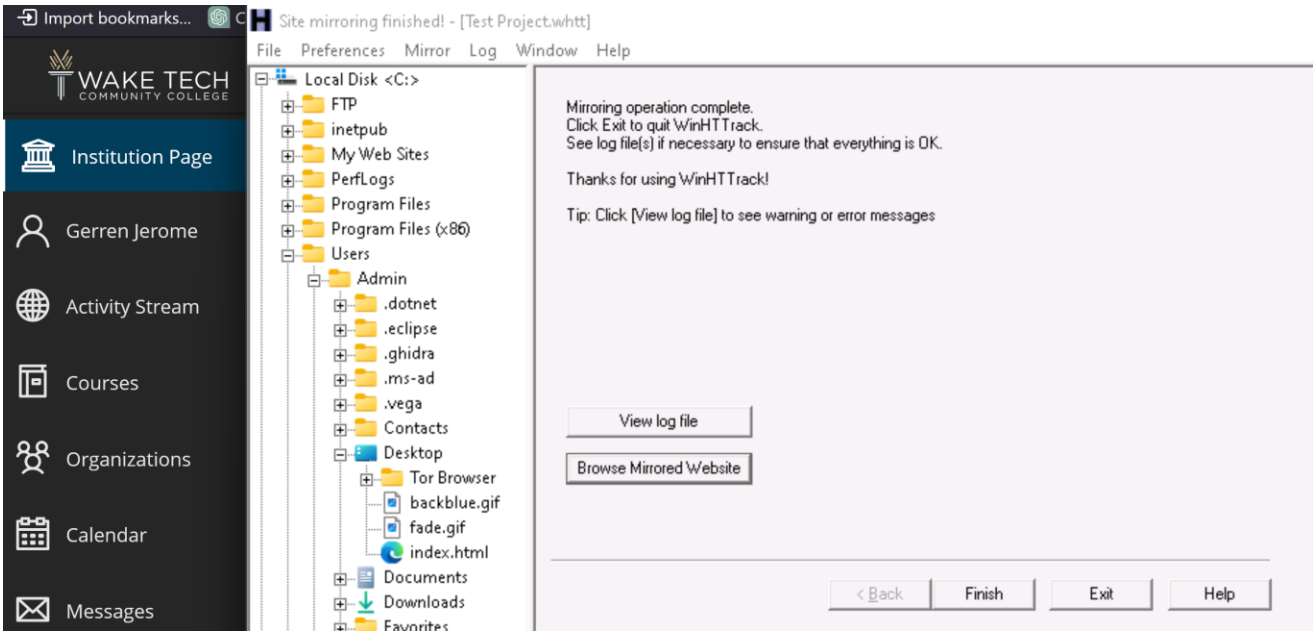


e) Mirror a target website using HTTrack Web Site Copier

Screengrab: Step 8 – Site mirroring progress

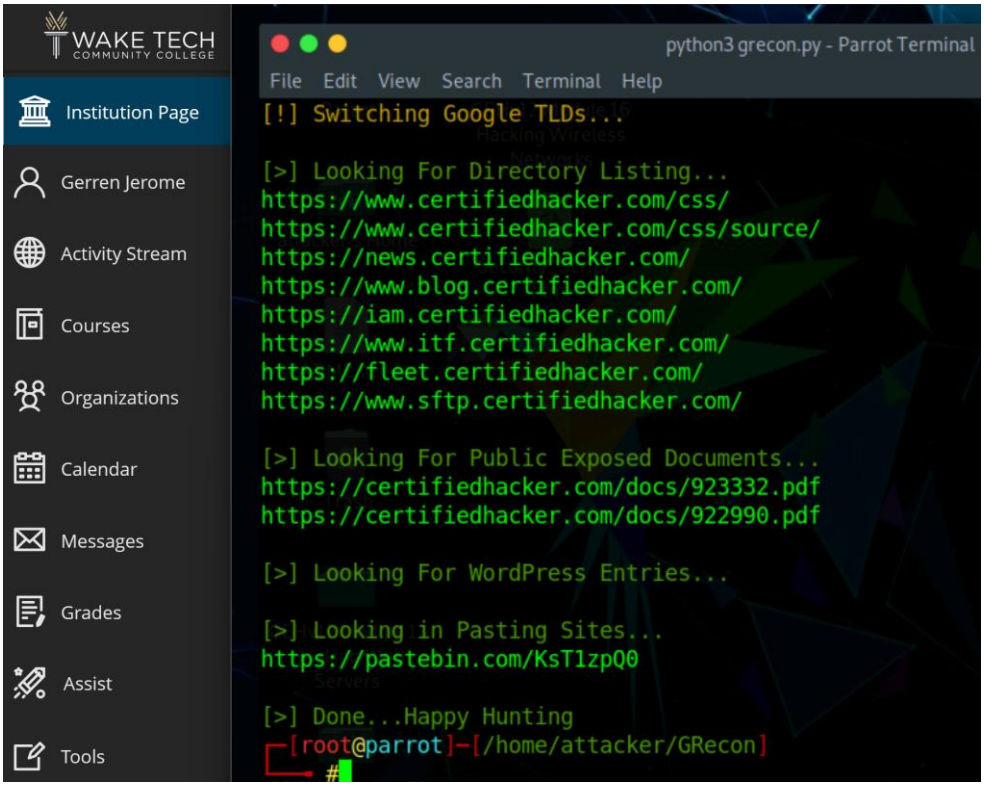


Screengrab: Step 11 – Completed mirroring results



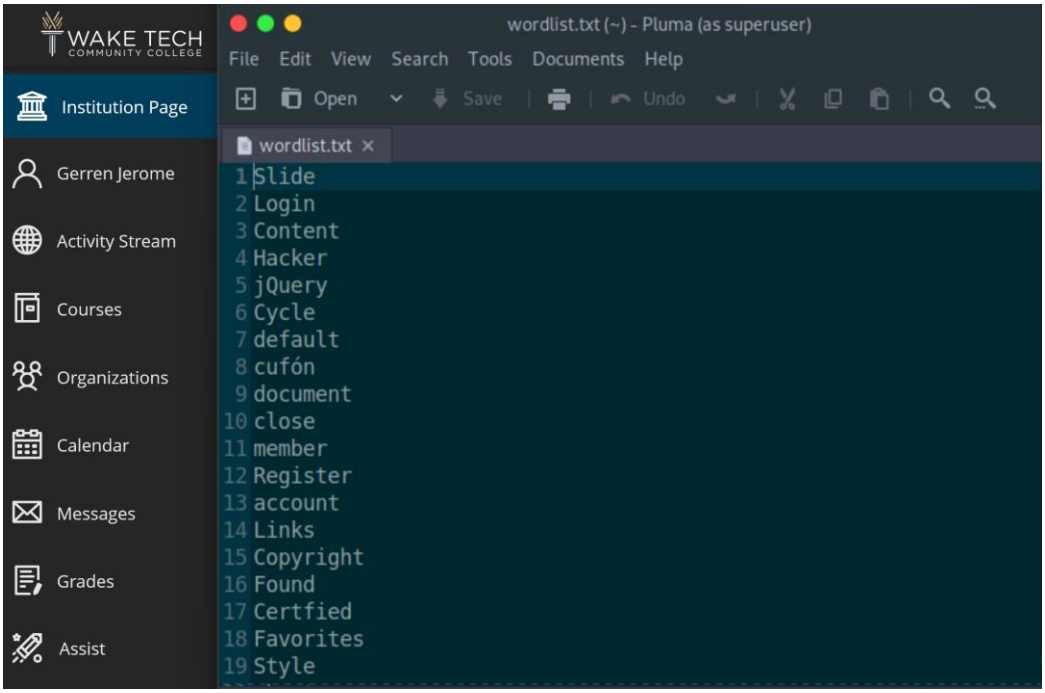
f) Gather information about a target website using GRecon

Screengrab: Step 8 – GRecon results



g) Gather a wordlist from the target website using CeWL

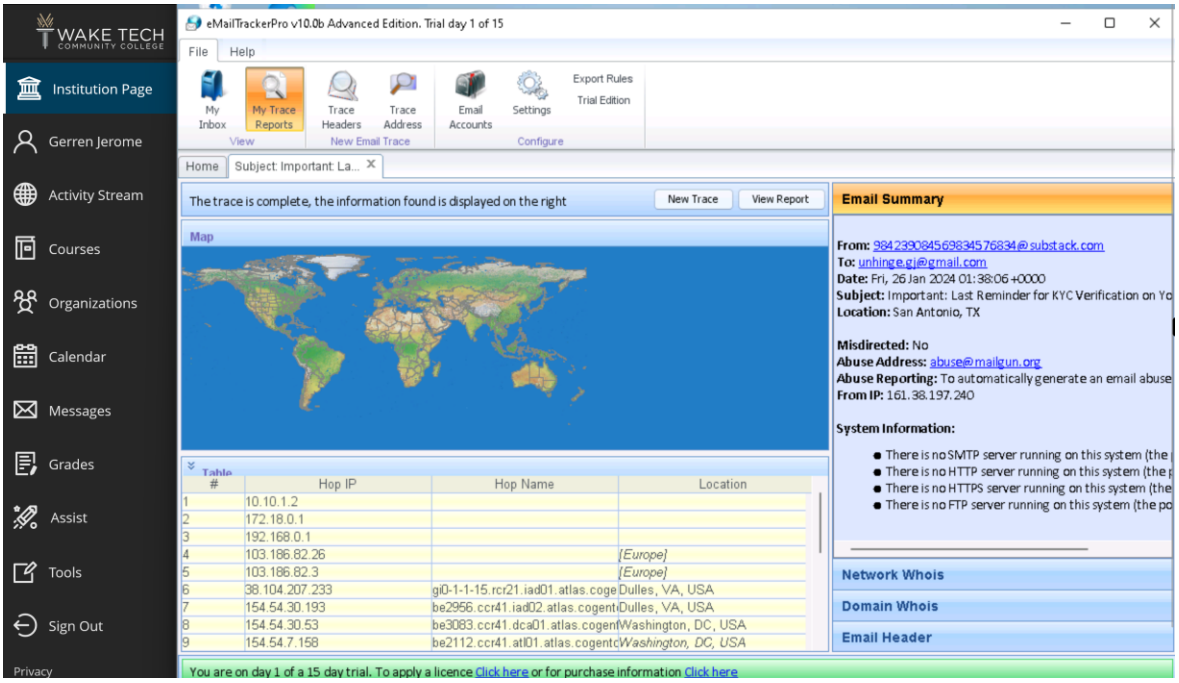
Screengrab: Step 9 – Wordlist output from CeWL



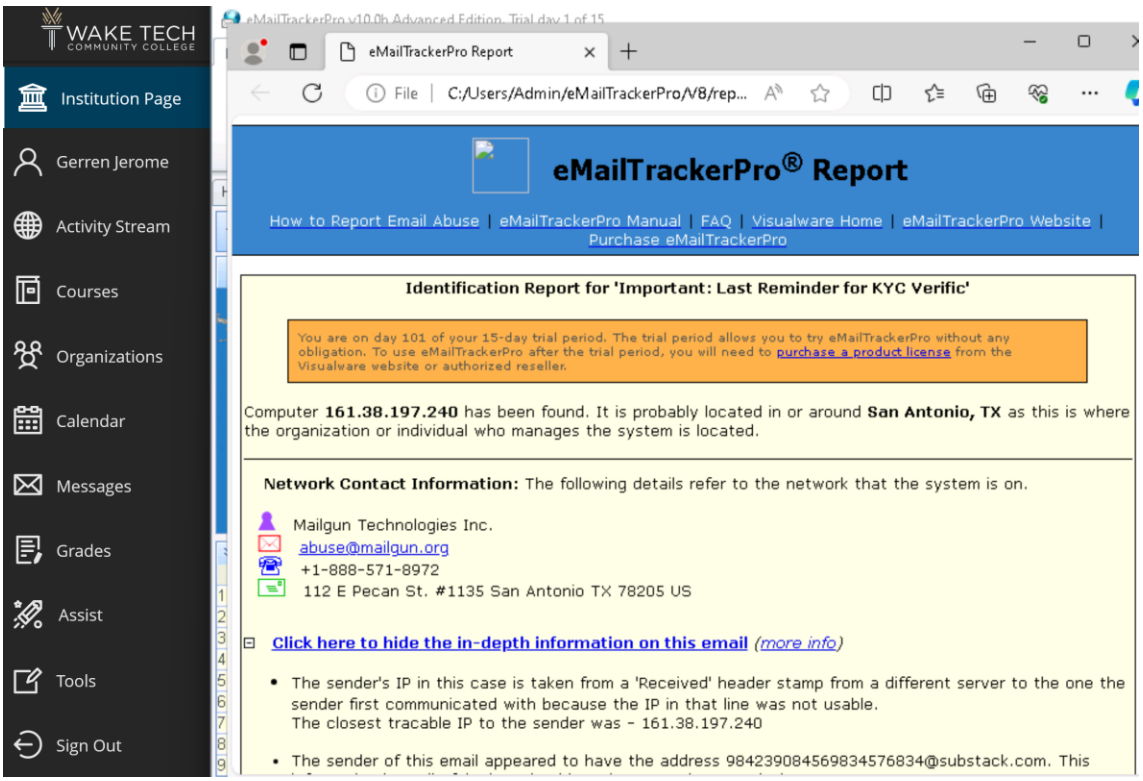
5) Perform email footprinting (2 items)

a) Gather information about a target by tracing emails using eMailTrackerPro

Screengrab: Step 13 – Tracing email header (Map and Summary)



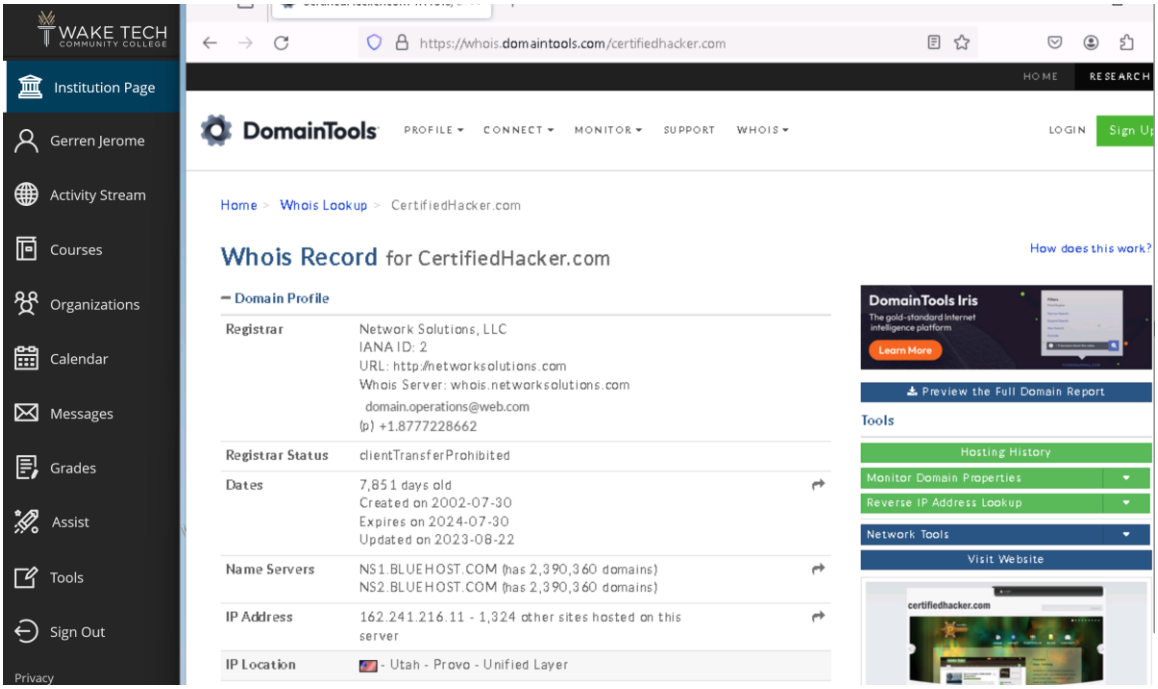
Screengrab: Step 13 – Tracing email header (Report)



6) Perform Whois footprinting (1 item)

a) Perform Whois lookup using DomainTools

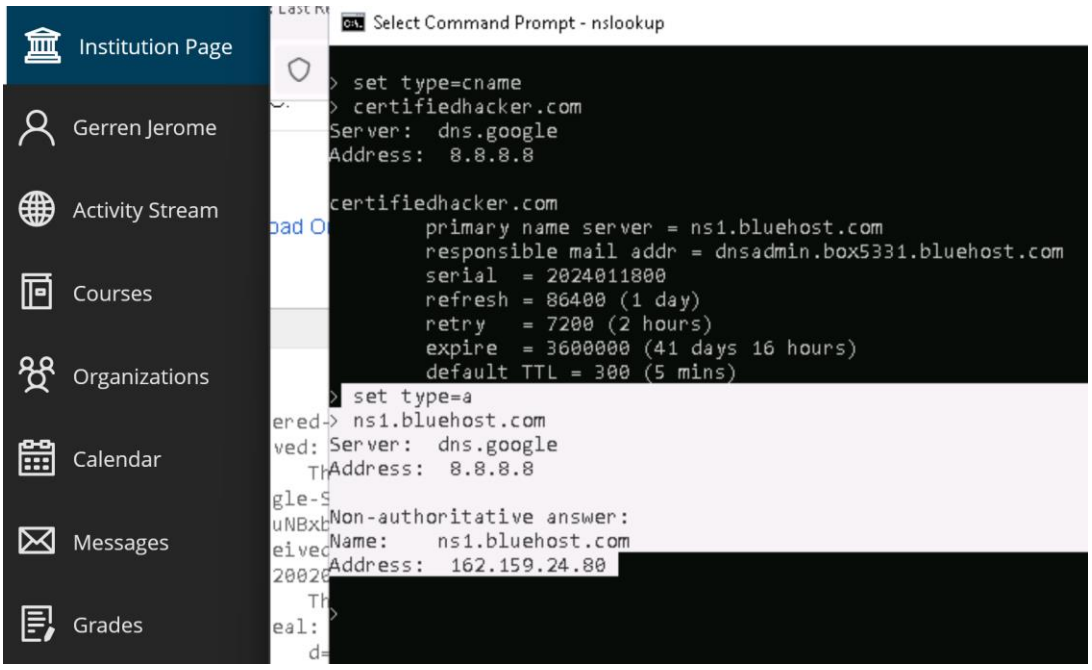
Screengrab: Step 3 – WHOIS Records



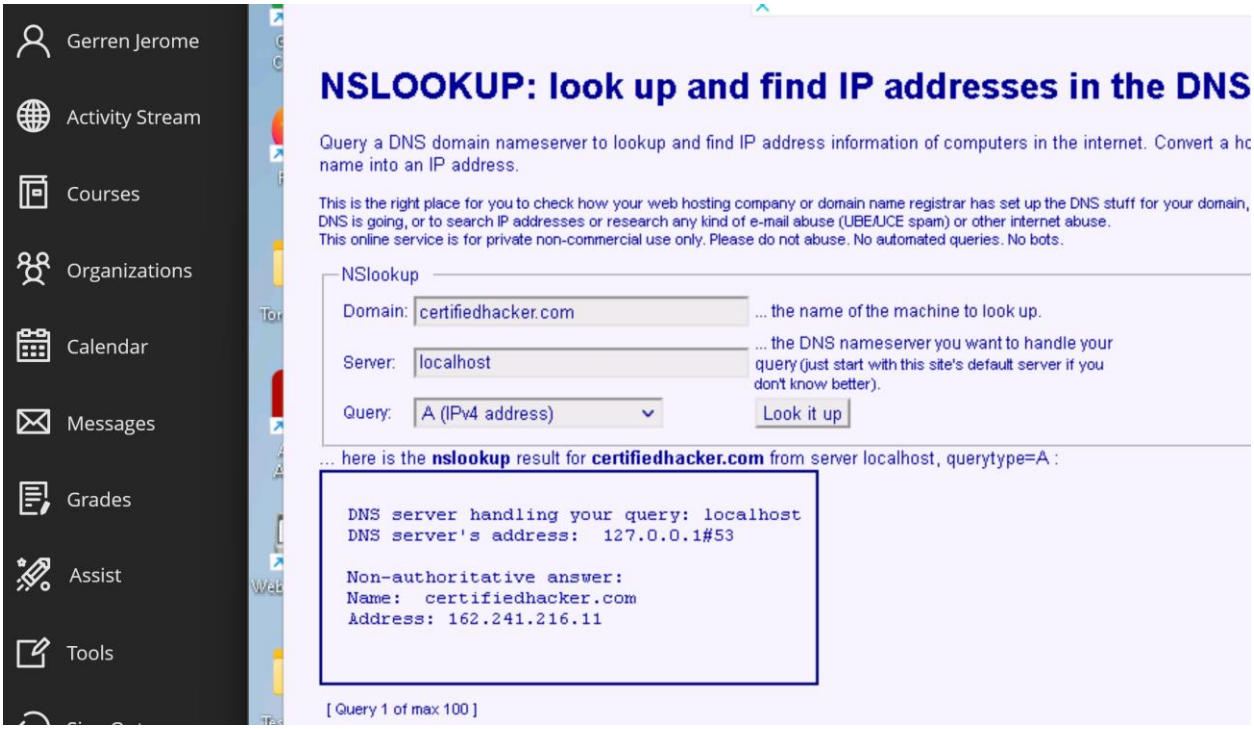
7) Perform DNS footprinting (6 items)

a) Gather DNS information using nslookup command line utility and online tool

Screengrab: Step 12 – DNS recon with nslookup

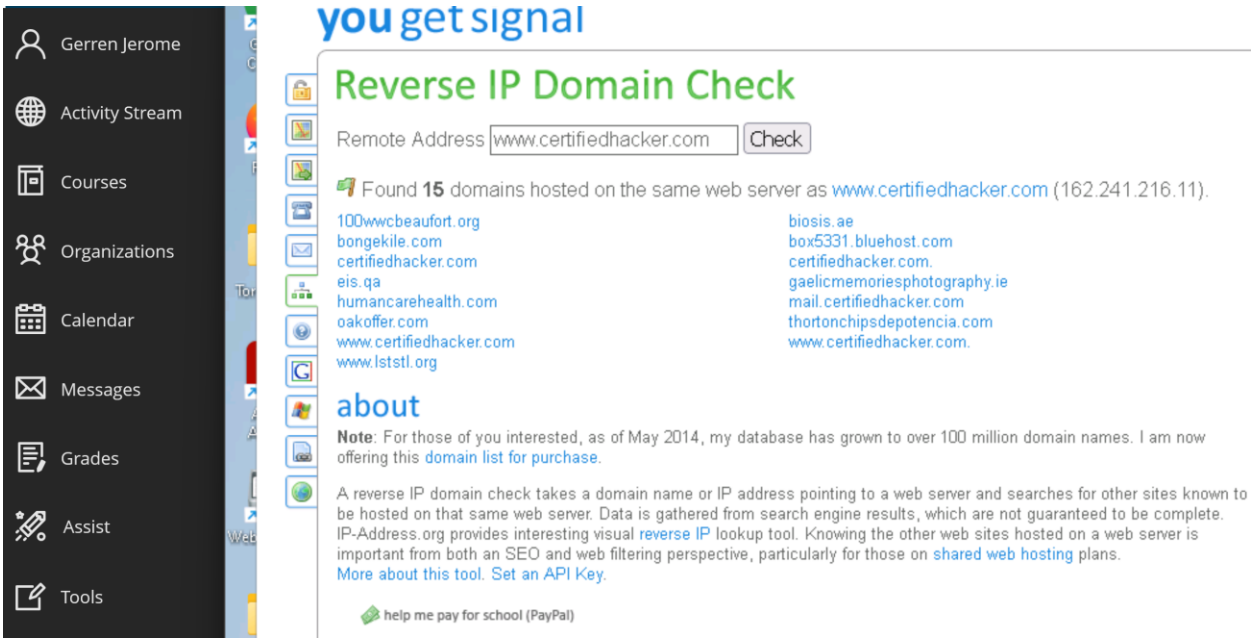


Screengrab: Step 18 – KLOTH.NET results

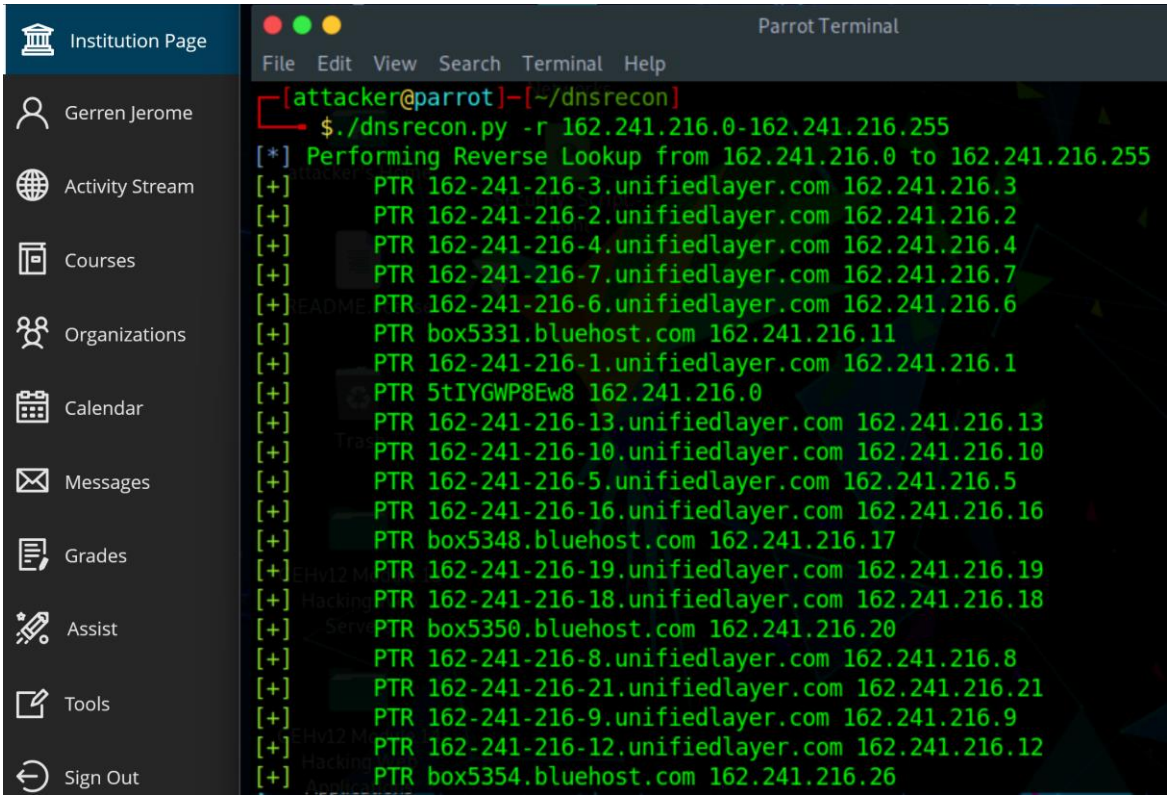


b) Perform reverse DNS lookup using reverse IP domain check and DNSRecon

Screengrab: Step 3 – yougetsignal.com results

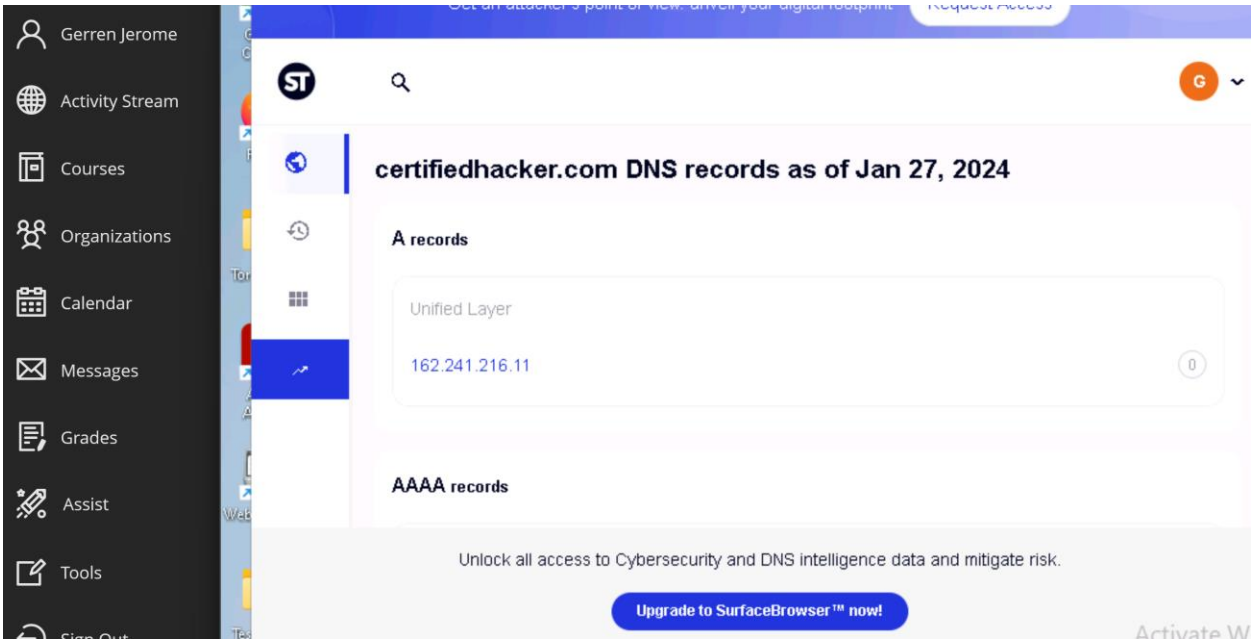


Screengrab: Step 8 – DNSRecon results

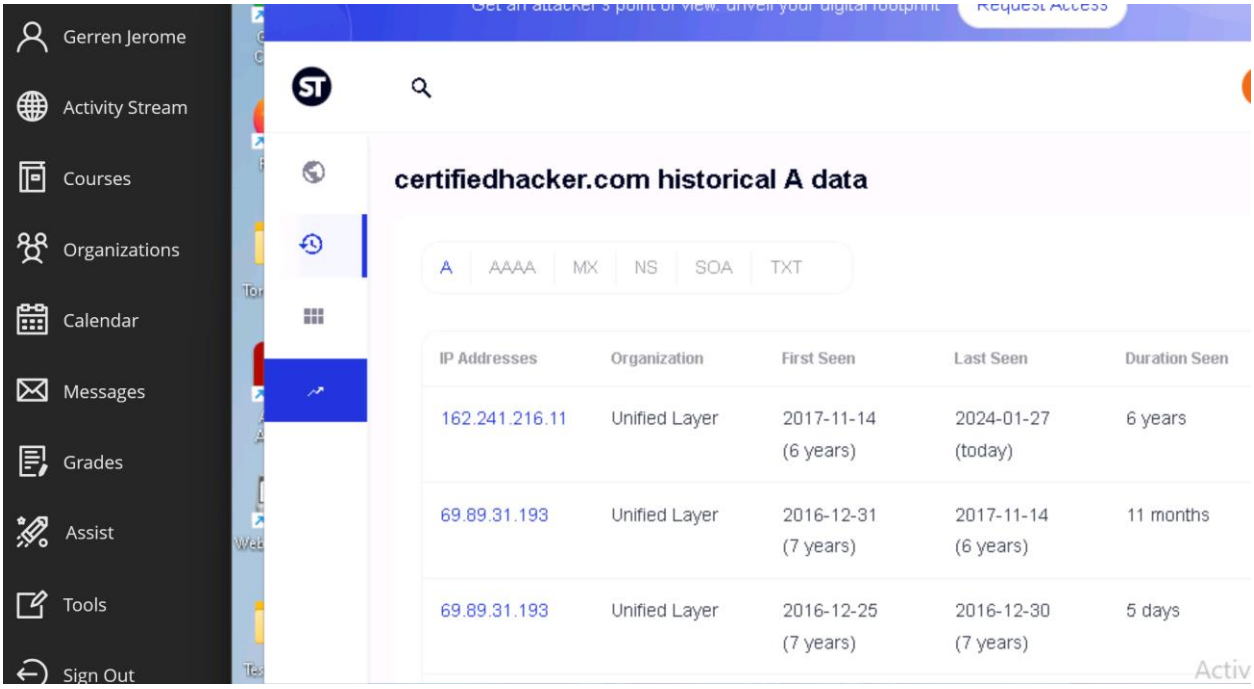


c) Gather information of subdomain and DNS records using SecurityTrails

Screengrab: Step 9 – SecurityTrails search results



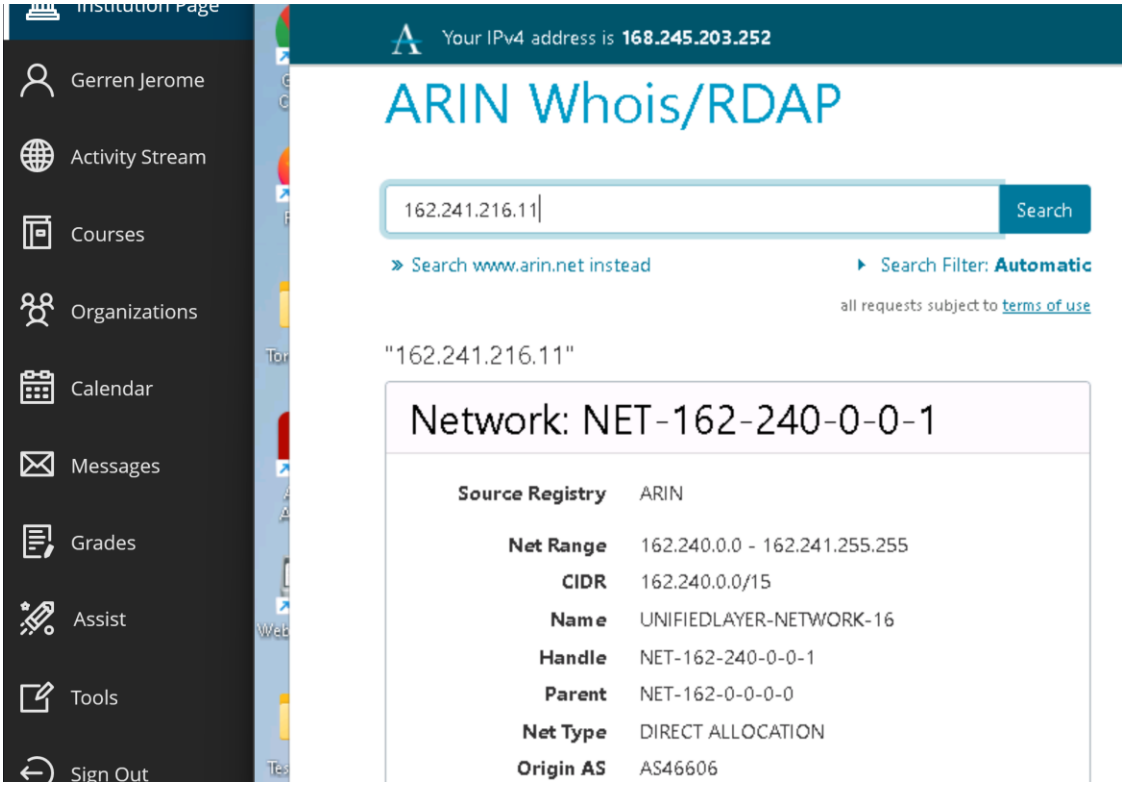
Screengrab: Step 10 – Historical data (A Record)



8) Perform network footprinting (3 items)

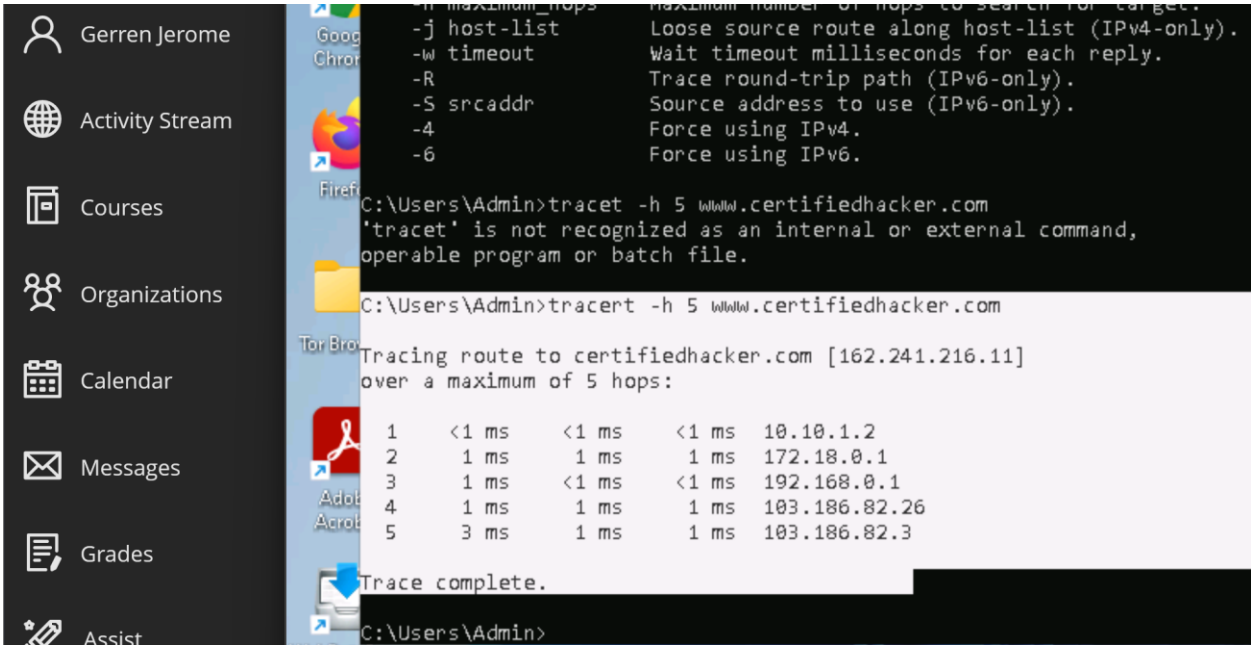
a) Locate the network range

Screengrab: Step 3 – ARIN.net search results

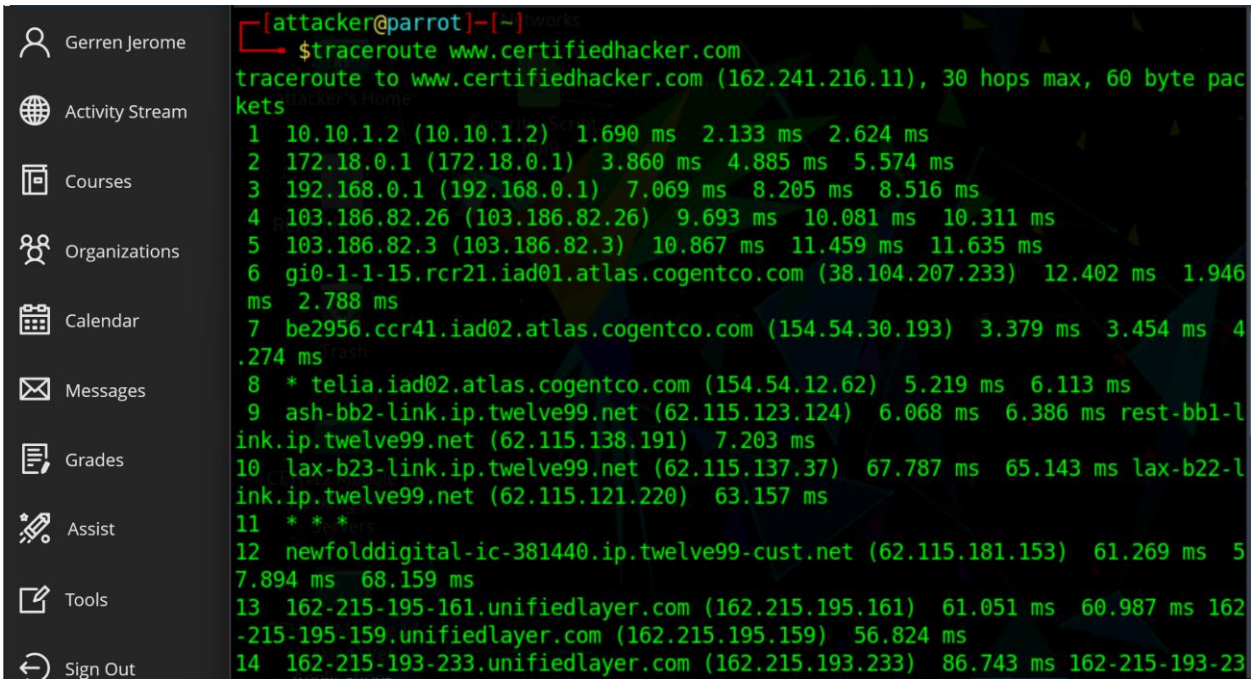


b) Perform network tracerouting in Windows and Linux Machines

Screengrab: Step 3 – tracert results (WIN)



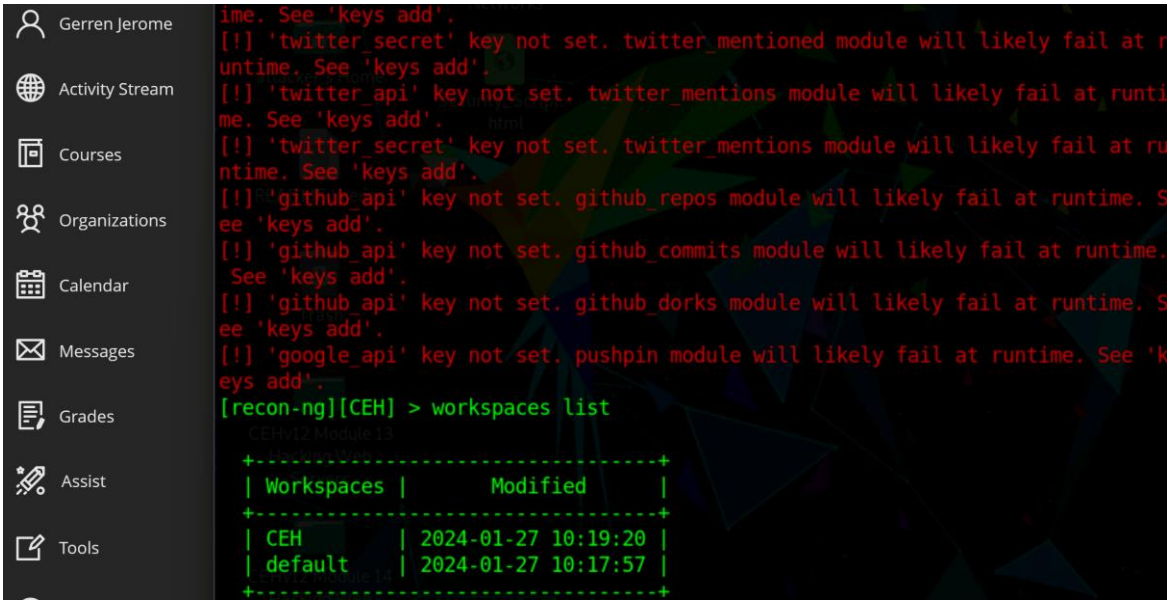
Screengrab: Step 7 - traceroute results (LNX)



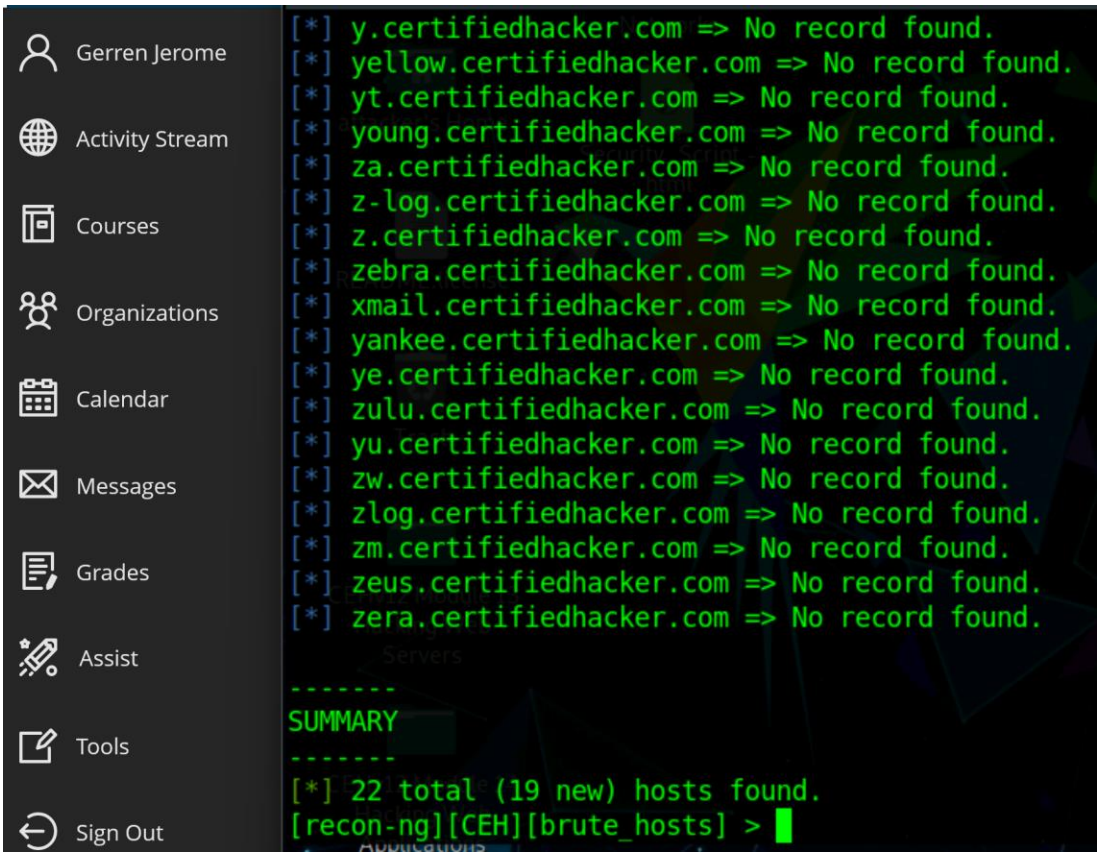
9) Perform footprinting using various footprinting tools (19 items)

a) Footprinting a target using Recon-ng

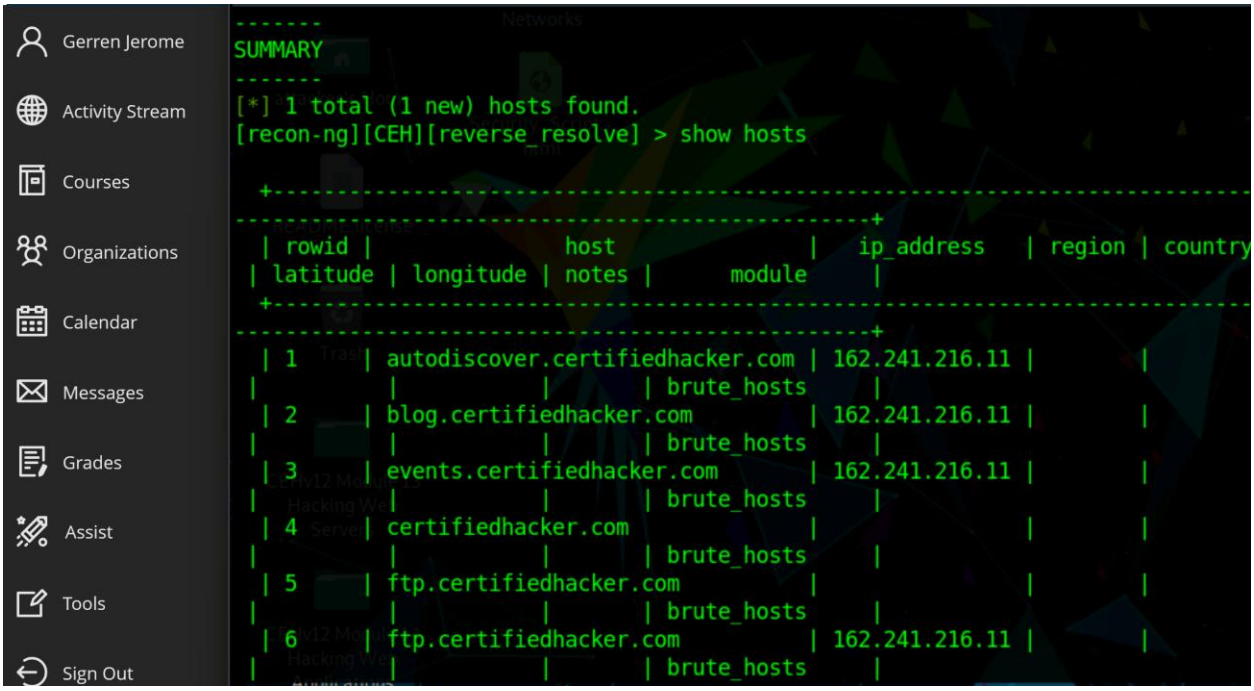
Screengrab: Step 14 – confirm created workspace



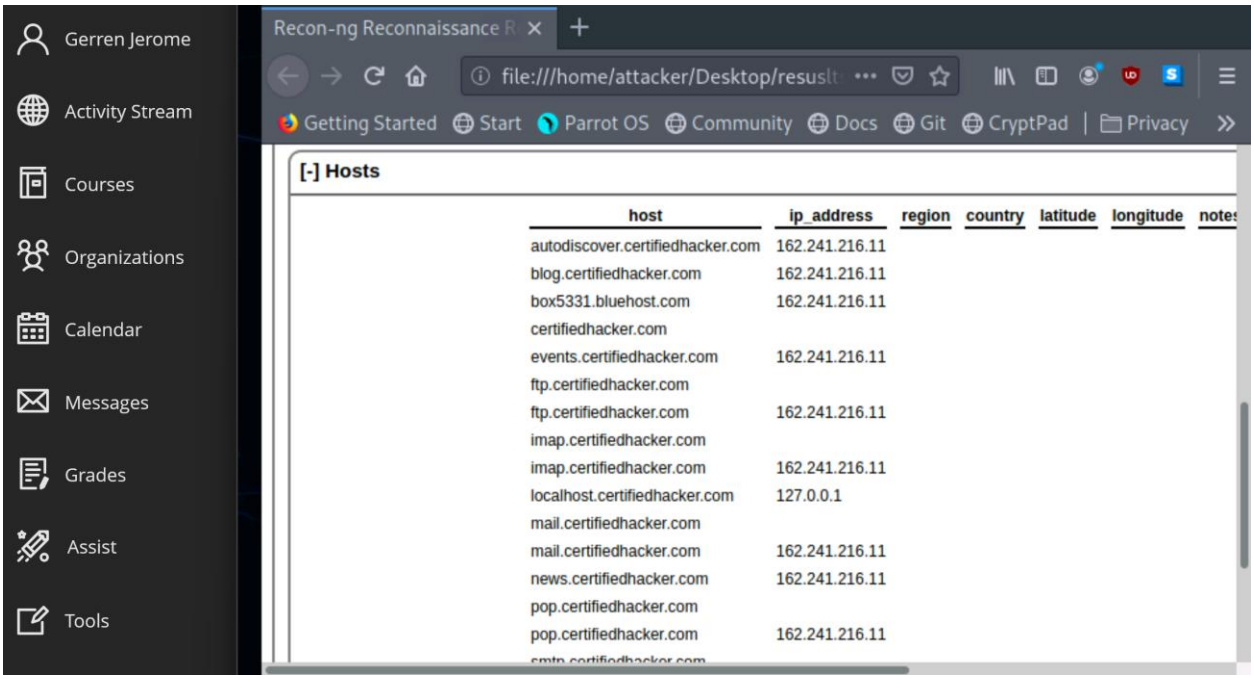
Screengrab: Step 23 – recon-ng results (brute_hosts)



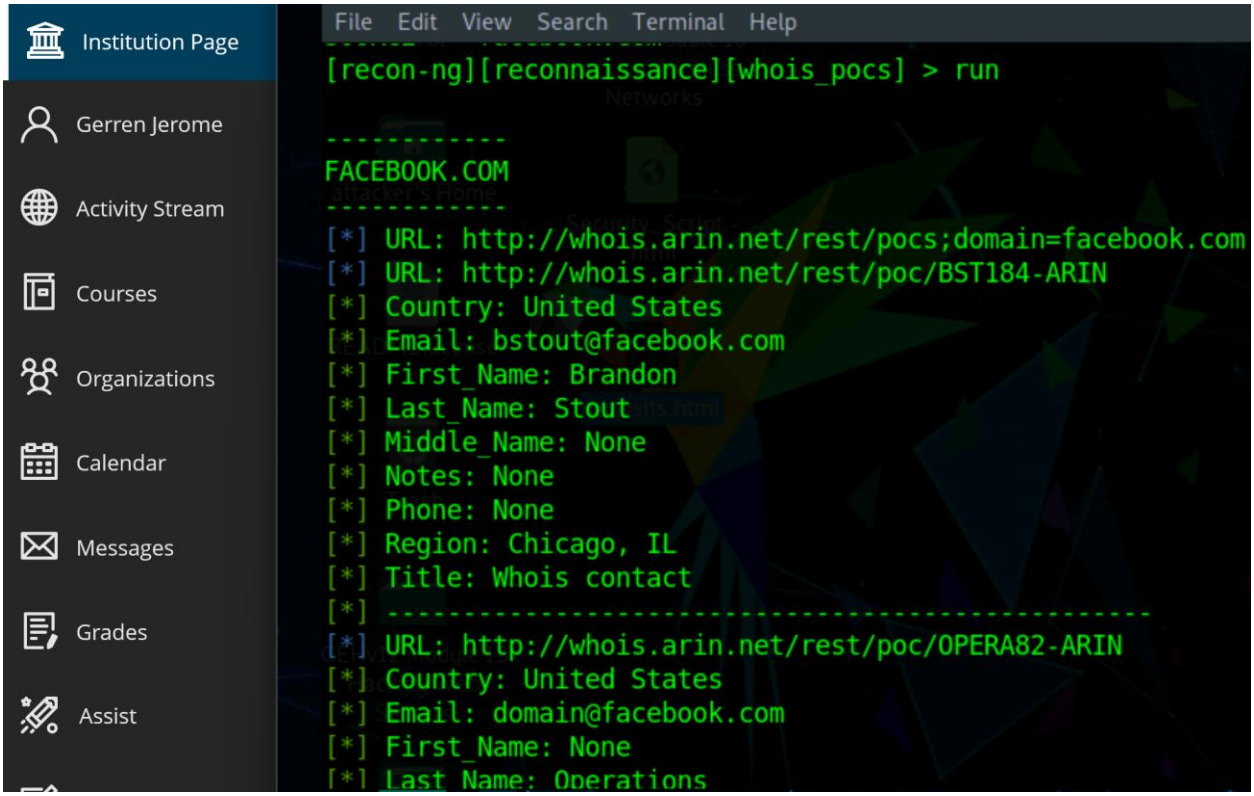
Screengrab: Step 29 – harvested host results (Attacker Window)



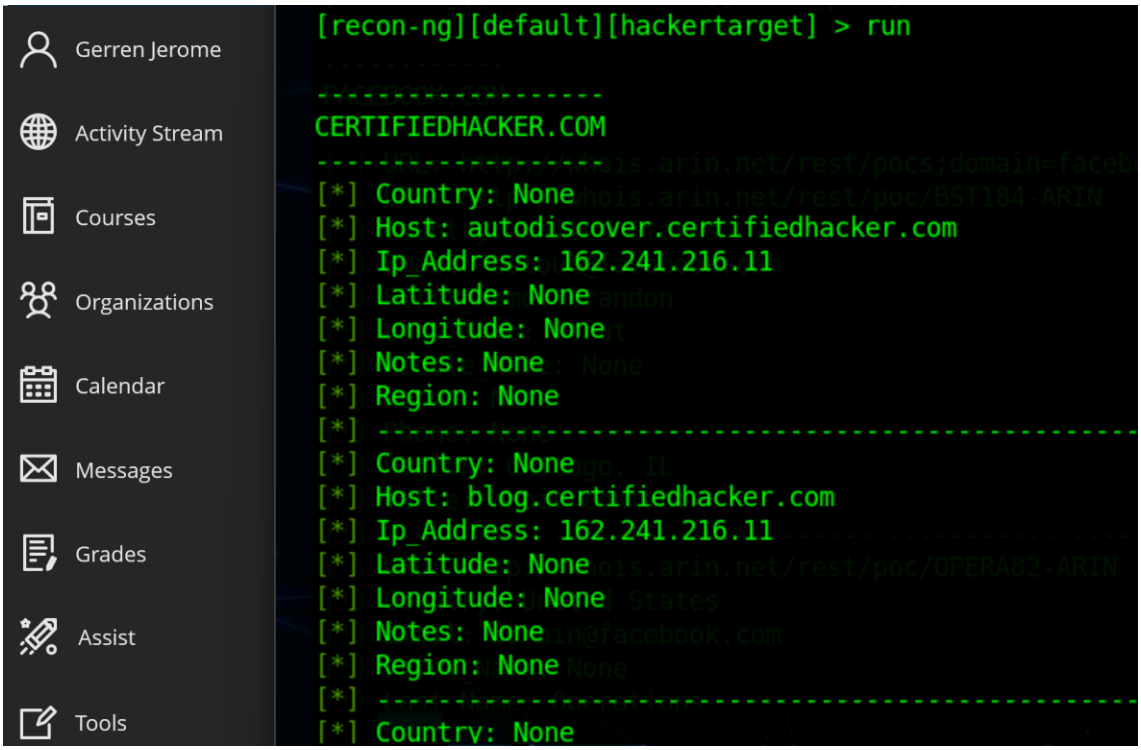
Screengrab: Step 43 - harvested host results (HTML report)



Screengrab: Step 56 – WHOIS_POCS results

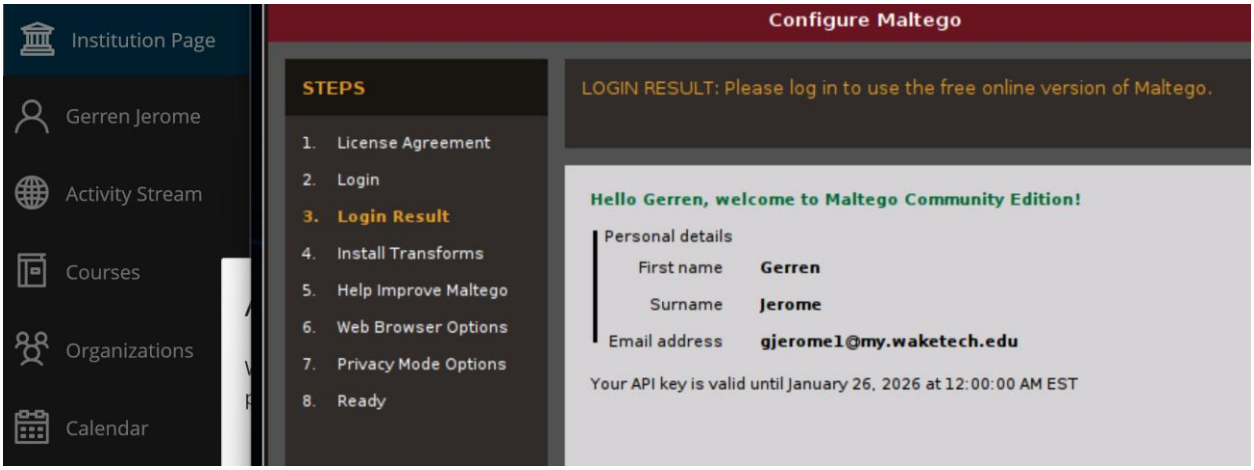


Screengrab: Step 66 – HackerTarget results

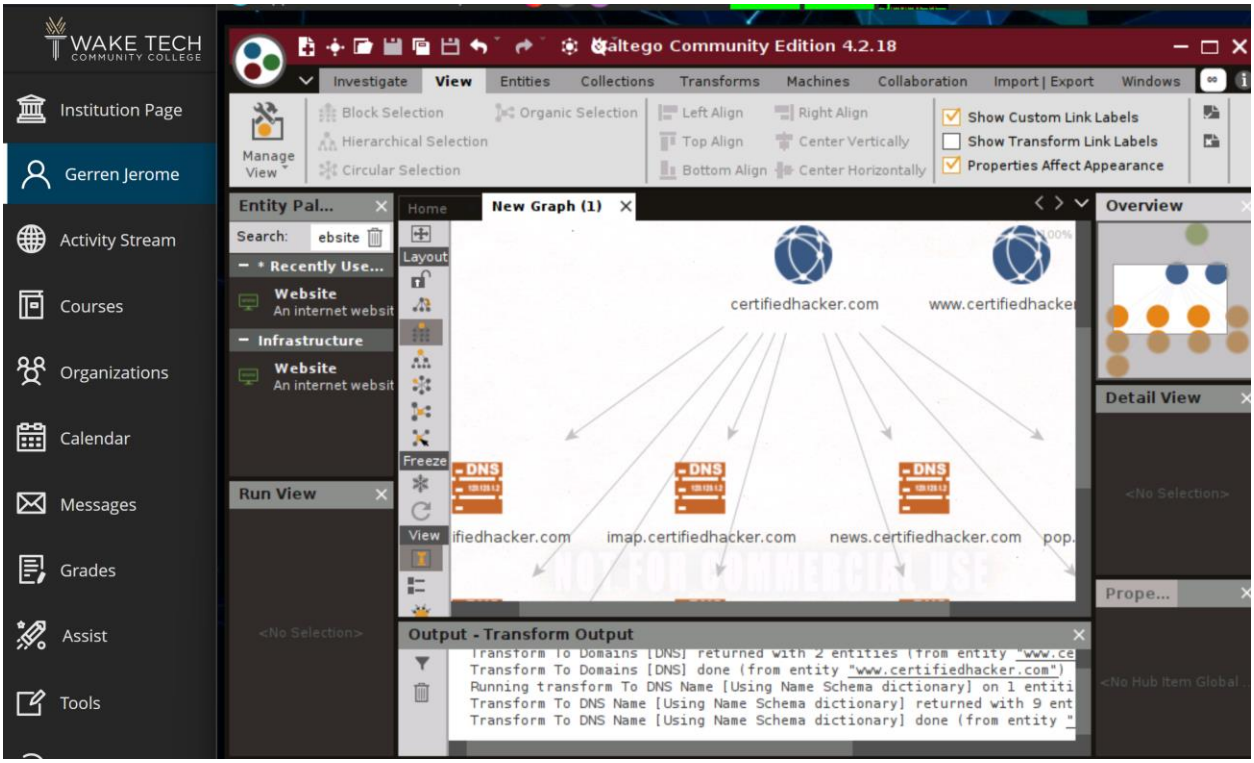


b) Footprinting a target using Maltego

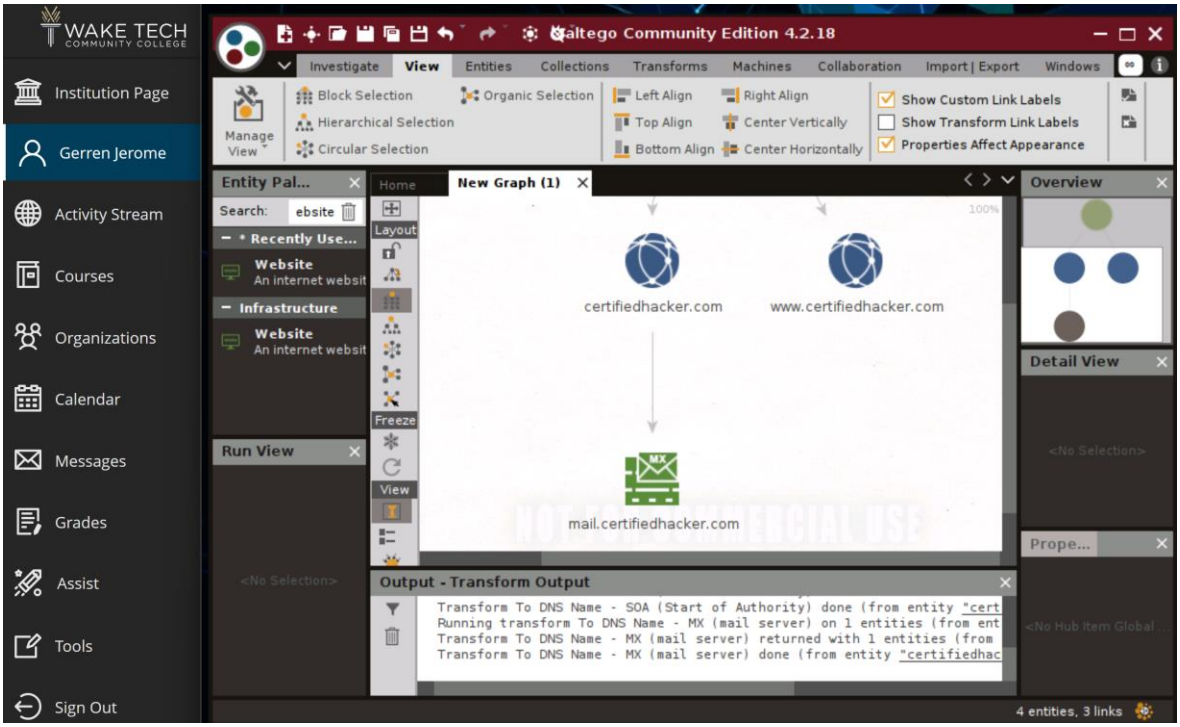
Screengrab: Step 11 – Login Successful



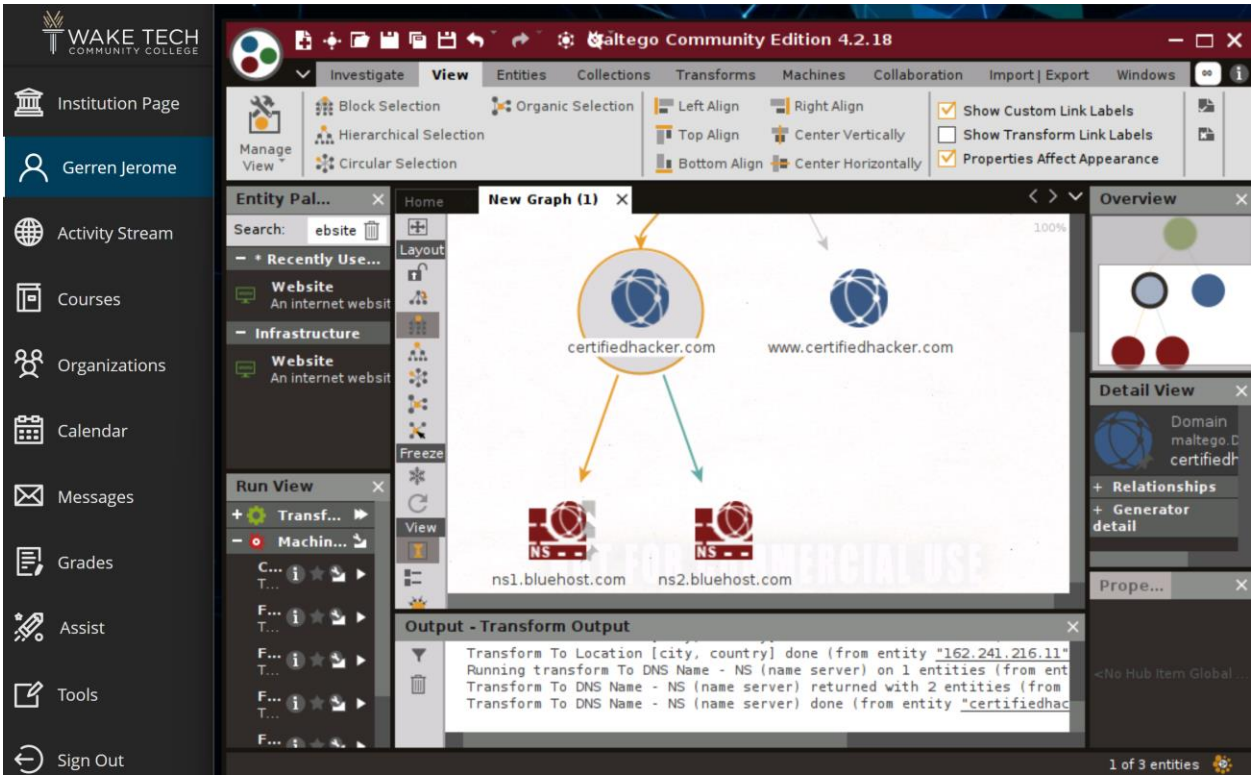
Screengrab: Step 27 – Transform (DNS) – identify and parse



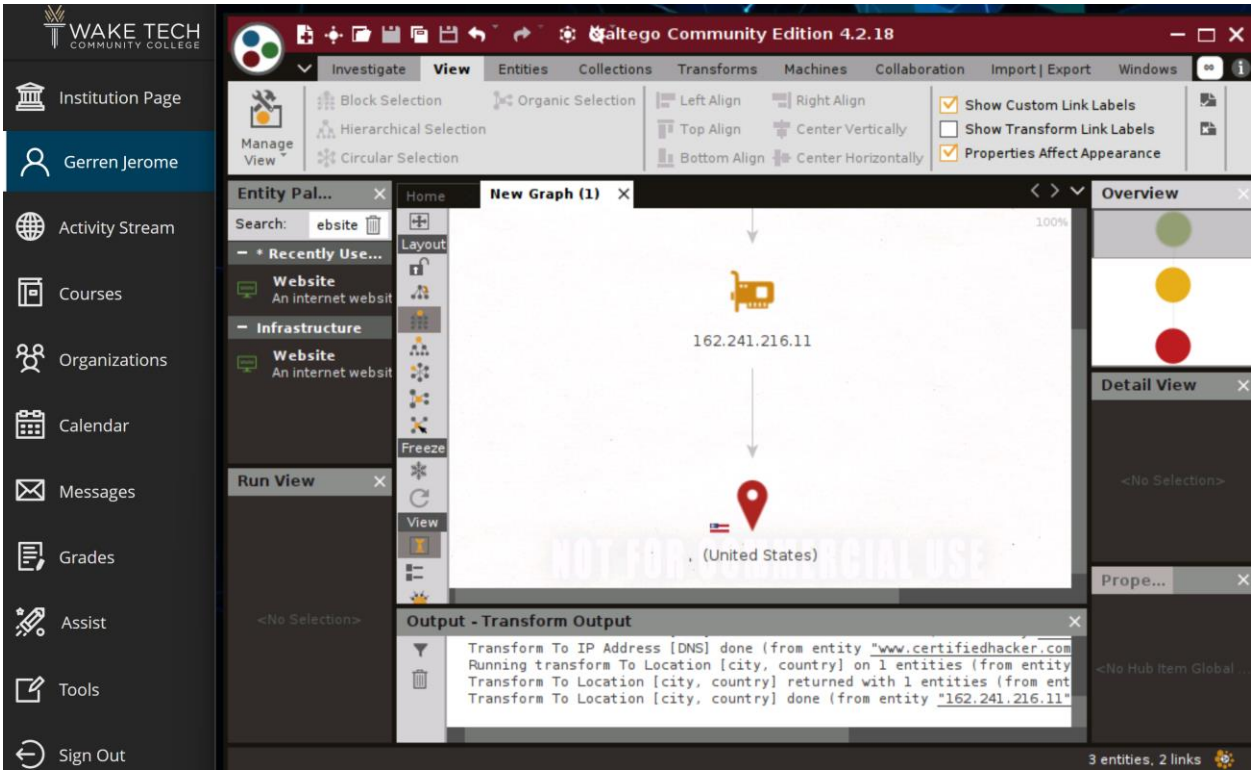
Screengrab: Step 35 – Transform (MX) - identify and parse



Screengrab: Step 39 – Transform (NS) - identify and parse

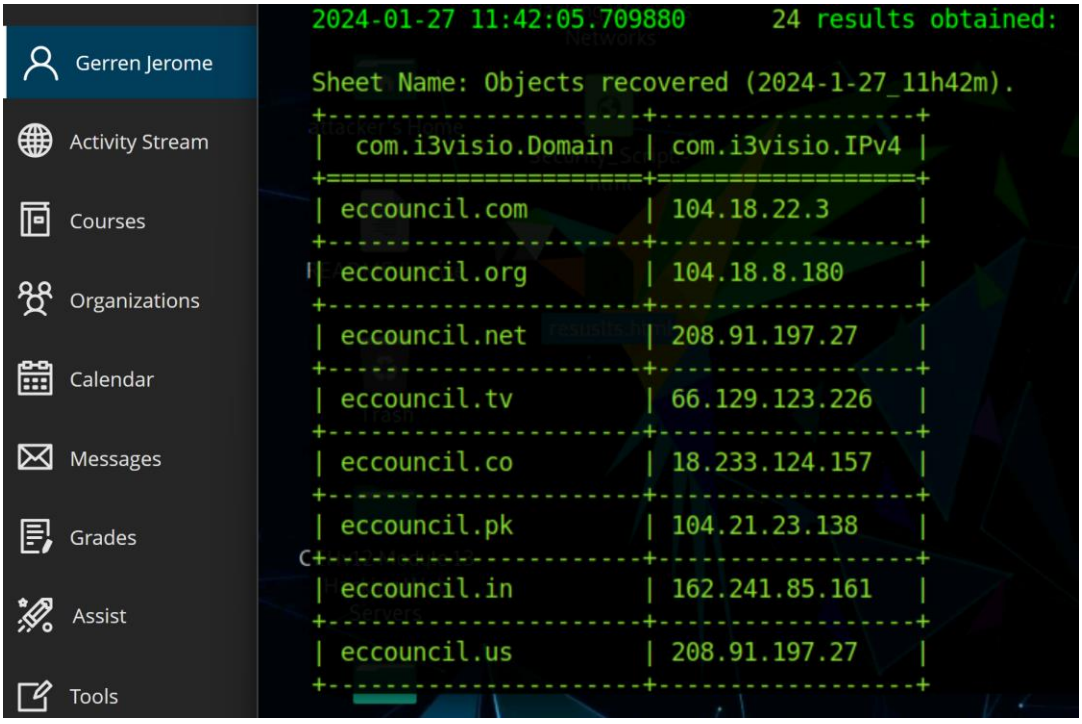


Screengrab: Step 46 – Location (city, country)

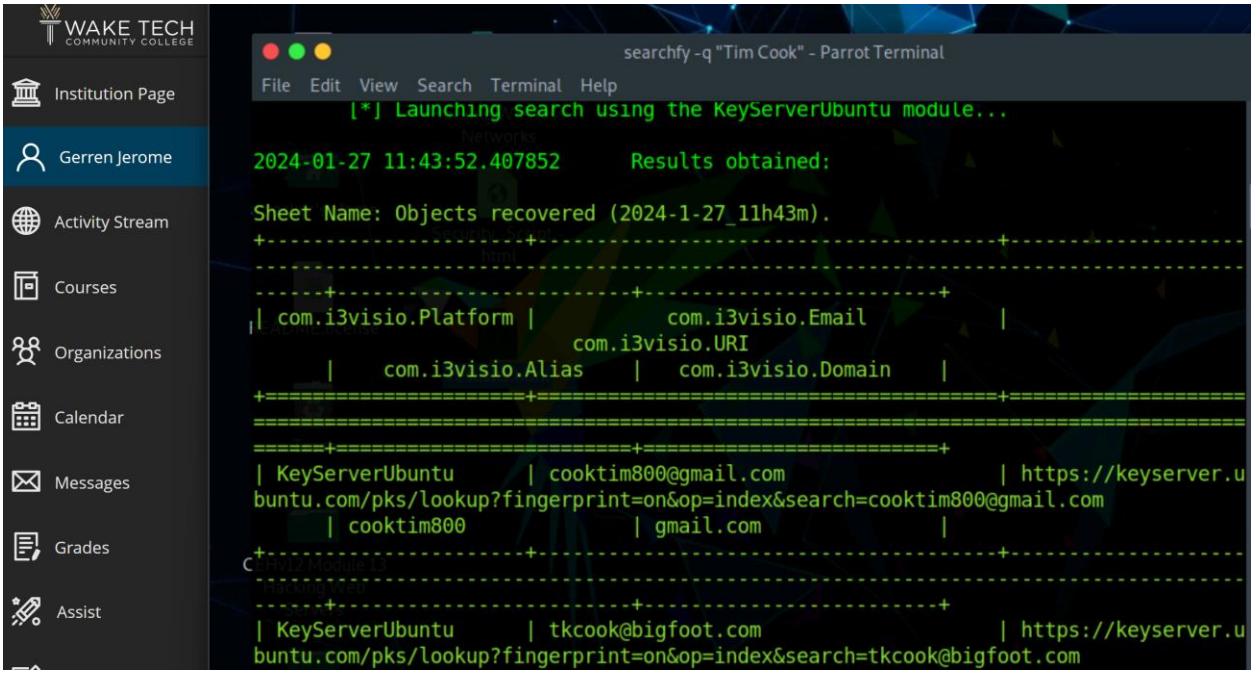


c) Footprinting a target using OSRFramework

Screengrab: Step 6 – Domainfy results

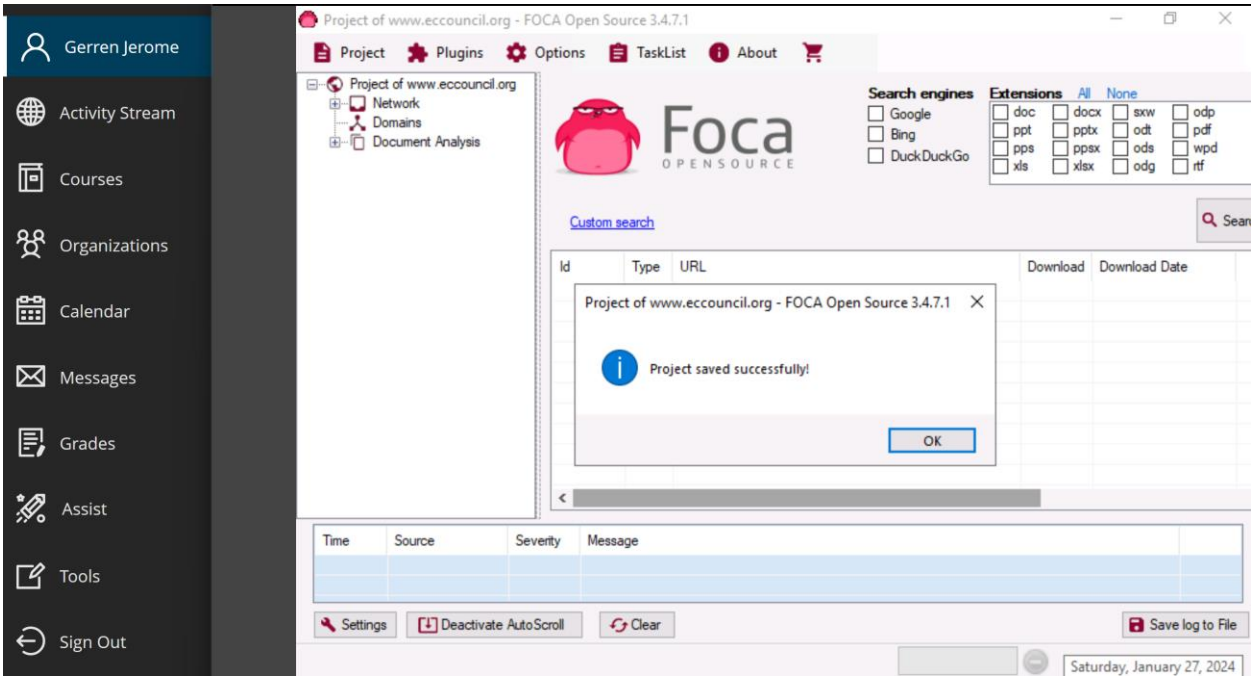


Screengrab: Step 8 – Searchfy results

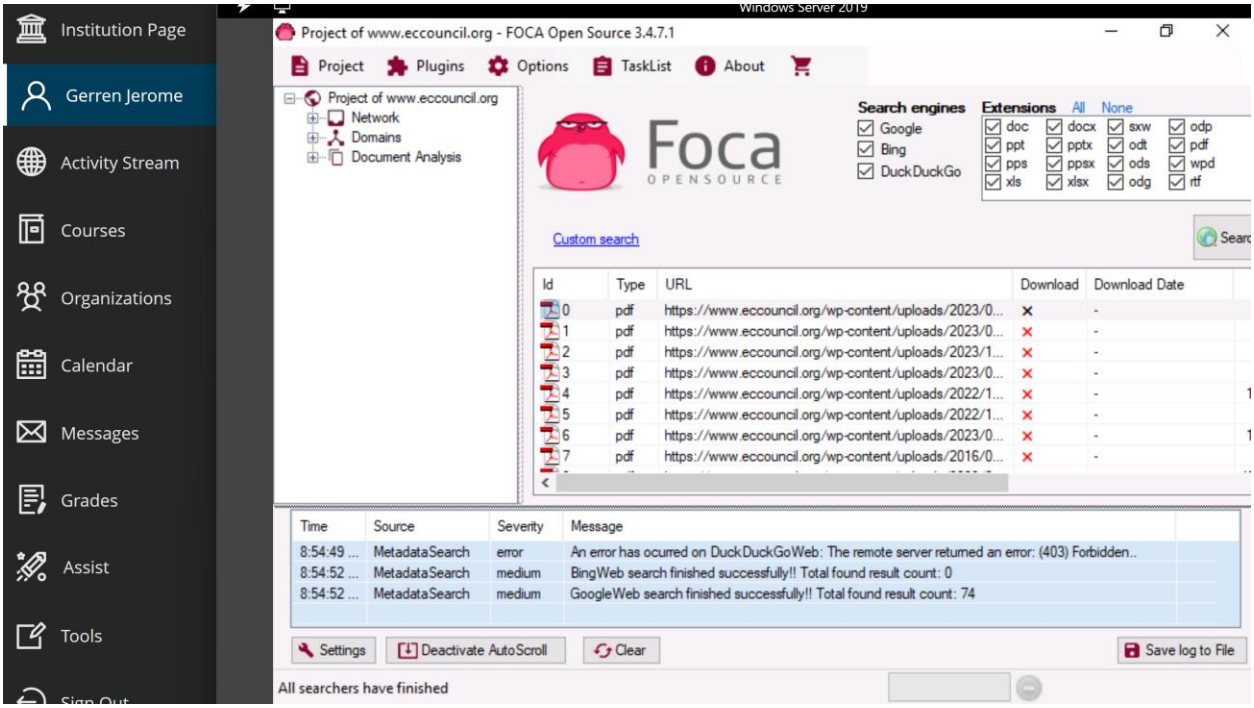


d) Footprinting a target using FOCA

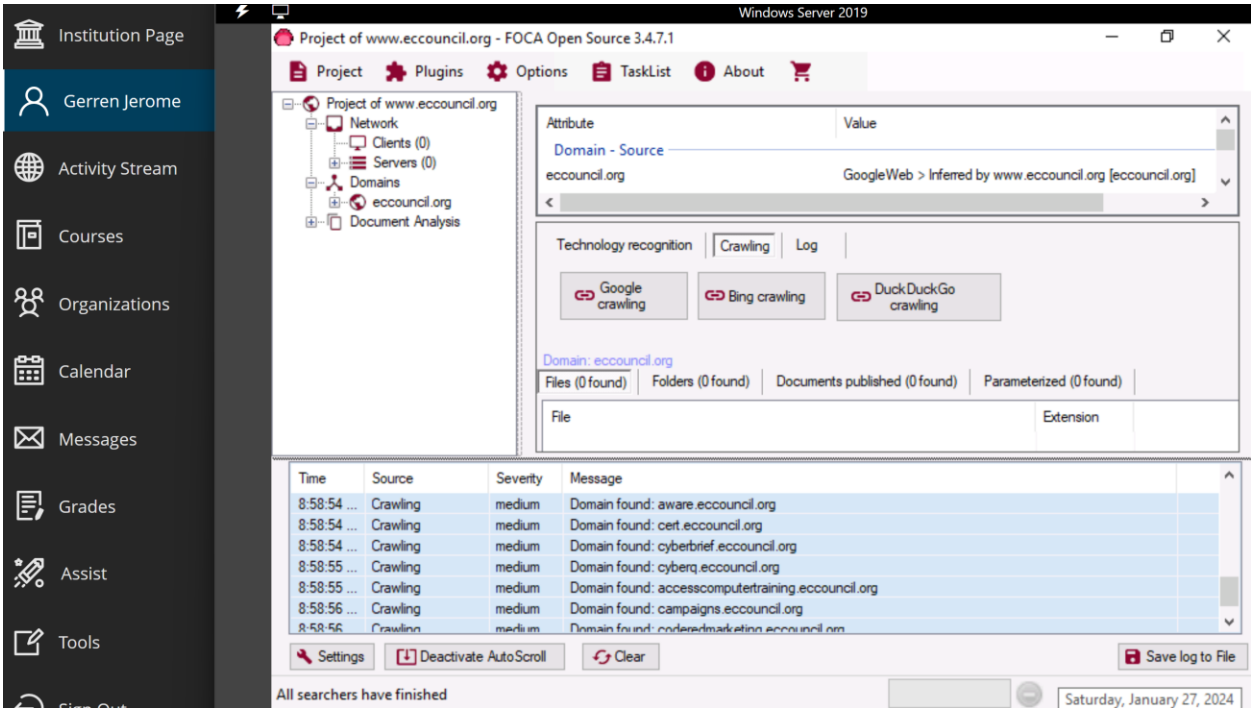
Screengrab: Step 8 – Project saved successfully!



Screengrab: Step 12 – Search All results

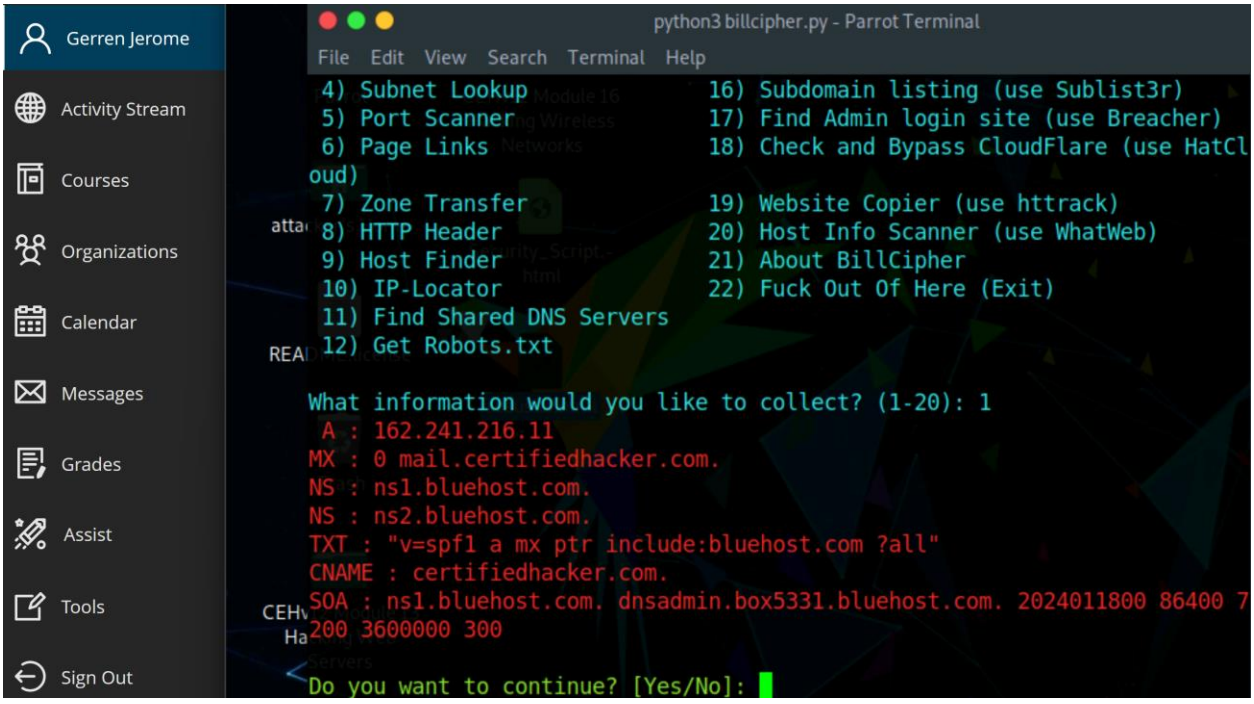


Screengrab: Step 20 – Crawling results

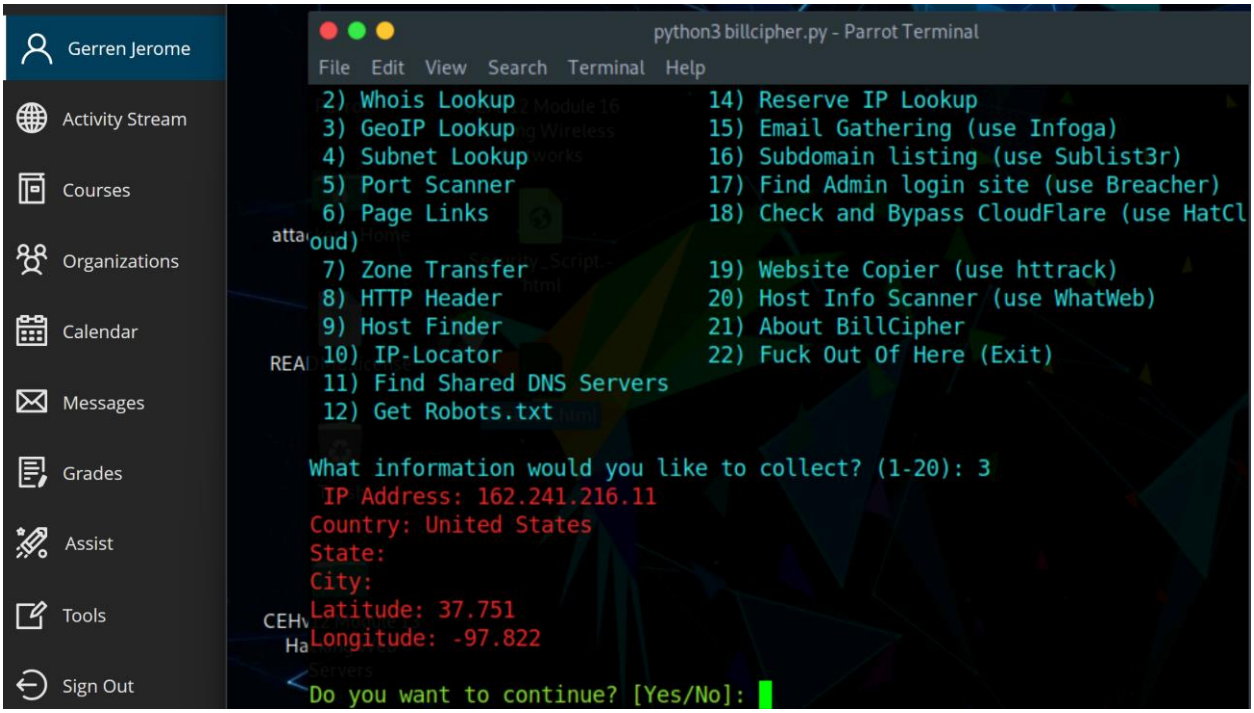


e) Footprinting a target using BillCipher (NSFW language in the interface)**

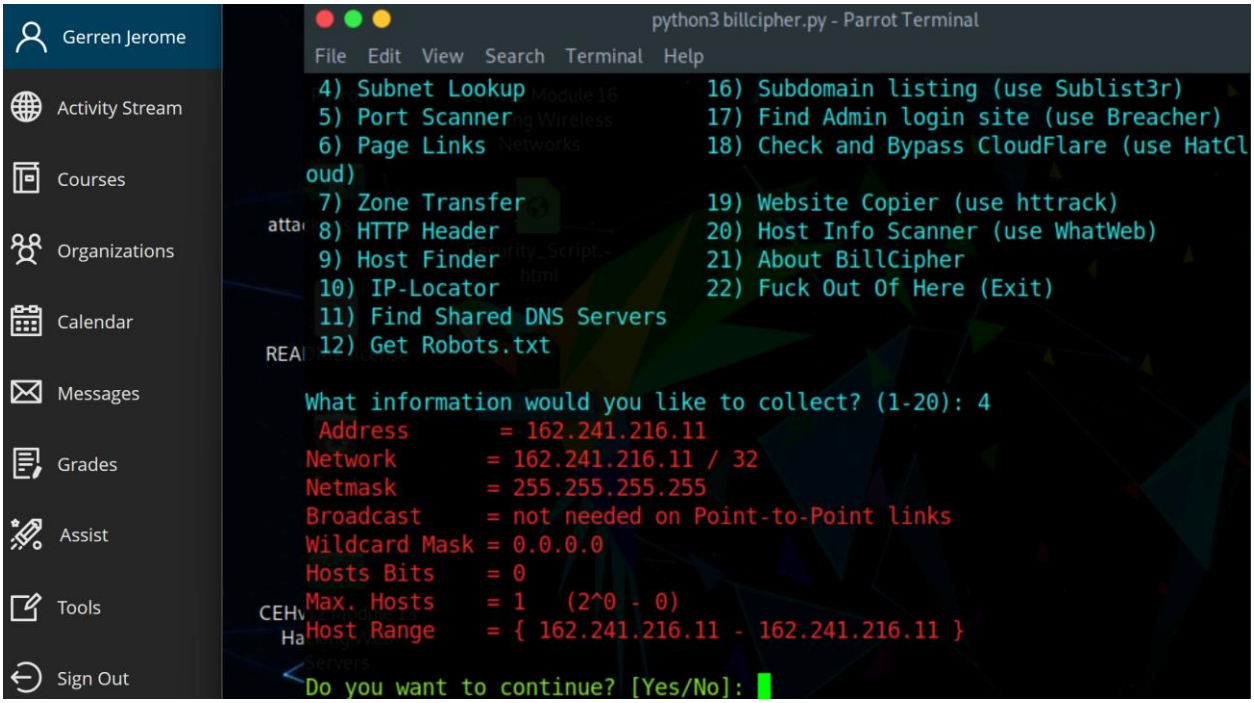
Screengrab: Step 10 – Results: DNS Lookup



Screengrab: Step 15 – Results: GeoIP Lookup



Screengrab: Step 20 - Results: Subnet Lookup



f) Footprinting a target using OSINT Framework

Eyes only