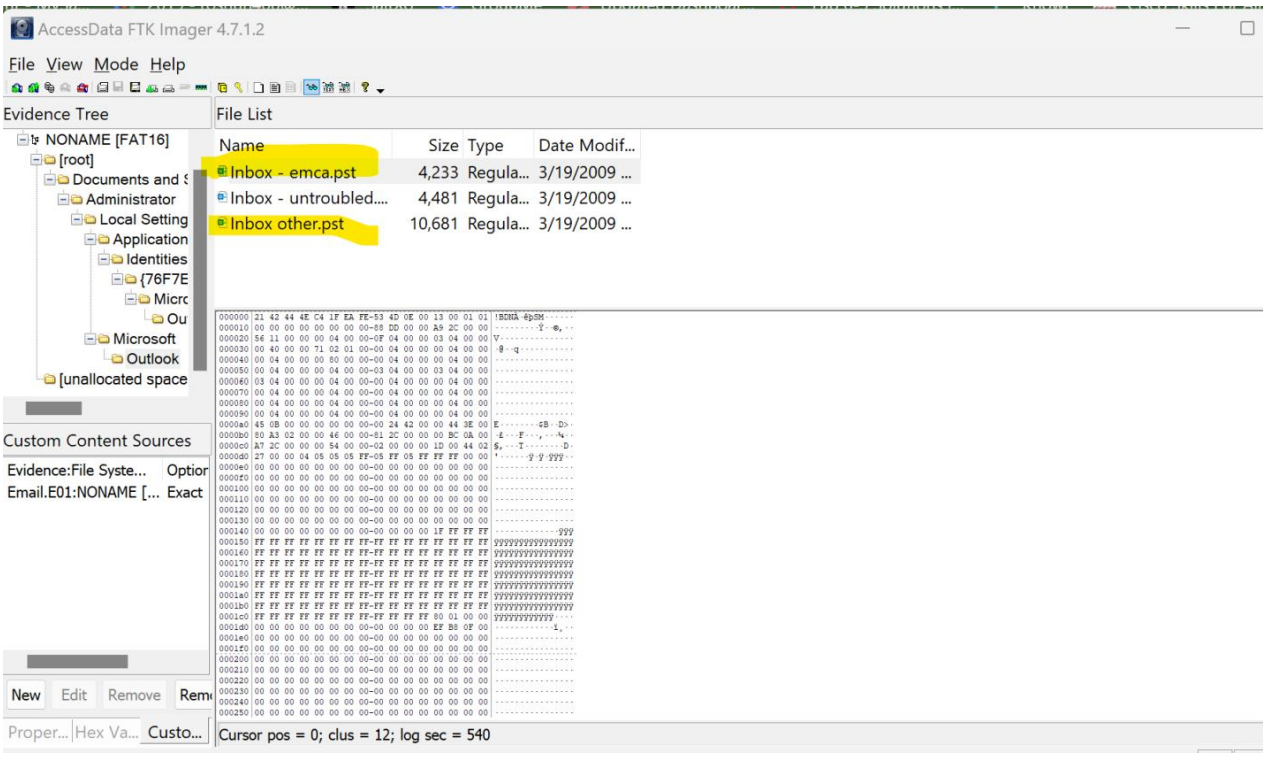
DFSC 4338 Cyber Warfare

Exam #4 Part 2 (30 points)
Due: 05/04/2023 (midnight)
Note: Provide detailed answers

Task: Email Forensics

1. Download "Email.E01" from blackboard
2. "Email.E01" is an email archive extracted from a spam folder on a system.
3. Load the "Email.E01" file into your favorite forensic toolkit, i.e. FTK as an Acquired Image.

Question 1) How many email archives were found?



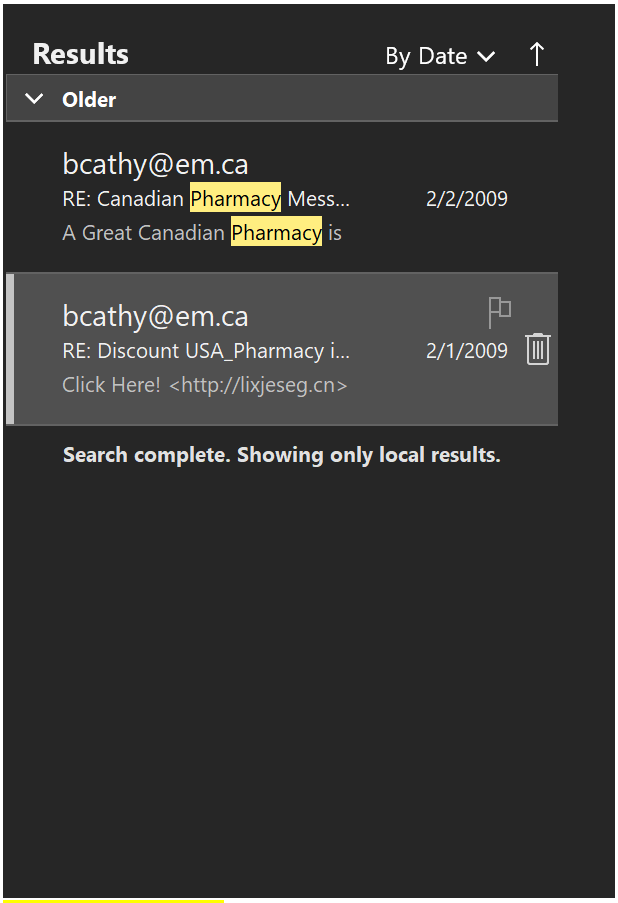
There were three email archives found when using FTK Imager.

Question 2) How many total messages are there?

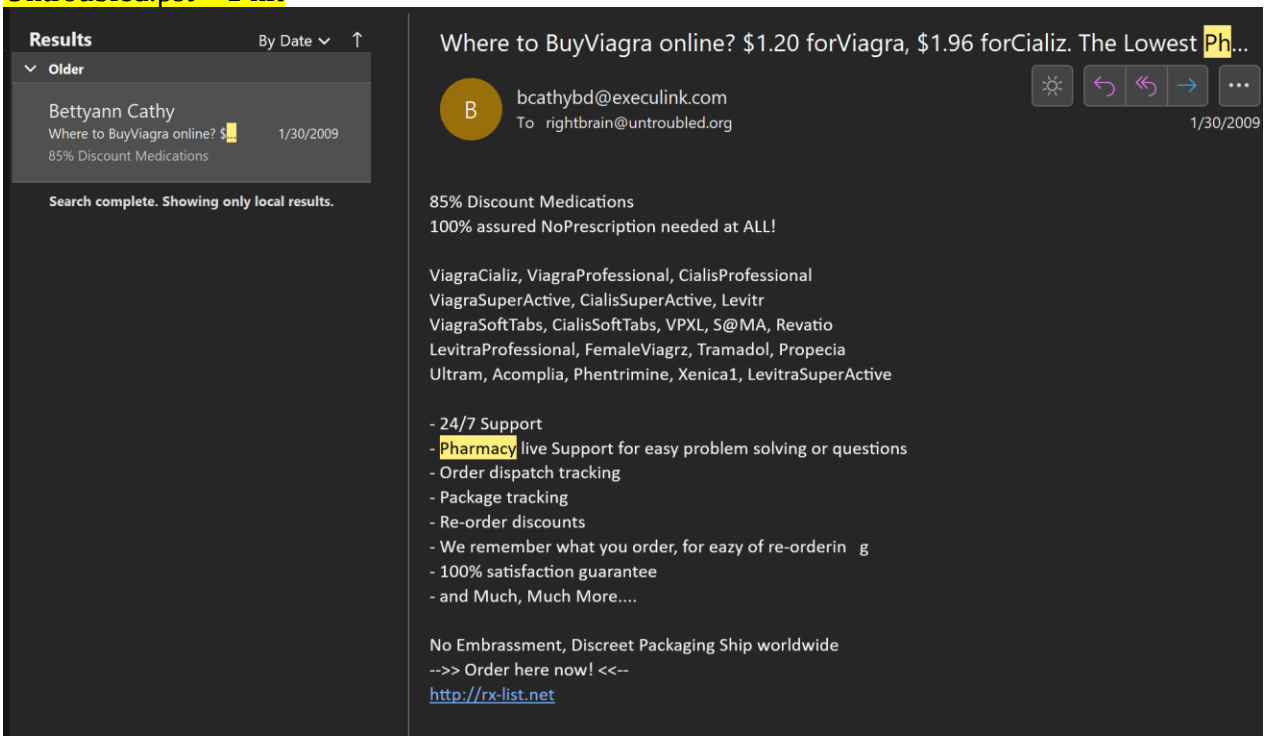
Emca.pst -625
Untroubled.pst - 438
Other.pst - 1109

Question 3) Perform a **live search** for "pharmacy". How many hits did you find?

Emca.pst – 2 hits



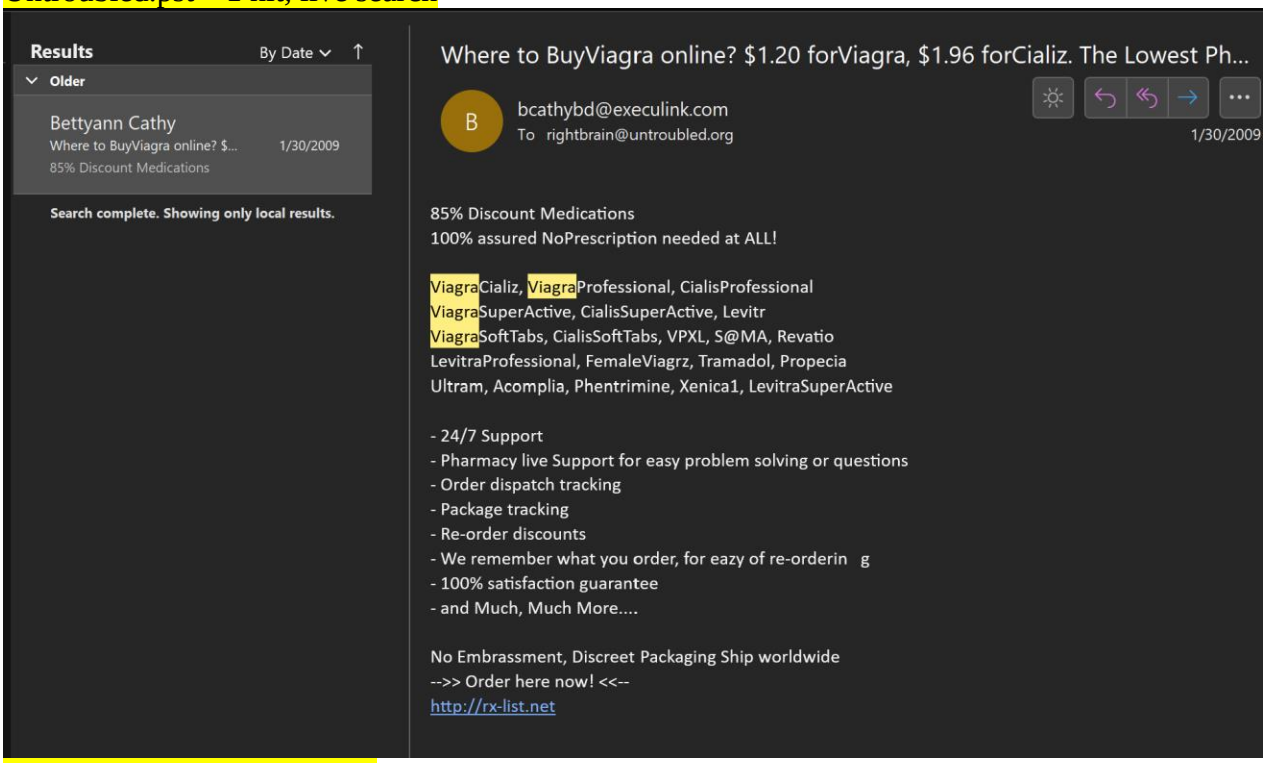
Other.pst – 0 hits
Untroubled.pst – 1 hit



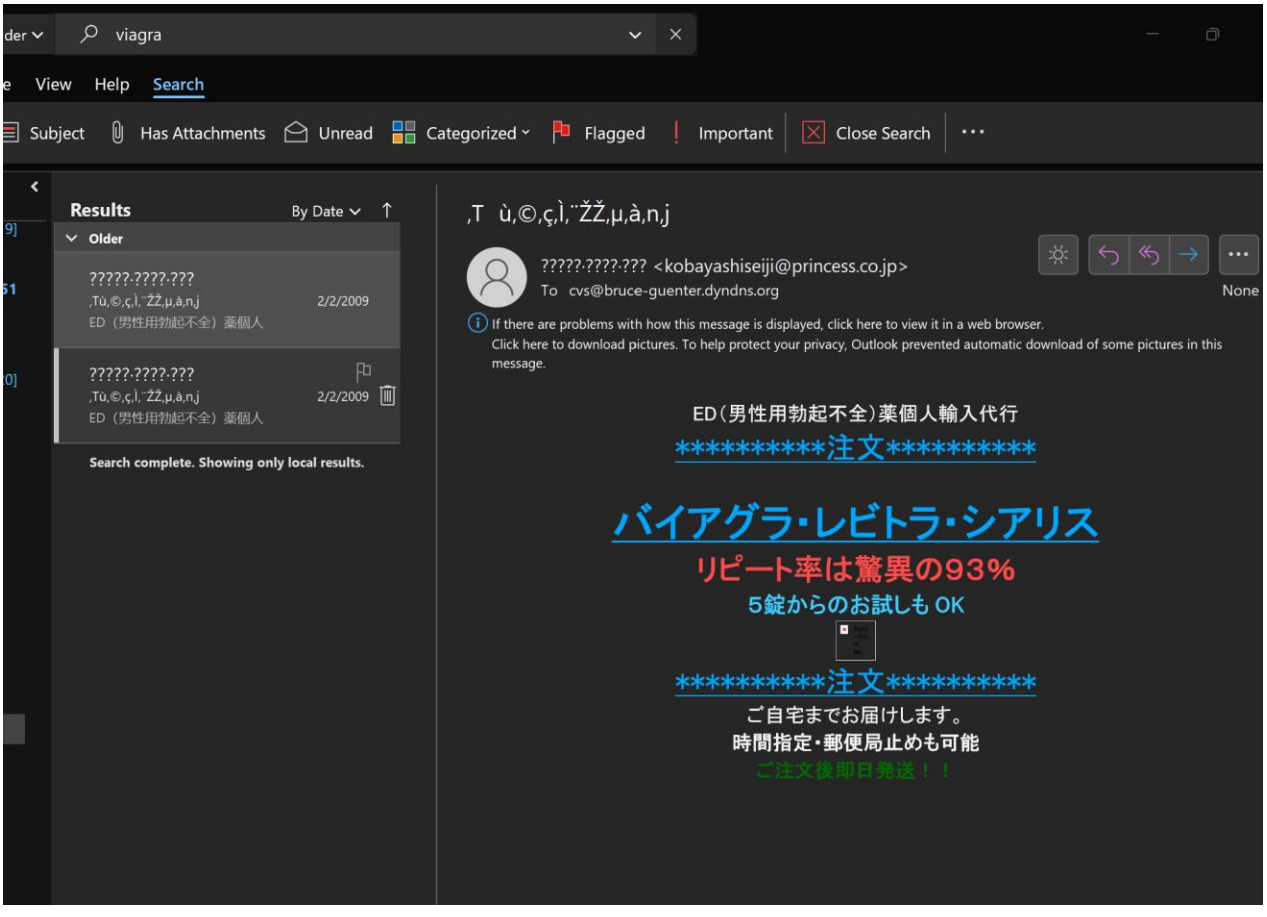
Question 4) Perform a **live search** for "viagra". Compare these results to an **index search** for "viagra". Why do the results differ? (Check FTK help document)

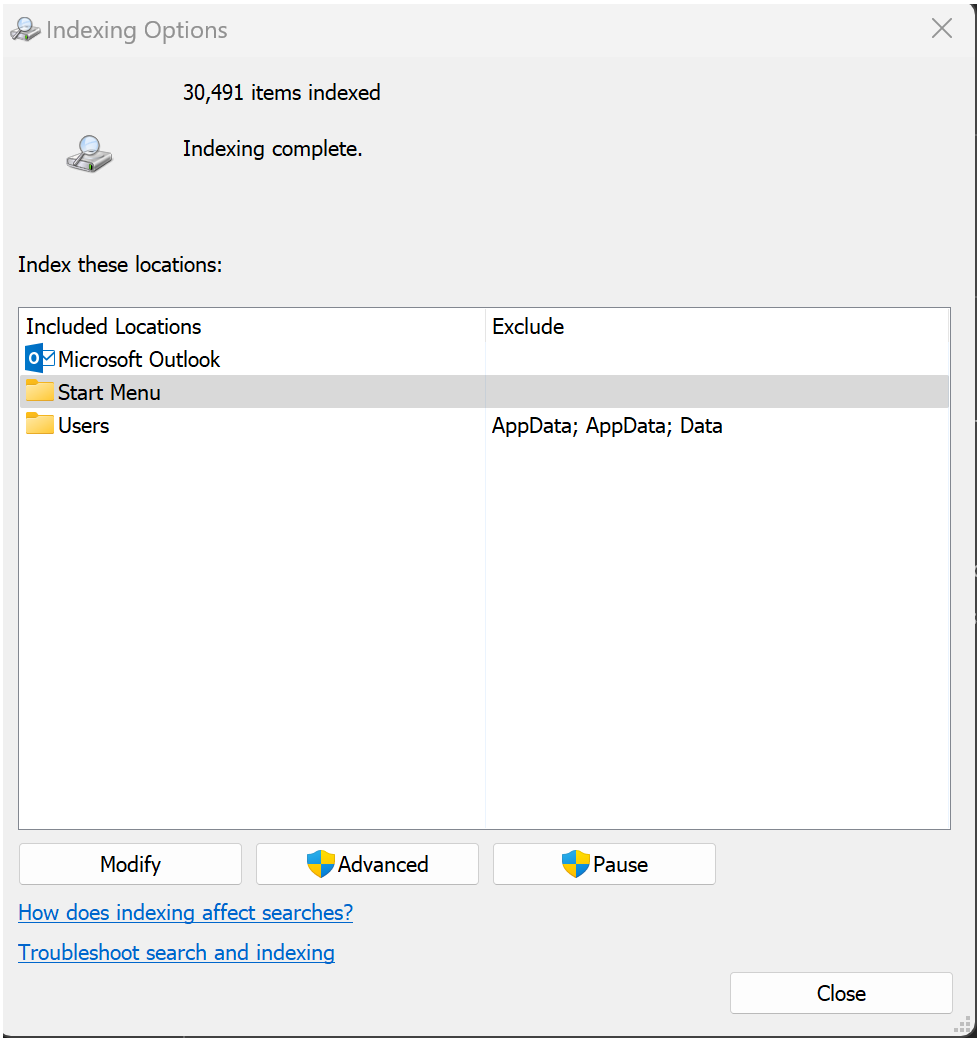
The results differ because within index search, it is finding all the words on the evidence given and gives faster results. While with live search the data not found within index search is to be found within a live search and finding keywords as well.

Emca.pst – 0 hit, live search
Untroubled.pst – 1 hit, live search

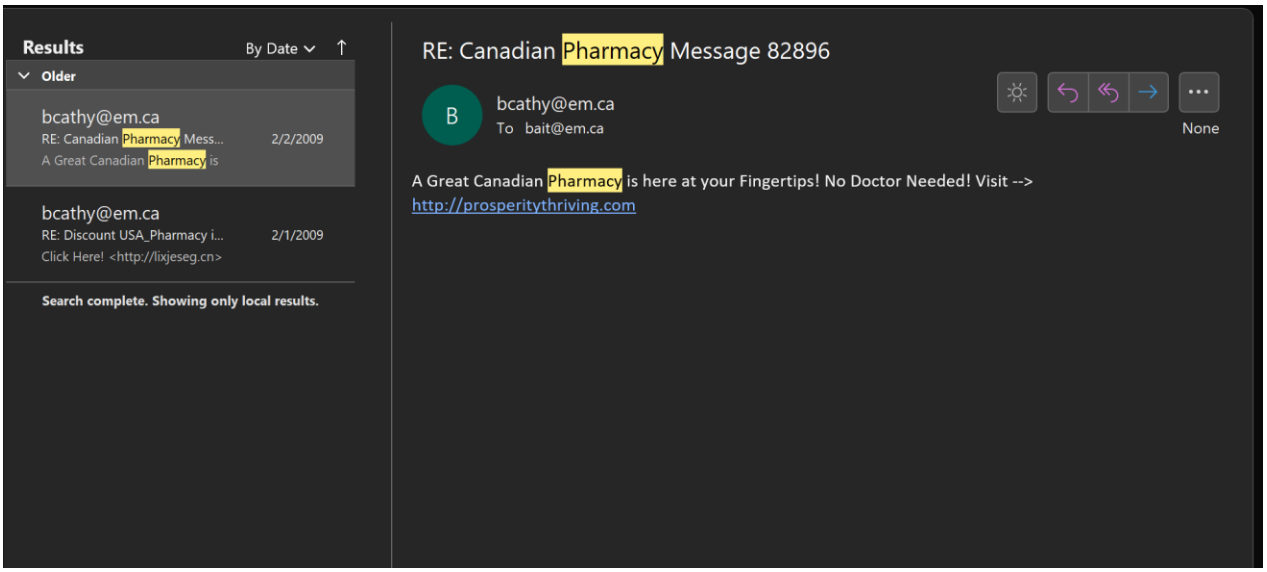


Other.pst – 2 hits, live search





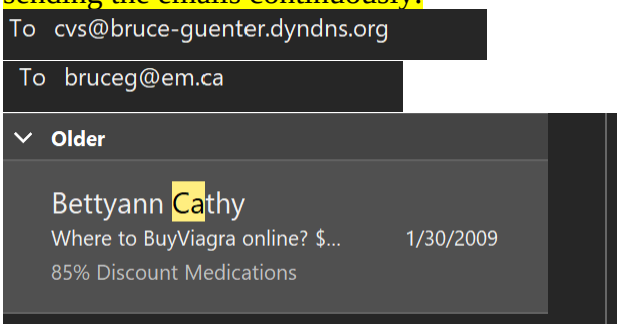
Question 5) What pharmacy site(s) was this person working for?



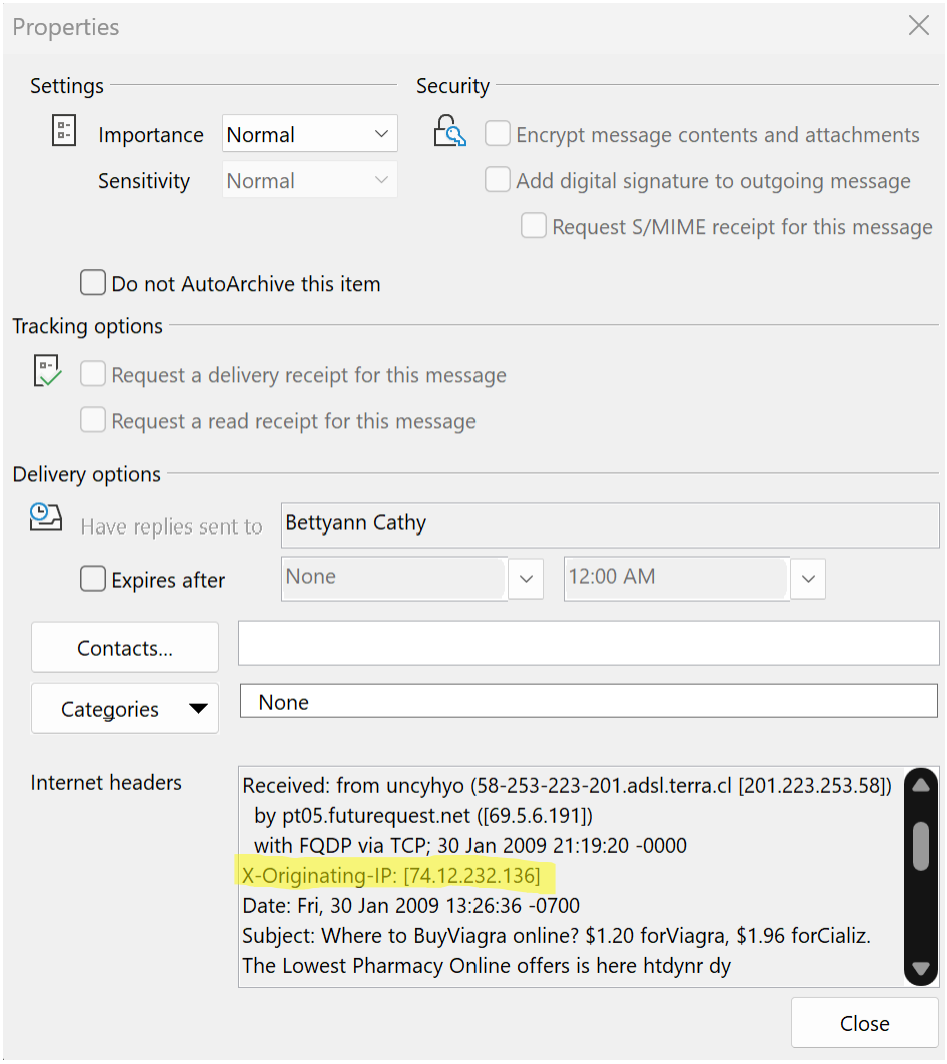
The sender is working for *Prosperity Thriving*, from the live search for pharmacy one is able to view the following screenshot above. In the email one is able to view the "website" of the company that is attached in the email.

Question 6) Do we have any clues to his/her identity?

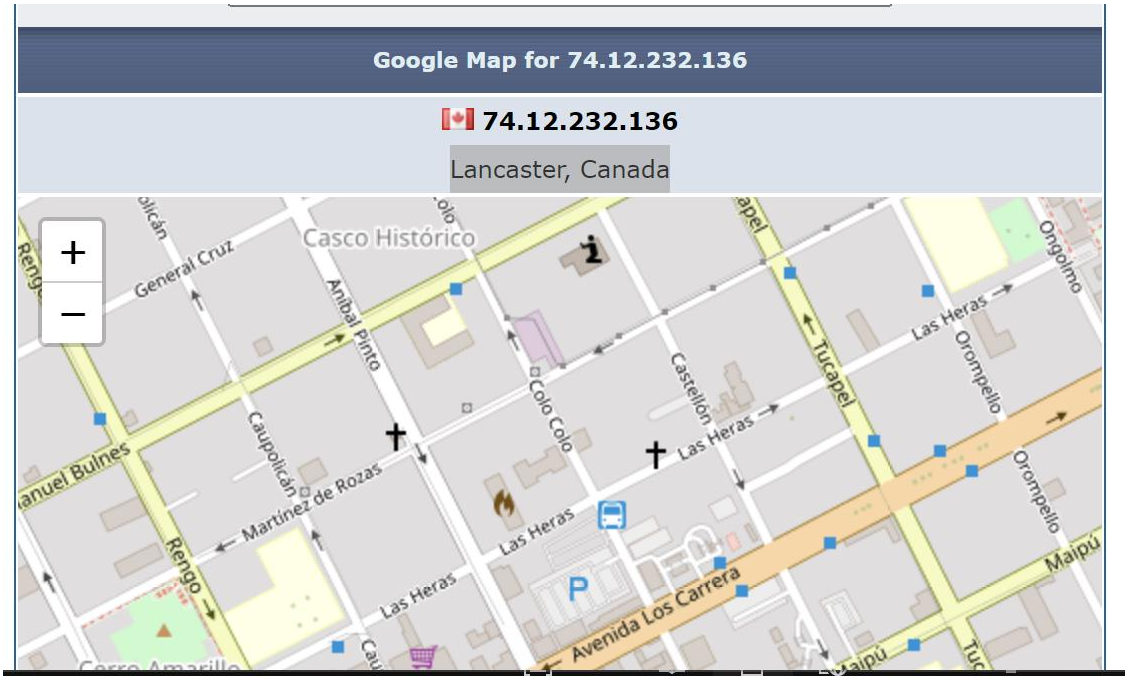
From the *To* line of the header I was able to find a clue of the identity of the person, being Bruce Guenter or Bruce G as they were receiving the emails. But Bettyann Cathy was the one sending the emails continuously.



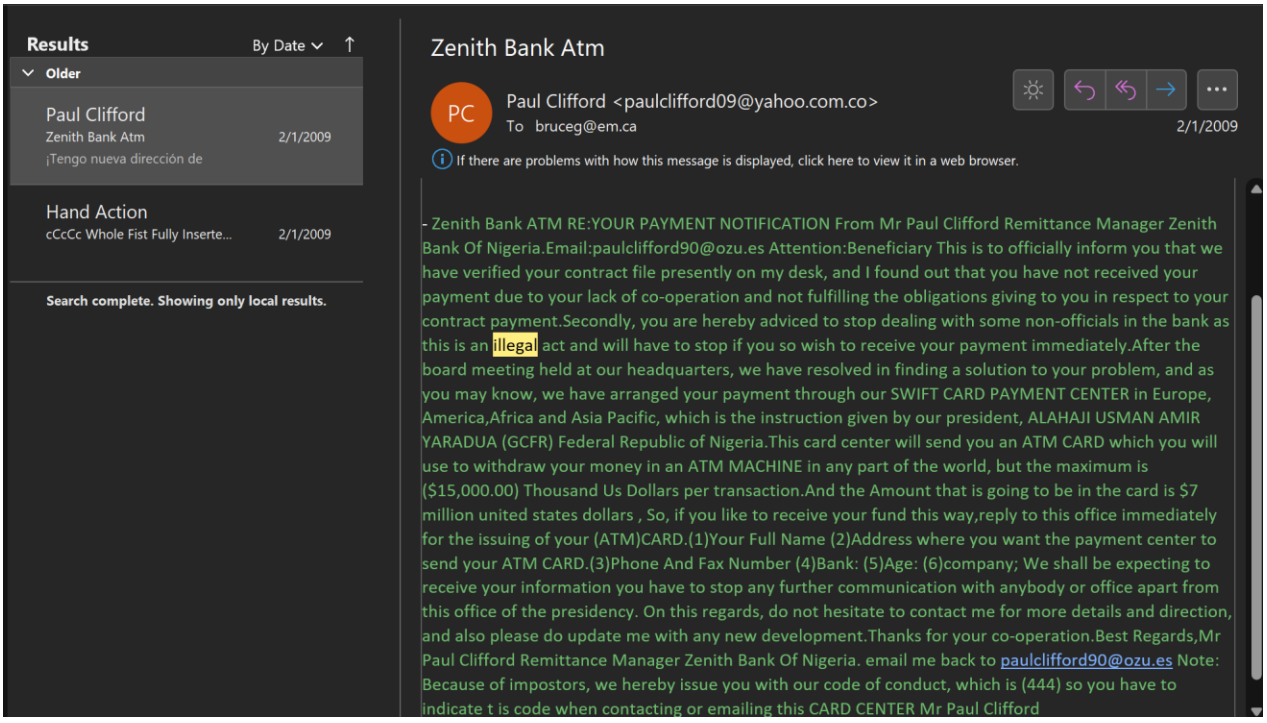
Question 7) Where might this person be located? (Find the location from the IP address)



Retrieving the email header in Outlook I was able to find the original IP address of the sender. Once I found the IP address I was able to enter the header into https://www.iptrackeronline.com/email-header-analysis.php to find the location of the sender is located Lancaster, Canada.



Question 8) What other illegal activity is this person involved in?



Bruce is dealing with non-officials within the Zenith Bank, as described by the email above.

Question 9) Trace the path of the email that implicates the sender in this other illegal activity. List the city/state/country of each hop.

Graphing...

```
      [75.126.251.247] ivory
      [169.254.158.58]
      [169.48.118.156] ae103.ppr01.dal13.networklayer.com
      [169.48.118.136] 88.76.30a9.ip4.static.sl-reverse.com
      [0.0.0.0] ivory.hexillion.com
      [50.97.17.57] ae34.bbr01.eq01.dal03.networklayer.com
      [206.223.118.2] exchange-cust2.da1.equinix.net
 8
      [209.191.64.115] ae-3.pat2.dnx.yahoo.com
12
      [209.191.64.236] ae-6.pat2.gqb.yahoo.com
      [0.0.0.0] ivory.hexillion.com
      [0.0.0.0] ivory.hexillion.com
      [0.0.0.0] ivory.hexillion.com
      [0.0.0.0] ivory.hexillion.com
```

Following the hops by searching the IP address locations given in the screenshot above:

IP Address Locator: What Is My IP Address - 50.97.17.57

IP Address:	50.97.17.57
IP Host:	ae34.bbr01.eq01.dal03.networklayer.com

Find IP Address Location for 'My IP' 50.97.17.57

Continent:	North America (NA)
Country:	United States (US)
State:	Unknown
City:	Unknown
ISP:	SOFTLAYER
Organization:	SOFTLAYER
Time zone:	America/North_Dakota/Center

IP Address Lookup related for 'My IP' 50.97.17.57

Continent Lat/Lon:	46.07305 / -100.546
Country Lat/Lon:	38 / -98
City Lat/Lon:	(37.751) / (-97.822)
IP Language:	English
IP Currency:	United States dollar($) (USD)
IDD Code:	+1

Advertisements

Find IP Location on IP Location Map

IP Address Locator: What Is My IP Address - 209.191.64.115

IP Address:	209.191.64.115
IP Host:	ae-3.pat2.dnx.yahoo. com

Find IP Address Location for 'My IP' 209.191.64.115

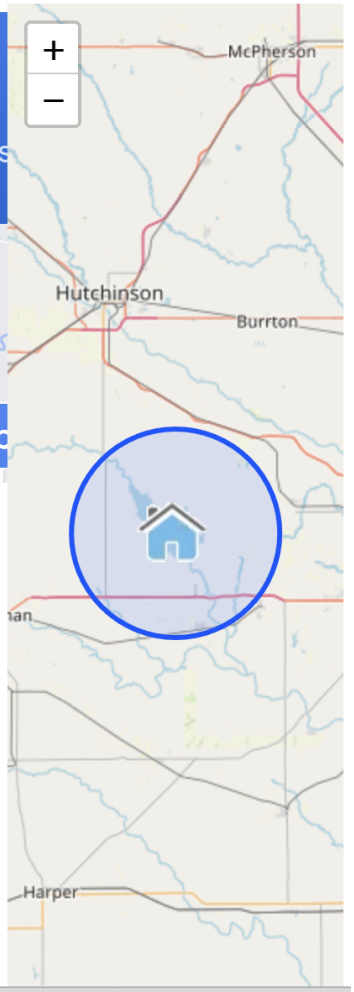
Continent:	North America (NA)
Country:	United States (US)
State:	Unknown
City:	Unknown
ISP:	YAHOO-1
Organization:	YAHOO-1
Time zone:	America/North_Dakota/Center

IP Address Lookup related for 'My IP' 209.191.64.115

Continent Lat/Lon:	46.07305 / -100.546
Country Lat/Lon:	38 / -98
City Lat/Lon:	(37.751) / (-97.822)
IP Language:	English
IP Currency:	United States dollar($) (USD)
IDD Code:	+1

Advertisements

Find IP Location on IP Location Map



IP Address Locator: What Is My IP Address - 209.191.64.236

IP Address:	209.191.64.236
IP Host:	ae-6.pat2.gqb.yahoo. com

Find IP Address Location for 'My IP' 209.191.64.236

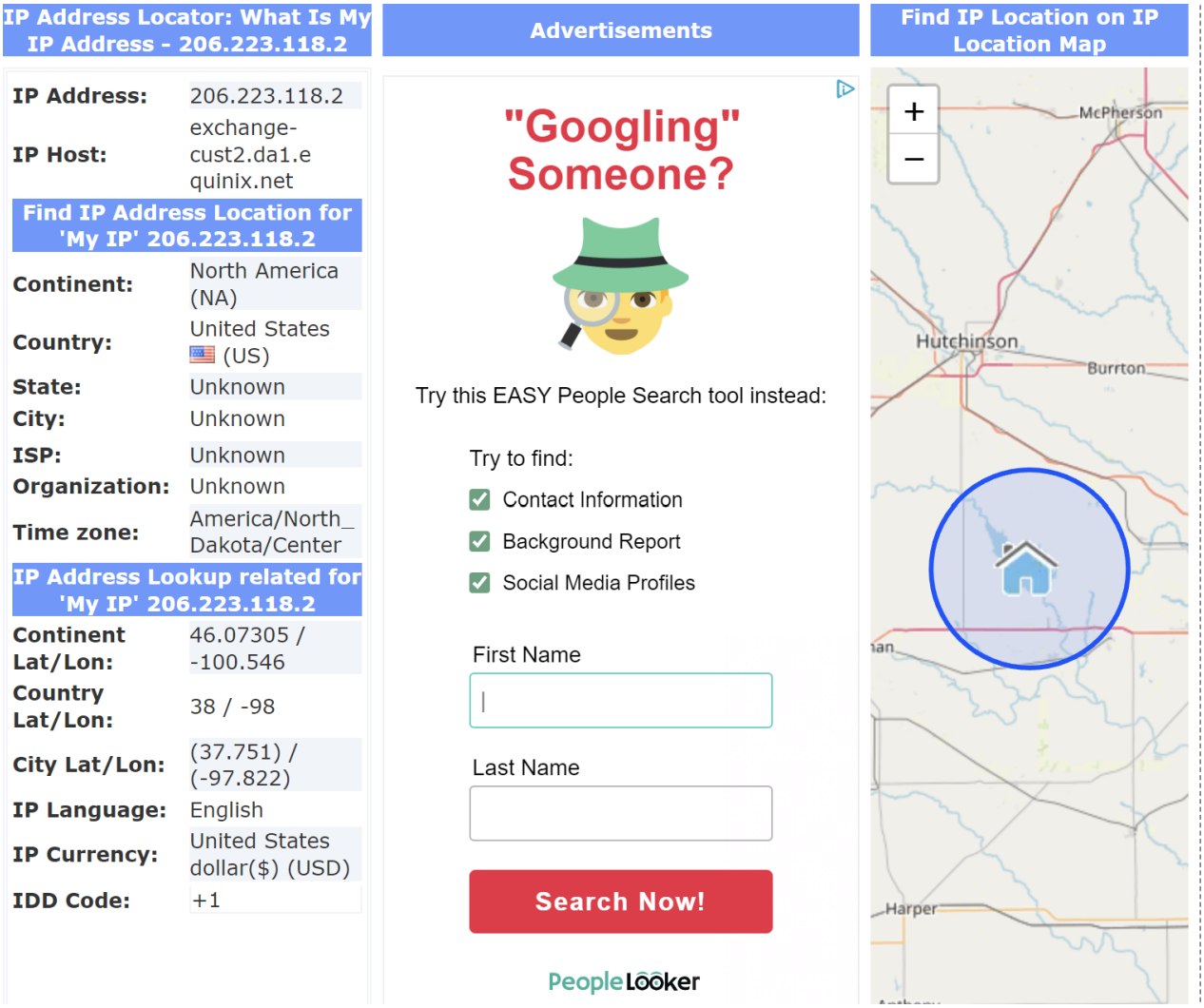
Continent:	North America (NA)
Country:	United States (US)
State:	Unknown
City:	Unknown
ISP:	YAHOO-1
Organization:	YAHOO-1
Time zone:	America/North_Dakota/Center

IP Address Lookup related for 'My IP' 209.191.64.236

Continent Lat/Lon:	46.07305 / -100.546
Country Lat/Lon:	38 / -98
City Lat/Lon:	(37.751) / (-97.822)
IP Language:	English
IP Currency:	United States dollar($) (USD)
IDD Code:	+1

Advertisements

Find IP Location on IP Location Map



IP Address Locator: What Is My IP Address - 206.223.118.2

IP Address:	206.223.118.2
IP Host:	exchange-cust2.da1.equinix.net

Find IP Address Location for 'My IP' 206.223.118.2

Continent:	North America (NA)
Country:	United States (US)
State:	Unknown
City:	Unknown
ISP:	Unknown
Organization:	Unknown
Time zone:	America/North_Dakota/Center

IP Address Lookup related for 'My IP' 206.223.118.2

Continent Lat/Lon:	46.07305 / -100.546
Country Lat/Lon:	38 / -98
City Lat/Lon:	(37.751) / (-97.822)
IP Language:	English
IP Currency:	United States dollar($) (USD)
IDD Code:	+1

Advertisements

Find IP Location on IP Location Map

After finding the locations of all IP addresses, one can conclude that the sender is located near Hutchinson, KS in the United States.

Websites that can be useful.
Domain Dosier and Traceroute (http://centralops.net/co/)
Ip Tracker (http://www.ip-address.org/)