

DFSC 4338 Cyber Warfare

Exam #4 Part 2 (30 points)

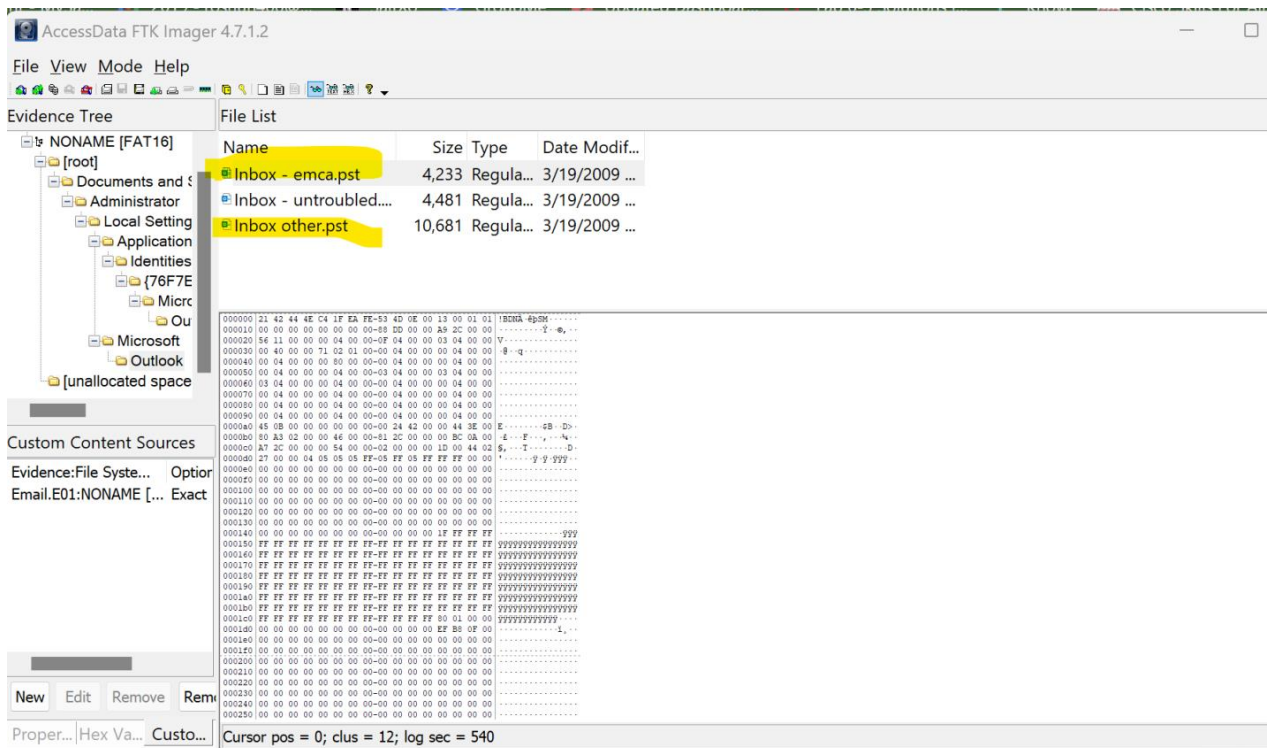
Due: 05/04/2023 (midnight)

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

Results By Date ▾ ↑

▼ Older

bcathy@em.ca
RE: Canadian Pharmacy Mess... 2/2/2009
A Great Canadian Pharmacy is

bcathy@em.ca
RE: Discount USA_Pharmacy i... 2/1/2009
Click Here! <http://lixjeseg.cn>

Search complete. Showing only local results.

Other.pst – 0 hits

Untroubled.pst – 1 hit

Results By Date ▾ ↑

▼ Older

Bettyann Cathy
Where to BuyViagra online? \$ 1/30/2009
85% Discount Medications

Search complete. Showing only local results.

Where to BuyViagra online? \$1.20 forViagra, \$1.96 forCialis. The Lowest Ph...

B bcathybd@execulink.com
To rightbrain@untroubled.org 1/30/2009

85% Discount Medications
100% assured NoPrescription needed at ALL!

ViagraCialis, ViagraProfessional, CialisProfessional
ViagraSuperActive, CialisSuperActive, Levitr
ViagraSoftTabs, CialisSoftTabs, VPXL, S@MA, Revatio
LevitraProfessional, FemaleViagrz, Tramadol, Propecia
Ultram, Acomplia, Phentrimine, Xenica1, LevitraSuperActive

- 24/7 Support
- Pharmacy live Support for easy problem solving or questions
- Order dispatch tracking
- Package tracking
- Re-order discounts
- We remember what you order, for eazy of re-orderin g
- 100% satisfaction guarantee
- and Much, Much More....

No Embrassment, Discreet Packaging Ship worldwide
-->> Order here now! <<--
<http://rx-list.net>

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

Results By Date ▾ ↑

Older

Bettyann Cathy
Where to BuyViagra online? \$... 1/30/2009
85% Discount Medications

Search complete. Showing only local results.

Where to BuyViagra online? \$1.20 forViagra, \$1.96 forCialis. The Lowest Ph...

bcathybd@execulink.com
To rightbrain@untroubled.org 1/30/2009

85% Discount Medications
100% assured NoPrescription needed at ALL!

ViagraCialis, ViagraProfessional, CialisProfessional
ViagraSuperActive, CialisSuperActive, Levitr
ViagraSoftTabs, CialisSoftTabs, VPXL, S@MA, Revatio
LevitraProfessional, FemaleViagrz, Tramadol, Propecia
Ultram, Acomplia, Phentrimine, Xenica1, LevitraSuperActive

- 24/7 Support
- Pharmacy live Support for easy problem solving or questions
- Order dispatch tracking
- Package tracking
- Re-order discounts
- We remember what you order, for eazy of re-orderin g
- 100% satisfaction guarantee
- and Much, Much More....

No Embarrassment, Discreet Packaging Ship worldwide
--> Order here now! <<--
<http://rx-list.net>

Other.pst – 2 hits, live search

der ▾ viagra ▾ ×

e View Help Search

Subject Has Attachments Unread Categorized ▾ Flagged Important Close Search ...

Results By Date ▾ ↑

Older

?????-????-???
,Tù,©,ç,ì,"ŽŽ,μ,à,n,j 2/2/2009
ED (男性用勃起不全) 薬個人

?????-????-???
,Tù,©,ç,ì,"ŽŽ,μ,à,n,j 2/2/2009
ED (男性用勃起不全) 薬個人

Search complete. Showing only local results.

,T ù,©,ç,ì,"ŽŽ,μ,à,n,j

?????-????-??? <kobayashiseiji@princess.co.jp>
To cvs@bruce-guenter.dyndns.org None

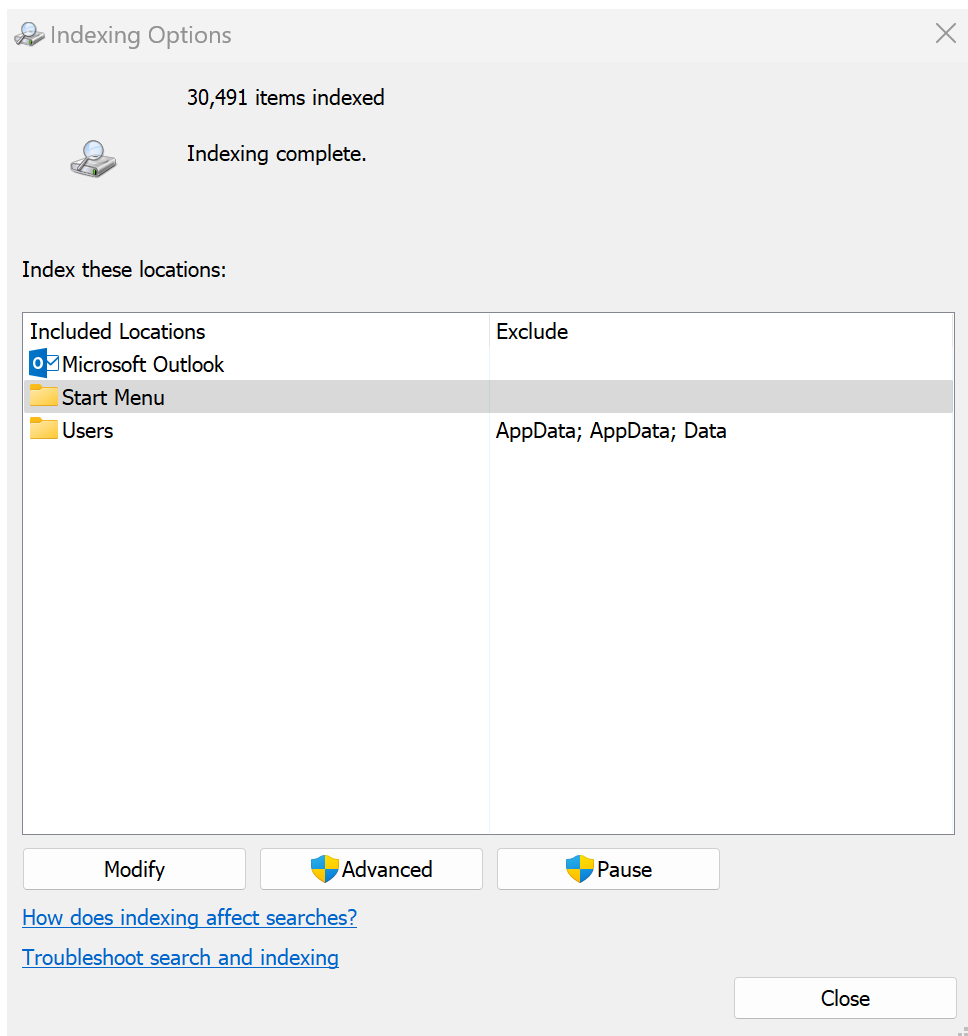
If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

ED (男性用勃起不全) 薬個人輸入代行
*****注文*****

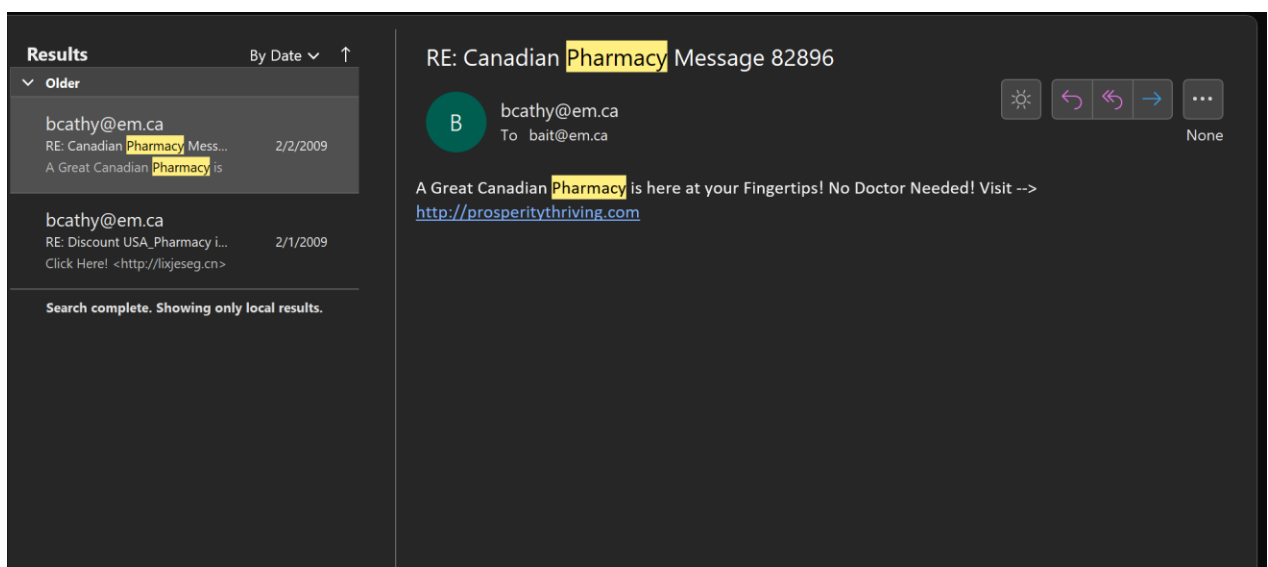
バイアグラ・レビトラ・シアリス
リピート率は驚異の93%
5錠からのお試しも OK

*****注文*****

ご自宅までお届けします。
時間指定・郵便局止めも可能
ご注文後即日発送!!



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.

To cvs@bruce-guenter.dyndns.org

To bruceg@em.ca

▼ Older

Bettyann Cathy

Where to BuyViagra online? \$...

1/30/2009

85% Discount Medications

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

Properties

Settings

Importance Normal

Sensitivity Normal

Security

☐ Encrypt message contents and attachments

☐ Add digital signature to outgoing message

☐ Request S/MIME receipt for this message

☐ Do not AutoArchive this item

Tracking options

☐ Request a delivery receipt for this message

☐ Request a read receipt for this message

Delivery options

Have replies sent to Bettyann Cathy

☐ Expires after None 12:00 AM

Contacts...

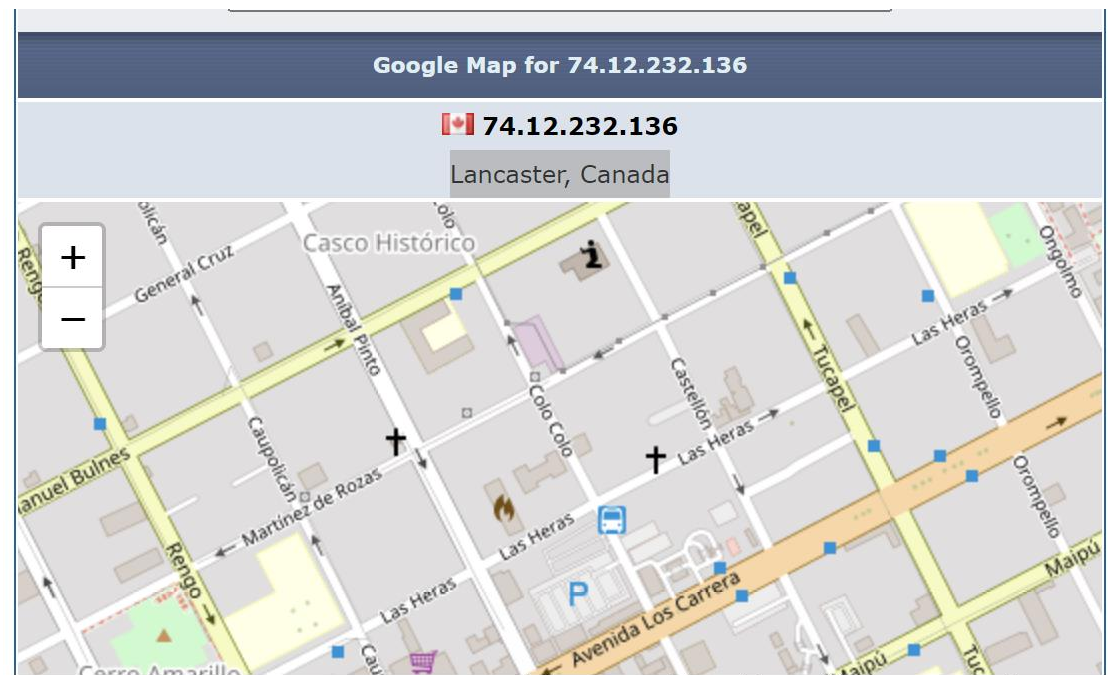
Categories ▼ None

Internet headers

Received: from uncyhyo (58-253-223-201.adsl.terra.cl [201.223.253.58])
by pt05.futurequest.net ([69.5.6.191])
with FQDP via TCP; 30 Jan 2009 21:19:20 -0000
X-Originating-IP: [74.12.232.136]
Date: Fri, 30 Jan 2009 13:26:36 -0700
Subject: Where to BuyViagra online? \$1.20 forViagra, \$1.96 forCializ.
The Lowest Pharmacy Online offers is here htdynr dy

Close

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?

Results By Date ↑

Older

Paul Clifford
Zenith Bank Atm
¡Tengo nueva dirección de

2/1/2009

Hand Action
cCcCc Whole Fist Fully Inserte...

2/1/2009

Search complete. Showing only local results.

Zenith Bank Atm

PC Paul Clifford <paulclifford09@yahoo.com.co>
To: bruceg@em.ca

2/1/2009

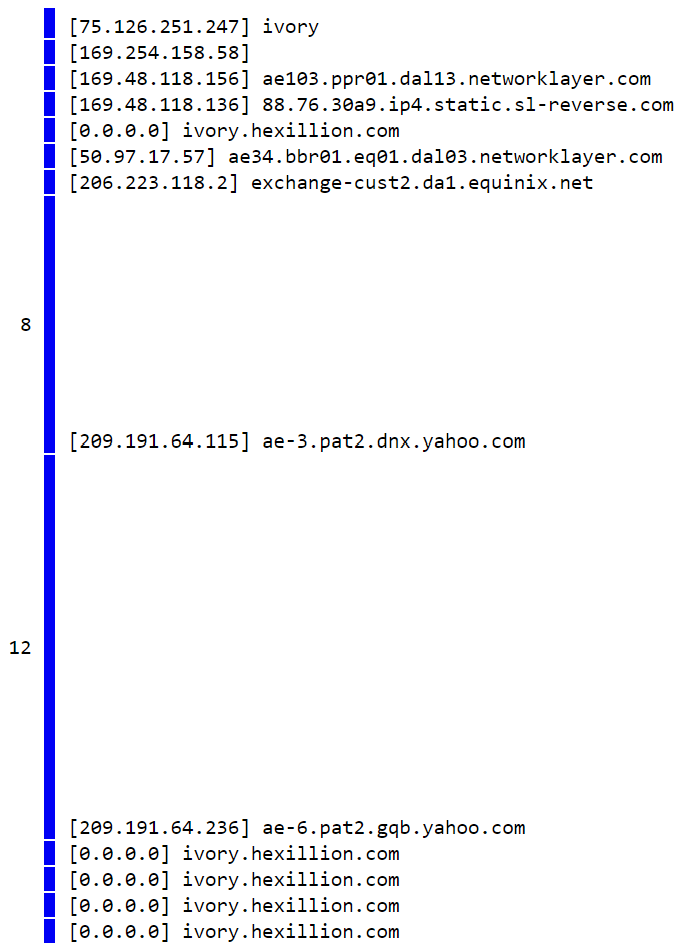
If there are problems with how this message is displayed, click here to view it in a web browser.

- Zenith Bank ATM RE:YOUR PAYMENT NOTIFICATION From Mr Paul Clifford Remittance Manager Zenith Bank Of Nigeria.Email:paulclifford90@ozu.es Attention:Beneficiary This is to officially inform you that we have verified your contract file presently on my desk, and I found out that you have not received your payment due to your lack of co-operation and not fulfilling the obligations giving to you in respect to your contract payment.Secondly, you are hereby adviced to stop dealing with some non-officials in the bank as this is an **illegal** act and will have to stop if you so wish to receive your payment immediately.After the board meeting held at our headquarters, we have resolved in finding a solution to your problem, and as you may know, we have arranged your payment through our SWIFT CARD PAYMENT CENTER in Europe, America,Africa and Asia Pacific, which is the instruction given by our president, ALAHAJI USMAN AMIR YARADUA (GCFR) Federal Republic of Nigeria.This card center will send you an ATM CARD which you will use to withdraw your money in an ATM MACHINE in any part of the world, but the maximum is (\$15,000.00) Thousand Us Dollars per transaction.And the Amount that is going to be in the card is \$7 million united states dollars , So, if you like to receive your fund this way,reply to this office immediately for the issuing of your (ATM)CARD.(1)Your Full Name (2)Address where you want the payment center to send your ATM CARD.(3)Phone And Fax Number (4)Bank: (5)Age: (6)company; We shall be expecting to receive your information you have to stop any further communication with anybody or office apart from this office of the presidency. On this regards, do not hesitate to contact me for more details and direction, and also please do update me with any new development.Thanks for your co-operation.Best Regards,Mr Paul Clifford Remittance Manager Zenith Bank Of Nigeria. email me back to paulclifford90@ozu.es Note: Because of impostors, we hereby issue you with our code of conduct, which is (444) so you have to indicate t is code when contacting or emailing this CARD CENTER Mr Paul Clifford

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...



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
ae34.bbr01.eq01.dal0
IP Host: 3.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 46.07305 /
Lat/Lon: -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

Finish Your Property Search



See available data on ownership history, deed info, and sales history.

ENTER ADDRESS

Search



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

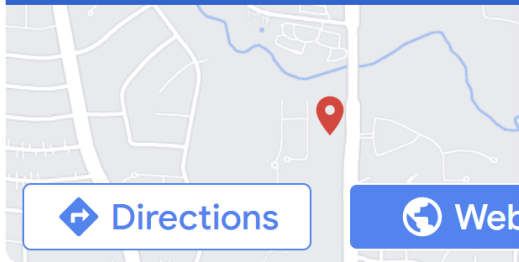
Continent: North America (NA)
Country: United States (US)
State: Unknown
City: Unknown
ISP: YAHOO-1
Organization: YAHOO-1
Time zone: America/North_Dakota/Center

IP Address Lookup related for 'My IP' 209.191.64.115

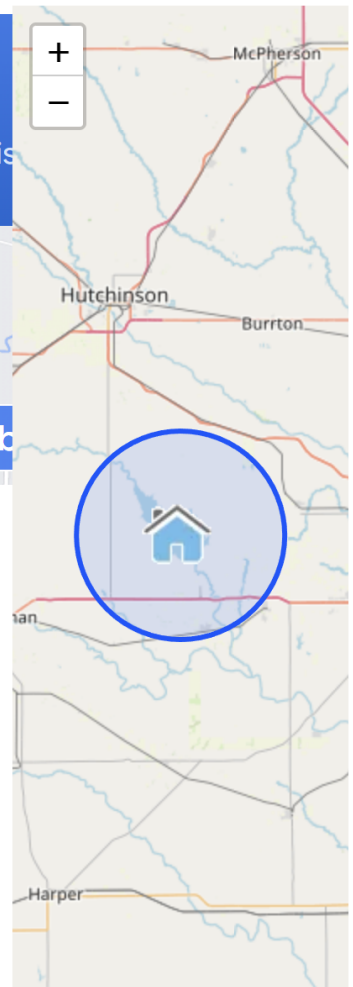
Continent Lat/Lon: 46.07305 / -100.546
Country Lat/Lon: 38 / -98
City Lat/Lon: (37.751) / (-97.822)
IP Language: English
IP Currency: United States dollar(\$) (USD)
IDD Code: +1

Advertisements

Addy & Ry Boutique
Addy & Ry Boutique
We Carry Trendy Clothing and Stylish Accessories.



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
ae-
IP Host: 6.pat2.gqb.yahoo
o. 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 46.07305 /
Lat/Lon: -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

Finish Your Property Search



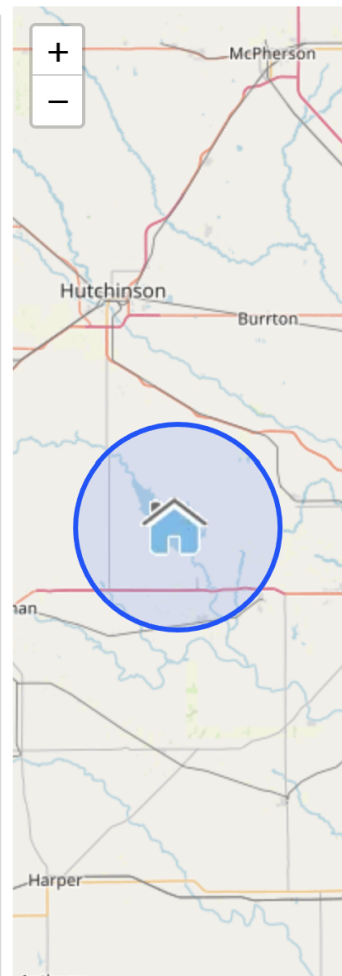
See available data on
ownership history, deed
info, and sales history.

ENTER ADDRESS

Search



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 46.07305 /
Lat/Lon: -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

"Googling" Someone?



Try this EASY People Search tool instead:

Try to find:

- ☒ Contact Information
- ☒ Background Report
- ☒ Social Media Profiles

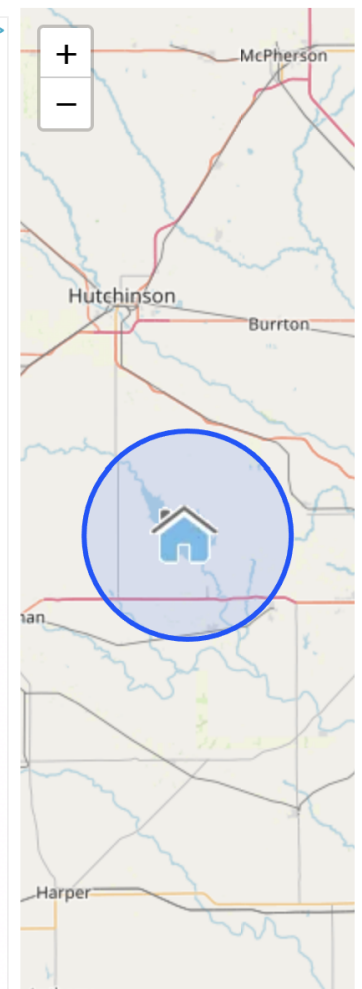
First Name

Last Name

Search Now!

PeopleLooker

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 Dossier and Traceroute (<http://centralops.net/co/>)

Ip Tracker (<http://www.ip-address.org/>)