

OSHINT Report

Here you provide me with two email addresses:

- apoderadosphja@gmail.com
- martinatorre8888@hotmail.com


Let's start with 'apoderadosphja@gmail.com'

Step 1: Finding IP address

First I analyze your header with well-known tools named 'Cyber forensics'.

Link: <http://www.cyberforensics.in/OnlineEmailTracer/index.aspx>

Header:



Resource Centre for
Cyber Forensics - India

☐ Web ☒ site

Home | About C-DAC | Products | Downloads | Training | Contact Us

Sunday, October 16, 2022

Members Area

Hello allstuck
Edit Profile
Logout

Navigation

E-MailTracer
Procedure
Photo Gallery

Featured

Press Release
Laws and Rules
FAQ

Support

Help Desk new
Enquiry
Request For CD
Providing Solution
Contact us

Online EMailTracer

EmailTracer is a tool to track email sender's identity. It analyzes the email header and gives the complete details of the sender like IP address, which is key point to find the culprit and the route followed by the mail, the Mail Server, details of Service Provider etc. EmailTracer traces up to Internet Service Provider level only. Further tracing can be done with the help of ISP and law enforcement agencies. The message-id will be useful for analyzing the mail logs at ISP.

Paste EMail Header here

Delivered-To: ttruan@gmail.com
Received: by 2002:a05:7208:c40a:b0:5b:9243:c7c0 with SMTP id bf10csp363927rbb;
Sun, 9 Oct 2022 15:44:10 -0700 (PDT)
X-Received: by 2002:a05:6402:1555:b0:458:ed89:24e9 with SMTP id p21-
20020a056402155500b00458ed8924e9mr15347773edx.55.1665355450031;
Sun, 09 Oct 2022 15:44:10 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1665355450; cv=none;
d=google.com; s=arc-20160816;
b=CQ2W3JxLyYRa08kvqjfyYk6eIPdqwGvnP7mmsGQtciueOyiUULh9PCPUF3TU/F
Xt6WncyhGrXnkhJqPrhQ0vdm0Dart1Zs0B9h6cWrVaGdG0gqEkFQtfe1daTVPJxp805
ZRUH7PZlnC2PvH3LHTvrCrrabSUUZ4tJNyg0Zy74rw67dwzUwezND/xf13hIaT21mCs
DbMmnu1jgugp3hyzzk1sXRRG7c+1YRyC7Vrb0EWIwGE++KPUznGwOH4t+b091D8qBbJ/
zIfFmb+0zbEzsf1hkRcBsaPsRzHeLHJKSADJVBfyBux7ouNGDEaqh4pNSFtEH12h/gkP
SpQw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=to:subject:message-id:date:from:mime-version:dkim-signature;
bh=NBTVt7rq3uTP2UTQ5Tep/03bG8IqeoYGQIAqdUnD+mK=;
b=03Yg8FH772FHYIE1XKuEFKqXhrpUxh8H+YovV3yNdxbr-jicw0NzXm1H79z8e4cV+bA
HnUCoxwZJB7P1gey1kQmI2YLSYu+9fSqD+r3y40W7n6haUuYdkzD1sW6TqJJan/ZC
+TIOw6L8veSZPn3NeJut9+du2IVzaBqZ0hx25JF3dw80KXrBg2Jd2gTYSObgo/HKDKA

Start Tracing EMail Crimes How to extract EMail Header?

Traceroute: This means The total path that sender sends you the mail.

The mail appears to be originated from the computer with IP address 209.85.220.41

The sender's email address is apoderadosphja@gmail.com

The message-id of the the mail is <CAL8ypnsb8n+UWLeZObRwuoSRx75nHPLBQ0cfHzNb_zkQhbbT=g@mail.gmail.com>.



IP address: 209.85.220.41

Received By	Received From	Date
"ttruana@gmail.com" ttruana@gmail.com	2002:a05:7208:c40a:b0:5b:9243:c7c0	--
2002:a05:7208:c40a:b0:5b:9243:c7c0	--	Sun, 9 Oct 2022 15:44:10 -0700 (PDT)
--	mail-sor-f41.google.com[209.85.220.41]	Sun, 09 Oct 2022 15:44:10 -0700 (PDT)
mail-sor-f41.google.com[209.85.220.41]	apoderadosphja@gmail.com	Sun, 9 Oct 2022 18:43:57 -0400

Details obtained from Regional Internet Registry

Domain/Registrant	IP	Registry	Country	City/Address	ISP
mail-sor-f41.google.com	209.85.220.41	ARIN			

Google admin toolbox: This header analyzer analyze the Gmail header and provide real information.

Link: <https://toolbox.googleapps.com/apps/messageheader/analyzeheader>

MessageId	CAL8ypnsb8n+UWLeZ0bRwuoSRx75nHPLBQ0cfHzNb_zkQhbbT=g@mail.gmail.com
Created at:	10/10/2022, 4:43:57 AM GMT+6 (Delivered after 13 sec)
From:	Apoderados PHJA <apoderadosphja@gmail.com>
To:	"ttruán@gmail.com" <ttruán@gmail.com>
Subject:	Sara y Simón Truan Navarro - IMPORTANTE
SPF:	pass with IP 209.85.220.41 Learn more
DKIM:	pass with domain gmail.com Learn more
DMARC:	pass Learn more

Here, we also get the same IP. So, this must be the real IP.

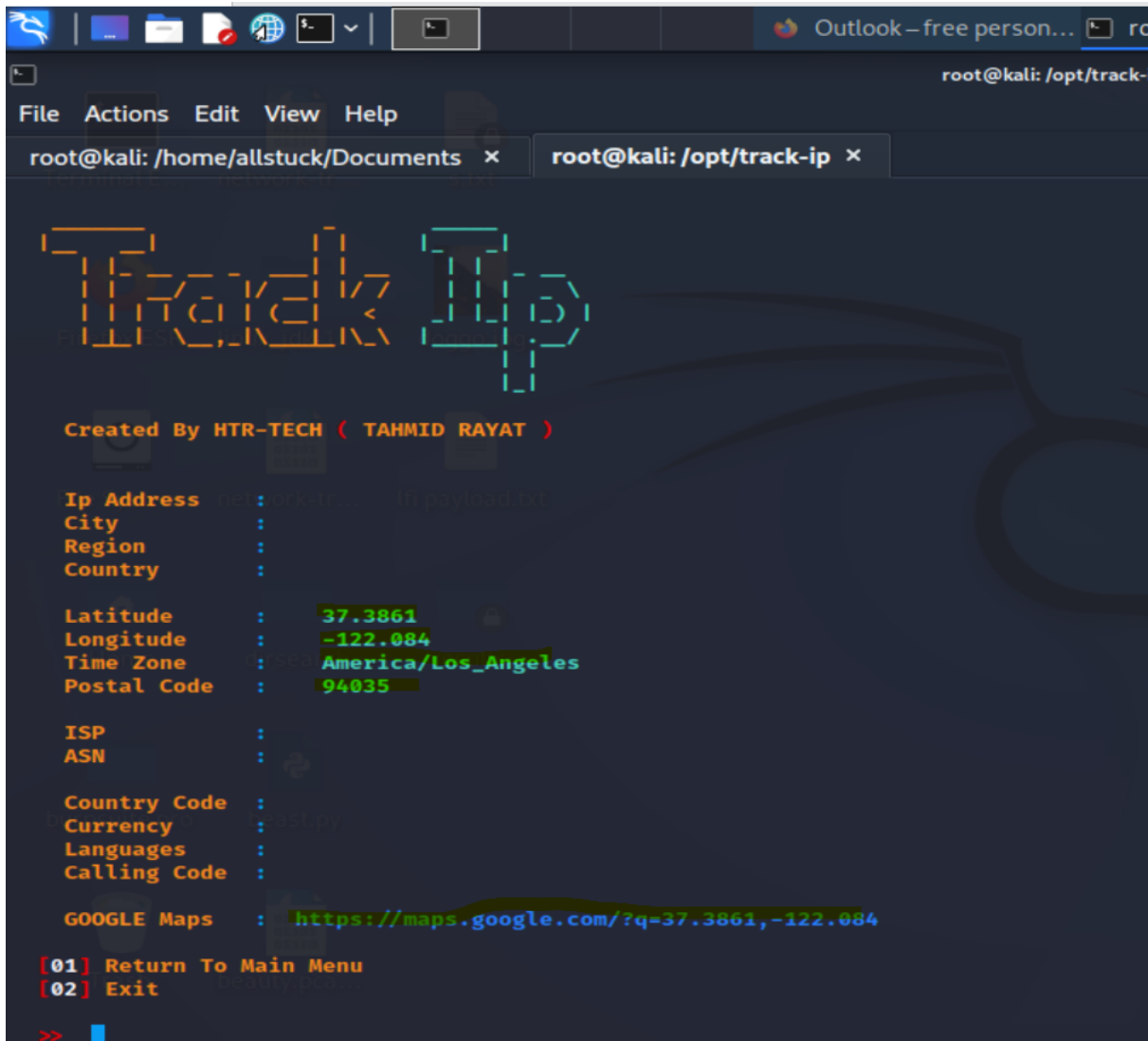
Step 2: Finding the Location:

Let's try to track the IP address with very reputable tools on kali Linux.

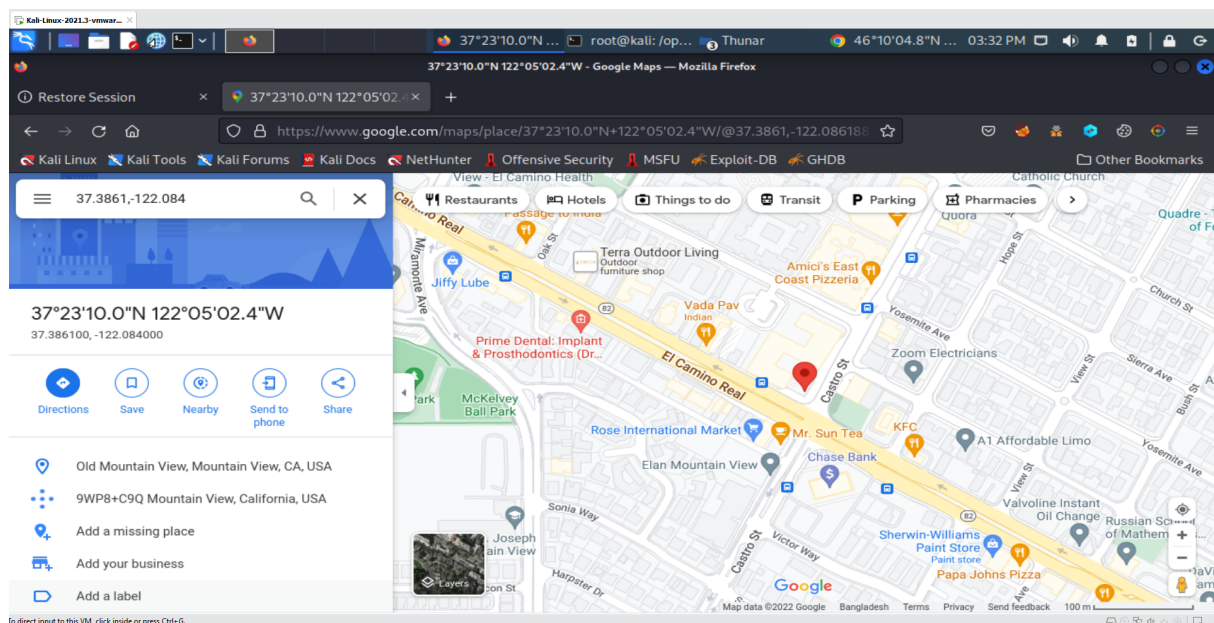
The git link of that tool is:

<https://github.com/htr-tech/track-ip?fbclid=IwAR2FSaZ5cEnxXbXA6NIW7Lk4zKfOAn7EW1xP4xkC0Z5grdqDxtXjrj1TtbU>

Here we Track the IP address and got the real location.



Geolocation:



Google map link:

<https://www.google.com/maps/place/37%C2%B023'10.3%22N+122%C2%B005'02.4%22W/@37.3862042,-122.0861887,17z/data=!3m1!4b1!4m5!3m4!1s0x0:0xc479177d9262e3cd!8m2!3d37.3862!4d-122.084>

Your IP: 209.85.220.41

Location: 800 W El Camino Real, Mountain View, CA 94040, United States

Second email: martinlatorre8888@hotmail.com

Step 1: Finding IP address

First I analyze your header with well-known tools named 'Cyber forensics'.

Link: <http://www.cyberforensics.in/OnlineEmailTracer/index.aspx>

Header:

Web site

Search

[Home](#) | [About C-DAC](#) | [Products](#) | [Downloads](#) | [Training](#) | [Contact Us](#)

6, 2022

Source Centre for Cyber Forensics - India

Online EmailTracer

Area ::

istuck

ofile

ut

EmailTracer is a tool to track email sender's identity. It analyzes the email header and gives the complete details of the sender like IP address, which is key point to find the cul Service Provider etc. EmailTracer traces up to Internet Service Provider level only. Further tracing can be done with the help of ISP and law enforcement agencies. The messa

Paste EMail Header here

Delivered-To: ttruan@gmail.com
Received: by 2002:a05:7208:c40a:b0:5b:9243:c7c0 with SMTP id bf10csp518572rbb;
Thu, 13 Oct 2022 14:19:09 -0700 (PDT)
X-Google-Smtp-Source: AfsMyM6c7aEevVFrpeEpkgyMfkuz2tyr2om9VQZnWtHK185650XUQZi790yKvaSwqcGqz
X-Received: by 2002:adf:fd50:0:b0:22e:5503:9c4c with SMTP id h16-
20020adfffd5000000b0022e55039c4cmr1224084wrs.375.1665695949741;
Thu, 13 Oct 2022 14:19:09 -0700 (PDT)
ARC-Seal: i=2; a=rsa-sha256; t=1665695949; cv=pass;
d=google.com; s=arc-20160816;
b=ukmkbkt1p6c1vfHZ5XbmLRTKmQ8TJkIGY7ai83dMRqa/WoCouZ7FIP1/OnmhUmjS+A
WcbboLbiEyIP5SAehWYTDYvha05x+ULW0vACTbuwX0xah2tsBr01+/aRKGsfsyXhonCO
4wileFL53qny/k7pE+Ke4Mw0810OVt0j2G7mUfVt5woojlMwdYeS2NoYJf6oTw1e76CO
epP3oqmHxHZJV7/u/hUHMvblHapdaPPHQE4KD7z8Gy3FjaeKck9YDJyYmA2Ef3MaIiq
5vqKmvNfPgB0+ZVyAs210VoRnyhp9IGLnz2Heuxx/MdPd0SIo31IIM2d13KSuhpUy3kj3
Kw2A==
ARC-Message-Signature: i=2; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=mime-version:msip_labels:content-language:accept-language
:message-id:date:thread-index:thread-topic:subject:to:from
:dkim-signature;
bh=97B7JrfXfCOyVavB41jxQQ0farCSX/J9Kig1MwFBsUUK4=;

Start Tracing

Email Crimes

How to extract EMail Header?

Traceroute: This means The total path that sender sends you the mail.


The mail appears to be originated from the computer with IP address 40.92.47.31

The sender's email address is

The message-id of the the mail is <>.

Path traced by the mail



 NAM04-BN8-obe.outbound.protection.outlook.com(40.92.47.31)
Thu, 13 Oct 2022 14:19:09 -0700 (PDT)



Thu, 13 Oct 2022 14:19:09 -0700 (PDT)



2002:a05:7208:c40a:b0:5b:9243:c7c0



sZFyIDK6+LqCnFbNyPybO6OUkU23/Zt4q5BMLwlo3fmC72dVTmmg3uueWIs/lofbhsnd1LFTVCr8m8lcR+Hbby9jFfsIeYGI

IP address: 40.92.47.31

Received By	Received From	Date
sZFyIDK6+LqCnFbNyPybO6OUkU23/Zt4q5BMLwlo3fmC72dVTmmg3uueWIs/lofbhsnd1LFTVCr8m8lcR+Hbby9jFfsIeYGI	2002:a05:7208:c40a:b0:5b:9243:c7c0	--
2002:a05:7208:c40a:b0:5b:9243:c7c0	--	Thu, 13 Oct 2022 14:19:09 -0700 (PDT)
--	NAM04-BN8-obe.outbound.protection.outlook.com[40.92.47.31]	Thu, 13 Oct 2022 14:19:09 -0700 (PDT)
NAM04-BN8-obe.outbound.protection.outlook.com[40.92.47.31]	--	--

Details obtained from Regional Internet Registry

Domain/Registrant	IP	Registry	Country	City/Address	ISP
NAM04-BN8-obe.outbound.protection.outlook.com	40.92.47.31	ARIN			

Step 2: Finding the Location:

Let's try to track the IP address with the same tools on kali Linux.

Here we Track the IP address and got the real location.


Google map link:

<https://www.google.com/maps/place/36%C2%B040'03.4%22N+78%C2%B023'14.6%22W/@36.6676043,-78.3895887,17z/data=!3m1!4b1!4m5!3m4!1s0x0:0xe33b23b2e85ad702!8m2!3d36.6676!4d-78.3874>

IP: 40.92.47.31

Location: 525 Madison St, Boydton, VA 23917, USA

More tools reference:



[Home](#) [All Tools](#) [DNS Lookup](#) [ISP DNS Servers](#) [Public DNS List](#) [Get Android App](#) [Get Chrome Extension](#)

Email Source Ip Info

Source IP Address	40.92.47.31
Source IP Hostname	mail-bn8nam04olk2031.outbound.protection.outlook.com.
Country	United States
State	Virginia
City	Boydton
Zip Code	23917
Latitude	36.6676
Longitude	-78.3874

IP Address	40.92.47.31
Country	 United States of America ⓘ
Region & City	Virginia, Boydton
Coordinates	36.667640, -78.387500 (36°40'4"N 78°23'15"W)
ISP	Microsoft Corporation
Local Time	15 Oct, 2022 03:58 PM (UTC -04:00)
Domain	microsoft.com
Net Speed	(COMP) Company/T1
IDD & Area Code	(1) 434
ZIP Code	23917
Weather Station	Boydton (USVA0084)
Mobile Carrier	-
Mobile Country Code (MCC)	-
Mobile Network Code (MNC)	-
Elevation	107m
Usage Type	(DCH) Data Center/Web Hosting/Transit

Bonus information:

I found all the cookies from apoderadosphja@gmail.com email.

Link:

<https://drive.google.com/file/d/1uTvurt5fWuxTJ4kCgbTyqRj8M8KFgiU0/view?usp=sharing>