

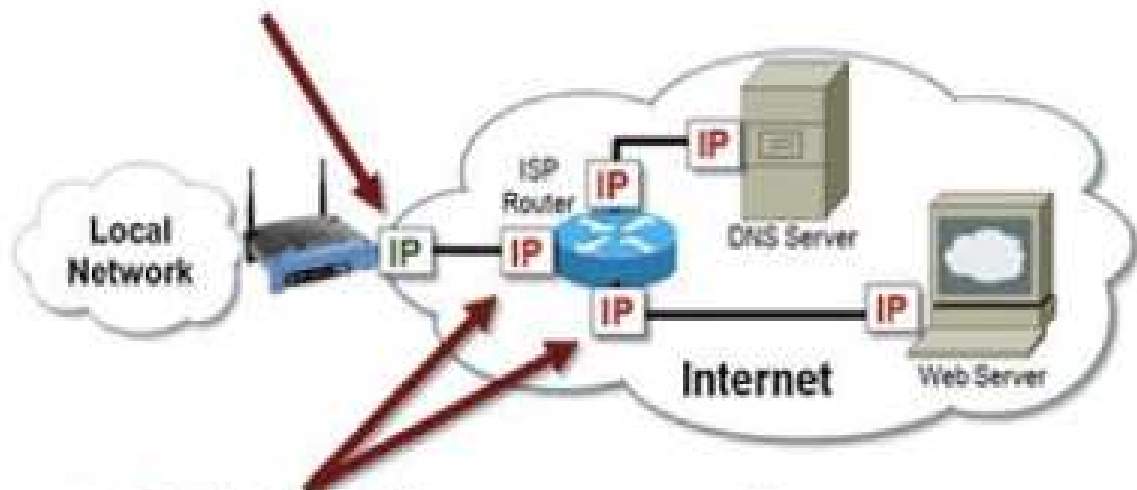
## Tracing an email address to an IP number

**Internet Service Provider (ISP)** will assign customers either;

**a static IP address** (Never changing)

or **a dynamic IP address** (Changes regularly).

- **Dynamic IP addresses periodically change**
  - Typically assigned to ISP customers



- **Static IP addresses never change**

Most IP addresses assigned today by Internet Service Providers (ISP) are dynamic IP addresses and change regularly or periodically.

*Tracing an email name/address to an IP address is very difficult because the IP address changes and the tracking information, or header, is deleted by the ISP or email provider.*

The email providers (gmail, yahoo, aol) DELETE ALL PREVIOUS digital information of the source of the email in the header before sending the email to the recipient.

# Emails are mostly hearsay as evidence in court of law.

Emails sent through gmail or yahoo are almost impossible to trace, because gmail and yahoo truncates the email header containing the originating senders source IP address information. Without the originating IP there is NO TRACING the source.

Phones do not regularly change numbers. Texting and email IP locations can be more accurately traced when a cell phone is used to send messages.

## (Expert Computer Forensic analyst website - Summary documentation)

Emails are considered *hearsay evidence*. Overall emails cannot be taken as evidence.

**1** One can create Emails using Microsoft Word, Publisher, etc., applications not send through internet. **One can copy and paste the email headers/body** including x-Originating IP Addresses.

**2** Emails can be automatically created using someone's personal information such as Name, Address, Telephone Number, and Signature in the body. **There are online automated spam bots** that does trace internet activates of billions of people and generate automatic auto mailer spam with real life information.

**3** When one sends an email using an email service such as yahoo mail, aol mail, Gmail, Hotmail, etc.....first that email captures the originating PC IP address. Then the email go through several email servers that captures their IP addresses.

Finally, **the email goes to the recipient with the last email server information only, which does not show the first originating email IP address.**

An email has multiple IP address data once it originates from a computer / location, until it goes to the final recipient which has **the LAST IP ROUTER IP address** - Not the original email sender's IP address number.

**4** *One who really wants to put someone in trouble can use online fake email sites to spoof your name and cyber harass/stalk that will get you into trouble because your name was on the email name.*

**5** There are **online email re-mailers that generate fake content based** on online behavioral activities. Therefore, these emails cannot be taken as authentic.

## FALSE EMAIL HEADERS

People send emails with false or "forged" headers, which are common in spam and unwanted or even malicious e-mail. **Trace Email tools do not and cannot detect forged e-mail. That's why that person forged the header to begin with.**

Source: <https://wordtothewise.com/2008/06/authenticating-email-in-a-court-of-law/>  
Word to the Wise, LLC, 225 E Bayshore Rd #120, Palo Alto, CA 94303-3220

## Example of TRACEABLE electronic messages sent from a government office

**Details for 74.87.107.194** - Static IP Address captured from Internet text messages on a private Internet server, NOT AN EMAIL PROVIDER.


Name: **Leavenworth Legal Association**

You are a liar and the deception .... will be made public. Do you even know what the truth is anymore? Or are you so self deceived you are out of touch with reality? You claimed you give guitar lessons to children every Tuesday at the library. For your information "children" is plural, you teach one child, not children. I will ...you....the wrong people. ***You should e more careful with ..... judges and lawyers. We may not win .... but it will get very expensive, for you that is. You could mortgage your home. Just an idea. See you in court soon. As you should know, we lawyers know how to drag these things out, and we will.*** Better get a job ...\*#@\*!#\*.

[IP: 74.87.107.194]

## LEAVENWORTH KANSAS STATIC IP - Router location

Geolocation Map from IP Address recovered from Internet message received

IP:	<b>74.87.107.194</b>
Decimal:	1247243202
Hostname:	map.firstcity.org
ASN:	11427
ISP:	<b>Time Warner Cable</b>
Organization:	Time Warner Cable
Services:	None detected
Type:	<u>Broadband</u>
Assignment:	<u><b>Static IP</b></u>
Blacklist:	
Continent:	North America
Country:	United States 
State/Region:	<b>Kansas</b>
City:	<b>Leavenworth</b>
Latitude:	39.2956 (39° 17' 44.16" N)
Longitude:	-94.9803 (94° 58' 49.08" W)
Postal Code:	66048

## FirstCity.org is a NON-CHANGABLE IP ADDRESS (Traceable)

Messages and threats have been received by a single father and the sending IPv4 traced to the Leavenworth city employees and to a T-Mobile phone: [IP: 172.58.14x.xx]

**THE POLICE ARE NOT INTERESTED IN FINDING THE REAL CRIMINALS - THEY JUST ACCUSE THE SINGLE FATHER OF CRIMES IN LEAVENWORTH**

The father receives threatening messages on the internet from the FirstCity.org server  
The Leavenworth police send their emails from this address (lvpd\_example@firstcity.org)

# **How to trace an email sender and the email IPv6 source**

## **Tracing the source of an email for legal purposes requires the following steps:**

1. Secure a copy of the original electronic email for evidence. **ONLY** the electronic copy of the email can be verified as an actual email and can verify the content of that email. The electronic copy, not a paper copy has valuable information one can glean.
2. The email address or account name (subscriber) and the UTC time of the email is all that is needed to start tracing the email source. The email header information has no real exculpatory evidentiary value for gmail, yahoo, aol, or most all email service providers.
3. Write a subpoena for Google (or Yahoo / Oath) Legal department / LER to acquire the IPv6 and exact UTC of the source computer or device that both setup the email account, and sent the email being traced.
4. Google or Oath Holdings Legal team or LER should answer the subpoena providing the IPv6 and UTC time for the email account creation, and the IPv6 and exact UTC time for the traced email.
5. The IPv6 and UTC time information is the **ONLY** usable and valuable evidence from the Google LER subpoena response. **THE GMAIL RECOVERY EMAIL ADDRESS HAS NO VALUE FOR IDENTIFYING THE SOURCE** of the email. The **CONTACT TELEPHONE NUMBER** is **WORTHLESS** too.
6. Determine the ISP (Internet Service Provider) for the IPv6 and UTC time for all email records received from the Google or Oath Holding (yahoo, aol) subpoena. Find the ISP from the IPv6 on an internet location finder IP tracing website (iplocation.net).
7. Write a subpoena for the legal department LER of the **IDENTIFIED** ISP Internet Service Provider (Comcast, TMobile, Sprint, etc.) with the IPv6 and UTC information of the traced email. Request in the subpoena information of the device in control of the IPv6 at the UTC time of the email.
8. The information received from the subpoena sent to the ISP **WILL HAVE THE INTERNET ACCOUNT HOLDER INFORMATION OF THE DEVICE IN CONTROL** of the IPv6 at the UTC time of the traced email (responsible party for the account, where, and when the traced email was sent).
9. The ISP account holder or responsible party of the device in control of the IPv6 at the time of the traced email **MAY POSSIBLY** have information for authentication of the email sender. The ISP information will provide some evidence for determining a possible authentication for a case.
10. There is **NO OTHER WAY TO TRACE AN EMAIL FROM GOOGLE OR YAHOO. THERE IS NO EASY WAY OF JUST CHECKING THE EMAIL HEADER.** The ISP will take subpoenas from law enforcement almost exclusively, **SO GOOD LUCK** getting the police to help with securing evidence for a defense attorney.