How to trace an email and the source of a gmail message

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

1. The first step is to 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 verify the content of that email. A FAKE EMAIL word processing document can be created with ANY CONTENT.

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 original email contains the email header information, which has no value for gmail, yahoo, aol, or most all email service providers.

3. Write a subpoena for Google (or Yahoo / Oath) Legal department (LER Law Enforcement Relations) to acquire the IPv6 and UTC of the source computer or device that both setup the gmail account, and sent the email being traced.

4. Google Legal 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 Google email.

5. The IPv6 and UTC time information is the ONLY usable and valuable evidence from the Google LER subpoena response.

6. THE GMAIL RECOVERY EMAIL ADDRESS HAS NO VALUE FOR IDENTIFYING THE SOURCE of the email. The CONTACT TELEPHONE NUMBER is WORTHLESS too.

7. The IPv6 and UTC time for all email records received from the Google subpoena can be traced to an Internet Service Provider ISP. Enter the IPv6 on an internet location finder IP tracing website (iplocation.net) and find the ISP sending the gmail email.

8. 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 information of the device in control of the IPv6 at the UTC time of the email.

9. The information received from the subpoena to the ISP WILL HAVE THE INTERNET ACCOUNT HOLDER INFORMATION OF THE DEVICE IN CONTROL of the IPv6 at the UTC time of the email (where and when the traced email was sent).

10. 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.

DETAILED STEPS FOR TRACING THE SOURCE OF AN EMAIL

1. Secure the original electronic copy of the email for evidence and evidentiary purpose of authentication.

ONLY the electronic copy of the emails has (exculpatory) evidentiary value in court. The message or content of the email can only be verified by the complete electronic copy of the email for evidence. Otherwise the police, district attorney, or opposing party can create A FAKE EMAIL word processing document with ANY CONTENT to make accusations and allegations. This is the first step of authentication of the email.

2. The email account name / subscriber and the UTC time of the email is all that is needed to start tracing the email source.

The original email contains the email header information, which has no real value for gmail, yahoo, aol, or most all email service providers. The email header could have value if the email is sent from a business or government source, like firstcity.org, which the emails are sent from the Internet Service Provider (ISP) routers (devices connected to the internet which the data passes from the business or government).

Emails from Google gmail accounts have all IP address information of the sender removed before the email is sent to the recipient. The email header IP information will always be the LAST ROUTER IPv6 ADDRESS OF GOOGLE, not the sender's IP address.

3. Write a subpoena for Google (or Yahoo / Oath) Legal department (LER Law Enforcement Relations) to acquire the IPv6 and UTC of the source computer or device that both setup the gmail account, and the IPv6 and UTC of the device that sent the email being traced. Any other IPv6 information associated with the gmail account activity could be helpful if available and provided by Google legal LER.

4. Google Legal LER should respond and answer the subpoena with the IPv6 and UTC time for the email account creation, and the IPv6 and exact UTC time for the traced gmail email.

5. The IPv6 and UTC time information is the ONLY usable and valuable evidence from the Google LER subpoena response.

6. THE RECOVERY EMAIL ADDRESS HAS NO VALUE FOR IDENTIFYING THE SOURCE of the email. The CONTACT TELEPHONE NUMBER is WORTHLESS too. This information can and probably is FAKE and created to frame / railroad someone (like a father trying to protect his son from being harmed with a hammer and is in family court proceedings to get residential custody).

THE RECOVERY EMAIL ADDRESS IS NOT THE SUSPECT especially if it is the email address of the accused father's son. IT IS WORTHLESS ALONG WITH THE CONTACT PHONE NUMBER, especially if it is the accused father's home phone number available on the internet to anyone (Kansas case number available).

This "RAILROADING" prosecution HAS BEEN DONE by police and the district attorney to a single father's trying to protect his son in custody proceedings with the district courts.

7. The IPv6 and UTC time received from the Google subpoena can now be traced to an Internet Service Provider ISP. Enter the IPv6 on an internet location finder IP tracing website (iplocation.net) and find the ISP sending the gmail email. The first 4 digits of the IPv6 usually identifies the service provider. The ISP will need a subpoena to identify and release the account holder information of the DEVICE IN CONTROL of the IPv6 at the UTC time of the email. The

IPv6 has the Mac address of the device used (phone/computer) embedded and identifiable. It is doubtful that the device is needed to prove the railroaded father's innocence, but a search warrant would be required to access the device if it is identifiable and required.

8. Write a subpoena for THE IDENTIFIED Internet Service Provider ISP (Comcast, TMobile, Sprint, etc.) with the IPv6 and UTC information of the traced email and give legal service to the legal department or LER of the ISP.

Some email providers do not accept subpoenas for civil or domestic cases. A motion for an order to compel may be required if the police will not help identify the criminal creating the emails..

9. The return service and information from ISP for the subpoena WILL HAVE THE ACCOUNT HOLDER INFORMATION OF THE DEVICE IN CONTROL of the IPv6 at the UTC time requested (where and when the traced email was sent).

10. 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 identified device could be a cell phone, residence, library computer, "burner" phone, or other device NOT TRACEABLE to authenticate the author of the email (hearsay evidence). Other processes can help identify the email sender. Closed circuit cameras may identify a suspect if the ISP is a public address or location.

The value of this exculpatory evidence could allow for a motion to dismiss by an attorney DEFENDING FALSE ALLEGATIONS and the "railroading" of a single father seeking residential custody. The father would be free from prosecution and NOT a suspect if the location, device, or time proves innocence.

Unfortunately, police detective Tesh R St John and Leavenworth district attorney Todd G Thompson may be uneducated on simple computer forensics, and therefore filed charges in THREE CASES on a SINGLE FATHER that is in THEIR DISTRICT COURT with proceedings for residential care of his son to protect the minor child from abuse in his mother's residential custody. Typical anti-father actions by police and district attorney - Not in the best interest of the minor child..

CRIMINAL CASES AGAINST FATHERS FROM FALSE ALLEGATIONS OF FAKE EMAILS ARE NOW A REALITY IN CUSTODY OR MODIFICATION PROCEEDINGS.

Fathers BEWARE of false allegations from fake emails. Once prosecution of this ILLEGAL EMAIL crap gets started by police and the district attorneys in family courts, the family attorneys against fathers will not stop it. They will use fake emails against fathers every time they can. As long as the police and district attorneys believe EVERY LIE spoken by the mother, their lying to hurt children and fathers will continue.

STOP THIS ABUSE OF LEGAL PROCESS AND PROCEEDINGS AGAINST FATHERS in domestic and family courts.

National Parent Organizations NPO and local and national Child and Father's Rights groups and the MEDIA should promote awareness and help to prevent Child and Father ABUSES from legal processes and proceeding.

SUPPORT and Promote Kansas FAIRCOURTS.net Legislation.

End of document: How to trace an email and the source of a gmail message.