Learning Pathways
How
What
Obtaining Provider Records

How can we help?
We want to help support your investigation by sharing electronic evidence collection methods and best practices. But we know you might have a few questions.
Read on for details about identifying providers, collecting information, and more.

---

**Reverse Location Records**
- Reverse Location Search
- Cellular Network and Handset Based Positioning
- How to Request Records
- How to Analyze Records
- Tips
  - Learn more >

**Voice/Text Records**
- Determine Provider
- Historical Records
- Subscriber/CDMA
- How to Request Records
- Identifying an iMessage User
- Tips
  - Learn more >

**Internet Service Records**
- Recognize IP Addresses
- Determine Provider
- IP Address Attribution
- Historical Records
- Tips
  - Learn more >

---

**Email Records**
- Investigating Email Records
- Historical Records
- How to Request Records
- Email Attribution
- How to Identify an Account
  - Learn more >
Obtaining Email Records

Find out how to use an Email Address to identify an account, as well as details on serving legal process to obtain records and more.

Skip ahead to:
- How can Investigating Email Records be Valuable to Law Enforcement
- What Type of Records may be kept by an Email Provider
- How to Request Email Records
- How toAttribute the Sender of an Email Message
- How to Identify an Account that was Accessed from a Particular Email Address
- Special Note about Subscriber Notifications
- How to Identify Associated User ID’s using Advanced Open Source Searches
- Tips for Working with Email Providers

How can Investigating Email Records be Valuable to Law Enforcement

Email can be a starting point or a key element in many investigations. Analyzing a subject’s email can provide you with information such as:

- Other email messages related to this investigation
- Sender information
- IP addresses
- Date and time information
- User information
- Attachments
- Content of the communications
- Application logs

There is a lot of valuable information available in the email header, but you need to know what to look for. By analyzing the extended email header, you can determine the originating IP address, which will help you discover the Internet service provider (ISP) the subject was using when they sent the email. Once you know the ISP used by the subject, you can use various legal processes to obtain records related to the subscriber of the Internet service.

Click Here for additional information on tracing the sender of an email message

Was this topic helpful? Yes / No
Obtaining Internet Service Records

Find out how to obtain Internet Service Records from providers to identify an account, as well as details on serving Internet traffic.

How to Recognize IPv4 and IPv6 Addresses

You are likely familiar with IPv4 addresses because they are used to route most Internet traffic. However, the Internet has many other kinds of address.

<table>
<thead>
<tr>
<th>IP Version</th>
<th>IPv4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0:56:14</td>
</tr>
</tbody>
</table>

Because global demand for IP addresses now exceeds the total number of IPv4 addresses available, a successor protocol, IPv6, was developed to create a much larger inventory of IP addresses that are used interchangeably to route Internet traffic. You will be able to easily identify the difference between an IPv4 and an IPv6 IP address.
Examples of Linked Job Aids

Network based Investigative Information

This job aid supports information on the National Domestic Communications Assistance Center (NDCAC) computer based training course “Basic Networking for Law Enforcement.” If this job aid is not helpful to you or you want more information on this topic, please review the course which can be found at the NDCAC portal at the Follow section.

These tables show the different types of network-based information that you can obtain during an investigation.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner’s name and contact information</td>
<td>Yes</td>
</tr>
<tr>
<td>Range of IP addresses associated with the domain</td>
<td>Yes</td>
</tr>
<tr>
<td>Obtains records from ISP through appropriate legal process</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote access investigation information, delegation records, and billing records</td>
<td>Yes</td>
</tr>
<tr>
<td>Research found in original source will provide additional facts for the case that this information may not be</td>
<td></td>
</tr>
<tr>
<td>Research based IP addresses</td>
<td>May provide more information to include in your research report</td>
</tr>
</tbody>
</table>

Domain: nmsi

WINSK tools may be able to provide:

- Registered owner’s (registered name, address, and contact information)
- Registered name, address, and contact information
- IP address associated with the domain (if domain is hosted on the Internet)

Usage: Remote research information: Names and addresses may provide you additional tools (be aware that this information may be fake)

Research based IP addresses using WINSK’s tools: This will provide the IP tool but you cannot obtain additional information regarding the network. To obtain addition information regarding the user and billing records, billing records for registered owner will provide you with more information (contact law for the domain name)

Training Center: Basic Networking for Law Enforcement

Introduction to ARIN’s Database

This job aid supports information on the National Domestic Communications Assistance Center (NDCAC) computer based training course “Basic Networking for Law Enforcement.” If this job aid is not helpful to you or you want more information on this topic, please review the course which can be found at the NDCAC portal at the Follow section.

The information in this job aid comes from the American Registry for Internet Numbers (ARIN) work at: www.arin.net

Once you’ve identified the date/time stamp associated with the originating IP address, you need to consider time zones and time zone offsets. International time zone tables will indicate the time zone, such as UTC (Universal Time Standard) or EST (Eastern Daylight Time), or you may use a “time offset” such as -0500 to -0000 UTC. Each offset may use a different time zone format. So you may use one meter code and time zone offset with or without the “UTC” indicator at the time zone standard time.

Sample 1: Convert the UTC time to EST, subtract 7 hours from UTC time of 10:57, giving you 13:57 EST.

Sample 2: Convert the UTC time to EST, subtract 8 hours from UTC time of 21:37, giving you 14:37 EST.

Daylight Saving Time (DST)

Daylight Saving Time (DST) is a way of making better use of the daylight in the evenings by putting the clocks forward so that there is more energy available. The time is set to the number of hours to add as the fall, DST starts in the northern hemisphere between March 20th and ends between September-November. The clock moves ahead (*longer hours*) in the spring when DST ends, and falls back one hour (*shorter hours*) when DST ends as the fall. To remember which way the clock goes, keep in mind that these typical “spring forward, fall back” terms begin in the northern hemisphere between September-November and end between March 20th.
“Three separate times today, for unrelated cases, I passed along another NDCAC gem...I’ve never seen such a concise tool for agents to determine what is possible.”

- Senior Investigator