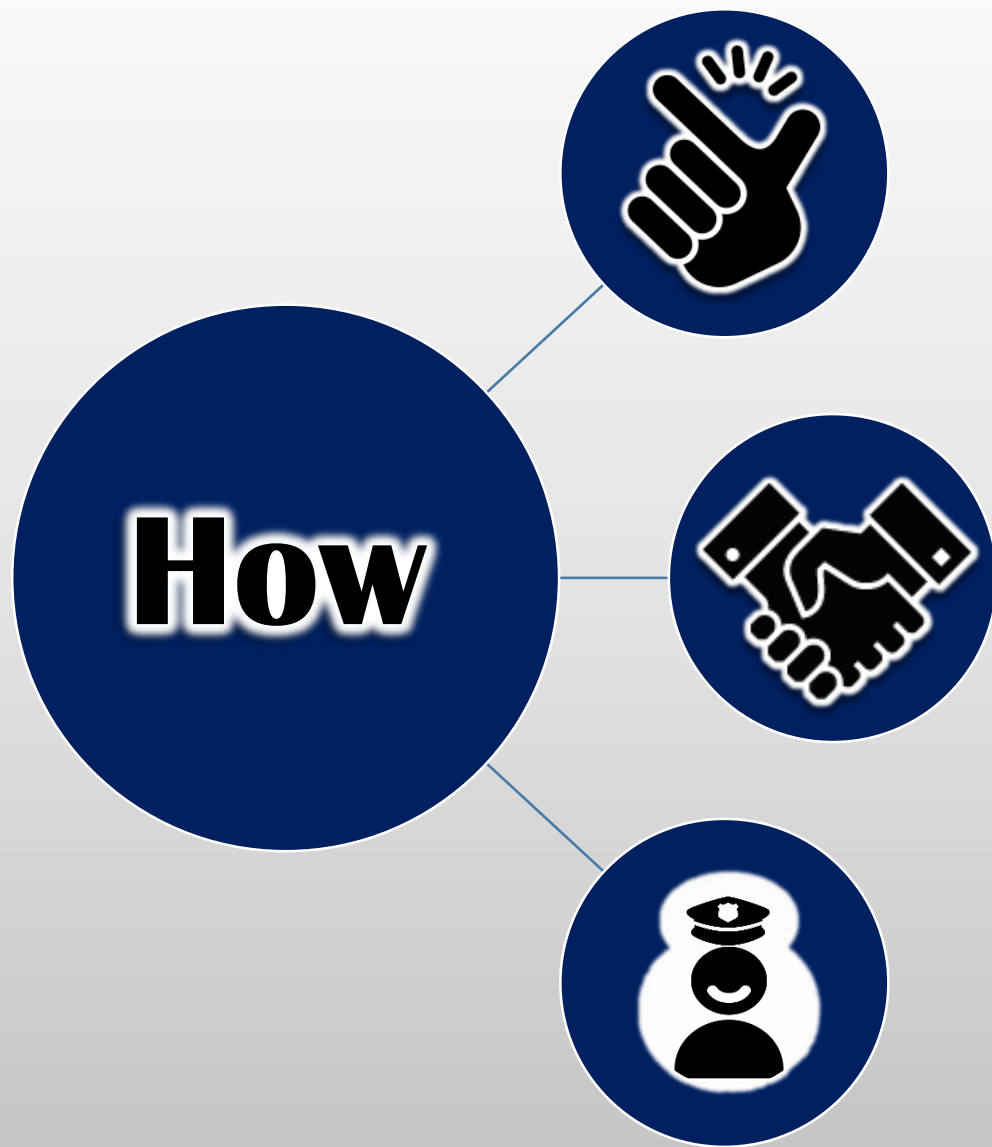




Learning Pathways









Obtaining Provider Records



Preserving Digital Evidence



NDCAC Tools for Record Analysis &
Management



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 Returns
Tips

[Learn more >](#)



Voice/Text Records

Determine Provider
Historical Records (Subscriber/CDRs)
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 >](#)



Preserving Digital Evidence



NDCAC Tools for Record Analysis & Management

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 Returns
Tips
[Learn more >](#)



Voice/Text Records

Determine Provider
Historical Records (Subscriber/CDRs)
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 >](#)

[Home](#) > [Obtain](#) > [Email Records](#)

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 to Attribute 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 e-mail 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

Sk

Ho

Ho

Ho

W

Ti

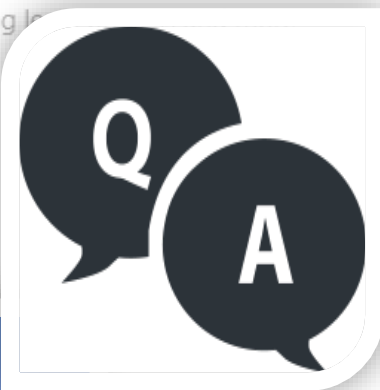


Address a Subject was Using

IP Address

er Account by IP Address

ined using an IP Address

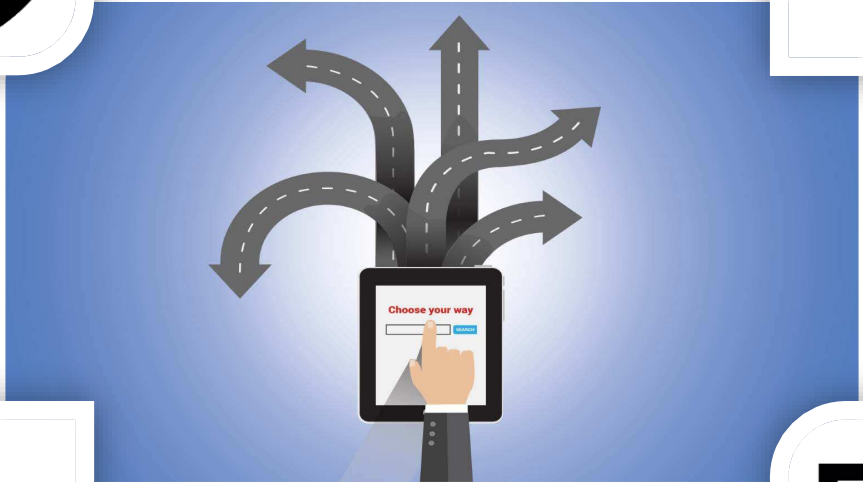
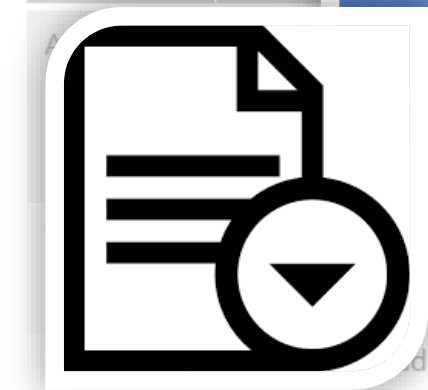


How to Recognize w

You are likely familiar w

are used to route most

IP Version	IPv4
------------	------



inning of the Internet and



ss.

0:56:14

address

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

UNCLASSIFIED

Network-based Investigative Information

This job aid supports information in the National Domestic Communications Assistance Center (NDCAC) computer based training course, "Basic Networking for Law Enforcement." If this job aid was helpful to you or you want more information on this topic, please review the course which can be found on the NDCAC portal in the [Training](#) section.

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

IP Address

Tools are available on the Internet that allow you to research information about an IP address associated with a subject. The typical information you can obtain includes:

- Owner's name and contact information
- Range of IP addresses associated with the domain

Next steps:

- Obtain records from ISP (through appropriate legal process): Records include subscriber information, allocation records, and billing records. Billing records for registered owner will provide more information (someone had to pay for the service)
- Research contact information: Names and addresses may provide additional leads (be aware that this information may be fake)
- Research related IP addresses: They may provide more information to include in your subpoena request

Domain name

WHOIS tools may be able to provide:

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

Next steps:

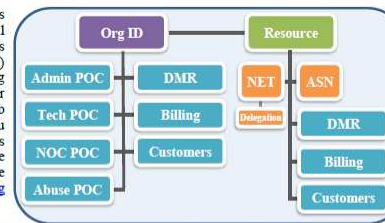
- Research registrant information: Names and addresses may provide you additional leads (be aware that this information may be fake)
- Research associated IP addresses using WHOIS tool: This will provide the Web host so you can subpoena additional information
- Subpoena registrar for records: You may be able to get subscriber records and billing records. Billing records for registered owner will provide you with more information (someone had to pay for the domain name)

Training Course: Basic Networking for Law Enforcement

UNCLASSIFIED

Introduction to ARIN's Database

This job aid supports information in the National Domestic Communications Assistance Center (NDCAC) computer based training course, "Basic Networking for Law Enforcement." If this job aid was helpful to you or you want more information on this topic, please review the course which can be found on the NDCAC portal in the [Training](#) section.



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

Perhaps ARIN's best-known function within the Internet community is the WHOIS directory service. WHOIS is driven by a large relational database with six classes of objects (as represented in the graphic), all of which interconnect to create meaningful searchable information.

Organization

Org ID

Example:

Org ID: An Org ID is a unique identifier representing an organization that is registered in the ARIN database. This identifier shows that entity's name, its physical address, and any Points of Contact (POCs) that have authority over it. In addition, all Internet number resources directly assigned or allocated from ARIN, as well as any downstream resources, must be registered to the appropriate Org ID. This means you must establish an Org ID before requesting resources. An entity may maintain multiple Org IDs for different accounts, or it may consolidate all of its resources under a single Org ID. For each Org ID, there must be at least one Admin, Tech, and Abuse POC with authority over it. NOC POCs are optional.

Field	Value
NetRange	190.212.0.0 - 190.212.0.255
ORIR	190.212.0.0/24
Name	ARIN PFS-IND
Handle	NET-190-212-0-1
Parent	NET-190-212-0-0-1
NetType	Dyn-Assignment
Origin AS	AS193225
Organization	ARIN Operations (BONICOPS)
Registration Date	2008-06-10
Last Updated	2010-07-15
Comments	
RESTful Link	https://whois.arin.net/rest/object/NET-190-212-0-1
See Also	Related organization's POC records.
See Also	Related delegations.

Course: Basic Networking for Law Enforcement

UNCLASSIFIED

Time Zones Job Aid

This job aid supports information in the National Domestic Communications Assistance Center (NDCAC) computer based training course, "Tracing Email Addresses for Law Enforcement." If this job aid was helpful to you or you want more information on this topic, please review the course which can be found on the NDCAC portal in the [Training](#) section.

The following information is available at www.timeanddate.com.

Coordinated Universal Time (UTC)

While you may be familiar with Greenwich Mean Time (GMT), Coordinated Universal Time or UTC replaced GMT as the official world time on January 1, 1972. UTC is based on atomic time at zero degrees longitude, which passes through Greenwich Observatory, a suburb of London, England. UTC uses a 24-hour clock that begins at 00:00 (midnight) and ends at 23:59 (11:59 p.m.).

Once you've identified the date/ time stamp associated with the originating IP address, you need to consider time zones and time zone offsets. Sometimes an extended email header will indicate the time zone, such as EST (Eastern Standard Time) or EDT (Eastern Daylight Time), or you may see a "time zone offset", such as -0500 or +0000 (UTC). Each server may use a different date/time stamp format. So, you may see time zone codes and time zone offsets with or without the "UTC" indicator in the same extended email header.

Example: To convert the UTC time to EDT, subtract 5 hours from UTC time of 19:57, giving us 14:57. The original email message was sent on Wednesday, Dec. 12 at 14:57 EDT.

Daylight Saving Time (DST)

Daylight Saving Time (DST) is a way of making better use of the daylight in the evenings by setting the clocks forward one hour during the longer days of summer, and back again in the fall. DST starts in the northern hemisphere between March-April and ends between September-November.

The clock moves ahead (= losing one hour) in the spring when DST starts, and falls back one hour (= gaining one hour) when DST ends in the fall. To remember which way the clock goes, keep in mind one of these sayings: "spring forward, fall back" or "spring ahead, fall behind"

Standard time begins in the northern hemisphere between September-November and ends between March-April.

DST Start/End Dates (2019-2020)

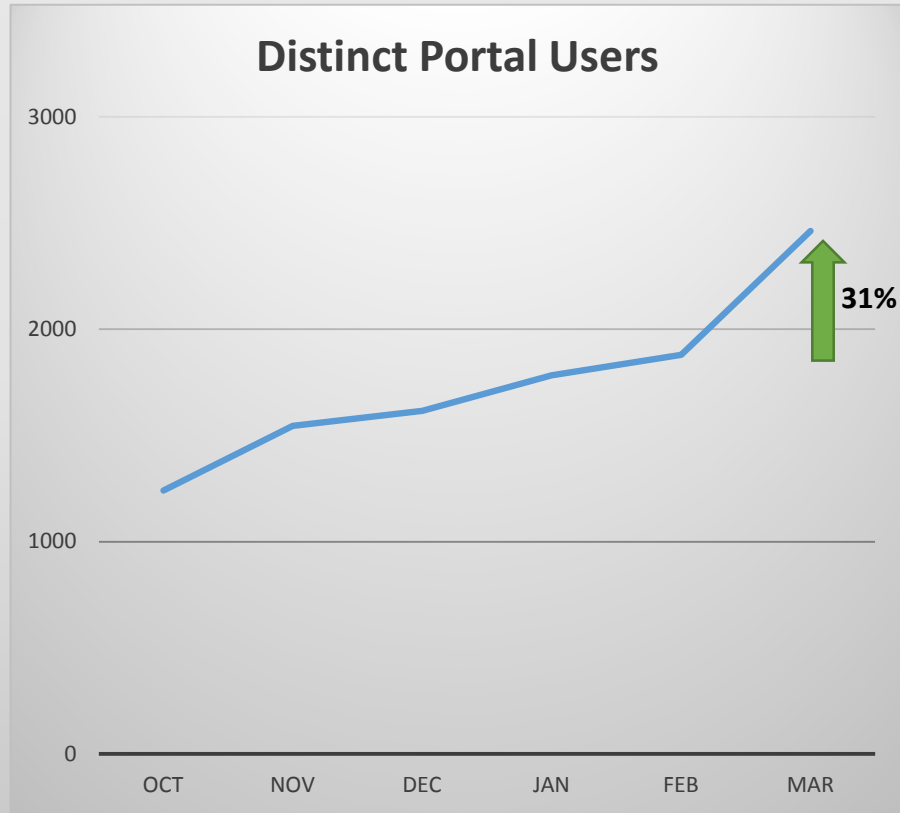
Time Zone	Date	Local Time	UTC Offset
EST	Sunday, March 10, 2019	1:59:59 AM	UTC - 5 hours
EDT (DST Starts)		2:00 AM → 3:00 AM	UTC - 4 hours
EDT	Sunday, November 3, 2019	1:59:59 AM	UTC - 4 hours
EST (DST Ends)		2:00 AM → 1:00 AM	UTC - 5 hours
EST	Sunday, March 8, 2020	1:59:59 AM	UTC - 5 hours
EDT (DST Starts)		2:00 AM → 3:00 AM	UTC - 4 hours
EDT	Sunday, November 1, 2020	1:59:59 AM	UTC - 4 hours
EST (DST Ends)		2:00 AM → 1:00 AM	UTC - 5 hours

Course: Tracing Email Addresses for Law Enforcement

Learning Pathways Dashboard



PORTAL USAGE TIMELINE



Highest Monthly Portal Usage



STAKEHOLDER FEEDBACK

COMMENTS RECEIVED

104

2

“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



~~~~~

Creating Provider Networks

Modern World  
Communication Systems  
Self Practice

