



***Subpoena Compliance
and
Special Investigations***

***Law Enforcement Assistance Guide
for Internet Investigations***

Law Enforcement Help Line (24/7): 877-646-6555

Facsimile: 703-886-0144



COMPLIANCE AND SPECIAL INVESTIGATIONS CONTACTS

	PHONE:	FAX:	EMAIL:
LAW ENFORCEMENT HELP LINE (24/7)	877-646-6555	703-886-0144	csi@mci.com
Maricon Corpuz, Investigator	703-886-3830	703-886-0144	maricon.corpuz@mci.com
L. Rebecca Rohrer, Investigator	703-886-3832	703-886-0144	laura.rohrer@mci.com
John St. Clair, Manager CSI	703-886-3822	703-886-0144	john.stclair@mci.com
Sally Weaver, Legal Assistant	703-886-4075	703-886-4399	sally.weaver@mci.com
Subpoena requests for <u>Internet</u> investigations:			
Director Network & Facilities Legal Team MCI 22001 Loudoun County Pkwy Ashburn, VA 20147	703-886-0700	703-886-0144	

NOTE: For investigations regarding telephone-related subscriber information, please direct requests to:

Subpoena Compliance
MCI
1133 19th Street, NW
Washington, DC 20036

Phone: 202-736-6885
Fax: 202-736-6970
Email: subpoena@mci.com

MCI COMPLIANCE AND SPECIAL INVESTIGATIONS

Introduction

MCI is a global telecommunications company with an expansive IP network, providing data and Internet services to businesses (including Internet Service Providers), state and federal government entities, and residential customers worldwide. **UUNET Technologies, Inc.**, an MCI Company, provides wholesale online dial-up, remote Internet access and high bandwidth dedicated access.

Compliance and Special Investigations (CSI) is an MCI resource dedicated to assisting Law Enforcement with *Internet* related criminal and civil investigations for which MCI may have evidence. The purpose of this guide is to provide Law Enforcement with a basic understanding of how MCI may assist with Internet investigations. The CSI staff is committed to providing timely and accurate responses to Law Enforcement requests. Questions and comments are encouraged.

Serving a Request on MCI

Subpoenas, search warrants and court orders may be served on MCI by any of the following methods:

- Facsimile (CSI requests a follow-up copy by mail)
- Mail
- Personal delivery

Upon receipt of a request, CSI assigns an internal MCI ticket (reference) number and acknowledges receipt of the request by fax. Investigation results are returned to the requesting officer by fax, unless CSI is otherwise instructed. The average subpoena response time is 7 – 10 business days. CSI endeavors to accommodate extraordinary circumstances or special response requirements when possible.

Request Format

In order to initiate an investigation, the following information is required to obtain accurate results:

- Internet Protocol (“IP”) address
- Date of connection
- Time of connection (if applicable)
- Time zone (when applicable, time zone information is *critical* to an accurate investigation as the time zone is determined by the machine on which the connection is logged, regardless of geographic location of the machine or the end user)

The language below, incorporating the above-referenced information, is suggested for a request pertaining to Internet connections:

“Please provide any and all subscriber and/or account information pertaining to the connection using [IP address], on [date], at [time; time zone.]”

Response Formats

The information available to CSI, and the format of CSI’s response, will vary depending upon whether the subject user’s Internet connection was established via a **dynamic** or **static** IP address. (Note: through its UUNET subsidiary, MCI sells Internet services to resellers or wholesale customers, who resell MCI products and services to Internet end-users, or large corporate customers. As such, MCI has no customer relationship with most end-users and therefore does not maintain detailed subscriber information or customer records for such users.)

Dynamic IP: An IP address that is temporarily assigned to an end user’s machine at the time and for the duration of each connection. The most common application of dynamic IP assignment is “dial-up” Internet access, which is established via a telephone line. Some DSL service connections are also dynamic in that a new IP address is assigned to the DSL end user each time the end user’s computer is turned on. MCI maintains dial-up and dynamic DSL connection logs. However, because many of these users are not direct customers of MCI, CSI has no visibility into the account information beyond the *username*. Generally, the MCI reseller who maintains the account can provide further information about the user (e.g. name, address, billing records, etc.). The reseller will most likely require a subpoena to do so.

Static IP: An IP address that is permanently assigned to a computer. This type of Internet connection is commonly referred to as *dedicated*, as it is “always on.” The end users are generally employees of MCI corporate customers or customers of resellers to whom MCI has

allocated a block of IP addresses. MCI does not maintain logs for dedicated access, however, CSI will provide contact information for the immediate MCI customer or reseller whom will most likely require a subpoena to provide information pertaining to the request.

The table below illustrates the information that may be provided by CSI depending on the subject user's means of Internet access.

Access Method	Response
Dynamic IP (e.g. dial-up access, some DSL services)	<ul style="list-style-type: none"> • Username (e.g. username@ispname.com) • Reseller (including contact information) • IP address of destination host, if available • IP address of source host, if available • Time of connection • Time of disconnect • ANI (Automatic Number Identification), if available • DNIS (Dialed Number Identification Service), if available
Static IP (e.g. dedicated connections, some DSL services)	<ul style="list-style-type: none"> • Site name (an MCI internal account identifier) • Company name (the reseller or corporate customer to whom subject IP has been allocated) • Company contact information (e.g. address, phone/fax numbers) • Technical contact (phone, fax and/or email, if available) • Security contact (phone, fax and/or email, if available)

Frequently Asked Questions

What is the turn-around time on a subpoena request?

CSI's average response time is 7 - 10 business days, but may vary depending on the circumstances.

Why is it important to provide the accurate time zone information on a request?

The correct time zone information is a *crucial* element for CSI to conduct an accurate investigation. A connection's time zone is determined by the machine that logs the connection, regardless of the machine's geographic location. For example, a logging machine that is physically located in the Pacific time zone may be set to log all connections in Eastern time. Please also note that the geographic location of the end user is irrelevant to the time zone of the connection.

When obtaining connection information, always confirm the correct time zone with the source of that information.

What is the retention period for MCI's connection logs?

Logs for dial-up connections are maintained for approximately two years. MCI does not maintain logs for dedicated access.

Why is ANI not always provided in responses?

The availability of ANI (origin telephone number) depends on the machine (or server) that records the log-on information. Older machines that are still in use may not be configured to record ANI. If requested, ANI information is always included in CSI's response when available.

Does MCI require a subpoena to confirm if a company or user associated with a particular IP address is an MCI customer?

Yes. Disclosure of customer or user information is limited by both contractual obligations to limit disclosure of such information and by federal and state laws that limit or prohibit disclosure of information.

Does MCI alert its customers about requests served seeking information relative to criminal investigations?

No. MCI maintains strict confidentiality with respect to all criminal matters. Customers are not notified by MCI.

In the case of an international investigation, can a request be served on MCI in the U.S. if the records reside with an MCI company overseas?

No. Requests seeking information relative to an overseas investigation must be served on the appropriate entity in the country where the records reside.

Common Terminology

Access number: A telephone number dialed by a subscriber to connect to the Internet. May also be referred to as DNIS (Dialed Number Identification Service).

ANI (Automatic Number Identification): The origin telephone number from which the connection to the Internet was established. (ANI information is not always available. When captured, it will be included in a subpoena response.)

Authentication: The verification of the identity of a person or process.

Dedicated connection: A high speed, "always on" connection to the Internet.

Destination host: The dial-up user's computer. The destination host is assigned a dynamic IP address by the *source host* upon, and for the duration of, a dial-up user's connection to the Internet. Because this IP address is "dynamic" it varies with each connection.

Dial-up connection: A temporary connection between computers established over a telephone line.

DNIS (Dialed Number Identification Service): The number dialed by a user or computer to connect to the Internet. (Also known as an Access Number.)

DNS (Domain Name Server or Domain Name System): A mechanism on the Internet that translates Internet addresses (URLs) into their corresponding IP addresses.

DSL (Digital Subscriber Line): High speed Internet connection over ordinary telephone lines. Depending on type of DSL services, the associated IP address may be dynamic or static.

Dynamic IP: A temporary IP address assigned to an end-user at the time and for the duration of each Internet connection.

Host: A computer that allows users to communicate with other host computers on a network.

IP address (Internet Protocol address): A unique, 32-bit number assigned to a specific host (computer) on the Internet. All Web addresses (e.g. www.mci.com) and email addresses (e.g. abuse@mci.com) have a corresponding IP address.

Message header: The information at the beginning of an email or bulletin board message that contains the identities of the mail servers that the original message traveled through to get to its final destination.

Point of Presence (PoP): A physical site with a collection of telecommunication equipment, including devices designed for network access via dial-up connections.

Protocol: A series of rules and conventions that allow different kinds of computers and applications to communicate over a network.

Reseller: A direct MCI customer who resells MCI's products and services under its own name. MCI allocates blocks of IP addresses to reseller customers who may reallocate the IP numbers to their own customers.

Server: A computer that provides information to other computers and/or machines on a network. For example, *web servers* send out web pages; *mail servers* deliver email; *list servers* administer mailing lists, etc.

Source host (Source IP): The network access server that assigns the dynamic IP address for a dial-up Internet connection to the dial-up user's computer (the *destination host*).

Static IP: An IP address permanently assigned to a computer or other network machine; typically associated with *dedicated* connections.

Traceroute: A utility that displays the connection path from one machine to a destination machine, showing the amount of time it takes to get from start to finish and identifying each machine through which the traffic travels.

URL (Universal Resource Locator): An Internet address, such as *www.mci.com*.

Username: The unique account identifier of an Internet user.

Whois: An online, searchable database of domain names available via the Internet. Whois search results can provide detailed contact information for persons or entities to whom IP addresses are assigned and/or domain name registrations are registered. (See www.arin.net)