Standard Operating Procedures -- Pueblo High-Tech Crimes Unit Investigative and Technical Protocols -- Tracing an E-mail Address to an Account Holder/User 5 Jan 2000

Cmdr. Dave Pettinari Pueblo County Sheriff's Office davepet@cops.org

# Tracing an E-mail Address to an Owner

Many times you can identify someone with as little as an e-mail address. If you've ever posted to a newsgroup, signed a guest book, participated in a mailing list or forum, chances are people can find out a lot of information about you with just an e-mail address. Here are some things that you can try:

### 1. Go to http://www.dejanews.com

click on POWER SEARCH, (in the upper right hand corner in the tan box) in the AUTHOR box, type the e-mail address that the person is using. This should bring up any articles that he/she has posted. Pay close attention to this because often the author will post an article looking for teen boys, illegal weapons or drugs then a few months ago he tried to sell a VCR and has included a home telephone number. You may also find Web page addresses, other e-mail addresses, an online resume or something that will help you identify him or her.

#### 2. Go to http://www.altavista.com

and type in an e-mail address. This could show other places on the Internet that he has posted something using that e-mail address. Again, you may find a Web page or some other important information.

- 3. If you do happen to find a Web Page, download it while you are there because it can be changed or deleted at anytime.
- 4. Go to Infospace.com and do a reverse e-mail search. You can also use this site to do other searches such as reverse phone number searches and address searches.
- 5. If you would just like to know where the ISP (Internet Service Provider) is located, go to Internic.com and type in the domain name. It will tell you who that domain is registered to. This of course will not be of much help if he or she has a nationwide ISP such as Netcom, AOL, Compuserve or Prodigy.
- 6. Go to Search.com and type in a name or an e-mail address. If that e-mail address has been used to post anything to the Internet, you should get some hits.

## Does Your Target Have a Web Page?

If you have an e-mail address for your target there is a chance that he or she could have a web page that could give you more information about them. Here are some things that may help you find their web page:

- 1. If you have an e-mail address of a person such as badguy@hisplace.com, you could check for it by going to http://www.hisplace.com/~badguy Of course you would replace the word hisplace with the name of the ISP he is using and the word badguy with his username.
- 2. Here are some places that you can look for a home page: If the person is using AOL, try going to http://members.aol.com/username. Be sure to replace the word username with his or her screen name.

If the person is using an ATT account (user@worldnet.att.net) you can find out if he has a home page by going to: http://home.att.net/ and search for a member page or try http://home.att.net/~username. Remember to replace the actual user name of your suspect with the word username.

If the person is using a Netcom account (user@ix.netcom.com) you can find out if he has a home page by going to http://pw1.netcom.com/~username or http://pw2.netcom.com/~username.

3. Once you do find a web page, you may want to check the source. Sometimes you'll find real name information in the top part of the HTML code. With your mouse, right click in the center of the page and go down to VIEW SOURCE. If there is any personal information, it will be included in the META TAGS near the top.

# Tips and Tricks

If you are undercover on the Internet, make sure that you stay undercover and pay attention to what the target asks you to do. One little slip up can blow a case real fast. Here are some things to look out for:

1. If your suspect happens to give you any hyperlinks to follow, be sure that you use \*ONLY\* the account that you have created for your undercover work. If you happen to be at home or somewhere else and must go to an unknown hyperlink, go to http://www.anonymizer.com/surf\_free.shtml.

Standard Operating Procedures -- Pueblo High-Tech Crimes Unit Investigative and Technical Protocols -- Tracing an E-mail Address to an Account Holder/User 5 Jan 2000

Type in or cut and paste the address in the URL box so that you can use the anonymous Free Anonymizer.

- 2. If your suspect asks you to type a certain type of document and attach it to e-mail to send it use caution! While posing as a teen I was once asked to produce a doctor's statement proving that I was not HIV positive. I prepared the document using MSWord and luckily I had used some alias at the time that I installed MSWord. The person that I was talking to downloaded the document, opened it using MSWord, checked the properties and found the name that I had used at the time of the installation of Word. He asked me about it and I told him it was my mother that set up my machine.
- 3. DO NOT send e-mail from anywhere other than your undercover account even if you change the configuration of the software. The headers will show what ISP the e-mail came from. Try it out first by sending e-mail to yourself.
- 4. If you do not have an undercover line, be sure to block your line by pressing \*67. You can have it blocked permanently by calling your local telephone company. Also remember that when calling an 800 or 888 number or by using a cell phone that has not been blocked, the party that you call will have your name and phone number too. Keep all of this in mind when using any of the Web based voice mail programs http://www.pagoo.com as well.
- 5. Use a pre-paid phone card from a local discount store to make necessary long- distance calls.
- 6. If you are posing as a kid, be careful about opening links that contain a web-based greeting card. Some of those services will send a message to the greeting card sender and tell them the date and time that they card was received.
- 7. If you are using an http://www.hotmail.com or http://www.yahoo.com web-based e-mail account, make sure that you sign completely out every time or someone can log in and read your e-mail.

#### **AOL Powertools**

If you are using AOL for an undercover account, I suggest you try PowerTools 7.6.38 from BPS SoftWare Inc. It is Shareware and can be downloaded and tried for about two weeks free of charge. Sign on to AOL and go to KEYWORD BPS to download your copy. Features include:

1. The PowerIM Manager consolidates all of your active IMs into a single window. It has tabs for each person so that you don't get lost with all of the windows that are open. It will also log the IM so that you can read it easily.

Standard Operating Procedures -- Pueblo High-Tech Crimes Unit Investigative and Technical Protocols -- Tracing an E-mail Address to an Account Holder/User 5 Jan 2000

- 2. Custom Phrase Manager (a.k.a. macro) allows you to create and manage prepared text phrases which can be sent to Chat Rooms, Instant messages, E-mail messages or Forum postings. This is great for things that you need to remember or say frequently.
- 3. With the PowerTools Action Recorder, you simply click the Start button to activate its recorder, and then navigate to anywhere on AOL. The Action Recorder will record your every move.
- 4. If you do not use AOL but need to talk to someone that does have an AOL account, go to http://www.aol.com and register and download the free AOL Instant Messenger.