is required for creating an e-mail account. Criminals exploit this advantage and create e-mail accounts using false identities.

In case a Web-based e-mail account is used for sending offending messages, an investigator can contact the provider of the account to find the IP address of the user who connected to the Web site to send the mail. After performing IP address authentication, the investigator can get the sender’s information.

**Searching E-Mail Addresses**

After getting the suspect’s contact information, such as e-mail address, name, and phone number, the investigator can use various Internet search engines to find more information about the suspect.

The following search engines are used for searching for e-mail addresses:

- **http://www.dogpile.com**: This site searches all the most popular engines and then provides more comprehensive and relevant results. The site provides a comprehensive background report that has all the information about a suspect, including age, current and previous addresses, phone number, occupation, bankruptcies, tax liens and judgments, and property ownership.

- **http://www.searchscout.com**: This is a powerful tool that assists in tracing an offender by delivering relevant search results for keyword queries and giving ample search options to investigators. This search site provides investigators with the option to look up e-mail addresses and trace e-mails back to the source. It has powerful lookup tools, an e-mail directory, and an in-depth guide for advanced searching so an investigator can find names connected to street addresses, phone numbers, and e-mail addresses.

- **http://www.altavista.com**: This site allows an investigator to search for a suspect based on various criteria, including name, phone number, and e-mail address.

- **http://www.mamma.com**: This is a metasearch engine, which concurrently searches a variety of engines and directories and provides the most relevant results after eliminating duplicate information. It provides various options to allow an investigator to refine the search.

- **http://www.infospace.com**: This site has a reverse lookup option that makes tracing e-mails easy and quick. An investigator can refer to e-mail directories and public records while investigating a suspect.

- **http://www.emailaddresses.com**: This is a free e-mail address directory. It provides a wide range of search criteria, such as reverse lookup and search by city, state, and business. Any single piece of information can be used to retrieve a suspect’s information.

- **http://www.google.com**: This search engine serves as a convenient way for tracing e-mails. The people search has two criteria: phone number and e-mail address. An investigator can also perform an instant background check. Many popular e-mail search sites use this search engine.

**Tool: LoPe**

LoPe (Figure 7-22) is an e-mail forensic tool that has the following features:

- It extracts all e-mail messages and attachments from multiple .pst files.
- It recreates the internal .pst folder structure.
- It extracts all message headers and properties.
- Files are exported in MSG, EML, or XML format.
- It hashes every message and attachment.
- It offers a command-line interface so it can be easily batch scripted.
- LoPe allows a user to customize XML output format using XSL style sheets.

**Tool: eMailTrackerPro**

eMailTrackerPro analyzes e-mail headers and provides the IP address of the machine that sent the e-mail. It also provides the graphical location of that IP address so an investigator can track down the sender (Figure 7-23).

eMailTrackerPro also protects users from spam by blocking mail that comes from blacklisted sites. Users can also easily report e-mail abuse. eMailTrackerPro can create a report and send it to the offending user’s ISP.