Setting up an Online Investigative Computer:
Hardware, Connectivity and Software Recommendations

Keith I. Daniels
SEARCH Training Services
June 2004

SEARCH
The National Consortium for Justice Information and Statistics
7311 Greenhaven Drive, Suite 145 • Sacramento, California 95831
Phone: (916) 392-2550 • Fax: (916) 392-8440 • Internet: www.search.org

Introduction

There are many considerations a justice agency should address in setting up an undercover investigative computer. This computer will, after all, contain sensitive documentation that at some point will become *real* evidence to be used in court proceedings. Continuity and preservation of evidence will come into play every time defense counsel feels there has been a breach. With this in mind, agencies also must create a machine that is not only legally secure but also operationally protected from hackers. It is also imperative that investigators have as many of the tools they may need to conduct the wide array of investigations they will be called upon to perform. As with the rapidly changing face of technology and the criminals who use it, the configuration of a computer such as the one described here will also change with time. This list is by no means exhaustive and will be updated at regular intervals as required. For online updates, see SEARCH's Training Resource Links page (www.search.org/training/resources.asp), which also offers a wide range of useful investigative and forensic links.

The Undercover Computer: General Guidelines

- **The computer must be standalone and must not be networked with another computer in any way**. In and of itself, this network issue can raise considerable discussion among investigators. However, the fewer people who have contact with the potential evidence on the undercover hard drive, the better. This leaves fewer "smoke and mirror" arguments from defense attorneys.
- **The computer should have removable drive-trays**. This permits the investigator to remove and lock up a particular drive when it is not in use. This also permits other investigators to utilize the computer using their own drives.
- **Online investigators should work in an office that is not open to pedestrian traffic from coworkers or visitors**. This type of work can be very demanding, requiring concentration and minimal distractions.
- **With respect to the computer configuration, there are many schools of thought, but no "hard and fast" rules**. Consider the following guidelines some suggest in setting up a computer for investigative purposes:
  - Use the largest, fastest computer available
  - Use the largest-size drive available
  - Use the maximum amount of RAM
  - Use an internal CD burner
  - Use an external Firewire or USB2 DVD burner
  - Consider a video card with as much onboard RAM as possible
  - Consider dual flat-panel monitors with the largest screen size possible (this permits more usable space for investigative tools and is easier on the eyes)
  - Use a laptop that permits 802.11b or g wireless access (g is preferred)
  - **Note:** Using a laptop computer as the main investigative unit is *not* recommended, for a variety of usability and expense issues.

Connectivity Recommendations

The following are our minimum recommendations for providing Internet connectivity to the undercover computer:

- 1 high-speed connection not shared with the department
- 1 dialup
- 1 America Online (AOL) account
- 1 cold phone line

Multiple connections permit the investigator to attack a suspect from several angles. There are occasions in which one connection is just not enough. It is possible that the investigator may want to pretend to be two different people when communicating online with a suspect.

Software Recommendations

While software programs are as varied as online investigations, there are some standard programs that we recommend—some that offer general functions, and some more specific to online investigations.

General

- **Microsoft Office Suite** (http://office.microsoft.com/home/default.aspx), which offers desktop business applications, specifically:
  - Microsoft Word
  - Outlook
  - PowerPoint
  - Excel
  - Access
  - Live Meeting
  - Front Page
- **Windows XP Professional** (www.microsoft.com/windowsxp/pro/default.asp). With Microsoft being the de facto standard operating system for both home and office usage, Windows XP Professional is preferred over the Home edition. Online investigators are considered "power users" who may wish to take advantage of the added features of XP Professional, such as:
  - EFS (Encrypting File System)
  - System restore, which is more robust and offers more options in the event of a system crash

Web Browsers

- **Internet Explorer** (www.microsoft.com/windows/ie/default.mspx).
- **Mozilla** offers some interesting alternatives in Web browsing and can greatly assist in a hacker investigation (www.mozilla.org/).
- **Netscape Navigator** (http://channels.netscape.com/ns/browsers/download.jsp).

Image Viewers/Enhancers and Log Viewers

- **PowerDesk Pro** is like Windows Explorer, but on steroids. It aids in viewing logs and images very quickly. There is a free version but it does not offer the viewer. The viewer for this software makes it possible to scroll rapidly through images, moving files and text documents, and can save considerable time in the log/image review process (www.v-com.com).
- **Photoshop 7 or CS** is desktop digital imaging software that enables investigators to enhance images, even at a basic level. While expensive, this tool can manipulate images in ways that other programs cannot. This permits investigators to view parts of an image that ordinarily cannot be seen using regular viewers. The ability to do this can open up other avenues in the investigation by providing additional evidence (www.adobe.com/products/photoshop/main.html).
- **Irfanview** is **a** free graphic viewer program (www.irfanview.com).
- **Quick View Plus** provides added features for a viewer, such as print, copy, paste, compile and archive functions (www.avantstar.com/).

System Protection

System protection is extremely important and often overlooked as an unnecessary expense. It is not until a virus strikes or a system attack is launched that these programs pay for themselves.

- **Norton SystemWorks Suite** (www.symantec.com).
- **McAfee Internet Security Suite** (http://us.mcafee.com/root/package.asp?pkgid=144).

Firewalls

A good firewall can be invaluable in protecting the online computer and can function as an investigative tool (such as by capturing IP addresses).

- **Tiny Personal Firewall** is freeware (www.tinysoftware.com).
- **ZoneAlarm Pro** (www.zonelabs.com).
- **Sygate personal firewall** (www.sygate.com).

Spyware Utilities

With the ever-increasing problem of computers being bombarded with spyware, it is imperative that online investigators download one or more of these utilities and keep it up-to-date at all times.

- **Ad-Aware**, a spyware removal program, is free to agencies, organizations and individuals, but is not free to corporations (www.lavasoftusa.com).
- **Spybot-Search & Destroy** is a free spyware removal program (www.safer-networking.org).
- **Spy Hunter** (www.enigmasoftwaregroup.com/).

Screen/Image/Webpage Captures and Trackers

During the online investigation, the ability to capture images, moving files and entire Web pages can enhance the evidence capture, continuity and court preparation.

- **Camtasia Studio** is an outstanding screen capture utility that can also make moving image captures in "real time" of images like Webcam sessions. It is also possible to record a complete online session and create an audio voiceover to accompany it. Bear in mind that Camtasia does not capture *all* moving files from a Web page—this has to be done using other methods (www.techsmith.com/).
- **Photo Studio** is a small utility program that permits investigators to read the Exif headers of digital photographs, thus providing a myriad of information about the camera, its settings, and the date and time that the image was taken. In the event that there is a partial download of an image, a complete thumbnail of those images arrives first and is embedded into the EXIF header. This is a free program (www.stuffware.co.uk).
- **Cogitum Co-Citer** is a tool used to create collections of texts from the Internet. It captures the selected text, its Internet address, its title and the date it was added to the collection (www.cogitum.com).
- **Cogitum Image Co-tracker 2.0** is a tool used to create a database of images from the Internet. It captures the image itself, its Internet address, the Internet address where it refers to, its name and the date it was added to the database. This is a free program (www.cogitum.com).
- **Adobe Acrobat 6.0** enables Web page captures and converts documents to .PDF format for evidence disclosure purposes (www.adobe.com/products/acrobatpro/main.html).
- **Web capture utilities.** A number of shareware or freeware Web capture utilities are available; these tend to vary in ease of use and cost. (Review potential downloads at www.tucows.com/.)

Chat/Instant Messenger Utilities

- **Peer-to-Peer file-sharing programs,** such as Kazaa (www.kazaa.com/us/index.htm)
- **MIRC**, a shareware chat script, which provides a user-friendly interface for Internet Relay Chat (www.mirc.com).
- **Instant Messengers:**
  - **Yahoo! Instant Messenger**, a free service (http://messenger.yahoo.com/).
  - **America Online Instant Messenger** (AIM), a free service (www.aim.com/get_aim/win/latest_win.adp?aolp=).
  - **I.M. Frame**, an AIM Instant Messenger logger (www.bpsssoft.com).
- **PowerTools Professional**, which logs AOL chat sessions and manages chatrooms. For example, while attempting to enter rooms that are full, it will actually continue to "knock on the door" until someone leaves; at that point, the user is automatically entered into the room (www.bpssoft.com/IMFrame/).
- **Dead AIM**, an AIM chat log capture utility (www.jdennis.net).

Newsgroup Readers

Newsgroups/Usegroups should not be overlooked as an investigative tool or a place where proactive investigations can be conducted. As such, the investigator will require a newsgroup feed that provides the maximum amount of groups available. While most, if not all, Internet Providers give access to newsgroups, the number actually permitted can vary. Some are content-filtered and others are not. In choosing a newsgroup feed, it is imperative that questions are asked as to the completeness of service. It is suggested that a separate account be created with one of the main newsgroup providers that will provide an up-to-date list in the area of 85,000 groups. Once an account has been established, a newsgroup reader will be required.

- **Newsgroup/Usegroup feeds**
  - www.giganews.com/
  - www.newsfeedsunlimited.com/
- **Newsgroup Readers**
  - Free Agent (www.forteinc.com/)

Necessary Web-based Accounts

Sign up for these Web-based accounts, which offer chat message groups and boards, instant messaging, and email, among other functions.

- **An Ebay account** (www.ebay.com/).
- **An ICQ account** (www.icq.com/).
- **An MSN Hotmail account** (www.msn.com/).
- **An MSN Passport account** (www.msn.com/).

Connection Identification and Internet Protocol (IP) Address Tracers

- **TCPVIEW**, a program that shows detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections (www.sysinternals.com/ntw2k/source/tcpview.shtml).
- **An account with MaxMind GeoIP Region**, which is a country and regional IP address locator program. It is not free, but it is well worth the price. While only accurate for the United States and Canada, it will provide the location of a user of a particular IP address to the city and postal code. They have achieved this by purchasing databases that have been created from online purchases. They have millions of addresses in their database but do not cover such addresses as AOL or Earthlink. While GeoIP does not identify a user, it can aid in pinpointing the jurisdiction in which the perpetrator resides (www.maxmind.com/).

Online Investigation Training

Training is available in online investigations from SEARCH, including these courses:
— Investigation of Online Child Exploitation, Level I
— Investigation of Online Child Exploitation, Level II
— Basic Digital Media Analysis for the Online Investigator
— Proactive Online Prevention for Schools
— Introduction to Internet Crime Investigations
— Advanced Internet Investigations

See www.search.org/training for course descriptions and dates. These courses are offered at our facility in Sacramento, California, and also at sponsoring sites nationwide. (Various sources fund SEARCH training courses, including agencies of the U.S. Department of Justice and the California Commission on Peace Officer Standards and Training.)

Remember to bookmark SEARCH's **Training Resource Links page** on our training page (www.search.org/training/resources.asp). Here, investigators will find numerous links to aid in online investigations.

If you know of any other programs that you find useful for online investigative purposes, please advise us and they will be added to this list. Submit your suggestions, or your questions, to:

Keith I. Daniels
Computer Training Specialist
SEARCH Group, Inc.
keith@search.org