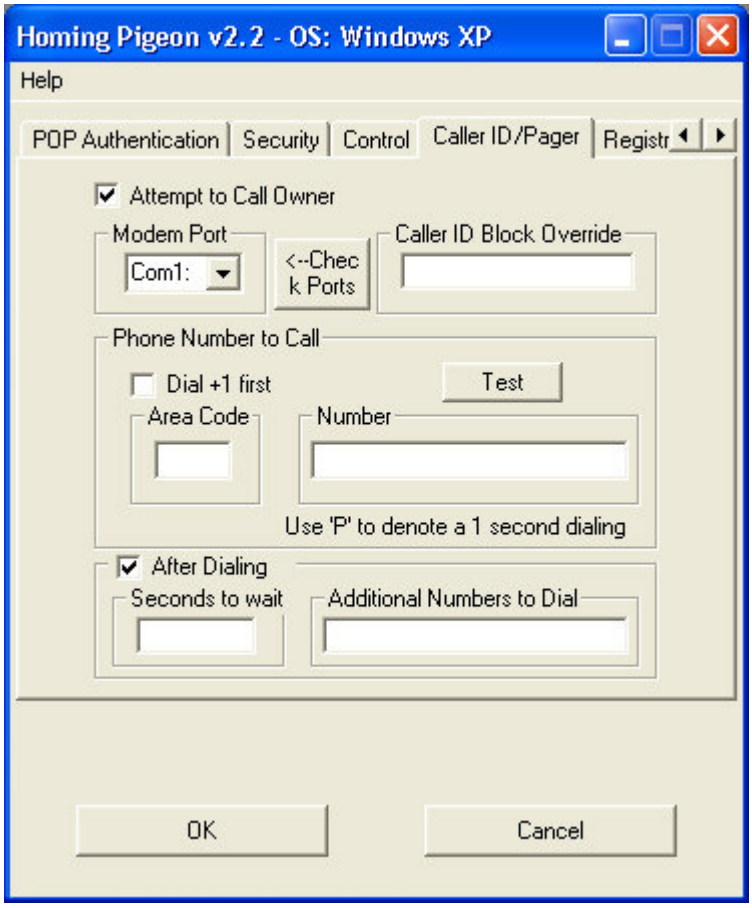
Caller/ID pager Tab



Under this tab, you can set up Homing Pigeon™ to attempt to use your modem, if you have one, to try and call a number of your choosing in order to trigger Caller ID or a Pager. Homing Pigeon™ will dial the number and let it ring for 25-30 seconds, long enough for Caller ID to register.[1] *NOTE: If you have Homing Pigeon™ running periodically, and the Caller ID/Pager option turned on, the Caller ID/Pager option will also then run periodically*

Attempt to call owner Checkbox

If this box is checked, and the rest of the items under this tab are filled out, then Homing Pigeon™ will, in addition to emailing you on boot or periodically, it will check the modem to see if an operating phone line is attached and if so, will attempt to call the number you've given it. It will also dial all of the additional info, so you can use this to call your pager and send you a message. The idea is to exploit Caller ID to provide additional information on your PC's location.

[1] We hate to have to point out the obvious, but the number you have Homing Pigeon™ call must have Caller ID service in order for you to capture the phone number Homing Pigeon™ is dialing from.

Modem Port Listbox

In this drop down list, a list of Com ports is displayed. On Windows 9x/Me systems, if you select a Com port and there is a modem on that port, the name of the modem will be displayed next to the "Attempt to Call Owner" checkbox. On Windows NT/2000/XP systems, a "← Check Ports" button will be display which if you click it, a list of modems and what Com port they are on will appear. On Windows 9x/Me systems, the "← Check Ports" will not be visible. In either case, make sure the List of Com ports is set to the Com port that your modem is using.

Check Ports Button (shows on NT/2000/XP only)

Not to sound redundant, but on Windows 9x/Me systems, if you select a Com port and there is a modem on that port, the name of the modem will be displayed next to the "Attempt to Call Owner" checkbox. On Windows NT/2000/XP systems, a "← Check Ports" button is shown which if you click it, a list of modems and what Com port they are on will appear. In either case, make sure the List of Com ports is set to the Com port that your modem is using.

Caller ID Block Override Textbox

Enter the dialing combination that the telephone company indicates will send out a caller ID signal even on phones whose default is to not be seen by caller ID. In most of the U.S. this is "*82" (that is, the * key followed by the 8 key followed by the 2 key). You can find this information in the front of your telephone book. The purpose of this is to try and make sure that if Homing Pigeon™ does successfully make the phone connection, that your Caller ID module or pager can grab the phone number Homing Pigeon™ is calling from.

Phone Number to Call Area

Dial +1 first Checkbox

In the US, since you should assume that you should have Homing Pigeon™ dial as if the call is long distance, you should have this checked. It then tells Homing Pigeon™ to follow the 1-area code-number format for dialing. If you live in a country that uses a dialing format that does not mimic the US format, then leave this unchecked.

Area Code Textbox

You should be sure to enter the area code. Don't assume the call will be local – long distance dialing works even if the call is across the street. What do you care if you drive the thief's long distance bill up? If you live in a country that uses a dialing format that does not mimic the US format, then leave this blank.

Number Textbox

Fill in the number you want Homing Pigeon™ to dial. In the Number box, you can put in extensions and pauses in the dialing as well. To put in a 1 second pause, type a P. If you know your modem is Hayes compatible, you can also use a comma (,) to create

a 1 second pause in the dialing.[1] For example, if you knew the number is 555-1212 but also knew that you had to wait at least 3 seconds before dialing a pager or voice mail extension at 123, you would fill in the Number box with 555-1212PPP123. If you live in a country that uses a dialing format that does not mimic the US format, then use this for the entire phone number including any required country and city codes.

Test Button

If the modem is connected to a phone line, you can have the Homing Pigeon™ configuration program test your dialing instructions by hitting the Test button. Remember, for the test to work, you need to dial out on a different line than the one you tell Homing Pigeon™ to dial. If Homing Pigeon™ detects the phone is already in use when it wants to make a call, it will skip making the call. If Homing Pigeon™ detects the phone it is trying to call is busy, it will simply hang up and skip the call.

After Dialing Checkbox

In the After Dialing area, you can set a delay, and then another dialing sequence. This is useful if a long delay is needed between dialing and further action such as accessing a pager and/or sending it a text message.

Seconds to wait textbox

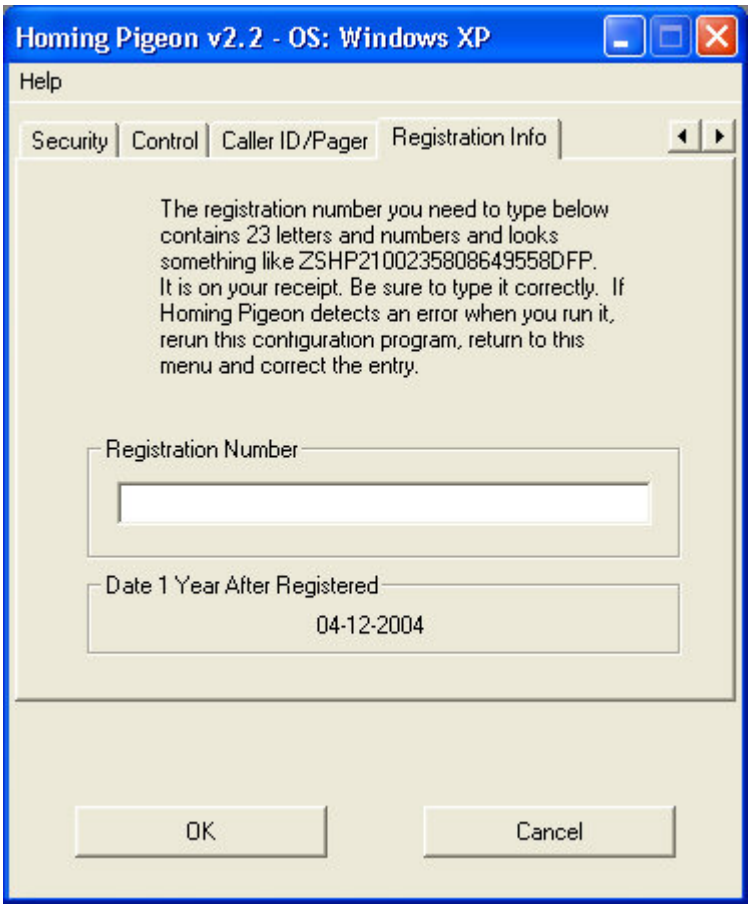
Set the delay in the Seconds to Wait box

Additional Numbers to Dial Textbox

Enter the additional numbers in the **Additional Numbers** to Dial box. To put in a 1 second pause in this number sequence, type a P. If you know your modem is Hayes compatible, you can also use a comma (,) to create a 1 second pause in the dialing.[2] If you pager does not support Text Messaging, you should consider having Homing Pigeon™ dial a noticeably unique number in order to identify itself to you.[3] If you are having Homing Pigeon™ call a number that you might answer or that might have an answering machine, you might consider having Homing Pigeon™ transmit a number series which plays a song in order to identify itself to you.

[1] We recommend that you use a "P" as that way Homing Pigeon is handling the pause, and so if you changed modems to one that does not understand the "," command, things should continue to work.
[2] We recommend that you use a "P" as that way Homing Pigeon is handling the pause, and so if you changed modems to one that does not understand the "," command, things should continue to work.
[3] For example, while "HomingPigeon" is "466464744366" and "StolenComputer" is "78653626678837", they are not all that recognizable. But something like "6666666666666666" is clearly not a real number and is recognizable.

Registration Info Tab



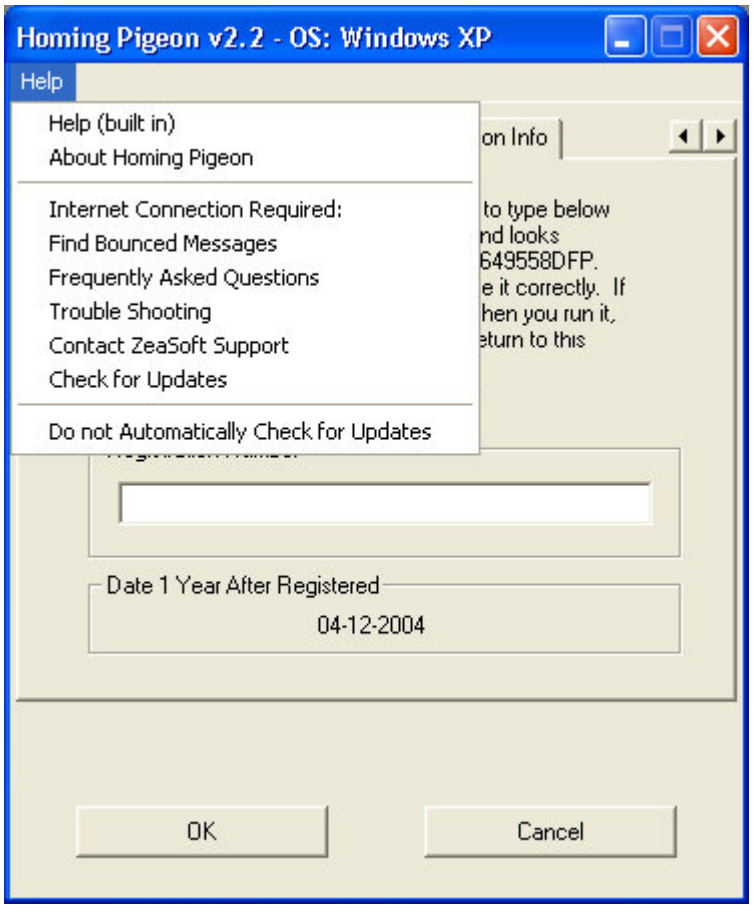
Registration Number Textbox

In this box you should enter the registration number that you were given when you purchased Homing Pigeon™. The software will not operate without a valid registration number. The registration number is case sensitive, so all letters which were sent to you capitalized must be entered capitalized.

Date 1 Year After Registration

This displays the date at which your ability to be sure of being provided with free updates expires. ZeaSoft reserves the right to extend free updates past this date, and the updater programs know whether to abide by this date or to ignore it. If you run an updater after this date and it functions, then it means we have waived this date for that updater. Waiving this may also be a specific function of your registration number. However, just because we have waived this date at some point, does not mean we will waive it at future dates.

Help Menu



Help (built in) Selection

This selection opens the help file for Homing Pigeon™. The help file is a condensed version of this manual.

About Homing Pigeon Selection

This selection displays the program name, version info, and intellectual property reminder. In addition, the Homing Pigeon™ configuration program's window title displays version information along with the Operating System Homing Pigeon™ believes the PC is running.

Items Requiring A Live Internet Connection

The following items all require an active internet connection. When selected, Homing Pigeon™ launches the default web browser on the PC and points the browser to the appropriate URL in order to display the selected information.

Find Bounced Messages Selection

This selection starts the web browser and points it to the ZeaSoft web page where we list messages that attempted to pass through our servers but generated errors. (http://www.zeasoft.com/hpgntrbl/bounced.htm) The list is updated several times a week, and a given source of errors is only listed once per week. Please note that URL's on our Web Site are case sensitive.

Frequently Asked Questions Selection

Starts the web browser and points it to the ZeaSoft Homing Pigeon™ Frequently Asked Questions (FAQ) page, http://www.zeasoft.com/FAQ/HPGNFAQ.htm. Please note that URL's on our Web Site are case sensitive.

Trouble Shooting Selection

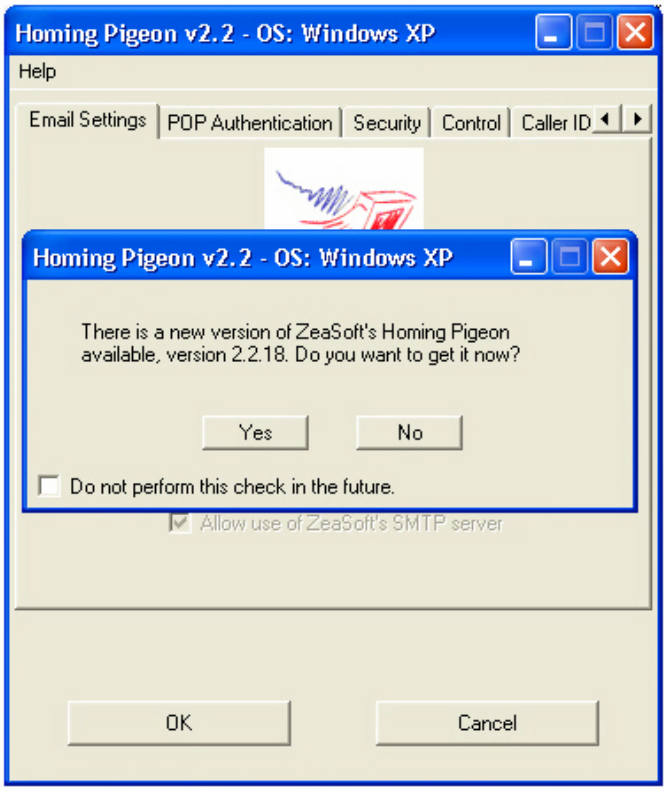
Starts the web browser and points it to the ZeaSoft Homing Pigeon™ trouble shooting main page. http://www.zeasoft.com/hpgntrbl/HPGNTROU.htm. Please note that URL's on our Web Site are case sensitive.

Contact ZeaSoft Support Selection

Starts the web browser and points it to the ZeaSoft Support Contact page, http://www.zeasoft.com/Contsup.htm. Please note that URL's on our Web Site are case sensitive.

Check For Updates Selection

Starts the web browser and points it to the ZeaSoft Homing Pigeon™ update page, http://www.zeasoft.com/Downloads/HomingPigeon.htm. Please note that URL's on



our Web Site are case sensitive.

Do not Automatically Check for Updates Selection

If this menu item is checked, then the Homing Pigeon™ configuration program will not automatically attempt to contact our server to check for a more recent version of Homing Pigeon™. This menu item can be checked and unchecked merely by selecting it. If the automatic update check is operating, and a different version of Homing Pigeon™ is designated on our web site as the "most recent", the user will be informed and asked if they want to be taken to the Homing Pigeon™ update page. An illustration of the pop-up window which tells the user about the newer version is illustrated above. ***This version check is done without sending any personal information to ZeaSoft***[1], and requires an active internet connection at the time the Homing Pigeon™ configuration program is started. If there is not an active internet connection at the time the Homing Pigeon™ configuration program is started, no check will be performed.

[1] The configuration program mimics a web browser to take a peek at the ZeaSoft web site. So the only information "sent" to the ZeaSoft web site is the minimalist information that a web browser has to tell a web site in order for web site's server to address the packets of web page data in order for them to transit cyber space and reach the viewers PC.

Interpreting the Homing Pigeon™ Email Message

Below is an illustration of a Homing Pigeon™ v2.2 email with the headers contracted, and displayed using courier font, as many email programs are set to for default display. We have color coded various sections in order to make it easier to discuss the information they contain. Please note that if this manual is printed on a black and white printer, depending on the specific printer, some of the colors may be converted to gray tones that render those colored sections unreadable.

```
DATE: 3 April 03 07:36:31 AM
FROM: Homing_Pigeon@zeasoft.com
TO: test@zeasoft.com
SUBJECT: Just surfaced somewhere in Cyberspace.
X-RCPT-TO test@zeasoft.com

Homing Pigeon has just run under Windows XP.
Windows Registered Owner: ZeaSoft, Inc.
Registration Number: ZSHP2100235808649558DFP
CPU Type Reported: GenuineIntel Intel(r) Celeron(tm) Processor
CPU Serial Number Reported Processor serial number not supported by
this CPU or disabled.
Original Manufacturer of this PC Dell Computer Corporation
Physical RAM found 392736 KB.

Windows recognizes the following drives:
Drive       Volume
Letter      Type                    Serial Number     Name
-------------------------------------------------------------------
A:\         Removable Disk Drive
C:\         Fixed Drive             167992319
D:\         Removable Disk Drive    8413196742        ZIP-10
E:\         CD Rom Drive
F:\         CD Rom Drive            -771524581        DN60AENU

Windows recognizes the following user accounts

Account Name: Administrator
User Name:
Description: Built-in account for administering the computer/domain
Level: Administrator
Login Capability: Enabled

Account Name: Clod
User Name: Clod Tester
Description:
Level: Administrator
Login Capability: Enabled

Account Name: Guest
User Name:
Description: Built-in account for guest access to the computer/domain
Level: Guest
Login Capability: Disabled
```

```
Network Card and Dial-UP Adapter (PPP) Serial Numbers (MAC hardware
Addresses):
PPP Adapter. (Ethernet Adapter) with MAC Address: AA-45-43-54-17-02
3Com HomeConnect 3C450 Adapter (Ethernet Adapter) with MAC Address: 00-
5D-D4-6E-A6-F1

Homing Pigeon has detected the primary IP Address to be "192.168.0.1"
and the local network name appears to be "portal".

To remote computers, this PC appears as portal.zeasoft.com
[24.218.190.7].

According to the internal clock, the PC thinks the time is 07:36:31 on
04-03-2003.

If you make sure your mailer shows expanded headers, you should be able
to trace the route this message took to get from your PC to your
mailer.

Homing Pigeon scanned for additional IP addresses. The total list found
assigned to this machine:
IP Address        DNS Name
192.168.0.1       portal.zeasoft.com

The following DHCP servers are actively providing Dynamic Host
Configuration Protocol Services to this PC:
24.218.190.212    dhcp.zeasoft.com

The following DNS servers are actively providing Domain Name Services
to this PC:
216.168.225.149   ns19.worldnic.com
216.168.225.150   ns20.worldnic.com
206.253.214.11    NS1.NIC.CC
206.253.214.12    NS2.NIC.CC

The PC appears to have someone logged into Windows as "clod".

Homing Pigeon can ascertain DialUp Networking (DUN) information
relevant to tracking the PC on the following DUNs:
DialUp Networking Account "Thief" logs in with user name: "badguy".
DialUp Networking Account "LW" logs in with user name: "#test".
DialUp Networking Account "BR" logs in with user name: "#brazilnut".
DialUp Networking Account "CS3 Connection" has no listed user name.
DialUp Networking Account "Compuserve Kansas" has no listed user name.
DialUp Networking Account "Netcom 56K" logs in with user name: "#bozo".
DialUp Networking Account "My Connection" logs in with user name:
"test".

There may be other DUNs present on the machine.

An internet WHOIS on zeasoft.com (from portal.zeasoft.com) shows the
domain belongs to the following:
Organization:
ZeaSoft, Inc. (ZEASOFT30-DOM)
P.O. Box 342
Arlington, MA 02476
US
```

```
Domain Name: ZEASOFT.COM

Administrative Contact:
ZeaSoft, Inc. (ZEASOFT30-DOM) webmaster@zeasoft.com
P.O. Box 342
Arlington, MA 02476
US
617-812-5900

Technical Contact:
master, host (HM7084) hostmaster@INTERLAND.NET
Interland, Inc
303 Peachtree Center Ave. Suite 500
Atlanta, GA 30303
US
404-586-9999 404-586-0001

Record expires on 18-Feb-2011.
Record created on 18-Nov-2001.
Database last updated on 3-Jun-2002 23:52:18 EDT.

This machine appears it might be on a private LAN. See the Homing
Pigeon™ web page for details.

Because it appears your PC is on a private LAN, Homing Pigeon tried to
determine the location where your LAN is connected to the Internet.
Homing Pigeon has performed a trace route between the PC and the
ZeaSoft Web Server at IP address 216.247.191.197. The first machine
with an IP address which DOES NOT begin with 10.x.x.x, 192.168.x.x,
169.254.x.x, or 172.16.x.x through 172.31.x.x is the first non-LAN
machine the LAN is connected to the internet through. The resulting
trace is:
Tracing Route to 216.247.191.197:
Hop         Delay(ms)   Route IP Address  Registered Name
Number
1           1           10.218.190.1      main-portal
2           9           10.63.34.1
3           14          172.25.33.5
4           13          12.123.40.138     gbr1-p60.cb1ma.ip.att.net
5           10          12.122.5.53       gbr3-p70.cb1ma.ip.att.net
6           16          12.122.2.13       gbr4-p10.n54ny.ip.att.net
7           14          12.122.1.121      gbr3-p60.n54ny.ip.att.net
8           23          12.122.3.54       gbr3-p10.wswdc.ip.att.net
9           31          12.122.1.130      gbr4-p60.wswdc.ip.att.net
10          52          12.122.2.161      gbr4-p10.attga.ip.att.net
11          36          12.122.5.49       gbr6-p70.attga.ip.att.net
12          35          12.123.21.77      gar2-p370.attga.ip.att.net
13          37          12.124.58.6
14          41          64.224.0.68
15          35          216.247.191.197   zeasoft.com

This mail was sent through the ZeaSoft server (mail.zeasoft.com) as
permitted by the user. DO NOT REPLY to this email, as the ZeaSoft
server will ignore it.
--------------------------------------------------
Message generated by Homing Pigeon(TM) v2.2
```

```
Copyright 1997-2003 by ZeaSoft, Inc.
http://www.ZeaSoft.com
```

In our discussions of the message shown above, we will color code the discussion paragraphs to match the message sections that they are talking about. Please note that if this manual is printed on a black and white printer, depending on the specific printer, some of the colors may be converted to gray tones that render those colored sections unreadable.

The first section of the Homing Pigeon™ message consists of conventional email headers. In the message displayed above, the headers are contracted as most email programs default their displays. If you expand the headers, you can trace the path through cyberspace the message took from the SMTP server that handled the outgoing message, all the way to the email server that holds your account. We will discuss expanded headers later.

Just after the headers, the email contains some identifying information on the PC, who made the PC, the drives on the PC, version of Windows running, and Homing Pigeon™ installation. This is primarily to help identify the PC and to see if any major configuration changes have been made or are being made.

After the identifying information, account information is listed. On Windows NT/2000/XP systems, the account userID's, names, descriptions and whether the account is enabled for logins is listed. On Windows 9x/Me systems, this will only be the account userID's. This information can often be informative especially if additional user's have been added after the PC has gone missing. Occasionally Windows will report incorrectly whether or not logins are enabled for an account.

After the account information, the network adapters are listed including their MAC addresses. MAC stands for "Media Access Control". The MAC address (also known as the adapter address, physical address, Ethernet address, hardware address) is a unique identifying code for the Network Interface Card (NIC) or Ethernet adapter, the piece of hardware that allows you to connect to a LAN (Local Area Network) or to a high-speed internet connection. It is unique and can often substitute for a CPU serial number in terms of identifying a PC. If the network interface is built into the laptop or PC, then it does positively identify the PC. If the network interface is a card or USB LAN adapter, it positively identifies that card or USB device only. MAC hardware addresses are 48 bits, expressed as 12 hexadecimal digits (0-9, plus A-F, capitalized). These 12 hex digits consist of the first/left 6 digits (which should match the vendor of the Ethernet interface within the station) and the last/right 6 digits which specify the interface serial number for that interface vendor. MAC addresses might be written unhyphenated (e.g. 123456789ABC), or with one hyphen (e.g. 123456-789ABC), but should be written hyphenated by octets (e.g. 12-34-56-78-9A-BC). We should point out that if the PC has a modem, then it will display a network interface called "PPP Adapter" which is a software construct to make the modem interface look like a NIC to Windows under Dial-Up Networking. In the case of the PPP Adapter, the MAC Address is also a software

construct and so cannot be counted on to be unique, although once a PPP Adapter is created on a PC usually when DUN was installed, it's MAC Address should not change.

Next in the message is the primary IP address of the PC as well as the name the PC thinks is assigned to it.

After the primary IP address, there is a listing of what remote computers, such as servers hosting web pages, believe the IP address to be and the DNS name belonging to that IP address, if it has one. The purpose of this is to spot if the PC is interfacing to the internet through a proxy of some kind. If so, then this entry will differ from any IP addresses listed in the total list of IP addresses assigned to the PC that will be discussed below. In any case, this entry is telling you the exact machine that is making the real connection to the internet. In general, this is the IP address to focus on first when attempting to recover the PC.

After the report on how remote machines view the PC, we list the time and date that the PC believes is the time and date that it generated the message. This can give you an indication of whether the PC has been moved to a different time zone.

After the time and date section, the message will list all of the IP addresses assigned to the PC. A PC can have multiple IP addresses depending on a number of factors. Getting a complete list can help determine not only its location on the internet, but whether it is also on a private LAN. The message also lists any DHCP servers[1] and DNS servers[2]. Identifying these can often tell us what ISP (or other organizations) is being used to connect to the internet.

After the list of IP addresses, DHCP servers and DNS servers, the name of the user logged in is listed. Often on Windows NT based systems (NT/2000/XP), this will be "SYSTEM" if the message is sent after booting but before anyone logs in.[3] This is provided as a legacy item, as it is redundant with the account information listed earlier in the message.

After the current user is listed, any DUN (Dial-Up Networking) accounts that Homing Pigeon™ can find are listed. These are the accounts for ISP's accessed over a modem. If there are no DUN accounts this entry will not be displayed. Windows

---

[1] DHCP stands for Dynamic Host Configuration Protocol. DHCP is a protocol for dynamically assigning IP addresses to networked computers. With DHCP, a computer can automatically be given a unique IP address each time it connects to a network--making IP address management an easier task for network administrators. When a computer logs on to the network, the DHCP server selects an IP address from a master list and assigns it to the system.

[2] DNS stands for Domain Name Service (or sometimes Domain Name System) When you send email or point a browser to an Internet domain such as zeasoft.com, the domain name system translates the names into IP addresses (a series of numbers looking something like this: 123.123.23.2). The term refers to two things: the conventions for naming hosts and the way the names are handled across the Internet.

[3] This will be true even though in the account listings there may be no user named "SYSTEM". Windows reserves this user ID for itself.

reporting of DUN information can be unreliable, and so we place the weasel words at the end of the listing that there may be DUN accounts not listed.

After any DUN information is displayed, Homing Pigeon™ attempts to identify an authoritative name server for the domain associated with either the PC itself in the Primary IP address section of the message or in the domain associated with how the PC is perceived remotely. If it is successful, it performs a WHOIS lookup.[1] This usually provides the contact information, including phone numbers, of the person or organization who owns the domain that the PC was a part of or connected to the internet through.

After any WHOIS might be attempted, Homing Pigeon™ will evaluate whether it thinks additional information might be gained about the PC's location (including where within a private network it may be) by performing a **Trace Route** between itself and the ZeaSoft web server. A **Trace Route** shows the path that packets of data take from the origination point to the destination server. By exploiting the TTL (Time to Live) function of a Ping or Echo operation, it also shows the time it takes for a packet to travel from router to router along the way. This also allows **Trace Route** to identify each server, router or computer the packet passes through starting with your PC and ending with the ZeaSoft web server at IP address 216.247.191.197. This is the exact same path that data packets would take if the PC were to view web pages on our server at http://www.zeasoft.com.

At this point, the message has enough information that with a little legwork Law Enforcement should be able to locate and recover your laptop. Different agencies have different criteria and legal restrictions on them, so that should be kept in mind. Additional information about reading the headers of the Homing Pigeon™ email can be found on our website at http://www.zeasoft.com/Interp/hpgninte.htm.

[1] An Internet directory service used to look up names of people on a remote server. Most commonly, you use whois to look up domain ownerships and contact addresses. Most domain registrars provide a Web-based whois service, such as this one, to show the details of the domain's owner and other contacts for administrative and technical matters. Some registrars shield the domain owner's contact information to cut down spam, in which case the registrar's contact information will appear rather than the true domain owner. However they will divulge the true owner's name to Law Enforcement (or aggressive lawyers).

Troubleshooting

We understand the frustration of purchasing a new piece of software, installing it, and having it not work. While Homing Pigeon™ is generally robust and trouble free, every PC is different and so occasionally things just don't seem to work right.

Symptom:	Action:
The Homing Pigeon™ message never arrives	1. Rerun hpgncong.exe and check your settings. The most common reason for no message arriving is that the email address is invalid or has been mistyped. 2. No valid internet connection is made within the first 15 minutes after boot. Check setting under Control Tab. Try testing by making an internet connection right after boot, and leave it connected for 20 minutes or so. 3. If you do not have the "Allow Use of ZeaSoft's SMTP Server" checkbox checked, it is possible Homing Pigeon™ is having trouble with your SMTP server. Try checking this box 4. If you have any anti-spam filters running on your PC, ISP or firewall, make sure they allow all email coming from "zeasoft.com" as well as from your own email address to come through. Some of the less sophisticated anti-spam filters block all messages encoded with in-line MIME. Also try turning off the encryption and MIME encoding settings under the Security Tab in hpgnconf.exe. 5. Check for bounced messages at http://www.zeasoft.com/hpgntrbl/bounced.htm

continued…

Symptom:	Action:

Message looks like:
 	
`Content-Type: multipart/mixed; boundary="====================_335889614==_"`
 	
`--====================_335889614==_`
`Content-Type: text/plain`
`Content-Transfer-Encoding: base64`
`Content-Disposition: inline`
 	
`SG9taW5nIFBpZ2VvbiBoYXMganVzdCBydW4gdW5kZXIgV2luZG93cyBYUC4NCldpbmRvd3MgUmVnaXN0ZXJlZCBPd25lcjogTWljaGFlbCBCdXJucw0KUmVnaXN0ZXJlZCBPcmdhbml6YXRpb246IFpl`
.
.
(lots more of the same looking letters and numbers)
.
.
`YnkgWmVhU29mdCwgSW5jLg0KaHR0cDovL3d3dy5aZWFTb2Z0LmNvbQ0KDQo=`
 	
`--====================_335889614==_--`
	1. Your email reader does not understand how to decode inline MIME. Download our program MIMEView.exe in order to convert the message into plain text. MIMEView.exe can be downloaded from http://www.zeasoft.com/hpgntrbl/hash.htm.
	1. Your email reader does not understand how to decode inline MIME. Turn off the encryption and MIME encoding settings under the Security Tab in hpgnconf.exe.

The ZeaSoft web site also has extensive online troubleshooting help for Homing Pigeon™ at http://www.zeasoft.com/hpgntrbl/HPGNTROU.htm, as well as answers to questions in your Frequently Asked Questions section at http://www.zeasoft.com/FAQ/HPGNFAQ.htm. Some more common issues and their fixes are listed below.

PC Security Software and Software Compatibility

"Obscurity is to security what camouflage is to armor. Just an illusion." - Michael J. Burns

PC Security

Our position on PC security is that your "security software priorities" should be:

1. If you are running Windows 3.x or Windows 95, you should upgrade to at least Windows 98 SE. You can do this very cheaply. EBay.com is one place to look for inexpensive but legal Windows upgrades. Be aware that "OEM" versions of Windows installation CDs usually require that you reformat the hard drive. If you are purchasing a new PC, get it with Windows XP Professional rather than with Windows XP Home. Windows XP Home lacks security for shared folders, printers or drives.[1]
2. You should run Windows Update every week and install *all* Critical Updates the Windows Updater recommends. If you are running Windows XP or Windows 2000 and are connected to a high bandwidth "always on" internet connection[2], we recommend that you set Windows to automatically download and install all Critical Updates.
3. Anti-Virus Software: As for added software, you should first invest in anti-virus software from a reputable company like Symantec, the makers of Norton Anti-virus. Keep it up to date, scan your entire PC periodically, and if it has any type of "Auto Protect" or "On-Access Scan", to turn it on so that it scans all files anytime they are accessed (for read or write). Our experience is that turning on any "automatic email scanning" features of an anti-virus software package is a waste of time if you are running a high-quality email client program like Eudora, in that if the anti-virus software is truly scanning all files on reading & writing, then all viruses will be caught anyway when your PC downloads the email. The only exception to this is if you use Outlook or Outlook Express as your email viewer as then it depends on how Outlook is configured.[3] In our opinion, the additional performance hit to the PC from the automatic email scanning is not worth it if running a high-quality email program such as Eudora.

[1] This means that if you are going to share files or printers, you are better off with Windows 9x/Me as those versions of Windows can be set to require passwords in order to access your shared folder, drive or printer over the network. With Windows XP Home, shared resources are open for anyone on the network - you don't have the option to demand passwords for access. With Windows XP Professional, be sure to turn off "Simple File Sharing" so the system will demand passwords for people on the network to access your shared folders, drives and printer.

[2] Cable modem home connections, DSL home connections, as well as corporate-government-university networks are high bandwidth "always on" internet connections.

[3] We do not recommend Microsoft Outlook or Microsoft Outlook Express for email. We recommend Eudora for email. Eudora is probably the oldest and most trusted email program for PC's and Mac's in existence. Eudora is vastly more robust against attacks by email viruses or email messages containing malicious scripts or html than Microsoft Outlook or Microsoft Outlook Express. And it's free. Eudora has fully functional free versions available at http://www.eudora.com Paid versions have the same functionality but do not display advertisements.

4. Firewalls: If you have an "always on" connection (cable modem, DSL, T1, etc.), you should make sure you have a firewall between yourself and the internet. If you are running Windows XP, you can simply turn on the firewall built into Windows XP even if your internet connection is a dial-up one and you are not connected for very long. Homing Pigeon™ is compatible with Windows XP's firewall. If you are connected to your "always on" connection through a Cable/DSL router, quality routers (e.g. Linksys BEFW11S4, Linksys BEFSR41 or equivalent) contain a built-in firewall that you should activate instead. If you have an "always on" connection and are not already behind a firewall such as the ones just mentioned, you should purchase firewall software from a reputable company like Symantec (makers of Norton Personal Firewall), Internet Security Systems (makers of BlackICE), or ZoneLabs (makers of ZoneAlarm). If you connect through a dial-up connection (and are not running Windows XP and hence have its built-in firewall), buying firewall software in our opinion is a waste of money.
5. Yes, we do suggest that Homing Pigeon™ is a good addition to any PC, especially laptops or any other PC's at risk of being stolen. Obviously laptops are especially at risk since they are small and easily concealed.
6. Ad removal software. A large number of "free download accelerators", "download helpers", "automatic form filling utilities", "file sharing utilities" and "streaming media" programs are often a facade for Ad Ware.[1] This is really a privacy issue rather than a security issue, as these organizations are tracking your web usage for marketing purposes. Sometimes, the vendors of these utilities bury in their End User License Agreements (EULA) the fact that they are doing this and/or modifying your system, knowing full well that the average user does not read the EULA. Other makers of this type of software are simply surreptitiously placing this type of software on your PC without even using the EULA fig leaf. Some Ad Ware will even replace key Windows system network files, thus making it even more likely your system will have problems, and making it harder to diagnose when it does. A large number of pop-up ads that you encounter, and many embedded ads in web pages, also place tracking cookies on your PC[2], and ads that appear inside programs themselves also track aspects of your computer usage.[3] Scanning your system periodically with ad removal software such as Ad-Aware (free from http://www.lavasoft.de/) will identify and remove this type of Ad Ware.

Passwords

There are a number of things users should know about passwords which keeping in mind can have a large effect on the security of your PC, on-line banking or online financial interactions.

[1] Gator (http://www.gator.com) is an example of this type of system.
[2] Doubleclick (http://www.doubleclick.com) is an example of this type of advertising.
[3] Cydoor (http://www.cydoor.com) is an example of this type of system.

1. Weak passwords are simple words that appear in dictionaries. A common cracking[1] technique is to simply take a spell checker dictionary and run through it. The exception is concatenating words together (e.g. "rentbugs"), which is actually as robust as the next level as long as the concatenation does not result in a word what would be in a dictionary because the concatenation is a real word (e.g. "another"= "an" + "other", all three will be in the dictionary.)

2. Alpha numeric passwords are the next best. They are better than words that appear in dictionaries or phone numbers (and dates). For a ***n*** character string the combinations go as 36^{n} if the system is case insensitive, 62^{n} if the system is case sensitive. An 8 character vowel substituted password for "fireplace" would be f1rpl4ce (vowel substitution makes things easy to remember, but is also predictable). This size alpha numeric has 36^8 unique combinations if the system is case insensitive, 62^8 unique combinations if the system is case sensitive. $36^8 = 2.82\text{x}10^{12}$ while $62^8 = 2.18\text{x}10^{14}$.

3. The same 8 characters, if QWERTY keyboard punctuation is allowed (e.g. "big-boy!", "dog-rat!") has 95^8 unique combinations if the system is case sensitive. (Only 69^8 if the system is case insensitive, which is still better that the best alpha numeric.) $69^8 = 5.13\text{x}10^{14}$ while $95^8 = 6.63 \text{ x } 10^{15}$.

4. Pass phrases are the best “passwords” of all. These “best passwords” are not words, but complete sentences with punctuation (a space counts as a non-alphanumeric). In other words, things like "Boy is this cheese great on tootsie rolls in the morning!!!!!" Generally, if the system will accept spaces, then the only thing stopping the use of a pass phrase is whether it has restrictions on "password length". For example, the pass phrase above has 95^{61} possibilities a cracker would have to cycle through assuming he even knew how long the phrase was. If he could try 1 billion combinations per second, it would take him over 10^{95} *billions of years* to try them all. $95^{61} = 4.38 \text{ x } 10^{120}$.

How often one should change ones passwords is actually a controversial topic. The reason is that when users change passwords frequently, they often write them down thus creating a larger security issue. This is especially true with systems where the administrators enforce periodic password changes and block the recycling of passwords. What very quickly happens is that users can't remember their passwords and start doing things like putting their passwords on post-it notes stuck on their monitors, or on scraps of paper in their desks.

Raw Sockets

There has been a lot of noise made in some circles about the manner in which Windows XP supports Raw Sockets. In the beta stages of Windows XP, some self-appointed “security experts” hyped this issue as a major security flaw. Raw Sockets allow a much higher degree of control over network connections, with one aspect being that a malicious program can “spoof” the machine’s IP address to send data packets that look like they are coming from somewhere else IF the driver supports Raw Sockets with UDP,

[1] “Cracking” is a subset of hacking that targets breaking passwords. Usually the term means breaking passwords by the brute force method of exploiting computer speed and power to sequence through all the combinations of characters that could possibly be in the password that one is trying to break.

IP or raw-IP protocols. A spoofed IP address can only be used to send packets. In order to receive packets, the machine's true IP address must be used. However if someone is trying to perform a Denial of Service (DOS) attack on another machine, they often want to use IP spoofing. The fact of the matter is that all versions of Windows from Windows 95 up support Raw Sockets. Windows 95 requires that it be using Winsock 2 rather than Winsock 1. On NT based systems, normally only users with Administrator Privileges[1] can open a Raw Socket connection, while on non-NT versions of Windows (Win 9x/Me) any user can open a Raw Socket connection.[2] To confuse things further, Windows NT4, 95, 98's support of Raw Sockets is limited to IGMP and ICMP protocols, thus preventing them from spoofing their IP addresses unless the Winsock 2 driver is modified.

The original claims were that Windows XP support of Raw Sockets was a new security issue. The problem was that this assertion, on face value, is simply wrong. The people making these claims didn't seem to know that if one wants to claim there is an issue here, it is not Raw Sockets *per se*, it is what protocols can be combined with a Raw Socket opening. The revisionist version of the Windows XP Raw Sockets issue, once Win 9x/Me's unrestricted IGMP/ICMP Raw Socket support and Windows 2000's IGMP/ICMP/UDP/IP Raw Socket support was pointed out by people who actually knew something about network programming, became that under Windows XP single user systems, the single user has Administrator Privileges. (Of course, the same had been true for Windows 2000 single user systems for years.) What was new is that under the Home Edition of Windows XP, the default is to give all users Administrator Privileges so that legacy software would continue to work. So most Windows XP machines have users who can "spoof" their IP addresses if they know how to program and learn a little bit about network programming in Windows. The other potential problem is that a virus running as that user could spoof the PC's IP address while running a Denial of Service (DOS) attack, or could make itself a System Service. The whole debate over Windows XP Raw Sockets ignores the fact that for years before XP, Windows 2000 machines have always allowed all users to open a Raw Socket capable of IP spoofing, and the world has not ended due to it.

We don't consider this a real security issue requiring a Windows XP user to modify their system in any way. If you have anti-virus software installed and are behind a firewall, it requires "cascading miracles" before your PC would be in a situation where a trojan would be able to exploit Raw Sockets. However, there are free utilities available on the web if you wish to disable most application's ability to open a Raw Socket. One such free utility, for Windows 2000 and Windows XP, is SocketLock.[3]

---

[1] Under Windows XP single user systems, the single user has Administrator Privileges. Under the Home Edition of Windows XP, the default is to give all users Administrator Privileges.

[2] You (or a virus) can disable the Raw Sockets security check on NT systems through the System Registry so that any user can open a Raw Socket.

[3] You can download SocketLock for free from http://grc.com/dos/sockettome1.htm We have not used this utility and so cannot vouch for it. We simply are telling you where you can get it.

To learn more about Raw Sockets, we recommend "Network Programming for Microsoft Windows (Microsoft Professional Series)" by Anthony Jones & Jim Ohlund.[1] If you buy the 1st edition, the Raw Sockets are Chapter 13, in the 2nd Raw Sockets are Chapter 11.

"IP Broadcasting"

We should point out that a number of software vendors have been exploiting the ignorance of PC users concerning this topic to advertise their "security" products, which are usually low-quality firewalls or worse, simple port connection monitors. Often they do so using pop up ads saying things like "Your PC is broadcasting its IP address. Using it, hackers can now attack your PC." If you fall for their bait and click on their ad, they try to impress the gullible by showing them their IP address, information about their web browser, and operating system. Such a display is easy to do, is a built-in capability of almost every web site thus requiring little computer knowledge to implement, and does not represent a security risk. We believe that exploiting the ignorance of the average PC user to try to scare them into buying a product is unethical. It is up to you whether you want to buy from a software company with such little regard for the truth as the ones using this type of misleading advertising. We'd suggest that such behavior calls into question whether any of their claims about their products, or their product's effectiveness, should be believed. If you want a quality personal firewall, see the section above.

TCP and IP were developed by a U.S. Department of Defense (DOD) research project to connect a number different networks designed by different vendors into a network of networks (the "Internet"). The combined implementation is TCP/IP. All machines on the network have unique addresses, called "IP Addresses". All packets on a TCP/IP network contain the IP Addresses of the sending and receiving machines. All Internet Protocol v4 (Ipv4) addresses are of the human readable[2] form X.X.X.X where X can range from 0-255.[3] In principle, there are 4,294,967,296 (4.2 billion or $256^4 = 2^{32}$) possible IP addresses on the internet. In reality, there are less than this number as some addresses are designated as reserved for private networks & network testing, and cannot be used on the public internet. If your PC is directly on the internet, you have one of these public IP addresses. If you are on a private LAN, then you do not.

Your PC does not ever broadcast its IP address. Broadcasting your IP address would be unsolicited transmission of your IP address out over the network. Does not happen. Period. If a remote machine seeks a connection to an IP address, and your PC has that address, then in most cases your PC sends back a "connection refused" reply since

---

[1] Available through the ZeaSoft web site at http://www.zeasoft.com/products/books.htm The book contains an entire Chapter devoted to Raw Sockets, including source code examples and System Registry information on disabling the Raw Sockets security check on NT systems.

[2] The computers internally store and communicate the Ipv4 address as an unsigned integer Double Word (32-bit, four-byte)

[3] Internet Protocol v6 (IPv6) by contrast, uses a 128-bit addressing scheme, which makes it possible to assign 2^{128} addresses or approximately 3.4×10^{38} addresses. Ipv6 is not widely used as of yet. Information on IPv6 as it will apply to Windows can be found at http://www.microsoft.com/ipv6

that is the Windows default.[1] The exception would be if you are running a server on your PC. If you have not installed any servers, then no one can even try to "hack" into your PC. (Windows printer and file sharing does count as a server in this context.)

Your PC does give its IP address specifically to any website server with which *it* connects to when viewing a web page, as *doing so is a requirement to view web pages, and no it is not a security risk*.[2] Your PC initiates the contact. Your PC while contacting a web server to view one of its web pages *has* to give that server your PC's IP address. That web server has to know your PC's IP address as that is the IP address it has to address the web page data packets for them to traverse cyberspace to you PC in order for the browser on your PC to display that web page to you.

In addition to the "secret" we mentioned above that your PC only sends its IP address to servers it initiates contact with, here is another little secret: If your PC is directly on the internet, "hackers" don't need your PC to tell them its IP address for them to find its IP address and test your PC for vulnerabilities.

If you want a quality firewall, see #4 in the PC Security section above.

Making it hard to impossible for someone to check on your web browsing

There are a number of programs on the market that purport to "wipe" your web browsing trail from your PC. This is so that if someone gains access to your PC, they can't determine what you've been looking at on the internet. If you are concerned about such "security", yet don't want to pay for such "protection", there are a number of things you can do on a PC to configure Internet Explorer to automatically wipe or even encrypt your web browsing "trail".

Set Internet Explorer to encrypt its cache

The Internet Explorer cache is where IE temporarily stores entire web pages that you are viewing including the photos they contain, so that if you return to that web page, it only has to check to see if that page has changed since the last time you viewed it, rather than download the entire page again. The default size of the IE cache can be hundreds of megabytes, and can contain entire web pages that you viewed days, weeks, months, even years before. This means that anyone, regardless of their Windows userID, who knows what they are doing on a Win 95, 98 or Me system can simply look in the cache to see what you've been doing on the web, and when. On a Windows 2000 or XP system, anyone with Administrator privileges (*all* XP Home users, or on a single user XP Pro system, anyone using the PC) can do the same thing.

---

[1] A quality firewall will not even send back a "connection refused" message. It will simply stay silent and ignore the connection request in order to hide the fact that there is even a computer assigned that IP Address. This is why we suggest that you follow item #4 above in the PC Security section.

[2] The exception to this is if you are on a private LAN and connected to the internet via a proxy. Then the proxy substitutes its IP address for the private LAN IP Address (and reverses the process for incoming packets). However, once you've made contact with a web site, the security issues generally are the same regardless of whether the contact is direct or through a proxy with the exception that depending on how the proxy is configured, it may have an extra layer of anti-virus software.

If you are running Windows 2000 or Windows XP, and the drive is NTFS formatted, files and folders can be transparently encrypted with an encryption tied to the user.[1] The file encryption process is based on a key public key and symmetric key encryption scheme. This means you can have Internet Explorer (IE) encrypt its cache. This means that even a System Administrator won't be able to see what is in the cache without going through some effort, which a user can make exceedingly difficult or even impossible.[2,3] And anyone simply reading sectors off the hard drive will see junk. The main point is that allowing Windows to encrypt the IE cache adds another layer of difficulty to someone trying to view your internet browsing habits. To encrypt Internet Explorer's cache for a given user, you must first be logged on as that user.

1. Pick a new location other than C:\WinNT or C:\Windows. If you are logged on as "*user*", it is best if you make it a subdirectory of C:\Documents and Settings\user
2. Create a new folder and label it "Temporary Internet Files"
3. Right-click on the folder → Properties →Advanced...
4. Check on "Encrypt contents to secure data"
5. When prompted, "Apply changes to this folder, subfolders and files"
6. Start Internet Explorer
7. Select Tools → Internet Options…
8. Under the "General" tab, in the "Temporary Internet files" box click the "Settings" button.
9. Click the "Move Folder" button.
10. In the location browse panel, locate and select the encrypted folder you made in step #2. Click "OK". Then click "OK" on the settings window.
11. The system will then tell you that the settings will take effect if you log out, and it will ask you if you want to log out now. Click on "Yes".
12. Once it logs you out, you can log back on. All Internet Explorer cached files, including cookies, are now stored in the encrypted folder.

Set Internet Explorer to delete its cache every time it exits

An additional thing one can do, on any version of Windows, is to tell Internet Explorer (IE) to delete all copies of web files from its cache every time it exits. When instructed to delete its cache when it exits, it will still retain cookie files in the cache. Someone scanning the drive at the sector level can still retrieve the files (unless they were encrypted), or whatever portions have not yet been reused by the system. If this is coupled on a Windows 2000 or XP system with the aforementioned encryption, it is essentially impossible to decrypt the file fragments.

---

[1] An good overview of NTFS encryption, including ways an Administrator may be able to "trick" it, written by Brian Posey is available at http://www.brienposey.com/kb/working_with_ntfs_encryption.asp

[2] If you are using a single-user machine where your account is the only account with Administrator privileges, then your encrypted cache is as secure as the level of encryption used. The Administrator "trick" mentioned in Posey's article cannot be implemented.

[3] On a Windows 2000 or Windows XP machine that was set up in a "single user" configuration, so that there is no Windows logon when the machine boots, then since anyone using the PC is, as far as the machine knows, the same user, then encrypting the cache won't give imbue any additional privacy.

1. Start Internet Explorer
2. Select Tools → Internet Options…
3. Under the "Advanced" tab, scroll all the way down.
4. Under the "Security" section, locate the "Empty Temporary Internet Files folder when browser is closed" checkbox, and check the box.
5. Hit the "OK" button.

Set Internet Explorer to not cache https (encrypted) web pages on your hard drive at all

This is one of those things that one cannot fathom why Microsoft does not implement as the default behavior for Internet Explorer (IE). Why would anyone viewing information over the web that is so sensitive they want it encrypted as it travereses cyberspace, such as credit card or other financial information, then want it written on their hard drive in plain view? One can set Internet Explorer, in *any* version of Windows, to simply always keep encrypted web pages in memory and *never* cache them on the hard drive at all.

1. Start Internet Explorer
2. Select Tools → Internet Options…
3. Under the "Advanced" tab, scroll all the way down.
4. Under the "Security" section, locate the "Do not save encrypted pages to disk" checkbox, and check the box.
5. Hit the "OK" button.

Lock down the My Computer zone in Internet Explorer

This is a security measure implemented by Microsoft in Windows XP Service Pack 2 (SP2), however for some reason they have not implemented it in other versions of Windows despite it being easy for them to do. Microsoft describes the procedure on their website at http://support.microsoft.com/default.aspx?scid=kb;en-us;833633

Other PC Security Measures

Identity theft is a growing problem all around the world. While not strictly a "PC Security Measure", we strongly suggest that everyone buy a paper shredder and before discarding anything financial in nature with your name and address on it (including "safe" junk mail like credit card applications), shred it! We also recommend buying a shredder that can shred credit cards, CD's and DVD's, and that you shred all of these items before discarding. In the United States, there are a number of governmental[1,2] and

[1] The U.S. Federal Trade Commission runs web site with useful Identity Theft info at http://www.consumer.gov/idtheft/

[2] The U.S. Department of Justice runs a web site with useful Identity Theft info at http://www.usdoj.gov/criminal/fraud/idtheft.html

NGOs[1,2,3] that distribute a great deal of information on how to protect yourself against Identity Theft.

Software Compatibility

Email Software

Homing Pigeon™ follows Internet Standards when composing and transmitting its message. As such, it is fully compatible with any email client program which either adheres to internet standards such as Eudora[4], something like Outlook when set from its default proprietary messaging system to following internet standards[5], or uses a system to automatically translate between its proprietary messaging system and internet email messages.[6]

Firewall Software

Homing Pigeon™ is fully compatible with firewalls including the firewall built into Windows XP, as well as BlackICE and ZoneAlarm which are both top-quality and very popular products. It should be compatible with other firewall products as well.

If you are connected to your "always on" connection through a Cable/DSL router, quality routers (e.g. Linksys BEFW11S4, Linksys BEFSR41 or equivalent) contain a built-in firewall that you should activate. If you have a firewall operating in your router, you don't need to install any firewall software on your PC (no need to activate the Windows XP firewall if you are running Windows XP).

If you are using a version of any firewall that also needs to know what TCP ports Homing Pigeon™ needs permanent permission to access, they are TCP/IP ports 7, 25, 43, 80, 110 and 465. These are all standard ports for the standard TCP functions of Ping (Echo), SMTP email, DNS lookups, web browsing, POP email and SMTP over SSL.

Some firewall software now comes with Application Protection (or some other similar sounding “feature”) whose function is to prevent any “unknown” programs or

---

[1] http://www.privacyrights.org/identity.htm
[2] http://www.idtheftcenter.org
[3] http://www.identitytheft.org/
[4] Eudora is probably the oldest and most trusted email program for PC’s and Mac’s in existence. Eudora is vastly more robust against attacks by email viruses or email messages containing malicious scripts or html than Microsoft Outlook or Microsoft Outlook Express. And it’s free. Eudora has fully functional free versions available at http://www.eudora.com Paid versions have the same functionality but do not display advertisements.
[5] Microsoft Outlook and Microsoft Outlook Express are an example of a email client program whose default is to use a proprietary messaging system (Microsoft Exchange Server) but which can also be set to follow and deal with email systems which adhere to Internet Standards. Due to the fact that Microsoft Outlook Express comes free with every Windows installation and gets reinstalled with every upgrade or Service Pack of Internet Explorer, Microsoft Outlook and Microsoft Outlook Express are the most popular email client programs both with users reading email and especially as target programs to attack by virus writers.
[6] An example of this would be AOL.

scripts from running on the PC. Usually when this type of feature is running, and a new program is installed, the Application Protection software will prevent the new software from running until the user gives it permission. If you install Homing Pigeon™ and you have this type of feature running, you will see a number of warnings and you will need to give permanent permission to all of the modules flagged by such warnings.

At ZeaSoft, we feel that the "Application Protection" feature of these personal firewalls is a waste of resources, and so we turn them off on our PC's which have personal firewalls which support this feature. Quite frankly, this feature arose in our opinion due to a combination of a marketing need to add "features" to increase firewall sales by up-reving coupled with the wish of some self-proclaimed "security expert's" to drive up hits to their web sites. The philosophy behind "Application Protection" is the premise that your anti-virus software failed and allowed a trojan or virus to infect your system, and so the "Application Protection" software will stop the virus/trojan from running because it is a program unknown to the "Application Protection" software. The "Application Protection" software is in fact very simple. The software sets what is called a System Hook to intercept all calls to Windows to start of any other software once the hook is set. The System Hook diverts the call to the "Application Protection" program. The "Application Protection" program looks at the file requested to be executed and performs a hash on it to create a signature for the file.[1] It compares this hash with the hash it created for the file when either the file was originally given permission to run by the user, or when the "Application Protection" was last told to scan the system and update its database. If the file is not in the database, then it alerts the user and asks for permission to let the file run. If it is in the database, then if even one byte is different the hashes won't match and it will alert the user that something is amiss. Because the earlier generations of this type of software were trivial to kill or fake out, later versions have gotten more sophisticated in resisting attack to halt their execution or surreptitious alteration of their databases.

We believe this type of software provides little if any additional security if one is running good anti-virus software, have it automatically update itself every day or two, and have its "Auto Protect" or "On-Access Scan" turned on[2]. The "Application Protection" features of commercial firewall software with this feature that we have examined can be surreptitiously halted once the user is tricked into giving a new program permission to run, their database altered to permanently assign run status to the new program, and the "application protection" even restarted. We don't do so during the installation of Homing Pigeon™ as we have a policy of not defeating other company's software products, so we tell the Homing Pigeon™ user to tell these programs to give

[1] A hash is a mathematical algorithm that produces a given value when applied to a given block of data. The result of a hash function can be used to ensure the integrity of a given block of data. For a hash function to be considered secure, it must be very difficult, given a known data block and a known result, to produce another data block that produces the same result. Most of these programs use a MD-5 or SHA based hash, most commonly a SHA1 hash like a lot of software download sites use to allow users to check that a file they downloaded was not tampered with as it traversed cyberspace.

[2] By "auto-protection" we mean the anti-virus software should be set to scan all files whenever they are accessed for reading and writing. In Norton Anti-Virus, this is literally done by turning on the "Auto Protect" feature.

Homing Pigeon™ permission.[1] But some viruses already do attack these programs, as well as attempt to cripple anti-virus software. So we feel the annoyance presented by "Application Protection" software outweighs any benefit since "the really bad guys" know how to defeat it and so all it does is hassle "the good guys".

Anti-Virus Software

Homing Pigeon™ is fully compatible with anti-virus software such as Norton Anti-virus. It should in general be compatible with all anti-virus software. Please note that if your anti-virus software contains a special email scanning feature that is poorly implemented, you may run into the same problems with Homing Pigeon™ when MIME encoding is active that poorly implemented Email or SMTP Content Filtering software can display. See the "Email or SMTP Content Filtering Software" section below.

Encryption Software

Homing Pigeon™ is fully compatible with hard drive encryption such as that found under Windows 2000 and XT, as well as higher quality encryption software and hard drive file wiping software such as Jetico's BestCrypt and BCWipe[2]. It should in general be compatible with all hard drive encryption software and hard drive file wiping software.

Remote Access Software

Homing Pigeon™ has been tested with Netopia's Timbuktu PC remote access software and was found to be fully compatible.[3] Timbuktu is a PC-to-PC remote access program which allows one to remotely control a PC over the internet, as well as upload and download files. We expect that Homing Pigeon™ would be fully compatible with other PC-to-PC remote access programs such as PC AnyWhere[4] & Laplink Everywhere[5]. Homing Pigeon™ has been tested with the PC-to-Web Server remote access program GotoMyPC and was found to be fully compatible.[6]

Remote file retrieval is one of those features which we are often asked to include in Homing Pigeon™. More often than not, the user of the stolen PC usually is not the thief and isn't aware that the PC is stolen. Basically, our legal council indicated that a user incurs a great deal of potential civil and criminal liability if they remotely access their stolen computer, especially if they remotely copy or delete files. While it is technically trivial to add remote file retrieval access to Homing Pigeon™, we don't want the potential liability so we don't include this capability. If you want to be able to remotely copy or delete files after your PC is stolen, we suggest you install one of the products above and learn to use it *before* your PC gets stolen. Once Homing Pigeon reports the IP address of the stolen machine, you can attempt to log into it with the remote access software.

---

[1] The point is that the hurdle here is legal/ethical rather than technical.
[2] http://www.jetico.com
[3] http://www.netopia.com
[4] http://www.pcanywhere.com
[5] http://www.laplink.com
[6] http://www.gotomypc.com

Anti-Spam Software

Anti-spam software is so unreliable and flaky that we can't guarantee what it will do when it sees a Homing Pigeon™ message if the software is left on its default settings. Even anti-spam software advertising itself using fancy sounding terms like "Heuristic and Bayesian Technology" is still flaky compared to other filters, such as anti-virus filters.[1,2] If you own anti-spam software or your ISP allows you to have your email run through their anti-spam filters, you should set the anti-spam software to accept messages from your own email address as well as from addresses originating from zeasoft.com. Depending on how Homing Pigeon™ sends its message, the "From:" field may contain your own email address or may contain "Homing_Pigeon@zeasoft.com", "Homing_Pigeon_Pro@zeasoft.com" or "Homing_Pigeon_Lite@zeasoft.com". However the later email address from ZeaSoft may change in future versions, and all email from us such as customer support email is from a "@zeasoft.com" address or "@mail.zeasoft.com" address, so it is best the accept all email from zeasoft.com.

Email or SMTP Content Filtering Software

Content filtering software, like anti-spam software, is so unreliable and flaky that we can't guarantee what it will do when it sees a Homing Pigeon™ message if the software is left on its default settings. We've already encountered users who have email content filtering software that will block all Homing Pigeon™ messages when MIME encoding is used (this includes when the Homing Pigeon™ message is encrypted). The Homing Pigeon™ message, when MIME encoded, adheres to internet standards by including as part of the MIME message body headers the "Content-Type: text/plain" header and the "Content-Disposition: inline", which tells the email client that the MIME encoding is encoded plain text and that it is to be displayed as a message not as a file attachment.[3] However, some email content filtering software is primitive and rather than decode the MIME before applying the content filter, they simply block all MIME encoded email. If you are running email or SMTP content filtering software and you have Homing Pigeon™ encrypt or MIME encode the message, and your Homing Pigeon™

---

[1] Bayesian Analysis is a method of combining the likelihood ratio with additional information to produce an overall estimate of the strength of a piece of evidence, named after the Reverent Bayes. Alteratively, a technique for optimizing the signal to noise decomposition such that a forecasting model is proportionate to the input data. Basically, collecting a lot of observations (in this case spam emails) and hoping you can notice that if an email contains a high proportion of certain words, it is likely spam, and so having the filter reject such email. As more spam makes it past the filter, but is flagged by the human as spam, the spam filter looks at the email and sees if updating its rules will result in blocking similar emails in the future. Very error prone compared to pure human judgement, but probably the best of the "computer" techniques for filtering spam.

[2] A heuristic is something "providing aid in the direction of the solution of a problem but otherwise unjustified or incapable of justification." Or, *Heuristic* :Having to do with a rule of thumb. We like the more down to earth definition as it pertains to spam filters of "a wild guess that if certain words appear in the email, it must be spam."

[3] "Content-Type: text/plain", which properly identifies the Homing Pigeon™ MIME encoded massages as simple text as per internet standard RFC1341, precludes any scripts being in the MIME encoded area. For example, if the message body was to be displayed as a web page, and hence could contain malicious scripts, the proper content type would be a web page format such as "Content-Type: text/html" or "Content-Type: text/xml".

message never arrived, try turning off encryption and MIME encoding.[1] If the Homing Pigeon™ messages start arriving, then this is the problem. We want to emphasize that if this is going on, the flaw is in the email or SMTP content filtering software not in Homing Pigeon™, which properly identifies its MIME encoded massages as simple benign (non-executable) text as per internet standard RFC1341.

Upgrading or reinstalling Windows

A PC with Homing Pigeon™ installed should have no problems if you decide to reinstall Windows over the existing installation. If you decide to upgrade Windows, Homing Pigeon™ should also have no problems. If you are upgrading from a non-NT based version of Windows (Win 95/98/Me) to a NT based version of Windows (Win NT/2000/XP), we would suggest that after the upgrade is performed that you reinstall Homing Pigeon™ over the existing installation, or re-run the latest Homing Pigeon™ updater. The reason is that while your existing Homing Pigeon™ will function just fine, by rerunning the installer or updater the Homing Pigeon™ installer will reoptimize the installation for the NT-based environment.

[1] Alternatively, try turning off the blocking of "Content-Type: text/plain" & "Content-Disposition: inline" MIME encoded messages in your Email/SMTP Content Filtering software, tell it to allow all email from zeasoft.com and from your own email address to pass unfiltered, or simply buy a higher quality Email/SMTP Content Filtering software package.

How Homing Pigeon™ works

In this section we will try to explain, in simple and vague terms, what Homing Pigeon™ does and how. We'll try to keep it to a simple descriptive to make it understandable to people who have no knowledge of PC operating systems or programming. We'll keep it vague simply because we don't want to give any helpful hints to anyone trying to break the program.

Basically, Homing Pigeon™ is composed of functional modules. Their functions can be broken down into three main functional areas: (1) timing, control and repair (2) internet interactions and (3) telephone interactions.[1] Copies of these modules exist redundantly on the PC.

Although the detailed mechanisms differ depending on the specific version of Windows that you are running, upon system boot, a redundant master module runs which, if "self repair" is active, examines the system to see if any modules are missing. If so, it attempts to replace them and rebuilds its RAM cache. It then examines the system to see if a Homing Pigeon™ message is supposed to be sent on boot. If so, it starts the module required for sending an email message and, if the Caller ID/Pager option was activated, the telephone module.[1] These modules then wait until their respective connection types become available. When a valid internet connection is created, then Homing Pigeon™ generates its message and transmits it. The exception is if the "Quit if unsuccessful within 15 minutes" option is active, in which case if no valid internet connection becomes available within 15 minutes of booting, then Homing Pigeon™ will quit until the next reboot, or if periodic rerunning is active, when the next run time comes up. When a working phone line is connected to the PC and the system has been idle for a while (so the chances of someone "watching" is lower), then Homing Pigeon™ will attempt to make the call using the parameters that you gave it.[2] When it makes the call, it does tell the modem to turn off its speaker.

If Homing Pigeon™ is not set to run periodically nor to attempt to survive a format, then at this point Homing Pigeon™ quits, to be restarted with the next booting of the system. If periodic running or format survival are active, then Homing Pigeon™ stays resident. If format survival is active, Homing Pigeon™ periodically examines the system to see if any modules are missing. If so, it attempts to replace them. If periodic running is active, Homing Pigeon™ checks periodically to see if it is time to send another message or make another call. If so, then it activates those modules.

---

[1] This is one of those functions which people ask for but which we consider to have a high risk of failure but big payoff if successful. The reason is that telephone systems are so non-standard around the world, and even within the United States, that a set of dialing parameters that work in one location often don't work in another. The plus side is that if you do snag a telephone number at the location of a stolen laptop, that is easier for Law Enforcement to track down as they have more experience tracing phone information and relating it to a geographical location.

[2] Windows 2000/XP only. On Windows 9x/Me, Homing Pigeon quietly tests the modem to see if it is already being used

What if my computer with Homing Pigeon™ on it is stolen?

Neither ZeaSoft nor you can simply "go and get your laptop" if it is stolen, and the Homing Pigeon™ messages told you directly where it is. Only the police can do that, and they will need to work with the ISP through which the stolen computer connected to the internet. First and foremost, report the theft to the police and to your insurance company (if the computer was covered) as quickly as possible. Let the police know that you have tracking software on the computer, so that they might be prepared to act quickly if or when the post-theft Homing Pigeon™ messages show up. Ask for a specific person in the department to contact if and when the post-theft Homing Pigeon™ messages show up. Second, make sure that your mailbox that you have Homing Pigeon™ send its messages to is not full. Third, you should let us know about the theft so that if we are contacted by the police for help with the Homing Pigeon™ messages, we can be prepared.

You should monitor the mailbox for any post-theft Homing Pigeon™ messages. When they come in, notify the appropriate police contact. If you forward the Homing Pigeon™ emails, be sure to first expand the headers on the email so that the person you forward them to has the maximum amount of information. If they need assistance understanding the emails and how to interpret them, have them contact us at theft-report@zeasoft.com

In addition, it is a good idea to register the computer in one of the on-line "stolen computer" registries. Links to some of them can be found in the ZeaSoft website at http://www.zeasoft.com/Links.htm.[1]

What if my computer without Homing Pigeon™ on it is stolen?

First and foremost, report the theft to the police and to your insurance company (if the computer was covered) as quickly as possible. Second, contact the manufacturer of the computer and let them know it was stolen. Depending on their record system, they may have the computer's serial number (or you may be able to supply that to them) and they may be able to alter their database entry for that serial number so that of the computer is ever serviced by them, it will get flagged as stolen and they can report it to law enforcement. [1,2]

In addition, it is a good idea to register the computer in one of the on-line "stolen computer" registries. Links to some of them can be found in the ZeaSoft website at http://www.zeasoft.com/Links.htm.[1]

[1] If you do this, and you get your computer back, remember to contact them to let them know to unmark the computer as "stolen".
[2] Not all computer makers will do this.

End User License Agreement (EULA)

END-USER SOFTWARE LICENSE AGREEMENT FOR ZEASOFT SOFTWARE

This ZeaSoft End-User Software License Agreement ("EUSLA") is a legal agreement between you, either an individual or a single entity, ("Licensee") and ZeaSoft, Inc. ("ZeaSoft") for the ZeaSoft software products ("PRODUCT"). By installing, copying, or otherwise using PRODUCT, the Licensee agrees to be bound by the terms of this EUSLA. If the Licensee does not agree to the terms of this EUSLA, do not install or use the PRODUCT; the Licensee may, however, return the PRODUCT to the place of purchase for a refund.

1. DEFINITIONS.
a. PRODUCT means all components of Homing Pigeon supplied by ZeaSoft including, but not limited to, the License Key, computer software, online electronic documentation, HTML files, help text, and PDF files, and may include associated media or printed materials.
b. LICENSE means the rights to use the PRODUCT on a single computer running one of the following operating systems, Windows 95, Windows 98, Windows Me, Windows 2000, Windows XP or Windows NT Workstation.
c. LICENSE KEY means a sequence of ASCII characters that uniquely identifies the Licensee and is entered into the PRODUCT to define and enable the PRODUCT's features for a period of time.
d. EFFECTIVE DATE means the date that the PRODUCT was delivered to the Licensee, where the delivery consists of a LICENSE KEY and WEB link (URL) from which the Licensee may download the PRODUCT.
e. TERM means the period of time ZeaSoft grants the LICENSE to the Licensee under the terms and conditions of this EUSLA and is defined by the Perpetual type LICENSE.
f. PERPETUAL LICENSE has an unlimited LICENSE TERM, unless the EUSLA has been terminated earlier.
g. MAINTENANCE means the Licensee's right to receive product and security updates, patches, product upgrades and technical support.
h. ANNUAL MAINTENANCE FEE means the fee paid by the Licensee to ZeaSoft for the right to receive one (1) year of MAINTENANCE.

2. RIGHTS AND LIMITATIONS.
a. Subject to the terms and condition of this EUSLA, ZeaSoft grants the Licensee a non-exclusive, non-assignable LICENSE to use the PRODUCT from the EFFECTIVE DATE and for the duration of the TERM.
b. The PRODUCT may only be installed on computers that are used solely for the Licensee's own personal or internal business. This EUSLA does not grant any rights to use or install the PRODUCT on computers used primarily to service or to benefit persons not having either an employment or contractual business relationship with the Licensee, such as a WEB server servicing the public.

c. Notwithstanding anything else contained in this EUSLA, ZeaSoft retains (i) all title to, and, except as expressly and unambiguously licensed herein, all rights to the PRODUCT, and all related documentation and materials, (ii) all of their service marks, trademarks, trade names or any other designations and (iii) all copyrights, patent rights, trade secret rights and other proprietary rights in the PRODUCT.
d. The initial purchase of a PERPETUAL LICENSE includes MAINTENANCE until the first (1st) year anniversary from the EFFECTIVE DATE. Thereafter, the Licensee must pay the then CURRENT ANNUAL MAINTENANCE FEE for continuation of PRODUCT MAINTENANCE.
e. The Licensee does not have any rights to use the PRODUCT on any operating system other than those explicitly sited in Section 1(b).

3. LICENSEE'S OBLIGATIONS.
Except as expressly and unambiguously provided herein and as conditions of the Licensee's LICENSE hereunder, the Licensee represents, warrants and agrees:
a. Not to reverse assemble, de-compile, or otherwise attempt to derive source code (or the underlying ideas, algorithms, structure or organization) from the PRODUCT or from any other information, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.
b. To keep all copies of the PRODUCT in the possession of the Licensee.
c. Not to sell, give, lend, give access to, or otherwise transfer the PRODUCT, or copies of the PRODUCT to anyone that is not an employee or consultant of the Licensee, or to anyone that is not bound to all of the terms and conditions of this EUSLA.
d. Not to use the PRODUCT for timesharing, outsourcing, hosting, or service bureau purposes or otherwise allow others, or third parties benefit from the use of the PRODUCT.
e. Not to remove from any copies of the PRODUCT any product identification, copyright or other notices.
f. Not to modify, incorporate into or with other software, or create a derivative work of any part of the PRODUCT.
g. Not to disseminate performance information or analysis (including, without limitation, benchmarks) from any source relating to the PRODUCT.

4. Termination.
a. Without prejudice to any other rights, ZeaSoft may immediately terminate the LICENSE if the Licensee fails to comply with all of the terms and conditions of this EUSLA. In such an event, the Licensee must destroy all copies of the PRODUCT and all of its component parts.
b. All of the terms and conditions of this EUSLA shall survive termination with the exception of the LICENSE as defined in Sections 1(b) and Sections 2(a) and 2(d). Termination is not an exclusive remedy and all other remedies will be available to Licensor whether or not the LICENSE is terminated.

5. GOVERNING LAW.
This EUSLA shall be deemed to have been made in, and shall be construed pursuant to the laws of the Commonwealth of Massachusetts and the United States, without regard to

conflicts of laws provisions thereof and without regard to the United Nations Convention on Contracts for the International Sale of Goods. The sole jurisdiction and venue for any dispute regarding the terms of this EUSLA or any action relating to the subject matter hereof shall be the Superior Court of Suffolk County, Massachusetts and the U.S. District Court for the District of Massachusetts. The prevailing party in any action to enforce this EUSLA shall be entitled to recover reasonable costs and expenses, including, without limitation, reasonable attorneys' fees.

6. Export Limitations.
The Licensee shall comply with all applicable export laws, restrictions, and regulations of any United States or foreign agency or authority. The Licensee agree not to export or re-export, or allow the export or re-export of any product, technology, or information the Licensee obtains or learns under this EUSLA (or any direct product thereof) from the country in which the Licensee has installed and is using the PRODUCT in violation of any such laws, restrictions, or regulations. The PRODUCT is a "commercial item," "commercial computer software," and/or "commercial computer software documentation" as defined under U.S. law in FAR section 2.101, DFAR section 252.227-7014(a)(1) and DFAR section 252.227-7014(a)(1), or otherwise. Consistent with DFAR section 227.7202 and FAR Section 12.212, any use, modification, reproduction, release, performance, display, disclosure or distribution of the PRODUCT by the U.S. government shall be governed solely by the terms of this EUSLA and shall be prohibited except to the extent expressly permitted in this EUSLA.

7. LIMITED WARRANTY AND DISCLAIMER.
ZEASOFT WARRANTS THAT FOR A PERIOD OF THIRTY (30) DAYS FOLLOWING THE EFFECTIVE DATE THE PRODUCT WILL MATERIALLY CONFORM TO ZEASOFT'S THEN CURRENT OPERATIONAL SPECIFICATIONS. THE FOREGOING WARRANTIES COVER ONLY PROBLEMS REPORTED TO ZEASOFT DURING THE WARRANTY PERIOD. ANY LIABILITY OF ZEASOFT WITH RESPECT TO THE SOFTWARE OR THE PERFORMANCE THEREOF OR DEFECTS THEREIN UNDER ANY WARRANTY, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY WILL BE LIMITED EXCLUSIVELY TO PRODUCT REPLACEMENT OR, IF ZEASOFT DETERMINES, IN ITS SOLE DISCRETION, THAT REPLACEMENT IS INADEQUATE AS A REMEDY OR IMPRACTICAL, TO REFUND OF THE LICENSE FEES PAID BY THE LICENSEE AND TERMINATION OF THE LICENSE. EXCEPT FOR THE FOREGOING, THE PRODUCT AND ZEASOFT PROPRIETARY MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FURTHER, ZEASOFT DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS THAT THE SOFTWARE WILL RESULT IN RECOVERY OF ANY HARDWARE ITEM. FURTHER, ZEASOFT DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS THAT THE SOFTWARE WILL BE FREE FROM BUGS, THAT ITS USE WILL BE UNINTERRUPTED, OR REGARDING THE USE, OR THE RESULTS OF THE USE, OF THE SOFTWARE OR OTHER ZEASOFT PROPRIETARY MATERIALS IN

TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. THE LICENSEE UNDERSTANDS THAT ZEASOFT IS NOT RESPONSIBLE, AND WILL HAVE NO LIABILITY, FOR HARDWARE, SOFTWARE, OR OTHER ITEMS OR ANY SERVICES PROVIDED BY ANY PERSON OTHER THAN ZEASOFT.

8. NO WARRANTIES.
To the maximum extent permitted by applicable law, ZeaSoft, its suppliers, distributors and resellers disclaim all other warranties, either express or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose, with regard to the PRODUCT.

9. NO LIABILITY FOR CONSEQUENTIAL DAMAGES.
To the maximum extent permitted by applicable law, in no event shall ZeaSoft or its suppliers, distributors and resellers be liable for any special, incidental, indirect, or consequential damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use the PRODUCT, even if ZeaSoft has been advised of the possibility of such damages. Because some states and jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to the Licensee.

10. CUSTOMER REMEDIES.
ZeaSoft's entire liability and the Licensee's exclusive remedy shall not exceed the LICENSE fees paid for the PRODUCT.

Some components are licensed from BigSpeedSoft. (http://www.bigspeedsoft.com) and from Catalyst Development Corporation (http://www.catalyst.com).

ZeaSoft, Inc. is incorporated in the Commonwealth of Massachusetts in the United States of America. ZeaSoft’s mailing address is:

ZeaSoft, Inc.
P.O. Box 342,
Arlington MA 02476-0004

Support

We strive to respond within 24 working hours. Please remember we can't respond without your email address and product registration number if applicable.
We appreciate how frustrating it is when you get a new program, install it, and it does not do what you expected. Even a "free" program that misbehaves is at a minimum a frustration, and maximum a very grave concern.

We hope you can also appreciate that when you contact us for support, that our goal is to make your experience with our products a rewarding one so that you'll recommend our products to your friends. Plus our goal is to assist you in achieving that as quickly as possible.

With that in mind, we would like to ask you to think about the problem you are experiencing before you contact us, so that you can supply us with the maximum amount of information right from the start. We'd also ask that you look through the troubleshooting guides to see if what you're experiencing seems similar to any of the problems listed there. (http://www.zeasoft.com/support.htm) Even if your problem is not exactly like one listed there, if you think it is *similar* to something listed there, that can help us figure out what is happening on your PC. Telling us something like "it crashes" is a start, but is unlikely to tell us enough to resolve your problem on the first try. But telling us something like "it crashes and the windows message says it is crashing in module kernel32.dll…" helps, and "it seems to do it 2 minutes after the program is run" helps even more. The point being that since we cannot sit down in front of your machine, examine things, check your system registry and poke around, we must rely on *you* to communicate what the program is doing, as well as communicate other information about the machine. As such, the completeness of your description, as well as the completeness of your answers if we come back with questions, is critical to us being able to solve your problem with the minimum of frustration for you.

If the problem is with a product like Homing Pigeon™ or Home Base, which support logging, if you turn on the logging and send us the log files (which is often the first thing we are going to ask you to do anyway), you can save time for us both.

You should then contact us on-line through our support web page, http://www.zeasoft.com/Contsup.htm. Please note that URL's are case sensitive, so the C in Contsup.htm needs to be capitalized. Technical support is available only through this online form. We do not offer telephone support.

If you find what you think are errors in this manual and the help files, find any sections unclear, or have suggestions, please feel free to contact us though our website's feedback form at http://www.zeasoft.com/feedback.htm.

<END OF MANUAL>