NTA Stealth

INTERNET LEAD ID SOFTWARE

By

New Technologies Armor, Inc. (NTI)
2075 Northeast Division Street
Gresham, Oregon 97030 USA
503-661-6912
http://www.forensics-intl.com

NTI is an Armor Holdings (NYSE:AH) Company

User's Guide

Identifies Prior Internet Activity on a Personal Computer

Table of Contents

Introduction

What is NTA Stealth™?

NTA Stealth™ is a patented lead identification software tool that identifies Internet activity (web sites, emails and graphic downloads) on a computer after-the- fact. NTA Stealth™ was developed to help probation and parole officers determine if offenders are complying with court-mandated requirements prohibiting the viewing of pornography, to assist law enforcement in finding evidence of child pornography and in finding clues regarding whom the perpetrator may be in kidnapping/abduction cases. NTA Stealth™ can also help businesses and governments determine inappropriate usage on workplace computers.

NTA Stealth™ can identify thousands of Internet pornographic web sites through its patented software technology. It answers the question, "Where has this computer been on the Internet?" It is all but impossible for a computer user to hide past Internet activities from NTA Stealth's™ patented logic. NTA Stealth™ is fast, powerful and extremely easy to use.

NTA Stealth™ processes an entire computer hard drive (at a physical level) from one or more floppy disks or from a USB device. NTA Stealth™ can also process individual files such as swap and page files. NTA Stealth™ will only run on computers with Microsoft Windows operating systems.

Since NTA Stealth™ runs in DOS, it does not write any data or make any modifications to the evidence hard drive when operated from another storage device, e.g. floppy disk, USB device or another hard disk drive in a computer forensics lab setting. NTA Stealth™ does not leave behind any trace of its processes or operation.

NTA Stealth™ is a lead identification tool only and **its findings are not conclusive.** NTA Stealth™ output is written in a dBase III Plus file format for review, evaluation and corroboration with **NTA Viewer™.** NTA Viewer™ will only run on computers with Microsoft Windows operating systems. NTA Stealth™ output can also be analyzed with standard spreadsheet and database applications.

NTA Viewer™ provides superior capabilities when compared to spreadsheet applications and generic database applications. With NTA Viewer™ you can, with the simple click of the mouse, view the suspected web site on the Internet in order to validate the NTA Stealth™ identified lead. NTA Viewer™ also provides an automatic statistical analysis of the findings based upon frequency of web sites and email addresses found.

Who Should Use NTA Stealth™*?*

NTA Stealth™ is not an evidence-gathering tool but generates leads for the purpose of gathering evidence. NTA Stealth™ identifies Internet pornographic sites accessed by the computer and the frequency of the web sites being accessed. It is ideal for use by probation and parole officers, law enforcement officials, businesses and governments. NTA Stealth™ also can identify email activity to assist law enforcement in kidnapping/abduction cases. Specific instances where NTA Stealth™ should be used are explained in the following examples.

Probation and Parole Officers

Probation and parole officers face the difficult task of monitoring the activities of convicted sex offenders to determine compliance with court-mandated requirements for avoiding pornography and contact with certain individuals. NTA Stealth™ reviews the offender's computer and identifies pornographic web sites being accessed and the frequency thereof even when the offenders believe they have deleted the information or reformatted their computers. NTA Stealth™ is currently in use with a number of probation and parole agencies and officers have reported that the tool has been successful in identifying a number of violations of offenders' parole requirements.

In addition to NTA Stealth™, NTI has developed a set of tools that can assist probation and parole officers in the performance of their duties. These additional tools include FNames Stealth™, FileList™, GFE Stealth™, and MSweepXP™.

FNames Stealth™ can be used to search the offender's hard drive for names of associates the court has prohibited the offender from contacting. **FileList™** identifies existing and deleted graphic and other files, as well as encrypted and compressed files, which could lead to further evidence of probation/parole violations. **GFE Stealth™** extracts prohibited graphic images residing on the offender's computer.

More information on FNames Stealth™, FileList™ and GFE Stealth™ can be found at

http://www.forensics-ntl.com/fnames.html

http://www.forensics-intl.com/filelist.html

http://www.forensics-intl.com/iextract.html

NTI's **MSweepXP™** should be used to overwrite the ambient (hidden) data areas of the offender's computer following his/her release from prison in order to have a benchmark from which reviews can be made. It should also be used to overwrite the computer's ambient data areas after a review when the officer does not find enough evidence to conclude that the offender has violated the conditions of his or her probation or parole. If, in the initial review or in a subsequent review, the officer determines that there may be enough evidence on the computer to violate the conditions of the offender's probation or parole, then the officer will have the assurance that ambient (hidden) data areas of the computer's hard drive did not contain any information prior to the offender's release from prison or from the previous review. Information on MSweepXP™ may be found at:

http://www.forensics-intl.com/ms.html

Law Enforcement

Numerous instances have occurred where women, teens, children or other individuals have been abducted or have been reported as missing persons. Time is of the essence in these investigations if these persons are to be found alive. NTA Stealth™ identifies email activity and the frequency thereof for possible clues of whom the missing person was communicating with.

Two other NTI software tools can assist law enforcement in providing leads as to whom the missing person has been communicating with prior to his/her disappearance. These tools are FNames Stealth™ and FileList™. **FNames Stealth™** used on the missing person's computer is a great way to find names of persons for whom the victim may have been corresponding with prior to the disappearance. Such FNames Stealth™ leads may help the police to focus on individuals that may have been involved with the missing person, and may even help save a life. **FileList™** provides a listing of files that were last used by the missing person including the dates the files were last accessed. Access to files identified by FileList™ may help to identify the perpetrator. More information on FNames Stealth™ and FileList™ can be found at:

http://www.forensics-ntl.com/fnames.html

http://www.forensics-intl.com/filelist.html

For child pornography cases, NTA Stealth™ can assist law enforcement agencies in gathering evidence of child pornography to convict sex offenders. NTA Stealth™ reviews the suspect's computer and identifies pornographic web sites being accessed and the frequency thereof even when the suspect believes he/she has deleted the information or reformatted the computer. NTA Stealth™ also identifies graphic file images on the computer with .gif and .jpg extensions.

Another NTI software tool that can be useful by law enforcement in a laboratory setting is GFE Stealth™. GFE Stealth™ identifies and extracts any graphic file images with the extensions of .jpg, .gif and .bmp that are stored on a computer's hard drive. Information about GFE Stealth™ can be found at:

http://www.forensics-intl.com/iextract.html.

Personal Use of Business/Government Computers

Desktop and notebook computers used in business and government should be used only for appropriate purposes. Too often employees surf the Internet for pornography and download offensive images, including child pornography, onto their computers. NTA Stealth™ can identify pornographic web sites accessed from the employee's computer as well as the number of times the web sites have been accessed. When processing an employee's computer used at work, it is essential that the business or government have a policy in place that indicates that the computers assigned to employees are the property of the business or government and the contents thereof are subject to appropriate review. Failure to have such a policy in place could violate the provisions of the Electronic Computer Privacy Act.

License Statement

NTA Stealth™, NTA Viewer™ and this User's Guide are the properties of New Technologies Armor, Inc. (NTI). The entire contents of this User's Guide are protected under Copyright © 1997-2005 by NTI and NTA Stealth™ processes are protected by U.S. Patent No. 5,279,010. Use of the software indicates your acceptance of this license statement, disclaimer of warranty, and choice of law contained herein.

NTA Stealth™ and NTA Viewer™ are owned by NTI. They are licensed for one year by specific individuals or by businesses and government entities under a site license. The name of the licensed user or entity is embedded in NTA Stealth™ and is displayed on the screen of the operating program. Use by others of NTA Stealth™ and NTA Viewer™ is not permitted under this license agreement. In the case of licensed entities, e.g., a county probation and parole division, a Fortune 500 corporation or a law enforcement agency, a site license may be involved and the name of the licensed entity will be displayed on the screen of the NTA Stealth™ operating program without the name of a specific individual.

At the end of the one-year license period, the NTA Stealth™ and NTA Viewer™ license can be extended at the option of the user. NTA Stealth™ and NTA Viewer™ are licensed in this fashion to keep the costs down and to allow a wider distribution of this technology to protect children in society.

Licensed users of NTA Stealth™ and NTA Viewer™ are allowed to make copies of the software for their sole use. Under the provisions of the license granted by NTI, the software can be used and operated on multiple computer systems by licensed individuals/entities. However, the software cannot be shared or provided to others for "evaluation", use or "testing". Such unauthorized distribution of the software is in violation of your license to use the software and could result in legal actions brought against you by NTI.

Any alteration of this User's Guide and/or the referenced software nullifies any licensing agreements between the user and NTI. Violation of this licensing agreement may also constitute a criminal and/or civil violation of United States and/or international copyright laws. Such violations will be pursued to the fullest extent of the law by NTI. **If your name (or the name of your agency/business in the case of site licenses) does not appear on the entry screen of NTA Stealth™, then you are not licensed to use this software for any purpose.** If you have questions about licensing, contact NTI before you put the programs to use.

Disclaimer of Warranty

NTI has made every effort to verify the accuracy of these programs. However, NTA Stealth™ and NTA Viewer™ are sold and distributed "as is," without any warranty of any kind. In no event shall NTI, Armor Holdings, Inc., the authors, and/or authorized dealers and distributors be liable or responsible for any problems that could arise because of defects in the programs or from the operation of the programs. **Test these programs thoroughly and read this User's Guide completely before you use the software!** As stated previously, NTA Stealth™ is a lead identification tool. Conclusions drawn from the NTA Stealth™ program output and from the analysis and viewing of such output using NTA Viewer™ are not those of NTI. Therefore, **NTI will not responsible for any decisions or actions that might be taken based upon the use of either of these software tools.**

Privacy Law Issues

When using NTA Stealth™ and NTA Viewer™, it is important that you have the legal right to review the data stored on the evidence computer. If the owner of the computer or stored computer data has an expectation of privacy, NTA Stealth™ should only be used under a court order or under the strict guidance of legal counsel. In no event shall NTI, Armor Holdings, Inc., the authors, and/or authorized dealers and distributors be liable or responsible for any problems that could arise from the improper or illegal use of this software. **Make sure that you have the legal right to review the contents of the subject computer system before you use this software!**

Choice of Law

This statement and the entire contents of this User's Guide shall be construed, interpreted, and governed by the laws of the state of Oregon and/or the courts of the United States of America, Judicial District of Oregon. By use of NTA Stealth™ and NTA Viewer™, the user of these programs agrees that any legal actions brought will be filed in those respective jurisdictions.

Upgrades and Notices

NTA Stealth™ and NTA Viewer™ upgrades will be provided free of charge during a period of one-year from the date of license. Upgrades are also provided free of charge with subsequent license renewals. Program logic updates for pornography web site identification will be updated periodically and will be made available for licensed users of NTA Stealth™ at NTI's Internet web site at http://www.forensics-intl.com/nta.html. If ground or air shipment of the upgraded software or logic updates is required, an additional charge will be involved.

Licensed users will also be provided periodically with information concerning the use of the software via email correspondence. For these reasons, it is important for NTI to have a valid email address (which accepts file attachments) on file for every licensed user of the NTA Stealth™ software. Be sure to advise NTI if your primary email address changes. It is also important that your email address accepts email attachments. Without it you will not receive notices of upgrades or the actual software upgrades when they become available. Be sure to allow email from **forensics-intl.com** through your spam filters and advise NTI if your primary email address changes.

What You Get with NTA Stealth™

Purchasers of NTA Stealth™ receive the following for running NTA Stealth™ on evidence computers that have floppy disk drives and for analyzing and viewing NTA Stealth™ output.

- **NTA Stealth™ Test Disk**

  Contains:

  - Files to boot the evidence computer from the NTA Stealth™ Test Disk
  - NTA Stealth™ program executable file, NTA.EXE
  - NTA Stealth™ program logic file, NTALOGIC.NTI
  - AUTOEXEC.BAT file, which automatically runs a specific NTA Stealth™ command on the evidence computer

- **NTA Stealth™ Support CD**

  Contains:

  - NTA Stealth™ Quick Start Instructions in PDF file format
  - NTA Stealth™ User's Guide in PDF file format
  - NTA Viewer™ software for analyzing and viewing NTA Stealth™ output
  - Folder containing 6 Custom NTA Stealth™ Images

- **Free upgrades for one year (An extra charge is involved if air or ground shipping is required)**

- **CopyQM floppy disk duplication software (optional). Information about this software can be found at:**

http://www.forensics-intl.com/copyqm.html

Accessories

Certain newer computers do not contain floppy drives and computers may have floppy drives that do not work. In these situations or in instances where you desire to utilize the greater storage capacities of running NTA Stealth™ from a USB device, then the following accessories can be purchased from NTI for an additional price:

- **NTA Stealth™ USB Boot CD that enables the evidence computer to recognize NTA Stealth™ USB Thumb Drive in DOS**
- **NTA Stealth™ USB Thumb Drive containing the following files:**
  - NTA Stealth™ program executable file NTA.EXE
  - NTA Stealth™ program logic file NTALOGIC.NTI
  - NTA.BAT file which automatically runs a specific NTA Stealth™ operation on the evidence computer

Special pricing is available for site license purchases involving 10 or more individual computer users. Contact NTI for pricing and details at 503-661-6912 or on the Internet at info@forensics-intl.com.

NTA Stealth™ Features

1. **Patented Internet Identification Processes** - NTA Stealth™ relies on patented processes to identify Internet web site addresses, email addresses and graphics stored on the evidence computer hard drive.
2. **Physical Hard Drive Access Capable** - NTA Stealth™ processes all or part of an evidence computer hard drive through physical access of the drive. Thus, Internet leads can be gleaned from almost any hard drive that can be accessed from an Intel-based personal computer system under DOS.
3. **No Modification of Computer Evidence or Data** - NTA Stealth™ does not modify or alter the evidence hard drive, provided that NTA Stealth™ is not run from that hard drive. It must be run from a floppy boot disk, a USB device, or another hard drive in order to not modify or alter the evidence hard drive.

4. **Pornography Web Site Aware** - NTA Stealth™ has been programmed with knowledge of thousands of child and pornography-based web sites. NTA Stealth™ is much more powerful than prior versions. When a known pornography-based Internet web site is encountered, the program will flag the item in the output file and it will also display a tally of pornography-based findings on the display screen of the operating program as "porn".

   NTA Stealth™ is also programmed to identify leads that are likely "possible porn" sites as well. These possible sites are flagged in the output file and a tally of possible pornography-based findings is displayed on the screen of the operating program as "possible porn".

   At your option, NTA Stealth™ can be set to identify *only* the pornography-based and suspected pornography-based web sites. This is done by inserting the **"/porn"** command line switch in the AUTOEXEC.BAT and/or the NTA.BAT files discussed elsewhere in this User's Guide.

5. **Suitable for Covert Uses** - Because NTA Stealth™ does not change anything on the hard drive and no trace is left behind of its operation, it is ideal for use in covert intelligence gathering activities.

6. **Floppy Disk Processing Capable** - NTA Stealth™ is a compact DOS-based program that occupies very little storage space. The program can easily be operated from the NTA Stealth™ Floppy Test Disk placed in a computer using Microsoft Windows operating systems. Enough space is left on the NTA Stealth™ Test Disk for a large sampling of NTA Stealth™ output and more output can be stored on additional floppy disks as they become full. The program will prompt you when to insert another floppy disk.

7. **USB Device Processing Capable** - NTA Stealth™ can be operated from a USB device on computers with Microsoft Window operating systems with or without floppy disk drives using the NTA Stealth™ Boot CD and the NTA Stealth™ USB Thumb Drive. The USB Boot CD and the NTA Stealth™ USB Thumb Drive contain the necessary program files to automatically run NTA Stealth™ from the USB Thumb Drive and are available for purchase from NTI**.**

8. **Automatic Batch Mode Operation -** The NTA Stealth™ Test Disk includes an AUTOEXEC.BAT file and the NTA Stealth™ USB Thumb Drive includes an NTA.BAT file. These files can automatically process an evidence computer using a desired NTA Stealth™ command once the evidence computer has been booted from either the NTA Stealth™ Test Disk or the NTA Stealth™ USB Thump Drive. The NTA Stealth™ Support CD also contains 6 Custom NTA Stealth™ Image Files that can automatically process NTA Stealth™ commands from a separate floppy disk.

9. **Internet Country Code Translation** - NTA Stealth™ has embedded knowledge of all of the Internet country codes. The program automatically translates the cryptic Internet country codes and records the full name of the country involved in the NTA Stealth™ output file.

10. **NTA Stealth™ Output Analysis and Viewing** - NTA Stealth™ output is save to a dBase III Plus file and **NTA Viewer™** is included free of charge with the purchase of NTA Stealth™ for analyzing and viewing NTA Stealth™ output. NTA Viewer™ is very easy-to-use. Instructions for using NTA Viewer™ are included in this User's Guide. The dBase III Plus file format is also compatible with most commercial database and spreadsheet applications.

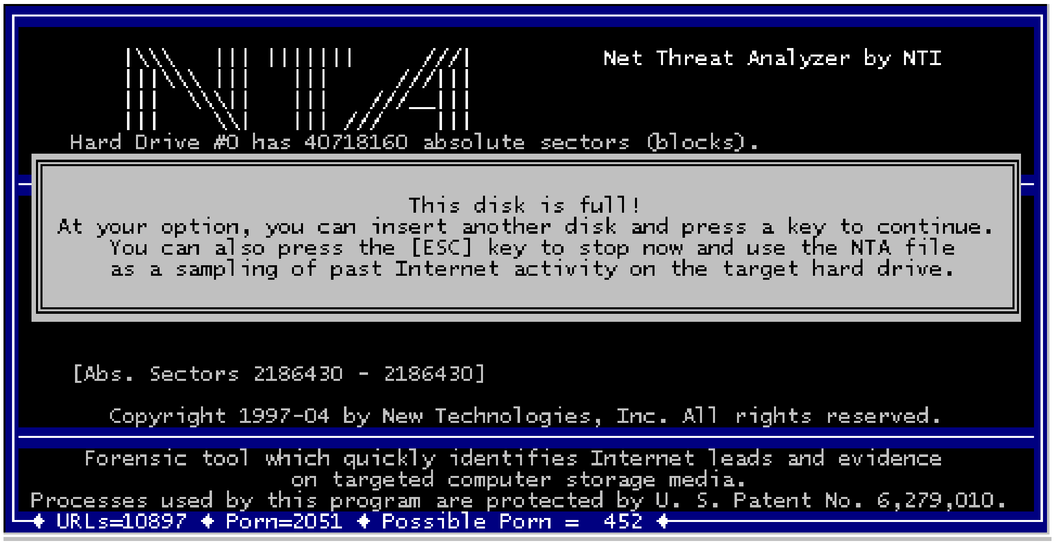
11. **Evidence Log File -** NTA Stealth™ automatically produces an evidence log when an output file is produced to document the date and time of processing the evidence computer, the number of leads generated, the hard drive examined, and other critical information to assist the user in preparing a case for presentation.

NTA Stealth™ Instructions

NTA Stealth™ can run on an evidence computer from a floppy boot disk or from a USB device. If an evidence computer has a workable floppy drive, we recommend you utilize the NTA Stealth™ Test Disk and the accompanying NTA Stealth™ Support CD containing the 6 Custom NTA Stealth™ Images. NTA Stealth™ will only work on computers with Microsoft Windows operating systems.

<u>NTA Stealth™ Test Disk</u>

The NTA Stealth™ Test Disk contains the files necessary for you to automatically run an NTA Stealth™ command from the floppy disk drive. NTA Stealth™ output is saved to the NTA Stealth™ Test Disk and, when the floppy is full, the program prompts you to insert another floppy disk to continue running NTA Stealth™ as depicted in the graphic below.



```
                                         Net Threat Analyzer by NTI
   Hard Drive #0 has 40718160 absolute sectors (blocks).

                         This disk is full!
   At your option, you can insert another disk and press a key to continue.
     You can also press the [ESC] key to stop now and use the NTA file
     as a sampling of past Internet activity on the target hard drive.

   [Abs. Sectors 2186430 - 2186430]

      Copyright 1997-04 by New Technologies, Inc. All rights reserved.

     Forensic tool which quickly identifies Internet leads and evidence
                     on targeted computer storage media.
  Processes used by this program are protected by U. S. Patent No. 6,279,010.
 ♦ URLs=10897 ♦ Porn=2051 ♦ Possible Porn =  452 ♦
```

NTA Stealth™ Support CD

The NTA Stealth™ Support CD contains, in addition to the Quick Start Instructions and this User's Guide, 6 Custom NTA Stealth™ Images that allow you to automatically run various NTA Stealth™ commands. Use of the 6 Custom NTA Stealth™ Image Files is discussed in a following subsection of these instructions. The NTA Stealth™ Support CD also contains NTA Viewer™ software that allows you to analyze NTA Stealth™ output leads generated. If your computer is connected to the Internet, you can use NTA Viewer™ to directly access the Internet web sites identified as leads by NTA Stealth™ through a simple click of your mouse in order to determine the validity of those leads.

USB Boot CD And NTA Stealth™ USB Thumb Drive

Many newer computers no longer contain floppy drives or the floppy drive on a computer may not work. In these situations, you will need to run NTA Stealth™ on an evidence computer with the following accessory products that can be purchased from NTI:

1) **USB Boot CD** (which allows the computer to recognize a USB device); and
2) **NTA Stealth™ USB Thumb Drive** (which includes the files necessary to automatically run NTA Stealth™ to process the computer and save the output to this same NTA Stealth™ USB Thumb Drive).

Please note that the files contained on the USB Boot CD are hidden and therefore you will be unable to view such files by looking at the CD from your Windows operating system.

Operating NTA Stealth™ from NTA Stealth™ Test Disk

Use the following instructions to run NTA Stealth™ from the NTA Stealth™ Test Disk.

1. The evidence computer should be turned off.

2. Insert the NTA Stealth™ Test Disk into the floppy disk drive of the evidence computer.

3. Turn on the evidence computer. The computer should begin booting from the floppy drive and automatically run the NTA Stealth™ command that you requested to be included in the AUTOEXEC.BAT file.

IMPORTANT!

Typically, most computer settings will cause a computer to boot from the floppy disk drive first before booting from the hard drive. Every computer is different and you only get one or two seconds to react if the hard disk is the default upon booting.

However, if you see that the machine is booting "normally" into a Windows operating system such as Windows98 or WindowsXP, then **IMMEDIATELY turn the power button off to shut down the computer!**

When this instance occurs, it means that the machine is configured to boot from the hard drive first and this will need to be changed in the machine's Basic Input/Output System (BIOS) settings. If you are not familiar with this procedure, please check and consult with an IT specialist before proceeding and processing this particular machine.

We recommend that the boot options be similar in the following order to:

1. Floppy
2. CD-ROM
3. Hard Drive

4. NTA Stealth™ will generate output files as explained under **"Analyzing And Viewing NTA Stealth™ Output Files"** in a following section of this User's Guide. You can analyze and view the output by inserting the NTA Stealth™ Support CD into the CD-ROM of your own computer (not the evidence computer) and loading NTA Viewer™. Follow the instructions contained in the "NTA Viewer™ Instructions"

section of this User's Guide for analyzing and viewing the various leads generated by NTA Stealth™.

5. You can use the various other NTA Stealth™ commands and options explained in later subsections of this User's Guide by following the instructions in the **"Changing AUTOEXEC.BAT AND THE NTA.BAT Files"** subsection of this User's Guide.

6. Regularly download the most recent NTALOGIC.NTI program logic file for NTI's web site at:

http://www.forensics-intl.com/tools.html

and save to the NTA Stealth™ Test Disk to ensure that you have the latest version of the NTA Stealth™ program logic (Please see the **"NTALOGIC.NTI"** subsection of this User's Guide for the need for regular downloads.). Follow the instructions in the subsection **"Downloading Updates Of NTALOGIC.NTI"** to download and save the file to your NTA Stealth™ Test Disk.

Using Custom NTA Stealth™ Images on a Separate Floppy Disk

The NTA Stealth™ Support CD contains 6 Custom NTA Stealth™ Images for automatically running specific NTA Stealth™ commands exclusively from a floppy disk. These custom boot images will not operate from the NTA Stealth™ USB Thumb Drive, only from a floppy disk. These images contain the files necessary to boot the evidence computer and run a specified AUTOEXEC.BAT file to start processing a particular NTA Stealth™ command/option on the first physical drive.

These custom boot images have been created in order to preserve floppy storage space for NTA Stealth™ output and for ease in running NTA Stealth™.

The following Custom NTA Stealth™ Images are included on the NTA Stealth™ Support CD:

- **Internet Porn Web Site Leads** - This image contains an AUTOEXEC.BAT file to automatically search for Internet web addresses related only to pornographic content on the first physical hard drive of a computer. The syntax is:

```
nta /h0 /auto1 /porn
```

- **Internet Porn (Web sites and Email) Leads** - The second image contains an AUTOEXEC.BAT file that automatically searches for Internet web addresses ***AND*** email leads specifically related to pornographic content stored on the first physical hard drive. The syntax for this image is:

```
nta /h0 /auto4 /porn
```

- **Internet Web Browsing Leads** - The image contains an AUTOEXEC.BAT file that will automatically search for Internet web addresses (or URLs) stored on the first physical hard drive of the computer. The syntax for this image is:

```
nta /h0 /auto1
```

- **Internet File Graphic File Downloads and Viewing Leads** - The fourth image contains an AUTOEXEC.BAT that will automatically search for Internet file downloads with the extensions of .gif and .jpg on the first physical hard drive. The syntax for this image is:

```
nta /h0 /auto3
```

- **Internet Email Address Leads**- The fifth image contains an AUTOEXEC.BAT file that will automatically search for email leads on the first physical hard drive of a computer. The syntax for this image is:

```
nta /h0 /auto2
```

- **All Internet Related Leads**- The last image contains an AUTOEXEC.BAT file that will automatically search for email leads ***AND*** Internet web addresses on the first physical hard drive. This command combines the /auto1 and /auto2 options. The syntax for this image is:

```
nta /h0 /auto4
```

Follow the instructions below to utilize the Custom NTA Stealth™ Images on a floppy diskette (These images will not work on a USB device.) using your computer, not the evidence computer. You should also use a separate floppy disk other than the NTA Stealth™ Test Disk.

1. Insert the NTA Stealth™ Support CD into your computer's CD-ROM drive.

2. Double click on the "My Computer" icon on your computer desktop (or select "Start" on your Task Bar located at the bottom left-hand side of your computer screen and then click on "My Computer")

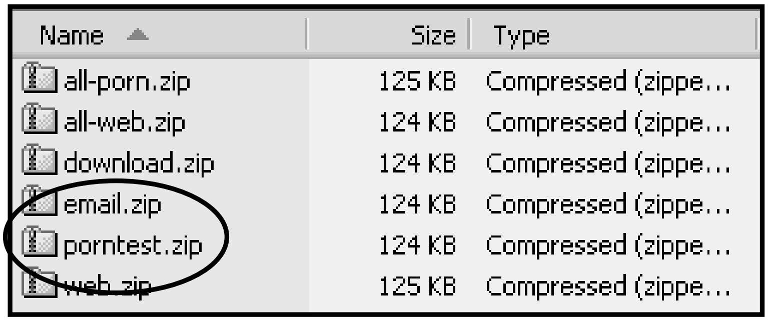
3. Double click on your CD-ROM drive icon in the "My Computer" window to view the files contained on the NTA Stealth™ Support CD.

4. From the NTA Stealth™ Floppy Test Disk, copy the NTA.EXE and the NTALOGIC.NTI program files to a location on the hard drive of your computer by right-clicking on the file and selecting "Copy".

5. Paste the NTA.EXE and the NTALOGIC.NTI files to a selected or created folder folder on your hard drive by clicking on "Paste" to protect these files and for easy access.

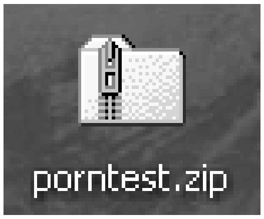
6. Copy the desired Custom NTA Stealth™ Image from the NTA Stealth™ Support CD to the desktop of your computer for easy access by following the aforementioned instructions, except that you should designate the location to copy the image as your desktop rather than a location on your hard drive.

Copy the NTA Stealth Image of your choice



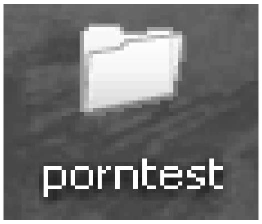
Name	Size	Type
all-porn.zip	125 KB	Compressed (zippe...
all-web.zip	124 KB	Compressed (zippe...
download.zip	124 KB	Compressed (zippe...
email.zip	124 KB	Compressed (zippe...
porntest.zip	124 KB	Compressed (zippe...
web.zip	125 KB	Compressed (zippe...

7. Once the Custom NTA Stealth™ Image is saved to your desktop, locate the Custom NTA Stealth™ Image icon as in the example of the "Porntest.zip" file icon below.



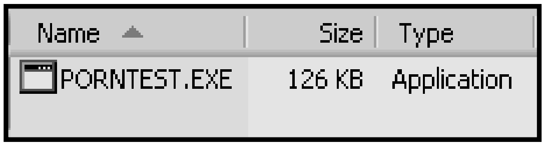
8. Unzip the file using the appropriate extraction software of your choice.

9. Unzipping the .zip file produces another folder as in the example below



Once you have unzipped this file, the original ***zip*** file is no longer needed. Since you have copies of this image file on NTI's Support CD, you may delete the previous ***zip*** file in instruction no.7 above.

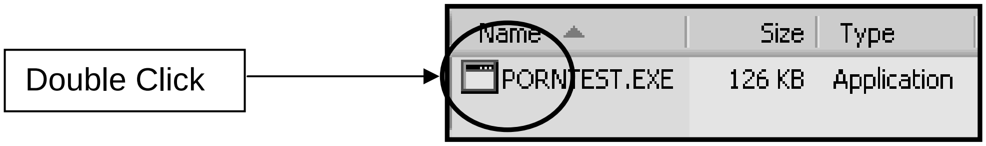
10. Double click on the "porntest" folder. The **porntest.exe** will be displayed. This application will be used to image a blank floppy disk with the files necessary to boot the computer and to run a specified NTA Stealth™ command.



Name	Size	Type
PORNTEST.EXE	126 KB	Application

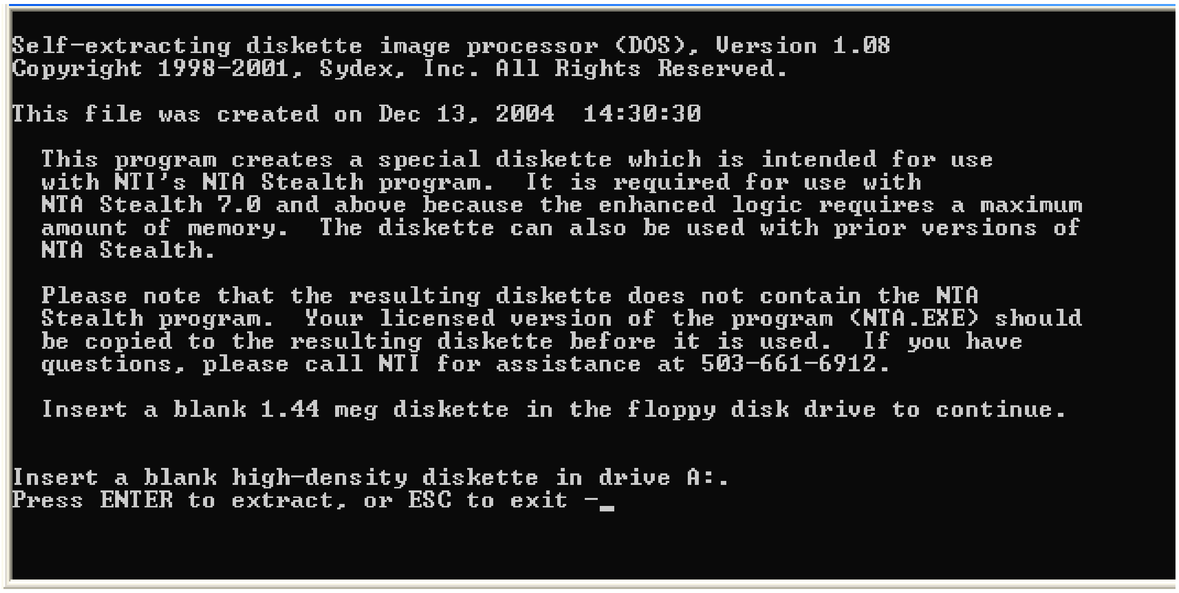
11. Set aside the NTA Stealth™ Test Disk and insert a **blank** floppy disk into the floppy drive of your computer.

12. Double click on the "porntest.exe" file.



Name	Size	Type
PORNTEST.EXE	126 KB	Application

A screen will be displayed explaining what is going to be formatted on the floppy disk. Using the previous custom image as an example, the AUTOEXEC.BAT file has been configured to identify pornography-based Internet web address (URL) leads.

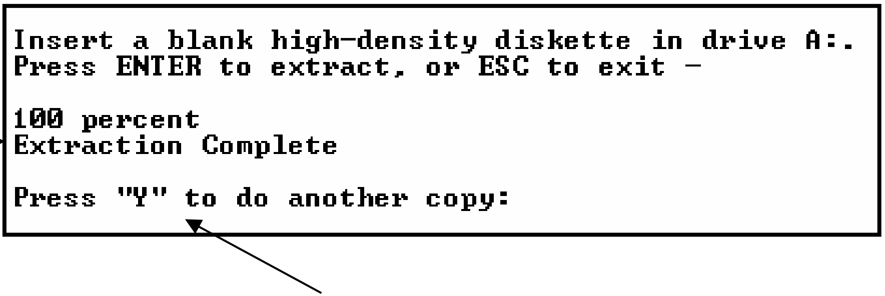


```
Self-extracting diskette image processor (DOS), Version 1.08
Copyright 1998-2001, Sydex, Inc. All Rights Reserved.

This file was created on Dec 13, 2004  14:30:30

  This program creates a special diskette which is intended for use
  with NTI's NTA Stealth program.  It is required for use with
  NTA Stealth 7.0 and above because the enhanced logic requires a maximum
  amount of memory.  The diskette can also be used with prior versions of
  NTA Stealth.

  Please note that the resulting diskette does not contain the NTA
  Stealth program.  Your licensed version of the program (NTA.EXE) should
  be copied to the resulting diskette before it is used.  If you have
  questions, please call NTI for assistance at 503-661-6912.

  Insert a blank 1.44 meg diskette in the floppy disk drive to continue.


Insert a blank high-density diskette in drive A:.
Press ENTER to extract, or ESC to exit -_
```

13. Press **ENTER** to start the process.

14. As the floppy disk is being formatted, a percentage of completion will be displayed. When it is 100% complete, the program will prompt you to continue or exit.

Completed!

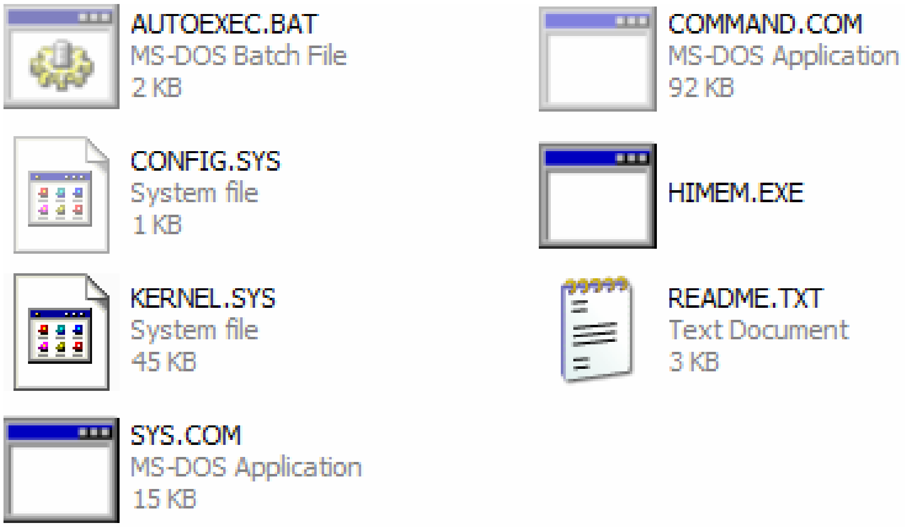


```
Insert a blank high-density diskette in drive A:.
Press ENTER to extract, or ESC to exit -

100 percent
Extraction Complete

Press "Y" to do another copy:
```

Press **"Y"** to format another floppy or any other key to exit

If you wish to format several floppies with this particular command line, then press the **"Y"** key. If you wish to exit, press any key on the keyboard to exit the program.

15. Double click on your floppy drive to view the contents of the disk. You should see the following seven files.



AUTOEXEC.BAT
MS-DOS Batch File
2 KB

COMMAND.COM
MS-DOS Application
92 KB

CONFIG.SYS
System file
1 KB

HIMEM.EXE

KERNEL.SYS
System file
45 KB

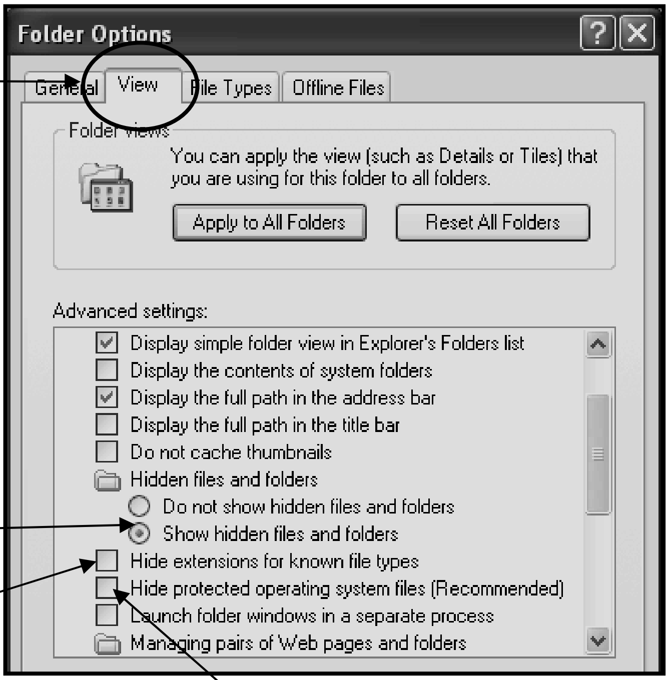
README.TXT
Text Document
3 KB

SYS.COM
MS-DOS Application
15 KB

Note: The "README.TXT" file contains instructions on the use of the NTA Stealth™ custom image. Please double click on this file and read the contents of the file before proceeding further. Afterwards if you wish, you may copy the README.TXT file to another location to save on disk space.

16. If you do not see all seven files, then your system is set to hide certain files and folders and you will need to change your folder settings. Typically you do this by clicking on **Tools/Folder** options in the Toolbar section at the top of the screen and then click on the **"View"** tab. Scroll down and:

    a. **Check** "Show hidden files and folders"
    b. **Uncheck** "Hide extension for known types"
    c. **Uncheck** "Hide protected operating system files



Folder Options

General | View | File Types | Offline Files

Folder views

You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Advanced settings:

- ☑ Display simple folder view in Explorer's Folders list
- □ Display the contents of system folders
- ☑ Display the full path in the address bar
- □ Display the full path in the title bar
- □ Do not cache thumbnails
- Hidden files and folders
  - ○ Do not show hidden files and folders
  - ● Show hidden files and folders
- □ Hide extensions for known file types
- □ Hide protected operating system files (Recommended)
- □ Launch folder windows in a separate process
- Managing pairs of Web pages and folders

View Tab

a. ***Check*** "Show hidden files …"

b. ***Uncheck*** "Hide extensions …"

c. ***Uncheck*** "Hide protected …"

17. Click **"Apply"** and then click "**OK".**

18. Copy your licensed NTA Stealth™ program executable **NTA.EXE** from the hard drive of your computer onto the floppy disk.

19. Copy the **NTALOGIC.NTI** program logic file from the hard drive of your computer onto the floppy disk or regularly download the most recent NTALOGIC.NTI program logic file for NTI's web site at:

http://www.forensics-intl.com/tools.html

and save to the floppy disk to ensure that you have the latest version of the NTA Stealth™ program logic (Please see the "NTALOGIC.NTI" subsection of this User's Guide for the need for regular downloads). Follow the instructions in the subsection "Downloading Updates Of NTALOGIC.NTI" to download and save this file to the floppy disk.

20. The above image example, which is the first selection of the 6 Custom NTA Stealth™ Images on the NTA Stealth™ Support CD, along with the NTA.EXE and NTALOGIC.NTI files, will cause NTA Stealth™ to start searching the first physical hard drive for all URLs or Internet web addresses for known and possible pornography-related web sites only.

21. Follow the instructions in the previous section of "**Operating NTA Stealth™ From The NTA Stealth™ Test Disk"** to process the evidence computer.

22. Follow the instructions in the subsection below entitled "Changing the AUTOEXEC.BAT FILE on the NTA Stealth™ Floppy Test Disk" if you desire to modify the NTA Stealth™ command on these images.

23. NTA Stealth™ will generate output files as explained under **"Analyzing And Viewing NTA Stealth™ Output Files"** in a following section of this User's Guide. You can analyze and view the output by inserting the NTA Stealth™ Support CD into the CD-ROM of your own computer (not the evidence computer) and loading NTA Viewer™. Follow the instructions contained in the "NTA Viewer™ Instructions" section of this User's Guide for analyzing and viewing the various leads generated by NTA Stealth™.

Running NTA Stealth™ from NTA Stealth™ USB Thumb Drive

DOS does not generally recognize USB devices. Therefore, in order to operate NTA Stealth™ from DOS using the NTA Stealth™ USB Thumb Drive, the **USB Boot CD *must* be used in conjunction with the NTA Stealth™ USB Thumb Drive.**

Use the following instructions to run NTA Stealth™ from the NTA Stealth™ USB Thumb Drive.

1. The evidence computer should be off.

2. Insert the NTA Stealth™ USB Thumb Drive into a USB port of the evidence computer.

3. Push the **ON** button to turn on the machine then **promptly** push the DVD-RW or CD-R drive tray button to open the drive tray and place the USB Boot CD in the tray.

   The CD drive tray will not open for the US Boot CD to be installed unless the computer is powered on. Therefore, it requires a quick push of the machine's power button, a quick push of the CD insert button and then another quick push of the CD insert button after the drive tray opens to push the drive tray back into the computer in time for the machine to boot from the US Boot CD.

IMPORTANT!

Every computer is different and you only get one or two seconds to react if the hard disk is the default upon booting. Fortunately most computers are configured to boot first from the floppy drive, second from the DVD-RW or CD-R drive and then the hard drive.

However, if you see that the machine is booting "normally" into a Windows operating system such as Windows98 or WindowsXP, then **IMMEDIATELY push the power button to shut down the computer!**

When this instance occurs, it means that the machine is configured to boot from the hard drive first and will need to be changed in the computer's Basic Input/Output System (BIOS) settings. If you are not familiar with this procedure, please check and consult with an IT specialist before proceeding and processing this particular machine.

4. After the NTA Stealth™ USB Thumb Drive and the USB Boot CD have been inserted in the machine and, assuming the system settings are configured as previously outlined, the computer should:

    - begin booting from the DVD-RW or CD-R drive
    - scan for the USB Thumb Drive and assign a drive letter to that device
    - automatically run the NTA Stealth™ command that you requested to be included in the NTA.BAT file on the USB Thumb Drive.

5. Regularly download the most recent **NTALOGIC.NTI** program logic file for NTI's web site at:

    http://www.forensics-intl.com/tools.html

    and save to the NTA Stealth™ USB Thumb Drive to ensure that you have the latest version of the NTA Stealth™ program logic (Please see the "NTALOGIC.NTI" subsection of this User's Guide for the need for regular downloads). Follow the instructions in the subsection "Downloading Updates Of NTALOGIC.NTI" to download and save the file to the NTA Stealth™ USB Thumb Drive.

6. NTA Stealth™ will generate output files as explained under **"Analyzing And Viewing NTA Stealth™ Output Files"** in a following section of this User's Guide. You can analyze and view the output by inserting the NTA Stealth™ Support CD into the CD-ROM of your own computer (not the evidence computer) and loading NTA Viewer™. Follow the instructions contained in the "NTA Viewer™ Instructions" section of this User's Guide for analyzing and viewing the various leads generated by NTA Stealth™.

NTA Stealth™ Files

The following files are included with your purchase of NTA Stealth™:

1. NTA.EXE (included on NTA Stealth™ Test Disk and NTA Stealth™ USB Thumb Drive)
2. NTALOGIC.NTI (included on NTA Stealth™ Test Disk and NTA Stealth™ USB Thumb Drive)
3. AUTOEXEC.BAT (included on NTA Stealth™ Floppy Test Disk)
4. NTA.BAT (included on NTA Stealth™ USB Thumb Drive)
5. 6 Custom NTA Stealth™ Images (included on NTA Stealth™ Support CD)

NTA.EXE File

NTA.EXE contains the various commands and options that allow NTA Stealth™ to perform its various functions. Detailed explanations of various command lines and options for running NTA Stealth™ are included in the subsections that follow.

NTALOGIC.NTI File

NTALOGIC.NTI is the program logic file that enables NTA Stealth™ to identify various pornographic leads on the evidence computer. This file contains the information to identify thousands of known pornography sites as well as *possible* pornography sites. Think of the NTA.EXE file above as being the "brain" for NTA Stealth™ and NTALOGIC.NTI file as being the "knowledge" that is necessary to allow the brain to function.

Because pornographers are constantly changing the names of various web sites, NTALOGIC.NTI is regularly updated for the latest changes to known as well as suspected pornography web sites. Therefore, you should regularly update the NTALOGIC.NTI file included on your NTA Stealth™ Test Disk and/or NTA Stealth™ USB Thumb Drive by downloading the most recent version of NTALOGIC.NTI from NTI's web site at:

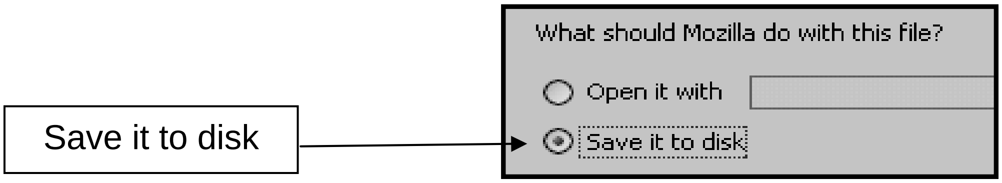
http://www.forensics-intl.com/tools.html

Downloading Updates of NTALOGIC.NTI

In order for your version of NTA Stealth™ to be current, you should **regularly download the latest version of NTALOGIC.NTI from NTI's web site**. Follow the instructions below to download the latest version of NTALOGIC.NTI:

1. Go to http://www.forensics-intl.com/tools.html and click on the NTALOGIC.NTI icon.

2. A window will appear on the screen indicating whether you wish to open the file or save the file to disk. Click on the **"Save it to Disk"** option.

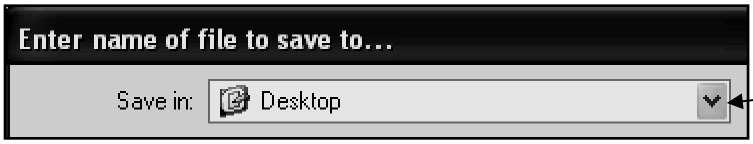


What should Mozilla do with this file?

○ Open it with

● Save it to disk

3. Another window will appear indicating where you would like to save the NTALOGIC.NTI file to your hard drive. For easy access, we recommend you temporarily save the file to your desktop. If desired, you can move the file to another location after this procedure.



Save to the Desktop

4. Once the latest version of NTALOGIC.NTI has been saved to your desktop, copy this file to the NTA Stealth™ Test Disk, a separate floppy disk for one of the 6 Custom NTA Stealth™ Images and to the NTA Stealth™ USB Thumb Drive, if applicable, as follows.

5. Insert the NTA Stealth™ Test Disk or a separate floppy disk (for one of the 6 Custom NTA Stealth™ Images) into the floppy drive and/or the NTA Stealth™ USB Thumb Drive into a USB port of your computer (not the evidence computer).

6. Right click on the NTALOGIC.NTI icon on your desktop and then click on "Copy" from the fly-out panel.

7. Double click on the "My Computer" icon on your computer desktop (or select "Start" on your Task Bar located at the bottom left-hand side of your computer screen and then click on "My Computer")

8. Double click on your floppy drive icon and or the USB port icon in the "My Computer" window.

9. Copy the NTALOGIC.NTI program logic file to the NTA Stealth™ Test Disk or a separate floppy disk (for one of the 6 Custom NTA Stealth™ Images) and/or the NTA Stealth™ USB Thumb Drive by clicking the **"Edit"** button in the upper right-hand corner of the window and then clicking on **"Paste"** in the drop down box.

NTA Stealth™ has been programmed to determine if any corruption has resulted from downloading the NTALOGIC.NTI file from the Internet. If corruption has occurred, NTA Stealth™ will not operate and will prompt you to again download the NTALOGIC.NTI from NTI's web site.

AUTOEXEC.BAT and NTA.BAT Files

The AUTOEXEC.BAT file is included on the NTA Stealth™ Test Disk and within the 6 Custom NTA Stealth™ Images included on the NTA Stealth™ Support CD. The NTA.BAT file is included on the NTA Stealth™ USB Thumb Drive. These files are essentially batch files that contain a specific NTA Stealth™ command that allow for the automatic processing of an NTA Stealth™ command/option when used with NTA.EXE and NTALOGIC.NTI.

The AUTOEXEC.BAT and the NTA.BAT files include the specific processing command/option that you requested when you purchased NTA Stealth™. For example, let's say that you wanted to use the software primarily for identifying pornography web sites on computers. The AUTOEXEC.BAT and the NTA.BAT files would contain the following command:

```
nta /h0 /auto1 /porn
```

By inserting the NTA Stealth™ Test Disk into the floppy drive (for running NTA Stealth™ on a floppy disk) or the USB Boot CD in the CD-ROM drive and NTA Stealth™ USB Thumb Drive in the USB port (for running NTA Stealth™ from the USB Thumb Drive) of the evidence computer and turning it on (see specific instructions in previous subsections), NTA Stealth™ will automatically process the first hard drive of the evidence computer (designated by the **"/h0"**) for all Internet web sites (designated by the **"/auto1"**) that could possibly be of a pornographic nature (designated by the **"/porn"**)**.**

Changing AUTOEXEC.BAT and NTA.BAT Files

NTA Stealth™ contains various commands/options that are explained in subsequent subsections in this User's Guide. To change the command/options for running NTA Stealth™, the **AUTOEXEC.BAT** file, included on the NTA Stealth™ Test Disk and in the 6 Custom NTA Stealth™ Images on the NTA Stealth™ Support CD, and the **NTA.BAT** file, included on the NTA Stealth™ USB Thumb Drive, must be changed for the desired commands and options.

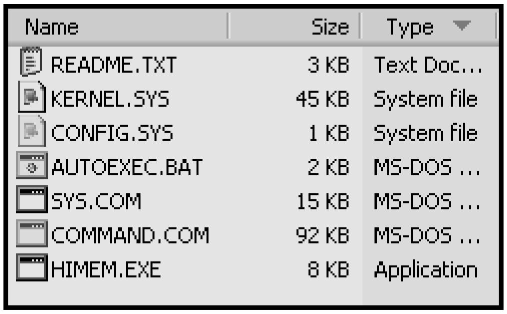
For example, the AUTOEXEC.BAT and the NTA.BAT files that may have come with your purchase of NTA Stealth™ were all configured to search the ***first*** physical hard drive on the machine (designated by the "/h0" on the DOS command line) for pornography-based Internet web sites. If you wish the second or third hard drive in the evidence computer be searched, or the "/porn" command option be removed, then the AUTOEXEC.BAT and the NTA.BAT files will need to be changed, as explained in the subsections that follow.

Changing AUTOEXEC.BAT FILE on NTA Stealth™ Floppy Test Disk

The command/option line can be changed by doing the following:

1. Insert the NTA Stealth™ Test Disk in the floppy disk drive of your computer. (**NOT** the evidence computer!)

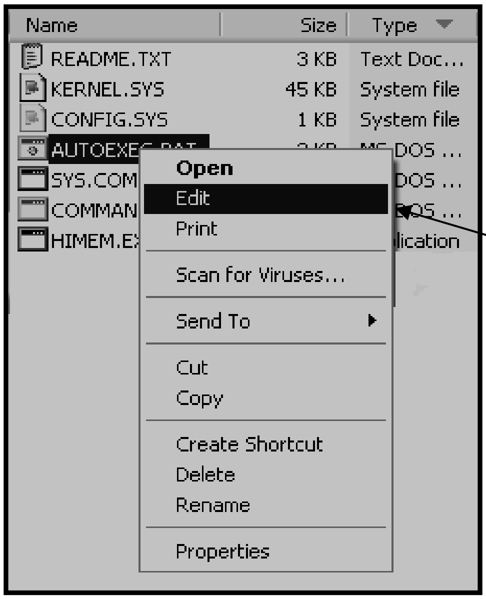
2. Locate and double click on the floppy disk icon to view the files.



Name	Size	Type
README.TXT	3 KB	Text Doc...
KERNEL.SYS	45 KB	System file
CONFIG.SYS	1 KB	System file
AUTOEXEC.BAT	2 KB	MS-DOS ...
SYS.COM	15 KB	MS-DOS ...
COMMAND.COM	92 KB	MS-DOS ...
HIMEM.EXE	8 KB	Application

3. Right click on the **AUTOEXEC.BAT** file on the NTA Stealth™ Test Disk.

4. Choose **"edit"** on the fly out panel as depicted in the graphic below.



Choose Edit

5. This will open the file and display on the last two lines the path to the A:\ drive and the NTA Stealth™ command/option. Below is an example.

path=:a:\
nta /h0 /auto1 /porn

As an example of changing the AUTOEXEC.BAT file, if your intention is to search the 2nd hard drive on the computer and capture ALL of the Internet URLs and not just the potential pornography links, then right-click on the AUTOEXEC.BAT file located on the floppy disk and choose **"edit"** as shown above.

At the bottom of the AUTOEXEC.BAT file, change the NTA Stealth™ syntax **from "/h0" to "/h1"** and then delete the **"/porn"** option as shown below. After changing, save and close the file.

```
nta /h1 /auto1
```

Changing NTA.BAT FILE on NTA Stealth™ USB Thumb Drive

If you are running NTA Stealth™ from the NTA Stealth™ USB Thumb Drive by using the USB Boot CD, then simply follow the instructions in the previous section **"Changing the AUTOEXEC.BAT FILE On The NTA Stealth™ Test Disk."** The procedure is the same except that, instead of changing the AUTOEXEC.BAT file, you will need to change the NTA.BAT file.

The commands and options explained in the subsections that follow, with the exception of the **"/NTA**" and "**/filename**" commands/options since these are used to process files and not physical hard drives, can be inserted into or changed in the AUTOEXEC.BAT and the NTA.BAT files by following the instructions explained above.

Summary of NTA Stealth™ Commands and Options

A summary of NTA Stealth™ program commands and options are described as follows. These commands can be utilized, with the exception of the **"/NTA**" and "**/filename**" commands/options since these are used to process files and not physical hard drives, by changing the AUTOEXEC.BAT file and/or the NTA.BAT file, as previously discussed under the subsection **"Changing the AUTOEXEC.BAT and NTA.BAT Files."**

NTA This command will cause the NTA Stealth™ **System Menu** to be displayed for use in processing individual files with NTA Stealth™. This command should only be utilized in a laboratory setting and <u>should not</u> be used with the modification of the AUTOEXEC.BAT and NTA.BAT files, as previously discussed. The System Menu operation is described in the "Processing Files" section of this User's Guide.

NTA /h0

This command **targets the first physical hard disk drive** on the evidence computer system for processing. This option <u>must be</u> used with other switches to identify the NTA Stealth™ lead identification option desired (such as /auto1, /auto2, /auto3 and /auto4). **Please note that you cannot use the /H switch when processing individual files using the filename option.** Use of this option is mandatory if you intend to process the first physical hard disk drive on a system. If you desire to process the second hard drive in the evidence computer, the command would be **NTA /h1**.

NTA /AUTO1 This option directs NTA Stealth™ to **identify Internet web browsing leads**. If you want to identify all Internet web browsing leads on the *first* hard drive of the evidence computer then the program is operated from the command line using the following syntax:

```
nta /h0 /auto1
```

If you want to identify Internet web browsing leads on the second hard disk drive of the evidence computer then NTA Stealth™ is operated from the command line using the following syntax:

```
nta /h1 /auto1
```

If you want to limit the NTA Stealth™ findings to **only capture pornography-based web sites leads** on the first hard drive then the command line syntax would be:

```
nta /h0 /auto1 /porn
```

NTA /AUTO2 This option directs NTA Stealth™ to **identify Internet email leads**. If you want to identify all Internet email leads on the first hard drive on the evidence computer then NTA Stealth™ command line syntax would be:

```
nta /h0 /auto2
```

NTA /AUTO3 This option directs NTA Stealth™ to **identify Internet graphics files accessed with .gif and .jpg extensions that were accessed and downloaded.** If you want to identify leads of Internet graphics files downloaded and accessed from the first hard disk drive on the evidence computer then NTA Stealth™ command line syntax would be:

```
nta /h0 /auto3
```

NTA /AUTO4 This option directs NTA Stealth™ to **identify all Internet activity leads of web browsing and email addresses** over the Internet. This option combines all of the features of **/auto1** and **/auto2** into one feature. If your goal is to identify all leads of past Internet activity on the second hard disk drive on the evidence computer then NTA Stealth™ command line syntax would be:

```
nta /h1 /auto4
```

If you want to limit NTA Stealth™ findings to **just capturing pornography-based web site and email leads** on the third hard disk drive in the system, then the NTA Stealth™ command line syntax would be:

```
nta /h2 /auto4 /porn
```

NTA /PORN This option directs NTA Stealth™ to identify *only* pornography-based leads to conserve storage space on floppy disks and to focus specifically on pornography. This command line option can be used with either the **/auto1** or the **/auto4** command line switches. Below is an example of using the /porn command with the /auto4 command and searching the first hard drive.

```
nta /h0 /auto4 /porn
```

NTA /SKIPnnn This option directs NTA Stealth™ to **skip a specific number of physical sectors** by substituting a number for the "nnn" pattern. Typically, the first part of a hard drive is devoted to operating system files and program application files. The **/skip** command line option is used with a physical hard disk drive switch such as the **/h0**, or **/h1** to specify either the first or second hard drive.

To help conserve processing time, the NTA Stealth™ default is to skip the first 20,000 sectors of the physical hard disk drive. However, the default can be overridden through the use of the **/skip0** command line switch. By invoking the **/skip0** option, the program will start processing at the first sector of the hard drive being processed.

NTA /ENDnnn This option directs NTA Stealth™ to **stop processing when the program reaches a specific number** by substituting a sector number for the "nnn" pattern. This command line switch is used when a sampling of the physical hard disk drive is desired and it can be used in combination with the **/skip** switch. This command line switch is used with a physical hard disk drive option, such as the /h0 or /h1, to specify either the first or second hard drive as the target for processing.

NTA filename This option directs the program to **process a specific file**. The **filename** command can be used to process a Windows swap or page file for a sampling of Internet activity leads that passed through the Windows swap or page file during a Windows operating session. This command should only be utilized in a laboratory setting and **cannot** be used with the modification of the AUTOEXEC.BAT and NTA.BAT files, as previously discussed.

Typically the processing of files is done in a working directory on a separate laboratory computer that has been dedicated to the processing of computer-related evidence. In the case of Windows swap and Windows page files, the processing is performed after the imaged files have been copied from the evidence computer system to the laboratory computer.

As with the other command line options, this command can be used in combination with other command line switches. For example, the syntax

```
nta filename /auto1
```

would be used to process an evidence file to identify leads associated with past Internet web browsing activities.

If you want to limit the leads to pornography-based Internet web site leads identified in an evidence file, then you would use the following command line syntax:

```
nta filename /auto1 /porn
```

NOTE: The NTA filename option cannot be used with the **/hX**, **/skip** or **/end** command line switches.

More information on the filename command can be found in the **"Processing Files"** section of this User's Guide.

Identifying More Than One Hard Drive on Evidence Computer

NTA Stealth™ identifies the first physical hard drive in the computer as **/H0**, the second physical hard drive as **/H1,** the third physical hard drive in the computer **as /H2** and so forth. To save disk space, NTA Stealth™ does not automatically identify the number of hard drives that are on the computer.

To determine if there is more than one physical hard drive on the evidence computer that you want to process using NTA Stealth™, following the instructions under "Changing the AUTOEXEC.BAT And NTA.BAT Files" as explained in a previous subsection.
Replace the **/H0** in the command line with **/H1** and follow the instructions for running NTA Stealth™ in previous subsections of this User's Guide. If NTA Stealth™ begins processing the second hard drive; you will know that there are at least two hard drives in the computer.

To determine if there are additional physical hard drives in the evidence computer, replace the **/H1** in the command in the AUTOEXEC.BAT and NTA.BAT file with an **/H2** and follow the previously discussed procedures for running NTA Stealth™.

/AUTO1- Internet Web Browsing Option

The **/auto1** option directs NTA Stealth™ to **identify Internet web browsing leads and the frequency thereof**. If you want to identify all Internet web browsing leads on the first hard drive in the evidence computer, the command line syntax would be as follows (Note: you may need to change the AUTOEXEC.BAT and/or the NTA.BAT files as explained under "Changing the AUTOEXEC.BAT And NTA.BAT Files" in a previous subsection):

```
nta /h0 /auto1
```

This command will cause NTA Stealth™ to process the first physical hard drive on the evidence computer from the NTA Stealth™ Test Disk (or NTA Stealth™ USB Thumb Drive), starting at 20,000 absolute sectors. The **/h0** command targets the first physical hard drive on the computer and the **/auto1** command specifies the identification of Internet web browsing leads or URLs. NTA Stealth™ begins its processing at 20,000 sectors because most Windows operating system program files are stored in this area of the hard drive and it is unlikely that leads will be generated by NTA Stealth™ from those sectors.

Note: If you prefer to begin searching from the first absolute sector on the hard drive, you may use the **"/skip"** option and type the following at the command line prompt:

```
nta /h0 /auto1 /skip0
```

This will cause NTA Stealth™ to process the first physical hard disk drive on the evidence computer from the NTA Stealth™ Test Disk (or NTA Stealth™ USB Thumb Drive) starting at the very beginning of the evidence hard drive to the end of the hard drive or until the NTA Stealth™ Test Disk is full.

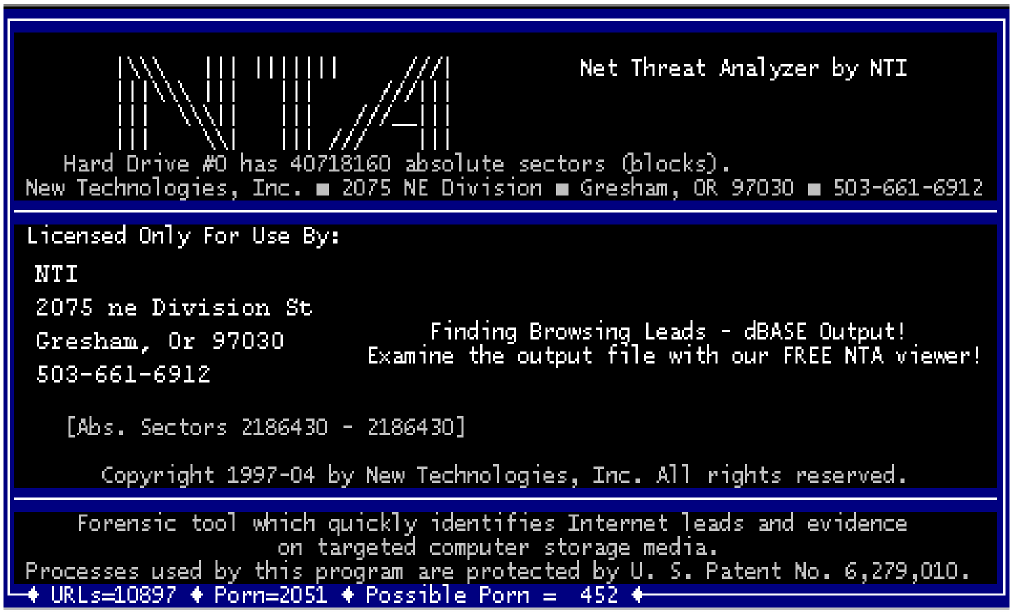
The resulting output file will be stored on the NTA Stealth™ Test Disk (or NTA Stealth™ USB Thumb Drive) and it will be named "**_NTAH0.DBF**" when the command line syntax listed above is used. If the second hard drive was processed, the output file will be named **"_NTAH1.DBF**".

The program will identify Internet web browsing leads and save the leads to the NTA Stealth™ Test Disk (or NTA Stealth™ USB Thumb Drive), as appropriate. The display screen will show a tally of the number of leads NTA Stealth™ has identified. The screen display will also indicate whether or not items of "possible porn" web sites have been found, e.g., possible pornography-based web sites.

The graphic below is an example of what NTA Stealth™ displays when the syntax

```
nta /h0 /auto1
```

is typed in the AUTOEXEC.BAT of the NTA Stealth™ Test Disk or NTA.BAT file of the NTA Stealth™ USB Thumb Drive.



```
        |\\\   ||| |||||||     ///|        Net Threat Analyzer by NTI
        |||\\\ |||   |||     ///|||
        |||  \\\||   |||   ///__|||
        |||    \\|   |||  ///    |||
     Hard Drive #0 has 40718160 absolute sectors (blocks).
  New Technologies, Inc. ■ 2075 NE Division ■ Gresham, OR 97030 ■ 503-661-6912

  Licensed Only For Use By:
   NTI
   2075 ne Division St
   Gresham, Or 97030              Finding Browsing Leads - dBASE Output!
                              Examine the output file with our FREE NTA viewer!
   503-661-6912

      [Abs. Sectors 2186430 - 2186430]

         Copyright 1997-04 by New Technologies, Inc. All rights reserved.

        Forensic tool which quickly identifies Internet leads and evidence
                        on targeted computer storage media.
  Processes used by this program are protected by U. S. Patent No. 6,279,010.
 ♦ URLs=10897 ♦ Porn=2051 ♦ Possible Porn =  452 ♦
```

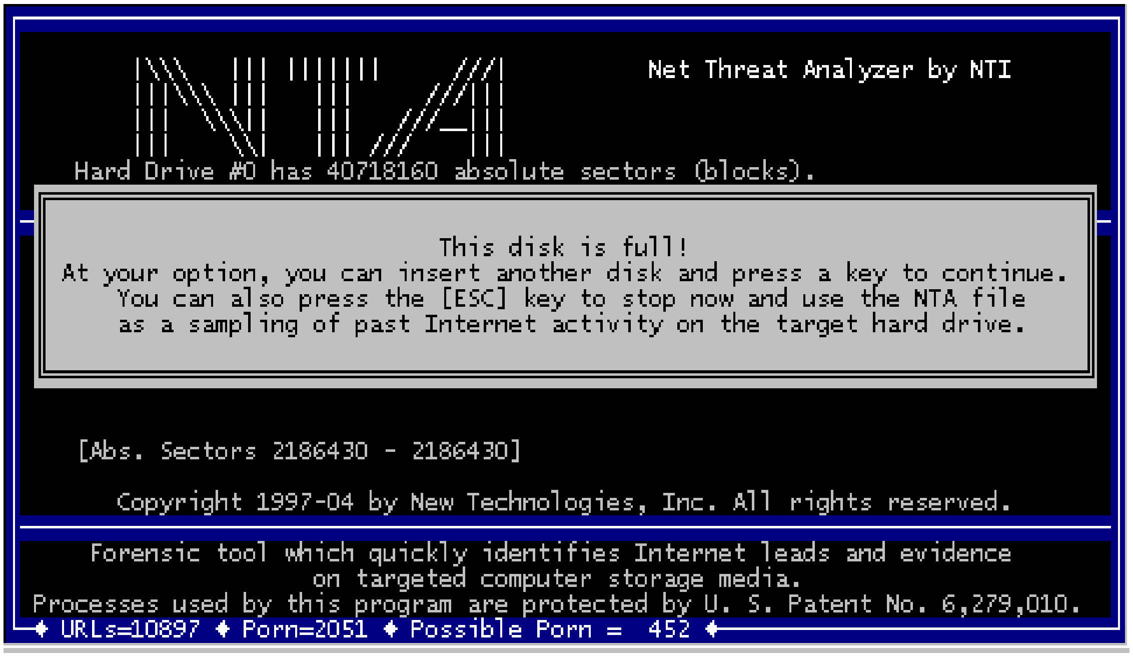
Identified URLs - Porn Count - Possible Porn

Notice that the bottom of the screen displays the number of URLs, known pornography sites, and possible pornography sites identified by NTA Stealth™. In this instance, NTA Stealth™ captured:

➢ URLs	10,897	Total URL sites
➢ Porn	2,051	Pornography sites
➢ Possible Porn	452	Possible Porn sites

NTA Stealth™ has been programmed with knowledge of thousands of known pornography-based web sites and it will automatically flag such items as they are identified. An added feature is that NTA Stealth™ will also flag sites that could be **"Possible Porn".** Each item is captured in the output file to be analyzed and viewed using NTA Viewer™.

If you are running NTA Stealth™ from the NTA Stealth™ Test Disk, allow the program to operate for several minutes or until the disk is full. At your option, you can insert another floppy disk into the floppy drive after the NTA Stealth™ Test Disk becomes full or you can simply stop the processing and rely upon the sampling of data written to the NTA Stealth™ Test Disk by following the instructions in the subsection "Manually Terminating Or Pausing NTA Stealth™".



```
                                          Net Threat Analyzer by NTI
  Hard Drive #0 has 40718160 absolute sectors (blocks).

                          This disk is full!
  At your option, you can insert another disk and press a key to continue.
     You can also press the [ESC] key to stop now and use the NTA file
     as a sampling of past Internet activity on the target hard drive.

  [Abs. Sectors 2186430 - 2186430]

     Copyright 1997-04 by New Technologies, Inc. All rights reserved.

     Forensic tool which quickly identifies Internet leads and evidence
                    on targeted computer storage media.
 Processes used by this program are protected by U. S. Patent No. 6,279,010.
 ♦ URLs=10897 ♦ Porn=2051 ♦ Possible Porn =  452 ♦
```

"This disk is full!"

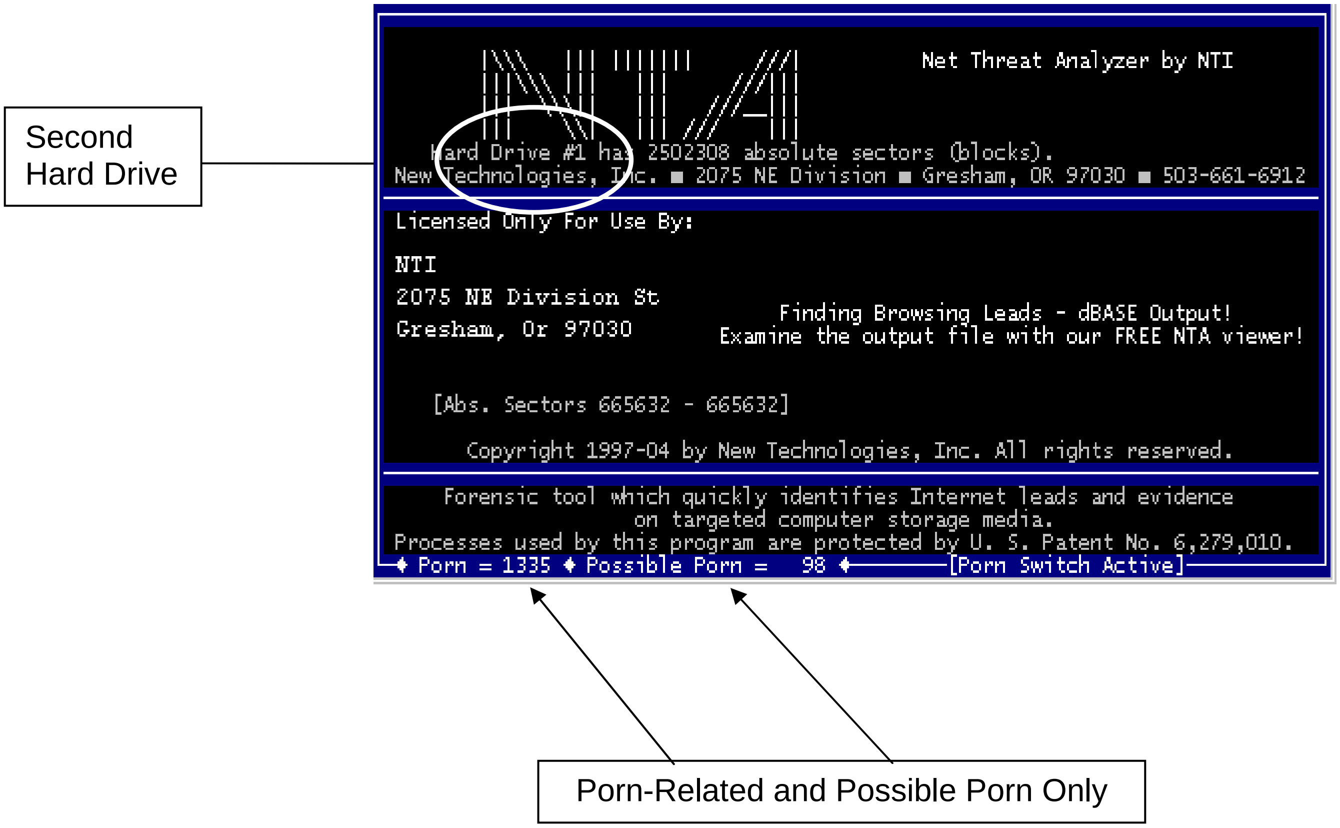
The NTA Stealth™ Test Disk can store up to approximately 10,000 to 11,000 possible leads before being prompted to either terminate the process or continue with the insertion of a new floppy disk as shown by the graphic above.

Internet Web Browsing with Pornography Only Option

If you want to limit NTA Stealth™ findings to just pornography-based web sites ONLY, and you want to process the second hard drive on the evidence computer beginning at 50,000 sectors of the hard drive, then the AUTOEXEC.BAT and/or the NTA.BAT files will need to be changed for the command line syntax as follows:

```
nta /h1 /auto1 /porn /skip50000
```

The screen below shows an example of the processing using this command.



```
                                        Net Threat Analyzer by NTI
   Hard Drive #1 has 2502308 absolute sectors (blocks).
New Technologies, Inc. ■ 2075 NE Division ■ Gresham, OR 97030 ■ 503-661-6912
Licensed Only For Use By:

NTI
2075 NE Division St
Gresham, Or 97030               Finding Browsing Leads - dBASE Output!
                            Examine the output file with our FREE NTA viewer!

   [Abs. Sectors 665632 - 665632]

      Copyright 1997-04 by New Technologies, Inc. All rights reserved.
    Forensic tool which quickly identifies Internet leads and evidence
                      on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
♦ Porn = 1335 ♦ Possible Porn =   98 ♦────────[Porn Switch Active]
```

Second Hard Drive

Porn-Related and Possible Porn Only

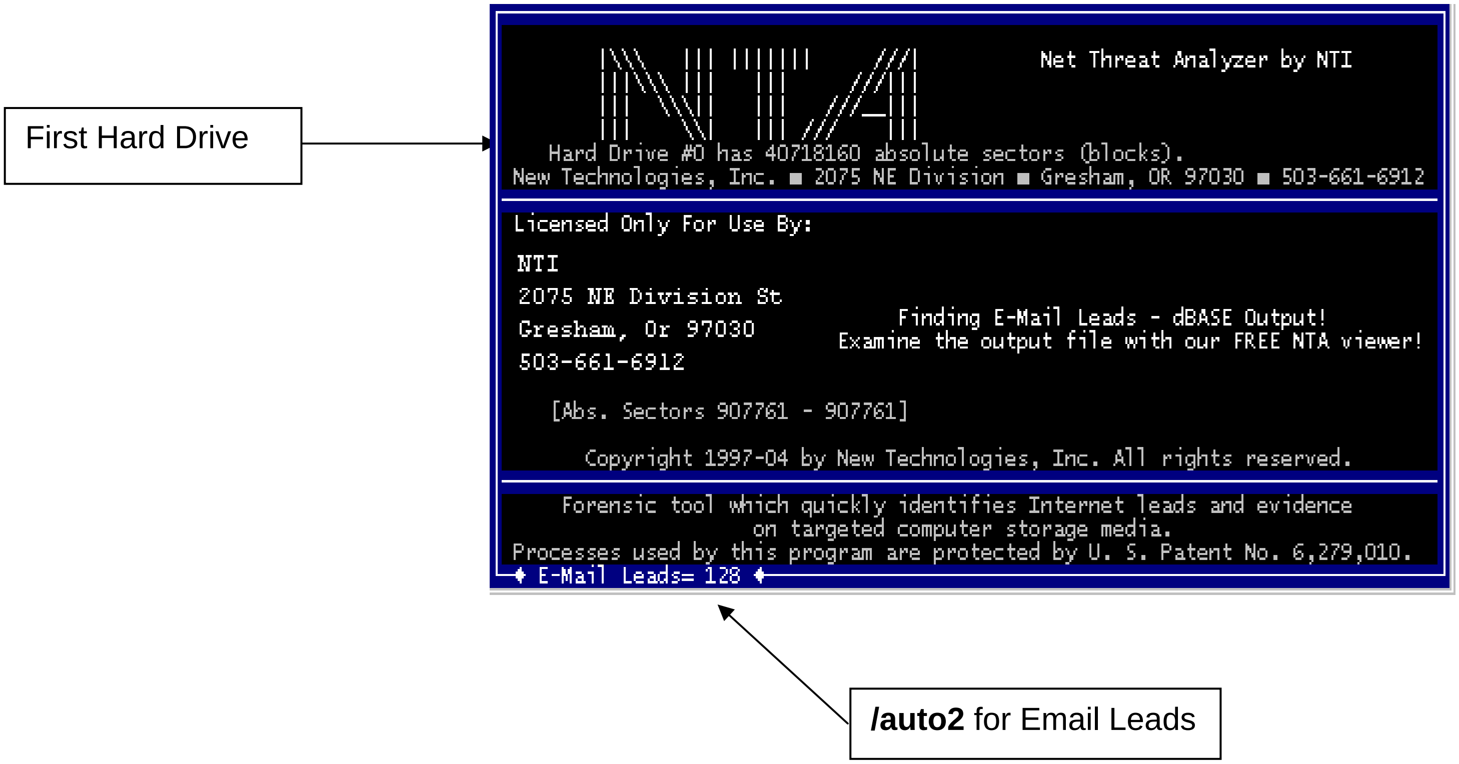
Notice the amount of URLs specific to known pornographic content captured thus far is 1,335 and the "Possible Porn" count is 98.

The command option of **nta /h0 /auto1 /porn /skip50000** will search the first physical hard drive on the computer for all Internet web addresses [URLs] related to pornography, beginning the processing at 50,000 sectors. The default setting for NTA Stealth™ to begin processing is 20,000 sectors.   More about the /skip and /end command options are discussed in the **"Skip and End Command Options"** subsection of this User's Guide.

/AUTO2- Email Leads Option

NTA Stealth™ identifies email addresses on the evidence computer using the **/auto2** option. The command line syntax for processing the first physical hard drive would be as follows (Note: you may need to change the AUTOEXEC.BAT and/or the NTA.BAT files as explained under “Changing The AUTOEXEC.BAT And NTA.BAT Files” in a previous subsection.):

```
nta /h0 /auto2
```



```
                                          Net Threat Analyzer by NTI
   Hard Drive #0 has 40718160 absolute sectors (blocks).
New Technologies, Inc. ■ 2075 NE Division ■ Gresham, OR 97030 ■ 503-661-6912

Licensed Only For Use By:
NTI
2075 NE Division St
Gresham, Or 97030                  Finding E-Mail Leads - dBASE Output!
503-661-6912                    Examine the output file with our FREE NTA viewer!

   [Abs. Sectors 907761 - 907761]

      Copyright 1997-04 by New Technologies, Inc. All rights reserved.

     Forensic tool which quickly identifies Internet leads and evidence
                     on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
♦ E-Mail Leads= 128 ♦
```

First Hard Drive

/auto2 for Email Leads

The **/h0** command targets the first physical hard drive on the computer and the **/auto2** command specifies Internet email addresses only.

The resulting output file will be stored on the NTA Stealth™ Test Disk or NTA Stealth™ USB Thumb Drive with the name of **“MNTAH0.DBF.”** The **“0”** relates to the first hard drive NTA Stealth™ was instructed to search.

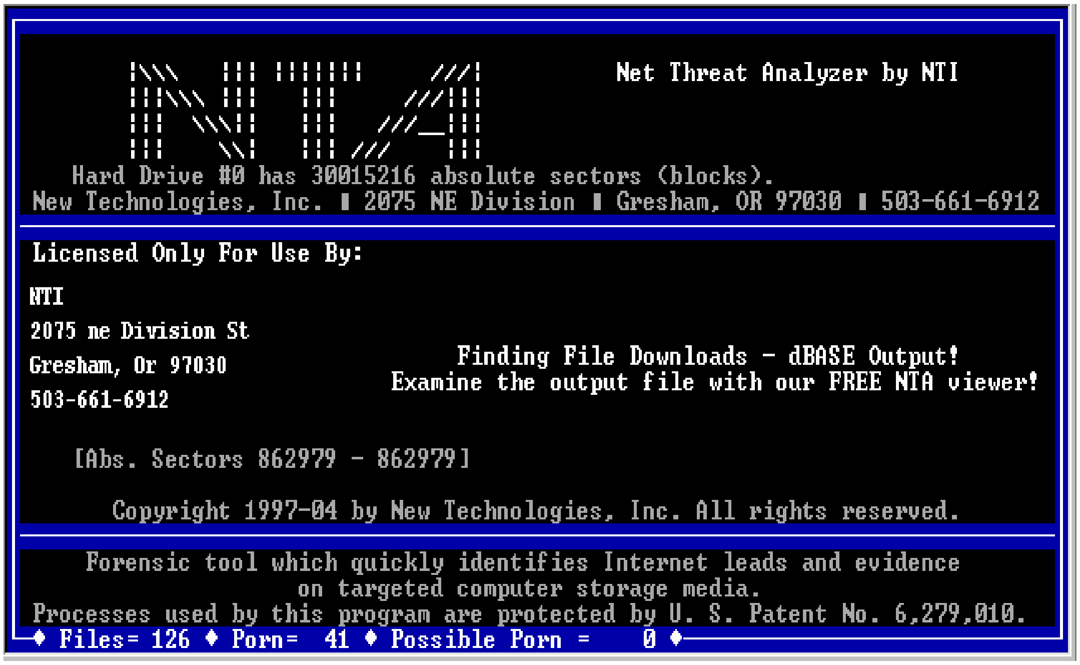
/AUTO3- Graphic File Option

Utilizing the command option **/auto3** directs NTA Stealth™ to **identify Internet graphic files with .gif and .jpg extensions that were downloaded** onto the evidence computer.

The syntax to identify leads of Internet graphic file downloads from the first physical hard disk drive of the evidence computer running NTA Stealth™ is as follows (Note: you may need to change the AUTOEXEC.BAT and/or the NTA.BAT files as explained under "Changing The AUTOEXEC.BAT And NTA.BAT Files" in a previous subsection.):

```
nta /h0 /auto3
```

This command option will produce the screen below as NTA Stealth™ is processing.



```
       |\\\    ||| |||||||     ///|          Net Threat Analyzer by NTI
       |||\\\ |||   |||     ///|||
       |||  \\\||   |||   ///__|||
       |||    \\|   ||| ///    |||
   Hard Drive #0 has 30015216 absolute sectors (blocks).
 New Technologies, Inc. ▮ 2075 NE Division ▮ Gresham, OR 97030 ▮ 503-661-6912

 Licensed Only For Use By:

NTI
2075 ne Division St
Gresham, Or 97030                 Finding File Downloads - dBASE Output!
503-661-6912                   Examine the output file with our FREE NTA viewer!

   [Abs. Sectors 862979 - 862979]

      Copyright 1997-04 by New Technologies, Inc. All rights reserved.

     Forensic tool which quickly identifies Internet leads and evidence
                     on targeted computer storage media.
 Processes used by this program are protected by U. S. Patent No. 6,279,010.
 ♦ Files= 126 ♦ Porn=  41 ♦ Possible Porn =    0 ♦
```

Note that NTA Stealth™ identified 126 graphic files with .gif and/or .jpg extensions of which 41 were tagged as being of a pornographic nature.

The resulting output file will be stored on the NTA Stealth™ Test Disk (or NTA Stealth™ USB Thumb Drive) with the name of **"~NTAH0.DBF"** The **"0"** relates to the first physical hard drive NTA Stealth™ was instructed to search. The output file name would be **"~NTAH1.DBF"** if the second hard drive was searched.

Graphic File Download Frequency

Unlike the web browsing and email lead identification options discussed previously; **it is important to look at every graphic file lead found when this command line switch is used.** This is because Internet file download frequencies are not generally issues when file downloads from the Internet are involved. Once the computer user has downloaded a file over the Internet, there is generally no need for the computer user to continue going back to the same web site repeatedly for the download of the same file. Please also remember that information found in the Windows swap file may be months or even years old. Thus, NTA Stealth™ leads for files downloaded may be old and the relevant files may have been deleted from the evidence computer long ago.

/AUTO4- Web Browsing and Email Combination Option

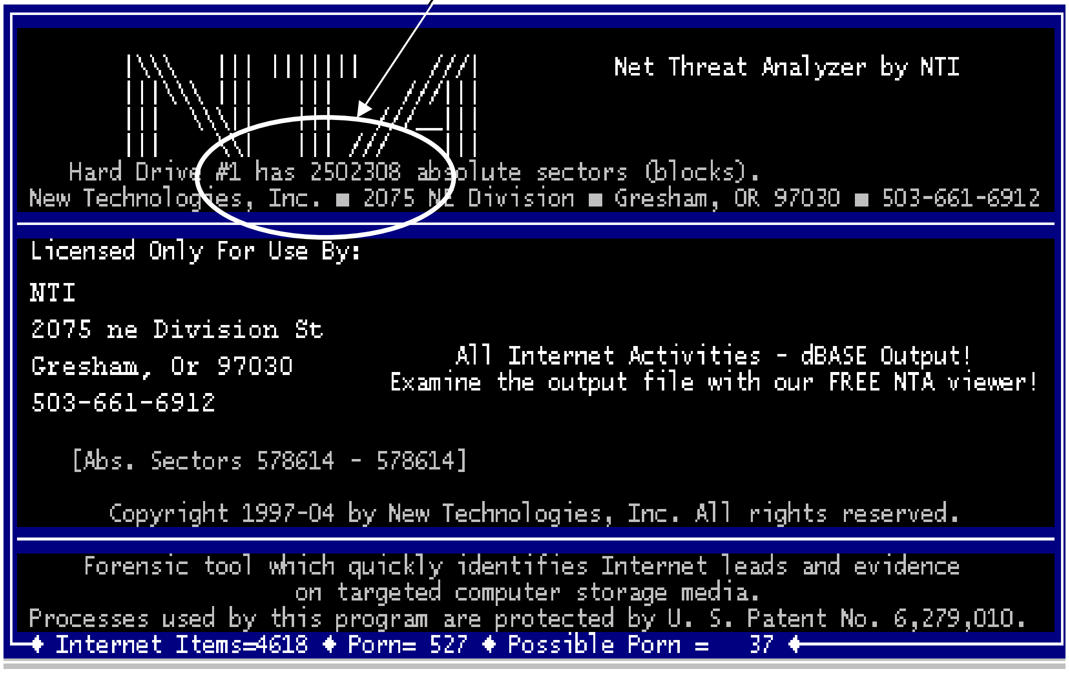
NTA Stealth's™ **/auto4** command option combines the **/auto1** *and* the **/auto2** option to identify all Internet activity leads that involve web browsing and email addresses.
This command line switch can also be used in conjunction with the **/porn** command line option to identify only pornography-based Internet leads.

The syntax to search the second hard drive for Internet URLs and email addresses on an evidence computer is (Note: you may need to change the AUTOEXEC.BAT and/or the NTA.BAT files as explained under **"Changing The AUTOEXEC.BAT and NTA.BAT Files"** in a previous subsection):

```
nta /h1 /auto4
```

The screen below illustrates the processing of NTA Stealth™ using this command. The sectors being searched and the count of Internet items, including possible pornography web-browsing sites, are instantly displayed on the display screen.

Number of sectors on 2nd hard drive



```
                                                   Net Threat Analyzer by NTI
   Hard Drive #1 has 2502308 absolute sectors (blocks).
New Technologies, Inc. ■ 2075 NE Division ■ Gresham, OR 97030 ■ 503-661-6912

Licensed Only For Use By:
NTI
2075 ne Division St
Gresham, Or 97030                 All Internet Activities - dBASE Output!
                              Examine the output file with our FREE NTA viewer!
503-661-6912

   [Abs. Sectors 578614 - 578614]

      Copyright 1997-04 by New Technologies, Inc. All rights reserved.

     Forensic tool which quickly identifies Internet leads and evidence
                      on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
♦ Internet Items=4618 ♦ Porn= 527 ♦ Possible Porn =   37 ♦
```

Count of Internet, Porn and Possible Porn Items as the hard drive is being searched

In the above example, notice that NTA Stealth™ has thus far processed 578,614 sectors out of a total of 2,502,308 sectors on the second hard drive and has identified 4,618 Internet Items with a 527 item count of pornography and a "possible porn" count of 37 items.

The resulting output file will be stored on the NTA Stealth™ Test Disk (or NTA Stealth™ USB Thumb Drive) with the name of "-**NTAH1.DBF**." The "1" relates to the second physical hard drive that NTA Stealth™ was instructed to search. The output file name would be "-**NTAH0.DBF**" if the first physical hard drive was searched.

Web Browsing and Email Combined Option-Porn Only

NTA Stealth's™ **/auto4** command option combines the **/auto1** and the **/auto2** option to identify all Internet activity leads that involve web browsing and email addresses. However, when the **/porn** command option is invoked along with the **/auto4** command option, NTA Stealth™ captures *only* the Internet activity and email addresses that may be of pornographic nature.

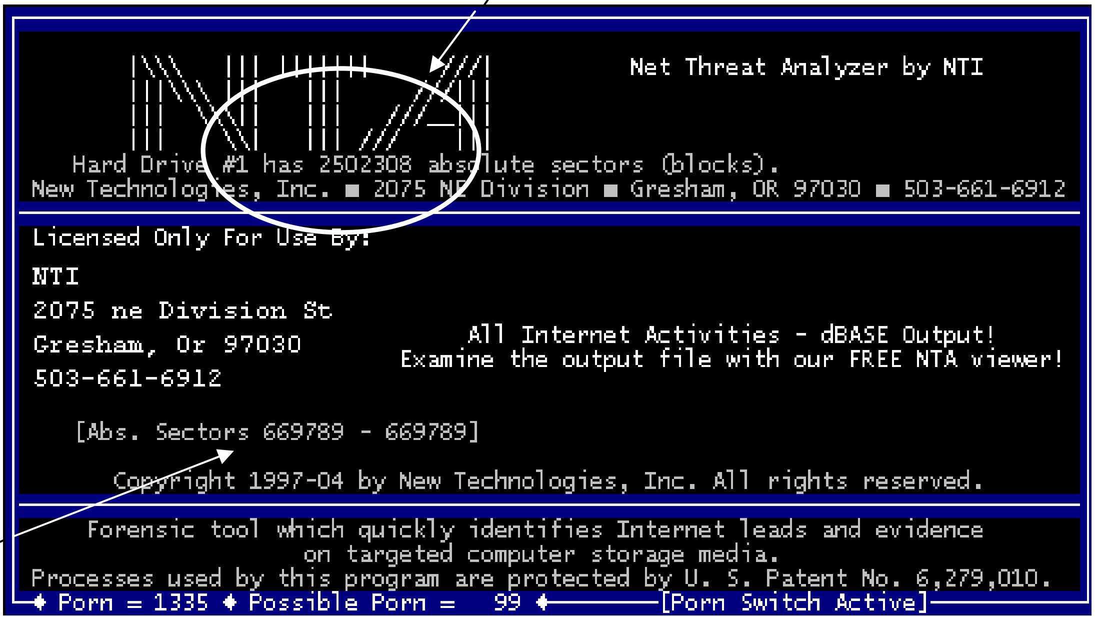
Although NTA Stealth™ is programmed to identify thousand of pornographic web sites, it does not have knowledge of all the possible child and adult pornographic Internet web sites. However, we know of no other tool that is more accurate in the identification of pornography-based Internet web sites but you should be aware that some sites will be missed when this command line switch (/porn) is used.

Below is an example of NTA Stealth™ syntax for identifying Internet web URLs and email leads that may contain pornographic content only and when only a portion of the hard drive is processed for sampling purposes.

```
nta /h1 /auto4 /porn /skip150000 /end2000000
```

The syntax tells NTA Stealth™ to begin processing the second hard drive (/h1) for all web sites downloaded and email addresses (/auto4) that may be pornographic (/porn) starting with sector 150,000 (/skip150000) and ending with sector 2,000,000 (/end2000000).

Total Sectors on 2nd Hard Drive

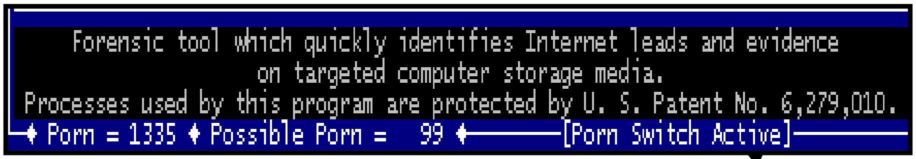


```
                                             Net Threat Analyzer by NTI
   Hard Drive #1 has 2502308 absolute sectors (blocks).
New Technologies, Inc. ■ 2075 NE Division ■ Gresham, OR 97030 ■ 503-661-6912
Licensed Only For Use By:
NTI
2075 ne Division St
Gresham, Or 97030                  All Internet Activities - dBASE Output!
                               Examine the output file with our FREE NTA viewer!
503-661-6912

   [Abs. Sectors 669789 - 669789]

      Copyright 1997-04 by New Technologies, Inc. All rights reserved.
     Forensic tool which quickly identifies Internet leads and evidence
                  on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
♦ Porn = 1335 ♦ Possible Porn =   99 ♦──────[Porn Switch Active]──
```

Sectors
669,789

Porn-related content only

In the example above, there are a total of 2,502,308 sectors on the second hard drive but, by utilizing the **/end** option, processing will end at sector 2,000,000. At sector 669,789, NTA Stealth™ captured 1,335 Internet web sites and email addresses of a pornographic nature with a "Possible Porn" content count of 99.



```
     Forensic tool which quickly identifies Internet leads and evidence
                  on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
♦ Porn = 1335 ♦ Possible Porn =   99 ♦──────[Porn Switch Active]──────
```

Notice the **'Porn Switch Active'** on the display screen

The "Porn Switch Active" on the display screen states that the **"/porn"** command option was used and only Internet activity of a pornographic content and possible pornographic content is being captured for evaluation.

The output generated by NTA Stealth™ will identify possible individual pornographic web and email addresses and the frequency thereof; however the screen above only lists the total number of "items" and does not distinguish between URLs and emails.

Please note that Internet web sites change frequently, therefore it is advisable to validate any web site in question by using NTI's NTA Viewer™ for confirmation. Instructions for using NTA Viewer™ are included in the section "NTA Viewer™ Instructions".

Skip and End Command Options

Typically, the first part of a physical hard drive is devoted to operating system files and program application files. Therefore, to help conserve processing time, NTA Stealth™ begins processing a hard drive starting at 20,000 sectors by default.

The **/skip** and **/end** command options are useful for capturing a **sample portion** of a large hard drive on a computer. These options are also useful when it may be necessary to leave the machine unattended.

You can override the default of skipping the first 20,000 sectors by modifying the command line in the AUTOEXEC.BAT and/or the NTA.BAT files with the following at the end of the command syntax:

```
/skip0
```

NTA Stealth™ will process the entire hard drive beginning at the first sector if the **/end** command option was not invoked.

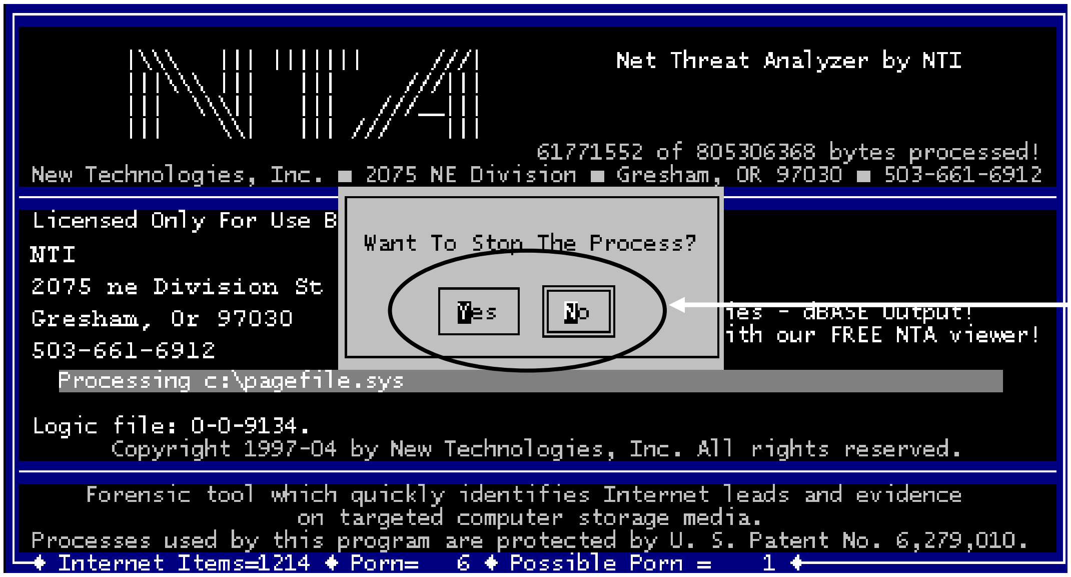
If you intend to search and capture a portion of Internet usage and email addresses on a large hard drive for sampling purposes, then the command line in the AUTOEXEC.BAT and/or the NTA.BAT files would be changed as follows:

```
nta /h0 /auto4 /skip1000000 /end2000000
```

This command instructs NTA Stealth™ to search the first physical hard drive (**h0**) on the evidence computer for all Internet web activity and email addresses (**/auto4**). The processing will begin at 1,000,000 sectors (**/skip1000000**) and terminate at 2,000,000 sectors (**/end2000000**).

Manually Terminating or Pausing NTA Stealth™

NTA Stealth™ processing can be terminated or paused manually by pressing the **"Esc"** key. The screen will display this message:

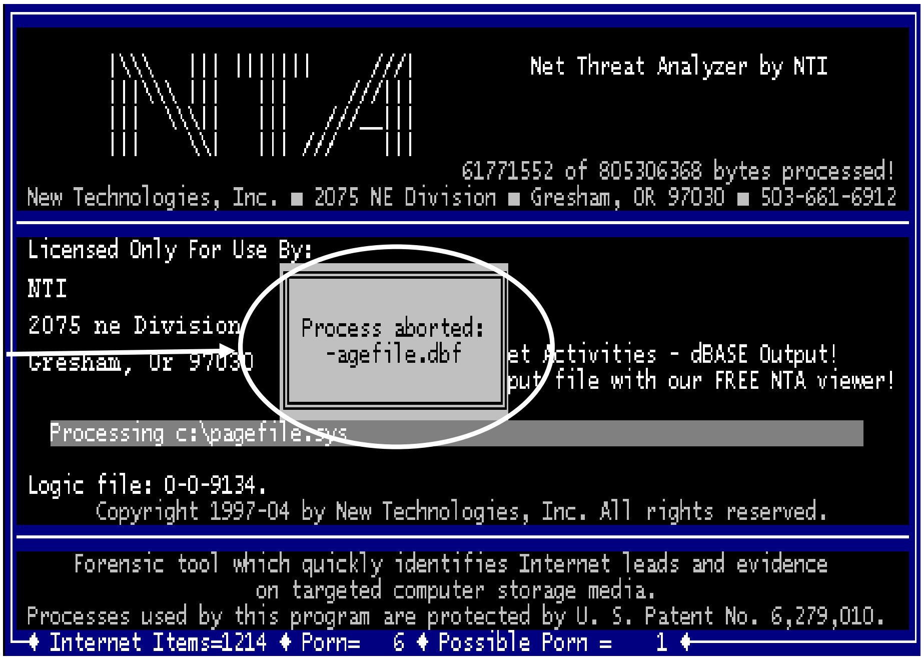


```
                                          Net Threat Analyzer by NTI

                                    61771552 of 805306368 bytes processed!
New Technologies, Inc. ■ 2075 NE Division ■ Gresham, OR 97030 ■ 503-661-6912
Licensed Only For Use B
NTI                       Want To Stop The Process?
2075 ne Division St
Gresham, Or 97030              Yes     No         ies - dBASE Output!
503-661-6912                                      ith our FREE NTA viewer!
  Processing c:\pagefile.sys

Logic file: 0-0-9134.
      Copyright 1997-04 by New Technologies, Inc. All rights reserved.

    Forensic tool which quickly identifies Internet leads and evidence
                    on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
 ♦ Internet Items=1214 ♦ Porn=   6 ♦ Possible Porn =    1 ♦
```

Press **Y** for Yes to terminate
or
N for No to continue

When the above "**Want To Stop The Process?"** message appears, you can either press the **"Y" key for YES to terminate the process or press the "N" key for NO to continue processing.**

If you choose to end the process, then the screen will display the box " **Process aborted"** with the name of the .dbf output file that was created and either saved to the NTA Stealth™ Test Disk or the NTA Stealth™ USB Thumb Drive. All NTA Stealth™ output files have .dbf extensions.



```
Net Threat Analyzer by NTI
61771552 of 805306368 bytes processed!
New Technologies, Inc. ■ 2075 NE Division ■ Gresham, OR 97030 ■ 503-661-6912
Licensed Only For Use By:
NTI
2075 ne Division
Gresham, Or 97030          Process aborted:     et Activities - dBASE Output!
                           -agefile.dbf         put file with our FREE NTA viewer!
Processing c:\pagefile.sys
Logic file: 0-0-9134.
     Copyright 1997-04 by New Technologies, Inc. All rights reserved.
    Forensic tool which quickly identifies Internet leads and evidence
                    on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
♦ Internet Items=1214 ♦ Porn=   6 ♦ Possible Porn =    1 ♦
```

Process aborted:
and the
"filename.dbf"

Processing Files

NTA Stealth™ can also **process a specific file** either by using the **/filename** option or the **System Menu** option. Windows swap or page files are important files for obtaining critical evidence on a computer. Processing files using NTA Stealth™ should only be done in a laboratory setting.

The **System Menu** option contains four standard NTA Stealth™ commands, consisting of the /auto1, /auto2, /auto3, and /auto4 options previously discussed in this User's Guide. When using the System Menu, you are not allowed to modify these standard commands for the other options of NTA Stealth™. Therefore, you should use the System Menu for processing a file only for the commands that are incorporated into the System Menu. The System Menu is also useful when the file location is not known on. Please refer to the subsection below entitled "System Menu Operation for Processing Files" for using the System Menu.

You would use the **filename** command if you desire to modify the command line syntax when processing a file. In order to use the /filename command you must know the complete path location of the file. Please refer to the subsection below entitled **"Pornography-Based Internet Activity in a Targeted File"** for use the /filename command.

What is a Swap or Page File?

A swap or page file in Microsoft Windows operating systems is a reserved portion of a hard drive that increases the computer's random access memory **(RAM)** when the operating system needs the additional RAM. The computer's operating system accesses the swap or page file in situations where the machine's RAM is being fully utilized through multiple program operations. Particular instances where an operating system might utilize a swap or page file are for example, the operating system has opened the word processing and spreadsheet functions and at the same time, the computer user is also accessing the Internet.

When the computer accesses the swap or page files, the potential exists for these files to contain remnants of word processing, email messages, Internet browsing activity, database entries and almost any other work that may have occurred during past Windows work sessions.

More information about Windows swap and page files can be found on the Internet at:

http://www.forensics-intl.com/def7.html

Please remember that information stored in a Windows swap or page file may be several months or even years old. Thus, the identified file download leads may be old and the relevant file(s) may have been deleted from the evidence computer long ago.

IMPORTANT!
The procedure for **processing files** or using the **System Menu** should be performed on a work computer and **NOT** on the evidence computer. A copy of the evidence hard drive should be made using a bit-stream backup such as NTI's SafeBack program and all processing should be done on the copy from your work machine to preserve the original hard drive source.

Information on NTI's SafeBack software can be found at:

http://www.forensics-intl.com/safeback.html

The processing of **a single source file** and utilizing **the System Menu option or the /filename option is primarily for advanced users** and for those who have had NTI's 5-Day Computer Forensics Training Course. Information on NTI's 5-Day Computer Forensics Training Course can be found at:

http://www.forensics-intl.com/forensic.html

System Menu Operation for Processing Files

The System Menu is used primarily in computer forensics laboratories when an examiner wishes to process single files for Internet activities, particularly when the location of the file is not readily known. This option should not be used in the field but rather on the examiner's work computer and on a bit-stream backup copy of the original hard drive in order to preserve evidence.

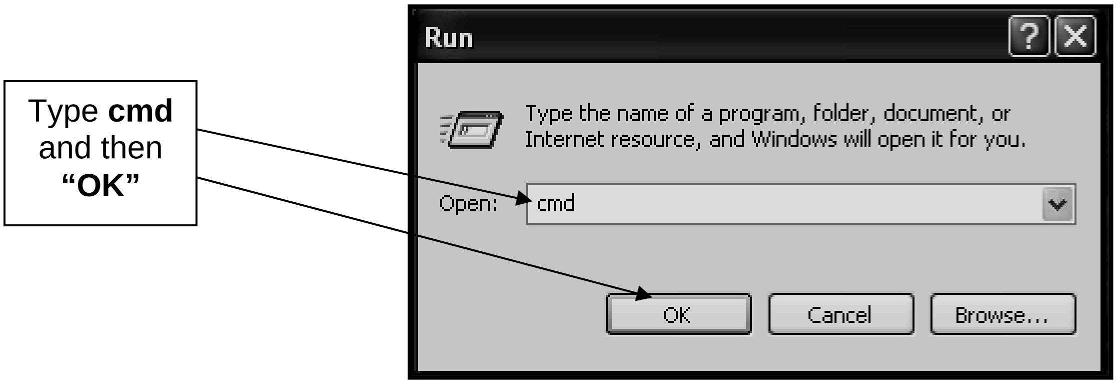
The System Menu cannot be used to process an entire physical hard drive unless you want to process non-compressed or non-encrypted bit-stream backup files that represent the contents of an entire logical or physical hard drive. If you desire to process an ***entire*** physical hard drive using NTA Stealth™, please refer to previous subsections of this User's Guide.

How To Use The System Menu

The **System Menu** can be run from a DOS command line prompt and also in a DOS prompt inside a Windows operating system. To access the System Menu by using a DOS prompt inside a Windows operating system, and assuming that the **NTA Stealth™** program executable, **NTA.EXE** and the **NTILOGIC.NTI** program is located on the floppy disk you wish to use, perform the following on your work computer:

1. Click on Start\Run in a Windows 95/98/2000/XP operating system.

2. When the RUN box appears, type **cmd** in the box and then click **"OK."**



Type **cmd** and then **"OK"**

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

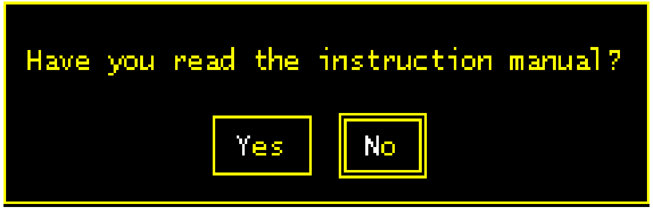
3. An MS-DOS window will appear. At the DOS prompt type "**a:**" to change to the floppy disk location where the NTA.EXE and the NTALOGIC.NTI files reside.

4. Then type:

```
nta
```

and press **Enter.** This will open the System Menu window.

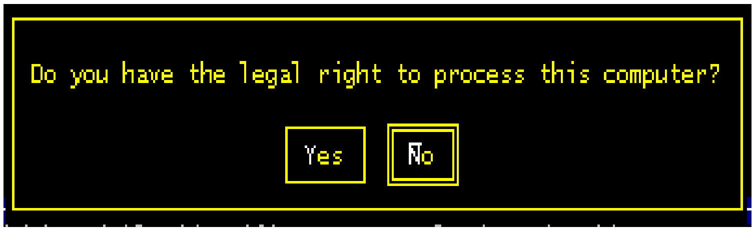
5. A message will appear asking **"Have you read the instruction manual?"**



Have you read the instruction manual?

If you have read this User's Guide, press "**Y"** for yes to continue.

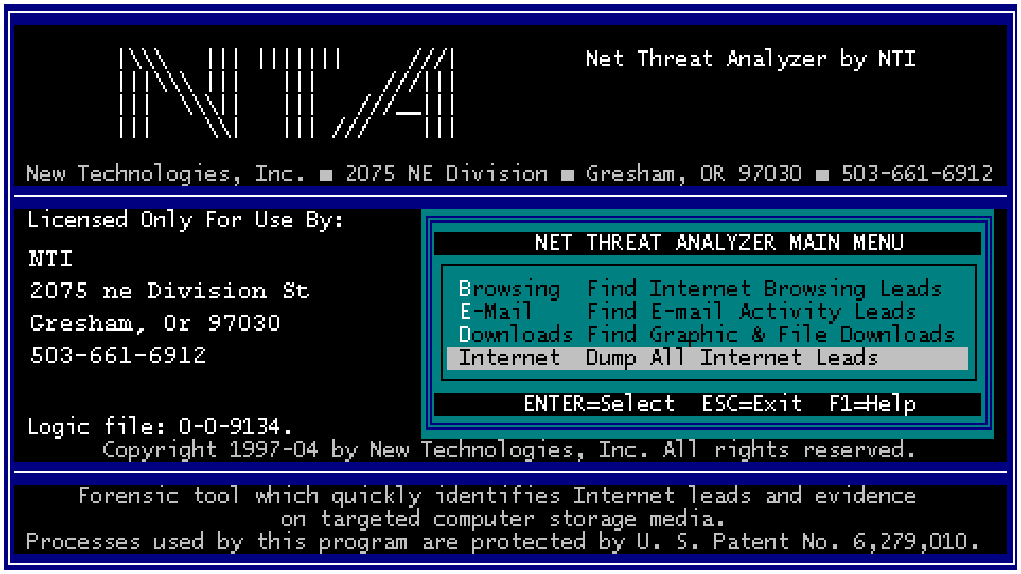
6. Another message will appear asking **"Do you have the legal right to process this computer?"**



Do you have the legal right to process this computer?

If you do, press **"Y"** for yes to continue.

7. The list of available options will appear as the screen below depicts.



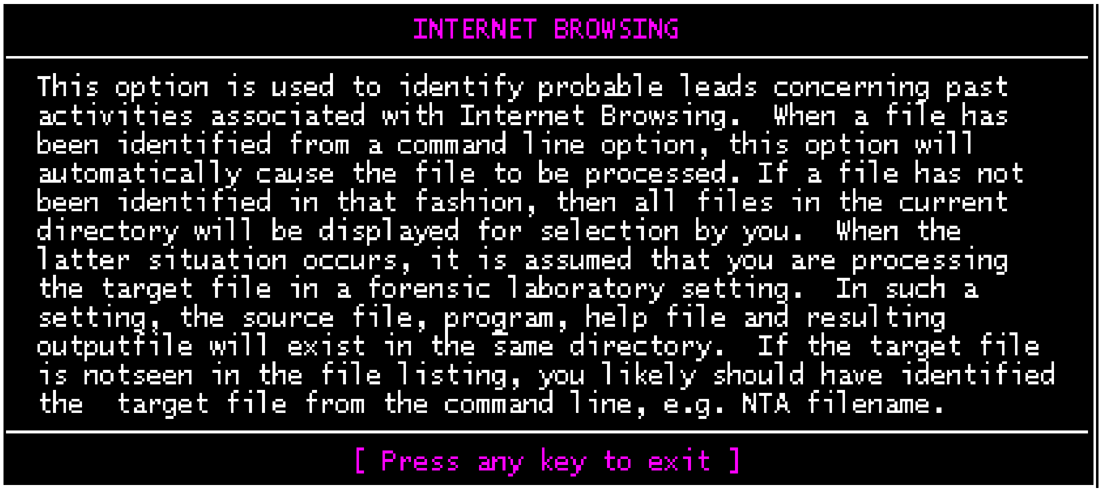
```
                                          Net Threat Analyzer by NTI

New Technologies, Inc. ■ 2075 NE Division ■ Gresham, OR 97030 ■ 503-661-6912

Licensed Only For Use By:          NET THREAT ANALYZER MAIN MENU
NTI
2075 ne Division St              Browsing  Find Internet Browsing Leads
Gresham, Or 97030                E-Mail    Find E-mail Activity Leads
503-661-6912                     Downloads Find Graphic & File Downloads
                                 Internet  Dump All Internet Leads

                                   ENTER=Select  ESC=Exit  F1=Help
Logic file: 0-0-9134.
      Copyright 1997-04 by New Technologies, Inc. All rights reserved.

     Forensic tool which quickly identifies Internet leads and evidence
                     on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
```

The System Menu options are selected by highlighting the desired option and then pressing the **Enter** key. The list of available System Menu options is as follows:

1	**Browsing**	**Find Internet Browsing Leads (/auto1)**
2	**E-Mail**	**Find E-mail Activity Leads (/auto2)**
3	**Downloads**	**Find Graphic & File Downloads (/auto3)**
4	**Internet**	**Dump All Internet Leads (/auto4)**

These options correspond with the **/auto1, /auto2, /auto3** and **/auto4** command options as discussed in previous subsections.

If you have a question about any of these options, you can highlight the desired item and press the **<F1>** key on the keyboard to get help on the specific System Menu option as illustrated in the graphic below.

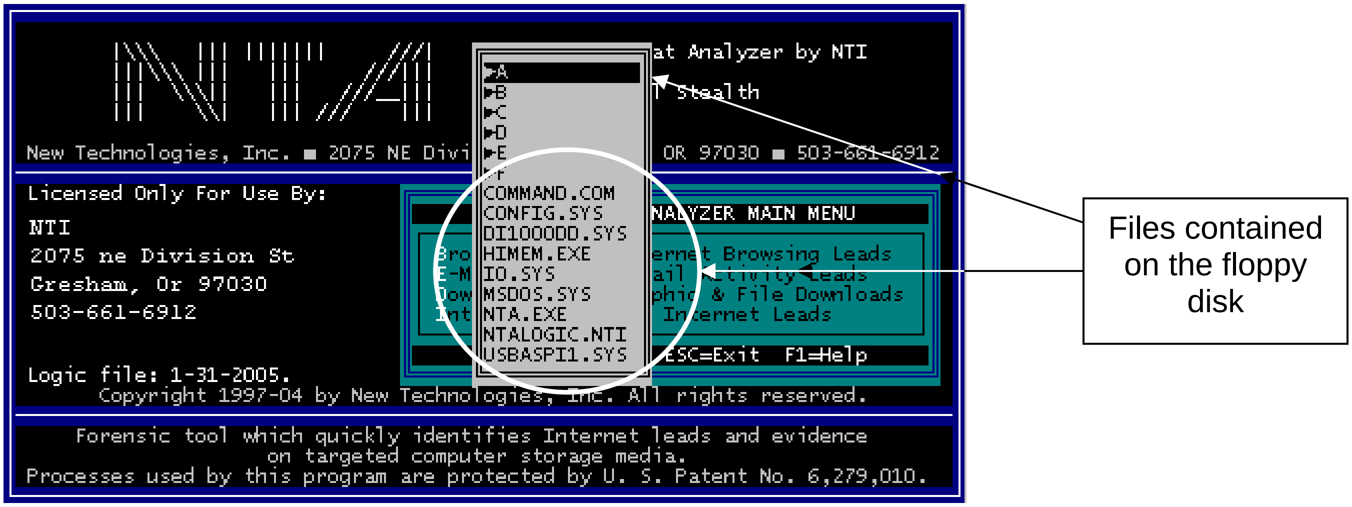


```
                         INTERNET BROWSING

 This option is used to identify probable leads concerning past
 activities associated with Internet Browsing.  When a file has
 been identified from a command line option, this option will
 automatically cause the file to be processed. If a file has not
 been identified in that fashion, then all files in the current
 directory will be displayed for selection by you.  When the
 latter situation occurs, it is assumed that you are processing
 the target file in a forensic laboratory setting.  In such a
 setting, the source file, program, help file and resulting
 outputfile will exist in the same directory.  If the target file
 is notseen in the file listing, you likely should have identified
 the  target file from the command line, e.g. NTA filename.

                      [ Press any key to exit ]
```

The above screen is displayed when the first option of **"Browsing"** is highlighted and then the **<F1>** key on the keyboard is pressed.

Pressing the **<ESC>** key on the keyboard will allow you to stop and exit the program or to move one step back in the NTA Stealth™ program processes.

8. After the System Menu option has been selected, NTA Stealth™ will list all of the files located in the current path of the drive highlighted.   Below is an example of highlighting the number **4** option of **"Internet – Dump All Internet Leads."**



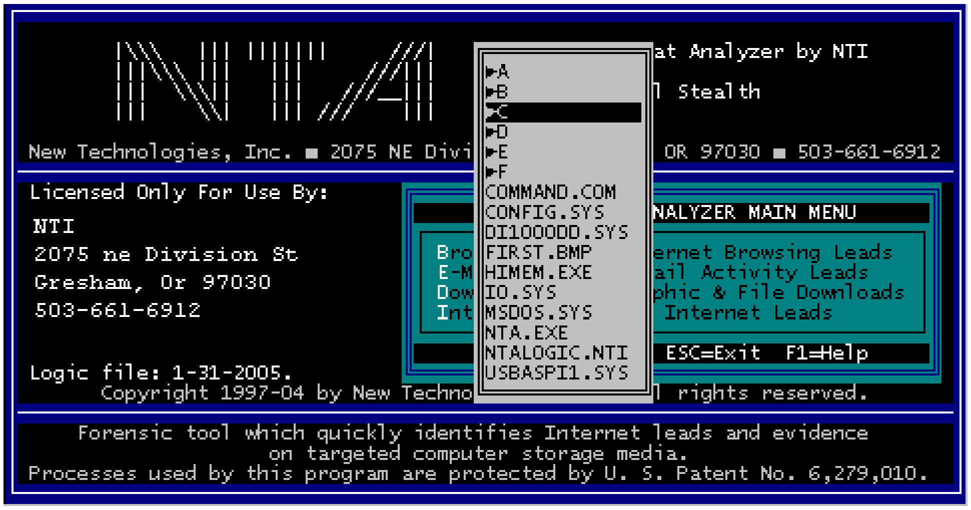
```
                                          at Analyzer by NTI
                                  ►A
                                  ►B      T Stealth
                                  ►C
                                  ►D
 New Technologies, Inc. ■ 2075 NE Divi►E  OR 97030 ■ 503-661-6912
                                  ►F
 Licensed Only For Use By:        COMMAND.COM
                                  CONFIG.SYS  NALYZER MAIN MENU
 NTI                              DI1000DD.SYS
 2075 ne Division St          Bro HIMEM.EXE   ernet Browsing Leads
 Gresham, Or 97030            E-M IO.SYS      ail Activity Leads
 503-661-6912                 Dow MSDOS.SYS   phic & File Downloads
                              Int NTA.EXE      Internet Leads
                                  NTALOGIC.NTI
 Logic file: 1-31-2005.           USBASPI1.SYS ESC=Exit  F1=Help
     Copyright 1997-04 by New Technologies, Inc. All rights reserved.

      Forensic tool which quickly identifies Internet leads and evidence
                        on targeted computer storage media.
 Processes used by this program are protected by U. S. Patent No. 6,279,010.
```

Files contained on the floppy disk

Notice how the **"A"** is highlighted. The fly out panel shows the files that are contained in the A (floppy disk) drive.

The target file can be identified from the list of displayed files. If a large volume of files are listed, you can scroll through the file listing using the up and down arrow keys until the target file has been located.

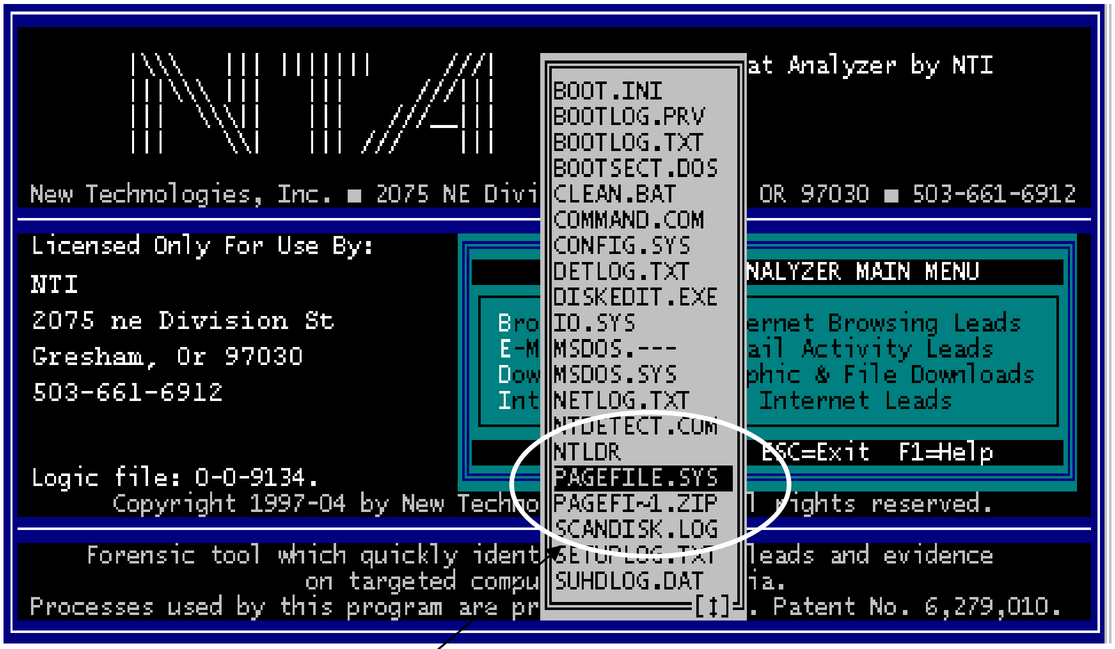
For instance if your intent is to process the pagefile.sys file, it may be located on the **"C"** volume. Then you would scroll to **"C"** using the arrow keys until highlighted and then press the **ENTER** key to begin searching for the file.



```
                                       ►A        at Analyzer by NTI
                                       ►B        ] Stealth
                                       ►C
                                       ►D
New Technologies, Inc. ■ 2075 NE Divi  ►E          OR 97030 ■ 503-661-6912
                                       ►F
Licensed Only For Use By:              COMMAND.COM
                                       CONFIG.SYS  NALYZER MAIN MENU
NTI                                    DI1000DD.SYS
2075 ne Division St               Bro  FIRST.BMP   ernet Browsing Leads
Gresham, Or 97030                 E-M  HIMEM.EXE   ail Activity Leads
503-661-6912                      Dow  IO.SYS      phic & File Downloads
                                  Int  MSDOS.SYS     Internet Leads
                                       NTA.EXE
                                       NTALOGIC.NTI  ESC=Exit  F1=Help
Logic file: 1-31-2005.                 USBASPI1.SYS
     Copyright 1997-04 by New Techno               l rights reserved.

     Forensic tool which quickly identifies Internet leads and evidence
                     on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
```

Scroll to desired drive letter and then press **ENTER** to reveal contents of drive

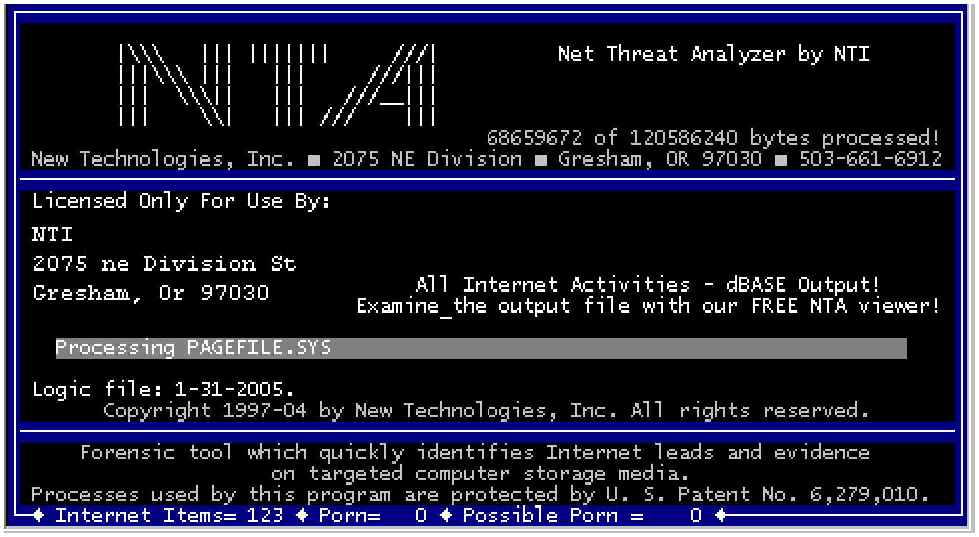
9. Once the file to be processed has been located, highlight the file and press the **ENTER** key to begin processing.



```
                                          at Analyzer by NTI
New Technologies, Inc. ■ 2075 NE Divi       OR 97030 ■ 503-661-6912
Licensed Only For Use By:
NTI
2075 ne Division St
Gresham, Or 97030
503-661-6912

Logic file: 0-0-9134.
      Copyright 1997-04 by New Techno        l rights reserved.
    Forensic tool which quickly ident       leads and evidence
               on targeted compu            ia.
Processes used by this program are pr       . Patent No. 6,279,010.
```

- ➢ Locate the file
- ➢ Highlight the file
- ➢ Press **ENTER**

10. NTA Stealth™ will process the file according to one of the four commands that you previously selected as the screen below depicts.



```
                                                  Net Threat Analyzer by NTI

                                          68659672 of 120586240 bytes processed!
New Technologies, Inc. ■ 2075 NE Division ■ Gresham, OR 97030 ■ 503-661-6912

Licensed Only For Use By:
NTI
2075 ne Division St
Gresham, Or 97030                    All Internet Activities - dBASE Output!
                                 Examine_the output file with our FREE NTA viewer!

  Processing PAGEFILE.SYS

Logic file: 1-31-2005.
      Copyright 1997-04 by New Technologies, Inc. All rights reserved.

    Forensic tool which quickly identifies Internet leads and evidence
                     on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
♦ Internet Items= 123 ♦ Porn=    0 ♦ Possible Porn =    0 ♦
```

Pornography-Based Internet Activity in a Targeted File

If your intent is to limit the leads to identify ***only*** the pornography-based Internet activities identified in a targeted file such as the pagefile.sys file example above, then the complete path or location of the file must be known for NTA Stealth™ to be able to process the file using the **filename** command.

For instance, if you intend to capture all the Internet web sites and email activity associated with pornography and possible pornography content, then you would use the following command line syntax at the DOS prompt:

```
nta c:\pagefile.sys /auto4 /porn
```

Please note that you cannot use the NTA Stealth™ filename option with the **/h, /skip** or **/end** command line switches because those commands relate to the processing of the physical hard drive. However, you must include in the syntax the **complete path of the file** that you wish to process.

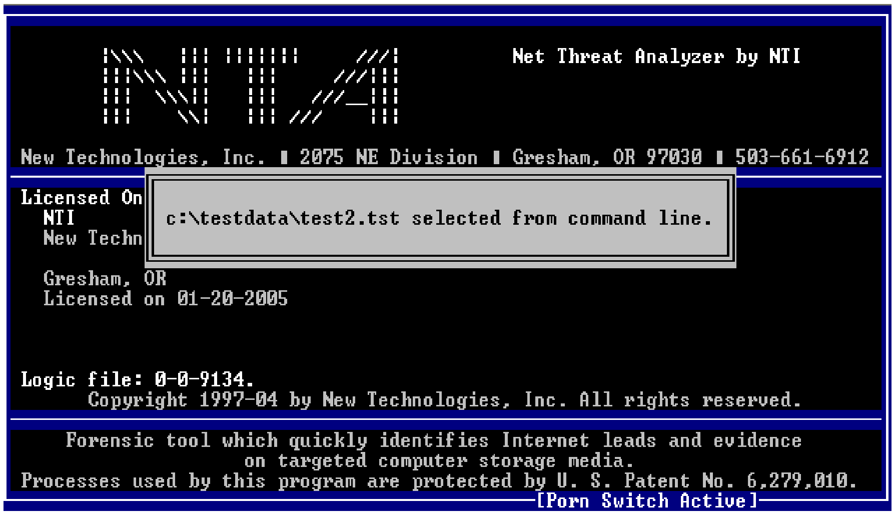
Therefore, when using NTA Stealth's™ filename option, if you wish to process a file that is located within a folder on a specific volume or drive, then the entire path must be typed at the command prompt which would include the volume on the hard drive where the file is located, the folder and the filename.

As an example, consider the name of the file to be processed is **"test2.tst"** and it resides within the folder **"testdata"** on the **C:** volume of a hard drive. You want to limit the leads to pornography-based Internet and email activity. The syntax would be:

```
nta c:\testdata\test2.tst /auto4 /porn
```

Use the following instructions to process the "**test2.tst**" with the previous command syntax.

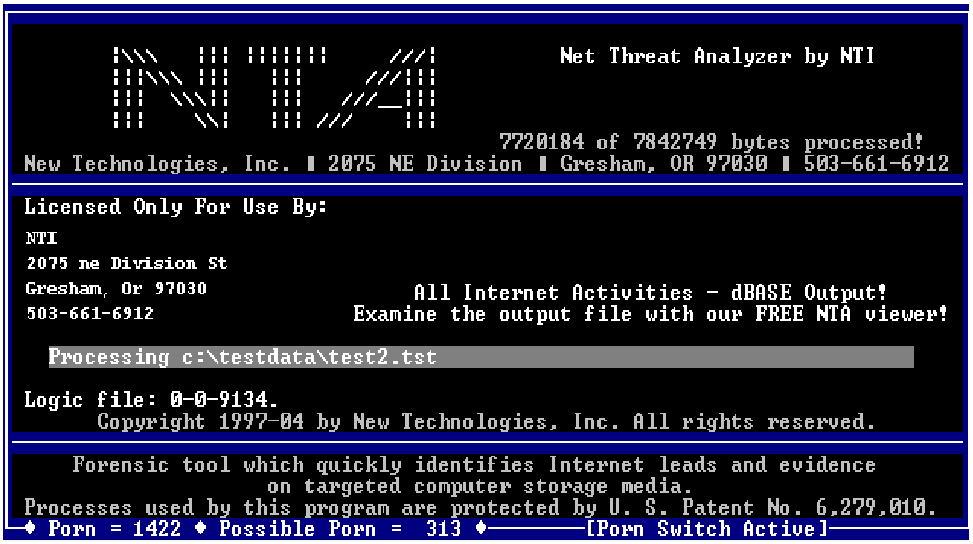
1. After pressing **Enter**, the following screen will appear confirming your command.



```
                                            Net Threat Analyzer by NTI

New Technologies, Inc. ▮ 2075 NE Division ▮ Gresham, OR 97030 ▮ 503-661-6912

Licensed On
  NTI          c:\testdata\test2.tst selected from command line.
  New Techn

  Gresham, OR
  Licensed on 01-20-2005


Logic file: 0-0-9134.
      Copyright 1997-04 by New Technologies, Inc. All rights reserved.

    Forensic tool which quickly identifies Internet leads and evidence
                    on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
                                               [Porn Switch Active]
```

2. You may either press **Enter** again or wait 10 seconds for the program to begin.

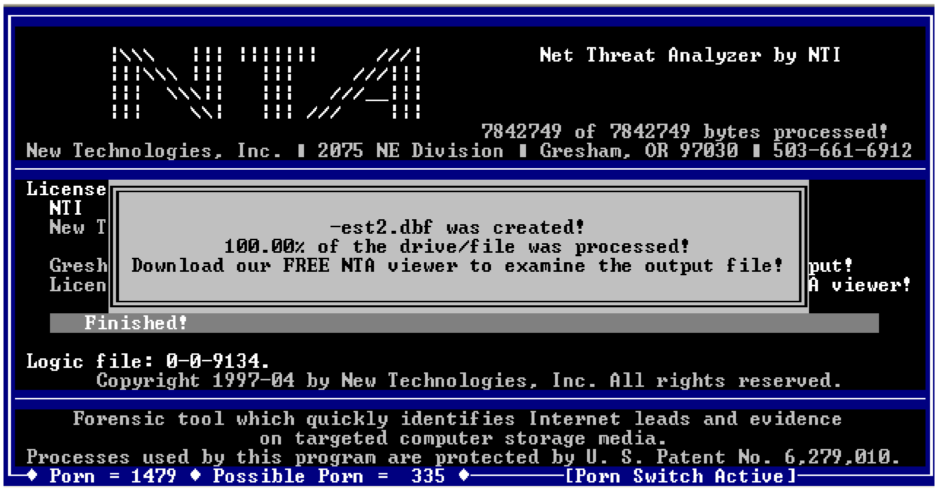
Notice the **"Porn Switch Active"** option displayed near the lower right-hand corner of the screen in the illustration below. This indicates that ***ONLY*** pornography-based and possible pornography-based content will be identified.



```
                                              Net Threat Analyzer by NTI

                                          7720184 of 7842749 bytes processed!
New Technologies, Inc. ▮ 2075 NE Division ▮ Gresham, OR 97030 ▮ 503-661-6912
Licensed Only For Use By:
NTI
2075 ne Division St
Gresham, Or 97030                        All Internet Activities - dBASE Output!
503-661-6912                         Examine the output file with our FREE NTA viewer!

  Processing c:\testdata\test2.tst

Logic file: 0-0-9134.
      Copyright 1997-04 by New Technologies, Inc. All rights reserved.
     Forensic tool which quickly identifies Internet leads and evidence
                     on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
♦ Porn = 1422 ♦ Possible Porn =  313 ♦────────[Porn Switch Active]
```

Pornography-based leads only

3. When the processing is complete, a message will appear for 10 seconds stating the name of the output file that was created and what percentage of the drive or file was completed and processed (See example screen below). NTA Stealth™ will automatically create an output fie with a name similar to the source file that was processed.

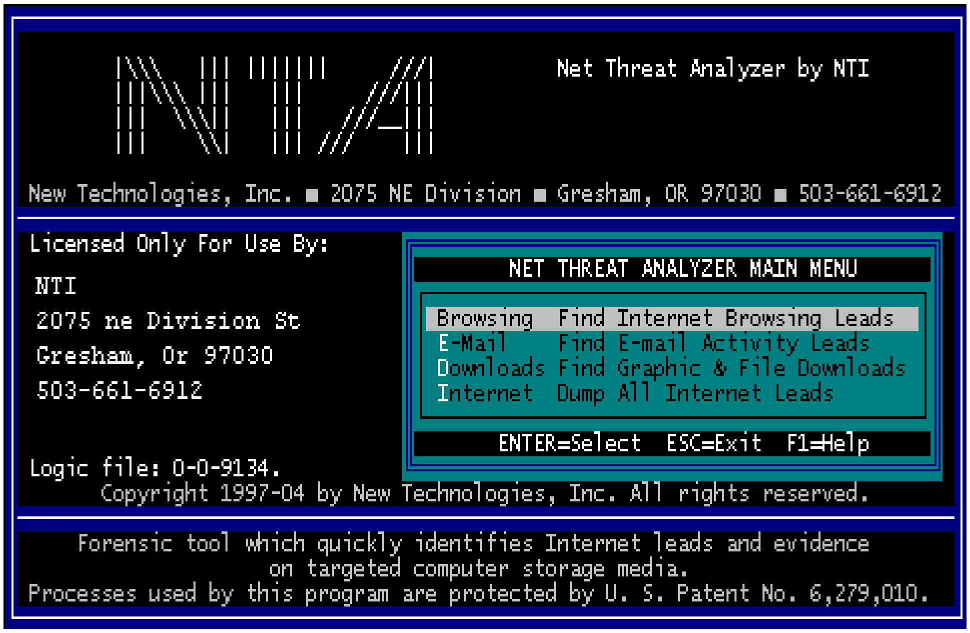


```
                                             Net Threat Analyzer by NTI

                                         7842749 of 7842749 bytes processed!
New Technologies, Inc. ▮ 2075 NE Division ▮ Gresham, OR 97030 ▮ 503-661-6912
License
  NTI
  New T                  -est2.dbf was created!
                 100.00% of the drive/file was processed!
  Gresh  Download our FREE NTA viewer to examine the output file!  put!
  Licen                                                            A viewer!
   Finished!

Logic file: 0-0-9134.
      Copyright 1997-04 by New Technologies, Inc. All rights reserved.
     Forensic tool which quickly identifies Internet leads and evidence
                     on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
♦ Porn = 1479 ♦ Possible Porn =  335 ♦────────[Porn Switch Active]
```

4. **If an option is not chosen**, such /auto1 or /auto2, at the command line, then the NTA Stealth™ Screen Menu will prompt you to choose an option. Using the example above and by typing the syntax below at the command prompt:

```
nta c:\testdata\test2.tst
```

the following screen will appear because you did not choose an option such as /auto1, /auto2, /auto3 or /auto4 .



```
                                       Net Threat Analyzer by NTI

New Technologies, Inc. ■ 2075 NE Division ■ Gresham, OR 97030 ■ 503-661-6912

Licensed Only For Use By:
NTI
2075 ne Division St
Gresham, Or 97030
503-661-6912

                                   NET THREAT ANALYZER MAIN MENU

                                  Browsing  Find Internet Browsing Leads
                                  E-Mail    Find E-mail Activity Leads
                                  Downloads Find Graphic & File Downloads
                                  Internet  Dump All Internet Leads

                                  ENTER=Select  ESC=Exit  F1=Help
Logic file: 0-0-9134.
     Copyright 1997-04 by New Technologies, Inc. All rights reserved.

    Forensic tool which quickly identifies Internet leads and evidence
                     on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
```

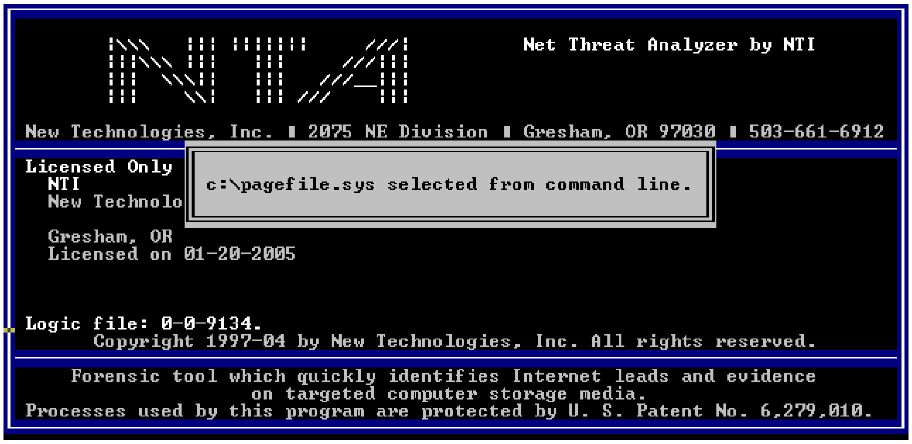
Using the **arrow keys** on the keyboard, scroll to the desired option and then press **Enter.**

This will start the program to process the entire command.

Below is example syntax to process a page file on the **C:** volume of a hard drive at the DOS prompt:

```
nta c:\pagefile.sys /auto4
```

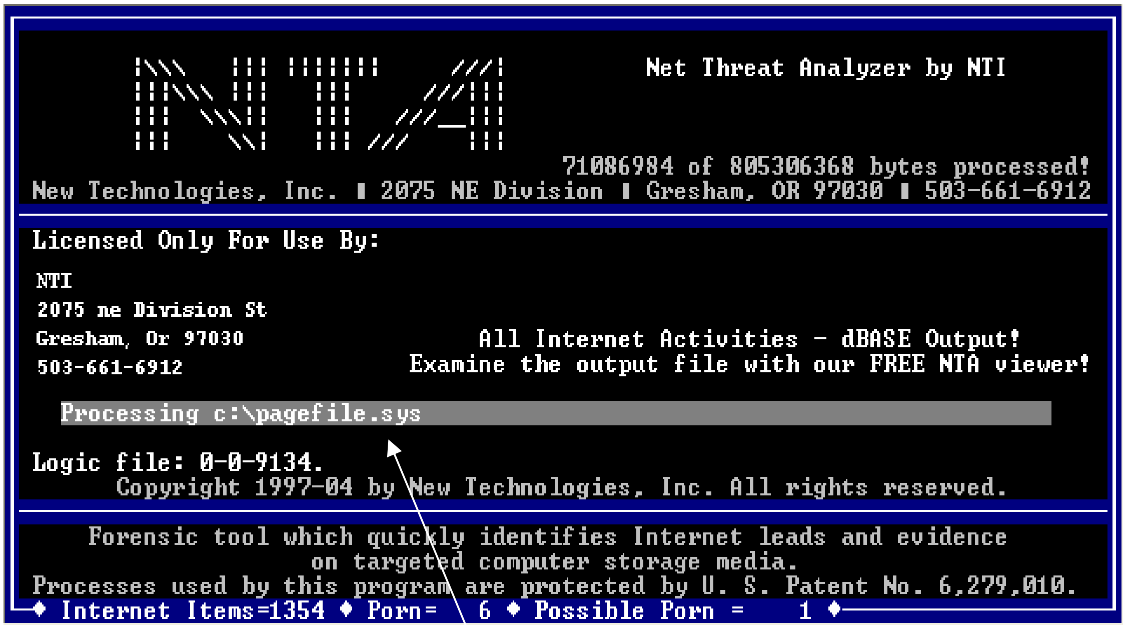
5. After typing the above command and pressing **ENTER**, a message confirming your choice will appear on the screen such as the example below.



```
                                                     Net Threat Analyzer by NTI

New Technologies, Inc. ▌ 2075 NE Division ▌ Gresham, OR 97030 ▌ 503-661-6912
Licensed Only
  NTI          c:\pagefile.sys selected from command line.
  New Technolo

  Gresham, OR
  Licensed on 01-20-2005


Logic file: 0-0-9134.
      Copyright 1997-04 by New Technologies, Inc. All rights reserved.

    Forensic tool which quickly identifies Internet leads and evidence
                    on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
```

6. You may either press **ENTER** again or wait 10 seconds for the program to begin. The NTA Stealth™ screen will appear confirming your command such as the message below.

"Processing c:\pagefile.sys"

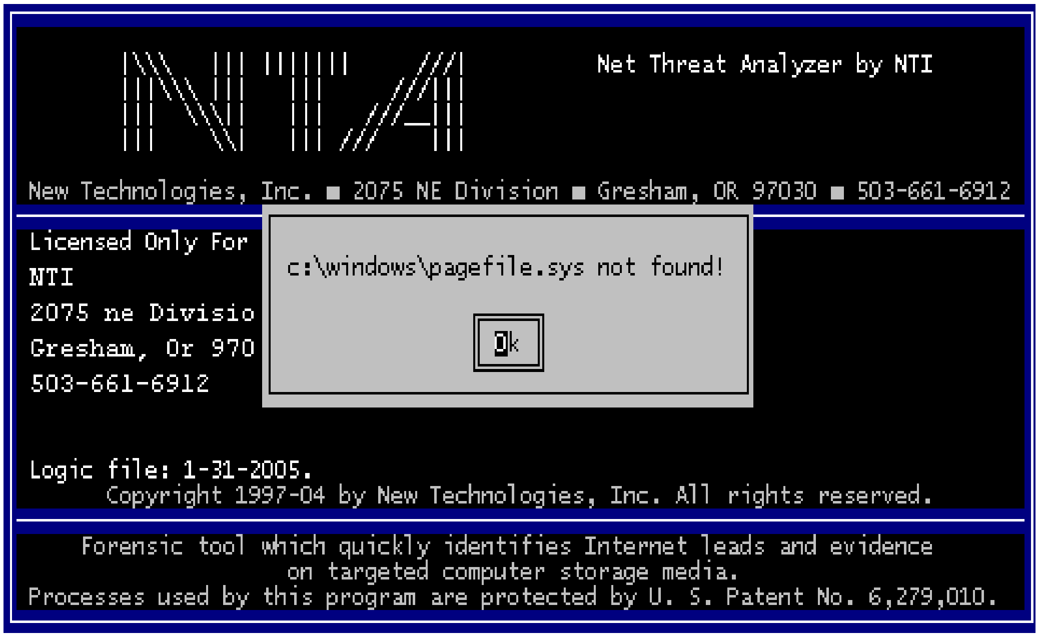


```
                                                  Net Threat Analyzer by NTI

                                              71086984 of 805306368 bytes processed!
New Technologies, Inc. ▌ 2075 NE Division ▌ Gresham, OR 97030 ▌ 503-661-6912

Licensed Only For Use By:

NTI
2075 ne Division St
Gresham, Or 97030                    All Internet Activities - dBASE Output!
503-661-6912                     Examine the output file with our FREE NTA viewer!

  Processing c:\pagefile.sys

Logic file: 0-0-9134.
      Copyright 1997-04 by New Technologies, Inc. All rights reserved.

    Forensic tool which quickly identifies Internet leads and evidence
                    on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
♦ Internet Items=1354 ♦ Porn=   6 ♦ Possible Porn =    1 ♦
```

Processing a single source file

7. The **/auto4** option used in the above example processes the targeted file to identify leads associated with past Internet web browsing and email activities. Please remember that the **complete path** of the file must be specified in order for NTA Stealth™ to process when typed manually on the DOS command line.

8. If the path of the file is incorrect, an error message will appear such as in the example below.



```
Net Threat Analyzer by NTI
New Technologies, Inc. ■ 2075 NE Division ■ Gresham, OR 97030 ■ 503-661-6912
Licensed Only For
NTI
2075 ne Divisio
Gresham, Or 970
503-661-6912

c:\windows\pagefile.sys not found!

Logic file: 1-31-2005.
     Copyright 1997-04 by New Technologies, Inc. All rights reserved.
    Forensic tool which quickly identifies Internet leads and evidence
                    on targeted computer storage media.
Processes used by this program are protected by U. S. Patent No. 6,279,010.
```

9. After pressing the **ENTER** key, the program will exit and return to the **A:\>** drive in the DOS prompt. At this point, you may re-type the command using the correct path location, or use the **System Menu** to pinpoint the exact location.

Analyzing and Viewing NTA Stealth™ Output

NTA Stealth™ output files are written in dBase III Plus format and are always include .dbf extensions. This dBase III Plus format was chosen because it can be read and analyzed with several commercially available computer applications, e.g., Microsoft Access, Microsoft Excel, Lotus, Quattro, etc. However, we recommend you use NTA Viewer™ to analyze the output files.

NTA Viewer™ was specifically developed by NTI to analyze and view NTA Stealth™ leads. NTA Stealth™ has identified more than two million email addresses and more than one million Internet web site address on single hard drives. These large volumes of leads could overwhelm a program like Microsoft Excel and the problem is magnified when NTA Stealth™ data are combined from the processing of multiple computer systems owned by the same individual.

If your computer is connected to the Internet, NTA Viewer™ allows you to view the web sites that were identified by NTA Stealth™ as possible leads with a simple click of the mouse. When viewing web sites on the Internet, we suggest that you select an Internet browser for your computer that will block popups and spyware. One such browser that does not allow popups and spyware is the Mozilla Firefox browser. You can download this browser free of charge by going to:

http://www.mozilla.org

NTA Viewer™ is Windows-based and can deal with essentially any volume of leads identified by NTA Stealth™ from processing one or more computer hard disk drives. It was designed to be a sophisticated analysis tool while providing robust report writing capabilities. NTA Viewer™ is a Windows-based program.

NTA Stealth™ also produces an **Evidence Log File** that corresponds to each .dbf output file. This log file contains information involving the specifics of that particular operation as further discussed in the following subsection **"NTA Stealth™ Evidence Log File".**

NTA Stealth™ Output File Names

1. When NTA Stealth™ is used to identify Internet **web browsing** leads by with the **/auto1** command option, the first character of the output file will be the underscore, i.e., "_", followed by "NTA". The **1** or **0** after the **"H"** for each of the .dbf files depicts which hard drive on the evidence computer that was searched; **H0** for the first physical hard drive and **H1** for the second drive. The output file extension for all the command options is always **.dbf.**

   Example: **_NTAH1.DBF**

2. When the **email leads** are identified by using the **/auto2** command option, the first character of the output file will be an **"M"**, followed by "NTA". The "**H0**" designation depicts which hard drive on the evidence computer that was searched. In this instance, NTA Stealth™ searched all or a portion of the first hard drive on the evidence computer.

   Example: **MNTAH0.DBF**

3. When NTA Stealth™ is used to identify **graphic files** downloaded from the Internet with the **/auto3** command option, the first character of the output file will be the tilde, tilde, i.e. "~", followed by "NTA". The "**H1**" designation depicts which hard drive on the evidence computer that will be searched. In this instance, NTA Stealth™ searched all or a portion of the second physical hard drive on the evidence computer.

   Example: **~NTAH1.DBF**

4. When NTA Stealth™ is used to identify **Internet-related** leads stored on a hard drive with the **/auto4** command option, the first character of the output file will be a hyphen, i.e., "**-**", followed by "NTA". The "**H0**" designation depicts which hard drive on the evidence computer that will be searched. In this instance, NTA Stealth™ searched all or a portion of the first hard drive on the evidence computer.

   Example: **-NTAHO.DBF**

5. When NTA Stealth™ is used to process **single source files** such as a Windows page file, it will automatically create an output file with a name similar to the source file.

   Example: **pagefile.dbf**

NTA Stealth™ Evidence Log File

NTA Stealth™ produces an evidence log file at the same time that an NTA Stealth™ output file is generated. The evidence log file contains the following information:

- The NTA Stealth™ version number
- The information of the licensee such as name, company and address
- The NTALOGIC.NTI logic file version used
- The date and time the process started
- The command line that was utilized to run NTA Stealth™
- The number of hard drives on the computer and which one was selected
- The number of items identified by NTA Stealth™ as leads
- The name of the NTA Stealth™ file created with a **.dbf** extension
- The percentage of the hard drive that was processed
- The termination and/or completion date and time

Below is an example of an NTA Stealth™ evidence log file:

```
NTA Version 7.0 NTI Technologies, Inc. (c) 2005

Licensed to:
NTI
New Technology, Inc.
2075 ne Division St
Gresham, OR
503-661-6912
Licensed on 01-20-2005

Logic file version: -32768 (0-0-9134)

Process started on: Fri Jan 21 14:45:32 2005

Command Line Issued: \NTA.EXE /h0 /auto1 /porn

This system has 2 hard drive(s).
Hard drive H0 was selected. It has 2502308 sectors.

/Porn switch was specified.

Items found: 4579  Porn: 4107  Possible Porn: 472

dBase file: _NTAH0.dbf created.

100.00% of the drive/file was processed!

Process terminated on: Fri Jan 21 15:39:46 2005
```

The evidence log file will also state whether the process was aborted by the user and cite the date and time of that termination as in the following example:

```
62.21% of the drive/file was processed!
Process aborted by user on: Mon Jan 24 11:10:39 2005
```

If you ran NTA Stealth™ using the NTA Stealth™ Test Disk and the output generated required more than one floppy disk, then this action will also be noted and documented in the evidence log file. Each floppy disk will have its own evidence log file until you terminate the process or when NTA Stealth™ completely processes the drive or file.

NTA Viewer™ Instructions

Opening NTA Viewer™ and Accessing NTA Stealth™ Output Files

NTA Viewer™ is a specialized Microsoft Windows-based software tool designed to provide easy and quick analysis of NTA Stealth™ output generated. Use the following instructions to run NTA Viewer™.

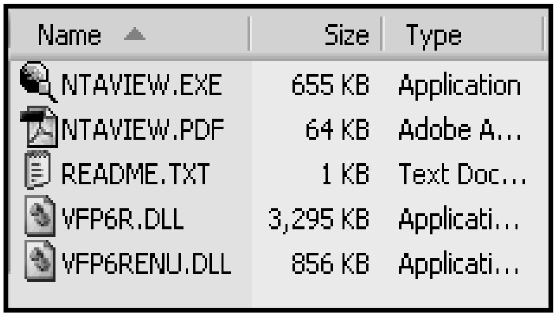
1. Insert the NTA Support CD into the CD-ROM drive of your computer.

2. Double click on "My Computer" on the desktop your Windows operating system (or select "Start" on your Task Bar in the lower left-hand corner of the desktop and then click on "My Computer") and click on the CD-ROM drive to view the various files contained on the NTA Stealth™ Support CD.

3. Locate the folder titled "**ntaview**."

4. Copy the **"ntaview**" folder located on the NTA Support CD to your computer's desktop for easy access by right clicking on the "ntaview" folder and then selecting "Copy from the fly-out panel. Then paste the "ntaview" folder to your desktop by clicking on "Paste" from the fly-out panel.

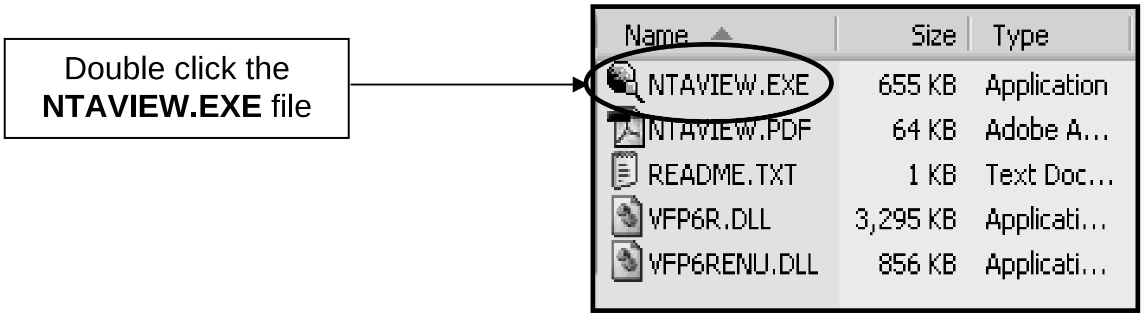
5. Double click the **"ntaview**" folder on your desktop. You should see the following files:



Name	Size	Type
NTAVIEW.EXE	655 KB	Application
NTAVIEW.PDF	64 KB	Adobe A...
README.TXT	1 KB	Text Doc...
VFP6R.DLL	3,295 KB	Applicati...
VFP6RENU.DLL	856 KB	Applicati...

The **NTAVIEW.EXE** and the **VFP6R.DLL** and **VFP6RENU.DLL** files **must** remain in the same folder in order to operate NTA Viewer™.

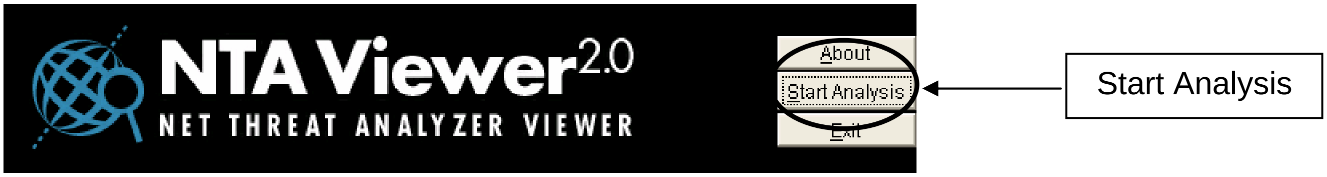
6. Double click on the **NTAVIEW.EXE** file in the **ntaview** folder.



Double click the **NTAVIEW.EXE** file

Name	Size	Type
NTAVIEW.EXE	655 KB	Application
NTAVIEW.PDF	64 KB	Adobe A...
README.TXT	1 KB	Text Doc...
VFP6R.DLL	3,295 KB	Applicati...
VFP6RENU.DLL	856 KB	Applicati...

This will launch the NTA Viewer™ 2.0 start screen. Click on the **"Start Analysis"** button on the upper right hand side of the Viewer.

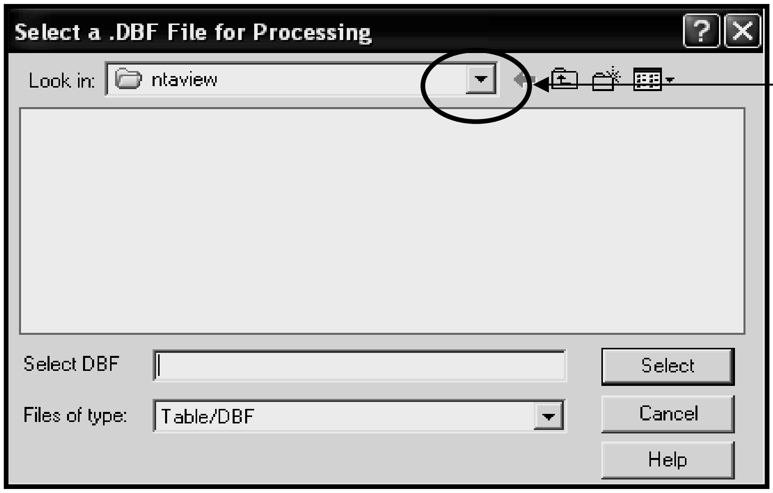


Start Analysis

7. Upon clicking the "**Start Analysis"** button, a box will appear prompting you to choose an NTA Stealth™ file to process as in the "**Select a .dbf File for Processing**" window illustrated below. Click on the drop down arrow in the "**Look in:**" box to locate and choose the NTA Stealth™ .dbf output file you wish to analyze.

If you ran NTA Stealth™ using the NTA Stealth™ Test Disk, insert the disk into the floppy drive and click on the **A:\** in the "**Look in:**" box to identify the NTA Stealth™ output files you would like to analyze.

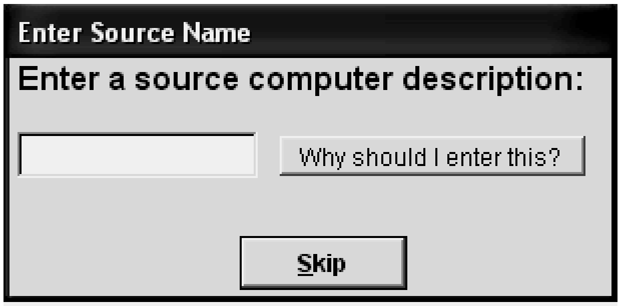
If you ran NTA Stealth™ from the NTA Stealth™ USB Thumb Drive, insert the NTA Stealth™ USB Thumb Drive into the USB port of your computer and click on the appropriate drive designation in the "**Look in:**" box to identify the location of the NTA Stealth™ output file that you would like to analyze.



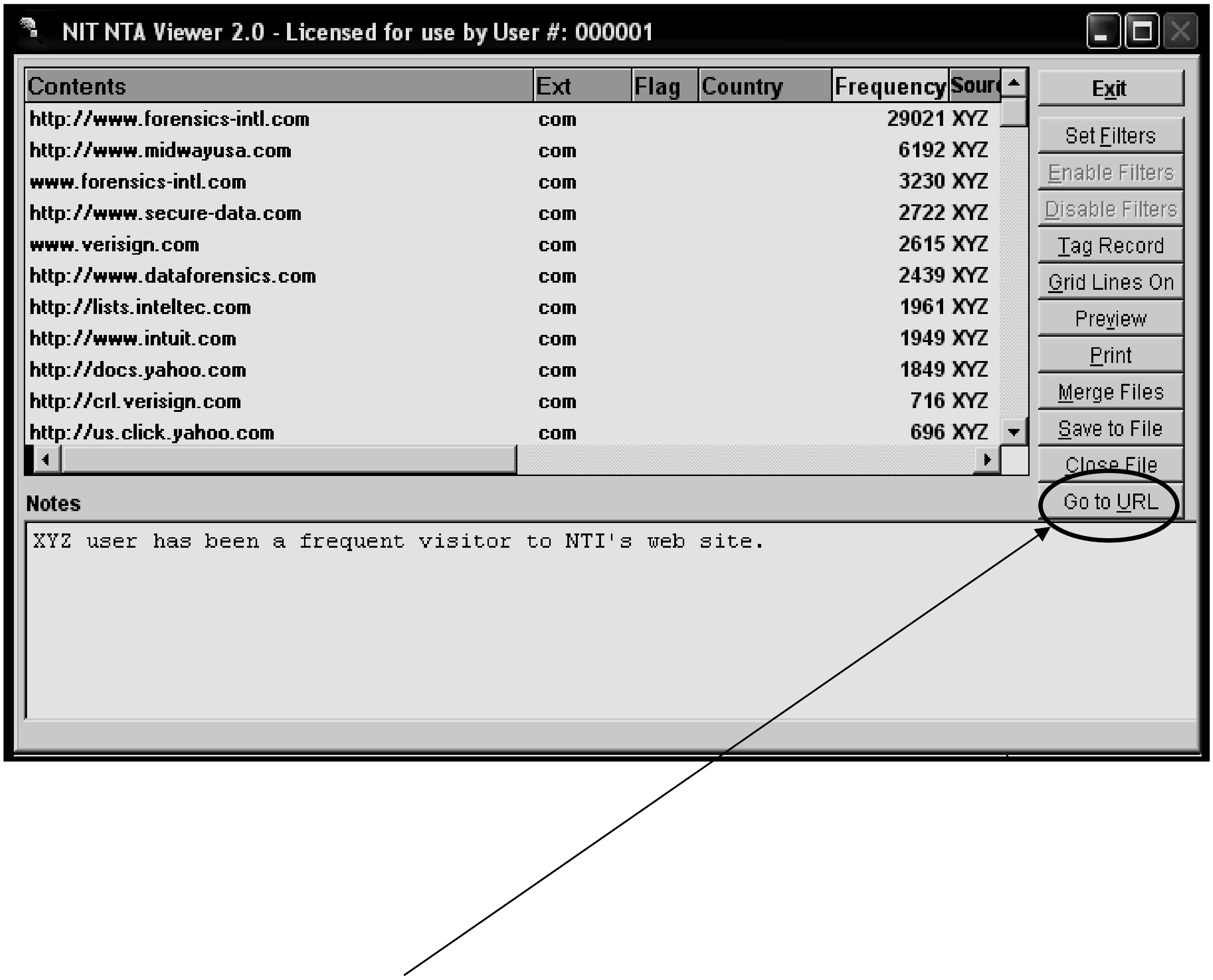
Locate the NTA-Stealth .dbf output

8. After locating and choosing the .dbf file you wish to process, an "Enter Source Name" box will appear prompting you to type in a **"Source Name"** for the file. You can either type in a name or description in the box or skip this step.

   It is advantageous to specify a name or description of the computer from which the selected output file was created when you are analyzing files from multiple computers.



9. Below is an example of a **_NTAH1.dbf** file using the **/auto1** option on the DOS command line for Internet web (URL) leads captured by NTA Stealth™ for analyzes.

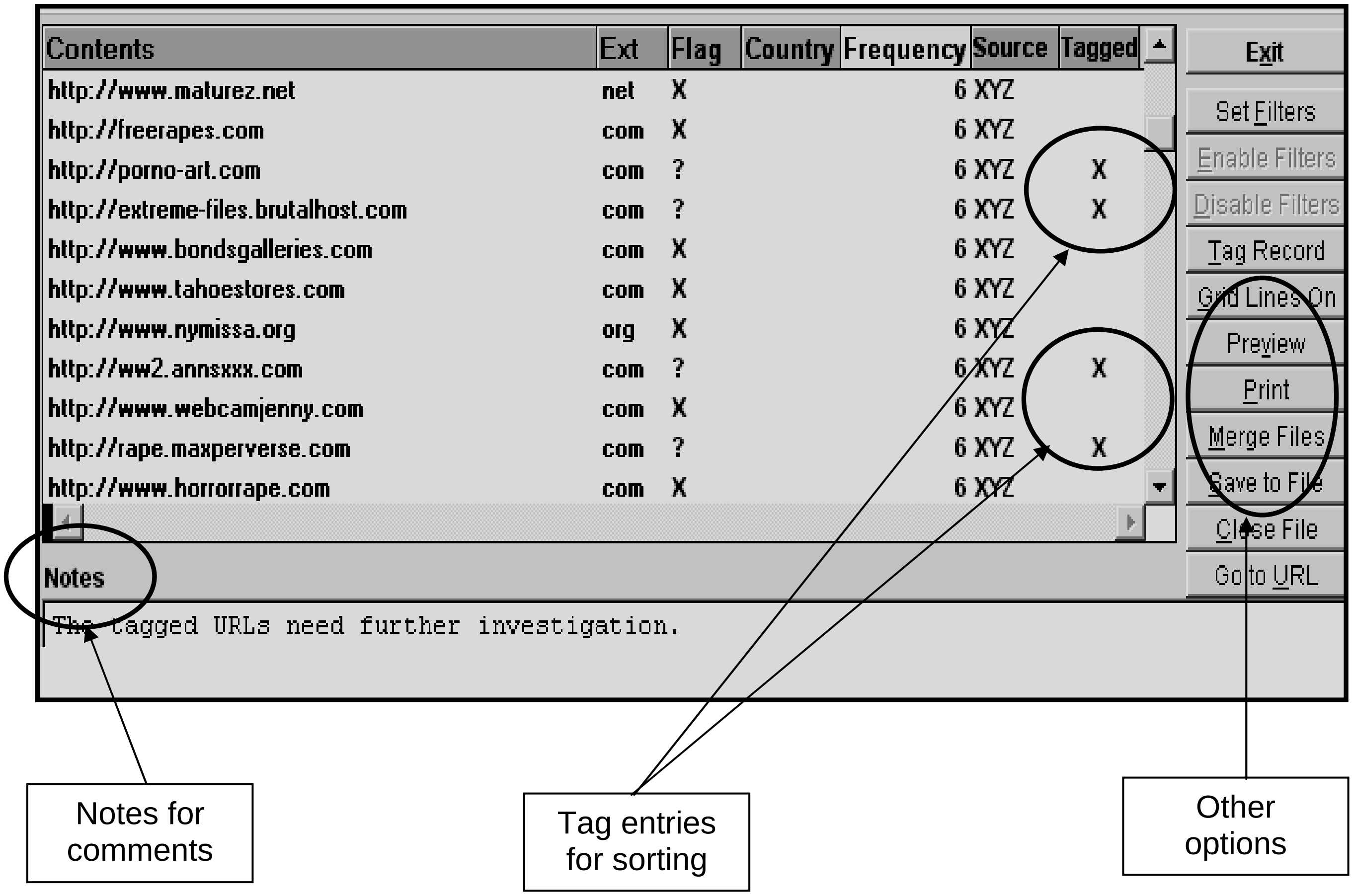


Contents	Ext	Flag	Country	Frequency	Sour
http://www.forensics-intl.com	com			29021	XYZ
http://www.midwayusa.com	com			6192	XYZ
www.forensics-intl.com	com			3230	XYZ
http://www.secure-data.com	com			2722	XYZ
www.verisign.com	com			2615	XYZ
http://www.dataforensics.com	com			2439	XYZ
http://lists.inteltec.com	com			1961	XYZ
http://www.intuit.com	com			1949	XYZ
http://docs.yahoo.com	com			1849	XYZ
http://crl.verisign.com	com			716	XYZ
http://us.click.yahoo.com	com			696	XYZ

```
XYZ user has been a frequent visitor to NTI's web site.
```

If your computer is connected to the Internet, just highlight one of the URLs and then click on **"Go to URL"** button on the right hand side of NTA Viewer™. This will open your default web browser and take you to the selected Internet web site.

10. The following screen is an example of a **MNTAH0.dbf** file from using the **/auto2** option on the DOS command line for Internet email leads captured by NTA Stealth™ for analysis.



Contents	Ext	Flag	Country	Frequency	Source	Tagged
http://www.maturez.net	net	X		6	XYZ	
http://freerapes.com	com	X		6	XYZ	
http://porno-art.com	com	?		6	XYZ	X
http://extreme-files.brutalhost.com	com	?		6	XYZ	X
http://www.bondsgalleries.com	com	X		6	XYZ	
http://www.tahoestores.com	com	X		6	XYZ	
http://www.nymissa.org	org	X		6	XYZ	
http://ww2.annsxxx.com	com	?		6	XYZ	X
http://www.webcamjenny.com	com	X		6	XYZ	
http://rape.maxperverse.com	com	?		6	XYZ	X
http://www.horrorrape.com	com	X		6	XYZ	

Notes

The tagged URLs need further investigation.

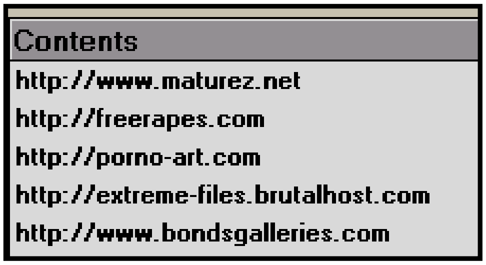
Under the **"Notes"** section, space is reserved for comments and to document the output findings. **Printing** and **saving** the output findings are just a few of the options available when using NTA Viewer™. You can also **"Tag"** certain entries and sort to display just those tagged sites.

NTA Viewer™ Output Database Fields

NTA Stealth™ output consists of data written into four fields described as follows for viewing in NTA Viewer™:

Content Field

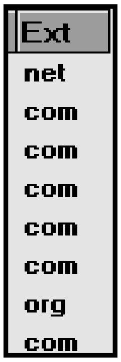
This field is used to store Internet web site and email addresses found by NTA Stealth™. The contents are stored in character form and the field is 70 bytes in length.



Contents
http://www.maturez.net
http://freerapes.com
http://porno-art.com
http://extreme-files.brutalhost.com
http://www.bondsgalleries.com

Extension Field

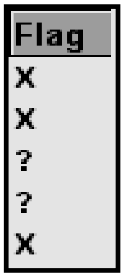
This field is used to store web site and email address **extensions**. This field is also used to store the Internet country codes for foreign web site and email addresses. The contents are stored in character form and the field is five bytes in length.



Ext
net
com
com
com
com
com
org
com

Flag Field

This is a special field that flags leads of potential interest, particularly leads tied to adult or child pornography. The flags are "best guess" efforts made by NTA Stealth™ to draw attention to leads that may have value in computer-related investigations. **These flags should not under any circumstance be considered conclusive.**



Flag
X
X
?
?
X

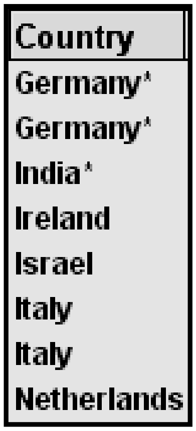
All leads identified by NTA Stealth™ should be corroborated before any actions are taken and before any legal decisions are made. The content in this field is stored in character form and the field is one byte in length. The key flag character potentially stored in this field is as follows:

Alert Flag = "X" This character is used to flag Internet leads which may be tied to adult or child pornography. Such leads can be relevant when the evidence computer is potentially involved in sex crimes or unauthorized uses in the workplace. These flags are determined by pre-programmed logic and thousands of known pornography-based Internet web sites are recognized by the program's logic. The criterion is not user definable and **this indicator is not conclusive. Leads tied to this flag should be corroborated before any action is taken**.

Alert Flag = "?" This character is used to flag Internet leads which *may be* **possible** adult or child pornography. Such leads can be relevant when the evidence computer is potentially involved in sex crimes or unauthorized uses in the workplace. These flags are determined by pre-programmed logic and thousands of known pornography-based Internet web sites are recognized by the program's logic. The criterion is not user definable and **this indicator is not conclusive. Leads tied to this flag should be corroborated before any action is taken**.

Country Field

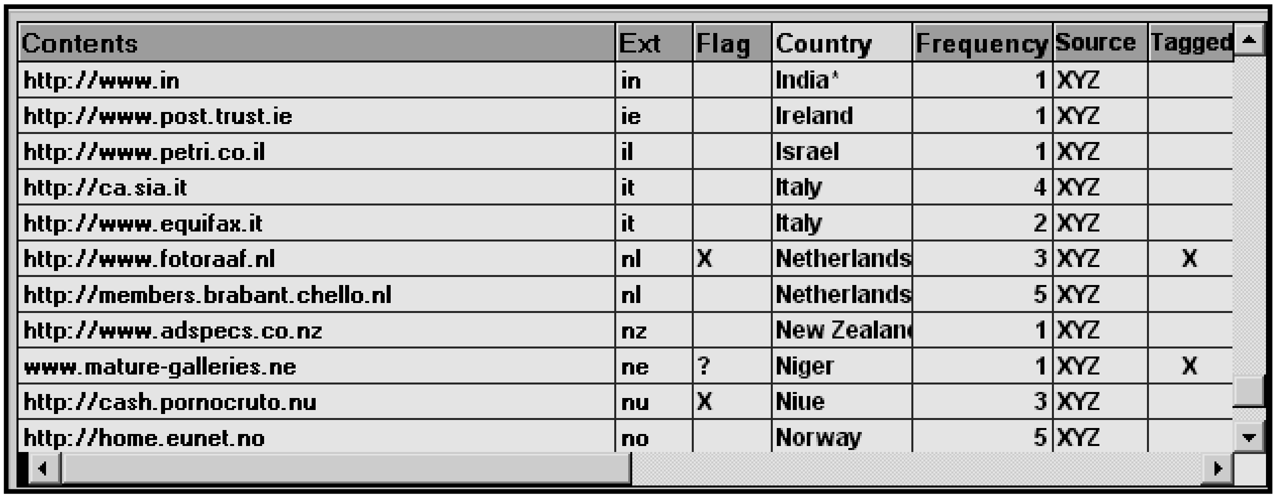
This is a special field that NTA Viewer™ uses to identify Internet leads tied to a specific Internet country code. The information is derived from country codes listed in web site and email addresses. When a known Internet country code is identified, the software automatically translates the cryptic country code into the complete name of the country identified. **Although this feature is quite accurate, it is not conclusive and corroboration of the finding is needed.** The field contents are stored in character form and the field length is 25 bytes.



Country
Germany*
Germany*
India*
Ireland
Israel
Italy
Italy
Netherlands

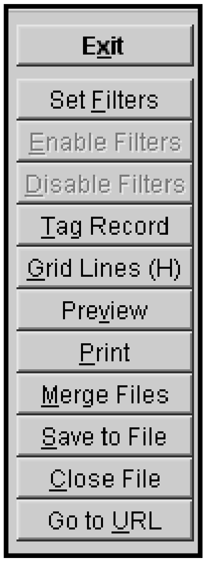
NTA Viewer™ Options

NTA Viewer™ displays NTA Stealth™ output in a **"grid"** format. Below is the NTA Viewer™ screen with one of the "grid" line options enabled.



Contents	Ext	Flag	Country	Frequency	Source	Tagged
http://www.in	in		India*	1	XYZ	
http://www.post.trust.ie	ie		Ireland	1	XYZ	
http://www.petri.co.il	il		Israel	1	XYZ	
http://ca.sia.it	it		Italy	4	XYZ	
http://www.equifax.it	it		Italy	2	XYZ	
http://www.fotoraaf.nl	nl	X	Netherlands	3	XYZ	X
http://members.brabant.chello.nl	nl		Netherlands	5	XYZ	
http://www.adspecs.co.nz	nz		New Zealan	1	XYZ	
www.mature-galleries.ne	ne	?	Niger	1	XYZ	X
http://cash.pornocruto.nu	nu	X	Niue	3	XYZ	
http://home.eunet.no	no		Norway	5	XYZ	

NTA Viewer™ is adjustable and offers the following features identified on the right-hand side of the NTA Viewer™ screen.



Moving Columns

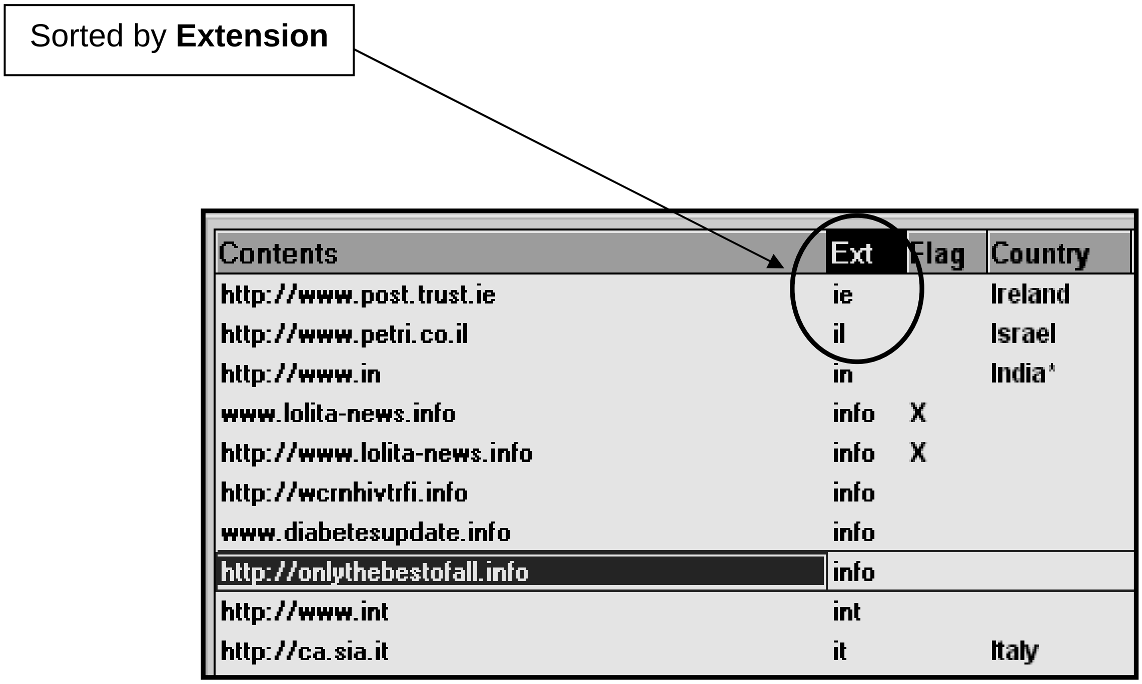
You may change the order in which the columns appear by clicking and holding on the column header with your mouse and then dragging the column into the desired position.

Changing Column Width

You may adjust the width of any of the columns by clicking and holding on any column border. Move your mouse to set the column to the desired width.

Changing Sort Order

You may change the order that records appear in by double clicking on any of the column headers in NTA Viewer™. When you double click on any column header, the data will be sorted within that column. NTA Viewer™ displays the currently sorted column header in yellow.



Sorted by **Extension**

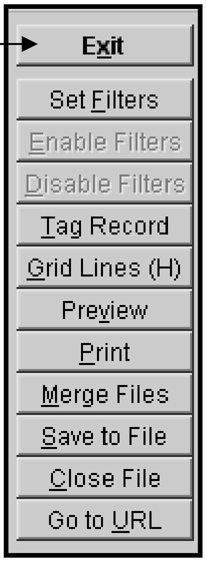
Contents	Ext	Flag	Country
http://www.post.trust.ie	ie		Ireland
http://www.petri.co.il	il		Israel
http://www.in	in		India*
www.lolita-news.info	info	X	
http://www.lolita-news.info	info	X	
http://wcrnhivtrfi.info	info		
www.diabetesupdate.info	info		
http://onlythebestofall.info	info		
http://www.int	int		
http://ca.sia.it	it		Italy

NTA Viewer™ Applications

The NTA Viewer™ screen illustration in the items above contains a group of buttons on the right-hand side of the screen that allow you to do the following:

Exit

Click on this button to exit NTA Viewer™.

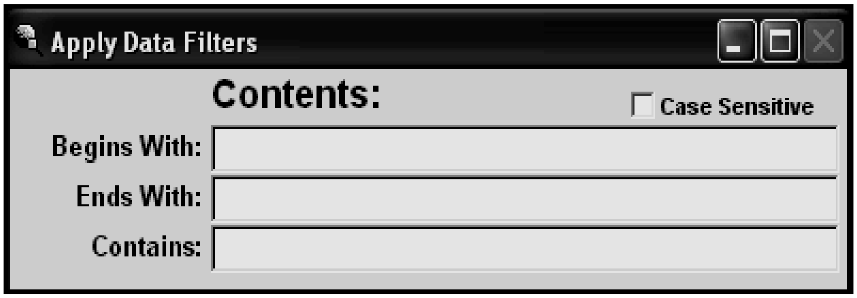


Set Filters

Filtering allows you to limit the display of entries to only those that meet your specific criteria. This button opens the Filter Screen where you can specify those criteria. You may filter data based on any combination of the following criteria:

<u>Contents</u>

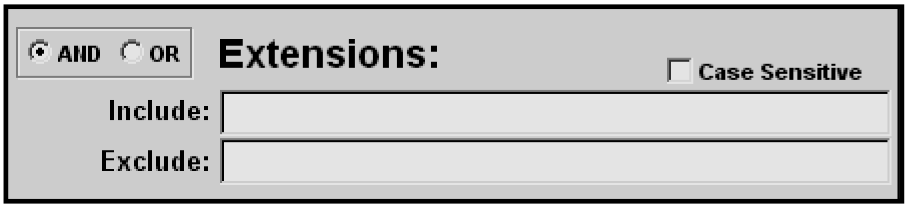
Contents-Begins With- this option allows you to limit the data displayed to only those entries that begin with at least one of the specified criteria.



Contents-Ends With- this option allows you to limit the data displayed to only those entries that end with at least one of the specified criteria.

Contents-Contains- this option allows you to limit the data displayed to only those entries that contain at least one of the specified criteria.

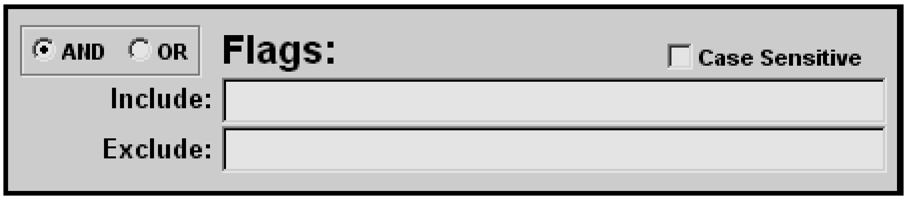
Extensions



Extensions-Include- this option allows you to limit the data displayed to only those entries that have an extension listed in the filter criteria.

Extensions-Exclude- this option allows you to limit the data displayed to only those entries that have an extension NOT listed in the filter criteria.

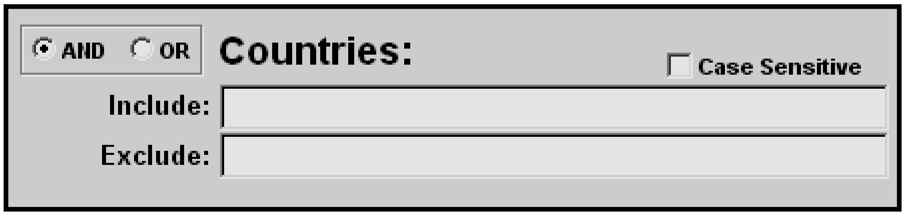
Flags



Flags-Include- this option allows you to limit the data displayed to only those entries that have a flag value listed in the filter criteria.

Flags-Exclude- this option allows you to limit the data displayed to only those entries that has a flag value NOT listed in the filter criteria.

Countries:

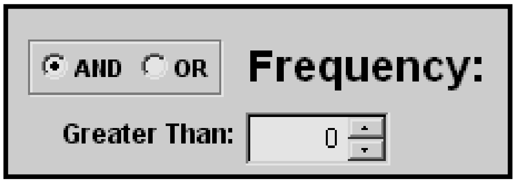


Countries-Include- this option allows you to limit the data displayed to only those entries that have a country code listed in the filter criteria. NTA will automatically identify countries associated with Internet addresses and NTA Viewer™ will display that information so that you can make decisions that relate to relevant countries in your investigation.

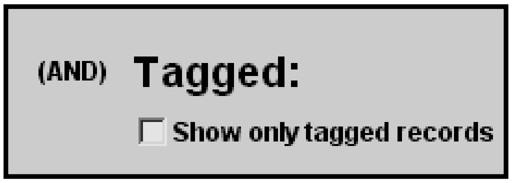
Countries-Exclude- this option allows you to limit the data displayed to only those entries that have a country code NOT listed in the filter criteria.

Frequency:

Frequency- this option allows you to limit the data displayed to only those entries that have frequency of occurrence greater than a number specified by you. Frequency analysis can be very helpful in investigations involving the misuse of corporate and government computers tied to the viewing and downloading of pornographic image files. Frequency analysis can also be helpful in cases involving relevant communications via email.

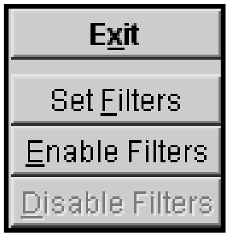


Tagged- this option allows you to limit the data displayed to only those entries that have a tag value. As stated previously, the tagging of items can help in determining the relevance of specific leads in your investigation. This feature is particularly helpful when it is combined with the review of identified URLs over the Internet. Once a relevant item is identified, you can tag it and create a report of tagged items for later use in trial or other investigative steps.



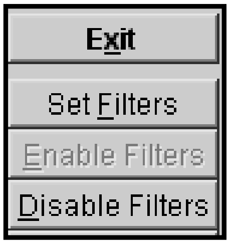
Enable Filters

This button activates the filtering criteria as specified in the Filter Screen.



Disable Filters

This button deactivates the current filter. The filtering criteria are left intact so you may enable/disable the filter without having to reset conditions in the Filter Screen.



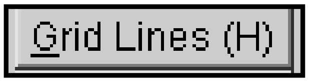
Tag Records

This button is used to tag or un-tag items that you deem to be important in your investigation. Once items are tagged, they can be filtered for the creation of custom views and reports. This field was added to aid you in the segregation of important and relevant items to your investigation.

Tagged records can easily be filtered, allowing you to view only entries that are of interest. Typically, this feature is used after the lead has been reviewed for relevance on the Internet. NTA Viewer™ allows you to directly access the Internet for viewing as explained under "**Go To URL"**.

Grid Lines

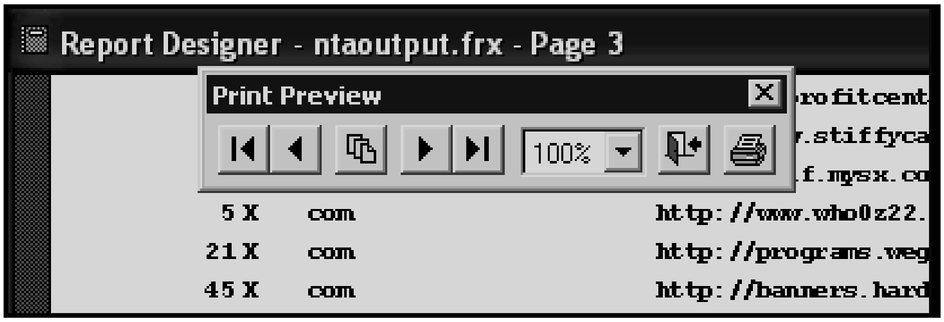
This button allows you to display horizontal and vertical grid lines in NTA Viewer™. This feature is helpful when NTA Stealth™ output files are voluminous.



When the above button for grid lines is displayed, it means that the Grid Lines are in the off position and the next position when the button is pressed will be horizontal grid lines.

Preview

This button opens the report preview window. The NTA Viewer™ report only contains the data shown in the viewer at the time of preview. Below is an example of the report preview window.

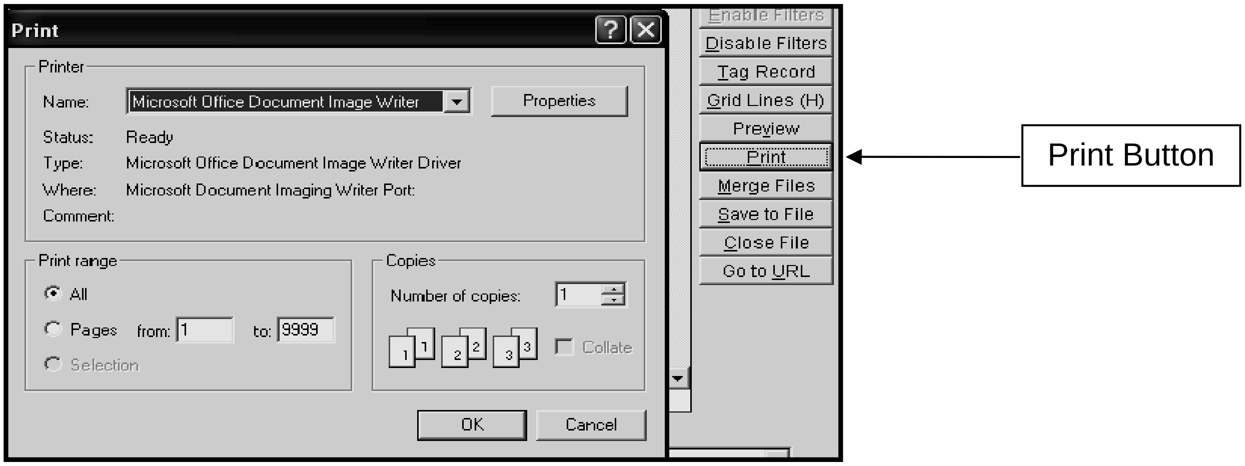

Report Designer - ntaoutput.frx - Page 3

```
                              rofitcent
                              .stiffyca
                              f.mysx.co
 5 X   com                    http://www.who0z22.
21 X   com                    http://programs.weg
45 X   com                    http://banners.hard
```

This feature is helpful when you combine filtering with the tagging of relevant items in your investigation.

Print

This button sends the NTA Viewer™ report to the printer of your choice. The NTA Viewer™ report only contains the data shown in the viewer at the time of printing.


Print

Printer
Name: Microsoft Office Document Image Writer
Status: Ready
Type: Microsoft Office Document Image Writer Driver
Where: Microsoft Document Imaging Writer Port:
Comment:

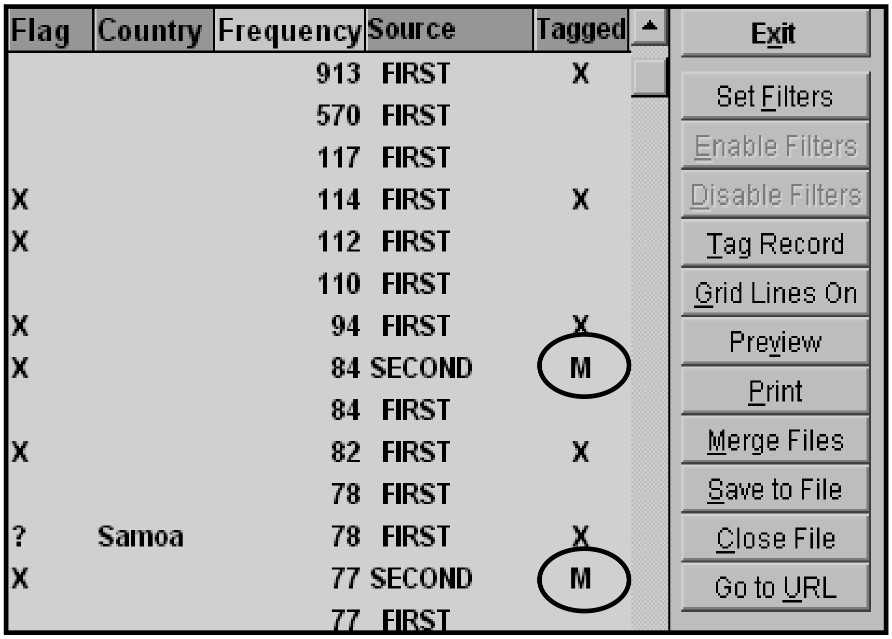
Print range
● All
○ Pages from: 1 to: 9999
○ Selection

Copies
Number of copies: 1
□ Collate

Print Button

Merge Files

This button allows you to merge NTA Stealth™ output files. This is helpful when an investigation involves the processing of several related computer systems tied to a single computer user or in conspiracy cases involving numerous individuals and computers. If NTA Viewer™ detects any matching entries during the merge, it will tag the matching merge records with an '**M**'.



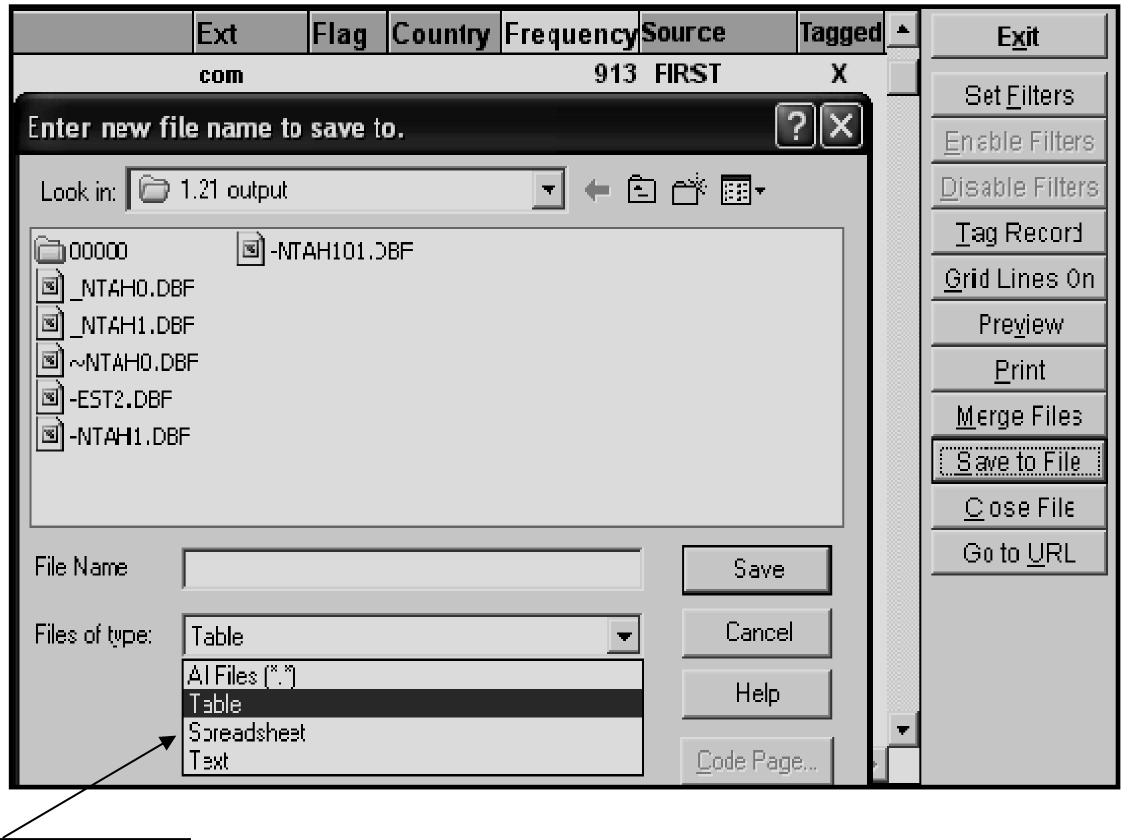
Flag	Country	Frequency	Source	Tagged
		913	FIRST	X
		570	FIRST	
		117	FIRST	
X		114	FIRST	X
X		112	FIRST	
		110	FIRST	
X		94	FIRST	X
X		84	SECOND	M
		84	FIRST	
X		82	FIRST	X
		78	FIRST	
?	Samoa	78	FIRST	X
X		77	SECOND	M
		77	FIRST	

The **FIRST** .dbf file when compared to the **SECOND** .dbf file shows 2 files that have matching entries when merged as denoted by the **"M".**

When the merge takes place, the original output files are not changed in any way. If you want to keep a disk file copy of the merged data, you will need to perform a **"Save To File"** function (see below).

Save To File

This button allows you to save the data currently displayed in the viewer to a file. You may save the information to a dBase database file (.dbf), an Excel spreadsheet (.xls) or a Tab Delimited text file (.txt).



	Ext	Flag	Country	Frequency	Source	Tagged
	com			913	FIRST	X

Enter new file name to save to.

Look in: 1.21 output

00000
_NTAH0.DBF
_NTAH1.DBF
~NTAH0.DBF
-EST2.DBF
-NTAH1.DBF
-NTAH101.DBF

File Name:

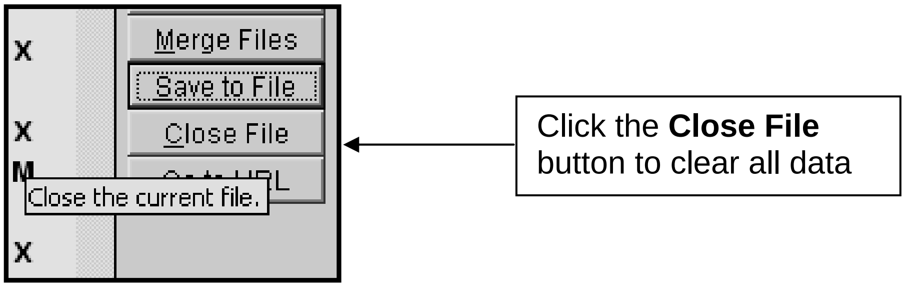
Files of type: Table

Choose the format you wish to **save** the file in

This feature is helpful when you need to retain relevant NTA Viewer™ output for testimony or further analysis at another time.

Close File/Open File

This button allows you to clear all data from the viewer screen. You may subsequently open another file without exiting NTA Viewer™ by using this feature.

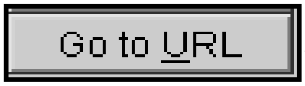


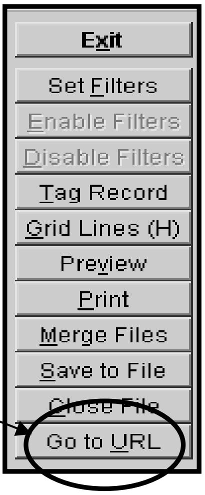
Click the **Close File** button to clear all data

Go To URL

This button allows you to open a browser window to look at a web site for corroboration. It is extremely helpful in reviewing suspicions of past Internet activity that may be indicated in your analysis of NTA Stealth™ output.

The "**Go To URL**" will only work if the analysis computer is connected to the Internet and Internet browser software is installed.

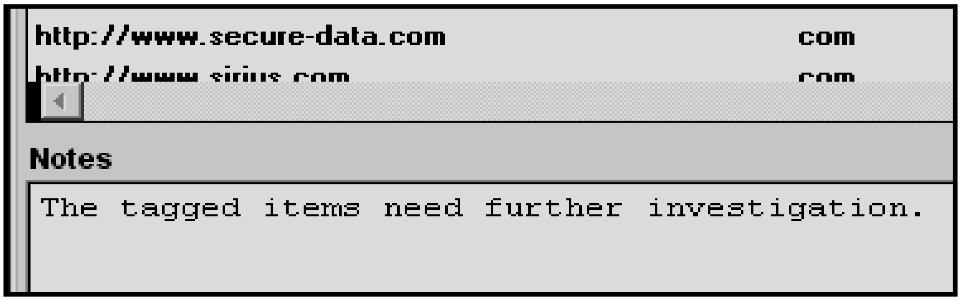




If the record is an email address, NTA Viewer™ will attempt to open the main page of the associated web site as well. If a URL is involved based on your suspicion of Internet web browsing, then NTA Viewer™ will attempt to open the relevant pages of the web site.

Investigative Notes

This area of the NTA Viewer™ screen allows you to enter notes as you are performing your analysis. The contents of the notes field are printed on the summary page of the NTA Viewer™ report. The notes are also saved to a text file. Notes **are not saved** to the .dbf or .xls format during the **"Save To File"** operation.



```
http://www.secure-data.com                    com
http://www.sirius.com                         com
```

```
The tagged items need further investigation.
```

Technical Support

NTI will provide technical support and assistance regarding the use of this program to registered users of the software. Technical support is available during the hours of 8:00 a.m. to 5:00 p.m. (Pacific Standard Time or Pacific Daylight Time, as appropriate), Monday through Friday by calling NTI at 503-661-6912. Technical support is also available via email at:

support@forensics-intl.com.

NTI is continually working to improve this software and to help its clients in the identification of Internet account abuses and in the identification of illegal uses of computer systems, e.g., the distribution of child pornography. Your comments and suggestions are appreciated and should be sent to:

New Technologies, Inc.
2075 Northeast Division Street
Gresham, Oregon 97030
503-661-6912

Email: info@forensics-intl.com

http://www.forensics-intl.com