



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

Copyright © 1997-2005 By New Technologies Armor, Inc. rev904a
Processes protected by U.S. Patent No. 6,279,010

Table of Contents

Introduction.....	1
What is NTA Stealth™?	1
Who Should Use NTA Stealth™?	2
Probation and Parole Officers	2
Law Enforcement	3
Personal Use of Business/Government Computers	4
License Statement.....	4
Disclaimer of Warranty	5
Privacy Law Issues.....	6
Choice of Law.....	6
Upgrades and Notices	6
What You Get with NTA Stealth™	7
NTA Stealth™ Features.....	8
NTA Stealth™ Instructions	10
Operating NTA Stealth™ from NTA Stealth™ Test Disk.....	12
Using Custom NTA Stealth™ Images on a Separate Floppy Disk.....	13
Running NTA Stealth™ from NTA Stealth™ USB Thumb Drive	21
NTA Stealth™ Files	22
NTA.EXE File	23
NTALOGIC.NTI File.....	23
Downloading Updates of NTALOGIC.NTI.....	23
AUTOEXEC.BAT and NTA.BAT Files	25
Changing AUTOEXEC.BAT and NTA.BAT Files	26
Changing AUTOEXEC.BAT FILE on NTA Stealth™ Floppy Test Disk	26
Changing NTA.BAT FILE on NTA Stealth™ USB Thumb Drive.....	28
Summary of NTA Stealth™ Commands and Options	28
Identifying More Than One Hard Drive on Evidence Computer	32
/AUTO1- Internet Web Browsing Option	32
Internet Web Browsing with Pornography Only Option.....	35
/AUTO2- Email Leads Option.....	37
/AUTO3- Graphic File Option	38
Graphic File Download Frequency	39
/AUTO4- Web Browsing and Email Combination Option	39
Web Browsing and Email Combined Option-Porn Only.....	41

Skip and End Command Options.....	43
Manually Terminating or Pausing NTA Stealth™	44
Processing Files.....	45
What is a Swap or Page File?	46
System Menu Operation for Processing Files	47
How To Use The System Menu	47
Pornography-Based Internet Activity in a Targeted File	53
Analyzing and Viewing NTA Stealth™ Output.....	59
NTA Stealth™ Output File Names.....	60
NTA Stealth™ Evidence Log File	61
NTA Viewer™ Instructions.....	63
Opening NTA Viewer™ and Accessing NTA Stealth™ Output Files	63
NTA Viewer™ Output Database Fields.....	68
Content Field	68
Extension Field.....	68
Flag Field.....	68
Country Field	69
NTA Viewer™ Options	70
Moving Columns.....	70
Changing Column Width.....	71
Changing Sort Order	71
NTA Viewer™ Applications	72
Exit	72
Set Filters	72
Contents	72
Extensions	73
Flags	73
Enable Filters	75
Disable Filters.....	75
Tag Records.....	75
Grid Lines	75
Preview.....	76
Print.....	76
Merge Files.....	77
Save To File	78
Close File/Open File	79
Go To URL	79
Investigative Notes	80
Technical Support.....	80

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.

