



# User's Guide

## Introduction:

NTA Viewer is a specialized software tool designed to provide easy and quick analysis of output generated by NTI's Net Threat Analyzer (NTA) software tool. Information about NTA and the new NTA Stealth™ program can be found on the Internet at <http://www.forensics-intl.com/nta.html>. The combination of NTA Stealth™ and NTA Viewer software is ideal for use by computer forensics examiners, probation and parole officers and school administrators who must make quick decisions about the extent to which a specific computer hard disk drive should be examined. This combination of software provides the end user of the software with the ability to quickly identify leads of past Internet activities associated with a specific computer hard disk drive. It is analogous to an electronic drug test kit except in this case it identifies past Internet web browsing activities and frequency. The resulting information is very helpful but it must be remembered that corroboration of the findings is necessary before binding legal decisions are made that may have legal ramifications.

NTA Viewer supports the simultaneous analysis of NTA output files originating from an unlimited number of related computers. This powerful feature can greatly increase the effectiveness of investigators dealing with conspiracy-type cases or when an individual has used several different computers. With the ability to quickly sort and filter NTA output data based on a number of different criteria, NTA Viewer provides a fast & powerful way to identify and prioritize Internet-related leads. This is especially true concerning the identification of leads associated with inappropriate or illegal Internet activities, e.g., the download and viewing of child pornography on workplace computers.

NTA Viewer is a specialized Microsoft Windows based software tool designed to provide easy and quick analysis of output generated by NTA. NTA Viewer software operates under Windows95, Windows 98, Windows 2000 and Windows XP. This user's guide and the supporting dlls can be downloaded over the Internet at <http://www.forensics-intl.com/ntaview.html>.

This software is only for use with NTI's NTA software and it is licensed for use by licensed users of NTA and NTA Stealth™ software.

## License Statement:

NTA Viewer software is owned by Armor Holdings, Inc., the parent company of NTI, and is licensed for use by licensed users of NTA and NTA Stealth™ software. This software is not licensed to be shared or copied for use by others. NTA Viewer is not shareware and, therefore, is not licensed for distribution other than by NTI or its authorized dealers and distributors.

Any alteration of this User's Guide or the referenced software nullifies any licensing agreements between the user and NTI. Violations of this licensing agreement constitute a violation of your license to use the software and may constitute a criminal and/or civil violation of United States and/or international copyright laws. NTI will pursue such violations to the fullest extent of the law.

## **Disclaimer of Warranty:**

NTI has made every effort to verify the accuracy of this program. However, NTA Viewer is sold and distributed "as is" without any warranty of any kind. In no event shall NTI, the authors, and/or authorized dealers and distributors be liable or responsible for any problems that could arise because of defects in the program or from the operation of the program. TEST THIS PROGRAM THOROUGHLY BEFORE PUTTING IT INTO USE!

## **Installation of NTA Viewer Software:**

The software is intended to be operated under Windows 98/NT/2000/XP from a dedicated subdirectory. Create a subdirectory with a name of your choosing and copy the software and supporting dlls (vfp6r.dll and vfp6renu.dll) into it. As stated above, the supporting dll files may not be provided with the software but they can be downloaded over the Internet from <http://www.forensics-intl.com/ntaview.html>. This User's Guide is also available for download from the same site.

## **Operation of NTA Viewer Software:**

NTA Viewer software can be accessed through the Microsoft Windows explorer interface and upon double clicking on the program file, the Main System Screen will be displayed. From there you can use the options available to process any file created by NTI's NTA and/or NTA Stealth™ software. This includes files created by the law enforcement version of NTA, the corporate version of NTA and the new NTA Stealth™ version that processes an entire hard disk drive (at a physical level) from a floppy diskette or a USB flash memory storage device. Information about NTA Stealth™ software can found on the Internet at <http://www.forensics-intl.com/nta.html>.

Upon execution of the program the system Main Screen will be displayed and the various options are accessed from this display screen:

## **MAIN SYSTEM SCREEN**

The main NTA Viewer screen displays NTA program output in a "grid" format. NTA Viewer is adjustable and offers the following features:

### **Moving Columns:**

You may change the order that the columns appear in by clicking & holding on the column header with your mouse, and then dragging the column to the desired position.

### **Changing Column Width:**

You may adjust the width of any of the columns by clicking & 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 the 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. If you are sorting on a column where not all of the records contain a value (flag for instance), the viewer will automatically place you on the first record with a value if you are not already on a record containing a value.

## **APPLICATION FEATURES**

On the right hand portion of the Main Screen is a group of buttons that give you access to the following features:

### **Exit:**

Press this button when you are ready to shut down the viewer software.

### **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. The Filter Screen is covered later in this User's Guide.

### **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 tags/un-tags items that you deem to be important in your investigation. Be aware that once items are tagged, they can be filtered for the creation of custom views and reports. We added this field specifically 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 relevant Internet item has been reviewed for relevance over the Internet that involves another feature of NTA Viewer that is described elsewhere.

### **Grid Lines:**

This button allows you to display horizontal and vertical grid lines in the viewer. The feature is helpful when your NTA output files are voluminous.

### **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. As stated above, this feature is very 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.

### **Merge Files:**

This button allows you to merge NTA output files. This ability is helpful when an investigation involves the processing of several related computer systems tied to a single user or in conspiracy cases involving numerous individuals and computers. If the viewer detects any matching entries during the merge, it will tag the matching merge records with an 'M'. It is important to note that the merge takes place in the viewer; the original input 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".

### **Save To File:**

This button allows you to save the data currently displayed in the viewer to a file. You may save to a dBase database file (.DBF), an Excel spreadsheet (.XLS) or a Tab-Delimited text file (.TXT). 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. You may subsequently open another file without exiting the viewer by using this feature.

**Go to URL:**

This button will open a browser window for the associated web site. It is extremely helpful in reviewing suspicions of past Internet activity that may be indicated in your analysis of NTA output. If the record is an E-mail address, NTA Viewer will attempt to open the main page of the associated web site as well. If a URL is involved based upon your suspicion of base Internet web browsing, then the viewer will attempt to open the relevant page of the web site. Be aware that this feature will only work if the analysis computer is connected to the Internet and Internet browser software is installed.

**Investigative Notes:**

This area of the Main 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 when you save to a text file. Notes are not saved to the .DBF or .XLS format during the save operation.

**FILTER SCREEN**

NTA Viewer gives you the ability to limit the data presented based on different filtering criteria that you can specify. You can access the filtering screen by pressing the "Set Filters" button on the Main screen. Specific help for any item on the Filters screen can be found by clicking on the item of interest, and then clicking on the yellow question mark in the lower right hand portion of the screen. You may filter data based on any combination of the following criteria:

**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 - 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 - Include:**

This option allows you to limit the data displayed to only those entries that have a flag value listed in the filter criteria. By way of example, NTA Stealth™ automatically marks Internet-based pornography leads with an "X" flag.

**Flags - Exclude:**

This option allows you to limit the data displayed to only those entries that have a flag value NOT listed in the filter criteria.

**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:**

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 download of pornographic image files. It can also be helpful in cases involving relevant communications via E-mail.

**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 determine 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 in other investigative steps.

## HOW-TO'S

Although by no means a complete compendium of how NTA Viewer can be used to analyze NTA output files, the following "How-To's" cover some of the more frequently requested uses of NTA Viewer.

**How do I quickly identify the most frequently referenced web sites or E-mail addresses on a computer?**

1. The first step is to use NTI's Net Threat Analyzer (NTA) tool to extract web site address names from subject computers. NTA will produce a dBase (.DBF) output file that is compatible with NTA Viewer and other commonly used database and spread sheet programs.
2. Open the file using NTA Viewer and enter a "Source Computer Description" at the prompt. The source description is not required, however if you plan to simultaneously analyze data extracted from more than one computer, entering a source description will make it much easier for you to keep track of where entries came from.
3. The main screen in NTA Viewer will by default sort the addresses in order of frequency. Therefore you will find the most frequently referenced web sites or E-mail addresses at the top of the list. We find this sorted view to be very helpful in investigations so we made it the default. However, you can change the screen display through the use of the various options described earlier.

### **How do I determine if an E-mail address is on more than one computer?**

1. Follow the steps described above and open any NTA generated output file. Be sure to enter a source computer description.
2. If you have specific E-mail addresses that you are interested in, tag them by pressing the space bar. You can also tag records with the “Tag Records” button, or by typing “Alt+T”.
3. After opening any NTA generated input file, you may open additional input files by selecting the “Merge Files” button on the main screen of the NTA Viewer program. Make sure to enter a different source computer description for each merged file so that you will be able to tell where each name came from. NTA Viewer displays the source descriptions you’ve entered in the “Source” column of the main screen.
4. During the merge process, NTA Viewer will automatically tag any content matches with an ‘M’ to indicate that the entry was matched to an entry from another source. You have the option of viewing only those records that have been tagged by selecting that option on the Filter Screen, accessed by selecting the “Set Filters” button on the main screen.
5. You can also double-click the “Tag” column header so that all tagged records are grouped together regardless of whether or not you have any filtering conditions set.

### **How do I search for a specific E-mail or web site address?**

With “Sorting” and “Filtering” you can quickly determine if specific E-mail or web site addresses were extracted from the subject computer(s).

You can sort entries by address by simply double-clicking on the “Content” column header. Once you have the entries sorted by address, you can move through the list alphabetically looking for addresses of interest.

Another feature of NTA Viewer is the ability to filter data based on criteria you specify. This can greatly improve your efficiency when you have specific address or partial addresses you are interested in finding. When you click on the “Set Filters” button on the main screen, you will be presented with a screen where you can enter your data filtering criteria. Refer to the “Filter Screen” section of this document for additional information. General instructions follow:

1. In the Filter Screen enter the address (or a portion of the address) you are looking for in the ‘Contains’ box under the ‘Content’ category.
2. Click the “Apply” button to apply to filter criteria to the viewer.
3. After closing the Filter screen the viewer will display any entries that contain the address you specified.

### **Does NTA Viewer allow me to review an identified URL over the Internet?**

The answer is yes. This ability exists with both Internet web addresses and E-mail addresses. Simply highlight the desired web address or E-mail address and click the <Go To URL> button on the right hand side of the screen. Assuming your analysis computer is connected to the Internet and that the site is still active, you will be directed to the targeted site on the Internet. When you click on an E-mail lead, the program will attempt to link with the related web site. The program will not allow you to interactively communicate with the E-mail address indicated. If that is desired, you will need to use an E-mail application.

## **CONTACT INFORMATION**

Please read this User's Guide thoroughly before contacting us for support. This program was designed to be easy to use and is very powerful when you are aware of all of the features available. In case you have questions or problems please use the contact information provided below:

### **Armor Forensics – NTI**

13386 International Parkway

Jacksonville, FL 32218

Tel: (800) 852-0300 or (904) 485-1801

Fax: (800) 588-0399 or (904) 741-5407

Web: [www.forensics-intl.com](http://www.forensics-intl.com)