April 2010 Newsletter

NetScanTools Pro 10.96.1 released.
NetScanTools Pro version 11 coming soon.

Follow us on Twitter:
http://twitter.com/netscantools

Blog:
http://netscantools.blogspot.com

In this newsletter:

News

- NetScanTools® Pro 10.96.1 Released April 12, 2010
- Sending Malformed UDP Packets
- NetScanTools® Pro version 11 Coming Soon – Really!
- Laura Chappell's New Wireshark Network Analysis Book
- NetScanTools® LE 1.20 Released March 15, 2010
- NetScanTools® Pro Versions Compatible with Windows 7 and Windows Vista
- NetScanTools® Pro on Windows 7 - 64 bit

Reminders

- Managed Switch Port Mapping Tool 1.99 released October 20, 2009
- How to Upgrade NetScanTools® Pro
- USB Version Users – Backup Your Software!
- About the Maintenance Plan – NetScanTools® Pro
- Contact Information

NEWS…

NetScanTools® Pro Version 10.96.1 Released April 12, 2010

NetScanTools Pro version 10.96.1 was released on April 12 following soon after the release of 10.96 on April 6. There are important new features in these two releases, namely the ability to send malformed UDP packets and MD5 signatures for exported results. **To upgrade**, click on Help/Check for New Version (requires an active maintenance plan). Here are some highlights.

New

- Packet Generator: added new field to override UDP packet length in UDP header. The data payload (either the text payload or the 'data from file') is used in its entirety whether or not you override the packet length in the UDP header or the IP header. UDP packets no longer need to have an even number of bytes for the payload. **These changes now allow malformed UDP packets to be generated.** Script language updated to allow control of the UDP packet length value. Thanks for M.I. at AT&T for the suggestion.

Changes to Existing Tools

- Reworked the automatic version checking function. You can control it in Help/Set Preferences.

10.96 April 6, 2010 was released for the Installed Version only. There was no USB version release at this revision level.

New

- Added MD5 Hash Signature option to save a companion text signature file whenever text results, databases and capture files are saved. You are prompted at the time of file saving.
- Added .fo and .co .nl to the whois database.
- Packet Generator: added simple looping and infinite looping to the script language. Included a new sample script for this.

Changes to Existing Tools

- Packet Generator: speeded up send continuous mode.
- Packet Generator: now displays error if packet is not sent.
- Fixed minor lookup issue when finding a country given an IP address.
- NetBIOS Basic now correctly reports Windows 7 machines instead of 'nt 6.1'.
- Corrected ICMP parsing type response.
- Removed Clear Passive Discovery Database Files button.
- Automatic Private IP Addressing (169.254.x.x) is now identified on program startup and the user is asked if they want to include those interfaces. Those addresses normally only appear in Windows if DHCP fails.
- Clear button for entered DNS IP addresses now added to Whois and Real Time Blacklist Check.
- Packet Viewer: corrected parsing of IGMP packets and now identifies Spanning Tree Protocol and HP Logical Link Control packets.
- Updated SQLite to version 3.6.23.

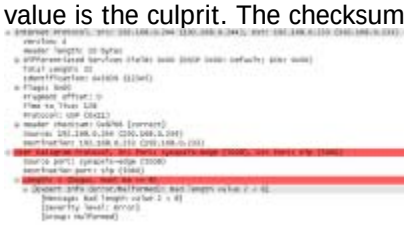
Sending Malformed UDP Packets

Malformed UDP Packets are easily generated with the new changes to the Packet Generator tool in NetScanTools Pro 10.96.1. Normally a UDP packet consists of an IP header followed by a UDP header followed by data. Usually all the parameters of those two headers are calculated at the time the packet is sent by the sockets layer, but with our Packet Generator tool we can create the packet from beginning to end including all parts of the headers.

This view from Wireshark shows a normal UDP packet:

You can see that the packet is complete and correct with all checksums and field lengths normal. The payload is only 4 bytes - it is the word 'test'.

Now look what happens if we put a value of 2 bytes into the UDP length field - remember that the UDP header itself is 8 bytes. The data payload is still the same 4 bytes. Wireshark's 'Expert Info' analyzer tells us that it is malformed and the length value is the culprit. The checksum is not analyzed and the data is not commented on.



See how Wireshark complains that the length value is less than the data and the UDP header? The message it gives is correct, the UDP length field must have a value of 8 or greater because that is the size of the UDP header itself. Can you send a UDP packet without any data? -sure, but it will also be tagged as malformed by Wireshark (exception error).

Next let's try setting the UDP header length field to something greater than the UDP header length + the data payload length. You can see that it notes that the length value (24) is greater than the payload (8 UDP header + 4 data = 12 bytes) and it does not complete the checksum calculation since all the data is not present.

A few words about what the Packet Generator tool can do. It can generate TCP, UDP, ICMP and CDP packets and send them out at a maximum repetition rate of roughly 10,000 packets per second - it is not a traffic generator capable of saturating your connection. It has a simple scripting language that allows you to send packets and even do some minor looping or use infinite looping. This is useful for connection test purposes. It uses WinPcap to generate packets, so it is pretty much limited to wired connections, not wireless connections. But even within these limits it really can show the response of applications or devices to malformed packets.

If you are interested in trying out the demo, you can do that by following this link. Please keep in mind that the demo will limit you to your local subnet but the full version does not have this limitation.

NetScanTools® Pro Version 11 Coming Soon – Really!

NetScanTools Pro version 11 is being worked on daily (even on evenings and weekends). The existing tools are still being transferred to the new user interface. Once that is complete, new tools will be added.

- **If your v10 maintenance plan is 'current' or 'active' at the time of release, you will be getting version 11 for free.**
- **If your maintenance plan has expired, there will be an upgrade fee.**

- **When will v11 be released? Probably not in May, but we will keep you posted.**

Here are a few of the changes we intend to make, feel free to comment on them:

- **There will be a FAVORITES left panel control bar.** You can add the tools you most frequently use to that list.
- **The user interface will be updated to be very similar to NetScanTools LE.** The advantage this brings is the ability to use more than one tool at once.
- **The last query results that appear many tools will no longer be available between sessions.** When you view the tool now, the results from the last query are shown even if the program is exited and restarted.
- **Results will be optionally saved to a database as they are in NetScanTools LE.** This database is required if you want to use the Automated Tools.

Laura Chappell's New Wireshark Network Analysis Book

After many months of hard work, Laura has done it again. This is an absolutely huge book (800 pages) – a brain dump of everything Laura knows about Wireshark. I have only read snippets of the book on the wiresharkbook.com website, but I can see that the quality is superb and it will definitely be in-depth!

Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide

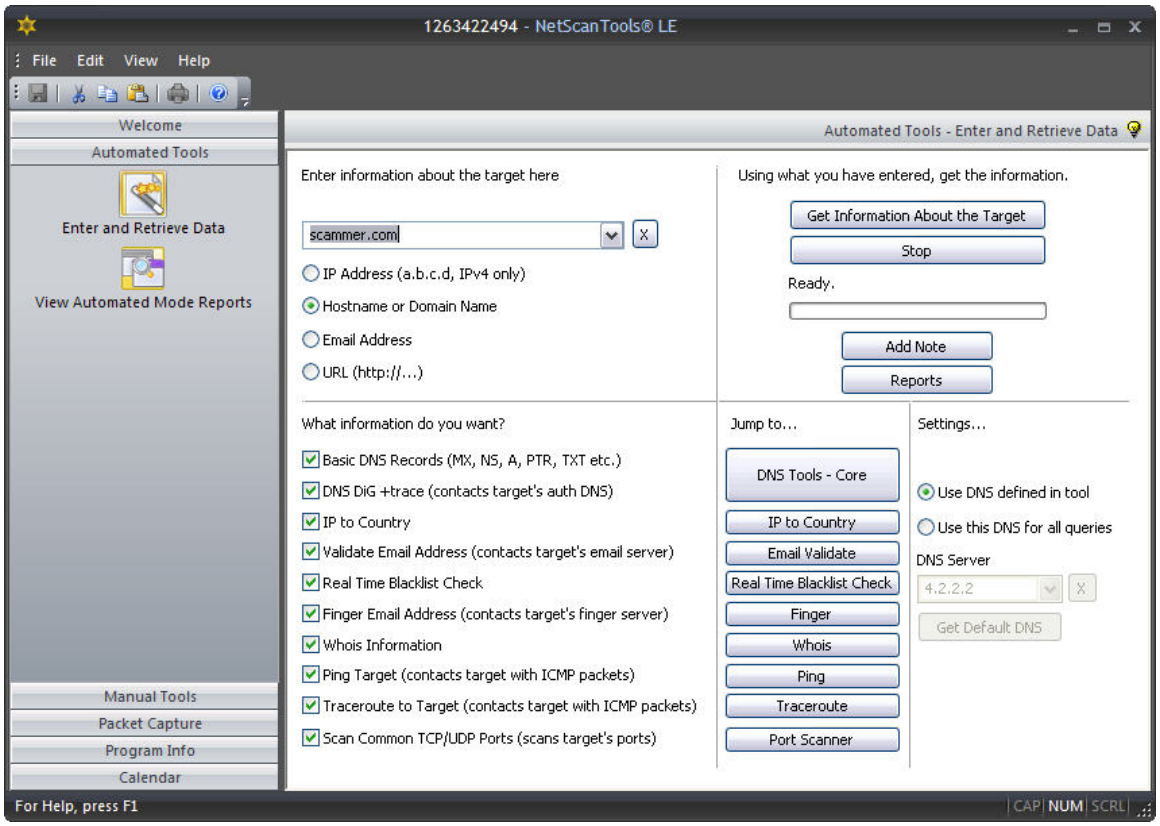
Paperback:	800 pages
Publisher:	Protocol Analysis Institute
Website:	http://www.wiresharkbook.com
Language:	English
ISBN10:	1-893939-99-8
ISBN13:	978-1-893939-99-8
Dimensions:	7.44 x 9.69 inches
Weight:	3.5 pounds
Contact:	info@chappellU.com or +1 408-378-7841
Exam Version:	Version 1 (WCNA-100 Exam) (Q2 2010 Release)
Exam Link:	www.wiresharkU.com/certification.html

NetScanTools® LE 1.20 Released March 15, 2010

NetScanTools LE (Law Enforcement version) 1.20 was released on March 15, 2010. We have added MD5 Hash Signature files that are automatically saved as companion files to the manual tool text results files. MD5 has signature files are also saved with the packet capture files giving you confidence in the data integrity and a method of showing that the data you have saved has not been altered. These MD5 files are text files and the signatures they contain can be compared using any suitable MD5 checksum utility. We also added internal hash signatures to the database tables to help assure that the contents of the rows in the tables have not been altered. You can see the results of this check when you select an automated or manual report. This new release also addressed a minor few problems with earlier releases.

NetScanTools LE has 12 important tools and it has the Packet Capture utility from NetScanTools Pro. As in NetScanTools Pro, Packet Capture runs outside the main toolset as a standalone application launched from within NetScanTools LE. It is used to capture packet traffic entering and leaving the computer while you use the various tools. Its purpose is to document the process used in the acquisition of network data – but you have to activate it separately. The packet capture files are saved in industry standard WinPcap format compatible with advanced packet analysis tools like Wireshark. A companion MD5 hash signature file is also saved along with the packet capture file.

NetScanTools LE pricing:
Law Enforcement: **$69**
Everyone else: **$129**



NetScanTools LE uses several tools from NetScanTools Pro with an emphasis on the tools Law Enforcement uses. Some features of NetScanTools LE will be migrated back into NetScanTools Pro version 11. For instance, the ability to use two or more manual tools simultaneously returns and a completely reworked and simplified Automated tool section. The user interface is also updated.

Remember, this is a subset of the tools in the Pro and it's not intended to be a replacement. There are 13 tools in LE vs at least 42 in Pro. Network management tools such as Advanced DNS Tools, SNMP and Packet Generator etc. are not found in NetScanTools LE. NetScanTools LE does not depend on WinPcap unless you need to use Packet Capture. Tools in common with Pro are simplified and use only the basic modes needed to find the data you are looking for. The advanced modes found in many tools like NetScanTools Pro TCP Traceroute are not available.

Main NetScanTools LE Description Page:
http://www.netscantools-le.com/

Try It!
http://www.netscantools.com/nst_le_trial.html

Tool by Tool Comparison between NetScanTools LE and NetScanTools Pro
http://www.netscantools.com/nst_le_pro_feature_comparison.html

NetScanTools® Pro Versions Compatible with Windows 7 and Windows Vista

People have asked us which versions of NetScanTools Pro 10.x can be used on Windows 7 and Windows Vista. These are the minimum NetScanTools Pro versions that you should be using on each operating system.

- **Windows 7 - 64 Bit:** We highly recommend using NetScanTools Pro version 10.94 or newer because it incorporates WinPcap 4.1.1 which is designed for Windows 7.
- **Windows 7 - 32 Bit:** NetScanTools Pro version 10.81 or newer. For best results, use version 10.94 because it incorporates WinPcap 4.1.1 which is designed for Windows 7.
- **Windows Vista/2008:** You must have NetScanTools Pro version 10.42 or newer. All known Vista issues were completely fixed by version 10.52.
- **Windows XP/2003/2000:** Any NetScanTools Pro version 10.
- **We no longer recommend using the first three versions: 10.0, 10.1, or 10.20.**

What happens if you use an earlier version of NetScanTools Pro on Windows Vista? The difference between Windows Vista and Windows XP was much greater than between Vista and 7. You may experience crashing particularly in the Network Statistics Tool. You may experience missing results in certain modes of traceroute. These are some examples – there are others. If you use Windows 7 or Vista, please use a version equal to or newer than what we are showing above.

NetScanTools® Pro on Windows 7 – 64 Bit

NetScanTools Pro version 10 is a 32 bit program that runs fine in the 32 bit subsystem found in Windows 7 - 64. It will show up in task manager as "nstpro.exe *32". If you are using the USB version, we highly recommend using version 10.94 or newer if you are plugging it into Windows 7 - 64 bit. And yes, we plan on making a 64 bit native version at some point.

REMINDERS

Managed Switch Port Mapping Tool 1.99 released October 20, 2009

This is the last release before version 2.00 which is currently under development.
Changes in the program:

- Switch Properties window: Added display of Switch IP Address.
- Setup: Autosizing of column widths is now optional. It can also be done on an individual column basis or all columns from the right click menu.
- Fixed error where a switch without a formal internal name was showing an error referring to the Dell brand even it if was not that brand.
- Fixed problem where duplicate mac addresses might show up in the same cell.
- Added another method of obtaining Cisco Vlans.
- Added ability to launch an SSH program from the right click menu and the main menu.
- Updated SQLite to version 3.6.19 and converted it to static linkage to avoid interference with previous versions.
- Updated MAC address/Manufacturer database.
- Tested on Windows 7.

How to upgrade NetScanTools® Pro

Here is how to upgrade NetScanTools Pro. As you read through this, please refer to image below – check it out

How to upgrade:

Prerequisites:

- You must have the NetScanTools Pro v10.x installed.
- You must have a **valid active maintenance plan**.
- The software must be registered AND you must have applied the "NST Pro 10 Registration Code" email message we sent back to you – if it is not registered, our secure site will not have any login credentials ready for you.

1. Start NetScanTools Pro and click on the Online group in the left panel.

2. Then click on the Check for New Version icon. Once the web page appears in the right pane, you will see the Login link text. (**Alternative:** all versions after 10.54 have a Check for New Version link to the Help menu)
3. After clicking on the Login text, you will see a popup window asking for a username and password. Those are found in the Login Access Credentials area as shown in the image on the next page. **The username and password ARE CASE SENSITIVE.** We recommend using copy and paste.

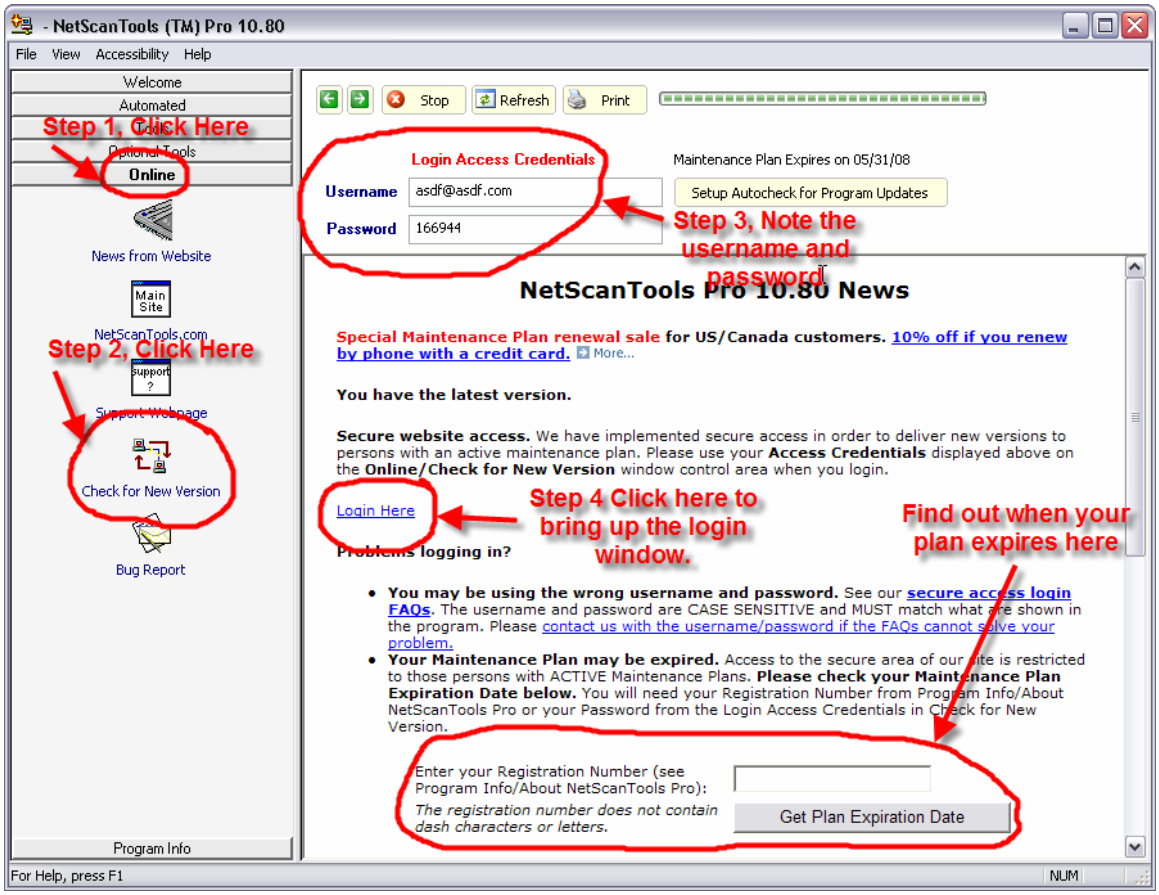
If your access credentials do not work please check for typos in your username or password (we recommend copy and paste). Your username is your email address that you gave when you registered and the password is the registration number.

It is also possible that your maintenance plan expired. Use the new online method to check your maintenance plan expiration date. Please contact us with the username and password you are using and we can check your access credentials. **You must have a valid maintenance plan to download an upgrade.**

Once you have logged in to the secure server, the **full download** is ready for installation by those of you with installed versions. You will need your CDKEY/serial number to run the installer – see the About NetScanTools Pro window to get it. Please install over the top of your current installation.

USB Version users can download an upgrade patch from the secure server. The latest version of the Managed Switch Port Mapping Tool is also available for download from this window and it is publically available elsewhere on our main site.

The image below shows where in the program you need to go to login to our secure site.



USB Version Users – Make a Backup of Your Software!

Please make a full backup of your USB Version after you have registered it and applied the NST Pro 10 Registration Code message we sent back by email. If you have a backup of the contents of the drive, we can easily assist you in restoring it to another drive in case you lose the original drive. Remember that the Lexar Lightning drive we supply the USB version on is one of the fastest drives currently available. If you do have to restore it, we highly recommend that same drive series or a faster model. Other types of larger USB drives that cost less are often much slower.

Backup your drive by copying all files and directories to another drive either on your computer or a portable backup drive. Saving the files to CDR is even better. Please do it today!

About the Maintenance Plan - NetScanTools® Pro

You need to have an active maintenance plan to obtain the latest release. A FULL Install of the "installed version 10.9X" (not a patch) is available on our secure site for download. Those who have the USB version are supplied with a patch for download from the secure site. You must have an active maintenance plan in order to login to the secure site. See the section **How to Upgrade NetScanTools Pro** below for help downloading the current release.

One year of maintenance (beginning at date of purchase) is included with a new or upgrade license. Benefits of the plan include telephone technical support and access to downloadable updates. We released seven updates in 2009. We released six updates in 2008. In 2007 we released 6 updates mostly targeted towards Windows Vista compatibility.

If you let your maintenance plan expire, the cost to renew the plan increases the longer you wait to renew. We give a 30 day grace period after your expiration date during which the renewal cost is $75 per license. If you are unsure when your plan expires, please feel free to contact us by email or phone or using the new method outlined earlier in this newsletter before renewing (see end of newsletter for contact information). You can always continue using the program even after the maintenance plan expires, but you will not get any changes or updated databases. And you will not get version 11 for free if your version 10 maintenance plan has expired.

Contact Information

If you have any questions or suggestions, please feel free to email.

Northwest Performance Software, Inc.
PO Box 1375
Sequim WA 98382-1375
(360) 683-9888
www.netscantools.com
sales [at] netscantools [dot] com