

NetScanTools® Pro



Monthly Newsletter

www.netscantools.com

July 2015

 <http://twitter.com/netscantools>

 <http://www.facebook.com/NetScanTools>

 <http://www.youtube.com/user/netscantools>

 <http://netscantools.blogspot.com/>

In this newsletter:

News

- **NetScanTools Products and Windows 10**
- **NetScanTools Basic 2.40 released July 28, 2015**
- **Managed Switch Port Mapping Tool 2.53 released July 9, 2015**
- **ipPulse 1.85 released June 29, 2015**
- **NetScanTools Pro 11.70 released June 12, 2015**

News...

From the Editor...

Windows 10 was released today and I've been using it for 9 months. I'm pretty happy with it, but I have not yet installed it as the primary OS. It should address most of those issues Windows 8 introduced – like the Start menu. Meanwhile, it is hot and very dry here in Sequim, Washington, USA. Have a good summer!

-Kirk

NetScanTools Products and Windows 10

All of our products have been tested on Windows 10 in its various iterations. I last tested on build 10240 and have not yet tested on the official version. I will be doing that within the next few days. The biggest problems we had were with WinPcap. That appears to have stabilized and work is being done to bring WinPcap out of the Windows XP world of NDIS5 to NDIS6. The nmap folks have a beta which seems to work well. Another that works is Win10Pcap – I only tested the first '5001' build and have not checked any subsequent builds. In either case, since these are GNU open source licensed, we will not be including them with our installer rather we will direct you to their download pages. WinPcap is required for NetScanTools Pro and optional for NetScanTools LE.

NetScanTools Pro, NetScanTools LE, NetScanTools Basic, ipPulse and the Managed Switch Port Mapping Tool have all be recently compiled for and tested on Windows 10 technical previews.

NetScanTools Basic 2.4 released July 28, 2015

NetScanTools Basic is a freeware version of NetScanTools with a few very basic tools. It was recently updated and compiled for Windows 10. These are the changes:

- Windows 10 compatible.
- Whois: Improved algorithm to check for many new domains. Added new messages if a user enters IPv6 or ASN.
- Updated Whois database - added a number of new whois servers.
- Added button to clear no-responding IPs from the Ping Scanner results.
- Code moved from VC2008 to VC2012.
- Updated SQLite DLL to v3.8.10.2

Managed Switch Port Mapping Tool v2.53 Released July 9, 2015

Version 2.53 was released to add a few minor changes. Not really any bugs, but just some additions that were suggested. If you have suggestions, feel free to contact us. Another release will be coming soon.

Download version 2.53 from here:

<http://www.switchportmapper.com/>

Changes in v2.53

- New command line option: "-historydb databaseName" allows you to select a previous or create new history database when running the software from the command line.
- Web browser reports and error messages now all have unique filenames making it easier to refresh one if several are open. They are all temporary and are deleted at the end of the session.
- Added detection of Microsoft Hyper-V devices for the VM section of the web browser reports.
- The SQLite error message window now correctly identifies Windows 10 and Windows Server 2016 operating systems. It also now shows the path, size and attributes of the current history database.
- Added new Switch Info reporting panel in the left control panel below the Database Maintenance button.
- Updated SQLite to version 3.8.10.2
- Updated MAC address/Manufacturer database.

ipPulse 1.85 released June 29, 2015

ipPulse is a network connectivity monitoring application primarily using ping to keep in contact with a list of targets. Once a target cannot be reached, a notification can be sent – full logging is also available. It runs on Windows 10 build 10158, 8.x, 7, Vista and XP and Server 2012GUI/2008.

This release added a new column 'Last Ping Time' – it shows the last round trip time in milliseconds of the last ping packet. We also added a new checkbox to the Email Settings controlling whether or not to do a 'verification' on any SSL certificates used during a STARTTLS email negotiations.

Please visit <http://www.ippulse.com/> to download the trial or update your current version.

This is a list of the changes:

- Added new checkbox 'Validate SMTP Server Certificate' to Email Settings (see Settings/Failure Alerts/Email Settings). This checkbox controls whether or not any email server certificates are validated. Default is checked.
- Added new column 'Last Ping Time' to the main window. It shows the last ping round-trip-time in milliseconds. To activate this column, click on Settings/Program Control/Edit Column Visibility. Ensure that the checkbox 'Last Ping Time' is checked.
- User defined SNMP OID columns are now not visible by default.

NetScanTools Pro 11.70 released June 12, 2015

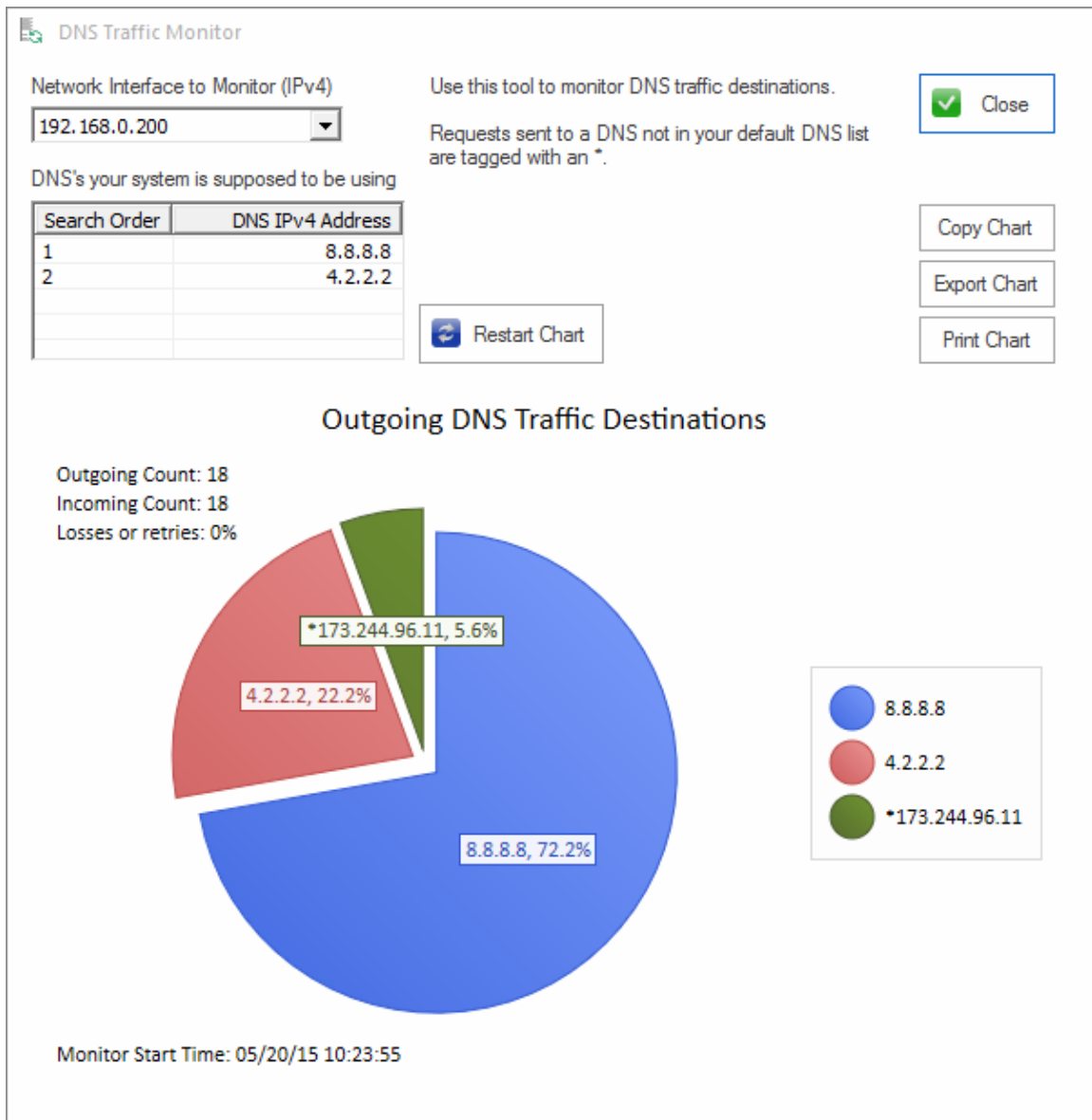
This version was long overdue, but it is the first NetScanTools Pro version 100% compiled with Visual Studio 2012 on Windows 8.1 moving everything off of Windows XP VS2008. We expect a minor release 11.71 soon with some changes to SSL Certificate Scanner. When Visual Studio 2015 is finalized, we will move the code base to that compiler skipping VS2013.

Another release will be coming soon.

There were many changes to the software and we added one new tool. The changes concentrated on WinPcap, speed enhancement to the ARP based scanners, user interface changes for all separately launched sub-programs and printing fixes for the grid based results tools. The software was fully tested on Windows 10 build 10130 (last build before 10158).

As we mentioned last month, there is a new tool called the DNS Traffic Monitor. The purpose of the tool is to show the DNS's assigned to your system and show the percentage of traffic going to each DNS. Any packets sent to a DNS not in the list are shown – this could indicate everything from a program with the ability to query any DNS (like NetScanTools Pro) to a malware.

A screenshot of the DNS Traffic Monitor is on the next page.



The full list of changes in v11.70 are shown here:

- All parts of NetScanTools Pro have now been recompiled with the Visual C++ 2012 compiler on Windows 8.1. Appearance and look and feel of all subprograms has been updated.
- General Cleanup: Removed old pre-Windows XP code that would not compile on the newer compiler. Expanded error messaging when Results Database cannot be opened.
- We now specifically test to verify the WinPcap packet driver is actually running. Any tools depending on WinPcap will have a popup warning if the service is not running and WinPcap is installed.
- All tool results using grid control (traceroute, arp scanner, etc): fixed printing output so that what is printed matches the current width of the control columns. Previously, it found the maximum string length in each

- column and printed based on that width no matter the column widths.
- New Tool: DNS Traffic Monitor added to Manual Tools, Passive Discovery Tools and DNS Tools left control panel panes. The DNS Traffic Monitor Tool shows you the default DNS's assigned to your system and the percentage of queries directed to each. Lost or retried DNS queries are shown and any queries to non-default DNS's are shown.
 - SSL Certificate Scanner: the 'Validity' column now displays any errors. Since TLS1 is now considered by some to be a security risk, the 'yes' is now shown with a yellow background for caution.
 - Added method for editing the Dictionary in the SNMP Dictionary Attack Tool and changed the dictionary file location to allow editing.
 - ARP Scan: removed floating progress window that caused program hang if Cancel was pressed. Speeded up scan process and changed default interpacket send delay to 10 milliseconds.
 - Database Maintenance: Added text showing the current path of the shared data, user data and temporary file data. Also added a button next to each to open and view each folder in your file management program.
 - DNS Tools/Advanced: Added method for following SPF record redirection in SPF Domain Keys tool. Examples of sites using redirects are facebook.com and yahoo.com.
 - Duplicate IP Scanner: removed floating progress window that caused program hang if Cancel was pressed. Speeded up scan process and changed default interpacket send delay to 10 milliseconds. Also added clarification of when to use the Reset Scanner Tables button.
 - Maintenance Plan Reminder Window: Reminder text changes and we added a button to manually query our server for your maintenance plan expiration date. The automatic update of the date from our server has been reduced from once every 30 days to once every 14 days.
 - Network Shares: now identifies Windows 10 computers.
 - Port Scanner: Changed default interpacket send delay to 15 milliseconds and changed default maximum threads to 512. Going to a smaller delay value may not give desired results.
 - Promiscuous Mode Scanner: removed floating progress window that caused program hang if Cancel was pressed. Speeded up scan process and changed default interpacket send delay to 10 milliseconds.
 - SNMP Core and Advanced: Added method in Settings for selecting string translations: 'guess, ascii or hex'. Added button to open the MIBs storage directory so you can quickly copy in your MIB in the format .mib, .txt or .my. NetScanTools Pro must be restarted before accessing the new MIBs through the SNMP tools.
 - Updated SQLite to 3.8.10.2
 - Updated database files.

Contact Information

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

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

'NetScanTools Pro', 'NetScanTools Standard', 'NetScanTools Basic', 'NetScanTools LE', 'ipPulse', 'Northwest Performance Software' and 'NetScanTools.com', are trademarks of Northwest Performance Software, Inc. 'NetScanTools' is a registered trademark of Northwest Performance Software, Inc.