



SmartSniff v2.07

Copyright (c) 2004 - 2013 Nir Sofer

Web site: <http://www.nirsoft.net>

Description

SmartSniff allows you to capture TCP/IP packets that pass through your network adapter, and view the captured data as sequence of conversations between clients and servers. You can view the TCP/IP conversations in Ascii mode (for text-based protocols, like HTTP, SMTP, POP3 and FTP.) or as hex dump. (for non-text base protocols, like DNS)

SmartSniff provides 3 methods for capturing TCP/IP packets :

1. **Raw Sockets (Only for Windows 2000/XP or greater):** Allows you to capture TCP/IP packets on your network without installing a capture driver. This method has some [limitations and problems](#).
2. **[WinPcap Capture Driver](#):** Allows you to capture TCP/IP packets on all Windows operating systems. (Windows 98/ME/NT/2000/XP/2003/Vista) In order to use it, you have to download and install WinPcap Capture Driver from [this Web site](#). (WinPcap is a free open-source capture driver.) This method is generally the preferred way to capture TCP/IP packets with SmartSniff, and it works better than the Raw Sockets method.
3. **Microsoft Network Monitor Driver (Only for Windows 2000/XP/2003):** Microsoft provides a free capture driver under Windows 2000/XP/2003 that can be used by SmartSniff, but this driver is not installed by default, and you have to manually install it, by using one of the following options:
 - o **Option 1:** Install it from the CD-ROM of Windows 2000/XP according to the [instructions in Microsoft Web site](#)
 - o **Option 2 (XP Only) :** Download and install the [Windows XP Service Pack 2 Support Tools](#). One of the tools in this package is netcap.exe. When you run this tool in the first time, the Network Monitor Driver will automatically be installed on your system.
4. **Microsoft Network Monitor Driver 3:** Microsoft provides a new version of Microsoft Network Monitor driver (3.x) that is also supported under Windows 7/Vista/2008. Starting from version 1.60, SmartSniff can use this driver to capture the network traffic.

The new version of Microsoft Network Monitor (3.x) is available to

download from [Microsoft Web site](#).

Notice: If WinPcap is installed on your system, and you want to use the Microsoft Network Monitor Driver method, it's recommended to run SmartSniff with /NoCapDriver, because the Microsoft Network Monitor Driver may not work properly when WinPcap is loaded too.

System Requirements

SmartSniff can capture TCP/IP packets on any version of Windows operating system (Windows 98/ME/NT/2000/XP/2003/2008/Vista/7/8) as long as [WinPcap capture driver](#) is installed and works properly with your network adapter. You can also use SmartSniff with the capture driver of Microsoft Network Monitor, if it's installed on your system.

Under Windows 2000/XP (or greater), SmartSniff also allows you to capture TCP/IP packets without installing any capture driver, by using 'Raw Sockets' method. However, this capture method has some limitations and problems:

- Outgoing UDP and ICMP packets are not captured.
- On Windows XP SP1 outgoing packets are not captured at all - Thanks to Microsoft's bug that appeared in SP1 update...
This bug was fixed on SP2 update, but under Vista, Microsoft returned back the outgoing packets bug of XP/SP1.
- On Windows Vista with SP1, only UDP packets are captured. TCP packets are not captured at all.
- On Windows 7, it seems that 'Raw Sockets' method works properly again, at least for now...

Versions History

- Version 2.07:
 - Fixed to flickering in the upper pane.
- Version 2.06:
 - Fixed to display HTTP POST URLs on 'URL List' display mode.
- Version 2.05:

- Added 'Capture On Program Start' option.
- Added 'Mark Odd/Even Rows' option, under the View menu. When it's turned on, the odd and even rows are displayed in different color, to make it easier to read a single line.
- Version 2.00:
 - Added support for [GeoLite City database](#). You can now download the GeoLite City database (GeoLiteCity.dat.gz), put it in the same folder of smsniff.exe, and SmartSniff will automatically use it to get the country/city information for every IP address.
 - Added 'Auto Size Columns+Headers' option, which allows you to automatically resize the columns according to the row values and column headers.
- Version 1.95:
 - Added Find option (Ctrl+F) to easily find text in the lower pane.
 - Fixed issue: The properties dialog-box and other windows opened in the wrong monitor, on multi-monitors system.
- Version 1.93:
 - Fixed bug: When opening the 'Capture Options' dialog-box after Network Monitor Driver 3.x was previously selected, SmartSniff switched back to Raw Sockets mode.
- Version 1.92:
 - Added accelerator key to the 'URL List' mode (Ctrl+F4)
- Version 1.91:
 - Fixed a crash problem occurred with some Web pages when using the 'Extract HTTP Files' option .
- Version 1.90:
 - Added 'Put Icon On Tray' option.
- Version 1.85:
 - Added 'Use DNS Queries & Cache For Host Names' option. When it's turned on, SmartSniff analyzes the captured DNS queries and uses them for displaying the local/remote host names. The internal DNS cache of Windows is also used.
- Version 1.82:
 - Added 'Duration' column, which displays the difference between the capture time and last packet time.
- Version 1.81:
 - Updated the internal country names list (Added more 14 countries) for using with the IP to country file (IpToCountry.csv).
- Version 1.80:

- Added 'Extract HTTP Files' option (under the File menu), which allows you to easily extract all HTTP files stored in the selected streams, into the folder that you choose.
- Version 1.79:
 - Fixed bug: 'Restart Capture' option caused SmartSniff to crash in some circumstances.
- Version 1.78:
 - Added 'Restart Capture' option (Ctrl+R), which stops the capture and then immediately starts it again.
- Version 1.77:
 - Increased the size of total filter string (Capture Filter and Display Filter) that can be saved into the .cfg file.
- Version 1.76:
 - When 'Retrieve process information while capturing packets' option is turned on, the 'Process User' column now displays the user name of the specified process.
- Version 1.75:
 - Added 'Decompress HTTP Responses' option. When it's turned on, HTTP responses compressed with gzip are automatically detected, and displayed in decompressed form.
- Version 1.72:
 - Fixed bug: The status bar packets counter displayed a little higher value than the total packets counters in the upper pane table.
- Version 1.71:
 - Added 'Hide Lower Pane' option (under the Options menu), which is useful when you work in statistics only mode, and you don't need the lower pane.
- Version 1.70:
 - Added 'Display only active connections' in Advanced Options window. When this options is turned on, SmartSniff automatically hide all streams that their connection was closed. This means that SmartSniff will only display the streams that their connection is still opened.
- Version 1.65:
 - Added support for .csv files in 'Save Packet Summaries' option.
 - Added 'Add Header Line To CSV/Tab-Delimited File' option. When this option is turned on, the column names are added as the first line when you export to csv or tab-delimited file.
- Version 1.63:
 - Added 'Automatically Scroll Down in Live Mode' option, under the

Options menu

- Version 1.62:
 - Added /StartCapture and /LoadConfig command-line options.
 - Added x64 version of SmartSniff, to work with Microsoft Network Monitor Driver 3.x on Windows x64.
- Version 1.60:
 - Added support for capturing with Microsoft Network Monitor 3.x driver. (Very useful for Windows Vista/7 users, because the old Network Monitor driver is not supported in these OS)
 - For Microsoft Network Monitor 3.x driver, there is also 'Wifi Monitor Mode' button which only works under Windows 7/Vista, and only for wireless devices that supports 'Monitor Mode'. When you switch the wireless card to monitor mode, SmartSniff can capture all unencrypted Wifi/TCP streams in the channel that you chose to monitor.
 - Added support for opening the capture file (.cap) of Microsoft Network Monitor 3.x
 - Added support for viewing the content of unencrypted Wifi/TCP streams. This feature works on WinPCap driver and Microsoft Network Monitor 3.x
 - Added 'Promiscuous Mode' check-box for WinPCap and Microsoft Network Monitor 3.x driver. In the previous version, SmartSniff always turned on the 'Promiscuous Mode', but in some wireless adapters, the capture doesn't work at all if Promiscuous Mode is turned on.
- Version 1.53:
 - Fixed bug: SmartSniff displayed a crash message on msvcrt.dll when reading TCP packets with invalid data length.
- Version 1.52:
 - In 'Export TCP/IP Steams' - Added 2 new file types - 'Raw Data Files - Local' and 'Raw Data Files - Remote' for exporting only one side of the stream.
- Version 1.51:
 - Added Drag & Drop support - you can now drag .ssp file from Explorer into the window of SmartSniff.
- Version 1.50:
 - Added 'Last Packet Time' column - Displays the date/time of the last packet received.
 - Added 'Data Speed' column - Displays the calculated speed of the TCP connection in KB per second.

- Version 1.45:
 - New option: Display Outgoing/Incoming Data - When this option is turned on, separated values for outgoing and incoming packets are displayed for the following columns: 'Packets', 'Data Size', and 'Total Size'. The values are displayed in the following format: {Outgoing ; Incoming}
- Version 1.40:
 - Added local/remote MAC addresses (relevant only for local network, and it doesn't work with raw sockets)
 - Added [IPNetInfo](#) integration - When you put IPNetInfo utility in the same folder of SmartSniff, You can view the information about the remote IP addresses.
 - Added IP Country columns to display the country name of IP addresses. (requires to download an external file from [here](#))
- Version 1.38:
 - Under Vista, automatically run as administrator.
- Version 1.37:
 - Fixed bug: The main window lost the focus when the user switched to another application and then returned back to SmartSniff.
- Version 1.36:
 - Fixed bug: SmartSniff hang when you work with 'URL List' mode.
- Version 1.35:
 - New Display Mode - 'URL List': Allows you to view the list of URLs for the select TCP/IP items (only for HTTP protocol)
 - Increased the buffer of raw sockets to avoid packet loss.
 - The configuration is now saved to a file, instead of the Registry.
- Version 1.32:
 - Fixed bug: Wrong capture time displayed when "Only display TCP/IP statistic..." option was selected.
 - Added 'Summary Mode' in Advanced Options - Allows you to view general TCP/IP statistics by addresses only, without adding a separated line for each connection.
- Version 1.31:
 - Added support for Microsoft Network Monitor driver (Under Windows 2000/XP/2003).
- Version 1.30:
 - New option: Only display TCP/IP statistic, do not store the captured data in file.
 - New option: Retrieve process information while capturing packets.

- In 'Load Packets Data From File', you can now choose to load tcpdump/libpcap file saved by Ethereal or by other capture programs.
 - A tooltip is displayed when a string in a column is longer than the column length.
 - When running SmartSniff in the first time, the first found network adapter with IP address is now automatically selected. (In previous versions, the user had to select an adapter in order to start capturing)
- Version 1.21:
 - Fixed Bug: packets in TCP/IP conversations sometimes displayed in wrong order.
- Version 1.20:
 - New option in Live Mode: Display the beginning of TCP/IP conversation content while capturing.
 - Save / Load SmartSniff configuration.
 - Filters are now saved when you exit from SmartSniff, and loaded again in the next time that you run it.
 - Significant improvement in performances of Live Mode when there are a lots of TCP/IP conversations.
 - Fixed bug: pressing F2/F3/F4 while capturing packets in live mode caused the capture to be corrupted.
- Version 1.11: Improve in performances while capturing with WinPcap driver.
- Version 1.10:
 - Performances - Large TCP/IP conversations are now displayed much faster than in previous version.
 - Live Mode - View the TCP/IP conversation list while capturing.
 - Capture and display filters.
 - New option: Resolve IP Addresses to host names (displayed in 'Local Host' and 'Remote Host' columns)
 - New option: On Automatic display mode, don't display data in hex format if the data size is larger than... (The default is 100 KB)
 - New option: In the lower pane, don't display items with data size larger than... (The default is 1000 KB)
 - Added more accelerator keys.
 - XP style support.
- Version 1.00: First release.

Using SmartSniff

In order to start using SmartSniff, simply copy the executable (smsniff.exe) to any folder you like, and run it (installation is not needed).

After running SmartSniff, select "Start Capture" from the File menu, or simply click the green play button in the toolbar. If it's the first time that you use SmartSniff, you'll be asked to select the capture method and the network adapter that you want to use. If WinPcap is installed on your computer, it's recommended to use this method to capture packets.

After selecting the capture method and your network adapter, click the 'OK' button to start capturing TCP/IP packets. While capturing packets, try to browse some Web sites, or retrieve new emails from your email software. After stopping the capture (by clicking the red stop button) SmartSniff displays the list of all TCP/IP conversations that it captured. When you select a specific conversation in the upper pane, the lower pane displays the TCP/IP streams of the selected client-server conversation.

If you want to save the captured packets for viewing them later, use "Save Packets Data To File" option from the File menu.

Display Mode

SmartSniff provides 3 basic modes to display the captured data: Automatic, Ascii, and Hex Dump. On Automatic mode (the default), SmartSniff checks the first bytes of the data stream - If it contains characters lower than 0x20 (excluding CR, LF and tab characters), it displays the data in Hex mode. otherwise, it displays it in Ascii mode.

You can easily switch between display modes by selecting them from the menu, or by using F2 - F4 keys. Be aware that 'Hex Dump' mode is much slower than Ascii mode.

Starting from version 1.35, there is a new mode - 'URL List'. This mode only displays the URL addresses list (http://...) found in the captured packets.

Exporting the captured data

SmartSniff allows you to easily export the captured data for using it in other applications:

- **The upper pane:** you can select one or more items in the upper pane, and then copy them to the clipboard (You can paste the copied items into Excel or into spreadsheet of OpenOffice.org) or save them to text/HTML/XML file (by using 'Save Packet Summaries').
- **The lower pane:** You can select any part of the TCP/IP streams (or select all text, by using Ctrl+A), copy the selected text to the clipboard, and then paste it to Notepad, Wordpad, MS-Word or any other editor. When you paste the selected streams to document of Wordpad, OpenOffice.org, or MS-Word, the colors are also transferred.
You can also export the TCP/IP streams to text file, HTML file, or raw data file, by using "Export TCP/IP Streams" option.

Displaying characters above ASCII 127

By default, characters above ASCII 127 are not displayed in the TCP/IP streams. You can enable high ASCII characters by using "Display Characters Above ASCII 127". When you use this option, the TCP/IP streams are displayed without colors. Be aware that when working in this mode, the loading process of the lower pane might be very slow.

The 'IP Country' columns

In order to watch the countries of the local/remote IP addresses, you have to download the latest IP To Country file from [here](#). You have to put the 'IpToCountry.csv' file in the same folder of smsniff.exe

You can also use the [GeoLite City database](#). Simply download the GeoLite City in Binary / gzip (GeoLiteCity.dat.gz) and put it in the same folder of smsniff.exe. If you want to get faster loading process, extract the GeoLiteCity.dat from the GeoLiteCity.dat.gz and put it in the same folder of smsniff.exe

Capture and Display Filters

Starting from version 1.10, you can filter unwanted TCP/IP activity during the capture process (Capture Filter), or when displaying the captured TCP/IP data (Display Filter).

For both filter types, you can add one or more filter strings (separated by spaces or CRLF) in the following syntax:

[include | exclude] : [local | remote | both] : [tcp | udp | tcpudp | icmp | all] : [IP Range | Ports Range]

Here's some examples that demonstrate how to create a filter string:

- Display only packets with remote tcp port 80 (Web sites):
include:remote:tcp:80
- Display only packets with remote tcp port 80 (Web sites) and udp port 53 (DNS):
include:remote:tcp:80
include:remote:udp:53
- Display only packets originated from the following IP address range: 192.168.0.1 192.168.0.100:
include:remote:all:192.168.0.1-192.168.0.100
- Display only TCP and UDP packets that use the following port range: 53 - 139:
include:both:tcpudp:53-139
- Filter most BitTorrent packets (port 6881):
exclude:both:tcpudp:6881
- Filter all ICMP packets (Ping/Traceroute activity):
exclude:both:icmp

Notice: A single filter string must not include spaces !

Live Mode

Starting from version 1.10, a new option was added to 'Advanced Options' section - 'Live Mode'. When SmartSniff capture packets in live mode, the TCP/IP conversations list is updated while capturing the packets, instead of updating it only after the capture is finished. Be aware that "Live Mode" requires more CPU resources than non-live mode. So if your computer is slow, or your have a very high traffic on your network, it's recommended to turn off this option.

Starting from version 1.20, you can also view the content of each TCP/IP conversation (in the lower pane) while capturing the packets. However, if the TCP/IP conversation is too large, you won't be able to watch the entire TCP/IP

conversation until the capture is stopped.

Viewing process information

Starting from version 1.30, you can view the process information (ProcessID and process filename) for captured TCP packets. However, this feature have some limitations and problems:

- Process information is only displayed for TCP packets (It doesn't work with UDP)
- Process information may not be displayed for TCP connections that closed after short period of time.
- Retrieving process information consume more CPU resources and may slow down your computer. It's not recommended to use this feature if you have intensive network traffic.
- Process information is currently not saved in ssp file.

In order to activate this feature, go to 'Advanced Options' dialog-box, check the "Retrieve process information while capturing packets" option and click the 'OK' button. 2 new columns will be added: ProcessID and Process Filename. Start capturing, and process information will be displayed for the captured TCP conversations.

The structure of .ssp file (SmartSniff Packets File)

The structure of .ssp file saved by SmartSniff is very a simple. It contains one main header in the beginning of the file, followed by sequence of all TCP/IP packets, each of them begins with a small header.

The main header structure:

00 - SMSNF200 signature.

08 - (2 bytes) The number of bytes in the header (currently 4 bytes for the IP Address)

0A - (4 bytes) IP Address

Header of each packet:

00 (2 Bytes) packet header size (currently 0x18 bytes)

02 (4 Bytes) number of received bytes in packet.

06 (8 Bytes) Packet time in Windows FILETIME format.

0E (6 Bytes) Source Mac Address.

14 (6 Bytes) Dest. Mac Address.

1A The remaining bytes are the TCP/IP packet itself.

Translating to other languages

SmartSniff allows you to easily translate all dialog-boxes, menus, and strings to other language.

In order to do that, follow the instructions below:

1. Run SmartSniff with /savelangfile parameter:
smsniff.exe /savelangfile
A file named smsniff_lng.ini will be created in the folder of SmartSniff utility.
2. Open the created language file in Notepad or in any other text editor.
3. Translate all menus, dialog-boxes, and string entries to the desired language.
4. After you finish the translation, Run SmartSniff, and all translated strings will be loaded from the language file.
If you want to run SmartSniff without the translation, simply rename the language file, or move it to another folder.

Command-Line Options

Command	Description
/StartCapture	Start to capture packets immediately.
/LoadConfig <.cfg filename>	Starts SmartSniff with the specified configuration file.
/NoCapDriver	Starts SmartSniff without loading the WinPcap Capture Driver .
/NoLoadSettings	Starts SmartSniff without loading your last settings.

License

This utility is released as freeware. You are allowed to freely distribute this utility via floppy disk, CD-ROM, Internet, or in any other way, as long as you don't charge anything for this. If you distribute this utility, you must include all files in the distribution package, without any modification !

Disclaimer

The software is provided "AS IS" without any warranty, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The author will not be liable for any special, incidental, consequential or indirect damages due to loss of data or any other reason.

Feedback

If you have any problem, suggestion, comment, or you found a bug in my utility, you can send a message to nirsofer@yahoo.com