NirSoft

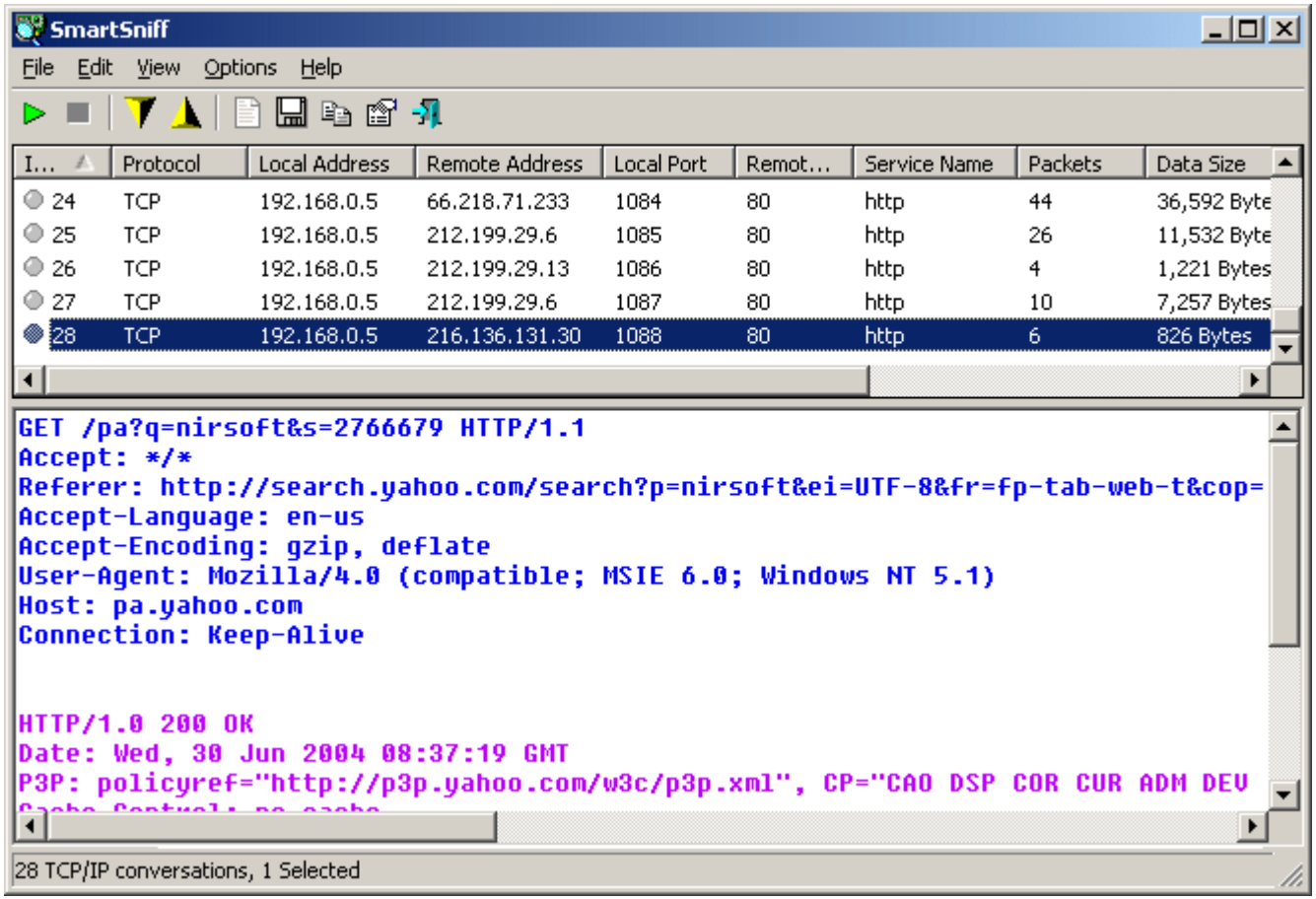
Main Page
Utilities
Passwords
Visual Basic
Visual C++
Components
.NET Tools
Articles
FAQ
TOP 10
Links
Awards
Search
Pad Files
Contact

SmartSniff v1.30

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 2 methods for capturing TCP/IP packets :

- 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.
- WinPcap Capture Driver: Allows you to capture TCP/IP packets on all Windows operating systems. (Windows 98/ME/NT/2000/XP/2003) 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.



System Requirements

SmartSniff can capture TCP/IP packets on any 32-bit Windows operating system (Windows 98/ME/NT/2000/XP) as long as WinPcap capture driver is installed and works properly with your network adapter.
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.

Versions History

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

Display Mode

SmartSniff provides 3 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.

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.
  Your 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.

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:tcpupd: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.

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
/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

Download SmartSniff (In ZIP file)

Download self-install executable for installing SmartSniff with uninstall support

SmartSniff is also available in other languages. In order to change the language of SmartSniff, download the appropriate language zip file, extract the 'smsniff_lng.ini', and put it in the same folder that you Installed SmartSniff utility.

Language	Translated By	Version
Italian	Marco D'Amato	1.30
Polish	wins	1.21
Spanish	Hector Sanjuan	1.00
Traditional Chinese	qq123	1.00
	Xos Antn Vicente Rodrguez	

Galician	http://www.iespana.es/engalego http://engalego.blogspot.com	1.00
Dutch	Bob Loeffen	1.00
Korean	KIM JaeGeun	1.21
French	int24h	1.11
Czech	http://www.martinkozak.czweb.org/	1.11
German	Latino	1.30
Simplified Chinese	yang xiang, Updated to 1.30 by Renda	1.30
Traditional Chinese	Eros	1.21
Taiwanese	Eros	1.21