Comparison of packet analyzers

From Wikipedia, the free encyclopedia

The following tables compare general and technical information for several packet analyzer software utilities, also known as network analyzers or packet sniffers. Please see the individual products' articles for further information.

Contents

General information

Basic general information about the software—creator/company, license/price, etc.

	Creator	Latest release	User interface	Software license	Cost
Analyze This	Comoe Networks (http://comoe-networks.com)		Web GUI	N/A	?
Cain and Abel	Massimiliano Montoro	4.9.56 / April 7, 2014	GUI	Freeware	Free
Capsa	Colasoft (http://www.colasoft.com)	8.3 / 29 March 2016	GUI	Proprietary	$0-$995, depending on version[1]
Carnivore	Federal Bureau of Investigation	?	?	N/A	?
Clarified Analyzer	Clarified Networks		GUI	Proprietary	Non-free
Clusterpoint Network Traffic Surveillance System	Clusterpoint		web GUI	Proprietary	?
CommView	TamoSoft (http://www.tamos.com/)	6.5	GUI	Proprietary	$299-$599, $149 1 year subscription
Debookee	iwaxx (https://debookee.com)	5.1.0 / May 18, 2016	GUI	Proprietary	$29.90-$69.90
dSniff	Dug Song	2.3 / December 17, 2000[2]	CLI	BSD License	Free
EtherApe	Juan Toledo	0.9.14 / February 6, 2016[3]	GUI	GNU General Public License	Free
Ettercap	ALoR and NaGA	0.8.2-Ferri / March 14, 2015[4]	Both	GNU General Public License	Free
Fiddler	Eric Lawrence	4.6.3.50306 / 9 December 2016	GUI	Freeware	Free
justniffer	The Justniffer team	0.5.15 / March 21, 2016[5]	CLI	GNU General Public License	Free
Kismet	Mike Kershaw (dragorn)	2016-01-R1 / January 31, 2016[6]	CLI	GNU General Public License	Free
Microsoft Message Analyzer	Microsoft	1.4 / October 28, 2016 [7]	GUI	Proprietary	Free
Microsoft Network Monitor	Microsoft	3.4 / June 24, 2010	GUI	Proprietary	Free
netsniff-ng	Daniel Borkmann	0.6.2 / November 7, 2016	CLI	GNU General Public License	Free
ngrep	Jordan Ritter	1.45 *(11/18/06)*	CLI	BSD-style	Free
Observer	Viavi Solutions (formerly Network Instruments)		GUI	Proprietary	Price on request
OmniPeek (formerly AiroPeek, EtherPeek)	Savvius (formerly WildPackets) (https://www.savvius.com/)	9.2 / May 27, 2016	GUI	Proprietary	$1194-$5994, depending on version[8]
SteelCentral Transaction Analyzer	OPNET Technologies/Riverbed Technology	17.0.T-PL1 / June 9, 2014[9]	GUI	Proprietary	Non-free
snoop	Sun Microsystems	Solaris 10 / December 11, 2006	CLI	CDDL	Free

	Creator	Latest release	User interface	Software license	Cost
tcpdump	The Tcpdump team	4.8.1 / October 25, 2016[10]	CLI	BSD License	Free
Wireshark (formerly Ethereal)	The Wireshark team	2.2.2 / November 16, 2016	Both	GNU General Public License	Free
Xplico	The Xplico team	1.1.2 / January 10, 2016[11]	Both	GNU General Public License	Free

Operating system support

The utilities can run on these operating systems.

Client	Microsoft Windows	macOS	Linux	BSDs	Solaris	Other
Cain and Abel	Yes	No	No	No	No	No
Capsa Free Edition	Yes	No	No	No	No	No
Carnivore	Yes	No	No	No	No	No
Clarified Analyzer	Yes	Yes	Yes	No	No	?
Clusterpoint Network Traffic Surveillance System	Yes	Yes	Yes	Yes	No	Any virtual-machine compatible OS
CommView	Yes	No	No	No	No	No
Debookee	No	Yes	No	No	No	No
dSniff	?	Yes	Yes	Yes	Yes	?
EtherApe	No	Yes	Yes	Yes	Yes	?
Ettercap	Yes	Yes	Yes	Yes	Yes	?
justniffer	No	Yes	Yes	Yes	Yes	?
Kismet	Yes	Yes	Yes	Yes	?	?
LANMeter	No	No	No	No	No	Fluke proprietary hardware
netsniff-ng	No	No	Yes	No	No	No
ngrep	Yes	Yes	Yes	Yes	Yes	AIX, BeOS, HP-UX, IRIX, Tru64 UNIX
Microsoft Network Monitor	Yes	No	No	No	No	No
Observer	Yes	No	No	No	No	No
OmniPeek (formerly AiroPeek, EtherPeek)	Yes	No	No	No	No	No
SteelCentral Transaction Analyzer	Yes	Version 3.5 capture agents on PowerPC only	GUI, plus version 3.5 capture agents	No	Version 3.5 capture agents on SPARC only	Version 3.5 capture agents on AIX and PA-RISC HP-UX only
snoop	No	No	No	No	Yes	No
tcpdump	Yes (WinDump)	Yes	Yes	Yes	Yes	AIX, HP-UX, IRIX, Tru64 UNIX
Wireshark (formerly Ethereal)	Yes	Yes	Yes	Yes	Yes	AIX, HP-UX, IRIX, Tru64 UNIX
Xplico	No	No	Yes	No	No	No

Features

	Process grouping	Monitor mode	Capture filter
Wireshark	?	?	?

References

1. "Capsa Enterprise Edition & Professional Edition & Free Edition - Colasoft".
2. "CHANGES". *www.monkey.org*.
3. "EtherApe, a graphical network monitor". *etherape.sourceforge.net*. Retrieved 2016-12-13.
4. "Downloads « Ettercap". *ettercap.github.io*. Retrieved 2015-12-11.
5. "justniffer - Browse /justniffer at SourceForge.net". *sourceforge.net*. Retrieved 2016-12-13.
6. "Kismet". *www.kismetwireless.net*. Retrieved 2016-06-03.
7. https://www.microsoft.com/en-us/download/details.aspx?id=44226
8. "store.savvius.com".
9. https://support.riverbed.com/content/support/software/steelcentral-npm/transaction-analyzer.html
10. tcpdump. "Tcpdump/Libpcap public repository". *www.tcpdump.org*. Retrieved 2016-12-13.
11. http://www.xplico.org/archives/1472

Retrieved from "https://en.wikipedia.org/w/index.php?title=Comparison_of_packet_analyzers&oldid=773862411"

Categories: Network software comparisons | Network analyzers

- This page was last modified on 4 April 2017, at 21:16.
-