Appendix B
Open-source/Free PCAP Compatible Tools

List of open-source PCAP compatible tools (probably incomplete!)

****IX Based Tools**

Name	Website
Argus	https://www.qosient.com/argus/
Barnyard2	https://www.forensicswiki.org/wiki/Barnyard2
Bro/Zeek	https://www.zeek.org/
Chaosreader	http://chaosreader.sourceforge.net/
Daemonlogger	https://github.com/Cisco-Talos/Daemonlogger/releases/tag/v1.2.1
Driftnet	http://www.ex-parrot.com/~chris/driftnet/
Etherape	https://etherape.sourceforge.io/
GrassMarlin	https://github.com/nsacyber/GRASSMARLIN
Libpcap	https://www.tcpdump.org/
Mergecap	https://www.wireshark.org/docs/man-pages/mergecap.html
Moloch	https://github.com/aol/moloch
Net::Pcap	https://search.cpan.org/~kcarnut/Net-Pcap-0.05/Pcap.pm
Net::Pcap::Easy	https://search.cpan.org/~jettero/Net-Pcap-Easy-1.4207/Easy.pod
Netsniff-ng	http://netsniff-ng.org/
Nftracker	https://github.com/gamelinux/nftracker
Ngrep	https://github.com/jpr5/ngrep/
OSSEC	http://www.ossec.net/
Pcapcat	http://blog.kiddaland.net/dw/pcapcat
Securityonion	https://securityonion.net/
Sniffit	http://sniffit.sourceforge.net/
Snort	https://www.snort.org/
Suricata	https://suricata-ids.org/
Tcpdump	https://www.tcpdump.org/
Tcpick	http://tcpick.sourceforge.net/
Tcpreplay	https://tcpreplay.appneta.com/
Tcpslice	https://sourceforge.net/projects/tcpslice/
Tcpstat	https://www.frenchfries.net/paul/tcpstat/
Tcpxtract	http://tcpxtract.sourceforge.net/
Tshark	https://www.wireshark.org/docs/man-pages/tshark.html
Vortex	http://sourceforge.net/projects/vortex-ids/
Wireshark	https://www.wireshark.org/
Xplico	https://www.xplico.org/

Windows Based Tools

Name	**IX tool	Website
GrassMarlin		https://github.com/nsacyber/GRASSMARLIN
NetworkMiner		https://www.netresec.com/?page=Networkminer
Windump	Tcpdump	http://www.winpcap.org/windump/
Winpcap	Libpcap	http://www.winpcap.org
Wnetp::Pcap	Net::Pcap	http://www.bribes.org/perl/wnetpcap.html
Winsnort	Snort	http://www.winsnort.com/
Wireshark		http://www.wireshark.org/