Summary of tools commonly used to support network forensic investigations

Key:

C=Collection & filtering	R=correlation and analysis of multiple raw data sources
L=Logfile analysis	A= Application layer viewer
S= Stream reassembly	W=Workflow or case management

Name	Provider	Platform	Features
TCPDump, Windump	Open Source www.tcpdump.org	Unix, Windows	C
Ngrep	Open source http://ngrep.sourceforge.net/	Unix	C
Network Stumbler	Open source http://www.netstumbler.com/	Windows	C
Kismet	Open source http://www.kismetwireless.net	Unix Windows	C
Argus	Open Source http://www.qosient.com/argus/index.htm	Unix	CL
Flow-tools	Open Source http://www.splintered.net/sw/flow-tools/	Unix	CL
Flow-extract, Flow Scripts	Open Source http://security.uchicago.edu/tools/net-forensics/	Unix	L
Etherape	Open Source http://etherape.sourceforge.net/	Unix	C
Snort	Open Source www.snort.org	Unix	C
Observer	Network Instruments http://www.networkinstruments.com/	Appliance	C
Honeyd	Honey source http://www.citi.umich.edu/u/provos/honeyd/	Unix	C

Ethereal	Open Source www.Ethereal.com	Windows Unix	CLS
Etherpeek	Wild Packets, Inc. www.wildpackets.com	Windows	CLS
SecureNet	Intrusion Inc. http://www.intrusion.com	Windows with collector appliance	CS
FLAG Forensic and Log Analysis GUI	Open Source http://www.dsd.gov.au/library/software/flag/	Unix	L
ACID	Analysis Console for Intrusion Databases http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html	Unix	L
Shadow	http://www.nswc.navy.mil/ISSEC/CID/index.html	Unix	LS
DeepNines and Sleuth9	http://www.deepnines.com/sleuth9.html	Unix	CSR
Infinistream	Network Associates http://www.networkassociates.com/us/promos/sniffer/infinistream.asp	Appliance	CSR
Dragon IDS	Enterasys http://www.enterasys.com/	Unix	CLSR
NSM Incident Response	Intellitactics http://www.intellitactics.com/	Windows	CLSRW
neuSecure	GuardedNet http://www.guarded.net/investigation.html	Unix	CLSRW
NetDetector	Niksun http://www.niksun.com/	Appliance	CSRA
NetIntercept	Sandstorm Tech http://www.sandstorm.net/products/netintercept/	'Bundled Software' (dedicated Linux box)	CSRA
NetWitness	Forensics Explorers http://www.forensicsexplorers.com/	Windows	CLSRA