Useful Analyst Tools

OS	Tool	Details
⊞	`Autoruns`	Sysinternals tool
⊞ 🐧	`ophcrack`	Cracks Windows log-in passwords by using LM hashes through rainbow tables.
⊞ 🐧	`Autopsy`	Digital forensics platform and part of The Sleuth Kit
⊞ 🐧	`UPX`	UPX is an open source executable packer.
🐧	`DNSRecon`	A powerful DNS enumeration script
🐧	`theHarvester`	Gather emails, subdomains, hosts, employee names, open ports and banners from different public sources.
🐧	`FOCA`	Fingerprinting Organizations with Collected Archives. Used to find metadata and hidden information within documents
🤖	`zANTI`	Mobile penetration test toolkit with packet capture.
🐧	`arpspoof`	Used for arp poisoning attacks.
🐧	`DEFT`	Linux Distro with open source computer forensic tools.
⊞ 🐧	`FTK Imager`	Data preview and imaging tool used to acquire data in a forensically sound manner
⊞	`NetworkMiner`	Packet analyser
⊞ 🐧	`Wireshark`	
⊞ 🐧	`Log2Time`	Timeline generation and analysis.
⊞ 🐧	`GN3`	Network hardware emulation
⊞ 🐧	`Volatility`	Memory forensics framework
⊞	`Memoryze`	Command-line utility that allows advanced memory analysis even while your machine is running.
🐧	`p0f`	Passive TCP/IP stack OS fingerprinting tool.
🐧	`pdfinfo`	Document information extractor
🐧	`netcat`	Utility for reading from and writing to network connections
🐧	`tcptool`	
🐧	`pcapcat`	Extract files from captured TCP sessions.
⊞ 🐧	`tcpextract`	
⊞	`PEid`	Detects most common packers, cryptors and compilers for PE files.
⊞ 🐧	`FLOSS`	Extract, and decode obfuscated strings in Windows Portable Executable files.
⊞	`Resource Hacker`	Extraction utility and resource compiler