NETCAP Cheatsheet

> Documentation: docs.netcap.io

Command	Description
netcap -iface eth0	Read traffic live from interface, stop with *Ctrl-C* (*SIGINT*)
netcap -r traffic.pcap	Read traffic from a dump file (supports PCAP or PCAPNG)
netcap -r TCP.ncap.gz	Read a netcap dumpfile and print to stdout as CSV
netcap -fields -r TCP.ncap.gz	Show the available fields for a specific Netcap dump file
netcap -r TCP.ncap.gz -select Timestamp,SrcPort,DstPort	Print only selected fields and output as CSV
netcap -r TCP.ncap.gz -select Timestamp,SrcPort,DstPort > tcp.csv	Save CSV output to file
netcap -r TPC.ncap.gz -tsv	Print output separated with tabs
netcap -workers 24 -buf false -comp false -r traffic.pcapng	Run with 24 workers and disable gzip compression and buffering
netcap -r traffic.pcap -out traffic_ncap	Parse pcap and write all data to output directory (will be created if it does not exist)
netcap -r TCP.ncap.gz -select Timestamp,SrcPort,Dstport -utc	Convert timestamps to UTC
netcap -r TCP.ncap.gz -header	Show audit record header
netcap -r TCP.ncap.gz -struc	Print structured audit records
netcap -r TCP.ncap.gz -tsv	Print audit records as Tab Separated Values
netcap -r UDP.ncap.gz -table	Print as table
netcap -r TCP.ncap.gz -sep ";"	Print audit records with Custom Separator
netcap -r TCP.ncap.gz -check	Check if generated output contains the correct number of separator symbols
netcap-server -gen-keypair	generate keypair for distributed collection and write to disk
netcap -server -privkey priv.key -addr 127.0.0.1:4200	start collection server
netcap -sensor -pubkey pub.key -addr 127.0.0.1:4200	start a sensor agent for exporting data
netcap -iface en0 -bpf "host 192.168.1.1"	apply a BPF when capturing traffic live
netcap -r traffic.pcap -bpf "host 192.168.1.1"	apply a BPF when parsing a dumpfile
netcap -r traffic.pcap -include Ethernet,Dot1Q,IPv4,IPv6,TCP,UDP,DNS	Include specific encoders (only those named will be used)
netcap -r traffic.pcap -exclude TCP,UDP	Exclude encoders (this will prevent decoding of layers encapsulated by the excluded ones)
netcap -r UDP.ncap.gz -fields	Show available fields for the audit record type