Relevant flags	Corresponding tcpdump functionality
-D	Display available interfaces.
-n	Don't convert addresses (i.e., host addresses, port numbers, etc.) to names.
-nn	Stop Domain Name translation and lookups (Host names or port names).
-c count	Exit after receving count number of packets. (Here, count = 20)
-w file	Write the raw packets to file rather than parsing and printing them out.
-r file	Read packets from file (which was created with the -w option)
-ttt	Print a delta (micro-second resolution) between current and previous line on each dump line.
-A	Print packet information in Ascii format. Handy for capturing web pages.
host	Capture packets from specific hosts.
src	Capture packets from specific source.
dst	Capture packets from specific destination.
[port]	Capture packets from specific port.
-s snaplen	Snarf snaplen bytes of data from each packet.Setting snaplen to 0 sets it to the default of 262144.
	Setting snaplen to 0 sets it to the default of 262144.
-e	Print the link-level header on each dump line. This can be used, for example,
	to print MAC layer addresses for protocols such as Ethernet and IEEE 802.11.
-i interface	Listen on interface. If unspecified, tcpdump searches the system interface list
	for the lowest numbered, configured up interface (excluding loopback), which may be, for eg, eth0.
expression	Selects which packets will be dumped. If no expression is given, all packets on the net will be dumped.
	Otherwise, packets for which expression is true will be dumped.For expression syntax, see pcap-filter(7).