tcpdump

Quick Reference

By Harrison Kong @ Coursera

```
sudo tcpdump [options] [expression]
```

Task 1

Introduction and Project Overview

Stop after capturing *n* packets	`tcpdump -c n`
Add line numbers before captured packets	`tcpdump -#`
Show captured packets in ASCII	`tcpdump -A`
Show captured packets in hexadecimal	`tcpdump -XX`
Show human readable capture time	`tcpdump -tttt`

Task 2

Create Shell Script and Explore More Options

List all network interfaces	`tcpdump -D`
Only capture traffic in interface *abc*	`tcpdump -i abc`

Mixing display format shorthand options

Simply concatenate them after a single hyphen

e.g. `tcpdump -#XXtttt`

Mixing other shorthand options

Simply list them all with separate hyphens

e.g. `tcpdump -#XX -c 10`

Only capture traffic to/from host ***xyz.com***	`tcpdump host xyz.com`
Only capture traffic to/from IP ***11.222.33.444***	`tcpdump host 11.222.33.444`
Only capture traffic through port ***443***	`tcpdump port 443`
Only capture outgoing traffic to ***xyz.com***	`tcpdump dst xyz.com`
Only capture incoming traffic from ***xyz.com***	`tcpdump src xyz.com`

Mixing whole word options

Use *and*, *or*

e.g. `tcpdump host 11.222.33.444 and port 443`

Task 3

Create and Read Dump Files

Write capture to file ***abc.pcap***	`tcpdump -w abc.pcap`
read saved capture file ***abc.pcap***	`tcpdump -r abc.pcap`

Task 4

Create sequence of dump files with size and time limits

Capture every ***n*** seconds	`tcpdump -G n`
Limited captured file size to ***n*** million bytes	`tcpdump -C n`
