NETWORK ANALYSIS

ANALYZE NETWORK TRAFFIC FILES USING PYTHON

AGENDA - PART ONE

TASK 1

STANDARDIZED PORTS

Sorted by generated traffic

TASK 2

IP ADDRESSES

Top 10 of the IP addresses, sorted by generated traffic

TASK 3

TRANSPORT LEVEL TRAFFIC

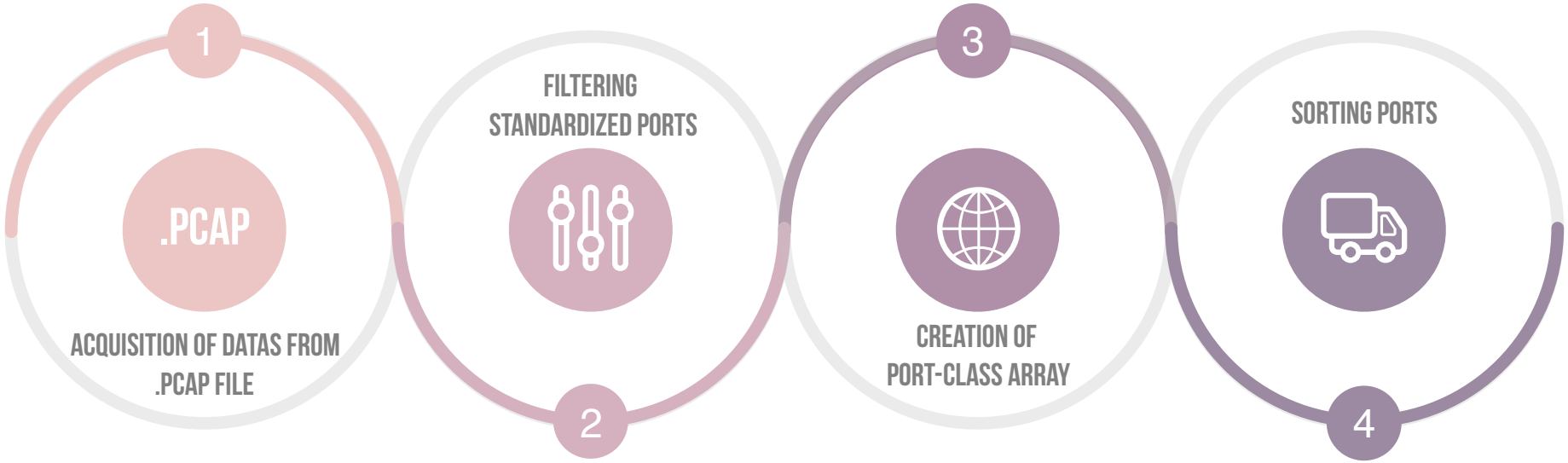
Transport level information related to the top 10 IPs

TASK 4

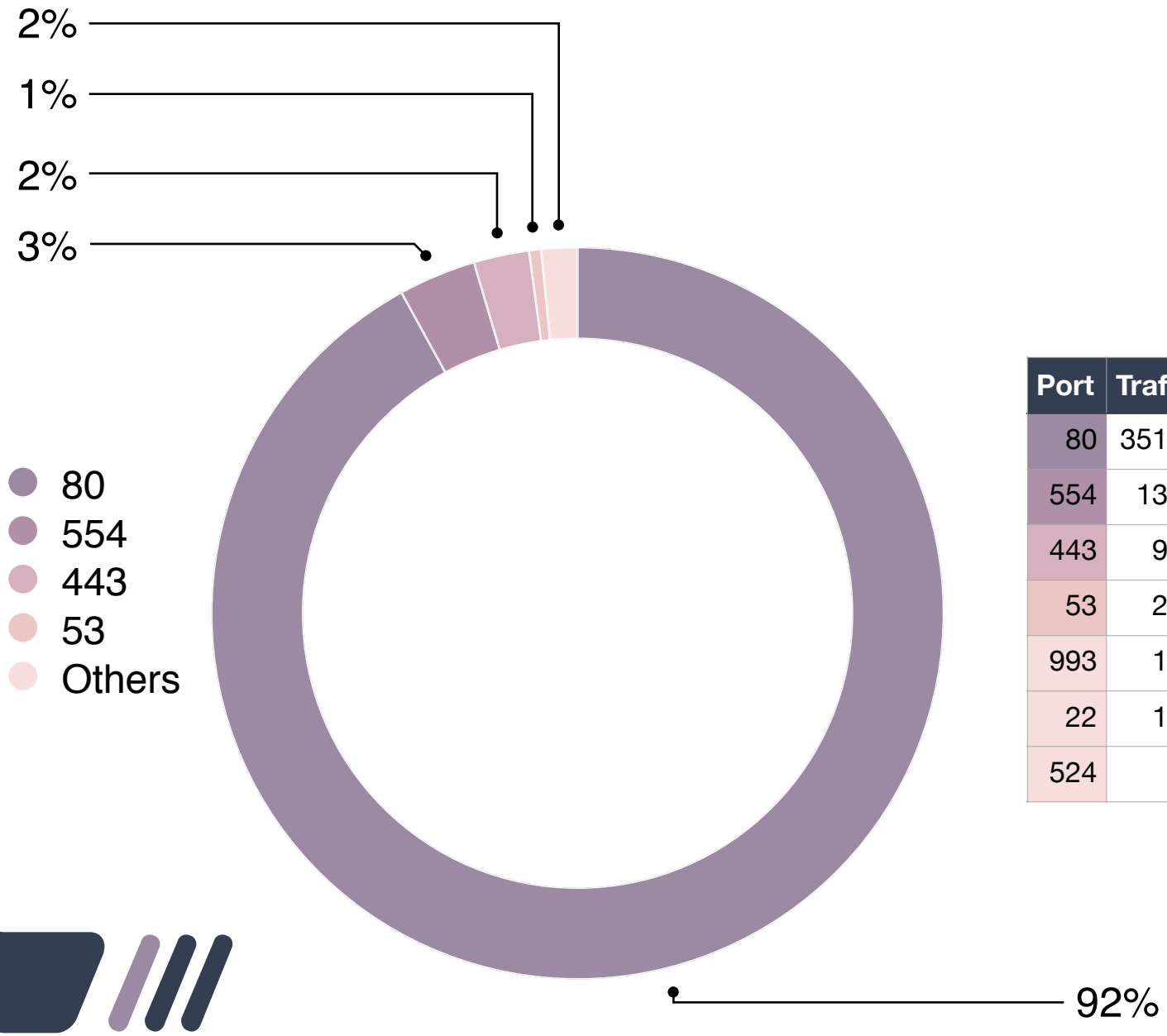
TIMES TO LIVE

Minimum, maximum, average and variance of the TTL values

TASK 1

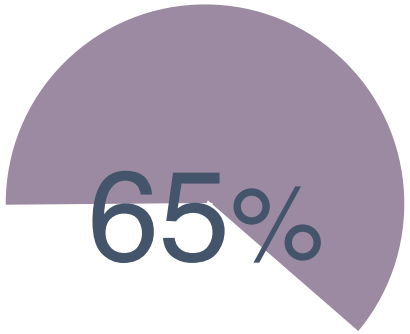

1
.PCAP
ACQUISITION OF DATAS FROM .PCAP FILE
FILTERING STANDARDIZED PORTS
2
3
CREATION OF PORT-CLASS ARRAY
SORTING PORTS
4

TASK 1



Port	Traffic	Port	Traffic	Port	Traffic	Port	Traffic	Port	Traffic
80	351463079	161	436475	25	18455	137	2184	445	320
554	13066481	20	409888	427	17840	636	1388	113	240
443	9363860	995	164968	68	10800	414	1140	26	68
53	2017664	110	89870	23	8531	500	1044	648	66
993	1845039	123	62624	520	4840	21	882	61	65
22	1232237	143	48579	631	4451	843	776	72	64
524	995130	1	35992	138	2289	404	608	808	60

IP	traffic
147.32.80.13	114682057
205.196.123.103	84306631
147.32.85.103	34011735
209.85.149.141	17022600
195.113.232.91	12576824
94.124.104.196	11886368
147.32.84.2	9903506
147.32.84.229	7987983
87.248.203.254	6724441
109.183.212.236	6394424



TRAFFIC GENERATED BY THE FIRST 2 IPS
IN THE TOP 10

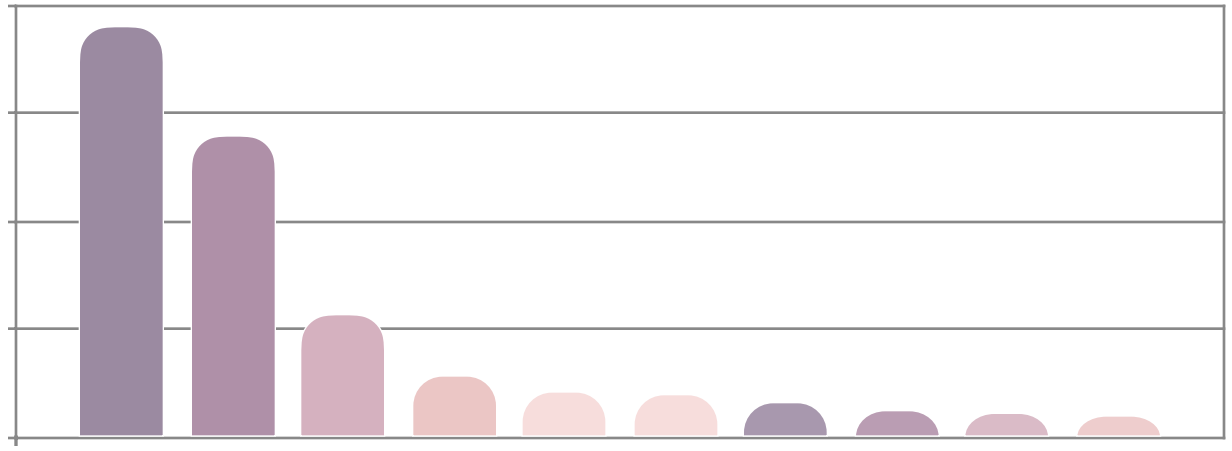
TASK 2

.PCAP

ACQUISITION OF DATAS FROM
.PCAP FILE

CALCULATION OF TOTAL TRAFFIC FOR IP

CREATION OF AN IP LIST



SORTING THE IP ADDRESSES,
BASED ON THEIR OVERALL TRAFFIC

TASK 3

First idea

Use scapy.sniff on the whole .pcap file. In the packets list, look for packs with IP in the top 10. For each of those packs, list all the protocols, sources and destinations and for each of these fields calculate the maximum total traffic

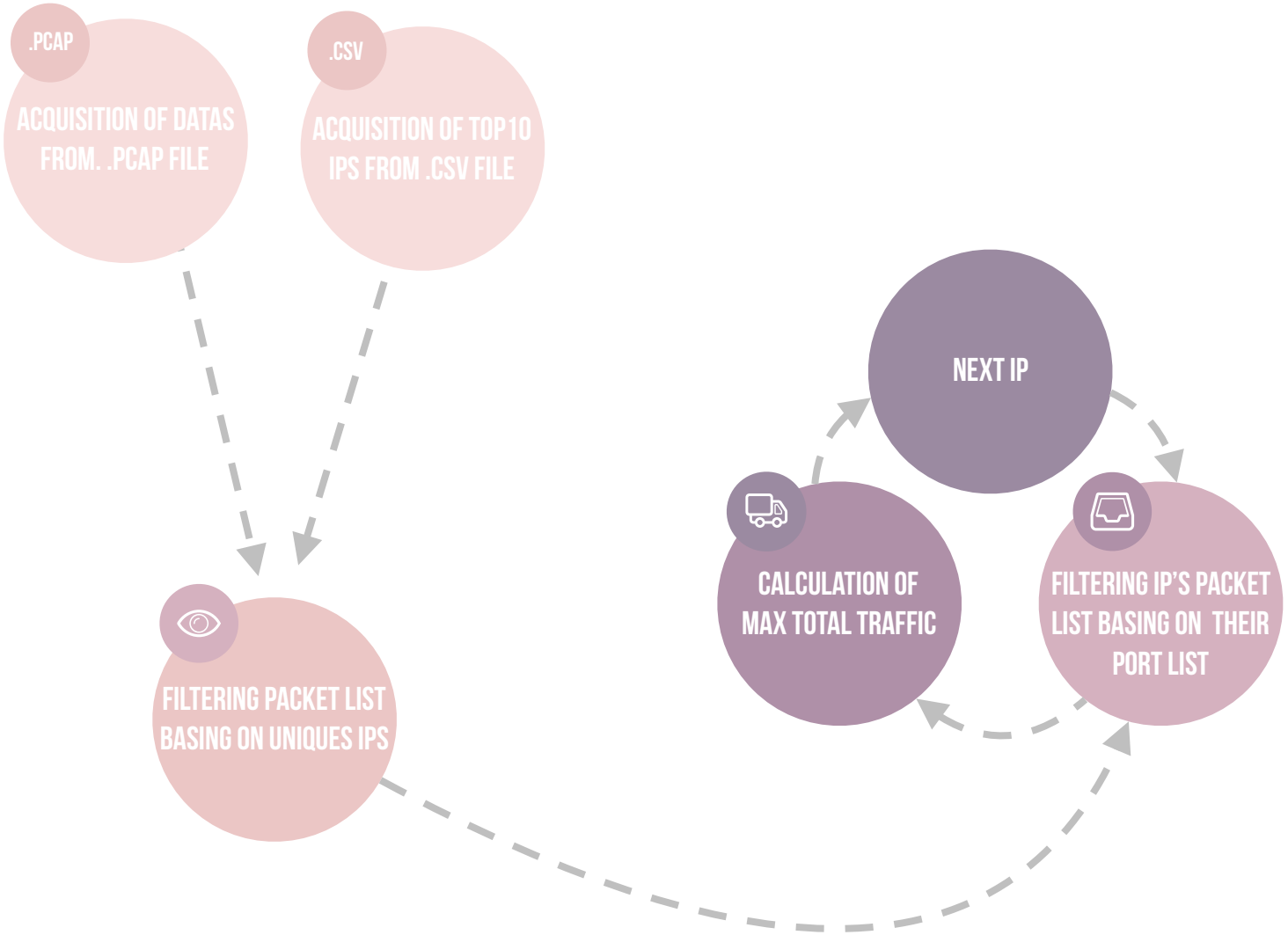
- ✓ FASTER WITH SMALL LOADS OF DATA
- ✗ EXTREMELY SLOWER WHEN THERE ARE MANY PORTS AND PROTOCOLS

Second idea

Use scapy.sniff(filter=src IP) for each address in the top 10. For each filtered list, get protcols, source and destination ports and filter again the list basing on each of those, then evaluate maximum traffic.

- ✓ CAN QUICKLY PROCESS BIG AMOUNTS OF DATA
- ✗ GENERALLY SLOWER ON SMALL CHUNKS OF DATA, DUE TO THE COST OF THE SNIFF FUNCTION

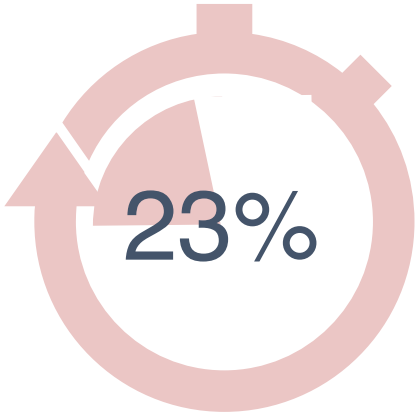
TASK 3


.PCAP
ACQUISITION OF DATAS FROM. .PCAP FILE
.CSV
ACQUISITION OF TOP10 IPS FROM .CSV FILE
FILTERING PACKET LIST BASING ON UNIQUES IPS
CALCULATION OF MAX TOTAL TRAFFIC
NEXT IP
FILTERING IP'S PACKET LIST BASING ON THEIR PORT LIST

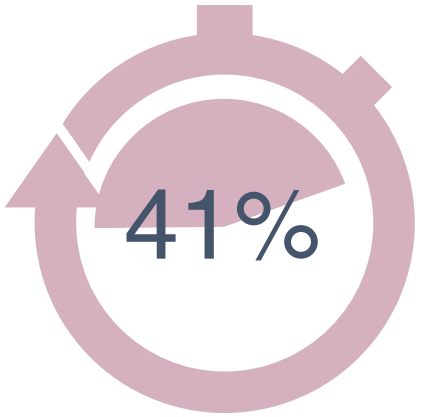
TASK 3

ip_addr	amount_of_total_traffic	protocol	amount_of_traffic_for_specific_protocol	source_port	amount_for_spec_source_port	destination_port	amount_for_spec_destination_port
147.32.80.13	114682057	6	113995003	80	113205544	10885	105681736
205.196.123.103	84306631	6	84306631	80	84306631	1714	84306631
147.32.85.103	34011735	6	34010348	49317	33933768	22	33933768
209.85.149.141	17022600	6	17022600	80	17022600	57717	4963022
195.113.232.91	12576824	6	12576824	80	12575857	49296	4923843
94.124.104.196	11886368	6	11886368	80	11886368	49504	5382092
147.32.84.2	9903506	6	9902923	80	9887437	62614	5505461
147.32.84.229	7987983	17	5885063	13363	6945590	59656	50217
87.248.203.254	6724441	6	6724441	80	6724441	49918	4247739
109.183.212.236	6394424	6	6394424	61775	6394424	20	6394424

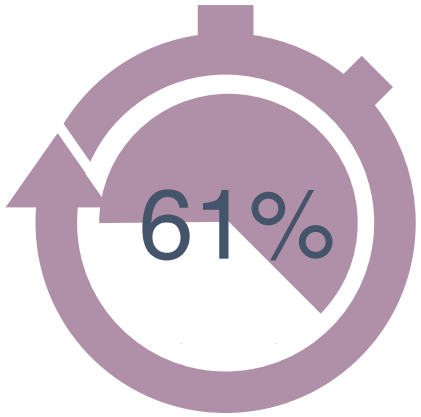
TASK 4



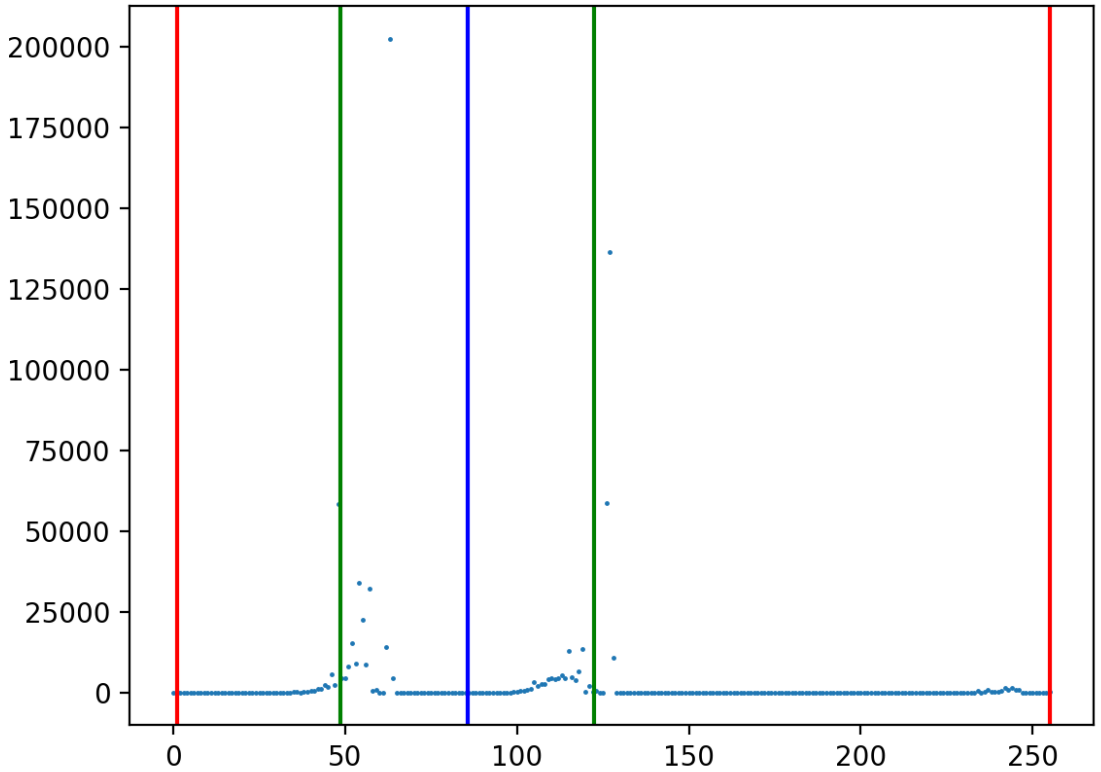
OVER 200K PACKS WITH TTL=64,
STANDARD TTL VALUE FOR LINUX-BASED SYSTEMS



PACKS WITH TTL>AVERAGE(85)



PACKS WITH TTL WITHIN THE VARIANCE



min	max	average	variance
1	255	85,524	1355,404

AGENDA - CREATIVE TASK

PART 1

SCATTER PLOT

With individual IP addresses
- size depending on their traffic

PART 2

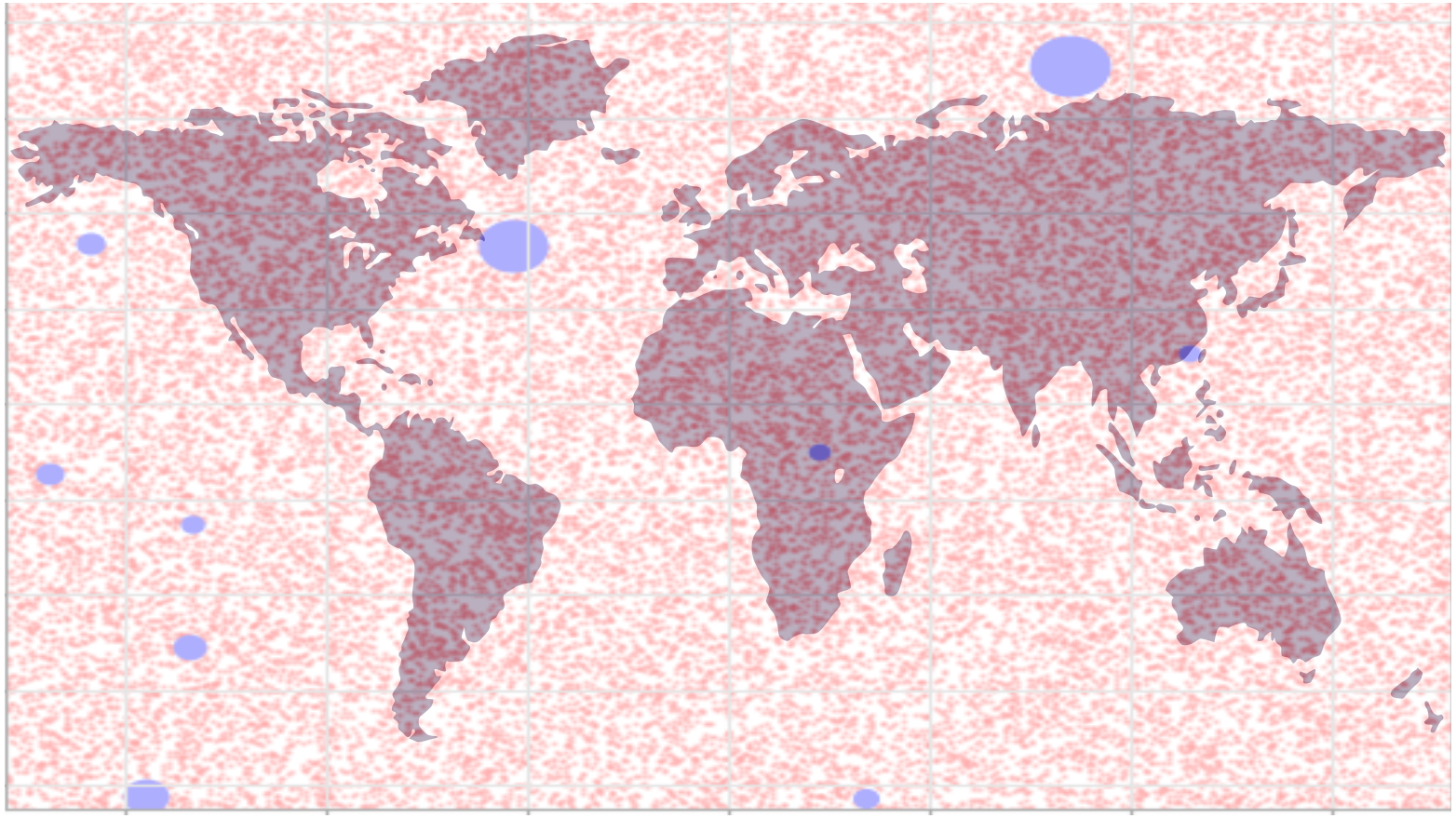
HEATMAP

Of busiest geographical zones
- traffic-wise

CREATIVE TASK - PART ONE

.PCAP

PLOT



CREATIVE TASK - PART TWO