About the data:

This data is a derivative of: http://www.caida.org/data/passive/telescope-educational_dataset.xml It is from a network telescope (aka darknet). http://www.caida.org/projects/network_telescope/

Instructions:

Color in all letters listed with the correct answer to a question. The result is a picture of an animal loved by CSE Students.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
Question 1																	
Question 2																	
Question 3																	
Question 4																	
Question 5																	
Question 6																	
Question 7																	
Question 8																	
Question 9																	
Question 10																	
Question 11																	
Question 12																	

Question 1: (**running tcpdump**) The UCSD-NT is a /8 darknet. Which class A network is it, according to this file (it's been anonymized)?

- 0 [i.e., all darknet IPs match 0.*.*.*] - (B, C, D, E, F, G, H, I, J, K, L, M, N, O, P)
- 10 – (A, C, E, G, I, K, L, O, Q)
- 132 – (B, D, J, N, P, Q)

Question 2: (**options**) The 5th packet has a correct IP checksum

- True - (C, D, F, N, O, Q)
- False – (A, B, E, F, L, M, P, Q)

Question 3: (**ip addresses**) The IP 245.169.35.188 is infected with Conficker. Which port does this worm attempt to propagate on?

- TCP/2566 – (A, B, E, F, I, J, M, N)
- UDP/2566 - (C, D, G, H, P, Q)
- TCP/445 – (A, D, N, Q)
- UDP/445 – (B, C, O, P)

Question 4: (**ip addresses**) The IP 222.210.238.84 is scanning on TCP port 23. Does it scan addresses outside of 0.215.0.0/16?

- Yes – (B, D, K, L, M)
- No – (A, B, F, L, P, Q)

Question 5: (**protocols**) What is the destination IP of the 8th UDP packet?

- 0.120.255.41 – (A, B, C, O, P, Q)
- 0.111.3.133 – (B, C, I, J, K, O, P)
- 0.121.72.141 – (H, I, J)

Question 6: (**protocols**) Which protocols other than TCP and UDP are used?

- ICMP – (C, E, F, G, O)
- Protocol 41 - (B, E, F, J, K, P)
- Both – (C, I, J, K, O)

Question 7: (**ports**) How many packets are sent to 0.27.2.2 on destination port 80?

- 3 – (B, C, J, L, P)
- 11 – (C, G, J, L, O)
- 13 – (B, C, L, O, P)
- 35 – (A, B, H, L, P)

Question 8: (**ports**) How many packets have both source port UDP/5060 and destination UDP/5060?

- 0 – (C, D, N, O)
- 199 – (B, F, G, H, N)
- 201 – (C, H, I, J, K, O)
- 1000 – (A, C, H, O, Q)

Question 9: (**indexing**) How many ICMP echo request packets are in this file? The ICMP header format is [type (1 byte)][code (1 byte)][checksum (2 bytes)]. ICMP echo requests have type=8.

- 0 – (B, C, O, P)
- 1000 – (D, E, F, M, N, O)
- 1019 – (C, D, I, J, N, O)
- 2039 – (B, K)

Question 10: (**indexing**) What is the source IP of the first packet with IP checksum 0xea08?

- 34.62.94.79 – (B, C, E, F, L, M, O, P)
- 150.26.54.148 – (A, D, K, N, Q)
- 0.27.2.2 – (B, C, O, P)

Question 11: (**bit operations and comparisons**) Normal TCP connections start with the client sending a SYN packet, and the server responding with a SYN-ACK packet. In a spoofed DoS attack, a darknet may receive SYN-ACK packets from the attacked machine. Which IP sent SYN-ACK packets in response to this type of attack?

- 37.226.32.239 – (B, C, D, N, O, P)
- 70.170.51.79 – (A, B, D, N, P, Q)
- 186.96.173.213 - (A, D, J, K, L, N, Q)

Question 12: (**bit operations and comparisons**) Conficker has a bug in its pseudorandom number generator. As a result only certain darknet IPs are sent Conficker traffic. Which expressions characterize darknet IPs (A.B.C.D) that are sent traffic? Look at source IP 245.169.35.188.

- B is even - (B, C, D, E, F, G, H, I, J, K, L, M, N, O, P)
- B < 128 – (A, D, N, Q)