4a) Most of the background traffic are a result of port scans, worm activities, misconfigured hardware and leaks from the private networks.

Details:

1. Port Scans: - The port scanning is predominantly for and by the windows systems for the well-known vulnerabilities.

2. Worm Activities: - In general, Conficker worm is responsible for huge background traffic generated by viruses looking for the new victims.

4b)

i) 10.10.1.2

ii) 64

iii) 6 by using tcp.flags.syn==1 && tcp.flags.ack==0

iv) 1.5 sec

v) Yes

List of figures:

4_b_1: DNS packet

4_b_2: Number of http request generated.

4_b_3: Number of TCP connections opened.

4_b_3_1: Verification on number of TCP connection by going to statitics->conversation.

4_b_3_1_a to 4_b_3_1_f: TCP Headers

4_b_4: Webpage loading time.

4_b_5: TCP Losses

4_b_6: IP Headers