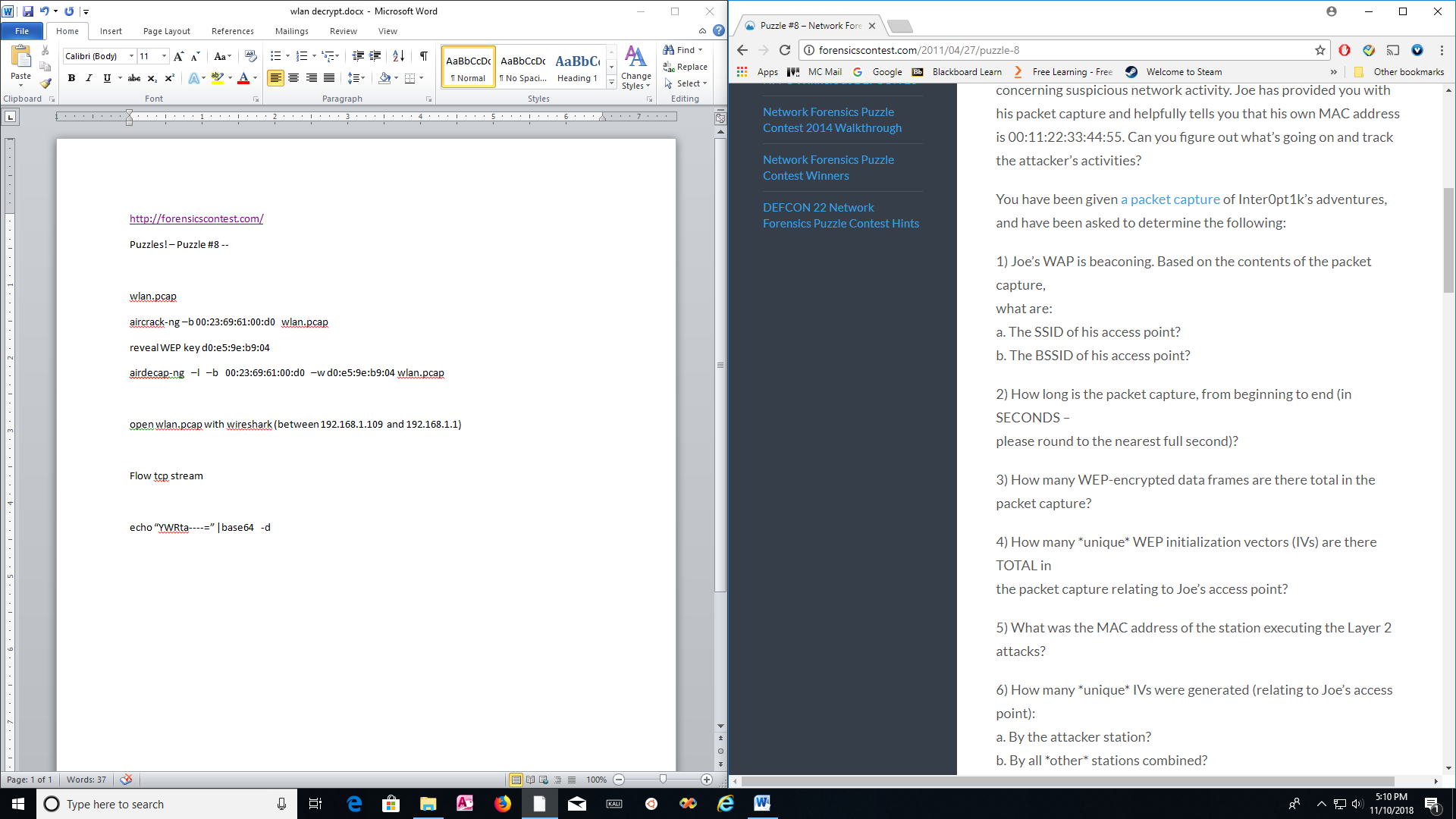
<http://forensicscontest.com/>

Puzzles! – Puzzle #8 --



evidence08.pcap

aircrack-ng –b 00:23:69:61:00:d0 evidence08.pcap

reveal WEP key d0:e5:9e:b9:04

airdecap-ng –l –b 00:23:69:61:00:d0 –w d0:e5:9e:b9:04 evidence08.pcap

<http://linux-commands-examples.com/airdecap-ng>

open (decap file from evidence08.pcap) with wireshark (between 192.168.1.109 and 192.168.1.1)

Flow tcp stream

echo “YWRta----=” |base64 -d