מבוא לרשתות

מגמים
תכנית הסייבר הלאומית

פילטרים נפוצים ל-Wireshark

סינון לפי פרוטוקול	
פרוטוקול (תמיד אותיות קטנות)	**http**
סינון לפי כתובת IP	
IP מקור	**ip.src == 192.168.0.1**
IP יעד	**ip.dst == 192.168.0.1**
IP מקור **או** יעד	**ip.addr == 192.168.0.1**
סינון לפי פורט (משתנה בין TCP ל-UDP)	
פורט מקור	**tcp.srcport == 80 / udp.srcport == 80**
פורט יעד	**tcp.dstport == 80 / udp.dstport == 80**
פורט מקור **או** יעד	**tcp.port == 80 / udp.port == 80**
סינון לפי טקסט	
חיפוש טקסט	**frame contains "GET"**

אופרטורים לוגיים

אופרטור	סימן	דוגמא
שווה	**==, eq**	tcp.port == 12
שונה	**!=, ne**	ip.src != 101.1.1.2
או	**or , ||**	http or dns
גם	**and, &&**	tcp.port == 80 and ip.dst == 12.12.2.2
לא	**not, !**	!http