

תרגיל כריש-כבל

1. כדי למצוא בקשות של DHCP יש לפלטר על bootp

רואים שכתוב ב- Destination

255.255.255.255

2. משתמשים בפילטר:

ip.addr == 255.255.255.255

3. על ידי פילטר http.host

4. פתיחת Hypertext Transfer Protocol שם רואים שכתוב ב- Full request URI: www.themarker.com

5. על ידי ביצוע: Statistics->HTTP->Load Distribution בפילטר (display filter) נכתוב:

http.host == www.themarker.com

חיפוש ברשימה של: www.themarker.com מוצאים שהיא: 104.71.205.112

6. 172.227.100.174

7. גלישת http נעשית תמיד לפורט 80 בחלק של ה- Transmission Control Protocol רואים שה -
Dst port (80)

8. כמו בסעיף 6 מסתכלים על: Src Port 57312

9. שימוש בפילטר: http.content_length == 14251 יוצא 599

10.

Analyze -> follow -> tcp stream

השדה של Date מראה 16 ליוני שעה 11:34:20

בפקטה האחרונה שהשרת שולח נבדוק את ה- Hypertext Transfer Protocol ושם נראה תאריך של 16 ליוני שעה 11:34:43 נחסיר את האחרון מהראשון ונקבל 23 שניות.