רשתות תקשורת מחשבים

תרגיל 3 – Wireshark

הגשה בזוגות בלבד

שימו לב, תרגיל זה מכיל מספר רב של סעיפים. אל תחכו לרגע האחרון.

לפני תחילת המעבדה יש להכיר את RFC 2616.

1. לאיזו שכבה שייך HTTP במודל השכבות?
2. לפניך ETHERNET FRAME ב-HEX. עליך לתרגם אותם כדי פענח התוכן ששייך לHTTP ולהסביר כל שדה של HTTP (**<u>הבהרה:</u>** לא מבקשים ששתרגמו השדות של IP וכו' אתם רק צריכים לזהות כל דבר איפוה הוא נמצא כך שתוכלו להשיג המידע ששייך לHTTP. את המידע הזה דווקא תתצטרכו לתרגם לצורה קריאה והלהסביר מה יש בו):

א. <u>חבילה 1</u>

00 03 ff 02 99 d4 00 01 29 00 99 d4 08 00 45 00 01 81 41 9e 40 00 80 06 31 bc c0
a8 02 65 c0 a8 02 67 dc fe 00 50 67 be 74 24 75 26 15 f6 50 18 40 29 bd 23 00 00
47 45 54 20 2f 66 6f 72 6d 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 41 63
63 65 70 74 3a 20 2a 2f 2a 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a
20 65 6e 2d 75 73 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61
2f 34 2e 30 20 28 63 6f 6d 70 61 74 69 62 6c 65 3b 20 4d 53 49 45 20 38 2e 30 3b
20 57 69 6e 64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 57 4f 57 36 34 3b 20 54 72 69
64 65 6e 74 2f 34 2e 30 3b 20 53 4c 43 43 32 3b 20 2e 4e 45 54 20 43 4c 52 20 32
2e 30 2e 35 30 37 32 37 3b 20 2e 4e 45 54 20 43 4c 52 20 33 2e 35 2e 33 30 37 32
39 3b 20 2e 4e 45 54 20 43 4c 52 20 33 2e 30 2e 33 30 37 32 39 3b 20 4d 65 64
69 61 20 43 65 6e 74 65 72 20 50 43 20 36 2e 30 3b 20 49 6e 66 6f 50 61 74 68 2e
33 3b 20 2e 4e 45 54 34 2e 30 43 3b 20 2e 4e 45 54 34 2e 30 45 29 0d 0a 41 63
63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74
65 0d 0a 48 6f 73 74 3a 20 31 39 32 2e 31 36 38 2e 32 2e 31 30 33 0d 0a 43 6f 6e
6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 0d 0a

עזרה: גודלו של Ethernet header הוא 14 בתים. מבנה HEADER של ETHERNET:

6 Bytes	
Destination Address	
Source Address	
DATA TYPE	Data
Data	

לפני ה-Header מופיעים 8 בתים של Preamble לזיהוי התחלת המסגרת, אך הם לא מופיעים ב-WireShark. גודלו של IP header ללא options הינו 20 בתים. מבנה HEADER של IP:

4 Bytes				
Version	Ihl	Type Of Service	Total Legth	
Identification			Flags	Fragment Offset
Time To Live		Protocol	Header Checksum	
Source Address				
Destination Address				
Options				Padding
Data				

גודלו של TCP header הינו 20 בתים. מבנה HEADER של TCP:

4 Bytes				
Source Port			Destination Port	
Sequence Number				
Acknowledgment Number				
Data Offset	Reserved	Control Bits	Window	
Checksum			Urgent Pointer	
Options				Padding

Data

3. צייר sequence diagram (עליך לצייר את הדיאגרמה או להשתמש בתכונה של ה-wireshark) של שיחות HTTP המופיעות ב-trace (HTTP-Full-Client.pcap).
4. אילו סוגי **בקשות** אתה מזהה ב-TRACE (HTTP-Full-Client.pcap)? ציין מספר PACKET עבור כל בקשה. אילו סוגי בקשות נוספים מוגדרים בפרוטוקול?
5. מה ההבדל בין סוגי בקשות אלו?
6. מתי כדאי להשתמש בכל סוג בקשה?
7. אילו סוגי **תשובות** אתה מזהה ב-TRACE (HTTP-Full-Client.pcap)? ציין מספר PACKET עבור כל תשובה וכן את הבקשה עבורה התקבלה התשובה. כיצד זיהית את הבקשה? כמה סוגי תשובות מוגדרים בפרוטוקול?
8. מה המשמעות של כל תשובה?
9. בתוך איזה פרוטוקול ארוז פרוטוקול HTTP? מדוע? מה מוסיף פרוטוקול זה ל-HTTP?
10. ב-PACKET כלשהו התחילה שיחה עם השרת. מה תוכנה של השיחה? על פני כמה PACKETS מתפרסת השיחה?
11. מדוע כאשר ביקשנו את דף with_css_img.htm יש יותר מבקשה אחת לשרת? מי אחראי לטפל בזה?
12. בקובץ HTTP-NOTRECOGNIZE.pcap ישנה שיחת HTTP אבל wireshark לא מזהה זאת. מדוע?
13. לתרגיל מצורף קובץ בשם Wireshark_DNS_ בעזרת תוכנת ה-wireshark ענו על השאלות במסמך יש לענות על שאלות 1-15 בלבד