רשתות מחשבים

פרק 6ג- שכבת התעבורה, פרוטוקול UDP

ברק גונן

מבוסס על ספר הלימוד "רשתות מחשבים" מאת

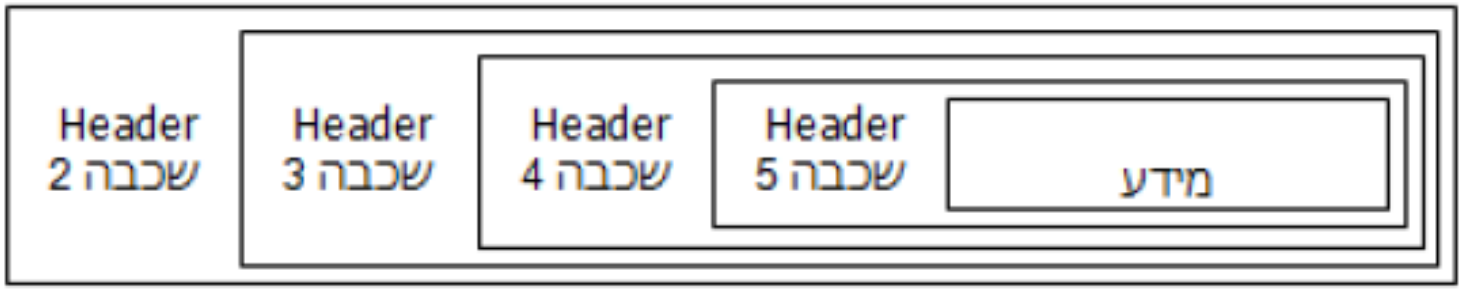
עומר רוזנבוים

מטרות הפרק

- בפרק זה נעמיק בפרוטוקול UDP
- נבחן את השדות השונים של ה- Header של UDP
- נכתוב שרת ולקוח UDP
- נממש nslookup באמצעות scapy

UDP Header

- מהו Header? (תחילית)
  - כזכור, שכבת התעבורה עושה encapsulation לשכבת האפליקציה - מוסיפה לה שדות של שכבת התעבורה
  - ה-Header הוא אוסף השדות הללו
- בצעו את תרגיל מודרך 6.4 ומיצאו את השדות השונים של UDP Header



גבהים
תכנית הסייבר הלאומית

Checksum

- מטרה: לזהות האם נפלו שגיאות (לא לתקן אותן)
- הרעיון הכללי:
  - נוסיף "ספרות ביקורת" לרצף המידע
  - חישוב הספרות מבוסס על המידע
  - אם אין התאמה- נפלו שגיאות
- משמש לבדיקת תקינות קבצים, פקטות רשת ועוד

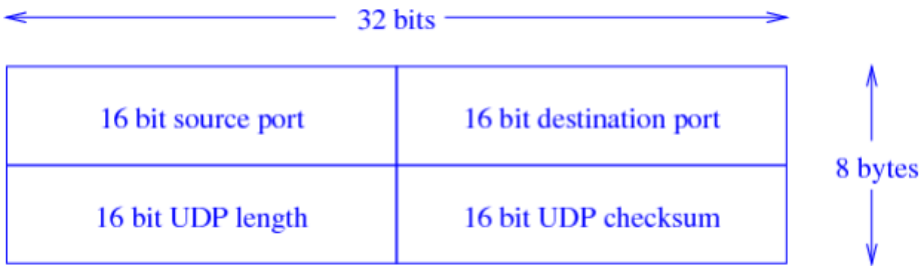
דוגמה ל-checksum

- ספרת ביקורת בתעודת זהות ישראלית
  - 8 הספרות מוכפלות בסדרה 12121212
  - מחברים את סכום המכפלה
  - ספרת הביקורת- ההשלמה של סכום המכפלה למספר הבא שמתחלק ב-10
  - לא את כל סוגי הטעויות אפשר לגלות
  - לדוגמה, ת.ז 34137705:

	3	4	1	3	7	7	0	5
X	1	2	1	2	1	2	1	2
	3	8	1	6	7	14	0	10

$3+8+1+6+7+(1+4)+0+(1+0) = 31$ ⇒ $40 - 31 = \mathbf{9}$

שדות של UDP Header -סיכום

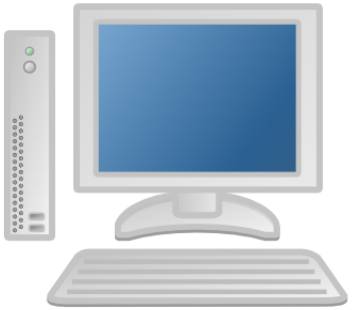


- פורט מקור / פורט יעד
  - הלקוח פונה לפורט היעד, פורט מוכר בשרת
  - פורט המקור הוא פורט אקראי שנבחר על ידי הלקוח
  - בתשובת השרת פורט היעד הוא הפורט של הלקוח
- שדה אורך
  - אורך = length(UDP Header + Application layer)
- Checksum
  - גילוי שגיאות (לא תיקון, רק גילוי)

למה בכלל צריך UDP?

- אמרנו ש-UDP לא פרוטוקול אמין. חישבו- למה צריך אותו? למה "להתאמץ" ולהוסיף מידע לפקטות ה-IP?
  - בשכבת הרשת אין פורטים- אי אפשר לדעת לאיזו תוכנה פנינו
  - לעיתים בשכבת הרשת אין checksum. במקרים אלו, UDP מזהה פקטות תקולות וזורק אותן

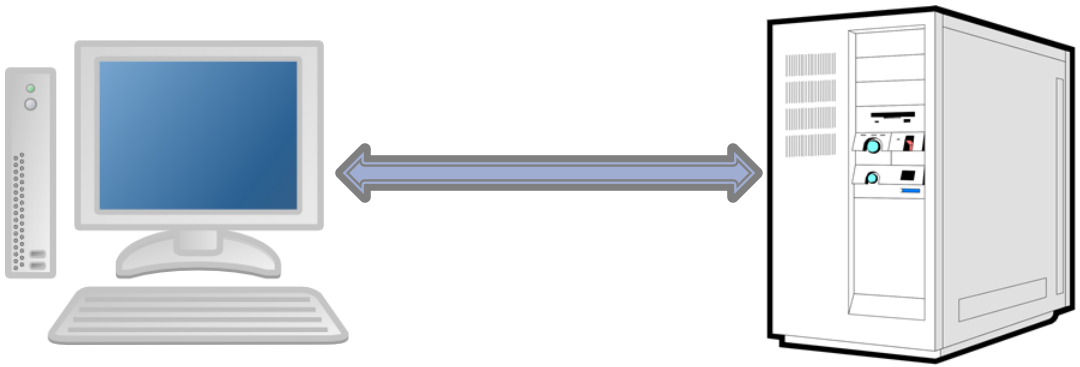
כתיבת לקוח UDP



- בצעו את תרגיל 6.5 בספר הלימוד
- על בסיס הלקוח שכתבתם ב-6.5, בצעו את תרגיל 6.6- כתיבת לקוח לשרת הדים
- הדרכה:
  - הפרמטר socket.SOCK_DGRAM מציין קישור UDP
  - שימוש במתודות sendto, recvfrom: לא דורשות קישור לשרת

כתיבת שרת UDP

- בצעו את תרגיל 6.8 מודרך
- על בסיס 6.8, בצעו את תרגיל 6.9 שרת הדים UDP
- שימו לב:
  - כיוון ש-UDP הוא פרוטוקול connectionless, השרת לא מבצע listen ו-accept
  - עדיין נדרש bind כדי לקשר בין הסוקט לפורט



כתיבת nslookup ע"י scapy

- זוכרים את הכלי nslookup?

```
c:\Cyber>nslookup www.google.com
Server:  Broadcom.Home
Address:  10.0.0.138

Non-authoritative answer:
Name:    www.google.com
Addresses:  2a00:1450:4009:800::2004
          216.58.208.36
```

- בקרוב נכתוב כלי כזה בעצמנו!

```
c:\Cyber>python my_DNS.py
Please enter domain address
www.google.com
Begin emission:
Finished to send 1 packets.
...*
Received 4 packets, got 1 answers, remaining 0 packets
IP address number 1 is: 216.58.208.68
```

כתיבת nslookup ע"י scapy

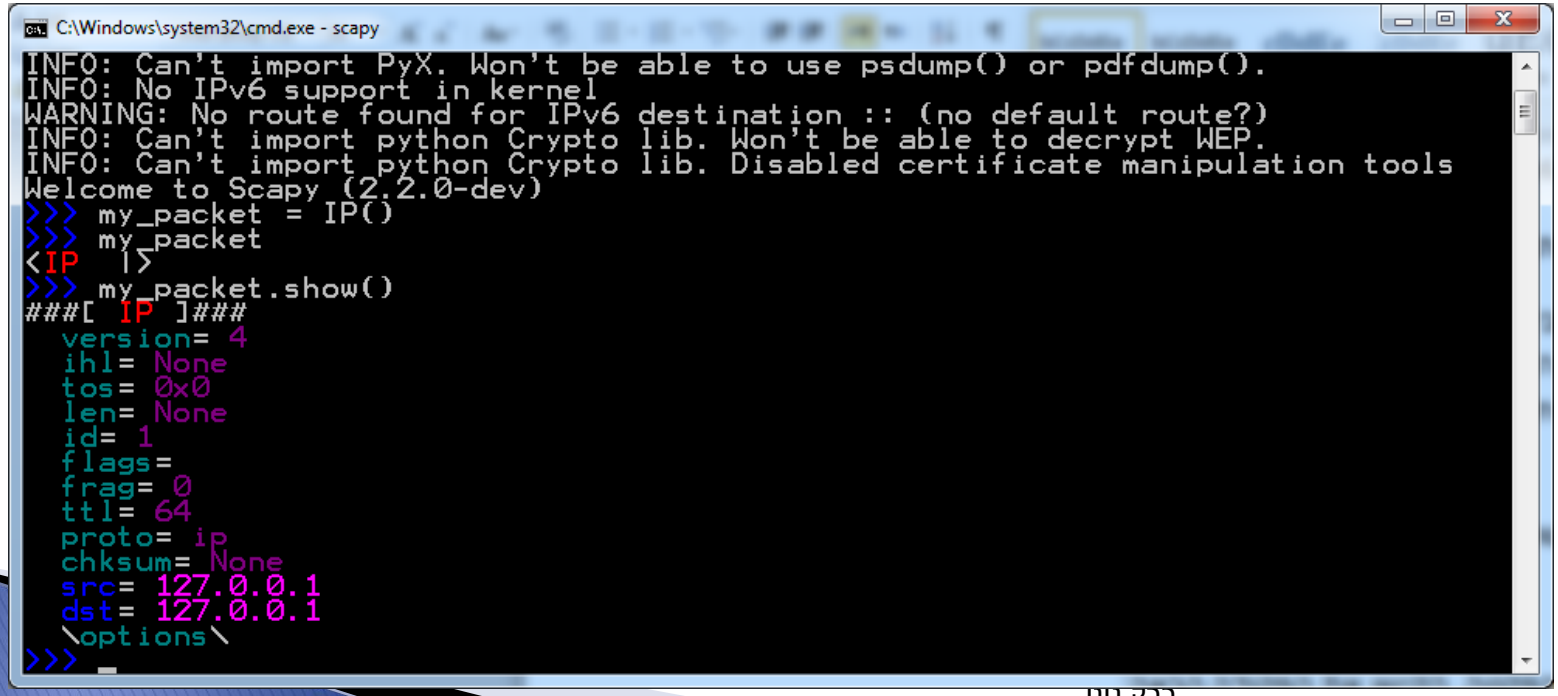
- נלמד לבצע "תפירה עילית" של פקטות בעבודת יד
- שלבי הלימוד:
  - נבין איך משתמשים ב-scapy ליצירת חבילות
  - נלמד ליצור שכבות בתוך הפקטות
  - נלמד לשלוח את הפקטות שיצרנו
  - נלמד לחבר את scapy לסקריפט פייתון

יצירת "שלד" של פקטת רשת ע"י scapy

- מבוסס על "יצירת חבילות" פרק 5
- בתוך scapy נכתוב:

```
>>> my_packet = IP()
>>> my_packet.show()
```

- קיבלנו פקטה של שכבת הרשת, בה כל השדות הם ברירת מחדל:



שינוי פרמטרים בפקטה

- הבה נשנה את יעד הפקטה:

```
>>> my_packet.dst = '10.1.1.1'
```

- אם נכתוב my_packet יוצגו רק הפרמטרים שאינם ברירת מחדל:

```
>>> my_packet.dst='10.1.1.1'
>>> my_packet
<IP  dst=10.1.1.1 |>
```

- ניתן ליצור מראש חבילה עם שדות כרצוננו:

```
>>> my_packet = IP(dst = '10.1.1.2', ttl = 6)
>>> my_packet
<IP  ttl=6 dst=10.1.1.2 |>
```

הוספת שכבות

- ניתן להוסיף שכבה פשוט ע"י כתיבת שם הפרוטוקול המבוקש
- סדר הכתיבה- משמאל (שכבות נמוכות) לימין (גבוהות)

```
>>> my_packet = Ether() / IP() / UDP ()
>>> my_packet.show()
###[ Ethernet ]###
  dst= ff:ff:ff:ff:ff:ff
  src= 00:00:00:00:00:00
  type= 0x800
###[ IP ]###
     version= 4
     ihl= None
     tos= 0x0
     len= None
     id= 1
     flags=
     frag= 0
     ttl= 64
     proto= udp
     chksum= None
     src= 127.0.0.1
     dst= 127.0.0.1
     \options\
###[ UDP ]###
        sport= domain
        dport= domain
        len= None
        chksum= None
>>>
```

שכבת הקו

שכבת הרשת

שכבת התעבורה והשדות המוכרים לנו של UDP

```
>>> my_packet = Ether ()/ IP() / UDP()
```

הוספת מידע לפקטה

- אפשר להוסיף לכל שכבה מידע שעובר מעליה
  - לדוגמה נעביר פרוטוקול HTTP מעל שכבת התעבורה, שמיוצגת ע"י פרוטוקול TCP:

>>> my_packet = Ether() / IP() / TCP() / “GET / HTTP/1.0\r\n\r\n”

```
>>> my_packet = Ether() / IP() / TCP() / Raw("GET / HTTP/1.0\r\n\r\n")
>>> my_packet
<Ether  type=0x800 |<IP  frag=0 proto=tcp |<TCP  |<Raw  load='GET / HTTP/1.0\r\n
\r\n' |>>>>
```

שליחת פקטות שיצרנו- Send

- scapy יודע לתרגם מכתובת דומיין לכתובת IP
  - לדוגמה, אם נכתוב:

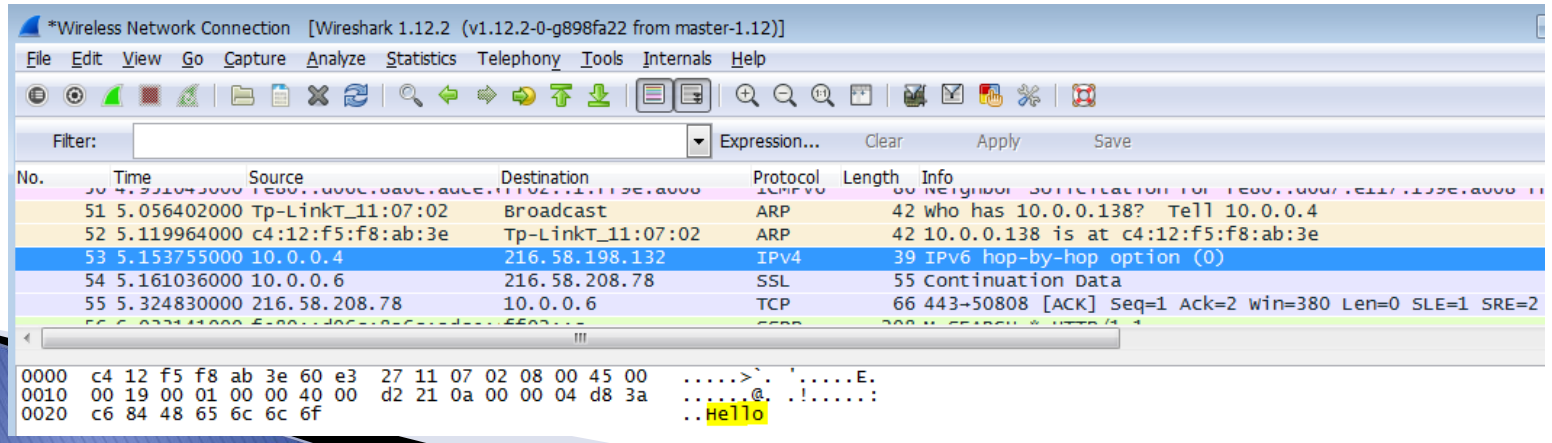
```
>>> my_packet = IP(dst =‘www.google.com’)
```

אז scapy יידע לשלוח לכתובת ה-IP הנכונה

- ניצור פקטה עם מידע סתמי, ונשלח אותה לגוגל:

```
>>> my_packet = IP(dst =‘www.google.com’) / ‘Hello’
>>> send(my_packet)
```

  - השתמשו ב-wireshark ומיצאו את הפקטה ששלחתם



כתיבת nslookup ב-scapy

- כהכנה יש ללמוד איך לשלוח פקטת DNS ולקבל תשובה – תרגילים 6.10, 6.11
- צרו פקטת DNS שכוללת את המידע הנדרש:
  - IP של שרת ה-DNS
  - פורט יעד (רצוי להוסיף גם פורט מקור)
  - דגלים- מהם הדגלים ההכרחיים?
    - העזרו ב: http://www.zytrax.com/books/dns/ch15/
  - שם הדומיין הנבחר, שדות שמתארים את סוג השאילתא
- עיברו על השדות בפקטת התשובה וחפשו תשובות מסוג type A
  - ניתן לבחור שדה על ידי אינדקס בתוך סוגריים מרובעות [ ]: http://itgeekchronicles.co.uk/2014/05/12/scapy-iterating-over-dns-responses/

גבהים
תכנית הסייבר הלאומית

תרגיל מסכם UDP

- בצעו את תרגיל 6.13 – תקשורת סודית מעל מספרי פורטים

סיכום

- הסבירו מהו checksum?
- אילו עוד שדות קיימים ב-header של UDP?
- כשלקוח UDP פונה לשרת, לשם מה הוא שולח פורט מקור?
- אילו פעולות של שרת "מיותרות" בשרת UDP?
- פרטו איך יוצרים שאילתת DNS? אילו דגלים נדרשים?