Mark Seliternikov
picoCTF - shark on wire 1 [150 points]

לאתגר הזה מקבלים קובץ pcap.

```
mark@DESKTOP-19NBBKR:/mnt/c/users/markm/downloads$ ls
capture.pcap  desktop.ini
```

ניסיתי לחפש string שמזכיר את הדגל בטרמינל וזה מה שמצאתי

```
mark@DESKTOP-19NBBKR:/mnt/c/users/markm/downloads$ strings capture.pcap | grep pico
Upico
Upico
Upico
Upico
```

פתחתי את הקובץ בעזרת wireshark כדי לראות את התוכן של הקובץ בצורה נוחה.
לאחר שפתחתי ראיתי שיש כמות מאוד גדולה של packets.

Packets: 2317 · Displayed: 2317 (100.0%)

חיפשתי את ה-string ב-wireshark כדי לראות את התוכן של החבילה וזה מה שמצאתי

[redacted]	[redacted]	[redacted]	UDP	60	5000 → 9999 Len=4[Malformed Packet]
[redacted]	[redacted]	[redacted]	UDP	60	5000 → 9999 Len=4[Malformed Packet]
[redacted]	[redacted]	[redacted]	UDP	60	5000 → 9999 Len=4[Malformed Packet]
[redacted]	[redacted]	[redacted]	UDP	60	5000 → 9999 Len=4[Malformed Packet]

```
ff ff ff ff ff ff 00 0c  29 b9 02 a9 08 00 45 00   ........ )·····E·
00 20 00 01 00 00 40 11  66 bc 0a 00 00 06 0a 00   · ····@· f·******
00 0b 13 88 27 0f 00 0c  dd 55 70 69 63 6f 00 00   ····'··· ·Upico··
00 00 00 00 00 00 00 00  00 00 00 00               ........ ····
```

זה היה התוכן של החבילה

`picopicopicopico`

ראיתי שהחבילה עברה ב-UDP אז החלטתי לעבור על מספר סטרימים עד שאגלה משהו חדש.
לאחר שעשיתי זאת מצאתי ב אחד ה-streams שהתוכן נראה כך

`picoCTF{StaT31355_636f6e6e}`

כפי שניתן לראות זה הדגל של האתגר.

לאחר שמצאתי את הדגל חיפשתי עוד קצת כדי לראות אם יש עוד משהו מעניין ומצאתי את זה

`picoCTF{N0t_a_fLag}`

<u>מה למדתי</u>

תוך כדי האתגר הייתי צריך להעמיק את הידע שלי בפרוטוקול TCP/IP וגם UDP.
אתגר זה הוא הצעד הראשון שלי להעמקת הידע ברשתות.