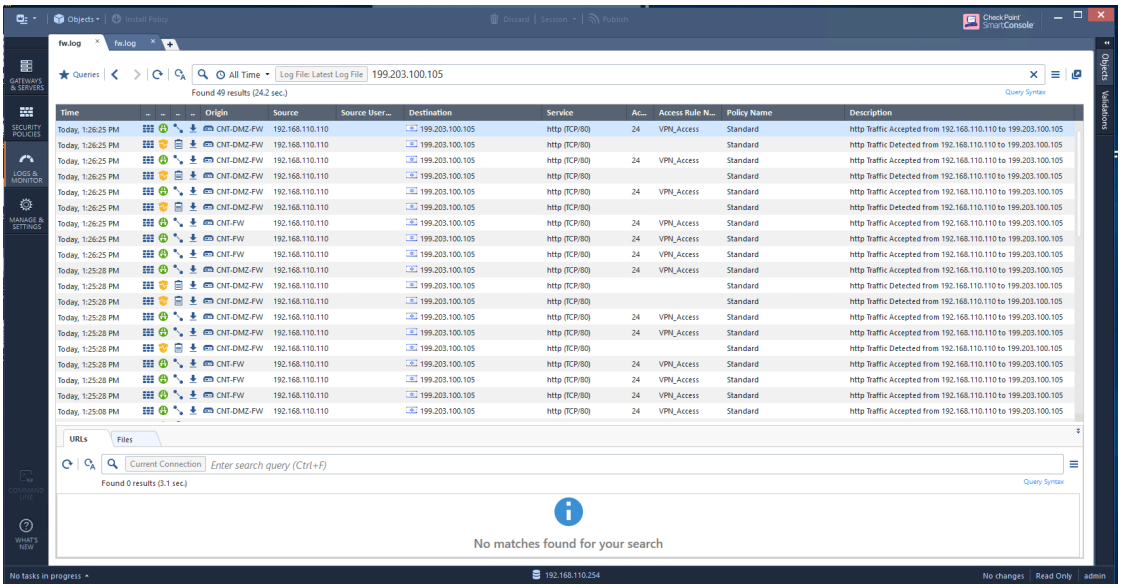
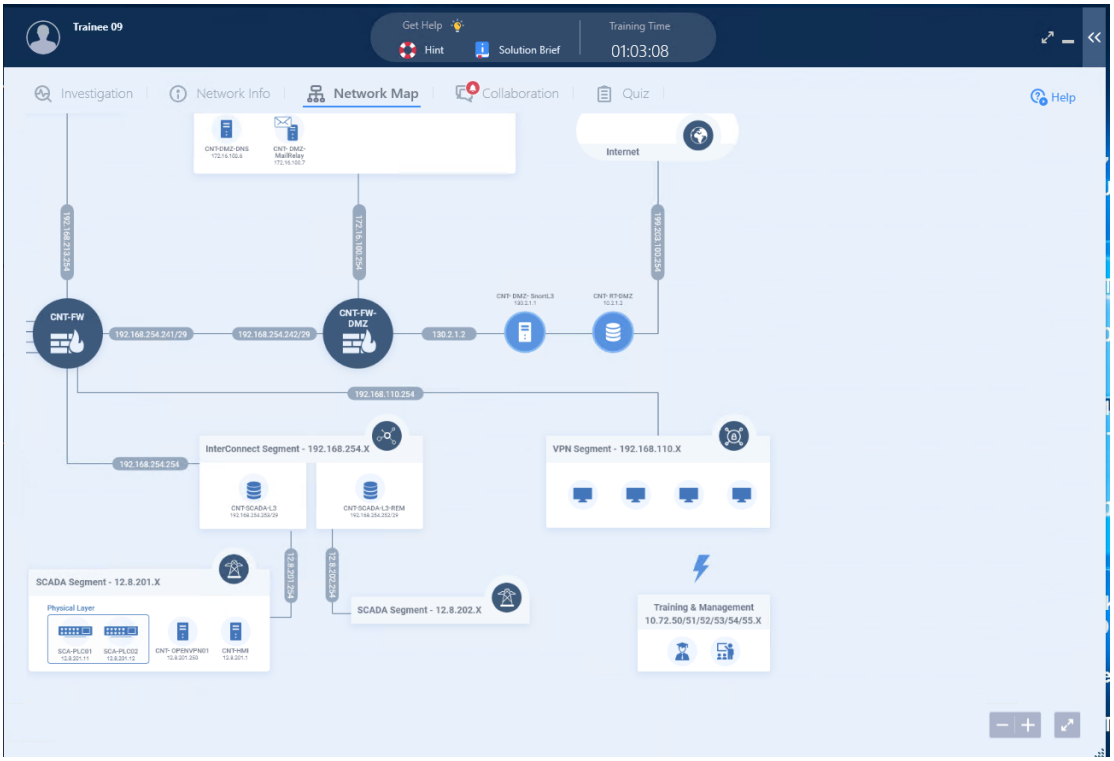
ארגון מסוים התלונן שקיבל הצפת מידע. הכתובת של מי שהוצף הוא: 199.203.100.105
מה שגילינו נכון לעכשיו שיש מחשב מהרשת שלנו בכתובת 192.168.100.100 שמציף את הארגון.





אנחנו רוצים לראות את התעבורה שעברה בfirewall שלנו ויש סוג של firewall שיכול לזכור את התעבורה שעברה בו – נקרא snort . הכתובת שלו היא: 130.2.1.1

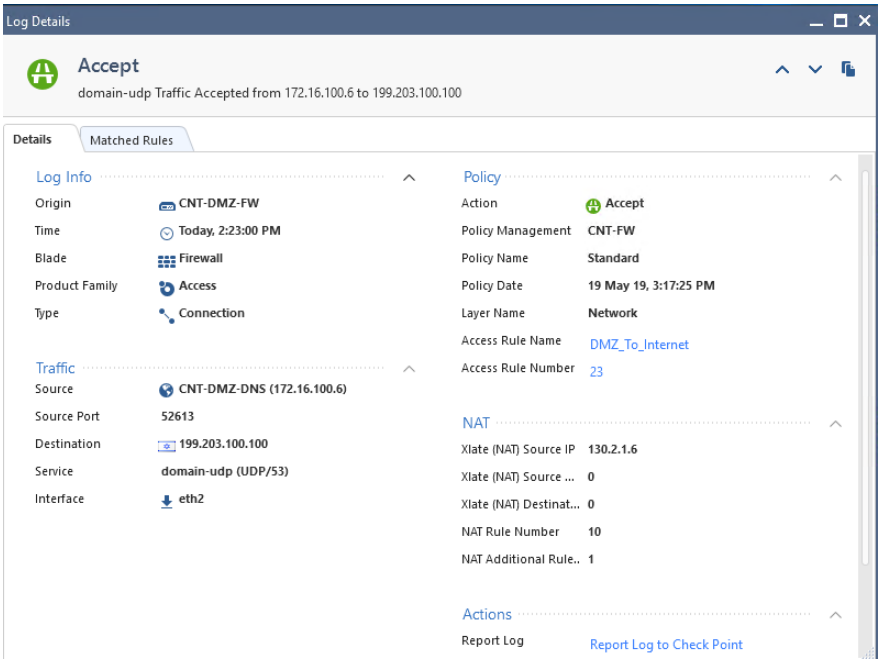
נכנסו לputy בכתובת 130.2.1.1 כדי לראות את התעבורה שעברה שם.

```
09:05:03.050999 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.051005 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.051036 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.051043 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.051143 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.051155 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.051159 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.051203 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.051211 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.051283 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.051319 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.051364 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.051402 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.051444 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.051498 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.051551 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.051555 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.051603 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.051640 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.051675 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.051682 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.051719 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.051778 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.051816 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.051873 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.051949 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.051958 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.051999 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.052072 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.052108 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.052236 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.052238 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.052266 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.052275 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.052278 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.052369 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.052376 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.052384 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.052389 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.052501 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.052575 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.052638 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:05:03.052644 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.052651 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.052726 IP 130.2.1.6.domain > 199.203.100.105.42000: 16962 0/1/0 (87)
09:05:03.052733 IP 130.2.1.112.60159 > CNT-DMZ-Snort.ssh: Flags [P.], seq 6881:6945, ack 8107008, win 0, length 64
^Ctcpdump: Unable to write output: Interrupted system call
root@CNT-DMZ-Snort:/#
```

רצינו למקד את הOutput אז עשינו פילטור tcpdump dst 130.2.1.6 - ומצאנו שהתעבורה היא טוויטר

```
09:11:43.469632 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.469825 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.469832 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.469836 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.470072 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.470079 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.470084 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.470269 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.470275 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.470279 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.470421 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.470426 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.470638 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.470644 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.470777 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.470782 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.470876 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.470935 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.471022 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.471084 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.471139 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.471196 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.471258 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.471341 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.471445 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.471531 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.471602 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.471679 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.471751 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.471820 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.471894 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.471993 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.472094 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.472154 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.472221 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.472561 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.472625 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.472699 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.472778 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.472835 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.472911 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.473133 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
09:11:43.473137 IP 199.203.100.105.42000 > 130.2.1.6.domain: 16962+ [b2&3=0x500] A? twitter.com. (29)
```

גילינו שהכתובת: 172.16.100.6 היא של שרת הdns שלנו.



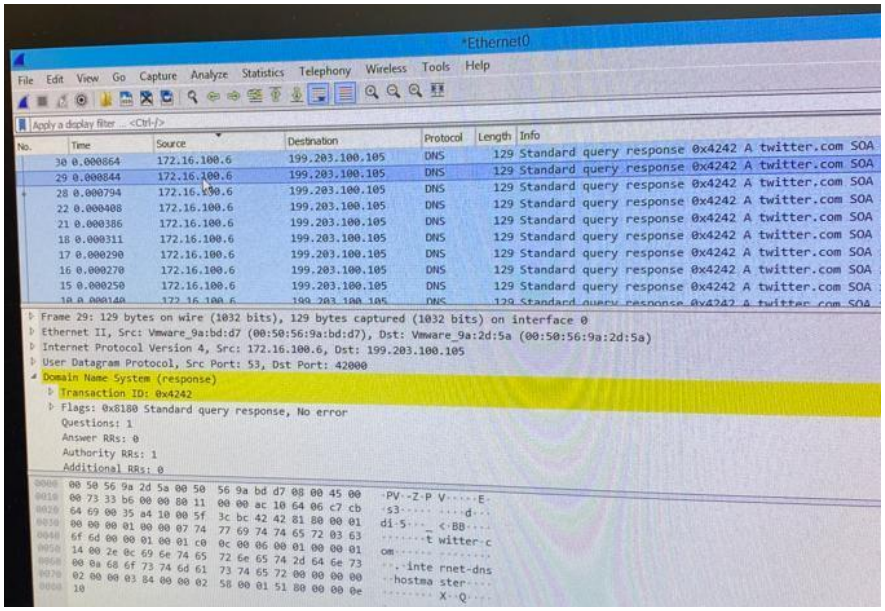
הכתובת 199.203.100.105 שולחת לDNS בקשה לדעת מה הכתובת ip של טוויטר.

הA? שרואים בתעבורה זה גורם לפעולת החיפוש של DNS . תפקידו של הDNS להחזיר לנו כתובת IP שתואמת לשם.

עכשיו אנחנו רוצים לראות את התעבורה של הDNS שלנו.
חיפשנו את הכתובת של הdns בתוכנה הראשית 172.16.100.6 וגילינו שמערכת ההפעלה היא windows .

בשביל שנראה את התעבורה בwindows צריך Wireshark לכן נכנסנו לתיקיה סודית ששם אפשר להוריד את התוכנה והורדנו.

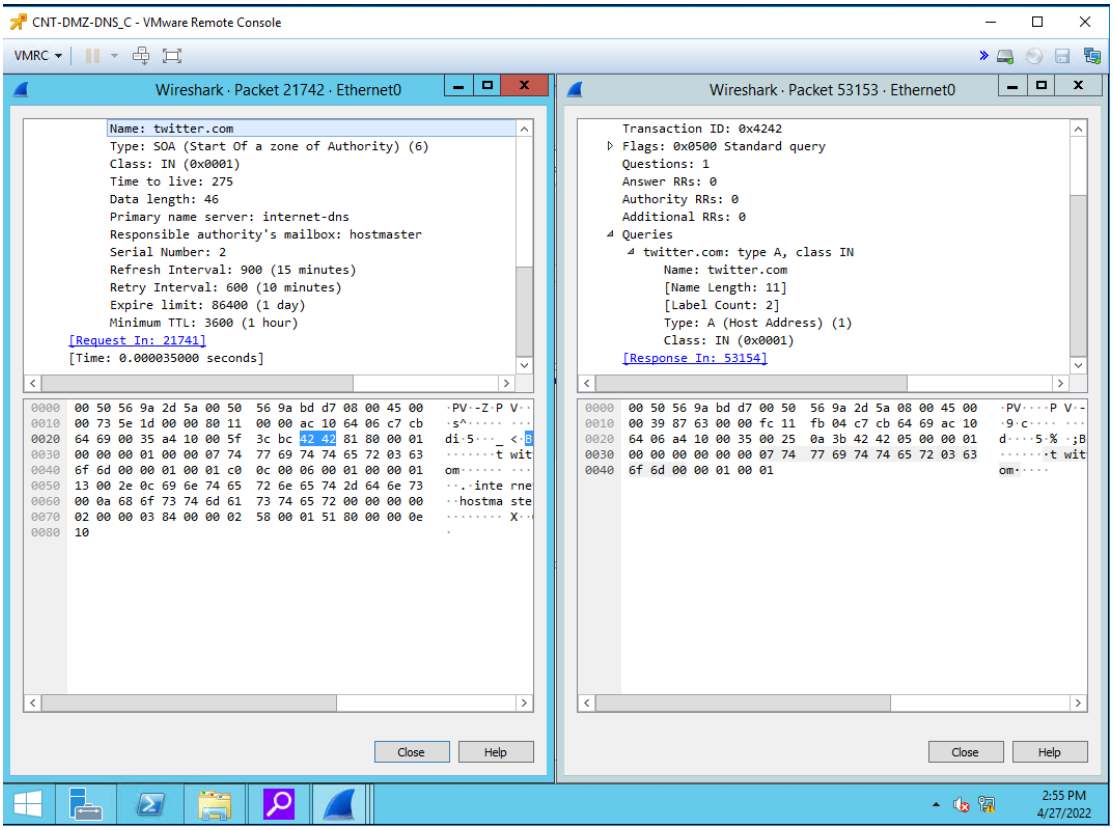
התעבורה:



אפשר לראות את כתובת הנתקף (מי שהוצף בעצם 199.203.100.105)
עכשיו אנחנו רוצים לראות את הפקטות שהתוקף שולח לנו ולכן עכשיו חיפשנו פקטה שאנחנו הdestination .

בתמונה פה למטה יש 2 פקטות:

ימין – התוקף שלח , שמאל – אנחנו שלחנו



אפשר לראות שהפקטה שאנחנו שולחים יותר גדולה ממה שהתוקף שולח. מפה אפשר להבין שהתוקף מנצל את המשאבים שלנו ואז נשלחת פקטה עם יותר מידע .

התוקף התחזה לIP שלנו וכך הגדיל את הפקטה שלו.

<u>אפשרות התגוננות מהתקפה זו:</u>

1. הרחבת גודל פס האינטרנט
2. לגרום לכך שברשת הפנימית יהיו רק חבילות שהכתובת מקור שלהן היא מהרשת עצמה ולא ממישהו ששייך לרשת אחרת. כך לא יקרה המצב של גניבת IP.