5) הסנפת פקטת DHCP Request שנקלטה במחשב המחובר ל-WiFi, הפקטה נשלחה כאשר טלפון סלולרי התחבר לרשת

1. אפשר לראות שהשדה Source IP מכיל 0.0.0.0 ("this host") – כפי שלמדנו, מכיוון שלמרות שההתקן החדש החליט אישר באמצעות הפקטה את הכתובת שהוקצתה לו, הוא צריך לחכות ל-ACK מהשרת לפני שישתמש בה. בנוסף, השדה Destination IP מכיל 255.255.255.255 ("broadcast") – ההתקן מבקש לשלוח את הפקטה לכל השרתים ברשת כדי להודיע להם שהוא קיבל הצעת כתובת של אחד מהם, וכך השרתים האחרים מבינים כי הצעתם נדחתה והם יכולים להציע את הכתובת שהציעו להתקן אחר שיבקש להתחבר בעתיד.
2. ניתן לראות מצילום המסך שהפרוטוקולים בשכבות נמוכות יותר שהפקטה נשענת עליהם הם UDP ו BOOTP.

BOOTP (Bootstrap Protocol) הוא פרוטוקול ניתוב אשר DHCP מתבסס עליו, והמידע נשלח דרך פרוטוקול UDP כאשר ב Source (Client) Port של הטלפון הוא 68 וה- Destination (Server) Port הוא 67, כפי שלמדנו (אין צורך ב-TCP מכיוון שלא חשוב לנו לקבל אישור שהפקטה הגיעה לכל היעדים, האישור שנחכה לו הוא DHCP-ACK מהשרת).

6)

ג. הקוד יבצע הסנפה ויפלטר את התוצאות כך שהוא ישמור את 10 הפקטות הראשונות שמכילות את מחלקת ה DNS ב scapy

(כלומר פקטות של פרוטוקול DNS)

ד. נלכדו 10 פקטות כצפוי, נציג אחת מהן (בוצע במכונה וירטואלית):



הפרוטוקולים שאנו רואים הם Ethernet, IP, UDP, DNS.