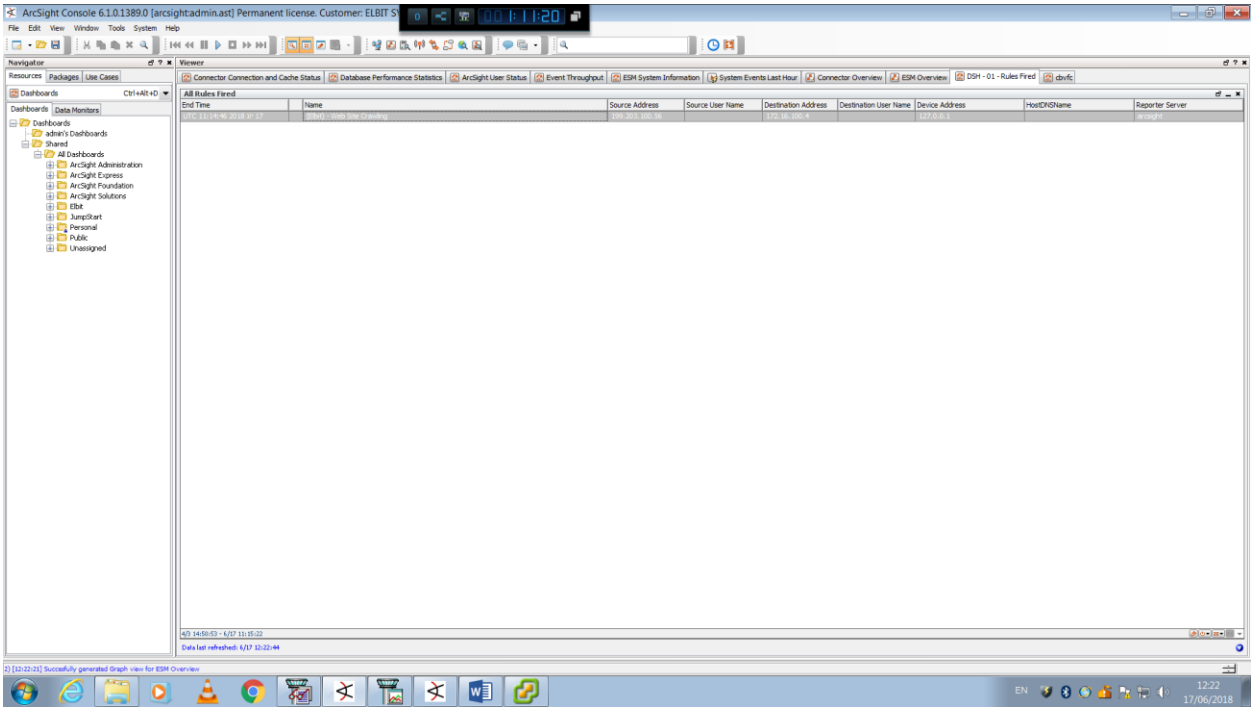
דו״ח מבחן

פרטים:

מגיש: שגיא סעדה

תהליך ההתקפה:

זיהוי ראשון בתרחיש הוא Web Site Crawling בכלי Arcsight –



הסבר על Web Site Crawling – זחלן רשת, הוא כינוי לסוג של בוט או תוכנה אשר סורקת את הרשת הכלל עולמית, באופן אוטומטי, שיטתי וסדרתי.

תוכנה זו יכולה להיקרא גם רובוט חיפוש.

אתרים רבים, בייחוד מנועי חיפוש, משתמשים בזחלנים כדי לקבל תמונה עדכנית של הרשת.

הזחלן שומר העתק של האתרים כדי שניתן יהיה לעדכן אותם מאוחר יותר באינדקס של מנוע החיפוש ובכך מאפשר למנוע החיפוש מתן תוצאות מהיר.

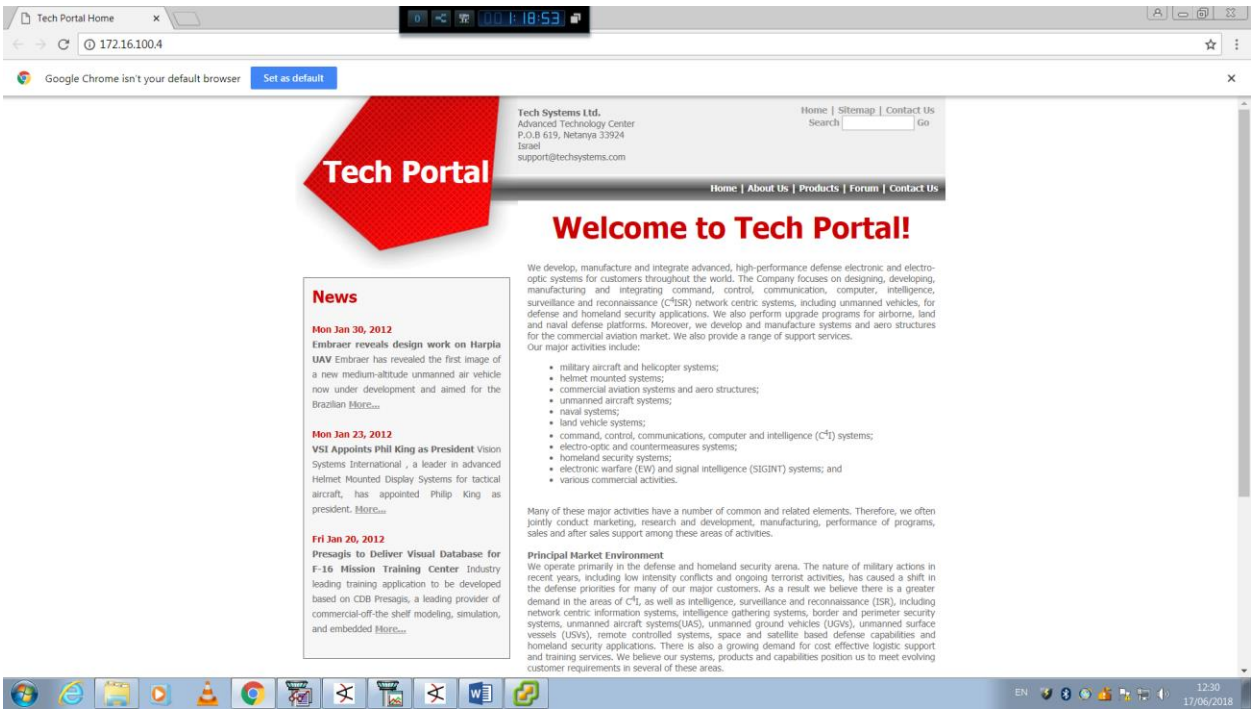
כמו כן, תוכנות זחלן יכולות לאתר קישורים מתים בדפי אינטרנט או לאסוף כתובות דואר אלקטרוני.

בדרך כלל הזחלן מתחיל לסרוק דף מתוך רשימה נתונה של דפים ומשם הוא מתקדם באופן רקורסיבי דרך הקישורים בדף לדפים נוספים.

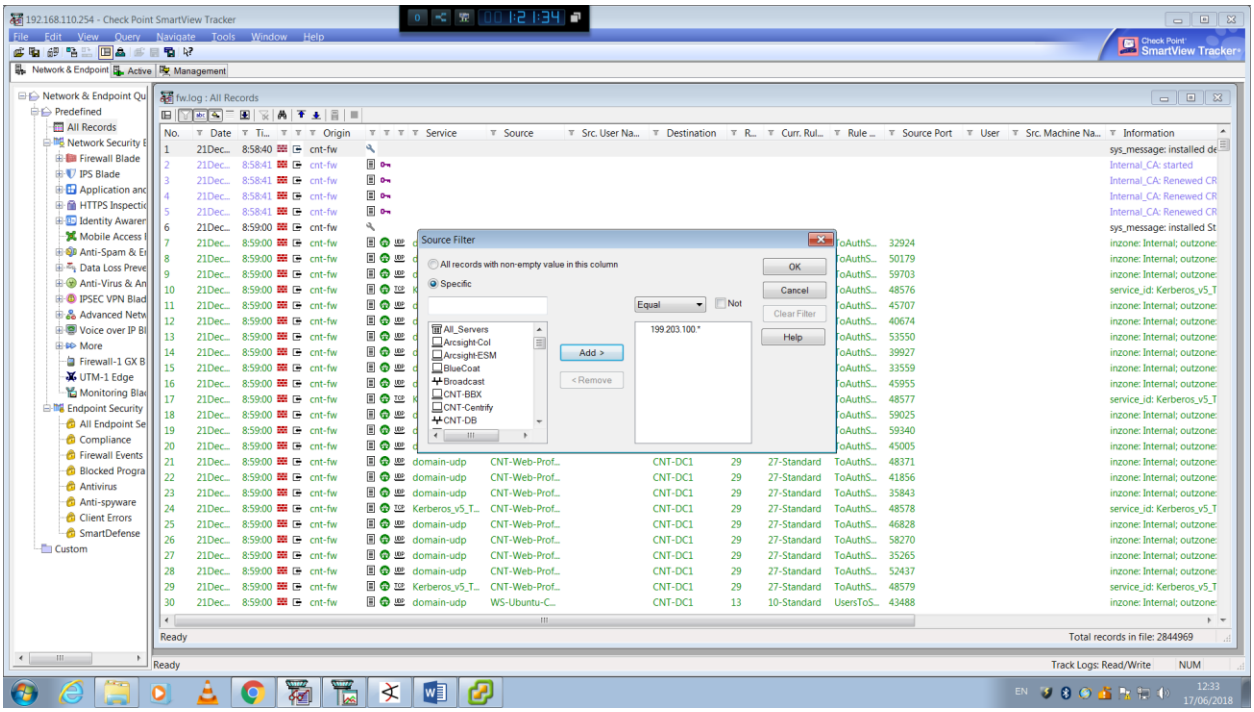
כתובת IP מקור – 199.203.100.53 – כתובת IP חיצונית.

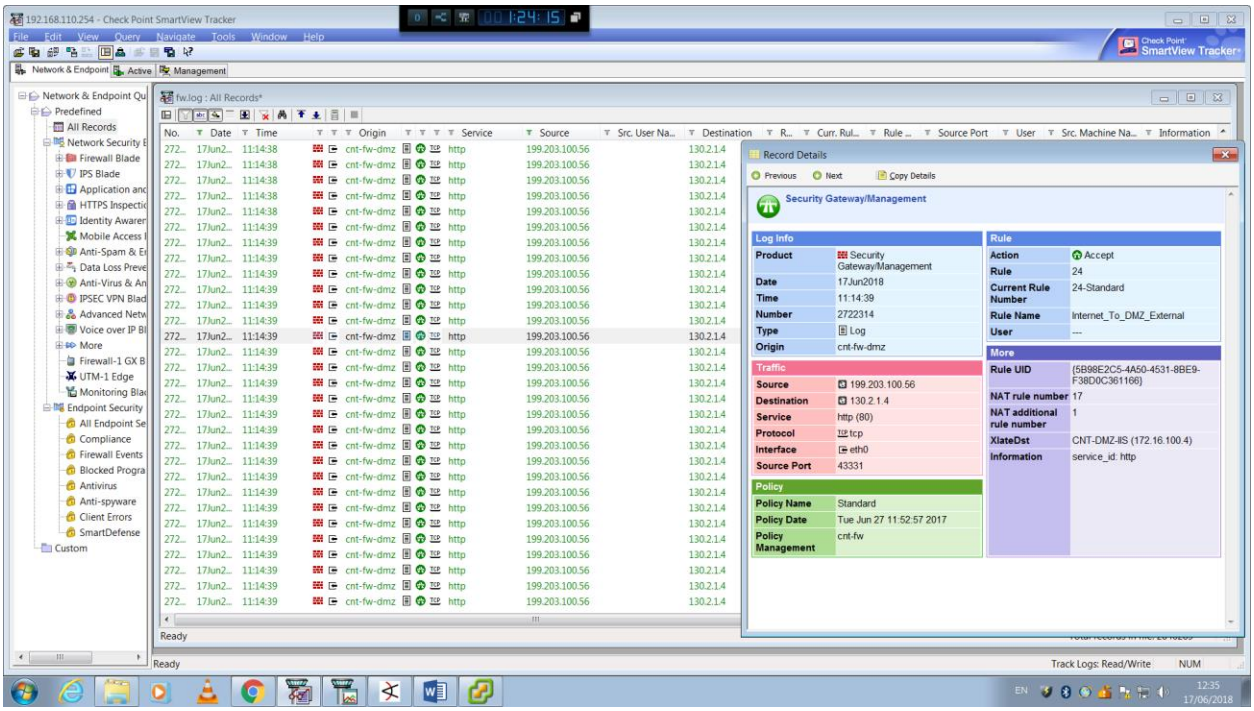
כתובת IP יעד – 172.16.100.4 – כתובת IP פנימית – CNT-DMZ-IIS.

לכתובת זו יש אתר פעיל ולכן נכנס לבדוק האם משהו השתנה –



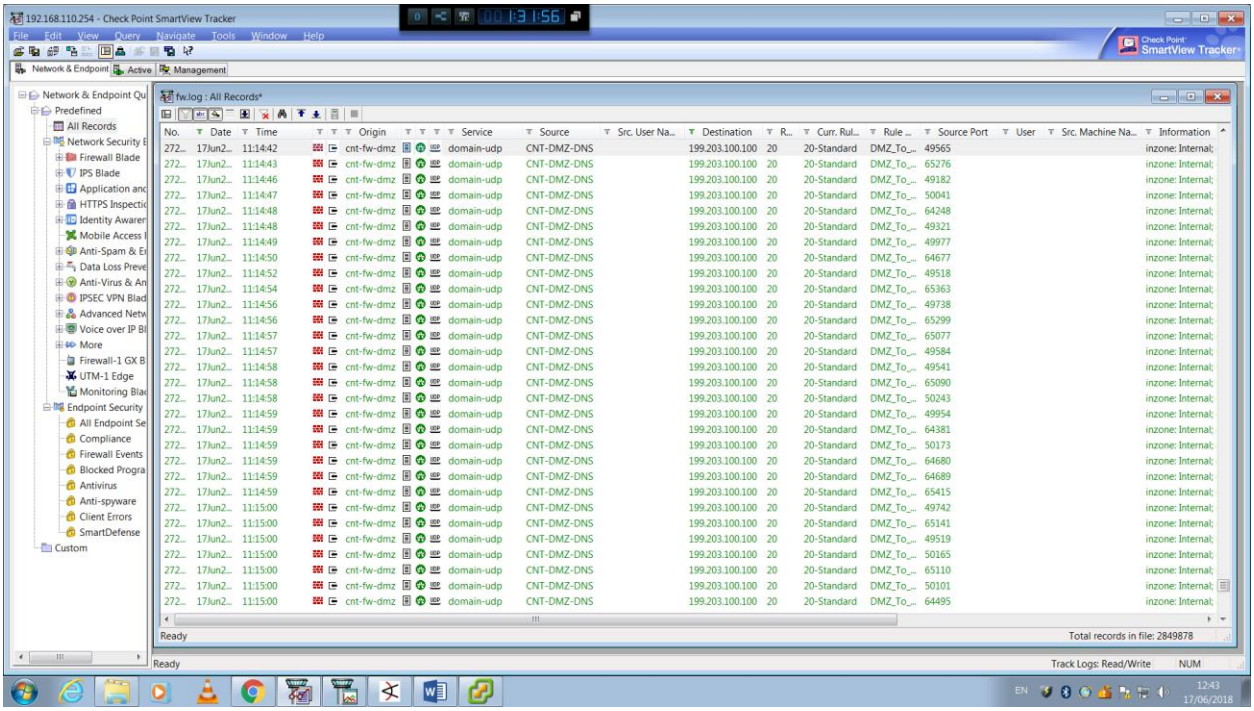
על מנת לאסוף מידע נוסף על התעבורה ברשת נכנס לכלי - Tracker ולאחר פילטור המקור נוכל לדעת האם יש דברים חשודים נוספים –





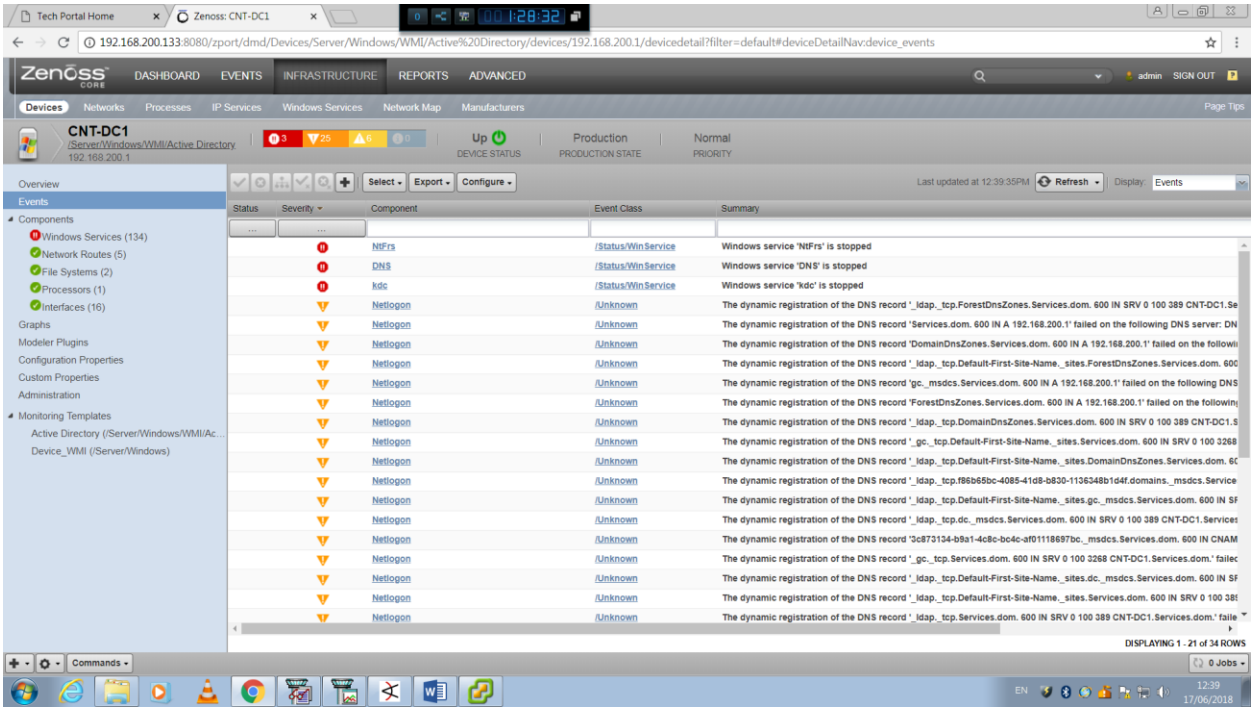
כפי שניתן לראות, ישנם הרבה תעבורה בפרוטוקול HTTP – TCP בהפרשי זמן מאוד קצרים בין ה- IP החיצוני לשרת האתר DMZ-IIS בארגון שלנו.

בנוסף, אם נכניס את האפשרות שכתובת ה- IP החיצונית תהיה ב- Destination נקבל –

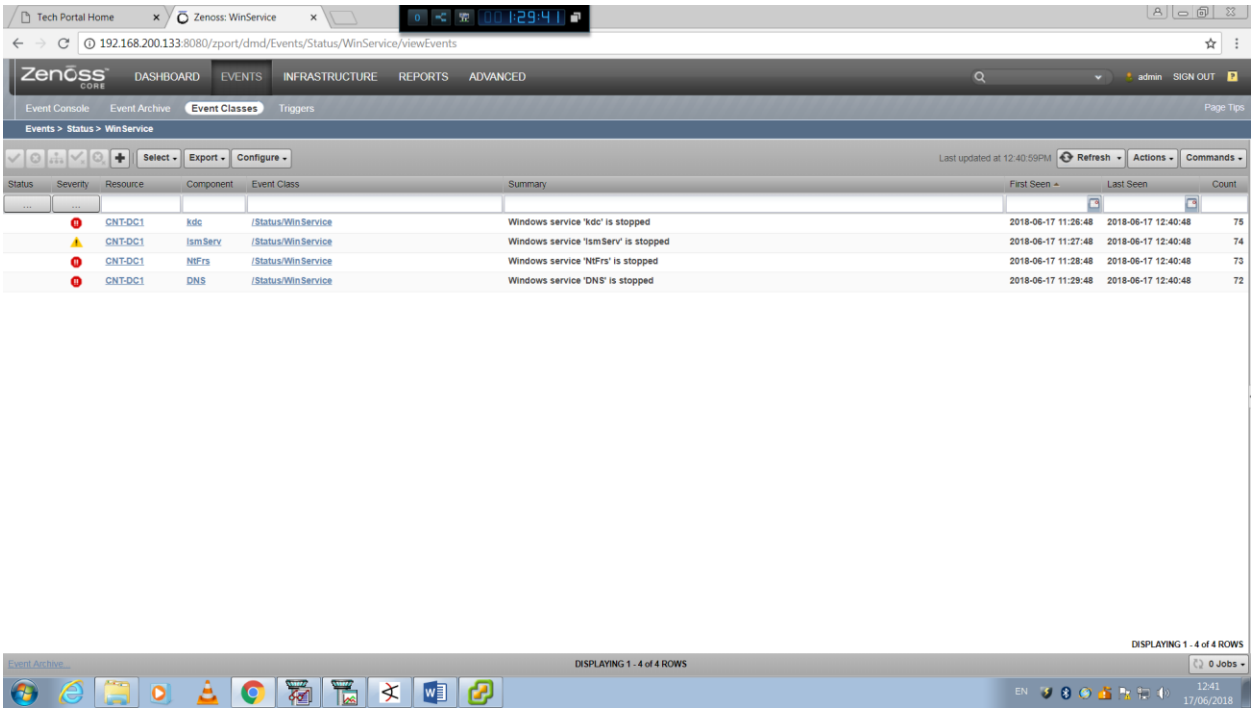


ניתן לראות ששרת ה- DMZ-DNS שלנו פונה ל- IP החיצוני בפרוטוקול UDP בהפרשי זמן קצרים.

לאחר מכן, כיוון שאנחנו יודעים שיש משהו חשוד שמתרחש בארגון, נבדוק את הכלי Zenoss אשר מציג את מצב השרתים והסרוויסים ברשת הארגון.



כפי שניתן לראות,

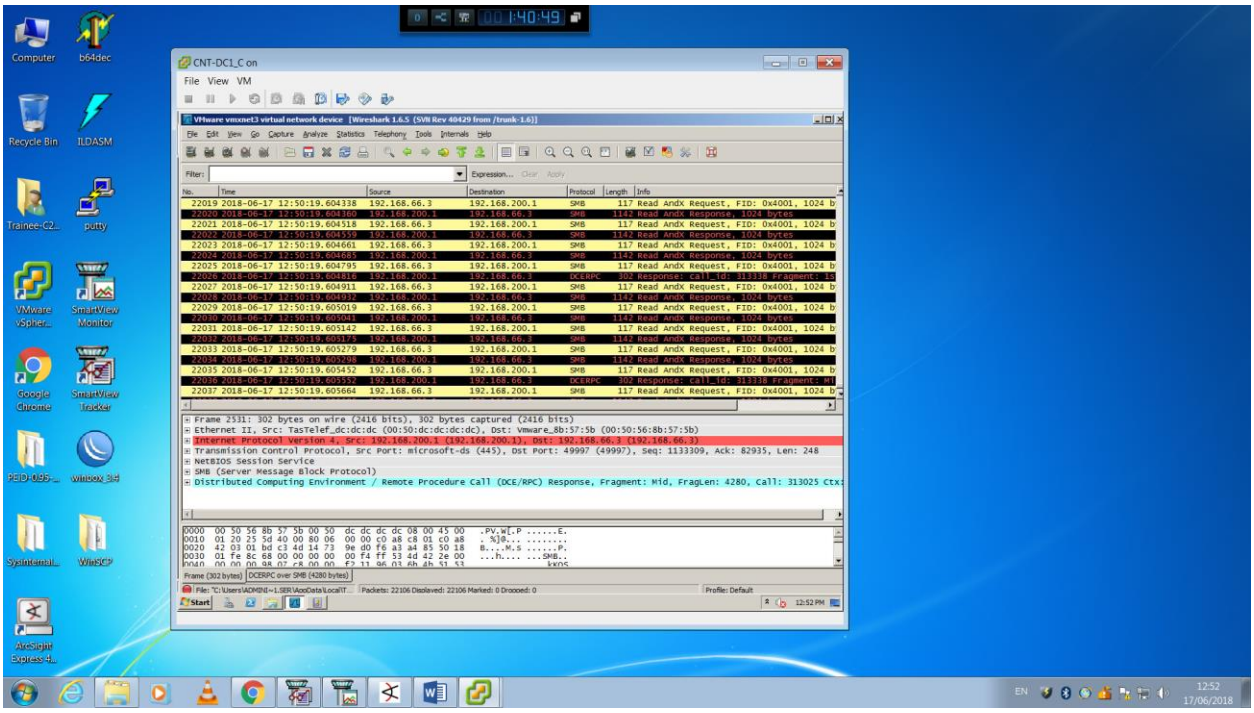


שירות ה- DNS, KDC, ISMSERV ו- NTFRS בשרת CNT-DC1 הופסקו.

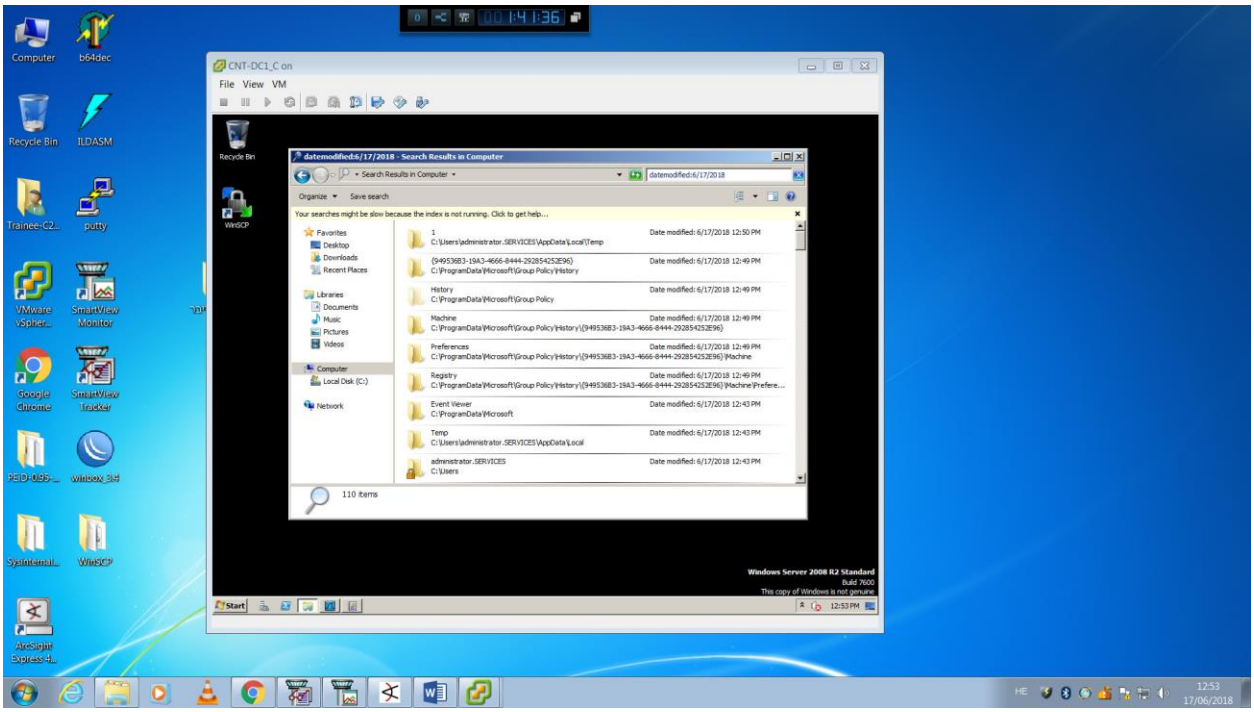
מכאן, נרצה להתחבר לשרת ה- CNT-DC1 ו- DMZ-IIS ולעשות עליהם בדיקה מעמיקה.

התחברות לשרת ה- CNT-DC1 –

הפעלת Wireshark -

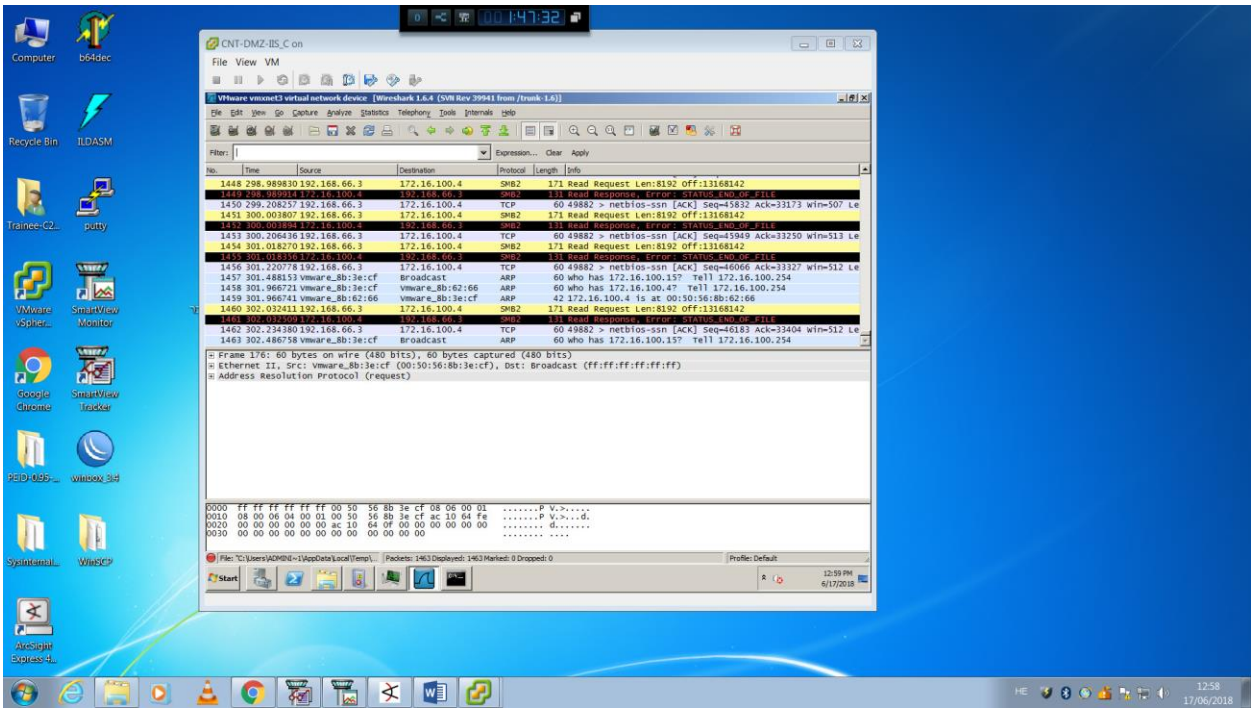


בדיקת קבצים שנוצרו / שונו לאחרונה –

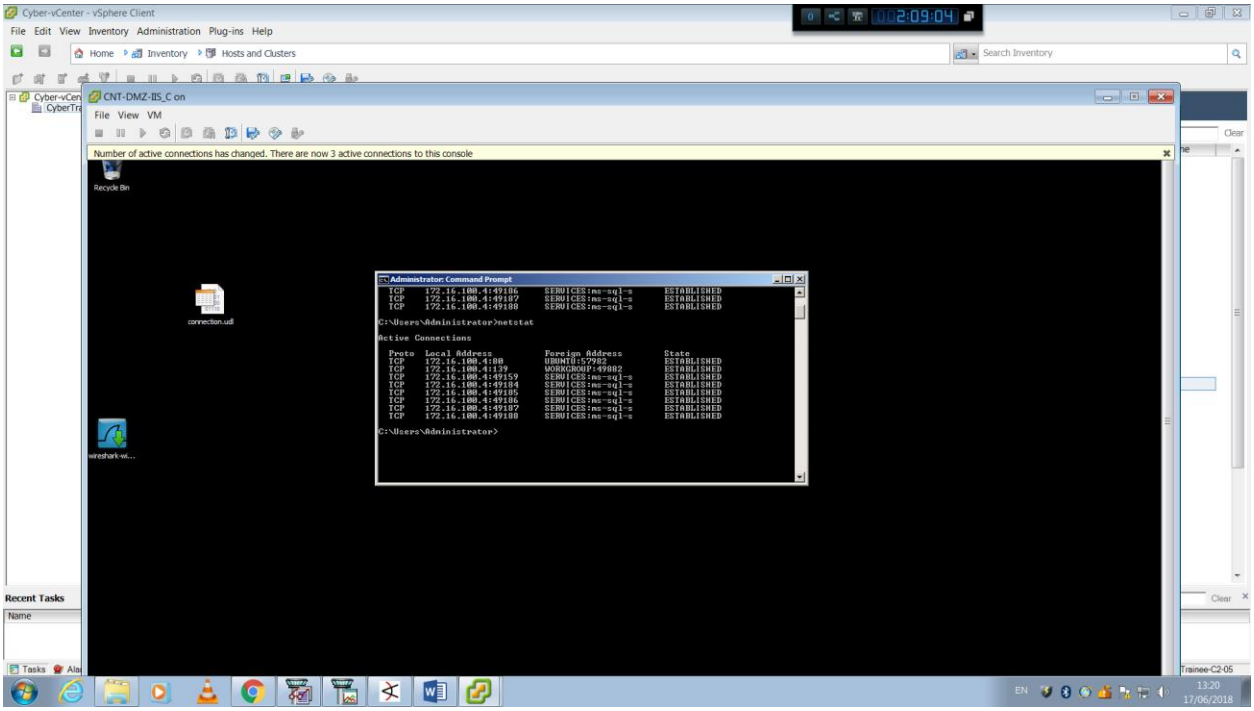


התחברות לשרת ה- DMZ-IIS –

הפעלת Wireshark –

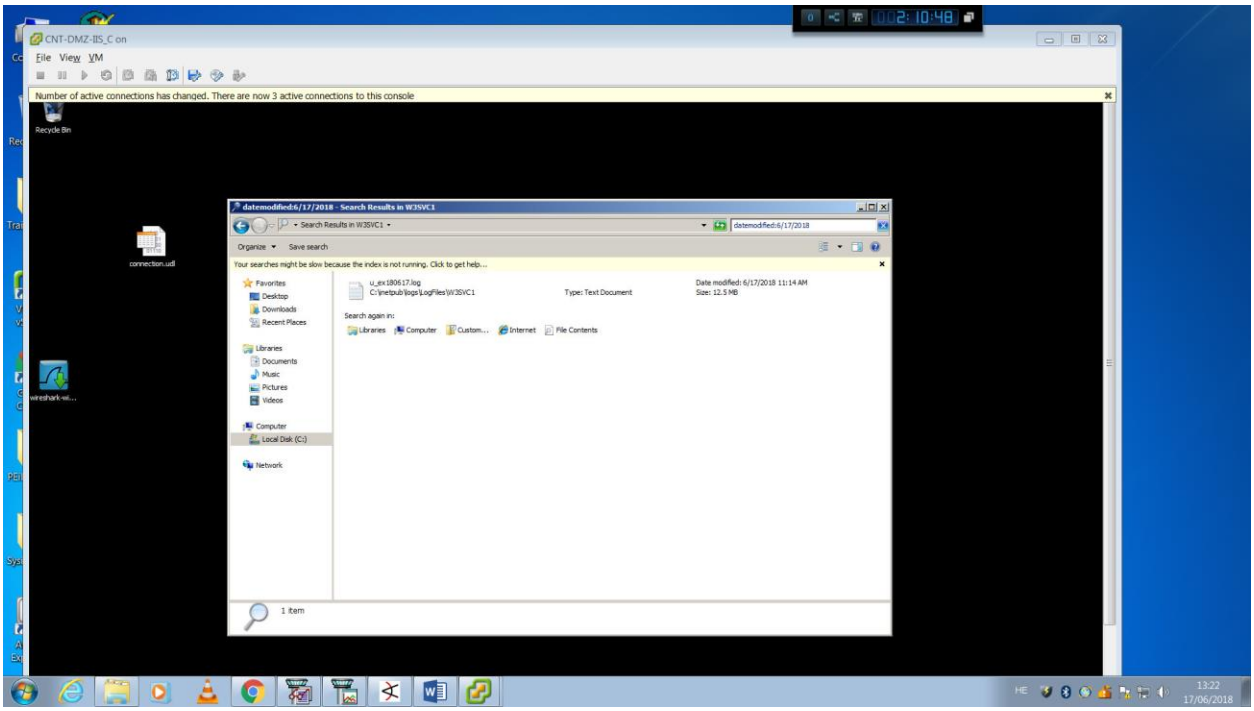


הרצת Netstat בשרת –

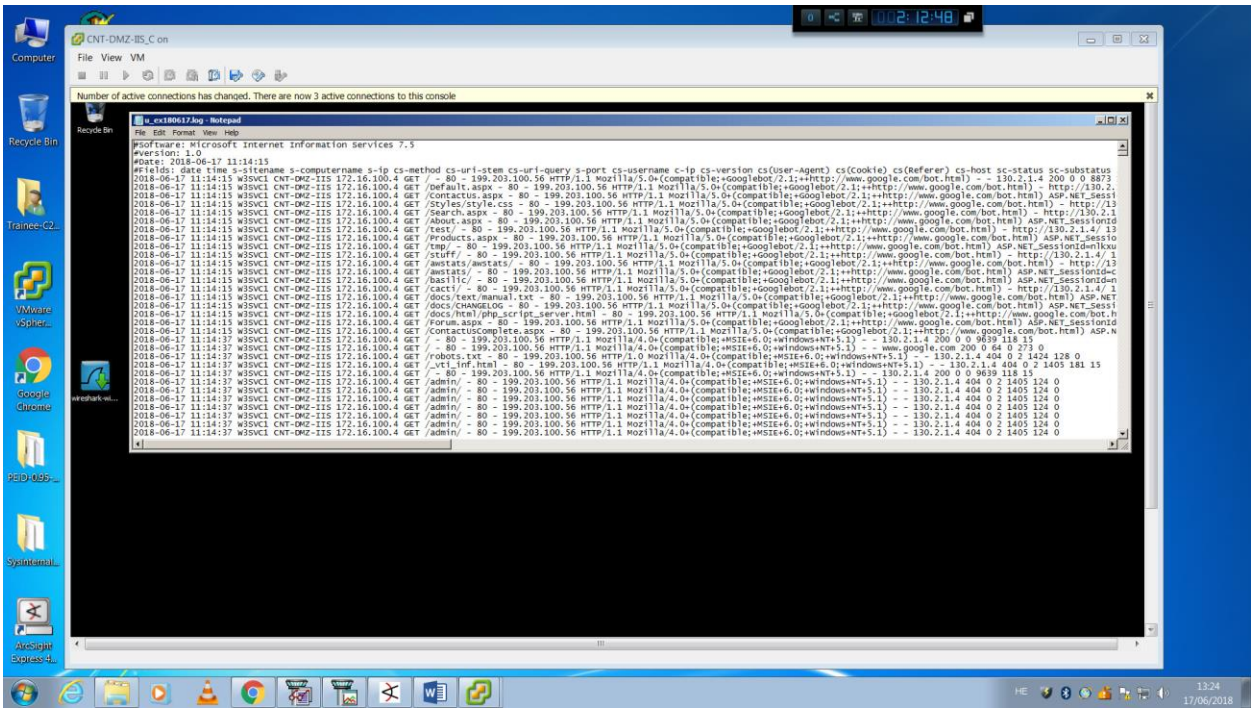


לא נראה חשוד במיוחד.

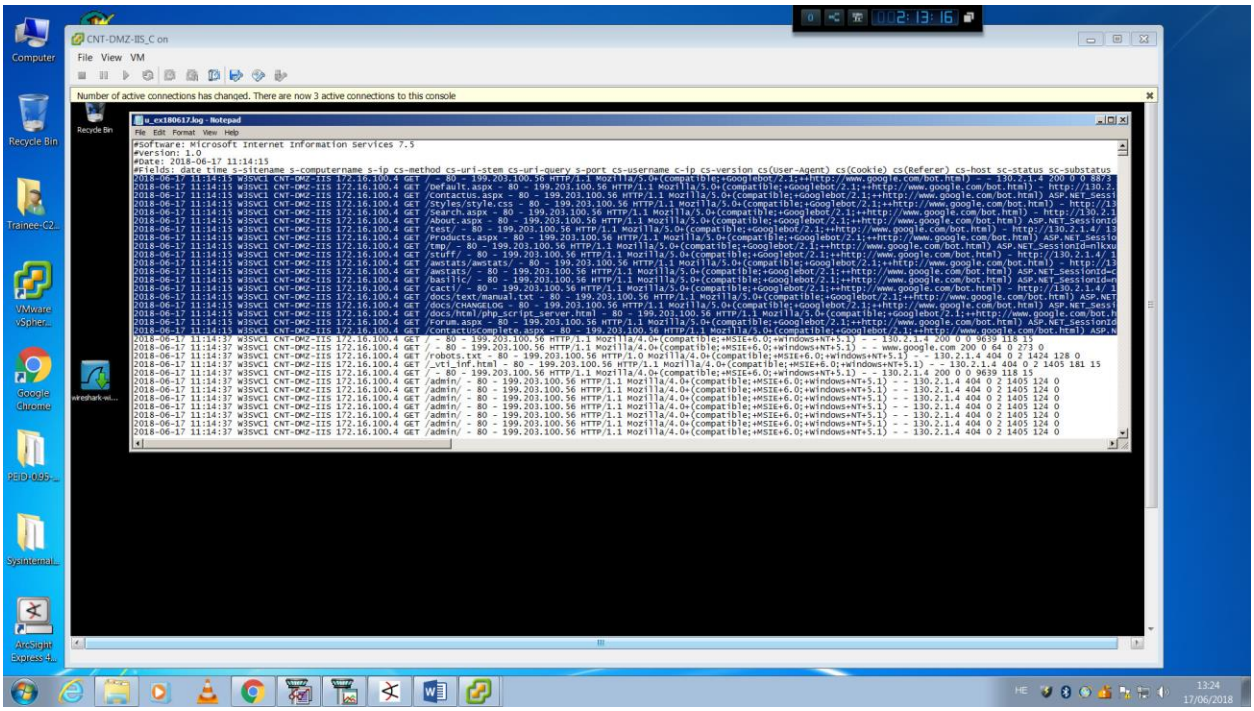
בדיקת קבצים שנוצרו / שונו לאחרונה –



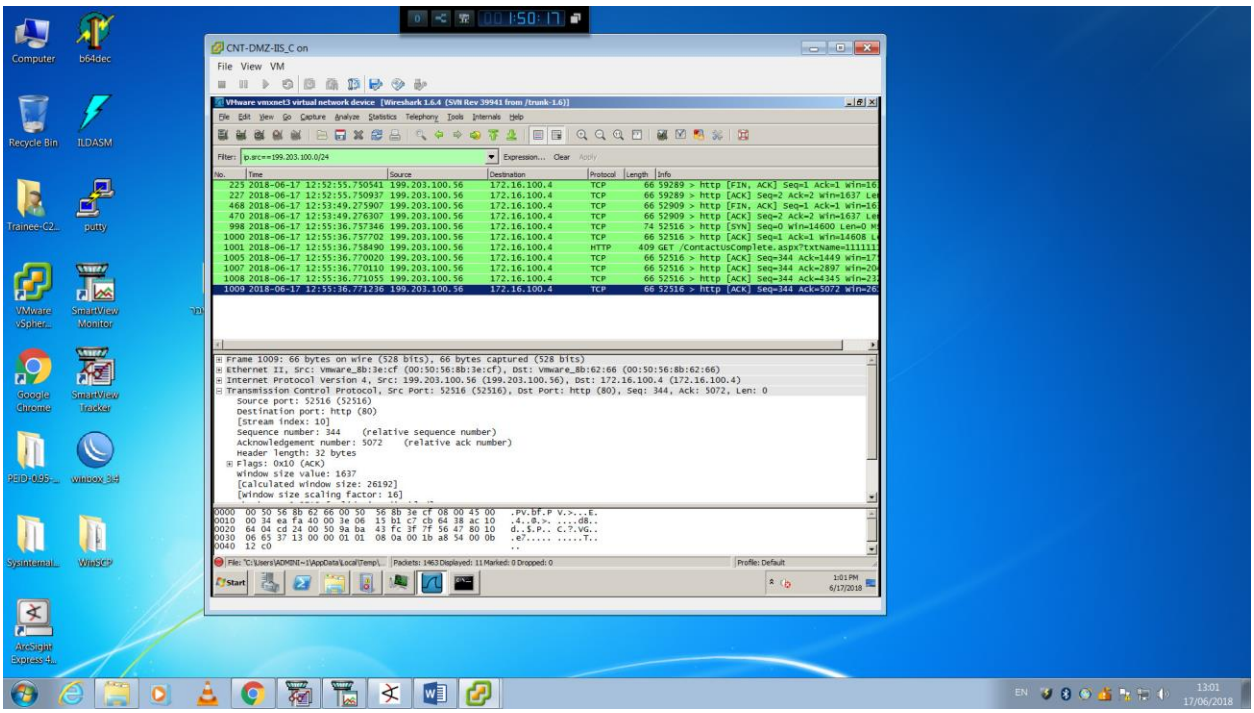
כניסה לקובץ הלוגים –



ניתן לראות בשורות המסומנות את הטקסט החשוד –

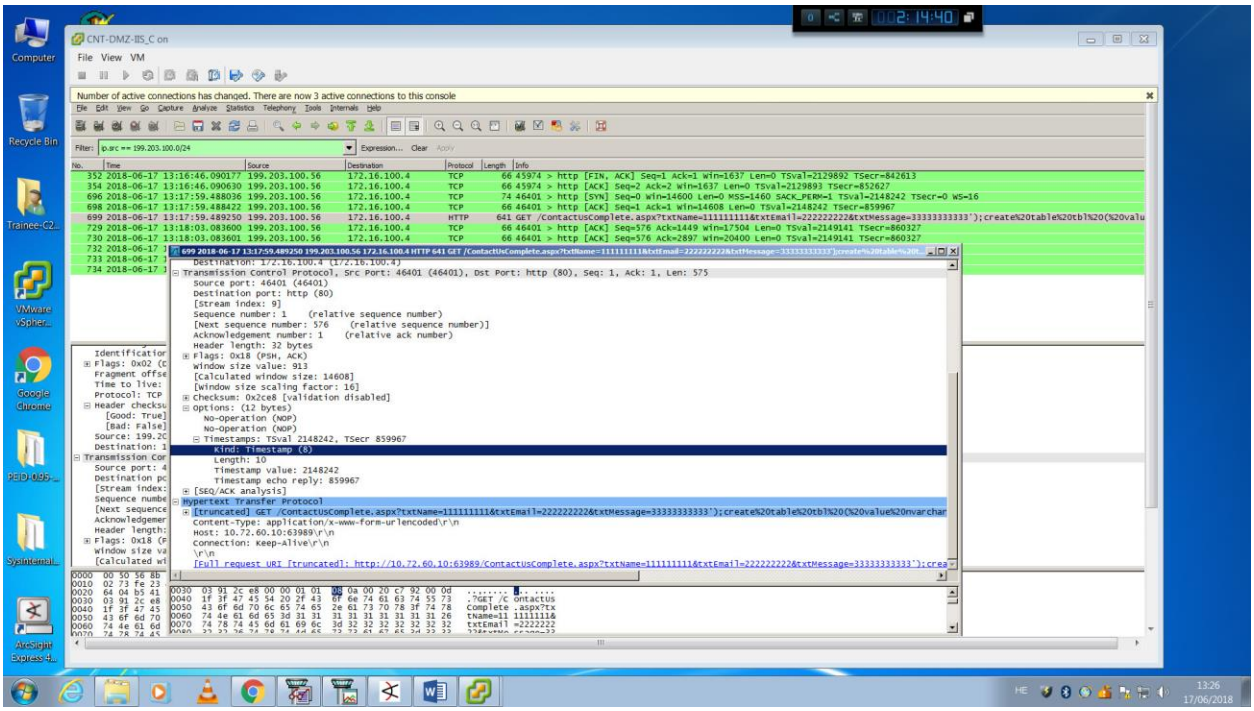


כאשר מגדירים את ה- Source IP להיות IP חיצוני בכלי Wireshark –



ניתן לראות שיש IP חיצוני שמתקשר עם השרת DMZ-IIS.

שנכנסים לבקשת ה- GET רואים את הדברים הבא –

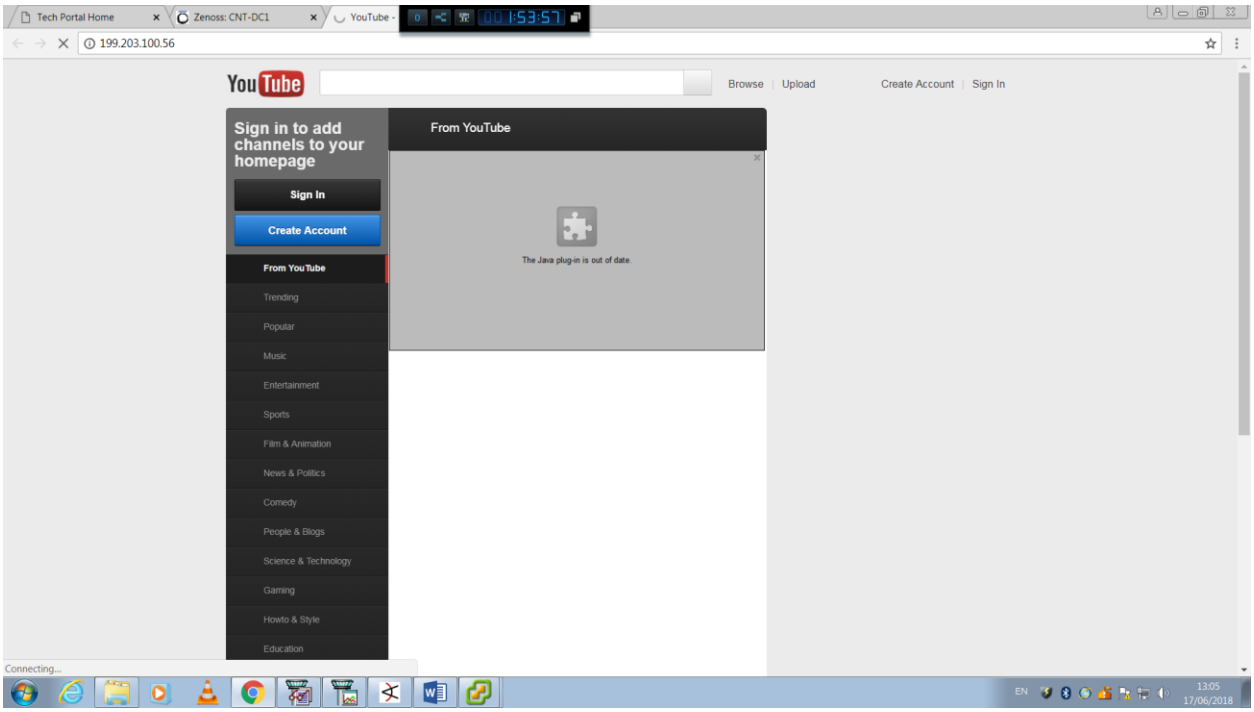


ניתן להסיק שאולי יש כאן בקשת SQL ונחקור לכיוון "הזרקת SQL".

הזרקת SQL היא שיטה לניצול פרצת אבטחה בתוכנית מחשב בעזרת פניה אל מסדי הנתונים.

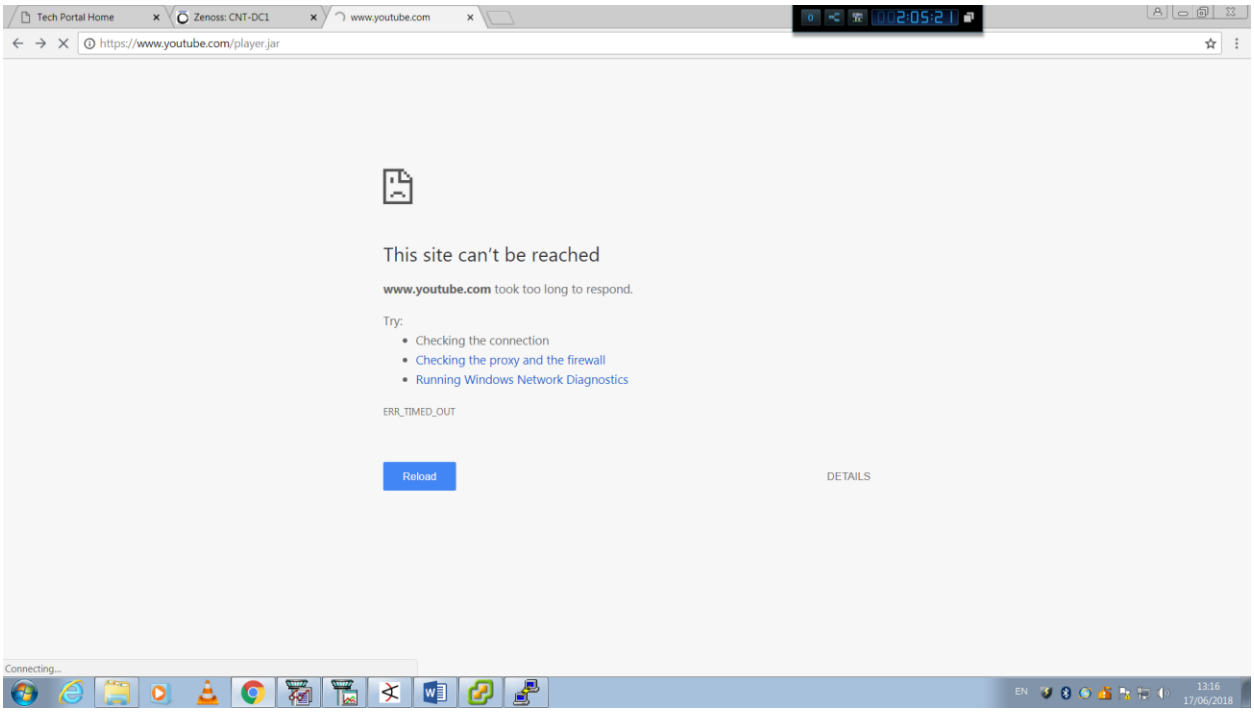
המשך בשלב זה בתהליך הזיהוי.

ברגע שנכנס לכתובת ה- IP דרך הדפדפן נזהה את הדבר הבא –



מכאן, נשאלת השאלה מדוע כתובת זו פונה לשרת ה- DMZ-IIS? ואיך תהליך זה קרה? ולמה האתר הזה הוא חיקוי של האתר YouTube?

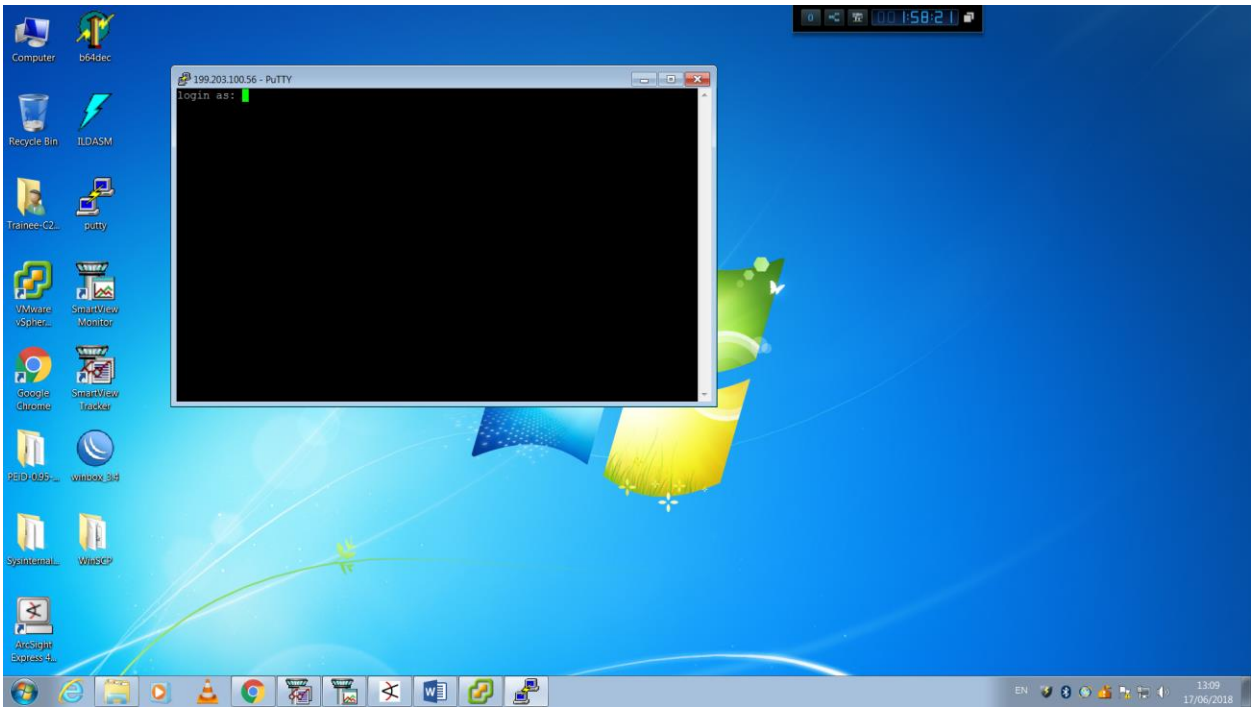
לאחר זמן ממושך באתר הוא מעביר אותו לכאן –



כחלק מתהליך "חקירת התוקף" נרצה לבדוק כמה דברים כגון,

- מהו ה- IP החשוד שפוגע בארגון שלנו?
- אילו שירותים פתוחים אצל התוקף? (פורט 80, 22 וכו').
- פעולותיו השונות של התוקף בעזרת הכלים שעומדים לרשותנו.
- מה מטרת התוקף?

מכאן, ניסיון התחברות באמצעות פורט 22 בפרוטוקול SSH –



תהליך הזיהוי:

בתהליך הזיהוי, להבין מדוע יש לנו שאילתת SQL ב- GET מ- IP חיצוני.

נרצה להתחבר ל- SQL שאליו שרת ה- DMZ פונה בבקשת השאילתא.

לאחר מכן, נבדוק איזה מידע רגיש התוקף ניסה לשאוב מה- Database שלנו, ונבדוק האם הצליח.

בנוסף לכך, נרצה למנוע את האפשרות הזאת שתוקף יצליח לגשת למידע רגיש בארגון באמצעות (הזרקת SQL).

תהליך הגנה:

בתהליך ההגנה נצטרך לשמור על הארגון שלנו מתקיפות מסוג זה.

תהליך הגנה מונעת:

- הארגון שלנו פרוץ לשאילתות SQL דרך הדפדפן.

  זה לא תקין ולכן נצטרך לטפל בכך.

- לא הגיוני שעובר מידע רגיש מ- SQL לשרת DMZ בעזרת שאילתא.

הפרצות באבטחת הארגון

ראה "תהליך הגנה מונעת".