**פרויקט גמר - הסבר במילים על הקוד:**

TOOLS:

## FeaturesExtraction.py

קוד זה אחראי על ייצוא כל 16 הפיצ'רים שלנו וייצוא שלהן לקובץ CSV.

RatioMatrix.py

TESTS:

test\_ann.py:

test\_elm.py:

test\_features\_permutations.py:

בודק את כל ה permutations של הפיצ'רים שלנו

test\_lr.py:

test\_robustness.py:

בודק רובסטיות של הפיצ'רים שלנו

test\_svm.py:

MODELS:

DATASET COLLECTORS:

urlScan.py:

אוסף מידע מהשירות urlscan.io

Sniffer.py:

המחלקה Sniffer משתמשת בScapy לצורך איסוף תעבורת הרשת שעוברת בכרטיס הרשת - מסננת לפי הDATA הרצוי (ככה למשל מחלקת CollectDNS מצליחה לאסוף את רשומות הDNS).

CollectDNS.py:

מחלקה שאוספת רשומות של הDNS

מחוץ לתיקייה TOOLS של DATASET COLLECTORS:

append\_whois\_urlscan.py

אחראית להוסיף מידע מurlscan.io לרשומות dataset של DNS.

collectDns.py:

אוסף מידע DNS מקובצי CSV (אקסל)

collect\_vt.py:

אוסף מידע מvirusTotal

vt\_to\_features.py:

מייצא את המידע הרצוי מvirustotal מקובץ JSON.