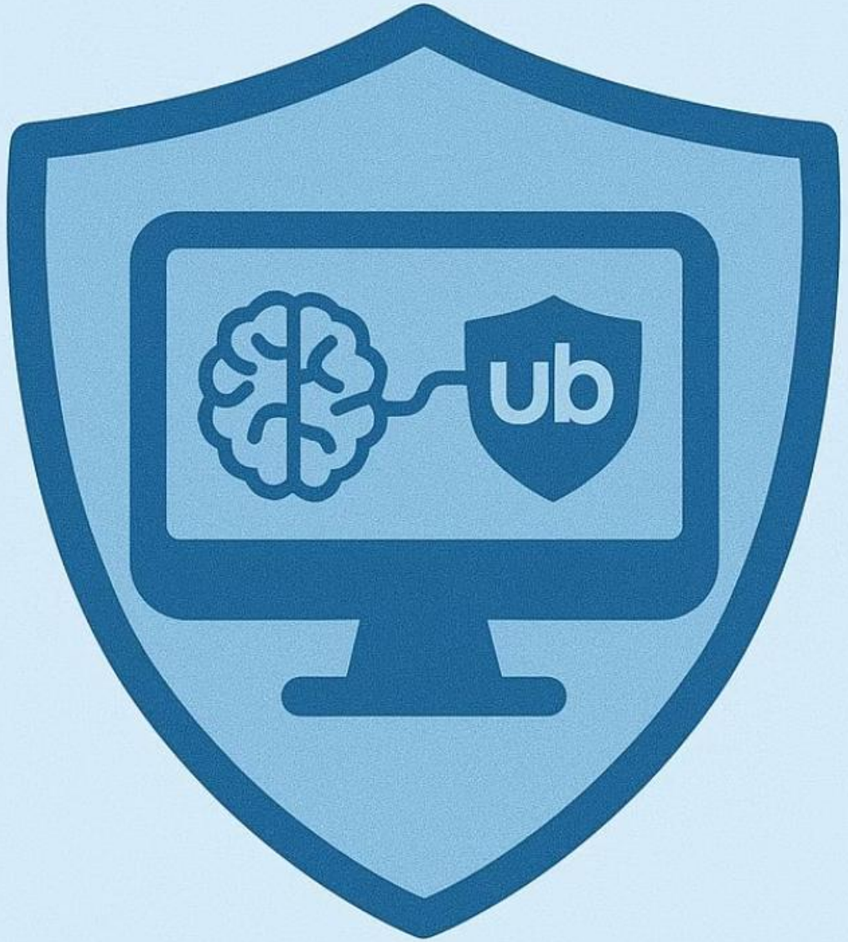
UBE - uBlock Enhanced ML-Powered Phishing Detection

Enhancing online security through real-time, client-side machine learning for phishing detection.
Showcasing our end-to-end development journey, from initial design to native integration directly into uBlock Origin.

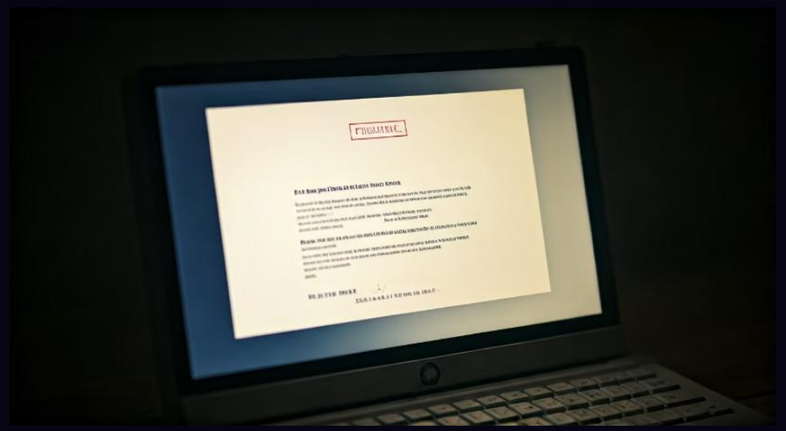
By Niv Levy, Michael Ben-Zur and Roy Tentzer



Project Idea & Problems Addressed

Key Problems

- Users are increasingly targeted by advanced phishing methods.
- Dynamic content can bypass basic checks.
- Static lists are ineffective against new threats.



The Idea

Integrate a lightweight, client-side ML model into uBlock Origin.

- Perform real-time analysis of URL
- Parse HTML structure and JavaScript behavior
- Assess site authenticity.

High-Level Overview of Detection Flow

Dynamic Feature Collection 1

Extension observes page navigations, records URL and HTML details.

Real-Time Classification 2

Data is processed by the ML model to classify the page as safe or phishing.

Clear Popup Alert 3

Displays the verdict through familiar color indicators.

Crafting the Dataset & Training Model

Collection

Collected confirmed phishing and safe URLs from trusted domain feeds.

Verification & Filtering

Cross-validated and filtered URLs, discarding any unreachable domains.

Python Implementation

Developed an efficient pipeline for data collection and feature extraction.

Model Sweep

Evaluated multiple ML models for accuracy, speed, and efficiency.

Feature Selection

Filtered low-impact features to improve accuracy and prediction consistency.

Browser Implementation

Ported the full pipeline and ML model to JavaScript for native in-browser execution.

Integration

Integrated into uBlock Origin to enhance real-time phishing protection in-browser.

Technical Architecture: Analysis Pipeline (Stages)

URL Analysis

Quickly extracts features such as length, resources, and other token patterns.

Metadata Enrichment

Queries an API to retrieve additional domain data, including SSL validity, WHOIS records, and other key attributes.

HTML Parsing

Parses raw HTML to identify forms, scripts, and other structural or textual patterns.

Model Assessment

Combined features from all stages are passed to the ML model to produce the final verdict.

System Components & Technologies

Extension

JavaScript, Node.js, Python, WebExtensions API

Metadata Micro-service

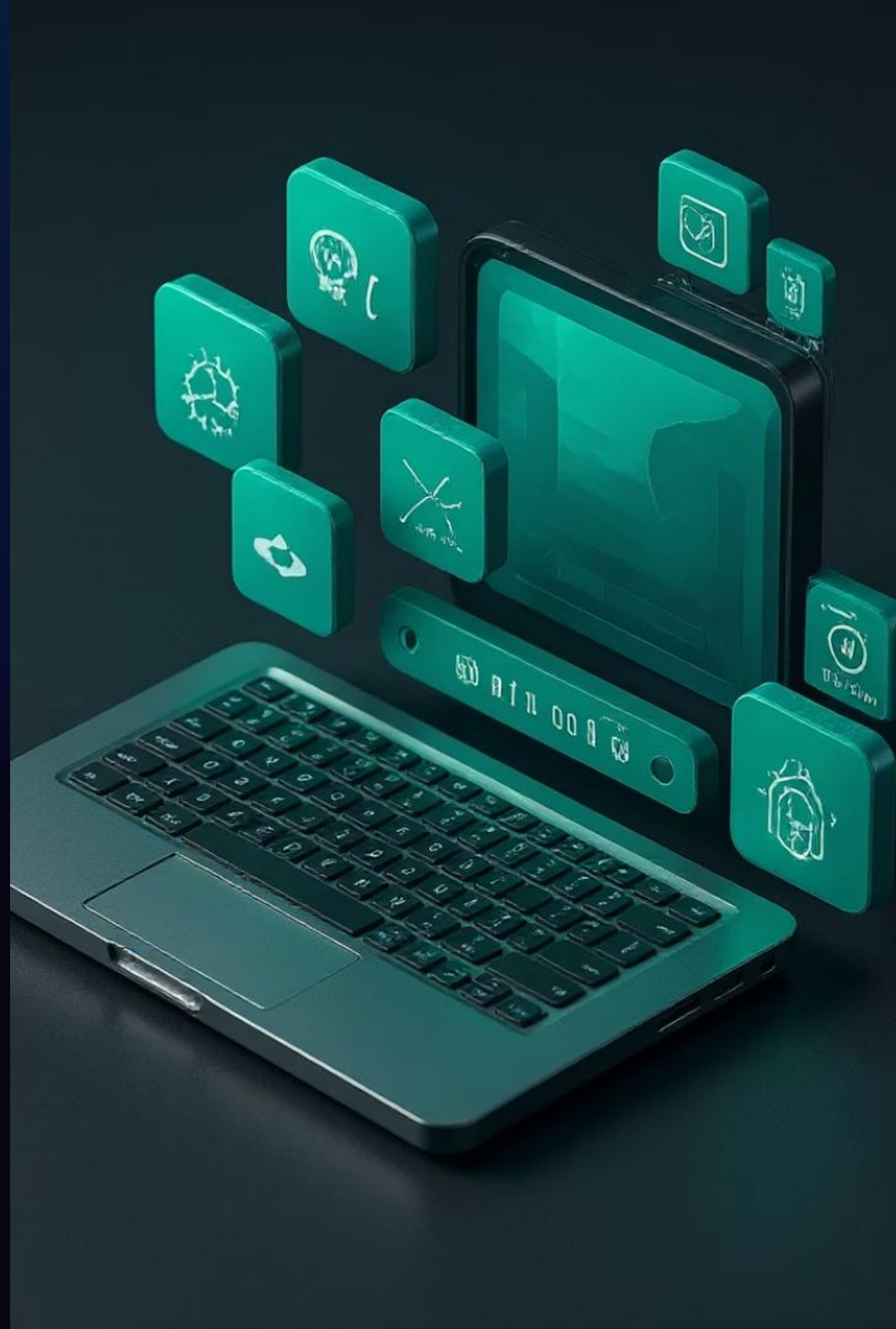
AWS Lambda & API Gateway

uBlock Origin (Foundation)

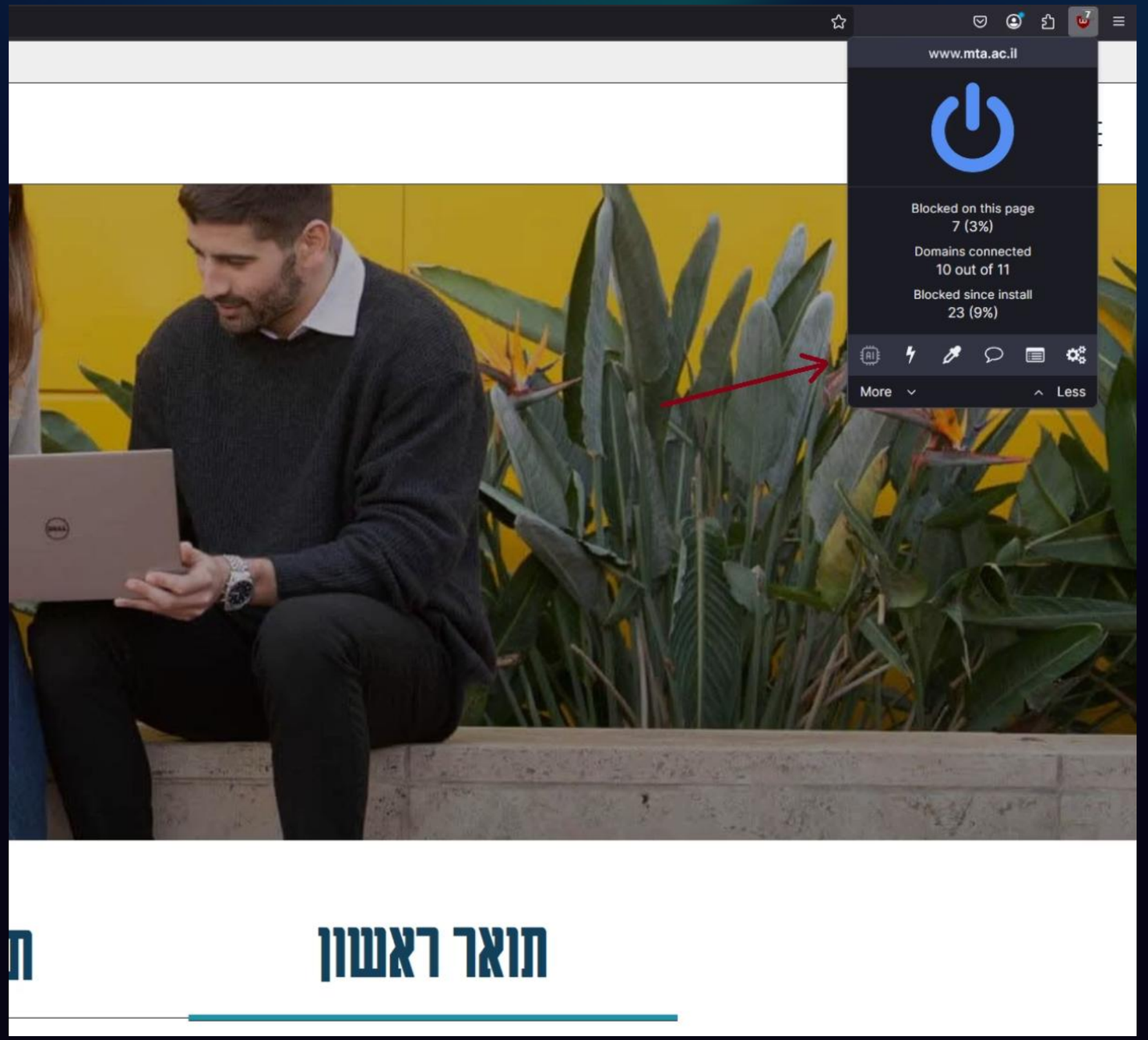
Provides baseline static threat blocking

Libraries

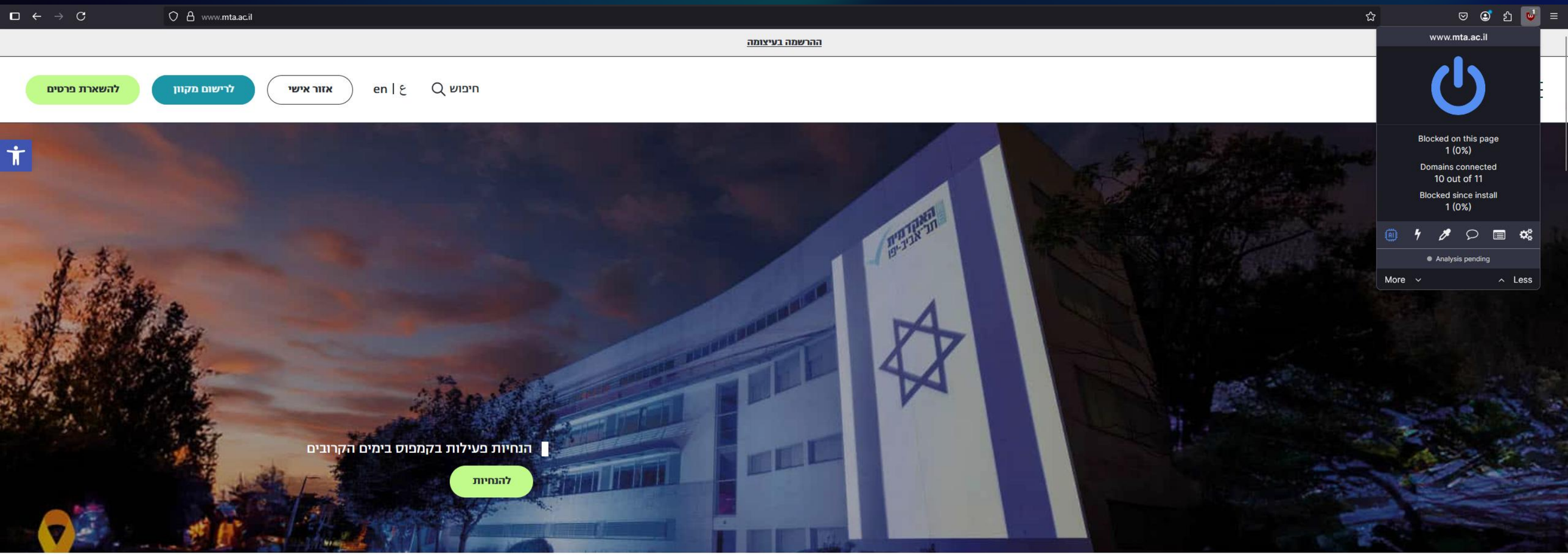
Scikit-Learn, Selenium, Beautifulsoup, Playwright, esbuild



Toggle Off


www.mta.ac.il
Blocked on this page
7 (3%)
Domains connected
10 out of 11
Blocked since install
23 (9%)
More
Less
תואר ראשון

Toggle On - Pending

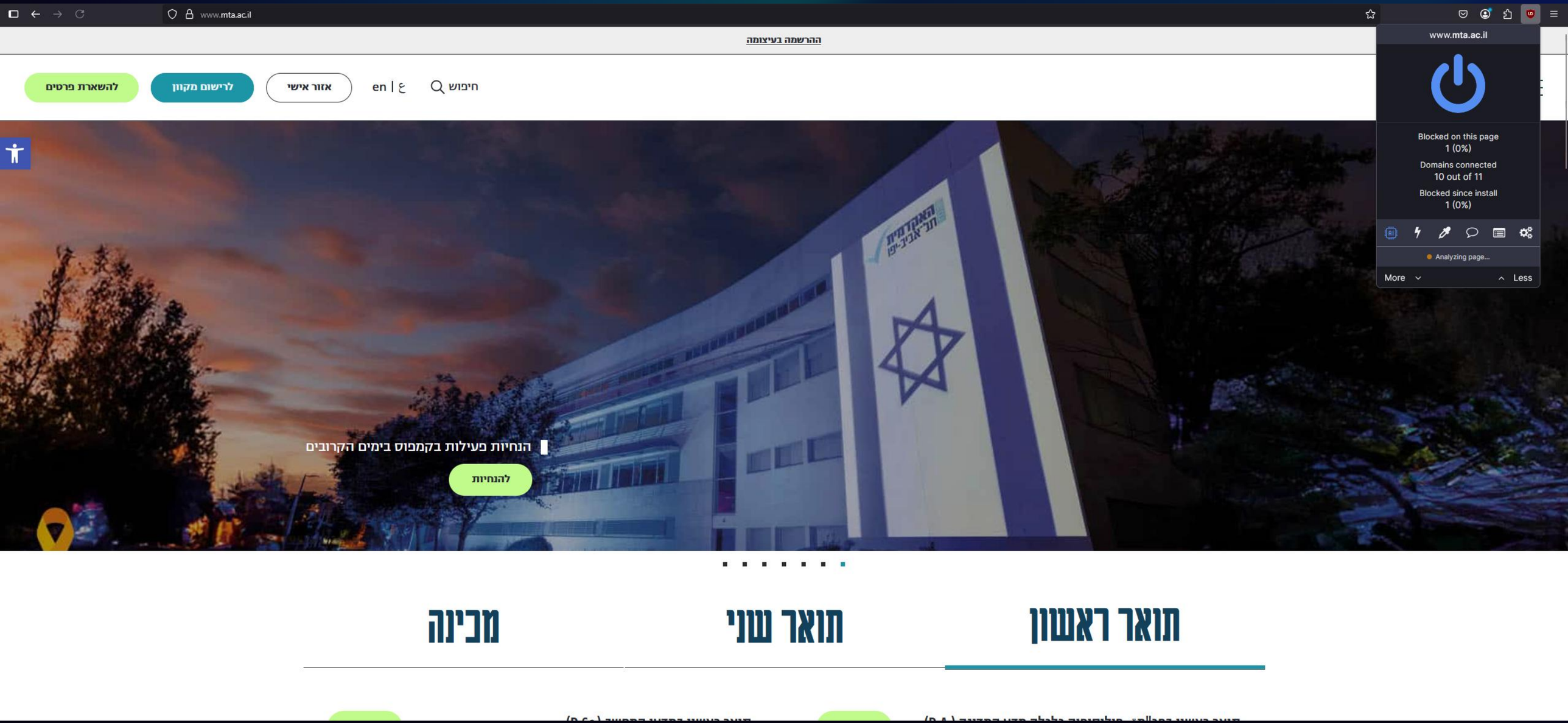


תואר ראשון

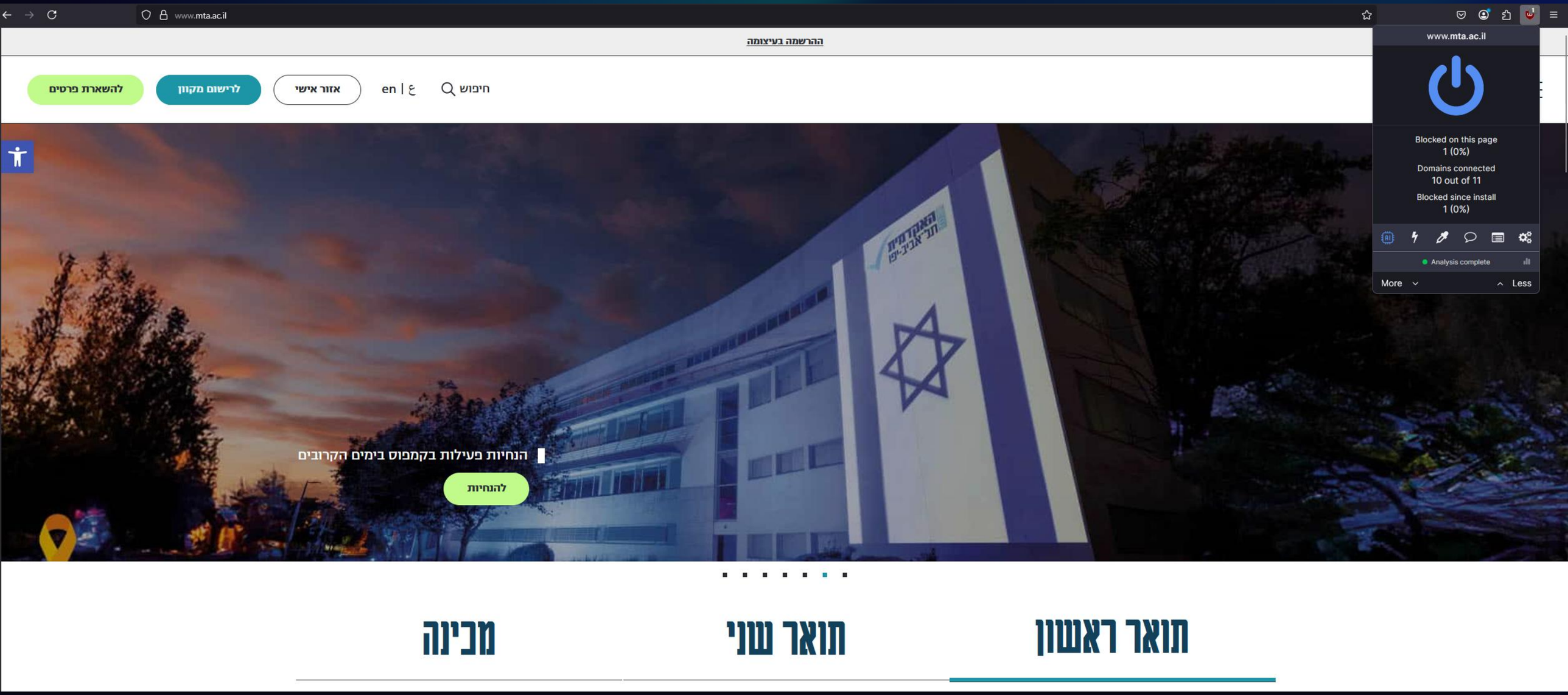
תואר שני

מכינה

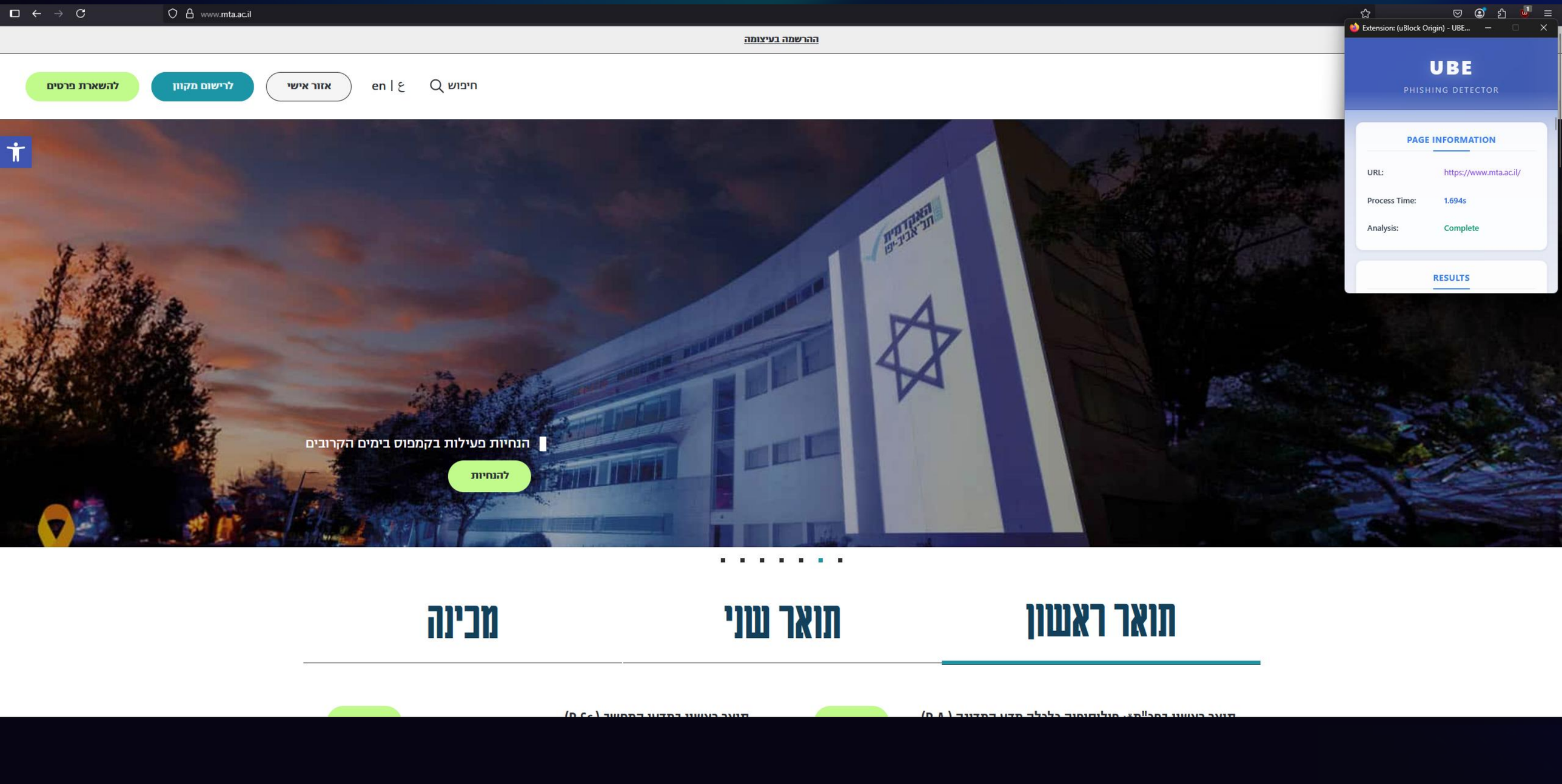
Toggle On - Analyzing



Toggle On - Complete



Results Example



Future Work & Enhancements

Integrate NAS

Host blacklist data, model updates, and user reports.

Dynamic blacklist for uBlock Origin's filtering

Local cache that collects phishing data and syncs with a remote-hosted blacklist.

Android Firefox Support

Extend compatibility to mobile browsing environments.

Explore Lightweight Models

Evaluate performance for potential future upgrades.

Thank you for listening to our presentation

- Michael Ben-Zur - michaelbe2@mta.ac.il
- Roy Tentzer - royte@mta.ac.il
- Niv Levy - nivle2@mta.ac.il