

MICHIGAN STATE
UNIVERSITY

Alpha Presentation

Packet Forge: AI Network Protocol Engine

The Capstone Experience

Team Vectra AI

Samuel Barnhart

Nihar Bollareddy

Sean Finkel

Yeji Lee

Kaajal Shah

Aanshik Upadhyay

Department of Computer Science and Engineering

Michigan State University

Fall 2025



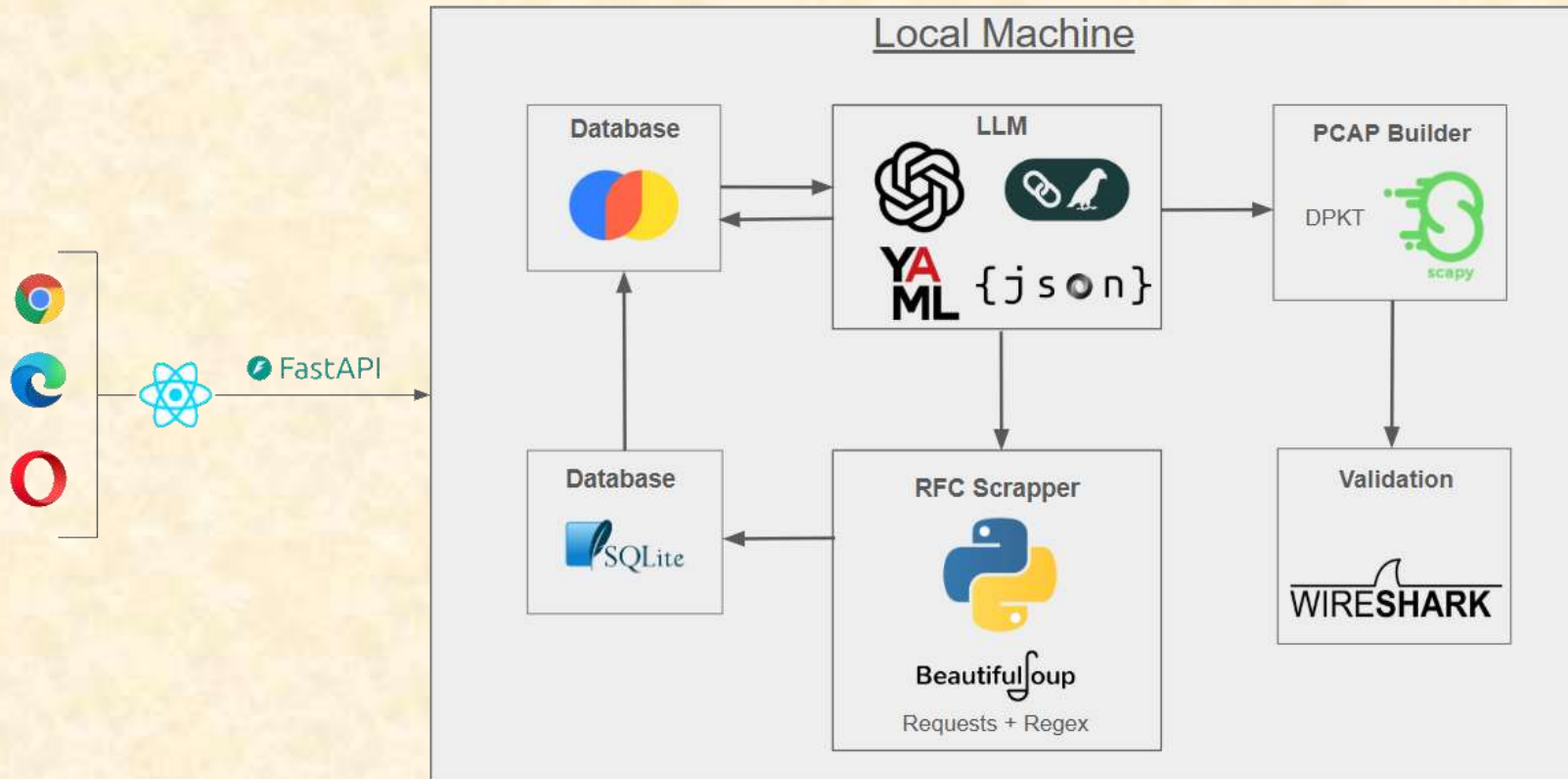
From Students...
...to Professionals

Project Overview

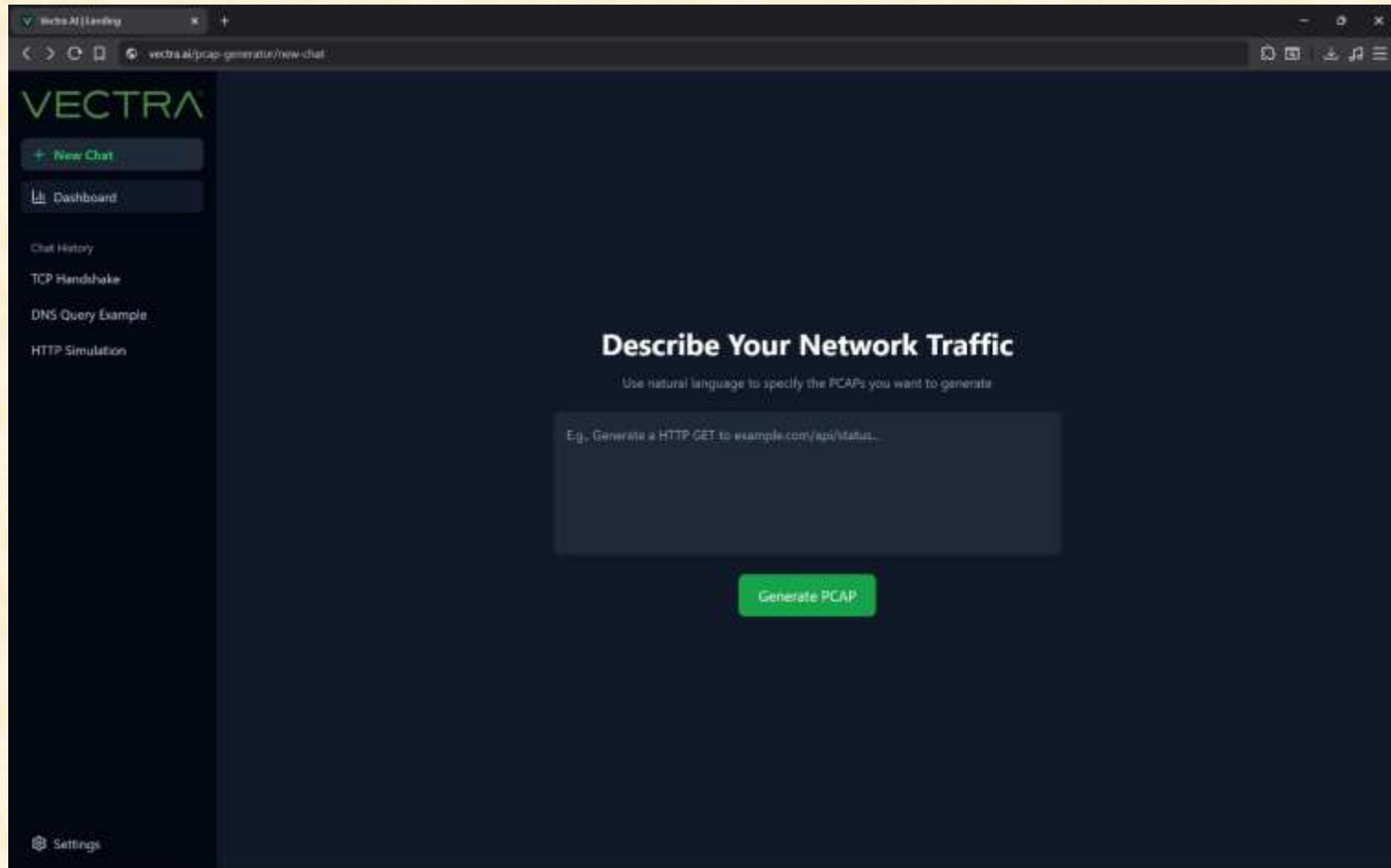
- Vectra AI is the industry leader in preventative cybersecurity AI, relying on vast, high-quality network data to train its detection systems
- A major obstacle is the strenuous and intricate process of creating realistic network traffic for training such models, which is not yet automated
- Packet Forge solves this problem by automating high-quality, AI-driven packet generation



System Architecture



Landing Page



Use Case 1

The screenshot displays the Vectra AI Chat web application. The interface includes a sidebar on the left with navigation links: 'New Chat', 'Dashboard', 'Chat History', 'TCP Handshake', 'DNS Query Example', 'HTTP Simulation', and 'Settings'. The main content area shows a chat conversation. A green button at the top right says 'Simulate a directory login packet capture'. Below it, a message from the AI states: 'Done ✅ Your packet capture has been generated and validated! The scenario models the standard flow behavior for the described protocol, ensuring each step aligns with expected communication patterns. Download it below and review the validation panel for detailed structural checks.' A green 'Download PCAP' button is provided. A toggle switch 'Hide Validation Results' is set to 'off'. A table displays the validation results:

Check	Status
Structure Valid	Pass
Checksum OK	Pass
Scenario Matched	Pass

Below the table, another green button says 'Create another capture where multiple clients query the same LDAP server'. A second message from the AI follows: 'Success! 🎉 Your PCAP is ready and has passed validation checks for correctness. It contains simulated client-server transactions modeled on the typical request-response structure of the given protocol. Download it below and open the validation panel to review all checks and ensure accuracy.' Another green 'Download PCAP' button is shown, along with a 'View Validation Results' toggle. At the bottom, there is a text input field with a placeholder 'Type a request (e.g. "Generate a standard LDAP packet capture")' and a green send button.



Use Case 2

The screenshot displays the Vectra AI web application interface. On the left is a dark sidebar with navigation links: '+ New Chat', 'Dashboard', 'Chat History', 'TCP Handshake', 'DNS Query Example', and 'HTTP Simulation'. The main content area has a dark background. At the top, a green banner reads 'Generate a packet capture for a client requesting a webpage over HTTP'. Below this, a success message states: 'Success! 🎉 Your PCAP is ready and has passed validation checks for correctness. It contains simulated client-server transactions modeled on the typical request-response structure of the given protocol. Download it below and open the validation panel to review all checks and ensure accuracy.' A green 'Download PCAP' button is present. Below the button, a collapsed section 'Hide Validation Results' reveals a table with three rows of validation checks, all marked as 'Pass'. A second green banner prompts: 'Now show a follow-up capture with multiple GET requests from the same client.' This is followed by another success message: 'Great news — your requested PCAP has been successfully built! 🎉 It includes realistic packet exchanges derived from your prompt, capturing accurate message sequencing and flow direction. You can download the PCAP file below and explore it in Wireshark to review structure and protocol integrity.' A second 'Download PCAP' button is shown. At the bottom, a 'View Validation Results' link and a chat input field with a green send button are visible.

Generate a packet capture for a client requesting a webpage over HTTP

Success! 🎉 Your PCAP is ready and has passed validation checks for correctness. It contains simulated client-server transactions modeled on the typical request-response structure of the given protocol. Download it below and open the validation panel to review all checks and ensure accuracy.

Download PCAP

Hide Validation Results

Check	Status
Structure Valid	Pass
Checksum OK	Pass
Scenario Matched	Pass

Now show a follow-up capture with multiple GET requests from the same client.

Great news — your requested PCAP has been successfully built! 🎉 It includes realistic packet exchanges derived from your prompt, capturing accurate message sequencing and flow direction. You can download the PCAP file below and explore it in Wireshark to review structure and protocol integrity.

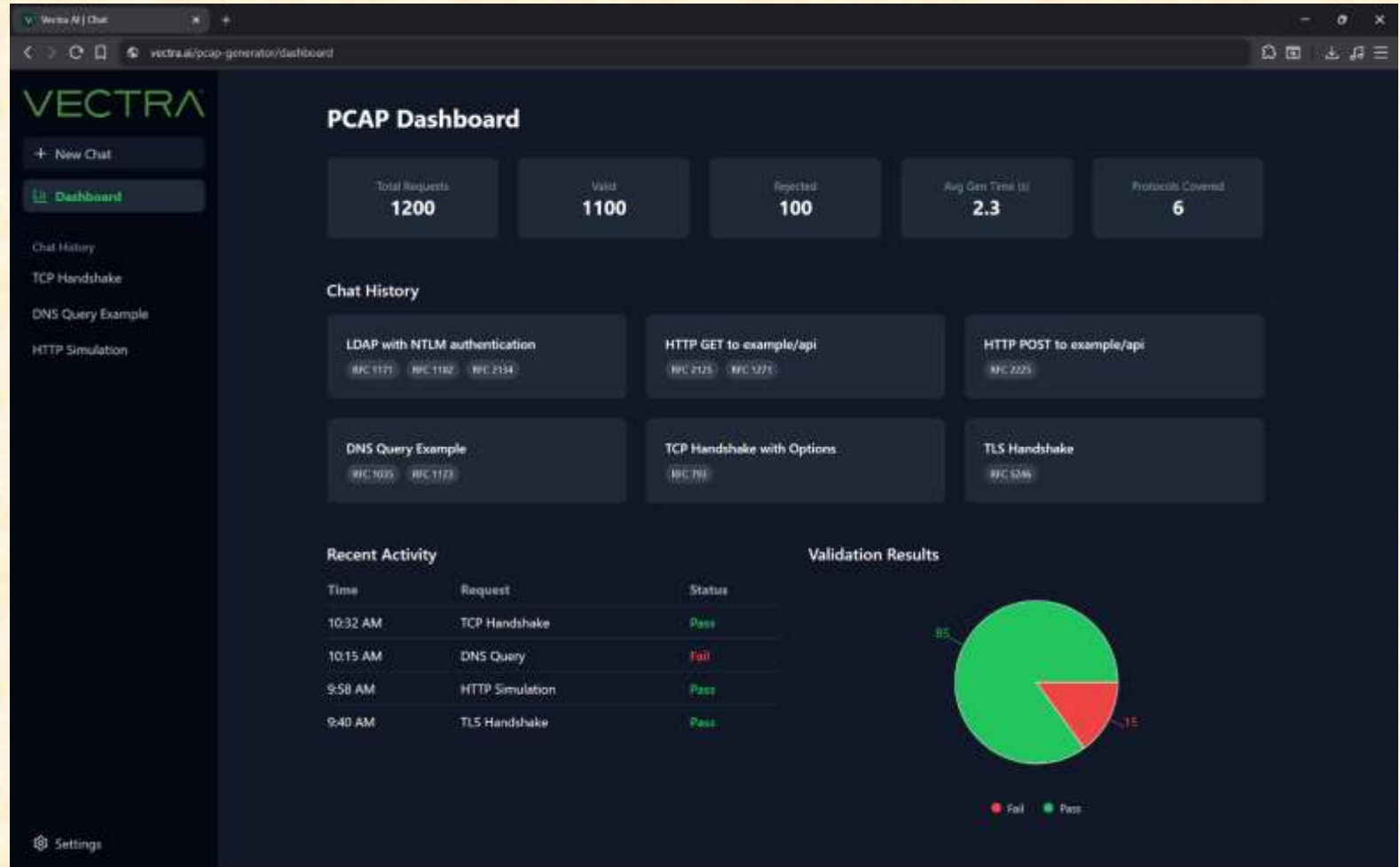
Download PCAP

View Validation Results

Type a request (e.g. 'Generate a standard ICMP packet capture').



Dashboard



What's left to do?

- Make the back-end fully modular and ready for all protocols
- Allow the system automatically learn protocol behavior from RFCs or technical PDFs
- Verify PCAP accuracy using Wireshark and Scapy
- Containerize full system

Questions?

?

?

?

?

?

?

?

?

?

