



Beta 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



Team Member's Technical Tasks

Technical Tasks Assigned

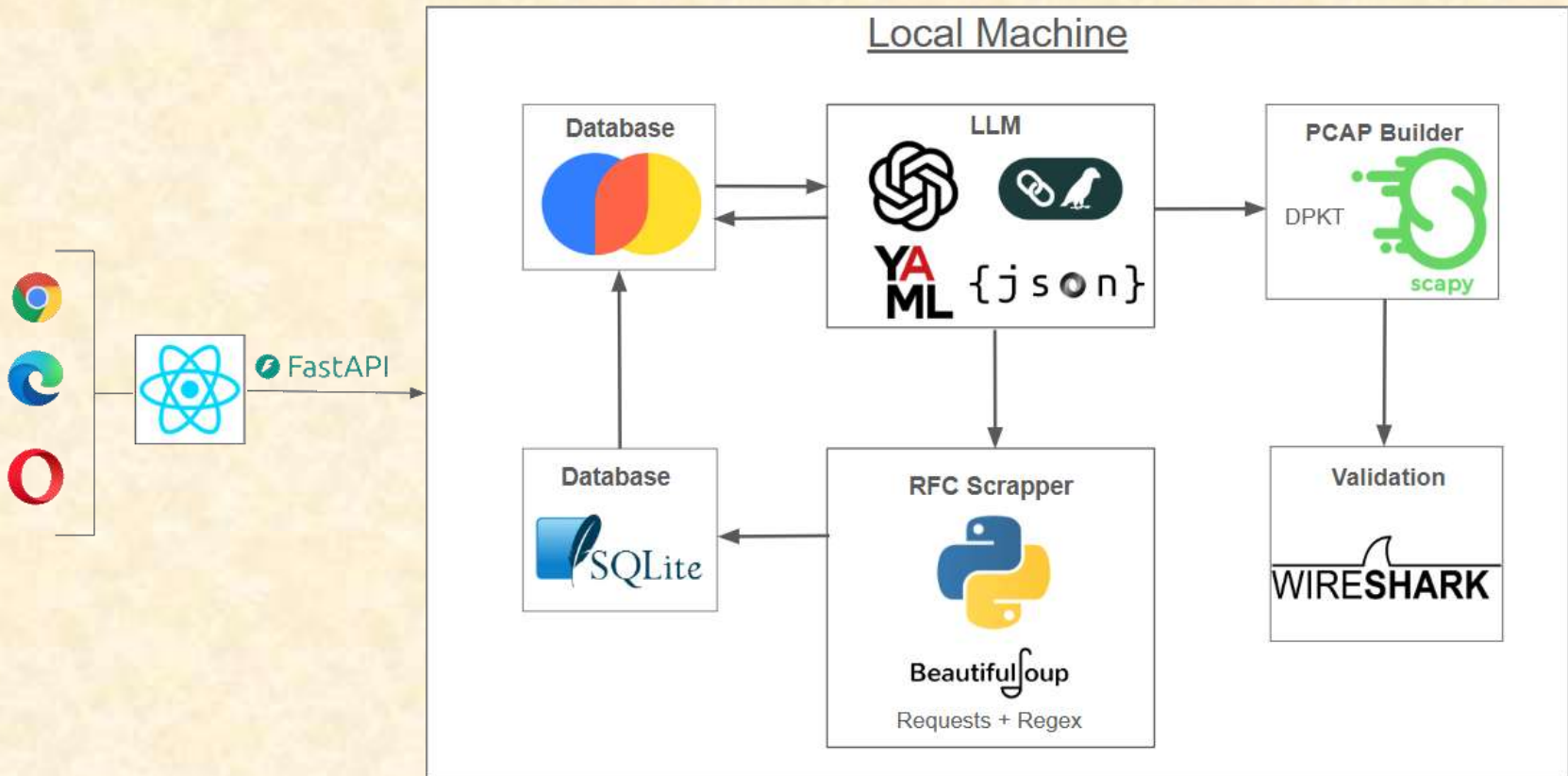
- Sean Finkel
 - Programmatic pcap generation
 - LLM pcap generation
 - Creation of fabricated metadata
- Aanshik Upadhyay
 - Database setup and management
 - Frontend work
 - Validation for protocols
- Sam Barnhart
 - RFC scraper
 - Database Visualizer
 - Pcap annotator
- Yeji Lee
 - Orchestrator
 - Self submitted pcap validator
 - Validation rules
- Kaajal Shah
 - Asn1 Encoder
 - Chat history
 - Generate pcap for non ruled protocols
- Nihar Bollareddy
 - Vector Embeddings
 - LLM base functionality
 - ChromaDB

Technical Tasks Completed

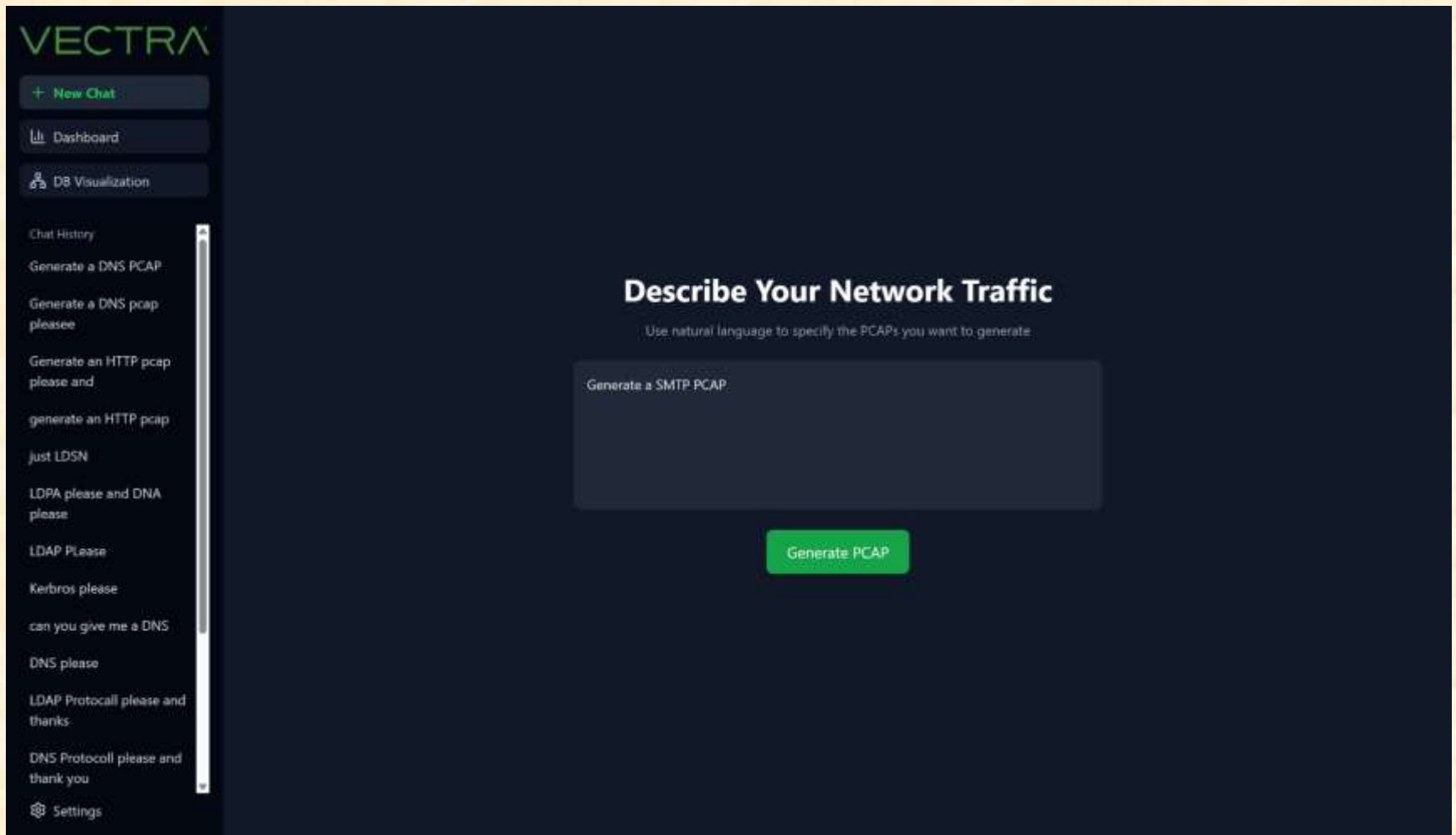
- Sean Finkel
 - Programmatic pcap generation
 - LLM pcap generation
 - Creation of fabricated metadata
- Aanshik Upadhyay
 - Database setup and management
 - Frontend work
 - Validation for protocols
- Sam Barnhart
 - RFC scraper
 - Database Visualizer
 - Pcap annotator
- Yeji Lee
 - Orchestrator
 - Self submitted pcap validator
 - Validation rules
- Kaajal Shah
 - Asn1 Encoder
 - Chat history
 - Generate pcap for non ruled protocols
- Nihar Bollareddy
 - Vector Embeddings
 - LLM base functionality
 - ChromaDB



System Architecture



Landing Page



Chat

The screenshot displays the Vectra AI web interface. On the left is a dark sidebar with a 'VECTRA' logo at the top. Below the logo are navigation links: '+ New Chat', 'Dashboard', and 'DB Visualization'. A 'Chat History' section follows, listing several chat titles such as 'Generate a SMTP PCAP', 'Generate a DNS PCAP', and 'LDAP please and DNA please'. At the bottom of the sidebar is a 'Settings' icon. The main content area has a dark background. At the top right is a green button labeled 'Generate a SMTP PCAP'. Below this, a message states: 'Great news — your requested PCAP has been successfully built! 🎉 It includes realistic packet exchanges derived from your input and verified structural integrity. Download the file below and expand the validation section to explore packet-level compliance results.' Below the message is a green 'Download PCAP' button. Underneath is a toggle for 'Hide Validation Results' and a file selection area with a 'Choose File' button and the text 'No file chosen'. A table with two columns, 'Check' and 'Status', lists five validation checks, all of which are marked as 'Pass'. At the bottom is a chat input area with a dropdown menu set to 'LDAP', a text field containing 'Type a request (e.g. "Generate a Kerberos AS-REQ/AS-REP capture")', and a green send button with a paper plane icon.

VECTRA

+ New Chat

Dashboard

DB Visualization

Chat History

Generate a SMTP PCAP

Generate a DNS PCAP

Generate a DNS pcap please

Generate an HTTP pcap please and

generate an HTTP pcap

just LDAP

LDAP please and DNA please

LDAP Please

Kerberos please

can you give me a DNS

DNS please

LDAP Protocol please and thanks

Settings

Generate a SMTP PCAP

Great news — your requested PCAP has been successfully built! 🎉 It includes realistic packet exchanges derived from your input and verified structural integrity. Download the file below and expand the validation section to explore packet-level compliance results.

Download PCAP

Hide Validation Results

Choose File No file chosen

Check	Status
SMTP must use port 25, 465, or 587	Pass
SMTP session must start with HELO or EHLO	Pass
MAIL FROM command must appear before RCPT TO	Pass
DATA command must follow RCPT TO and precede the message body	Pass
SMTP session must end with QUIT command	Pass

LDAP Type a request (e.g. "Generate a Kerberos AS-REQ/AS-REP capture")



Pcap validation

The screenshot displays the Vectra AI Chat application interface. On the left is a sidebar with navigation options: '+ New Chat', 'Dashboard', 'DB Visualization', and a 'Chat History' section listing various chat requests such as 'Generate a SMTP PCAP', 'Generate a DNS PCAP', 'Generate a DNS pcap pleasee', 'Generate an HTTP pcap please and', 'generate an HTTP pcap', 'just LDSN', 'LDPA please and DNA please', 'LDAP Please', 'Kerberos please', 'can you give me a DNS', 'DNS please', and 'LDAP Protocol please and thanks'. The main area shows the results of a chat request. At the top, a list of five SMTP validation checks is shown, all with a 'Pass' status: 'SMTP must use port 25, 465, or 587', 'SMTP session must start with HELO or EHLO', 'MAIL FROM command must appear before RCPT TO', 'DATA command must follow RCPT TO and precede the message body', and 'SMTP session must end with QUIT command'. A green button labeled 'Generate a LDAP PCAP' is visible. Below this, a message states: 'Great news — your requested PCAP has been successfully built! 🎉 It includes realistic packet exchanges derived from your input and verified structural integrity. Download the file below and expand the validation section to explore packet-level compliance results.' A green 'Download PCAP' button is present. A 'Hide Validation Results' link is followed by a 'Choose File' button and the text 'No file chosen'. A table titled 'Check' and 'Status' lists six LDAP validation checks, all marked as 'Pass': 'LDAP must use port 389 or 636 (LDAPS)', 'LDAP sessions must begin with a BindRequest message', 'LDAP requests use non-zero IDs; responses reuse the same ID', 'SearchRequest messages must include baseObject and scope fields', and 'ModifyRequest messages must contain at least one change operation'. At the bottom, a dropdown menu is set to 'LDAP' and a text input field contains the prompt 'Type a request (e.g. "Generate a Kerberos AS-REQ/AS-REP capture")'.

VECTRA

+ New Chat

Dashboard

DB Visualization

Chat History

Generate a SMTP PCAP

Generate a DNS PCAP

Generate a DNS pcap pleasee

Generate an HTTP pcap please and

generate an HTTP pcap

just LDSN

LDPA please and DNA please

LDAP Please

Kerberos please

can you give me a DNS

DNS please

LDAP Protocol please and thanks

Settings

SMTP must use port 25, 465, or 587

Pass

SMTP session must start with HELO or EHLO

Pass

MAIL FROM command must appear before RCPT TO

Pass

DATA command must follow RCPT TO and precede the message body

Pass

SMTP session must end with QUIT command

Pass

Generate a LDAP PCAP

Great news — your requested PCAP has been successfully built! 🎉 It includes realistic packet exchanges derived from your input and verified structural integrity. Download the file below and expand the validation section to explore packet-level compliance results.

Download PCAP

Hide Validation Results

Choose File No file chosen

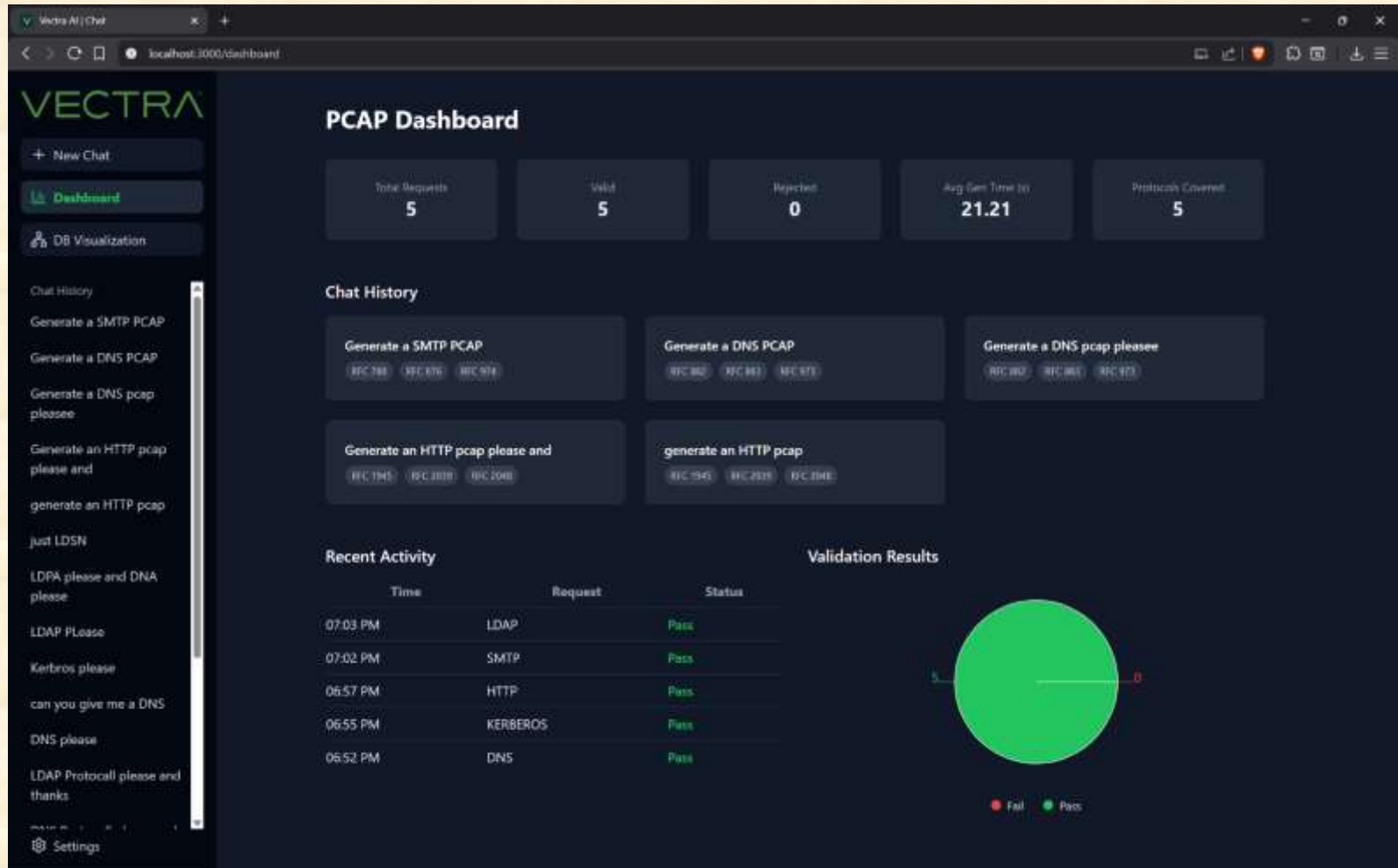
Check	Status
LDAP must use port 389 or 636 (LDAPS)	Pass
LDAP sessions must begin with a BindRequest message	Pass
LDAP requests use non-zero IDs; responses reuse the same ID	Pass
SearchRequest messages must include baseObject and scope fields	Pass
ModifyRequest messages must contain at least one change operation	Pass

LDAP

Type a request (e.g. "Generate a Kerberos AS-REQ/AS-REP capture")



Dashboard



What's left to do?

- Features
- Stretch Goals
- Other Tasks
 - Improve metadata
 - Test with new protocols



Questions?

?

?

?

?

?

?

?

?

?

