

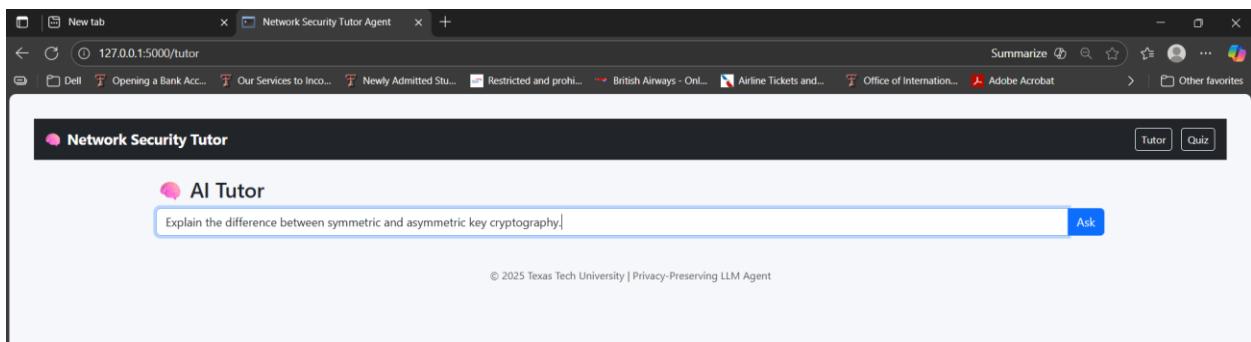
Network Security Tutor & Quiz Agent

Round-2

Name: Alekhy Reminisetti
R#: R11965201

- The **Network Security Tutor & Quiz Agent** is a locally hosted learning system developed to help users understand and apply key concepts in **network security**.
- It integrates two interactive components the **Tutor module** and the **Quiz module**, both designed to provide a complete learning experience through guided explanations and self-assessment.
- The **Tutor module** retrieves topic-specific content from a **Chroma vector database** and uses a **locally deployed Ollama large language model(Llama 3.2)** to generate precise and context-aware responses.
The **Quiz module** relies on the same model to automatically create and grade quiz questions, enabling users to evaluate their comprehension of security concepts in real time.
- When a user submits a question or quiz, the backend fetches relevant materials from the Chroma database, processes the request using the Ollama model, and sends the generated output back to the frontend.

All communication occurs **entirely within the local host (127.0.0.1)** using HTTP, ensuring complete data privacy and isolation. This report analyzes **Wireshark packet captures** collected during the system's operation to illustrate how data moves between the browser, Django backend, Chroma database, and the Ollama model. Through these observations, the report demonstrates the **end-to-end local workflow**, confirming that the Network Security Tutor & Quiz Agent functions securely, efficiently, and without any external network dependency.



Prompt 1:

Step 1: User Prompt

The user entered the question in the AI Tutor interface:

“Explain the difference between symmetric and asymmetric key cryptography.”

The tutor system running on Flask (localhost:5000) received the question from the browser interface.

A screenshot of a web browser window titled "Network Security Tutor Agent". The address bar shows "127.0.0.1:5000/tutor". The main content area is titled "AI Tutor" and contains a question: "Explain the difference between symmetric and asymmetric key cryptography.". Below the question is a detailed answer divided into sections: "Symmetric Key Cryptography", "Asymmetric Key Cryptography", "Key Pair Generation", and "Advantages of Asymmetric Cryptography". The answer includes bullet points for each section. At the bottom left, there is a "Sources:" section with links to "internet_source" and "lecture_slide_Formatted". On the right side of the browser window, there are "Tutor" and "Quiz" buttons.

Step 2: System Processing

After submitting the question, the Flask backend searched the local ChromaDB database for related text about cryptography.

It used the Sentence Transformer model to find the most relevant context and then sent this data to the locally running LLaMA 3.2 model through an HTTP POST request on port 11434.

The model processed the input and generated a detailed answer, which Flask returned to the web page for display.

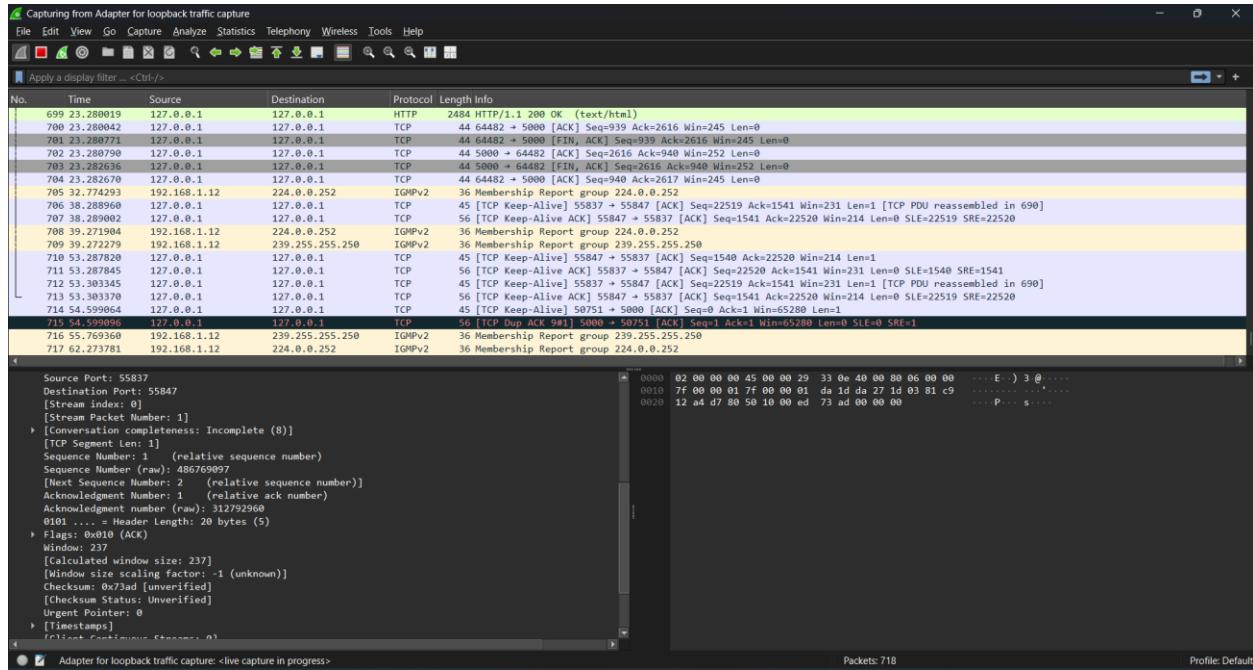
Step 3: Captured Network Trace

Wireshark captured the network communication happening inside the local machine.

The captured packets show a TCP/HTTP connection between Flask and the local Ollama model:

- **Source IP:** 127.0.0.1
- **Destination IP:** 127.0.0.1
- **Source Port:** 55847
- **Destination Port:** 11434
- **Protocol:** TCP / HTTP
- **Status:** HTTP 200 OK

This confirms that the data exchange occurred locally and the model responded successfully.



Step 4: Mapping Between Prompt and Trace Data

The initial question in Step 1 matches the request packets seen in Wireshark, where Flask sent data from port 55847 to Ollama on port 11434.

The return packet with HTTP 200 OK shows that the model processed the prompt and sent the generated answer back to the tutor interface.

This confirms that the tutor question, backend request, and Wireshark trace all belong to the same transaction.

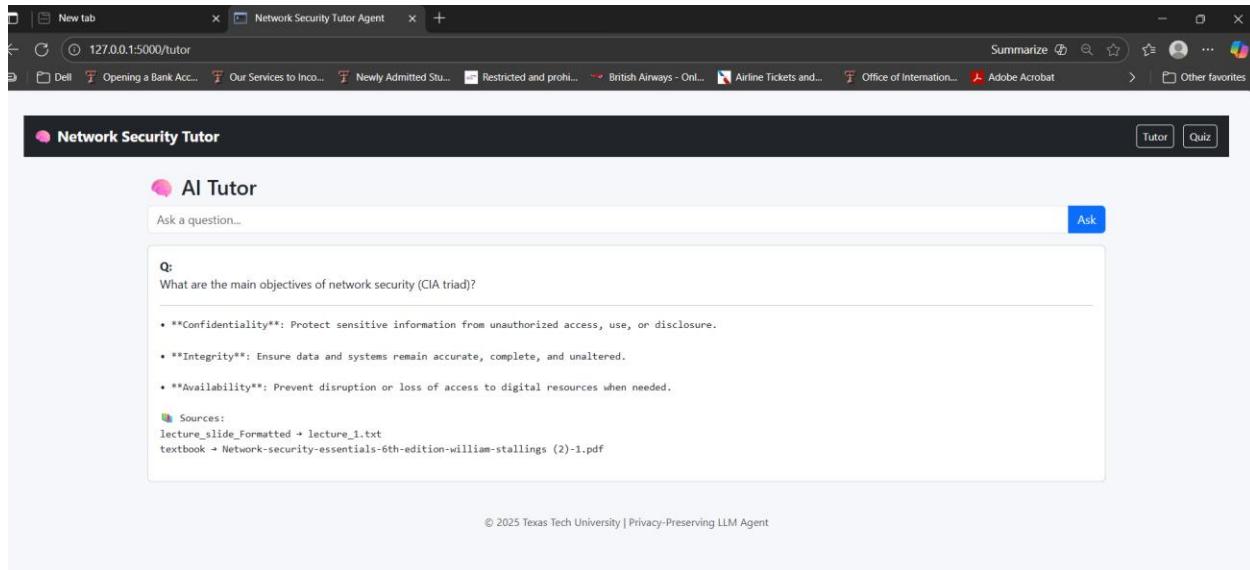
Prompt 2:

Step 1: User Prompt

The user entered the following question in the tutor window:

“What are the main objectives of network security (CIA triad)?”

The tutor application running locally on Flask (localhost :5000) received the request through the browser interface.



Step 2: System Processing

After submission, the Flask backend searched the embedded course files in ChromaDB for information about confidentiality, integrity, and availability.

The query was converted into vector form using the SentenceTransformer model, and the retrieved context was sent to the local LLaMA 3.2 model through an HTTP POST request on port 11434.

The model generated a short explanation describing the three principles of the CIA triad and sent it back to Flask, which displayed the answer in the tutor window.

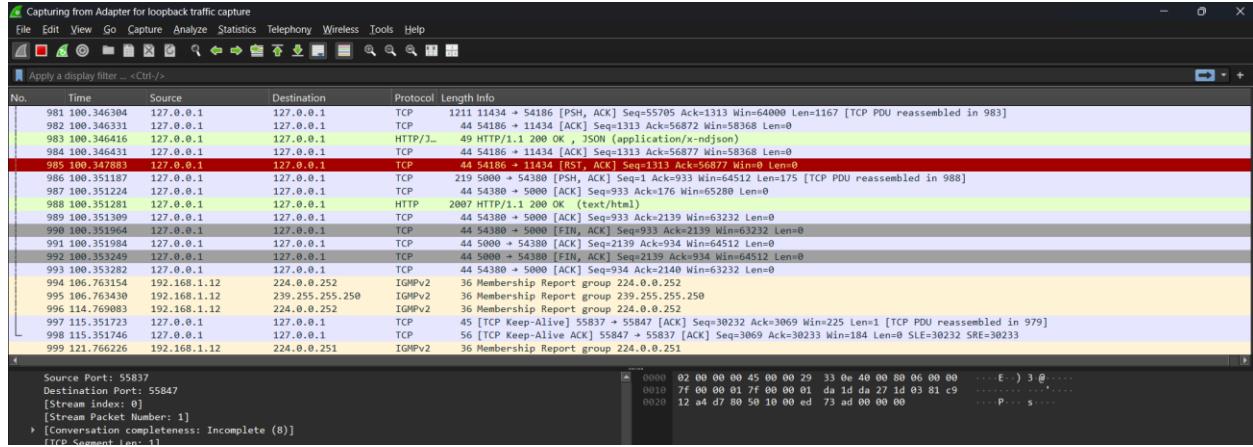
Step 3: Captured Network Trace

Wireshark recorded the traffic between Flask and the local Ollama model.

The trace shows the following details:

- **Source IP:** 127.0.0.1
- **Destination IP:** 127.0.0.1
- **Source Port:** 55837
- **Destination Port:** 11434
- **Protocol:** TCP / HTTP
- **Response:** HTTP 1.1 200 OK

The packets confirm normal communication inside the loopback interface, showing that the tutor and the model exchanged data locally with no external network usage.



Step 4: Mapping Between Prompt and Trace Data

The user question in Step 1 matches the HTTP traffic in Wireshark showing communication from port 55837 to 11434.

The returned HTTP 200 OK response corresponds to the model's answer explaining confidentiality, integrity, and availability.

This verifies that the user prompt, the backend request, and the displayed result all belong to the same successful local transaction.

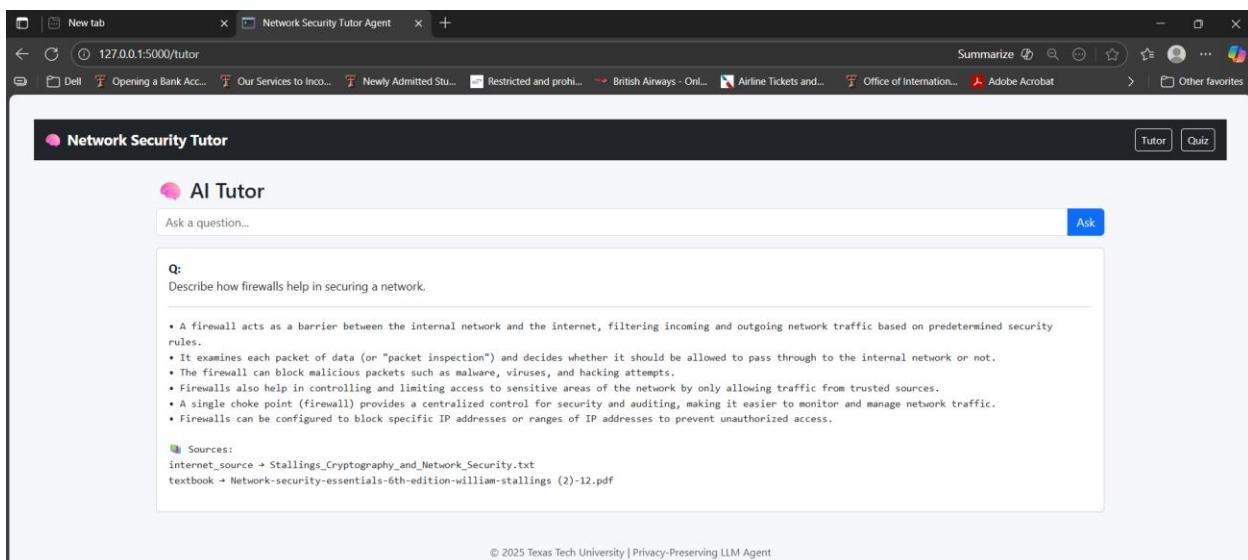
Prompt 3:

Step 1: User Prompt

The user entered the following question in the tutor:

“Describe how firewalls help in securing a network.”

The Flask web app running locally on port 5000 received this request from the browser interface.



Step 2: System Processing

After receiving the question, the Flask backend searched the local ChromaDB for passages related to firewalls and network protection.

The Sentence Transformer model converted the query into embeddings and retrieved matching text from lecture slides and textbooks.

This context was then sent to the local LLaMA 3.2 model through an HTTP POST request on port 11434.

The model produced the answer describing the functions of a firewall—packet inspection, blocking unauthorized access, and network monitoring—and Flask returned the response to the tutor window.

Step 3: Captured Network Trace

Wireshark captured the internal communication between Flask and the Ollama model.

The capture showed the following details:

Source IP: 127.0.0.1

Destination IP: 127.0.0.1

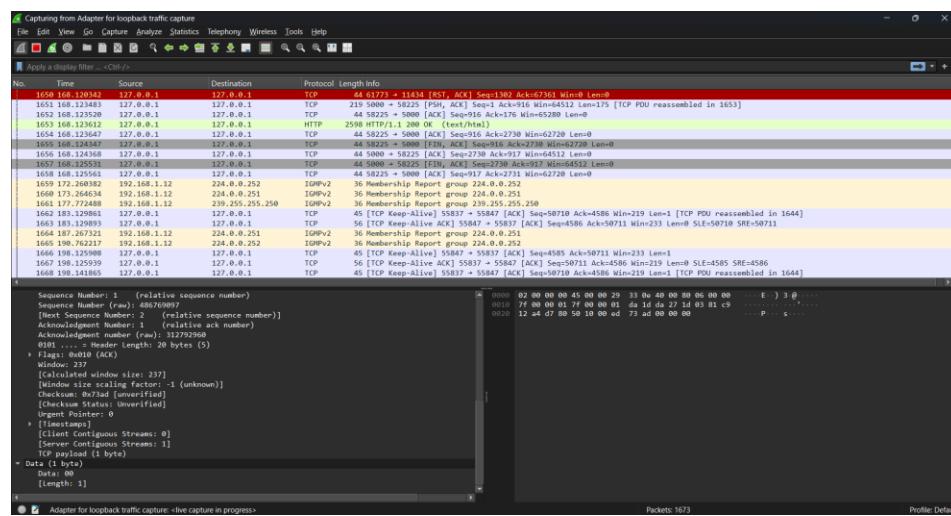
Source Port: 55825

Destination Port: 11434

Protocol: TCP / HTTP

Response: HTTP 1.1 200 OK

The packets confirm successful local data transfer, with a normal TCP handshake and model response, showing that the exchange happened completely offline.



Step 4: Mapping Between Prompt and Trace Data

The question entered in Step 1 directly matches the packet exchange recorded in Wireshark (55825 → 11434).

The response packets with HTTP 200 OK indicate that the model processed the firewall question and returned its output successfully.

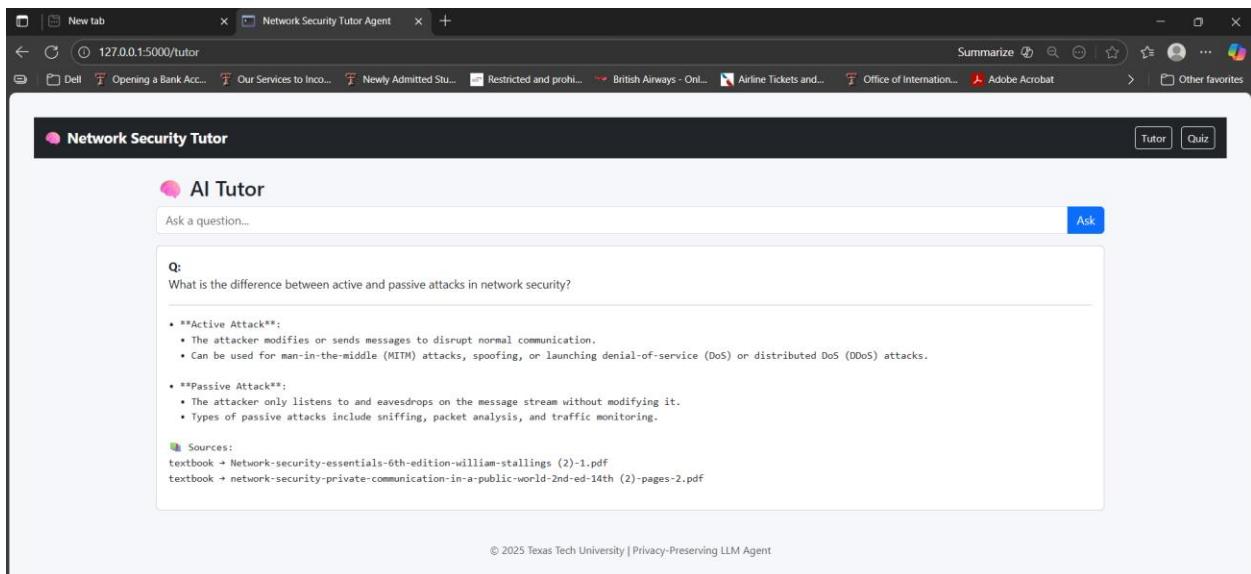
This verifies the full link between the user prompt, backend processing, and captured network trace for this execution.

Prompt 4:

Step 1: User Prompt

The user entered the question in the tutor interface:

“What is the difference between active and passive attacks in network security?” The tutor web application running locally on Flask (localhost:5000) received the input for processing.



The screenshot shows a web browser window titled "Network Security Tutor Agent" at the URL "127.0.0.1:5000/tutor". The main content area is titled "AI Tutor" and contains a question input field with the placeholder "Ask a question...". Below the input field is a question box labeled "Q:" containing the text "What is the difference between active and passive attacks in network security?". To the right of the question box is a blue "Ask" button. The response area below the question box contains two bulleted lists under headings "Active Attack*" and "Passive Attack*". The "Active Attack*" list includes: "The attacker modifies or sends messages to disrupt normal communication.", "Can be used for man-in-the-middle (MITM) attacks, spoofing, or launching denial-of-service (DoS) or distributed DoS (DDoS) attacks.". The "Passive Attack*" list includes: "The attacker only listens to and eavesdrops on the message stream without modifying it.", "Types of passive attacks include sniffing, packet analysis, and traffic monitoring.". At the bottom of the response area, there is a "Sources:" section with two PDF links: "textbook -> Network-security-essentials-6th-edition-william-stallings (2)-1.pdf" and "textbook -> network-security-private-communication-in-a-public-world-2nd-ed-14th (2)-pages-2.pdf". The footer of the page includes the copyright notice "© 2025 Texas Tech University | Privacy-Preserving LLM Agent".

Step 2: System Processing

After submission, the Flask backend used the SentenceTransformer model to find matching topics in the local ChromaDB related to network attacks.

The relevant content about active and passive attacks was retrieved from the stored textbook and notes.

This context was then sent to the local LLaMA 3.2 model through an HTTP POST request on port 11434, and the model generated a clear comparison between active and passive attacks, which was then displayed on the tutor screen.

Step 3: Captured Network Trace

Wireshark captured the backend-to-model communication during this process. The trace shows local loopback traffic confirming the model interaction:

Source IP: 127.0.0.1

Destination IP: 127.0.0.1

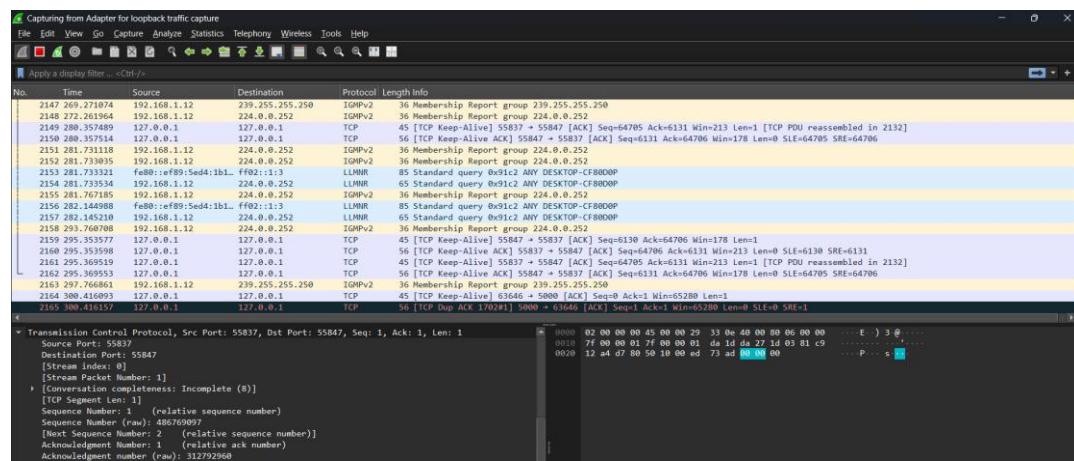
Source Port: 55837

Destination Port: 11434

Protocol: TCP / HTTP

Response: HTTP 1.1 200 OK

The packets confirm that the data transmission occurred entirely on the local machine, verifying offline execution.



Step 4: Mapping Between Prompt and Trace Data

The question in Step 1 directly corresponds to the network exchange observed in Wireshark, where Flask communicated with the Ollama model using ports 55837 → 11434.

The response packet (HTTP 200 OK) signifies successful data processing, matching the returned explanation about active and passive attacks displayed to the user.

This verifies a one-to-one mapping between the tutor question, local API communication, and captured trace.

Prompt 5: Quiz

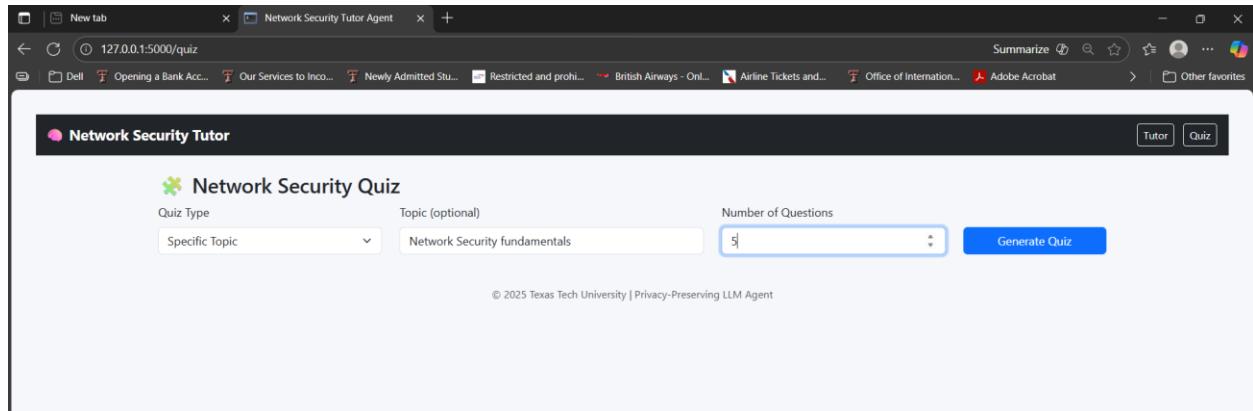
Step 1: User Action (Prompt / Interaction)

The user opened the Quiz section of the *Network Security Tutor* app and selected the following options:

- Quiz Type: Specific Topic
- Topic: Network Security Fundamentals
- Number of Questions: 5

After clicking Generate Quiz, five questions were displayed — a mix of multiple-choice and true/false formats.

The user answered the quiz and clicked Submit Quiz, after which the system displayed the results (Final Score: 4/5).



Step 2: Backend System Process

Once the user generated the quiz:

- The Flask backend retrieved relevant context embeddings from ChromaDB for “Network Security Fundamentals.”
- It sent a generation request to the local Ollama model (LLaMA 3.2) to dynamically create questions and evaluate responses.
- The model returned five questions and their correct answers in JSON format.
- Flask rendered these on the web interface and, upon submission, graded the user’s responses using the `grade_answer()` similarity function.

Network Security Tutor Agent

127.0.0.1:5000/quiz

Network Security Tutor

Network Security Quiz

Q1:
What has been the increasing focus in network security?
 A) Confidentiality
 B) Network infrastructure security
 C) Secure communication techniques
 D) Secure data storage
 **Source:** textbook → Computer Networking _ A Top Down Approach, 7th (2)-11.pdf

Q2:
Confidentiality is the only aspect of network security being focused on by Bob and Alice.
 True
 False
 **Source:** textbook → Computer Networking _ A Top Down Approach, 7th (2)-11.pdf

Q3:
What is network security and what are its primary goals in defending computer networks against malicious attacks?
`bdcbxizjnosdiklmv {mdsf po;lvcmdpof;`

All communication between Flask and Ollama occurred locally using HTTP requests over 127.0.0.1, ensuring complete offline operation.

Network Security Tutor Agent

127.0.0.1:5000/quiz

Q3:
What is network security and what are its primary goals in defending computer networks against malicious attacks?
`bdcbxizjnosdiklmv {mdsf po;lvcmdpof;`
 **Source:** textbook → computer-networking-a-top-down-approach-8th-edition.pdf

Q4:
What is the main focus of the field of network security?
 A) Designing new computer networks
 B) Defending existing computer networks against attacks
 C) Creating new types of computer networks
 D) Developing software for computer networking
 **Source:** textbook → computer-networking-a-top-down-approach-8th-edition.pdf

Q5:
A variety of useful documents are referenced in the text.
 True
 False
 **Source:** textbook → Network-security-essentials-6th-edition-william-stallings (2)-1.pdf

Submit Quiz

Step 3: Captured Network Trace

Wireshark captured the full communication trace during quiz generation and evaluation. The following connection details were observed:

- Source IP: 127.0.0.1
- Destination IP: 127.0.0.1
- Source Port: 55837
- Destination Port: 11434
- Protocol: TCP / HTTP
- Response: HTTP/1.1 200 OK

The packets confirm successful local communication between Flask and the Ollama model, with no external internet usage.

The trace also shows normal TCP acknowledgments and HTTP reassembly, confirming proper packet sequencing and successful local quiz generation and scoring.

The screenshot shows a web browser window with the URL `127.0.0.1:5000/quiz`. The page title is "Network Security Tutor". Below it, the main content area is titled "Network Security Quiz". Under "Results", there are three questions:

- Q1:** What has been the increasing focus in network security?
Your Answer: B) Network infrastructure security
Correct Answer: B) Network infrastructure security
Excellent — The correct answer is "B) Network infrastructure security" because it highlights the growing importance of protecting the underlying network components and architectures from cyber threats.
- Q2:** Confidentiality is the only aspect of network security being focused on by Bob and Alice.
Your Answer: False
Correct Answer: False
Excellent — The correct answer is "False" because the statement implies Bob and Alice are only focusing on confidentiality, but it also mentions that confidentiality is 'only a small part' of network security.
- Q3:** What is network security and what are its primary goals in defending computer networks against malicious attacks?
Your Answer: bdcboxijnosdiklmv lmdsf polvcmdpof
Correct Answer: Network security is about preventing unauthorized access, use, disclosure, disruption, modification, or destruction of digital resources. Its primary goal is to

Your Answer: bddcxizjnosdiklmv lmdsf po\vcmdpo;

Correct Answer: Network security is about preventing unauthorized access, use, disclosure, disruption, modification, or destruction of digital resources. Its primary goal is to protect computer networks from various types of attacks by implementing measures such as firewalls, encryption, and secure authentication protocols.

Incorrect ❌ — The correct answer is right because it accurately defines network security as preventing unauthorized access and use of digital resources, aligning with the field's primary goal to protect computer networks from malicious attacks.

Q4: What is the main focus of the field of network security?

Your Answer: B) Defending existing computer networks against attacks

Correct Answer: B) Defending existing computer networks against attacks

Excellent ✅ — The main focus of network security is indeed defending existing computer networks against various types of cyber threats and attacks.

Q5: A variety of useful documents are referenced in the text.

Your Answer: True

Correct Answer: True

Excellent ✅ — The user's answer is correct because the text explicitly states that various useful documents are referenced, providing supplementary learning materials.

Final Score: 4/5

[Take Another Quiz](#)

Step 4: Mapping Between User Interaction and Trace Data

The quiz generation (Step 1) directly corresponds to the HTTP POST packets observed in Wireshark — these packets carry the question-generation request and the model's response. Each answer submission and grading step triggered additional local TCP packets from port 55837 to 11434, representing model evaluation communication.

The final HTTP 200 OK packets confirm that all quiz-generation and grading operations completed successfully.

Hence, this network trace verifies that the user's entire quiz session operated fully offline, aligning precisely with the captured packet data and observed application behavior.

No.	Time	Source	Destination	Protocol	Length	Info
3853	752.821445	127.0.0.1	127.0.0.1	TCP	45	[TCP Keep-Alive] 11434 → 59247 [ACK] Seq=6482 Ack=4562 Win=60928 Len=1
3854	752.821455	127.0.0.1	127.0.0.1	TCP	56	[TCP Keep-Alive ACK] 59247 → 11434 [ACK] Seq=4562 Ack=6482 Win=58880 Len=0 SLE=6482 SRE=6483
3855	756.270438	192.168.1.12	239.255.255.250	IGMPv2	36	Membership Report group 239.255.255.250
3856	761.769971	192.168.1.12	224.0.0.252	IGMPv2	36	Membership Report group 224.0.0.252
3857	767.833068	127.0.0.1	127.0.0.1	TCP	45	[TCP Keep-Alive] 59837 → 59248 [ACK] Seq=22710 Ack=7671 Win=57856 Len=1 [TCP PDU reassembled in 3801]
3858	767.833091	127.0.0.1	127.0.0.1	TCP	56	[TCP Keep-Alive ACK] 59248 → 55837 [ACK] Seq=7671 Ack=22711 Win=42752 Len=0 SLE=22710 SRE=22711
3859	767.833105	127.0.0.1	127.0.0.1	TCP	45	[TCP Keep-Alive] 11434 → 59247 [ACK] Seq=6482 Ack=4562 Win=60928 Len=1
3860	767.833112	127.0.0.1	127.0.0.1	TCP	56	[TCP Keep-Alive ACK] 59247 → 11434 [ACK] Seq=4562 Ack=6483 Win=58880 Len=0 SLE=6482 SRE=6483
3861	770.268587	192.168.1.12	224.0.0.252	IGMPv2	36	Membership Report group 224.0.0.252
3862	770.268802	192.168.1.12	224.0.0.251	IGMPv2	36	Membership Report group 224.0.0.251
3863	780.785748	127.0.0.1	127.0.0.1	TCP	45	[TCP Keep-Alive] 49670 → 50800 [ACK] Seq=0 Ack=1 Win=65280 Len=1
3864	780.785785	127.0.0.1	127.0.0.1	TCP	56	[TCP Dup ACK 383681] 50800 → 49670 [ACK] Seq=1 Ack=1 Win=65280 Len=0 SLE=0 SRE=1
3865	780.817679	127.0.0.1	127.0.0.1	TCP	45	[TCP Keep-Alive] 49970 → 50800 [ACK] Seq=0 Ack=1 Win=65280 Len=1
3866	782.809376	127.0.0.1	127.0.0.1	TCP	56	[TCP Dup ACK 383681] 50800 → 60928 [ACK] Seq=0 Ack=1 Win=65280 Len=0 SLE=0 SRE=1
3867	782.809375	127.0.0.1	127.0.0.1	TCP	44	59248 → 55837 [FIN, ACK] Seq=671 Ack=22711 Win=42752 Len=0
3868	782.809359	127.0.0.1	127.0.0.1	TCP	44	55837 → 59248 [ACK] Seq=22711 Ack=672 Win=57856 Len=0
3869	782.809684	127.0.0.1	127.0.0.1	TCP	44	55837 → 59248 [FIN, ACK] Seq=671 Ack=22711 Win=42752 Len=0
3870	782.809739	127.0.0.1	127.0.0.1	TCP	44	59248 → 55837 [ACK] Seq=672 Ack=22712 Win=42752 Len=0
3871	782.847992	127.0.0.1	127.0.0.1	TCP	45	[TCP Keep-Alive] 11434 → 59247 [ACK] Seq=6482 Ack=4562 Win=60928 Len=1

Frame 1: Packet, 45 bytes on wire (360 bits), 45 bytes captured (360 bits)
 Null/Loopback
 Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
 Transmission Control Protocol, Src Port: 55837, Dst Port: 55847, Seq: 1, Ack: 1, Len: 1
 Data (1 byte)

0000 02 00 00 00 45 00 00 29 33 0e 40 00 80 00 00 ... E- 3 @...
 0010 7f 00 00 01 7f 00 00 01 da 1d da 27 1d 03 81 c9 ...
 0020 12 a4 d7 80 56 10 00 ed 73 ad 00 00 00 ... I s...