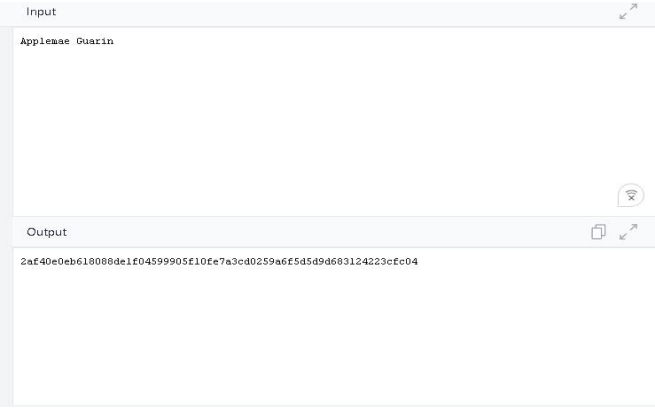
B. Integrity Test – Hash Comparison

Tool: Online SHA-256 Hashing Tool *https://emn178.github.io/online-tools/sha256.html*



Guide Questions:

- Did the hash values change? Why or why not?

- Yes, the hash values changed when the file or text was altered. Even a small change in the data (such as a single character) creates an entirely different hash value. If the data is the same, the hash value is the same.

- How does hashing help protect **integrity**?

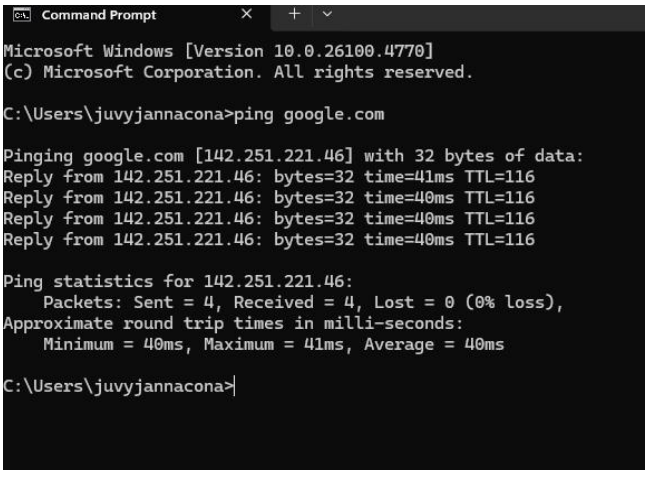
- Hashing helps protect integrity by generating a unique digital fingerprint for data. Provided that the hash value remains unchanged, users can confidently ascertain that the data has not been tampered with. Any change in hash means that the data has been altered or corrupted.

- How can hashing detect unauthorized modifications?

- Hashing detects unauthorized changes by checking the present hash value of data with the original hash. If they are not the same, it indicates that an unauthorized individual has altered the data.

📡 C. Availability Test – Network Ping

Tool: Command Prompt (Windows) or Terminal (Mac/Linux)



Guide Questions:

- What does the ping result indicate about network **availability**?

- The ping result indicates whether a computer or server is reachable over the network. If there are replies with response times, it means the network is available. If the requests time out or fail, the network is unavailable or experiencing issues.

- How could a **DDoS attack** affect this result?

- A DDoS attack might overwhelm the network or server with an abnormal amount of traffic, delaying it or even making it impossible for it to reply to pings. Consequently, the ping test would fail or report extremely high response times.

- Why is availability important in information systems?

- Availability is necessary since users and organizations require constant access to data and services. Unavailability of systems can halt operations, bring financial loss, and decrease trust in the system.