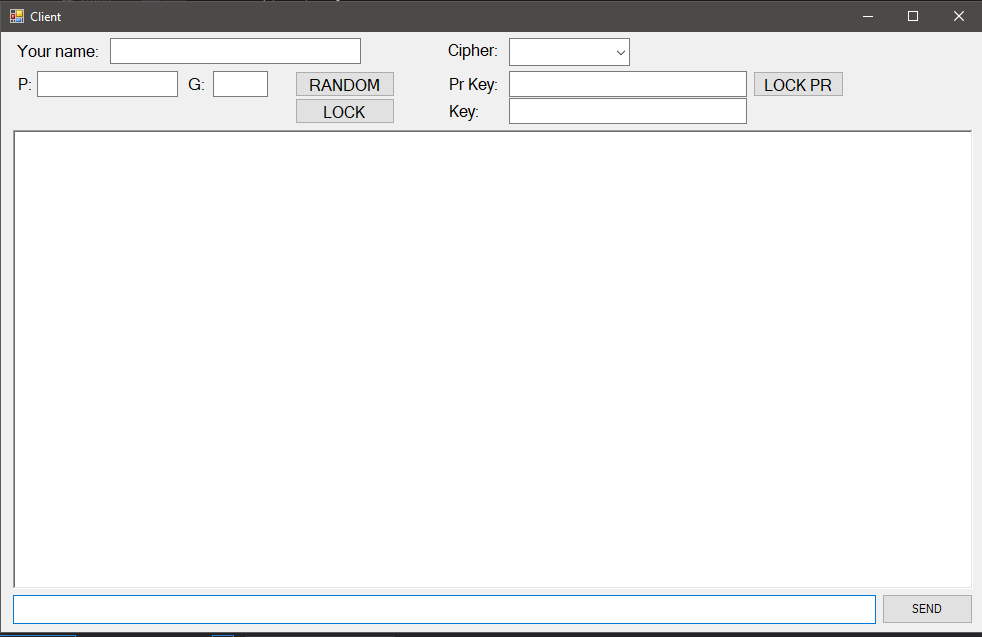
**Task 4.1:**

**ỨNG DỤNG SECURE CHAT:**

**Hướng dẫn sử dụng:**

* Ban đầu bật server lên để các client có thể giao tiếp với nhau.
* Có thể dùng Diffie – Hellman để tăng cường tính bảo mật khi giao tiếp, hoặc có thể không dùng cũng được.
* **Sử dụng Diffie – Hellman:**
  + Nhập số nguyên tố P, nhấn LOCK, sẽ tự tính ra G, hoặc là ấn random rồi LOCK.
  + Giá trị P và G sẽ được chuyển đến các client khác.
  + Mỗi client nhập giá trị Private Key của mình ở ô Pr Key, sau đó ấn LOCK.
  + Khi mỗi client đã nhập xong giá trị Private Key của mình, giá trị Key sẽ được tính toán và hiện ở ô Key.
  + Nhập tin nhắn gửi đi như bình thường.

**Giao diện người dùng:**



**TH1:** Khi chúng ta **chưa** **sử dụng** Diffie-Hellman cho giao tiếp:

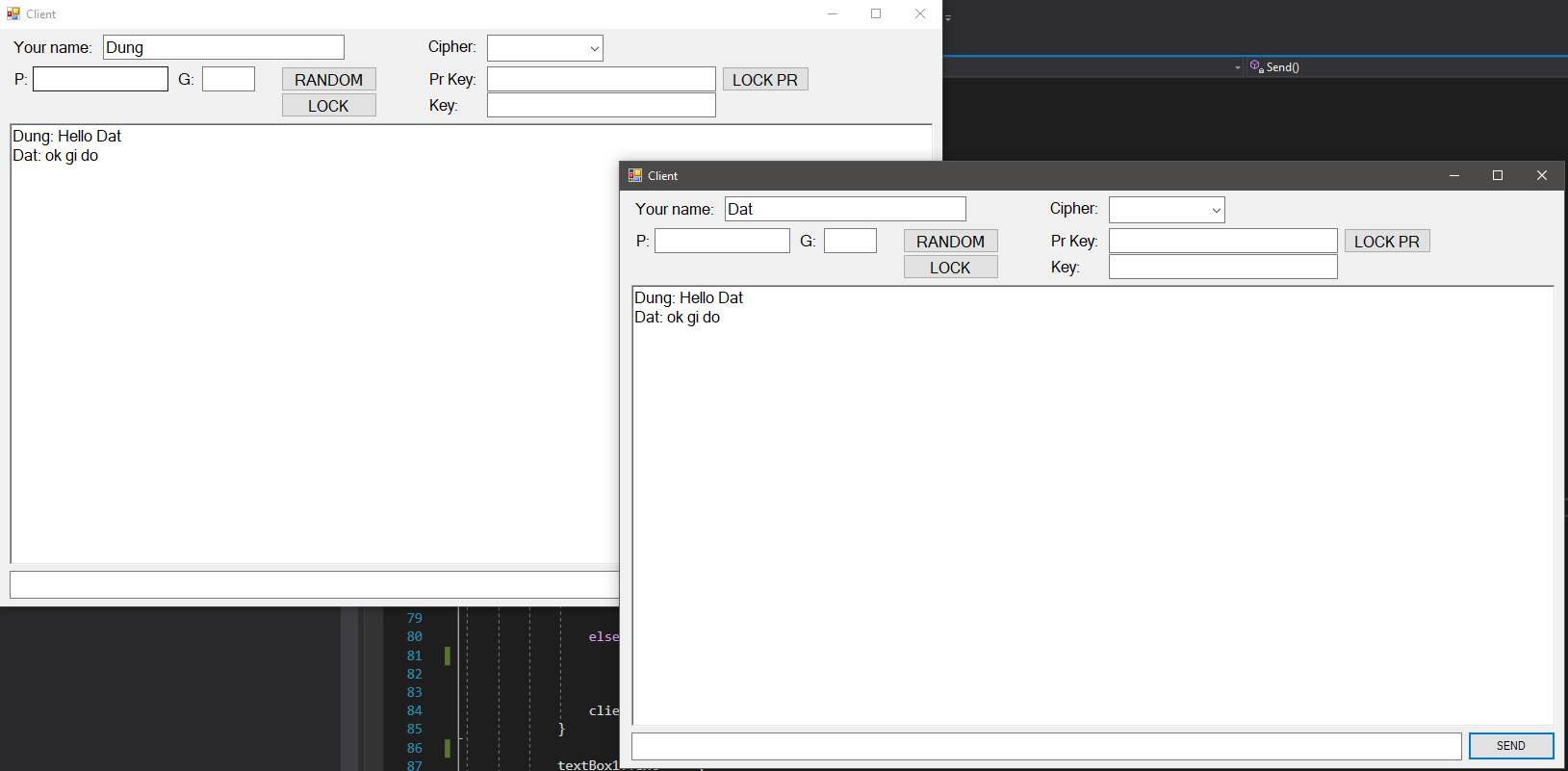


Figure : Dũng và Đạt đang nhắn tin cho nhau chưa sử dụng Diffie-Hellman.

Dễ dàng dùng **Wireshark** bắt được từng tin nhắn:

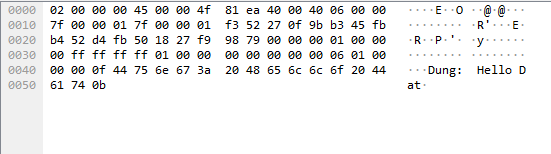


Figure : Tin nhắn Dũng gửi bị bắt được.

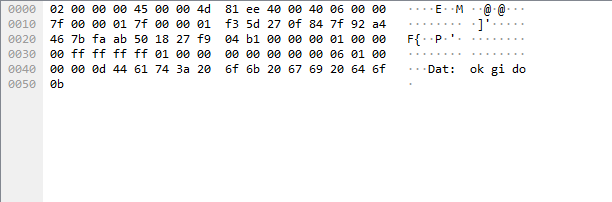


Figure : Tin nhắn Đạt gửi bị bắt được.

**TH2:** Khi chúng ta **sử dụng** Diffie-Hellman cho giao tiếp:

* Ở ví dụ đây chọn thuật toán mã hóa 3DES:

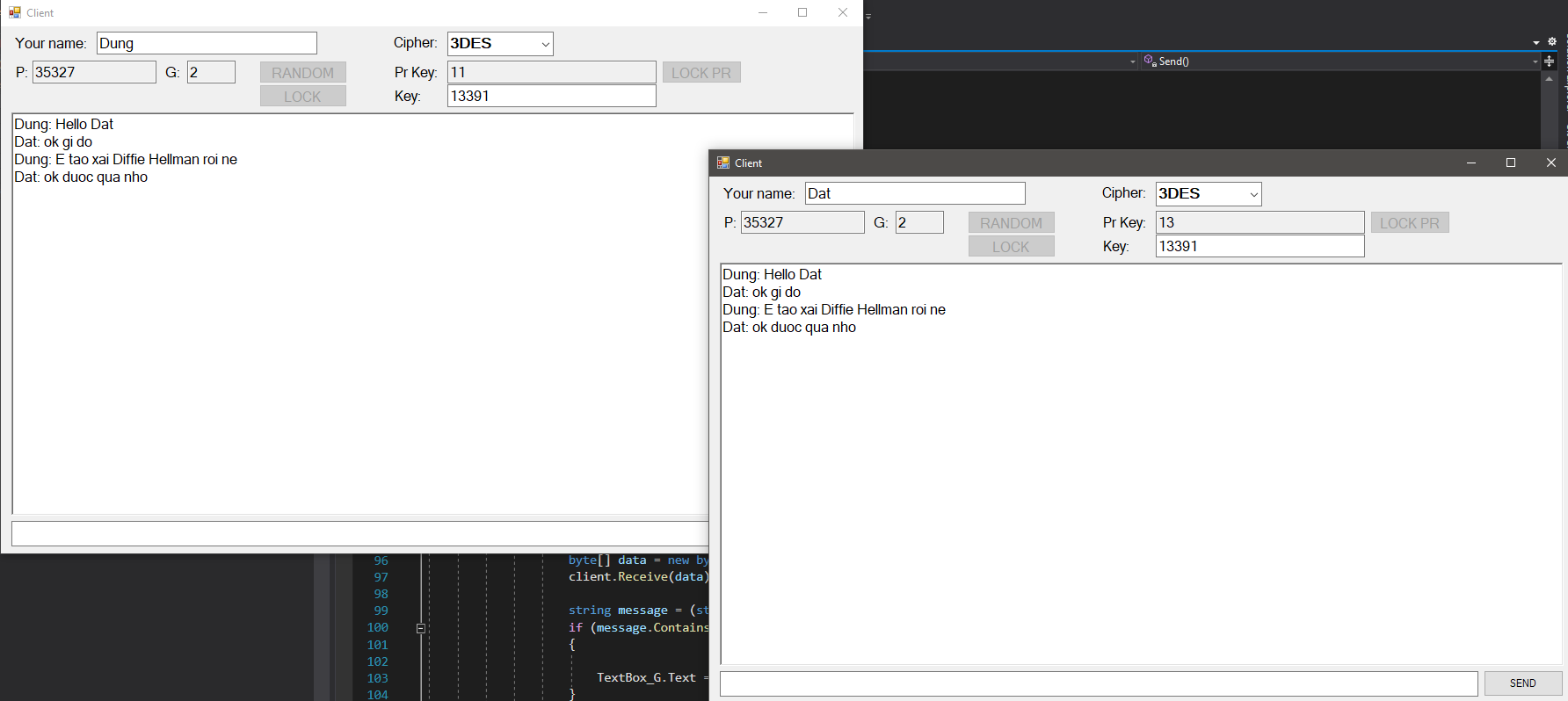


Figure : Đã sử dụng Diffie-Hellman và tin nhắn gửi đi vẫn bình thường.

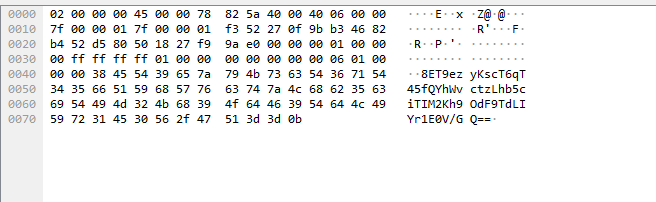


Figure : Wireshark bắt tin nhắn của Dũng, nhưng bị mã hóa nên không biết là đang nhắn gì.

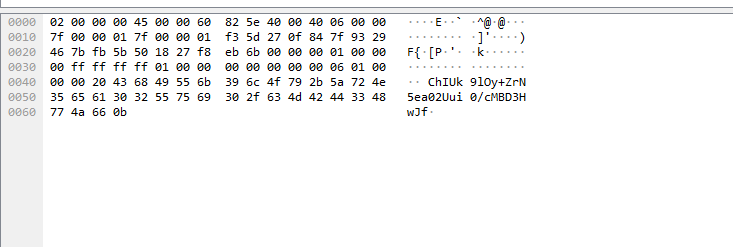


Figure : Wireshark bắt tin nhắn của Đạt, nhưng bị mã hóa.

* Ví dụ thuật toán mã hóa Ceasar.

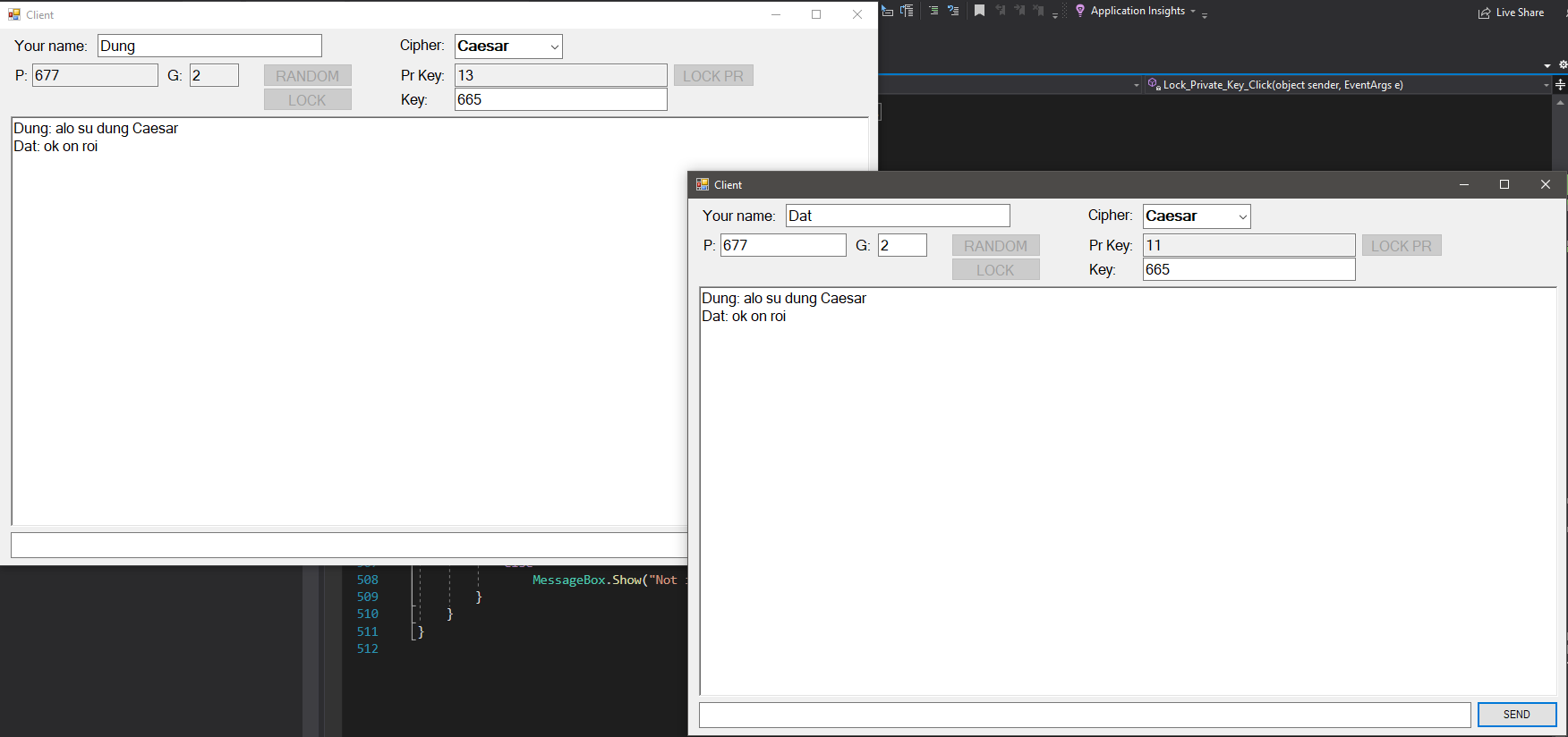


Figure : Gửi và nhận tin nhắn bình thường.

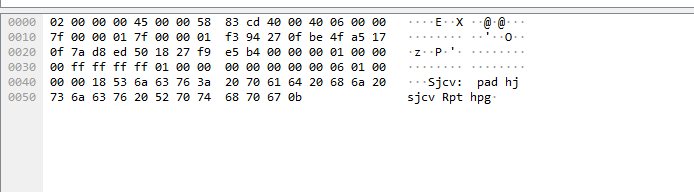


Figure : Tin nhắn cũng Dũng bị mã hóa khi gửi cho Đạt.

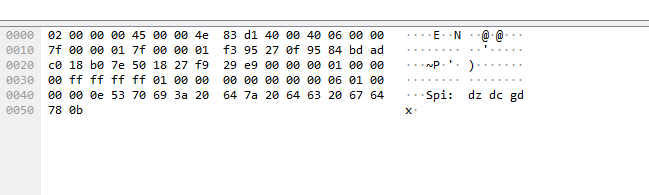


Figure : Tin nhắn của Đạt bị mã hóa khi gửi lại cho Dũng.

* Sử dụng thuật toán mã hóa AES-EBC.

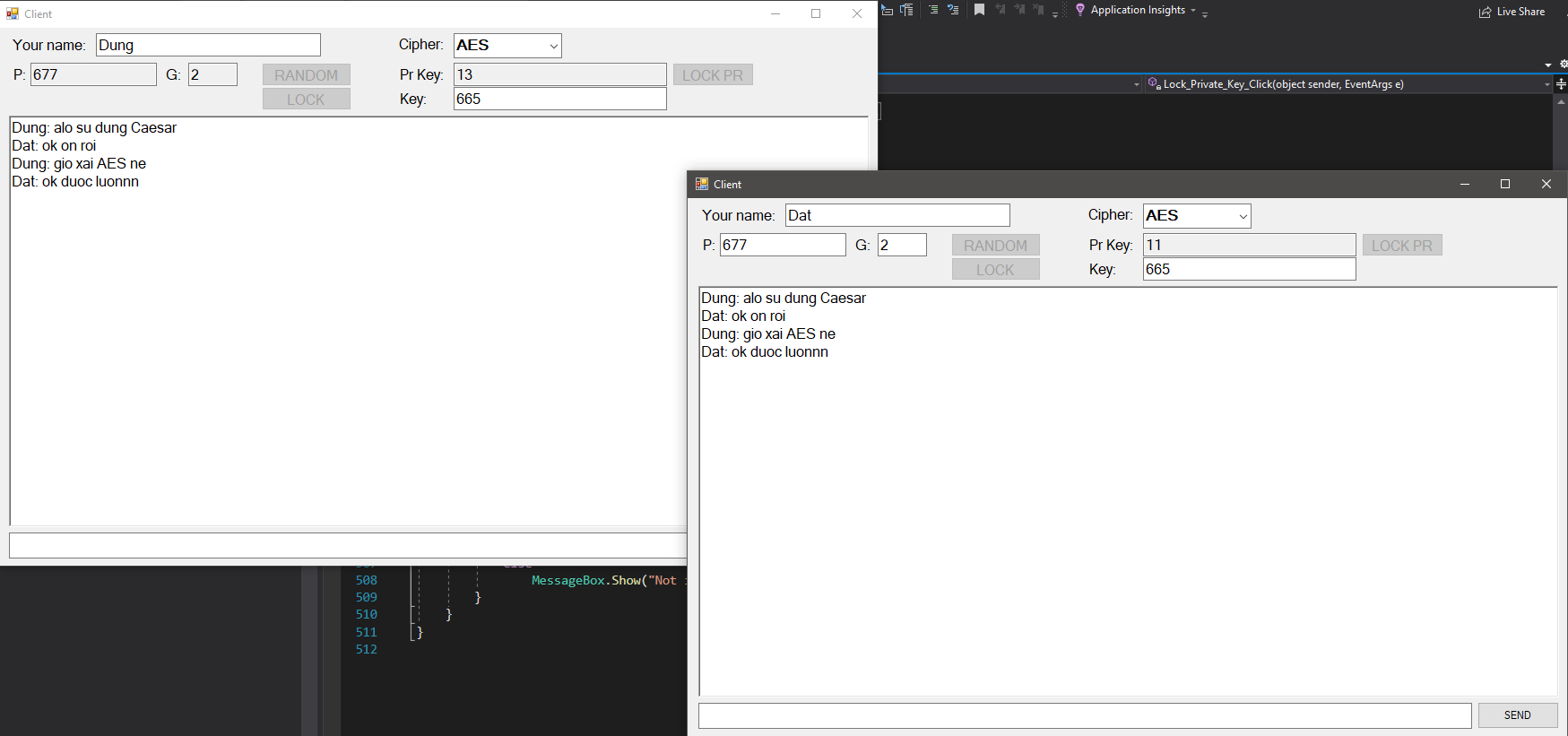


Figure : Tin nhắn vẫn gửi và nhận bình thường.

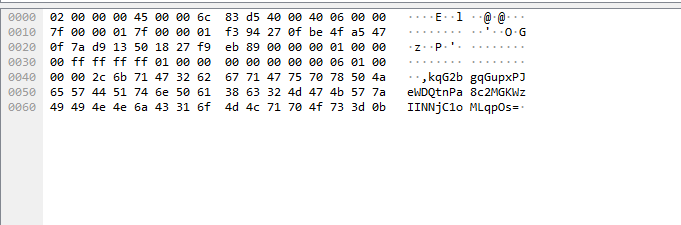


Figure : Tin nhắn của Dũng gửi đi đã được mã hóa.

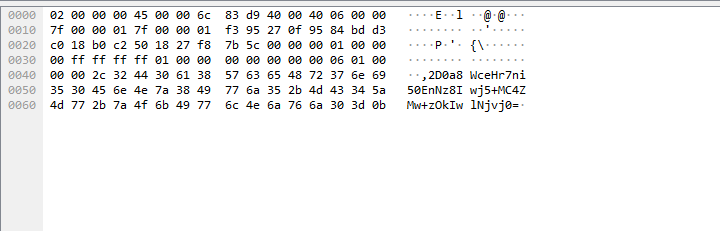


Figure : Tin nhắn của Đạt gửi lại cho Dũng cũng được mã hóa.