Chạy thử, thấy chỉ có duy nhất 1 button và 1 edit box



May mắn hàm button1\_Click không bị obfuscate



Khi bấm button, chương trình sẽ lấy text ở edit box, hash bằng hàm CreateHash() và sau đó encode với key among-us rồi so sánh với hex array "40-72-b1-25-9e-ff-83-f3-07-c4-e8-d6-8a-a6-0c-e0-ef-9f-a6-3f-e2-fc-0b-81-2a-47-dd-8b-1a-a3-4c-32" để kiểm tra.

Hàm Encode() vẫn là RC4 :)

Như vậy, ta cần decode RC4 payload và tìm hash trong database để có được key.

Trace theo hàm hash biết được thuật toán hash là MD5



Let's do it :)







-> ".NET"



Flag: traningctf{.NET\_is\_imposter!}