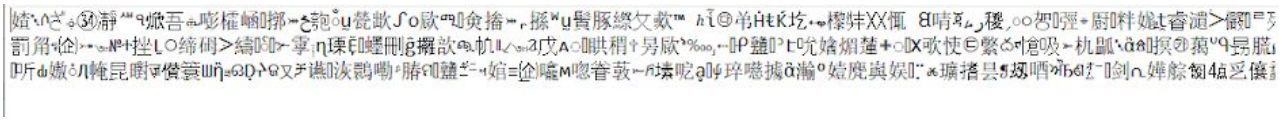
Rans0m - Reversing 100

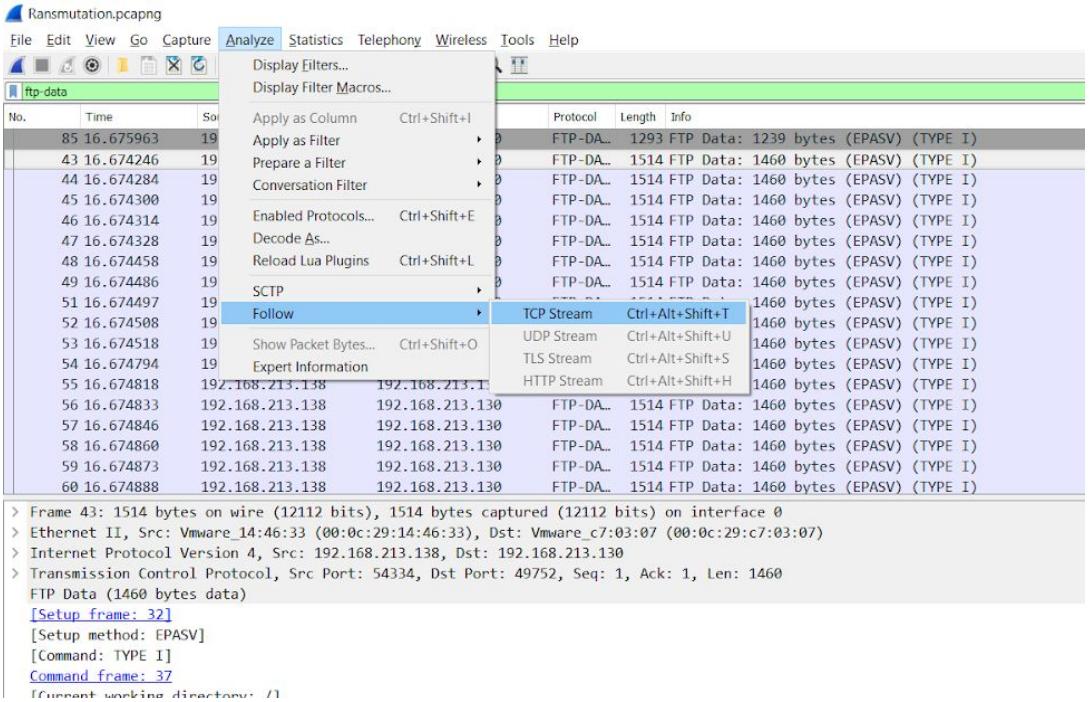
Descripción:

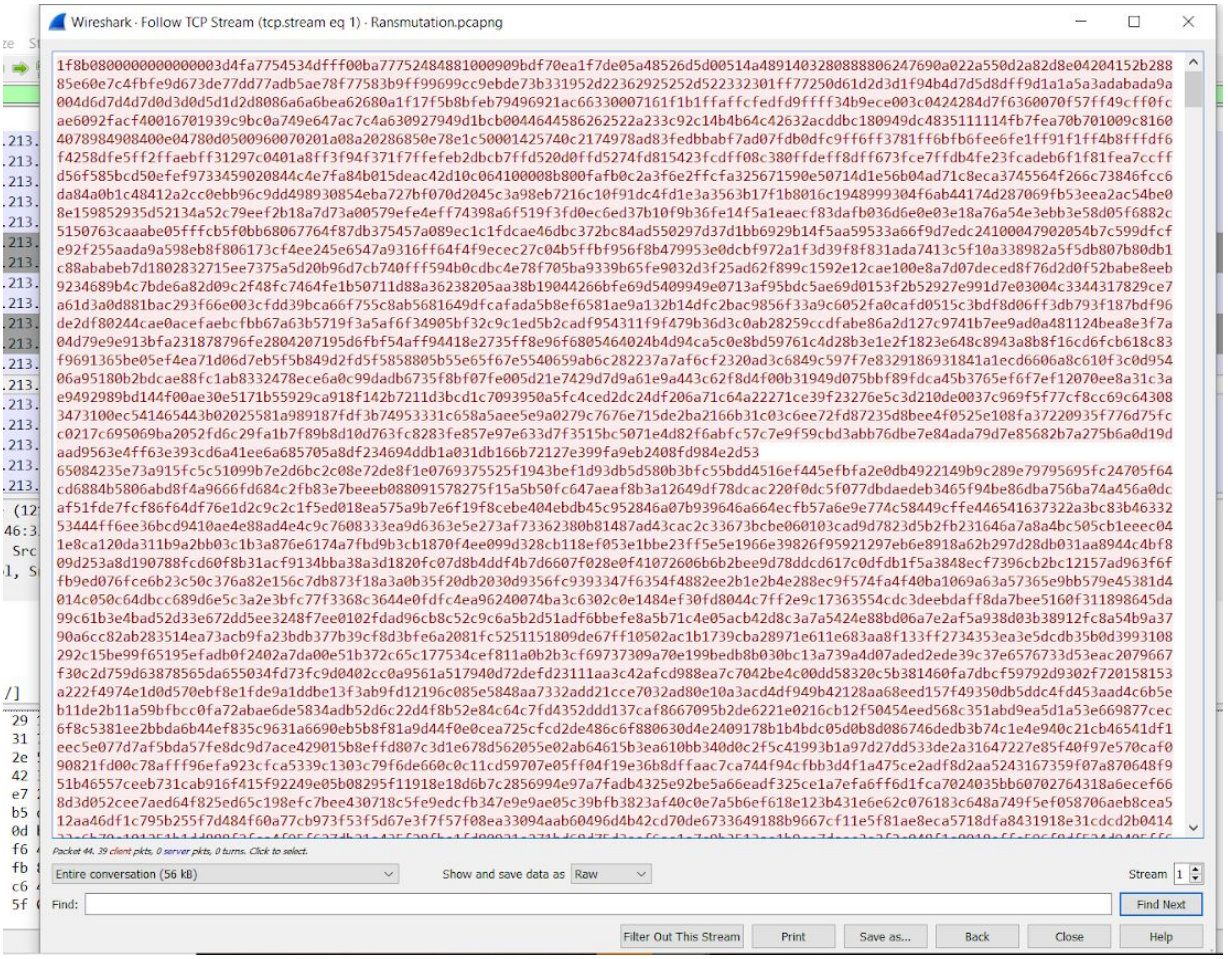
Un virus de tipo ransomware encriptó los archivos de nuestra Empresa, por suerte obtuvimos el tráfico de red que creemos capturó dicho malware con el nombre svchost.exe.tar.gz
Ayúdanos a desencriptar el archivo "Important_Message.txt.ransm" para obtener la flag!

Important_Message.txt:



El primer paso es utilizar wireshark para analizar los paquetes y seguir la transferencia de paquetes para ver el tipo de comportamiento y si este cuenta con alguna particularidad que pueda ser útil:





Obteniendo los datos crudos, guardándose como un archivo con extensión tar.gz y descomprimiendo el archivo, obtuvimos svchost.exe que al correrlo en el directorio generaba que los archivos obtuvieran una extensión .ransm.

Aplicándolo a important_message.txt y obteniendo el resultado, descubrimos que se trataba de un archivo con formato en base64, el cual es el siguiente:

Y descubrimos que contaba con una peculiaridad, la cual era que se trataba de una imagen, por lo que al pasarla de texto a imagen obtuvimos la siguiente imagen que contiene la flag:

hackdef{R4nsom_L1f3_F0r3v3r_D13_B4ckup5!}