## Desafío

I Cant Manipulate People

Partial traffic packet captured from hacked machine, can you analyze the provided pcap file to extract the message from the packet perhaps by reading the packet data?

ARCHIVO.pcap

## Resolución

Abrimos el archivo PCAP con Wireshark para inspeccionar el tráfico. Observé que cada paquete contenía un solo byte de información en hexadecimal. Este dato estaba en la capa de carga útil (payload) de los paquetes.

Para automatizar el proceso de extracción, escribimos un script en Python utilizando la librería scapy. Este script recorre todos los paquetes en el archivo PCAP, extrae los bytes del payload, y los concatena en una sola cadena hexadecimal.

La cadena hexadecimal concatenada fue:

*57474d597b31653362373164353765343636616237316234336332363431613462333466347d*

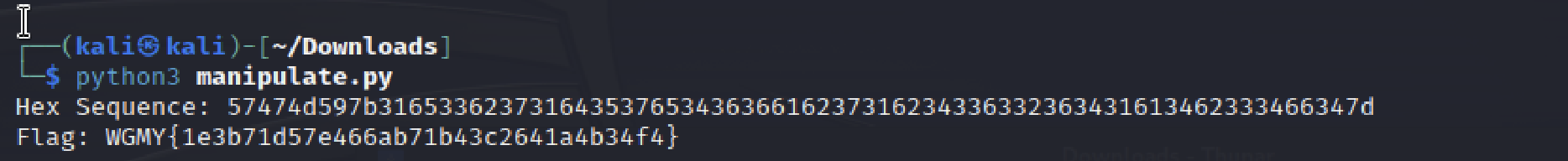
Utilizando el método *bytes.fromhex()* en Python, la cadena se decodificó a texto:

*WGMY{1e3b71d57e466ab71b43c2641a4b34f4}*

Se deberá ejecutar el siguiente comando:

*python3 manipulate.py*

Mostrará en el output la secuencia completa en hexadecimal y además la flag.



## Flag

*WGMY{1e3b71d57e466ab71b43c2641a4b34f4}*

