INTERCEPTED TRANSMISSION

INTRODUCTION

INTERCEPTED TRANSMISSION IS ONE OF OUR FORENSICS CHALLENGES.

FORENSICS ENCAPSULATES MANY DIFFERENT POINTS OF CYBER SECURITY.

FROM EMBEDDING MESSAGES IN NETWORK INTERACTIONS TO ALTERING THE DATA IN FILE HEADERS. FORENSICS IS A KEY COMPONENT IN CYBER SECURITY.

FORENSICS OFTEN INVOLVES HIDING INFORMATION WITHIN FILES, MEMORY CAPTURES, AND NETWORK TRAFFIC.

TIPS

HELPFUL TOOLS FOR FORENSICS INCLUDE

STEGHIDE - EXTRACT EMBEDDED INFORMATION IN ANOTHER FILE

STEGSOLVE - JAVA BASED GUI TO EXTRACT EMBEDDED INFORMATION

EXIFTOOL - EXTRACT INFORMATION IN A FILE'S METADATA

HINTS

- I. TRY USING SOME OF THE TOOLS LISTED AROVE
- 2. PEOPLE OFTEN HIDE SECRET AUDIO IN MESSAGES, DO YOU
 THINK IT'S EMBEDDED THERE?
- 3. AFTER USING STECHIDE, TRY FINDING THE MEANING BEHIND
 THE NEW AUDIO