**Документация по решению задач CTF**

*(Stego, Crypto, Forensic)*

**1. Стего (Steganography)**

**Цель:** Найти скрытые данные в файлах (изображениях, аудио, видео, тексте).

**Основные методы решения:**

**А) Изображения (**PNG**,**JPG**,**BMP**)**

* **Инструменты:**
  + binwalk, steghide, stegsolve, zsteg, exiftool.
* **Техники:**
  1. **Метаданные:**

bash

Copy

Download

exiftool image.jpg

Ищите комментарии, странные поля или base64.

* 1. **LSB (Least Significant Bit):**
     + Откройте в **StegSolve** → Analyze → Red/Green/Blue plane 0.
     + Ищите скрытый текст или QR-код.
  2. **Скрытые файлы:**

bash

Copy

Download

binwalk -e image.jpg # Извлечение вложенных файлов

* 1. **Цветовые каналы:**
     + Используйте stegsolve для просмотра отдельных каналов.

**Б) Аудио (**WAV**,**MP3**)**

* **Инструменты:**
  + audacity, sonic-visualizer, deepsound.
* **Техники:**
  1. **Спектрограмма:**
     + Откройте в Audacity → View → Spectrogram.
     + Ищите флаг в виде текста или Morse-кода.
  2. **Модификация амплитуды:**
     + Проверьте на наличие скрытых данных в тихих участках.

**В) Текст / Документы (**PDF**,**DOCX**,**TXT**)**

* **Инструменты:**
  + strings, pdftotext, olevba (для макросов).
* **Техники:**
  1. **Скрытый текст:**

bash

Copy

Download

strings file.pdf | grep "flag{"

* 1. **White text on white background** (в PDF или DOCX).

**2. Крипто (Crypto)**

**Цель:** Взломать шифрование или декодировать данные.

**Основные типы задач:**

**А) Кодировки**

* **Base64:**

bash

Copy

Download

echo "U0dWc2JHOGdWMjl5YkdRA==" | base64 -d

* **Hex:**

bash

Copy

Download

echo "666c61677b6865785f666c61677d" | xxd -r -p

* **ROT13 / Caesar:**  
  Используйте [CyberChef](https://gchq.github.io/CyberChef/" \t "_blank).

**Б) Классические шифры**

* **XOR:**

python

Copy

Download

data = bytes.fromhex("1f0a3e")

key = 0x41

print(bytes([b ^ key for b in data]))

* **Vigenère:**  
  Используйте [Decoder](https://www.dcode.fr/vigenere-cipher" \t "_blank).

**В) Современная криптография**

* **RSA (малые числа):**  
  Разложите n на множители через [FactorDB](http://factordb.com/" \t "_blank).
* **AES (известный ключ):**

python

Copy

Download

from Crypto.Cipher import AES

cipher = AES.new(key, AES.MODE\_ECB)

print(cipher.decrypt(encrypted\_data))

**3. Форензика (Forensic)**

**Цель:** Анализ файлов, дампов памяти, сетевого трафика.

**Основные методы:**

**А) Анализ файлов**

* **HEX-анализ:**

bash

Copy

Download

xxd file.bin | head -n 20

* **Скрытые разделы:**

bash

Copy

Download

binwalk -e suspicious.img

**Б) Дампы памяти (**memdump**,**hiberfil.sys**)**

* **Volatility (для анализа памяти):**

bash

Copy

Download

volatility -f dump.raw imageinfo

volatility -f dump.raw --profile=Win7 pslist

**В) Сетевой трафик (**PCAP**)**

* **Wireshark / Tshark:**

bash

Copy

Download

tshark -r traffic.pcap -Y "http.request"

* **Извлечение файлов:**

bash

Copy

Download

foremost -i traffic.pcap -o output\_dir

**Полезные инструменты**

| **Категория** | **Инструменты** |
| --- | --- |
| **Stego** | Steghide, Binwalk, StegSolve, Audacity |
| **Crypto** | CyberChef, RsaCtfTool, John the Ripper |
| **Forensic** | Autopsy, Volatility, Wireshark, Photorec |

**Заключение**

* **Stego:** Ищите скрытые данные в файлах.
* **Crypto:** Анализируйте шифры и кодировки.
* **Forensic:** Изучайте структуру файлов и дампы.