Intro

Steganography (Stego) là nghệ thuật che giấu một cái gì đó bên trong một cái gì đó khác, ví dụ: Một thông điệp bên trong một tập tin jpg, hoặc một binary bên trong một png. Stego đã được sử dụng từ thời cổ đại để truyền tải những thông điệp mà họ không muốn người khác nhìn thấy. Trong thời hiện đại, nó được sử dụng cho cùng một mục đích, chỉ là bây giờ chúng ta có các công cụ tiên tiến hơn nhiều. Căn phòng này được thiết kế để đi qua những công cụ đó và cách sử dụng chúng.

Tất cả các tệp cần thiết có thể được tìm thấy bên trong tệp zip đi kèm

**Note: Basic Linux knowledge required**

**steghide**

Steghide là một trong những công cụ steganography nổi tiếng nhất, cho lý do tốt. Đó là một phương pháp cổ điển, ẩn một thông điệp bên trong một hình ảnh, và steghide làm nó một cách hiệu quả. **Một nhược điểm của steghide là nó chỉ hoạt động trên jpgs;** tuy nhiên, điều đó có nghĩa là nếu bạn tin rằng có một thông điệp ẩn bên trong jpg, thì steghide là một lựa chọn có thể đề cập đến.

Một trong những lợi ích lớn nhất của **stegohide, là nó có thể encrypt data bằng cụm mật khẩu.** Có nghĩa là nếu họ không có mật khẩu thì họ không thể trích xuất bất kỳ dữ liệu nào.

steghide can be installed with the command   
sudo apt install steghide

+ What argument cho phép bạn nhúng(embed) dữ liệu (chẳng hạn như files) vào các tệp khác?  
+ What flag let’s you set the file to embed?  
+ What flag allows you to set the "cover file"?(i.e  the jpg)  
+ How do you set the password to use for the cover file?  
+ What argument allows you to extract data from files?

+ How do you select the file that you want to extract data from?  
+ Given the passphrase "password123", what is the hidden message in the included "jpeg1" file.

**zsteg**

**zsteg dùng cho png và steghide là jpg**. Nó hỗ trợ các kỹ thuật khác nhau để trích xuất bất kỳ và tất cả dữ liệu từ các tệp png.

**Note: zsteg cũng hỗ trợ các tệp BMP, nhưng nó chủ yếu được sử dụng cho png.**

zsteg can be installed by using ruby with the command   
gem install zsteg

+ Làm thế nào để bạn chỉ định **least significant bit** đến trước?  
+ What about the **most significant bit**?  
+ How do you specify verbose mode?   
+ How do you extract the data from a specific payload?  
+ In the included file "png1" what is the hidden message?  
+ What about the payload used to encrypt it.

Exiftool

Exiftool là một công cụ cho phép bạn xem và chỉnh sửa image metadata. Mặc dù bản thân điều này không phải là một công cụ stego, nhưng tôi sẽ rất hối hận nếu không bao gồm ít nhất một chú thích trên đó vì một trong những hình thức phổ biến nhất của image stego là ẩn tin nhắn trong metadata.

Exiftool can be installed with sudo apt install exiftool

+ In the included jpeg3 file, what is the document name?

Stegoveritas

Cá nhân đây là một trong những công cụ image stego yêu thích của tôi. Nó hỗ trợ gần như mọi tệp hình ảnh và có thể trích xuất tất cả các loại dữ liệu từ nó. Nó là một công cụ cực kỳ hữu ích nếu bạn không biết chính xác những gì bạn đang tìm kiếm và nó có vô số các thử nghiệm được xây dựng để trích xuất bất kỳ hoặc tất cả dữ liệu.

Lưu ý: Stegoveritas có các tính năng khác như: sửa màu ảnh.

Stegoveritas can be installed by running these two commands:

 pip3 install stegoveritas

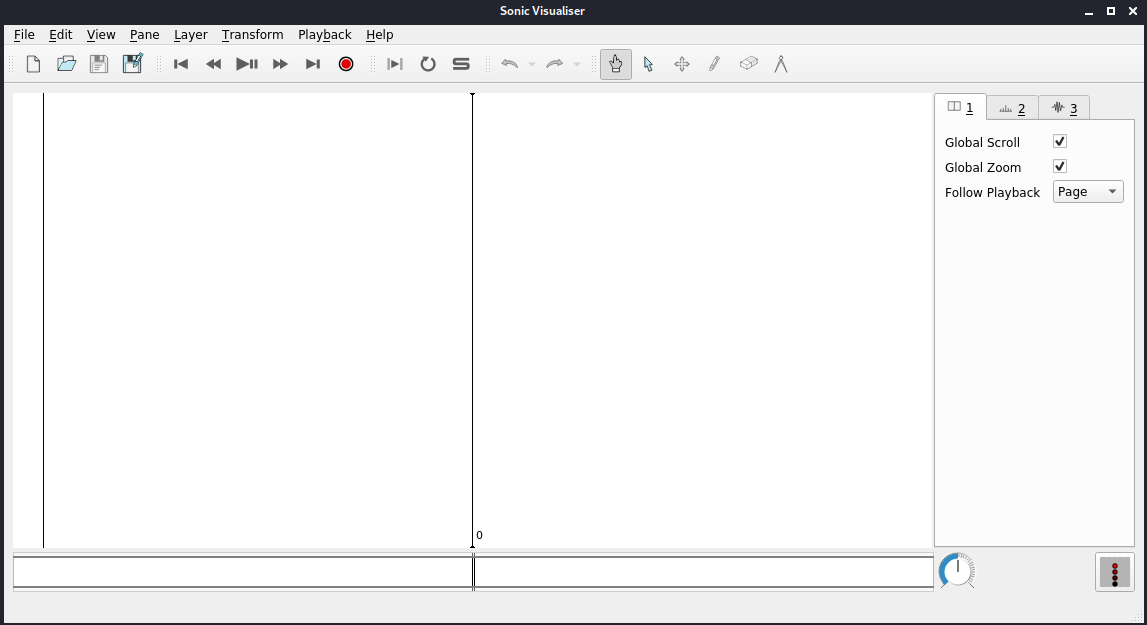
stegoveritas\_install\_deps

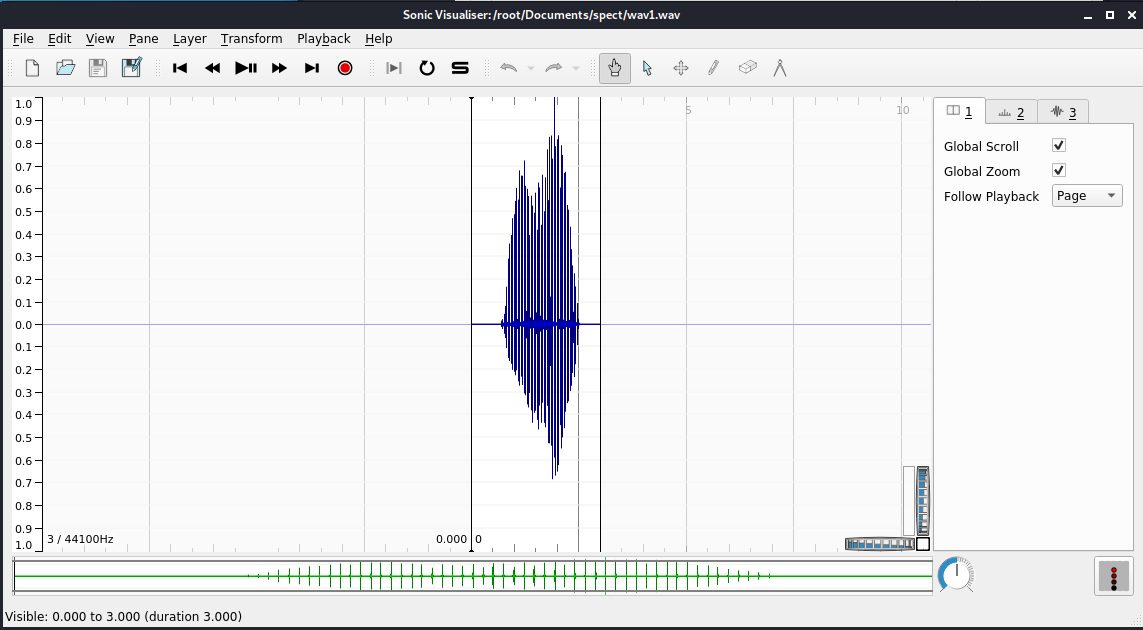
+ How do you check the file for metadata?  
+ How do you check for steghide hidden information  
+ What flag allows you to extract LSB data from the image?  
+ In the included image jpeg2 what is the hidden message?

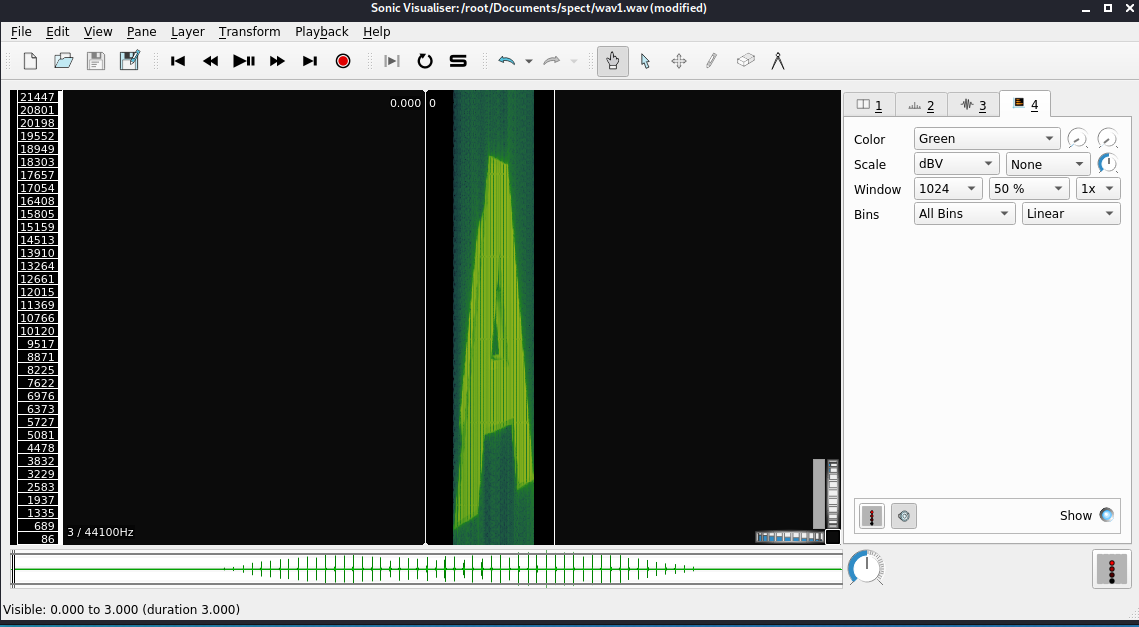
Spectrograms

Spectrograms(Quang phổ học/quang phổ) là nghệ thuật ẩn một image ẩn bên trong một audio file’s spectrograms. Do đó, khi đối phó với audio stego, luôn luôn phân tích spectrograms của âm thanh.Để thực hiện task này chúng tôi sẽ sử dụng Sonic Visualizer (<https://www.sonicvisualiser.org/download.html>)

Note: Phần giới thiệu này sẽ được thực hiện bằng cách sử dụng tệp wav1 đi kèm.

When you open Sonic Visualizer you should see this screen:  


From there click File->Open and then select the included wav1 file and you should see a screen similar to this:  


From there click Layer->Add Spectrogram and you should see this:  


And that’s it!

+ What is the hidden text in the included wav2 file?

The Final Exam

+ What is key1?  
+ What is key2?  
+ What is key3?