

politician

# Steganography 101

How to hide information, or  
“You’ll never look at the Internet  
the same way ever again”

# Disclaimer

Any opinions presented in this talk by the presenter do not in any way represent an official endorsement of these opinions by Freeside Technology Spaces, Inc., nor is intended to reflect the views of Freeside and its membership. Freeside does not encourage or promote any illegal activity, such as torture or other war crimes.

*“Reports that say there’s -- that something hasn’t happened are always interesting to me, because as we know, there are known knowns; there are things that we know that we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns, the ones we don’t know we don’t know.”*

Donald Rumsfeld

*“Am I a fool? I don’t think I’m a fool. But I think I sure was fooled.”*

Kenneth Lay

*“There’s an old saying in Tennessee - I know it’s in Texas, probably in Tennessee - that says, fool me once, shame on - shame on you. Fool me - you can’t get fooled again.”*

George W. Bush

*“We don’t get fooled again”*

The Who

# What is Stegosaurus?



Jefferson

democracy

# What is Steganography?



churches

secularism

# Image Metadata (Baby Steps)

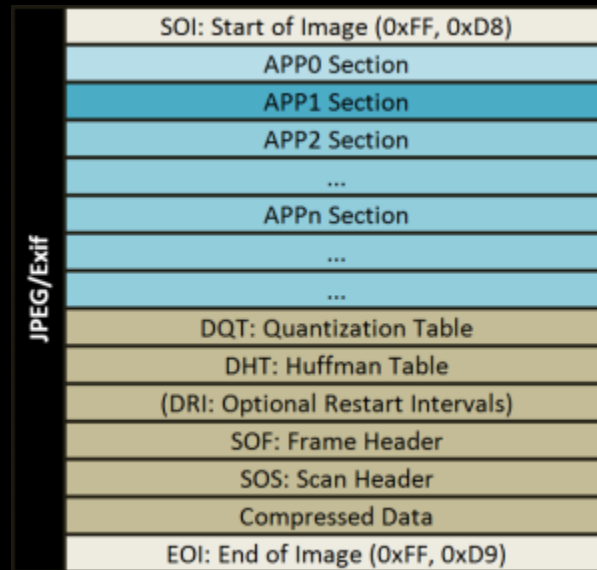
Using `exiftool`, we can extract the “hidden” information in the “Snakes are Awesome” image.

The information is “hidden” as image **metadata**, which is stored in specific locations in a file.

abortions

# JPEG/Exif Format

squeal rule



bureaucrats

<http://www.codeproject.com/Articles/43665/ExifLibrary-for-NET>

# exiftool Demo

This slide intentionally left uninteresting.  
Or is it?

# Steganography in Text

- Hide text within another text using markers (ex. bold words, words after commas, the next word every N characters)
- Translate (letters, words) into words, numbers, or phrases (ex. “A” becomes “the nefarious polyglot”)
- Translate letters, words into white space
- Misrepresent the text (ex. spam, PGP)



# Spammimic Demo

Dear E-Commerce professional ; This letter was specially selected to be sent to you . This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 1816 , Title 5 ; Section 303 . THIS IS NOT MULTI-LEVEL MARKETING ! Why work for somebody else when you can become rich within 55 DAYS . Have you ever noticed people love convenience and nobody is getting any younger .

# Files within Files



pornography

**YO DAWG WE HEARD YOU LIKE EXHIBITS SO WE PUT XZIBIT IN YO EXHIBIT SO YOU CAN LOOK AT XZIBIT WHILE YOU EXHIBIT XZIBIT IN YO EXHIBIT**

# Hide a Zip File in a JPEG Demo

```
$ cat taxiderpy_original.jpg >> taxiderpy.jpg  
$ zip secret.zip microsoft-spy.pdf  
$ cat secret.zip >> taxiderpy.jpg
```

```
$ ls -sh1 taxiderpy*  
1.6M taxiderpy.jpg  
40K taxiderpy_original.jpg  
$
```

transcending

# Before and After



# Extraction

```
$ unzip taxiderpy.jpg
Archive:  taxiderpy.jpg
warning [taxiderpy.jpg]:  37425 extra bytes at
beginning or within zipfile
    (attempting to process anyway)
    inflating: microsoft-spy.pdf
$ open microsoft-spy.pdf
```

proletariat

# Questions?

military



totalitarian

How many hidden messages did you find in this slideshow?  
Download this presentation at Freeside's Wiki!