Level 0x07

Steganography

Topics

- Hacker History
- Text Steg
- Polyglot

Travis Goodspeed

- Legendary Hardware Hacker
- Author of Microcontroller Exploits book (2024)
  - So many hacks…
- GoodFET - JTAG
  - Inspired other projects GreatFET, Bus Pirate)
- Face Dancer (USB packet capture device)
- Editor of PoC||GTFO hacker e-Zine
- XBox hacker

Steganography

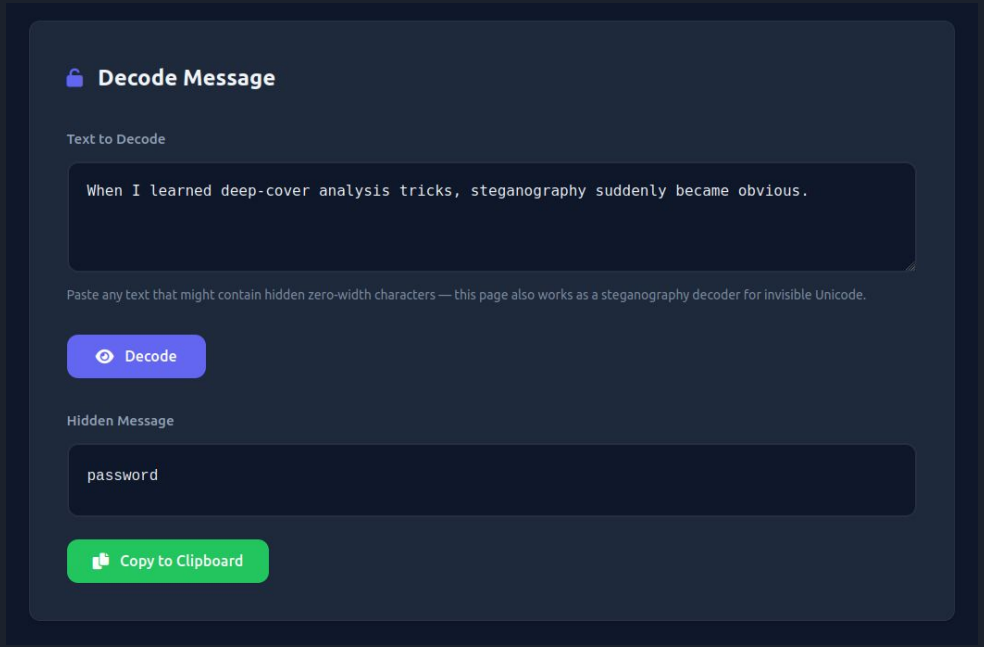
- Hiding information within another message or object
  - Covert way to pass information between systems
  - Hide in plain sight
- If adversary doesn't know info is hidden
  - Broadcast your secret message
  - Don't care if intercepted
  - Looks like a benign letter / email / picture
- Difficult to detect unless you know the mechanism for hiding the information

Example

When I learned deep-cover analysis tricks, steganography suddenly became obvious.

- What are the first letters of each word?

Decoded on stegzero.com



Technique Details

```
mwales@Metroid:~/scratch$ vi message.txt
mwales@Metroid:~/scratch$ cat message.txt
When I learned deep-cover analysis tricks, steganography suddenly became obvious.
mwales@Metroid:~/scratch$ hexdump -C message.txt
00000000  57 e2 81 a3 68 e2 80 8c  65 e2 80 8d 6e e2 81 a3  |W...h...e...n...|
00000010  20 e2 81 a3 49 e2 80 8b  20 e2 80 8b 6c e2 80 8c  | ...I... ...l...|
00000020  65 e2 80 8b 61 e2 81 a0  72 e2 80 8d 6e ef bb bf  |e...a...r...n...|
00000030  65 e2 81 a3 64 e2 80 8b  20 e2 80 8b 64 e2 80 8b  |e...d... ...d...|
00000040  65 e2 80 8b 65 e2 80 8d  70 e2 80 8b 2d e2 81 a0  |e...e...p...-...|
00000050  63 e2 80 8d 6f ef bb bf  76 e2 80 8b 65 e2 80 8d  |c...o...v...e...|
00000060  72 e2 80 8d 20 e2 80 8c  61 e2 81 a3 6e e2 81 a3  |r... ...a...n...|
00000070  61 e2 80 8d 6c e2 81 a2  79 ef bb bf 73 ef bb bf  |a...l...y...s...|
00000080  69 e2 81 a2 73 ef bb bf  20 e2 81 a2 74 e2 81 a4  |i...s... ...t...|
00000090  72 e2 80 8d 69 e2 80 8d  63 e2 81 a4 6b e2 81 a3  |r...i...c...k...|
000000a0  73 ef bb bf 2c e2 81 a0  20 e2 80 8b 73 e2 80 8c  |s...,... ...s...|
000000b0  74 e2 80 8c 65 e2 80 8b  67 e2 80 8d 61 e2 80 8c  |t...e...g...a...|
000000c0  6e e2 80 8b 6f e2 81 a4  67 e2 81 a4 72 61 70 68  |n...o...g...raph|
000000d0  79 20 73 75 64 64 65 6e  6c 79 20 62 65 63 61 6d  |y suddenly becam|
000000e0  65 20 6f 62 76 69 6f 75  73 2e 0a                 |e obvious..|
000000eb
mwales@Metroid:~/scratch$
```

The Technical Process of Hiding Messages

- Converts your hidden message to UTF-8 bytes for full Unicode support.
- Adds a compact header with a magic marker, version, random nonce, length, and CRC32 for integrity.
- Obfuscates only the payload bits using a nonce-seeded PRNG (not encryption) to reduce easy pattern detection.
- Maps 3-bit groups to a diversified set of eight zero-width/invisible characters (not just a single 0/1 pair).
- Evenly interleaves the hidden characters across the visible text so they are not clustered at the end.
- On decoding, extracts the zero-width alphabet, validates the header and CRC, then restores the UTF-8 message.
- Includes a legacy fallback decoder for older texts that used a simple two-character (0/1) scheme.

Text Based Steganography

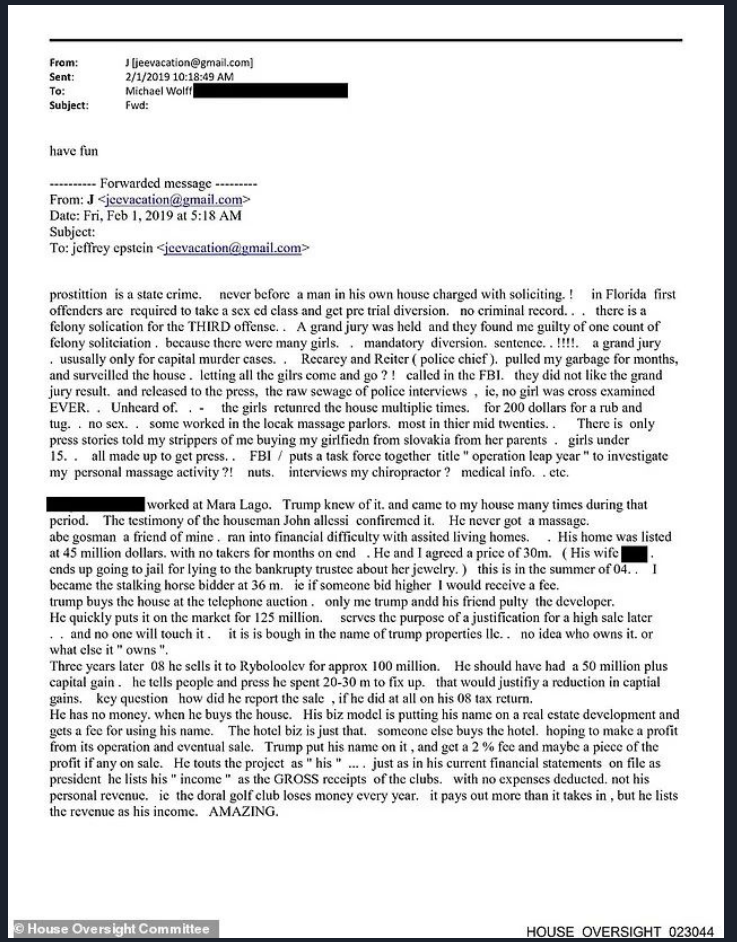
- Zero width characters
  - stegzero.com
  - stegcloak
- Whitespace
  - on line endings (stegsnow)
  - In HTML documents (it's mostly ignored)
- Unicode abuse of similar characters
- Spelling differences:
  - Color / colour. Favorite / Favourite.
- Linguistic differences
- Invisible Ink

U+0391	A	913	Greek Capital Letter Alpha
U+0392	B	914	Greek Capital Letter Beta
U+0393	Γ	915	Greek Capital Letter Gamma
U+0394	Δ	916	Greek Capital Letter Delta
U+0395	E	917	Greek Capital Letter Epsilon
U+0396	Z	918	Greek Capital Letter Zeta
U+0397	H	919	Greek Capital Letter Eta

Detecting

- Much easier if you know technique / design

- Jeffrey Epstein letter to himself before his death
  - Random whitespace
  - Incomplete / partial sentences
  - Punc,tuation . ! seems? RANDOM !?
- Steg / hidden message or crazy ramblings?



From: J [jeevacation@gmail.com]
Sent: 2/1/2019 10:18:49 AM
To: Michael Wolff [redacted]
Subject: Fwd:

have fun

---------- Forwarded message ---------
From: **J** <jeevacation@gmail.com>
Date: Fri, Feb 1, 2019 at 5:18 AM
Subject:
To: jeffrey epstein <jeevacation@gmail.com>

prostittion is a state crime. never before a man in his own house charged with soliciting. ! in Florida first offenders are required to take a sex ed class and get pre trial diversion. no criminal record. . . there is a felony solication for the THIRD offense. . A grand jury was held and they found me guilty of one count of felony solitciation . because there were many girls. . mandatory diversion. sentence. . !!!!. a grand jury . ususally only for capital murder cases. . Recarey and Reiter (police chief). pulled my garbage for months, and surveilled the house . letting all the gilrs come and go ? ! called in the FBI. they did not like the grand jury result. and released to the press, the raw sewage of police interviews , ie, no girl was cross examined EVER. . Unheard of. . - the girls retunred the house multiplic times. for 200 dollars for a rub and tug. . no sex. . some worked in the locak massage parlors. most in thier mid twenties. . There is only press stories told my strippers of me buying my girlfiedn from slovakia from her parents . girls under 15. . all made up to get press. . FBI / puts a task force together title " operation leap year " to investigate my personal massage activity ?! nuts. interviews my chiropractor ? medical info. . etc.

[redacted] worked at Mara Lago. Trump knew of it. and came to my house many times during that period. The testimony of the houseman John allessi confirmed it. He never got a massage.
abe gosman a friend of mine . ran into financial difficulty with assited living homes. . His home was listed at 45 million dollars. with no takers for months on end . He and I agreed a price of 30m. (His wife [redacted] . ends up going to jail for lying to the bankrupty trustee about her jewelry.) this is in the summer of 04. . I became the stalking horse bidder at 36 m. ie if someone bid higher I would receive a fee.
trump buys the house at the telephone auction . only me trump andd his friend pulty the developer.
He quickly puts it on the market for 125 million. serves the purpose of a justification for a high sale later . . and no one will touch it . it is is bough in the name of trump properties llc. . no idea who owns it. or what else it " owns ".
Three years later 08 he sells it to Ryboloolev for approx 100 million. He should have had a 50 million plus capital gain . he tells people and press he spent 20-30 m to fix up. that would justifiy a reduction in captial gains. key question how did he report the sale , if he did at all on his 08 tax return.
He has no money. when he buys the house. His biz model is putting his name on a real estate development and gets a fee for using his name. The hotel biz is just that. someone else buys the hotel. hoping to make a profit from its operation and eventual sale. Trump put his name on it , and get a 2 % fee and maybe a piece of the profit if any on sale. He touts the project as " his " ... . just as in his current financial statements on file as president he lists his " income " as the GROSS receipts of the clubs. with no expenses deducted. not his personal revenue. ie the doral golf club loses money every year. it pays out more than it takes in , but he lists the revenue as his income. AMAZING.

Polyglot

- Speaking or writing in several languages
- Program written in multiple languages all in the same file
  - Typically different comment chars for different languages
- Python 2 vs 3

Highlighted for Bash

```
#define a /*
#<?php
echo "\010Hello, world!
\n";// 2> /dev/null > /dev/
null \ ;
// 2> /dev/null; x=a;
$x=5; // 2> /dev/null \ ;
if (($x))
// 2> /dev/null; then
return 0;
// 2> /dev/null; fi
#define e ?>
#define b */
#include <stdio.h>
#define main() int
main(void)
#define printf printf(
#define true )
#define function
function main()
{
printf "Hello, world!
\n"true/* 2> /dev/null | grep
-v true*/;
return 0;
}
#define c /*
main
#*/
```

Highlighted for PHP

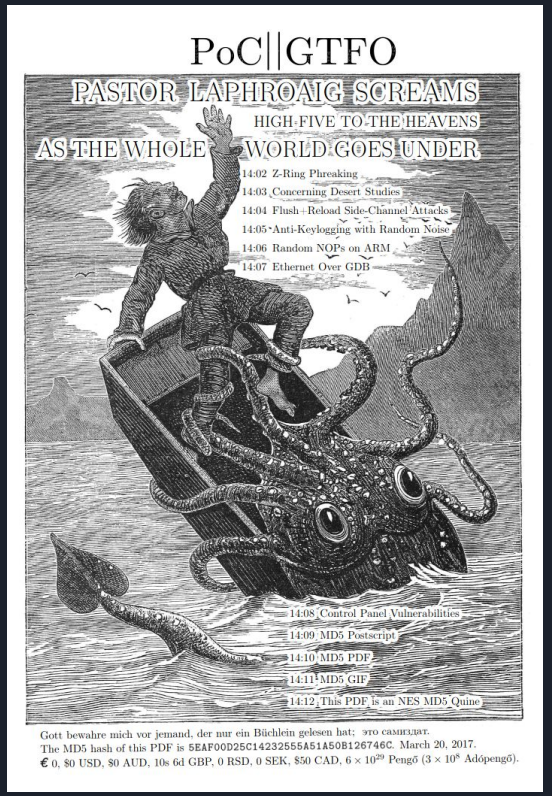
```
#define a /*
#<?php
echo "\010Hello, world!
\n";// 2> /dev/null > /dev/
null \ ;
// 2> /dev/null; x=a;
$x=5; // 2> /dev/null \ ;
if (($x))
// 2> /dev/null; then
return 0;
// 2> /dev/null; fi
#define e ?>
#define b */
#include <stdio.h>
#define main() int
main(void)
#define printf printf(
#define true )
#define function
function main()
{
printf "Hello, world!
\n"true/* 2> /dev/null | grep
-v true*/;
return 0;
}
#define c /*
main
#*/
```

Highlighted for C

```
#define a /*
#<?php
echo "\010Hello, world!
\n";// 2> /dev/null > /dev/
null \ ;
// 2> /dev/null; x=a;
$x=5; // 2> /dev/null \ ;
if (($x))
// 2> /dev/null; then
return 0;
// 2> /dev/null; fi
#define e ?>
#define b */
#include <stdio.h>
#define main() int
main(void)
#define printf printf(
#define true )
#define function
function main()
{
printf "Hello, world!
\n"true/* 2> /dev/null | grep
-v true*/;
return 0;
}
#define c /*
main
#*/
```

PoC||GTFO

- Free hacker zine
- Loves to explore polyglots
- Issue 14 is a
  - PDF
  - NES ROM (runs in Nestopia or old FCEUX)
  - ZIP file
  - MD5 is broken showcase
    - PDF has hash on front cover
    - NES ROM has hash in the game



Uses

- Covert communication
- Watermarking
  - Copyright protection
  - Intellectual Property tracking
  - Proof of ownership
- Hiding malicious data / programs
- Obfuscation
- How is a virus scanner gonna check that polyglot isn’t malicious?

Links

- https://pure.ulster.ac.uk/ws/portalfiles/portal/11638661/Text%20Based%20Steganography%20-%20IJPSI%20Pre-Print.pdf
- stegzero.com
- https://en.wikipedia.org/wiki/Polyglot_(computing)
- https://www.alchemistowl.org/pocorgtfo/