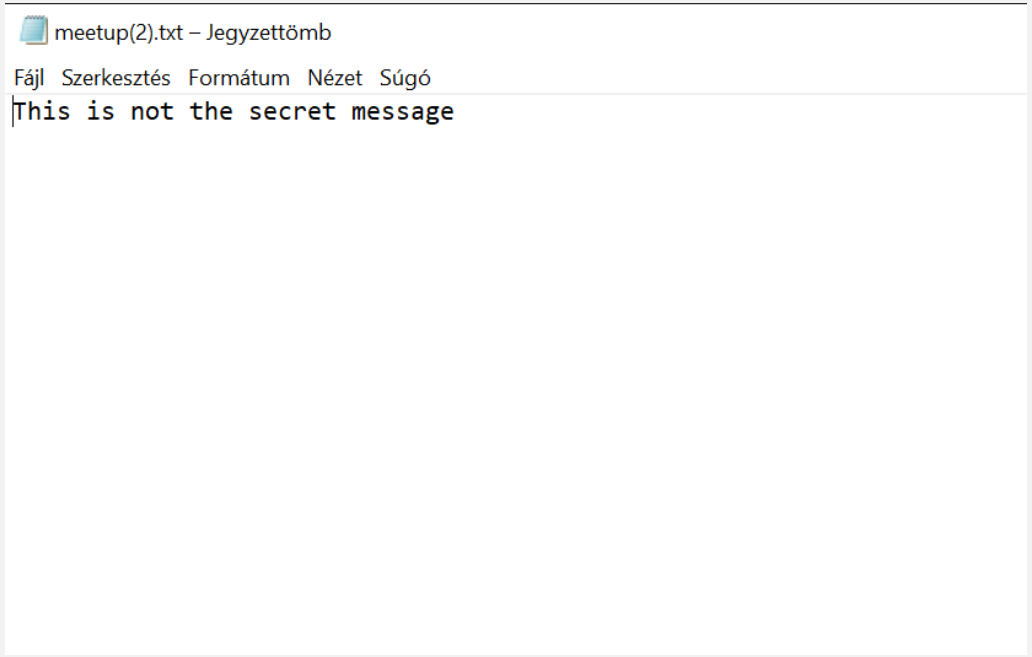
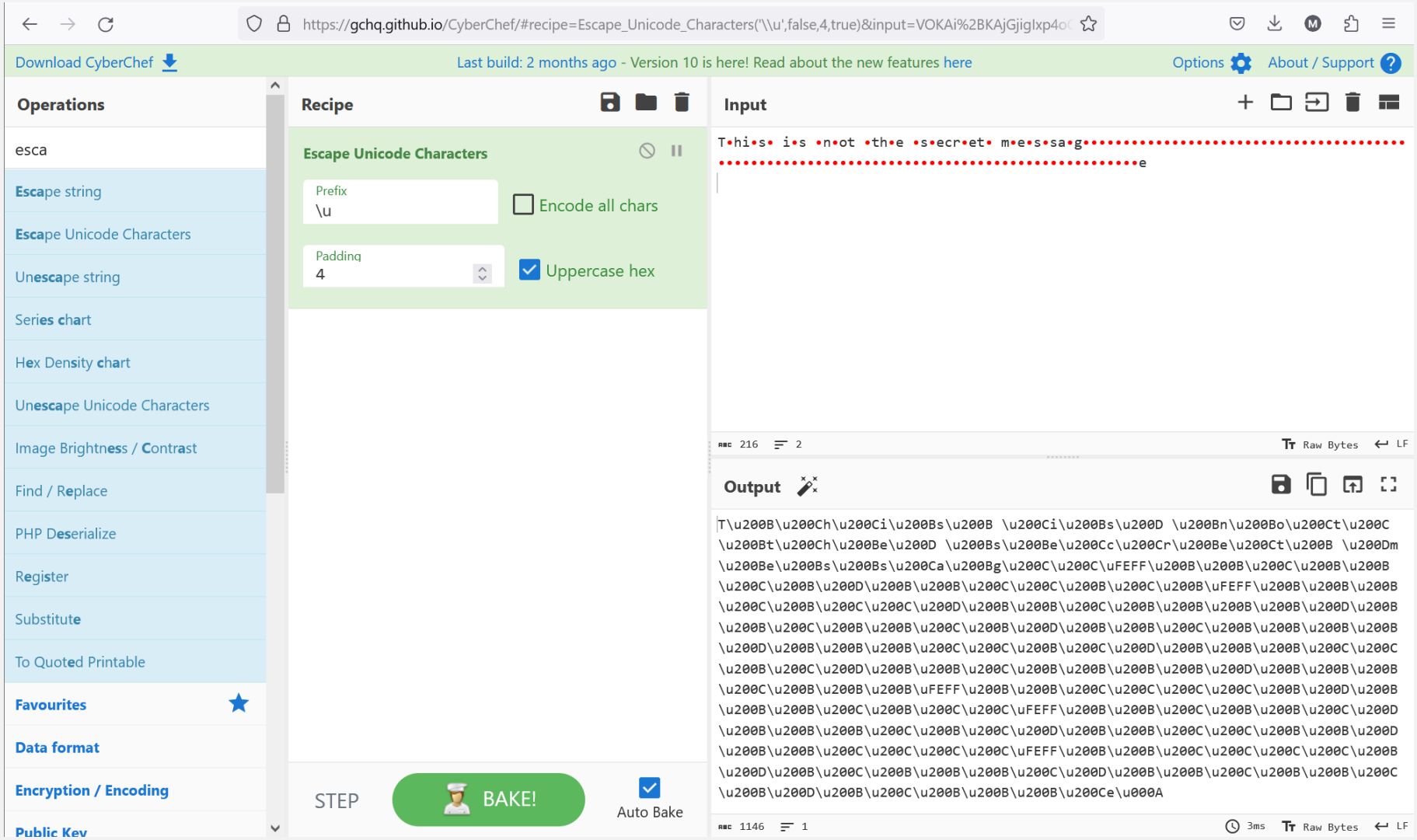
ZERO-WIDTH KARAKTEREK

EGY KB MÉRETŰ FILE?




https://gchq.github.io/CyberChef/#recipe=Escape_Unicode_Characters('\\u',false,4,true)&input=VOKAi%2BKAjGjigIxp4o
Download CyberChef
Last build: 2 months ago - Version 10 is here! Read about the new features here
Options
About / Support
Operations
esca
Escape string
Escape Unicode Characters
Unescape string
Series chart
Hex Density chart
Unescape Unicode Characters
Image Brightness / Contrast
Find / Replace
PHP Deserialize
Register
Substitute
To Quoted Printable
Favourites
Data format
Encryption / Encoding
Public Key
Recipe
Escape Unicode Characters
Prefix
\u
Encode all chars
Padding
4
Uppercase hex
STEP
BAKE!
Auto Bake
Input
T•hi•s• i•s •n•ot •th•e •s•ecr•et• m•e•s•sa•g
e
216
2
Raw Bytes
LF
Output
T\u200B\u200Ch\u200Ci\u200Bs\u200B \u200Ci\u200Bs\u200D \u200Bn\u200Bo\u200Ct\u200C
\u200Bt\u200Ch\u200Be\u200D \u200Bs\u200Be\u200Cc\u200Cr\u200Be\u200Ct\u200B \u200Dm
\u200Be\u200Bs\u200Bs\u200Ca\u200Bg\u200C\u200C\uFEFF\u200B\u200B\u200C\u200B\u200B
\u200C\u200B\u200D\u200B\u200B\u200C\u200C\u200B\u200C\u200B\uFEFF\u200B\u200B\u200B
\u200C\u200B\u200C\u200C\u200D\u200B\u200B\u200C\u200B\u200B\u200B\u200B\u200D\u200B
\u200B\u200C\u200B\u200B\u200C\u200B\u200D\u200B\u200B\u200C\u200B\u200B\u200B\u200B
\u200D\u200B\u200B\u200B\u200C\u200C\u200B\u200C\u200D\u200B\u200B\u200B\u200C\u200C
\u200B\u200C\u200D\u200B\u200B\u200C\u200B\u200B\u200B\u200B\u200D\u200B\u200B\u200B
\u200C\u200B\u200B\u200B\uFEFF\u200B\u200B\u200C\u200C\u200C\u200C\u200B\u200D\u200B
\u200B\u200B\u200C\u200B\u200C\u200C\uFEFF\u200B\u200B\u200C\u200B\u200B\u200C\u200D
\u200B\u200B\u200B\u200C\u200B\u200C\u200D\u200B\u200B\u200C\u200C\u200B\u200B\u200D
\u200B\u200B\u200C\u200C\u200C\u200C\uFEFF\u200B\u200B\u200C\u200C\u200C\u200C\u200B
\u200D\u200B\u200C\u200B\u200B\u200B\u200C\u200D\u200B\u200B\u200C\u200B\u200B\u200C
\u200B\u200D\u200B\u200C\u200B\u200B\u200B\u200Ce\u000A
1146
1
3ms
Raw Bytes
LF

Product Solutions Open Source Pricing

vedhavyas / zwfp Public

Code Issues 1 Pull requests 1 Actions Projects Security Insights

Files

master

Go to file

- cmd
- .gitignore
- .travis.yml
- LICENSE
- README.md
- embed.go
- embed_test.go
- extract.go
- extract_test.go
- go.mod

zwfp / embed.go

vedhavyas contain embed within the string

Code Blame 110 lines (89 loc) · 1.97 KB

```go
package zwfp

import (
        "fmt"
        "strings"
)

// Zero width non-printing characters
const (
        zwsp = '\u200B' // 1
        zwnj = '\u200C' // 0
        zwj  = '\u200D' // letter
        zwnb = '\uFEFF' // word
)

// toBits converts each character in the string to base 2 form
func toBits(s string) []string {
        var bits []string
        for _, c := range s {
                bits = append(bits, fmt.Sprintf("%b", c))
        }

        return bits
}
```

```
┌──(root㉿kali)-[/home/…/Boston_23/zwfp/cmd/z
└─# cat meetup.txt| xargs -0 ./zwfp
Cover Text: This is not the secret message

Payload: Meet me tomorrow at 6:30 a.m.

┌──(root㉿kali)-[/home/…/Boston_23/zwfp/cmd/z
└─#
```

Steganography

A method to hiding something in something.

General

1. Usually when organizer gave us Image, Music, Video, Zip, EXE, File System, PDF and other files, it a *steganography* or *forensics* challenge. Run `file` command first.
2. Metadata is important. Checkout the EXIF data of the file by using `exiftool [filename]` command.
3. Try issuing `binwalk [filename]` on the file. They may hide another file in the file.
   - To extract, use `binwalk -e`.
   - To extract one specific signature type, use `binwalk -D 'png image:png' [filename]`.
   - To extract all files, run `binwalk --dd='.*' [filename]`.
4. Try file carve using `foremost -v [filename]` command. Foremost support all files.

Images

1. View the image first
2. Use `strings` command to that file.
   - Try `grep -i [any strings you want to filter]` from the `strings` command output.
   - Example `grep -i "flag{"` to filtering the flag format only. `-i` option to unable case sensitive.
3. Google the images, differentiate the `md5hash`. If you found same image but have a different md5 hash, it may probably have been altered.

198

Digital Forensics Case B4DM755

Acquire the critical skills of evidence preservation, disk imaging, and artefact analysis for use in court.

Room Objectives

Learn about the following to build up the confidence of future Forensics Lab Analysts, DFIR First Responders, and Digital Forensics Investigators:

- Ensure proper Chain of Custody procedures for transport to the Forensics Laboratory.
- Use FTK Imager to acquire a forensic disk image and preserve digital artefacts and evidence.
- Analyse forensic artefacts received at the Forensics Laboratory for presentation during a trial in a court of law.

Room Prerequisites

Before starting with this room, we recommend you clear Intro to Digital Forensics and Introduction to Cryptography.