ADVANCED STEGANOGRAPHY

RUET
CYBER
SECURITY
CLUB

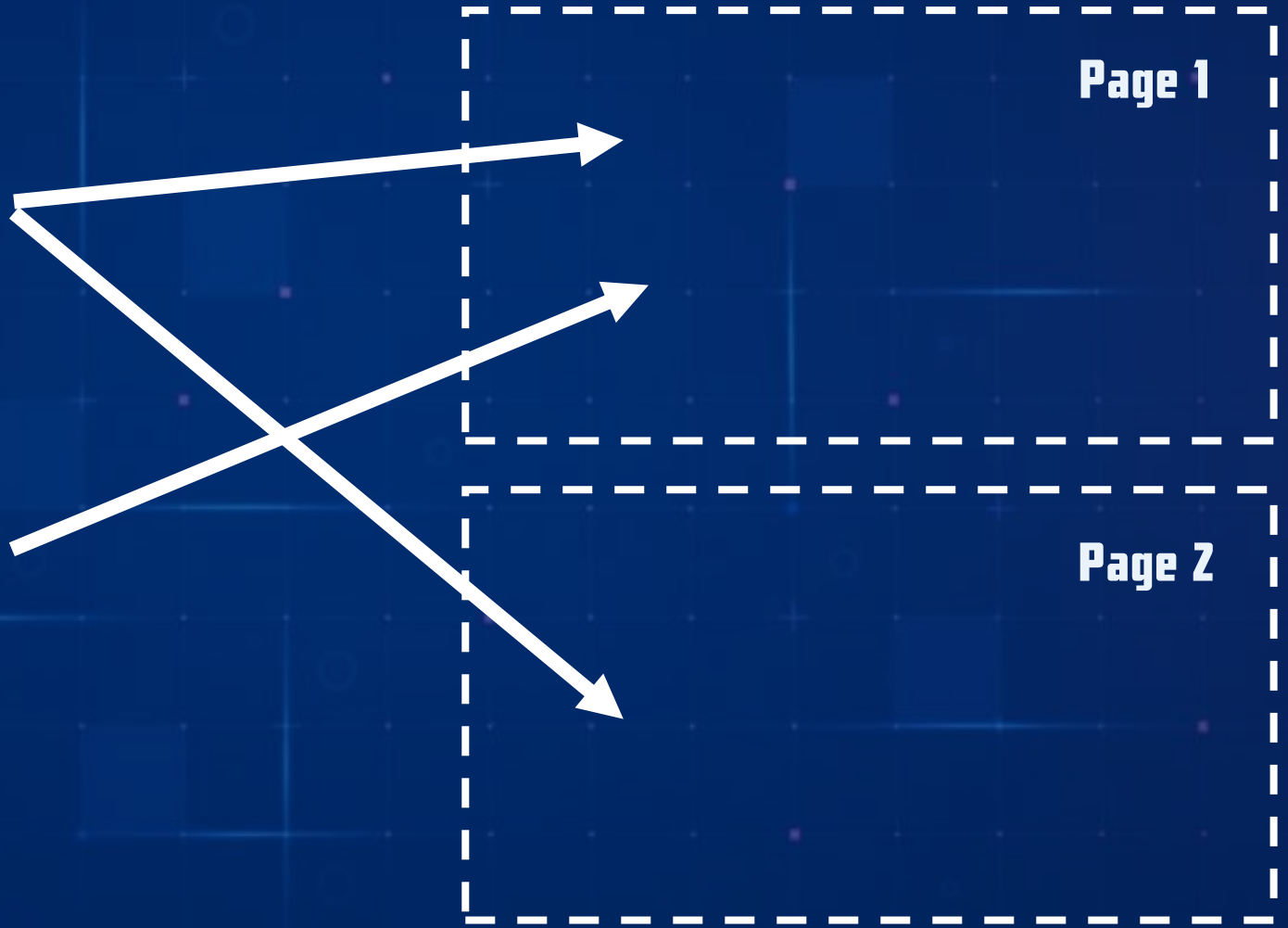
TOPICS TO BE COVERED...

- PDF STEGANOGRAPHY
- FILE MAGIC BYTES
- HEX EDITOR
- TEXT STEGANOGRAPHY

PDF STRUCTURE

IMAGES

Texts



PDF STRUCTURE

PDF STRUCTURE

THE MAGIC BYTES

PNG JPG ZIP MP4

THE MAGIC BYTES

JPG

11111111 11011000 11111111 11100000
00000000 00010000 01001010 01000110
01001001 01000110 00000000 00000001
00000001 00000001 00000000 01001000

. . . . . .

. . . . . .

THE MAGIC BYTES

JPG

FF D8 FF E0 00 10 4A 46 49 46 00
01 01 01 00 48 00 48 00 00 FF E1
00 2C 45 78 69 66 00 00 4D 4D 00
2A 00 00 00 08 00 01 01 3B 00 02
00 00 00 0A 00 00 00 1A 00 00 00
00 61 72 6B 68 61 6E 32 32 .. ..

.....

THE MAGIC BYTES

JPG

FF D8 FF E0 00 10 4A 46 49 46 00
01 01 01 00 48 00 48 00 00 FF E1
00 2C 45 78 69 66 00 00 4D 4D 00
2A 00 00 00 08 00 01 01 3B 00 02
00 00 00 0A 00 00 00 1A 00 00 00
00 61 72 6B 68 61 6E 32 32 .. ..

.....

THE MAGIC BYTES

PNG

89 50 4E 47 0D 0A 1A 0A 00 00 00
0D 49 48 44 52 00 00 01 90 00 00
01 DF 08 06 00 00 00 7E B1 8E 75
00 00 00 3C 74 45 58 74 43 6F 6D
6D 65 6E 74 00 32 20 34 33 20 35
33 20 34 33 20 37 62 20 37 .. ..

.....

THE MAGIC BYTES

Filetype	Magic Bytes
JPG	FF D8 FF
PNG	89 50 4E 47 0D 0A 1A 0A
ZIP	50 4B 03 04
PDF	25 50 44 46 2D
MP4	00 00 00 ?? 66 74 79 70 69 73 6F 6D
DOCX	50 4B 03 04

THE MAGIC BYTES

« MAGIC BYTES CAN APPEAR BOTH IN HEADER & FOOTER »

HEADER MAGIC BYTES ➡ **89 50 4E 47 0D 0A 1A 0A** 00 00 00
0D 49 48 44 52 00 00 01 90 00 00

.....

.....

F1 34 F0 8C B9 7A BC B1 F8 FF 7E
B2 9A 12 92 3B D3 0F 00 00 00 00

FOOTER MAGIC BYTES ➡ **49 45 4E 44**

PNG IMAGE

HEX EDITOR

TOOL TO EDIT BINARY DATA OF FILES

https://hexed.it/

THE MAGIC BYTES

HOW DOES BINWALK WORK?

JPG

FF D8 FF E0 00 10 4A 46 49 46 00
01 01 01 00 48 00 48 00 00 FF E1

. . . . . .

PNG

89 50 4E 47 0D 0A 1A 0A 00 00 00
0D 49 48 44 52 00 00 01 90 00 00

. . . . . .

HIDING DATA WIHTIN TEXTS

ASCII characters: A-Z, a-z, 0-9, special characters

Possible characters: 128

Then how do we add emoji? 🤔, non-English characters etc?

HIDING DATA WIHTIN TEXTS

Here comes UNICODE into play
Possible characters: More than 1 Million

- [x] Emojis
- [x] non-English characters
- [x] Hidden characters ‹‹‹

HIDING DATA WIHTIN TEXTS

HIDING DATA WIHTIN TEXTS

Hidden characters includes

ZERO WIDTH CHARACTERS

HIDING DATA WIHTIN TEXTS

HOW TO SEE HIDDEN CHARACTERS?

https://invisible-characters.com/view.html

THAT'S ALL FOR TODAY