Installeer alvast volgende:

- Wireshark
- Ghidra

Eten: https://haldis.zeus.gent/order/uh438a5e

Voor windows:

- 7zip
- WSL (windows subsystem for linux)

Wifi: Zeus Event

ww: eventisdemax1408

Intro hacking en CTF

gehakt

Wat is een CTF

Capture the flag

```
ZeusCTF{1k_b3n_33n_fl4g_H4DJ5D}
```

Jeopardy, Attack/Defence

Challenges

Verschillende categorieën

Algemene tips

Lees beschrijving en naam van challenge!

Zoeken naar gelijkaardige oude challenges

Kijk eens op de website van de maker van de challenge (tools, blogposts)

Encodings

binary

hexadecimal (hex)

base64

128	64	32	16	8	4	2	1
1	0	0	1	1	0	1	1

0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	10	A
1011	11	B
1100	12	C
1101	13	D
1110	14	E
1111	15	F

Encodings - Base 64

encoderen van 6 bits

Sophie Alpert
@sophiebits

> aGkgdHdpd…

me: I have no idea what this is

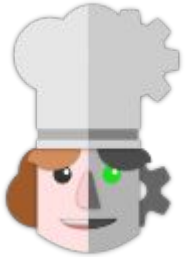
> aGkgdHdpdHRlcg==

me: oh it's base 64

10:20 PM · Mar 6, 2019 · Twitter for iPhone

Index	Binary	Char	Index	Binary	Char	Index	Binary	Char	Index	Binary	Char
0	000000	A	16	010000	Q	32	100000	g	48	110000	w
1	000001	B	17	010001	R	33	100001	h	49	110001	x
2	000010	C	18	010010	S	34	100010	i	50	110010	y
3	000011	D	19	010011	T	35	100011	j	51	110011	z
4	000100	E	20	010100	U	36	100100	k	52	110100	0
5	000101	F	21	010101	V	37	100101	l	53	110101	1
6	000110	G	22	010110	W	38	100110	m	54	110110	2
7	000111	H	23	010111	X	39	100111	n	55	110111	3
8	001000	I	24	011000	Y	40	101000	o	56	111000	4
9	001001	J	25	011001	Z	41	101001	p	57	111001	5
10	001010	K	26	011010	a	42	101010	q	58	111010	6
11	001011	L	27	011011	b	43	101011	r	59	111011	7
12	001100	M	28	011100	c	44	101100	s	60	111100	8
13	001101	N	29	011101	d	45	101101	t	61	111101	9
14	001110	O	30	011110	e	46	101110	u	62	111110	+
15	001111	P	31	011111	f	47	101111	v	63	111111	/
padding		=									

Algemene tools



Cyberchef | encodings

pwntools | Python library voor CTFs

cURL / wget | requests

netcat (nc) | connectie met een server

curl://

PWNTOOLS

Wi wa web - developer console

F12

Ctrl + Shift + i

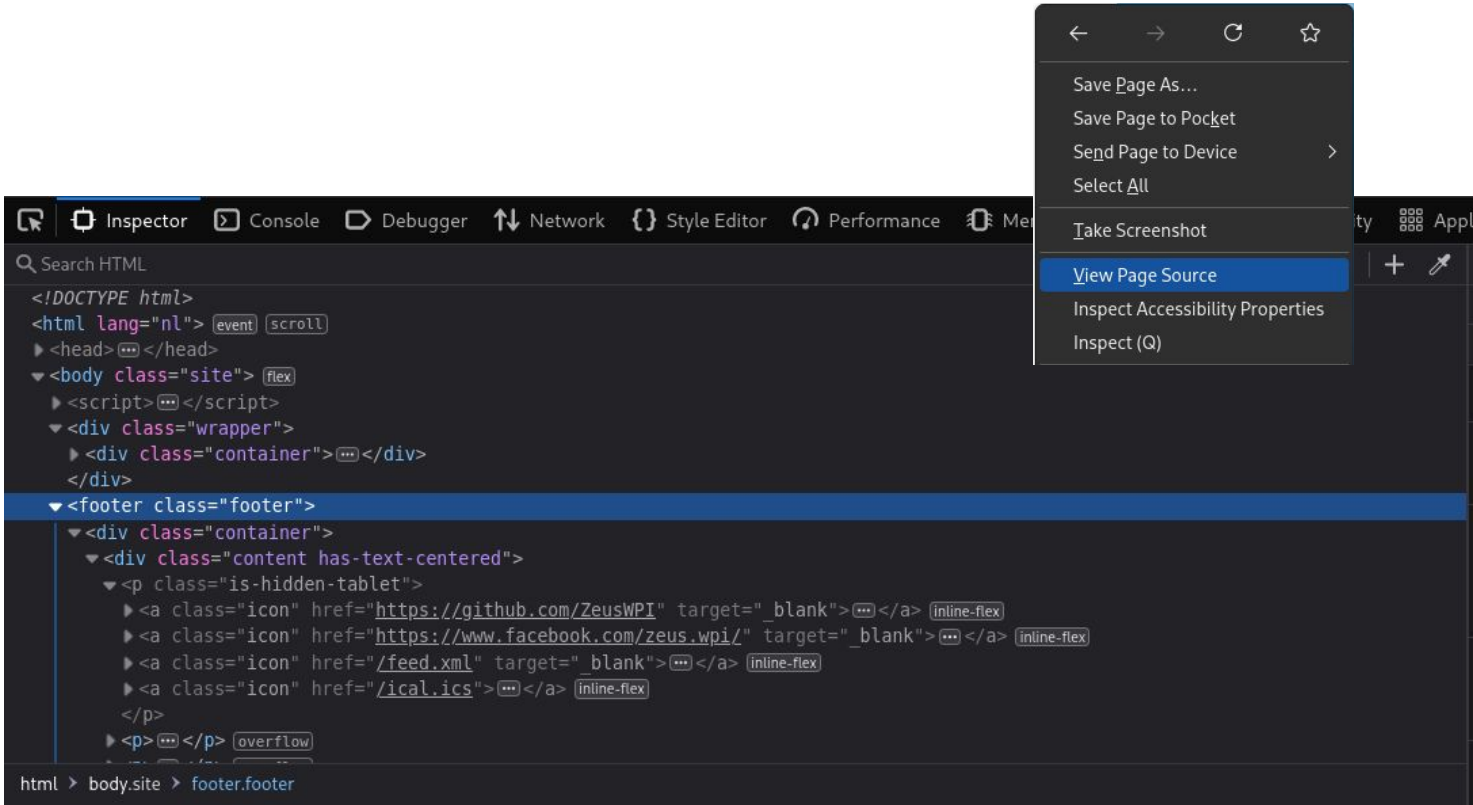
Rechts klik > inspect element

Console - Inspector

HTML

Comments

Hidden HTML



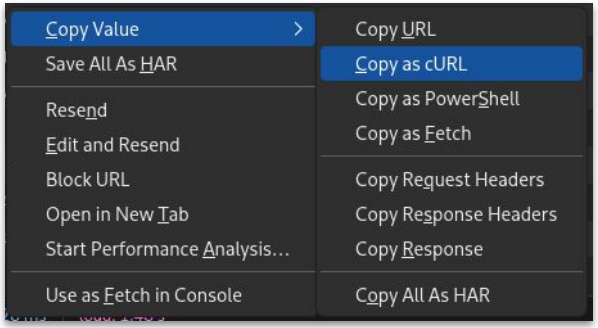
Console - Network

Requests tussen browser en server

images, javascript, json, ...

headers

Copy as cURL



Inspector | Console | Debugger | Network | Style Editor | Performance | Memory | Storage | Accessibility | Application

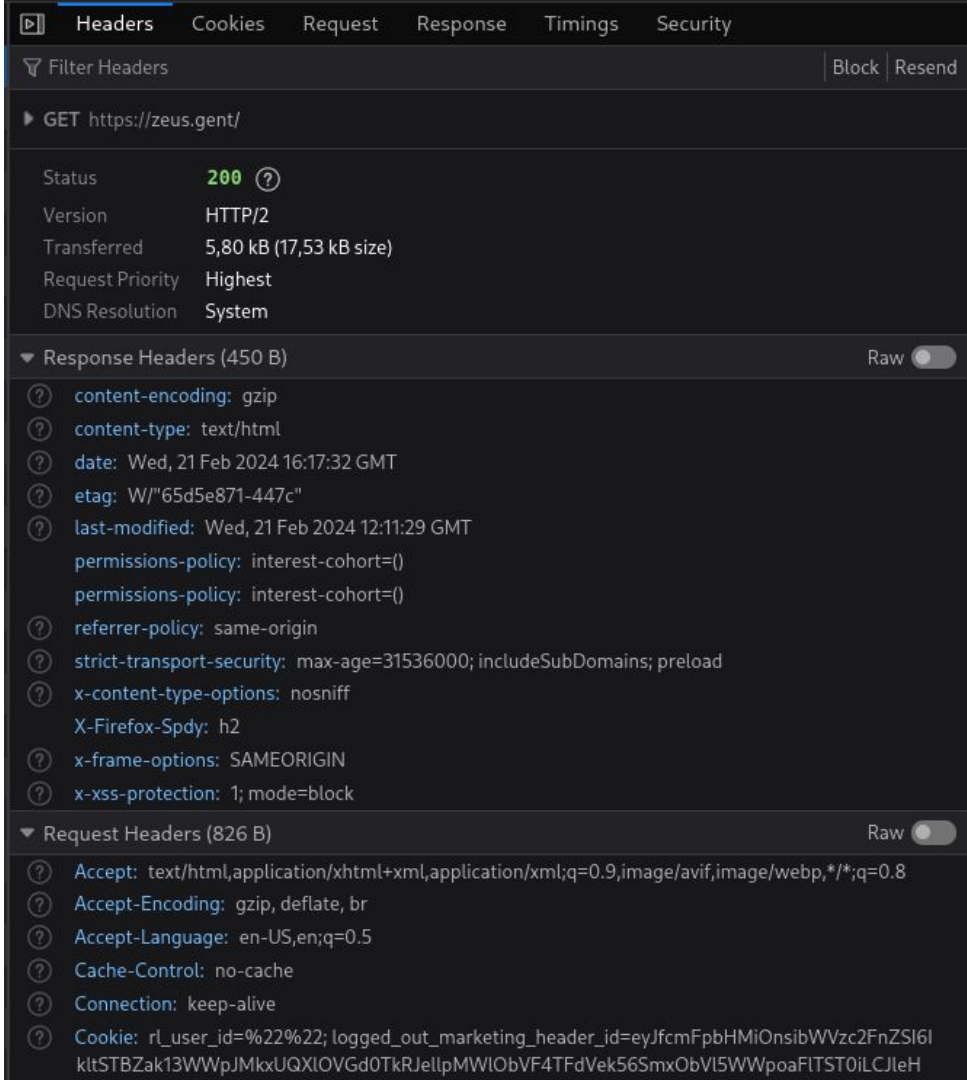
Filter URLs | All | HTML | CSS | JS | XHR | Fonts | Image

Status	Method	Domain	File	Initiator	Type
200	GET	zeus.gent	/	document	html
200	GET	zeus.gent	main.css	stylesheet	css
200	GET	cdnjs.cloudflare.com	all.min.css	stylesheet	css
200	GET	zinc.zeus.gent	/	img	svg
200	GET	zeus.gent	gamification.js	script	js
200	GET	zeus.gent	search.js	script	js
🚫	GET	stats.zeus.gent	tracker.js	/:1 (script)	
200	GET	gamification.zeus.gent	top4.json	gamification.js:1 (xhr)	json
200	GET	pics.zeus.gent	f5t5ZNCF3OquA4HUiik1ELyXTxqXixW4M0deTaEw.jpg	img	jpeg
200	GET	pics.zeus.gent	AsUFApGJa0MAxRDS9grfC950Gn6cTyWAGvDoEFIo.png	img	png
200	GET	pics.zeus.gent	TCxaalBxLGgCxTYYkjqrglgBn5ZRsG05TqRBfp6O.png	img	png

30 requests | 7,83 MB / 7,56 MB transferred | Finish: 1,20 min | DOMContentLoaded: 332 ms | load: 3,21 s

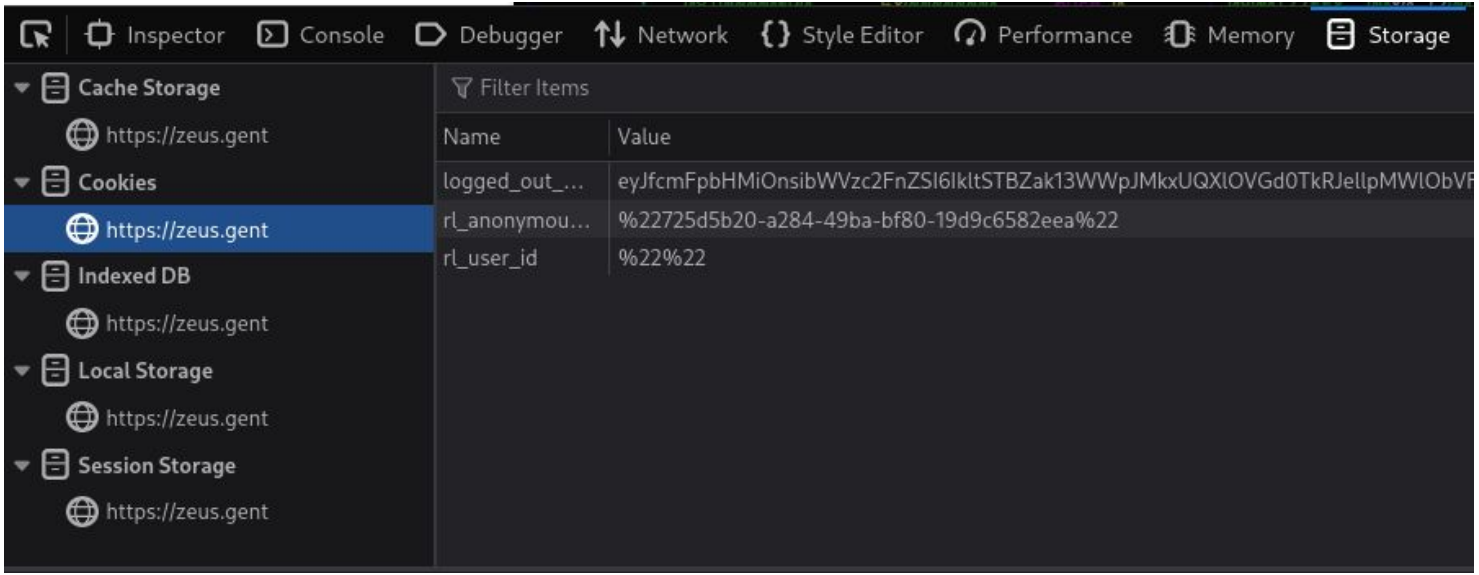
Console - Network - Requests

- Informatie over requests
- Status
- Headers
  - Informatie over request en response
  - Soms nuttig
- Cookies



Console - Storage

- Cookies
  - Waarden bekijken (en veranderen)
- Local storage (en varianten)



Web - Challenge

onotes - 3 flags

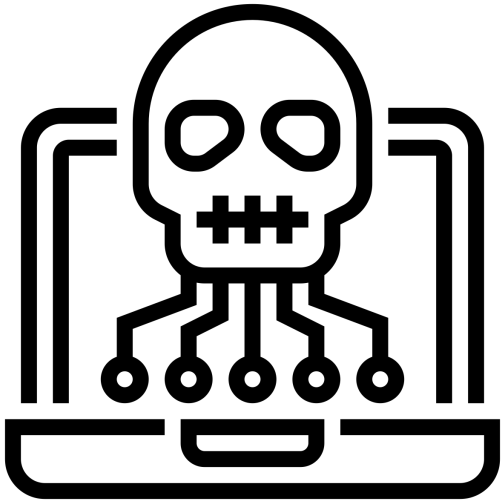
Browser naar IP: http://10.2.2.175:5000

Reverse engineering / Binary exploitation

Begrijpen wat een programma doet (met of zonder code)

Bugs vinden

Bugs gebruiken



RE/BE - Strings

zoekt strings in gelijk welke files

idee krijgen van wat het is

flags?

grep

```
~/c/r/intro_hacking_ctf/reversing > on git main ?1 > strings strings_example
/lib64/ld-linux-x86-64.so.2
*et(
__cxa_finalize
__libc_start_main
puts
printf
libc.so.6
GLIBC_2.2.5
GLIBC_2.34
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
plopkoek
CTF{1_h4v3_b33n_str1ng3d}
;*3$"
GCC: (GNU) 13.2.0
.B#>M$#=1
Lu=/
../sysdeps/x86_64/start.S
/builddir/glibc-2.38/csu
GNU AS 2.41
```

```
~/c/repos/intro_hacking_ctf/reversing > on git main ?1 > strings strings_example | grep -E '[[:alpha:]]+{[^}]+}'
CTF{1_h4v3_b33n_str1ng3d}
```

RE/BE - Assembly

Compiler:

Code ↠ binary

binary gelezen als assembly

Makkelijker om te begrijpen

```
#include <stdio.h>

int main() {
    int num = 0;
    char buf[10];

    printf("Name: ");
    scanf("%s", &buf);

    if (num > 0) {
        printf("Ohno\n");
        printf("%d", num);
    }

    printf("Hello %s!", buf);
}
```

```
                        ****************************************************************
                        *                          FUNCTION                            *
                        ****************************************************************
                        undefined main()
     undefined            AL:1           <RETURN>
     undefined4           Stack[-0xc]:4  local_c


     undefined1           Stack[-0x16]:1 local_16
                        main                                            XREF[4]:

00401136 55              PUSH        RBP
00401137 48 89 e5        MOV         RBP,RSP
0040113a 48 83 ec 10     SUB         RSP,0x10
0040113e c7 45 fc        MOV         dword ptr [RBP + local_c],0x0
         00 00 00 00
00401145 bf 04 20        MOV         EDI,s_Add_number:_00402004
         40 00
0040114a b8 00 00        MOV         EAX,0x0
         00 00
0040114f e8 dc fe        CALL        <EXTERNAL>::printf
         ff ff
00401154 48 8d 45 f2     LEA         RAX=>local_16,[RBP + -0xe]
00401158 48 89 c6        MOV         RSI,RAX
0040115b bf 11 20        MOV         EDI,DAT_00402011
         40 00
00401160 b8 00 00        MOV         EAX,0x0
         00 00
00401165 e8 d6 fe        CALL        <EXTERNAL>::__isoc99_scanf
         ff ff
0040116a 83 7d fc 00     CMP         dword ptr [RBP + local_c],0x0
0040116e 7e 23           JLE         LAB_00401193
00401170 bf 14 20        MOV         EDI,DAT_00402014
         40 00
00401175 b8 00 00        MOV         EAX,0x0
         00 00
0040117a e8 b1 fe        CALL        <EXTERNAL>::printf
         ff ff
0040117f 8b 45 fc        MOV         EAX,dword ptr [RBP + local_c]
00401182 89 c6           MOV         ESI,EAX
00401184 bf 18 20        MOV         EDI,DAT_00402018
```

RE/BE - Ghidra

Reverse engineering tools

Binary => (leesbare) assembly => decompile

```
undefined8 main(void)

{
  undefined local_16 [10];
  uint local_c;

  local_c = 0;
  printf("Name: ");
  __isoc99_scanf(&DAT_0040200b,local_16);
  if (0 < (int)local_c) {
    puts("Ohno");
    printf("%d",(ulong)local_c);
  }
  printf("Hello %s!",local_16);
  return 0;
}
```

```
                        *************************************************************
                        *                          FUNCTION
                        *************************************************************
                        undefined main()
     undefined           AL:1           <RETURN>
     undefined4          Stack[-0xc]:4  local_c


     undefined1          Stack[-0x16]:1 local_16
                        main                                                    XR

00401136 55              PUSH        RBP
00401137 48 89 e5        MOV         RBP,RSP
0040113a 48 83 ec 10     SUB         RSP,0x10
0040113e c7 45 fc        MOV         dword ptr [RBP + local_c],0x0
         00 00 00 00
00401145 bf 04 20        MOV         EDI,s_Add_number:_00402004
         40 00
0040114a b8 00 00        MOV         EAX,0x0
         00 00
0040114f e8 dc fe        CALL        <EXTERNAL>::printf
         ff ff
00401154 48 8d 45 f2     LEA         RAX=>local_16,[RBP + -0xe]
00401158 48 89 c6        MOV         RSI,RAX
0040115b bf 11 20        MOV         EDI,DAT_00402011
         40 00
00401160 b8 00 00        MOV         EAX,0x0
         00 00
00401165 e8 d6 fe        CALL        <EXTERNAL>::__isoc99_scanf
         ff ff
0040116a 83 7d fc 00     CMP         dword ptr [RBP + local_c],0x0
0040116e 7e 23           JLE         LAB_00401193
00401170 bf 14 20        MOV         EDI,DAT_00402014
         40 00
00401175 b8 00 00        MOV         EAX,0x0
         00 00
0040117a e8 b1 fe        CALL        <EXTERNAL>::printf
         ff ff
0040117f 8b 45 fc        MOV         EAX,dword ptr [RBP + local_c]
00401182 89 c6           MOV         ESI,EAX
00401184 bf 18 20        MOV         EDI,DAT_00402018
```

RE/BE - Stack (overflow)

Opslag van variabelen

In volgorde van uitvoering

scanf schrijft alle output naar buffer

11 chars => overschrijft num

=> num =/= 0

```c
#include <stdio.h>

int main() {
    int num = 0;
    char buf[10];

    printf("Name: ");
    scanf("%s", &buf);

    if (num > 0) {
        printf("Ohno\n");
        printf("%d", num);
    }

    printf("Hello %s!", buf);
}
```

Andere tools

- GDB: GNU Project Debugger
- pwntools
  - Veel tools voor binary exploitation
  - integratie met GDB
- Objdump
- Hexedit

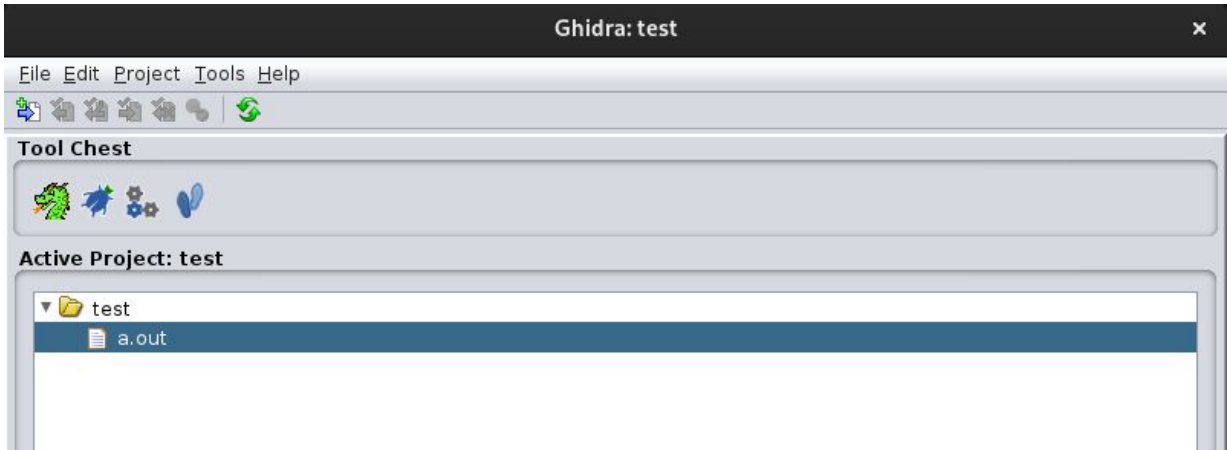
RE/BE - Challenge

buf.c - 1 flag

ono.c - 1 flag

http://10.2.2.175:8000/

Ghidra:
Maak project
Druk op draak icoon
(~animatie~)
Sleep binary op Ghidra



Mobile

Mostly Android APK's - IOS is very rare

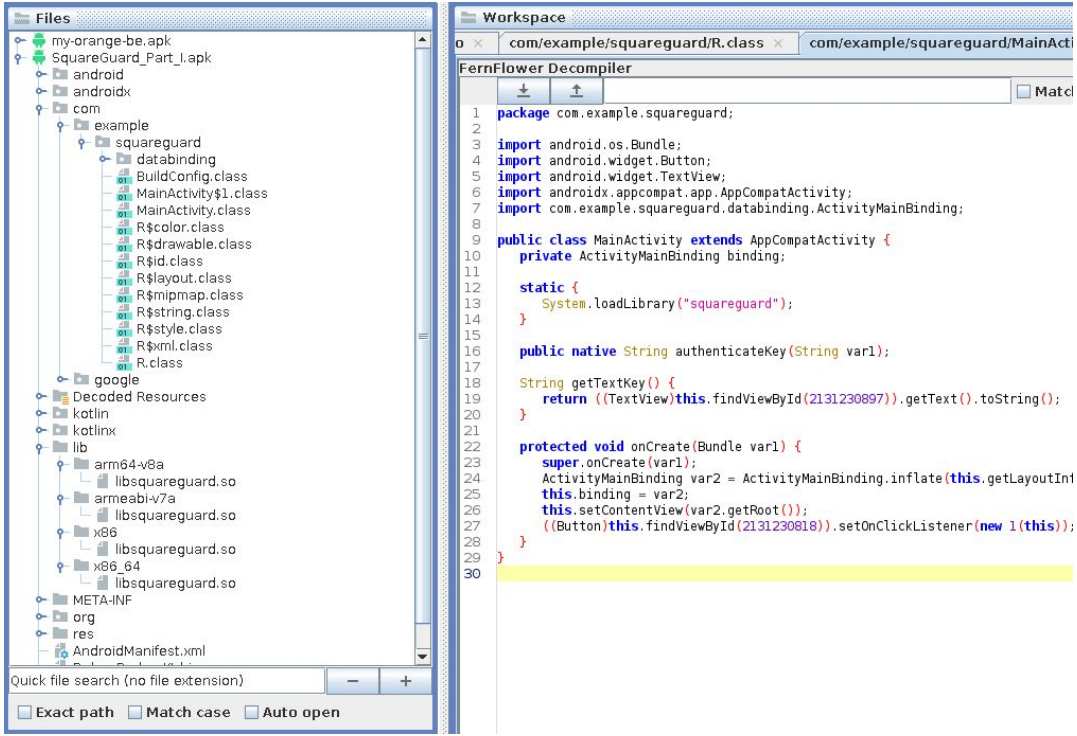
Languages:

- Java
- Kotlin
- Dart

APKs are just zip files. Use a decompiler on the final files.

Mobile - Native Libraries

Sometimes native libraries are used ↠ regular reversing techniques



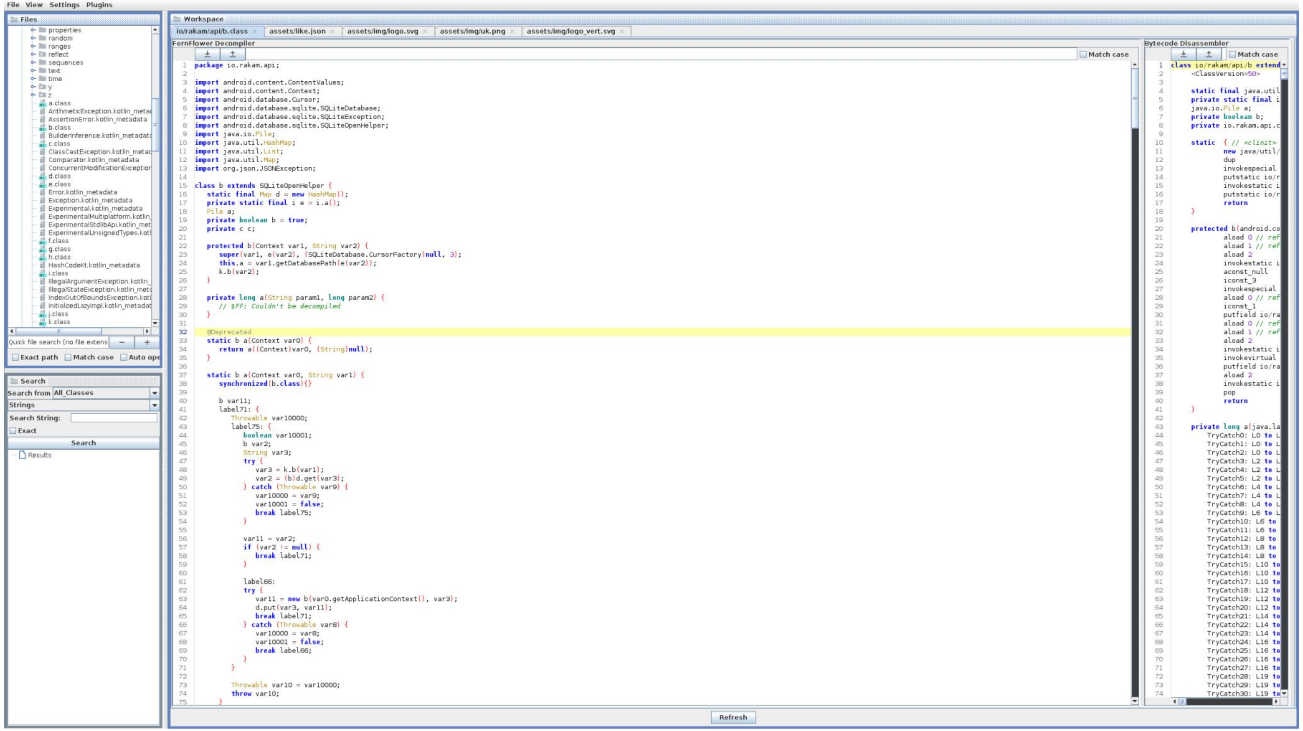
Mobile - Bytecodeviewer

Jar/Apk viewer

Multiple Decompilers

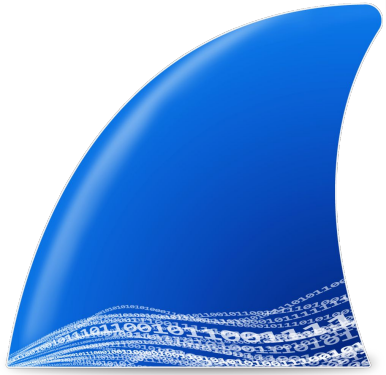
(recompiling)

https://github.com/Konloch/bytecode-viewer



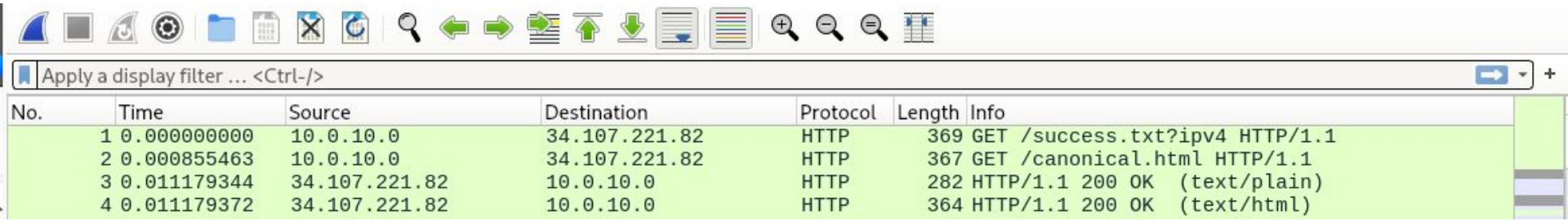
Forensics

- Verstoppen van data in een ander bestand (Steganography)
- Kijken naar inhoud van files (niet alleen interpretatie ervan)
  - metadata in foto's
  - verstopte data in pdf's
- Network traces (wireshark)
  - TCP, UDP, HTTP



Forensics - Wireshark

- pcap bestand
  - bevat de data over een connectie (bv wifi)
  - kan veel protocollen begrijpen: HTTP, TCP, UDP, ...



Forensics - Wireshark

Interpretatie van data

```
Frame 8: 367 bytes on wire (2936 bits), 367
Ethernet II, Src: Intel_0e:11:ef (3c:6a:a7:
Internet Protocol Version 4, Src: 10.0.10.6
Transmission Control Protocol, Src Port: 37
Hypertext Transfer Protocol
  GET /canonical.html HTTP/1.1\r\n
  Host: detectportal.firefox.com\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_6
  Accept: */*\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Cache-Control: no-cache\r\n
  Pragma: no-cache\r\n
  DNT: 1\r\n
  Connection: keep-alive\r\n
  \r\n
  [Full request URI: http://detectportal.fi
  [HTTP request 2/2]
  [Prev request in frame: 2]
  [Response in frame: 10]
```

Rauwe data

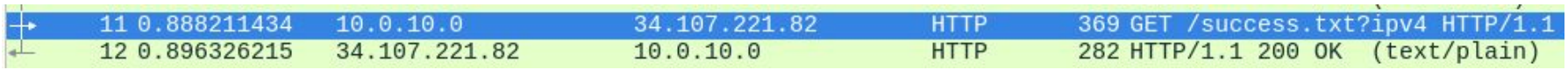
```
0000  4c ed fb 35 22 a8 3c 6a  a7 0e 11 ef 08 00 45 00   L··5"·<j ·····E·
0010  01 61 fa b4 40 00 40 06  2b 25 0a 00 0a 00 22 6b   ·a··@·@· +%····"k
0020  dd 52 92 d4 00 50 49 b3  4c 22 4a 7c ed 70 80 18   ·R···PI· L"J|·p··
0030  01 f5 f6 fa 00 00 01 01  08 0a b8 e7 2c de ba e8   ········ ····,···
0040  cd f8 47 45 54 20 2f 63  61 6e 6f 6e 69 63 61 6c   ··GET /c anonical
0050  2e 68 74 6d 6c 20 48 54  54 50 2f 31 2e 31 0d 0a   .html HT TP/1.1··
0060  48 6f 73 74 3a 20 64 65  74 65 63 74 70 6f 72 74   Host: de tectport
0070  61 6c 2e 66 69 72 65 66  6f 78 2e 63 6f 6d 0d 0a   al.firef ox.com··
0080  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Age nt: Mozi
0090  6c 6c 61 2f 35 2e 30 20  28 58 31 31 3b 20 4c 69   lla/5.0  (X11; Li
00a0  6e 75 78 20 78 38 36 5f  36 34 3b 20 72 76 3a 31   nux x86_ 64; rv:1
00b0  32 32 2e 30 29 20 47 65  63 6b 6f 2f 32 30 31 30   22.0) Ge cko/2010
00c0  30 31 30 31 20 46 69 72  65 66 6f 78 2f 31 32 32   0101 Fir efox/122
00d0  2e 30 0d 0a 41 63 63 65  70 74 3a 20 2a 2f 2a 0d   .0··Acce pt: */*·
00e0  0a 41 63 63 65 70 74 2d  4c 61 6e 67 75 61 67 65   ·Accept- Language
00f0  3a 20 65 6e 2d 55 53 2c  65 6e 3b 71 3d 30 2e 35   : en-US, en;q=0.5
0100  0d 0a 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e   ··Accept -Encodin
0110  67 3a 20 67 7a 69 70 2c  20 64 65 66 6c 61 74 65   g: gzip,  deflate
0120  0d 0a 43 61 63 68 65 2d  43 6f 6e 74 72 6f 6c 3a   ··Cache- Control:
0130  20 6e 6f 2d 63 61 63 68  65 0d 0a 50 72 61 67 6d    no-cach e··Pragm
```

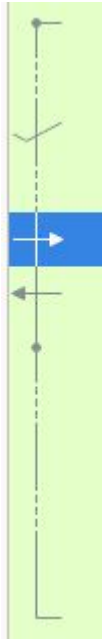
Forensics - HTTP

- Communicatie tussen browser en server
  - https = http maar versleuteld
- Request: welk document?
- Response: inhoud document

GET request ↔ HTTP response

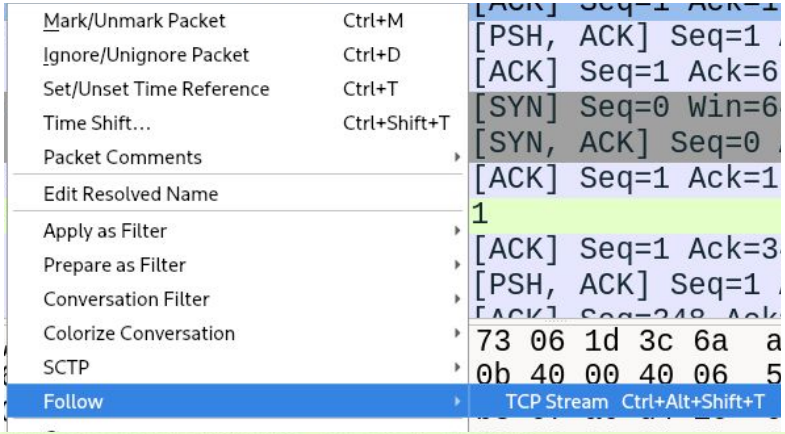
```
HTTP        369 GET /success.txt?ipv4 HTTP/1.1
HTTP        282 HTTP/1.1 200 OK  (text/plain)
```





Forensics - TCP/UDP

- Data over het netwerk
- Kan anders worden geïnterpreteerd (HTTP loopt over TCP)
- Kan gewoon data zijn
- TCP
  - conversatie
  - beloftes over aflevering
- UDP
  - roepen
  - dingen kunnen verloren gaan




```
TCP      74 40376 → 4000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1413192298 TSecr=0 WS=128
TCP      74 4000 → 40376 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1460 SACK_PERM TSval=1833962237 TSecr=1413192298 WS=128
TCP      66 40376 → 4000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1413192417 TSecr=1833962237
TCP      71 40376 → 4000 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=5 TSval=1413193769 TSecr=1833962237
TCP      66 4000 → 40376 [ACK] Seq=1 Ack=6 Win=31872 Len=0 TSval=1833963598 TSecr=1413193769
TCP      74 58766 → 8000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1413357434 TSecr=0 WS=128
TCP      74 8000 → 58766 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1460 SACK_PERM TSval=1834127251 TSecr=1413357434 WS=128
TCP      66 58766 → 8000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1413357442 TSecr=1834127251
```

Forensics - File extensies zijn een leugen (sorry windows)

Veel dingen zijn een zip (probeer dingen te openen met 7zip)

- docx, jar, apk

file command

- kijkt naar inhoud om te bepalen welke file het is

```
> file zeus.wpi
zeus.wpi: Zip archive data, at least v2.0 to extract, compression method=deflate
```

Forensics - Challenge

Wireshark - 2 flags

zeus.wpi - 1 flag

http://10.2.2.175:8000/

Extracurricular:
Andere protocollen in wireshark (ARP)
Crypto in protocollen
Formaat protocollen goed kennen
Checksums
Wifi handshake afluisteren & bruteforce

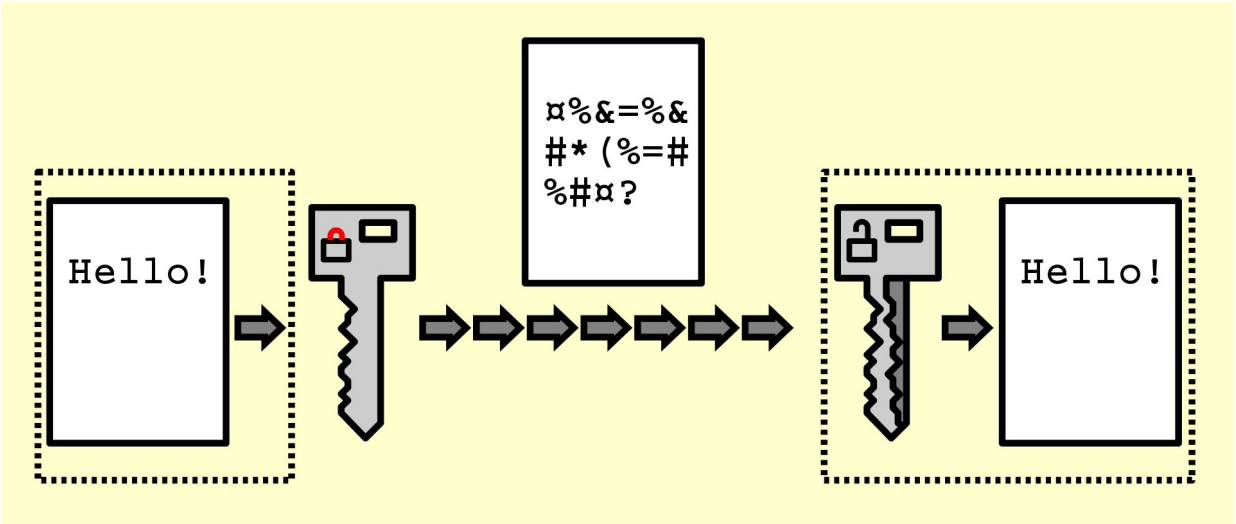
Crypto(graphy)

Versleutelen van informatie

Begrijpen algoritme en fout vinden en gebruiken

- Informatie lekken
- Foute input

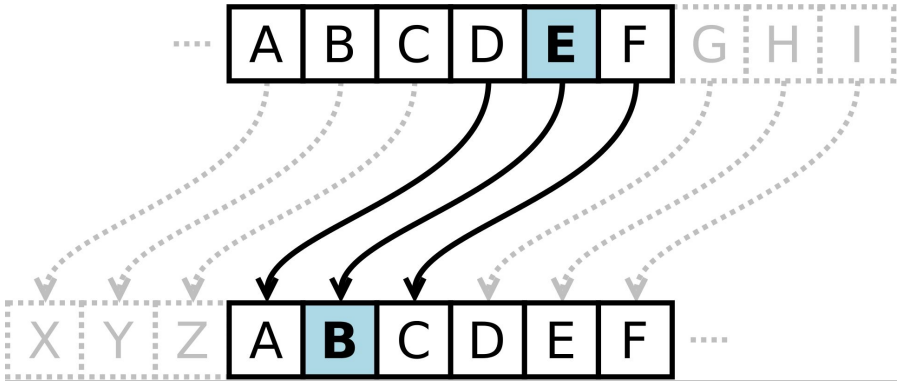
~W~i~s~k~u~n~d~e~

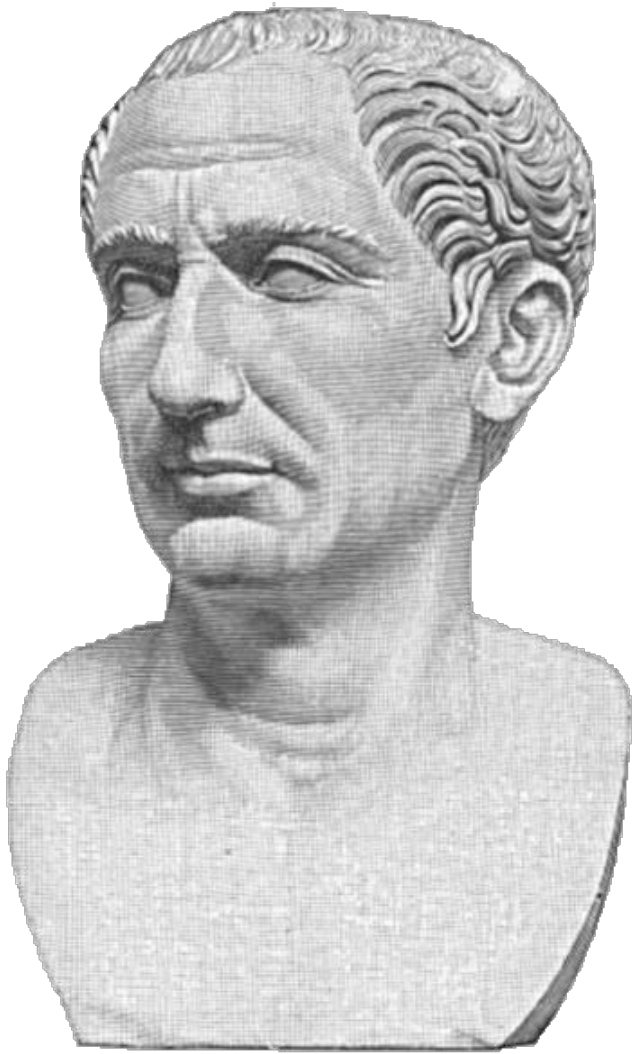


Crypto - Caesar cipher

Elke letter vervangen door de letter x plaatsen verder

Rot13: Caesar cipher met shift = 13





Crypto - XOR ⊕

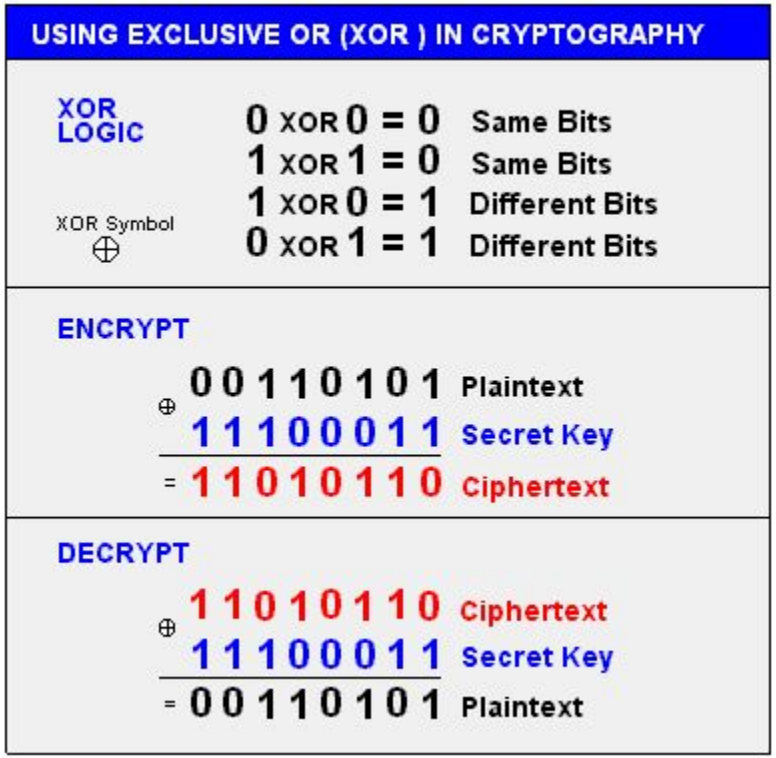
Exclusieve OR functie = ⊕

Volledig reversible:

Text ⊕ Key = Encrypted

Encrypted ⊕ Key = Text

Text ⊕ Encrypted = Key



Crypto - XOR ⊕ (advanced)

Korte keys = slecht

Key repetition

```
Zeus is the sky and thunder god
12312312312312312312312312312311
```

deel input geweten > key lekken?

```
ENCRYPTED
LONGDATAT
HATISLONG
```

elke 10de char is newline

Gekende file header (Magic bytes)

Crypto - Challenge

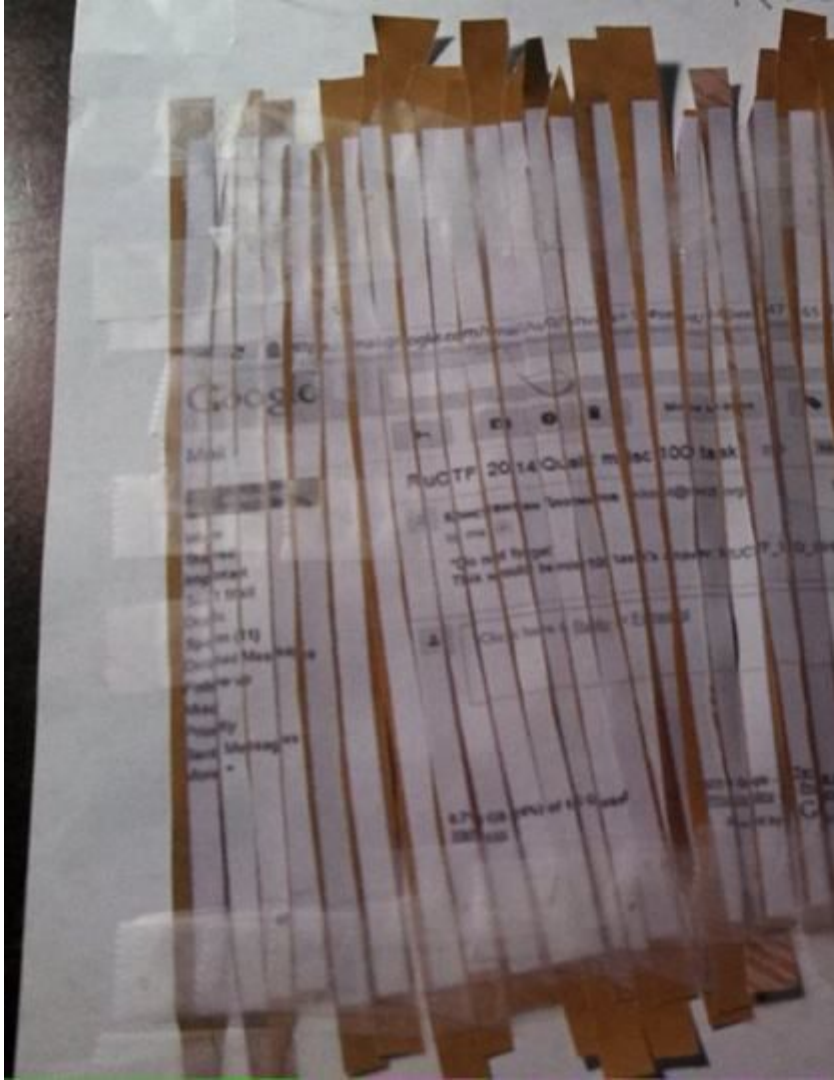
encrypted_flag.txt - 1 flag

flags.txt - 4 flags

Links:
https://www.dcode.fr/en/
https://gchq.github.io/CyberChef/
https://github.com/trou/rsbkb

Andere Categorieën

- OSINT
  - Verzamelen van publieke (open) informatie
- Misc
  - Random challenges
- Programming
  - Programming opdracht (scriptingtalen)
- Hardware
  - Microcontrollers



Next?

Volgende week zeus CTF

PicoCTF

Writeups lezen

Vragen?

Zeus kelder :D

Nu

cscbe@zeus.ugent.be