le challenge

UN TRUC DE GEEKS ?

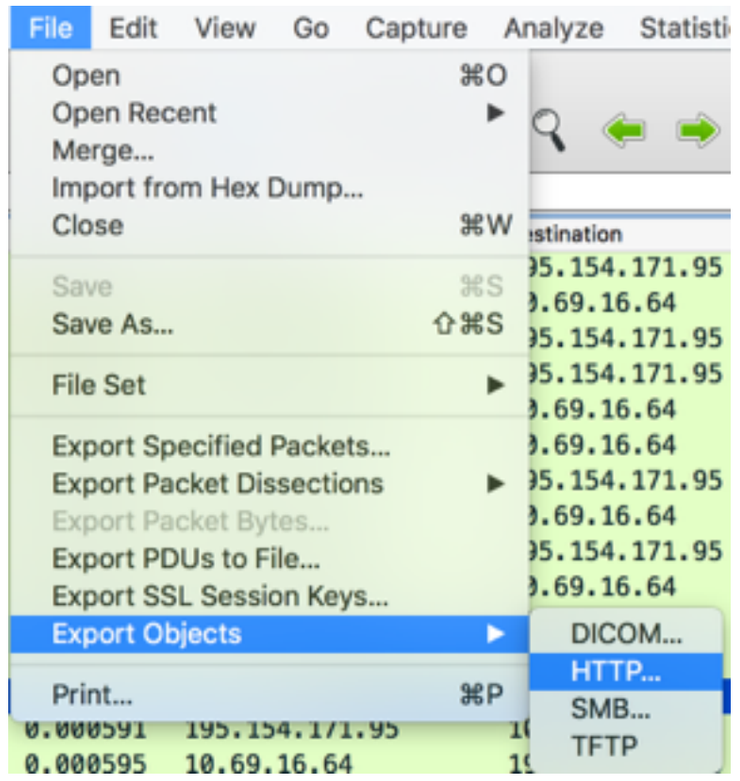
- trouver les adresses mail en sstic.org, preuve de résolution des énigmes
- orienté système et bas niveau (RE, architectures exotiques, formats de fichier, …)

- 2000 téléchargements
- 19 “finishers”
- 4 disqualifiés

- stage3 / ring n’a été résolue que par un unique participant !

TRACE RÉSEAU

- **entrée**: une trace réseau pcap de 50MB
- **analyse**:
  - la trace contient la récupération en HTTP du fichier *challenge.zip*
  - wireshark* n'arrive pas à extraire le fichier

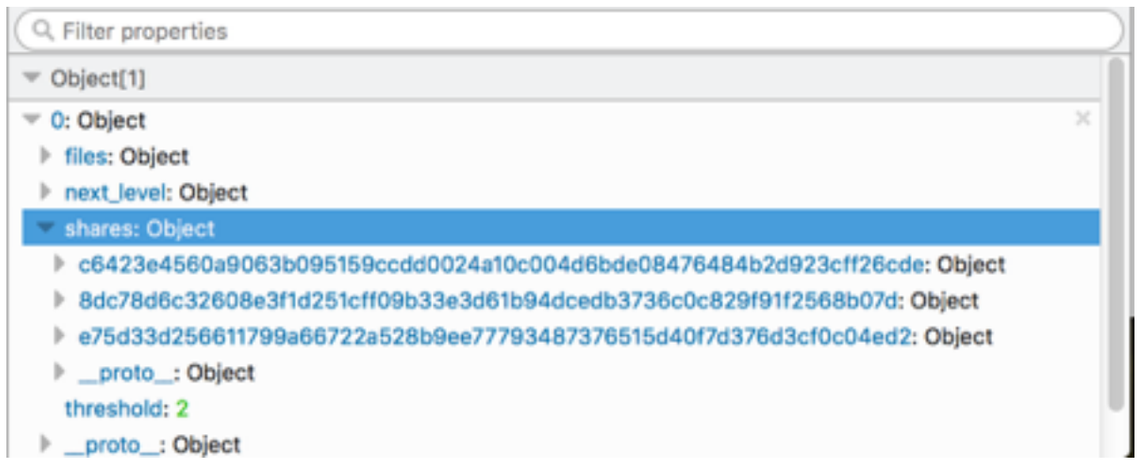


  - tcpick y parvient
  - un fichier *challenge.zip*, que l'on décompresse

LE JEU COMMENCE

- challenge.zip contient un jeu RPGJS
- succession de niveaux, plusieurs énigmes
- pas nécessaire de finir toutes les énigmes, il suffit d'avoir le nombre de points requis

- la console du navigateur permet d'accéder au DOM
- l'analyse du code js permet de détecter comment les clés sont vérifiées
- *shares* contient les SHA256 des clés du niveau



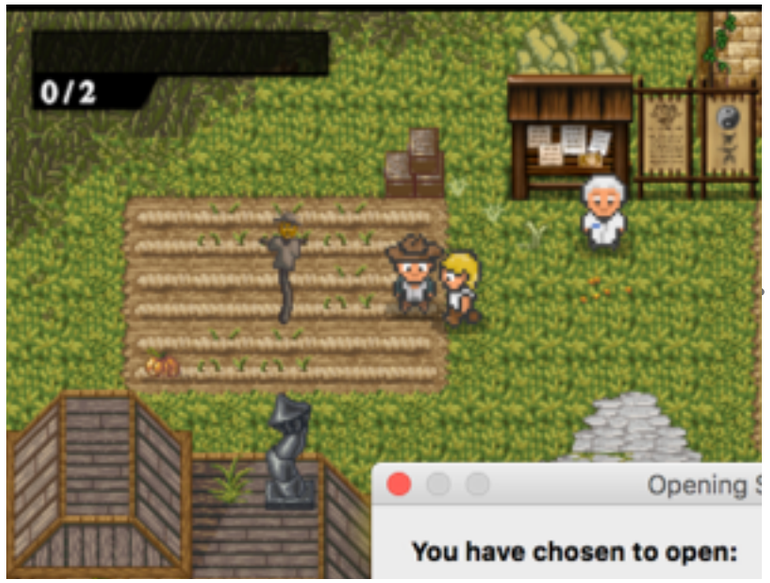
0 / 2

Touches :
[←] [↑] [→] [↓] pour bouger.
[Entrée] pour parler ou passer les dialogues

NIVEAU 1

Chasse aux oeufs

NIVEAU 1 / SOS-FANTOME



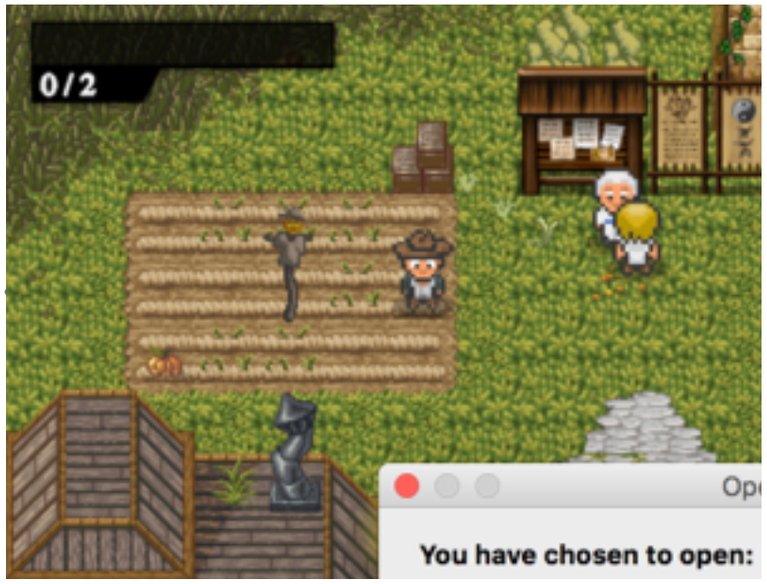
- **entrée**: SOS-Fant0me.pcap
- **analyse**:
  - Gh0st

```
00000000  47 68 30 73 74 4a 00 00  00 e0 00 00 00 78 9c 4b   Gh0stJ.. .....x.K
00000010  53 60 60 98 c3 c0 c0 c0  06 c4 8c 40 bc 41 96 81   S``..... ...@.A..
00000020  81 09 48 33 ac 1a 58 00  72 02 03 23 23 c3 11 4e   ..H3..X. r..##..N
00000030  06 06 ae 94 04 d1 e0 e0  10 4f 67 dd 00 67 43 06   ........ .Og..gC.
00000040  a2 41 39 88 00 00 65 58  5a ef                     .A9...eX Z.
    00000000  47 68 30 73 74 16 00 00  00 01 00 00 00 78 9c 63   Gh0st... .....x.c
    00000010  00 00 00 01 00 01                               ......
    00000016  47 68 30 73 74 16 00 00  00 01 00 00 00 78 9c 53   Gh0st... .....x.S
    00000026  06 00 00 24 00 24                               ...$.$
```

- Performs comprehensive RAT capabilities.
  - Keylogging
  - Mouselogging
  - Disabling the mouse and keyboard
  - Screenshot captures
  - Webcam snapshots
  - Webcam video surveillance
  - Microphone surveillance
  - Downloading and uploading files (to and from) the infected computer
  - Executing files
  - Disabling the screen
  - File listing, process listing
  - Remote shell
  - Remote shutdown/reboot

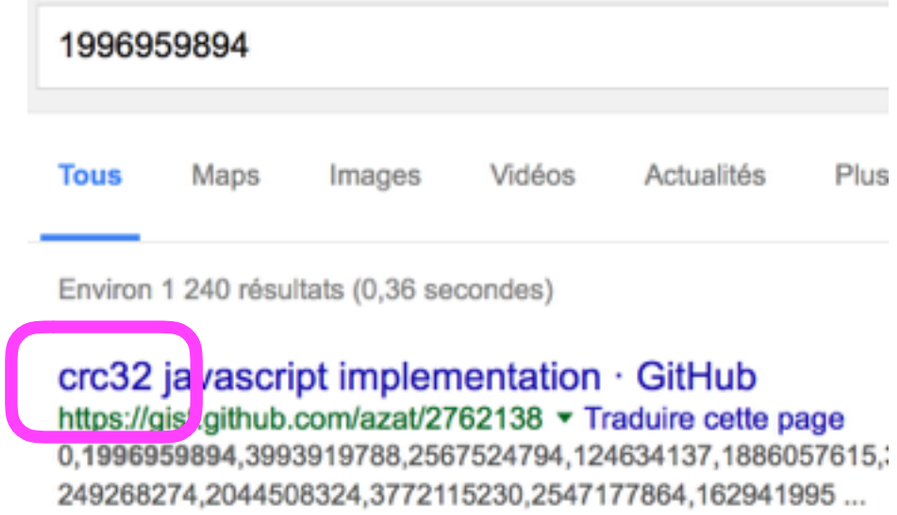
- fichier *solution.zip* et mot de passe sont contenus dans le dialogue

NIVEAU 1 / TI83+



- **entrée**: SSTIC16.8xp
- **analyse**:
  - programme pour TI83+, sous forme de tokens
  - `0xdeadbeef` devient "`11011110101011011011111011101111`"

```
Lbl 1
Input "Entrez le code : ",Z
4294967295->C
0->N
{0,1996959894,3993919788,2567524794,124634137
47,2428444049,498536548,1789927666,4089016648
7,1661365465,4195302755,2366115317,997073096,
06,2898065728,853044451,1172266101,3705015759
4,1594198024,3322730930,2970347812,795835527,
```

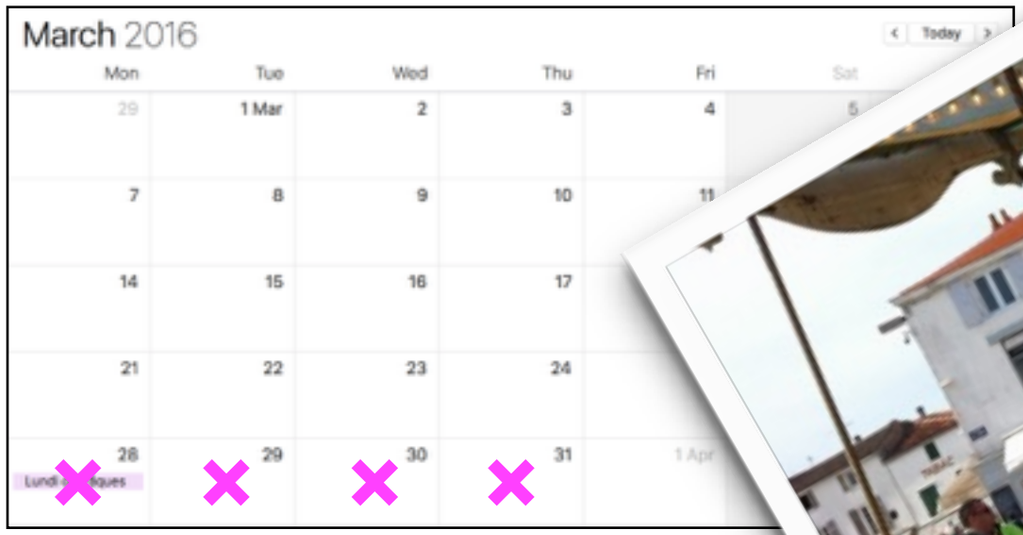


2/2

0/2

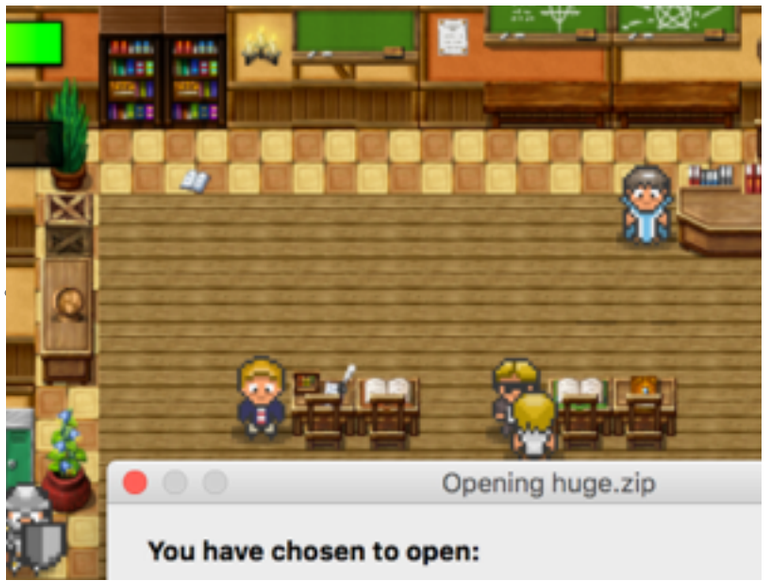
Tu as bien avancé !
Voici une adresse mail pour nous le dire :
UkQhxwnHoZIIKw9lPGK5BNLg@sstic.org

NIVEAU 2

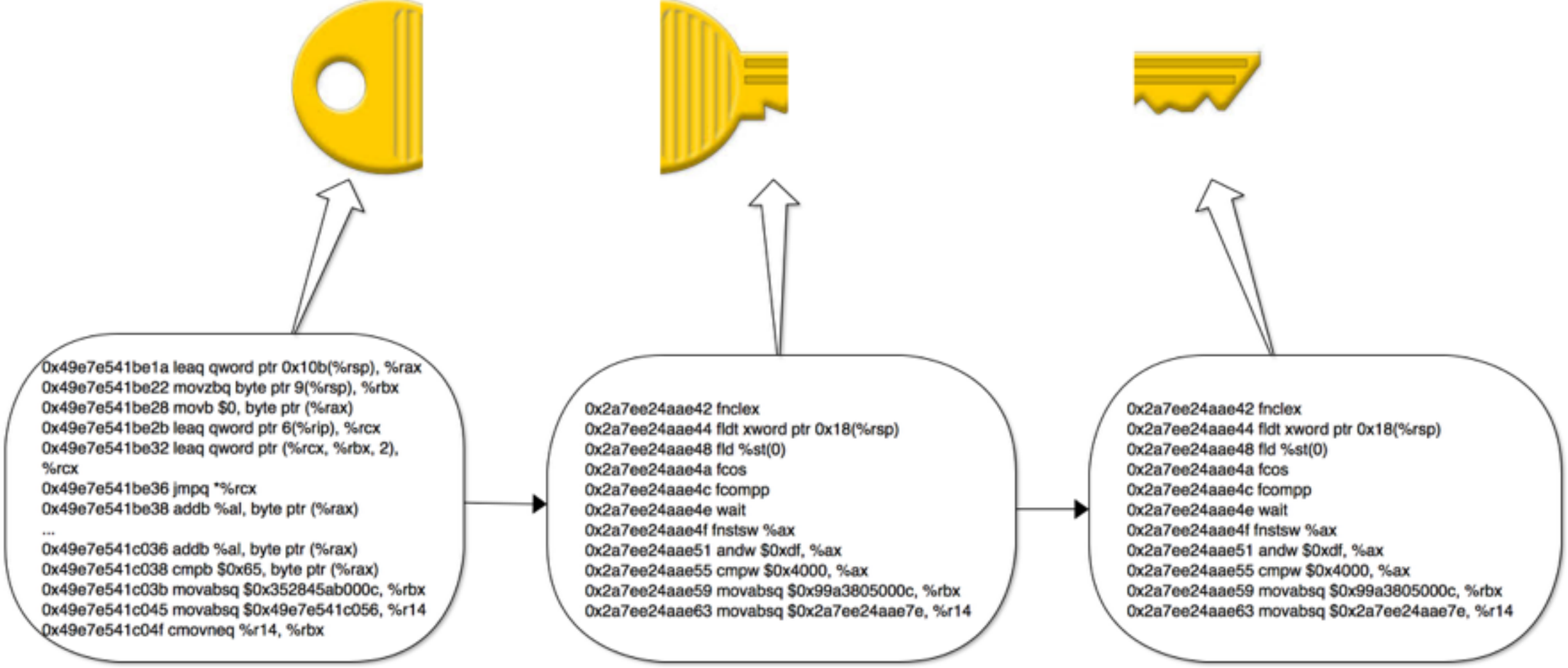


Vacances à l'île de Ré

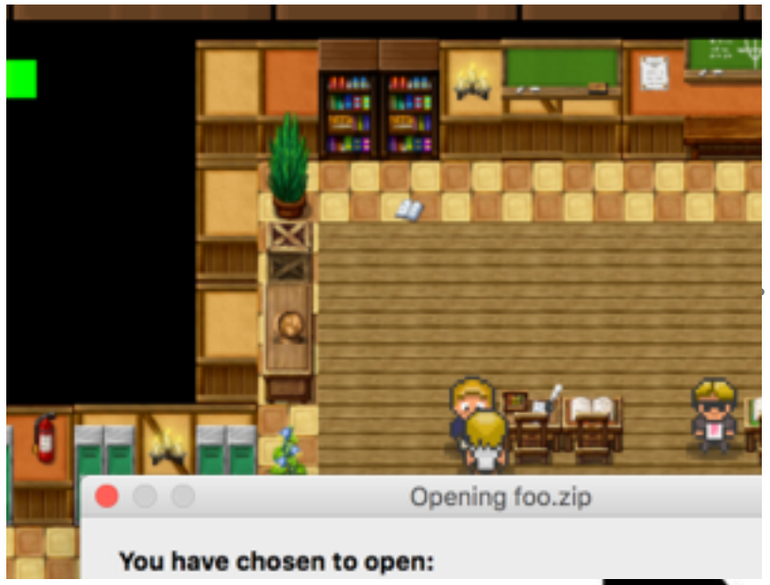
NIVEAU 2 / HUGE



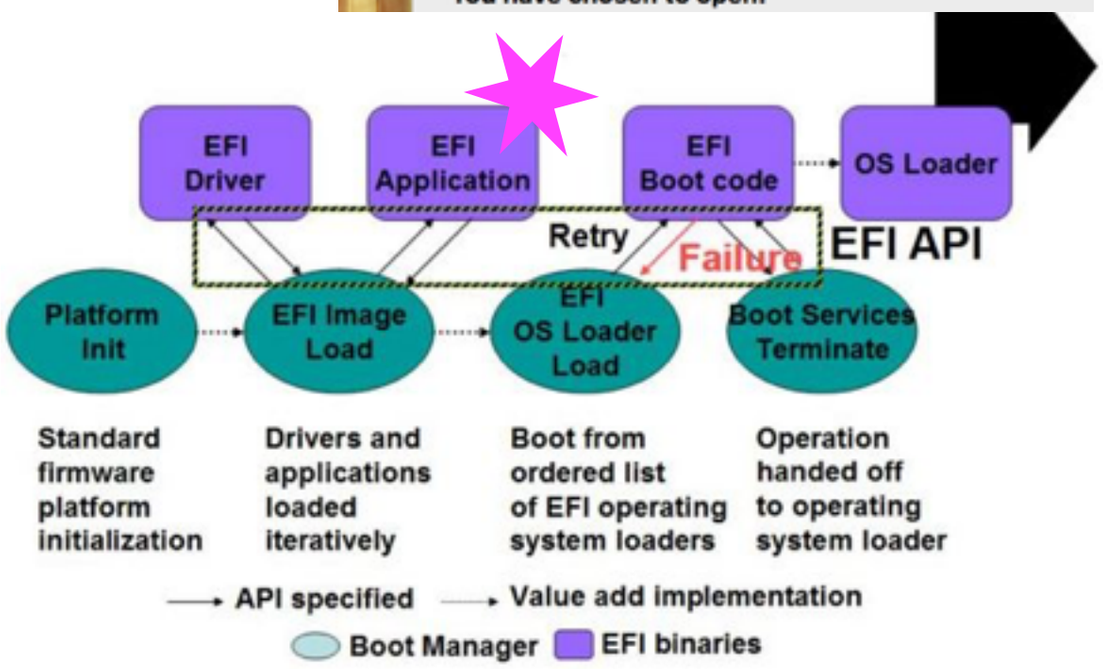
- **entrée**: huge.tar, puis Huge
- **analyse**:
  - huge.tar est une archive de type “sparse”
  - les systèmes de fichier n’offrent pas tous la même taille maximale de fichier !



NIVEAU 2 / EFI



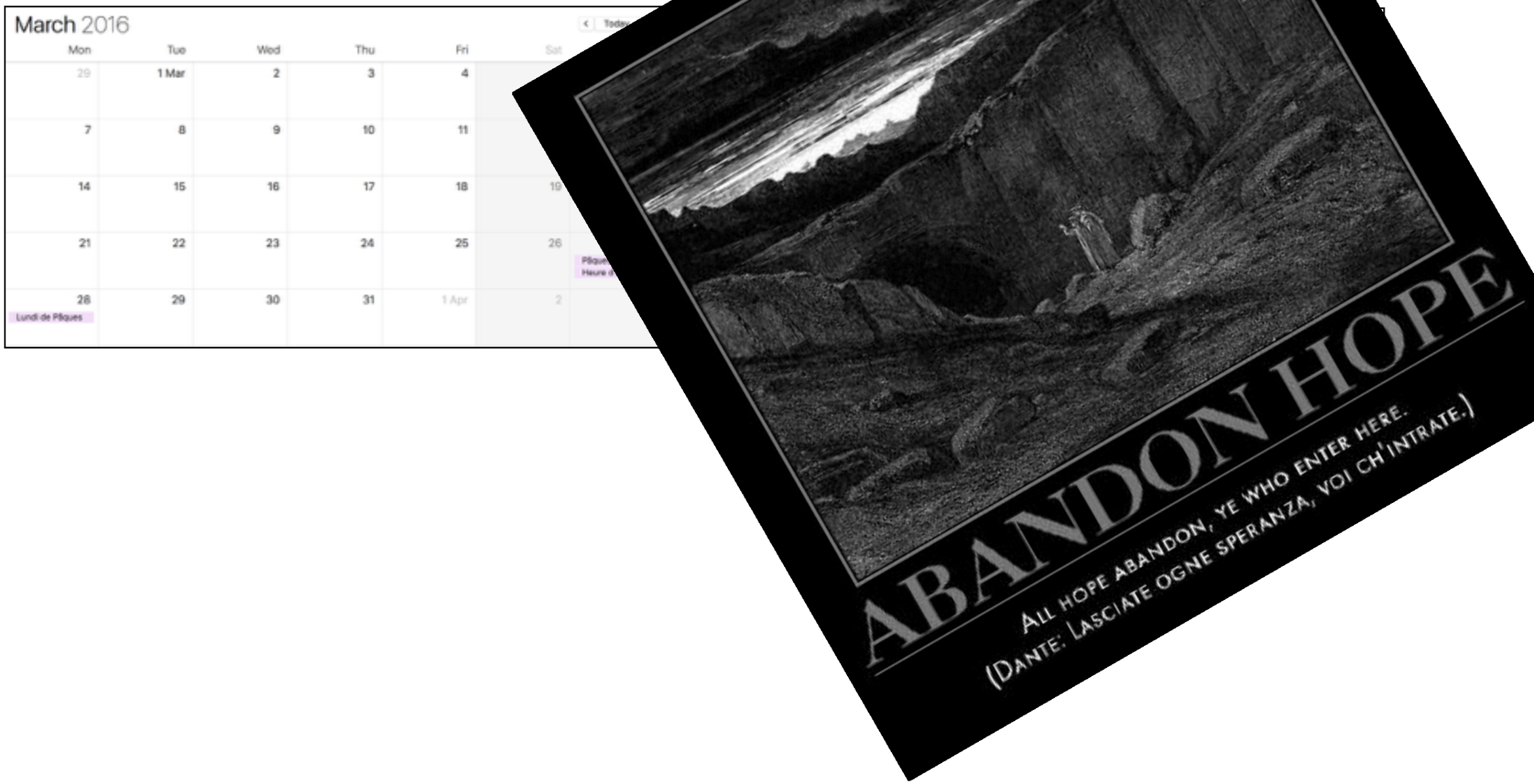
- **entrée**: foo.efi
- **analyse**:
  - module EFI
  - en EFI Byte Code



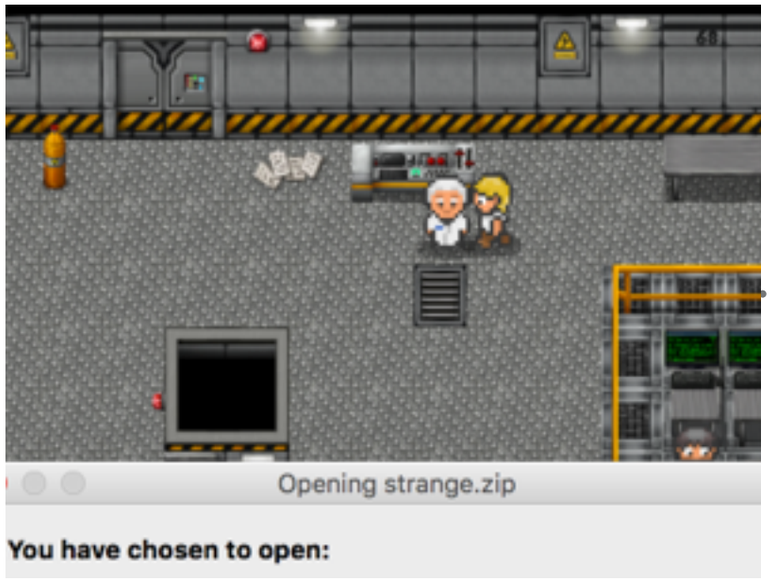
- le secret est protégé
  - via l'utilisation de compression EFI,
  - plus l'utilisation de crypto maison

Tu as bien avancé !
Voici une adresse mail pour nous le dire :
RkrjBeyqFzsQApQhUbPvvTmJ@sstic.org

NIVEAU 3


March 2016
Mon
Tue
Wed
Thu
Fri
Sat
29
1 Mar
2
3
4
7
8
9
10
11
14
15
16
17
18
21
22
23
24
25
26
28
Lundi de Pâques
29
30
31
1 Apr
2
ABANDON HOPE
All hope abandon, ye who enter here.
(Dante: Lasciate ogne speranza, voi ch'intrate.)

NIVEAU 3 / STRANGE



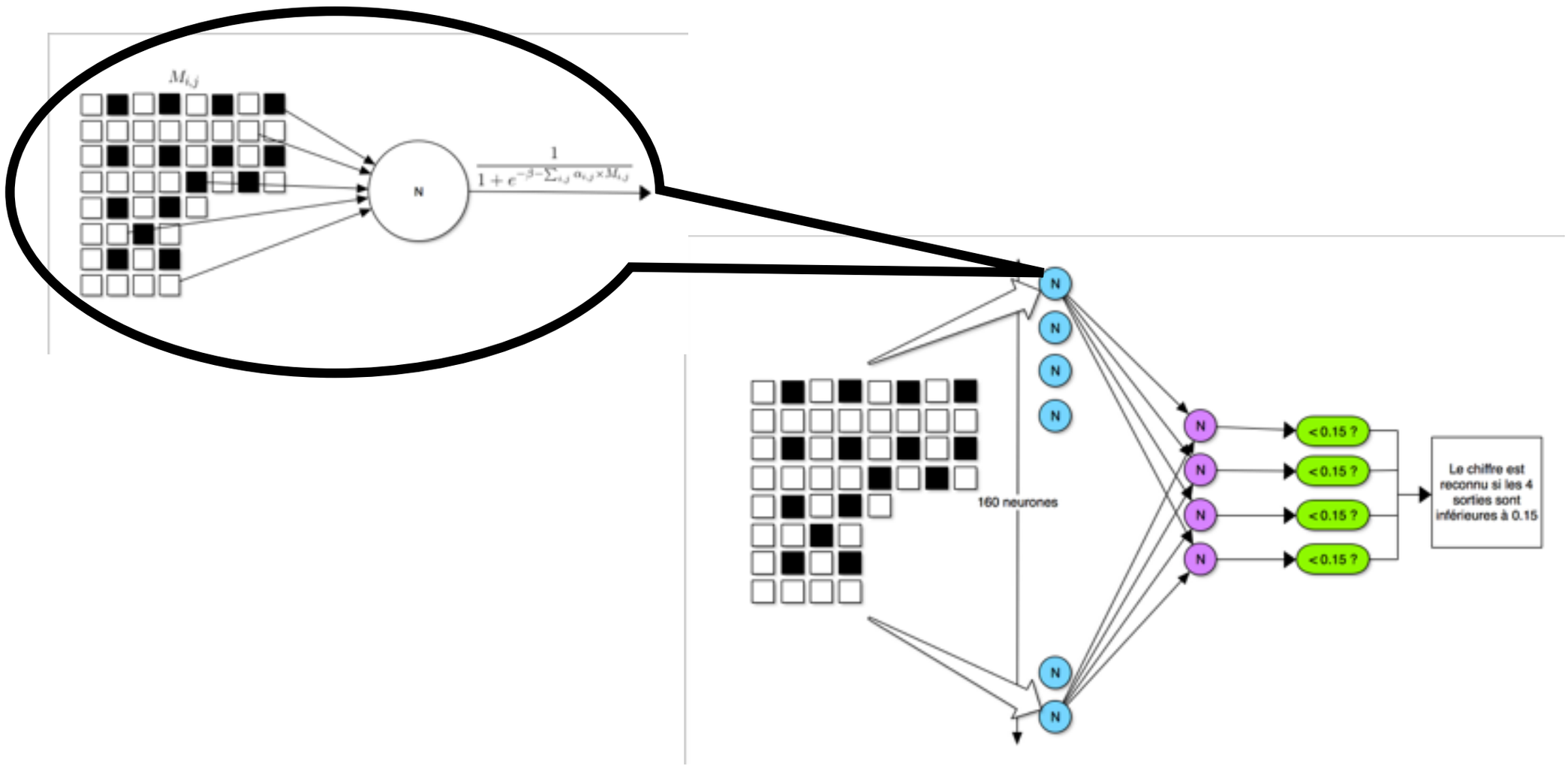
- **entrées**: a.out et 196
- **analyse**:
  - a.out est un binaire ELF **dynamique** pour IA64

```
Relocation section '.rela.IA_64.pltoff' at offset 0x520 contains 10 entries:
  Offset          Info           Type           Sym. Value    Sym. Name + Addend
600000000000f270  000100000081 R_IA64_IPLTLSB    0000000000000000 malloc + 0
600000000000f280  000200000081 R_IA64_IPLTLSB    0000000000000000 memcmp + 0
600000000000f290  000300000081 R_IA64_IPLTLSB    0000000000000000 fgets + 0
600000000000f2a0  000400000081 R_IA64_IPLTLSB    0000000000000000 fread + 0
600000000000f2b0  000500000081 R_IA64_IPLTLSB    0000000000000000 exp + 0
600000000000f2c0  000600000081 R_IA64_IPLTLSB    0000000000000000 printf + 0
600000000000f2d0  000800000081 R_IA64_IPLTLSB    0000000000000000 fopen + 0
600000000000f2e0  000a00000081 R_IA64_IPLTLSB    0000000000000000 sscanf + 0
600000000000f2f0  000c00000081 R_IA64_IPLTLSB    0000000000000000 __libc_start_main + 0
600000000000f300  000d00000081 R_IA64_IPLTLSB    0000000000000000 __gmon_start__ + 0
```

- l'analyse dynamique montre
  - la lecture d'une image du type PGM, de taille 640x20
  - l'image est en noir et blanc

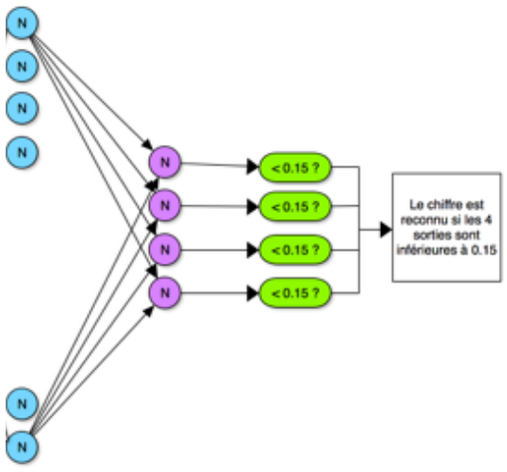
NIVEAU 3 / STRANGE (SUITE)

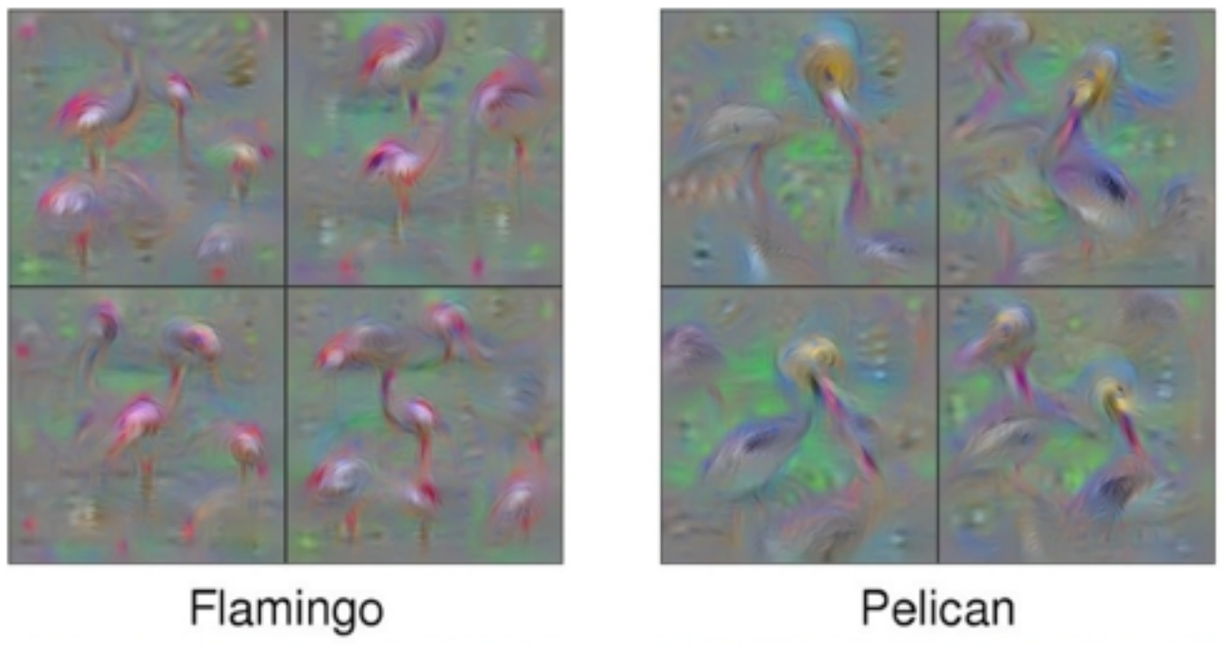
- **analyse:**
  - chaque bloc de 20x20 est analysé par l'appel à 164 fonctions, qui font des opérations similaires



NIVEAU 3 / STRANGE (SUITE)

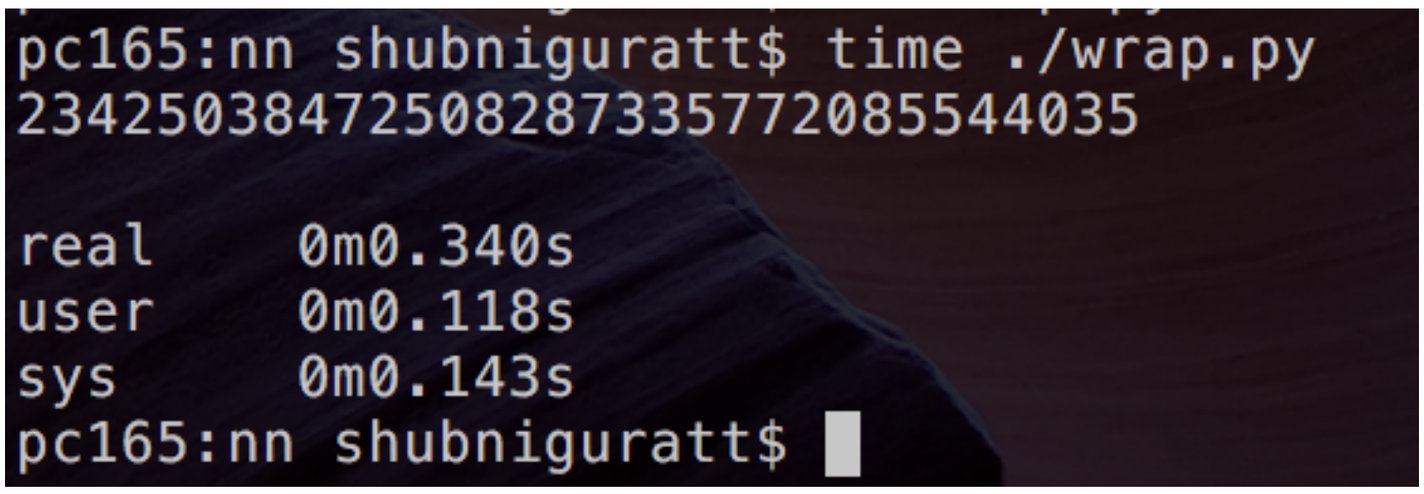
- **analyse:**
  - où trouver les blocs de 20x20 ?
    - utilisation de la base de données du mnist “hand-written digits” ?
    - génération à partir de polices via imagemagick ?
  - déduction à partir des coefficients du réseau neuronal ?



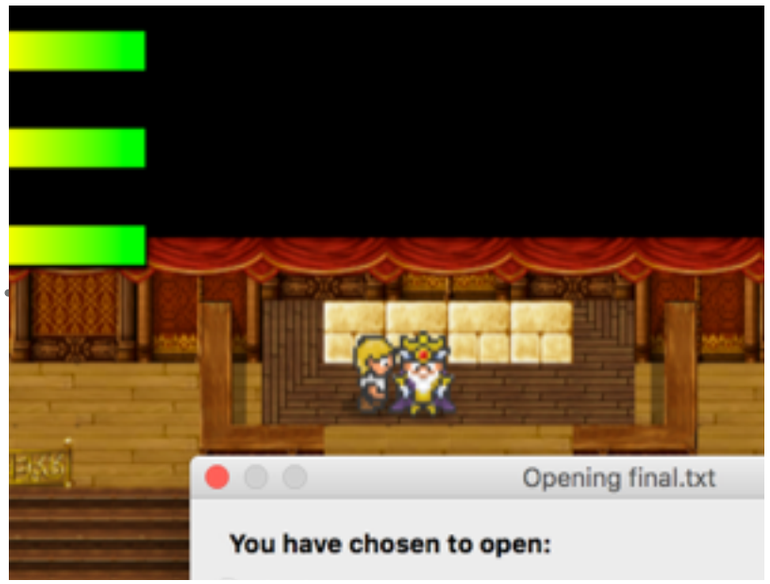


NIVEAU 3 / STRANGE (FIN)

- analyse:
  - dans le fichier 196 en fait !



LA FIN



- **entrée**: final.txt
- **analyse**:
  - le contenu du fichier ressemble à une adresse mail
  - I01p1 y'4qe3553 z41y : 8Y6d5j9Vy88HUGHfGSKsJvqA@ffgvp.bet
  - ffgvp.bet ressemble sstic.org, la ponctuation n'est pas modifiée
  - **ROT13** en shell `tr '[A-Za-z]' '[N-ZA-Mn-za-m]'`
- **sortie**:
  - V01c1 l'4dr3553 m41l : 8L6q5w9Il88UHTUsTFXfWidN@sstic.org

LIENS UTILES

A. http://tcpick.sourceforge.net

B. https://github.com/MITRECND/chopshop

C. http://merthsoft.com/linkguide/ti83+/fformat.html

D. https://www.cemetech.net/sc/

E. https://www.cemetech.net/projects/jstified/

F. https://www.gnu.org/software/tar/manual/html_node/sparse.html

G. https://www.gnu.org/software/gdb/

LIENS UTILES (SUITE)

G. https://fr.wikipedia.org/wiki/XFS

H. http://www.capstone-engine.org

I. http://www.unicorn-engine.org/showcase/

J. http://www.rodsbooks.com/efi-programming/hello.html

K. https://github.com/tianocore/tianocore.github.io

L. https://github.com/tianocore/edk2/tree/master/EmulatorPkg

M. https://github.com/radare/radare2/commits/master/libr/asm/arch/ebc/ebc_disas.c

N. https://packages.debian.org/fr/sid/binutils-multiarch

LIENS UTILES (FIN)

M. http://ski.sourceforge.net

N. http://www.intel.com/content/dam/www/public/us/en/documents/manuals/itanium-architecture-vol-3-manual.pdf

O. http://netpbm.sourceforge.net/doc/libnetpbm.html

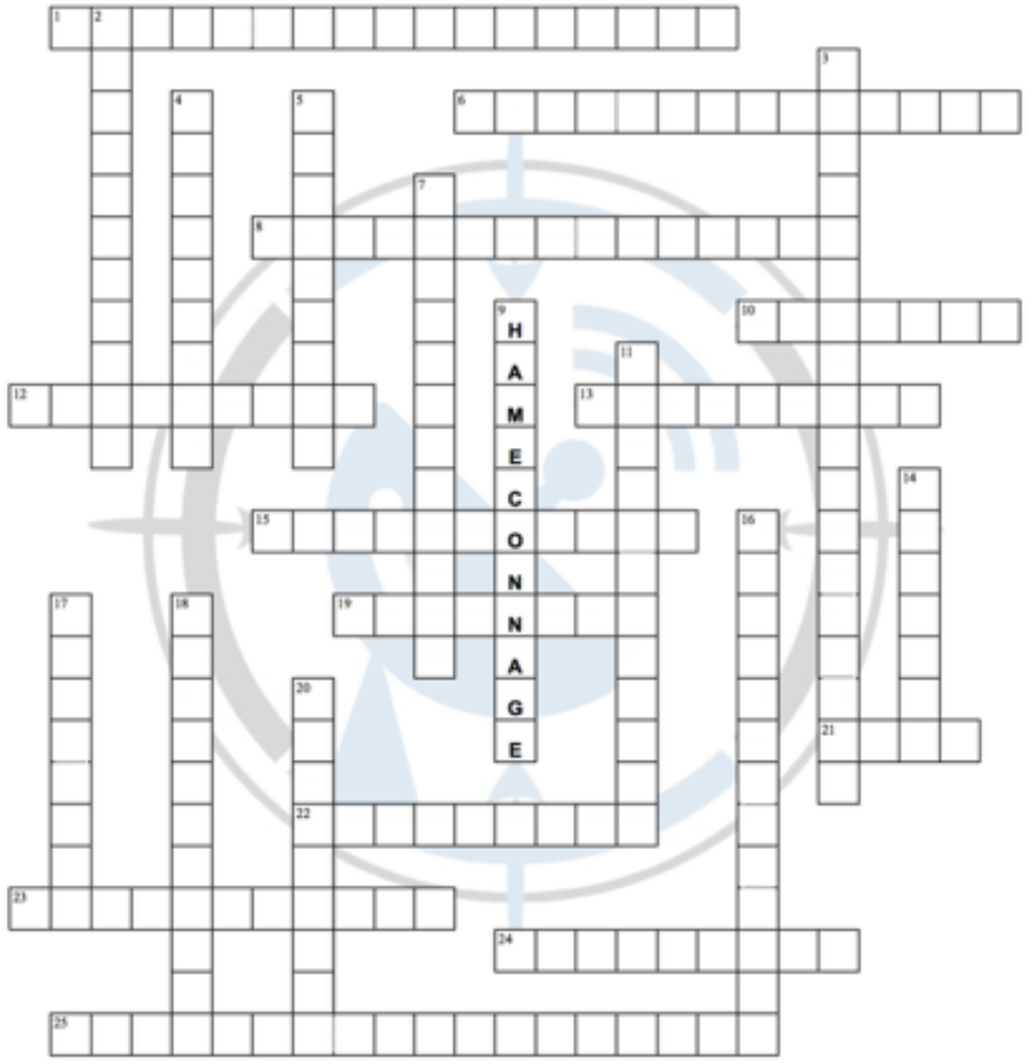
P. http://yann.lecun.com/exdb/mnist/

Q. http://yosinski.com/deepvis

R. https://github.com/yosinski/deep-visualization-toolbox

S. https://en.wikipedia.org/wiki/ROT13

CADEAU POUR LE TRAIN



Horizontal

1. MITM
6. Shellcode
8. Dangling pointer
10. Front office
12. Fuzzing
13. Sinkhole
15. To reverse
19. Hacker
21. BYOD
22. Smartphone
23. J.I.T.
24. Framework
25. URL

Vertical

2. Middleware
3. Heap spraying
4. Hash
5. Cloud computing
7. Random
9. Phishing
11. Backdoor
14. Patch
16. Stack cookie
17. 0-day
18. Cache memory
20. Autre phishing


SSTIC
SYMPOSIUM
SUR LA SÉCURITÉ DES TECHNOLOGIES DE
L'INFORMATION ET DE LA COMMUNICATION