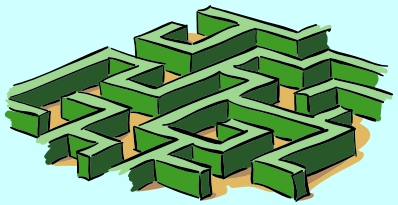
La rétroconception,

quel intérêt pour le RSSI ?

Bruno Kerouanton, CISSP

http://bruno.kerouanton.net

Rump Session
SSTIC 2006 – Rennes, France



Le point de vue de « Monsieur tout le Monde »

C'est interdit !

Législation répressive

Ce n'est pas bien !

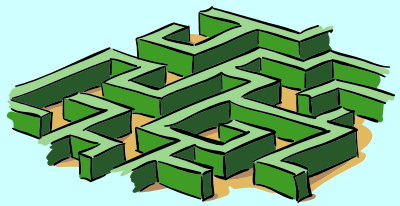
Connotation négative, « hackerish »

C'est pour les *geeks !*

Compétences pointues nécessaires

Ca ne sert à rien !

Fastidieux et sans garantie de résultat



Le point de vue du professionnel de la sécurité

C'est interdit !

Tout dépend de ce que l'on (en) fait

Ce n'est pas bien !

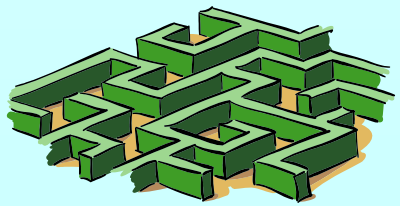
Usage professionnel et éthique possible

C'est pour les *geeks !*

Outils de plus en plus performants / intuitifs

Ca ne sert à rien !

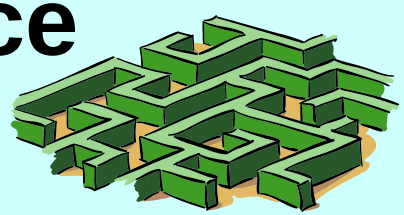
De nombreux usages utiles et légaux



Quelques applications pour le RSSI :

- Écarter les produits mal finalisés et “suspects”
- Évaluer la maintenabilité
- Améliorer la gestion du parc logiciel
- Évaluer rapidement les produits cryptographiques
- Effectuer des audits “live” de plateformes

➔ **Sécurité accrue, contrôle renforcé**



1. Écarter les produits mal finalisés

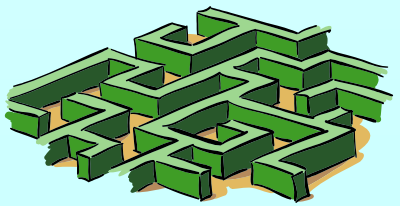
Exemple : Nombreuses références au code source dans la version finale :

```
push    offset asc_6FDC34; "C:/ob/bora-19175/bora/lib/vmdbschema/vm"...
mov     [esi+908h], eax
call    sub_553B80
```

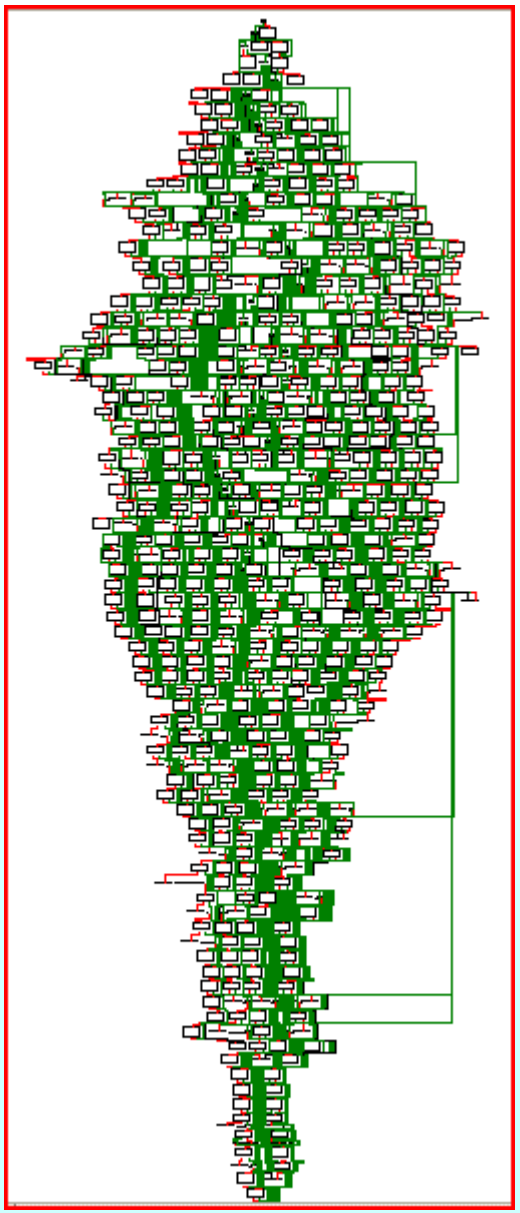
constat : versions de débogage livrées / vendues

- Contrôle qualité au rendez-vous ?
- Pression commerciale ?
- Logiciel fourni plus lent voire instable ?

➔ **Permet une sélection pertinente des produits et solutions**

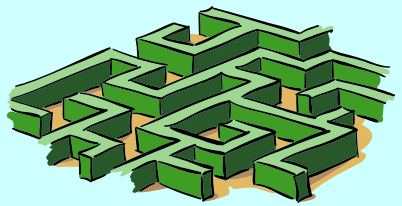


2. Évaluer la maintenabilité



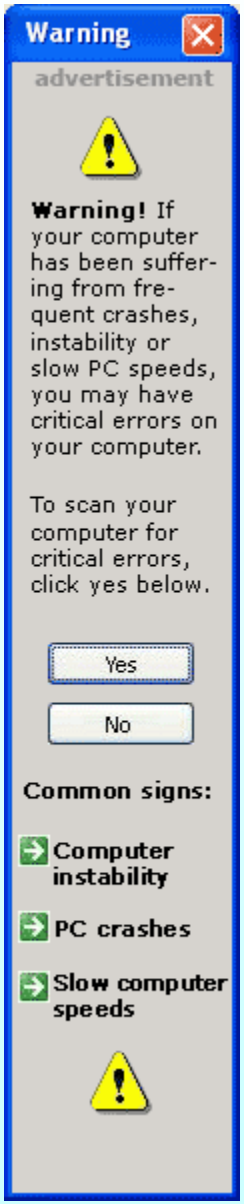
Exemple :
fonctions « fourre-tout ».

**Quid de la pérennité,
de la maintenabilité ?**

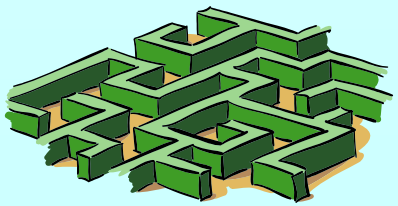


3. Écarter les produits “suspects”

- Spywares, backdoors, etc.

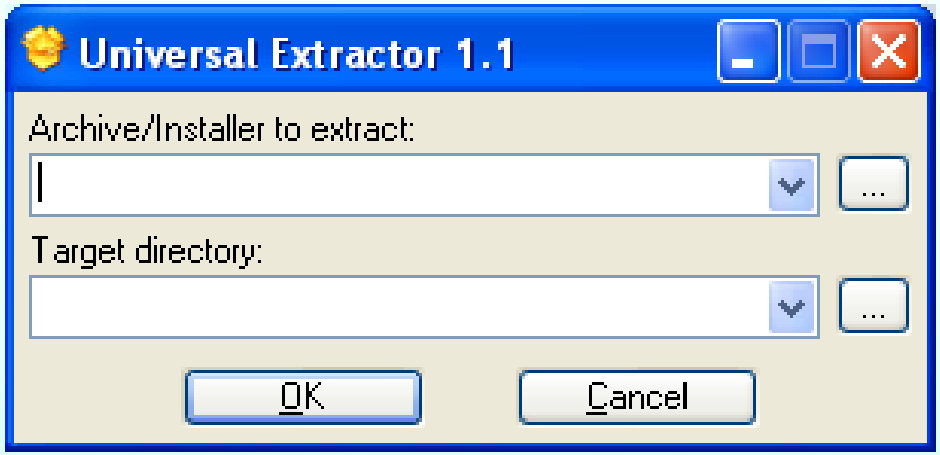


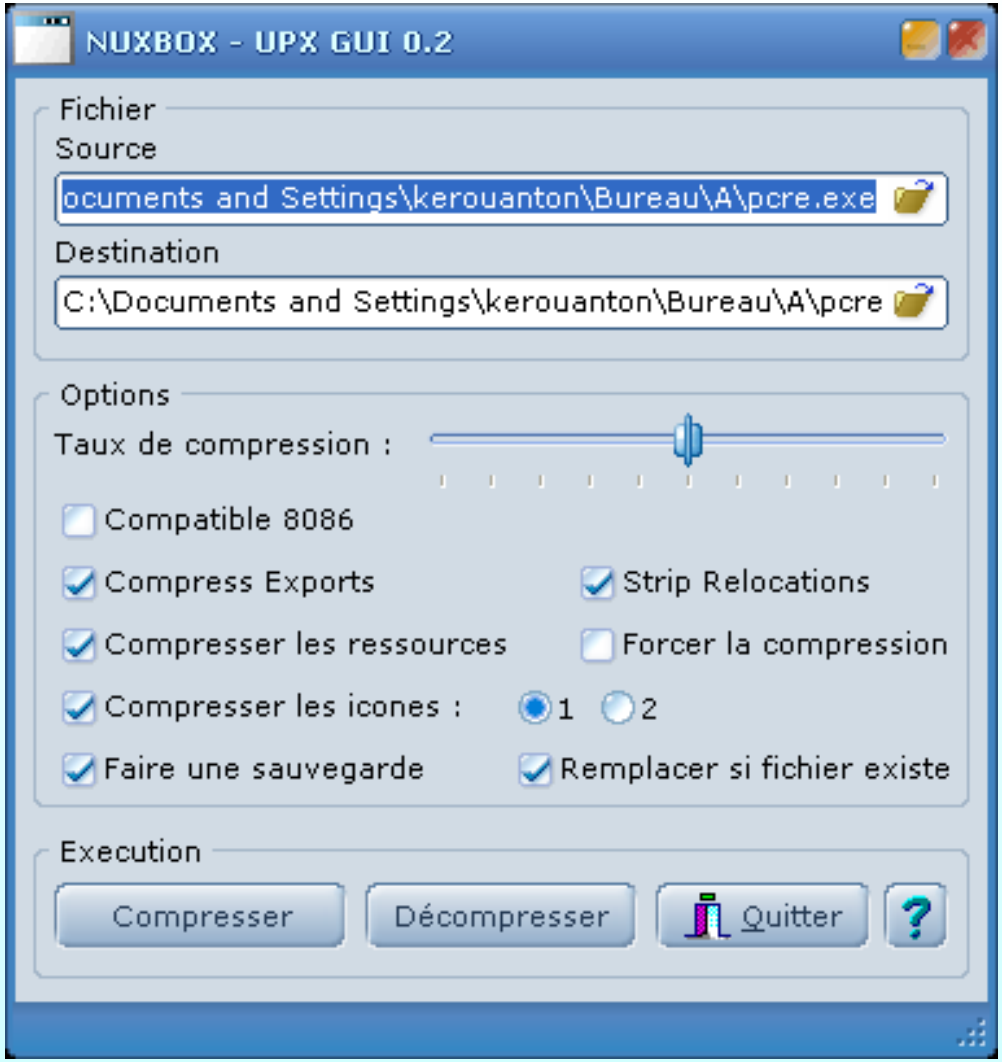
➔ **Renforce la sécurité**



4. Mieux gérer le parc logiciel

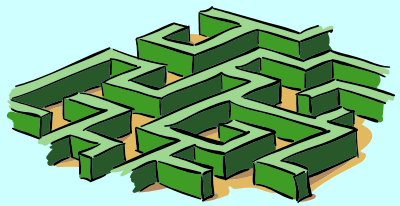
- Repackaging / reparamétrage des applications.





- Optimisation des installations et de la taille des exécutables.

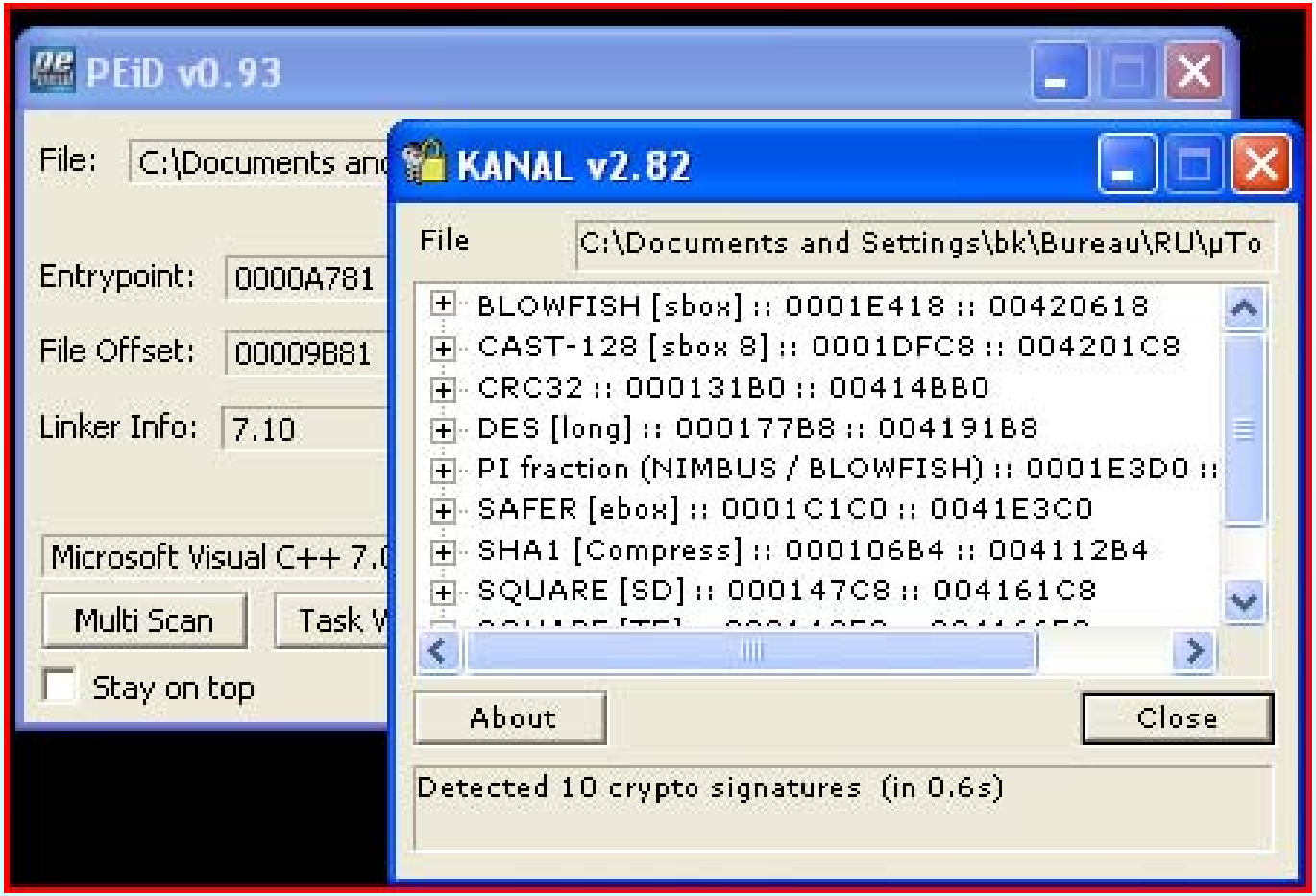
➔ **Bénéfice - pour les administrateurs**
- pour le RSSI



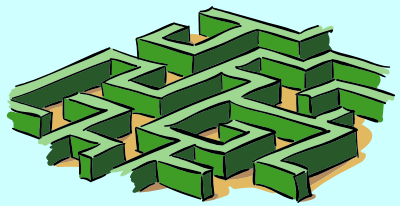
5. Evaluer rapidement les produits cryptographiques

Algorithmes annoncés réellement implantés ?

➔ moins de mauvaises surprises !

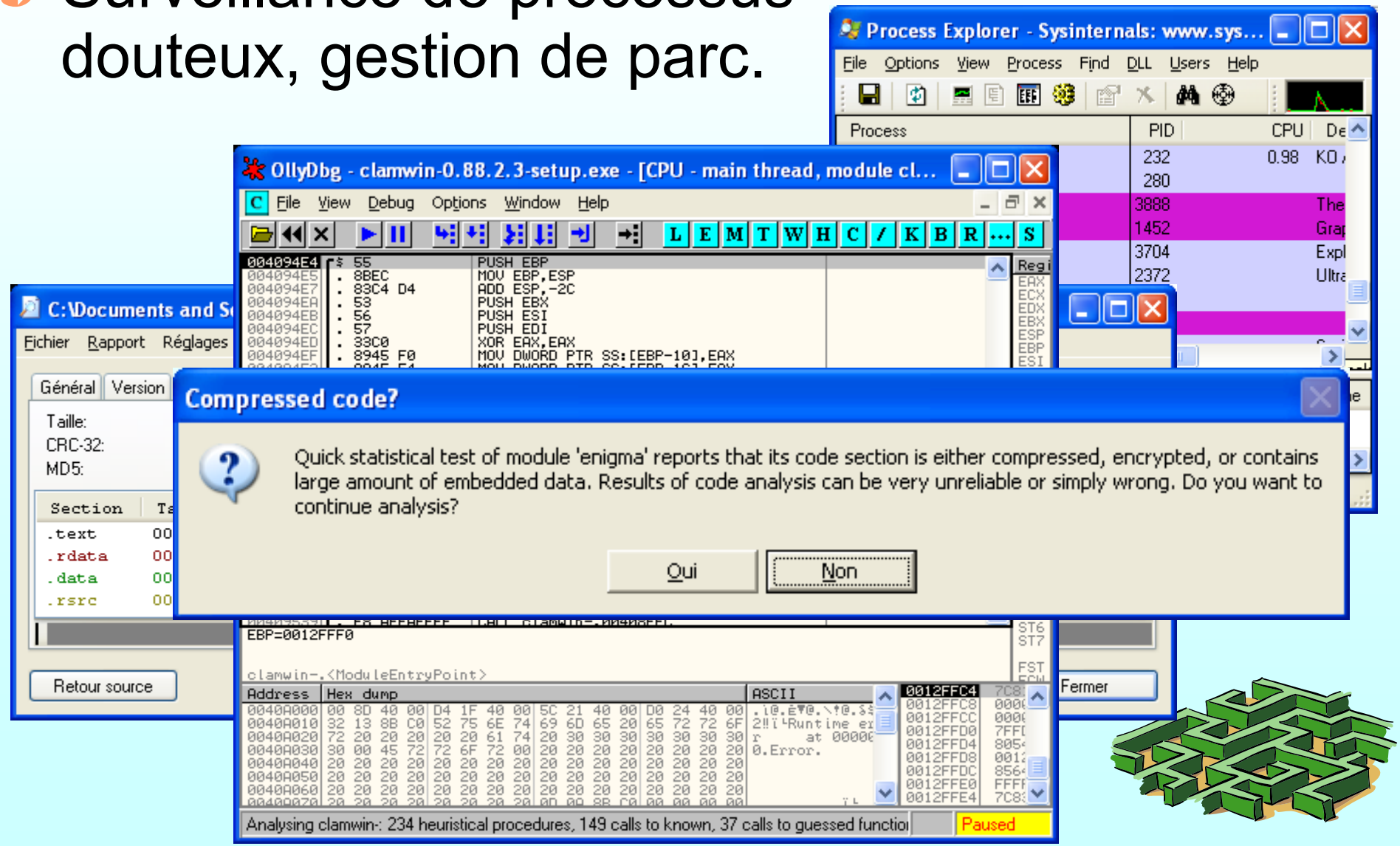


…face aux produits “Snake-Oil”



6. Effectuer des audits « live »

- Surveillance de processus douteux, gestion de parc.



7. Veille : apprendre l'état de l'art...

- Lecture de tutoriaux, de blogs, de forums...

Hex Blog
About IDA Pro, decompilation, programming, binary program analysis, information security.
By Ilfak Guilfanov

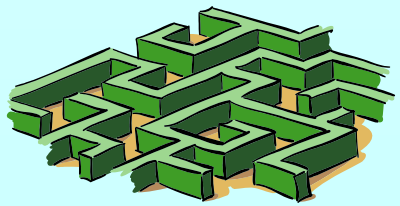
BeatriX

SECURITECH

OpenRCE.org

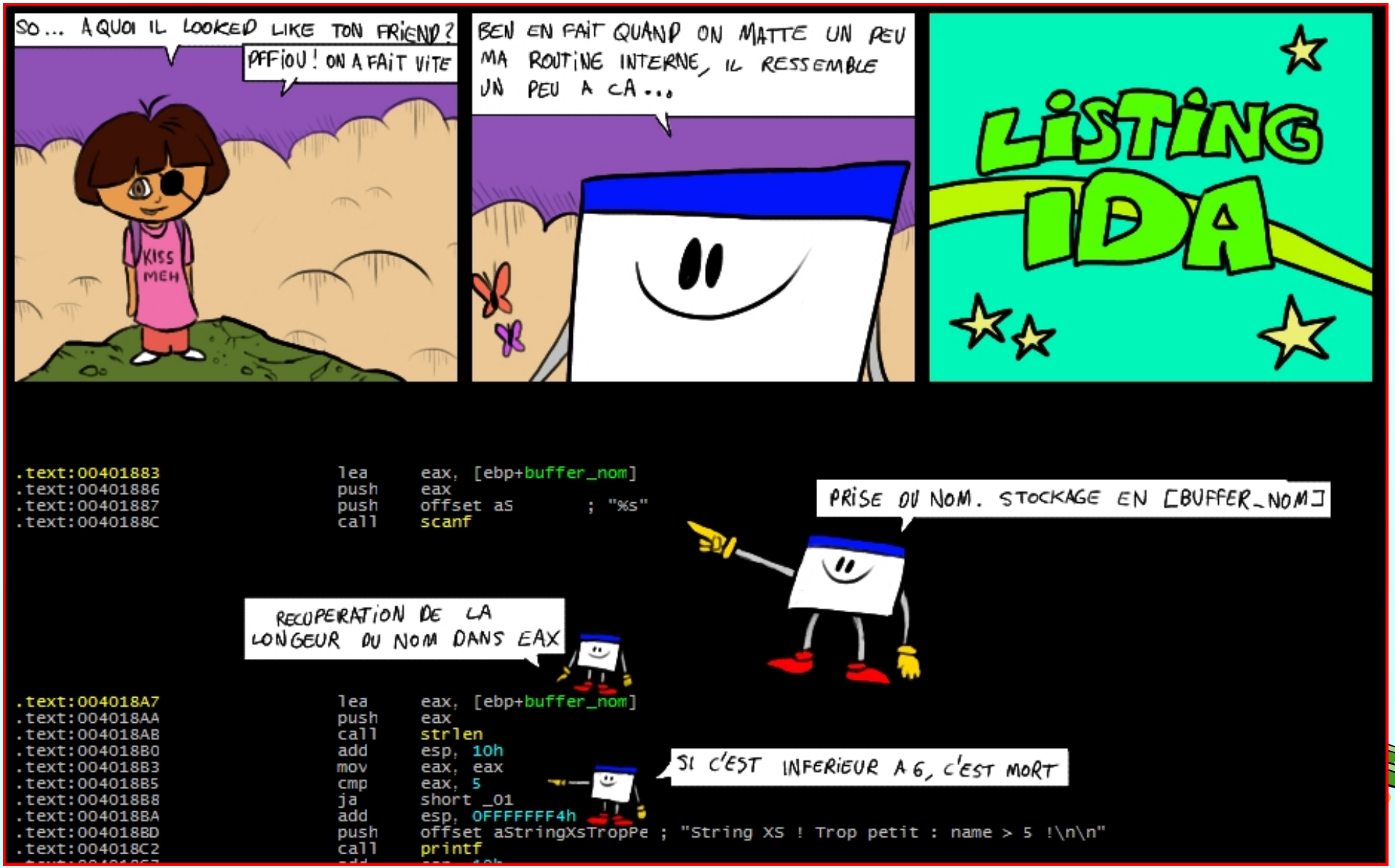
COMPRENDRE LE Kaine #5

➔ **Se tenir informé pour ne pas dire “je ne savais pas” !!**



... parfois même en s'amusant !

- Via les sites “underground”...



Outils in-dis-pen-sables !

0 €

Collections d'outils de Mark Russinovich (sysinternals.com) et de Nir Sofer (nirsoft.net)

PeID (+ plugins : Krypto Analyzer etc.)
Très pratique et simple d'utilisation.

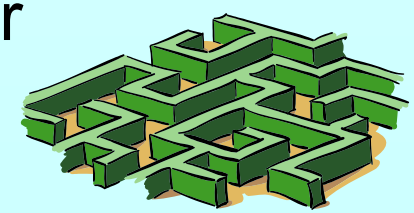
Universal Unpacker
Décompresse TOUT... ou presque.

OllyDbg (+ plugins)
« LE » débogueur par excellence... et gratuit en plus.

€€€

DataRescue IDA Pro (+ plugins)
Achetez-le, vous ne le regretterez pas. Franchement !

Vmware Workstation ou Microsoft Virtual Server
Ne prenez pas de risques en travaillant.



… et bien d'autres encore…