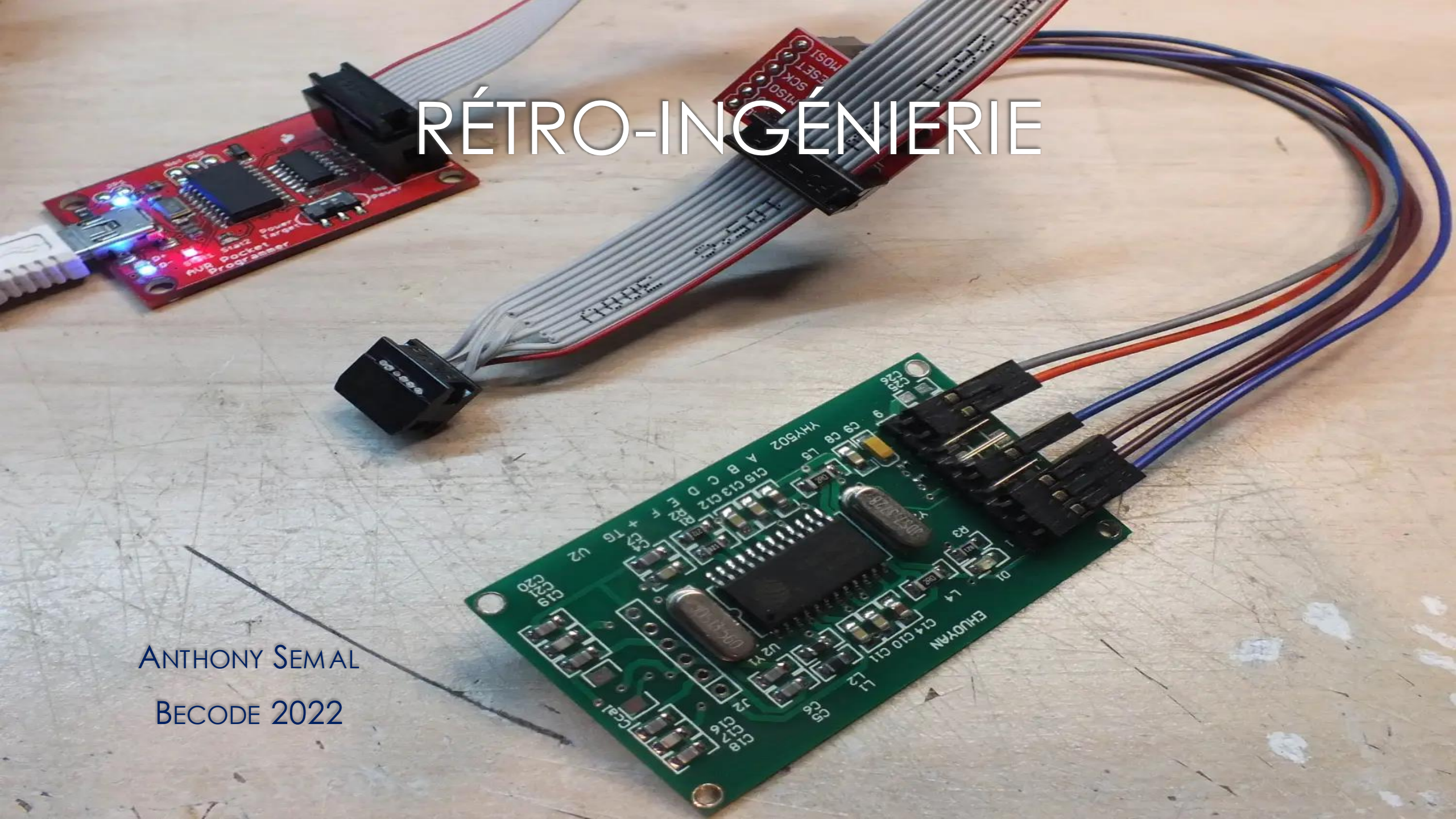
RÉTRO-INGÉNIERIE

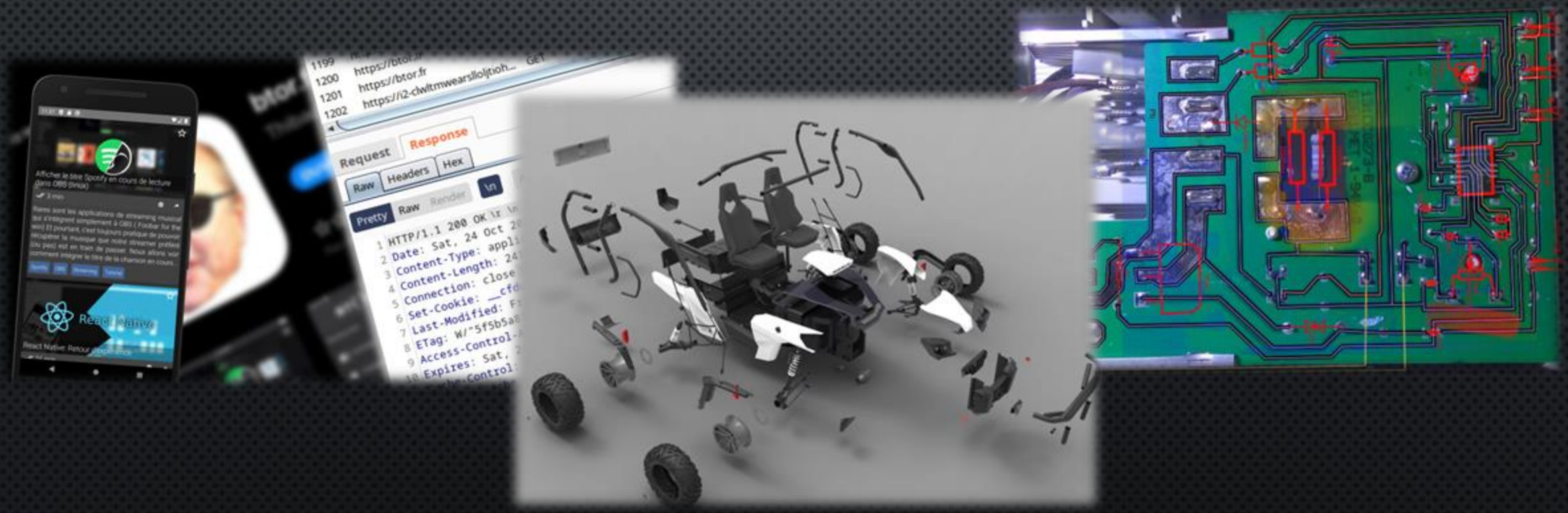


ANTHONY SEMAL

BECODE 2022

C'EST QUOI?

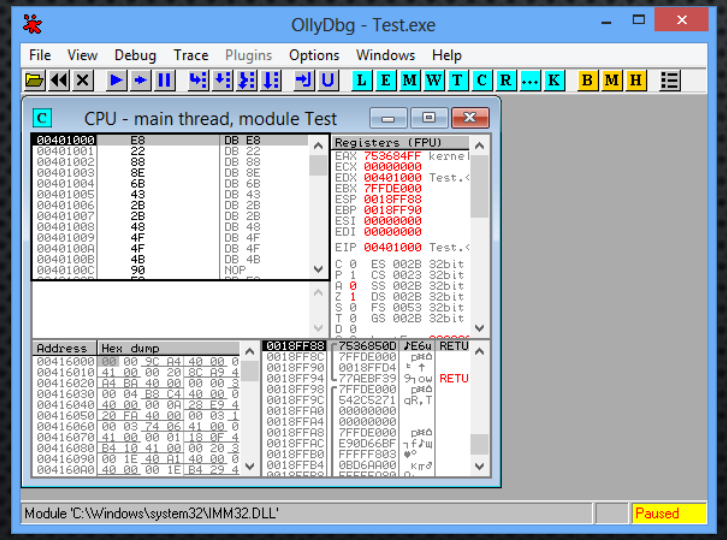
RÉALISER UN SCHÉMA, UN CODE, UNE DOCUMENTATION À PARTIR DE QUELQUE CHOSE QUI EXISTE (LOGICIEL OU MATERIEL)



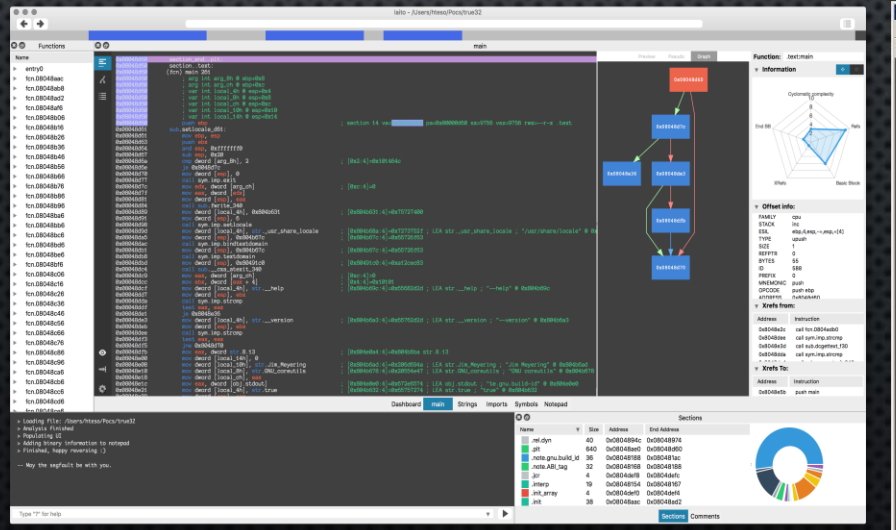
AU NIVEAU LOGICIEL

Il existe 3 types d'outils pour analyse un logiciel

Débogeur



Désassembleur



Décompilateur

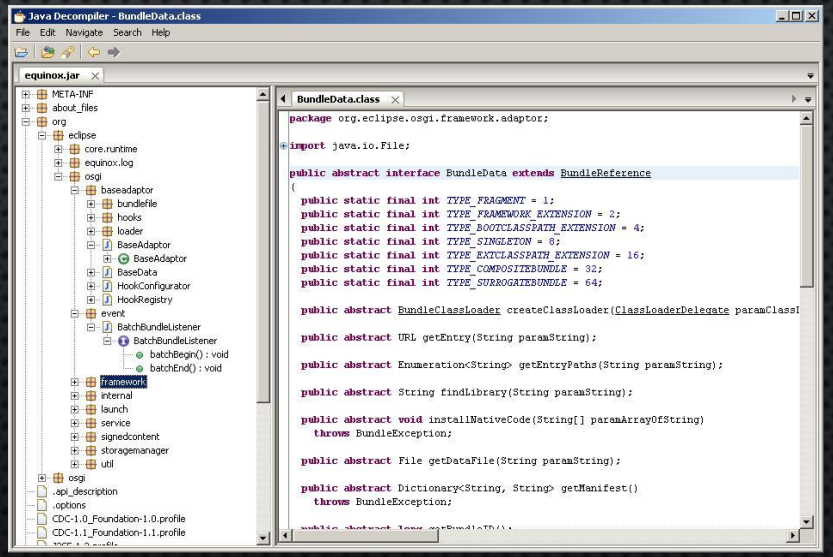
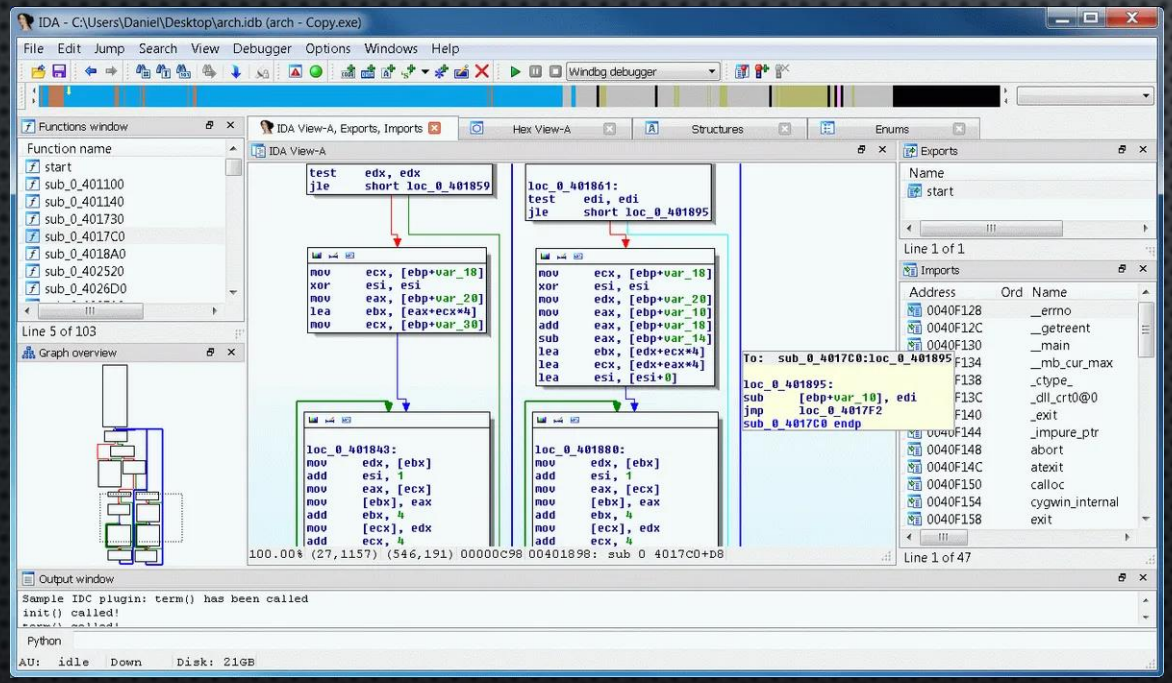


TABLEAU DES LOGICIELS DISPONIBLE (NON-EXHAUSTIVE)

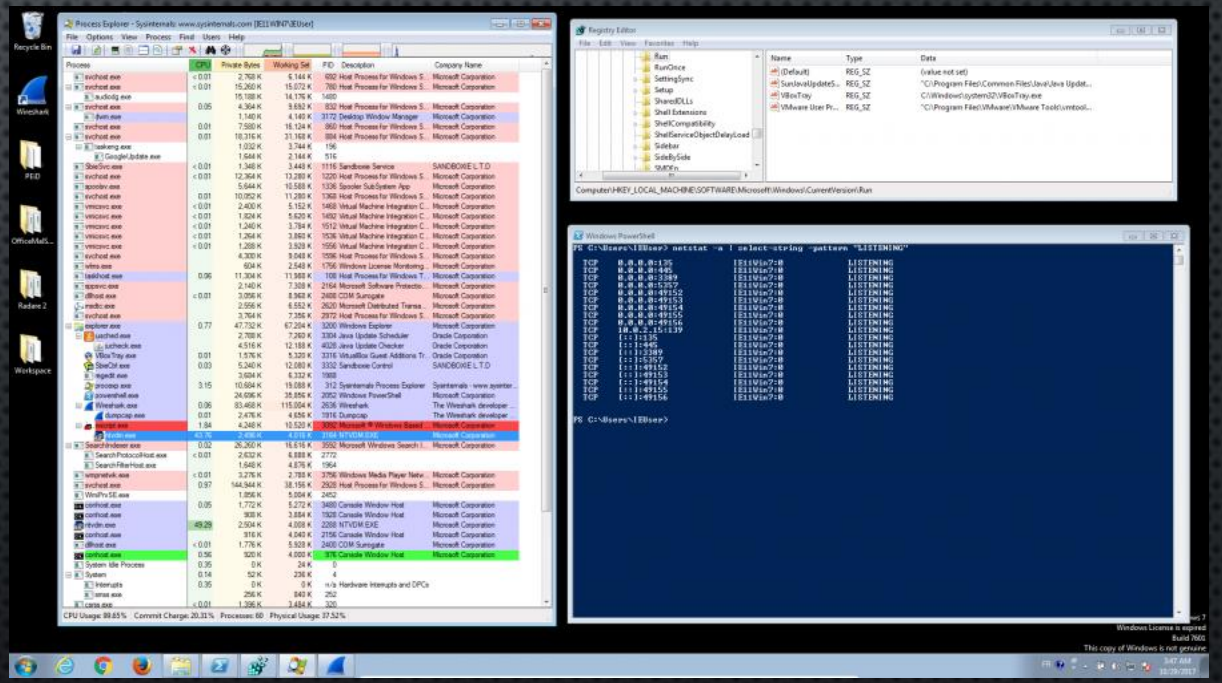
	AIO	DÉBOGUEUR	**Désassembleur**	**Décompilateur**
Windows	IDA (free/pro) Ghidra Ressource-hacker	Ollydbg X64dbg Windbg REDasm	Radare2 Ollydbg	Spice.decompilateur ILSpy DotPeek Java-Décompiler
Linux	IDA (free/pro) Ghidra	GDB (GNU Debugger) Valgrind	Radare2	Java-Decompiler Snowman C++ Decompiler
Android	IDA (free/pro) Ghidra	Android Debug Bridge	Dex2jar Apktool	Decompiler.com
MAC	IDA (free/pro) Ghidra		Radare2	
Editeur hexadécimale	HxD hex Editor MiniPro			

ANALYSE

ANALYSE STATIQUE

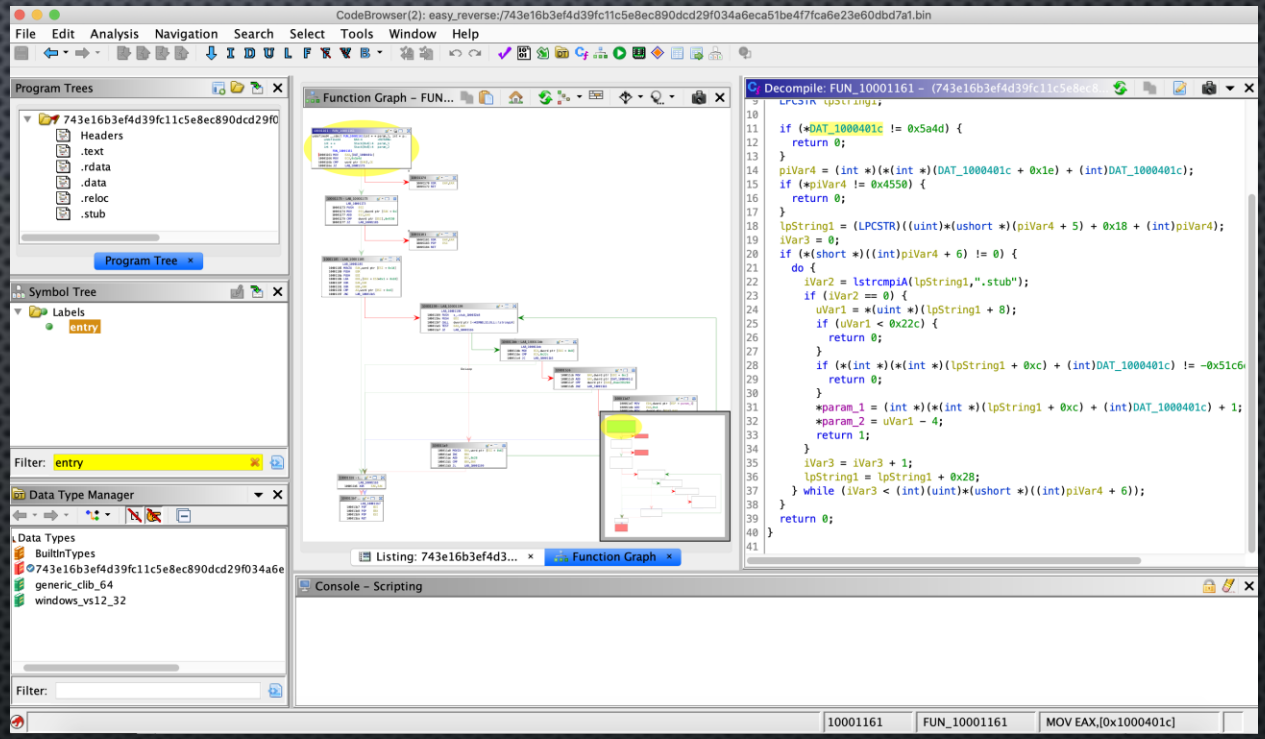


ANALYSE DYNAMIQUE



ANALYSE STATIQUE

ON CHERCHE À COMPRENDRE LE FONCTIONNEMENT D'UN MALWARE SANS L'EXÉCUTER



Analyse dynamique

Consiste à executer directement le malware dans un environnement controlé

Quelques outils:

- Les outils Sysinternals.
- SysAnalyzer: Analyseur système automatique de malware
- LordPE:Outil qui va analyser la mémoire de l'ordinateur.
- WireShark : Analyseur réseau.

Au niveau matériel

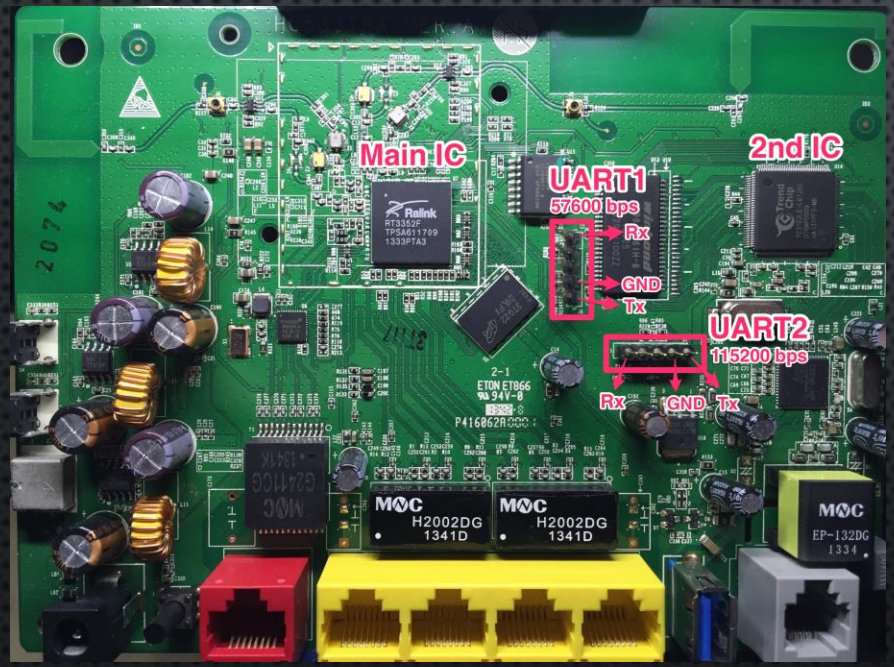
- Réparation
- Copier un logiciel propriétaire
- Trouver/exploiter des failles (meltdown/spectre)

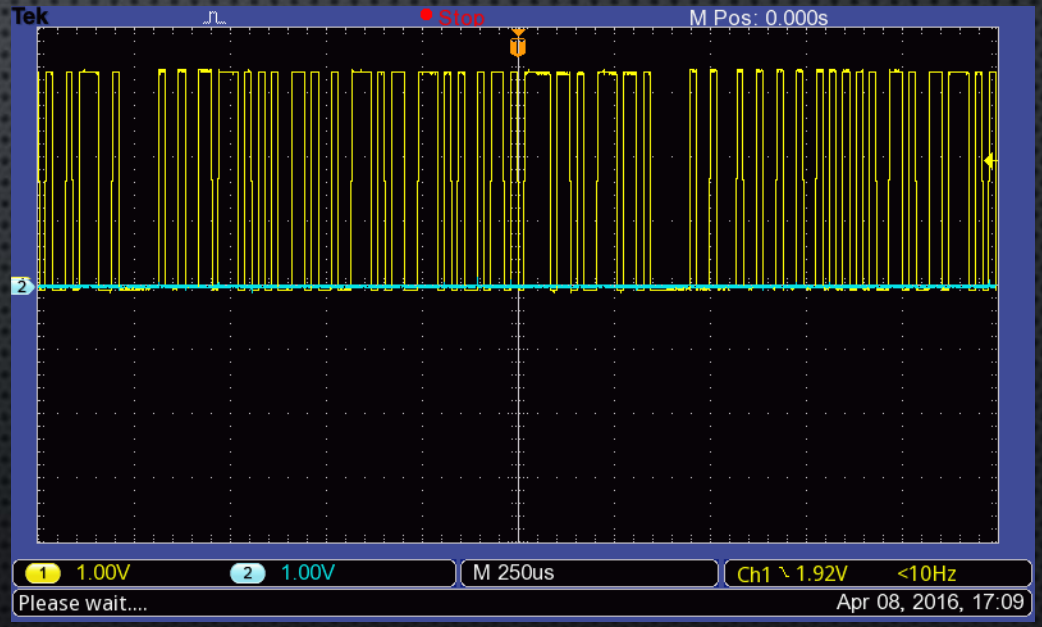
Mais...

Il faut du matériel (Programmateur, Oscilloscope, etc...

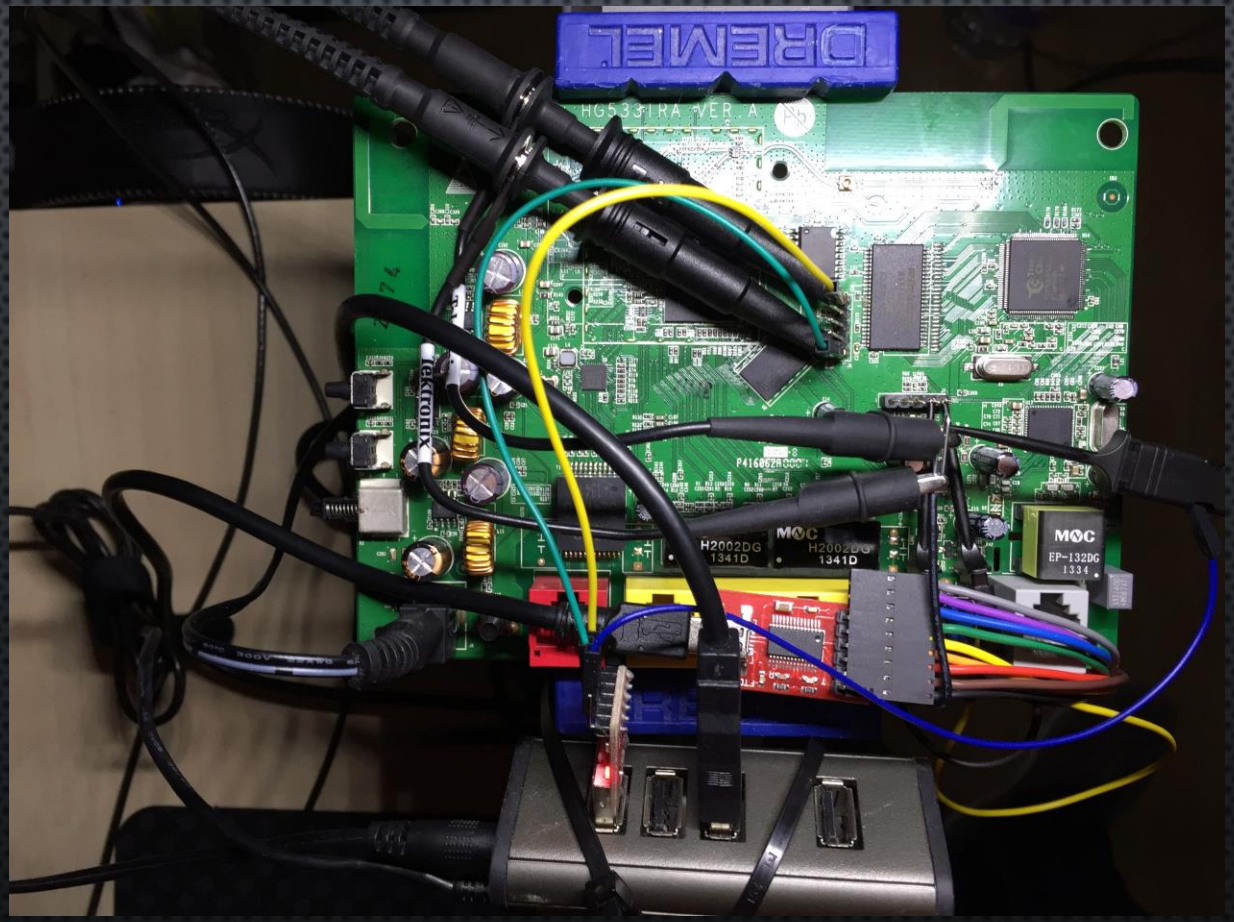
...et s'y connaitre en électronique

ANALYSER LA CARTE ET IDENTIFIÉ LES COMPOSANTS RECHERCHÉ

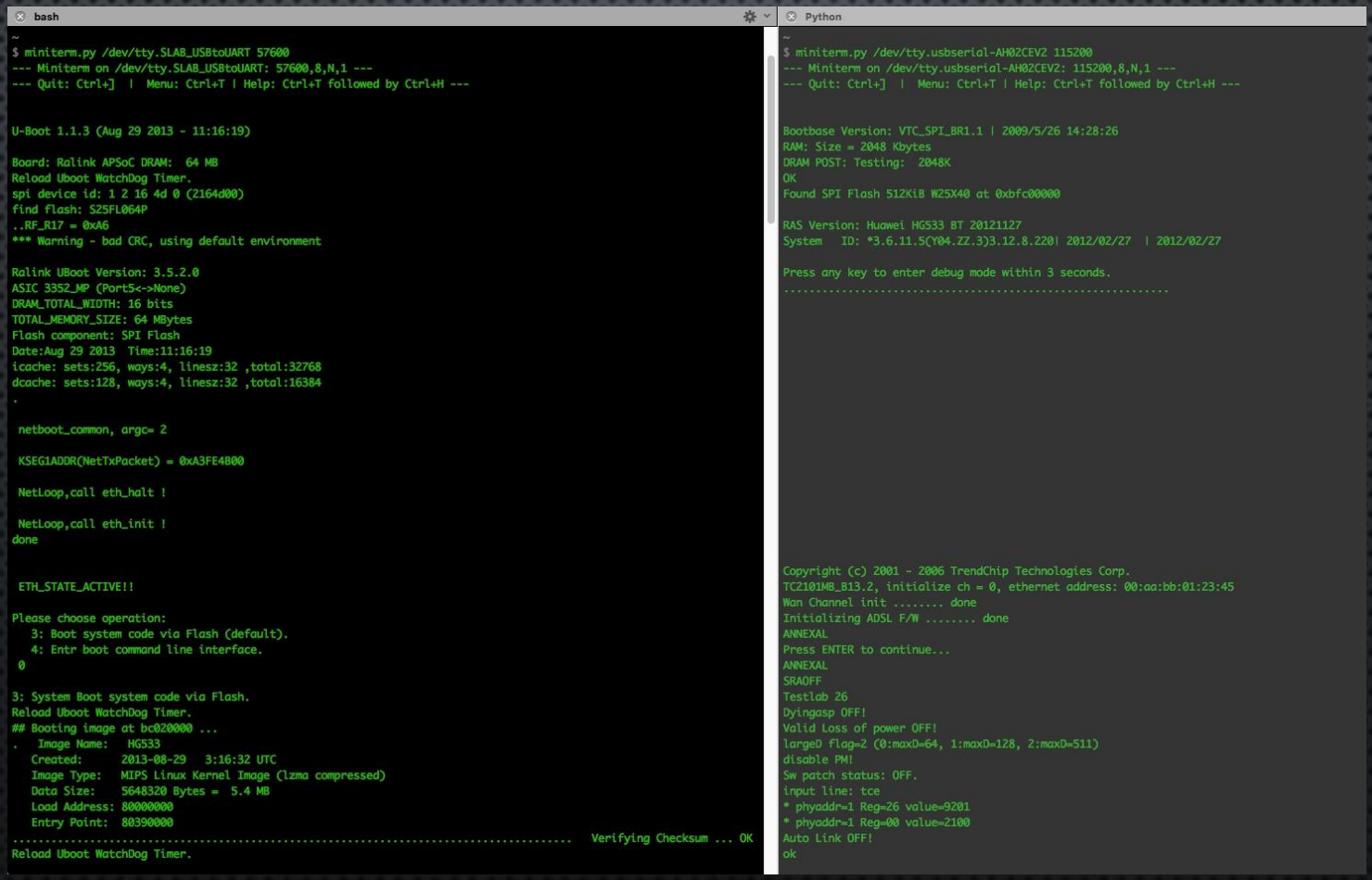




Trouver les ports séries et les connecter au PC (convertisseur uART-USB)



OUVRIR UN TERMINALE ET "ECOUTER" LES PORTS SÉRIES



Trouver des mots de passe root, informations sur la mémoire flash, etc...

CONCLUSION

L'analyse de malware est un monde à part entière, vaste et complexe. Plus on apprend, et plus l'on comprend qu'on ne sait rien…

Valou

SOURCE

Introduction à la rétro-ingénierie
https://dciets.com/dci-workshop/security/2020/01/29/Introduction-à-la-rétro-ingénierie/
https://clement-bouder.fr/Faire-de-la-retro-ingenierie-dans-le-cadre-dune-analyse-de-malware/
avec une petite liste d'outils : https://valou-tweak.fr/?p=2245
Vidéo présentant l'analyse d'un keyword
https://www.youtube.com/watch?v=NrFdBpplL0c

Hardware
https://korben.info/hardware-hacking.html
https://duo.com/blog/microcontroller-firmware-recovery-using-invasive-analysis
https://jcjc-dev.com/2016/12/14/reversing-huawei-5-reversing-firmware/
https://www.youtube.com/watch?v=vdEoQgTP0H4
https://connect.ed-diamond.com/misc/mischs-024/introduction-au-reverse-hardware
https://airbus-seclab.github.io/hdd/SSTIC2015-Slides-hardware_re_for_software_reversers-czarny_rigo.pdf
https://www.youtube.com/watch?v=vdEoQgTP0H4 - exploit contrôleur Bluetooth
https://skyduino.wordpress.com/2013/11/10/tutohack-la-retro-ingenierie-cest-la-vie/