

Reverse Engineering (Zakaria)

Definition

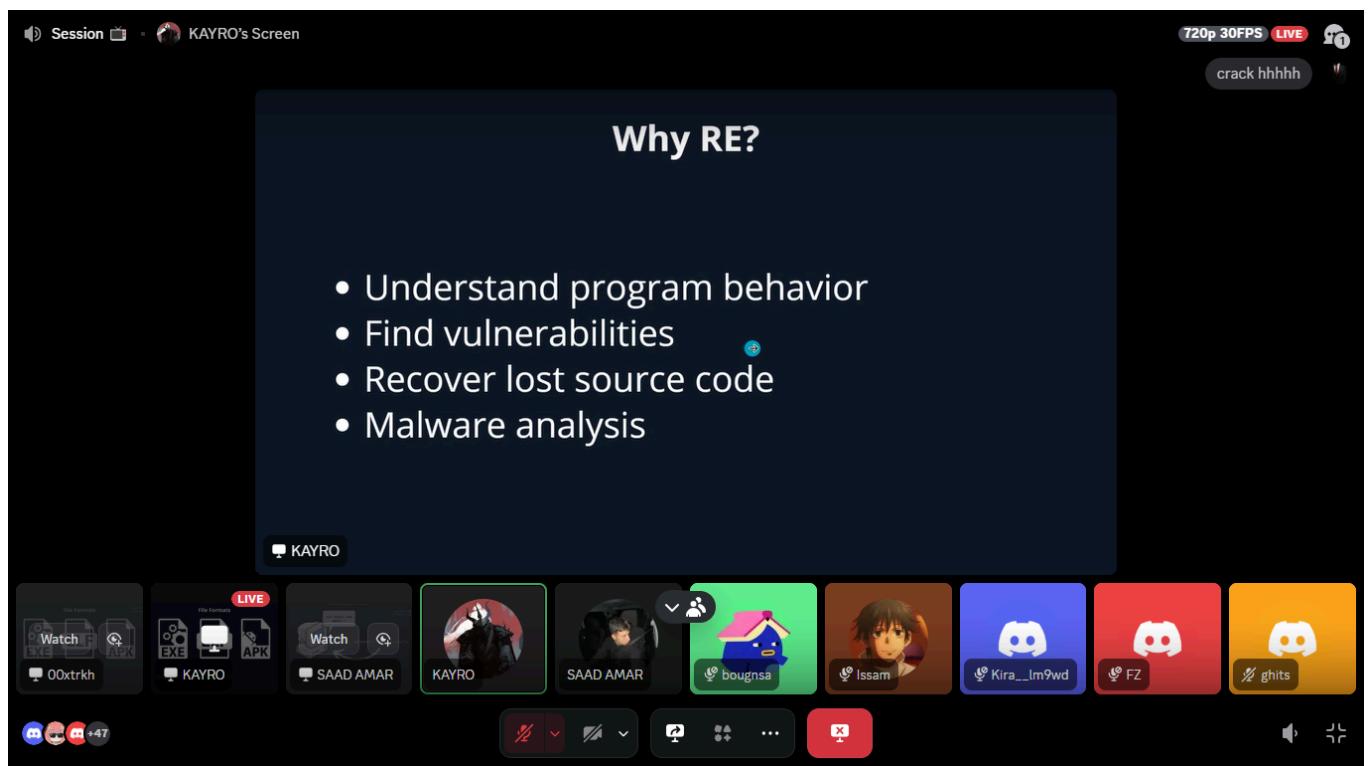
Reverse engineering (RE) = taking a suspicious binary or sample apart to understand what it does, how it does it, and what damage or risk it poses — without access to the original source code. Goal: identify capabilities, infection vector, persistence, network behavior, and indicators you can use to detect or remediate it.

File Formats

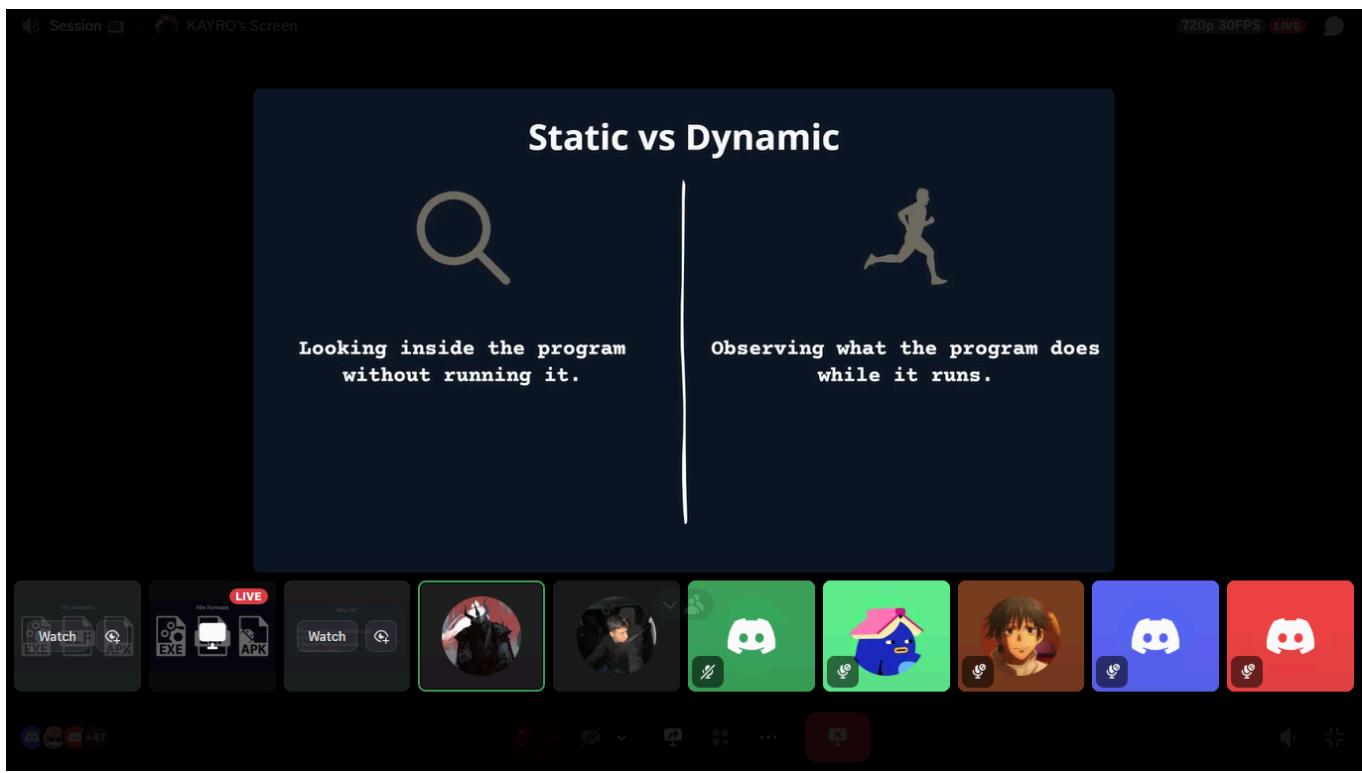
We can search a list of each file format signature in Wikipedia

An ELF (Executable and Linkable Format) file is a common standard file format used for executable files, object code, shared libraries, and core dumps on Unix-like systems such as Linux.

Why reverse Engineering

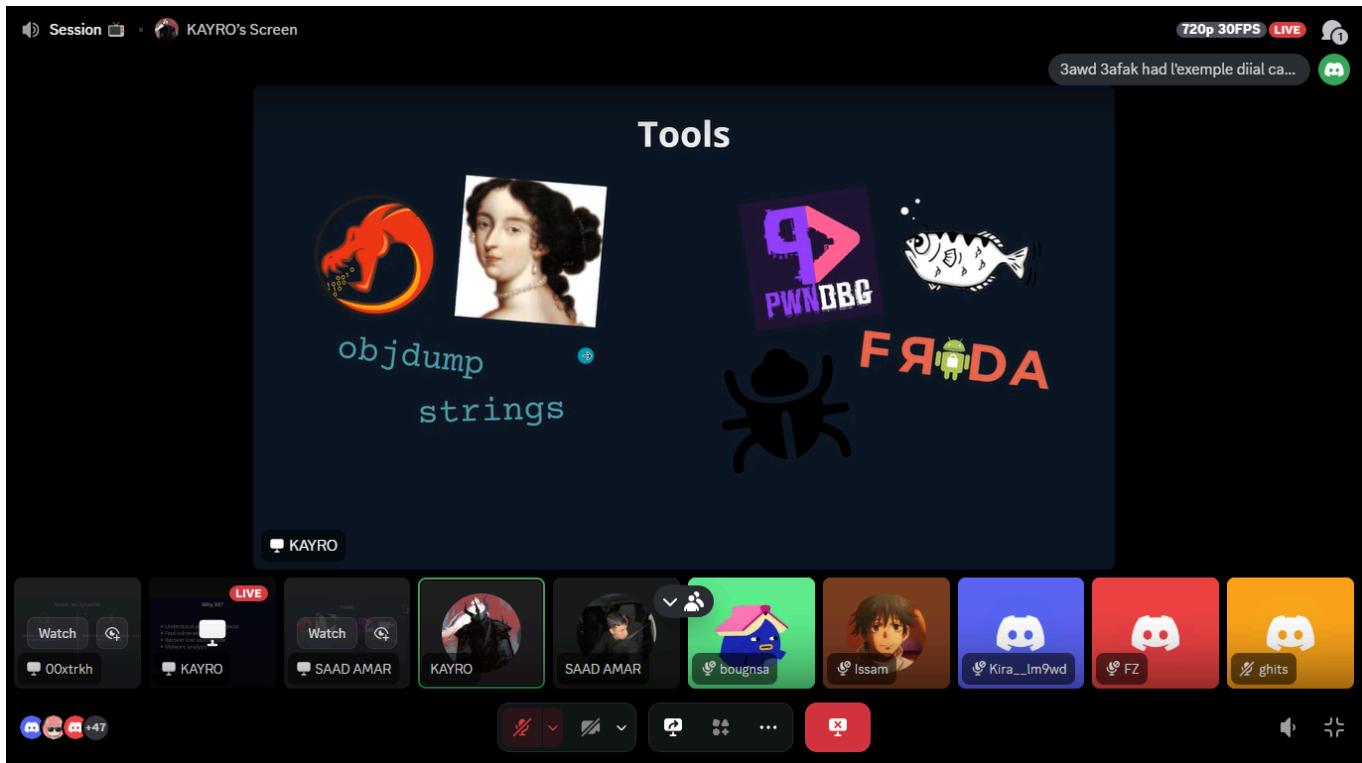


Malware Analysis (Static vs Dynamic)



Tools for Static and Dynamic malware analysis:

On the left static, and on the right dynamic :



How to block someone from analysing a malware:



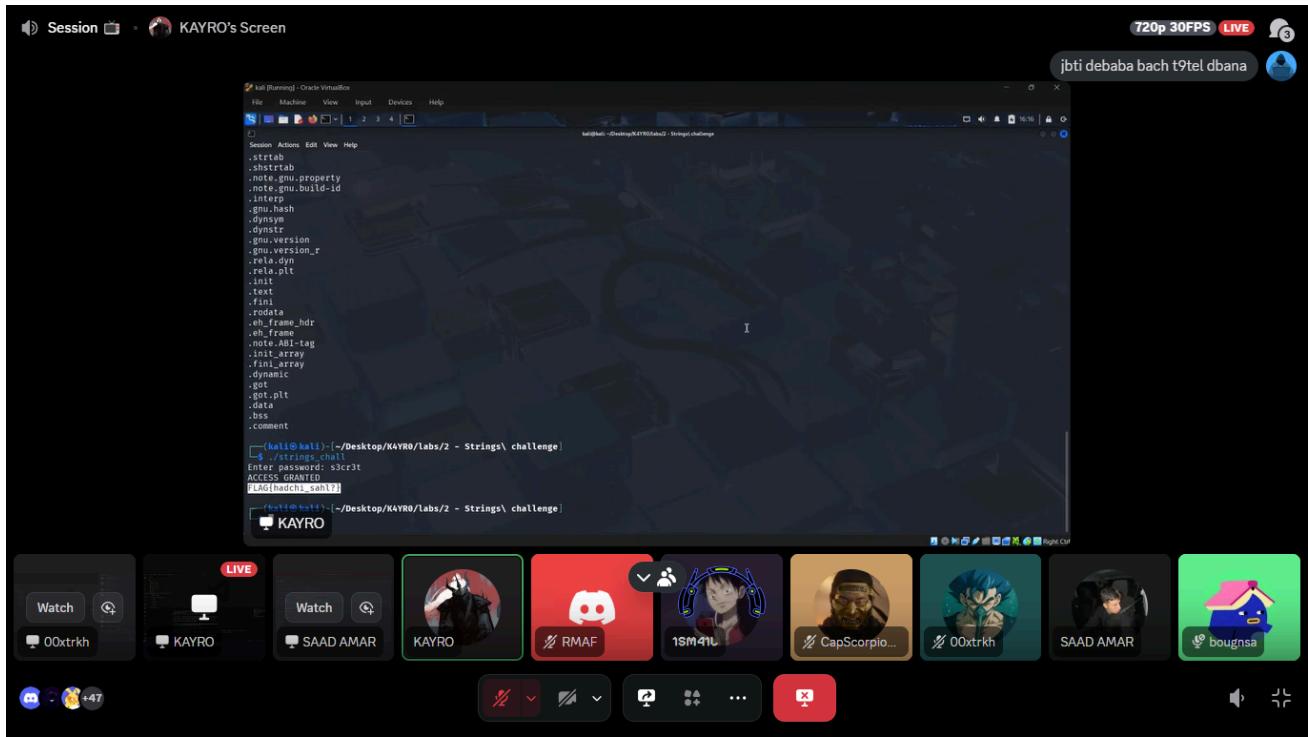
PIE, has a relation with memory. Chaque fois ta dir run l program les function dyal program taykhdo new address f memory donc mat9darch t3raf l address dyal function etc...

Tools to search and get ready for malwares:

- strings
- checksec
- Detect-it-easy (Die)

Practice :

- We can use the "diec" command to collect some format-like infos about a file.
- Or we can use the command "file [file_name]" also
- dnSpy tool, we open our file, and we can showcz
- jadx-gui, we can open the code source of an apk file (zip)
- "strings" command, we can use it to see what's inside a file, for example, if we run a file, and they tell us to enter a password, we can discover what's the expected correct input.



- If we don't find the password with strings, we use a command named "ghidra".
- Ghidra is a UI to better scan the a file.
- We can also use "Pwndbg", (inside of it we use the command "disassemble"), so we write the command "info functions" to see the functions, we notice that there is a function called "check_password", we enter a command called "break [function_name]", we enter a random input this time and we notice that there is a word "hello" we didn't enter, it's like what's being compared with our input, that is the answer.

