

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

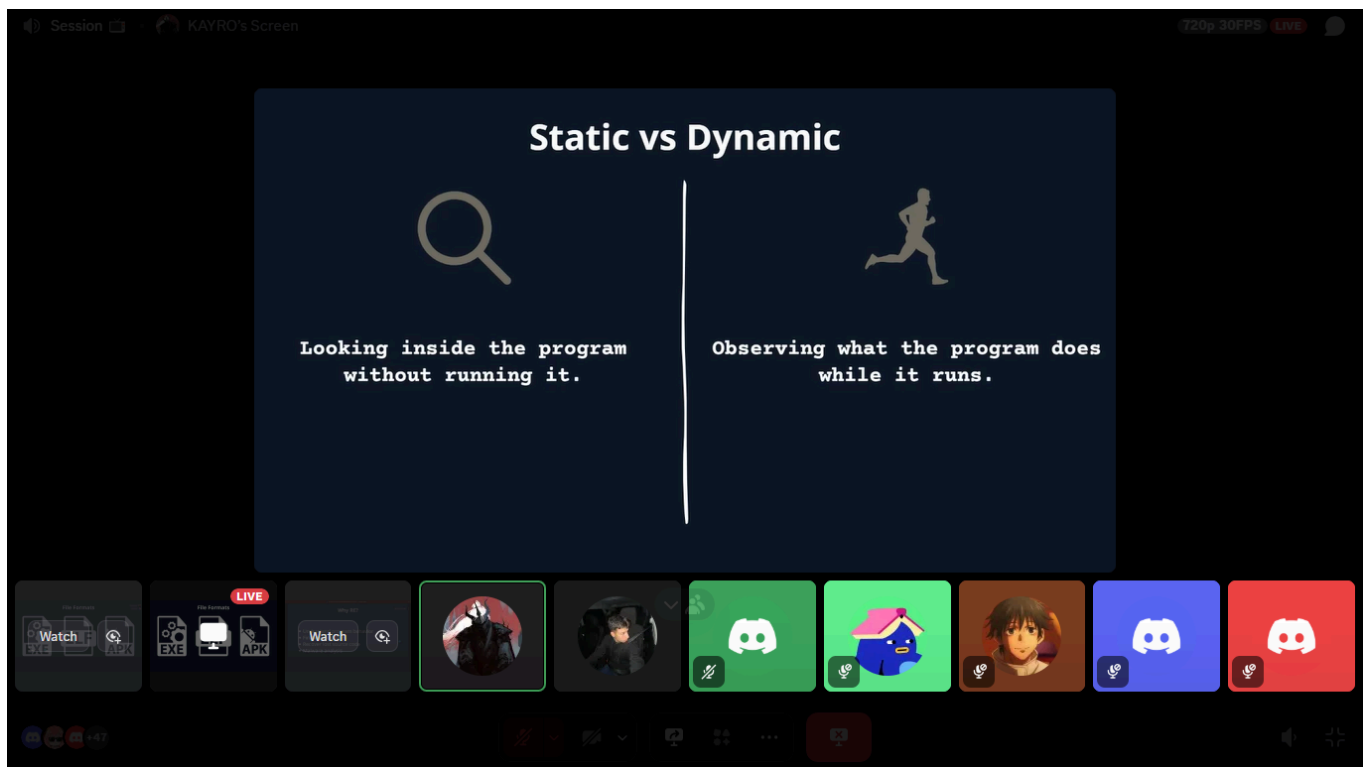


The screenshot shows a Discord live stream interface. At the top, it says "Session" and "KAYRO's Screen". In the top right corner, it displays "720p 30FPS LIVE" and a chat bubble with the text "crack hhhhh". The main content area is a dark blue rectangle with the title "Why RE?" and a bulleted list:

- Understand program behavior
- Find vulnerabilities
- Recover lost source code
- Malware analysis

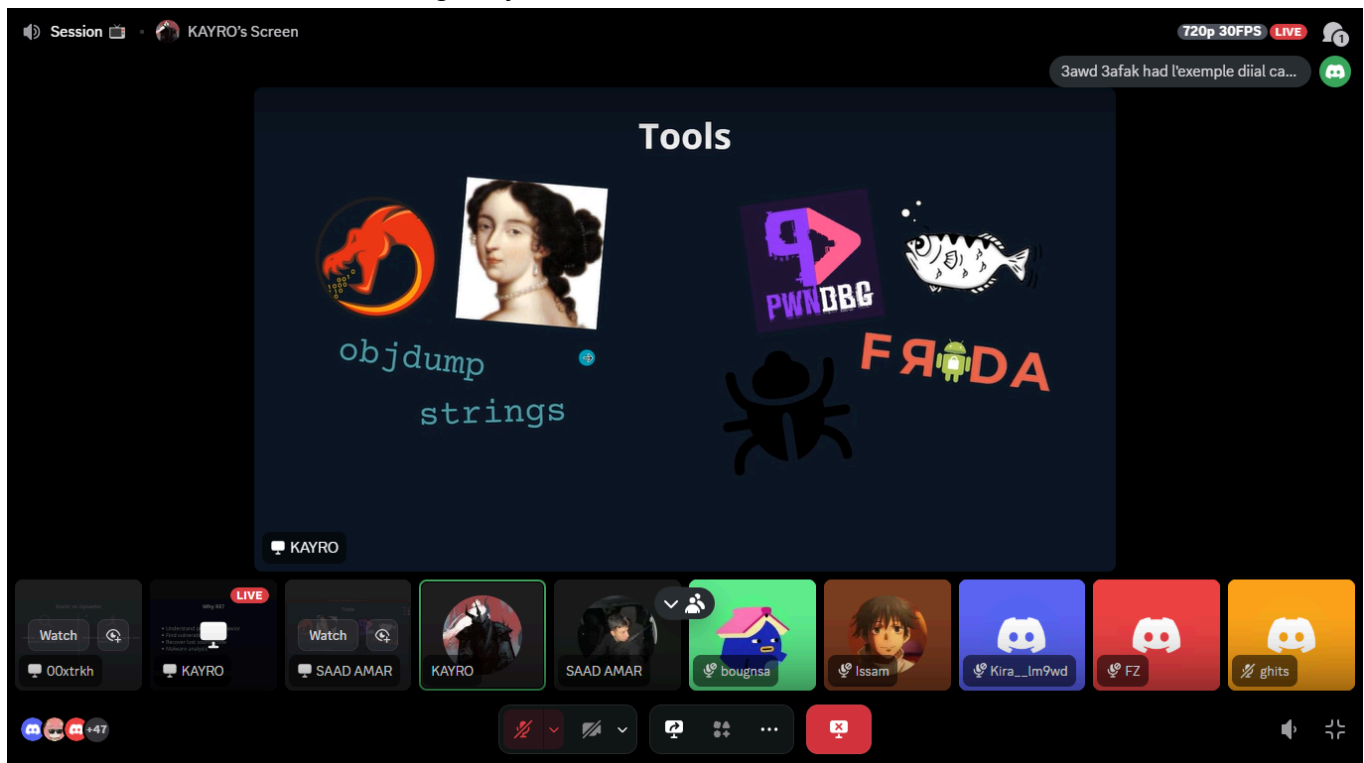
Below the main content area is a row of user avatars and names: KAYRO, SAAD AMAR, bougnsa, Issam, Kira__lm9wd, FZ, and ghits. At the bottom, there are icons for various Discord features and a red button with a white 'X'.

Malware Analysis (Static vs Dynamic)

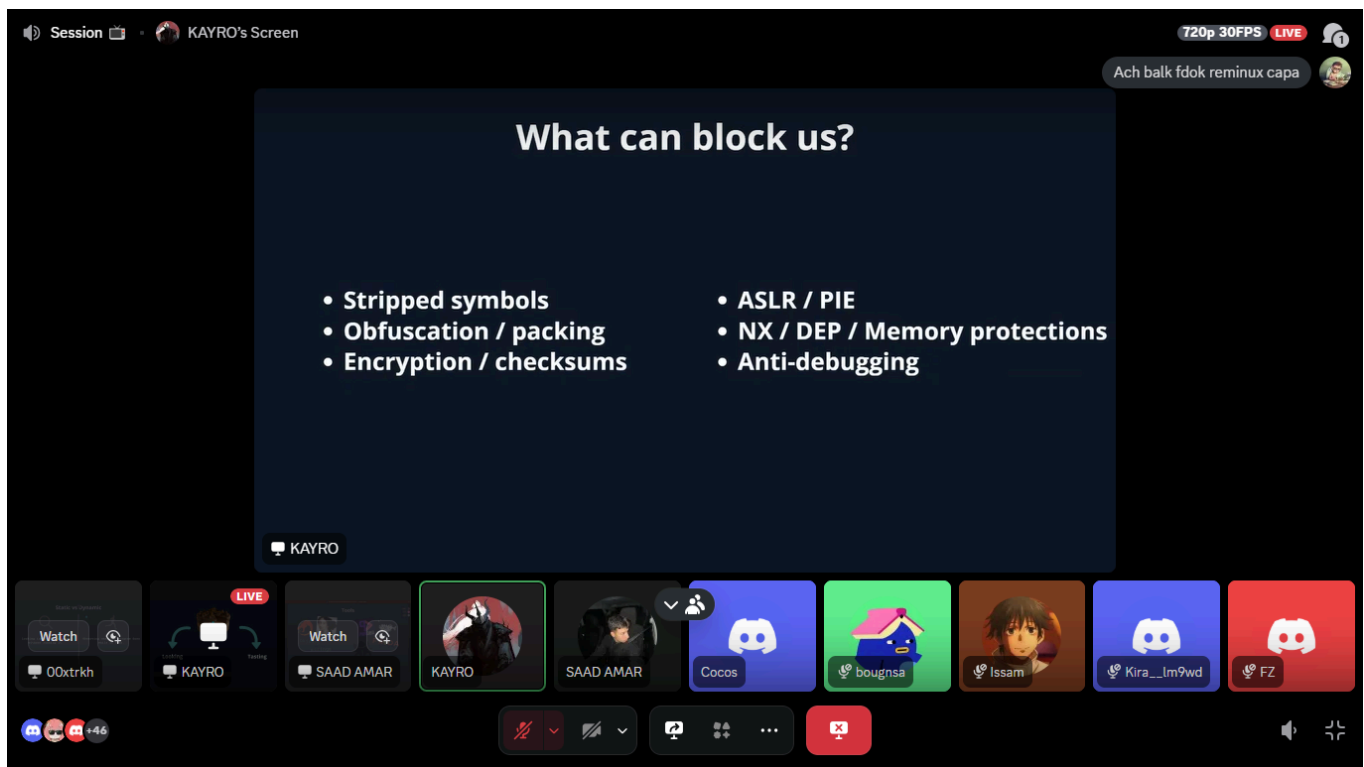


Tools for Static and Dynamic malware analysis:

On the left static, and on the right dynamic :



How to block someone from analysing a malware:



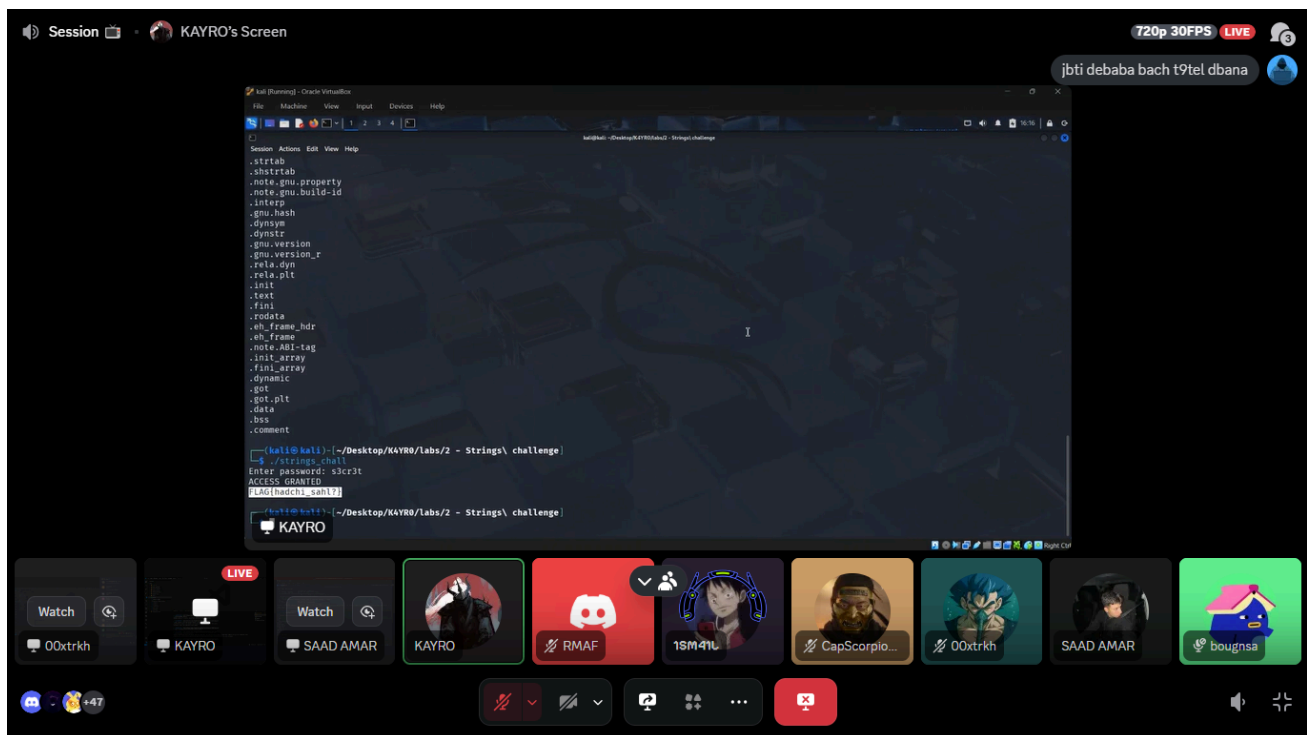
PIE, has a relation with memory. Chaque fois ta dir run l program les fonction d'yal program taykhdo new address f memory donc mat9darch t3raf l address d'yal function etc...

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.


Session




IMNOI HERE 

10:46 PM

achnahiya dik vm f cas dyal pe ou khask dir analyse dynamique ?



marlithor_cyber

10:46 PM

wordlist

 1
 



00xtrkh

10:47 PM

wordlist

 1
 



@amine khouya smh lia wakha ghankhrj 3la syaa9 ? wac...

10:47 PM

KillJoy 

it takes time+khask good wordlist w wakha hakkak machi 100% (edited)

 1
 



amine 

10:47 PM

ty



lux  PWIND

10:48 PM

a quel point khs n3rf fonctionnement dyal cpu



GouloJk 

10:48 PM

سمح ايا تقطع ليا الريني الى كان ممكن تادوح هاذ الصالاج جنتنوا
غير الانمسي

+

Message Session 





Session




IMNOI HERE 

10:46 P.M.

achnahiya dik vm f cas dyal pe ou khask dir analyse dynamique ?



marlithor_cyber

wordlist


1




O0xtrkh

wordlist


1




@amine khouya smh lia wakha ghankhrj 3la syaa9 ? wac...

KillJoy 

10:47 PM

it takes time+khask good wordlist w wakha hakkak machi 100% (edited)


1




amine

ty


10:47 PM



lux  PWIND

10:48 PM

a quel point khs n3rf fonctionnement dyal cpu



GouloJk 

10:48 PM

سمح ليا تقطع ليا اليرني الى كان ممكن نملود نطرح هاد الصالاج بختنخيا
عزير الاسامي


Message Session

