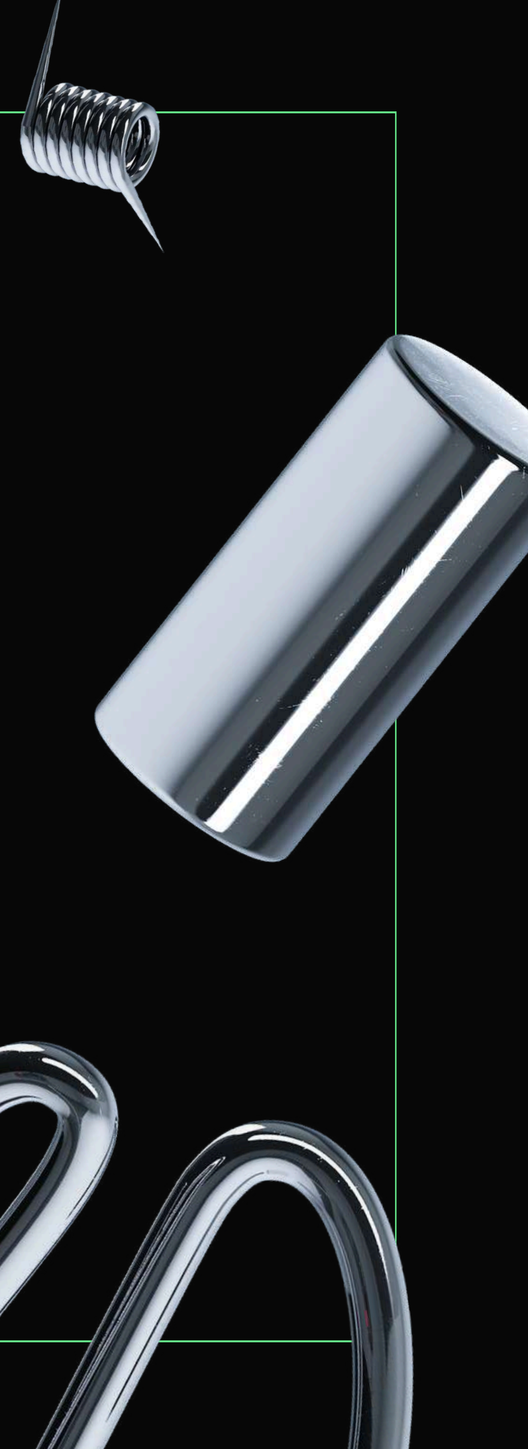
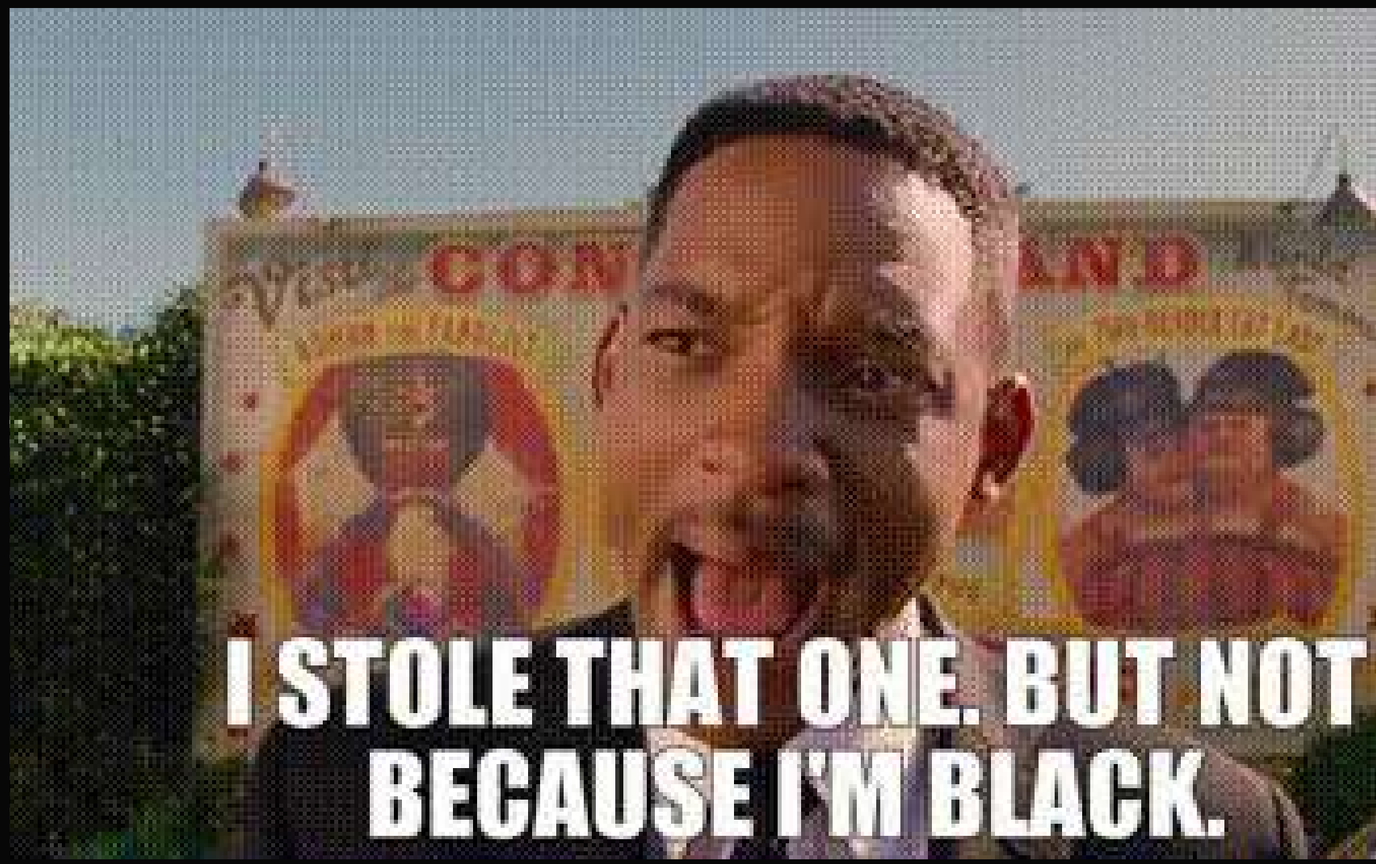
MalDev : Detection Fails, Evasion Prevails



But wait is this illegal ?

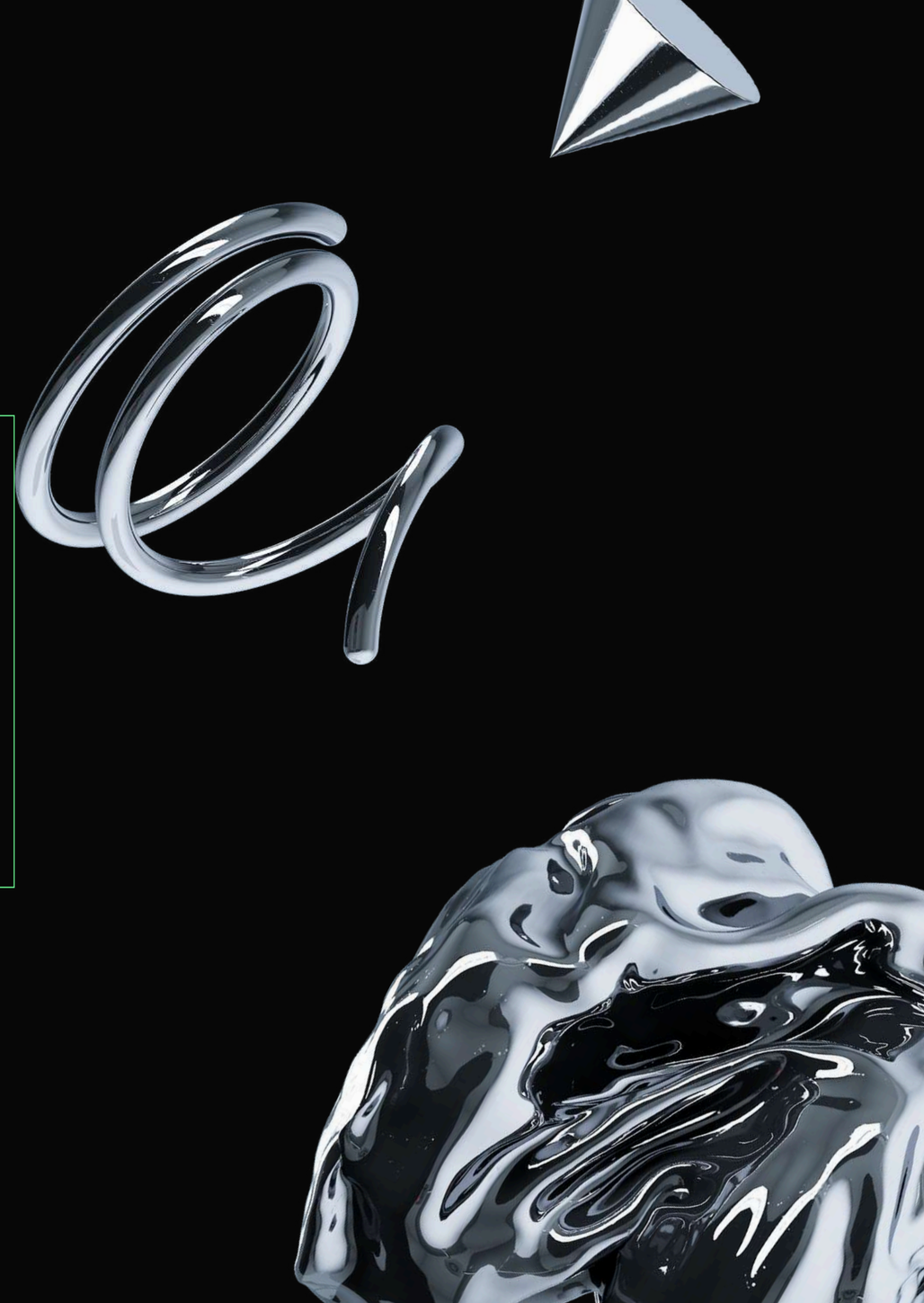


Discussion points

Key topics covered
in this presentation

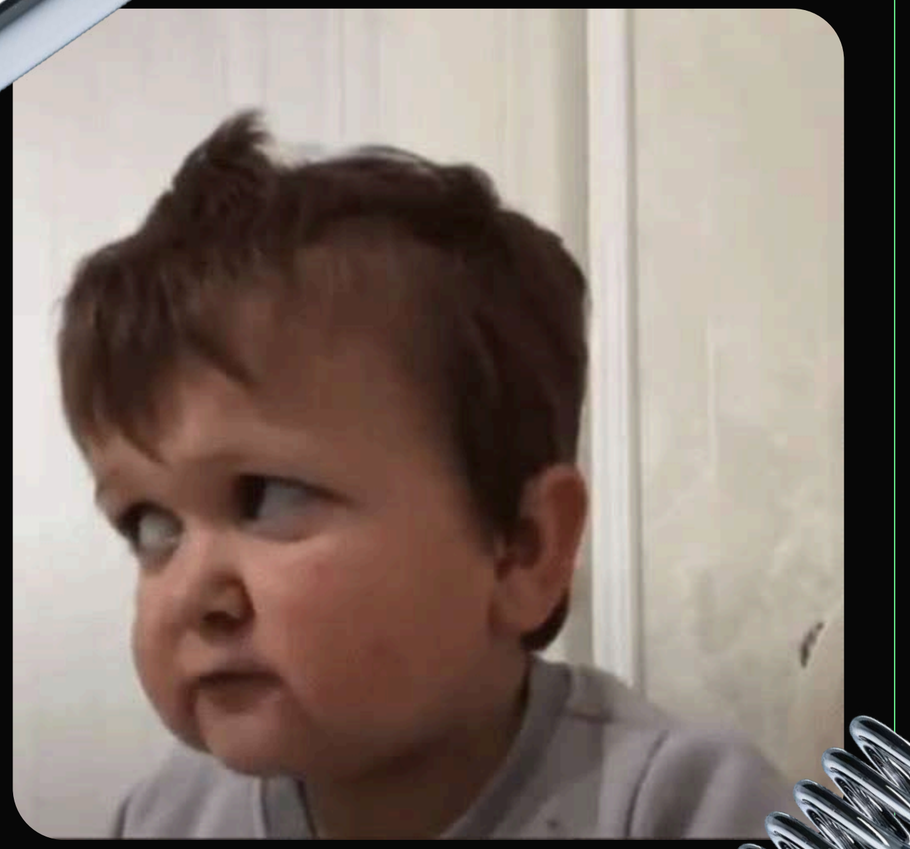
- Introduction
- What is AV & EDR ?
- What is AV & EDR Evasion?
- How Detection Works ?
- How to Evade ?
- Ressources , Q&A

Introduction



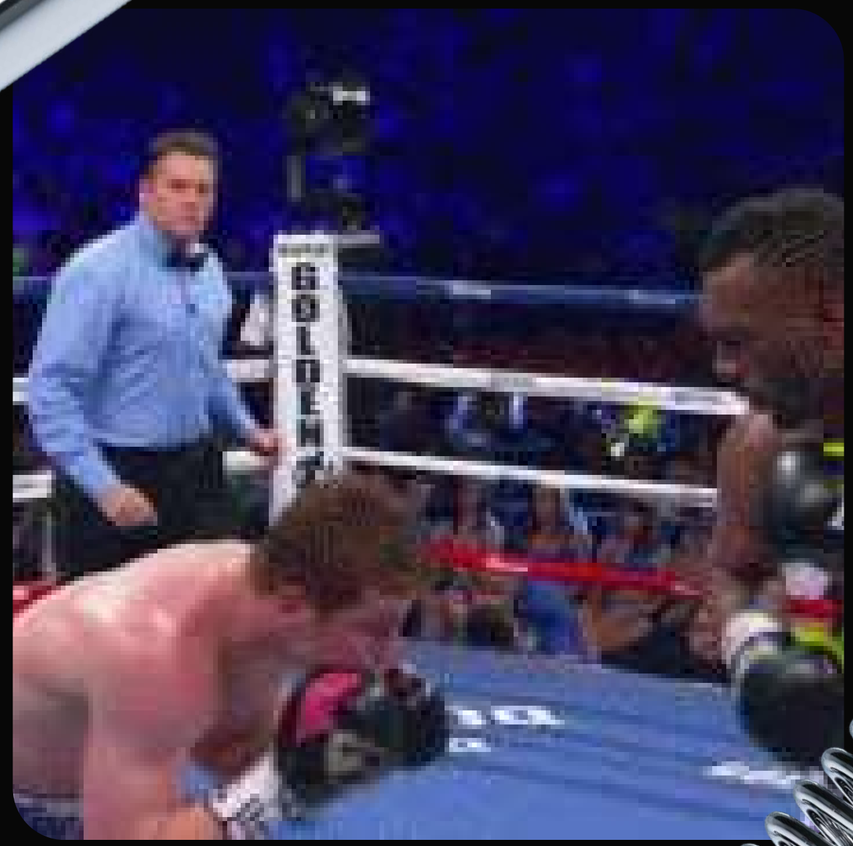
What is AV & EDR ?

- AV = Prevents known malware
- EDR = Detects & investigates advanced threats

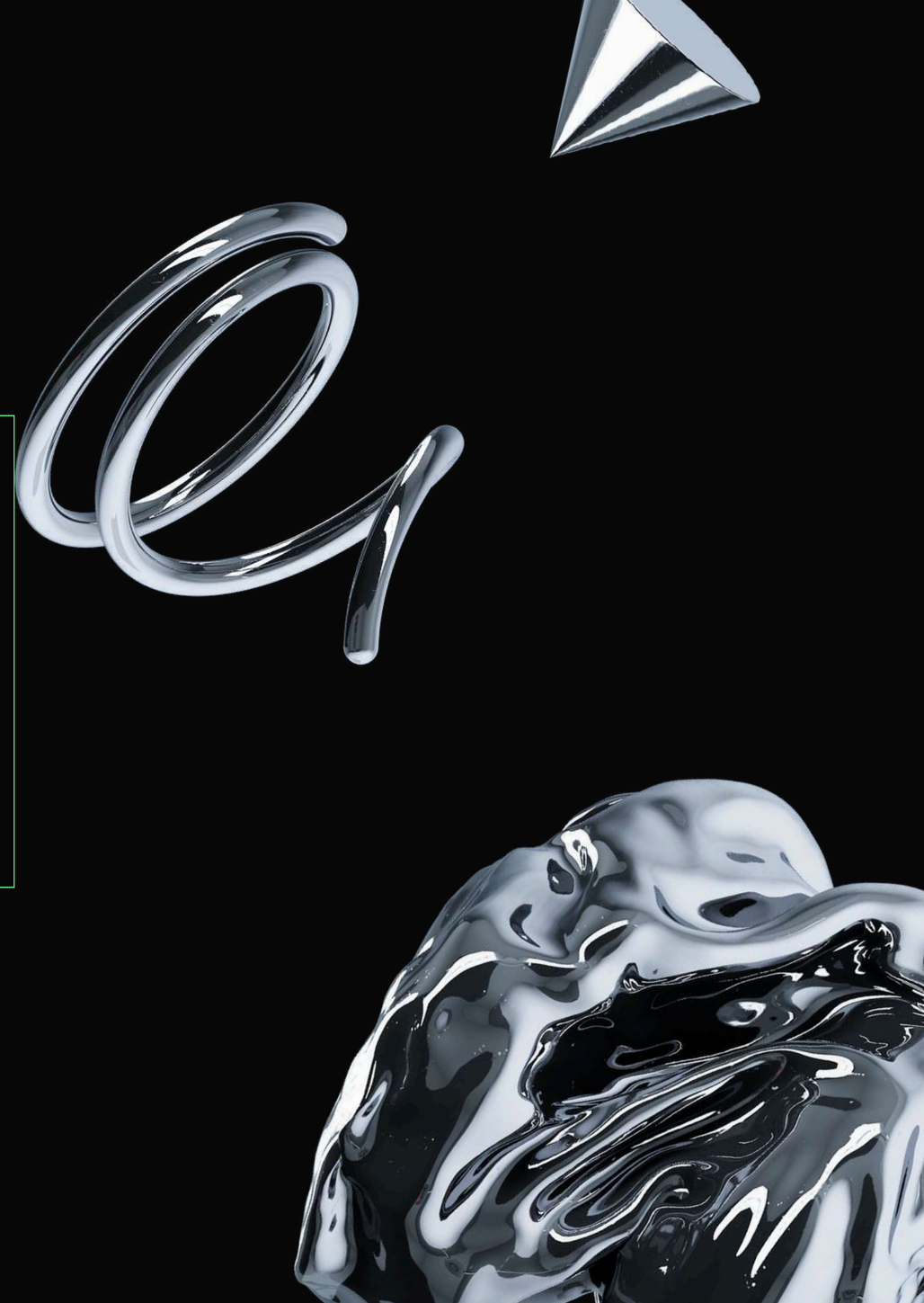


What is AV & EDR Evasion?

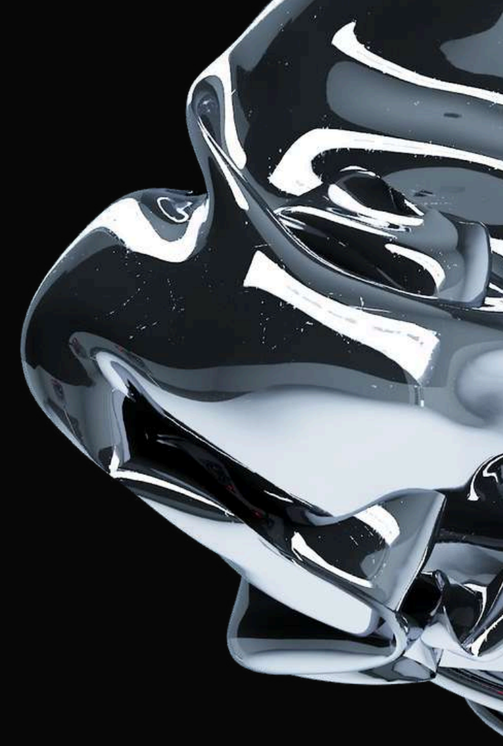
With the general term “AV Evasion” or “EDR Evasion” we refer to the set of techniques that allows an attacker to execute arbitrary code into a system, bypassing all controls that should prevent her from doing it.



Let’s Start



How Detection Works?



signature-based detection

FILE CHECKSUMS (MD5, SHA1)

- KNOWN STRINGS

HEURISTIC DETECTION

STATIC ANALYSIS of Malware Behavior

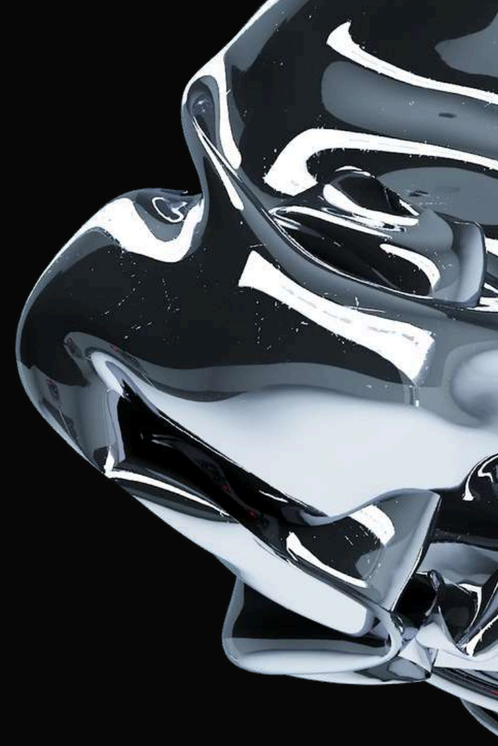
Malicious Functions

Sandboxing

Dynamic Analysis

Executing the malware

Can we evade those defenses?



signature-based detection

Code Mutation

Polymorphism

Encryption

HEURISTIC DETECTION

Code obfuscation

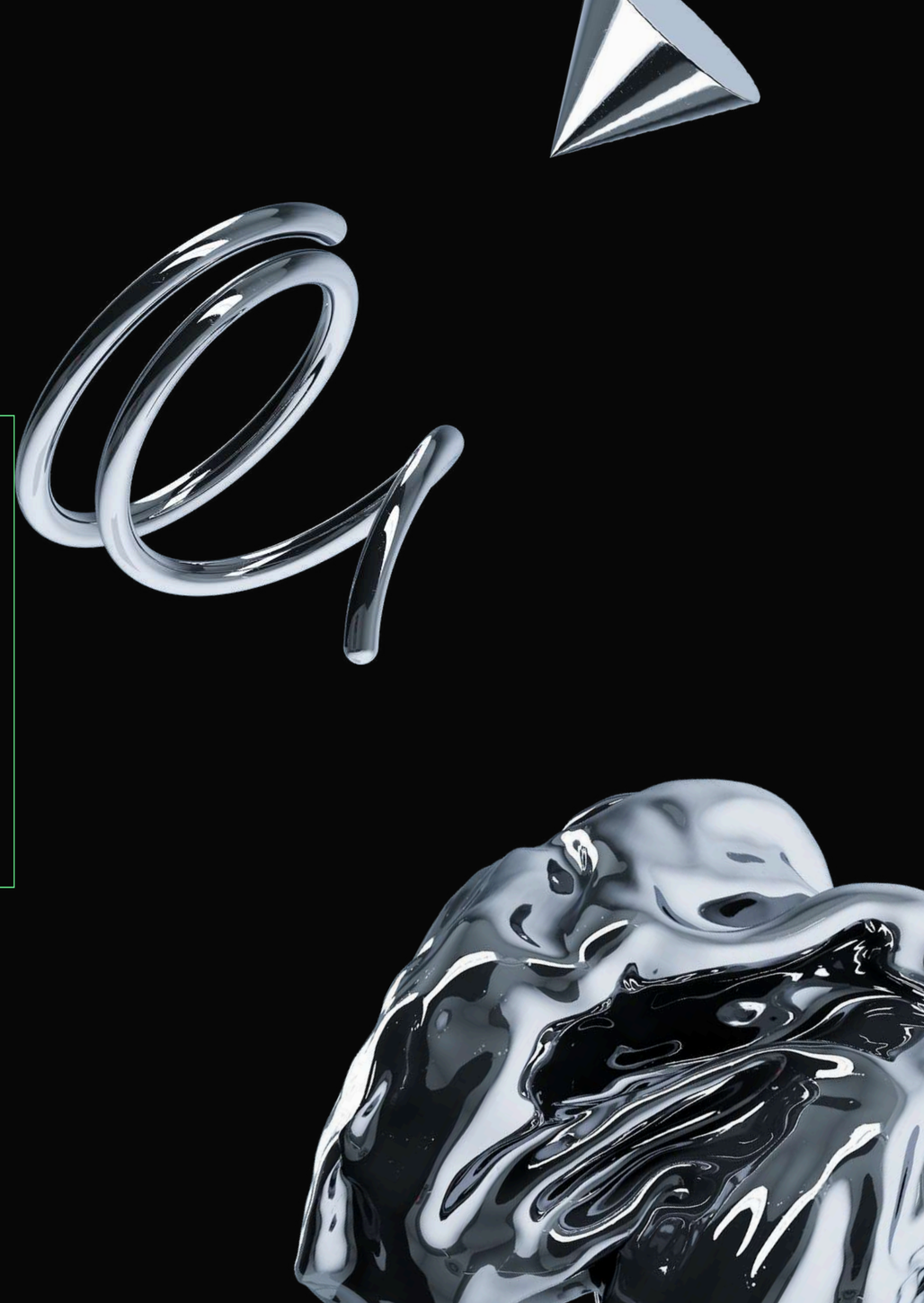
Dynamic code

Sandboxing

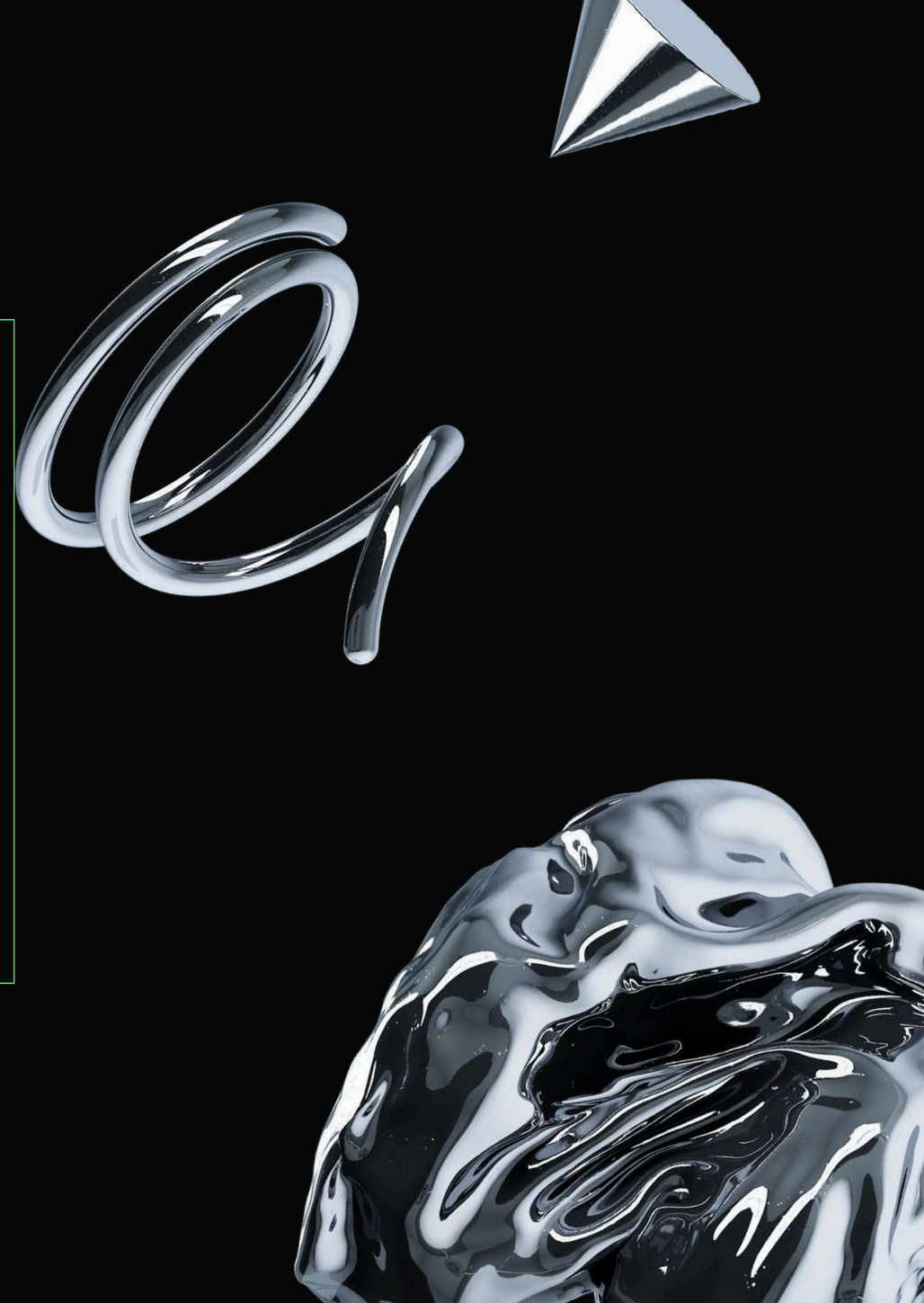
Env Checkers , User interaction Checkers

Time-Based Execution Delays,
Syscalls, Indirect Syscalls

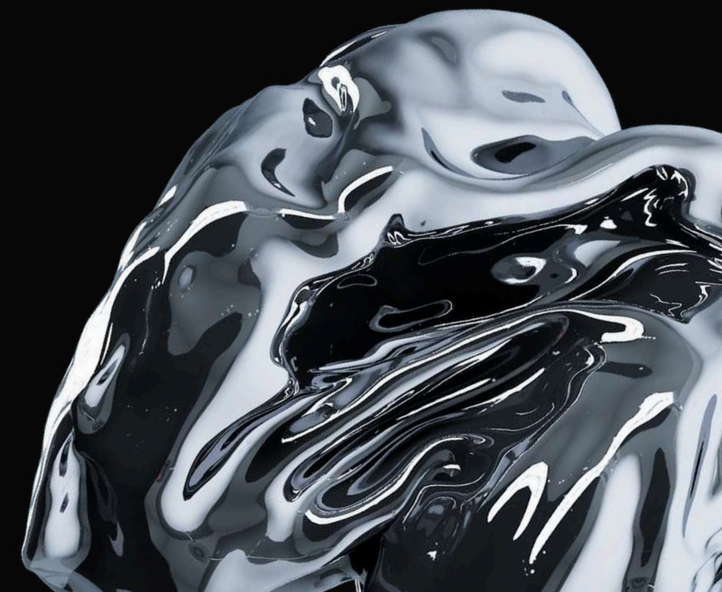
Real Stuff



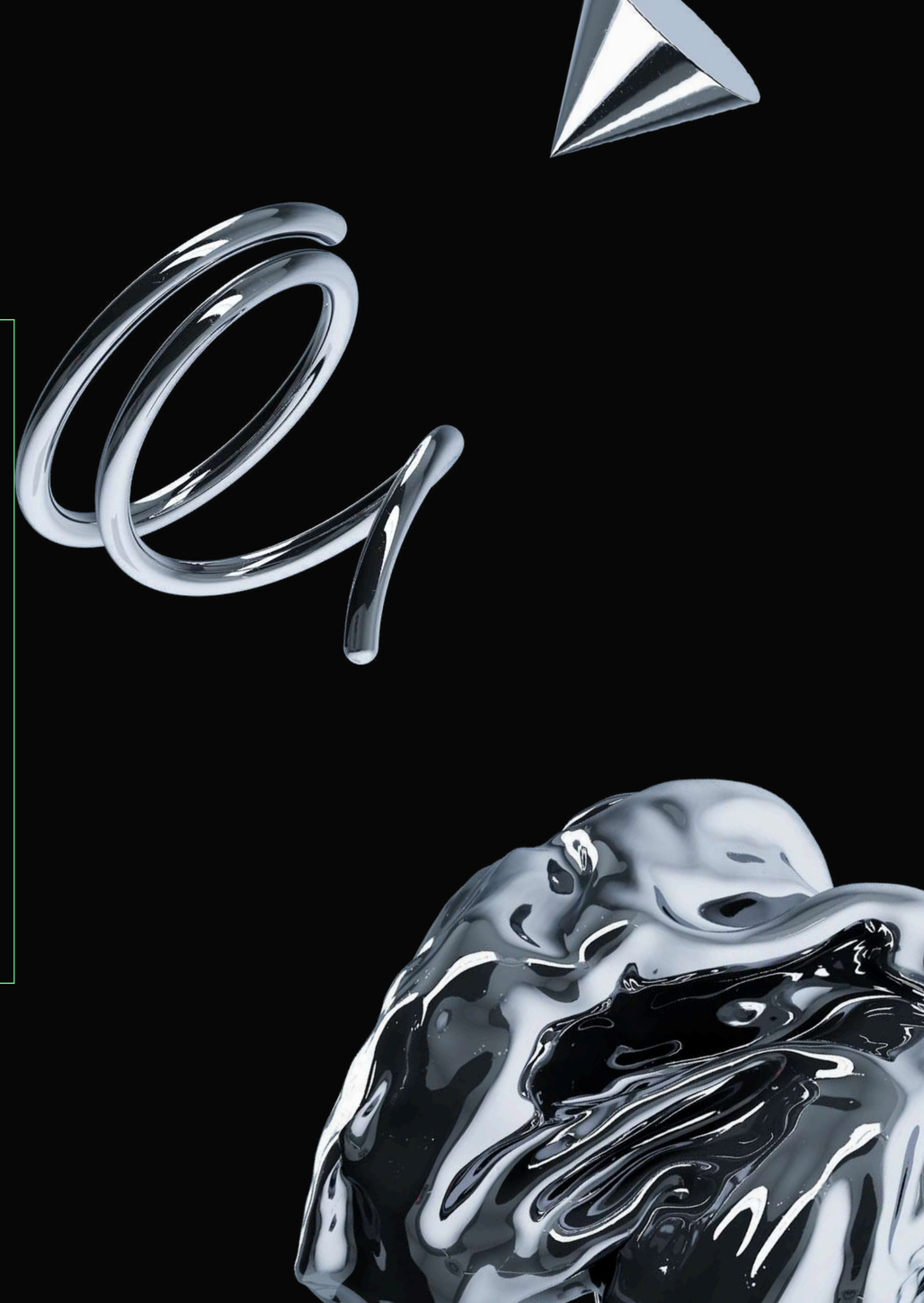
Based and Heuristic



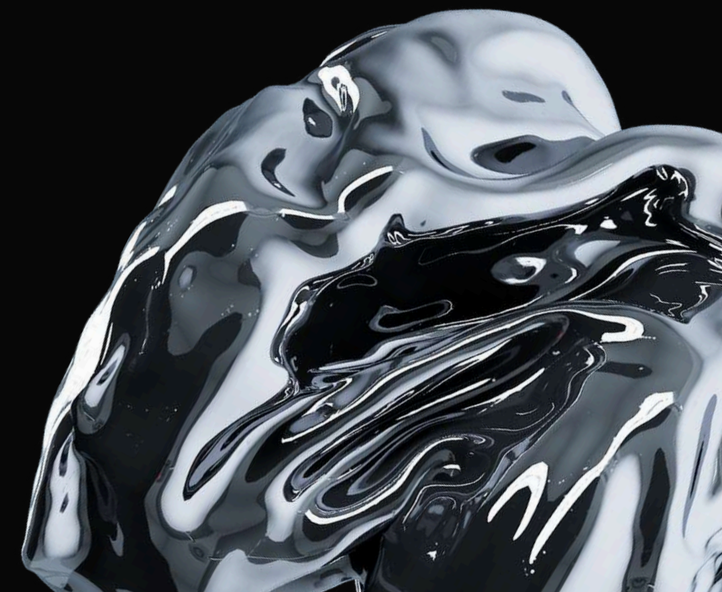
Simple metasploit Shellcode



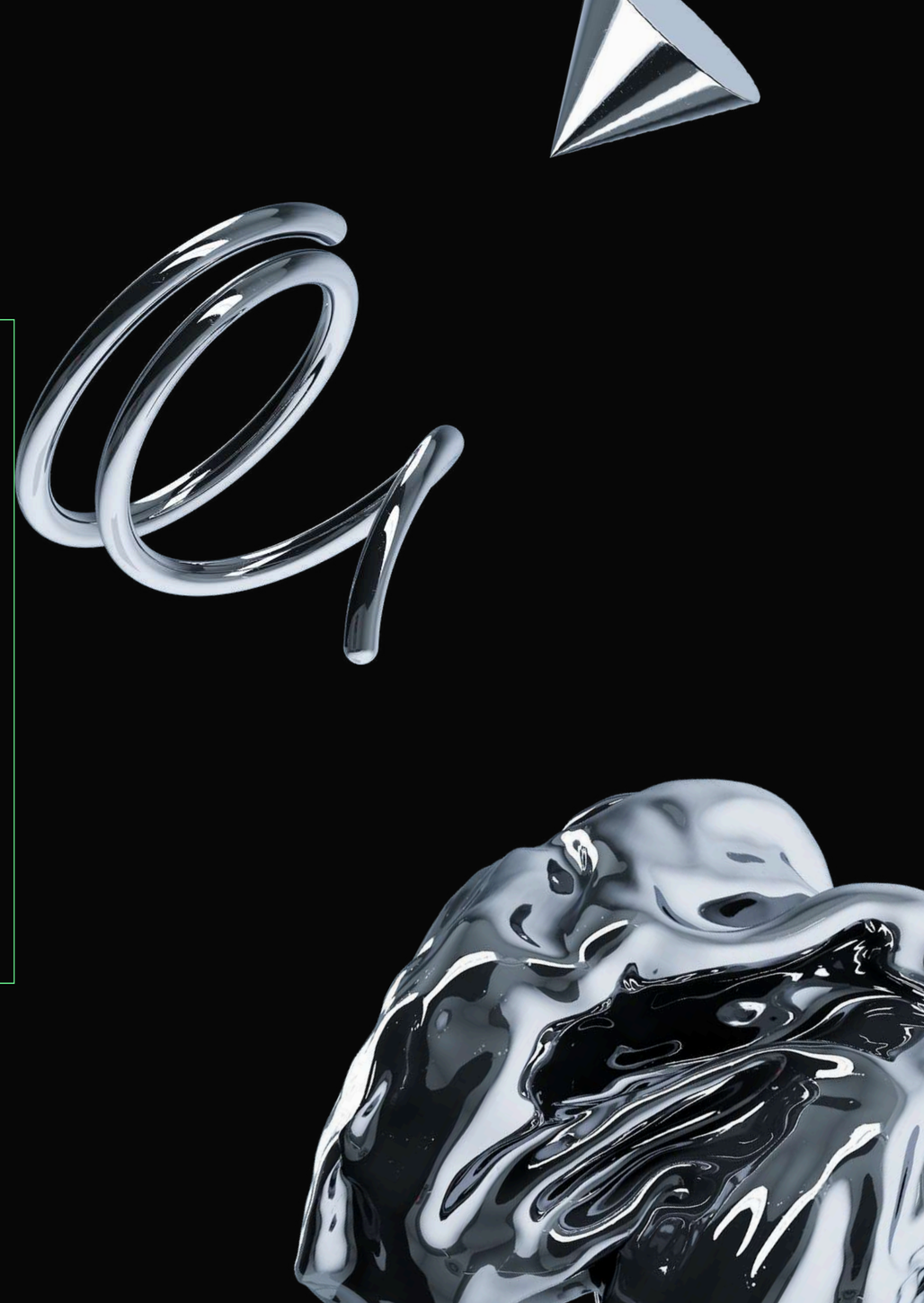
Virus Total test



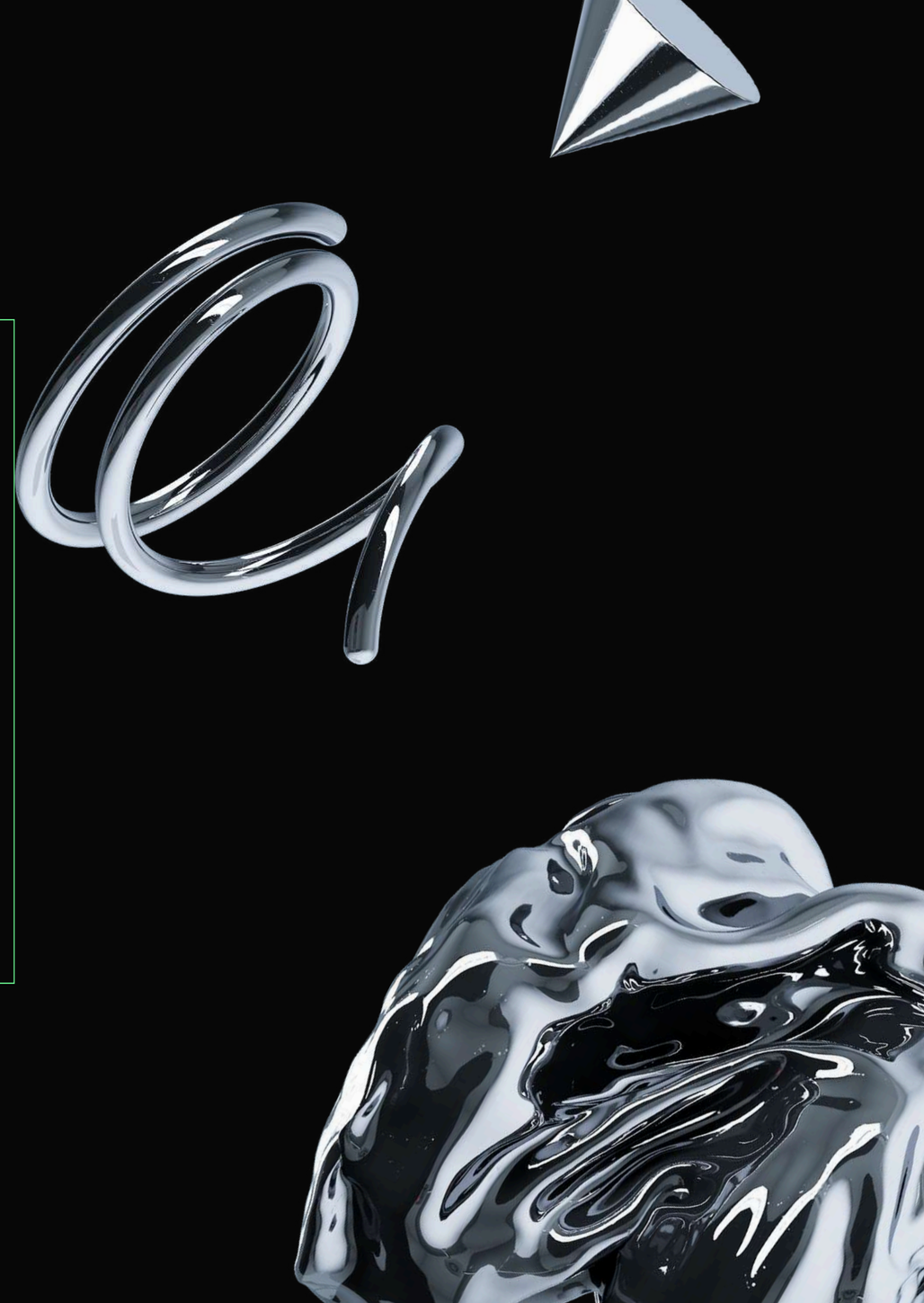
Simple metasploit x86 Shellcode



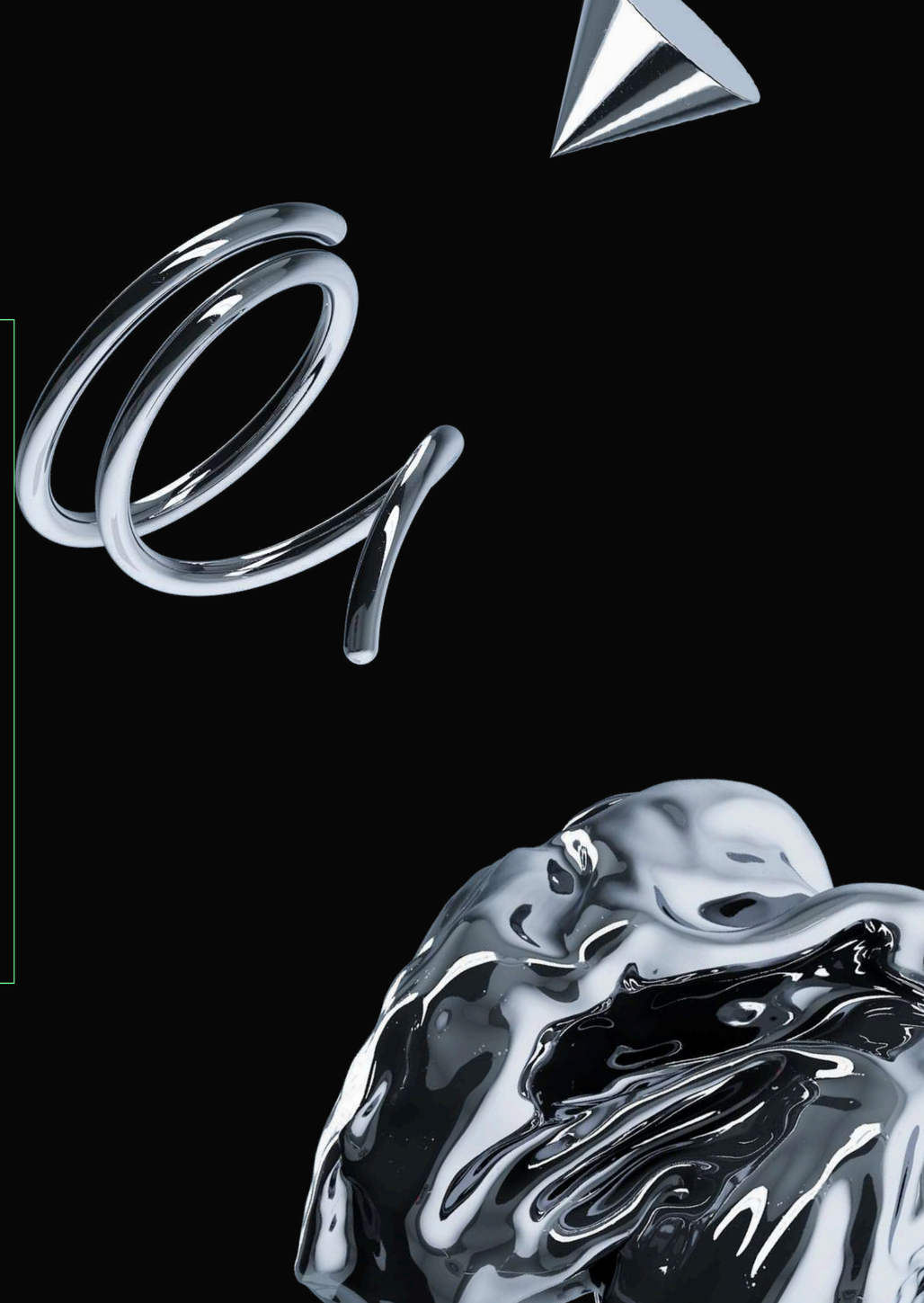
Virus Total test



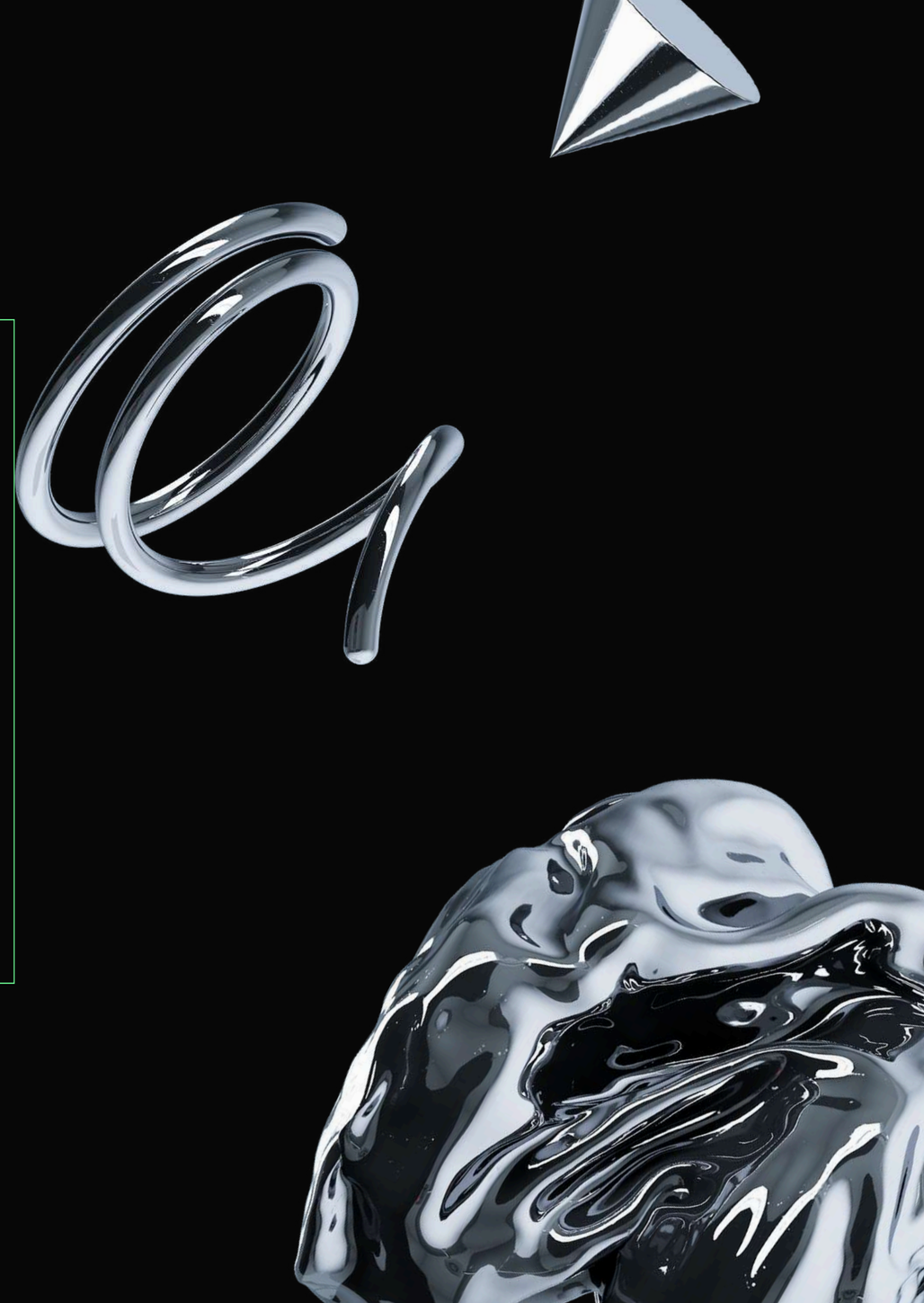
Empty Malware



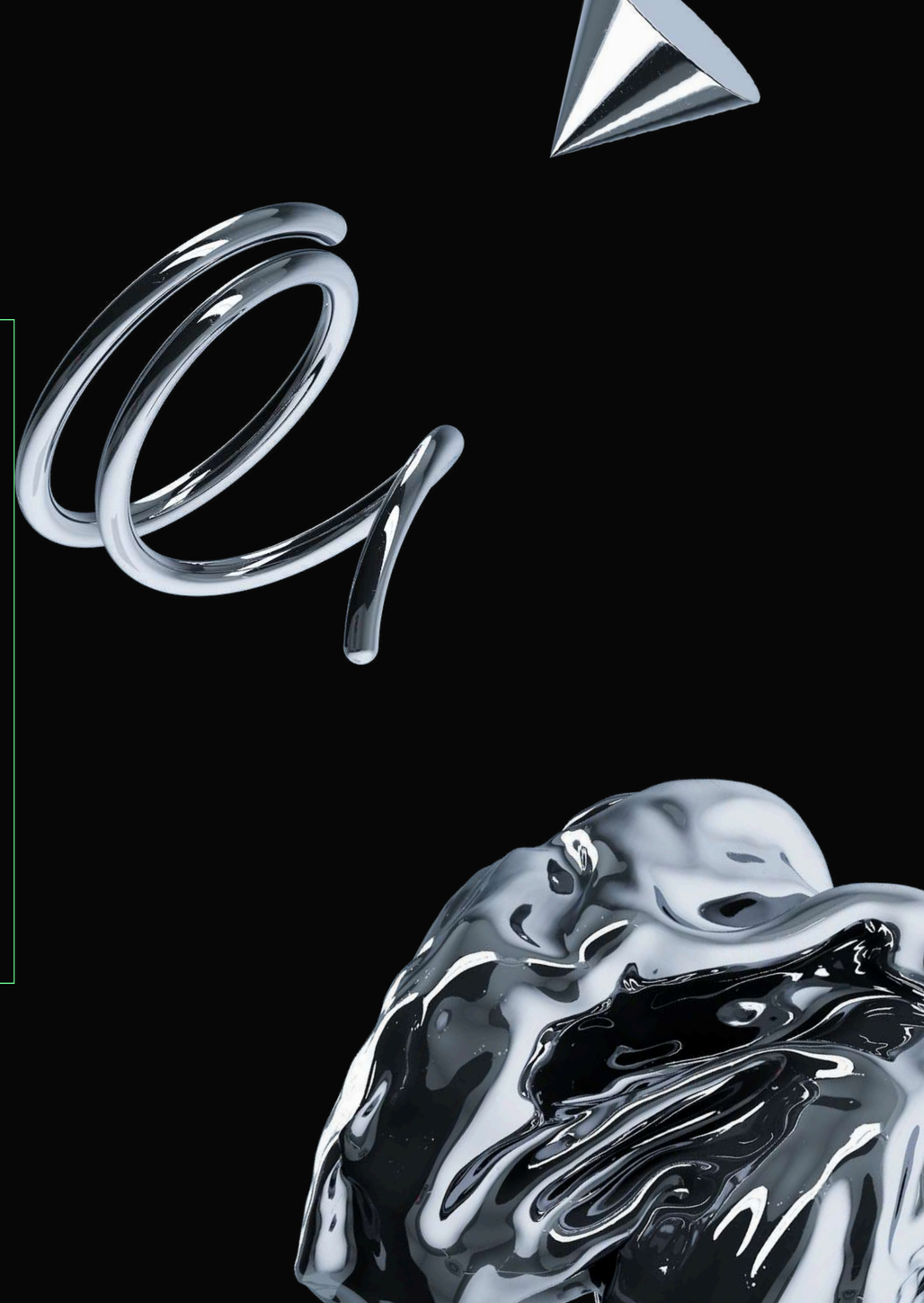
Virus Total test



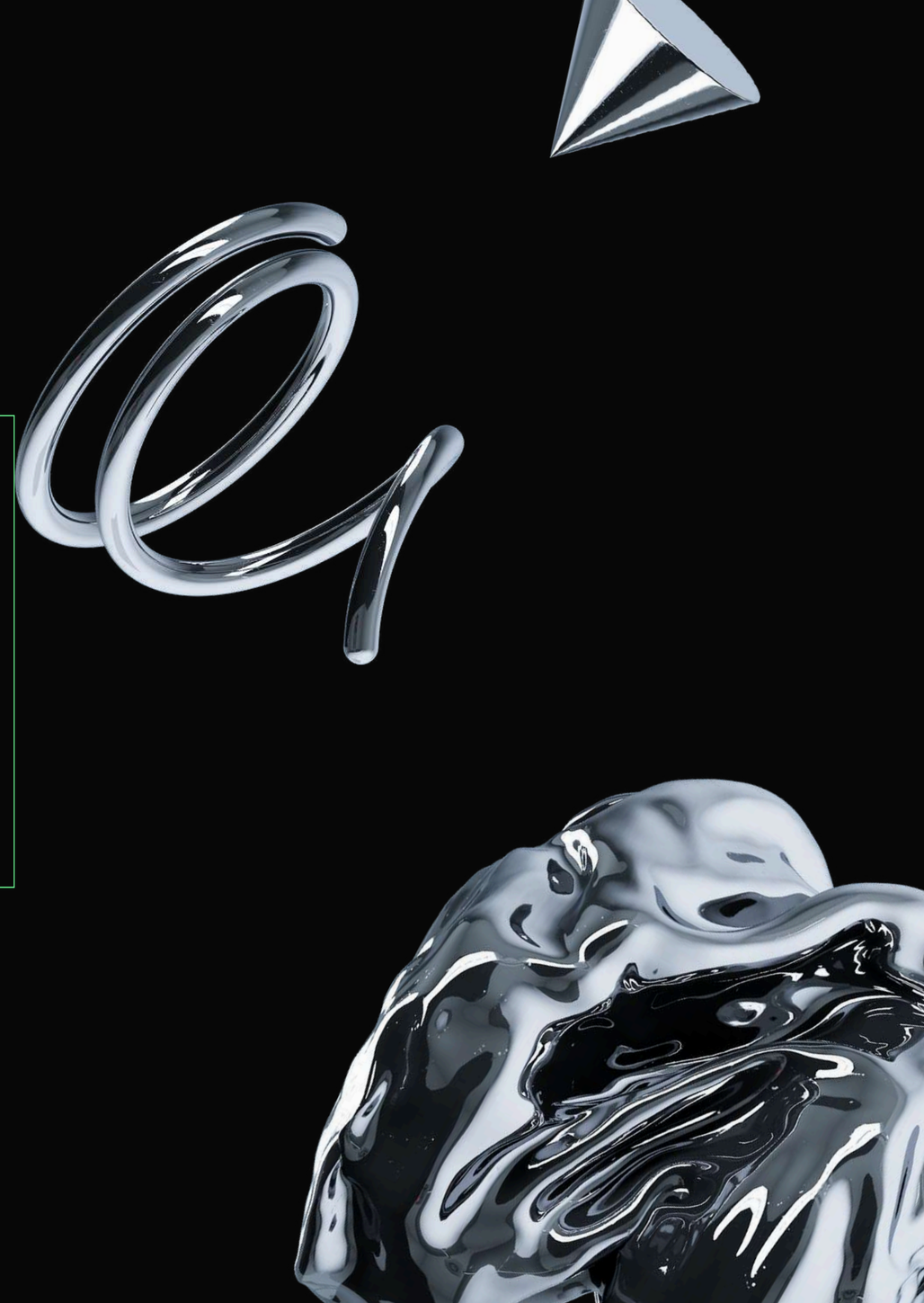
digital signature



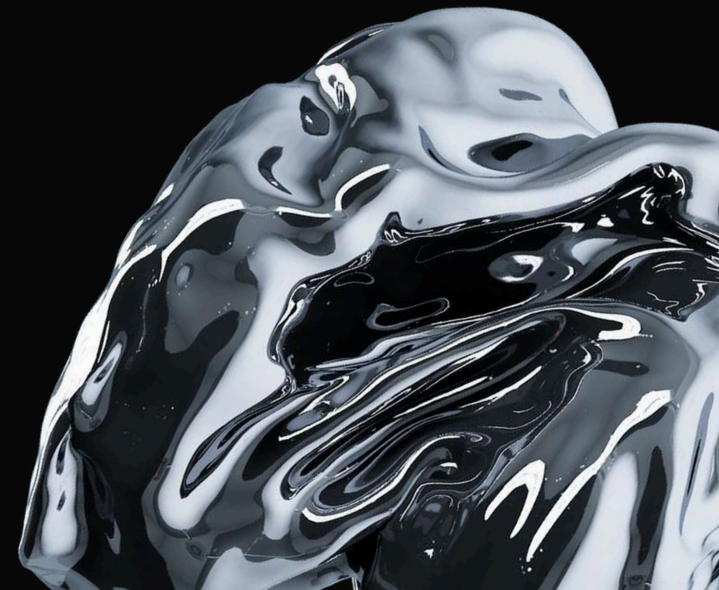
Shellcode Obfuscation



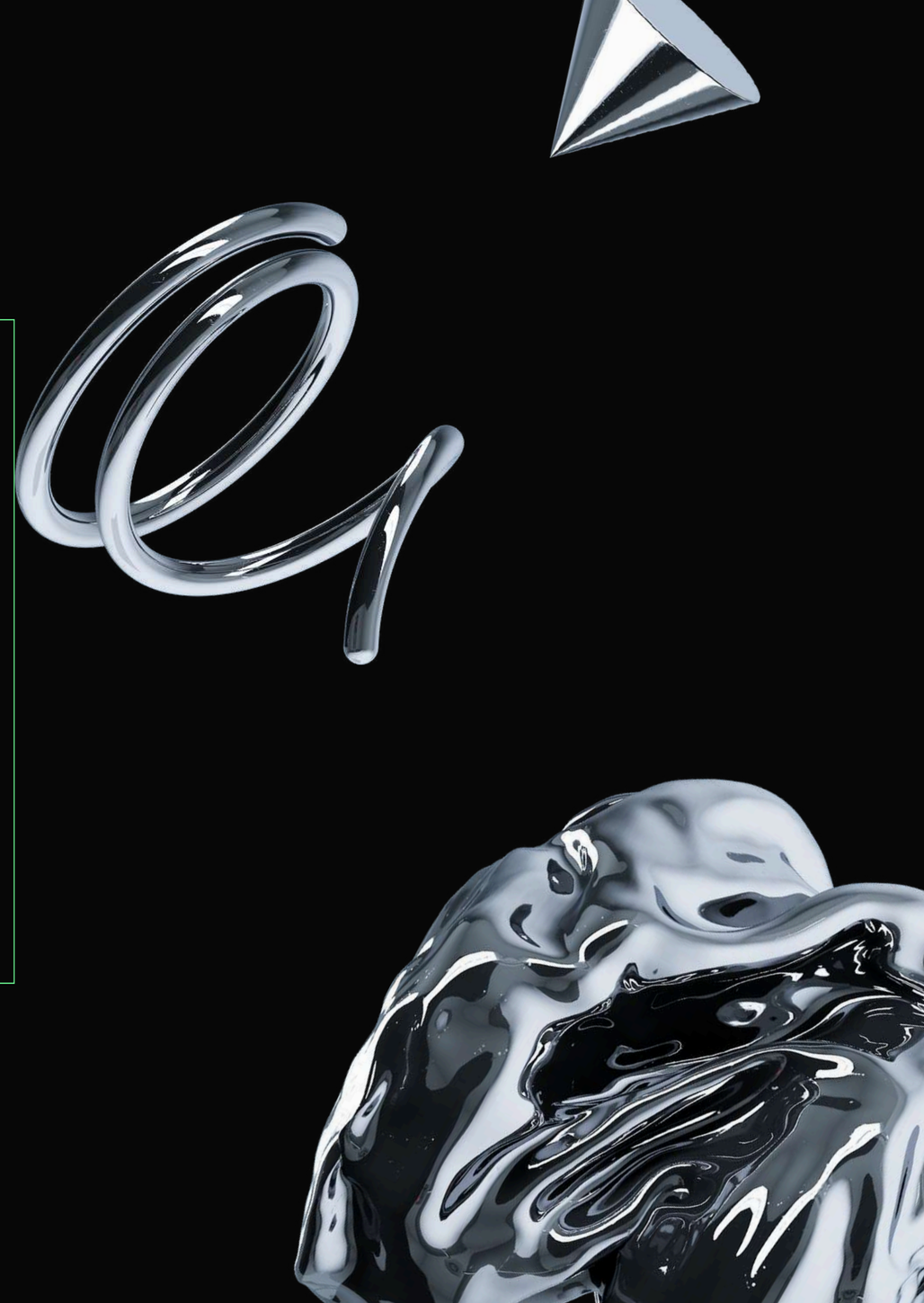
XOR enc



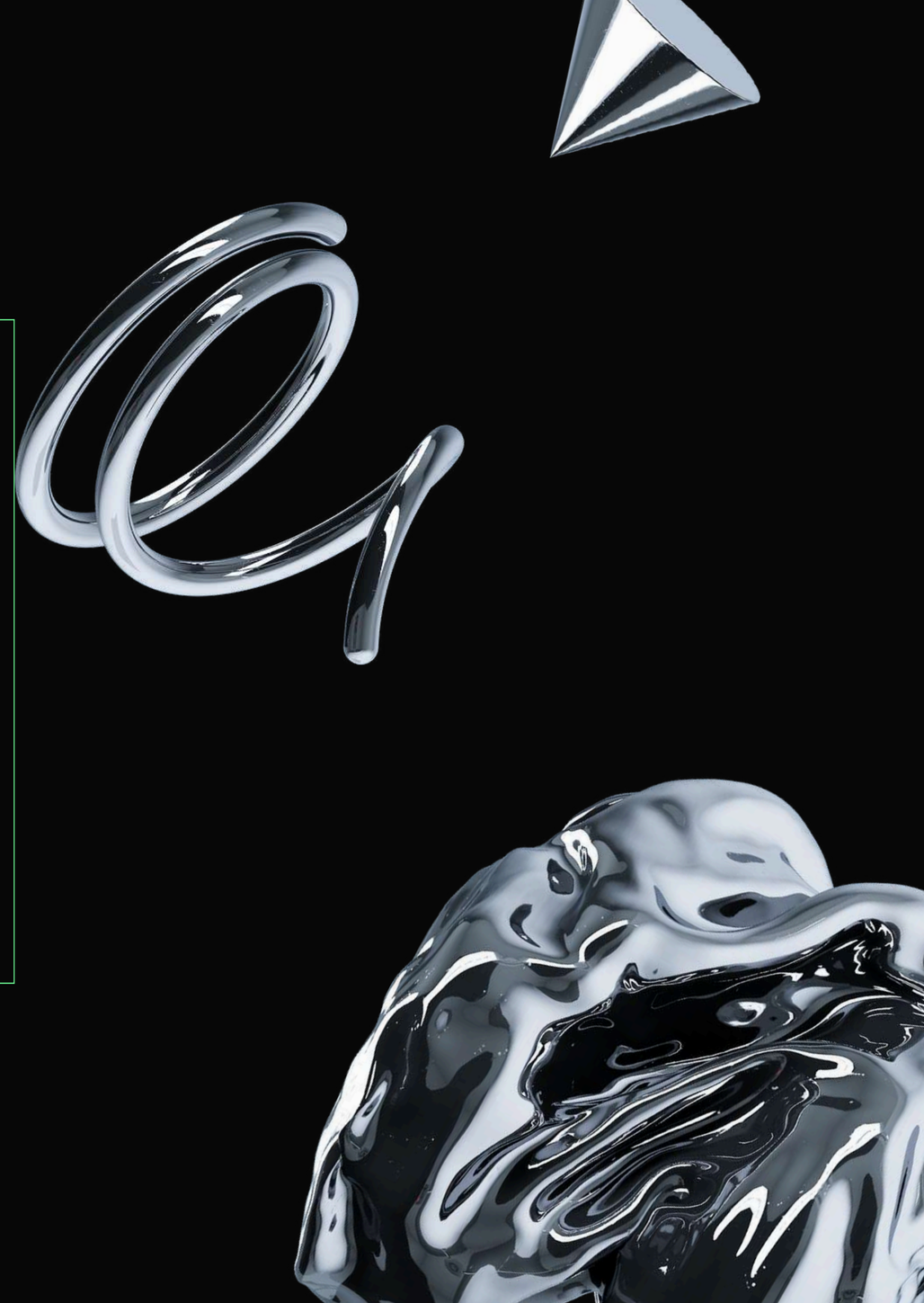
Check also the other repo for more obfuscation techniques



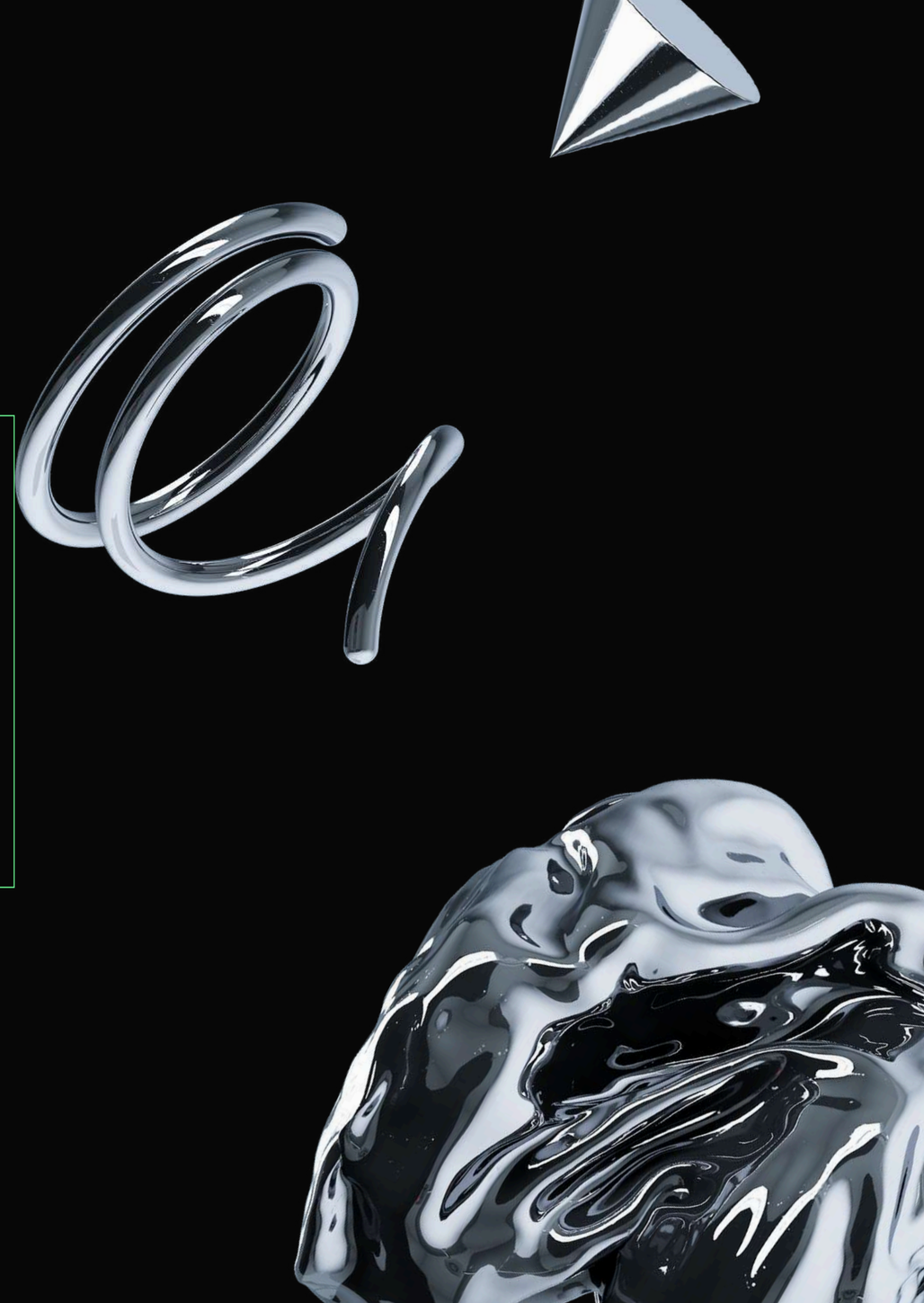
Dynamic Analysis



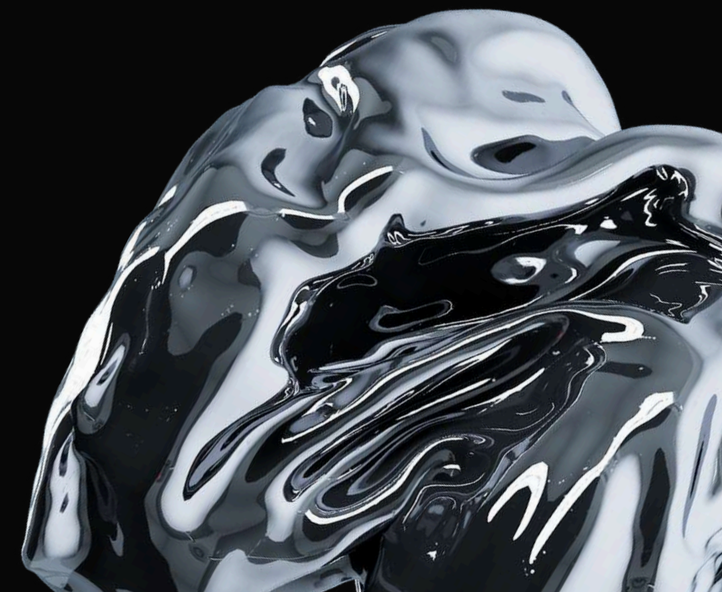
Anti Debugging



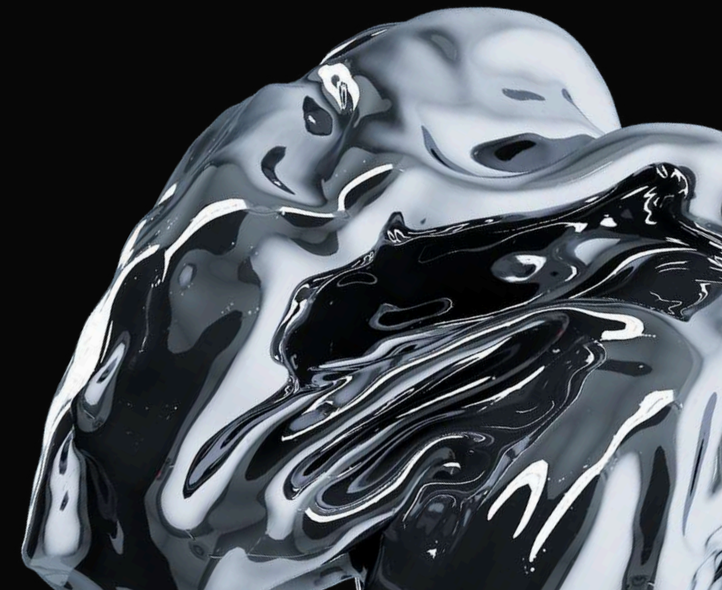
Anti Vm



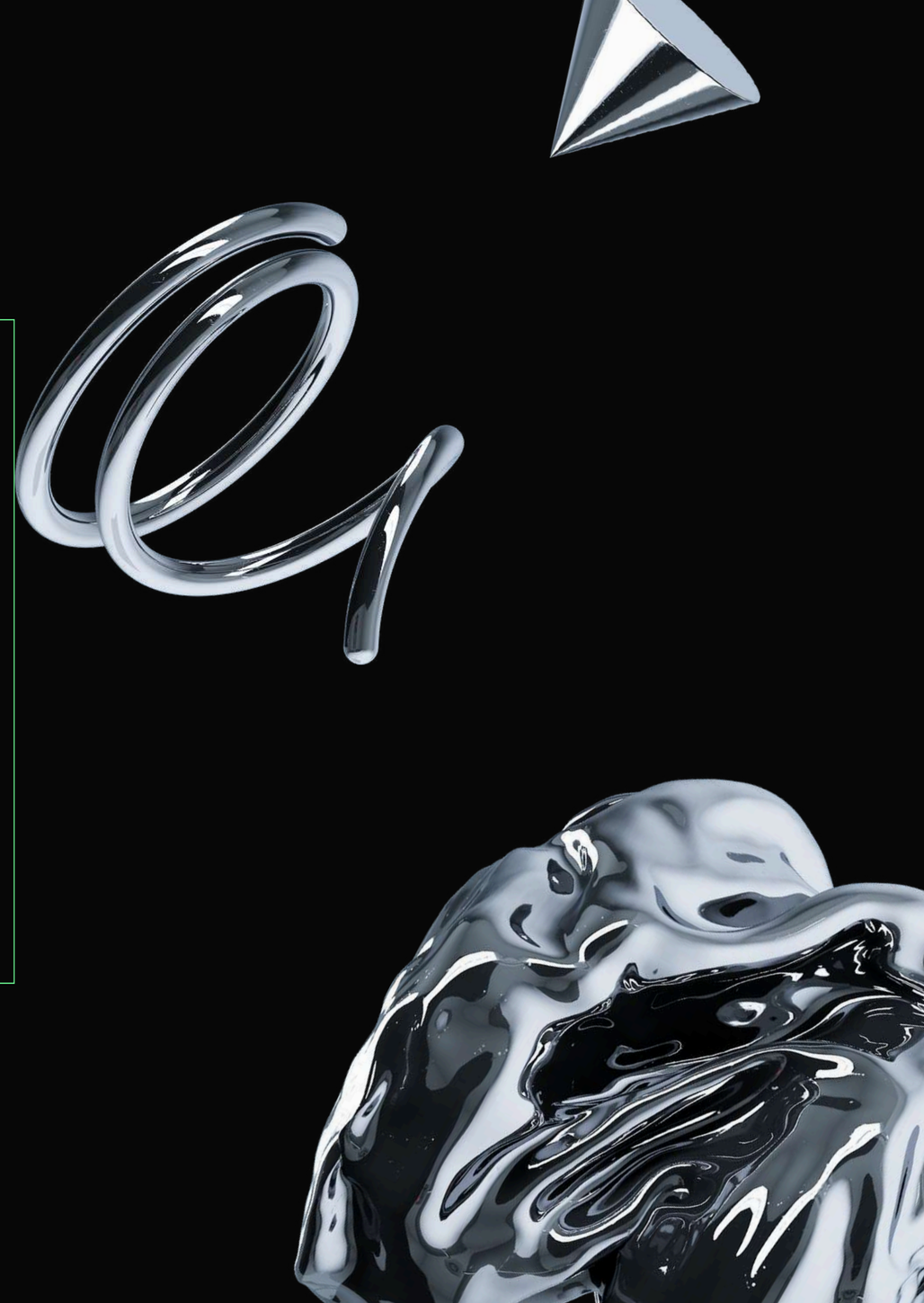
Cpu



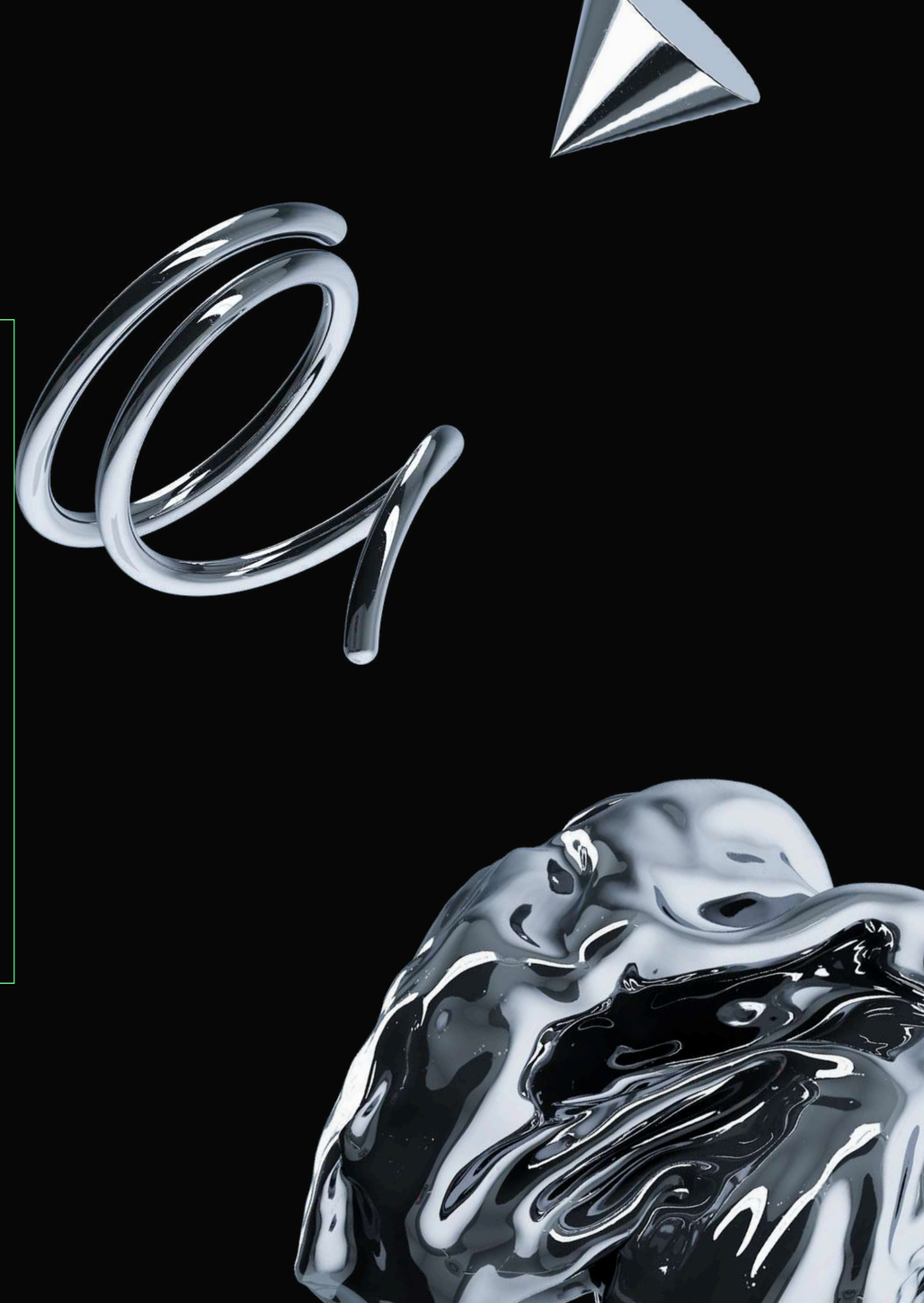
Ram and HDD



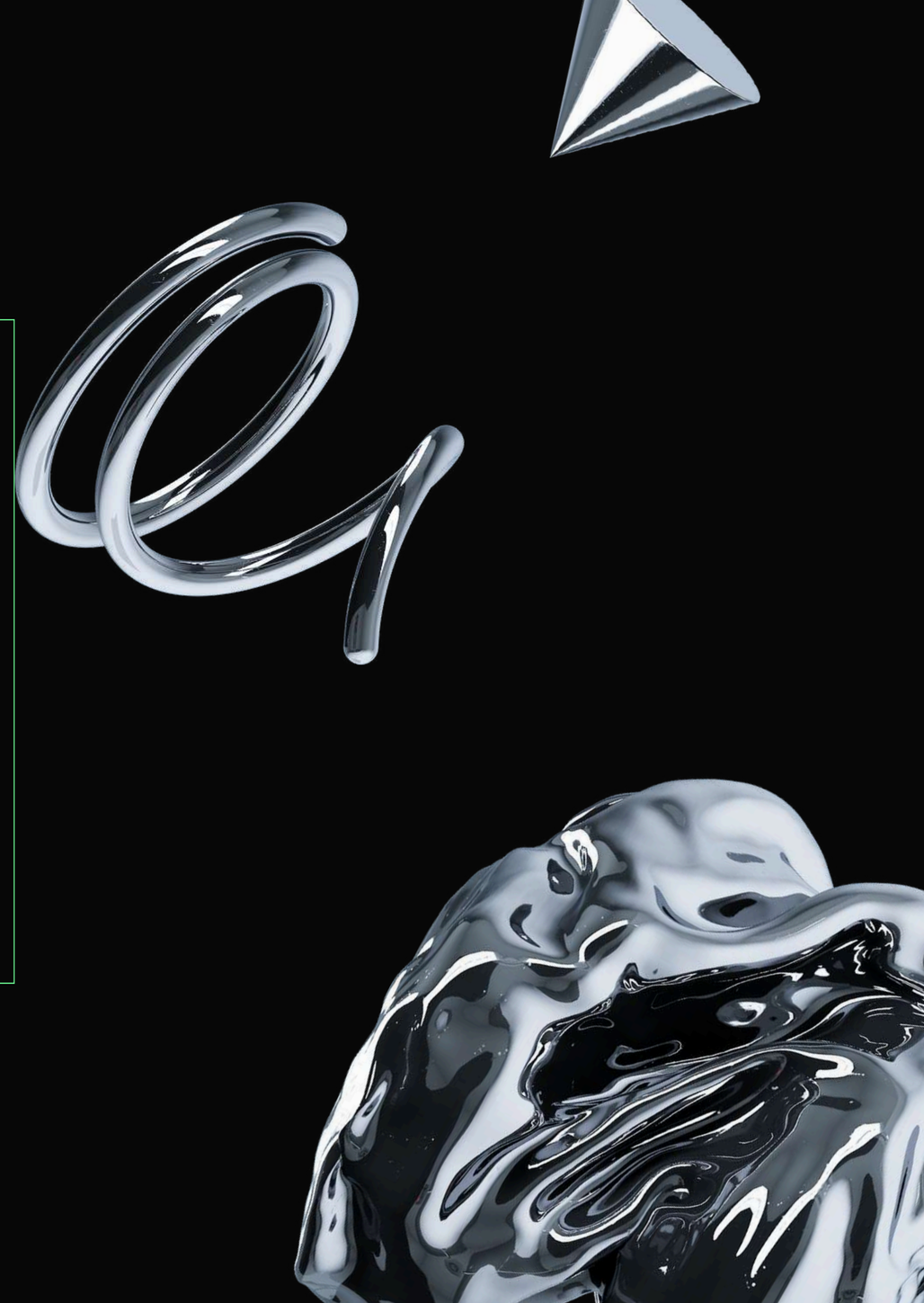
Mac addresses



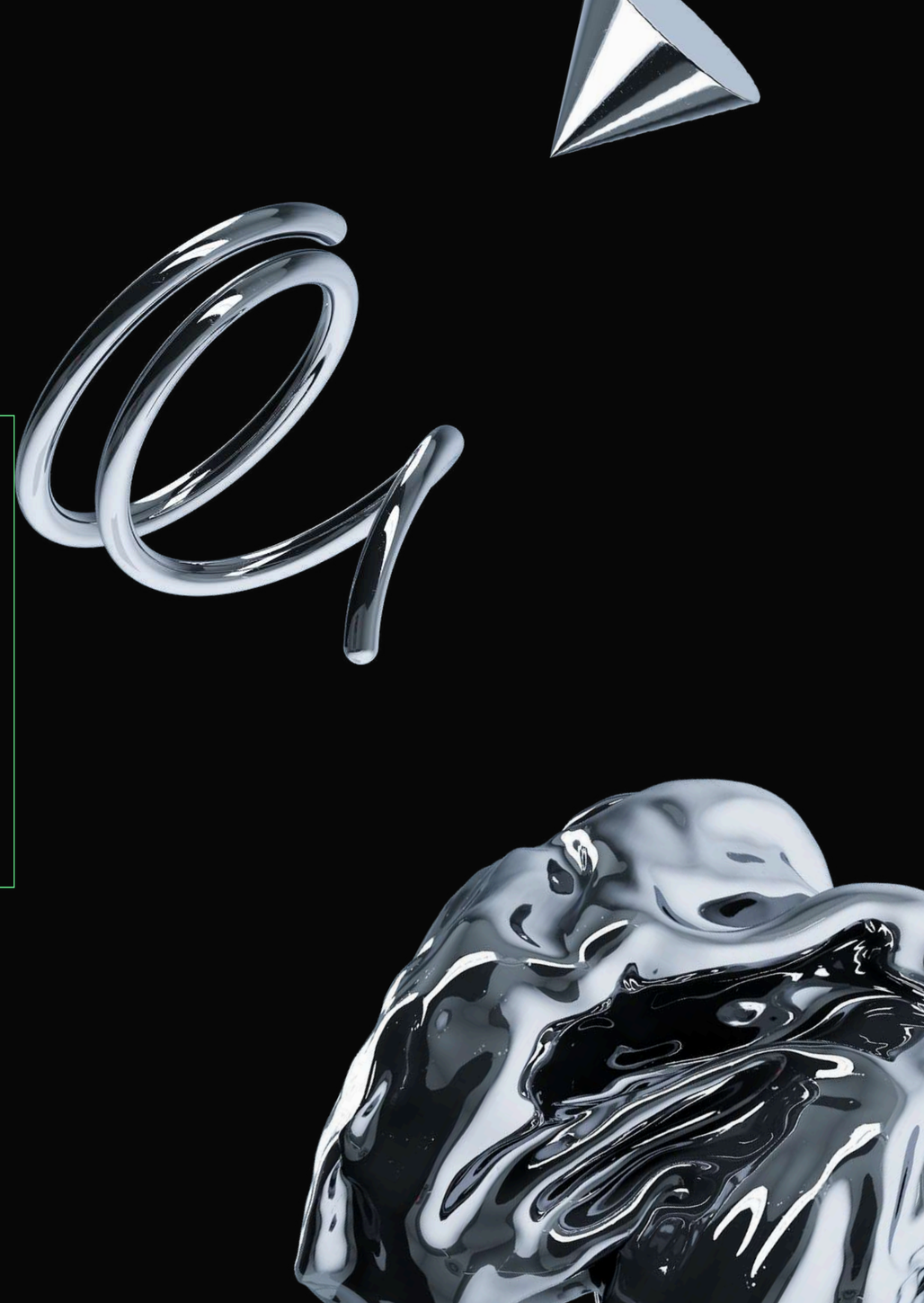
File path and folders



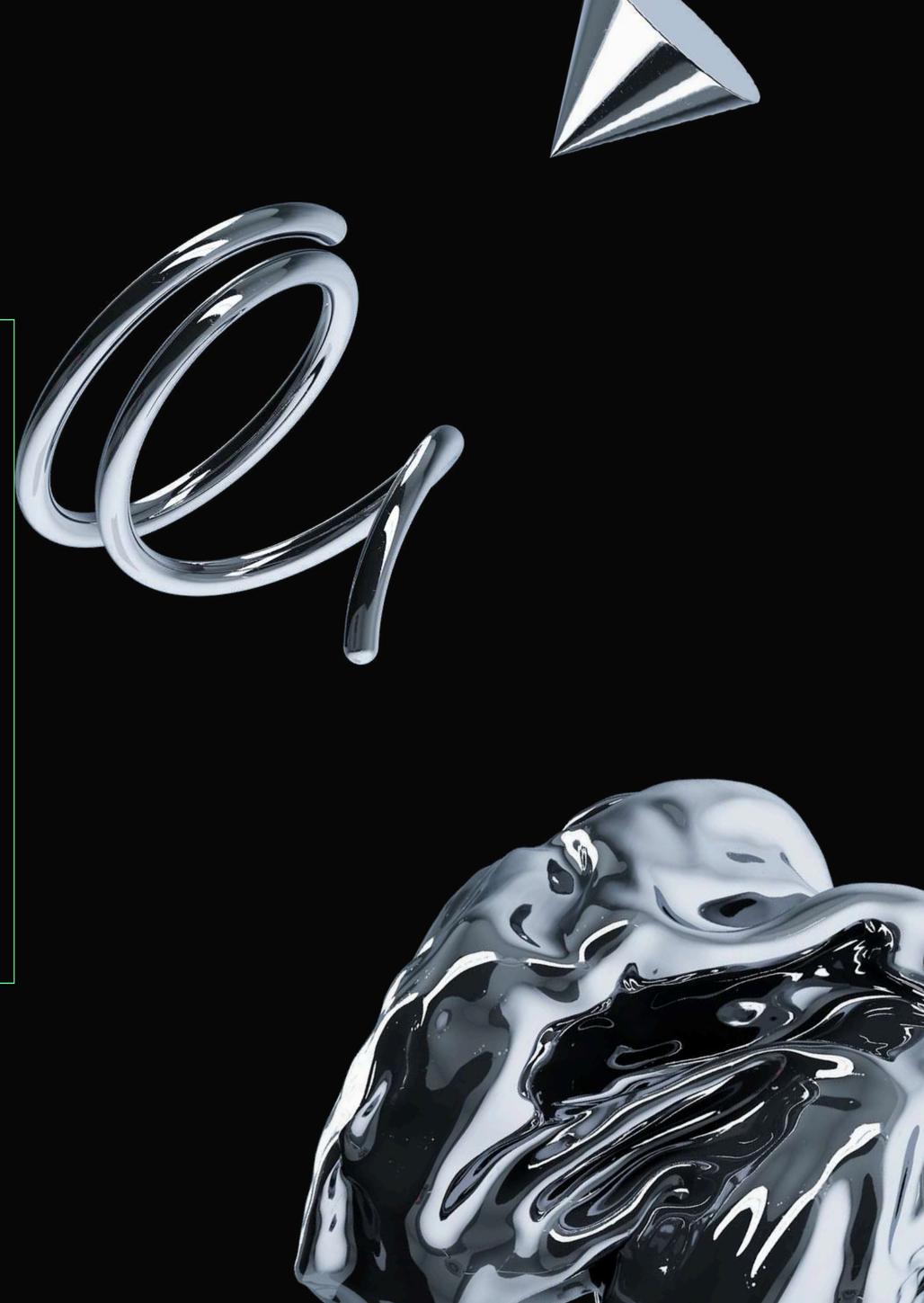
User interaction



Time Zone

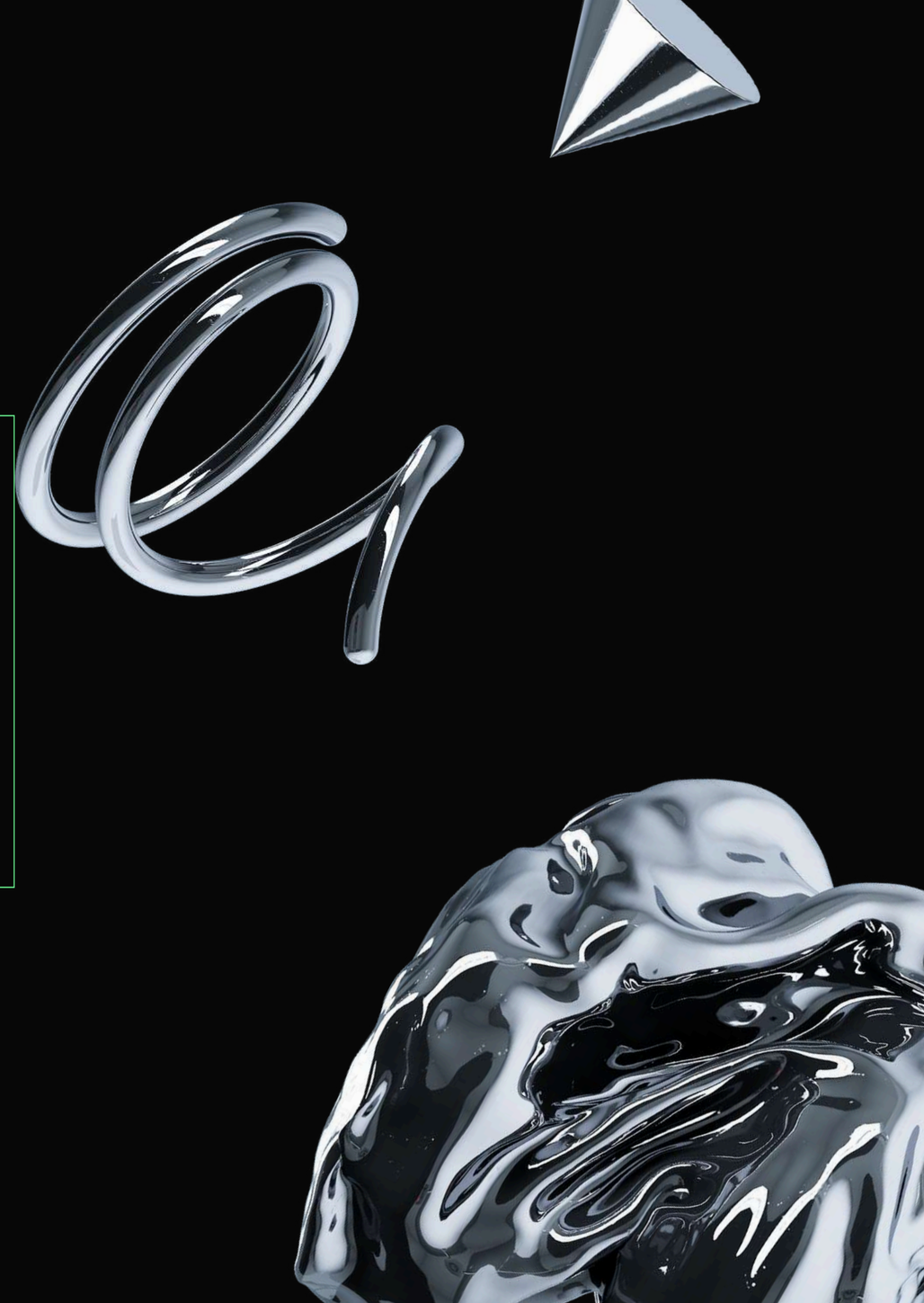


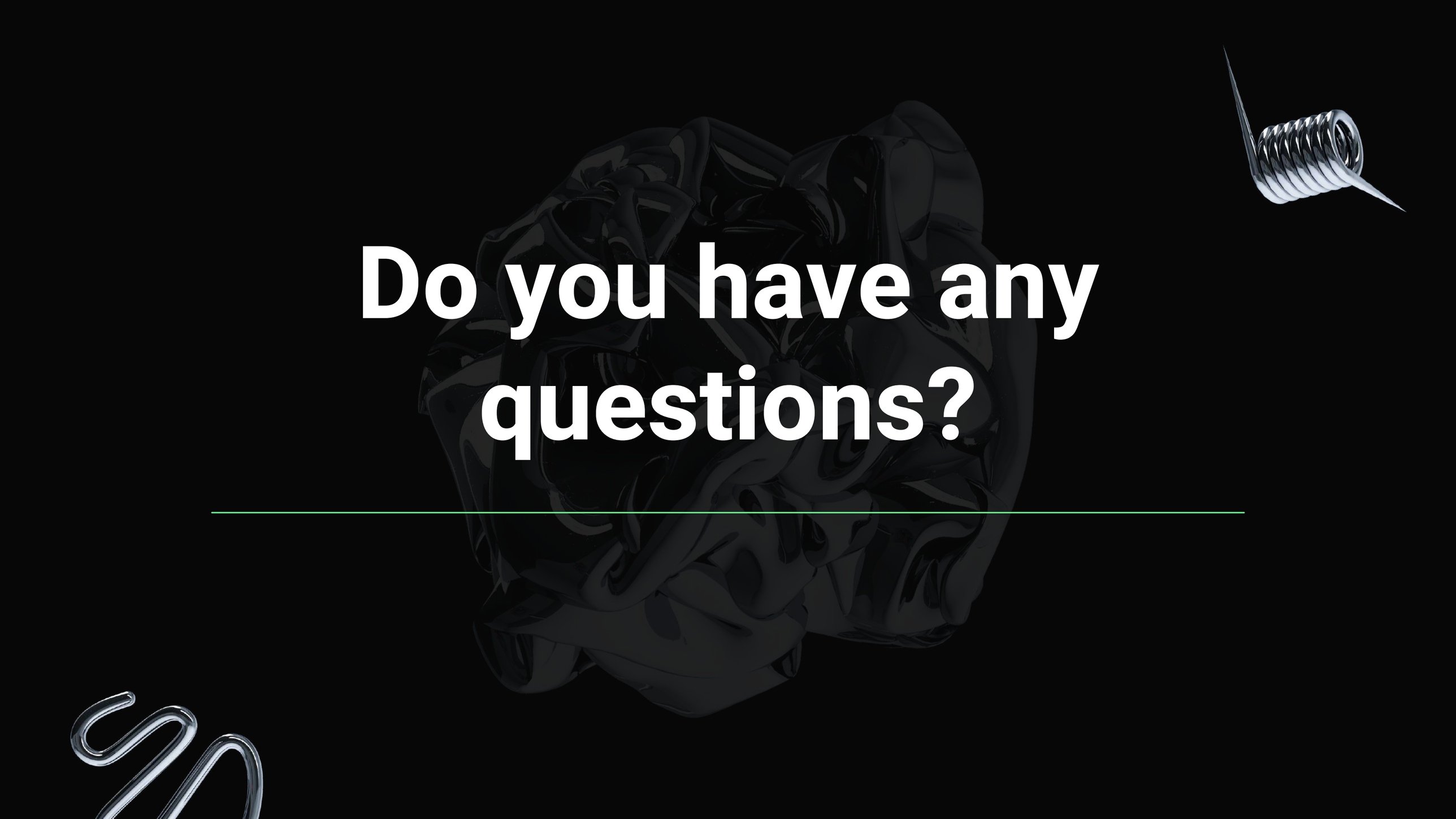
Running Processes



Done!

Ressources




Do you have any
questions?