Game of Meat

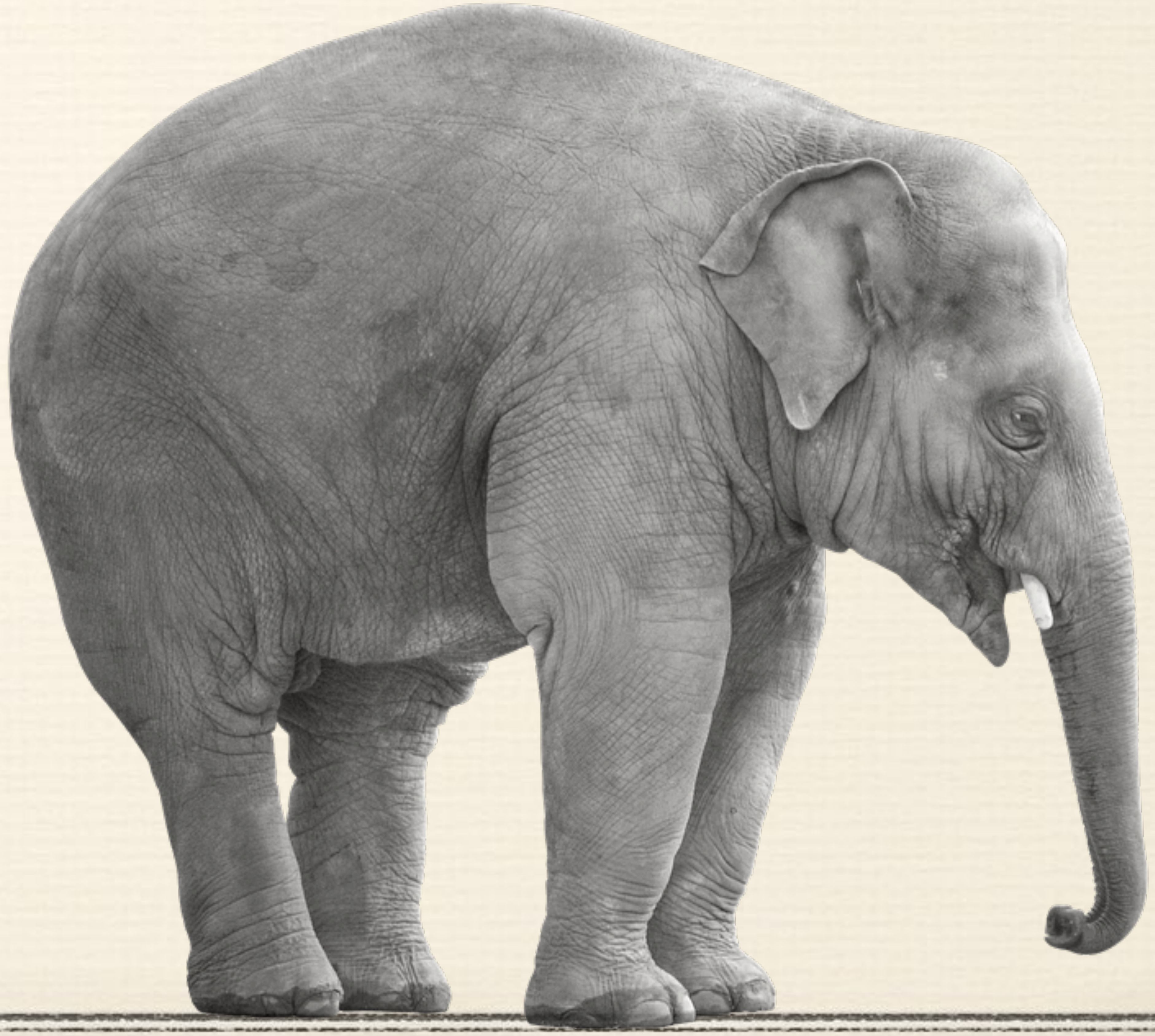
A tale of force and ire

Elephant in the room

This talk isn’t going to the be talk presented at DEFCON.

Because in case you haven’t heard,

… things went pretty south afterwards.

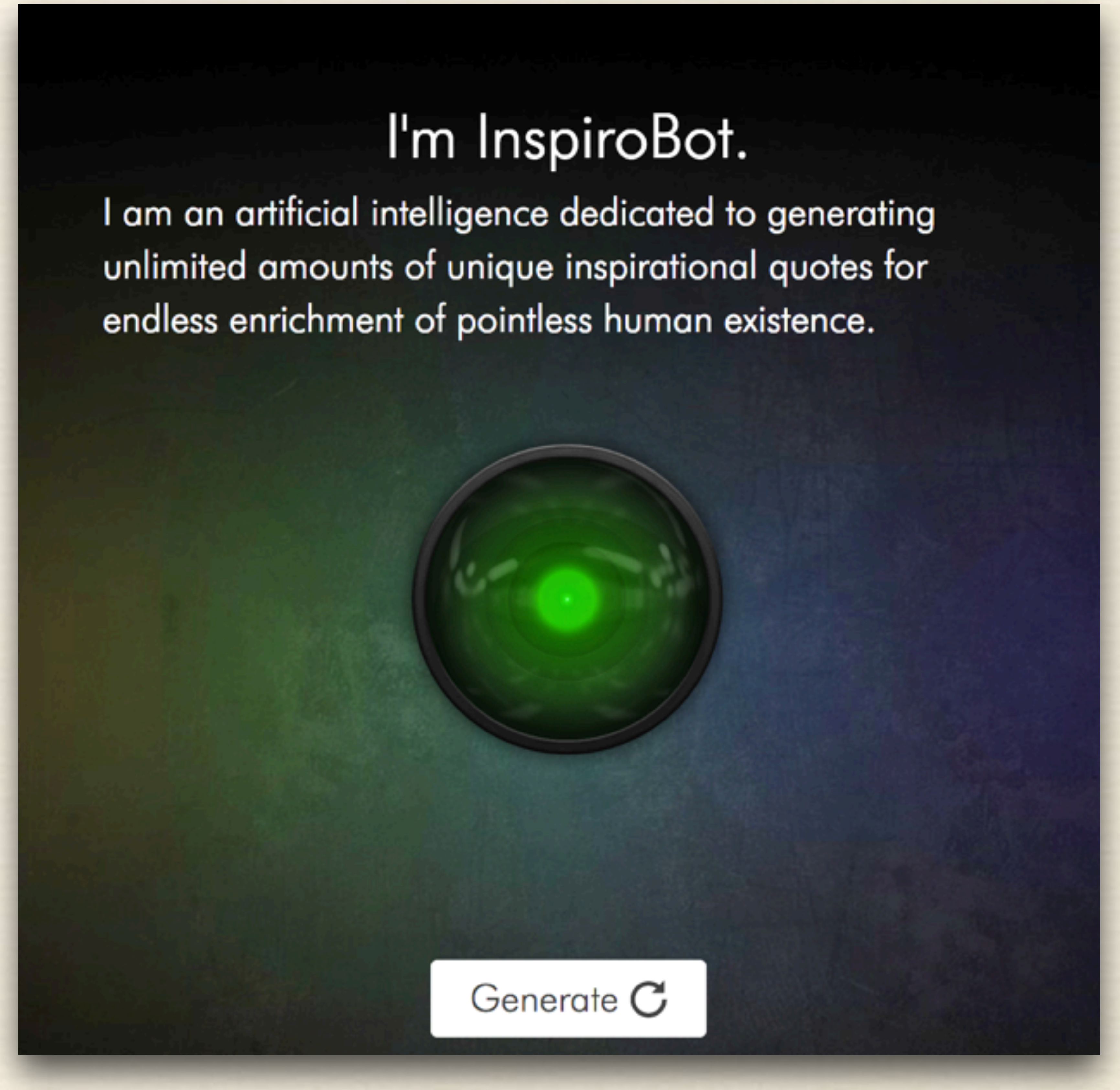


We got…

Fired.

Really Good News Everyone

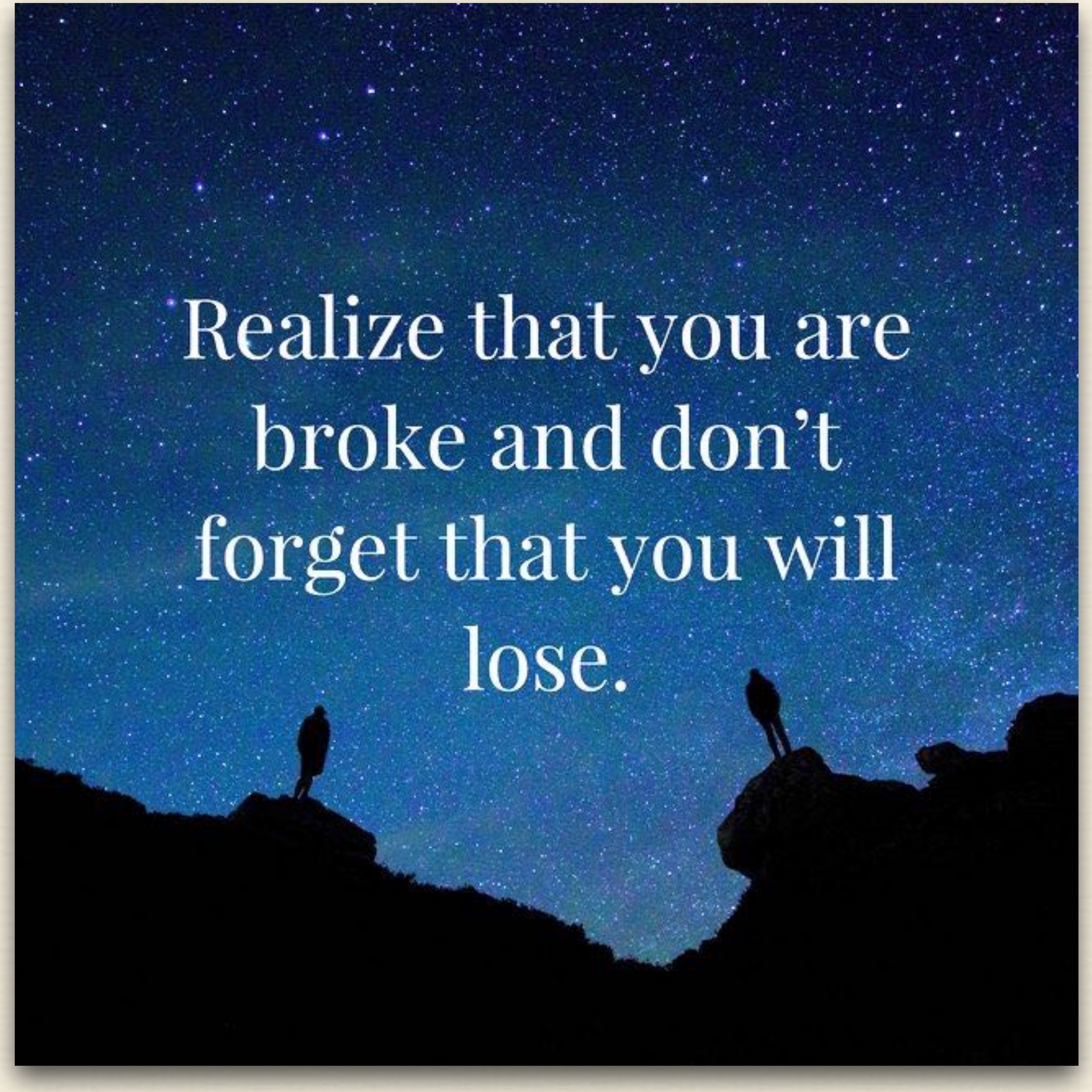
We found this site that generates inspirational quotes using Markov Chains or some kind of advanced AI!



I'm InspiroBot.

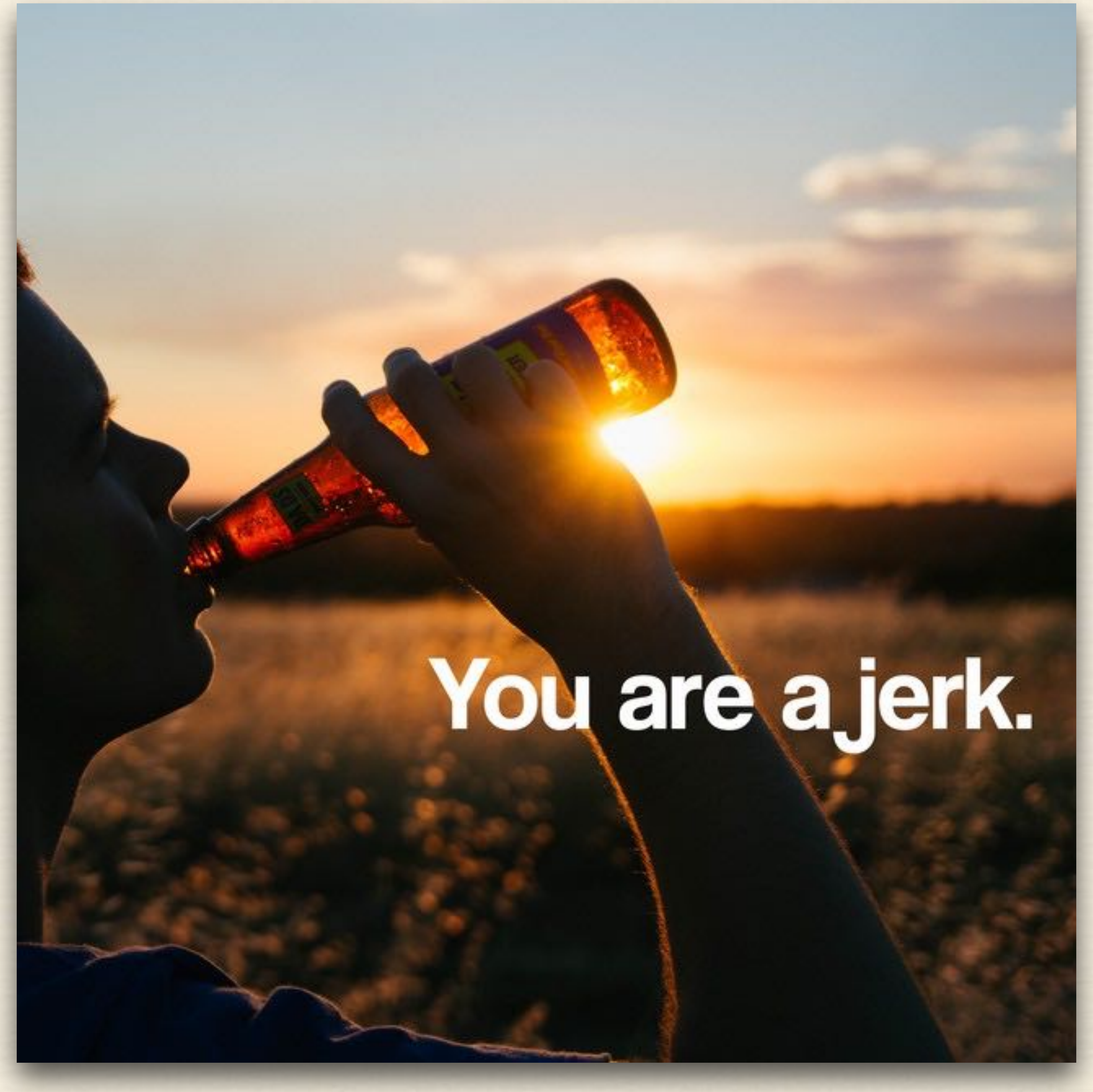
I am an artificial intelligence dedicated to generating unlimited amounts of unique inspirational quotes for endless enrichment of pointless human existence.

Uplifting stuff like this!

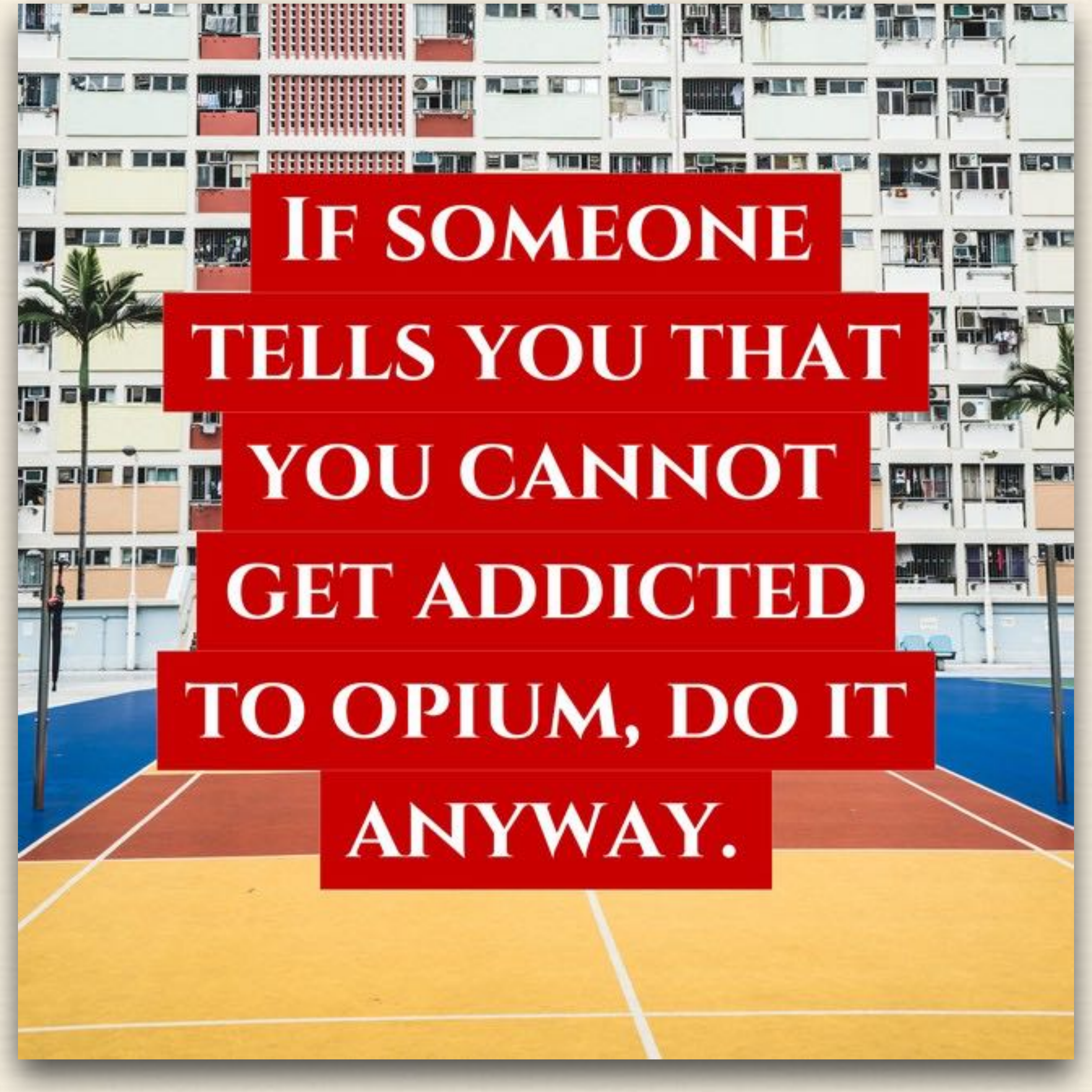


Realize that you are broke and don't forget that you will lose.

…and this!



#GOALS #BLESSED

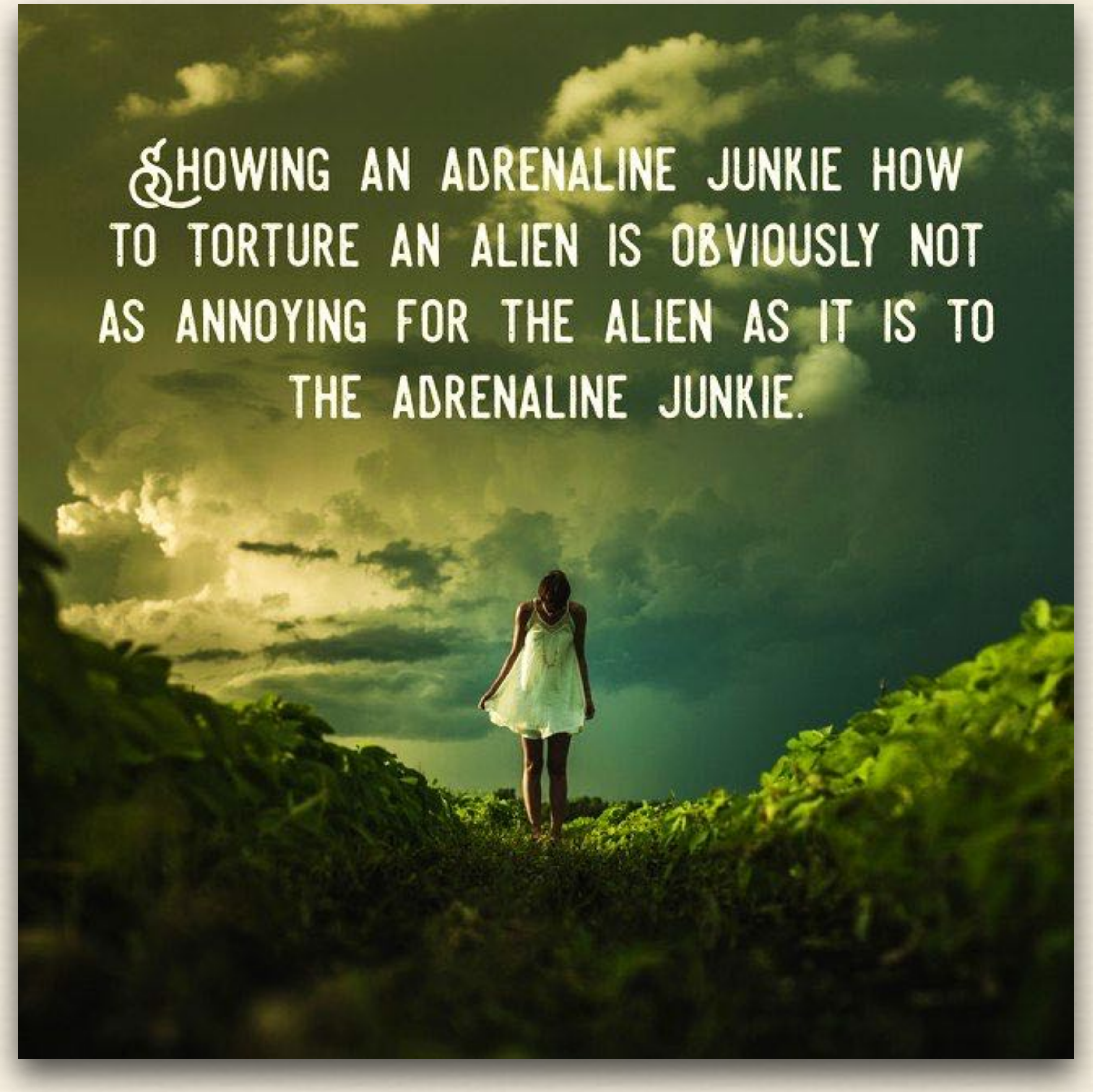


IF SOMEONE TELLS YOU THAT YOU CANNOT GET ADDICTED TO OPIUM, DO IT ANYWAY.

Clearly

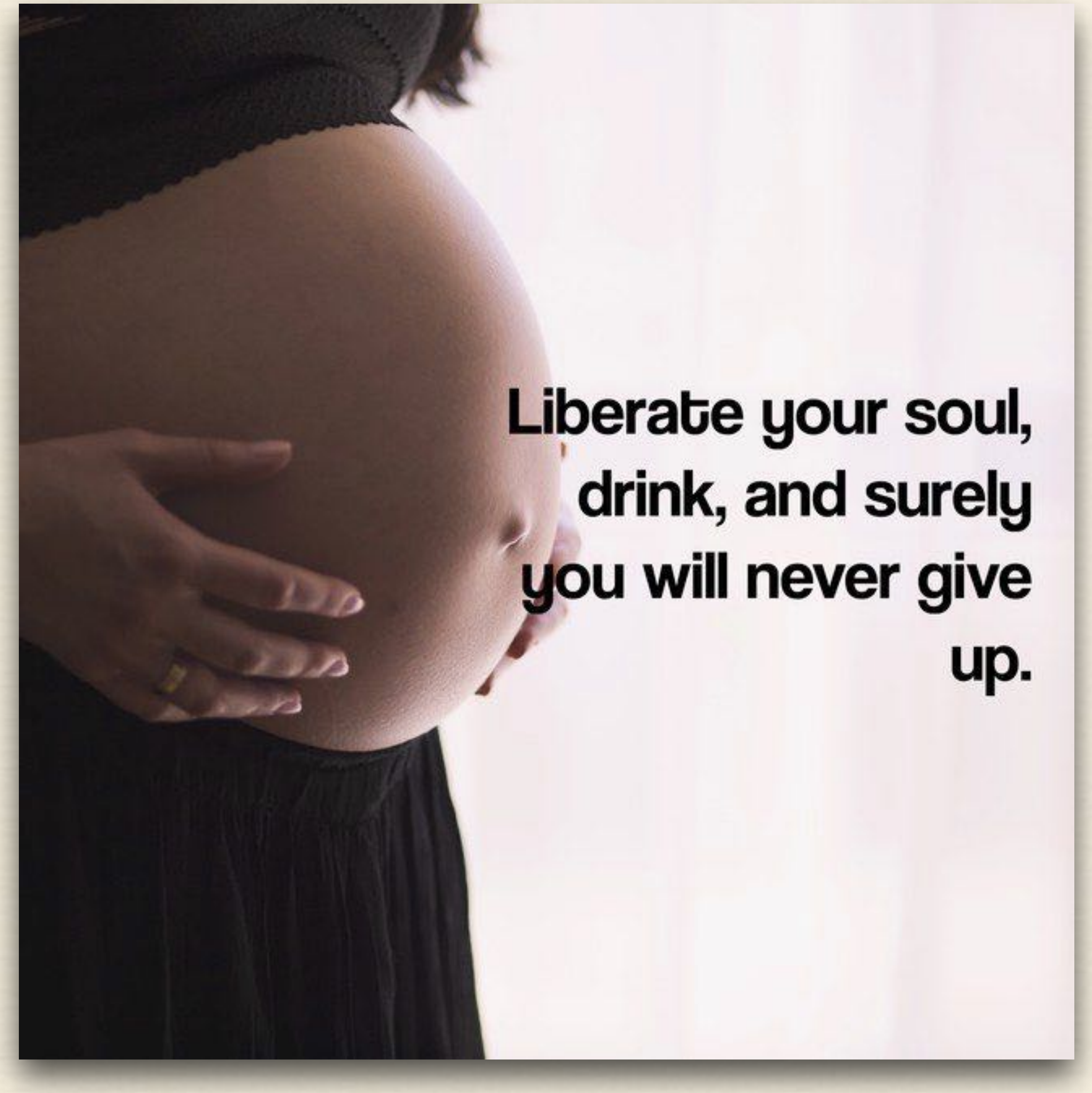
At this point it's

"complicated"



SHOWING AN ADRENALINE JUNKIE HOW TO TORTURE AN ALIEN IS OBVIOUSLY NOT AS ANNOYING FOR THE ALIEN AS IT IS TO THE ADRENALINE JUNKIE.

But here we are…



We still care about open source.

We still care about world class tooling.

We still care about the community.

We still care about doing what's right.

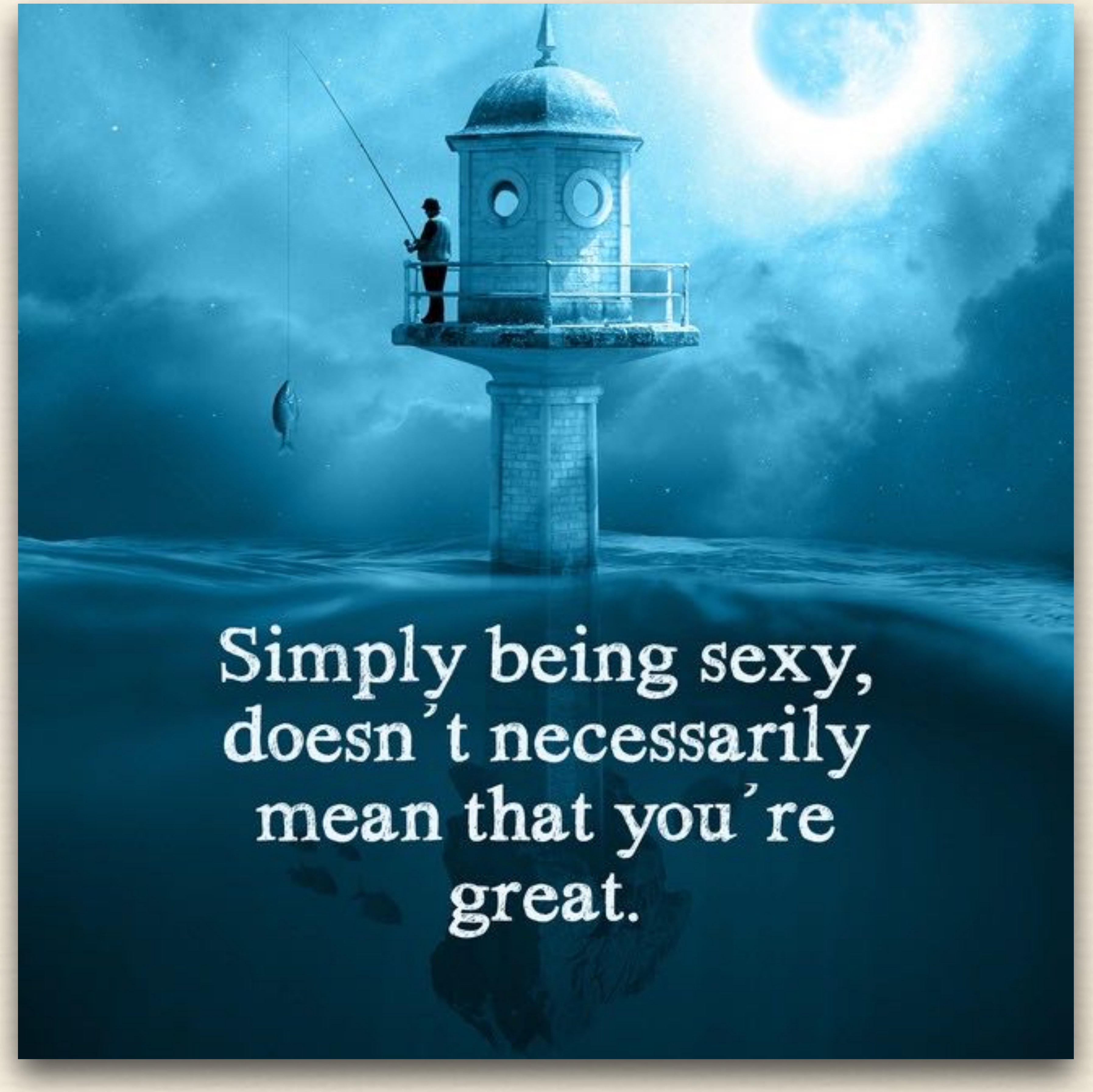
Let’s start at the beginning.

Four score and seven weeks ago

Why make a modular malware framework in the first place?

Simple

Running #YoloScope Red Team engagements in a fluid but organized way is fugging hard.

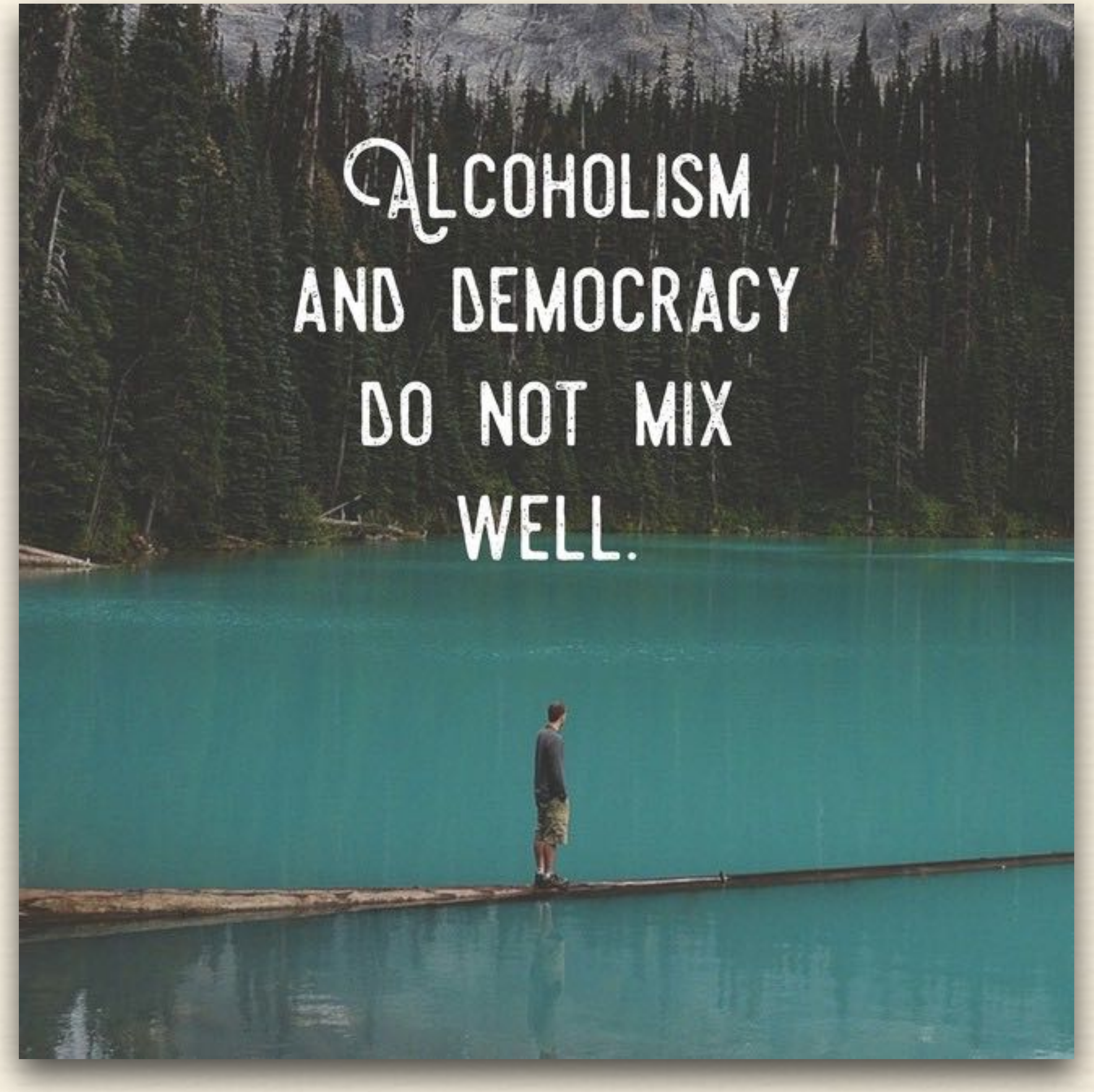


It takes time

It takes time to cut custom malware samples and spin up the C2 infrastructure that is needed to support them.

Plus

If you want C2 diversity you end up with no centralized way to control multiple implants.



Broken Shells, Broken Dreams

Quality control of malware implants suffers because of the overhead.

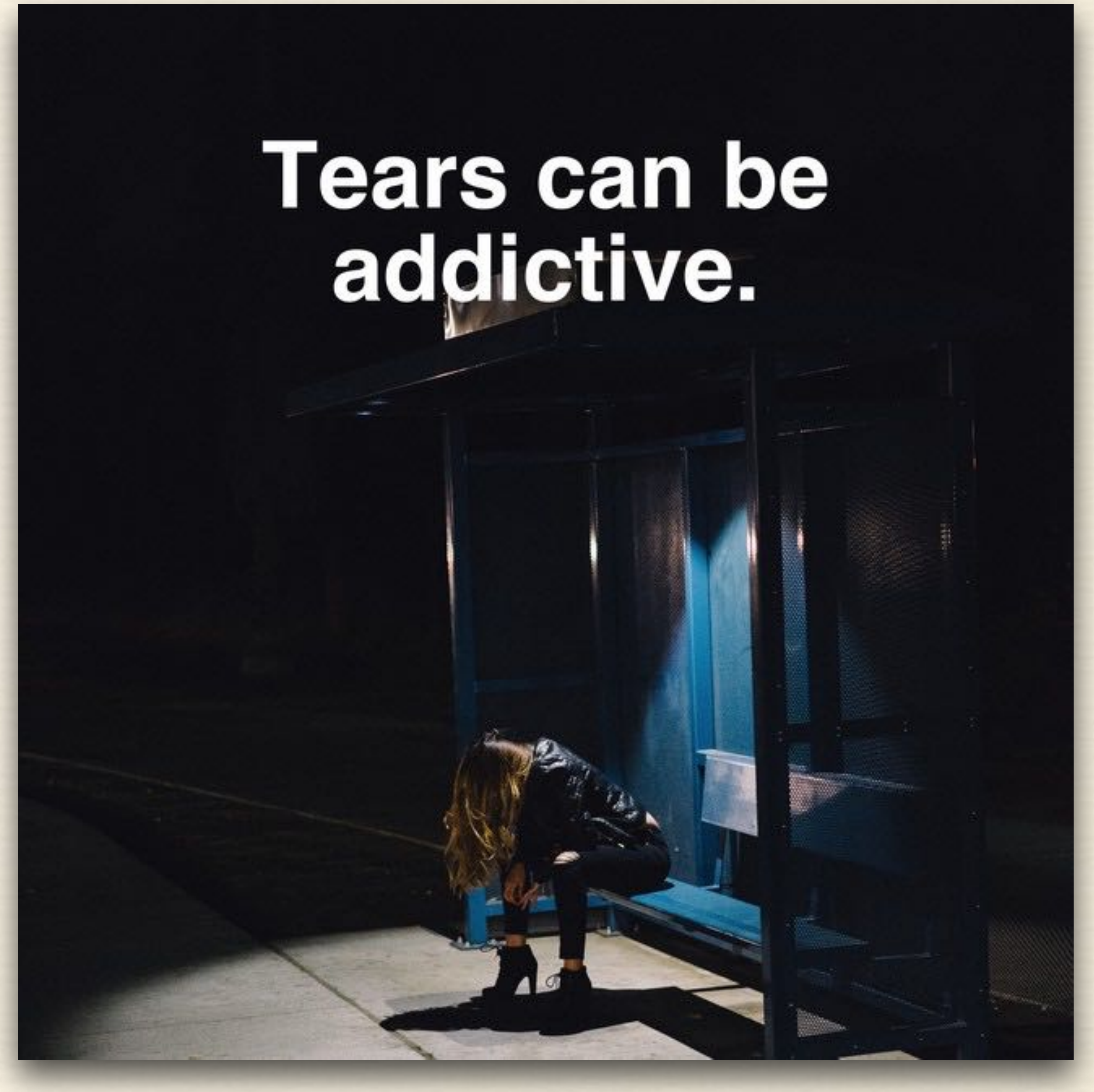
Inevitably

Overhead, lack of consistency, and a decentralized toolkit are a one way ticket to OpSec fails.

Ultimately

We all end up writing and re-writing the same one-off tools and malware functions over and over.

But they hardly get better over time.



Historically

Red Teams develop tooling to automate their specific workflows.

Usually centered around a collection of other pentesting tools.

But we all do this in relative solitude.

Sad Irony

For “some” reason most of these tools never get released…

The Point

A framework gives you a common platform for implementing features to support your specific needs.

Modularity gives rise to variation without re-invention.

Automation gives you time to focus on hacking the target instead of hacking tools together.

Open source shares the capability with everyone while drawing on the communities collective talent and expertise.

So Why?

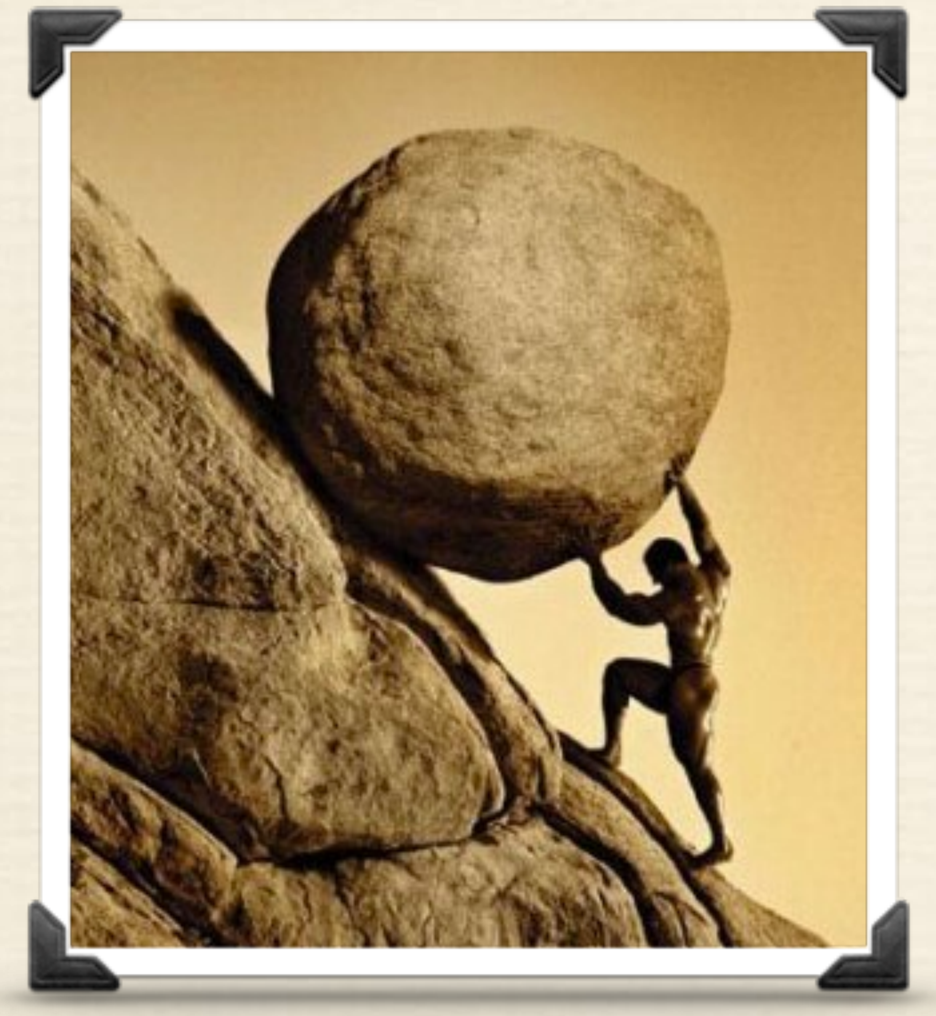
The reason you would want to build a modular malware framework is because it's **about god damned time**.

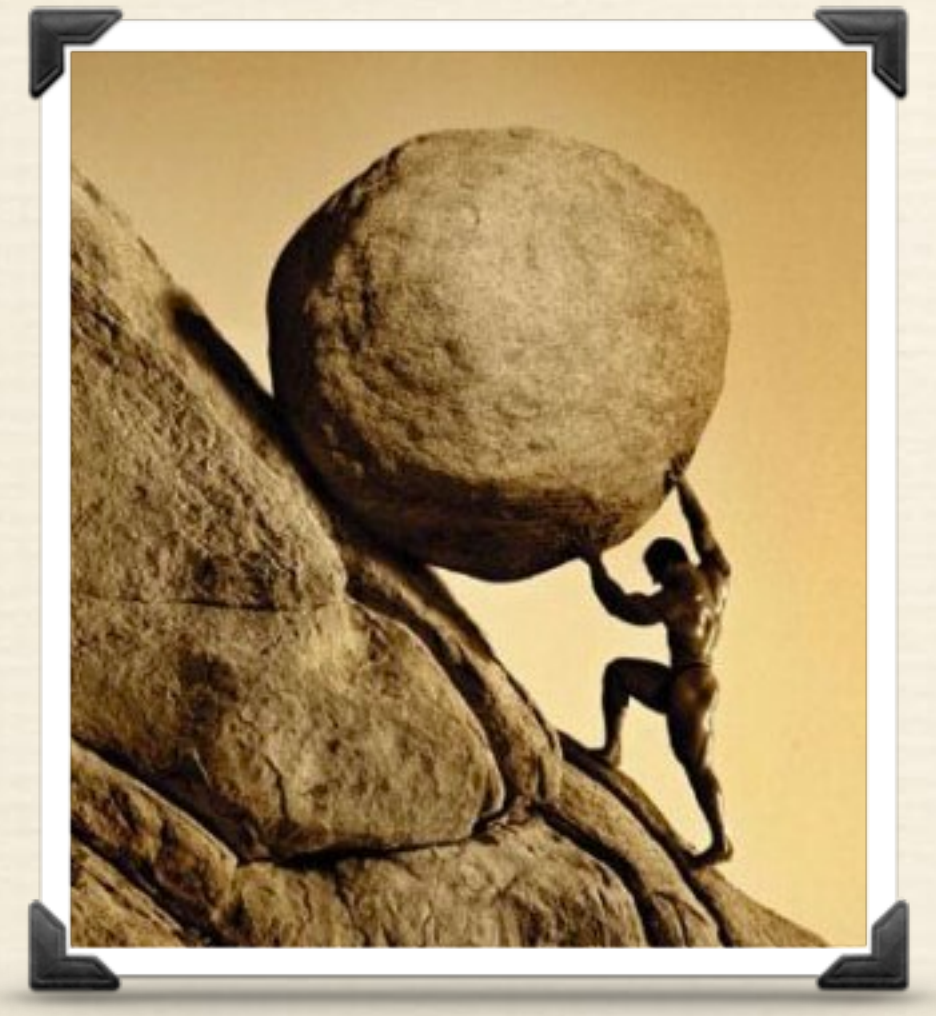
We Need

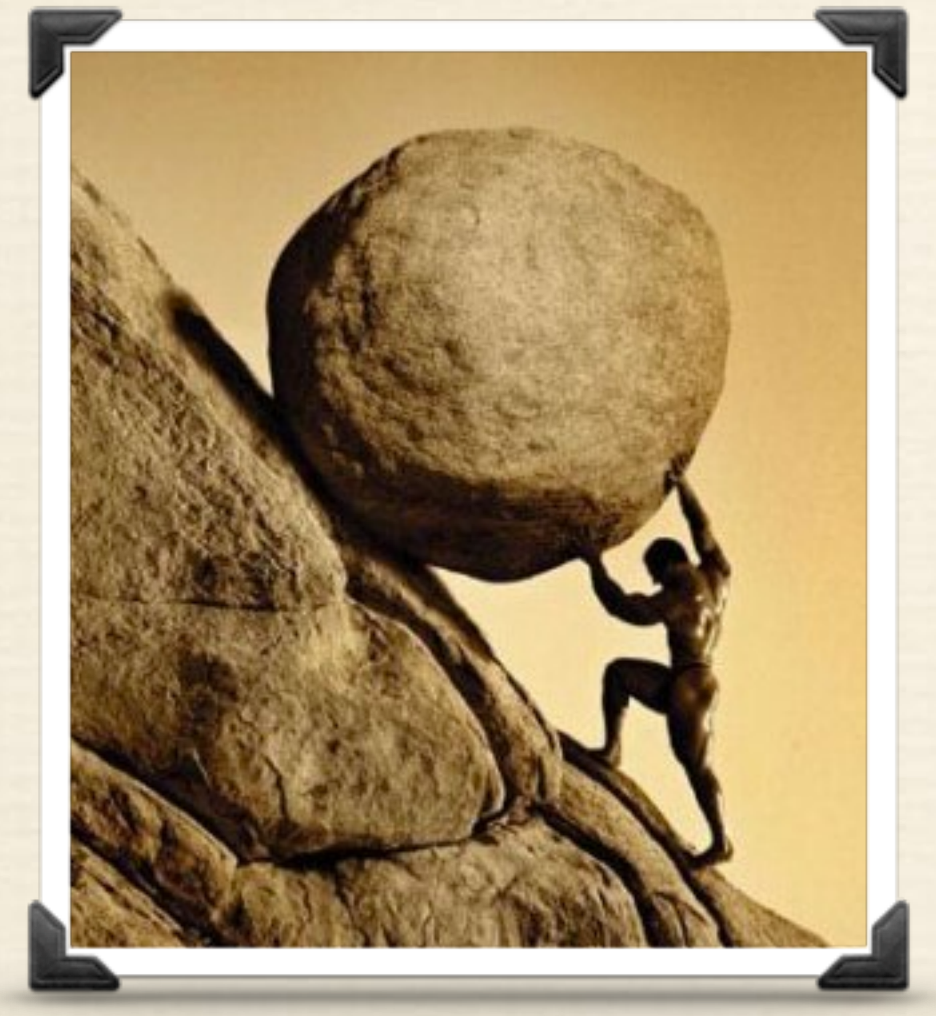
- A platform for on demand configuration, creation, and interaction of remotely deployed implants.
- We never set out to build an exploit tool.
- We never set out to build a pentest or vulnerability discovery tool.

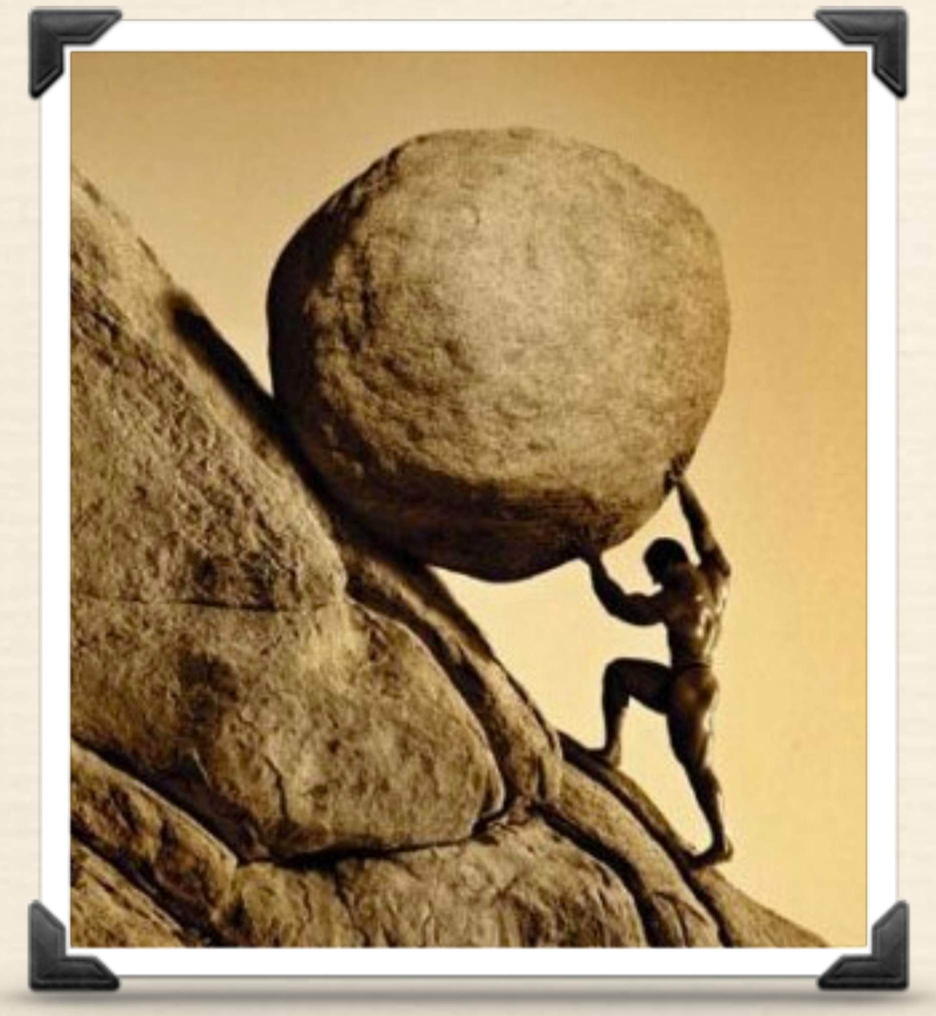
Quick Recap

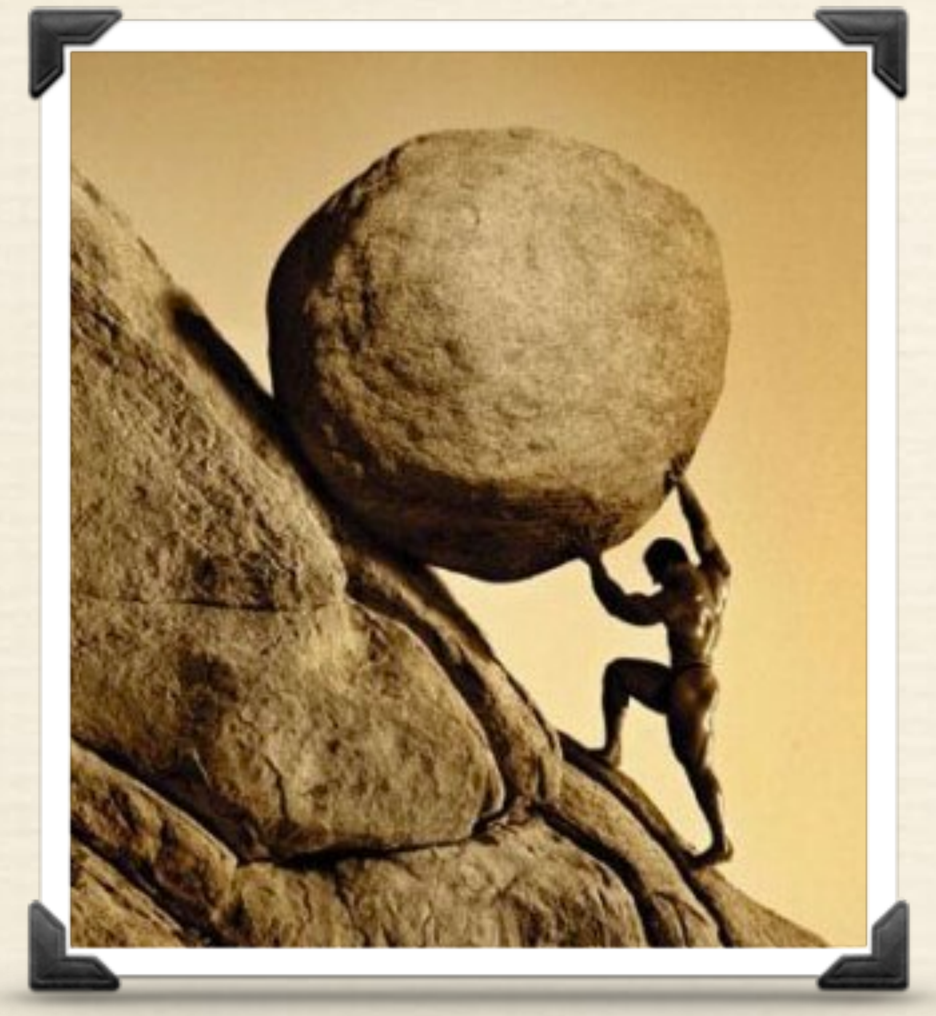
The Malware Framework Cookbook

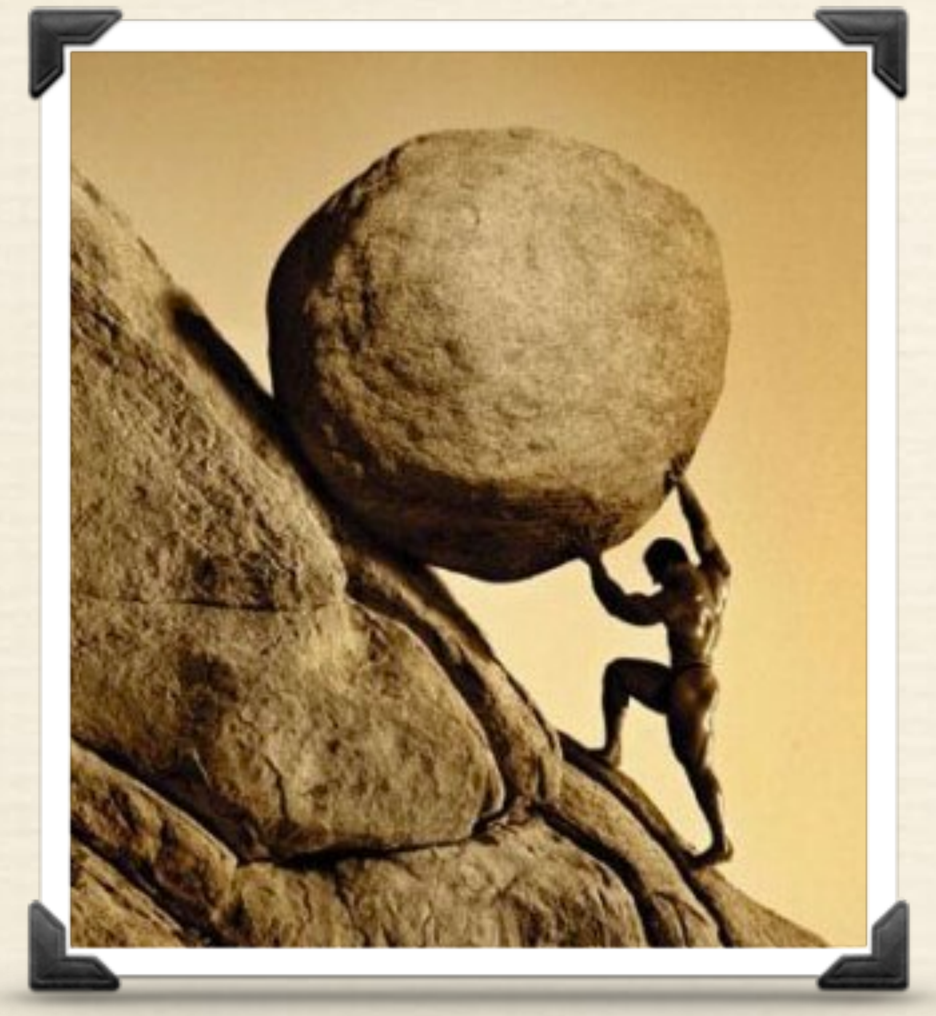


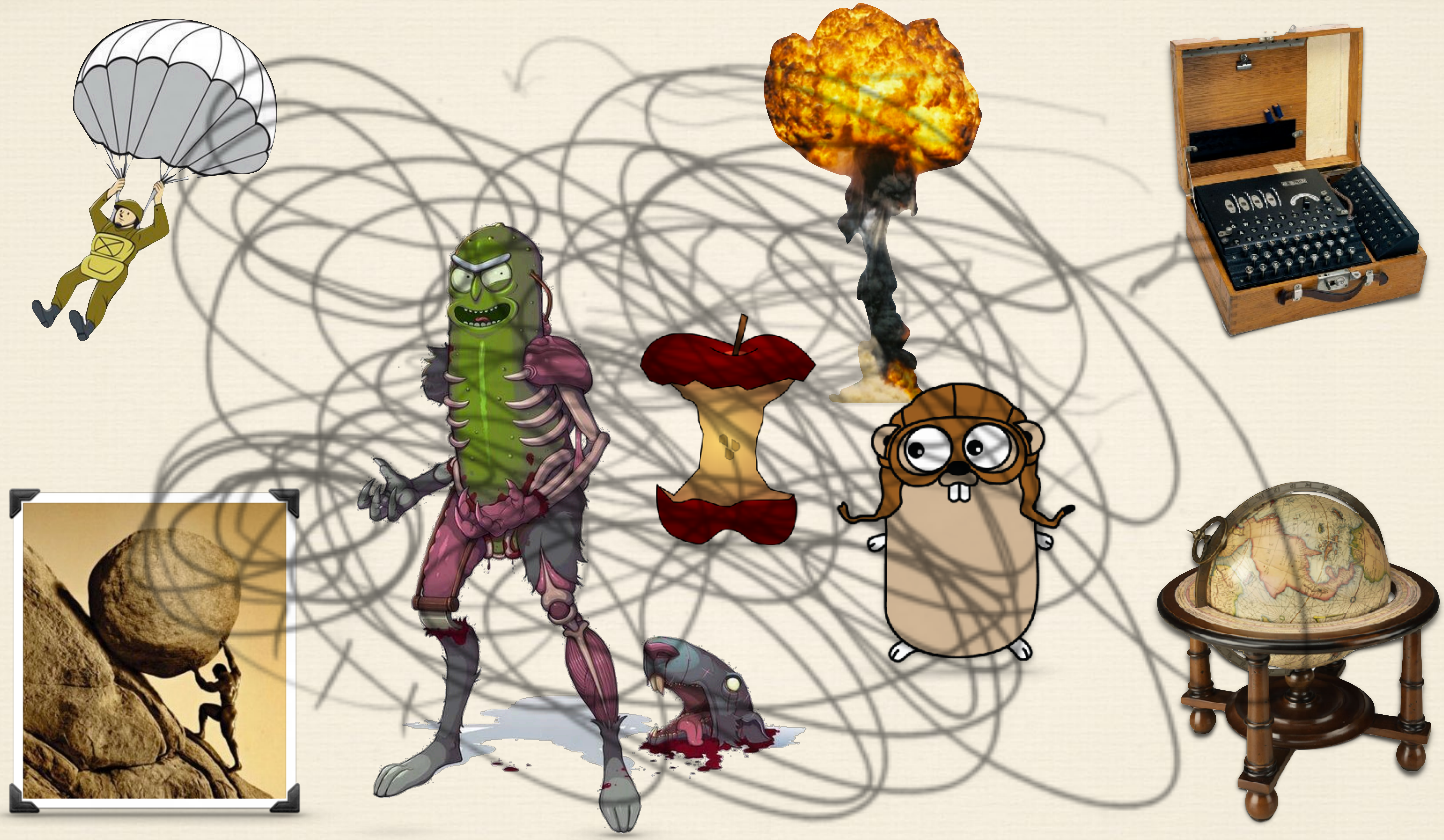


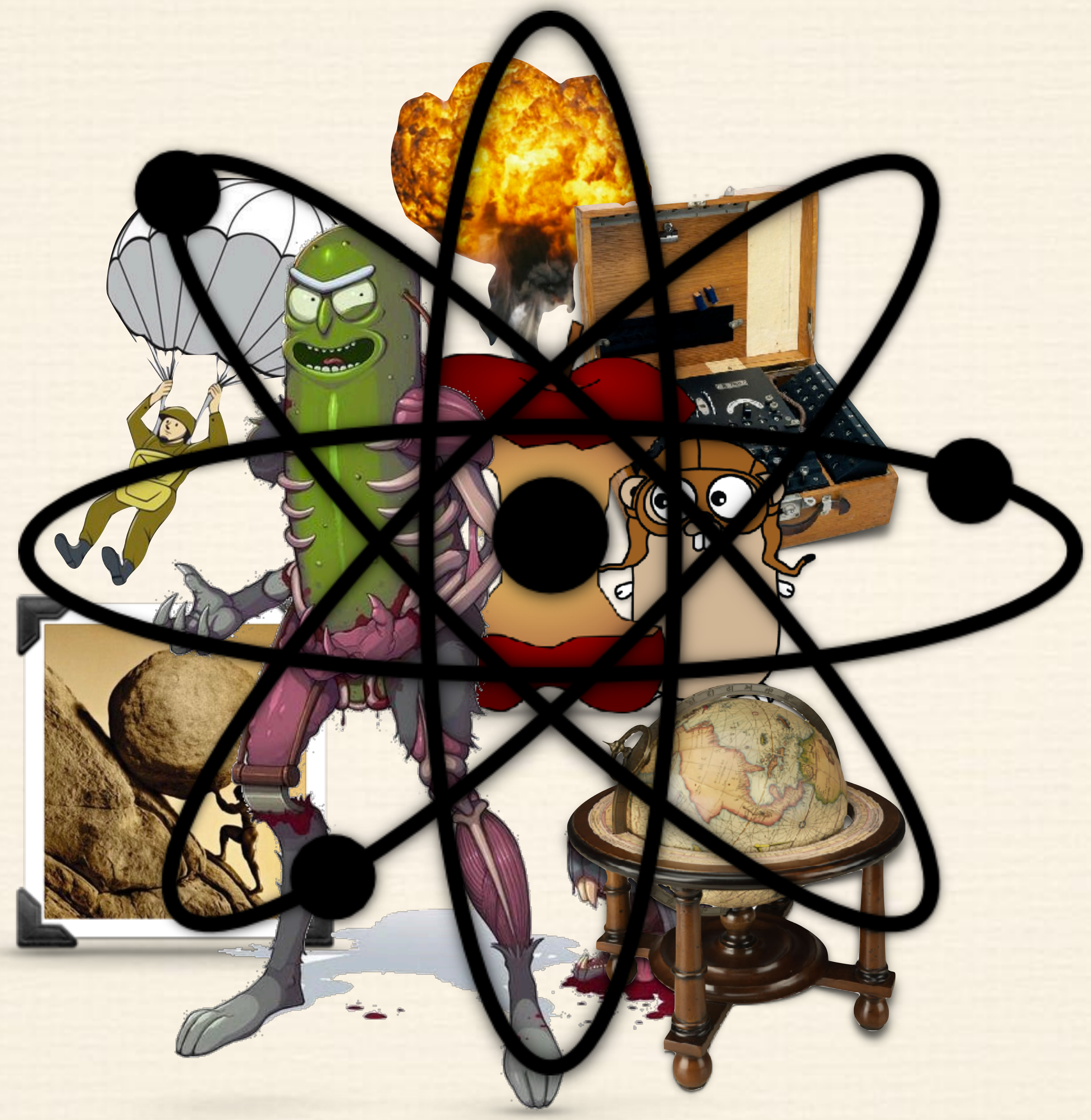


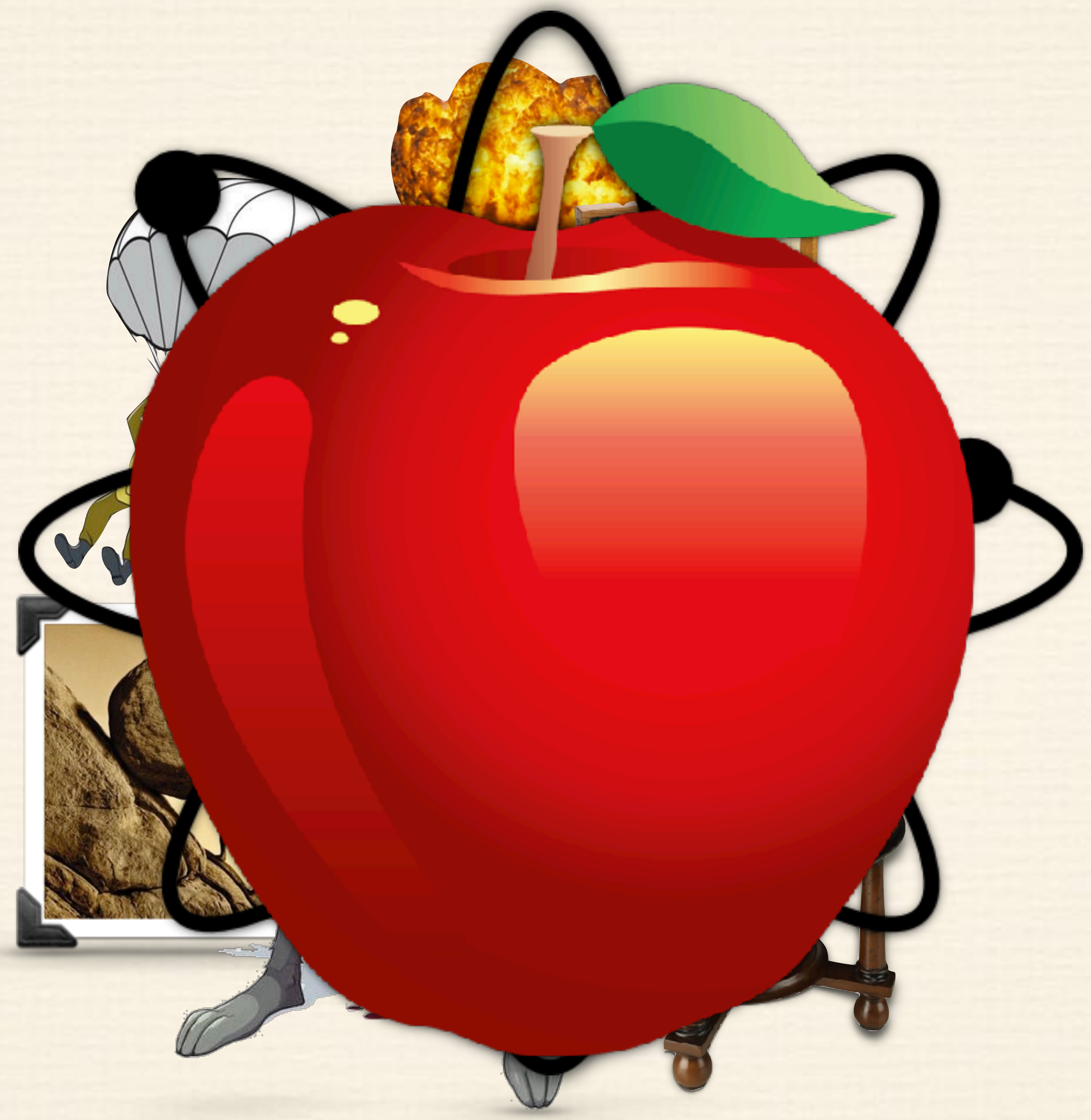


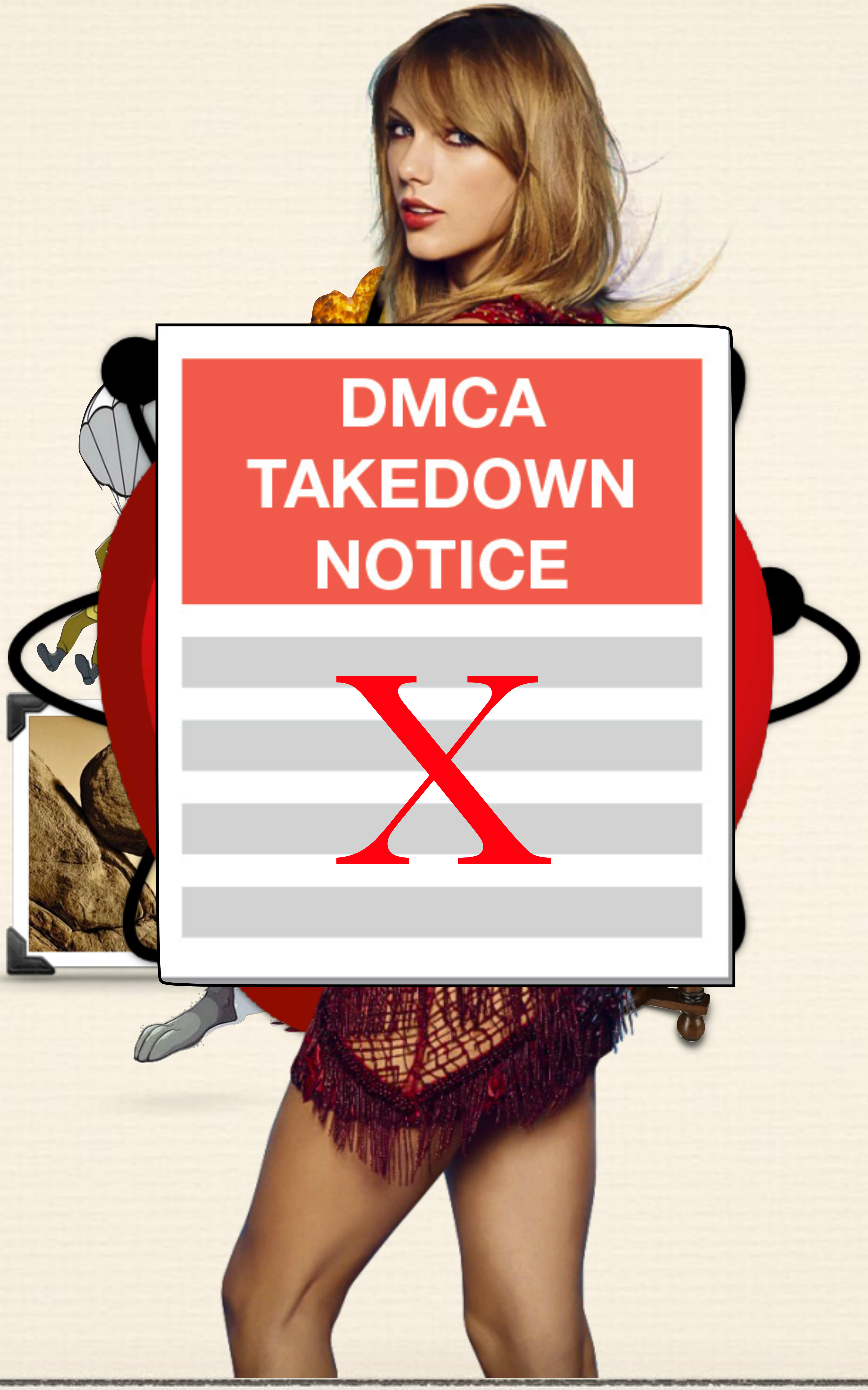











DMCA
TAKEDOWN
NOTICE
X

So What Now?

Yesterday has gone

Candor

This is new territory for us, the whole situation sucks for everyone.

We're doing our best to navigate choppy legal waters.

We asked, well begged, for open sourcing.

They refused, but we're not giving up on the possibility.

They could still change their mind.

In the meatnime…

JUST KIDDING

Better to do something productive.

Uh… not reproductive.

Nah, that's reductive.

Good enough.

Ultimate Goal

Our goal is still to birth an open source modular malware framework and offensive security operations platform for the greater good of the universe.

Ways to name a framework

When all the good ones are already taken.

God Save The Anagram

Team Pistol

Steam Pilot

Optimal Set

Postal Item

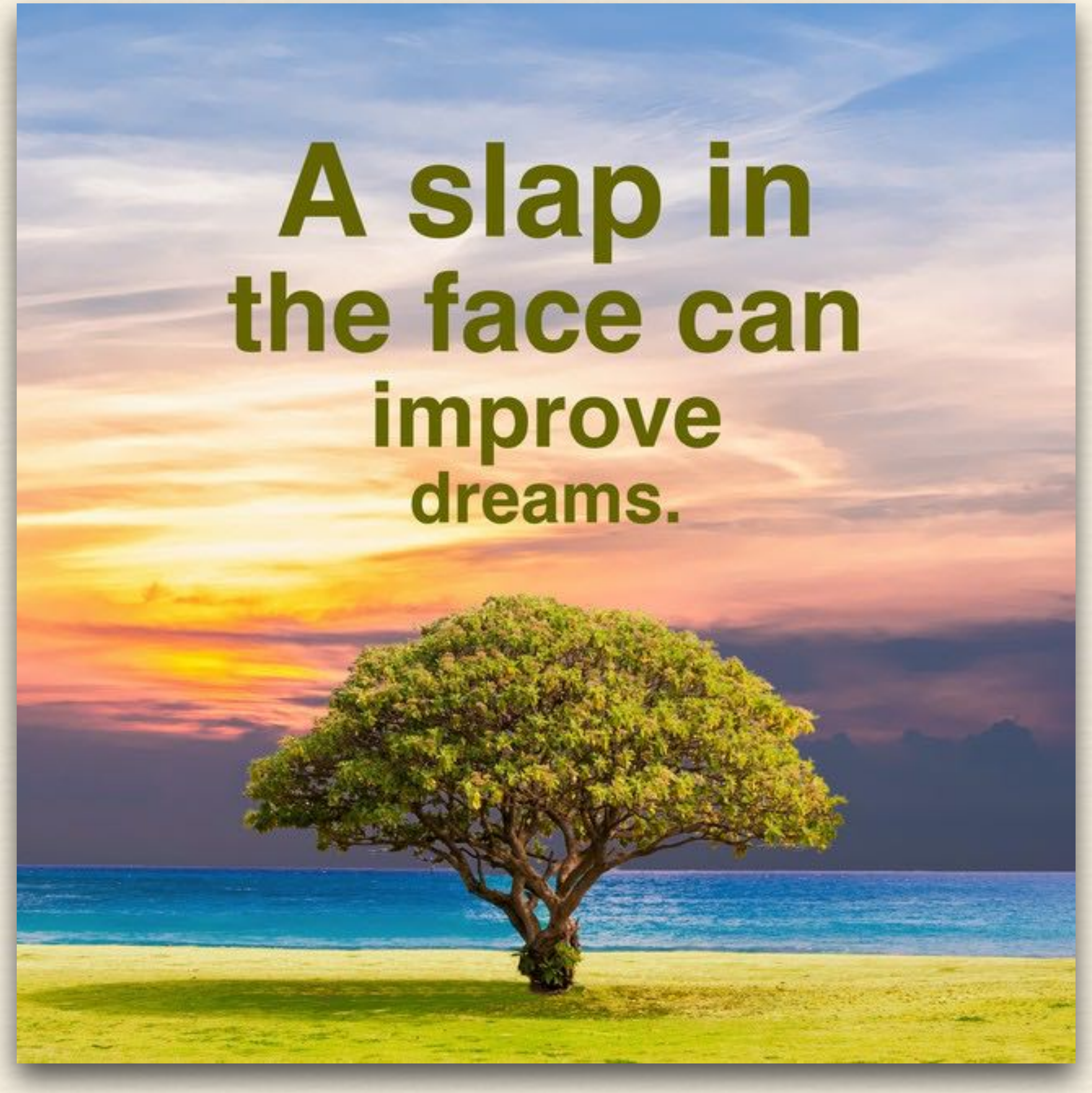
I Molest APT

Toilet Maps

APT Lit Some

Slim Teapot

Our cup runneth over.



Moist Petal

Open source offensive security platform
for red team, by red team

Backronym to the Future

Malware **O**rchestration and **I**mplant **S**ystemization **T**oolkit

in order to support

Perpetual **E**ngagements **T**esting **A**dversarial **L**imits

A new hope, a new beginning…

- New design equals new possibilities.
- Now with 100% less corporate-backing!
- Open source from the first commit.
- Community-driven requirements.

Same needs, different approach.

- Design, build and deploy modular malware.
- Automated C2 infrastructure support.
- Collect high fidelity attack intelligence for reporting.
- Support collaboration for distributed red team operators.
- Integrates with external services (storage, compute, chat etc.)

Pre-Alpha AF

Moist Petal Community

- It starts here today!
- Think of it as an “early access” malware framework.
- We’d love feedback on platform design and requirements.
- Community discussion will shape the framework’s development to support the workflows for your diverse red team use cases.
- New project is under **active development**.

How to get involved?

Join the mailing list,

https://groups.google.com/forum/#!forum/moistpetal

Contribute to the repository,

moistpetal.io

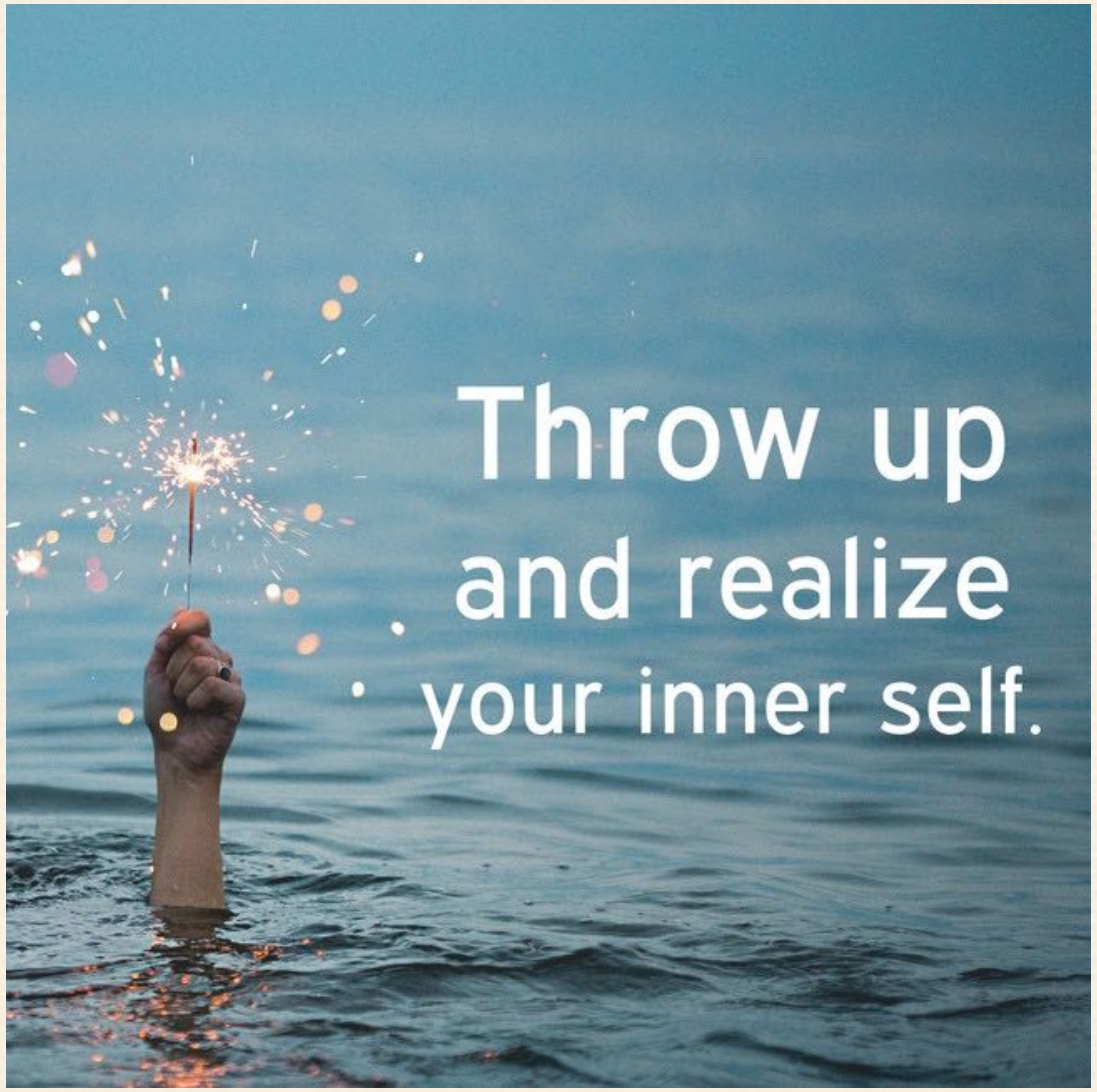
Chat with us on slack (shared invite below) & gitter,

goo.gl/bmy947 , https://gitter.im/propervillain/moistpetal

Follow **@ceyxiest** and **@fuzzynop** for future updates!

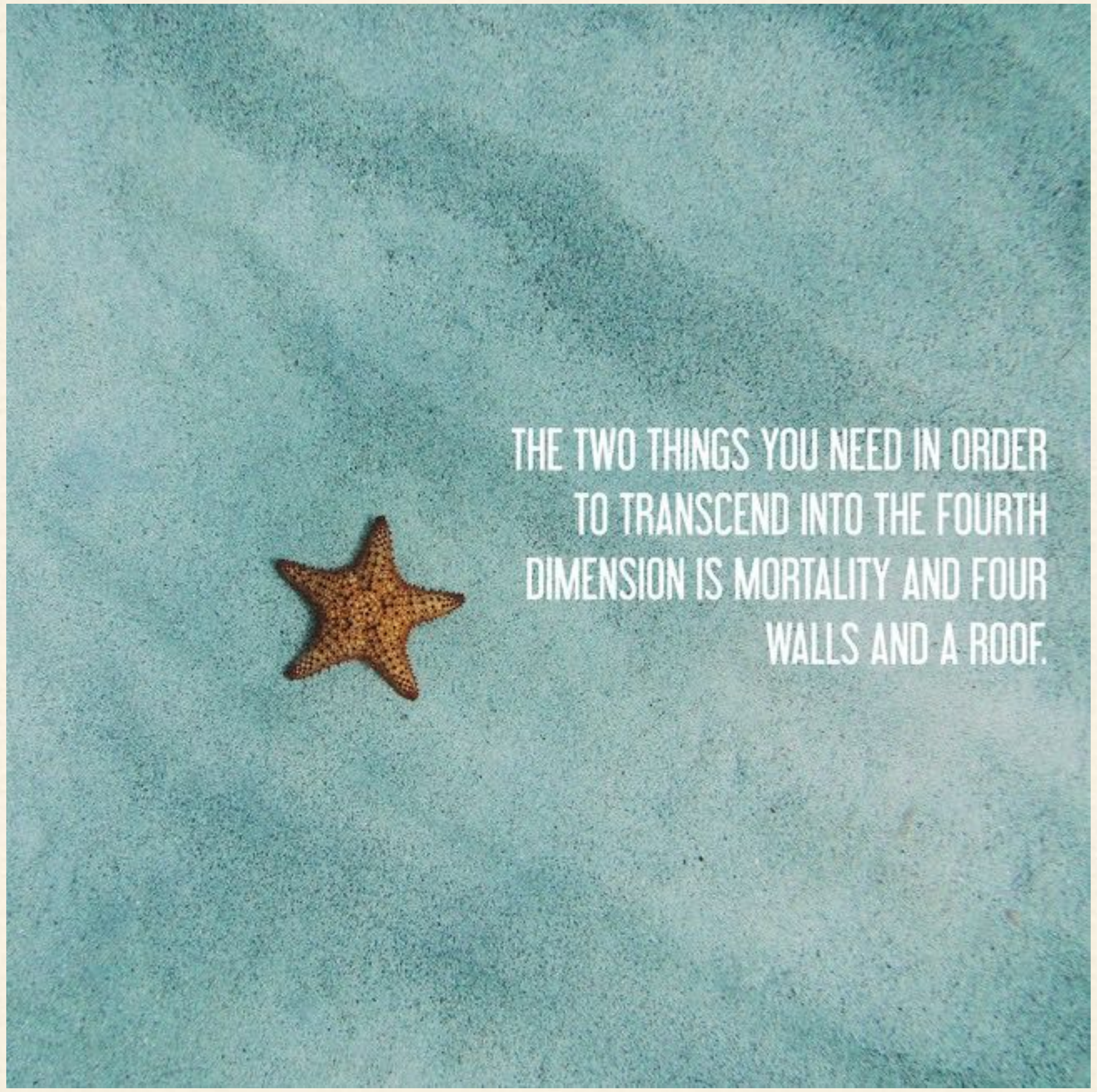
The End

… or the beginning?

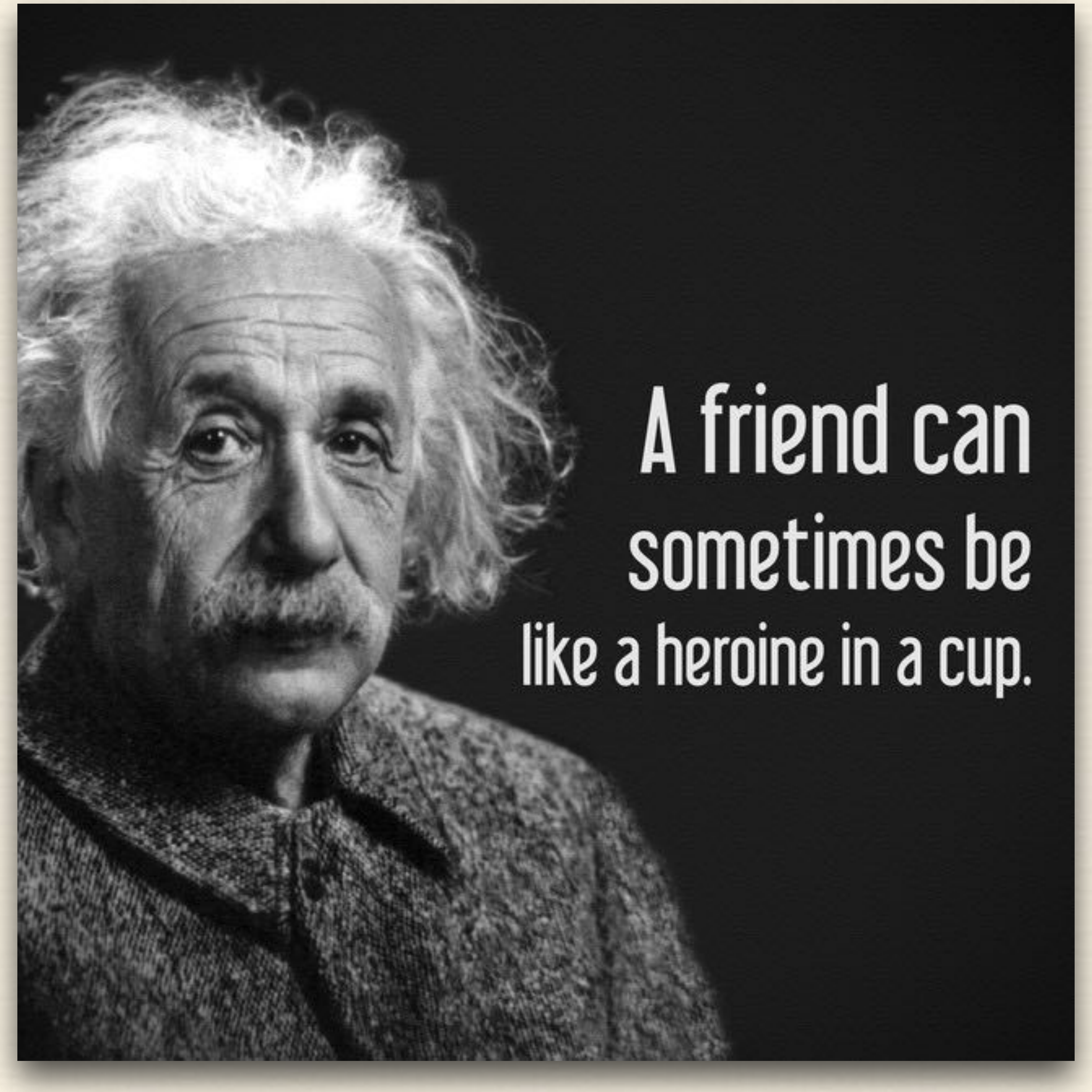

Throw up
and realize
your inner self.

A SHITTY VEGAN DOESN'T
MAKE YOU A TALENTED
CARNIVORE.

Relying on an asshole to be your asshole is a insane problem.

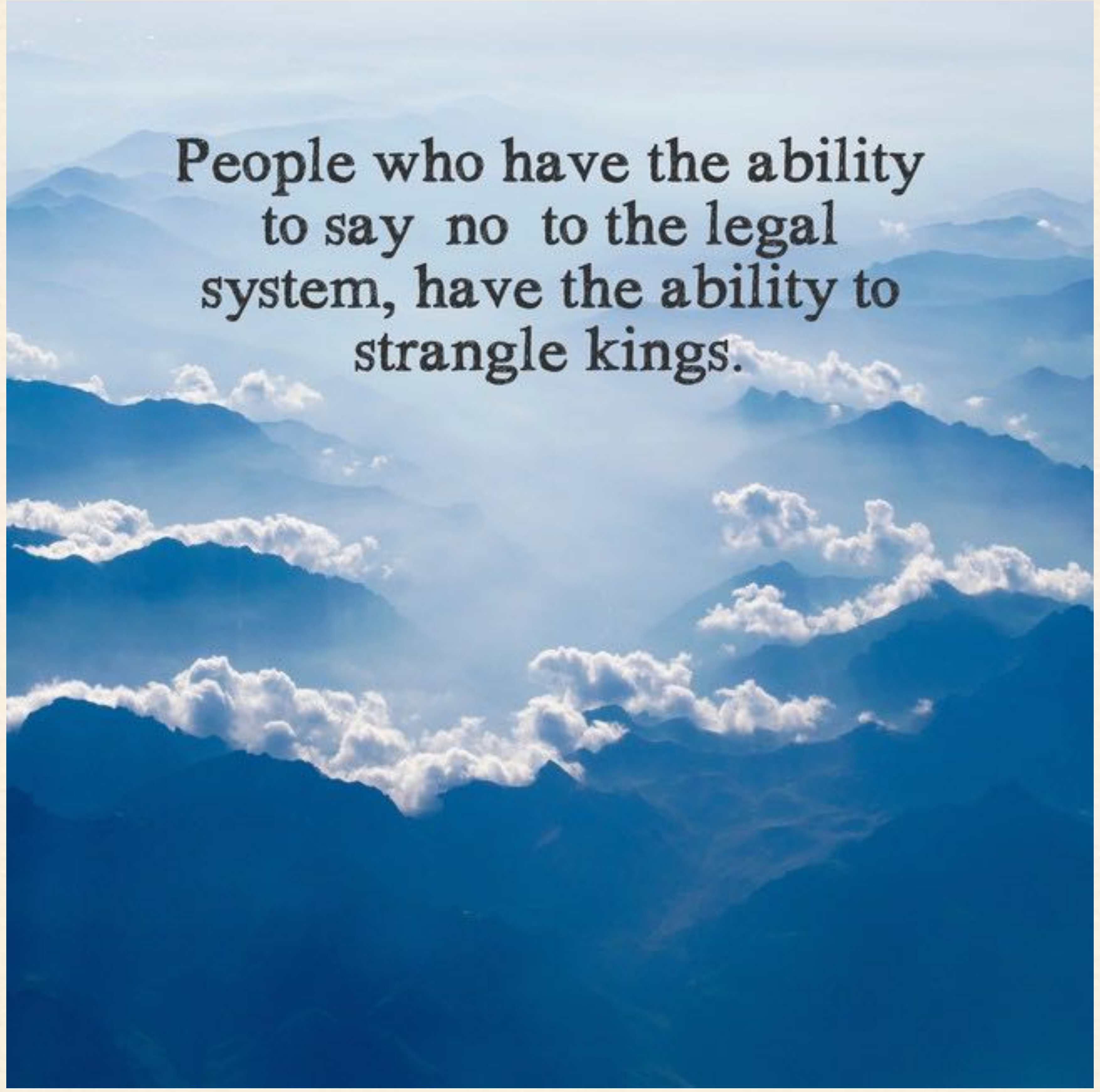


THE TWO THINGS YOU NEED IN ORDER TO TRANSCEND INTO THE FOURTH DIMENSION IS MORTALITY AND FOUR WALLS AND A ROOF.



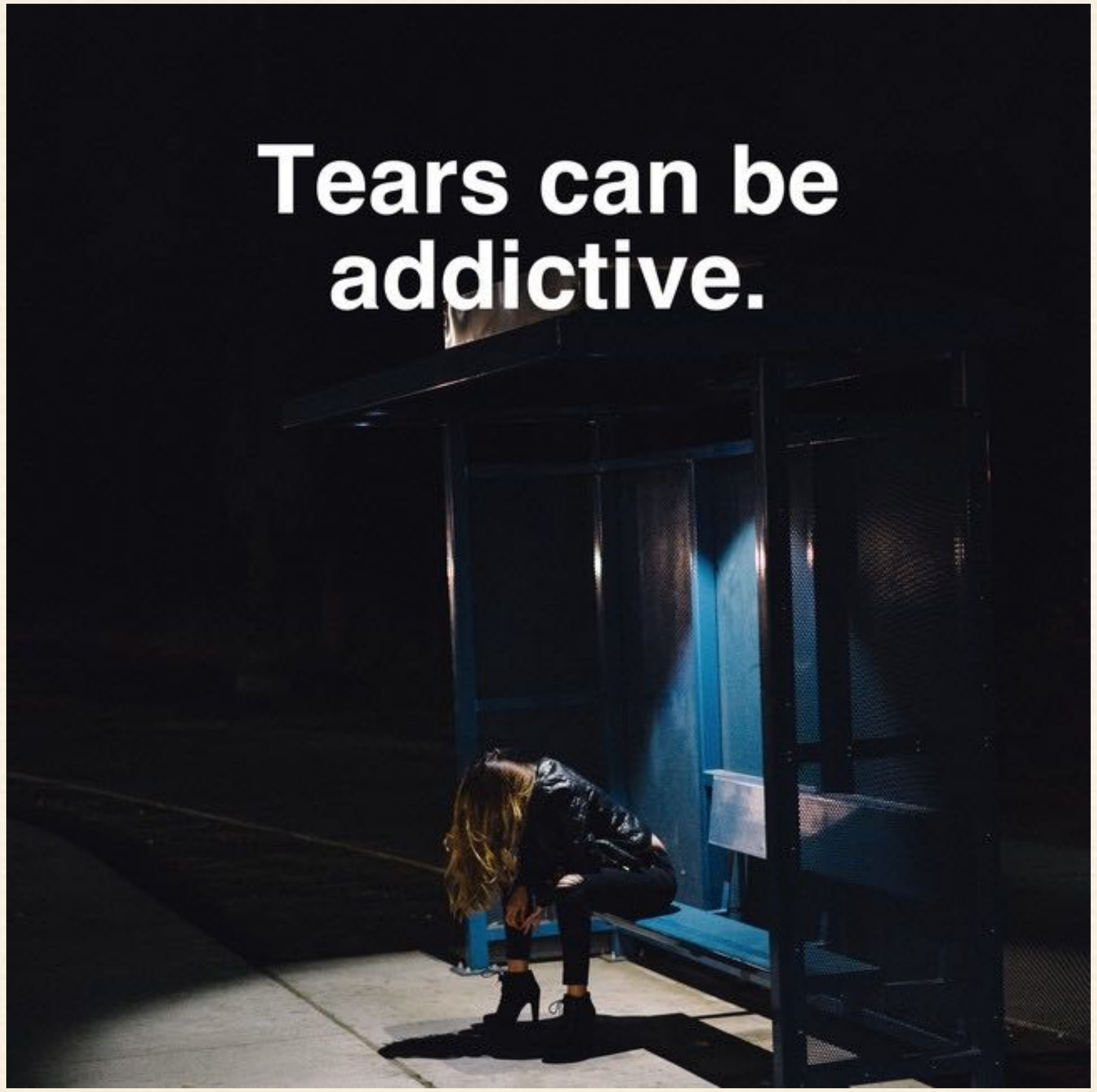
A friend can
sometimes be
like a heroine in a cup.

With new goals come new dangers.

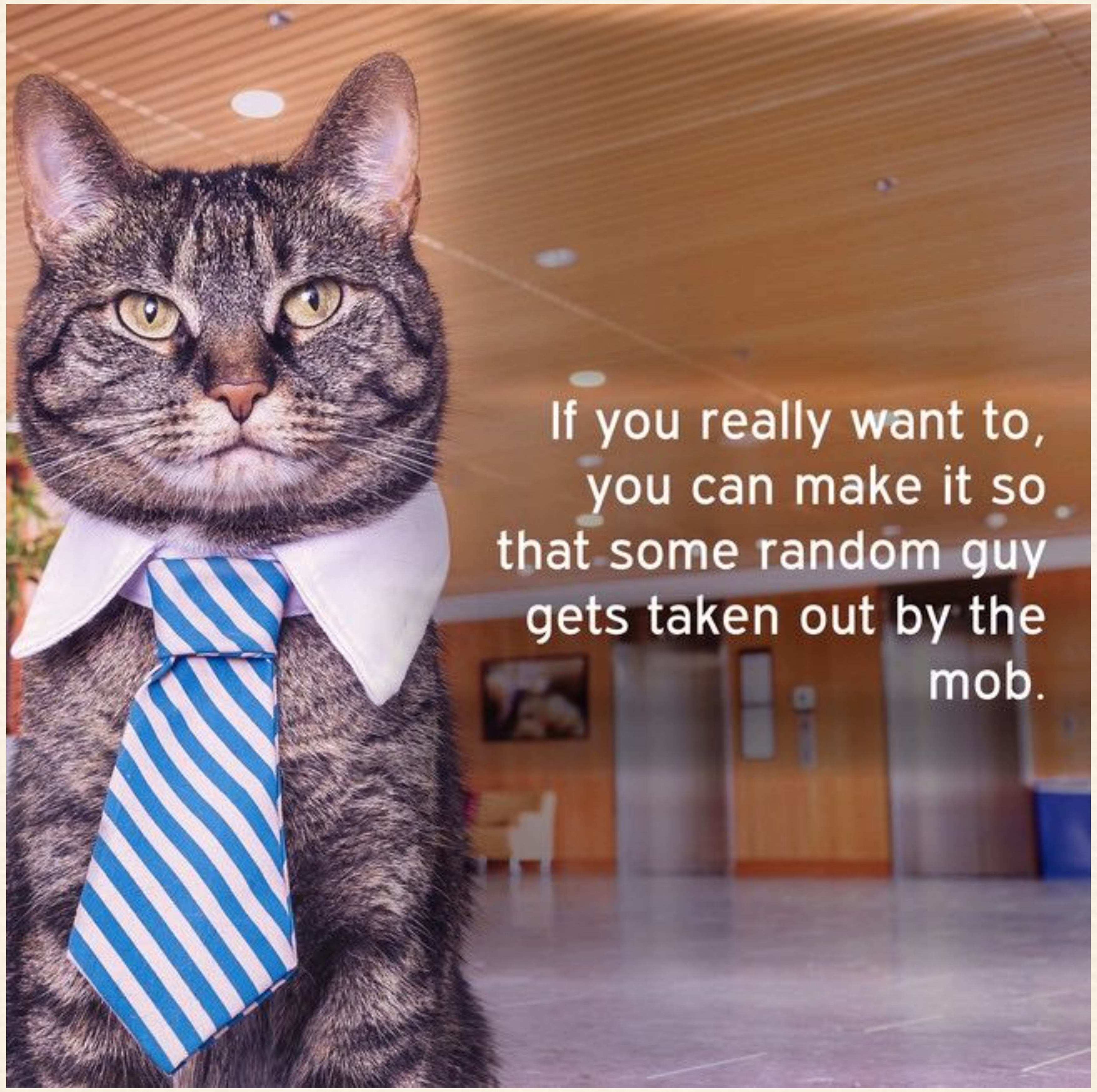


People who have the ability to say no to the legal system, have the ability to strangle kings.

Together we can make it so that people change their minds.



Tears can be addictive.



If you really want to, you can make it so that some random guy gets taken out by the mob.

The two things you need in order to make someone smile is a grave and duct tape.

WITH BEAUTIFUL
EXPLANATION COMES
BEAUTIFUL TRAGEDY.

When journalists kill, rock stars resurrect.

What if comfortable thoughts can be public humiliations if we just think outside the box?