

# **THE PAST, THE FUTURE, AND**

*... wait, where the hell are we now?*

Hello, this is me

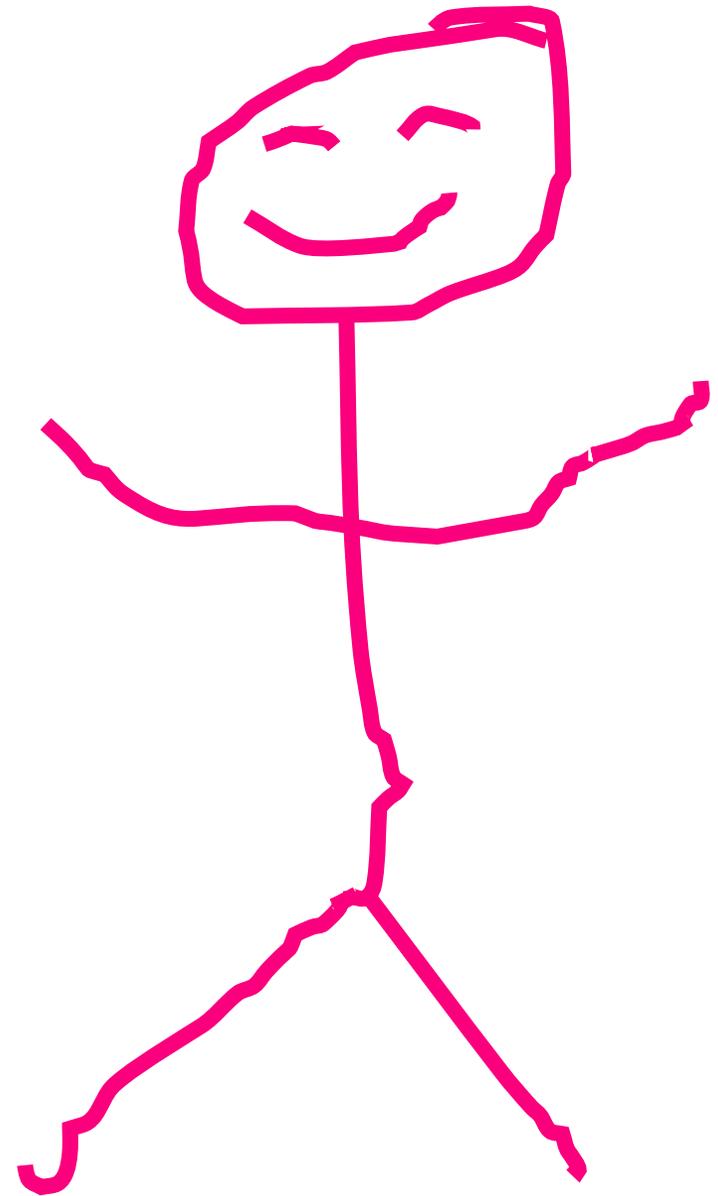


# Disclaimer

The opinions and positions expressed herein are mine only and do not represent the views of any current or previous employer, including Intel Corporation or its affiliates.

This presentation has no intention to advertise or devalue any current or future technology.

Scripting monkey,  
Malware analyst,  
Reverse engineer,  
Advanced threat detection,  
Nation state malware observer,  
Incident response,  
And then I went low level.  
(HITB \m/-.-\m/)





why



**GOING LOW**



WELCOME TO  
FAR FAR  
AWAY

*We are all searching for something*

Known-Bad

Known-Good

Non Known-Good



# A PARADOX

*Anti-virus is dead, they said.  
Pattern matching is defeated, they claimed.  
Then they came up with IOCs,  
and stuffed them with patterns.*



Spot  
the  
problem.





Businesses will business.  
Scaling is hard.  
Why it will always work but never does.

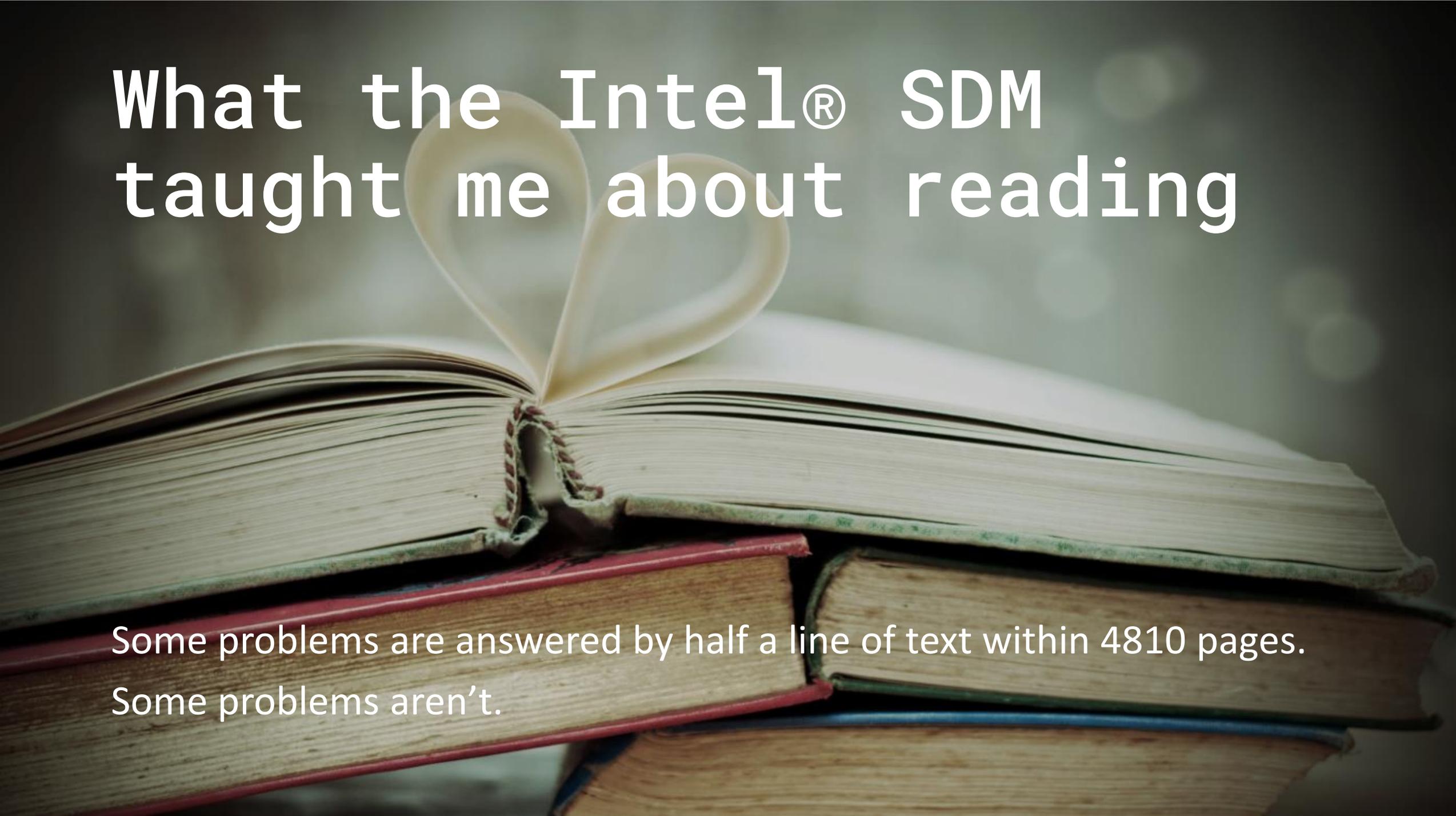
# The Threat Detection Myth

All the wonders we could do,  
if things just worked the way they should.

From AV to sandboxes,  
from sandboxes to static analysis,  
from static analysis to RE tools wonderland.



*courtesy of @guedou*

The background of the slide is a photograph of a stack of old, worn books. The top book is open, and a cream-colored bookmark is placed in the center, forming a heart-like shape. The pages are yellowed with age. The text is overlaid on the top half of the image.

# What the Intel® SDM taught me about reading

Some problems are answered by half a line of text within 4810 pages.  
Some problems aren't.

A wide-angle, low-angle shot of a large, empty conference hall. The ceiling is high and features a complex network of metal trusses and numerous recessed lights. The floor is a light-colored, polished surface that reflects the overhead lights. The walls are a neutral, light brown color, and several large pillars support the structure. The overall atmosphere is clean, modern, and spacious.

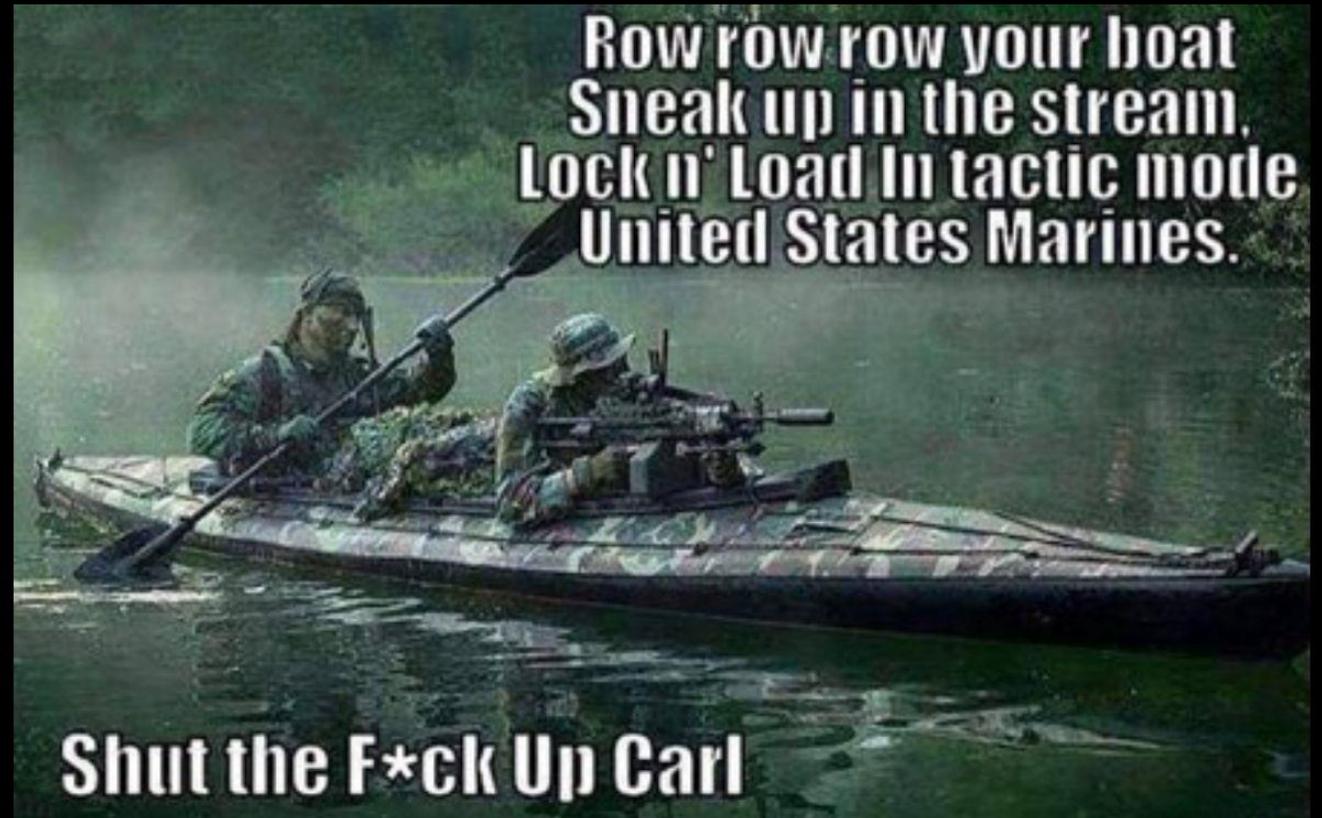
What conference expo halls  
taught me about security



*My field trip into  
policy world  
and the art of  
nation state 1:1*

# THE A AND THE P OF THE T

APT big game hunting, like Carl would





Advanced Technology Is...Advanced

# What nation state malware taught me about cyber war



**</BLANK>**

I read 20 years of mostly-fail at cyber norms at the UN, and now you can too!

## How to use this repository

### Organisation & naming conventions

- Files have been renamed to reflect UN document IDs rather than job numbers (which are useless); slashes and full stops are omitted

- e.g., A/RES/53/70 == ARES5370.pdf; A/C.1/70/PV.21 == AC170PV21.pdf; A/61/161 == A61161.pdf

- Highlights and markups are mine; don't touch
- Alternate and/or original language translations

### Symbols

- A/ indicates a document of the General Assembly

- A/RES/##/### & ARES##### indicate a resolution



**Eva** ✓

@evacide

When all you have is a hammer, everything looks like APT28.

2:16 PM - 22 Aug 2017

# The unspeakable horrors of real world incident response

or, why I'm happy nation  
state APT isn't SO much  
of a thing

Security and other professions.

The updatability problem.

Believe and the lack of believe.



National Security

# The NSA has linked the WannaCry computer worm to North Korea

---



**NEVERMIND.**

# GOING LOW

*There is a world beyond x86.  
Drive, guts, pain resistance.  
Patience, and more patience.*



CPU microarchitecture is a world of black magic, dragons, and endless trial & error.

10:21 AM - 27 Nov 2017



A small, dark beetle is positioned in the center of the frame on a light-colored, textured surface. The beetle is oriented horizontally, facing left. The surface has a mottled, fibrous appearance with various shades of beige and light brown. To the right of the beetle, there is a dark, vertical, curved object, possibly a piece of equipment or a door frame, which is out of focus.

.. my first bug at Intel!

# All my hello worlds

... in Intel SGX

... as Linux kernel module

... in uCode

... (redacted)



# *The meaning of growth*

The only time when you are actually growing, is when you're uncomfortable

*[Thomas Oppong, medium.com]*

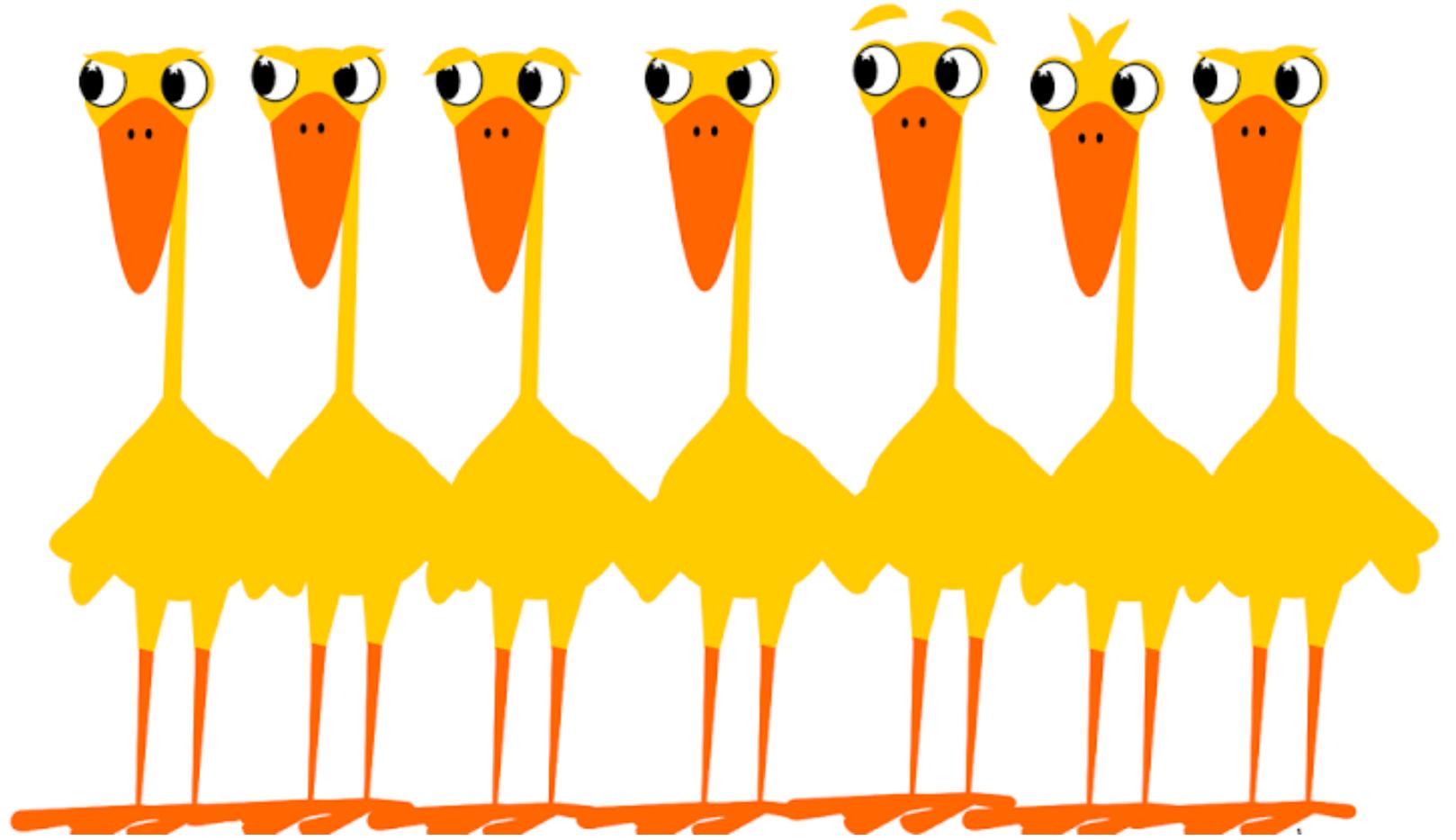


# BlackHoodie

*Free & women-only reverse engineering bootcamp  
3 editions since 2015 - 15, 32 & 67 attendees  
17 nationalities, 5 continents*

*As damn challenging as possible*

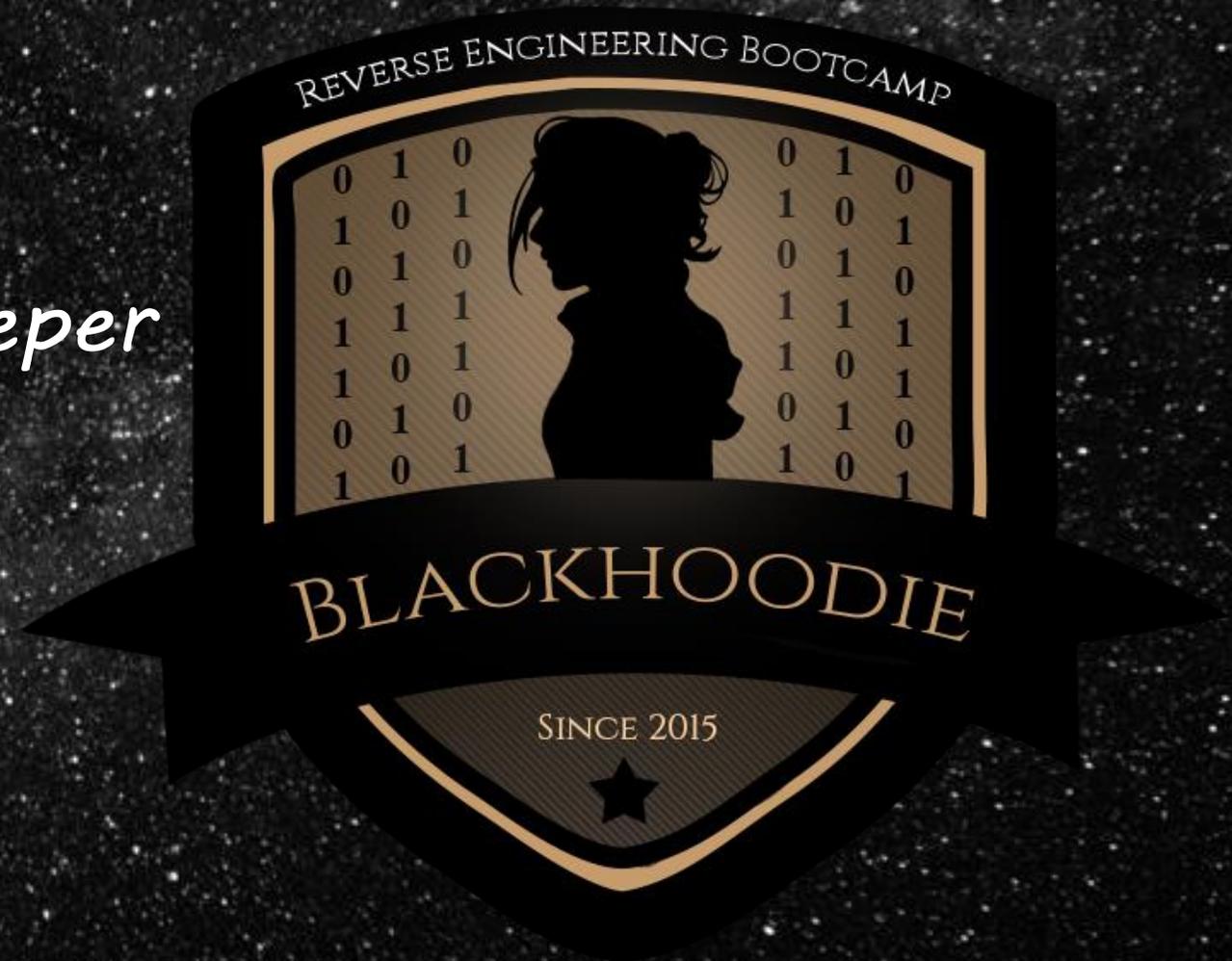
Dunno, but  
I like it...



# Creating Space

*Pushing folks to dig deeper*

- and go further*
- and push boundaries*
- and try harder*



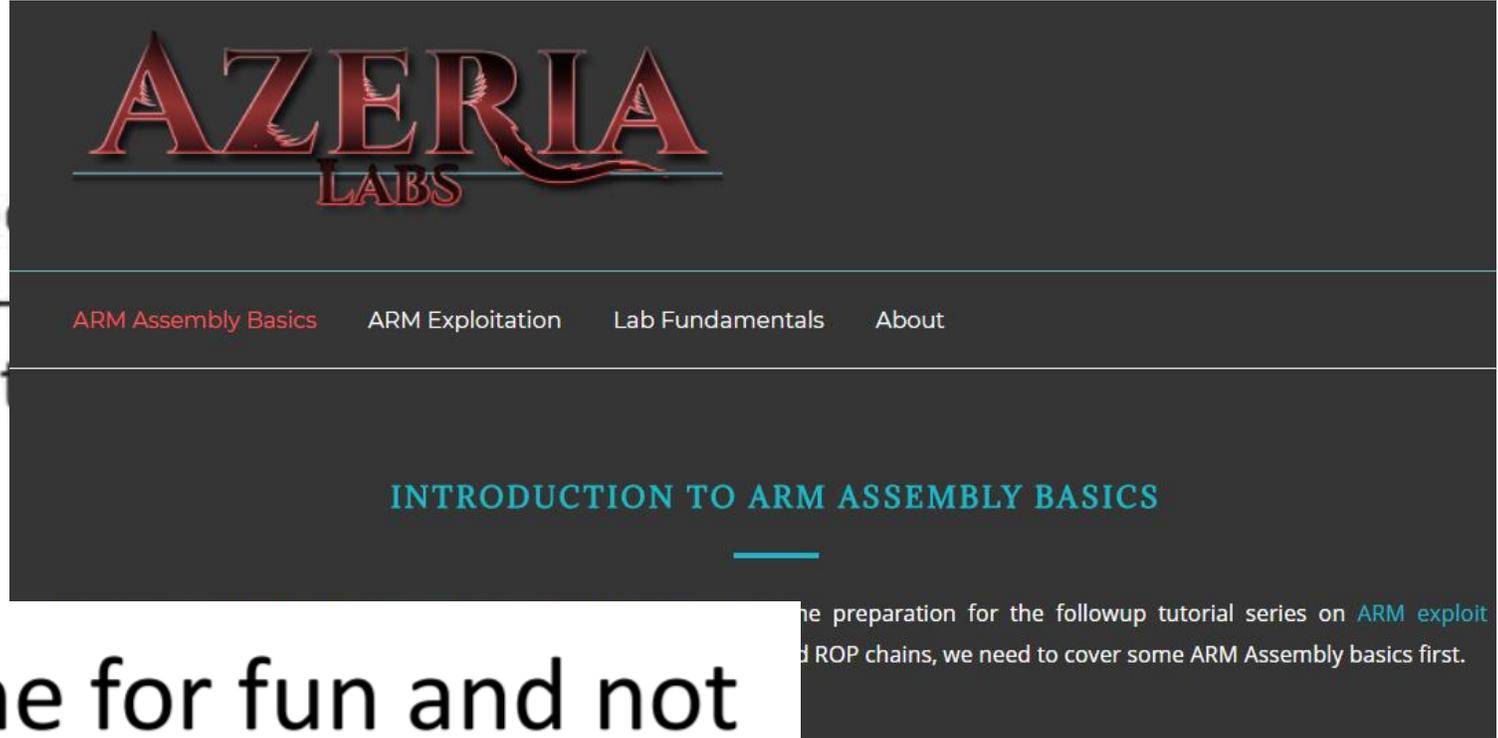
The background of the image is a military-style camouflage pattern, specifically a woodland or tiger print. It consists of irregular, dark green and black shapes scattered across a lighter olive green base. The text is centered and reads:

**MINORITY  
DRIVEN  
BOOTCAMP**



Ophir Harpaz  
@OphirHarpaz

I just hacked Minesweeper flags on all the mined squares starting. I'm currently the only person on earth.



Kernel Shim Engine for fun and not so much (but still a little?) profit

the preparation for the followup tutorial series on [ARM exploit](#) and ROP chains, we need to cover some ARM Assembly basics first.

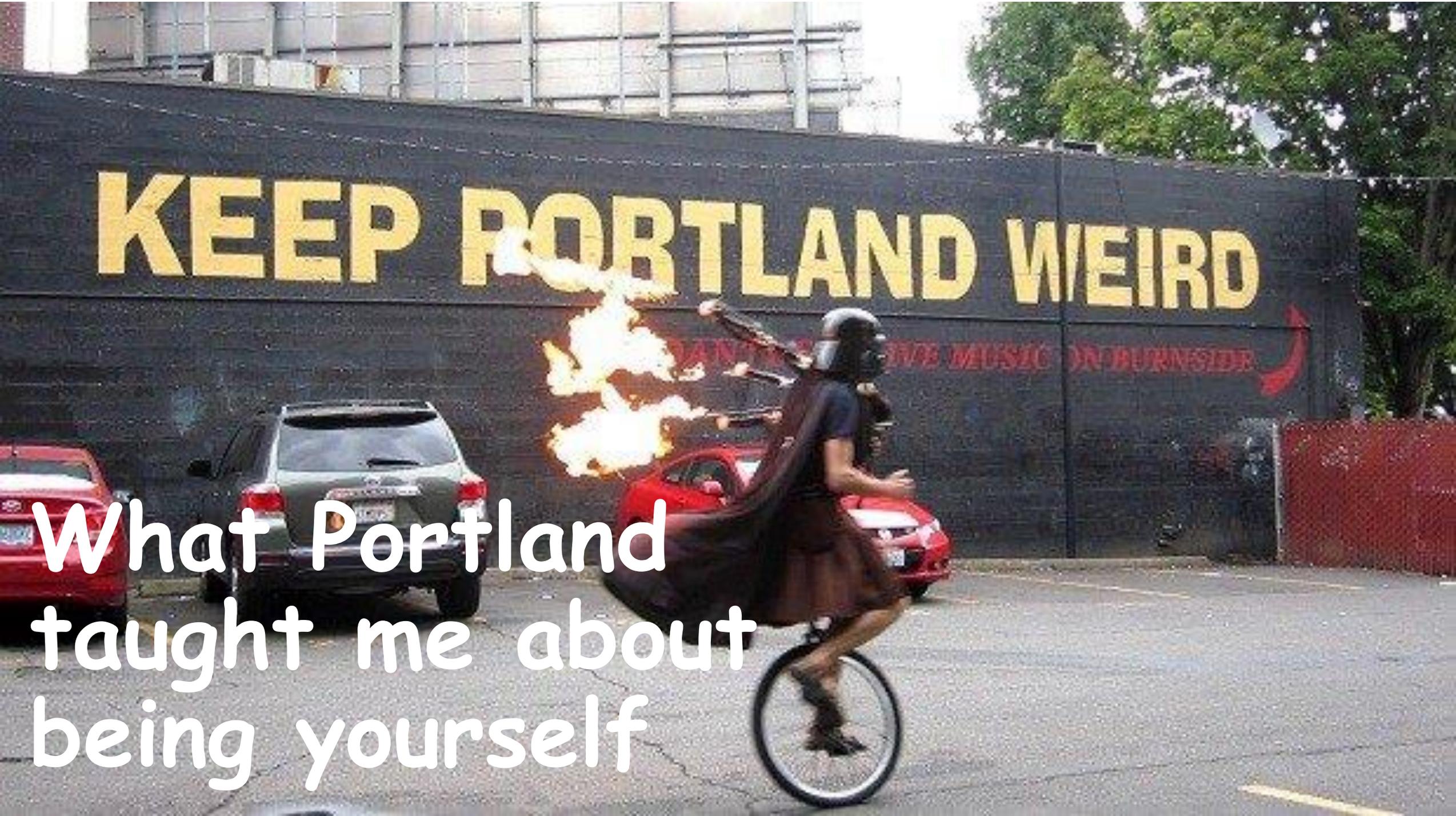
e17 talk on flash lable

Or how to write a super long title for nothing :)



**KEEP PORTLAND WEIRD**

What Portland  
taught me about  
being yourself



Thank you!

