A Dozen Years of Shellphish

From DEFCON to the Cyber Grand Challenge

SHELLPHISH

CGC CYBER GRAND_CHALLENGE

DEFCON

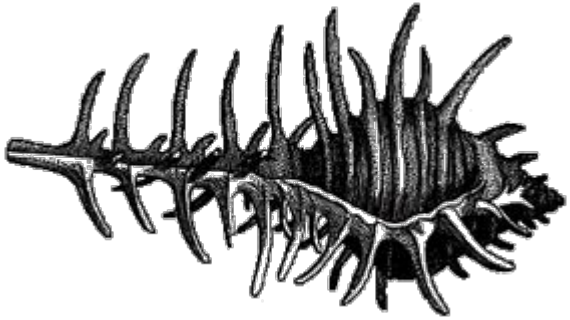
Zardus

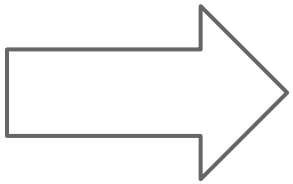

SHELLFISH
HEX on the Beach


SHELLPHISH

???


DEFCON



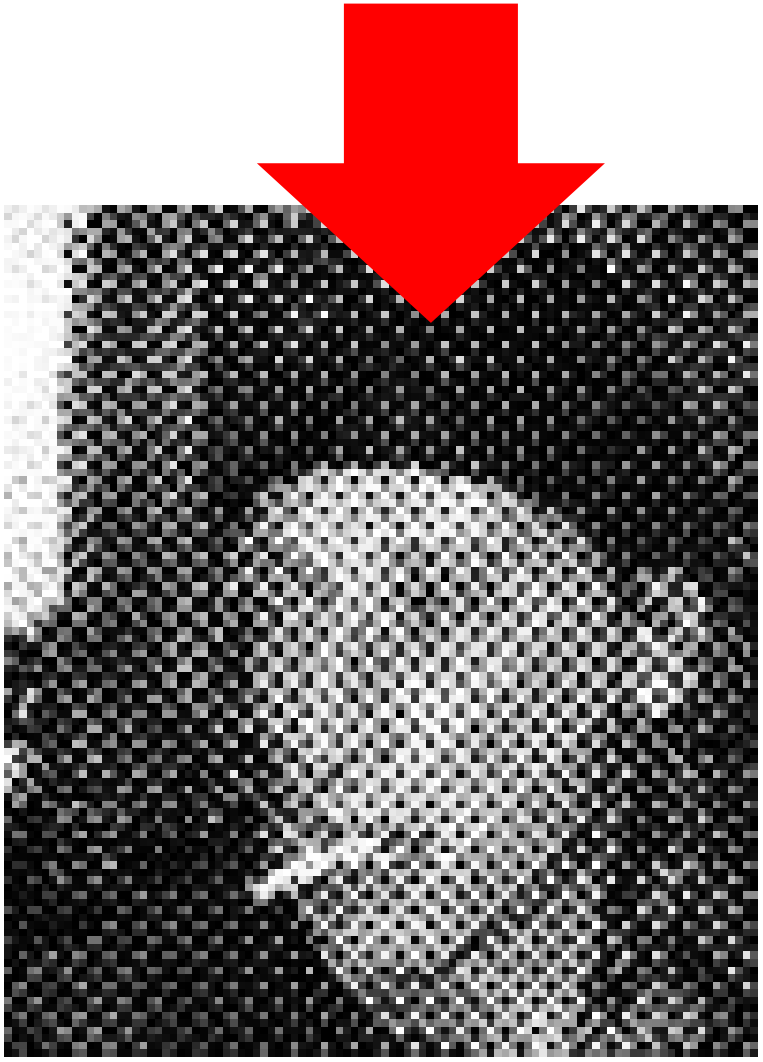



SHELLPHISH

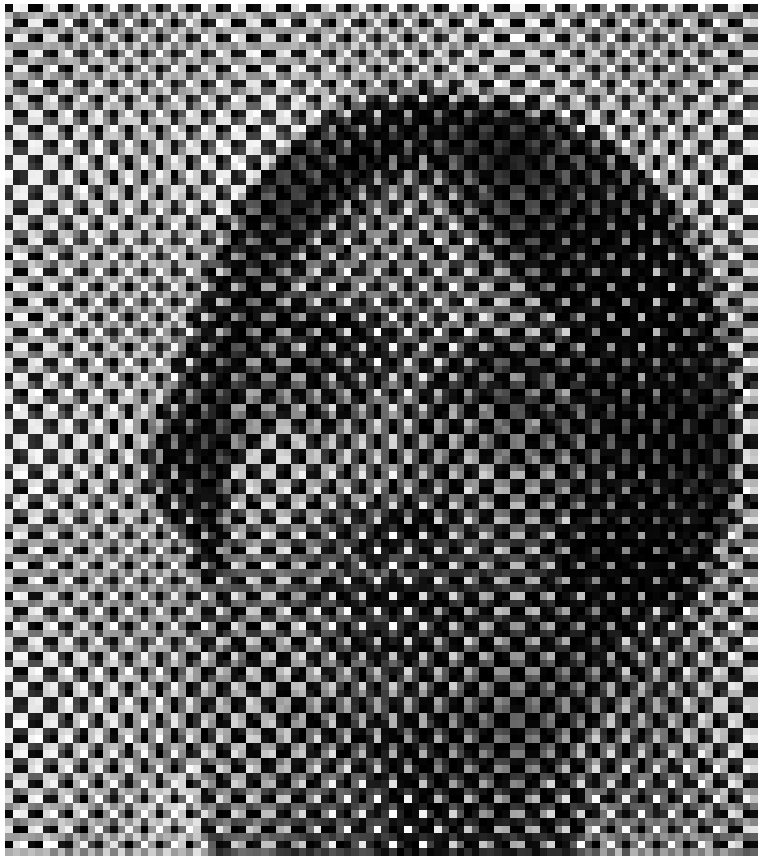
THE COMPUTER SECURITY GROUP AT UC SANTA BARBARA

Giovanni Vigna

Christopher Kruegel



zanardi



VOID

SIMULATION
2004

UC Santa Barbara

sicko irish

nullptr **zanardi**

balzaroth void

SIMULATION
2005

UC Santa Barbara

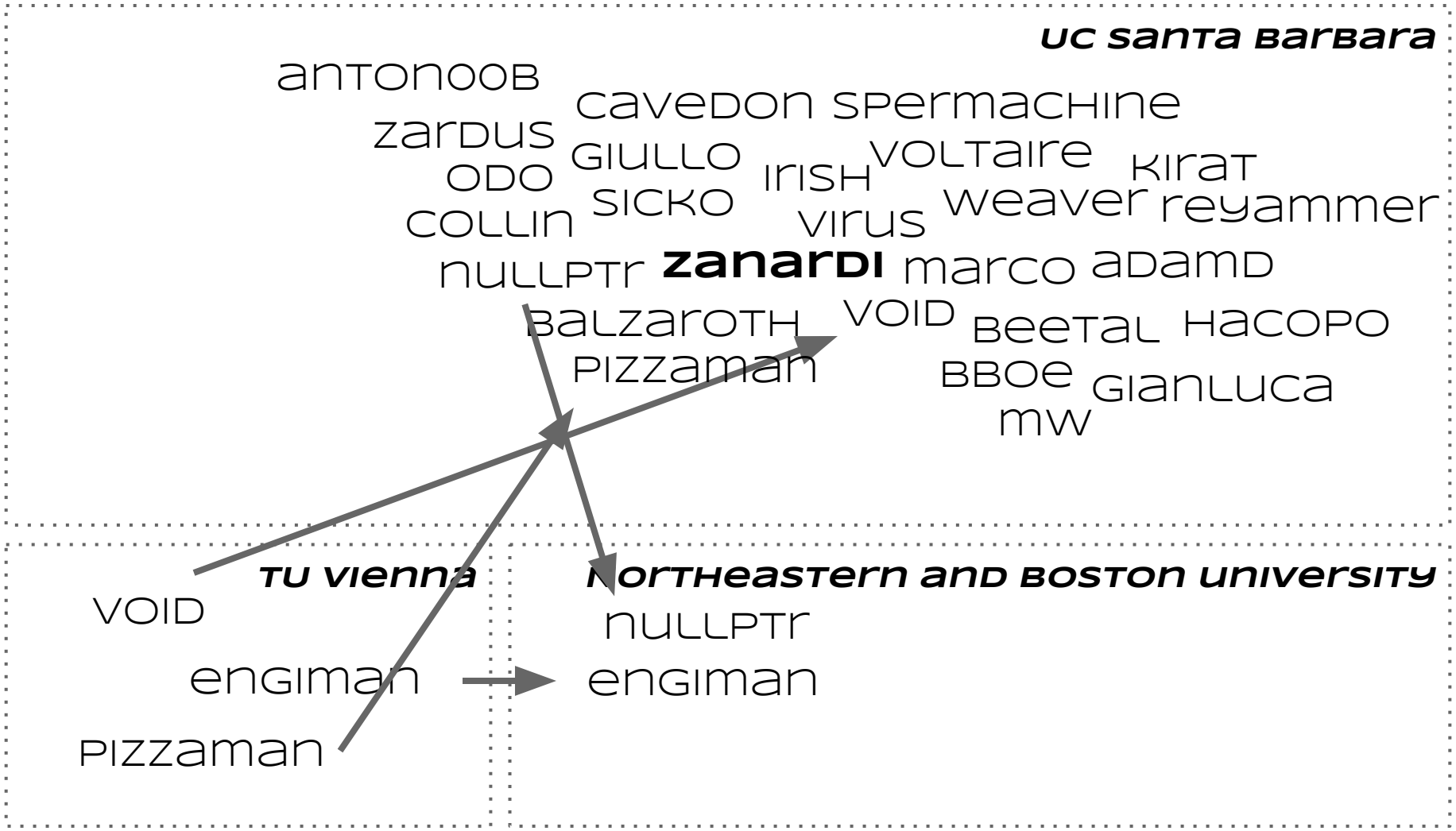
sicko irish
virus weaver
nullptr **zanardi** marco
balzaroth void beetal

TU Vienna

void
engiman
pizzaman

SHELLPHISH

SIMULATION
2006 - 2011



SIMULATION
2011 - 2014

UC Santa Barbara

antonoob
salls zardus cavedon spermachine
subwire fish odo giullo irish voltaire kirat
jay collin sicko virus weaver reyammer
zanardi marco adamd
balzaroth void beetal hacopo
pizzaman cao bboe gianluca
rhelmot nezorg mw vitor

Northeastern and Boston University

nullptr mw acez
engiman crowell
collin mossberg pizzaman

SIMULATION
2015

UC LONDON
GIANLUCA

ASU
ADAMD

EURECOM
BALZAROTH

UC SANTA BARBARA
ANTONOOB
SALLS ZARDUS
SUBWIRE FISH ODO
DONFOS JAY
DOUBLE
ACEZ
MIKE_PIZZA
CAVEDON SPERMACHINE
GIULLO VOLTAIRE KIRAT
SICKO IRISH WEAVER REYAMMER
VIRUS
ZANARDI MARCO ADAMD
BALZAROTH VOID BEETAL HACOPO
CAO BBOE GIANLUCA
RHELMOT NEZORG VITOR

NORTHEASTERN AND BOSTON UNIVERSITY
NULLPTR MW ACEZ
ENGIMAN CROWELL
COLLIN MOSSBERG PIZZAMAN

SIMULATION
MODERN DAY

UC LONDON

GIANLUCA

ASU

ADAMD

EURECOM

BALZAROTH

UC SANTA BARBARA

ANTONOOB
CAVEDON SPERMACHINE
SALLS ZARDUS
GIULLO VOLTAIRE KIRAT
SUBWIRE FISH ODO
IRISH
SICKO WEAVER REYAMMER
VIRUS
DONFOS JAY
ZANARDI MARCO
DOUBLE
VOID BEETAL HACOPO
ACEZ
CAO BBOE
MIKE_PIZZA
RHELMOT NEZORG
VITOR

NORTHEASTERN AND BOSTON UNIVERSITY

NULLPTR MW
ENGIMAN CROWELL
COLLIN MOSSBERG PIZZAMAN

SIMULATION
MODERN DAY

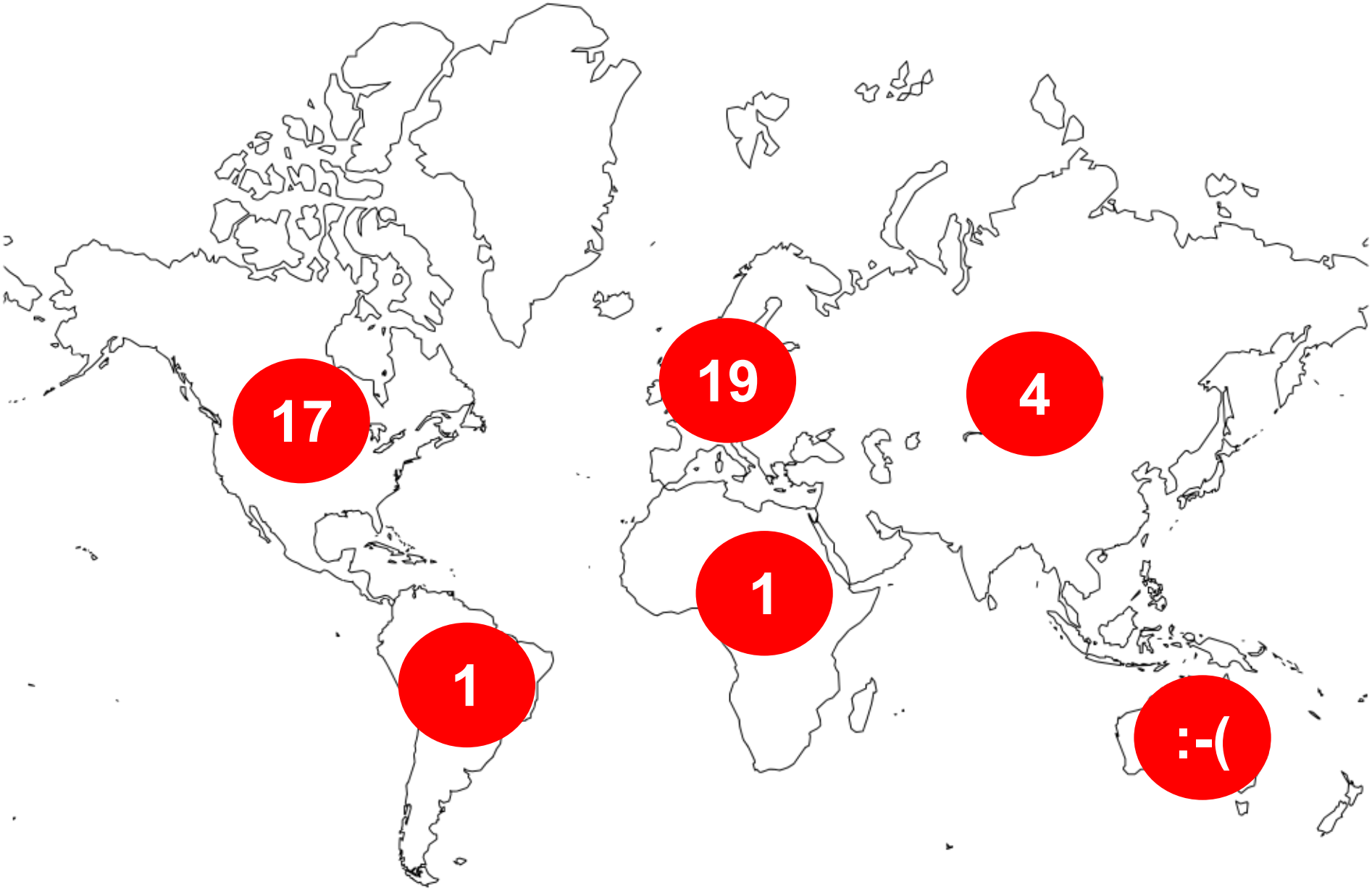
UC LONDON
GIANLUCA

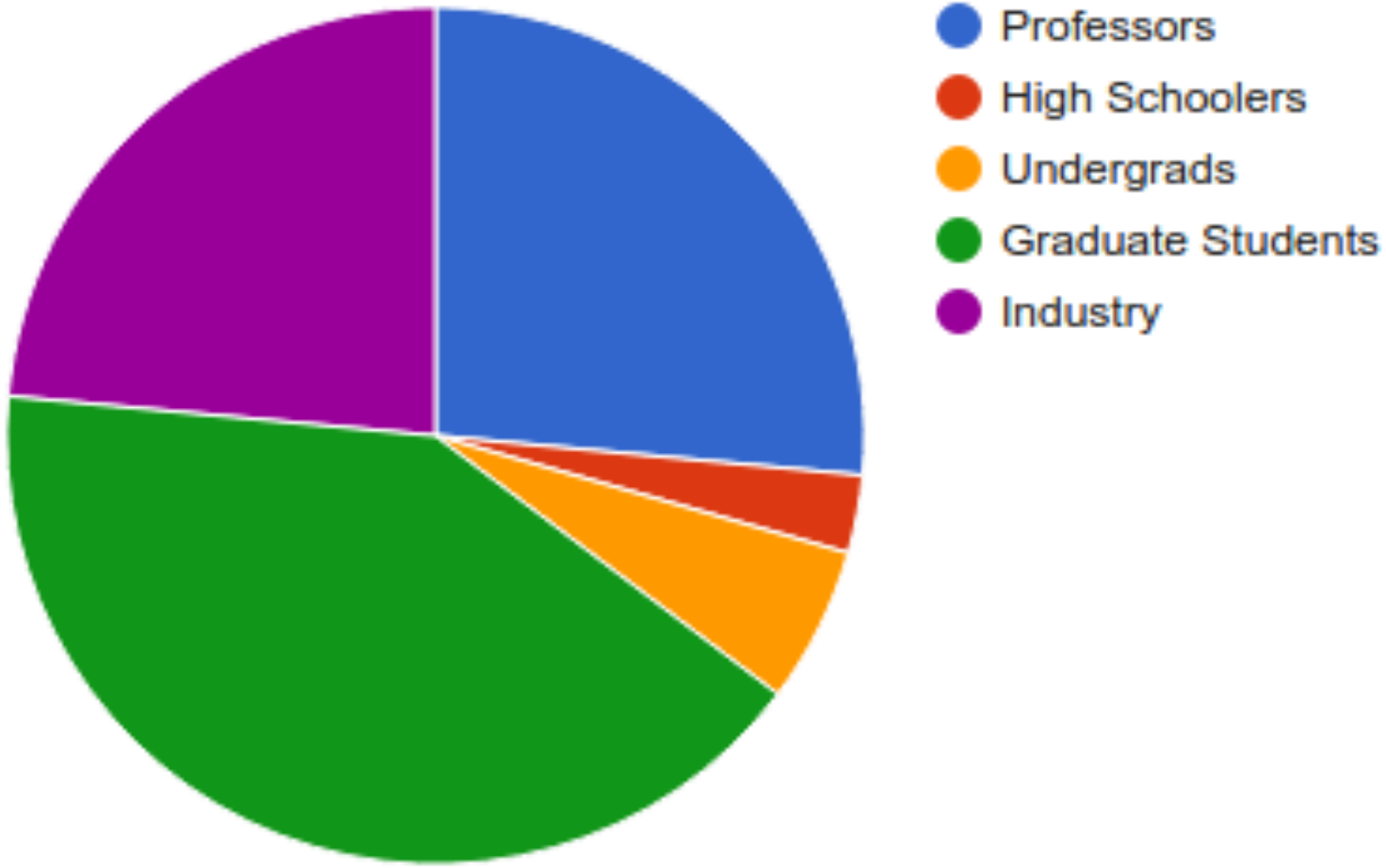
ASU
ADAMD

EURECOM
BALZAROTH

UC SANTA BARBARA
ANTONOOB
CAVEDON SPERMACHINE
SA ZARDUS
SUBWI FISH
KIRAT
REYAMMER
DONFOS JAY
ZANARDI
DOUBLE
VOID
HACOPO
ACEZ
CAO
MIKE_PIZZA
RHELMOT NEZORG

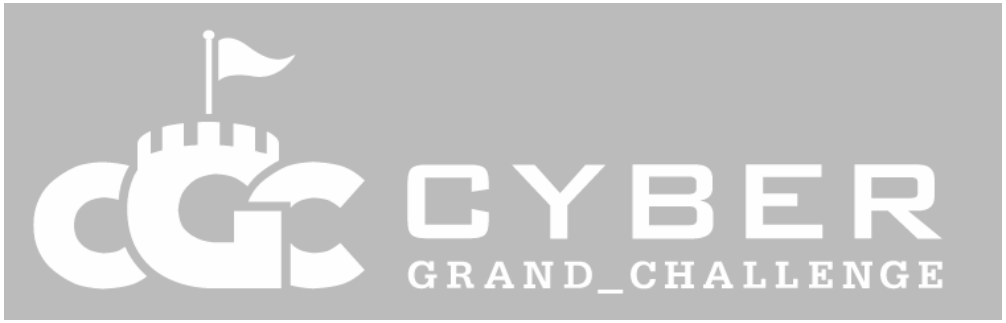
NORTHEASTERN AND BOSTON UNIVERSITY
NULLPTR MW
ENGIMAN CROWELL
MOSSBERG PIZZAMAN


17
19
4
1
1
:-(

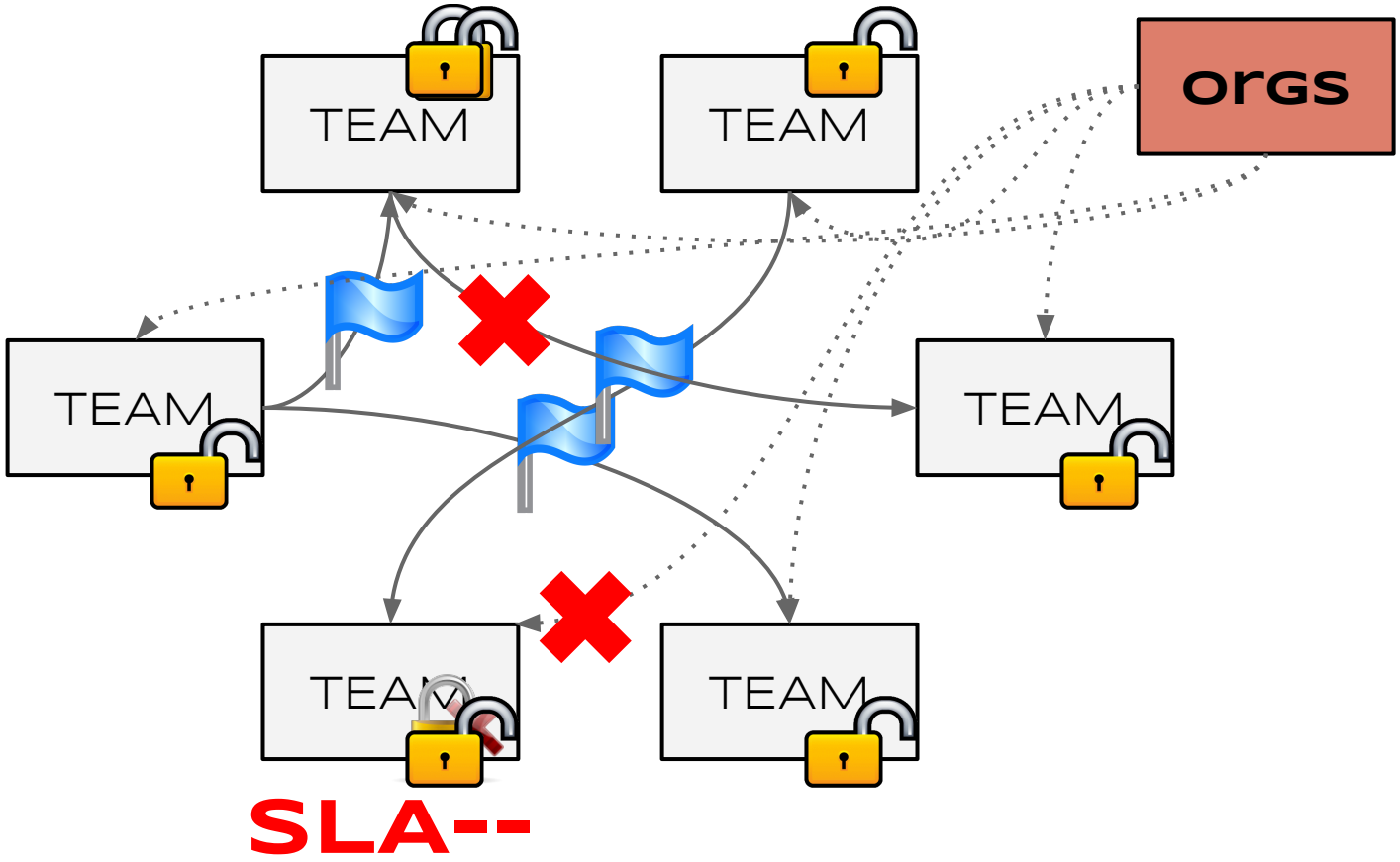

Professors
High Schoolers
Undergrads
Graduate Students
Industry


SHELLPHISH


DEFCON

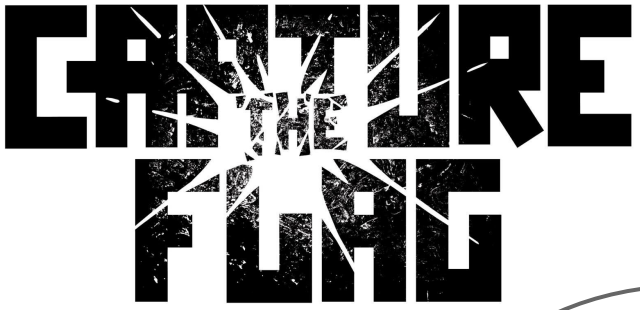

CGC
CYBER
GRAND_CHALLENGE

DEFCON



CAPTURE THE FLAG

BEFORE: practice!
DURING: hack!
AFTER: party!



BEFORE: write tools!

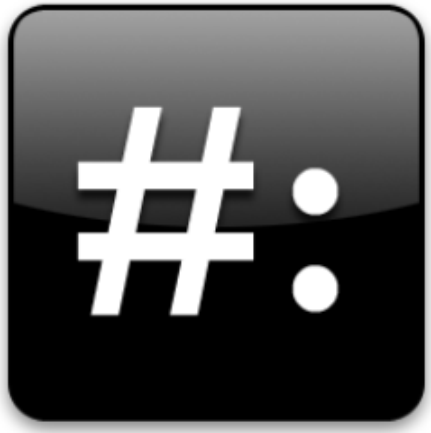
DURING: debug tools!

AFTER: plan new tools!

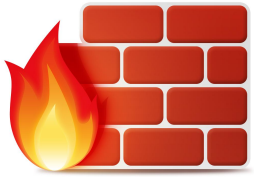
REMINISCING
2009

DEFCON

x86



SYSCALL IDS



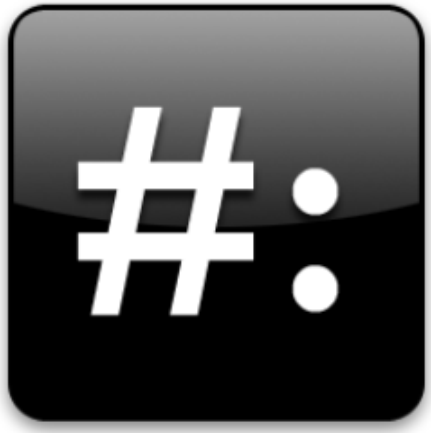
FAIL

0% SLA!
-2 Hackers

REMINISCING
2010

DEFCON

x86



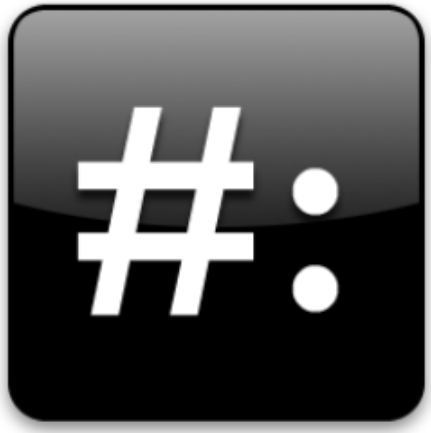
DTRACE

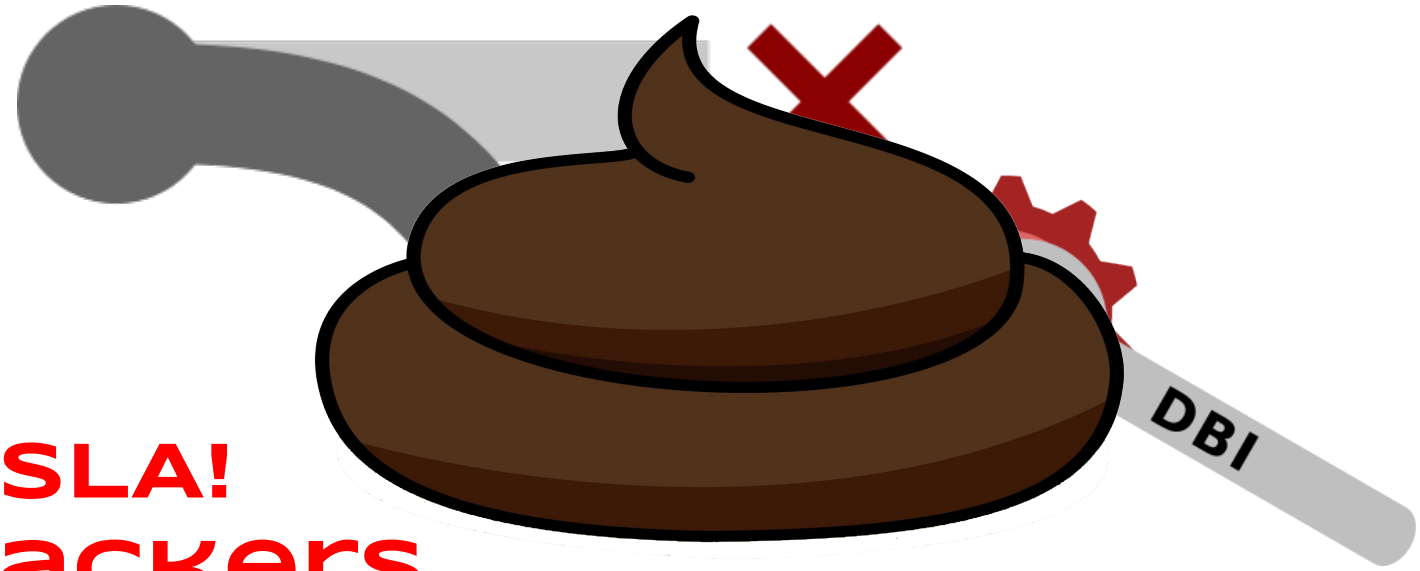
-2 Hackers

REMINISCING 2011

DEFCON

x86





0% SLA!

-4 Hackers

REMINISCING
2012+

DEFCON

0% SLA!

SHELLPHISH TOOLS!

https://github.com/shellphish/puppeteer

https://github.com/reyammer/shellnoob

https://github.com/acama/xrop

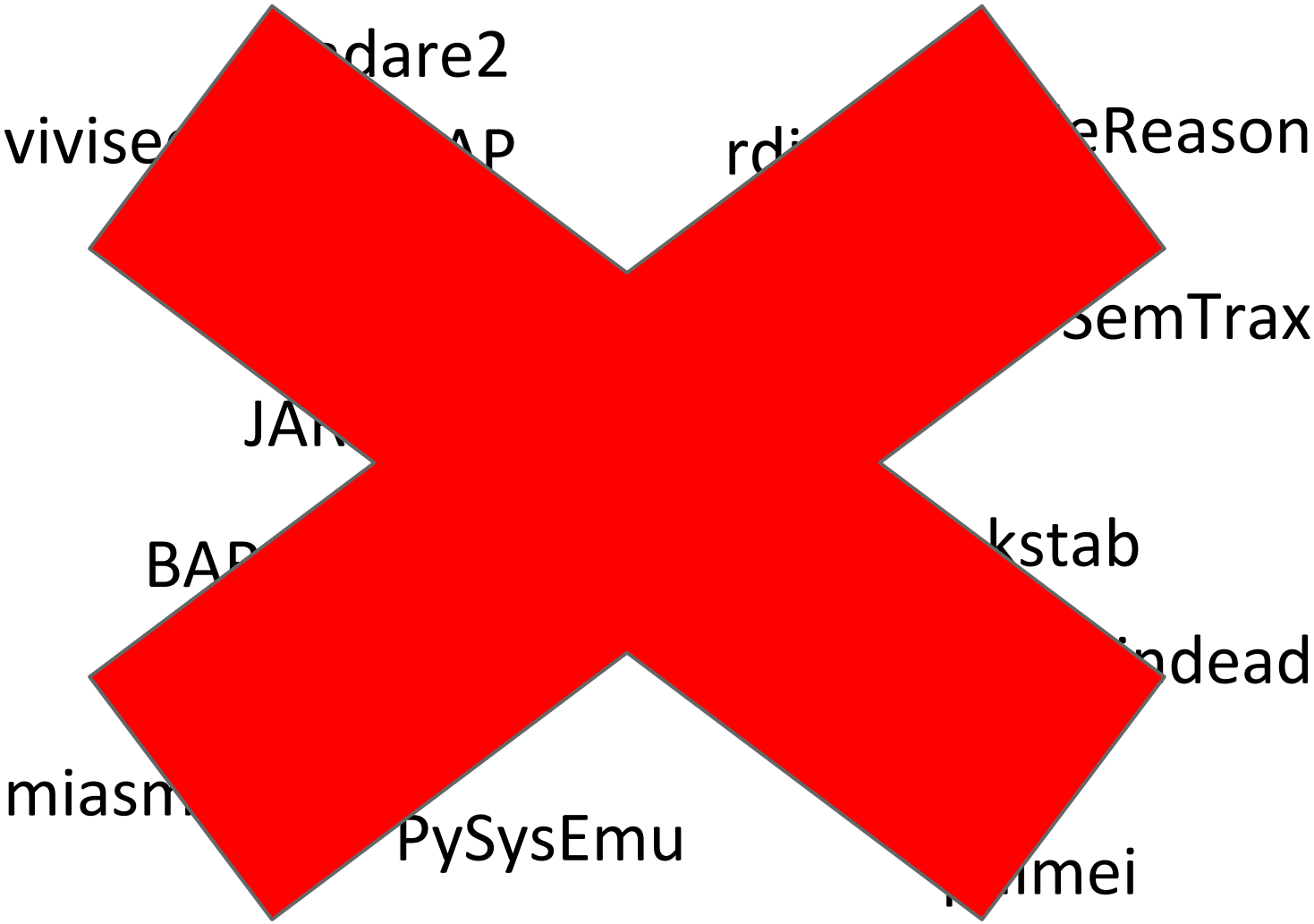
https://github.com/zardus/preeny

https://github.com/zardus/memcurses

https://github.com/zardus/idalink

https://github.com/angr/angr

The next generation of binary analysis.


dare2
eReason
SemTrax
kstab
ndead
PySysEmu
imei

2005 Hex-Rays was founded

2007 Hex-Rays Decompiler 1.0

2009 Hex-Rays IDA 5.5

2011 Hex-Rays IDA 6.1

2013 Hex-Rays IDA 6.4

2015 WHY???????

- Making binary analysis techniques usable!

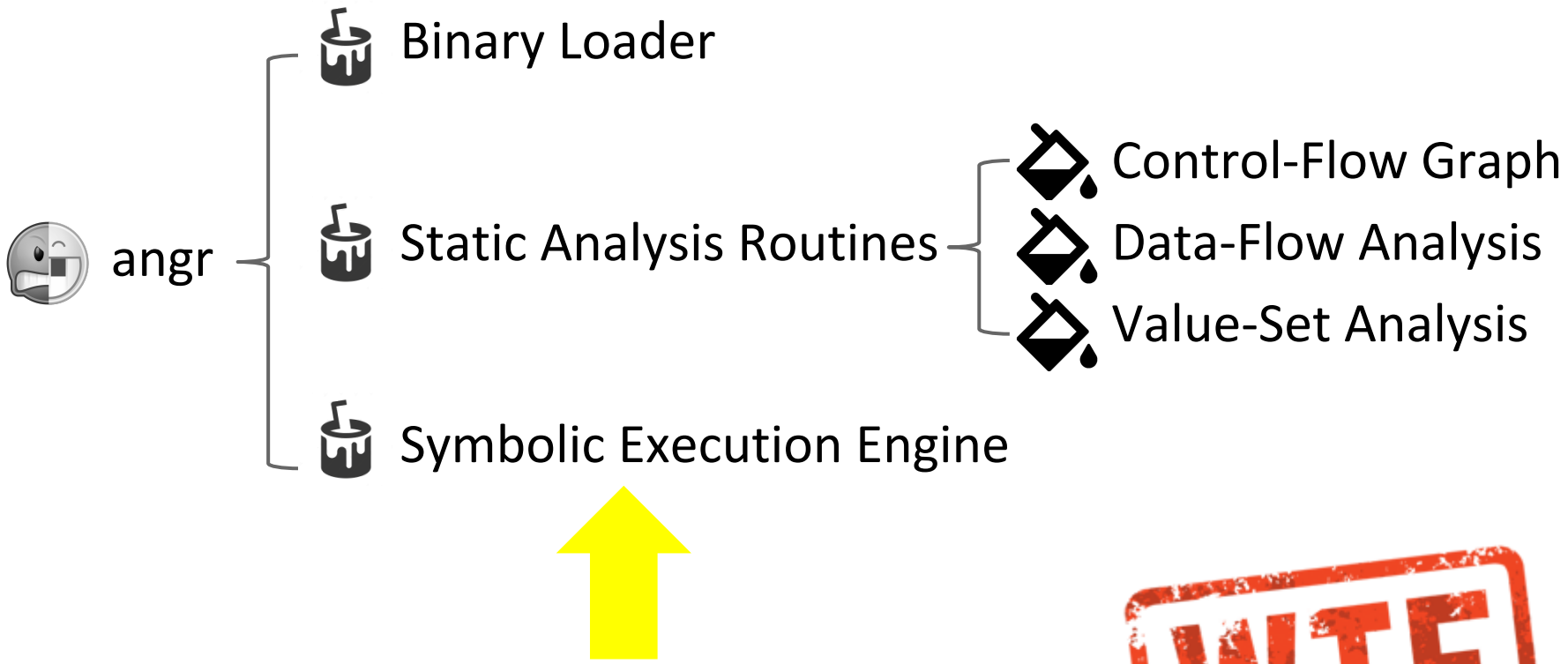
- Open-source:
  https://github.com/angr/angr (star it!)

- Written in Python!
  - installable with **`pip install angr`**
  - interactive shell (using ipython)
  - GUI

- Architecture independent

  x86, amd64, mips, mips64, arm, aarch64, ppc, ppc64

  ELF, **CGC**, PE


Binary Loader
angr
Static Analysis Routines
Control-Flow Graph
Data-Flow Analysis
Value-Set Analysis
Symbolic Execution Engine
WTF

"How do I trigger path X or condition Y?"

1. Interpret the application to identify symbolic variables.

   ```
   read(0, &x, 4);
   ```

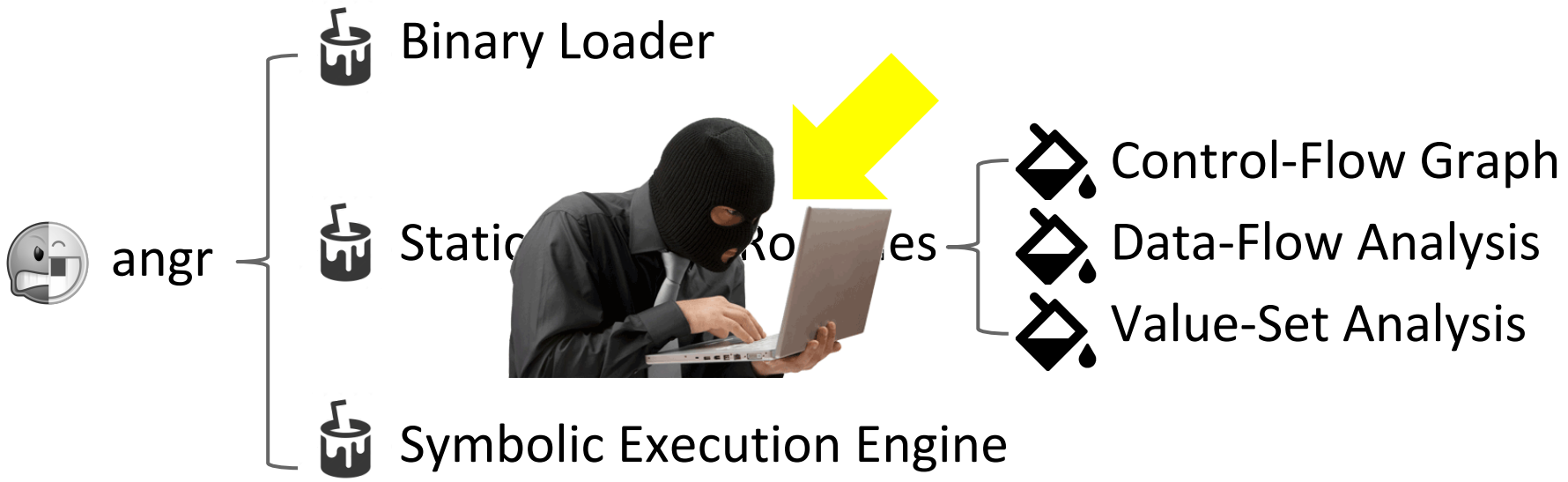
2. Track "constraints" on symbolic variables.

   ```
   if (x < 100 && x >= 10)
   ```

3. When the required condition is triggered, "concretize" to obtain a possible input.

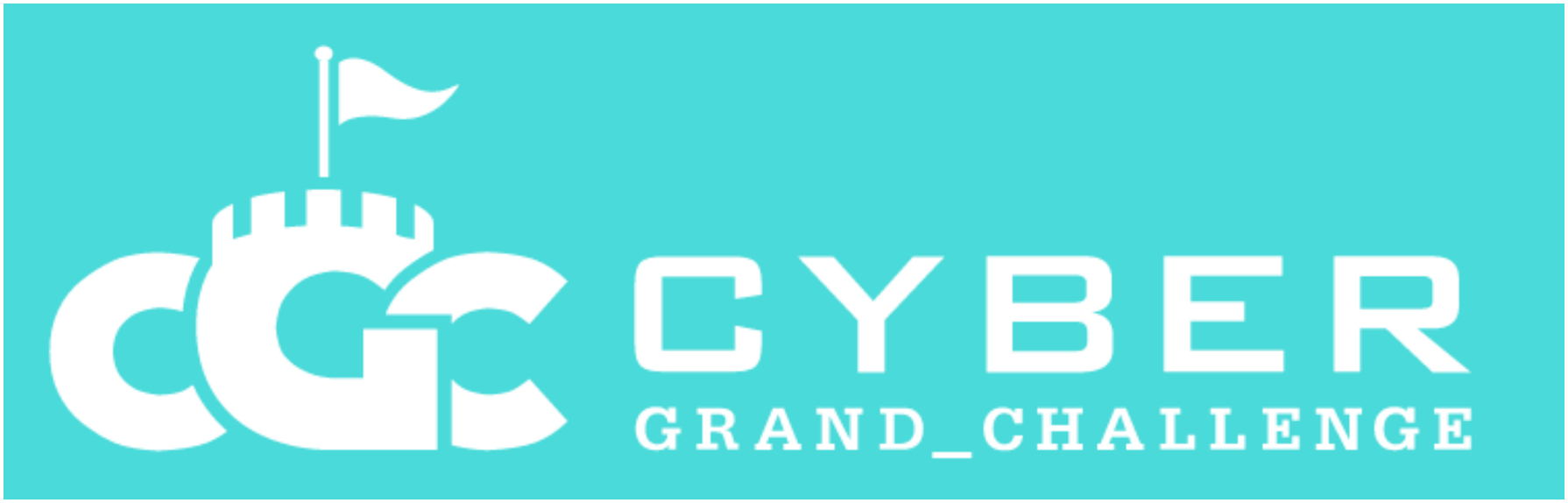
   ```
   if (x < 100 && x >= 10)
      puts("You win!");
   ```

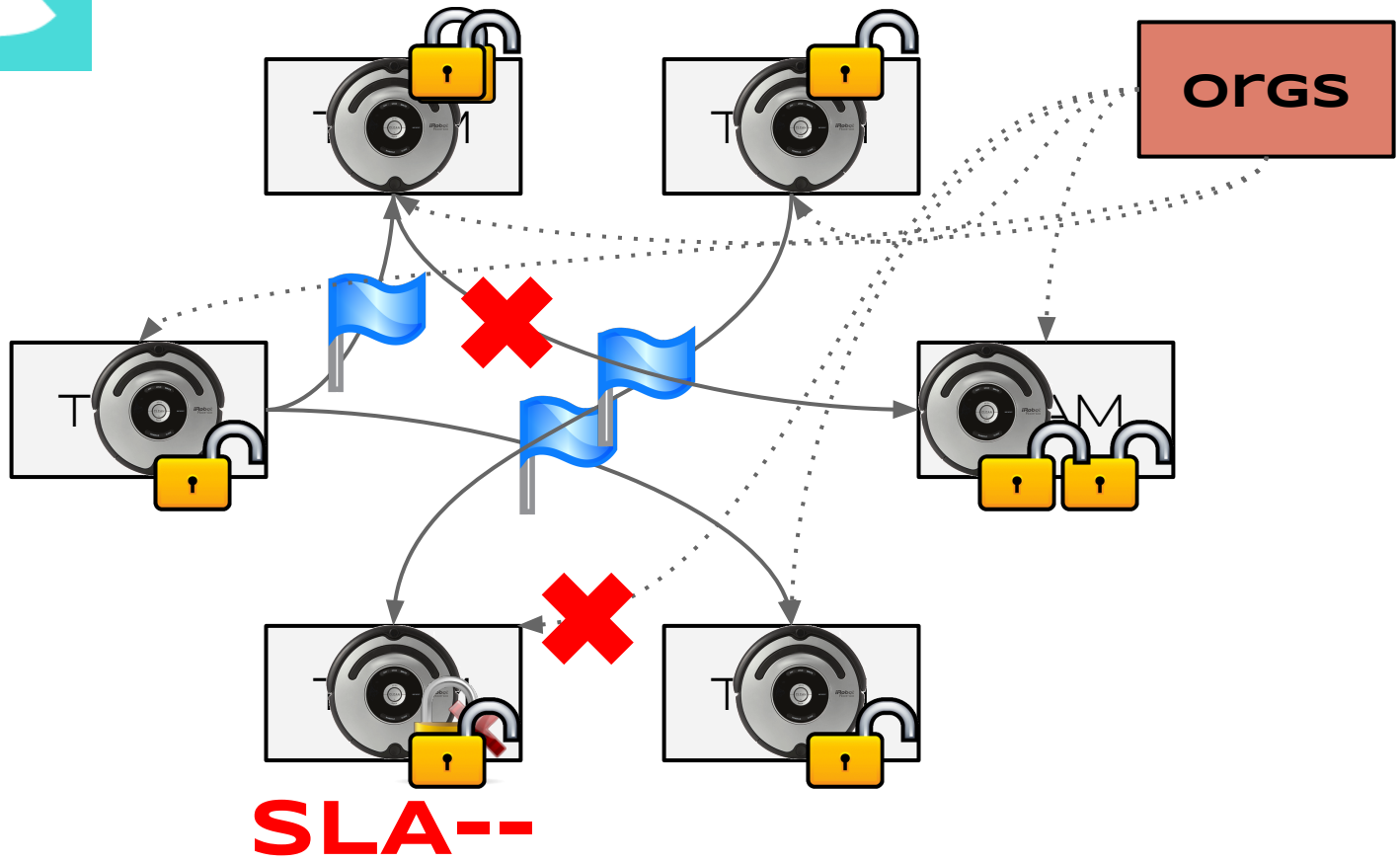

KEEP
CALM
ITS TIME FOR
A
DEMO!


angr
Binary Loader
Static
Ro
es
Control-Flow Graph
Data-Flow Analysis
Value-Set Analysis
Symbolic Execution Engine

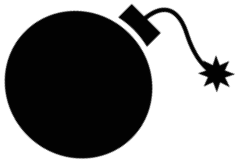
Whitehat CTF - crypto400

```
if (prefilter(input))
  error("PLEASE CHECK AGAIN!")
else
  puts("INPUT OK")
do_[illegible]crypto(input, result)
if (strcmp(result, "growfish") == 0)
  printf("FLAG: %s\n", ...)
else
  puts("INPUT IS NOT GOOD ENOUGH.")
```


CGC
CYBER
GRAND_CHALLENGE

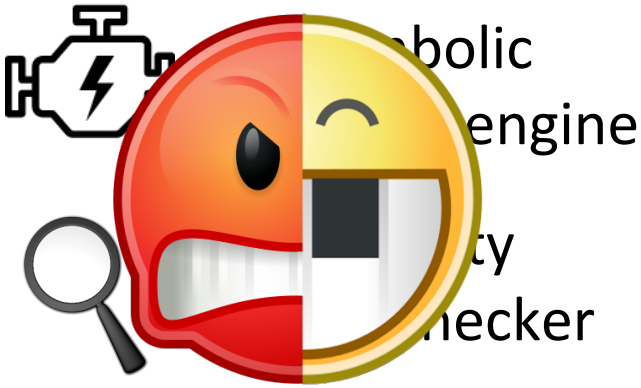

orgs
SLA--

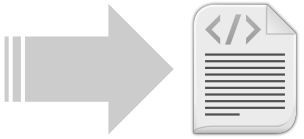

SHELLPHISH
inside



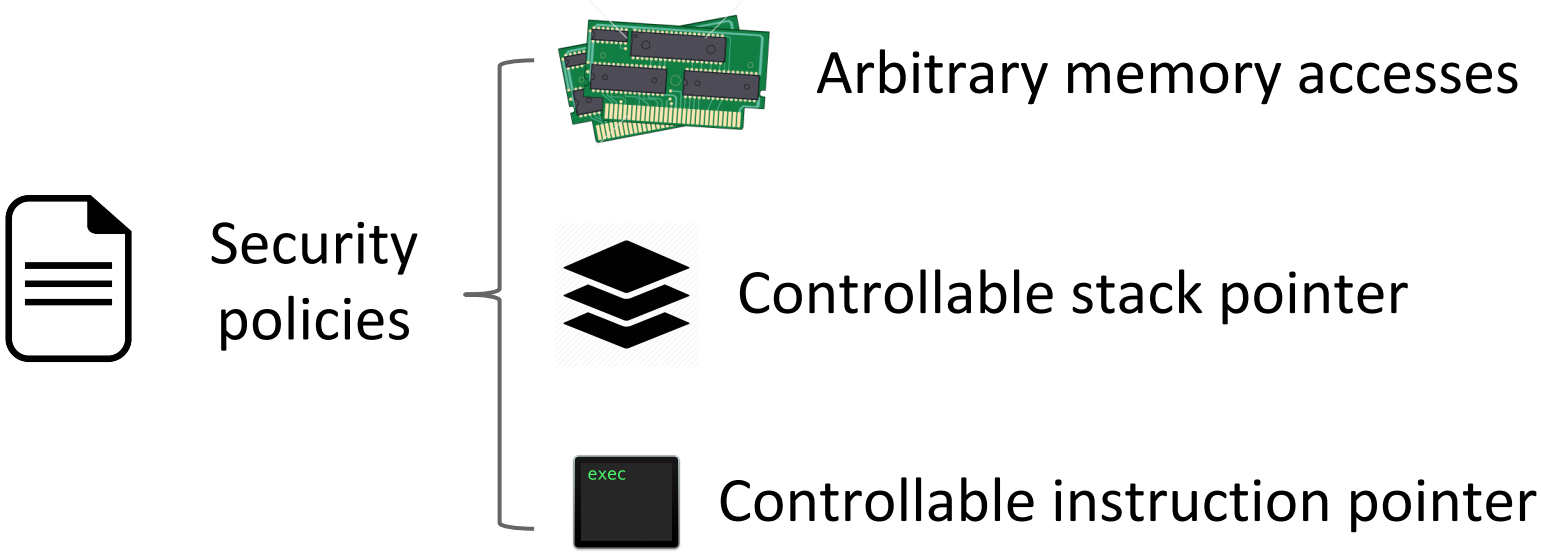
Program

Security policies





Exploit



CGC Qualifiers Goal: **CRASH**

CGC Finals Goal: **EXPLOIT**


WANTED
DEAD OR ALIVE
PRODIE "THE MAD
Italian
WESTMONT COLLEGE

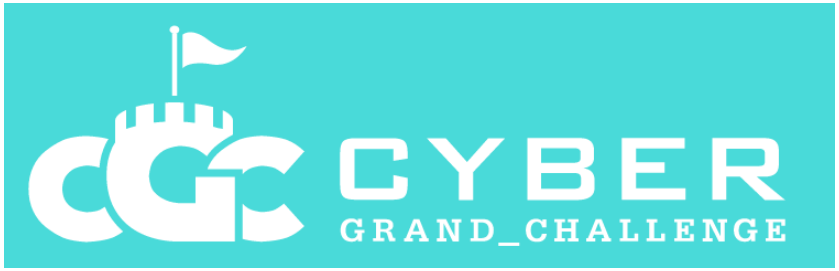

WANTED
DEAD OR ALIVE


WANTED
DEAD OR ALIVE
PRODIE "THE MAD
Italian
WESTMONT COLLEGE


SHELPHISH


SHELLFISH

~0% SLA!



56% SLA!

Looking toward the future!

- CGC finals!
  - $2,000,000 top prize
  - Shellphish VS Shellphish CRS
- CTFs
  - Can our tools finally help us?
- What do we do with our $750,000?

References:

this presentation: https://goo.gl/xFYltI
hitcon ent presentation: http://goo.gl/3ulxRa
angr: https://github.com/angr/angr
contact: yans@cs.ucsb.edu, @Zardus

2004

zanardi

void

nullptr

balzaroth

sicko

irish

2005

engiman

marco

virus

beetal

weaver

2006

collin

pizzaman

2008

odo

adamd

giullo

voltaire

bboe

Ancient History

zanardi

void

nullptr

Balzaroth

engiman

pizzaman

odo

adamd

gianluca

zardus

cavedon

spermachine

kirat

reyammer

antonoob

mw

hacopo

cao

fish

acez

crowell

nezorg

rhelmot

jay

mossberg

salls

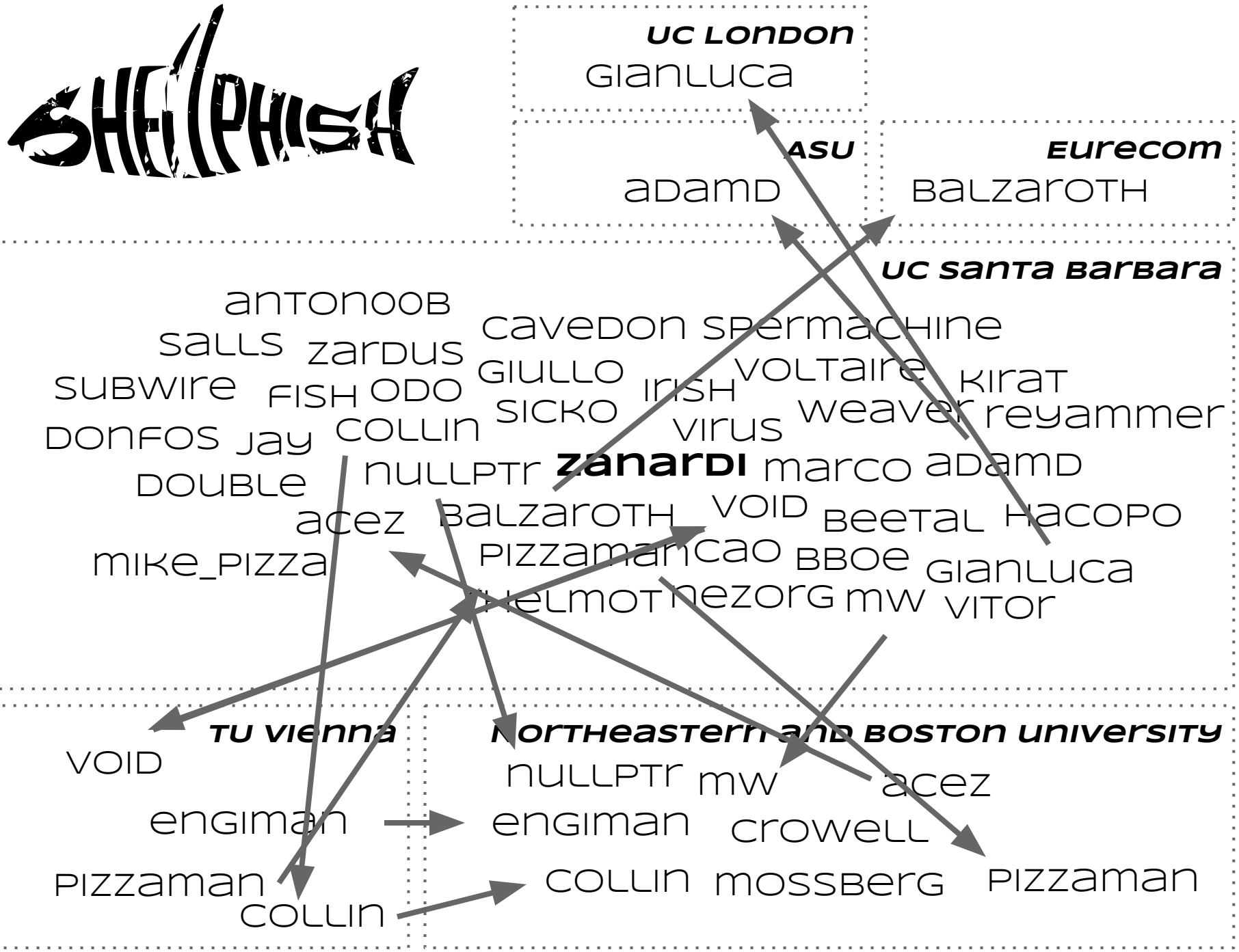
subwire

mike_pizza

vitor

donfos

double


SHELLPHISH
UC LONDON
GIANLUCA
ASU
ADAMD
EURECOM
BALZAROTH
UC SANTA BARBARA
ANTONOOB
CAVEDON
SPERMACHINE
SALLS
ZARDUS
GIULLO
VOLTAIRE
KIRAT
SUBWIRE
FISH
ODO
IRISH
SICKO
WEAVER
REYAMMER
DONFOS
JAY
COLLIN
VIRUS
DOUBLE
NULLPTR
ZANARDI
MARCO
ADAMD
ACEZ
BALZAROTH
VOID
BEETAL
HACOPO
MIKE_PIZZA
PIZZAMANCAO
BBOE
GIANLUCA
HELMOT
NEZORG
MW
VITOR
TU VIENNA
VOID
ENGIMAN
PIZZAMAN
COLLIN
NORTHEASTERN AND BOSTON UNIVERSITY
NULLPTR
MW
ACEZ
ENGIMAN
CROWELL
COLLIN
MOSSBERG
PIZZAMAN