KU LEUVEN

Cheating in Online Games

Stijn Volckaert
stijn.volckaert@kuleuven.be
@StijnVolckaert

DistriNet

Bio

2015: PhD in Computer Science Engineering @ Ghent University
Dissertation: "Advanced Techniques for Multi-Variant Execution"
Supervisors: Prof. Bjorn De Sutter & Prof. Koen De Bosschere

2015-2018: Post-doc @ University of California, Irvine
PI: Prof. Michael Franz


San Diego
(60 minutes)
UC Irvine
Los Angeles
(45 minutes)
Hollywood
(60 minutes)

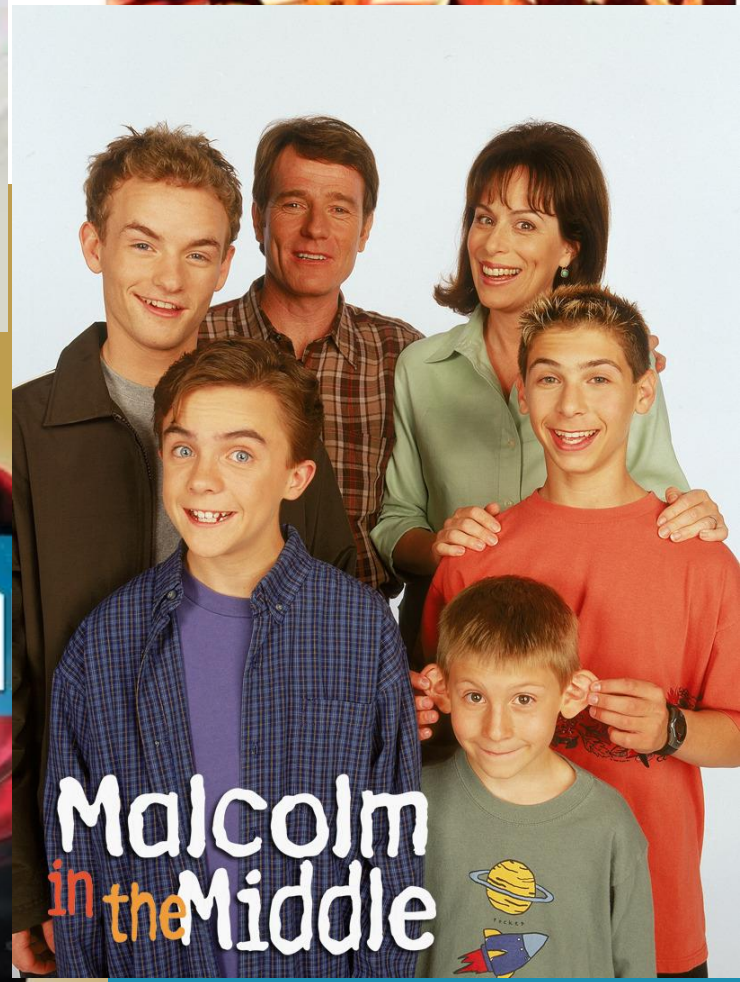

the Real Housewives
OF ORANGE COUNTY
bravo


WIDESCREEN EDITION
starring in alphabetical order
GEORGE CLOONEY
MATT DAMON
ANDY GARCIA
BRAD PITT
and JULIA ROBERTS
OCEAN'S ELEVEN


HORRIBLE BOSSES 2


20th Century-Fox presents
CHARLTON HESTON
ARTHUR P. JACOBS PRODUCTION
PLANET OF THE APES
PANAVISION® Colour by DE LUXE


MARVEL STUDIOS
IRON MA
MARVEL STUDIOS


Malcolm
in the Middle

Bio

2015: PhD in Computer Science Engineering @ Ghent University
Dissertation: "Advanced Techniques for Multi-Variant Execution"
Supervisors: Prof. Bjorn De Sutter & Prof. Koen De Bosschere

2015-2018: Post-doc @ University of California, Irvine
PI: Prof. Michael Franz

2018-…: Associate Professor @ KU Leuven
Research Interests: Memory Safety, Exploit Mitigations, Software Diversity, Compilers, Operating Systems, …

Research

- Protection against remote attackers
- Software diversity techniques and applications
- Secure programming
- Location privacy in social networks
- Protecting online games against cheaters

Alexios (Postdoc)


Jonas


Adriaan


Karel


Ruben


Alicia

Unofficial Bio

2001-…: I play(ed) games on the internet

- Unreal Tournament
- Enemy Territory
- Call of Duty 4
- League of Legends
- World of Warcraft

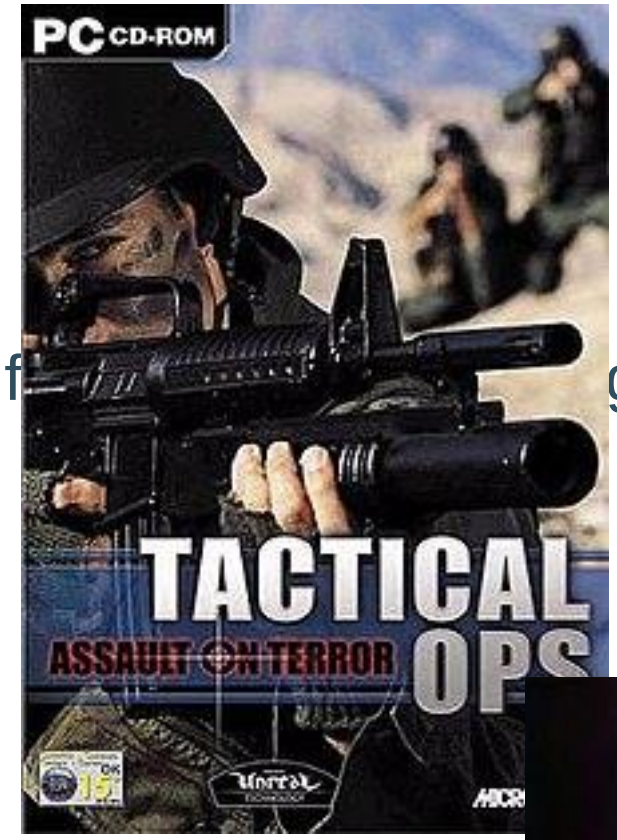
2002-2006: I wrote a lot of mods (modifications) and plugins for games on the internet

2007-…: I write cheat protection for games on the internet

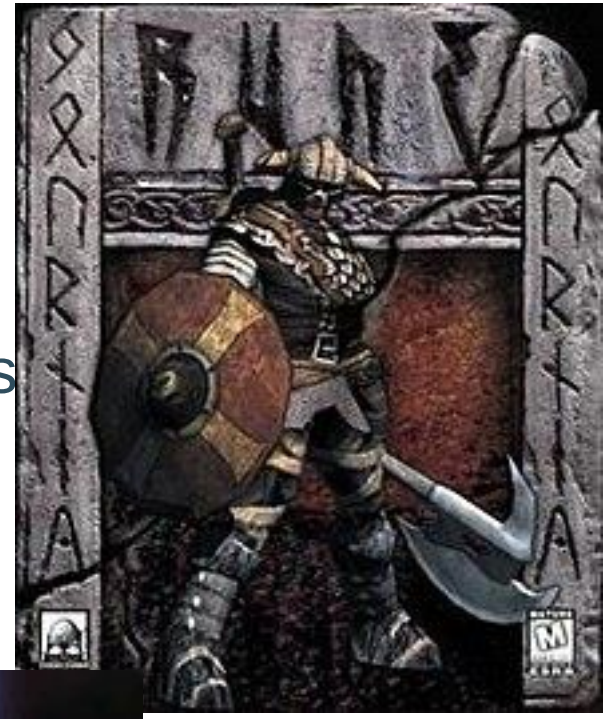
2019-…: I joined OldUnreal to maintain games on the internet

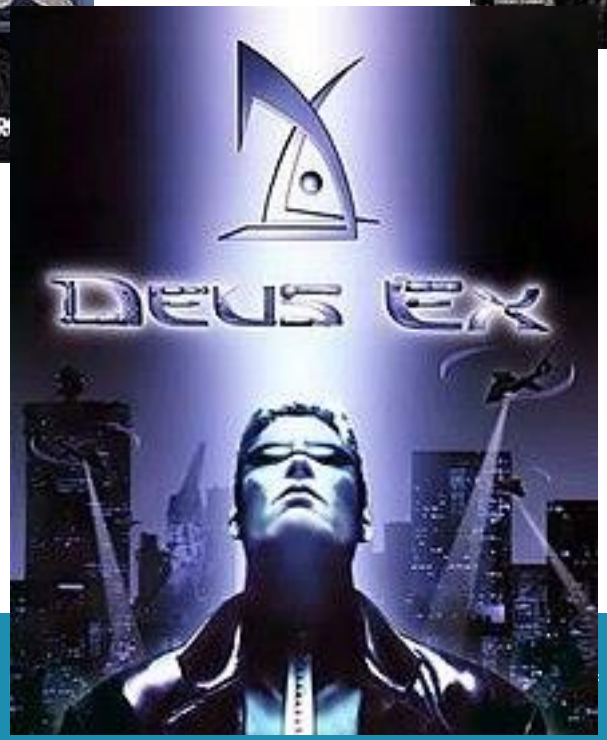
About ACE

f



gine 1 games





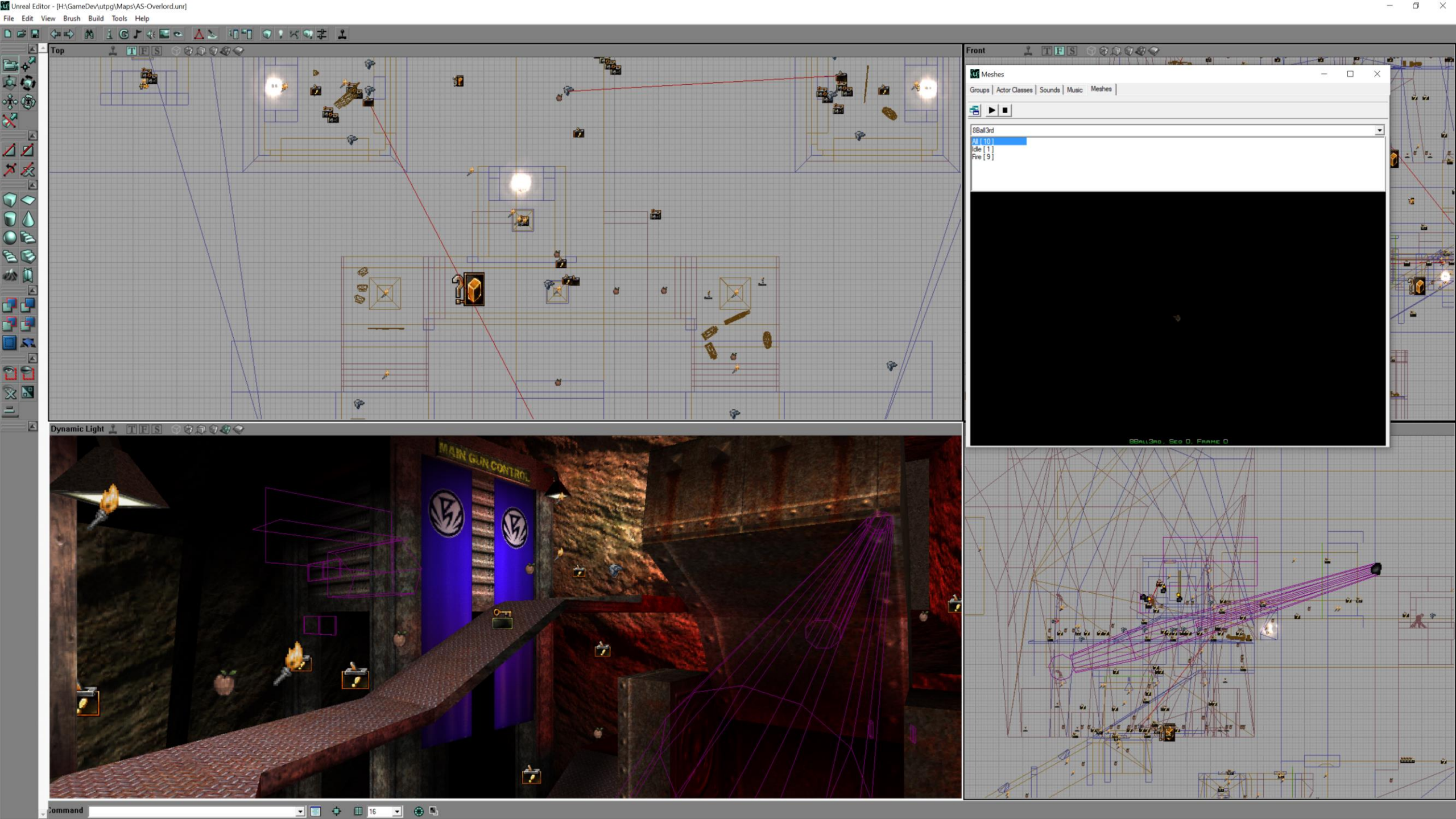
About ACE

- Unofficial cheat protection for several Unreal Engine 1 games
- Mandatory use in all major online competitions

- Most of these games are (close to) dead, but ACE lives on…

About Unreal Tournament

- Released by Epic Games in 1999
- First online game of the series
- First hit game based on Unreal Engine
- Received critical acclaim, sold millions of copies
- Years ahead of the competition technology wise
- Super competitive at the time
- Had its own scripting language (UnrealScript), C++ SDK, and great development tools


Unreal Editor - [H:\GameDev\utpg\Maps\AS-Overlord.unr]
File Edit View Brush Build Tools Help
Top
Front
Meshes
Groups | Actor Classes | Sounds | Music | Meshes
8Ball3rd
All [10]
Idle [1]
Fire [9]
Dynamic Light
MAIN GUN CONTROL
Command

About Unreal Tournament

- In all Unreal Engine 1-3 games, game logic is written in **UnrealScript**
- Interpreted language (like Python!)
- Strongly typed (like Java)
- Single inheritance (like Java)
- Compiled to bytecode (like Java)
- Great foreign function interface and bindings for interaction with C++ code

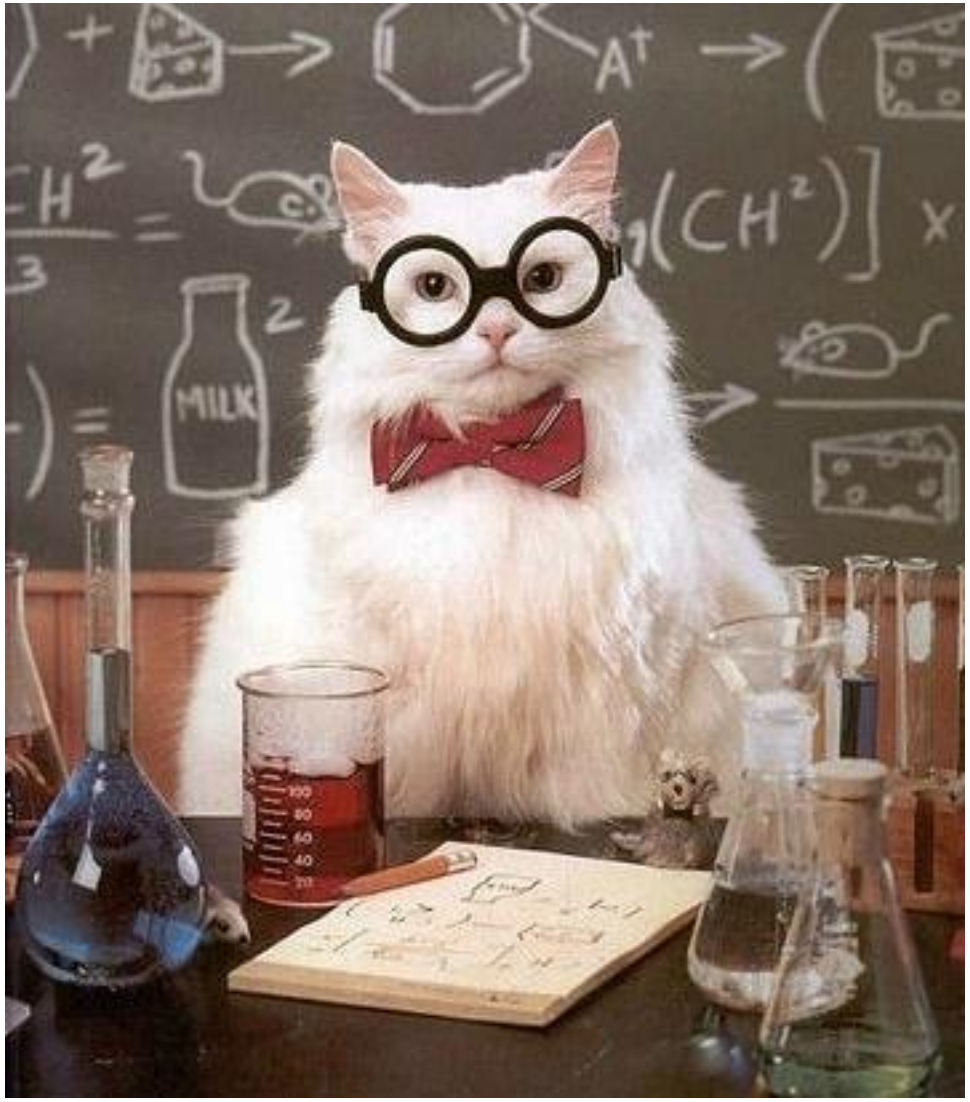
```
class SampleClass extends Actor;

// Declare some variables.
var int i;

// Called when gameplay begins.
function BeginPlay()
{
    SetTimer(1,true);
}

// Called every 1 second, due to SetTimer call.
function Timer()
{
    i=i+1;
    BroadcastMessage("Counting... "$i);
}
```

OldUnreal

- Took over maintenance of Unreal and Unreal Tournament after reaching an agreement with Epic Games
- Ported games to modern Linux, macOS, Raspberry PI, ...
- Fixed hundreds of game-breaking bugs and security vulnerabilities
- Added support for IPv6, modern DirectX, OpenGL, Vulkan, Metal, …
- …

Overview

- Cheats
  - Types of cheats
  - Why is cheating possible?
  - How do people develop cheats?
- Cheat protection
  - Common techniques
  - How do these techniques work?
  - What could be done to improve cheat protection?



Cheating

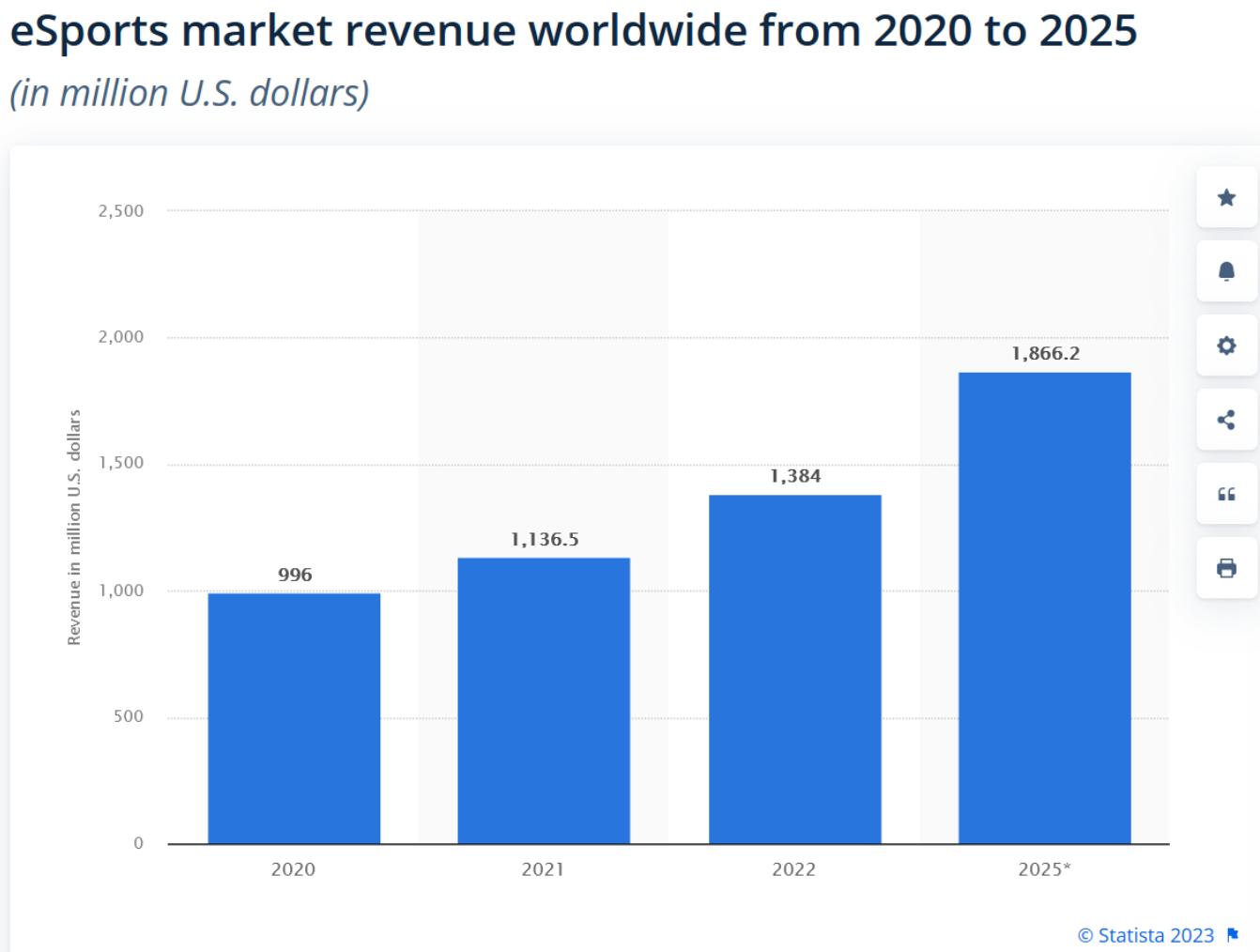
WCG


WORLDS 2016

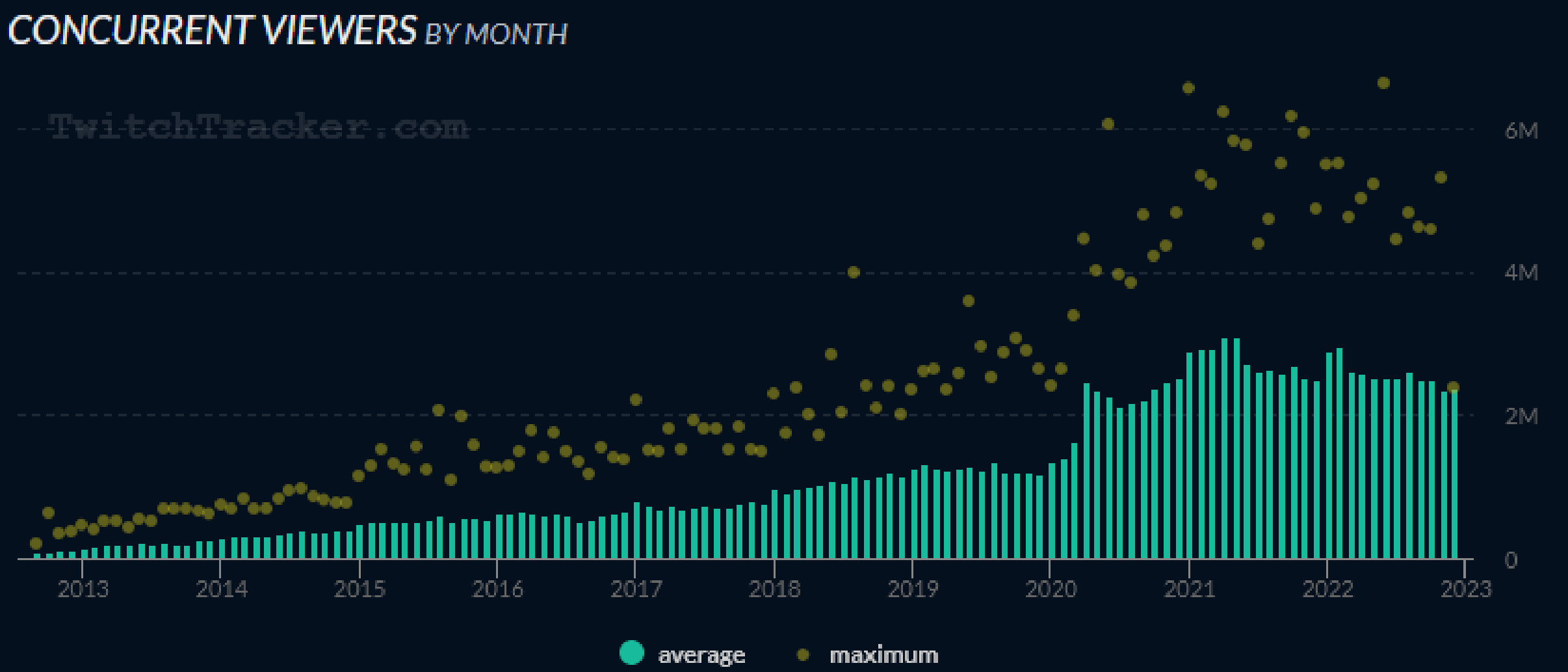
Gaming = Big Business

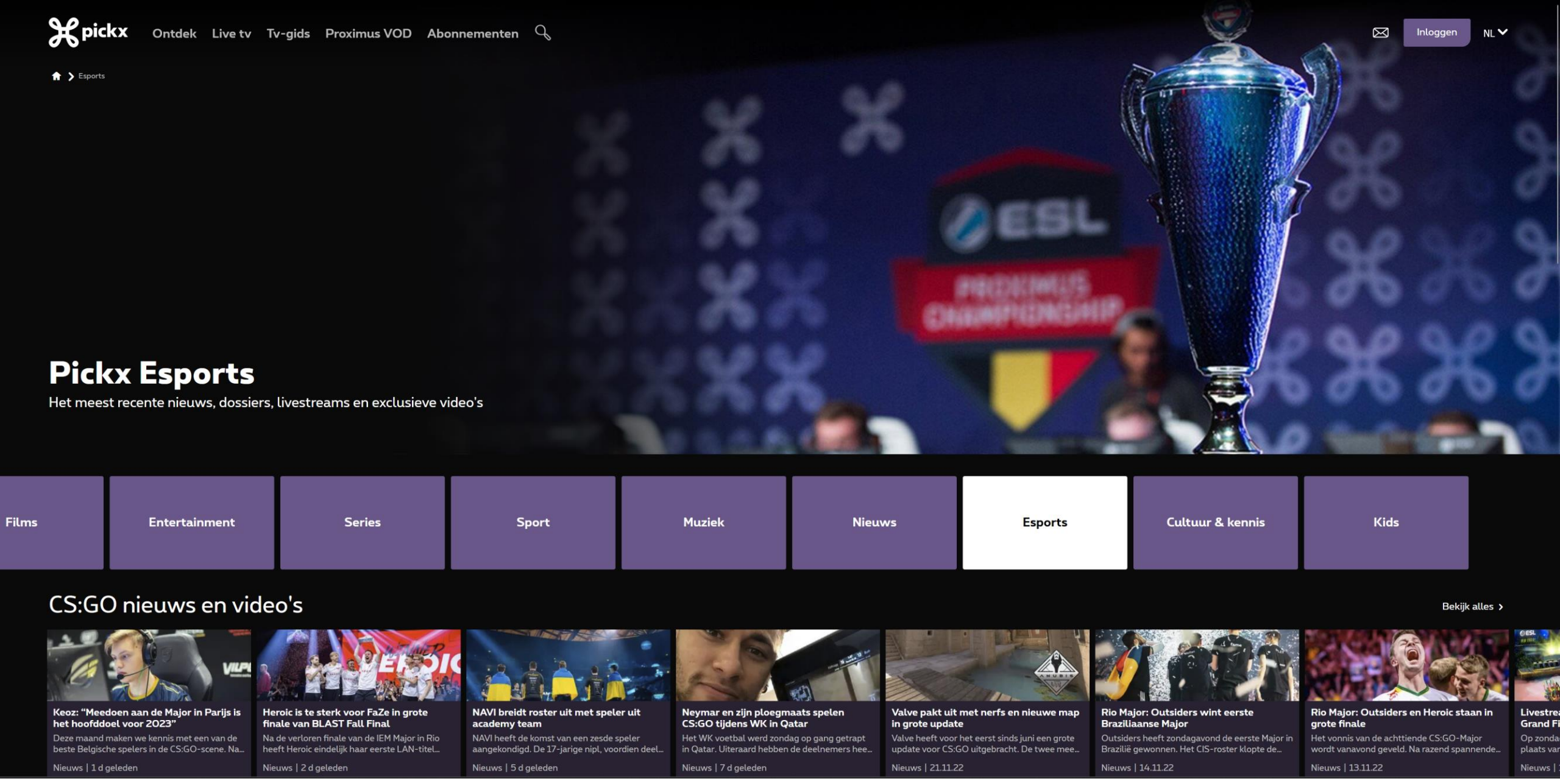
#	GAME	PRIZE MONEY TOTAL	Number of Tournaments
1	DOTA 2	$290,619,417.10	1689
2	Fortnite	$141,292,856.05	861
3	CS:GO	$139,967,670.07	6396
4	League of Legends	$95,944,675.41	2745
5	PUBG (PC only)	$48,748,397.38	548
6	Overwatch	$34,278,670.88	811

Gaming = Big Business

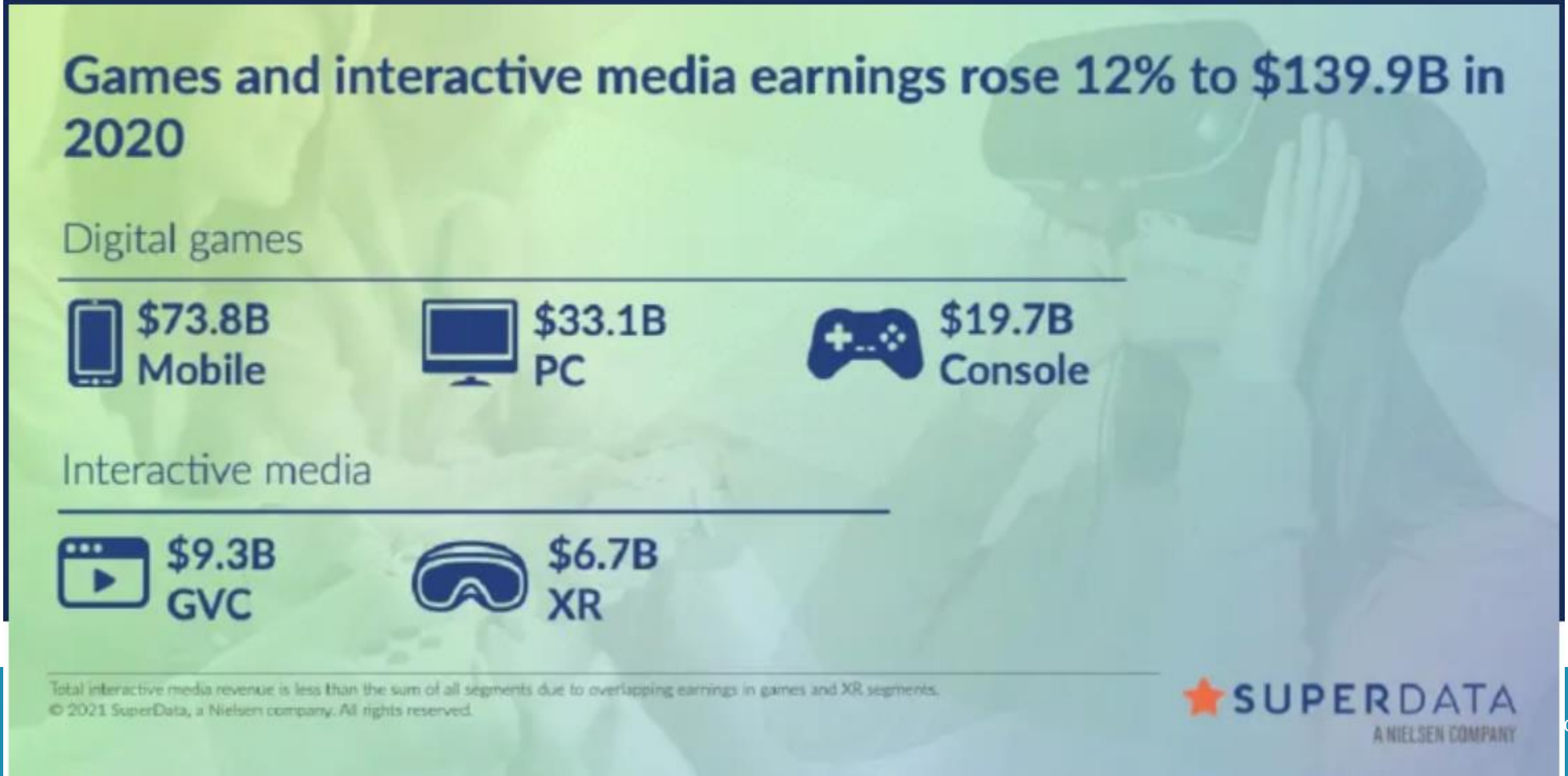


Gaming = Big Business




pickx
Ontdek
Live tv
Tv-gids
Proximus VOD
Abonnementen
Inloggen
NL
Esports
Pickx Esports
Het meest recente nieuws, dossiers, livestreams en exclusieve video's
Films
Entertainment
Series
Sport
Muziek
Nieuws
Esports
Cultuur & kennis
Kids
CS:GO nieuws en video's
Bekijk alles
Keoz: "Meedoen aan de Major in Parijs is het hoofddoel voor 2023"
Deze maand maken we kennis met een van de beste Belgische spelers in de CS:GO-scene. Na...
Nieuws | 1 d geleden
Heroic is te sterk voor FaZe in grote finale van BLAST Fall Final
Na de verloren finale van de IEM Major in Rio heeft Heroic eindelijk haar eerste LAN-titel...
Nieuws | 2 d geleden
NAVI breidt roster uit met speler uit academy team
NAVI heeft de komst van een zesde speler aangekondigd. De 17-jarige nipl, voordien deel...
Nieuws | 5 d geleden
Neymar en zijn ploegmaats spelen CS:GO tijdens WK in Qatar
Het WK voetbal werd zondag op gang getrapt in Qatar. Uiteraard hebben de deelnemers hee...
Nieuws | 7 d geleden
Valve pakt uit met nerfs en nieuwe map in grote update
Valve heeft voor het eerst sinds juni een grote update voor CS:GO uitgebracht. De twee mee...
Nieuws | 21.11.22
Rio Major: Outsiders wint eerste Braziliaanse Major
Outsiders heeft zondagavond de eerste Major in Brazilië gewonnen. Het CIS-roster klopte de...
Nieuws | 14.11.22
Rio Major: Outsiders en Heroic staan in grote finale
Het vonnis van de achttiende CS:GO-Major wordt vanavond geveld. Na razend spannende...
Nieuws | 13.11.22

SuperData: Games grew 12% to $139.9 billion in 2020 amid pandemic



The Cheating Problem

Country	How often, if at all, do you use third-party tools to cheat in multiplayer games online? (Please select the option that best applies)						
	Base: Gamers online who play multiplayer games						
	Net Answer: Always	*Net Answer: Often*	*Net Answer: Sometimes*	*Net Answer: Rarely*	*Net Answer: Never*	*Net Answer: Don't know*	*Net Answer: Prefer not to say*
Global	3%	9%	13%	12%	57%	5%	1%
China	5%	16%	20%	14%	43%	2%	0%
Germany	3%	5%	10%	7%	66%	5%	4%
Japan	3%	11%	10%	6%	59%	10%	0%
South Korea	1%	7%	15%	20%	50%	6%	0%
UK	1%	2%	8%	6%	78%	5%	0%
US	5%	6%	11%	9%	63%	5%	2%

The Cheating Problem

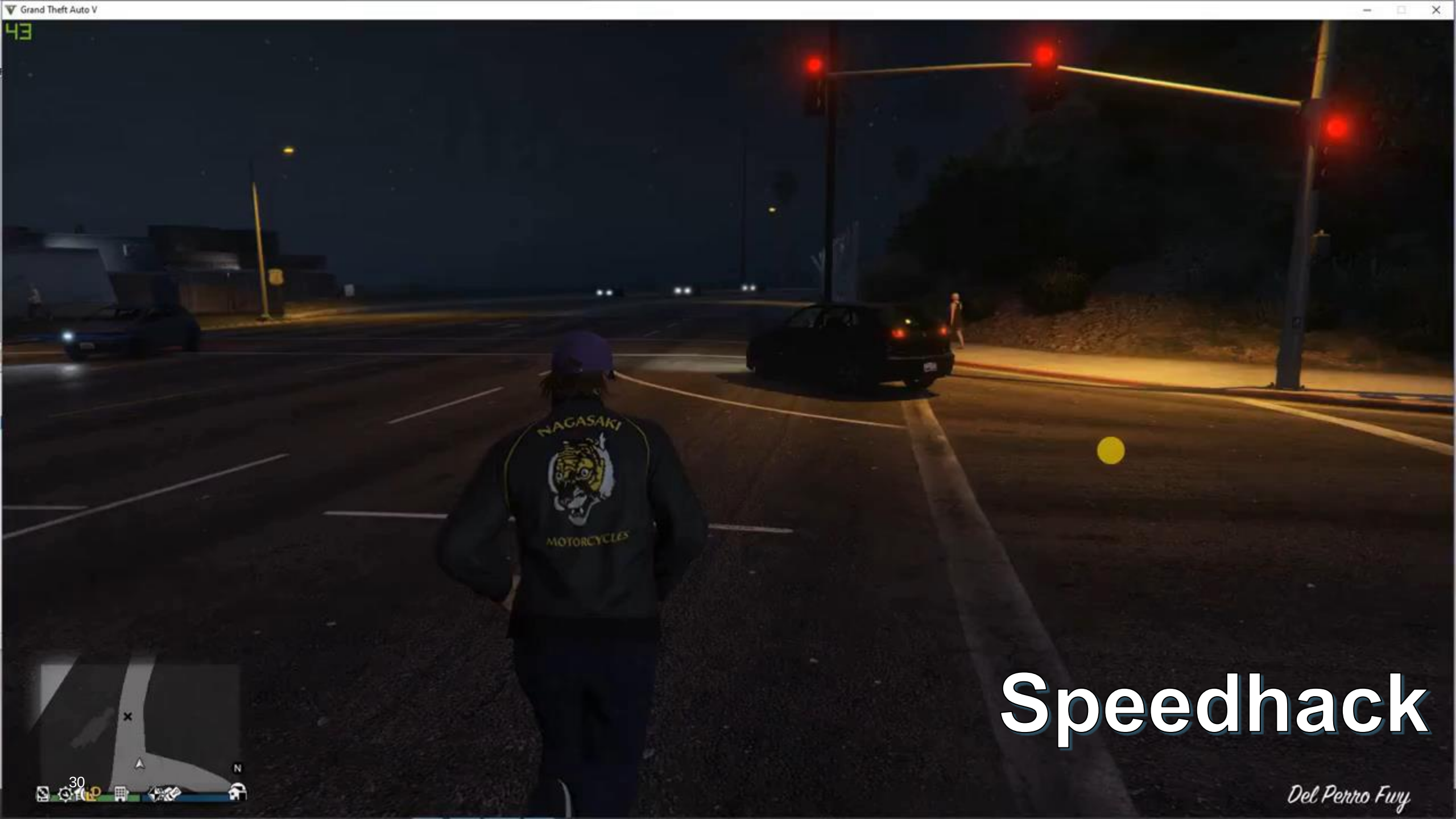

Точка закладки B
1:14
1 0
krutoi.pacan038 on gawd nigga
$4850
klapek maktin MP5-SD
+$300: Награда за нейтрализацию врага.
MEPTB Annulaire : sale fdp
MEPTB why you bully me : burn ur family
100
0
30 / 90
Wallhack

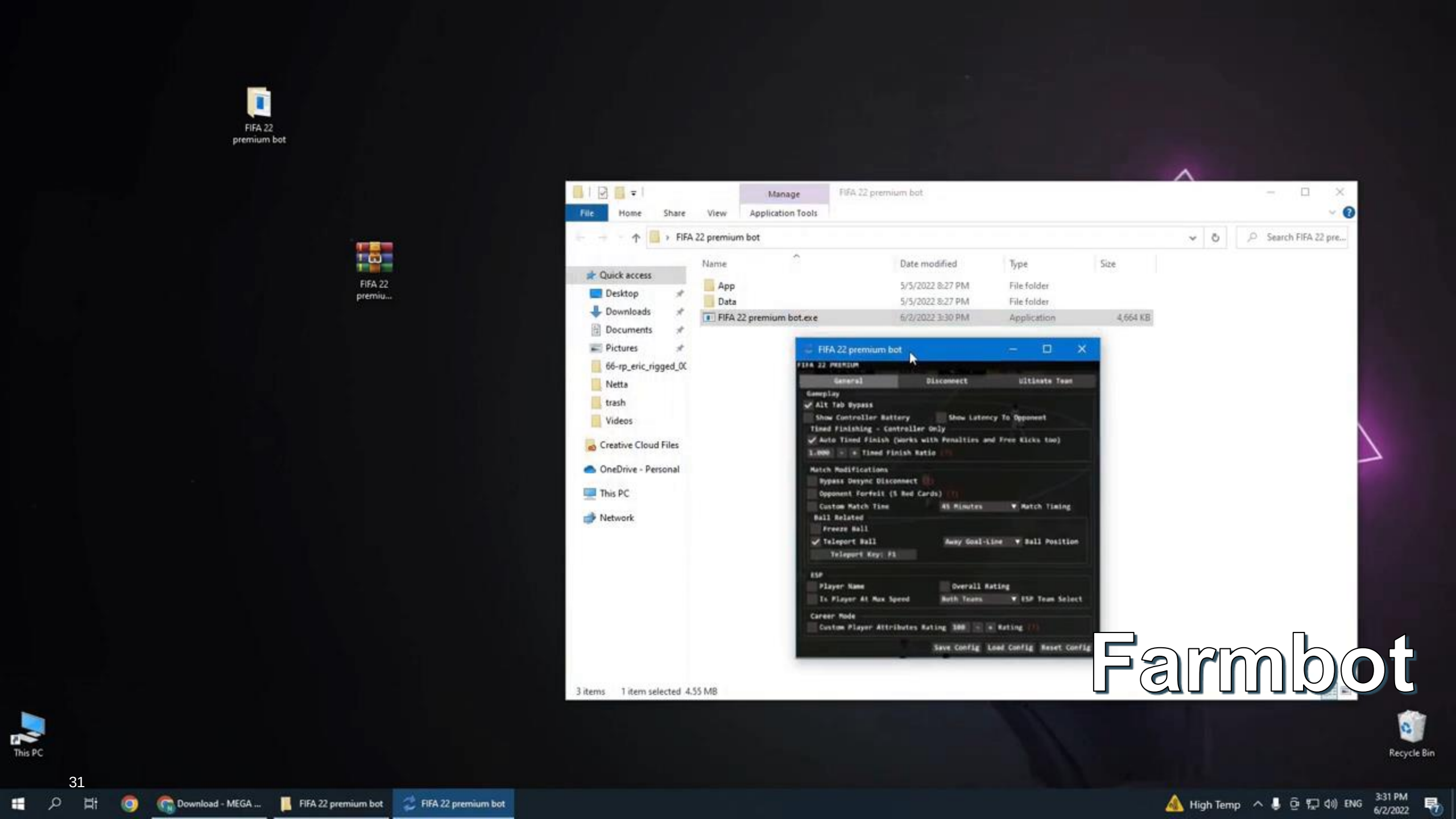

База террористов
A
B
$550
1:55
0 2
Внимание
Вам больше с собой не взять.
• (Террорист) asalamaleykum @ База террористов : domoy v pb nahoy
ХУЯРЬЕБАШЬ @ База террористов
100
100
20 / 90
Aimbot


GUZZLAH
ELIMINATED COLLECTOR 74
Triggerbot
UZZLAH

Triggerbot

Maphack


Grand Theft Auto V
43
NAGASAKI
MOTORCYCLES
30
Del Perro Fwy
Speedhack


FIFA 22 premium bot
FIFA 22 premiu...
Manage
FIFA 22 premium bot
File
Home
Share
View
Application Tools
FIFA 22 premium bot
Search FIFA 22 pre...
Quick access
Desktop
Downloads
Documents
Pictures
66-rp_eric_rigged_0(
Netta
trash
Videos
Creative Cloud Files
OneDrive - Personal
This PC
Network
Name
Date modified
Type
Size
App
5/5/2022 8:27 PM
File folder
Data
5/5/2022 8:27 PM
File folder
FIFA 22 premium bot.exe
6/2/2022 3:30 PM
Application
4,664 KB
3 items
1 item selected 4.55 MB
FIFA 22 premium bot
FIFA 22 PREMIUM
General
Disconnect
Ultimate Team
Gameplay
Alt Tab Bypass
Show Controller Battery
Show Latency To Opponent
Timed Finishing - Controller Only
Auto Timed Finish (Works with Penalties and Free Kicks too)
Timed Finish Ratio
Match Modifications
Bypass Desync Disconnect
Opponent Forfeit (5 Red Cards)
Custom Match Time
45 Minutes
Match Timing
Ball Related
Freeze Ball
Teleport Ball
Away Goal-Line
Ball Position
Teleport Key: F5
ESP
Player Name
Overall Rating
Is Player At Max Speed
Both Teams
ESP Team Select
Career Mode
Custom Player Attributes Rating
Rating
Save Config
Load Config
Reset Config
Farmbot
This PC
Recycle Bin
31
Download - MEGA ...
FIFA 22 premium bot
FIFA 22 premium bot
High Temp
ENG
3:31 PM
6/2/2022

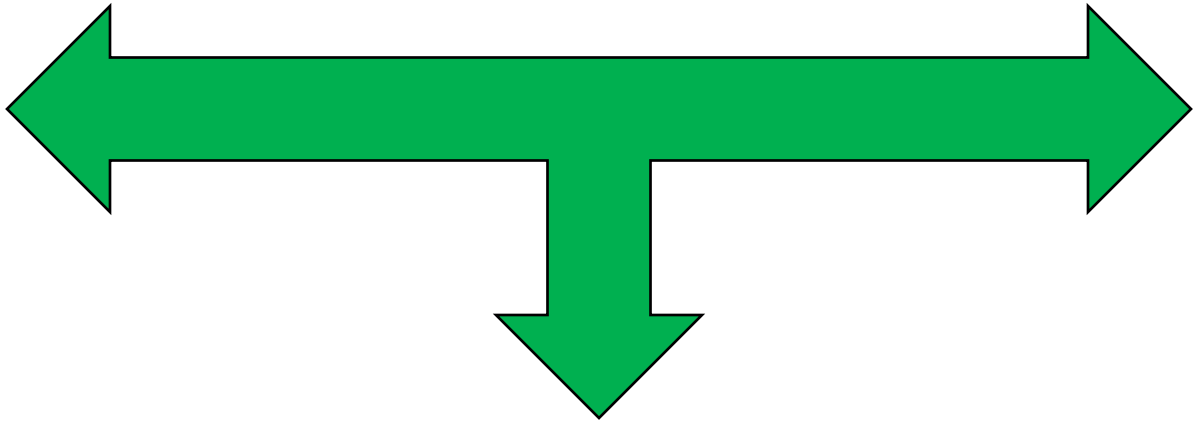

Szec|-| had a Mega Kill!
[AnthChecker] : You have been validated
Szec|-| had an ULTRA KILL!!
Szec|-| had a MONSTER KILL!!
GREAT ALASKA UNREALTOURNAMENT SERVER
Capture the Flag
Map: Untitled
Author:
Spawnkill
SPAWN KILLERS BAN
ASSHOLES BAN
Szec|-| is on a killing spree!
MONSTER KILL!!
SUCKS

Massmurder

Types of Cheats

Knowledge Assistance
Reveal information that is not available to legitimate players

Examples
Wallhacks
Radars
Maphacks



Abusing Game Bugs
Allows you to circumvent the game rules

Examples
Gold Hacks
Item Duplication Hacks

Mechanical Assistance
Enhance your capabilities or automate the game

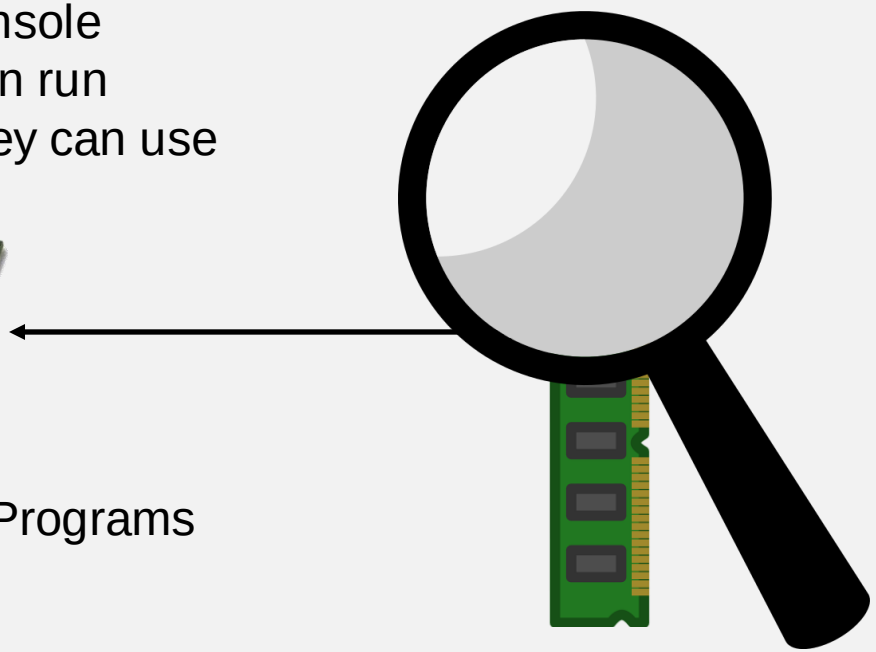
Examples
Aimbots
Triggerbots
Farmbots
Speedhacks

Background: Anatomy of a Computer Game

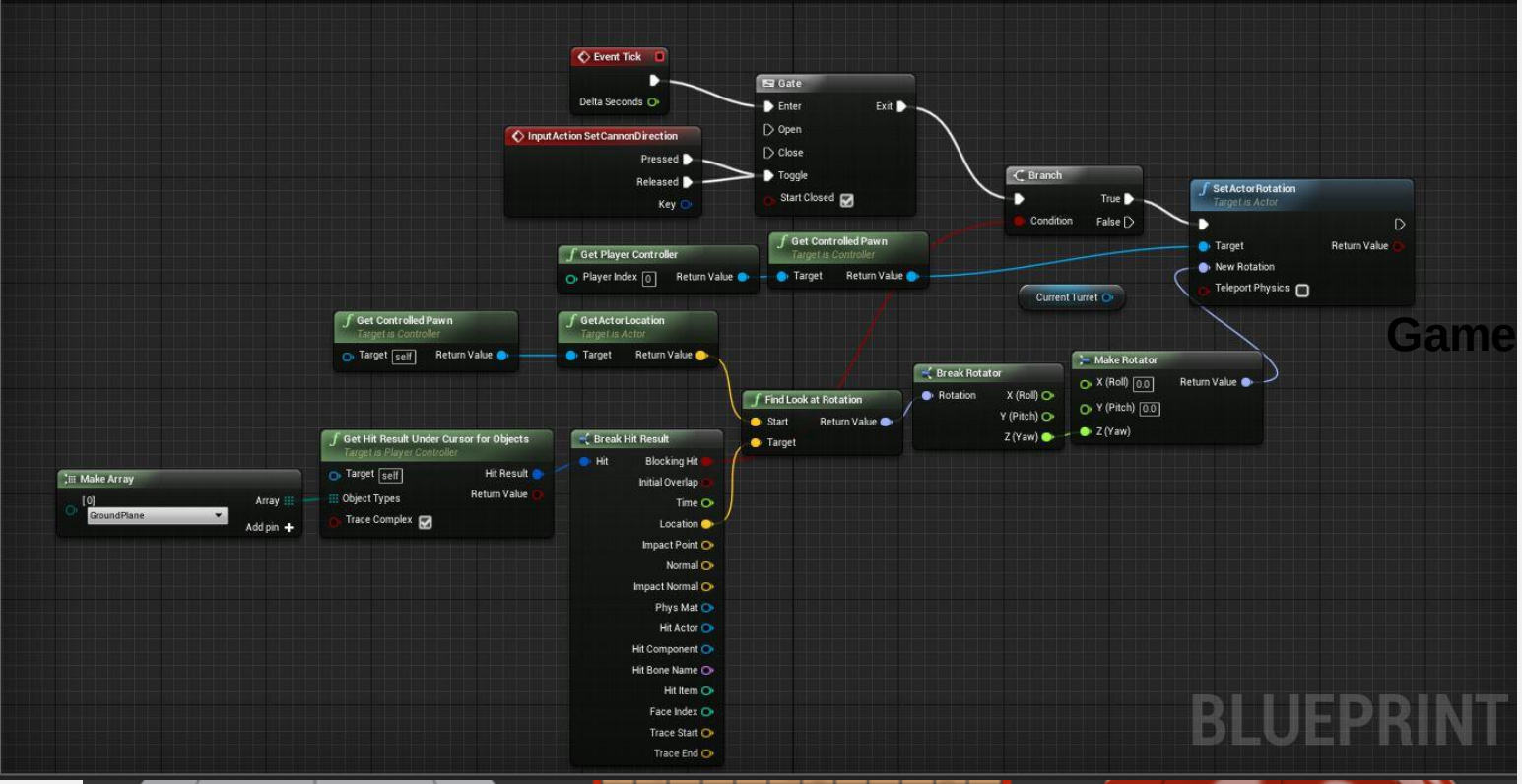
Hard Drive: Long-term Storage of Programs and Data

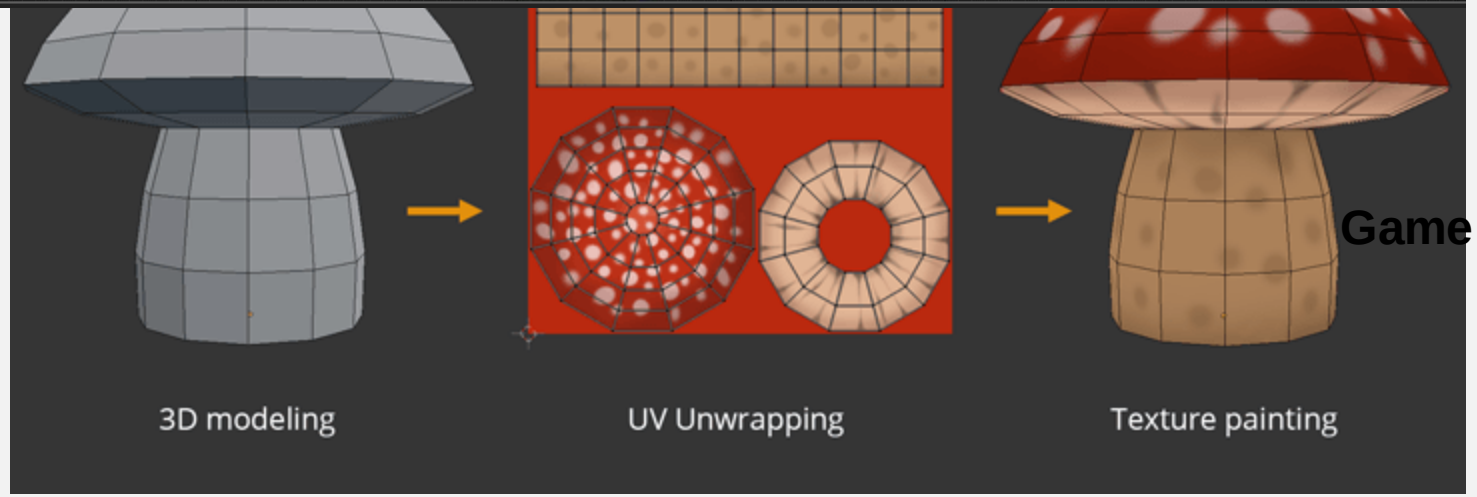
Operating System:
- Manages the Computer/Console
- Decides which programs can run
- Decides which hardware they can use

Processor: Executes Programs



RAM Memory: Stores Program Instructions and Data **while** they execute





Game Assets

- Data
- Sound
- Music
- 3D Meshes
- Textures + Texture Maps
- Scripts
- Game State

Game Engine

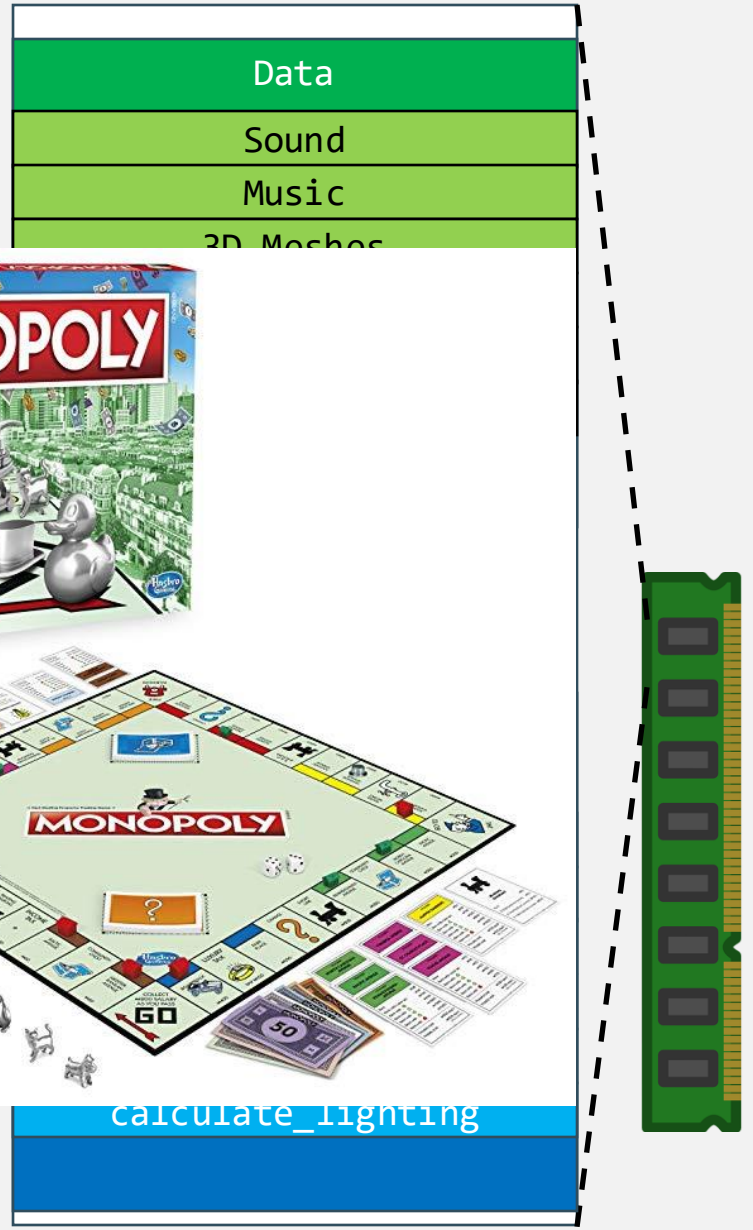
- Executable (machine) code
- read_input
- render_frame
- send_data
- play_sound
- play_music
- calculate_lighting

Background: Anatomy of a Computer Game

Game State = all **data** that describes the **current state of the game**

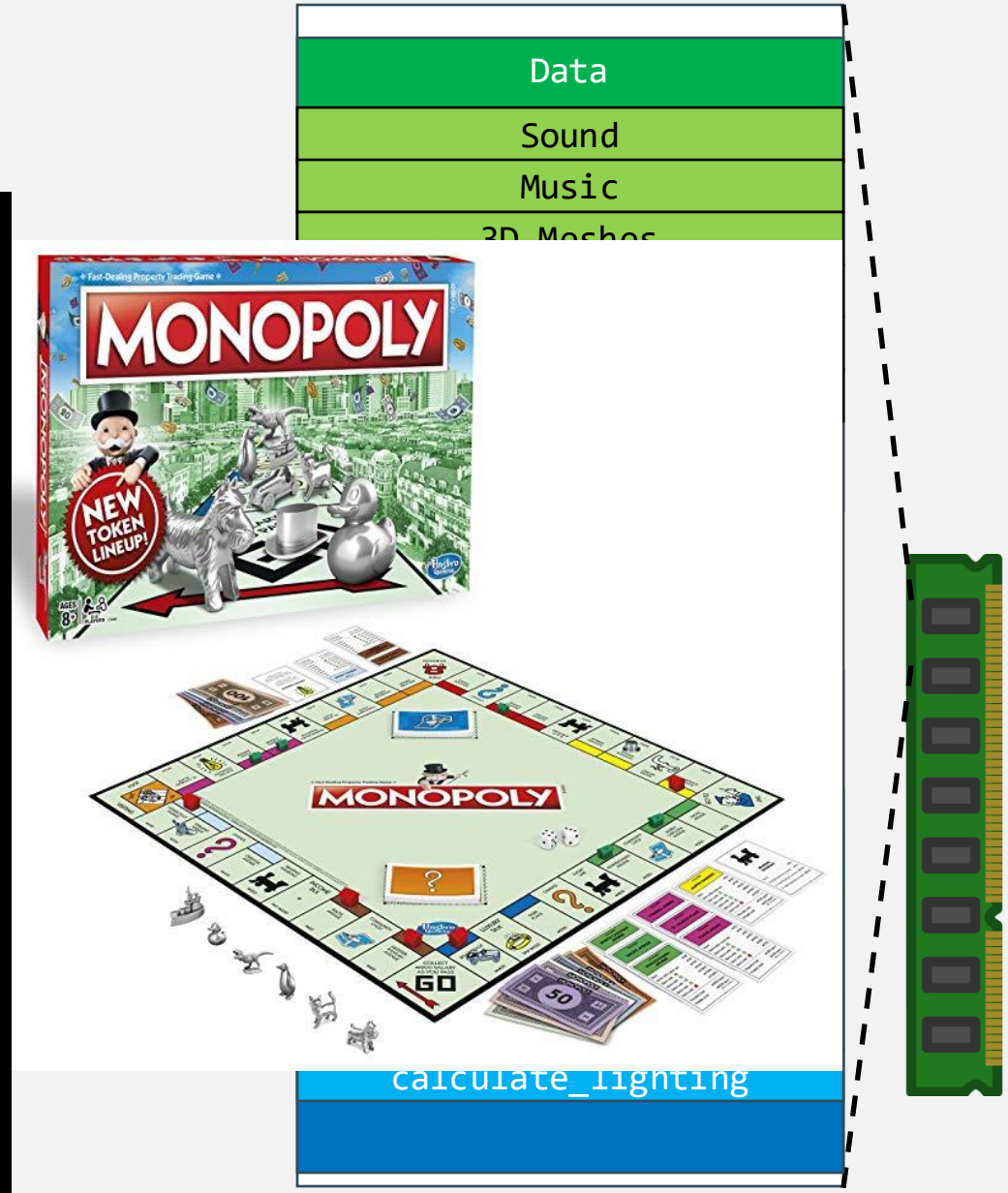
Example:

- In **monopoly:** state =
  - names of each player
  - token for each player
  - how much money each player has
  - which properties each player owns
  - whose turn it is



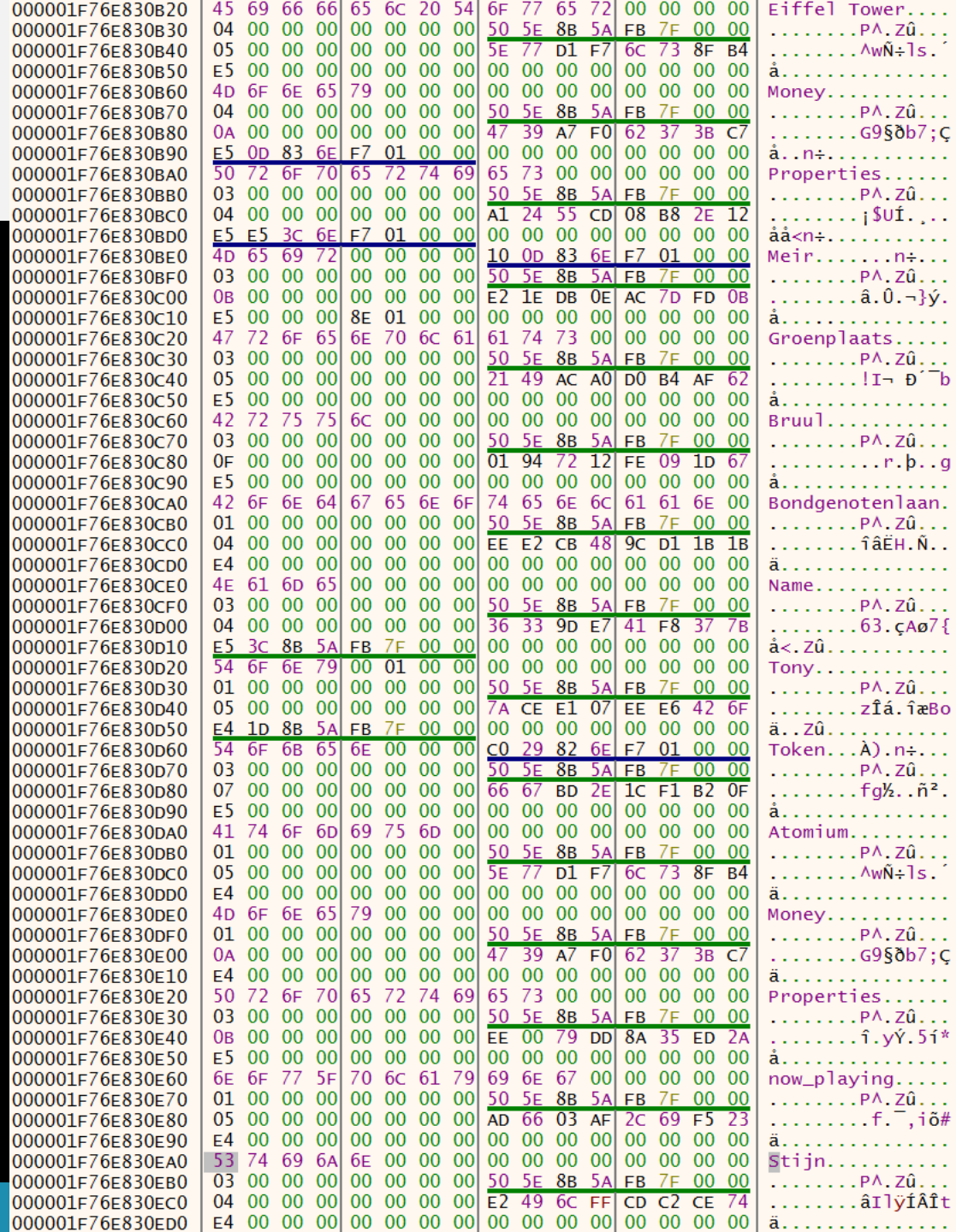
Background: Anatomy of a Computer Game

```
state = {
    "players" : [
        {
            'Name': 'Stijn',
            'Token': 'Eiffel Tower',
            'Money': 5000000,
            'Properties': ["Veldstraat", "Meir",
                           "Groenplaats", "Bruul",
                           "Bondgenotenlaan"],
        },
        {
            'Name': 'Tony',
            'Token': 'Atomium',
            'Money': 10,
            'Properties': ["Lange Zoutstraat"],
        }
    ],
    "now_playing" : "Stijn"
}
```



Background: Anatomy of a Computer Game

```
state = {
    "players" : [
        {
            'Name': 'Stijn',
            'Token': 'Eiffel Tower',
            'Money': 5000000,
            'Properties': ["Veldstraat", "Meir",
                           "Groenplaats", "Bruul",
                           "Bondgenotenlaan"],
        },
        {
            'Name': 'Tony',
            'Token': 'Atomium',
            'Money': 10,
            'Properties': ["Lange Zoutstraat"],
        }
    ],
    "now_playing" : "Stijn"
}
```



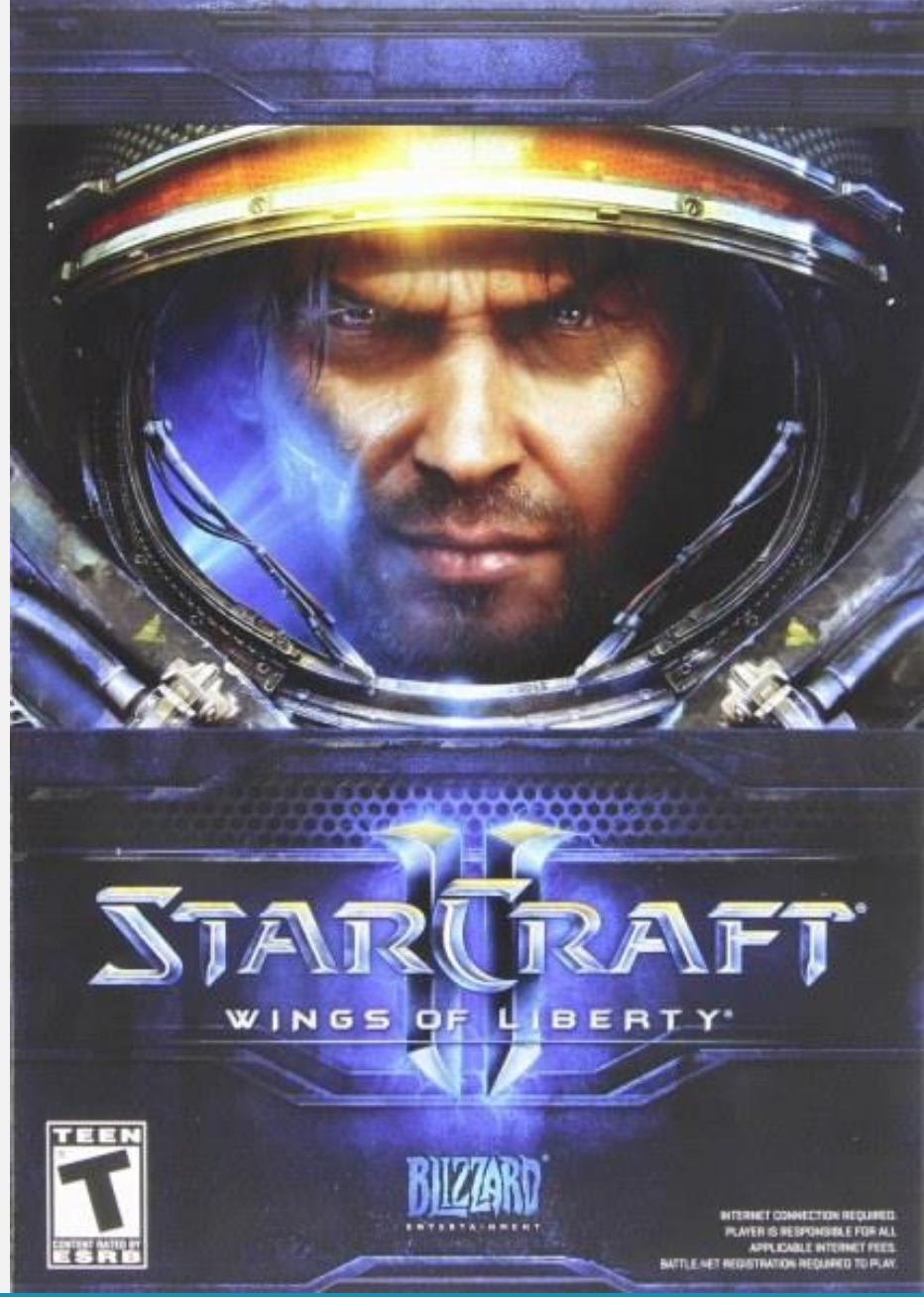
Background: Anatomy of a Computer Game

Game State = all **data** that describes the **current state of the game**

Example:

- In **real-time strategy games**, the state includes:
  - Which parts of the map are visible
  - …

```
map_fog_of_war_state = [
    [1, 1, 0, 0, 0],
    [1, 1, 0, 0, 0],
    [0, 0, 0, 0, 0],
    [0, 0, 0, 0, 0],
    [0, 0, 0, 0, 0],
]
```



Background: Anatomy of a Computer Game

Game State = all **data** that describes the **current state of the game**

Example:

- In shooter games, the state includes:
  - Names, positions, velocity, acceleration, hit points, experience, … of all moving objects
  - IP addresses of all players
  - State of the level
  - And **much much more**

Why is Cheating Possible?

Core Problems:

1. **Operating Systems let you do pretty much anything on your own computer**
2. Most of the game state is available in your RAM memory at any given time
3. Finding and tampering with relevant game state is easier than you would think
4. Cheating is a lucrative business

If You Own the Machine, You Can Do Anything

Typical **features** supported by **all mainstream operating systems:**

- Reading or overwriting programs or data stored on the hard drive
- Reading or overwriting program instructions or data stored in your RAM memory
- Starting, stopping, pausing programs that are currently running
- Drawing over the window of a running program
- Sending keystrokes, mouse clicks, or mouse movement to a running program

Operating System:
- Manages the Computer/Console
- Decides which programs can run
- Decides which hardware they can use

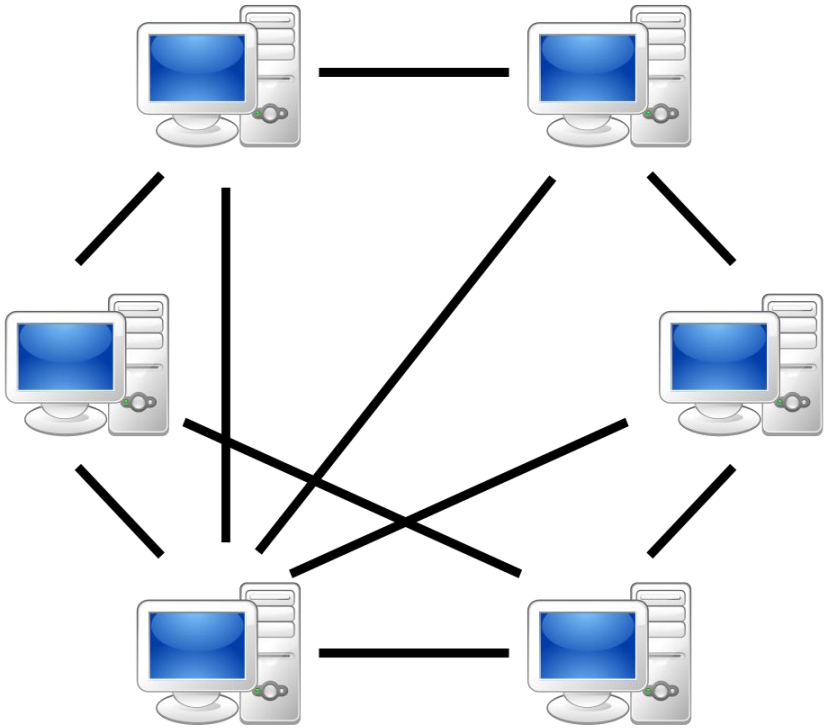
Why is Cheating Possible?

Core Problems:

1. Operating Systems let you do pretty much anything on your own computer
2. **Most of the game state is available in your RAM memory at any given time**
3. Finding and tampering with relevant game state is easier than you would think
4. Cheating is a lucrative business

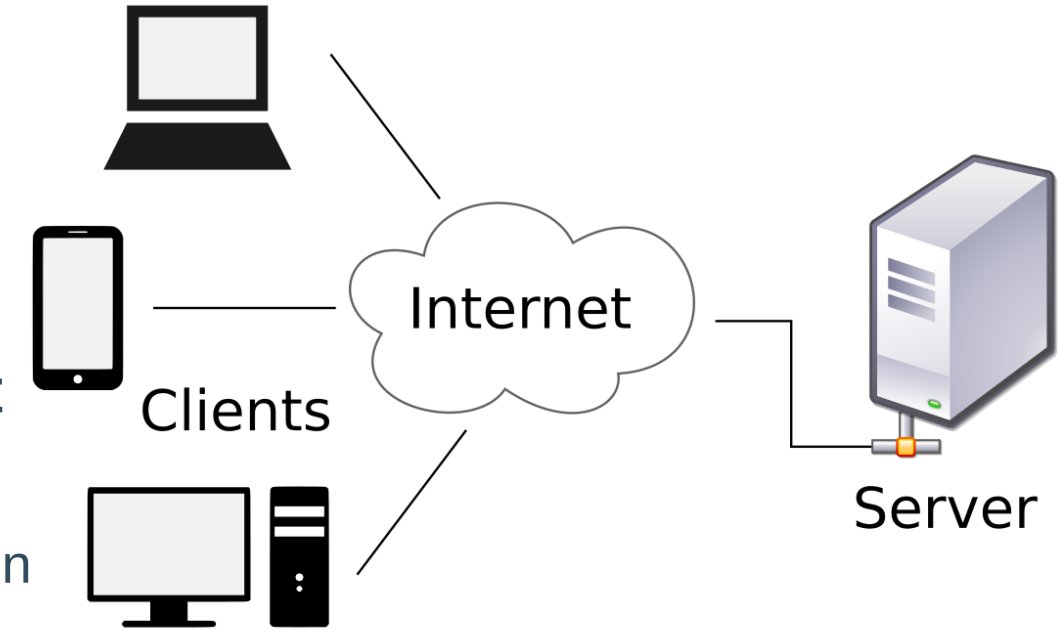
Why is Cheating Possible?

- **Core problem:** Most of the game state is available in your RAM memory at any given time
- **Peer-to-peer** games
  - No central authority
  - Used to be the dominant architecture, still common in RTS games
  - Every client has a full copy of the game state
  - At the end of every "frame", clients publish updates to game state
  - Hard to check legitimacy of updates and to keep irrelevant state private



Why is Cheating Possible?

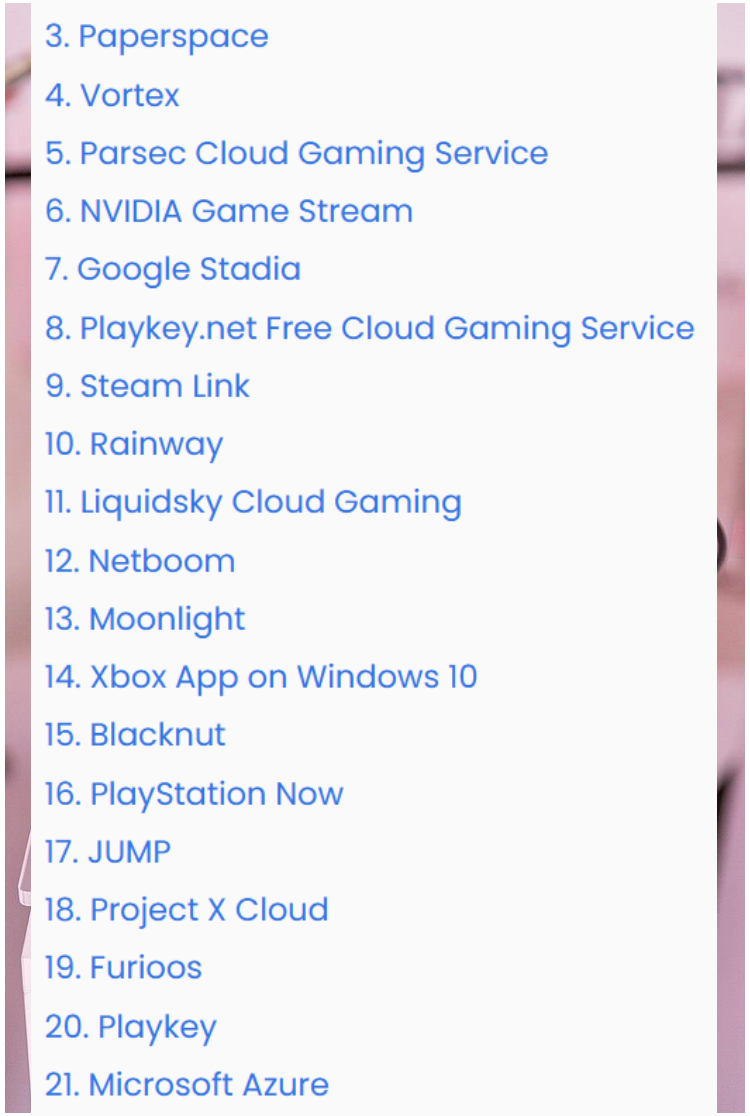
- **Client-server** games
  - Only the central server sees the full game state
  - Clients see only state that is relevant to them
  - **Problem:** calculating relevancy is **difficult**
  - Examples:
    - a player might **not** be visible, but might still be in audible range
    - a player might become visible very soon




FUEL STORAGE
WP-G

Why is Cheating Possible?

- **Cloud games**/game streaming
  - Ideally, game state is only stored in the cloud
  - Clients send inputs and receive rendered images
  - Unclear if this will ever be viable for first-person shooter games



24 Best Cloud Gaming Services of 2023:

1. GeForce Now
2. Shadow Cloud Gaming Service
3. Paperspace
4. Vortex
5. Parsec Cloud Gaming Service
6. NVIDIA Game Stream
7. Google Stadia
8. Playkey.net Free Cloud Gaming Service
9. Steam Link
10. Rainway
11. Liquidsky Cloud Gaming
12. Netboom
13. Moonlight
14. Xbox App on Windows 10
15. Blacknut
16. PlayStation Now
17. JUMP
18. Project X Cloud
19. Furioos
20. Playkey
21. Microsoft Azure
22. Project Xcloud
23. HP Omen Game Stream
24. Amazon Luna

Why is Cheating Possible?

Core Problems:

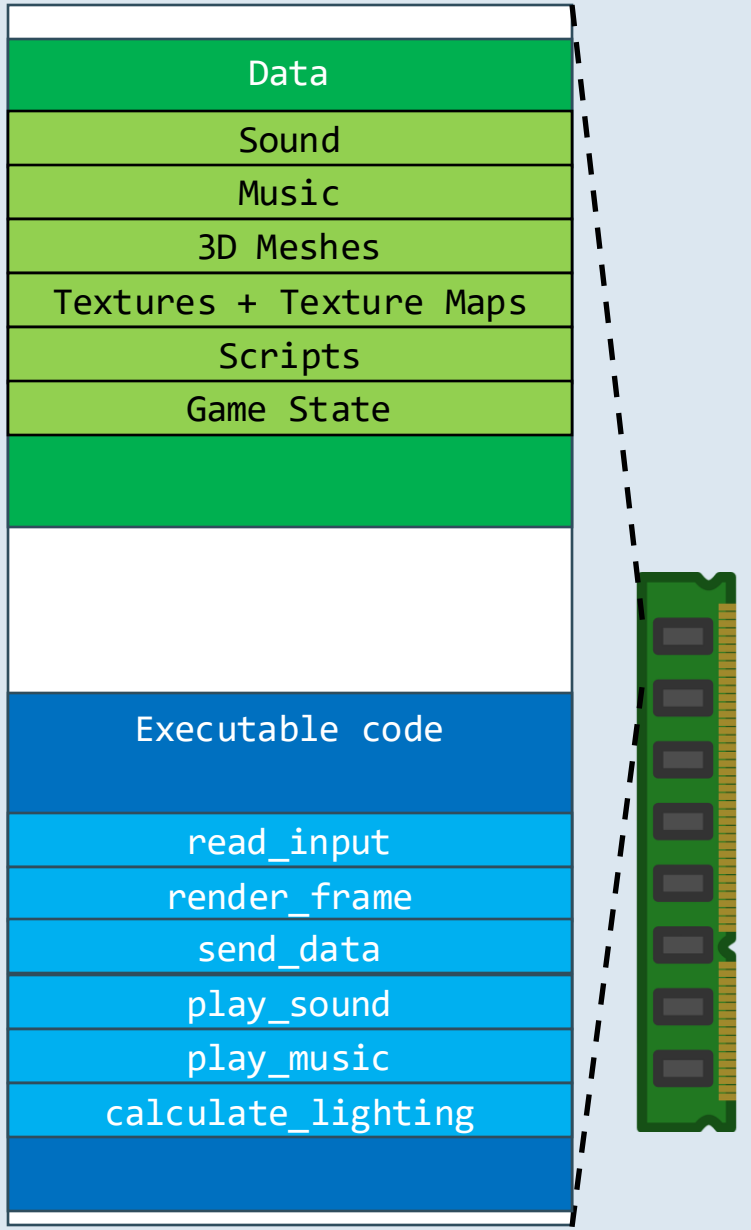
1. Operating Systems let you do pretty much anything on your own computer
2. Most of the game state is available in your RAM memory at any given time
3. **Finding and tampering with relevant game state is easier than you would think**
4. Cheating is a lucrative business

Cheating: Core Techniques

Cheat	Goal	Techniques
Wallhack Radar Maphack	Reveal hidden game state	Data exfiltration Overlay rendering API hooking

Background: Why is Data Exfiltration even possible?

- All modern operating systems enforce strict isolation between programs
- One program cannot read another program's memory
- This is possible because of the **Memory Management Unit** inside your CPU



But wait…

VirtualProtectEx function

12/05/2018 • 2 minutes to read

WriteProcessMemory function

12/05/2018 • 2 minutes to read

Writes d

ReadProcessMemory function

08/05/2019 • 2 minutes to read

Syntax

C++

```
BOOL ReadProcessMemory(
  HANDLE  hProcess,
  LPCVOID lpBaseAddress,
  LPVOID  lpBuffer,
  SIZE_T  nSize,
  SIZE_T  *lpNumberOfBytesRead
);
```

Parameters

`hProcess`

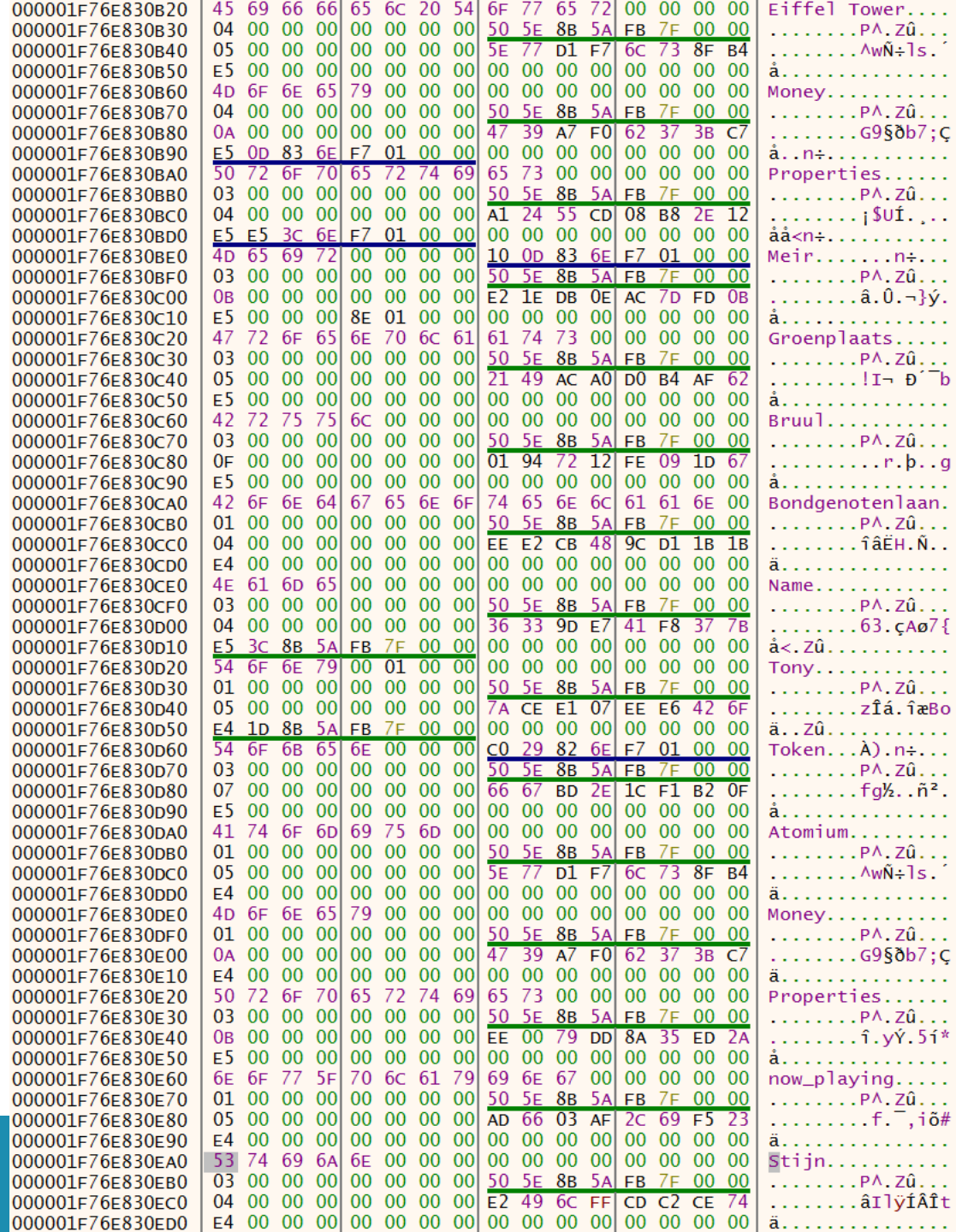
A handle to the process with memory that is being read. The handle must have PROCESS_VM_READ access to the process.

`lpBaseAddress`

A pointer to the base address in the specified process from which to read. Before any data transfer occurs, the system verifies that all data in the base address and memory of the specified size is accessible for read access, and if it is not accessible the function fails.

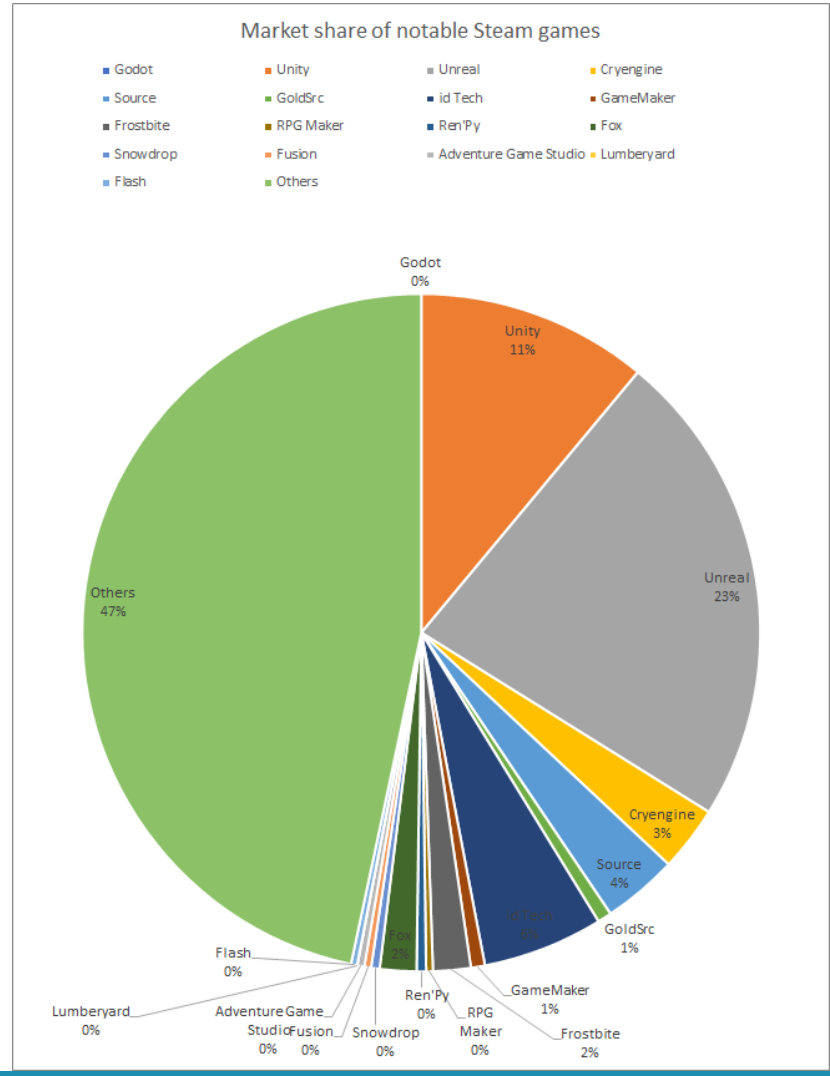
Data Exfiltration: What to Read?

- Now that we know **HOW** to read the game state, we need to know **WHERE** the game state is
- This is not that easy because the raw data has no obvious structure
- Searching for strings is still possible (with the right tools), but how do you find the rest of the game state?

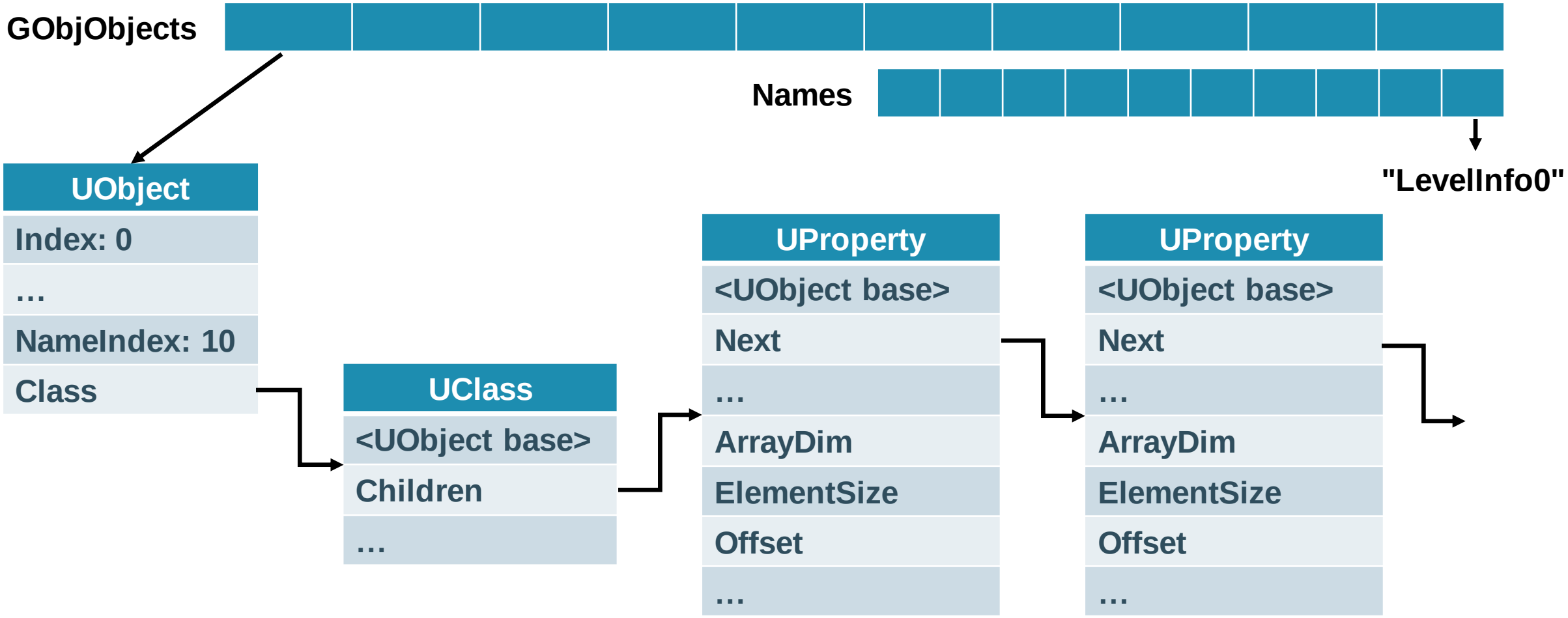


Data Exfiltration: What to Read?

- Luckily, there is much more structure than you would think
- There are only a handful of game engines people use to create AAA games
- If you know which engine the game uses, it is pretty easy to figure out how the game state is structured



Data Exfiltration: What to Read?



Data Exfiltration: What to Read?

- There are automated tools that can dump the blueprint from a running game
- Minimal effort, you only really need to find the GObjObjects array
- A trained reverse engineer can do this in less than 5 minutes

[*] https://github.com/polivilas/UnrealEngineSDKGenerator

Data Exfiltration: What to Read?

- In some cases, you don't even need a blueprint to cheat
- Having a clever tool that can search through raw data is often sufficient
- Luckily, there are plenty of clever tools available
- Example: **Cheat Engine**

File Edit View History Bookmarks Tools Help

Mr.NAMIK4ZE - YouTube

https://www.youtube.com/channel/UCMaYLz8DzE105gzuNTLsjnA

Search

YouTube ID

Telusuri

Login

Beranda
Trending
Histori

TERBAIK DARI YOUTUBE

Musik
Olahraga
Game
Berita
Live
Video 360°

Jelajahi channel

Login sekarang untuk melihat channel dan rekomendasi!

Login

Mr.NAMIK4ZE

Beranda Video Playlist Channel Diskusi Te

Intro

0:00 / 0:27

Upload

Cheat Global Strike Hack GOLD with Cheat

Cheat Shadowgun: Deadzone Hack v.

Farm Frenzy: Pizza Party

100 1000 10000 50000 2600 2500

100

Level goals
Best time:
00:26

Collect

2

For completing:

20

01:00 +30

02:00 +10

OK

Menu

0
2
00:00 01:00

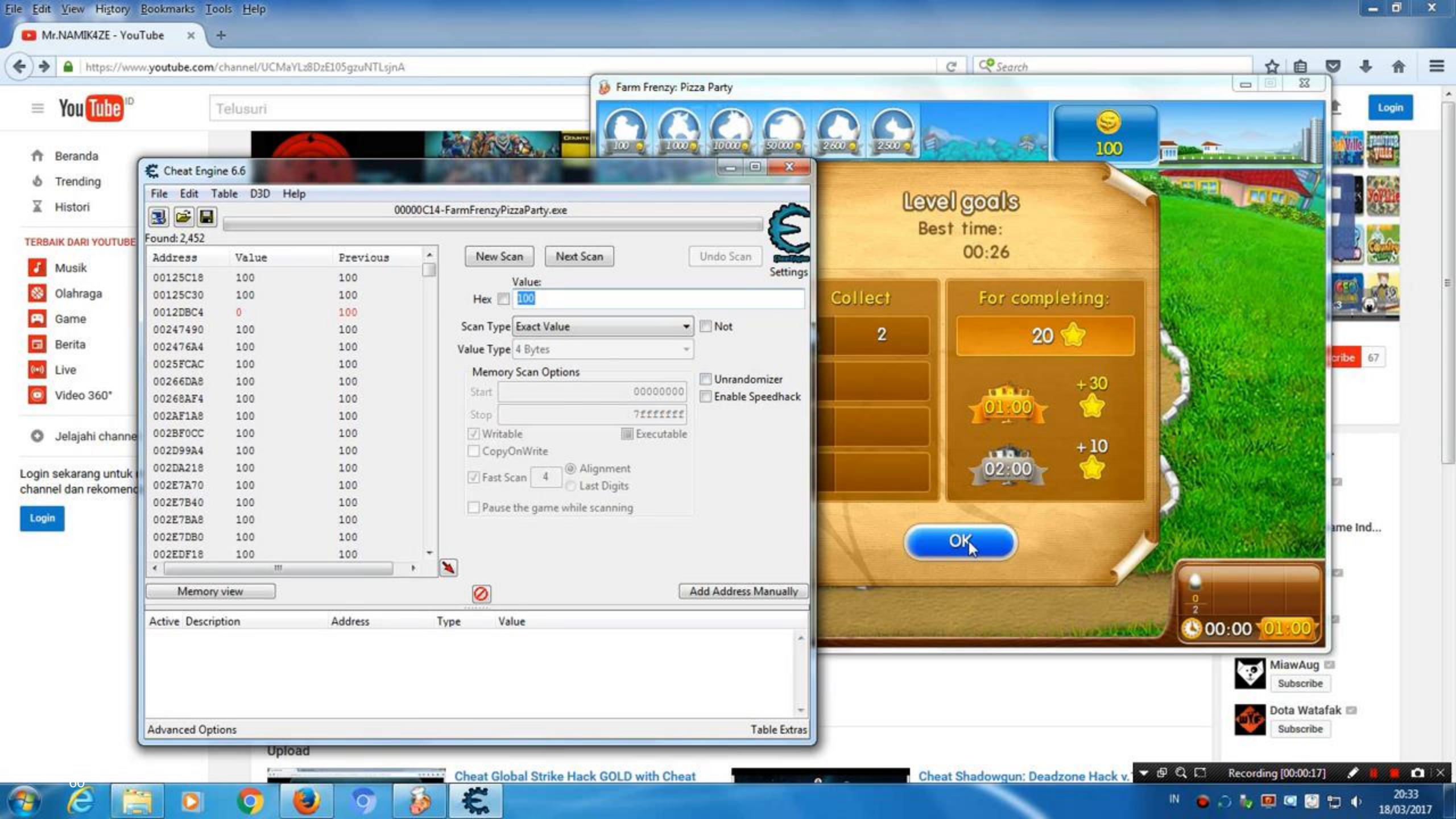
MiawAug
Subscribe

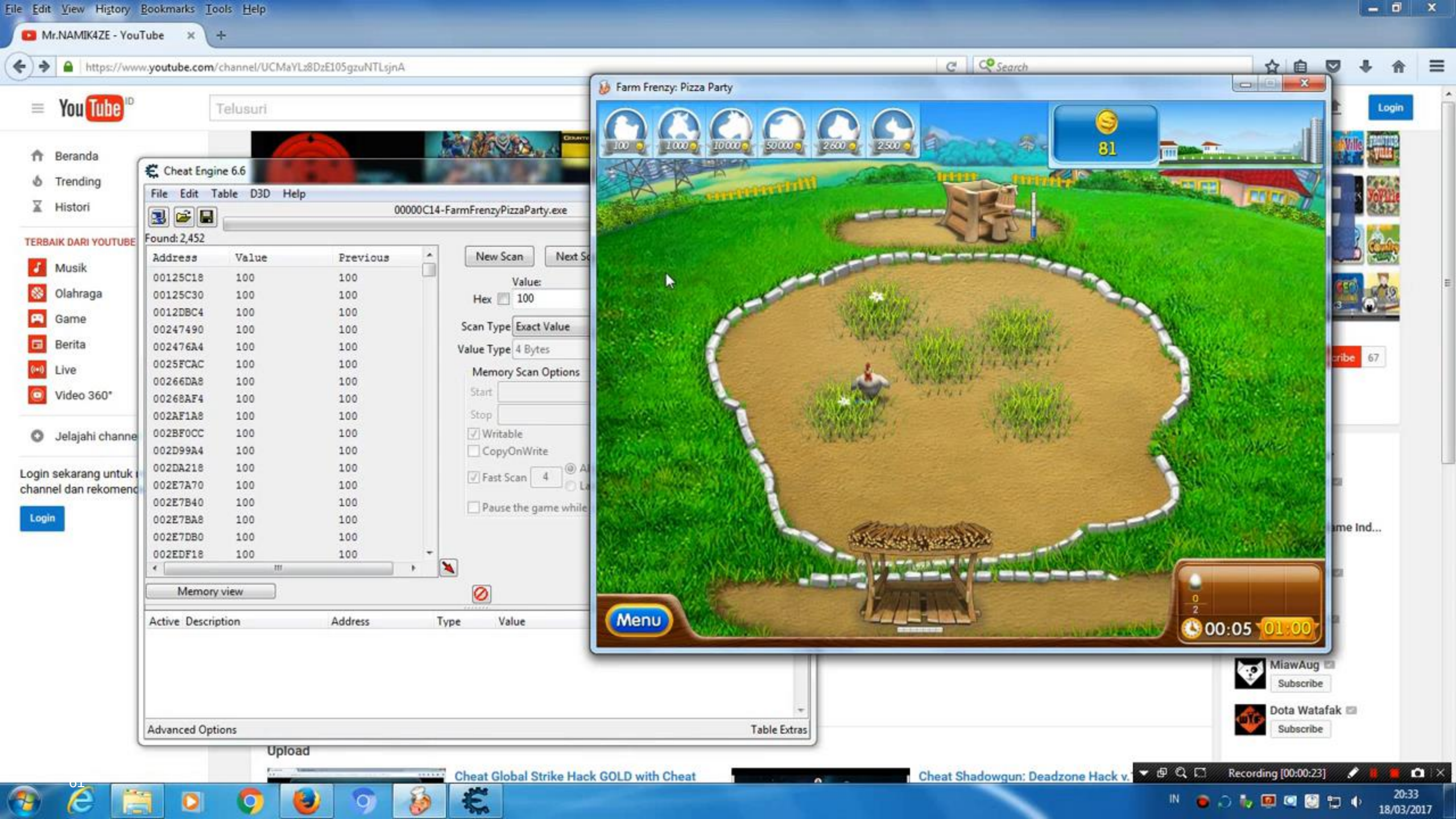
Dota Watafak
Subscribe

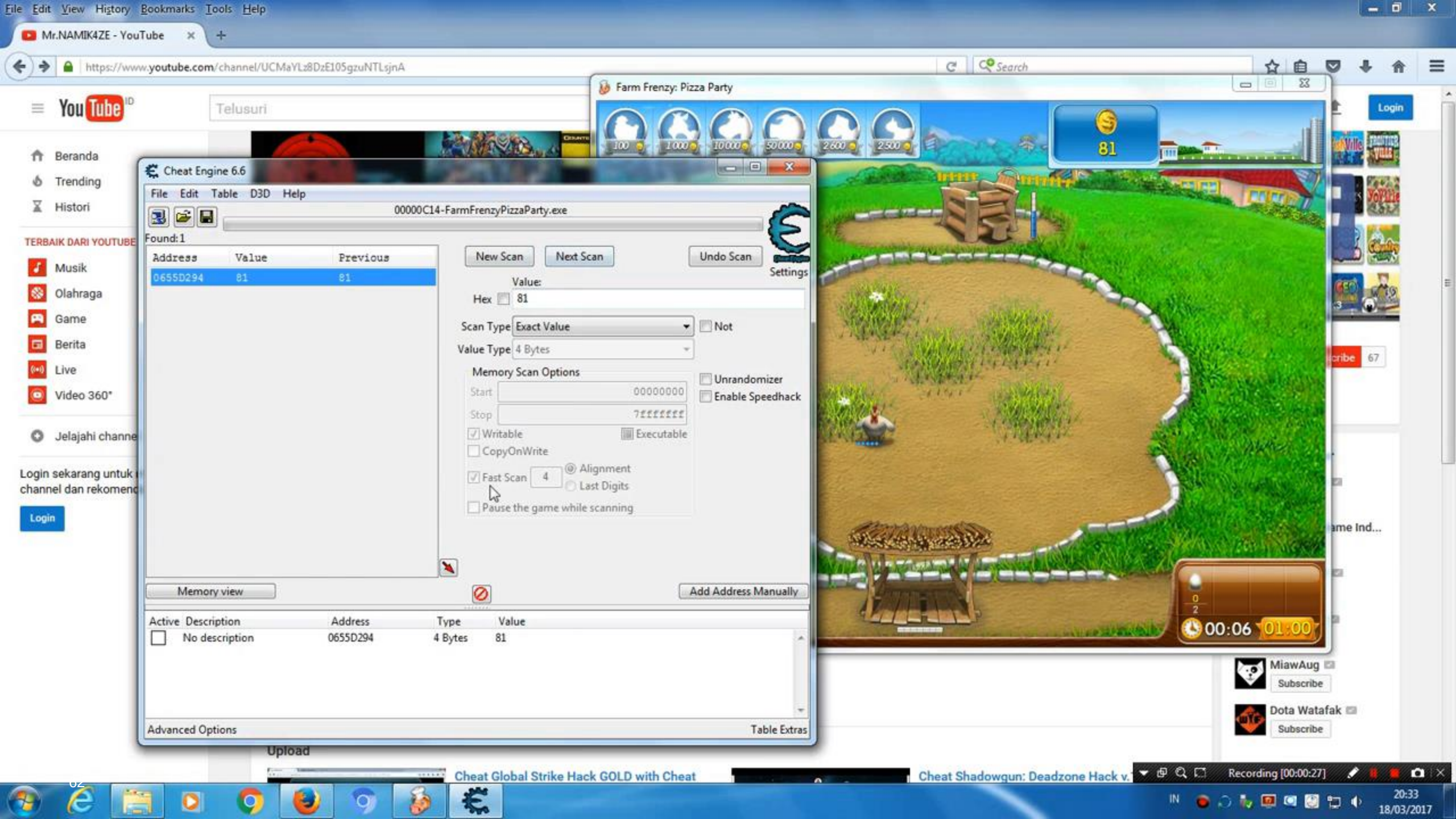
Recording

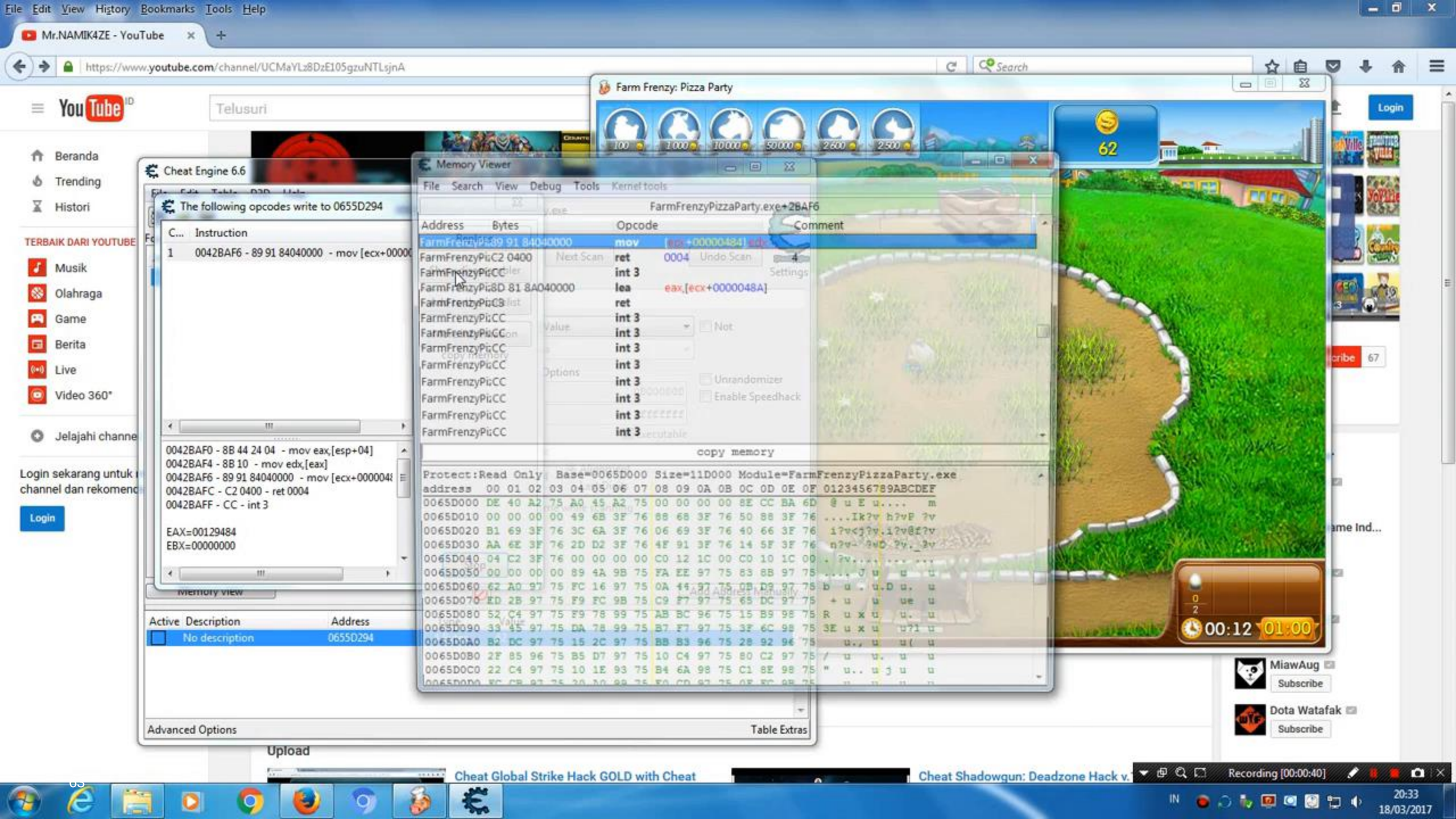
IN

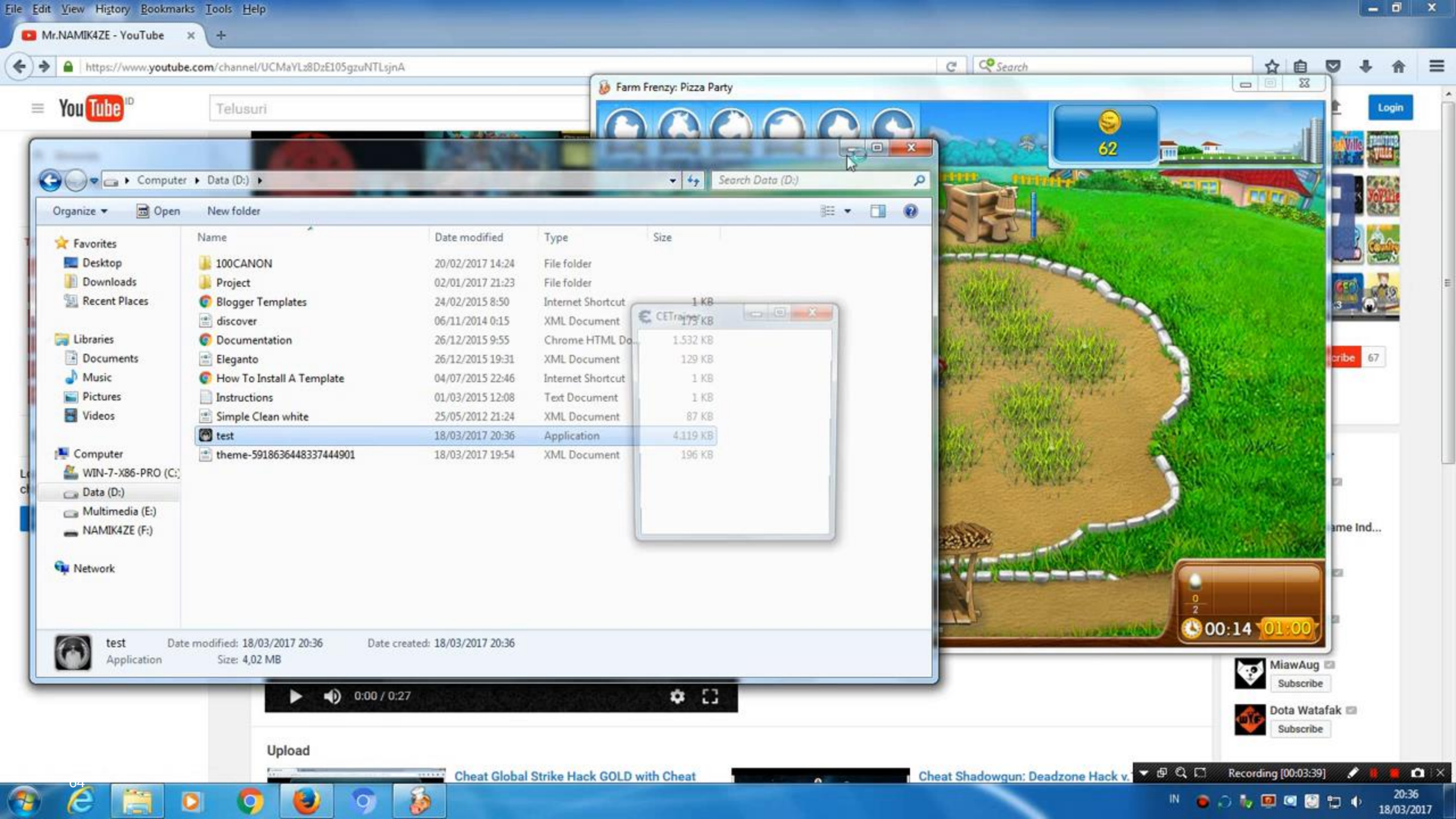
20:33
18/03/2017


Mr.NAMIK4ZE - YouTube
https://www.youtube.com/channel/UCMaYLz8DzE105gzuNTLsjnA
Telusuri
Login
Beranda
Trending
Histori
TERBAIK DARI YOUTUBE
Musik
Olahraga
Game
Berita
Live
Video 360°
Jelajahi channe
Login sekarang untuk
channel dan rekomend
Login
Upload
Cheat Global Strike Hack GOLD with Cheat
Cheat Shadowgun: Deadzone Hack v.
MiawAug
Subscribe
Dota Watafak
Subscribe
Farm Frenzy: Pizza Party
100
Level goals
Best time:
00:26
Collect
2
For completing:
20
+30
01:00
+10
02:00
OK
00:00
01:00
Cheat Engine 6.6
File Edit Table D3D Help
00000C14-FarmFrenzyPizzaParty.exe
Found: 2,452
Address Value Previous
00125C18 100 100
00125C30 100 100
0012DBC4 0 100
00247490 100 100
002476A4 100 100
0025FCAC 100 100
00266DA8 100 100
00268AF4 100 100
002AF1A8 100 100
002BF0CC 100 100
002D99A4 100 100
002DA218 100 100
002E7A70 100 100
002E7B40 100 100
002E7BA8 100 100
002E7DB0 100 100
002EDF18 100 100
New Scan
Next Scan
Undo Scan
Settings
Value:
Hex
100
Scan Type Exact Value
Not
Value Type 4 Bytes
Memory Scan Options
Start 00000000
Stop 7fffffff
Writable
Executable
CopyOnWrite
Fast Scan 4
Alignment
Last Digits
Pause the game while scanning
Unrandomizer
Enable Speedhack
Memory view
Add Address Manually
Active Description Address Type Value
Advanced Options
Table Extras
Recording [00:00:17]
IN
20:33
18/03/2017


File Edit View History Bookmarks Tools Help
Mr.NAMIK4ZE - YouTube
https://www.youtube.com/channel/UCMaYLz8DzE105gzuNTLsjnA
Search
YouTube ID
Telusuri
Login
Beranda
Trending
Histori
TERBAIK DARI YOUTUBE
Musik
Olahraga
Game
Berita
Live
Video 360°
Jelajahi channe
Login sekarang untuk
channel dan rekomend
Login
Cheat Engine 6.6
File Edit Table D3D Help
00000C14-FarmFrenzyPizzaParty.exe
Found: 2,452
Address Value Previous
00125C18 100 100
00125C30 100 100
0012DBC4 100 100
00247490 100 100
002476A4 100 100
0025FCAC 100 100
00266DA8 100 100
00268AF4 100 100
002AF1A8 100 100
002BF0CC 100 100
002D99A4 100 100
002DA218 100 100
002E7A70 100 100
002E7B40 100 100
002E7BA8 100 100
002E7DB0 100 100
002EDF18 100 100
New Scan
Next Sc
Value:
Hex 100
Scan Type Exact Value
Value Type 4 Bytes
Memory Scan Options
Start
Stop
Writable
CopyOnWrite
Fast Scan 4
Pause the game while
Memory view
Active Description Address Type Value
Advanced Options
Table Extras
Farm Frenzy: Pizza Party
100 1000 10000 50000 2600 2500
81
Menu
00:05 01:00
Upload
Cheat Global Strike Hack GOLD with Cheat
Cheat Shadowgun: Deadzone Hack v.
MiawAug
Subscribe
Dota Watafak
Subscribe
Recording [00:00:23]
IN
20:33
18/03/2017

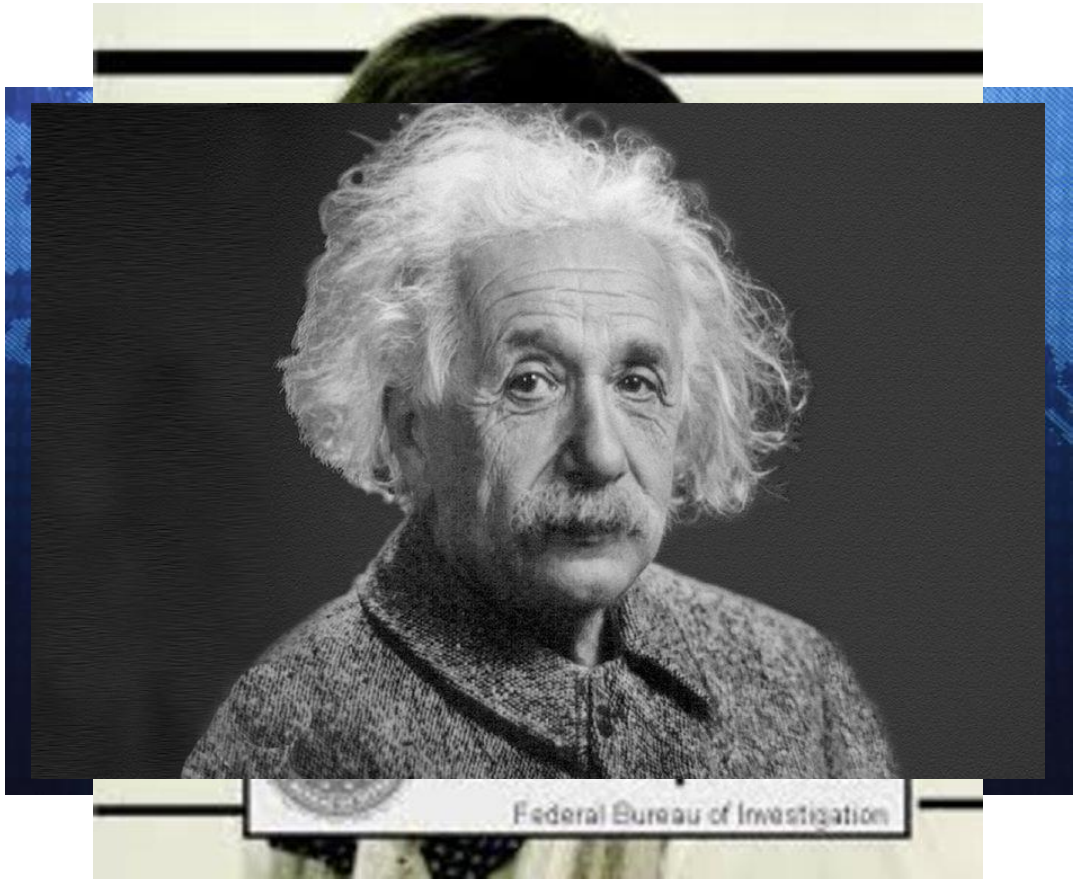

Mr.NAMIK4ZE - YouTube
https://www.youtube.com/channel/UCMaYLz8DzE105gzuNTLsjnA
Farm Frenzy: Pizza Party
81
Cheat Engine 6.6
00000C14-FarmFrenzyPizzaParty.exe
Found:1
Address Value Previous
0655D294 81 81
New Scan
Next Scan
Undo Scan
Settings
Value:
Hex 81
Scan Type Exact Value
Not
Value Type 4 Bytes
Memory Scan Options
Start 00000000
Stop 7fffffff
Writable
Executable
CopyOnWrite
Fast Scan 4
Alignment
Last Digits
Pause the game while scanning
Unrandomizer
Enable Speedhack
Memory view
Add Address Manually
Active Description Address Type Value
No description 0655D294 4 Bytes 81
Advanced Options
Table Extras
00:06 01:00
Upload
Cheat Global Strike Hack GOLD with Cheat
Cheat Shadowgun: Deadzone Hack v.
MiawAug
Subscribe
Dota Watafak
Subscribe
Recording [00:00:27]
20:33
18/03/2017


Mr.NAMIK4ZE - YouTube
https://www.youtube.com/channel/UCMaYLz8DzE105gzuNTLsjnA
Farm Frenzy: Pizza Party
Cheat Engine 6.6
The following opcodes write to 0655D294
0042BAF6 - 89 91 84040000 - mov [ecx+00000484],edx
Memory Viewer
FarmFrenzyPizzaParty.exe+2BAF6
Address Bytes Opcode Comment
mov [ecx+00000484],edx
ret 0004
int 3
lea eax,[ecx+0000048A]
ret
copy memory
0042BAF0 - 8B 44 24 04 - mov eax,[esp+04]
0042BAF4 - 8B 10 - mov edx,[eax]
0042BAF6 - 89 91 84040000 - mov [ecx+00000484],edx
0042BAFC - C2 0400 - ret 0004
0042BAFF - CC - int 3
EAX=00129484
EBX=00000000
Active Description Address
No description 0655D294
Advanced Options
Table Extras
Upload
Cheat Global Strike Hack GOLD with Cheat
Cheat Shadowgun: Deadzone Hack v.
MiawAug
Subscribe
Dota Watafak
Subscribe
Recording [00:00:40]
20:33
18/03/2017


File Edit View History Bookmarks Tools Help
Mr.NAMIK4ZE - YouTube
https://www.youtube.com/channel/UCMaYLz8DzE105gzuNTLsjnA
Search
YouTube ID
Telusuri
Login
Farm Frenzy: Pizza Party
62
00:14
01:00
Computer ▸ Data (D:) ▸
Search Data (D:)
Organize
Open
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
WIN-7-X86-PRO (C:)
Data (D:)
Multimedia (E:)
NAMIK4ZE (F:)
Network
Name
Date modified
Type
Size
100CANON 20/02/2017 14:24 File folder
Project 02/01/2017 21:23 File folder
Blogger Templates 24/02/2015 8:50 Internet Shortcut 1 KB
discover 06/11/2014 0:15 XML Document 175 KB
Documentation 26/12/2015 9:55 Chrome HTML Do... 1.532 KB
Eleganto 26/12/2015 19:31 XML Document 129 KB
How To Install A Template 04/07/2015 22:46 Internet Shortcut 1 KB
Instructions 01/03/2015 12:08 Text Document 1 KB
Simple Clean white 25/05/2012 21:24 XML Document 87 KB
test 18/03/2017 20:36 Application 4.119 KB
theme-5918636448337444901 18/03/2017 19:54 XML Document 196 KB
test Date modified: 18/03/2017 20:36 Date created: 18/03/2017 20:36
Application Size: 4,02 MB
0:00 / 0:27
Upload
Cheat Global Strike Hack GOLD with Cheat
Cheat Shadowgun: Deadzone Hack v...
MiawAug
Subscribe
Dota Watafak
Subscribe
Recording [00:03:39]
IN
20:36
18/03/2017

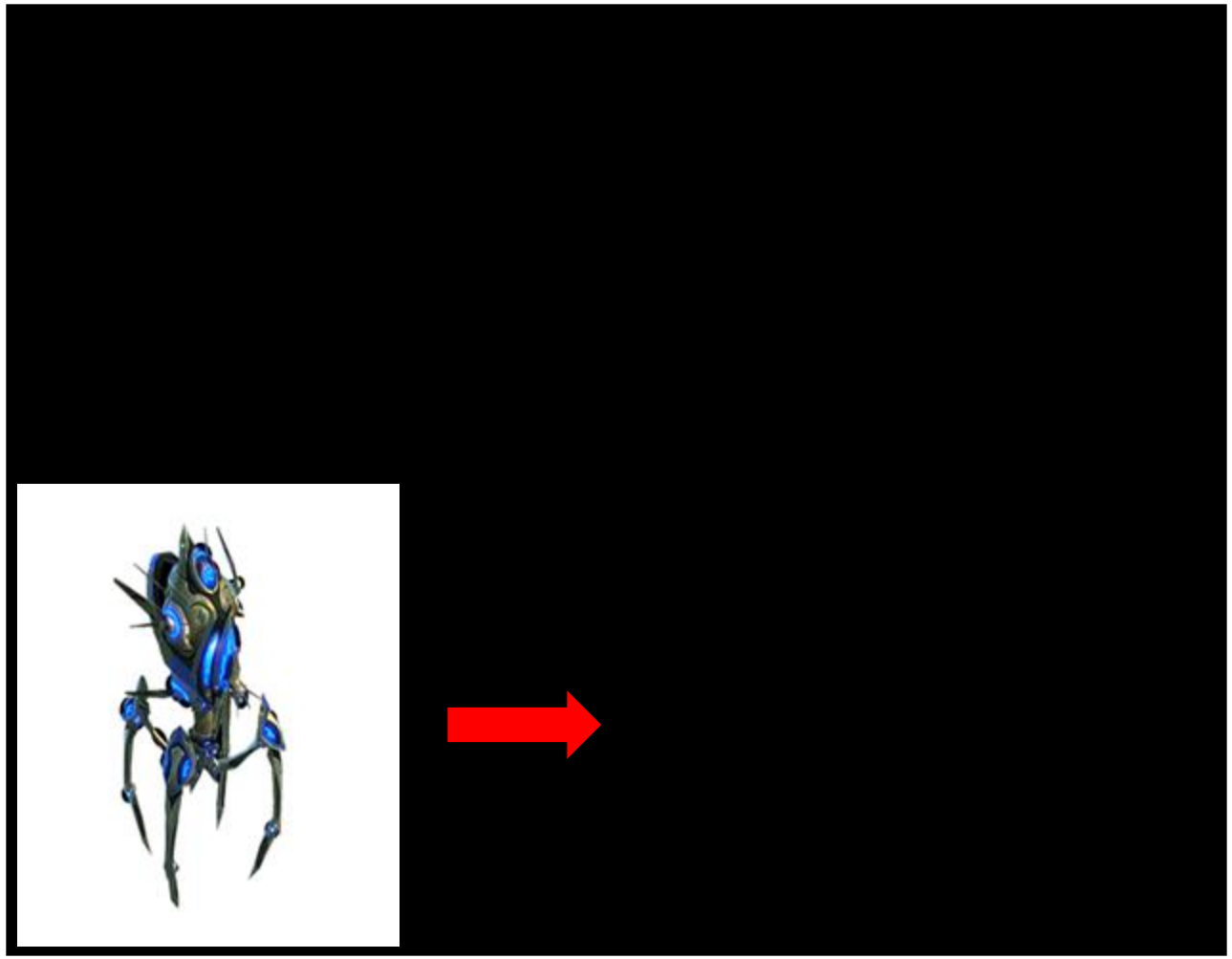
Data Exfiltration: What to Read?

- Known game engine
  - Generate **blueprint**
  - Requires some reverse engineering skills
- Unknown game engine with easy to find data
  - Use **Cheat Engine**
  - A scriptkiddie could do this
- Unknown game engine with complex data structures
  - Really, **really** hard



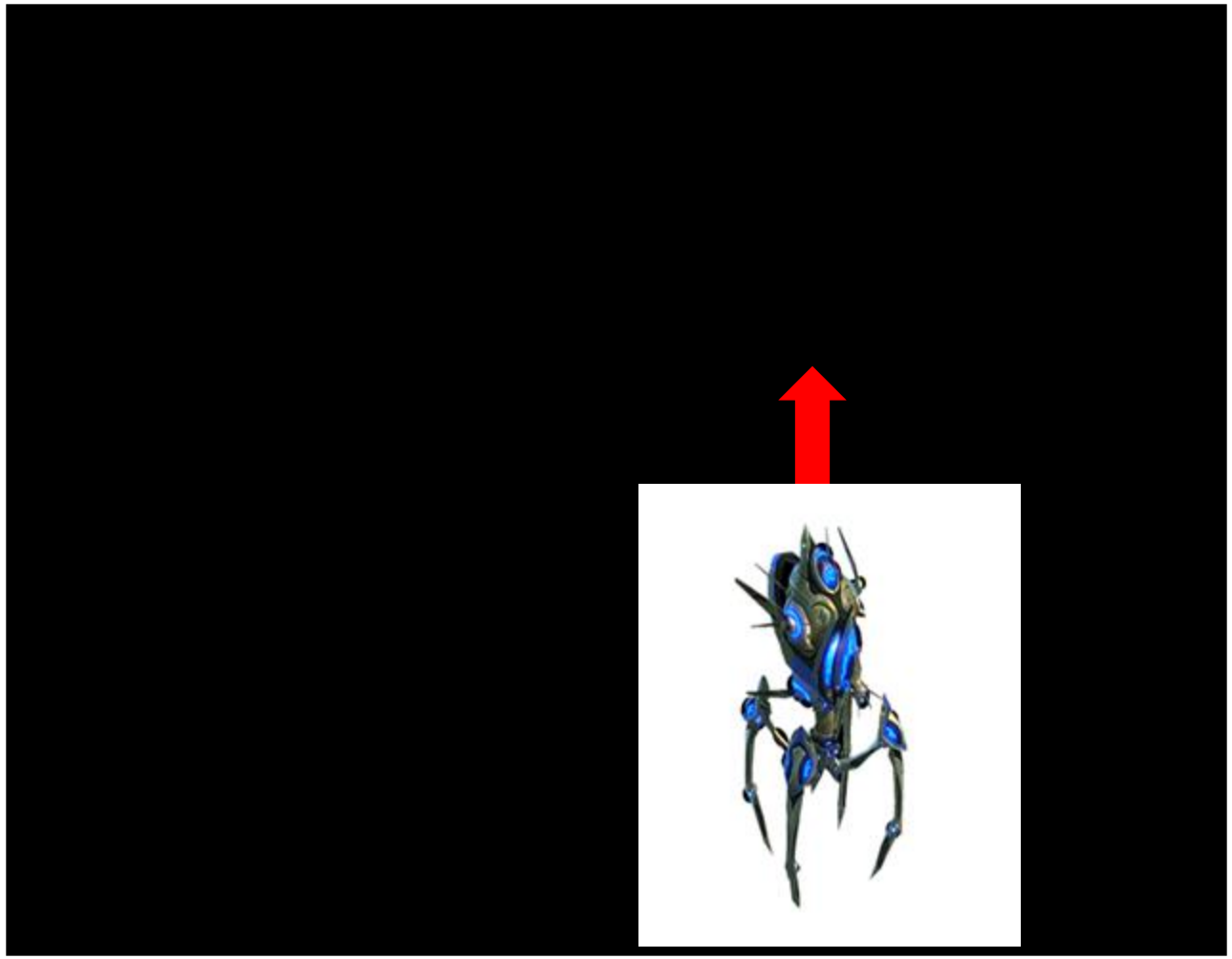

195
8
19/31
Workers: 14/16
Workers: 1/3
map_fog_of_war_state = [
[0, 0, 0, 0, 0],
[0, 0, 0, 0, 0],
[0, 0, 0, 0, 0],
[0, 0, 0, 0, 0],
[0, 1, 0, 0, 0],
]
F1
F2
1:44
Menu
SCV
Kills: 0
Rank: Recruit
45 / 45
Light - Biological - Mechanical

Data Exfiltration: Advanced Memory Diffing



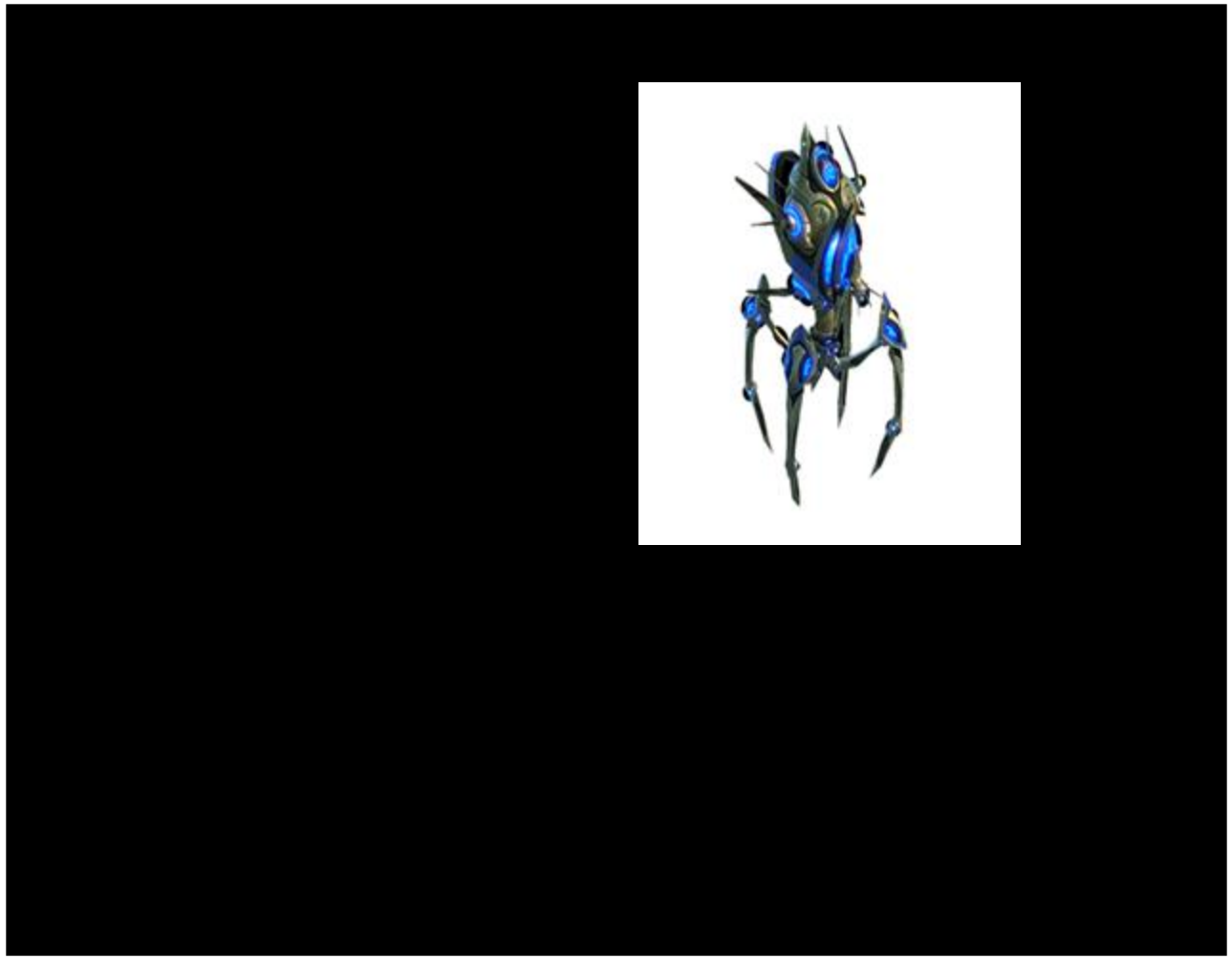
```
map_fog_of_war_state =
[
    [0, 0, 0, 0, 0],
    [0, 0, 0, 0, 0],
    [0, 0, 0, 0, 0],
    [1, 1, 0, 0, 0],
    [1, 1, 0, 0, 0],
]
```

Data Exfiltration: Advanced Memory Diffing



```
map_fog_of_war_state =
[
    [0, 0, 0, 0, 0],
    [0, 0, 0, 0, 0],
    [0, 0, 0, 0, 0],
    [0, 0, 1, 1, 0],
    [0, 0, 1, 1, 0],
]
```

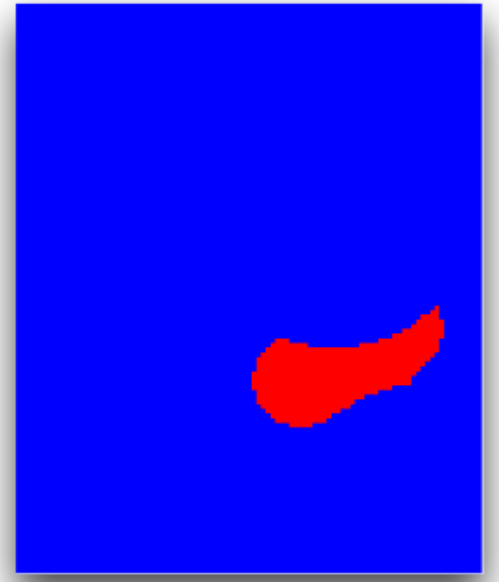
Data Exfiltration: Advanced Memory Diffing



```
map_fog_of_war_state =
[
    [0, 0, 0, 0, 0],
    [0, 0, 1, 1, 0],
    [0, 0, 1, 1, 0],
    [0, 0, 0, 0, 0],
    [0, 0, 0, 0, 0],
]
```

Data Exfiltration: Advanced Memory Diffing

Move a unit in game



Diff map of the memory

- Move game units around and generate diff maps
- Find contiguous bytes of memory that change when revealing fog of war
- Highly automatable and even defeats basic data obfuscation techniques

[*] Bursztein, E., Hamburg, M., Lagarenne, J. and Boneh, D. Openconflict: Preventing real time map hacks in online games. In *2011 IEEE S&P.*

Cheating: Core Techniques

Cheat	Goal	Techniques
Wallhack Radar Maphack	Reveal hidden game state	Data exfiltration Overlay rendering API hooking
Speedhack	Illegally modify game state	API hooking

API Hooking: Speedhacks

```
while (!RequestedExit) {
  // Calculate deltatime
  double TimeNow = getTime();
  double DeltaTime = TimeNow - TimePrev;
  TimePrev = TimeNow;
  // Process player input
  readInput();
  // update local game state
  MyPlayer.Position.X += XDirection * XVelocity * DeltaTime;
  MyPlayer.Position.Y += YDirection * YVelocity * DeltaTime;
  // replicate game state to server
  replicateState();
  // render a frame
  renderWorld();
  // wait until the next loop iteration
  sleep(...);
}
```

```
double getTimeHook() {
  return getTime() * 1.1;
}
```

```
// System function that reads from
// some high-precision timing source
double getTime() {
  // ...
}
```

Cheating: Core Techniques

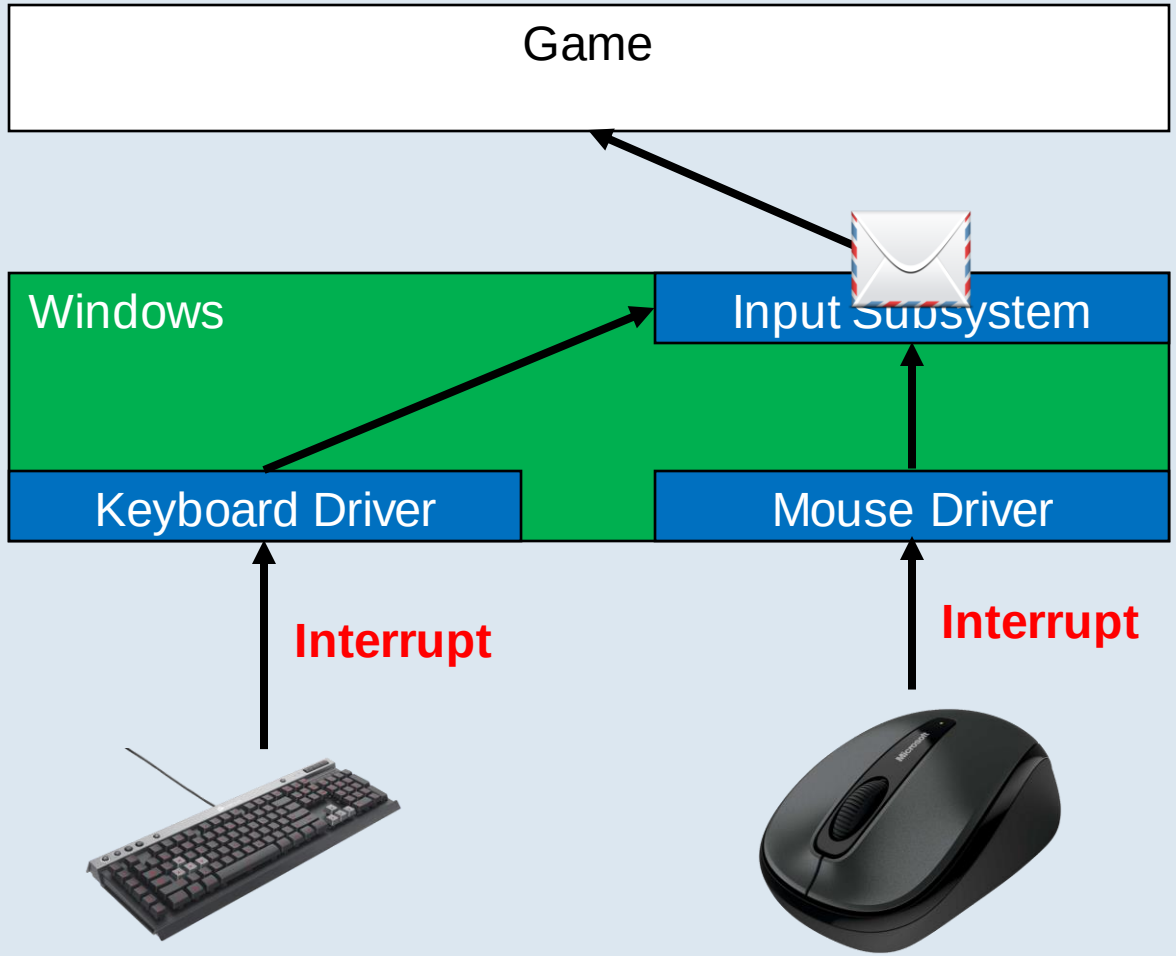
Cheat	Goal	Techniques
Wallhack Radar Maphack	Reveal hidden game state	Data exfiltration Overlay rendering API hooking
Speedhack	Illegally modify game state	API hooking
Aimbot Triggerbot Massmurder Farmbot	Automate the game	Rogue API calls Input emulation

Automating the Game: Data Tampering?

- Modifying the game state directly often does not work in online games
- Anti-cheat software can easily see that your modifications were not the result of human input
- Most cheats **emulate human input**

Background: How do Games Receive Keyboard and Mouse Input?

- When you move your mouse, click a mouse button or tap a key on your keyboard, the keyboard/mouse generates an **interrupt**
- The operating system catches this interrupt and sends it to the **device driver**
- The device driver decodes the input event and forwards it to the **input subsystem**
- The input subsystem sends an input **message** to the game's **message queue**



Emulating Human Input

- You can generate fake input by sending input messages directly to the game

SendMessage function

05-12-2018 • 2 minuten om te lezen

Sends the specified message to a window or windows. The **SendMessage** function c
window and does not return until the window procedure has processed the messag

To send a message and return immediately, use the SendMessageCallbac
thread's message queue and return immediately, use the PostMessage or

Syntax

```
C++

LRESULT SendMessage(
  HWND   hWnd,
  UINT   Msg,
  WPARAM wParam,
  LPARAM lParam
);
```

WM_INPUT message

05/31/2018 • 2 minutes to read •

Sent to the window that is getting raw input.

A window receives this message through its **WindowProc** function.

Copy

WM_MOUSEMOVE message

05/31/2018 • 2 minutes to read •

Posted to a window when the cursor moves. If the mouse is not captured, the message is posted to the window that contains the cursor. Otherwise, the message is posted to the window that has captured the mouse.

A window receives this message through its **WindowProc** function.

```
C++                                                    Copy

#define WM_MOUSEMOVE                    0x0200
```

Why is Cheating Possible?

Core Problems:

1. Operating Systems let you do pretty much anything on your own computer
2. Most of the game state is available in your RAM memory at any given time
3. Finding and tampering with relevant game state is easier than you would think
4. **Cheating is a lucrative business**

Cheating = Big Business

As soon as a game becomes popular, people try to cheat.

Cheats for competitive online games usually require a subscription

Typical prices range between $5-$50/Month

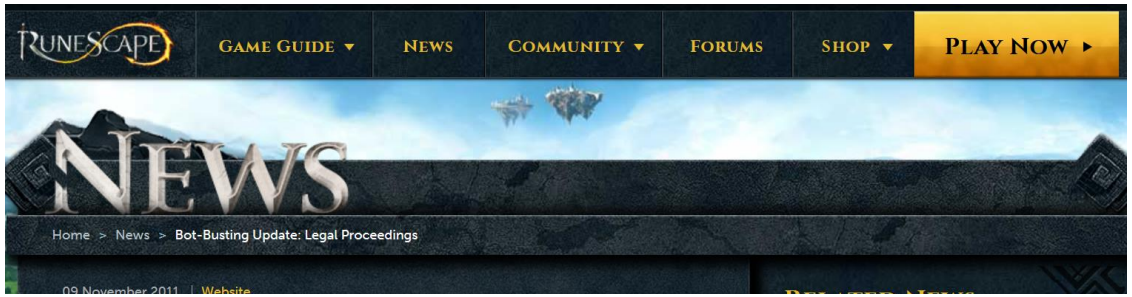
Bungie wins lawsuit against cheat maker, awarded $13.5 million

Elite Boss Tech admits to integrating its own overlay into Destiny 2's copyrighted work

News by Danielle Partis | News Editor
Published on June 21, 2022

Bossland GMBH has been ordered to pay **Blizzard** $8.6 million by a federal court in California. ... **Blizzard** has **sued** Bossland before, in Germany, over a Heroes of the Storm cheat, but the publisher lost that case and was ordered to pay Bossland's legal fees. Apr 4, 2017

Blizzard wins $8 million judgment against Overwatch cheat maker ...
https://www.polygon.com/2017/4/4/.../overwatch-cheat-maker-sued-loses-judgment



EPIC Bravely Defeats 14 Year Old's Mom In Court To Continue Lawsuit Against Her Son For Cheating In Fortnite


Copyright

from the *punching-down* dept
Wed, Jul 18th 2018 7:41pm — Timothy Geigner

Earlier this year, we wrote about EPIC, makers of the popular *Fortnite* game, picking up the baton from Blizzard to pretzel copyright law such that it believes it can sue those that cheat in its game for copyright infringement. This belief centers on the claim that these cheaters break the EULA, despite the fact that no actual copying occurs when breaking a EULA. To make PR matters worse for EPIC, the company managed to sweep up a fourteen

Riot Games wins $10 million in lawsuit against League of Legends cheating service

2017-03-07 13:00:00 by Chris Carter

MDY Industries, LLC v. Blizzard Entertainment, Inc.

From Wikipedia, the free encyclopedia

MDY Industries, LLC v. Blizzard Entertainment, Inc and Vivendi Games, Inc., 629 F.3d 928 (9th Cir. 2010), is a case decided by the United States Court of Appeals for the Ninth Circuit. At the district court level, MDY had been found liable under theories of copyright and tort law for selling software that contributed to the breach of Blizzard's End User License Agreement (EULA) and Terms of Use (TOU) governing the World of Warcraft software.[1]
The court's ruling was appealed to the United States Court of Appeals for the Ninth Circuit, which reversed the district court in part, upheld in part, and remanded for further proceedings. The Court of Appeals ruled that for a software licensee's violation of a contract to constitute copyright infringement, there must be a nexus between the license condition and the licensor's exclusive rights of copyright. However, the court also ruled, contrary to *Chamberlain v. Skylink*, that a finding of circumvention under the Digital Millennium Copyright Act does not require a nexus between circumvention and actual copyright infringement.

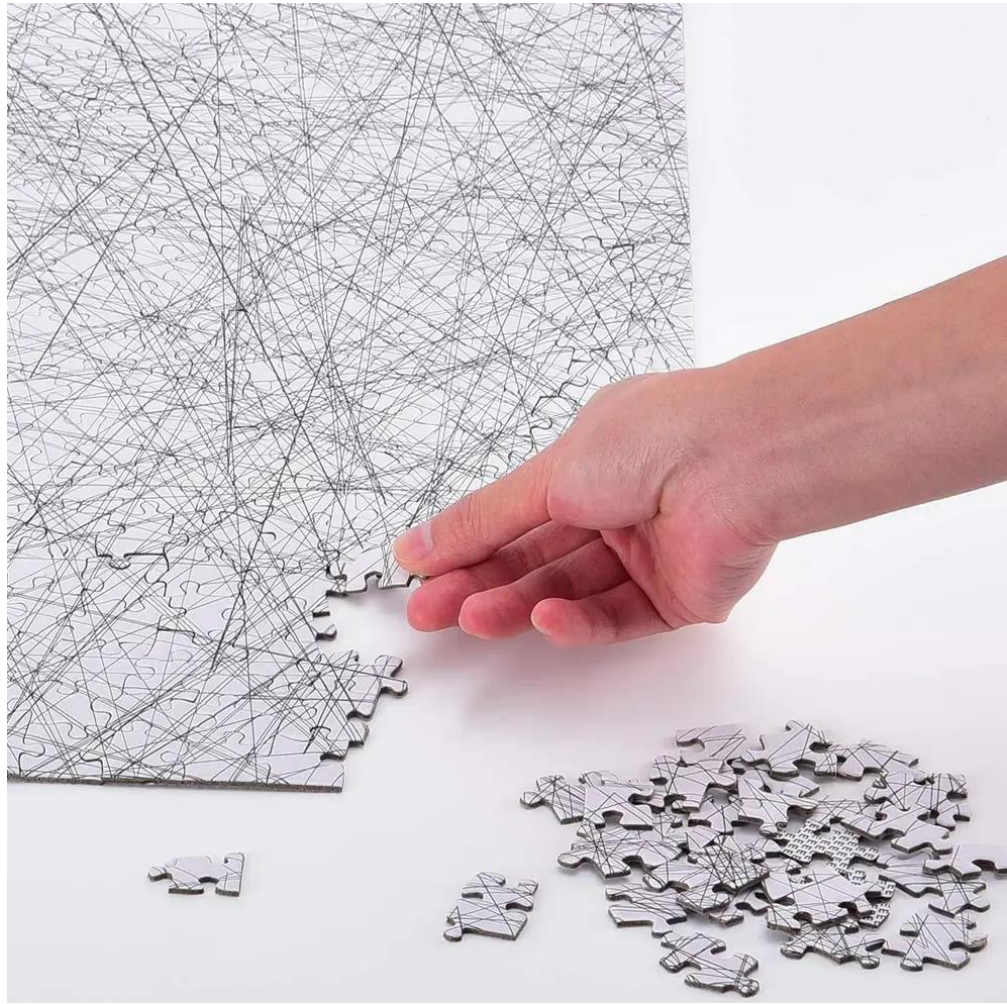
Video: Jarvis Kaye breaks down after receiving life-time ban for CHEATING

Putting All the Pieces Together

Cheating in a nutshell:

1. You launch a game
2. You start the cheat software
3. The cheat extracts relevant game state from the game
4. The cheat visualizes the extracted state to give you information other players don't have (e.g., wallhacks) …
5. … OR the cheat uses the extracted state to automatically perform game actions (e.g., aimbots)

Some cheats are easy to spot. Others are nearly impossible to see with the naked eye.



Anti-Cheat

What Can We Do About Cheating?

Cheat Prevention

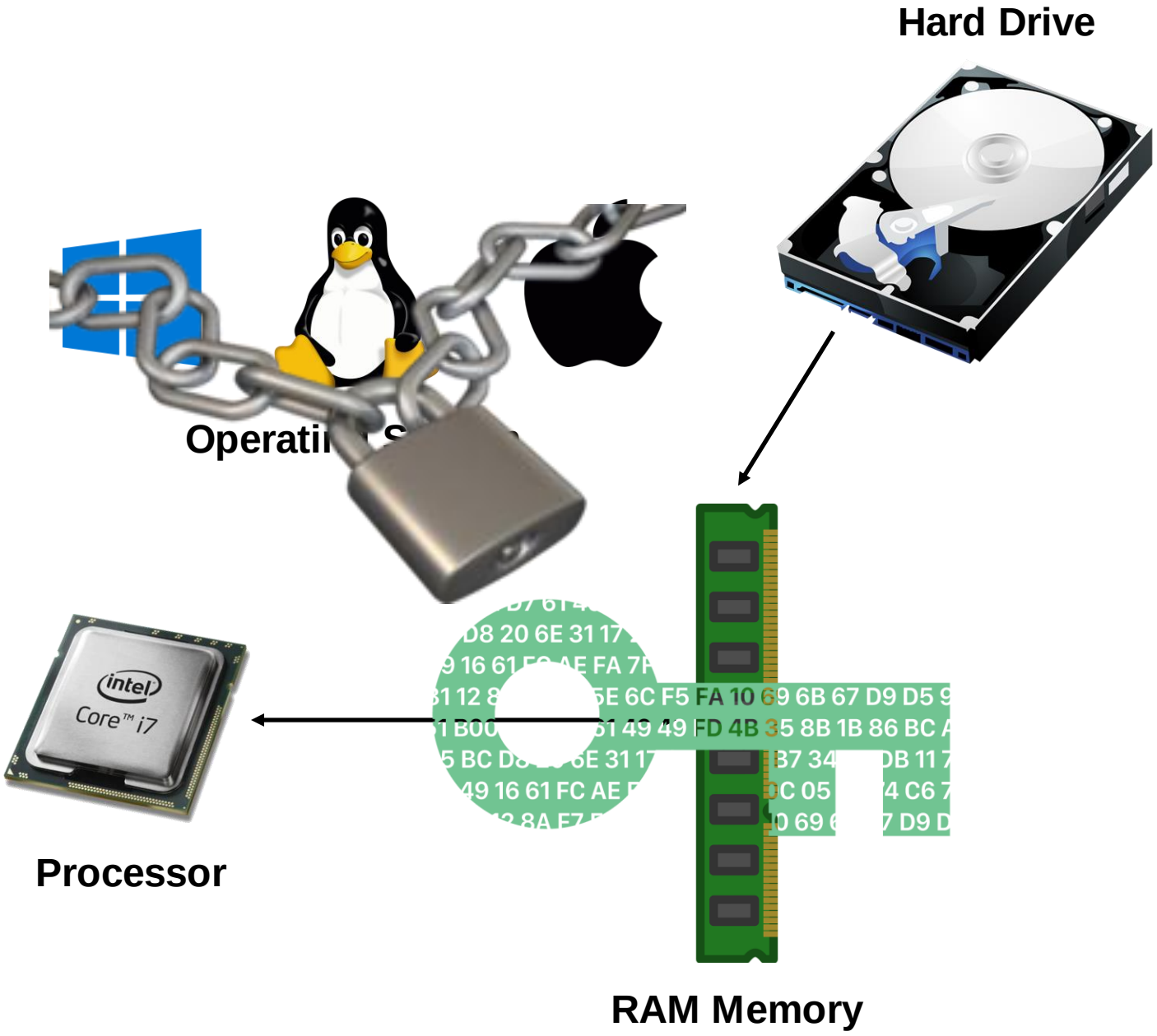
Many possibilities:

- Hide your **game state** (e.g., encryption, obfuscation)

⇒ **Performance concerns!**

- Lock down the **operating system**

=> OK for specialty devices (gaming consoles, mobile devices), **unacceptable for PCs**!



Cheat Prevention

Many possibilities:

- Move the game client into the **cloud**

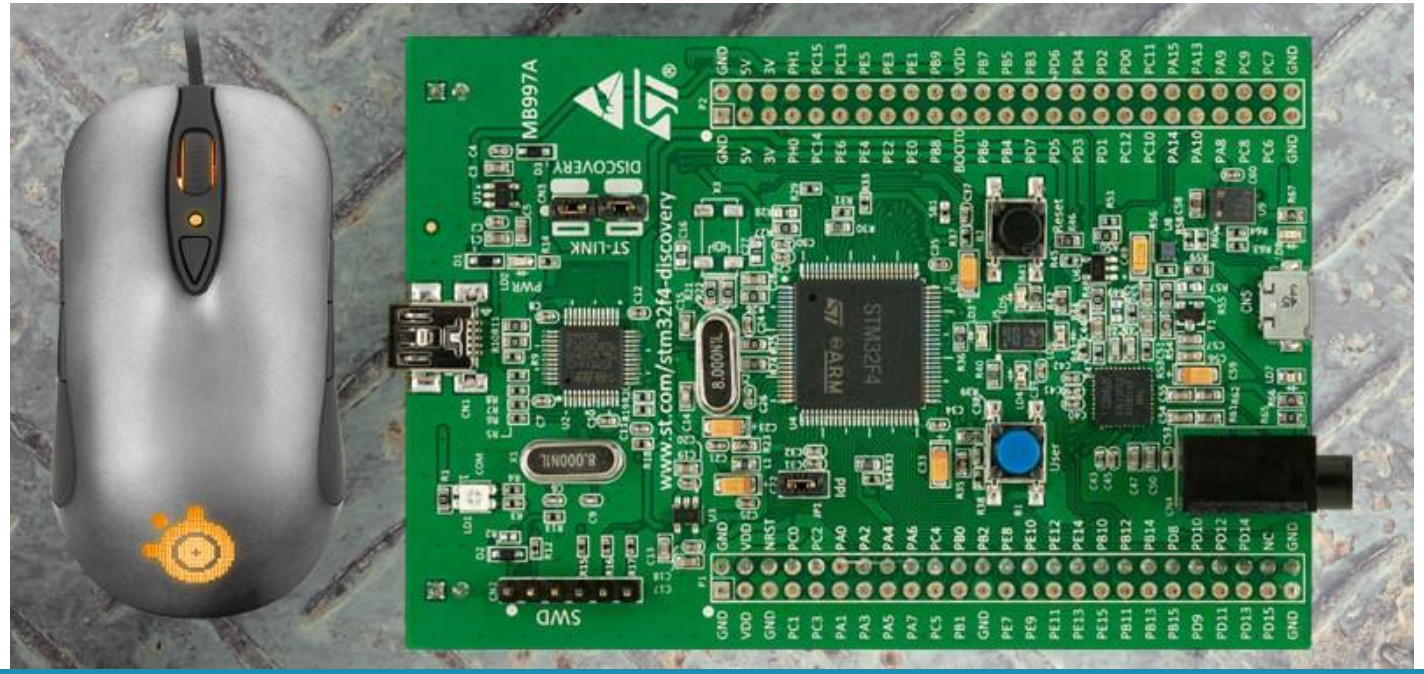
⇒ OK for casual games. Problematic for **esports**!

- Do not let players use their **own hardware**

⇒ OK for live tournaments. **Impractical** for online play!

Hardware Cheats

- Some tournaments allow you to bring your own peripherals (mouse, keyboard, headset) …
- … but you can embed cheats directly into hardware!



Cheat Detection

Many possibilities:

- Run w
  client
- ⇒ Peop
  differe
  - Us
  - La
  - Ta
  - Rc

Valve has 1,700 CPUs working non-stop to bust CS:GO cheaters

By Evan Lahti March 26, 2018

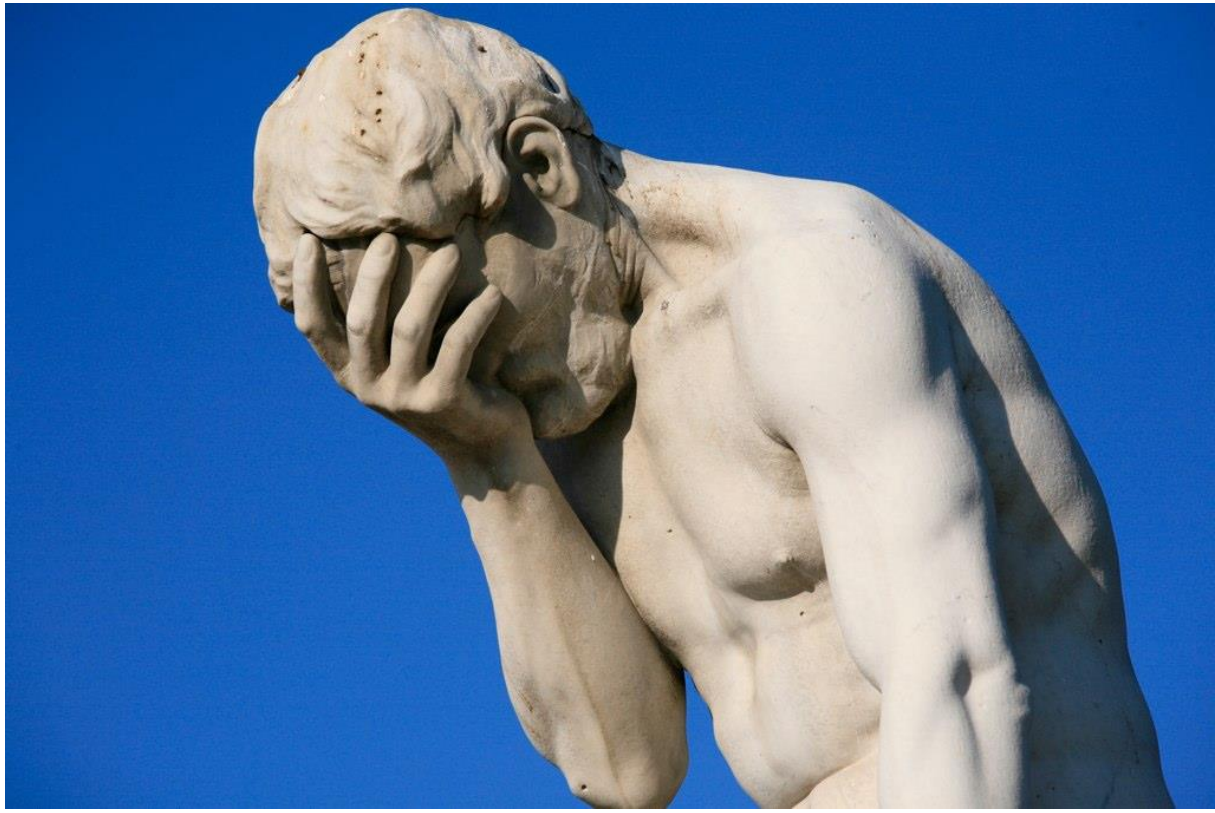
Meet VACnet, the deep learning system Valve used to smash CS:GO's hacking problem.

⇒ Watchdog software is often **controversial**

- Analyze **player input/behavior** using AI

AI-Based Cheat Detection

- AI-based Cheat Detection
  - Highly effective at spotting obvious cheaters
  - … but cheat developers now use AI to learn what normal human input looks like and to replicate that in-game



Conclusions

- **Cheating is a big problem**, especially on PC platforms
- State-of-the-art **software protection** measures would help, but cannot be used in games due to **performance constraints**
- Hackers and anti-cheat developers are playing a **perpetual cat-and-mouse game** to try and stay ahead of each other