OpenConflict

Preventing Map Hack in online games

Elie Bursztein, Mike Hamburg, Jocelyn Lagarenne, Dan Boneh
Stanford University

Welcome to the real world

#kartograph / @elie


273 Millions games sold in 2009


Strategy account for 35% of the games sold in 2009


GSL Pre-Season
StarCraft II Open Season1
우승
₩100,000,000
GOMTV
TG삼보
intel
BLIZZARD

Cash prize up to 200,000$

Outline

Outline

- Background

Outline

- Background
- Memory based map-hack with Kartograph

Outline

- Background
- Memory based map-hack with Kartograph
- Defending against map-hack

Outline

- Background
- Memory based map-hack with Kartograph
- Defending against map-hack
- Starcraft 2 case study

Outline

- Background
- Memory based map-hack with Kartograph
- Defending against map-hack
- Starcraft 2 case study
- Open conflict benchmark

Background

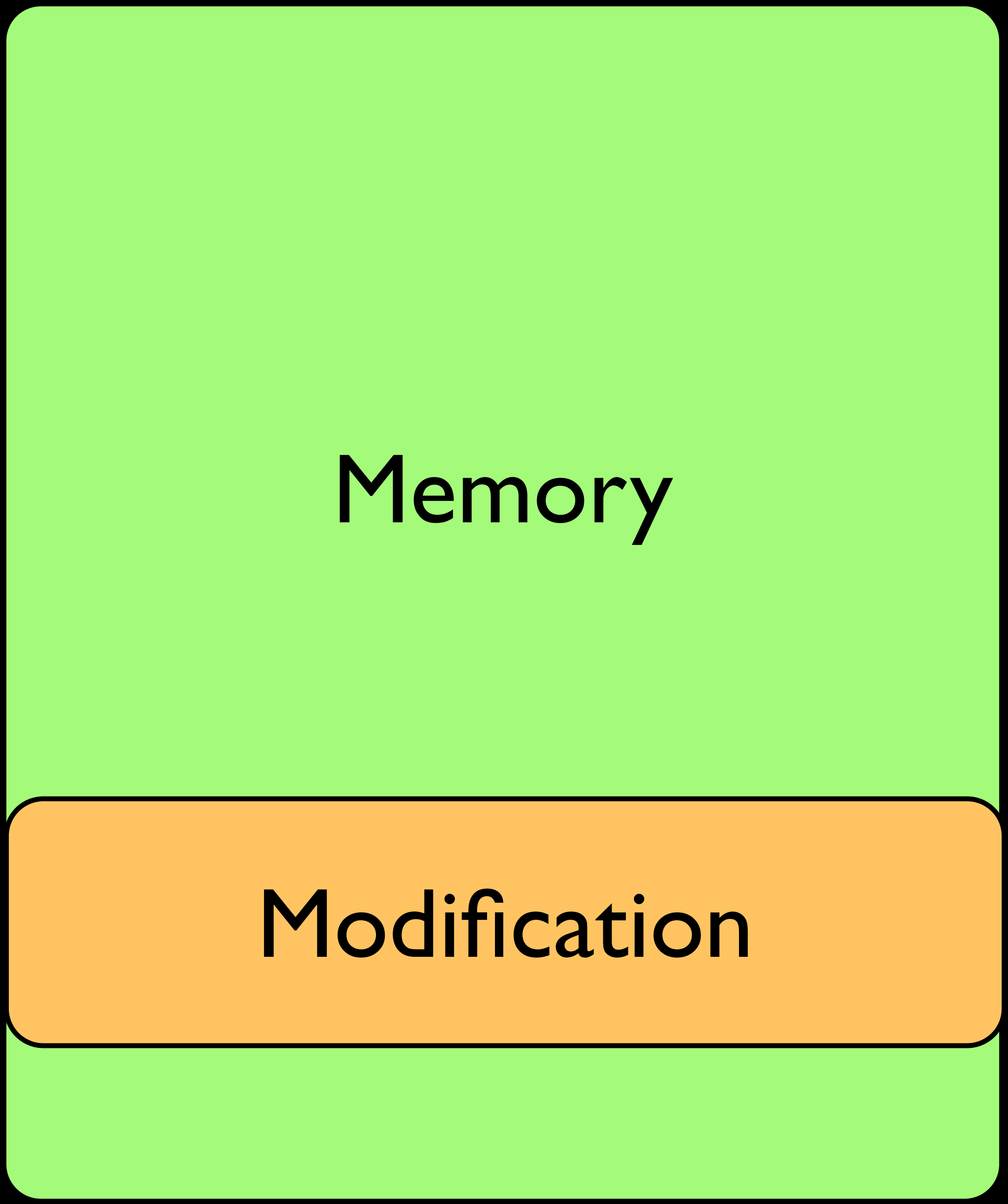
supernatural powers !

- Learn kungfu
- Infinite money
- Xray vision
- god mode

Memory based attack

Memory

Memory based attack

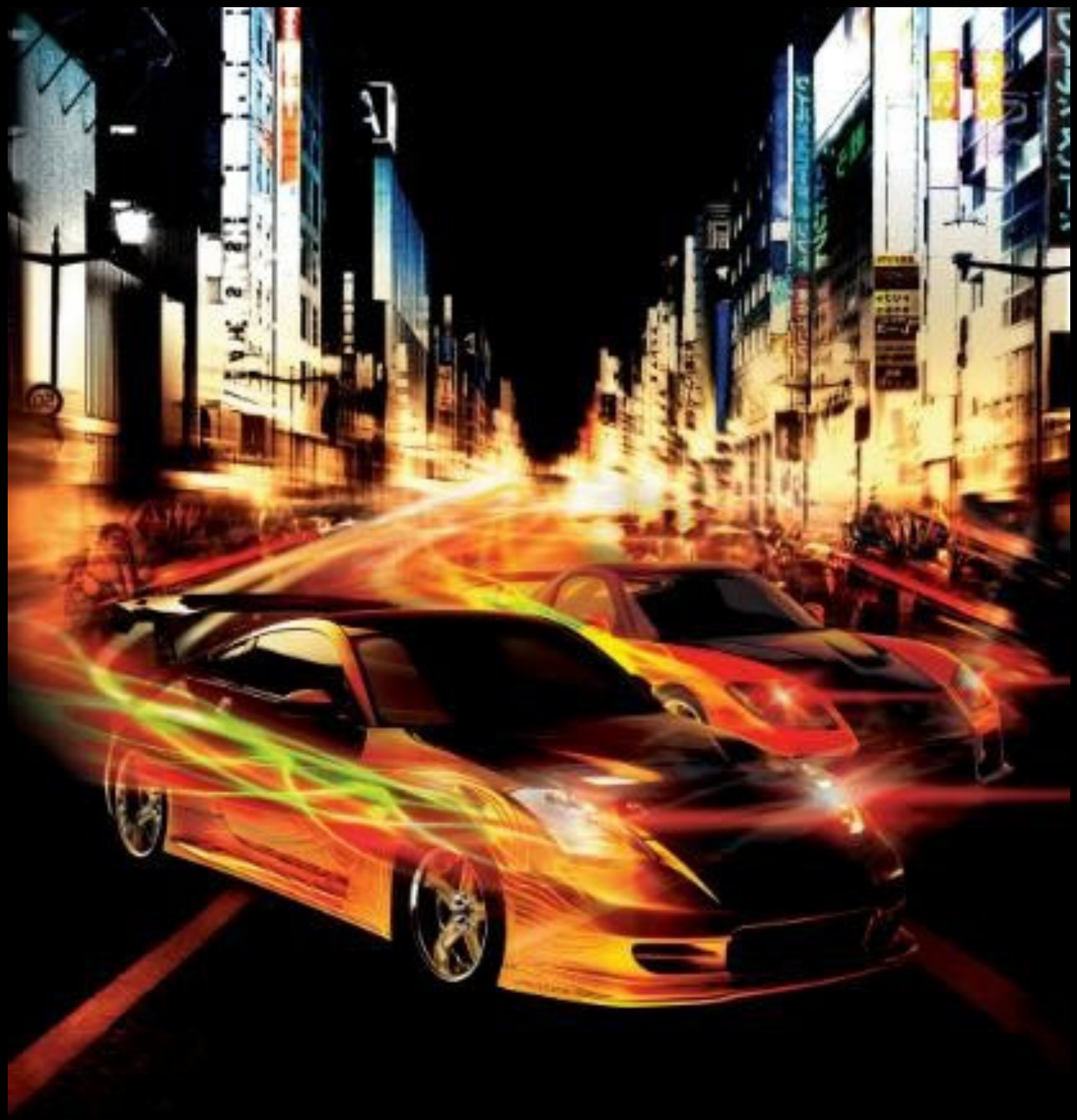


Memory based attack

Memory

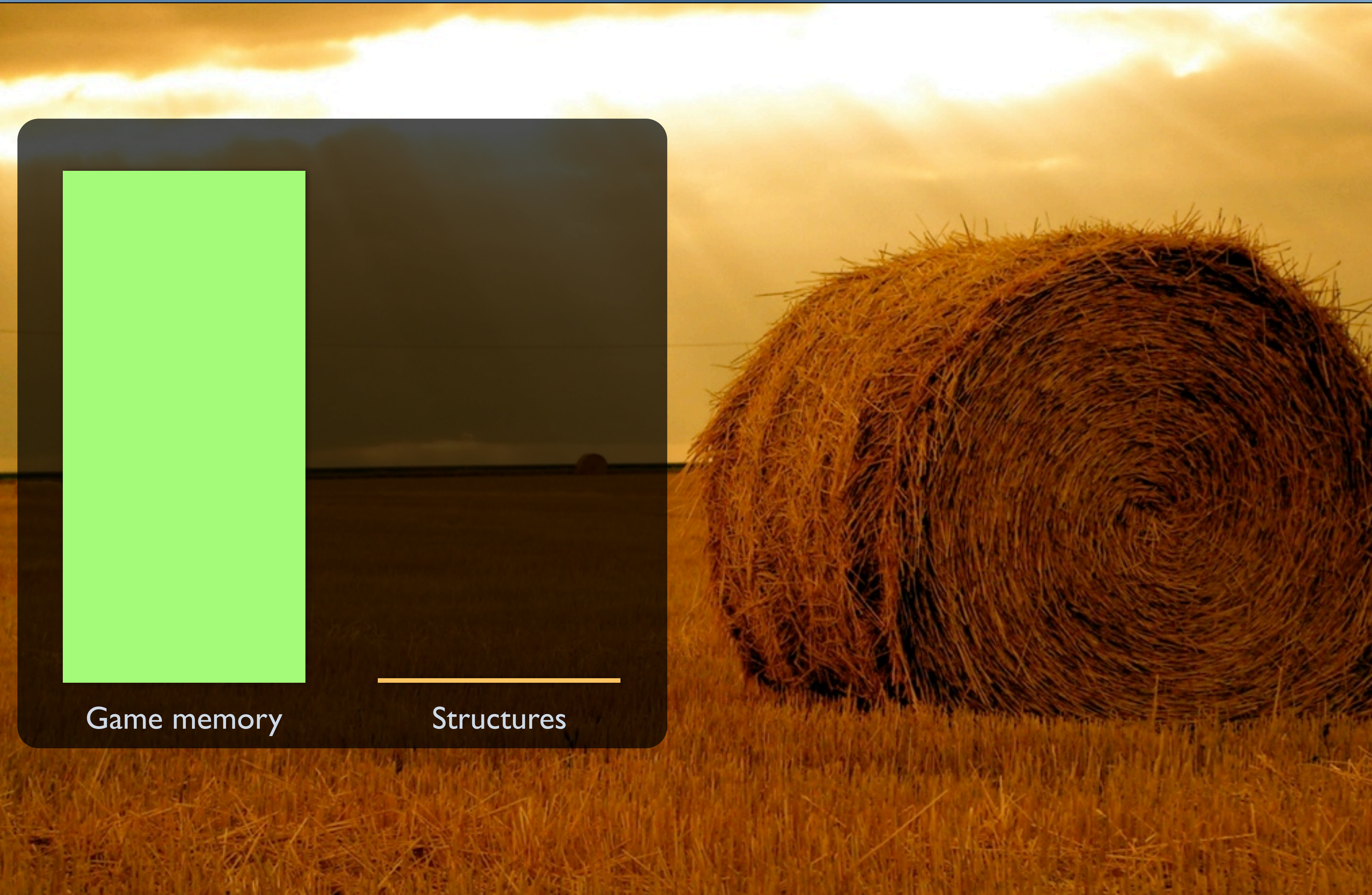
Modification

Benefits (fast and furious)



- Generic
- Fast
- Invisible

Drawbacks: Needle in a Haystack




4650
Tankbuster
$ 300
0:05
Anti-Armor
Steely-cold warriors whose personal plasma-cutter cannons can slice through enemy armor.
Instant Dojo
1


Resources
4650
Tankbuster
$ 300 0:05
Anti-Armor
Steely-cold warriors whose personal plasma-cutter cannons can slice through enemy armor.
Instant Dojo

Resources
4650
Tankbuster
$ 300
0:05
Anti-Armor
Steely-cold warriors whose personal plasma-cutter cannons can slice through enemy armor.
Instant Dojo

Building
4650
Tankbuster
$ 300 0:05
Anti-Armor
Steely-cold warriors whose personal plasma-cutter cannons can slice through enemy armor.
Instant Dojo

Units
4650
Tankbuster
$ 300
0:05
Anti-Armor
Steely-cold warriors whose
personal plasma-cutter
cannons can slice through
enemy armor.
Instant Dojo


Minimap
4650
Tankbuster
$ 300
0:05
Anti-Armor
Steely-cold warriors whose personal plasma-cutter cannons can slice through enemy armor.
Instant Dojo


4650
Tankbuster
$ 300
0:05
Anti-Armor
Steely-cold warriors whose personal plasma-cutter cannons can slice through enemy armor.
Instant Dojo


Production (D)
SPeCiaLiST
psystarcraft
Everyone (E)
Orbital Command
2
3
4
5

How to cheat at a RTS ?

How to cheat at a RTS ?

Resources

How to cheat at a RTS ?

Resources

units

How to cheat at a RTS ?

Resources

units

map

What is a map hack ?

What is a map hack ?


There is no spoon

Defeating security via obscurity

- Find the information hidden by the game
- Understand the data structures
- Abuse this knowledge

Kartograph

What is Kartograph ?

- Memory analysis techniques
- Visualization techniques

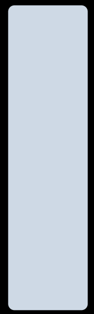
How Kartograph works ?

How Kartograph works ?

How Kartograph works ?

Reduce
haystack

How Kartograph works ?



Reduce haystack

Find

How Kartograph works ?

Reduce haystack

Find

Understand

How Kartograph works ?

Reduce haystack

Find

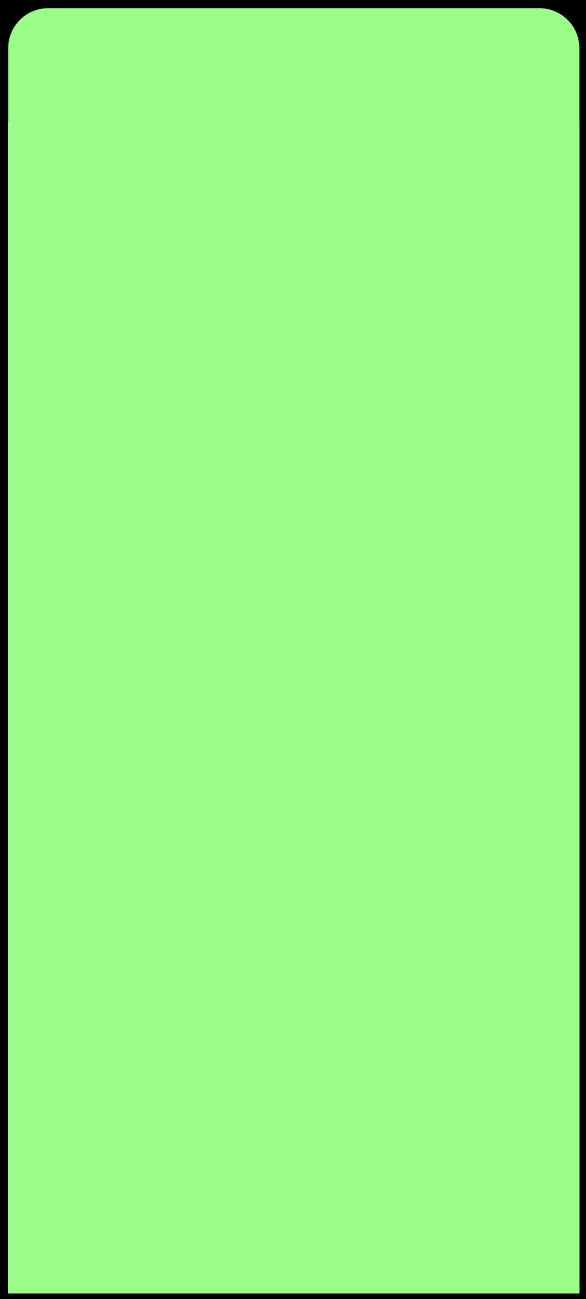
Understand

Rewrite

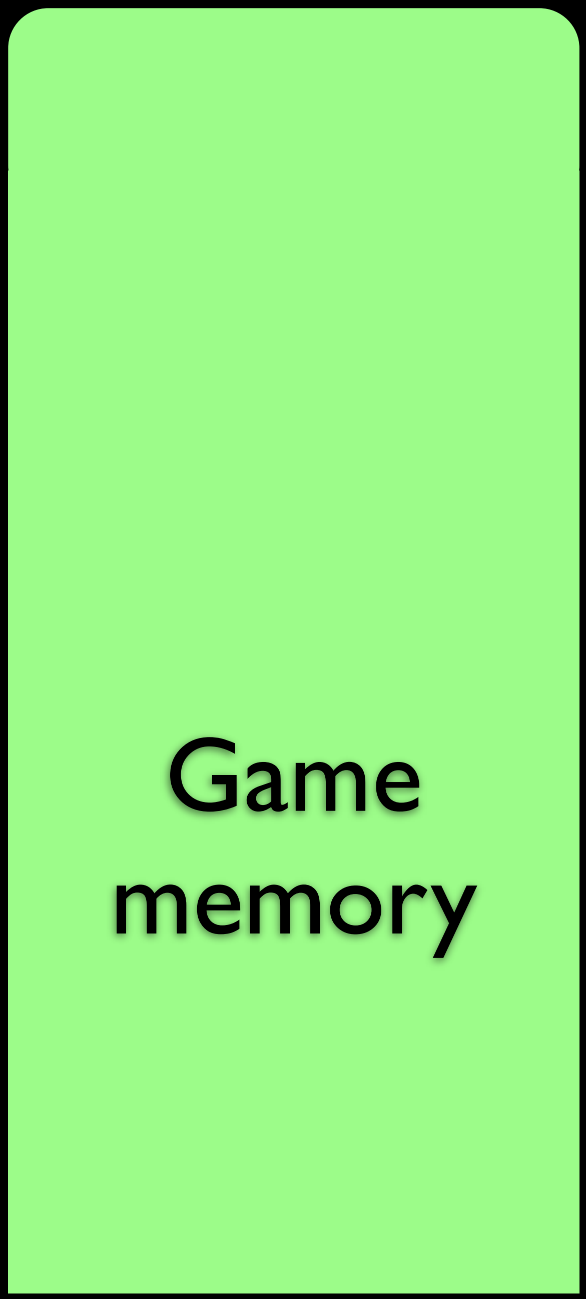
Acquiring game memory

Game memory

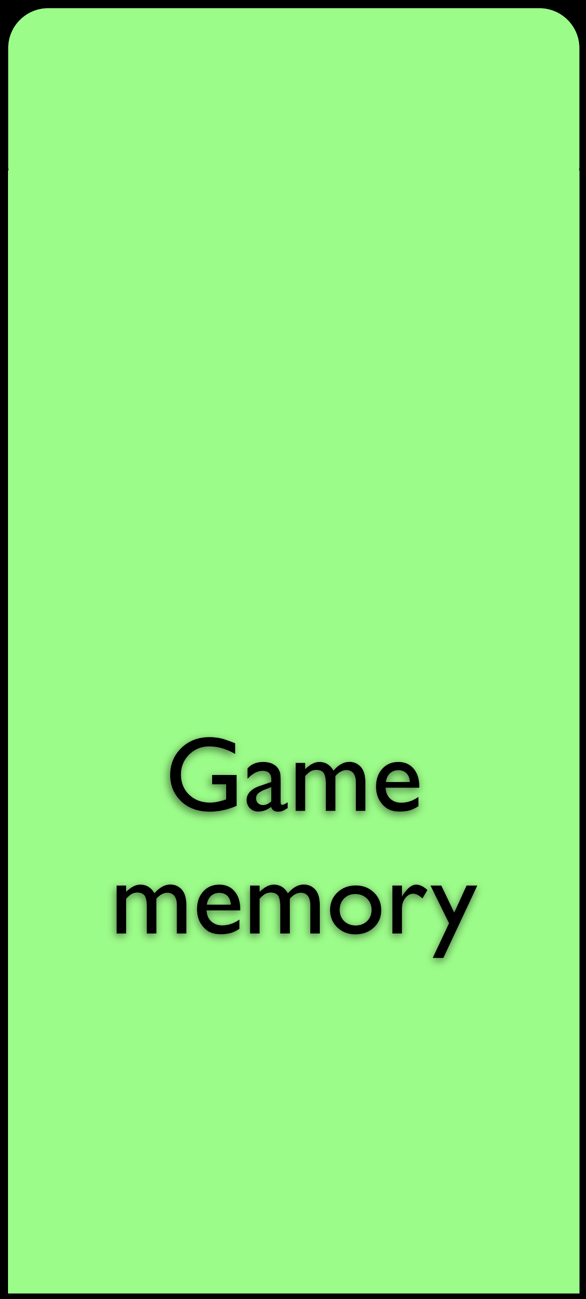
Acquiring game memory



Reducing memory

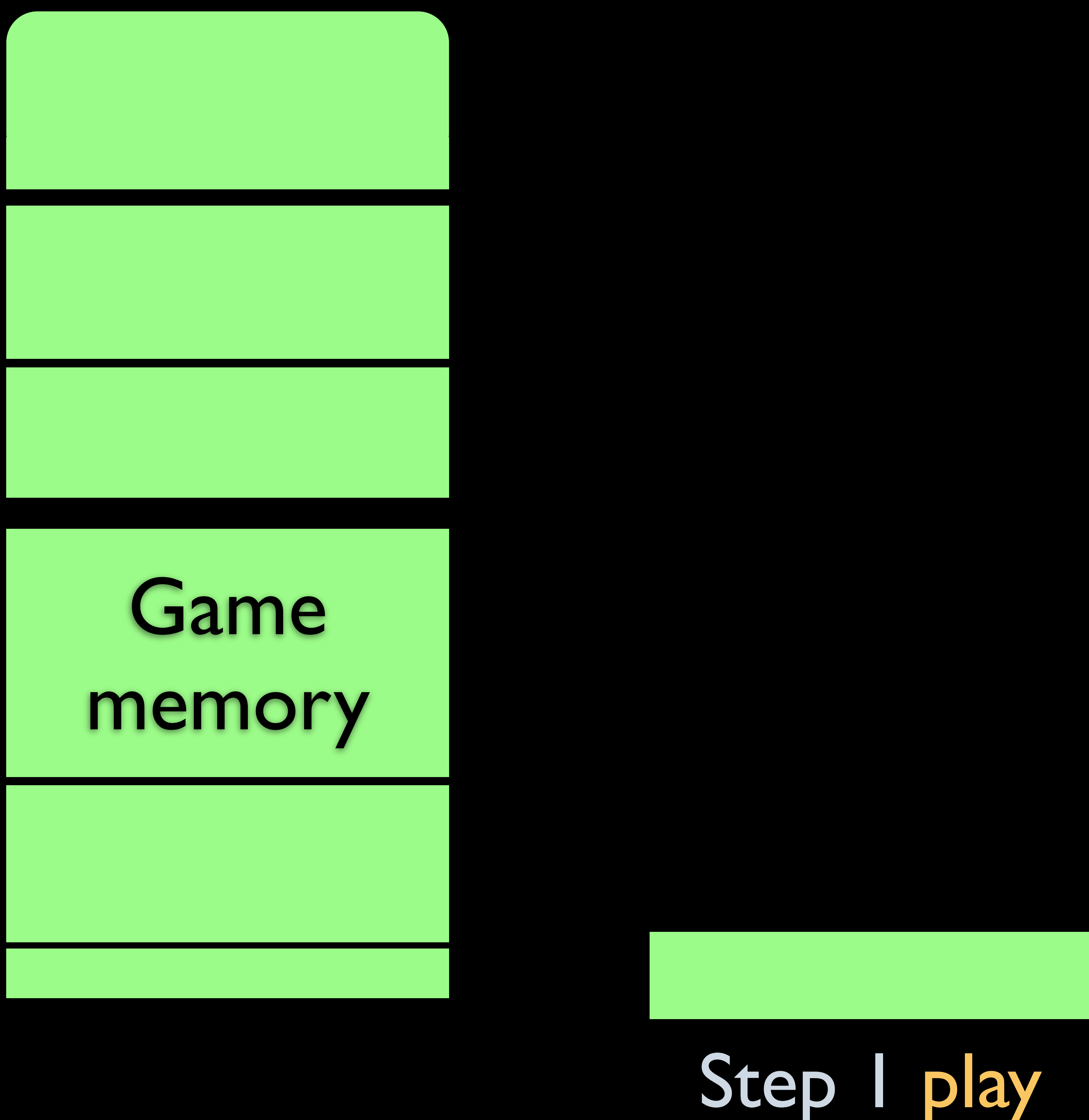


Reducing memory

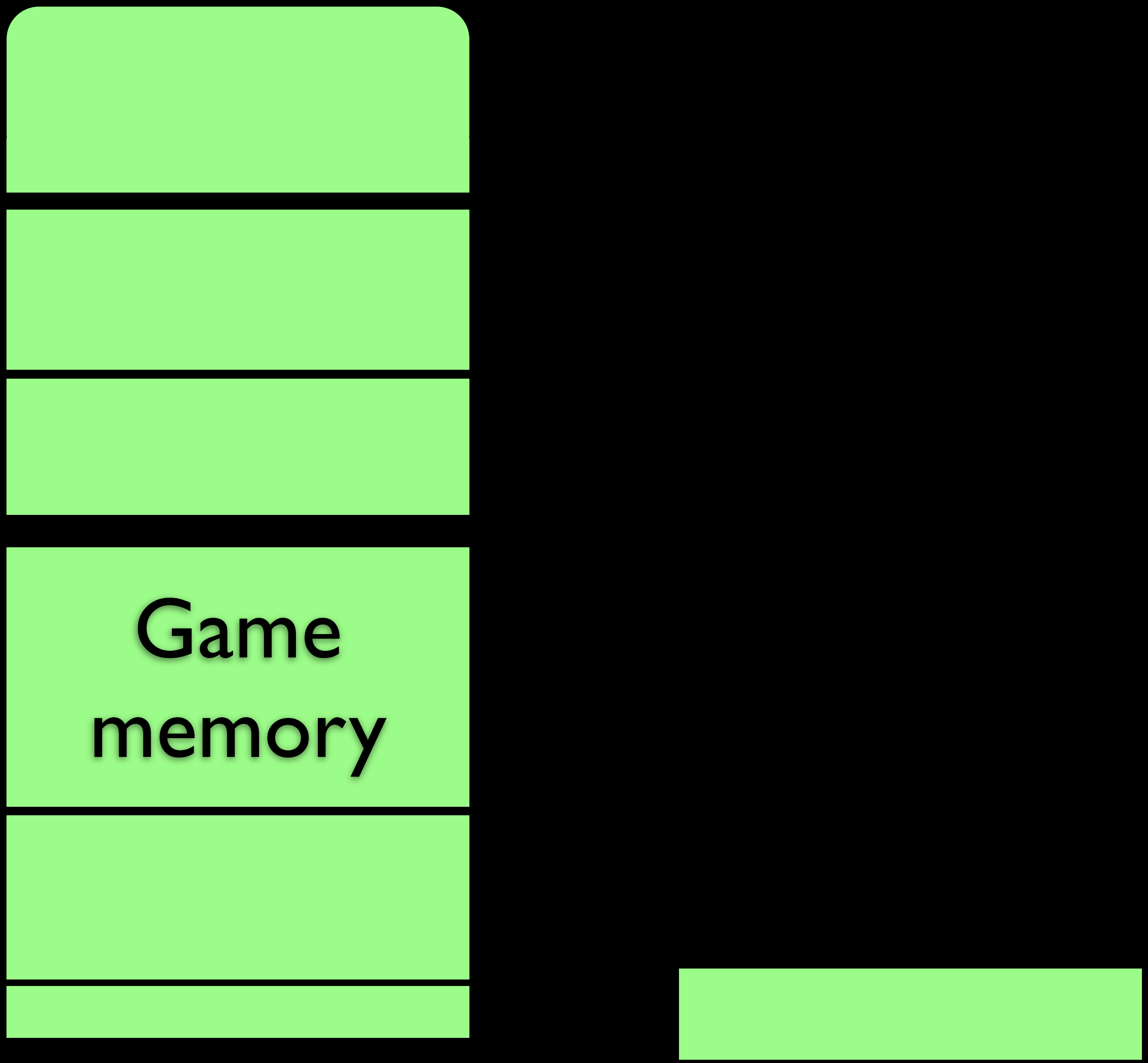


Step 1 play

Reducing memory

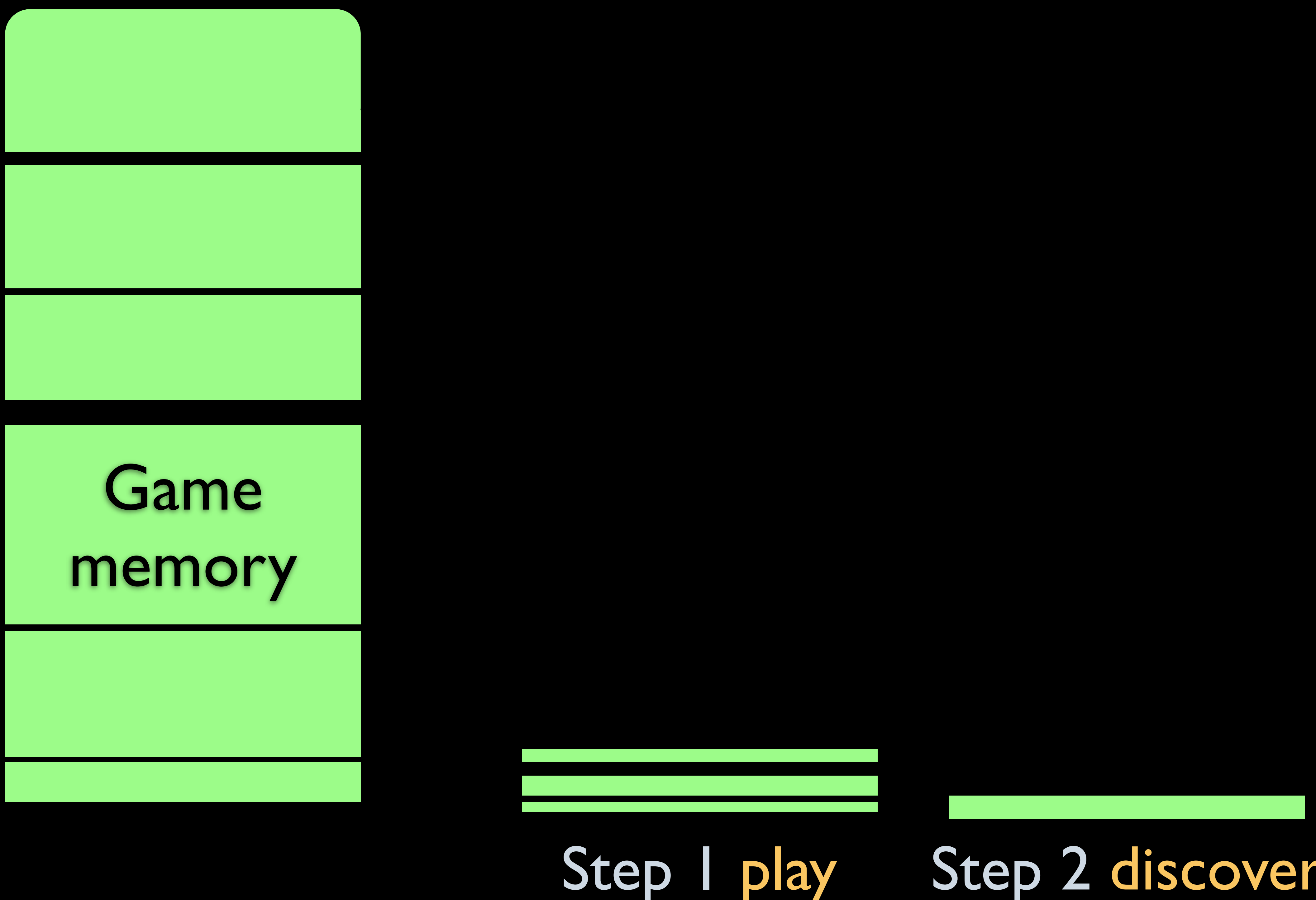


Reducing memory

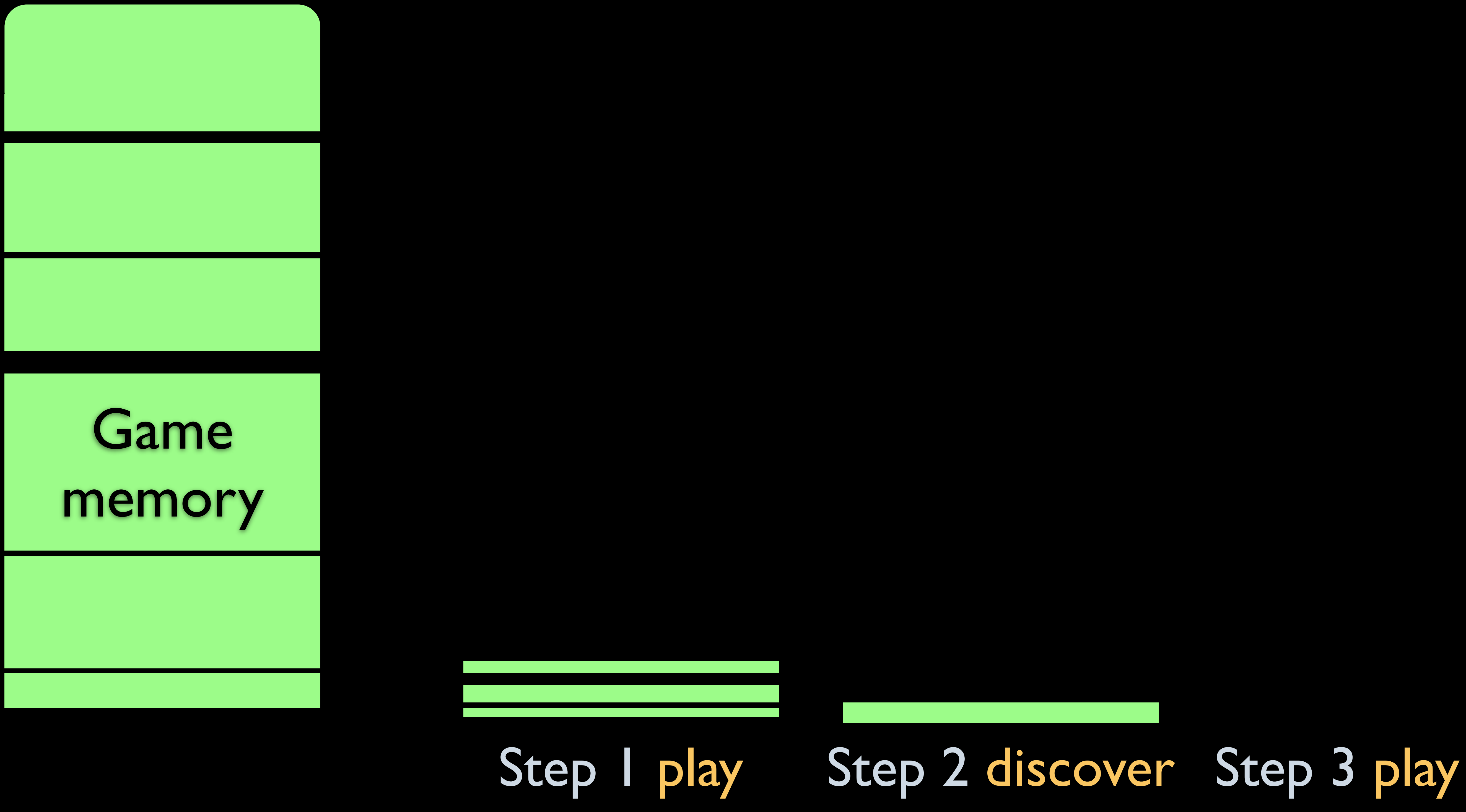


Step 1 play   Step 2 discover

Reducing memory



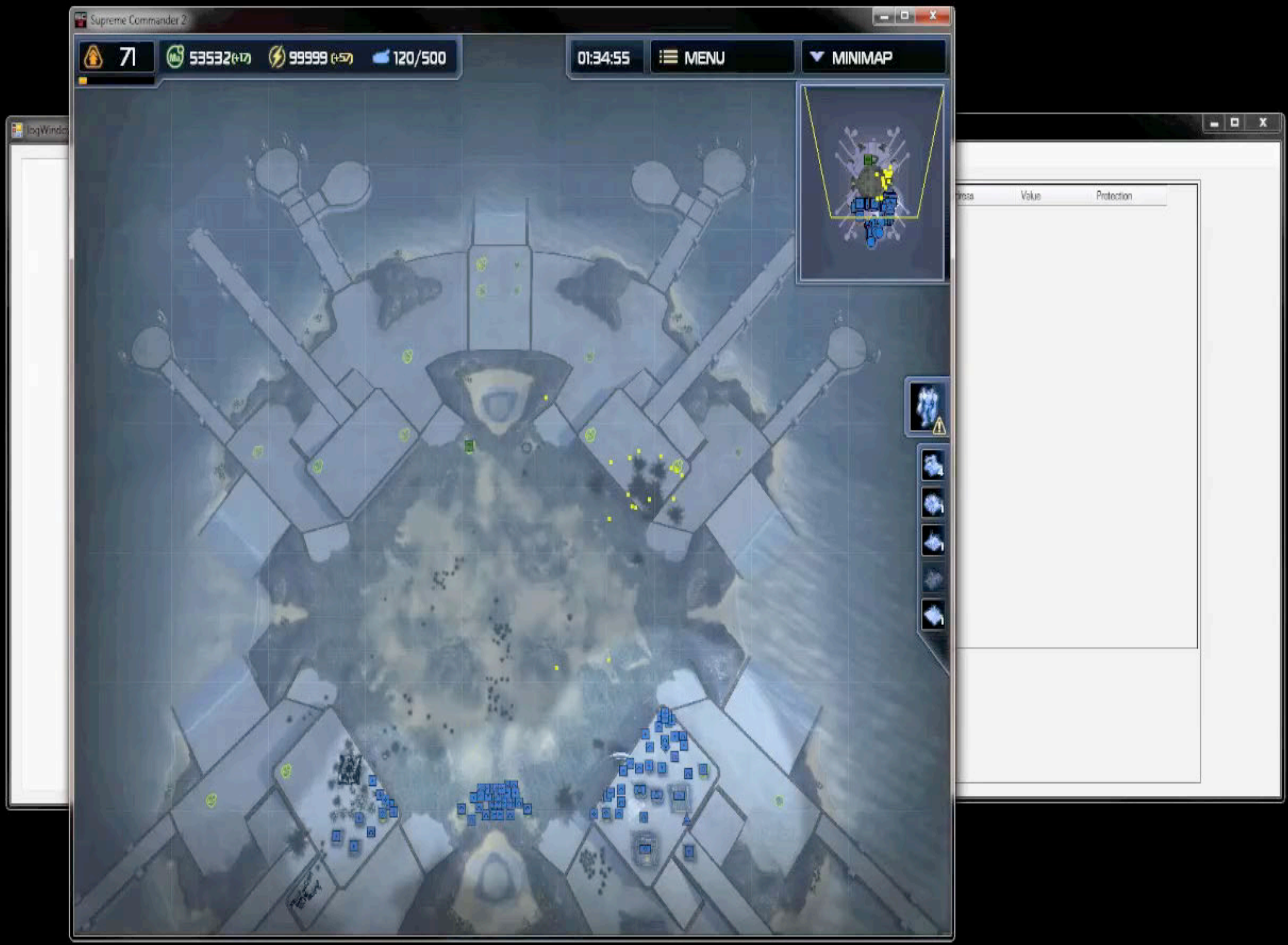
Reducing memory



Reducing memory

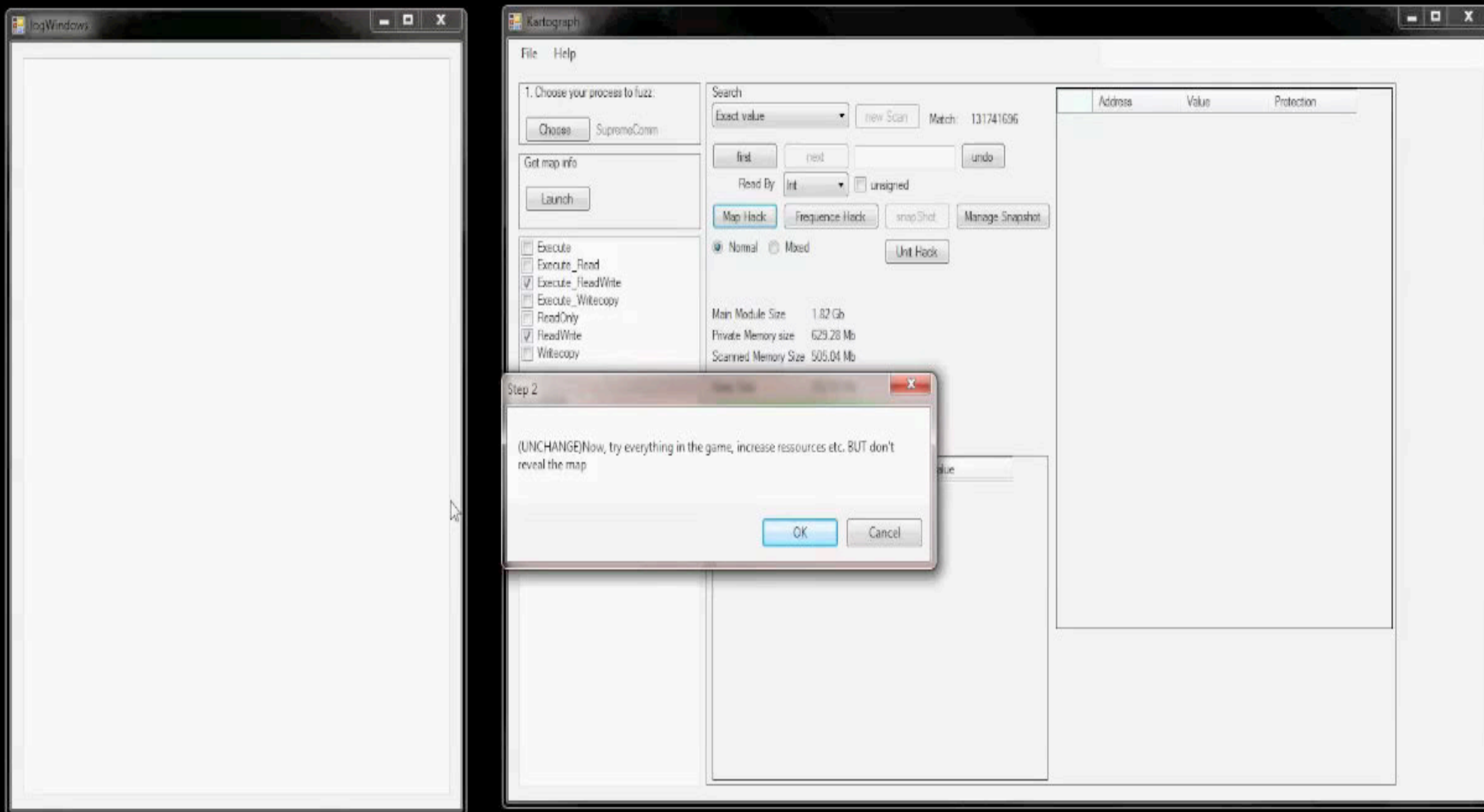
Reducing memory

Acquiring the game's memory



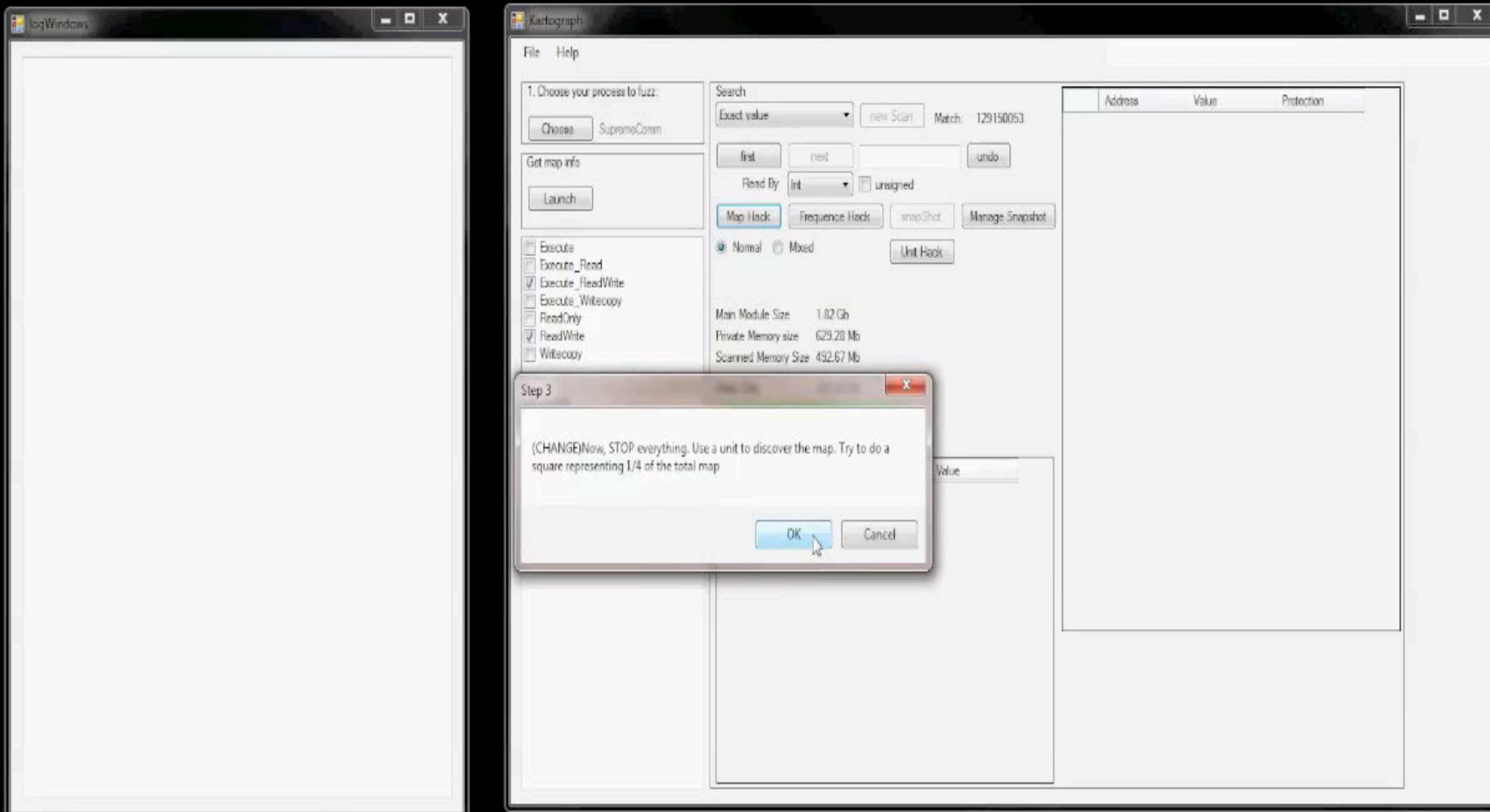
Supreme Commander 2
71
53532(+17)
99999 (+57)
120/500
01:34:55
MENU
MINIMAP
Value
Protection

Step 1
Removing unrelated memory

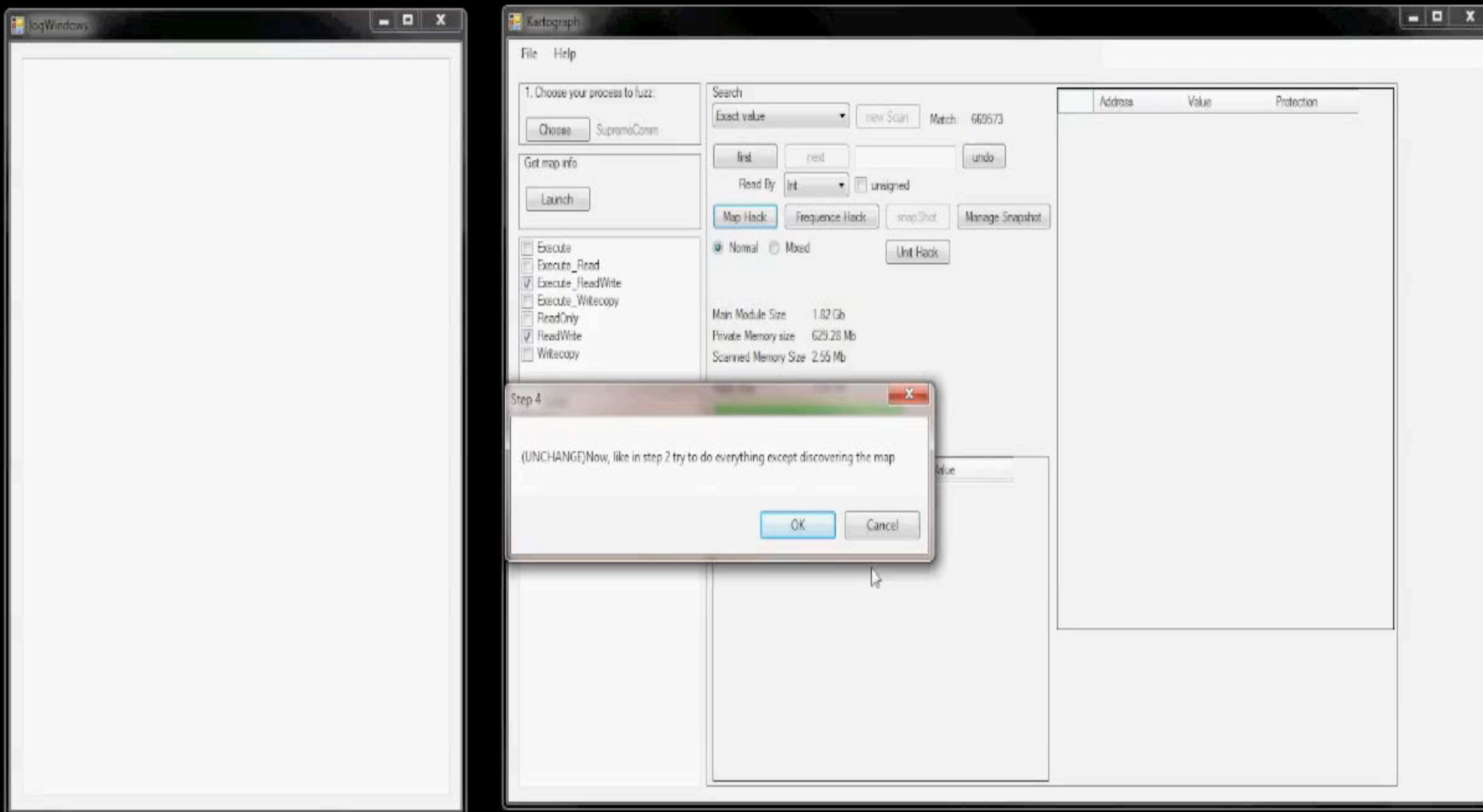

logWindows
Kartograph
File
Help
1. Choose your process to fuzz:
Choose
SupremeComm
Get map info
Launch
Execute
Execute_Read
Execute_ReadWrite
Execute_Writecopy
ReadOnly
ReadWrite
Writecopy
Search
Exact value
new Scan
Match:
131741696
first
next
undo
Read By
Int
unsigned
Map Hack
Frequence Hack
snapShot
Manage Snapshot
Normal
Mixed
Unit Hack
Main Module Size
1.82 Gb
Private Memory size
629.28 Mb
Scanned Memory Size
505.04 Mb
Address
Value
Protection
Step 2
(UNCHANGE)Now, try everything in the game, increase ressources etc. BUT don't reveal the map
OK
Cancel

Step 2

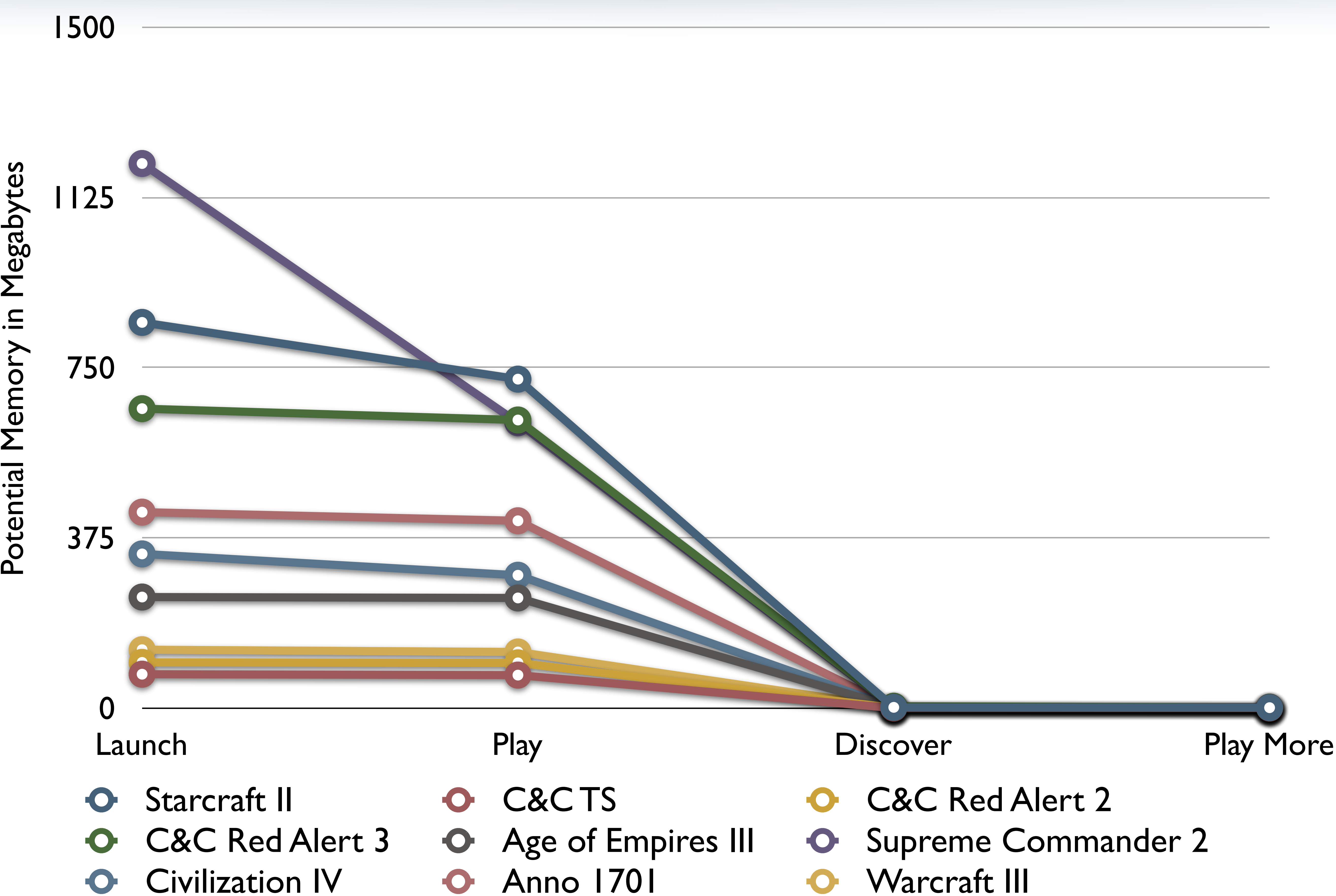
Discovering the map and keeping relevant memory


logWindows
Kartograph
File
Help
1. Choose your process to fuzz:
Choose
SupremeComm
Get map info
Launch
Execute
Execute_Read
Execute_ReadWrite
Execute_Writecopy
ReadOnly
ReadWrite
Writecopy
Search
Exact value
new Scan
Match: 129150053
first
next
undo
Read By
Int
unsigned
Map Hack
Frequence Hack
snapShot
Manage Snapshot
Normal
Mixed
Unit Hack
Main Module Size 1.82 Gb
Private Memory size 629.28 Mb
Scanned Memory Size 492.67 Mb
Address
Value
Protection
Value
Step 3
(CHANGE)Now, STOP everything. Use a unit to discover the map. Try to do a square representing 1/4 of the total map
OK
Cancel

Step 3
Removing more unrelated memory


logWindows
Kartograph
File
Help
1. Choose your process to fuzz:
Choose
SupremoComm
Get map info
Launch
Execute
Execute_Read
Execute_ReadWrite
Execute_Writecopy
ReadOnly
ReadWrite
Writecopy
Search
Exact value
new Scan
Match:
669573
first
next
undo
Read By
Int
unsigned
Map Hack
Frequence Hack
snapShot
Manage Snapshot
Normal
Mixed
Unit Hack
Main Module Size
1.82 Gb
Private Memory size
629.28 Mb
Scanned Memory Size
2.55 Mb
Address
Value
Protection
Step 4
(UNCHANGE)Now, like in step 2 try to do everything except discovering the map
OK
Cancel

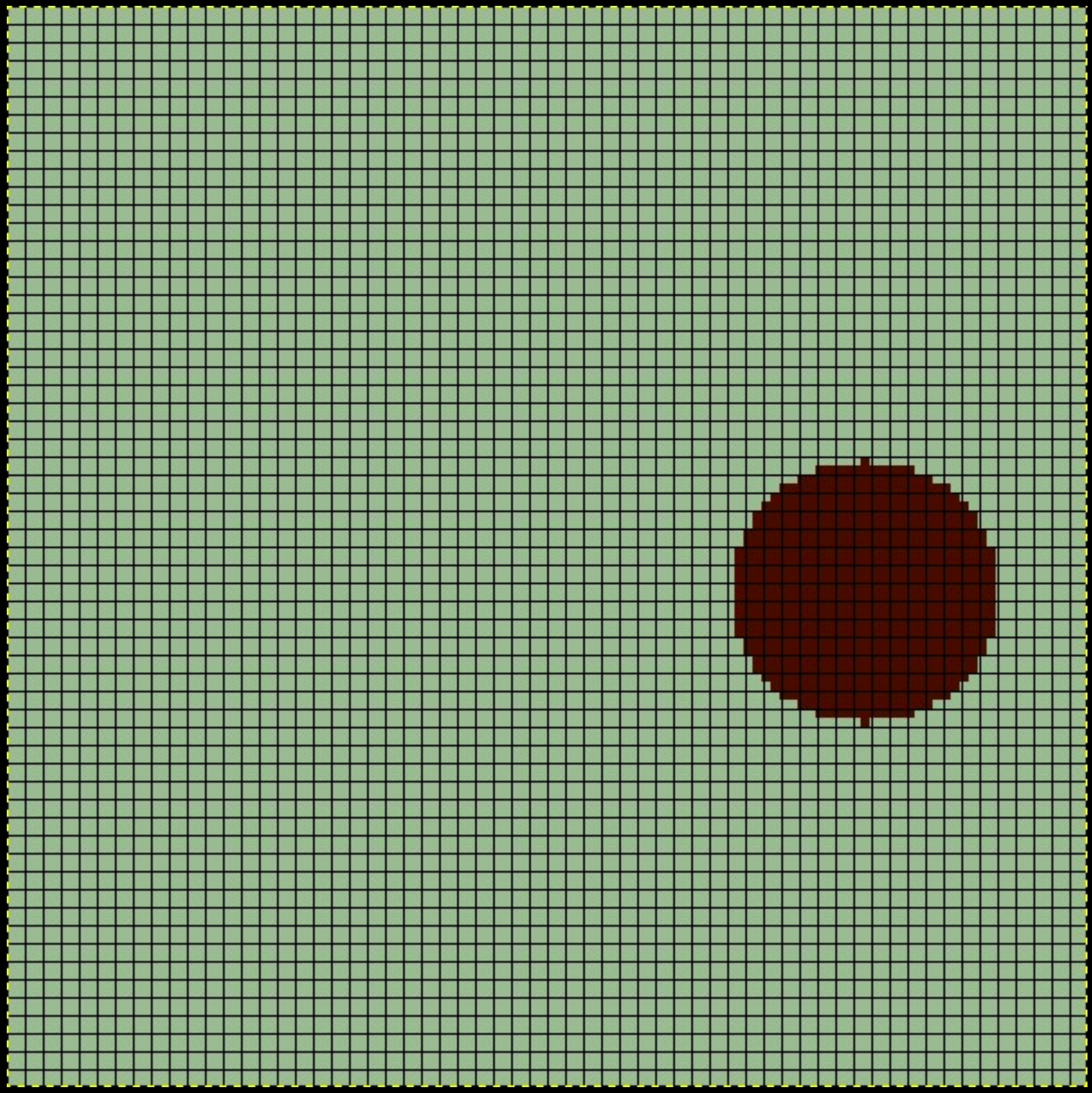
Memory reduction algorithm efficiency

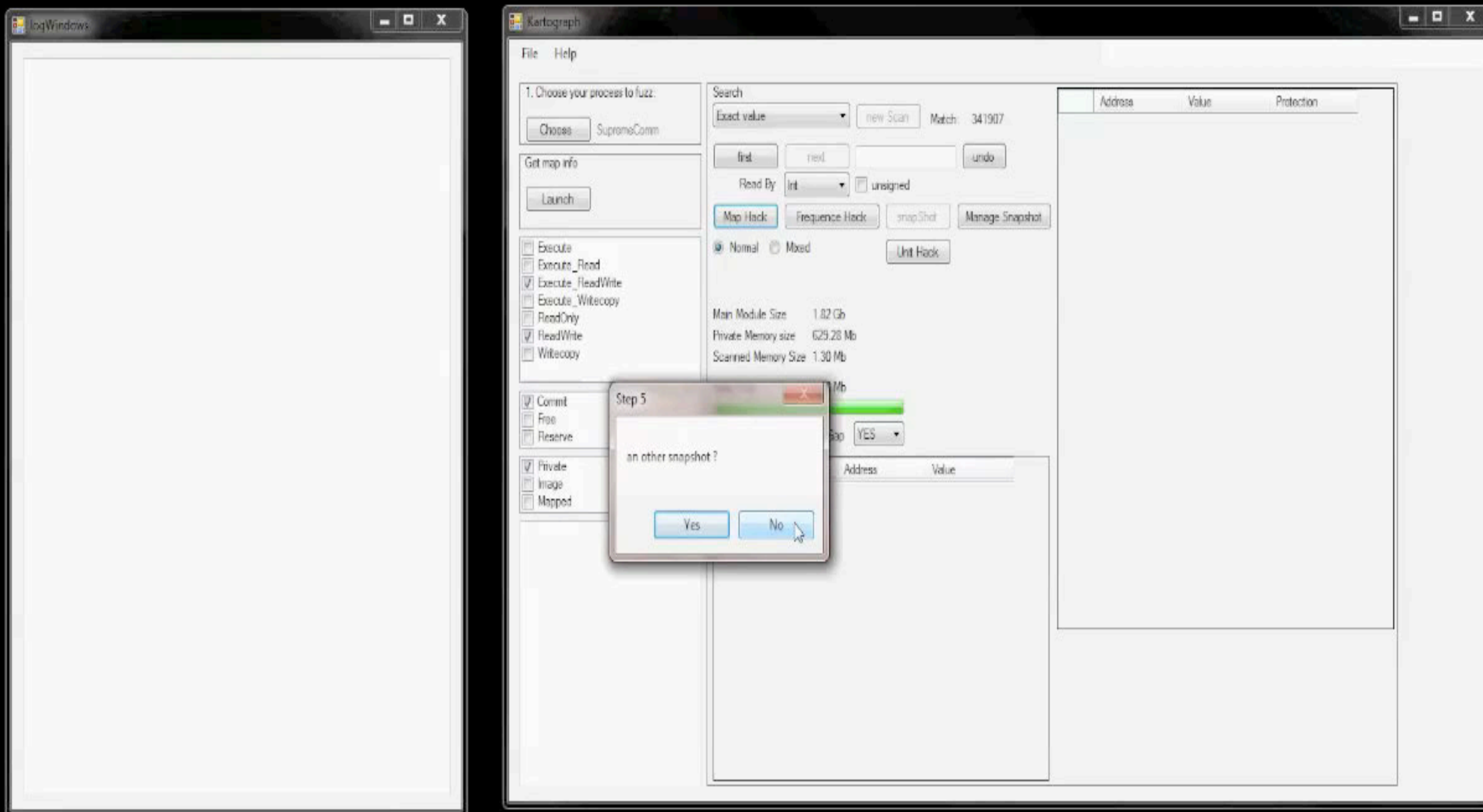


Step 4
Finding the map in the remaining memory

Working assumption

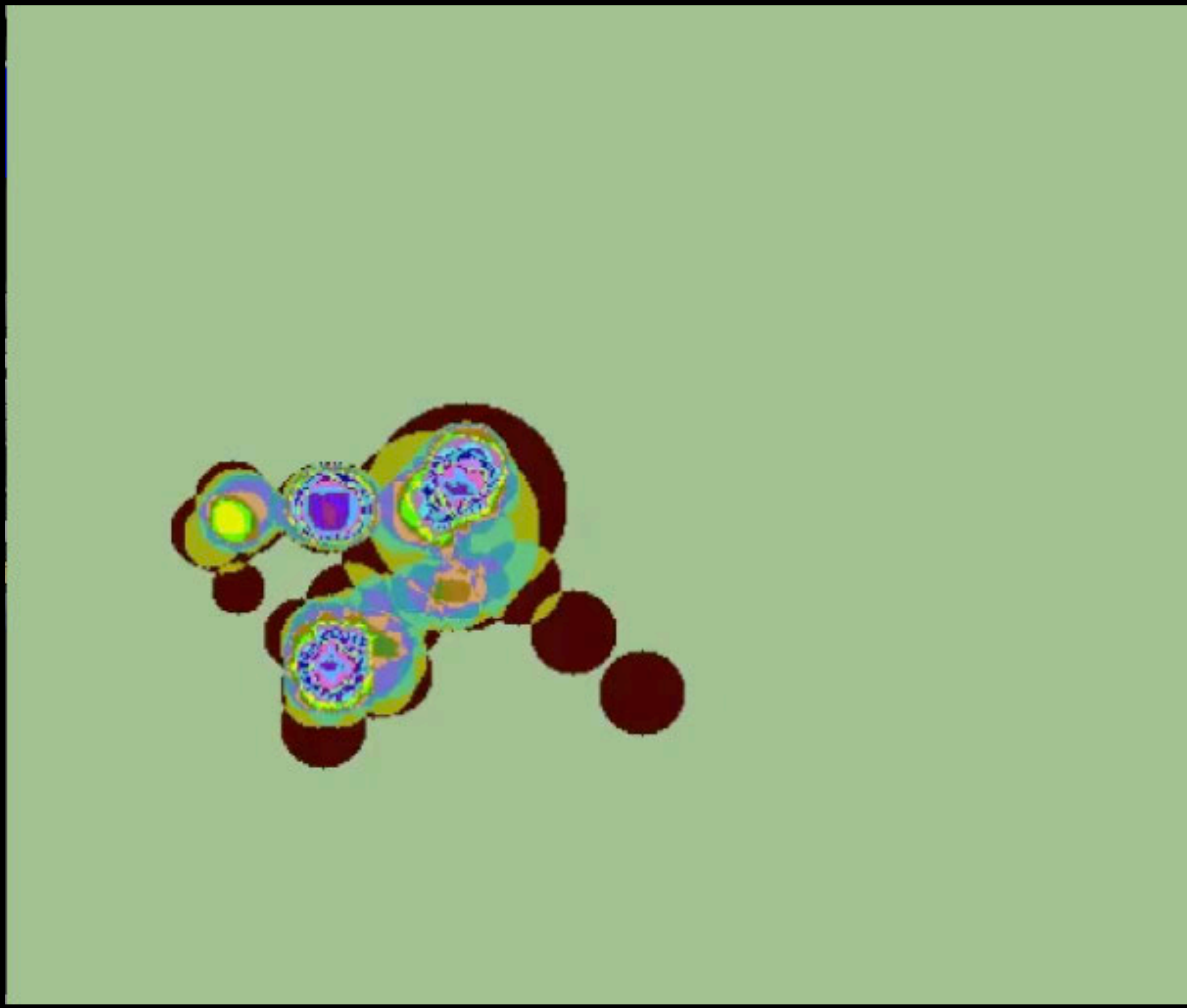
Working assumption




logWindows
Kartograph
File
Help
1. Choose your process to fuzz:
Choose
SupremeComm
Get map info
Launch
Execute
Execute_Read
Execute_ReadWrite
Execute_Writecopy
ReadOnly
ReadWrite
Writecopy
Commit
Free
Reserve
Private
Image
Mapped
Search
Exact value
new Scan
Match:
341907
first
next
undo
Read By
Int
unsigned
Map Hack
Frequence Hack
snapShot
Manage Snapshot
Normal
Mixed
Unit Hack
Main Module Size
1.82 Gb
Private Memory size
629.28 Mb
Scanned Memory Size
1.30 Mb
YES
Address
Value
Protection
Step 5
an other snapshot ?
Yes
No

Step 5
Isolating the potential map

In game



In memory

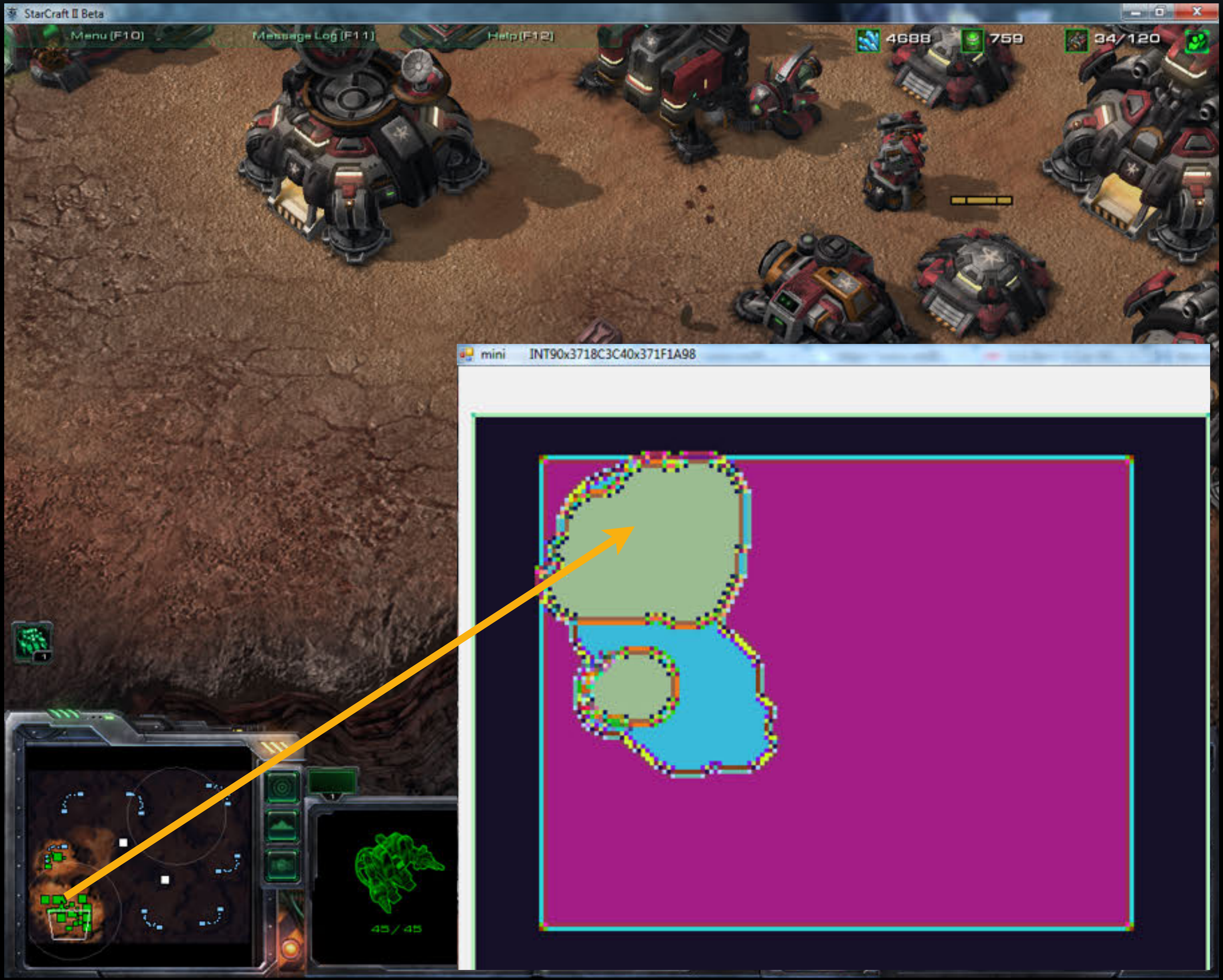
Step 6
Understanding the map's structure


Supreme Commander 2
80
56985 (+16)
99999 (+57)
121/500
01:38:23
MENU
MINIMAP
File
Before INT
Address
Value
Protection

Step 8
Rewriting game memory for fun and profit

Starcraft 2 mini map

Starcraft 2 mini map



Unexpected effects


+88
20
Santa Maria

Defense requirements

The passive eavesdropping adversary

- Complete control of his machine
- Can understand the game memory structure
- Can identify and parse any data structure

Attacker objective definition

We say that a passive attacker defeats the game if the attacker can write a program P that reveals information about the opponent beyond what is revealed by the game's rules. Otherwise we say that the game is secure against a passive adversary.

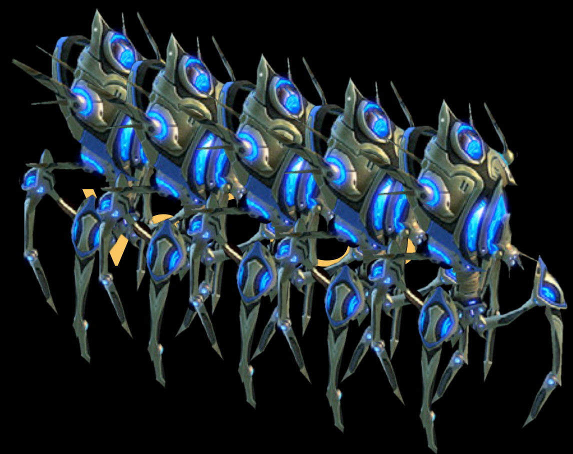
Making games secure

- Use two-party (multi-party) cryptography protocol to ensure that the memory contains only the data the user need

Set intersection protocol

Alice

Bob

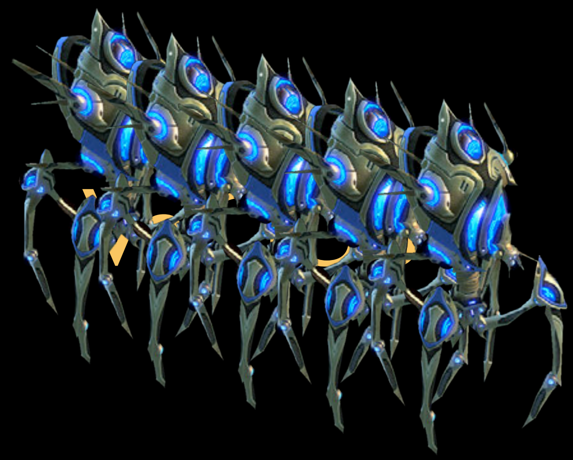


Set intersection protocol

Alice

Va

Bob



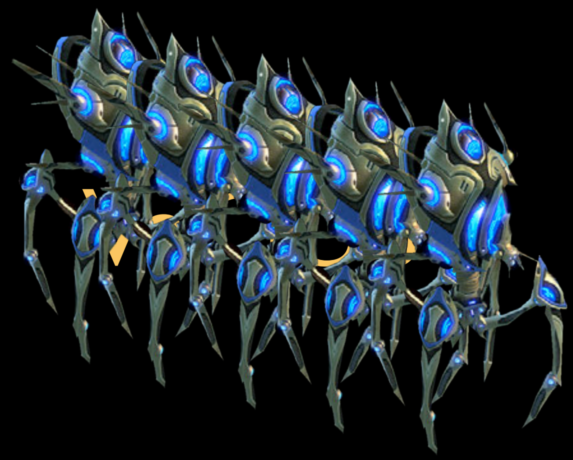
Set intersection protocol

Alice

Va

Bob

Va



Set intersection protocol

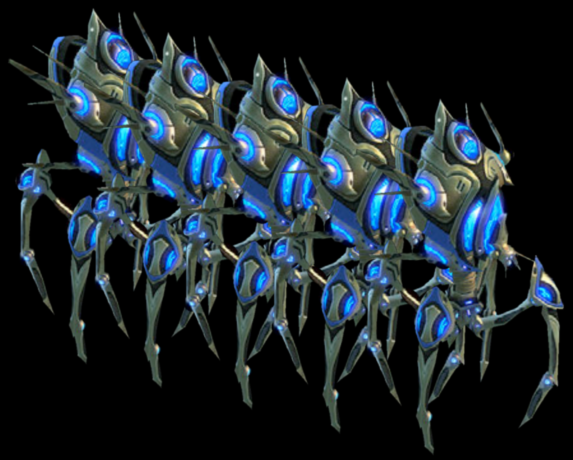
Alice

Va

Bob

Va

Va $\cap$ Ub



Set intersection protocol

Alice

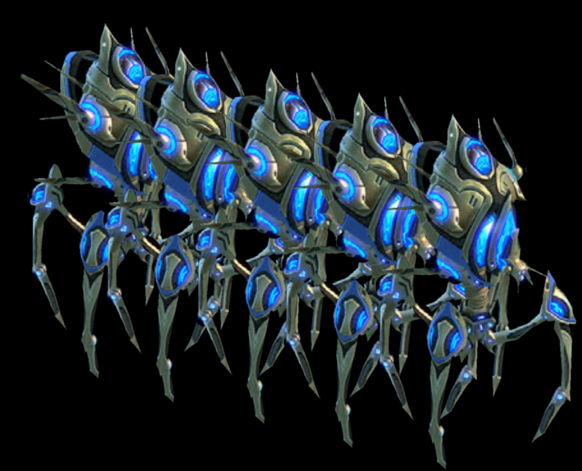
V_a

$V_a \cap U_b$

Bob

V_a

$V_a \cap U_b$



Constraints

- Bob learn nothing about Va
- Alice learn nothing about Ub other than $Va \cap Ub$

Constraints

- Bob learn nothing about Va
- Alice learn nothing about Ub other than Va$\cap$Ub

Computing with these constraints is called the

oblivious intersection set problem

Chosen oblivisous intersection protocol

- Due to Jarecki and Liu
- Use an oblivious function evaluation as sub-protocol
- Adapted and optimized for our problem

For one unit

Alice

unit key:

$$o_k(v) := H_1(v)^k \in \mathbb{G}$$

Bob

For one unit

Alice

unit key:

$$o_k(v) := H_1(v)^k \in \mathbb{G}$$

Bob

$$\xrightarrow{H_1(v)^r}$$

For one unit

Alice

unit key:

$$o_k(v) := H_1(v)^k \in \mathbb{G}$$

Bob

$$\xrightarrow{H_1(v)^r}$$

$$\xleftarrow{H_1(v)^{rk}}$$

For one unit

Alice

unit key:

$$o_k(v) := H_1(v)^k \in \mathbb{G}$$

Bob

$$\xrightarrow{\quad H_1(v)^r \quad}$$

$$H_1(v)^k = H_1(v)^{rkr^{-1}} \xleftarrow{\quad H_1(v)^{rk} \quad}$$

Multi-units

Alice

$V_A \xrightarrow{v_1^{r_1}, \ldots, v_n^{r_n}} U_B$

k

$\xleftarrow{v_1^{kr_1}, \ldots, v_n^{kr_n}}$

encrypted chunks from U_B

Bob

Chaff

- The basic protocol leaks information
  - The number of Alice visible cell
  - The number of bob unit (nb encrypted chunk)
- Both are resolved by adding a chaff
  - Bob and Alice add random values that "pad" the data

Challenge

Design a protocol that is fast enough so the added game latency is imperceptible to users.

Establishing a baseline

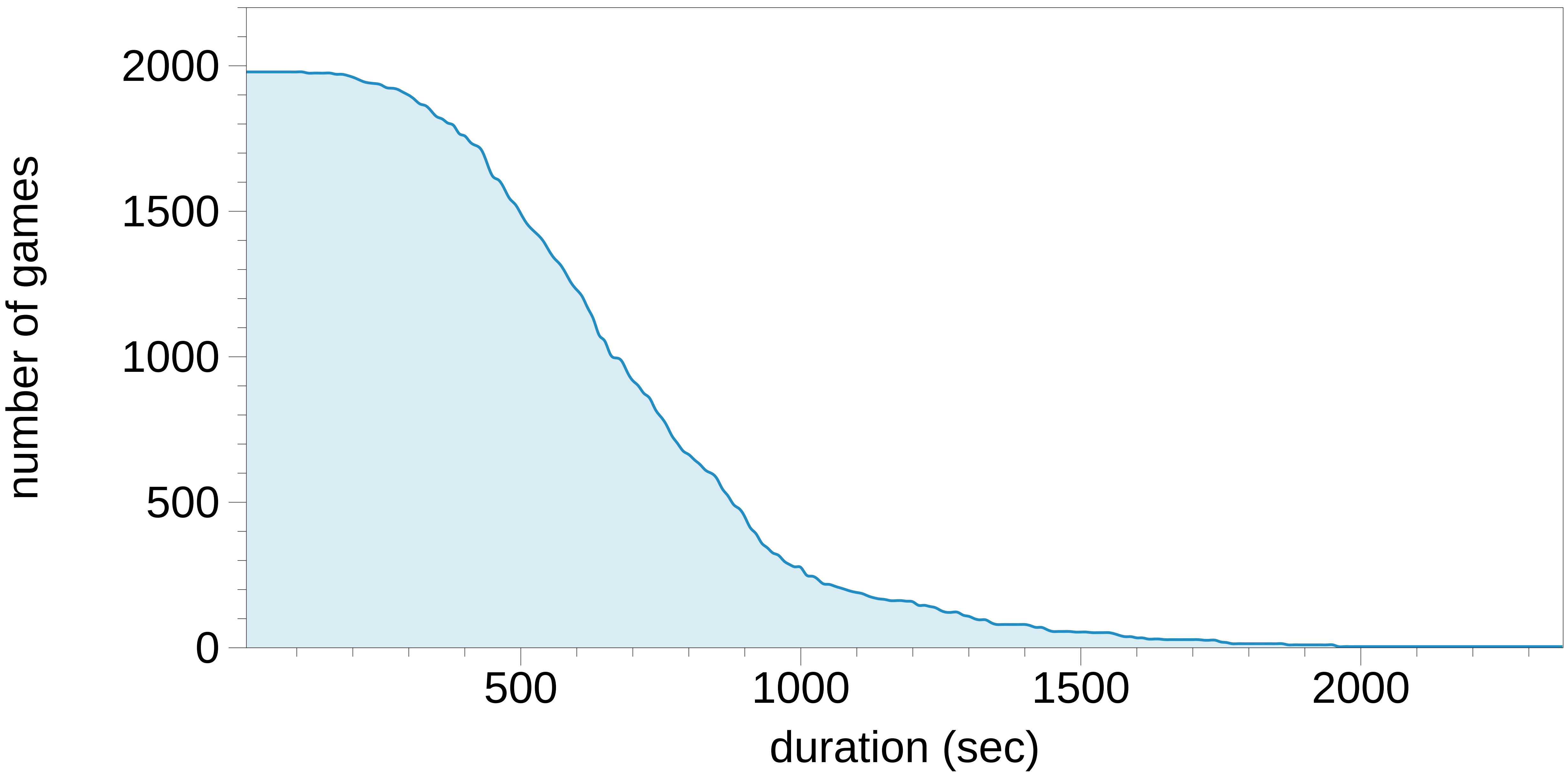
Methodology

- 1000 Starcraft 2 replays from pro-gamer
  - Game duration
  - Number of units by players
  - Number of visible cells
  - Number of actions by seconds
- Map playable size:
  - min 15180 cells
  - max 24640 cells

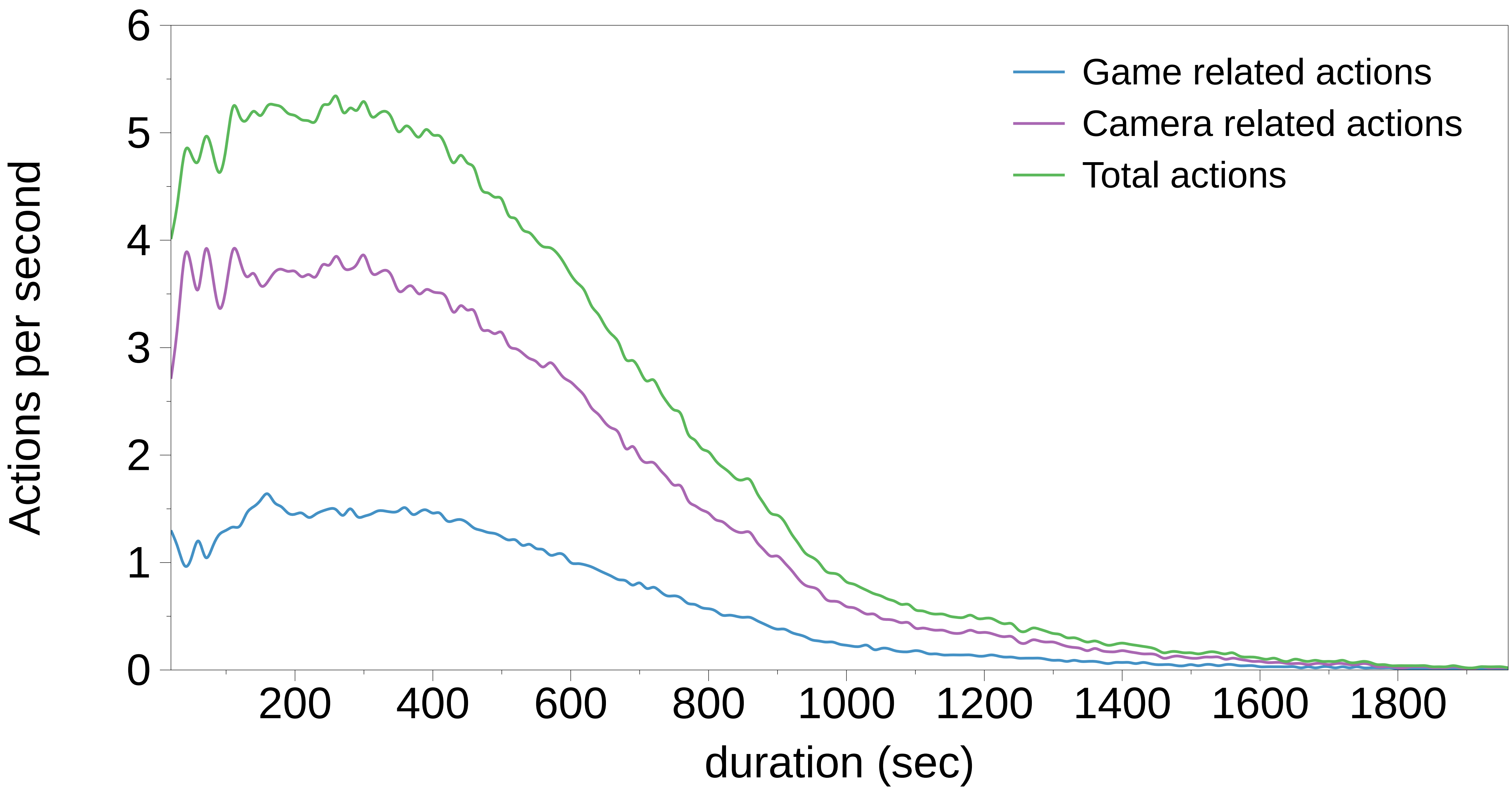
Analysis difficulty

1. Replays use a proprietary file format (MQP)
    - Wrote a custom parser
2. Replay only record players actions
    - Wrote a minimal game engine
    - return an upper-approximation

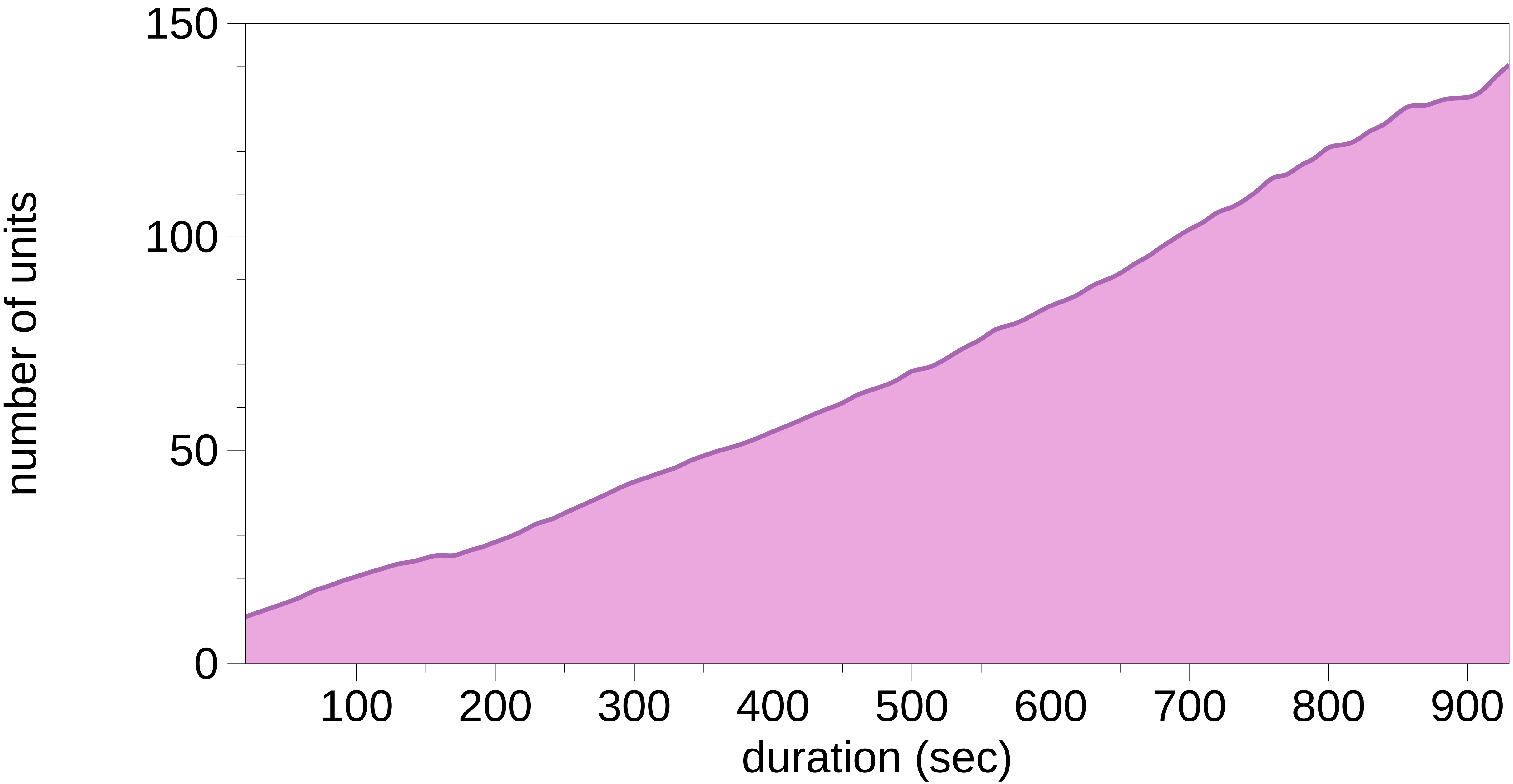
Game duration



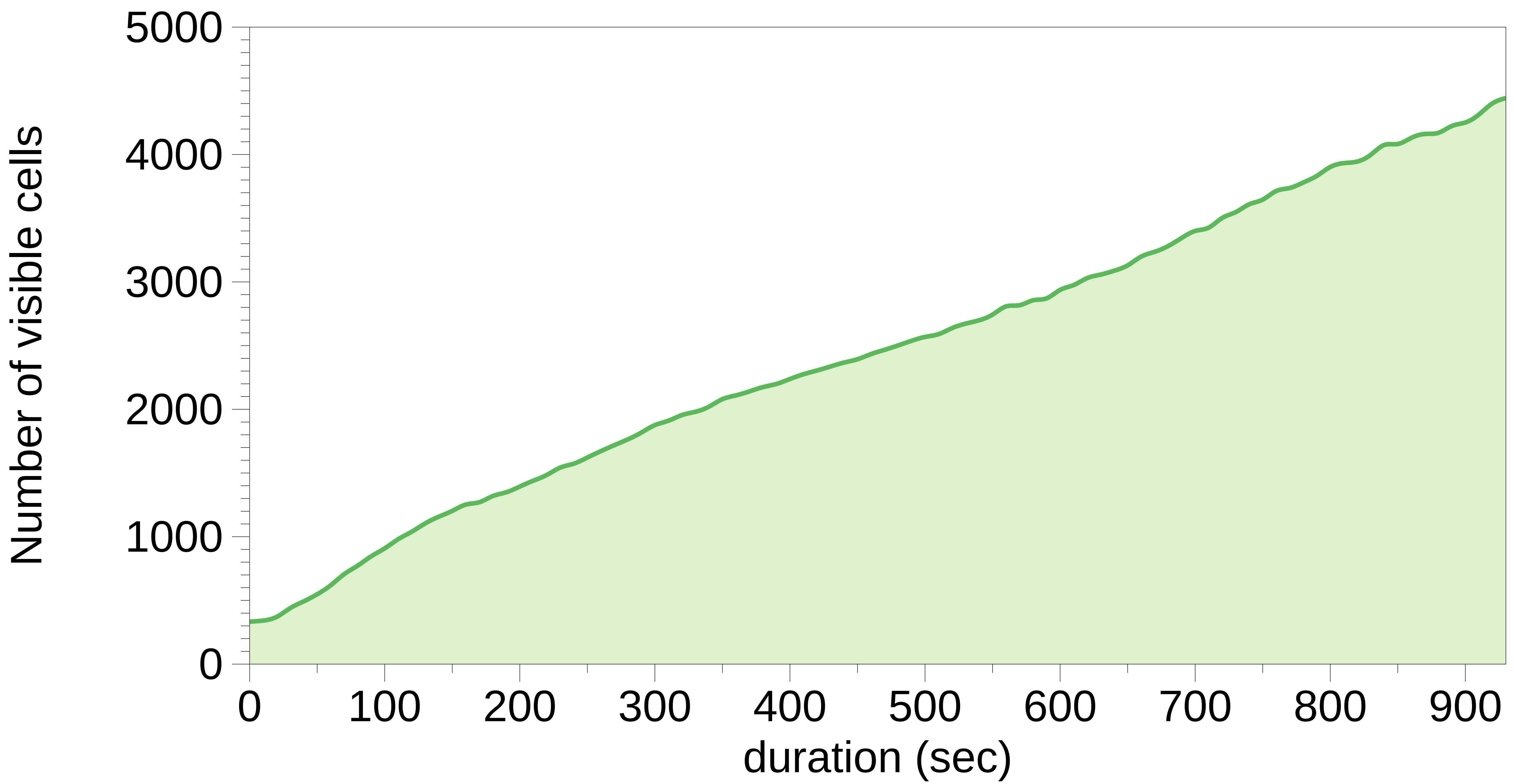
Actions per second



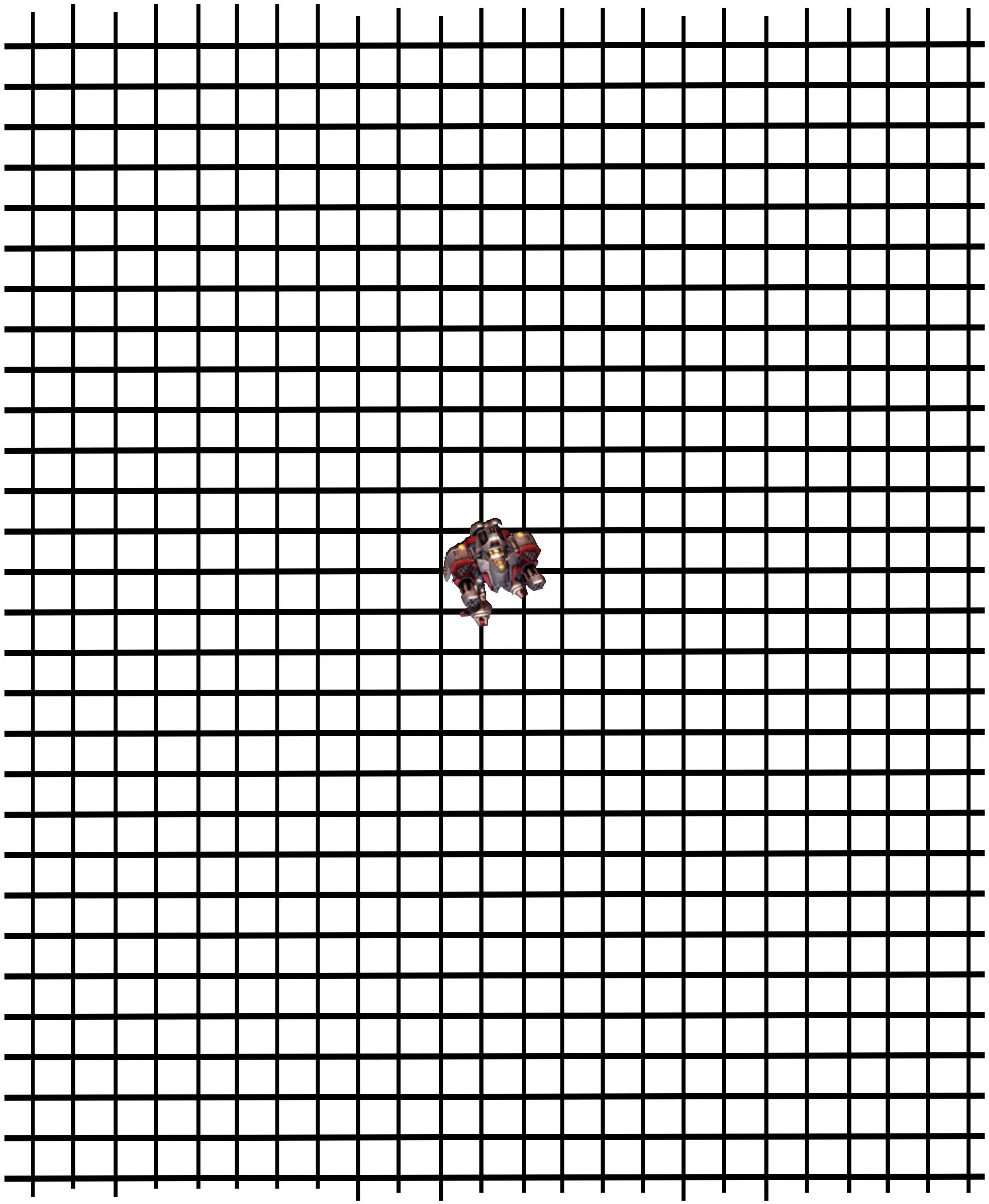
Units by duration



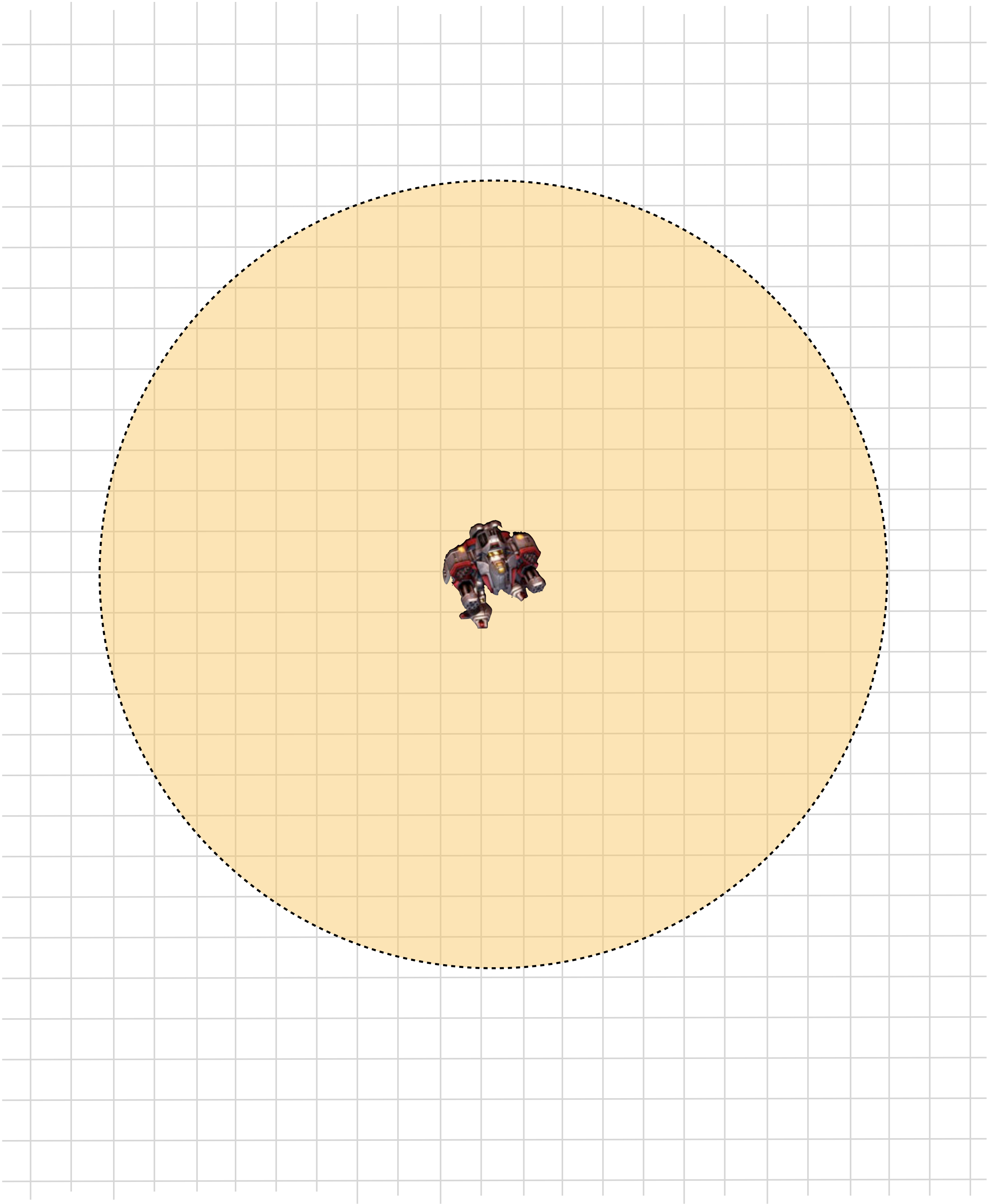
Map cell visible by duration



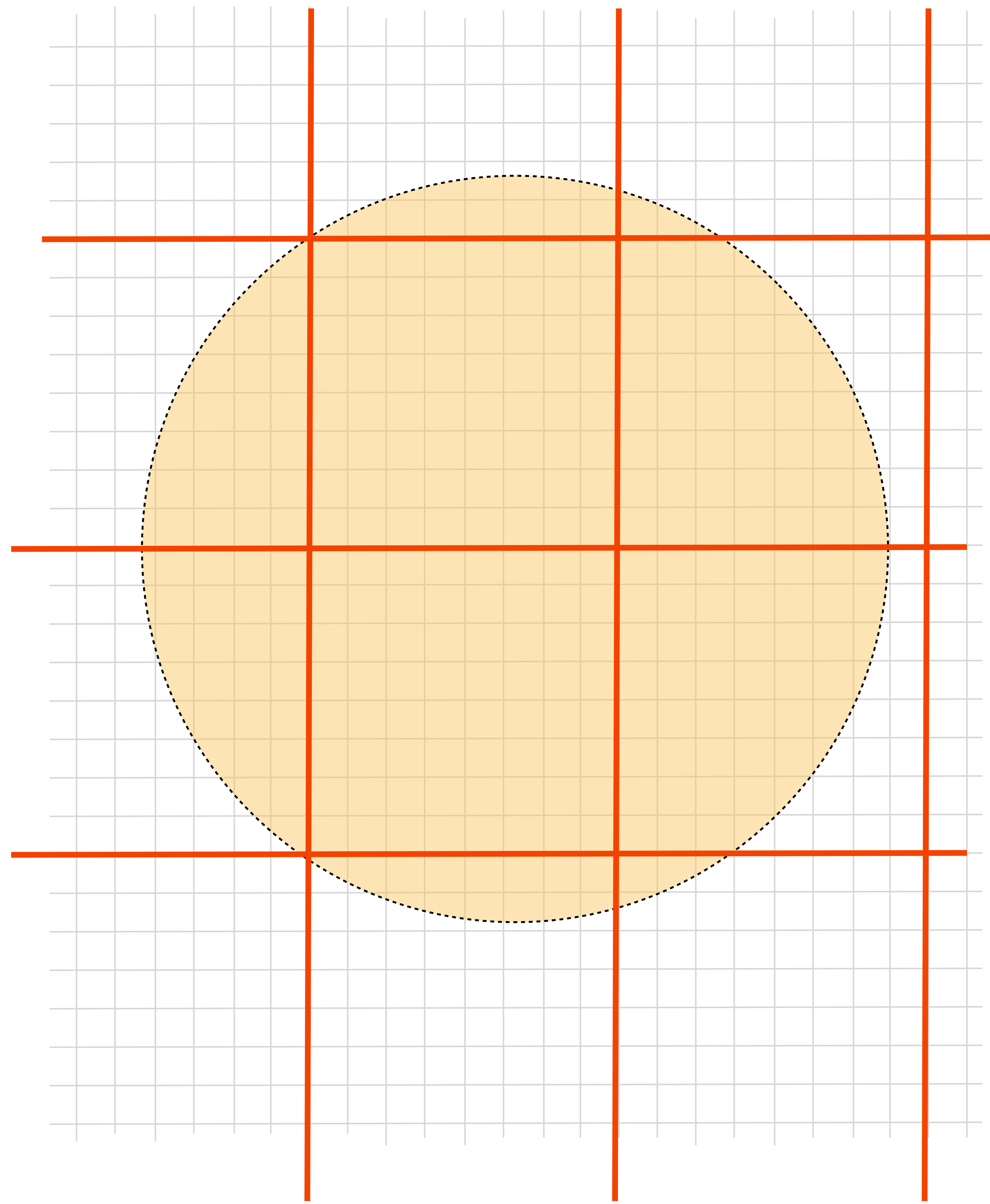
- Hypergrid: 4 grid instead of 1
  - 1x1cells
  - 2x2 cells
  - 3x3 cells
  - 4x4 cells
- Lest visible cells
- 4 times more units



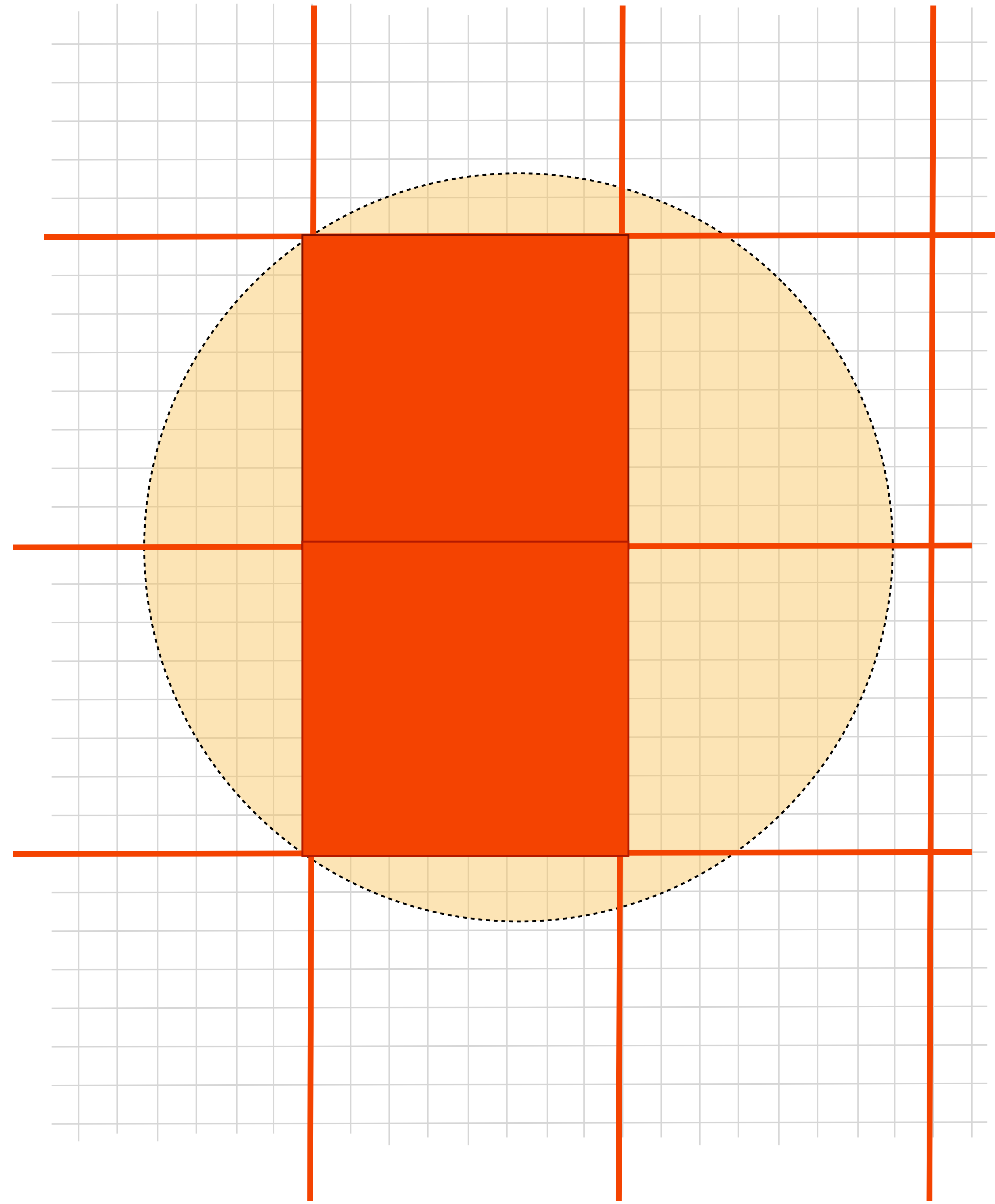
- Hypergrid: 4 grid instead of 1
  - 1x1cells
  - 2x2 cells
  - 3x3 cells
  - 4x4 cells
- Lest visible cells
- 4 times more units



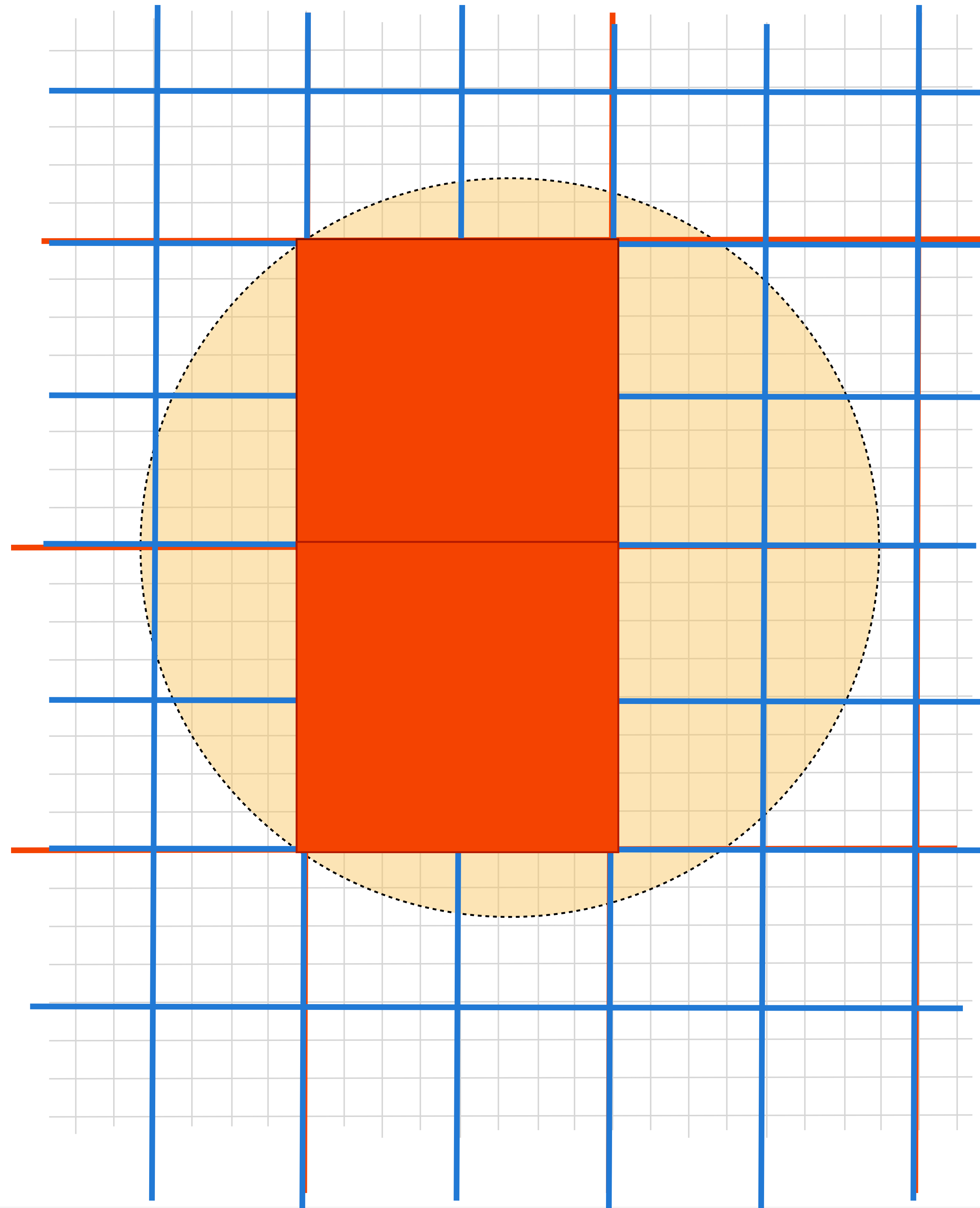
- Hypergrid: 4 grid instead of 1
  - 1x1cells
  - 2x2 cells
  - 3x3 cells
  - 4x4 cells
- Lest visible cells
- 4 times more units



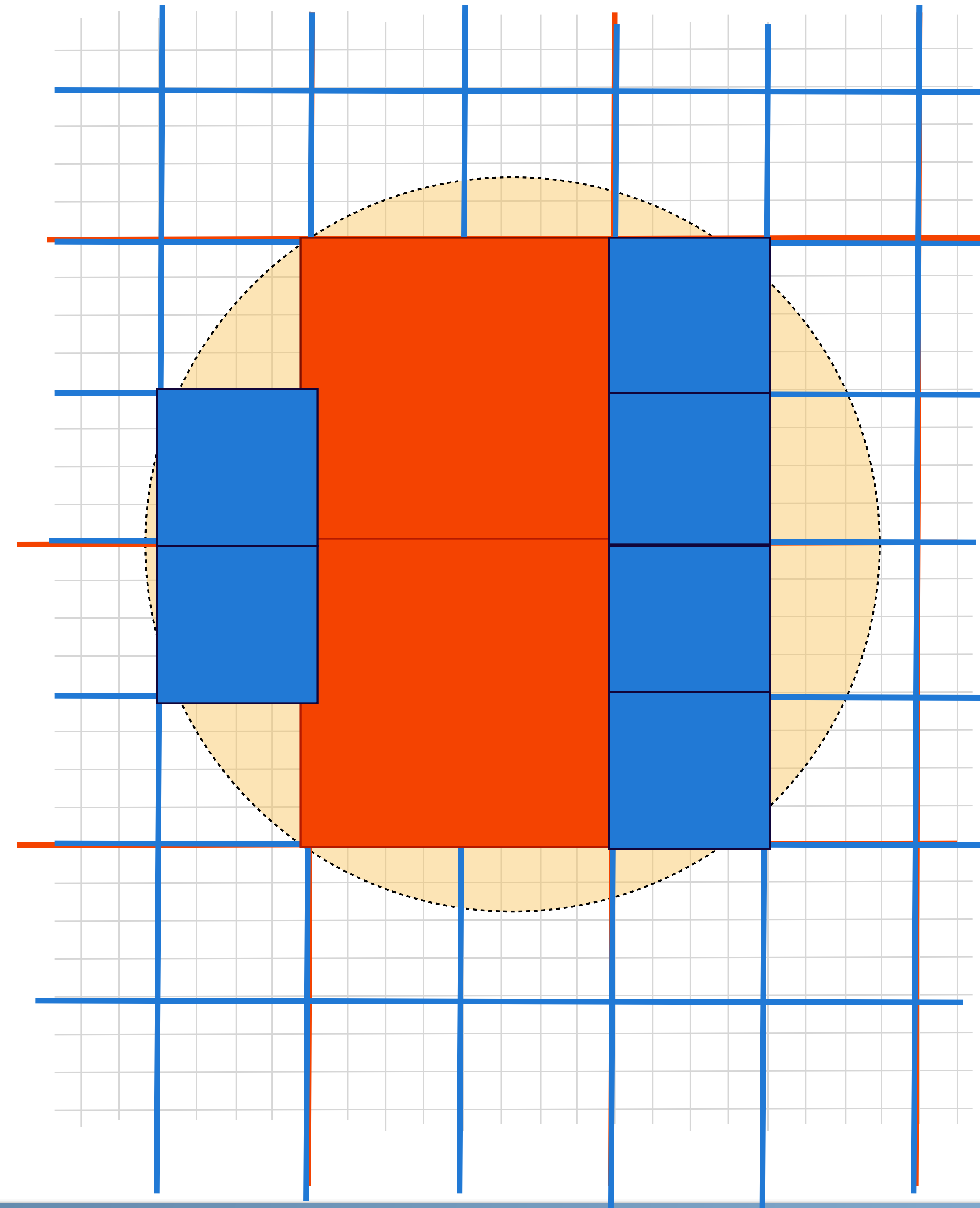
- Hypergrid: 4 grid instead of 1
  - 1x1cells
  - 2x2 cells
  - 3x3 cells
  - 4x4 cells
- Lest visible cells
- 4 times more units



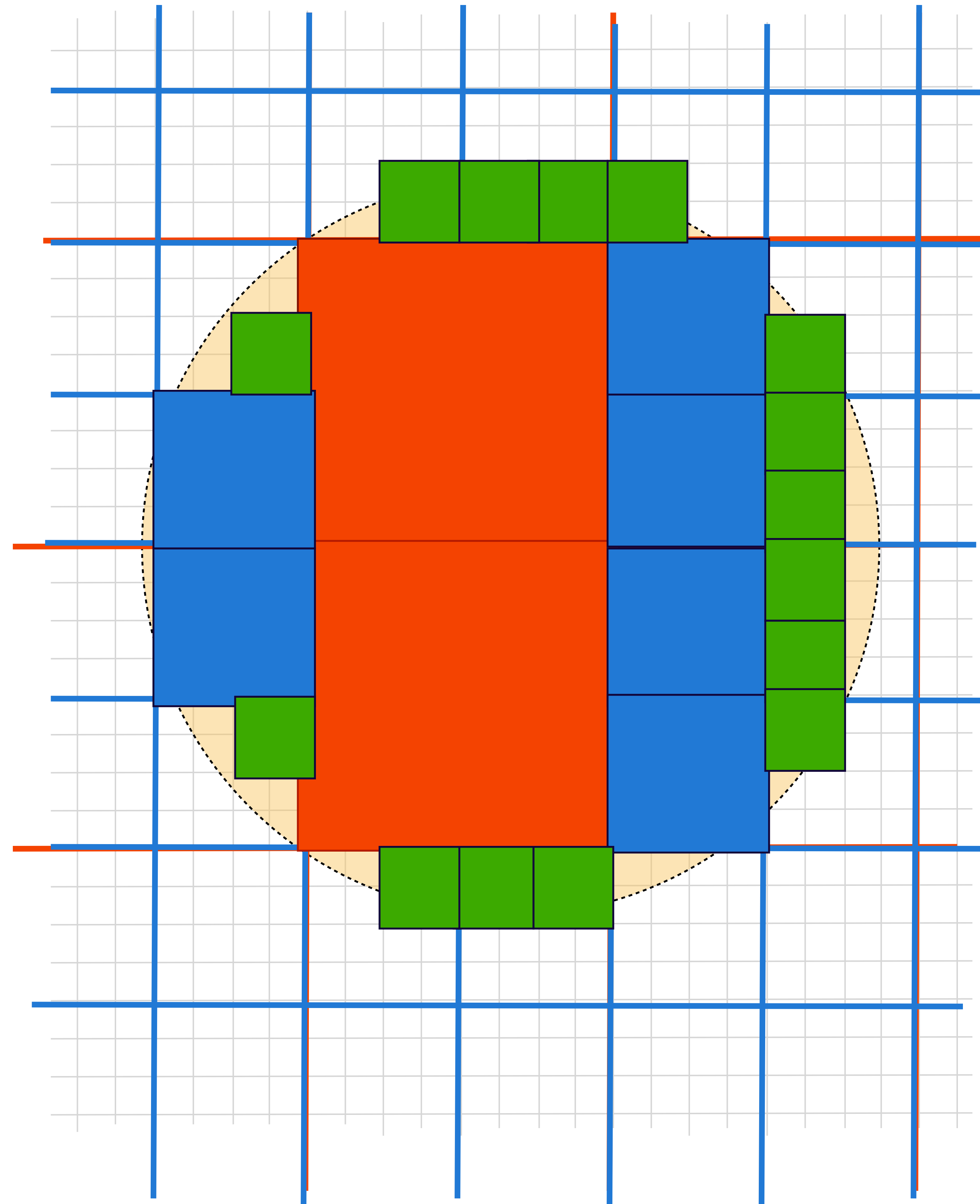
- Hypergrid: 4 grid instead of 1
  - 1x1cells
  - 2x2 cells
  - 3x3 cells
  - 4x4 cells
- Lest visible cells
- 4 times more units



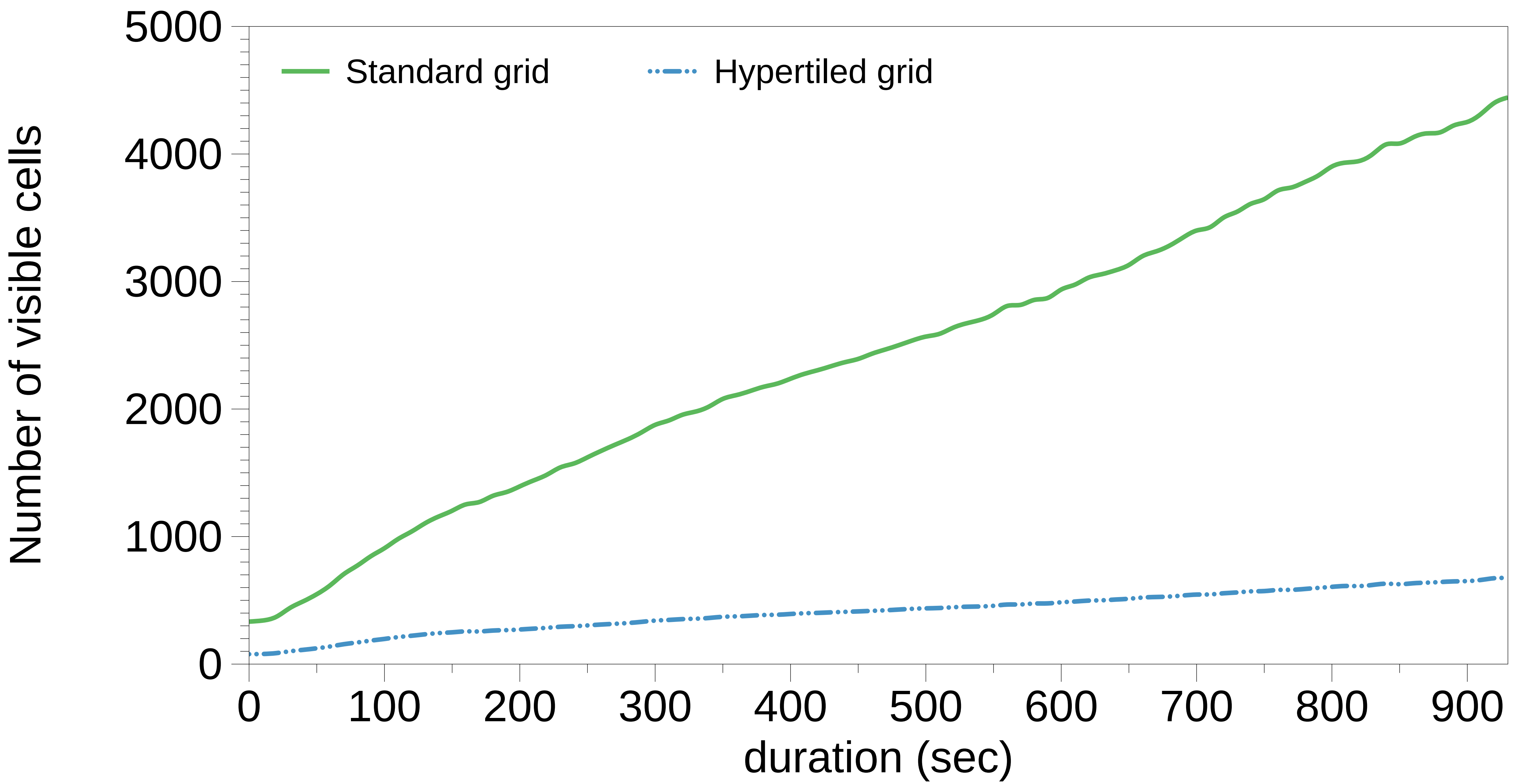
- Hypergrid: 4 grid instead of 1
  - 1x1cells
  - 2x2 cells
  - 3x3 cells
  - 4x4 cells
- Lest visible cells
- 4 times more units



- Hypergrid: 4 grid instead of 1
  - 1x1cells
  - 2x2 cells
  - 3x3 cells
  - 4x4 cells
- Lest visible cells
- 4 times more units



Impact of the hypertiled grid



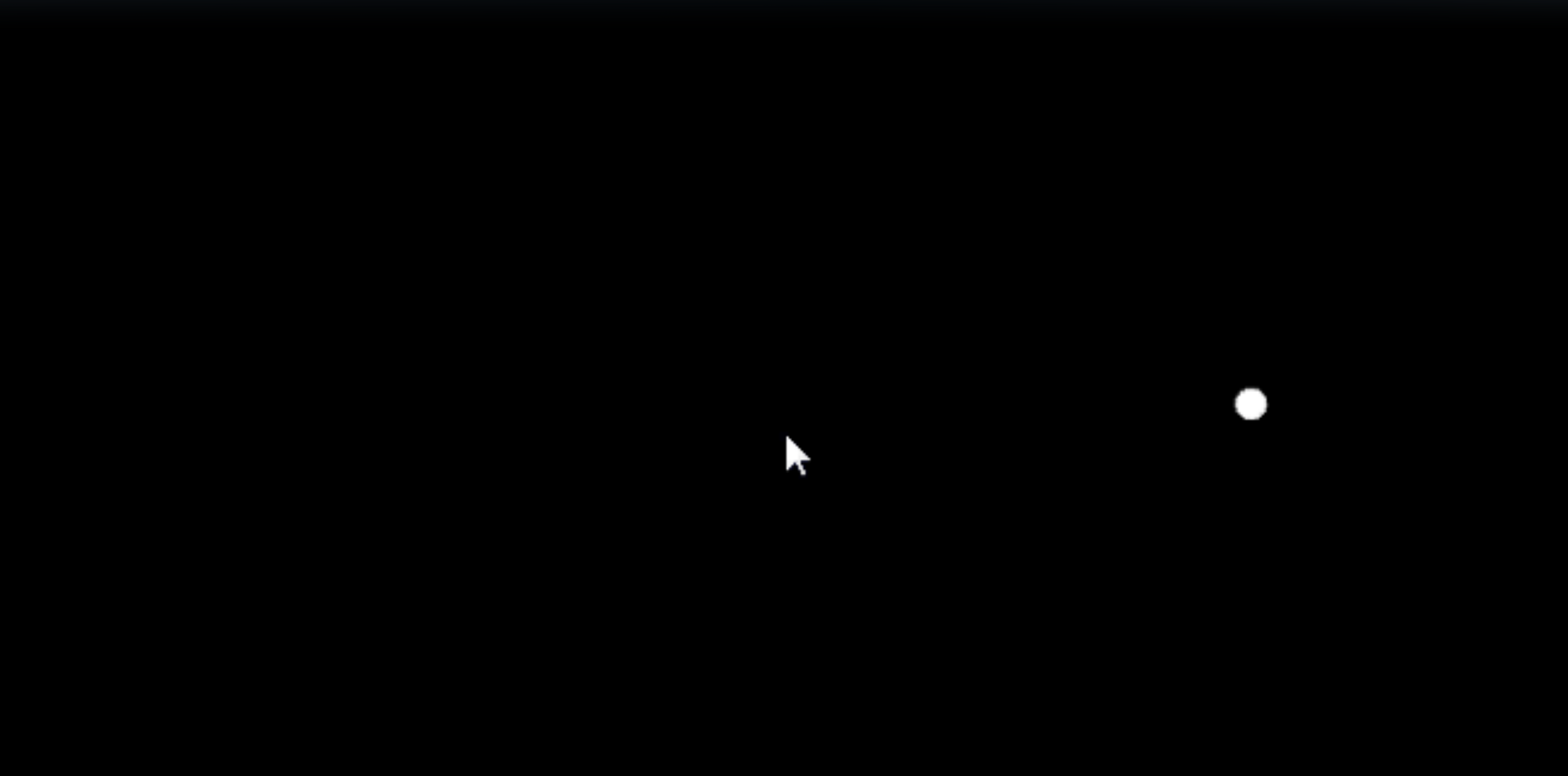
Open-Conflict Benchmark

$v \downarrow \quad u \rightarrow$	100	200	300	400	500
100	5ms	6ms	8ms	9ms	11ms
200	8ms	9ms	11ms	12ms	14ms
300	11ms	13ms	14ms	16ms	17ms
400	14ms	16ms	17ms	19ms	20ms
500	17ms	19ms	20ms	22ms	24ms

Conclusion

- Developed a generic method to perform memory based attack
- Established a defense performance baseline based on real world data
- Designed and implemented an oblivious set intersection protocol that prevents passive attacks
- Future work: defending on active attacks

Thank you !



Paper and video available from http://ly.tl/p19

Twitter: @elie

Finding units information

When things become harder

- Unit lists are very small
- Visualization won’t work this time to find it :(
- Solely based on memory shape analysis algorithms

Stack detection heuristics

- Only one new integer by unit
- Each integer is a valid pointer

Unit hack Step

Game memory

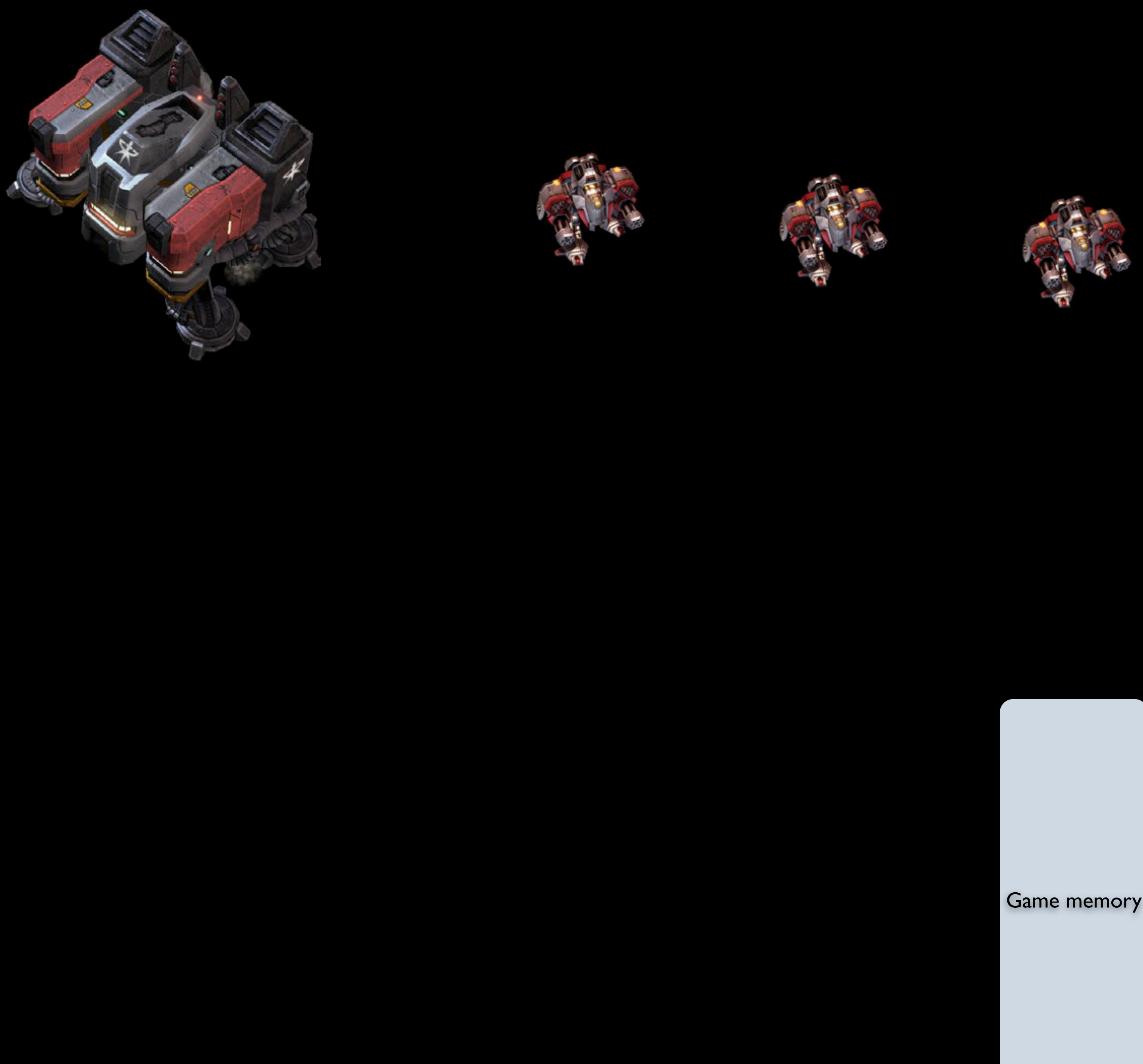
Unit hack Step

Game memory

Unit hack Step

Game memory

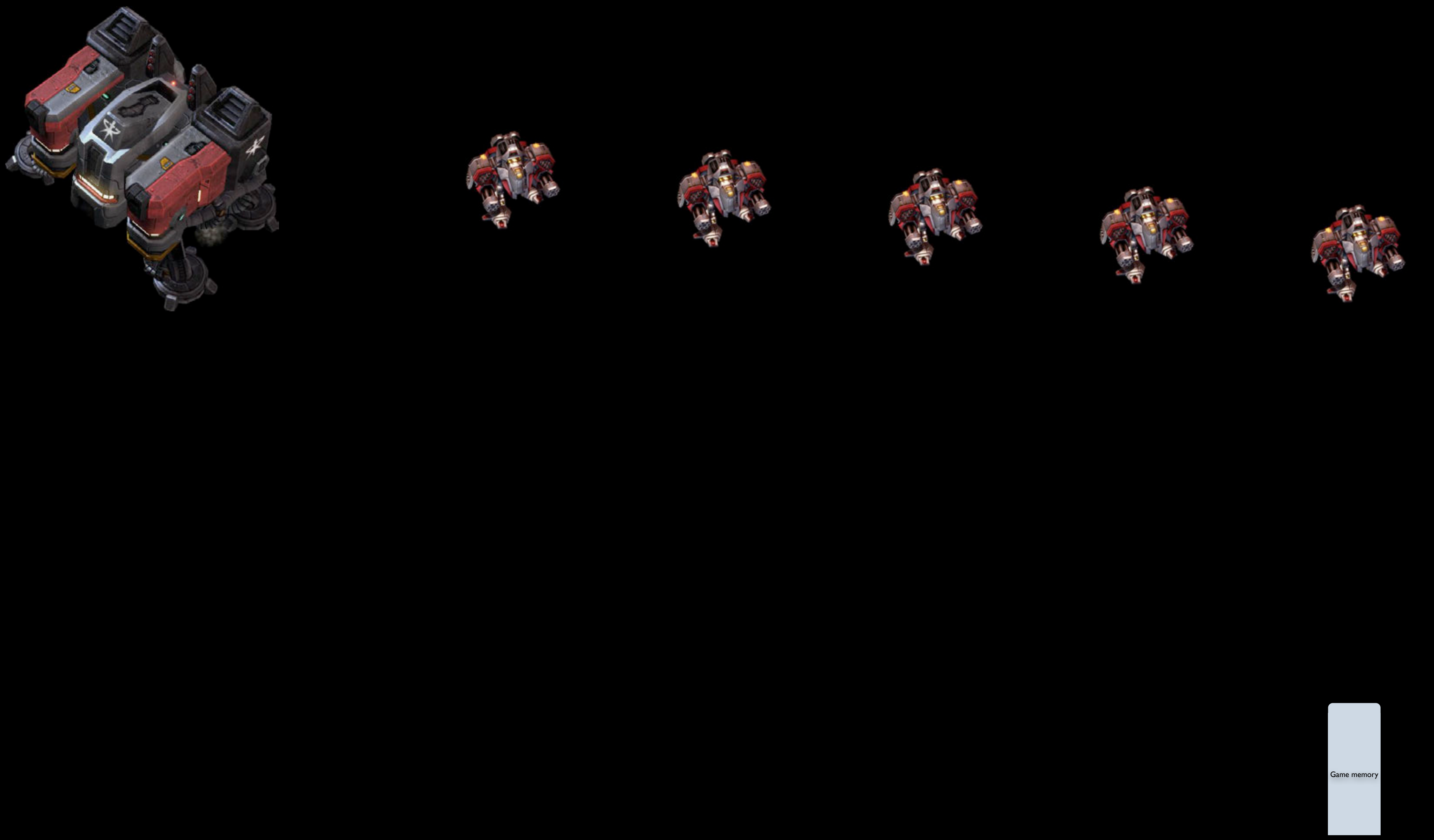
Unit hack Step



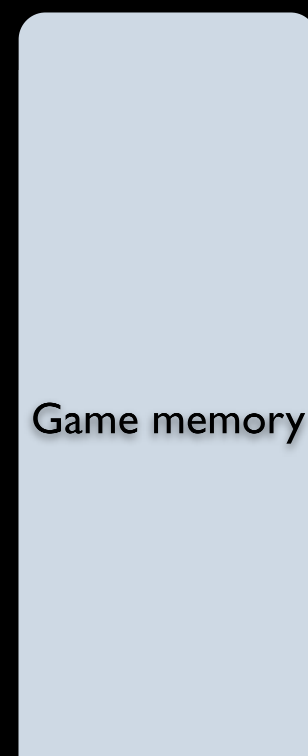
Unit hack Step

Game memory

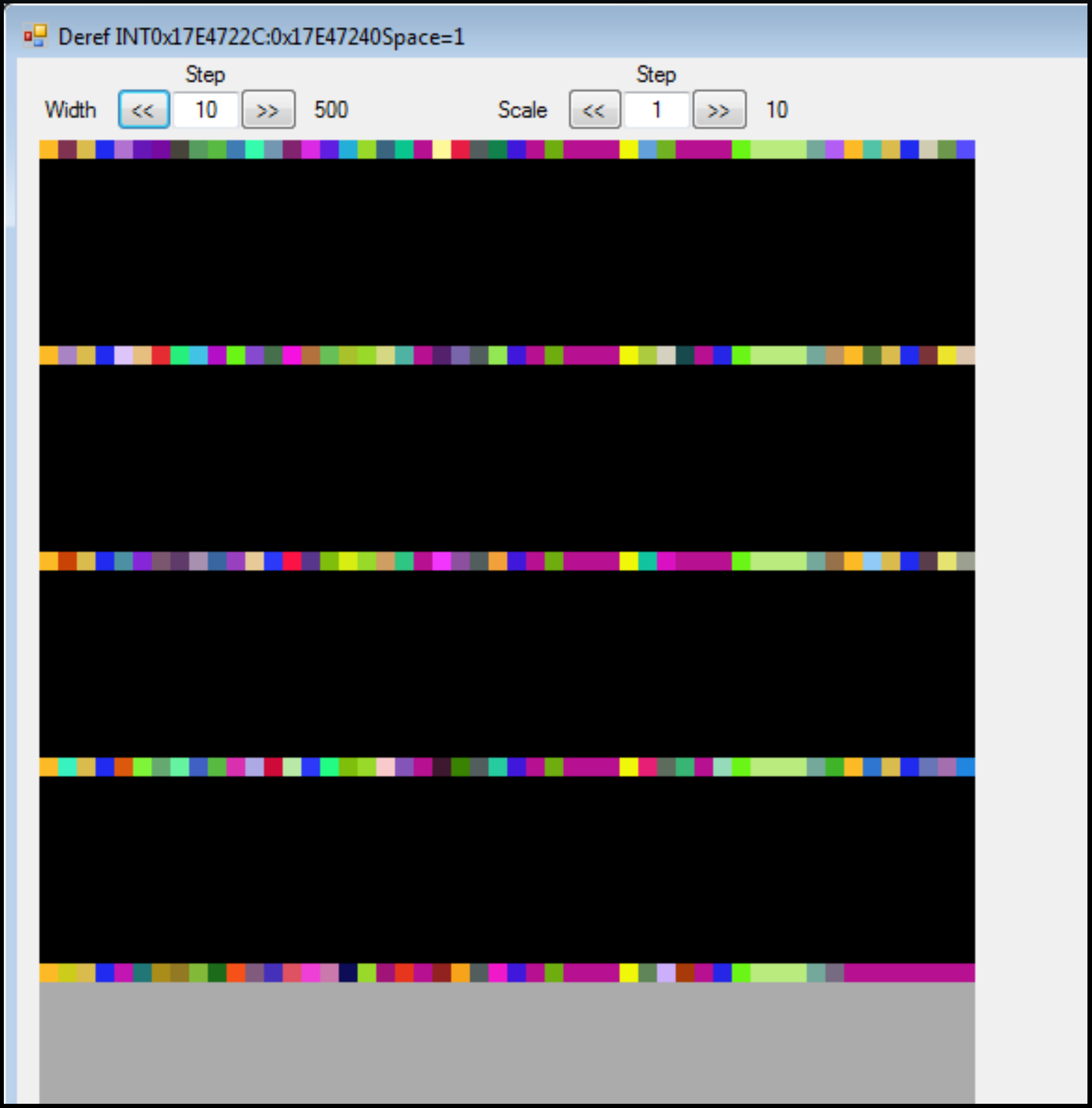
Unit hack Step



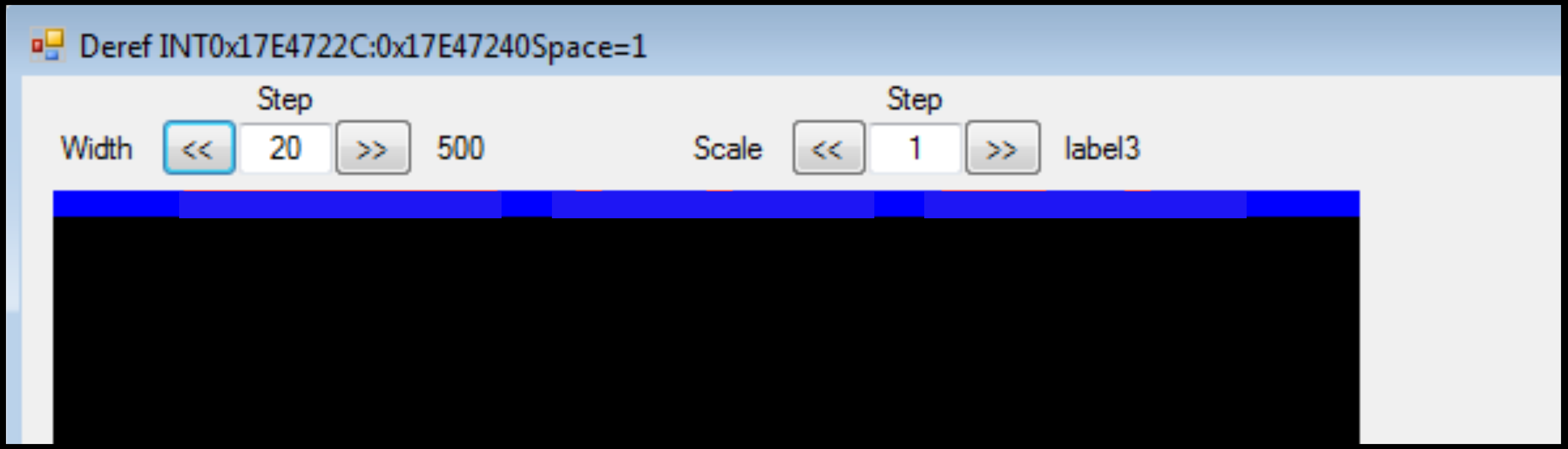
Unit hack Step



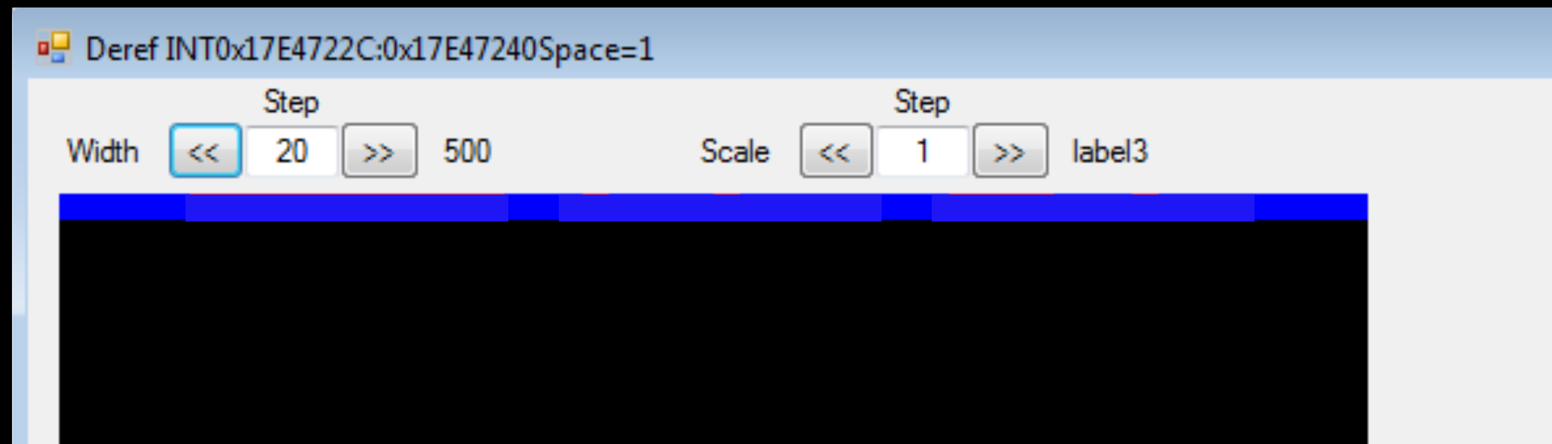
Unit Hack shape



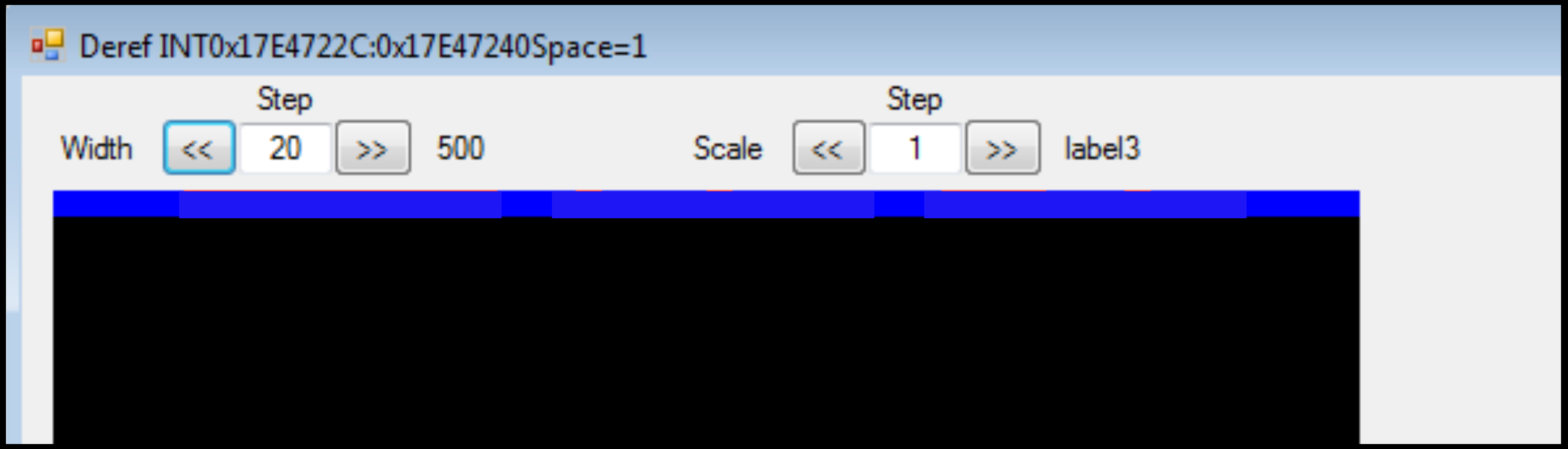
Understanding unit structure

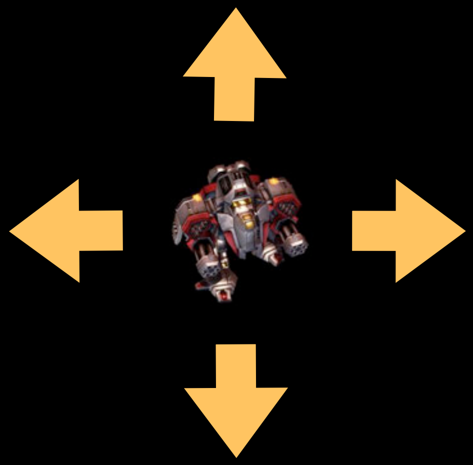


Understanding unit structure



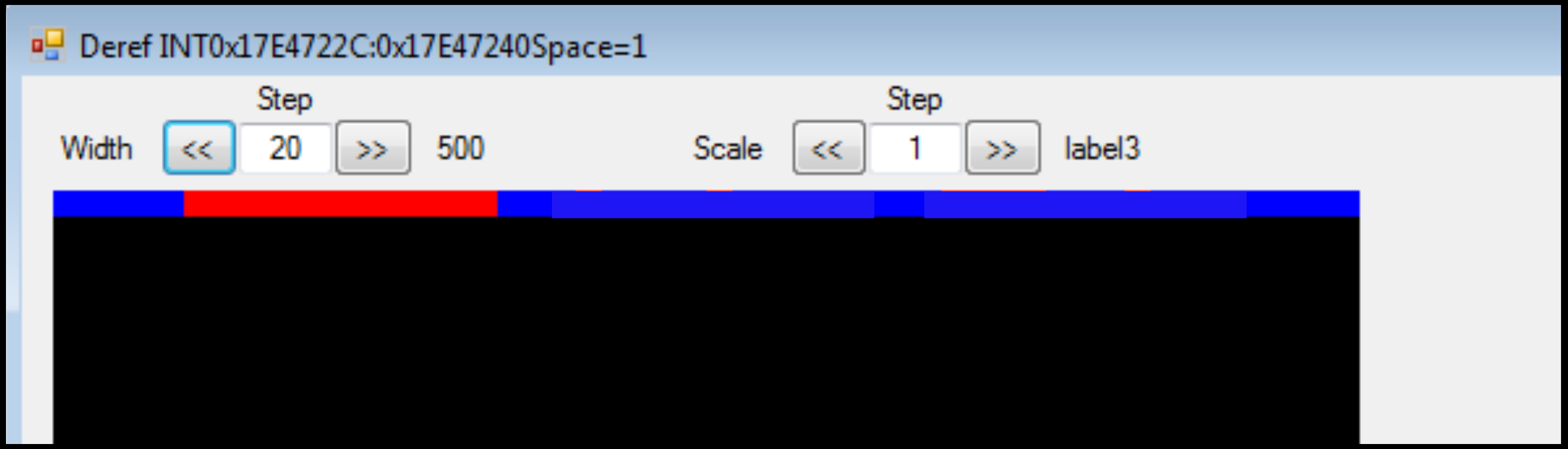
Understanding unit structure

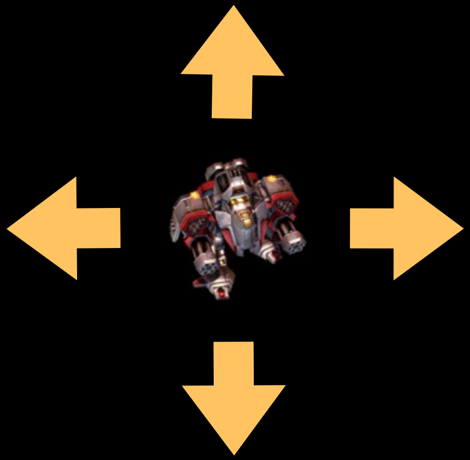




make it move

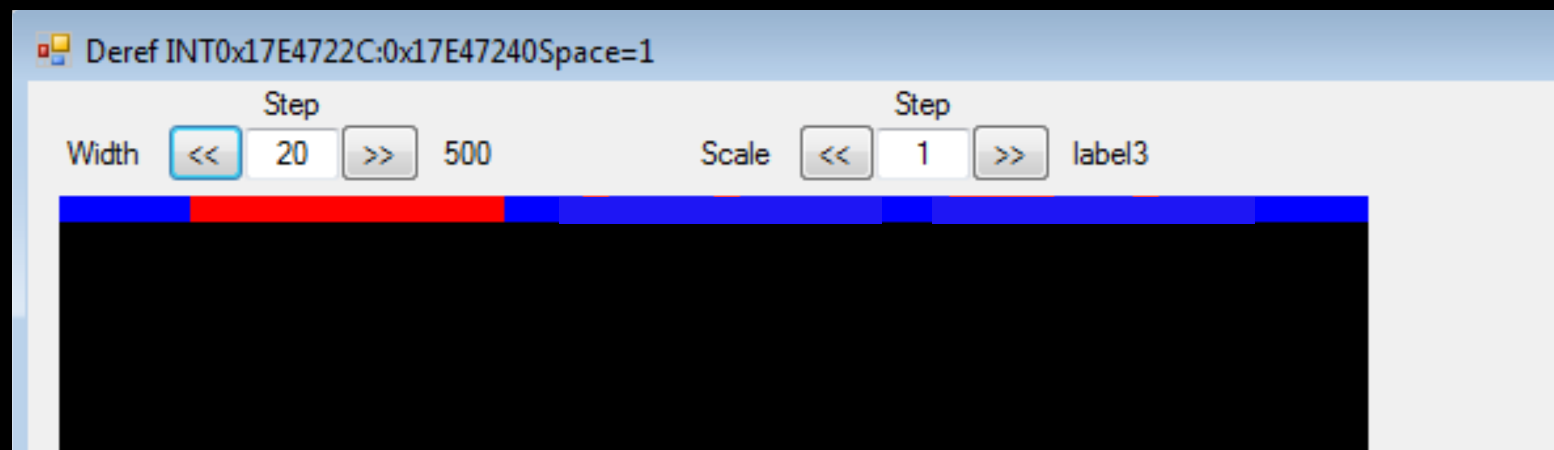
Understanding unit structure

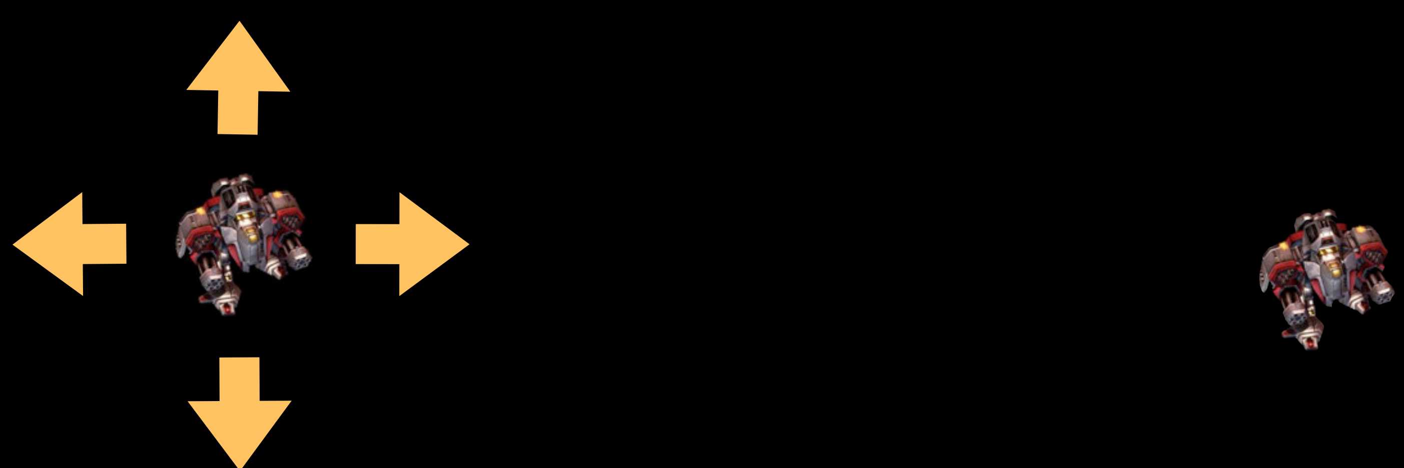




make it move

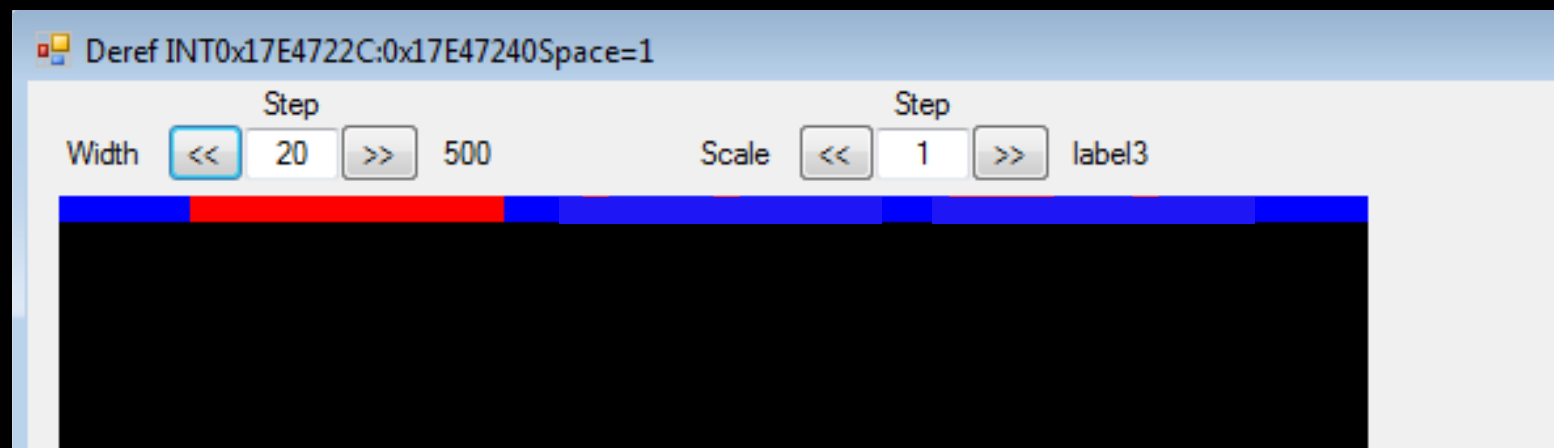
Understanding unit structure

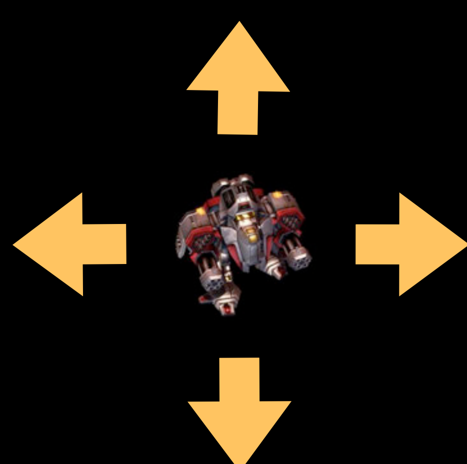




make it move

Understanding unit structure

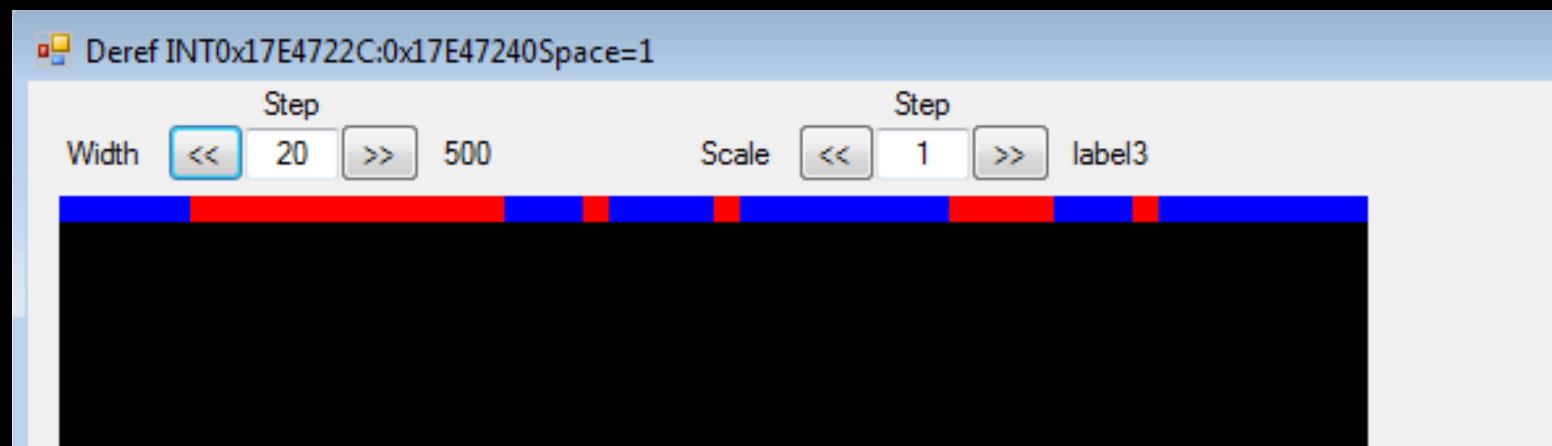


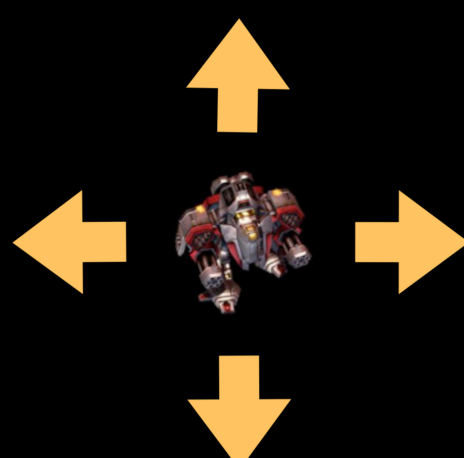


make it move

make it bleed

Understanding unit structure





make it move

make it bleed

Kartograph performance

Game	Unit 1	Unit 2	Unit 3	Unit 4	Unit 5
Supreme Commander 2	176454	13546	428	55	12
Age of empire 3	3443	177	48	29	10


V: Imperial Age
Menu
+12
Imperial Nassauer
· Hand infantry
6
10 / 110
2293
1359
925
4
Imperial Espada
Commands

Kartograph performances

Game	Launch	Play	Discover	Play more
Starcraft 2	850	725	2	1.3
C&C Tiberium Sun	75M	73M	400K	400K
C&C Red Alert 2	101M	100M	935K	915K
C&C Red Alert 3	660M	635M	4.4M	1.6M
Age of Empire 3	245M	243M	2.7M	2.5M
Supreme Commander 2	1.2G	629M	2.5M	1.5M
Civilization IV + ext	340M	293M	2M	1.9M
Anno 1701	432M	413M	1.9M	1.8M
Warcraft 3	129M	124M	1.9M	1.8M

Network based maphack

Rewriting network traffic

- Resync the game or get caught
- Use LSP (Layer service provider) to rewrite network traffic

Understanding the network traffic

Understanding the network traffic

Bucket

Understanding the network traffic

Bucket

Visualize

Understanding the network traffic

Bucket

Visualize

Understand

Understanding the network traffic

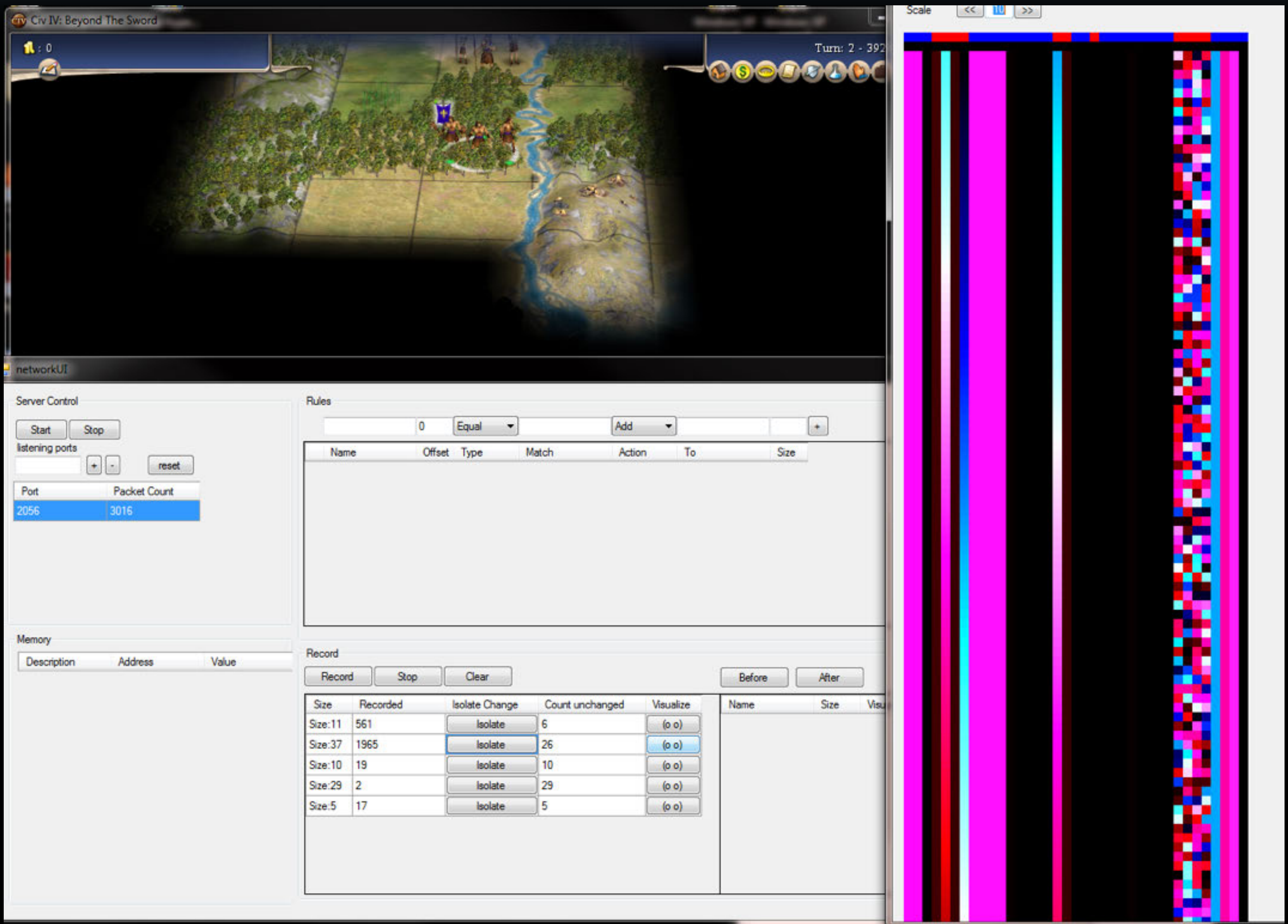
Bucket

Visualize

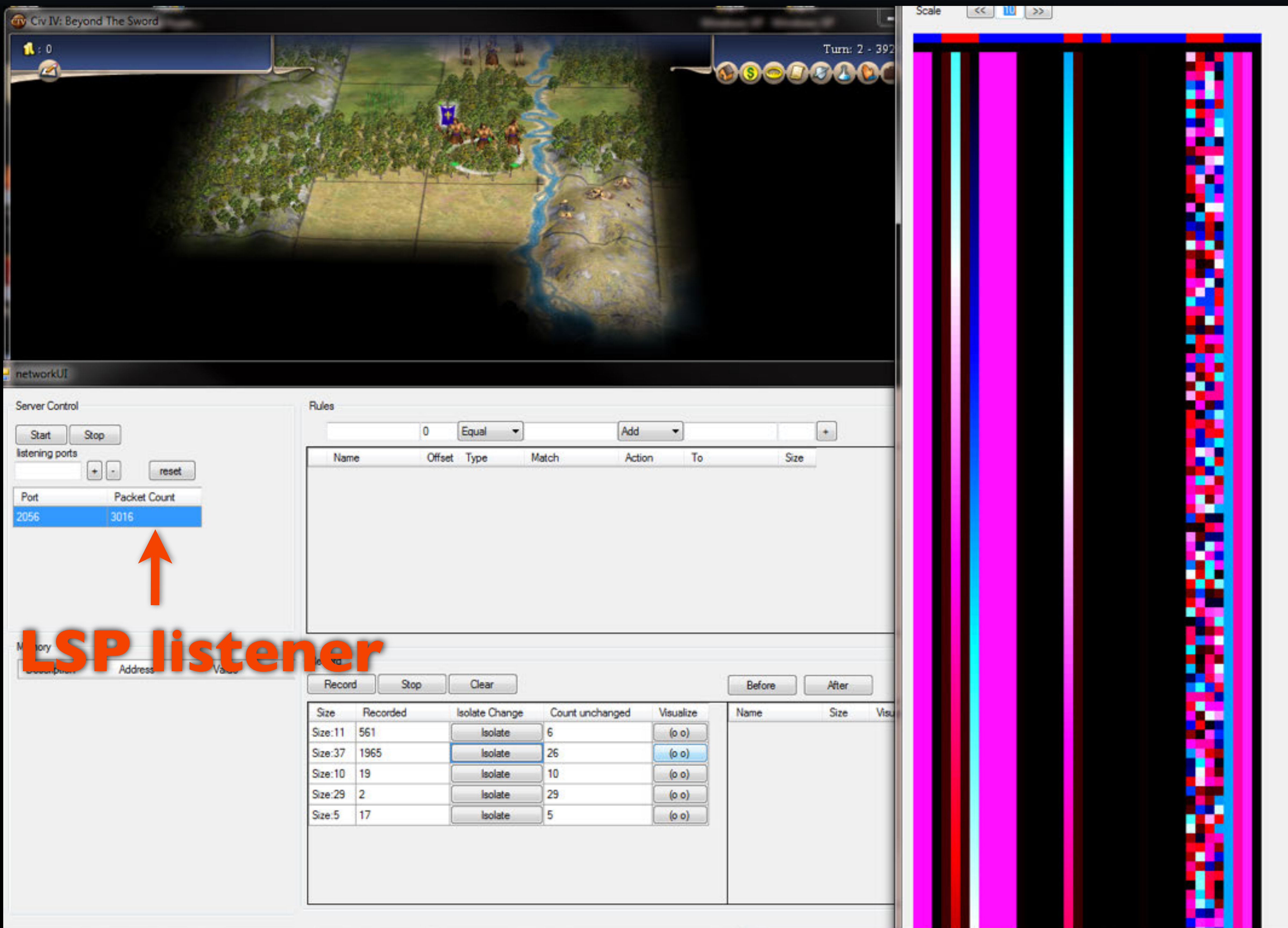
Understand

Resync

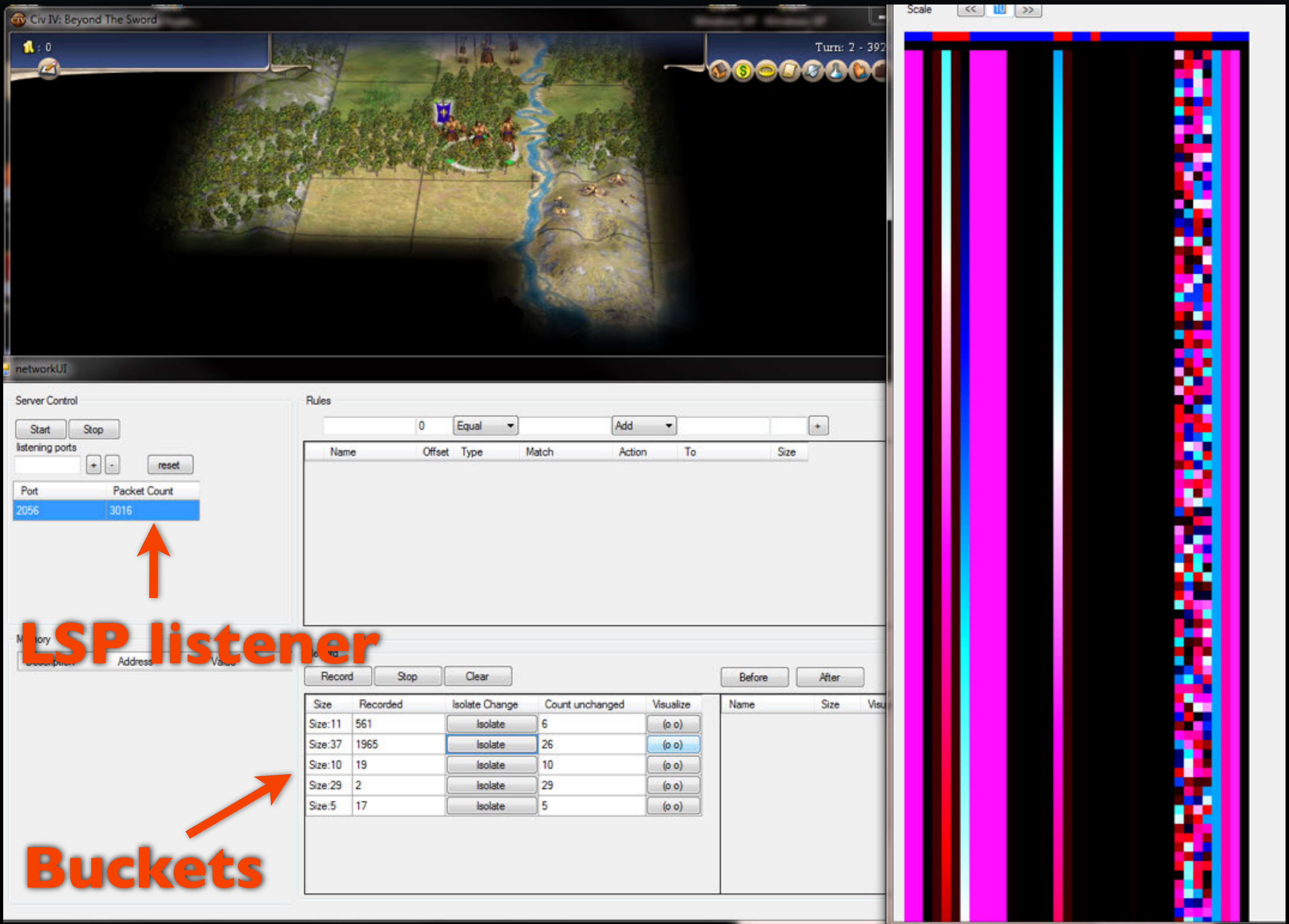
Civilization 4 vizualization



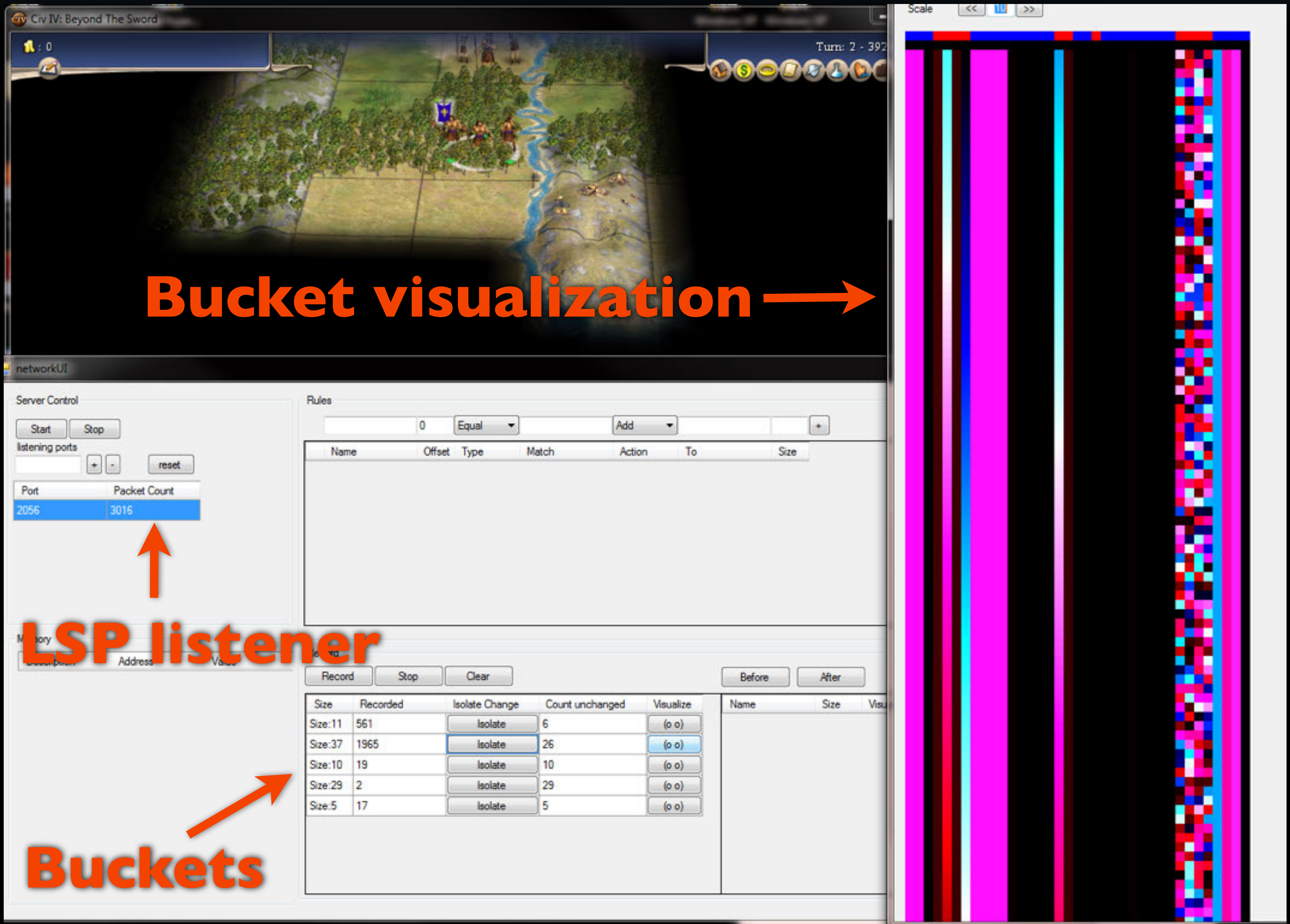
Civilization 4 vizualization



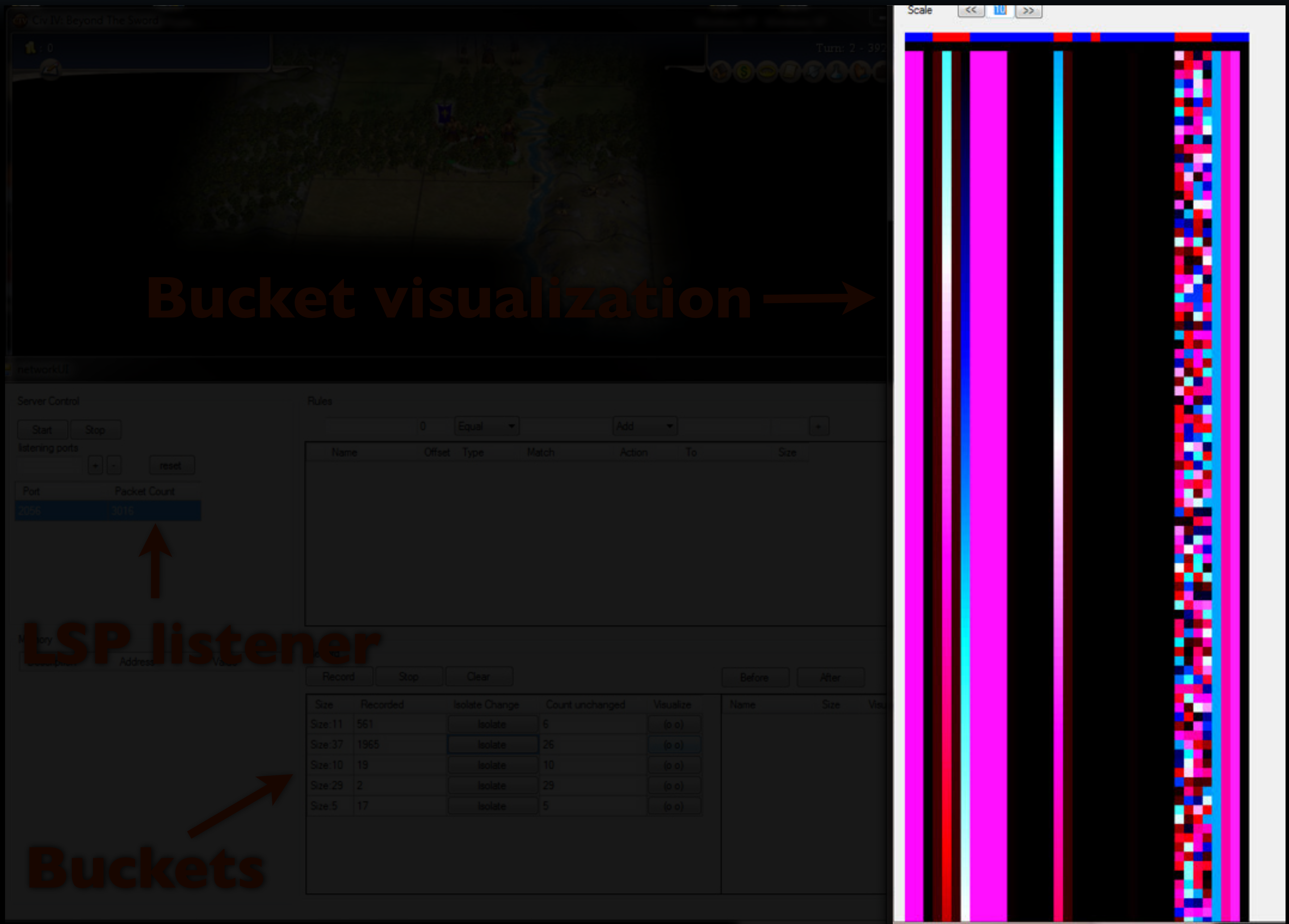
Civilization 4 vizualization



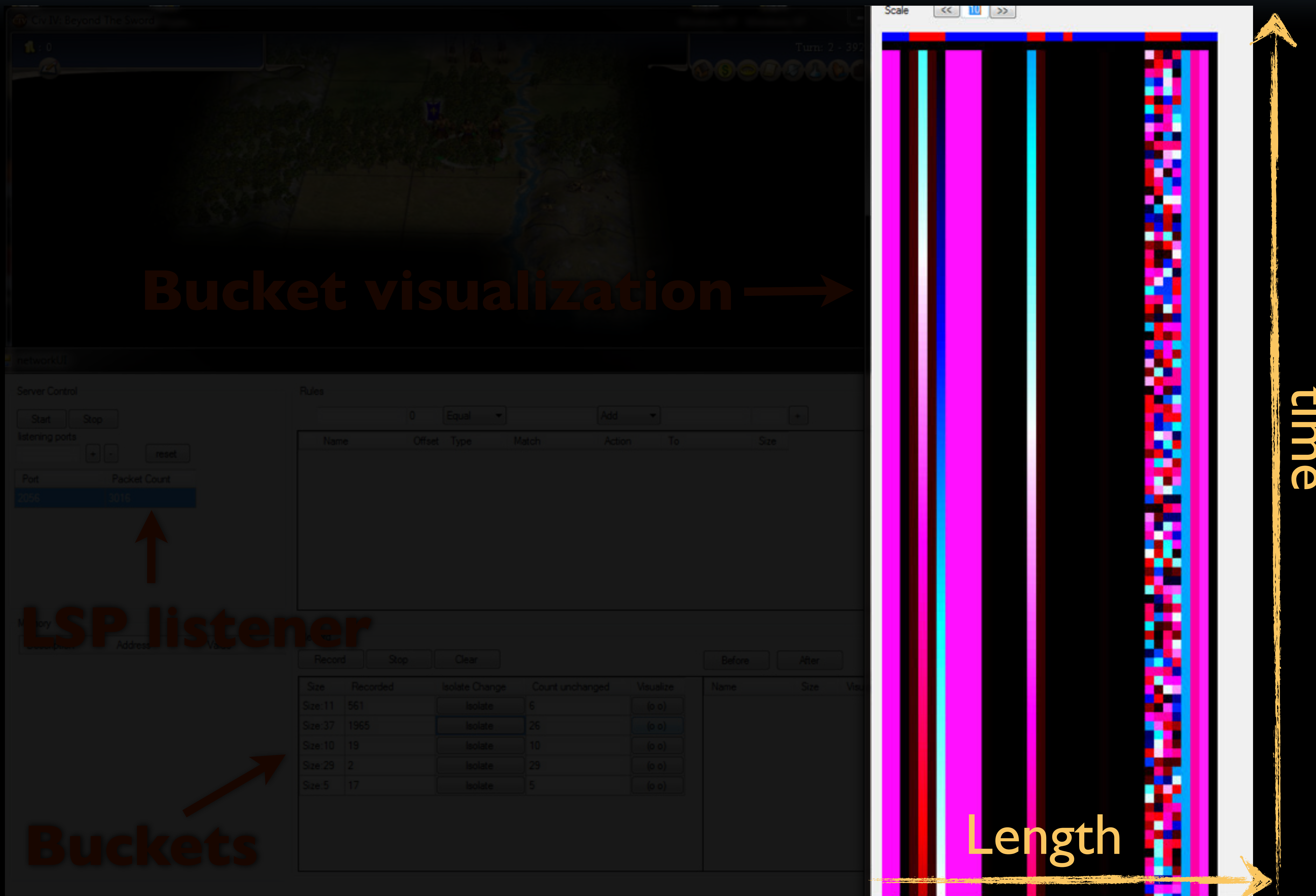
Civilization 4 vizualization



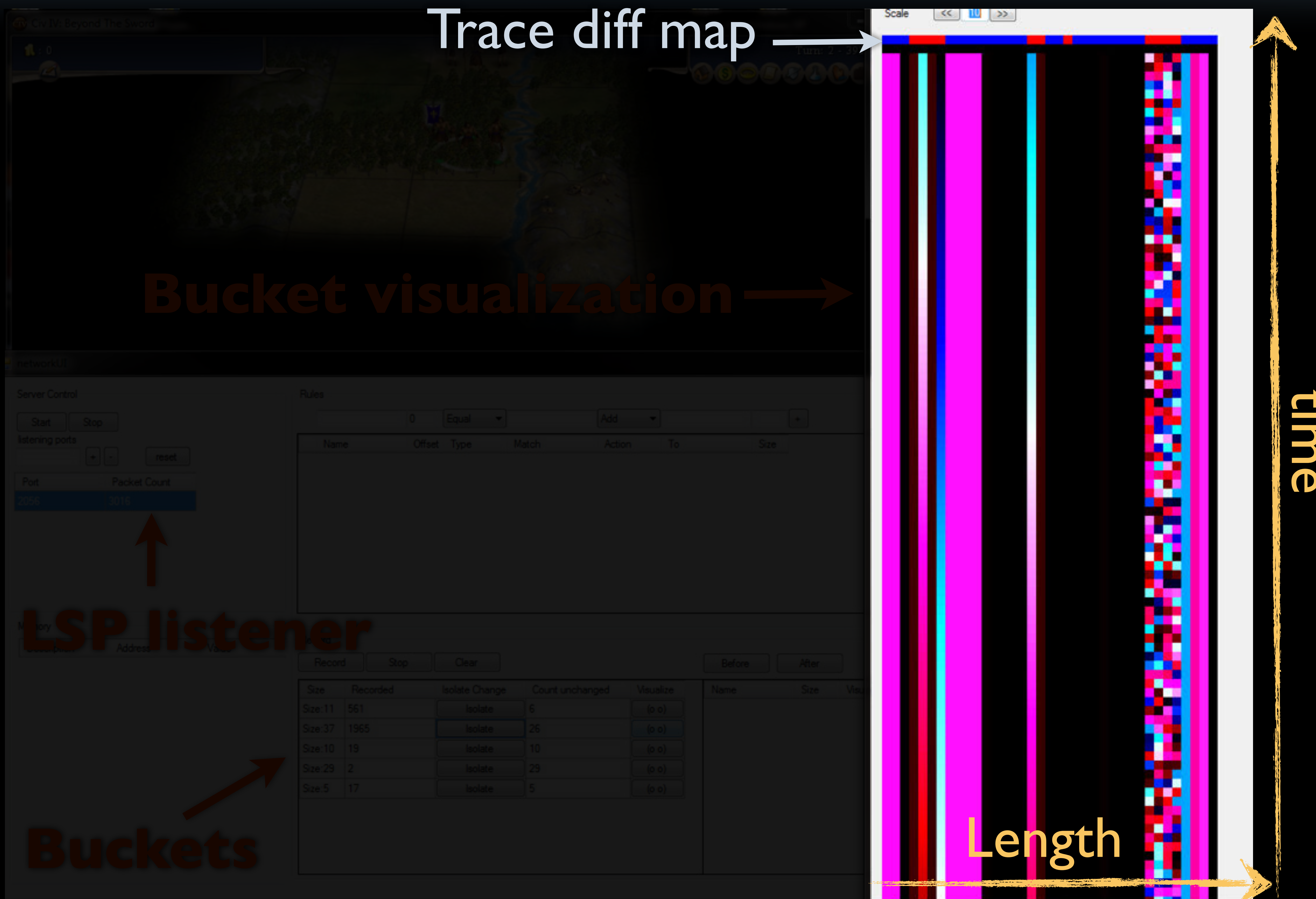
Civilization 4 vizualization



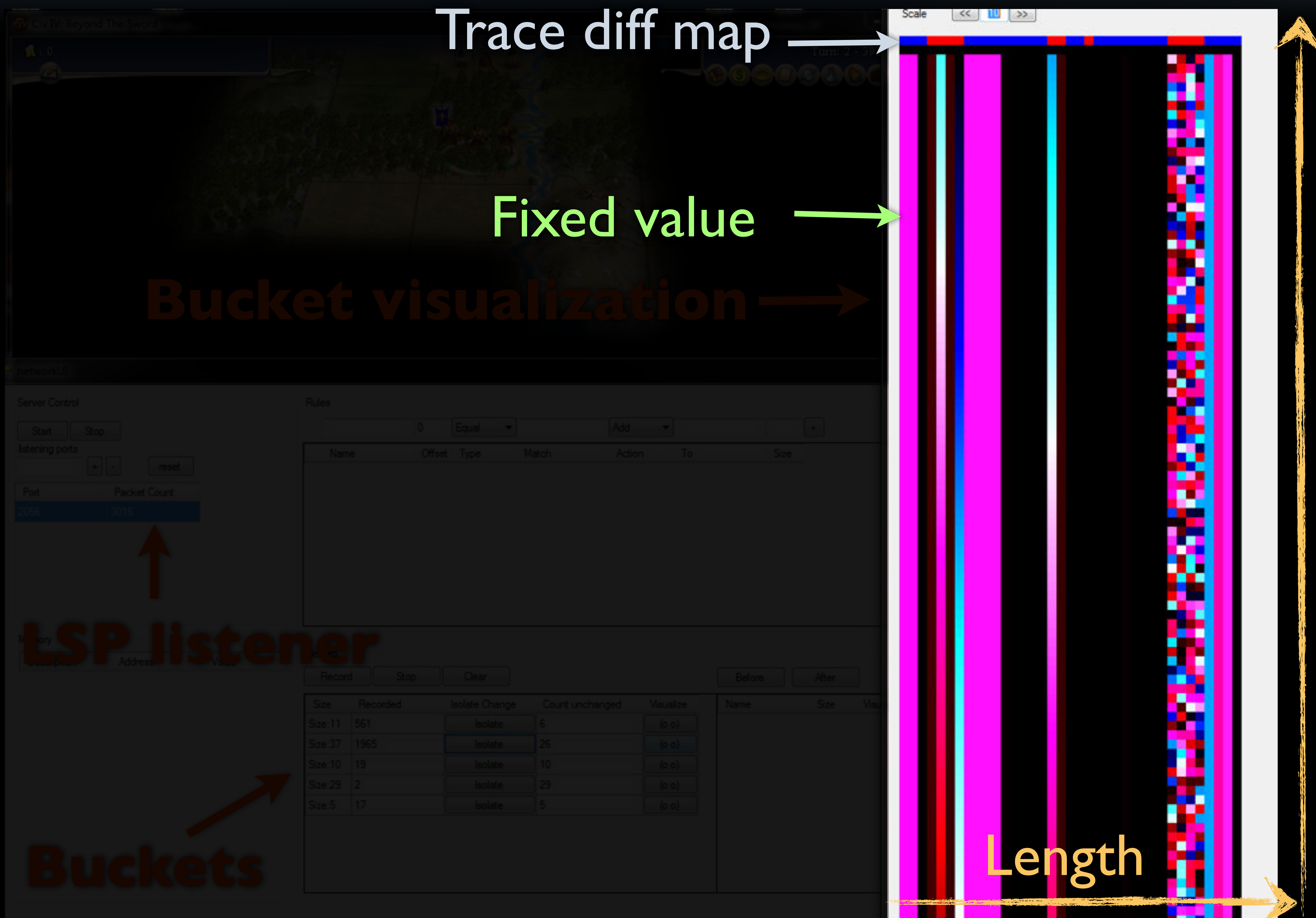
Civilization 4 vizualization



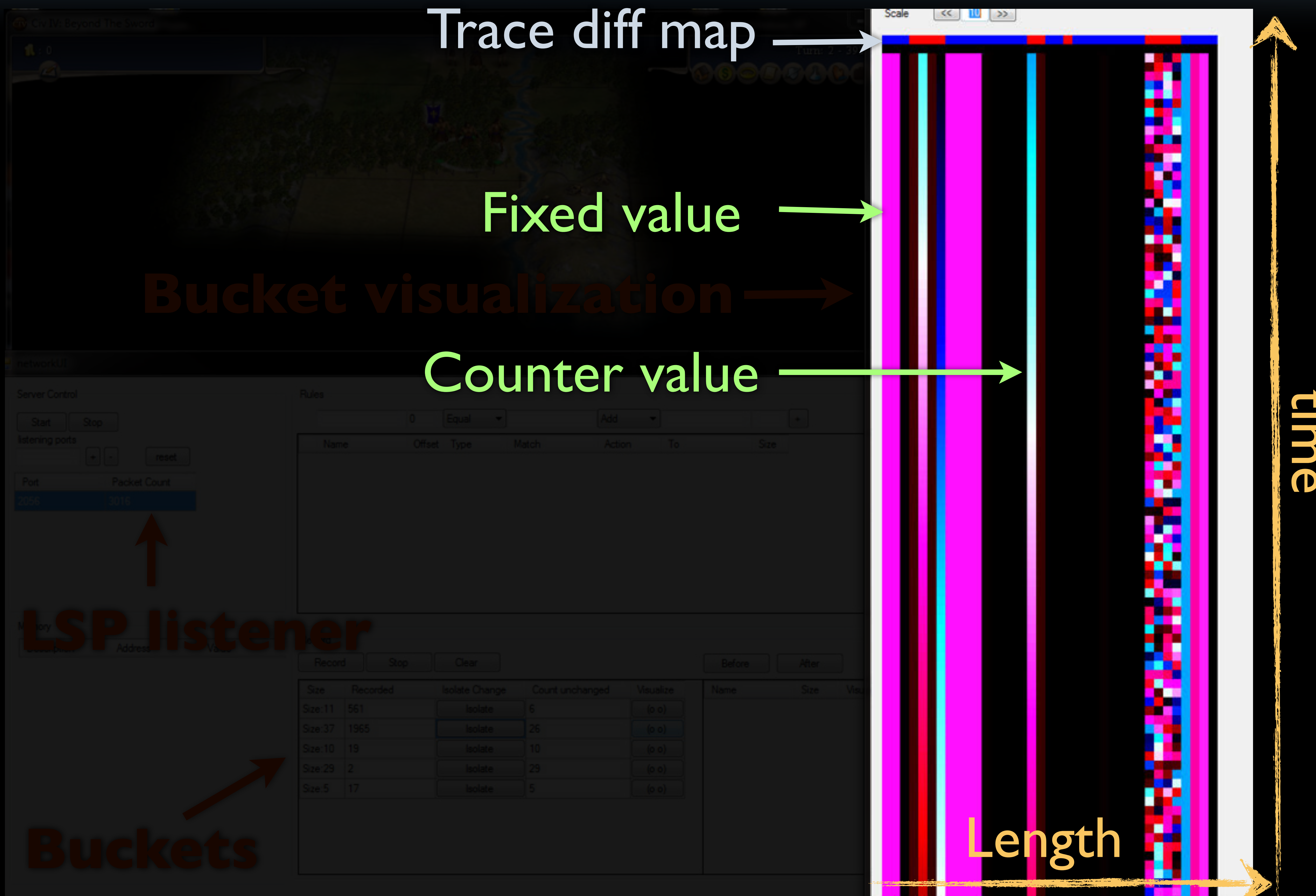
Civilization 4 vizualization



Civilization 4 vizualization



Civilization 4 vizualization



Civilization 4 vizualization