Kartograph

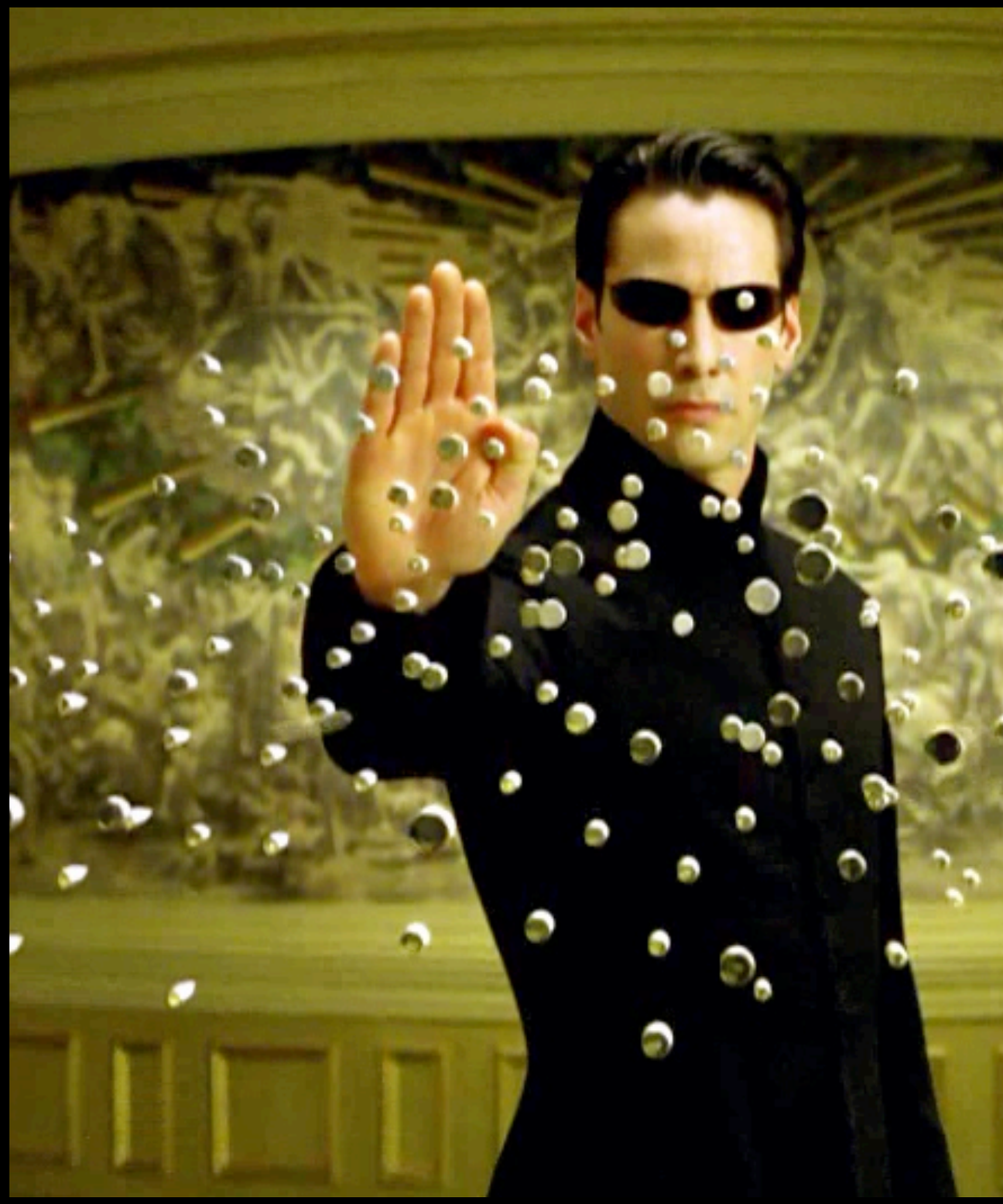
Elie Bursztein, Jocelyn Lagarenne
Stanford University

Welcome to the real world

#kartograph

supernatural powers !

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



Supreme commander 2

Memory based attack

Memory

Memory based attack

Memory

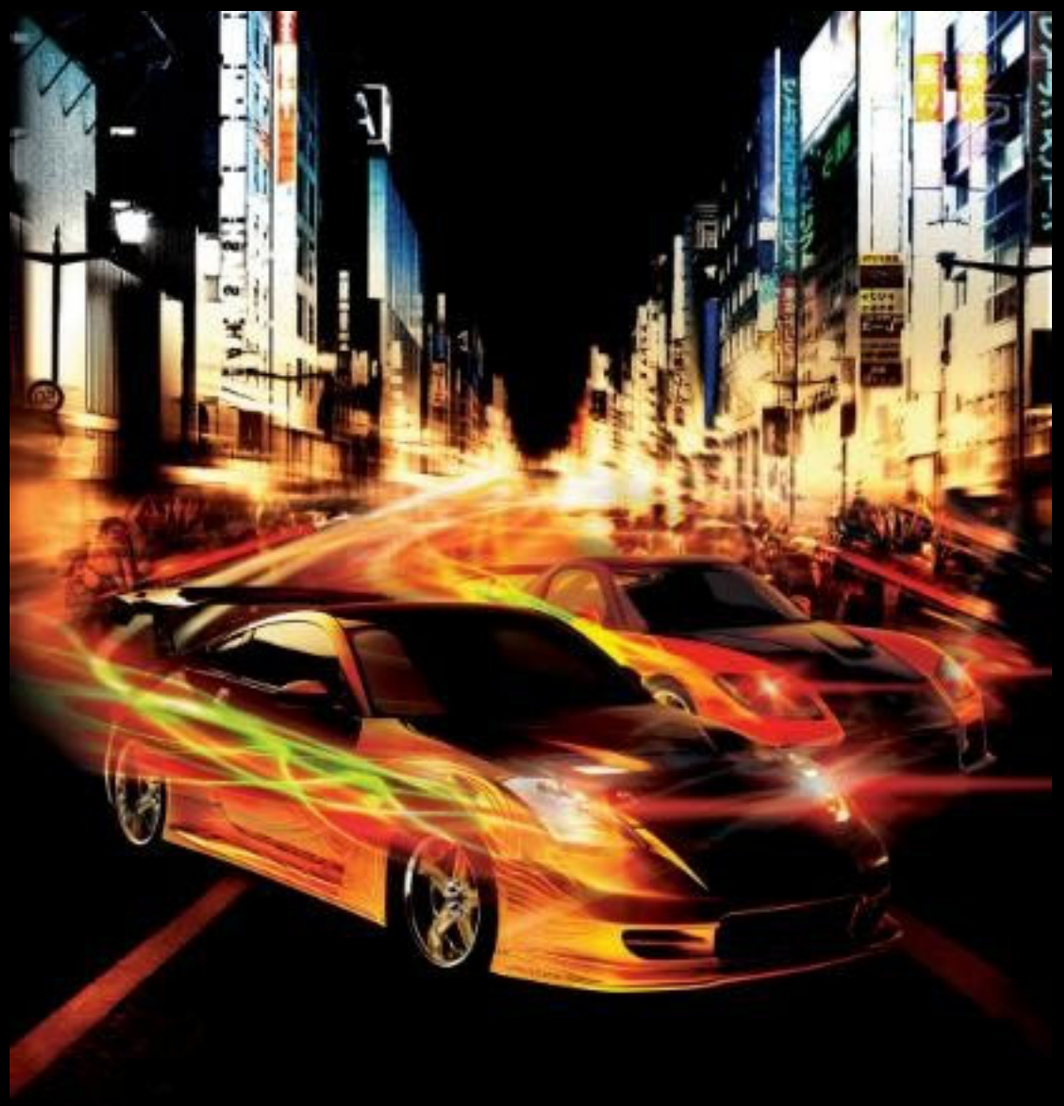
Modification

Memory based attack

Memory

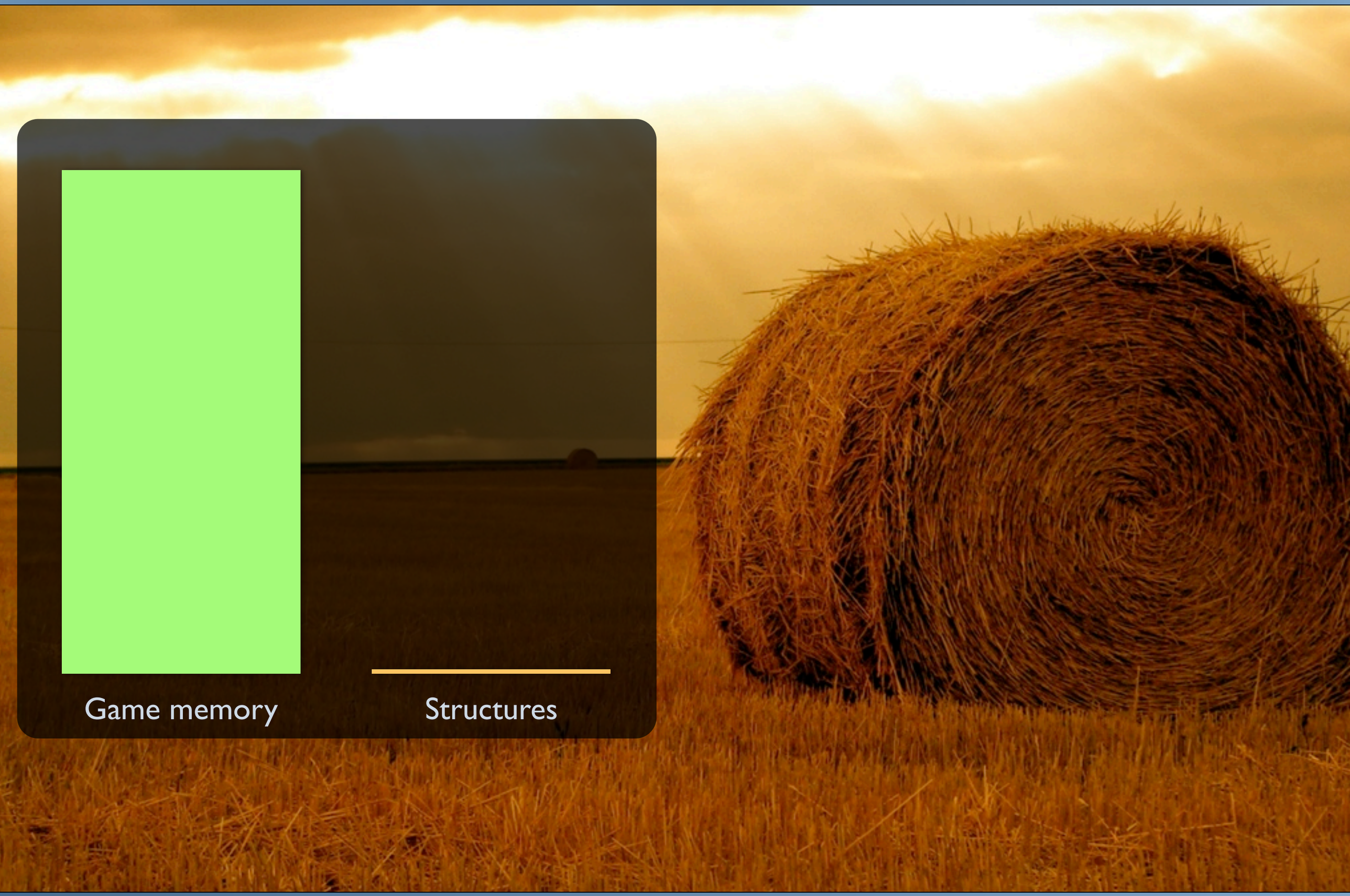
Modification

Benefits (fast and furious)



- Generic
- Fast
- Invisible

Drawbacks: Needle in a Haystack



Outline

Outline

- Background

Outline

- Background
- Building a maphack

Outline

- Background
- Building a maphack
- Invulnerable unit

Outline

- Background
- Building a maphack
- Invulnerable unit
- Network

Outline

- Background
- Building a maphack
- Invulnerable unit
- Network
- Demo

Background

273 Millions games sold in 2009

Game type

Action

Game type

Action

First person

Game type

Action

First person

Sport

Game type

Action

First person

Sport

Role playing

Game type

Action

First person

Sport

Role playing

Adventure

Game type

Action

First person

Sport

Role playing

Adventure

Strategy

Game type

Strategy account for 35% of the games sold in 2009


4650
Tankbuster
300
0:05
Anti-Armor
Steely-cold warriors whose personal plasma-cutter cannons can slice through enemy armor.
Instant Dojo
1
1x
2x
3x


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


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


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


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

Supreme commander 2

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

Maphack

Map hack step

Map hack step

Map hack step

Reduce haystack

Map hack step

Reduce haystack

Find

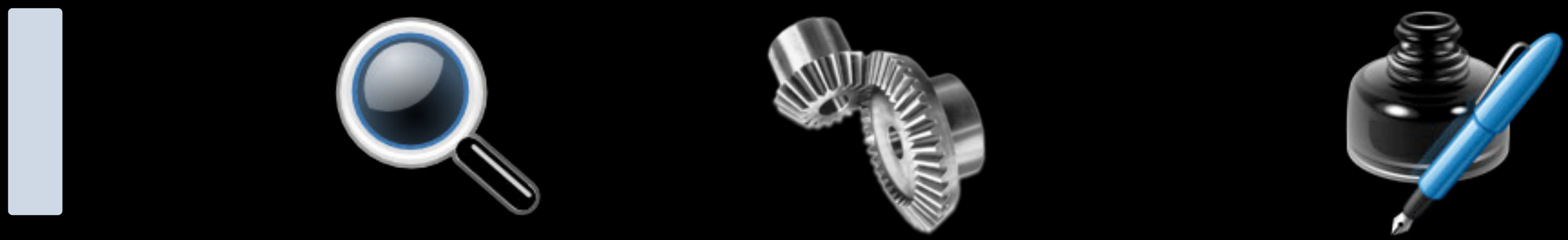
Map hack step

Reduce haystack

Find

Understand

Map hack step



Reduce haystack

Find

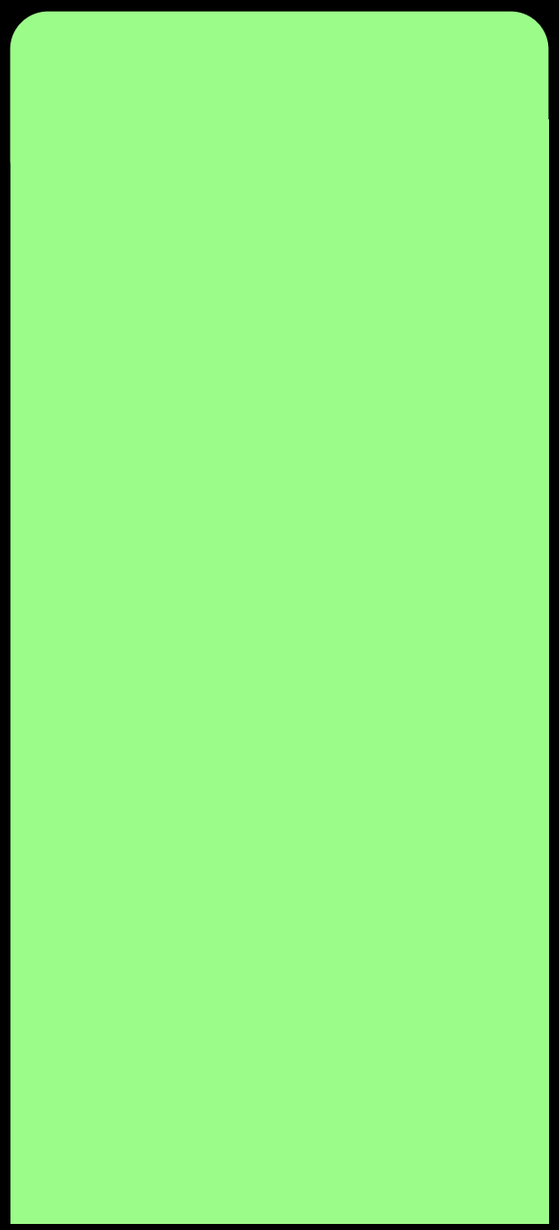
Understand

Rewrite

Acquiring game memory

Game memory

Acquiring game memory



Reducing memory

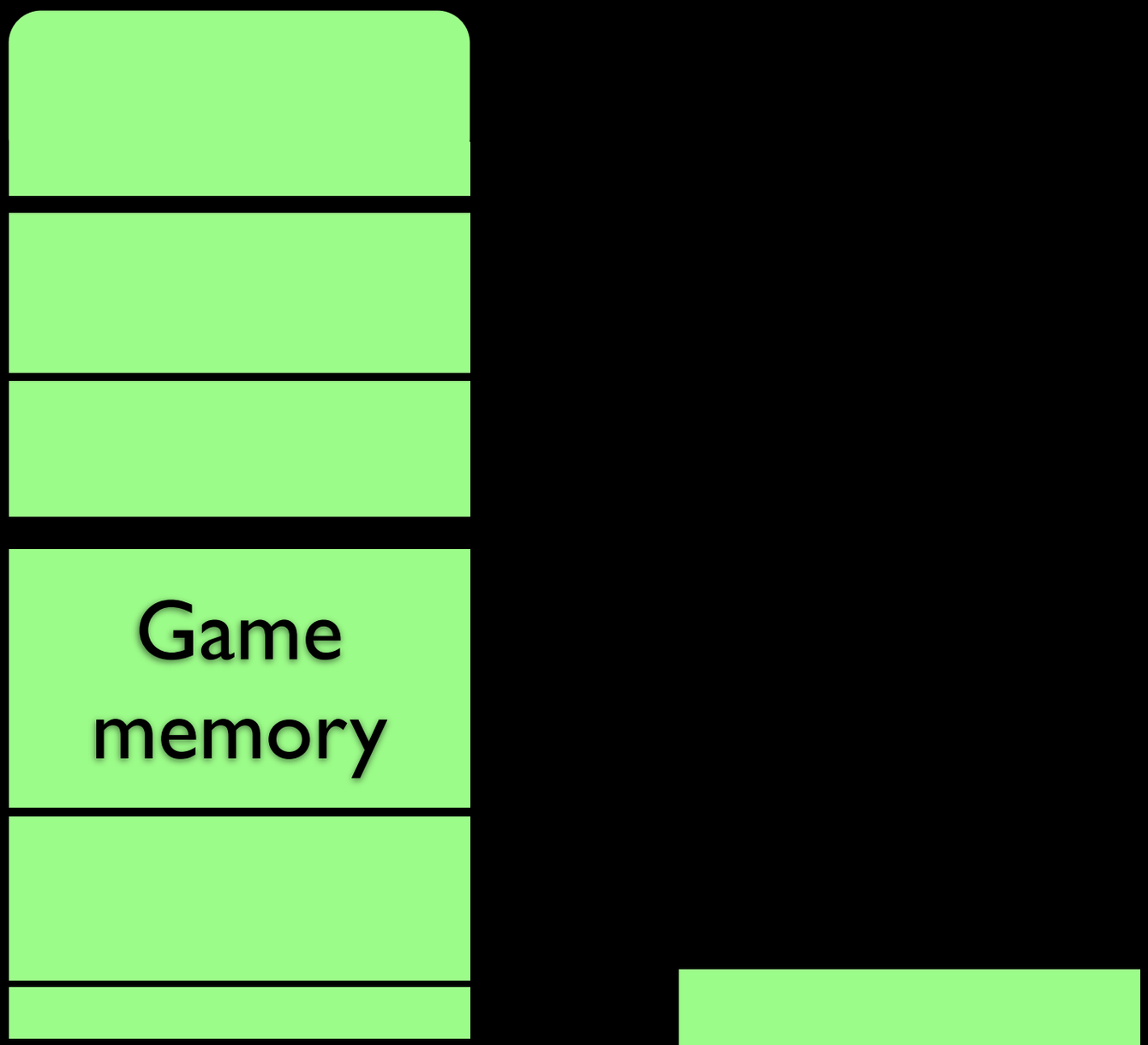
Game memory

Reducing memory

Game memory

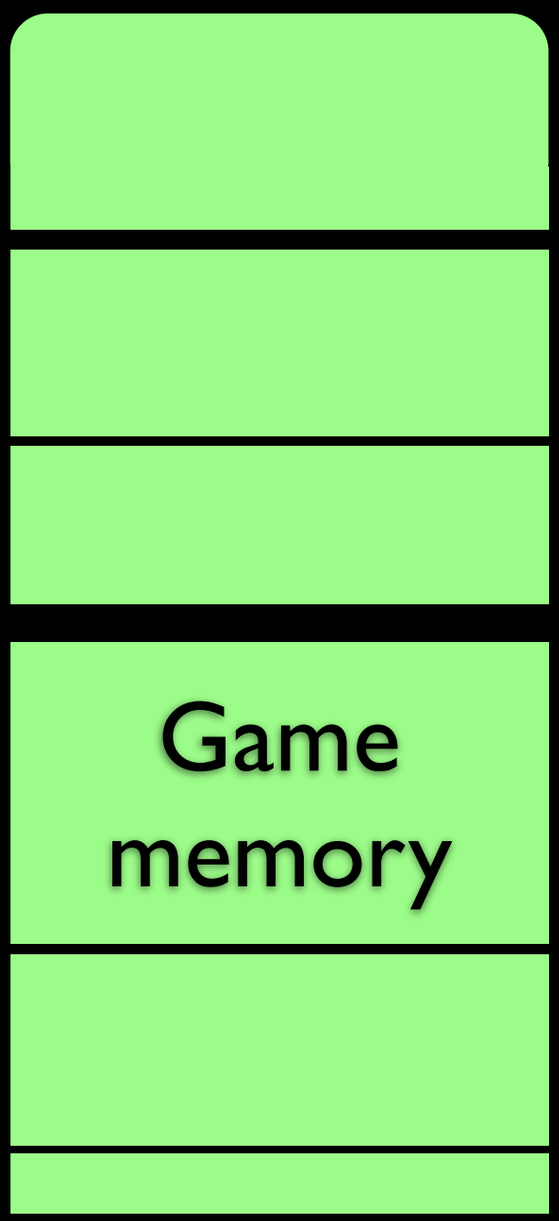
Step 1 play

Reducing memory



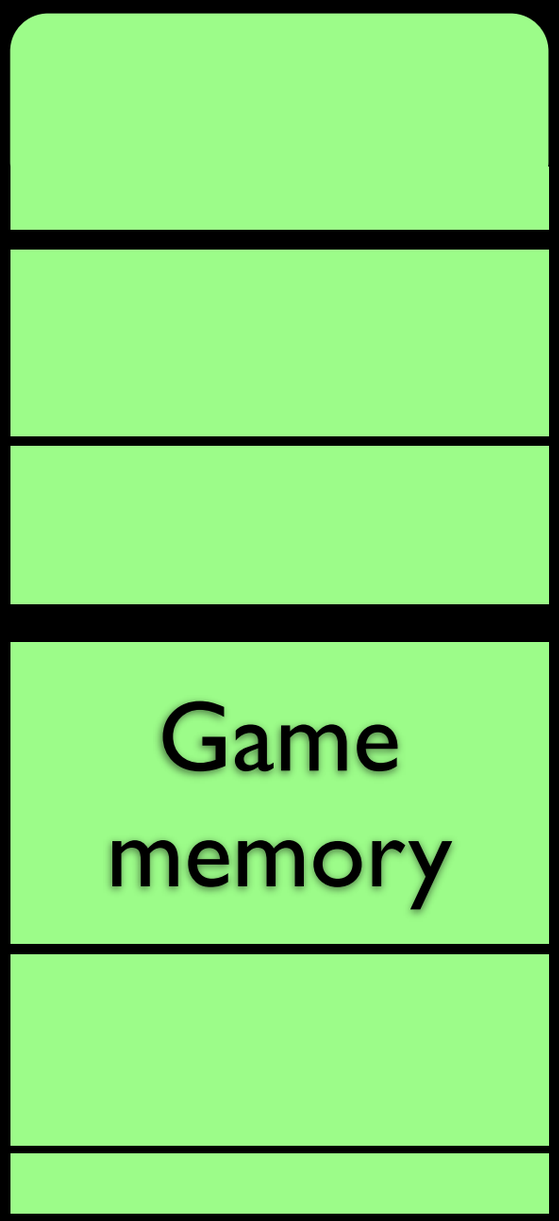
Step 1 play

Reducing memory



Step 1 play Step 2 discover

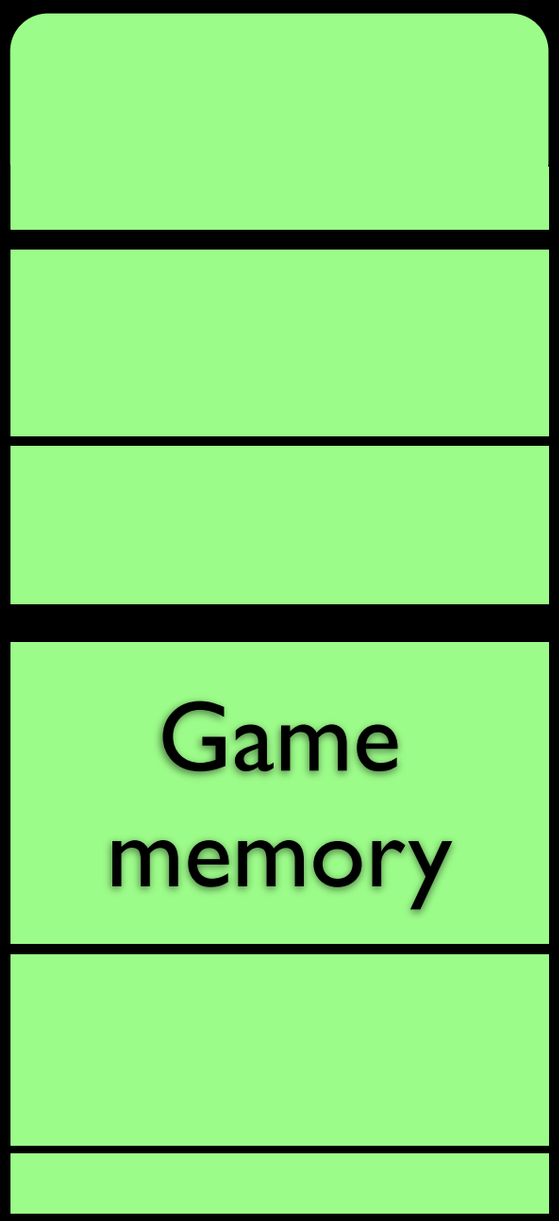
Reducing memory



Step 1 play

Step 2 discover

Reducing memory

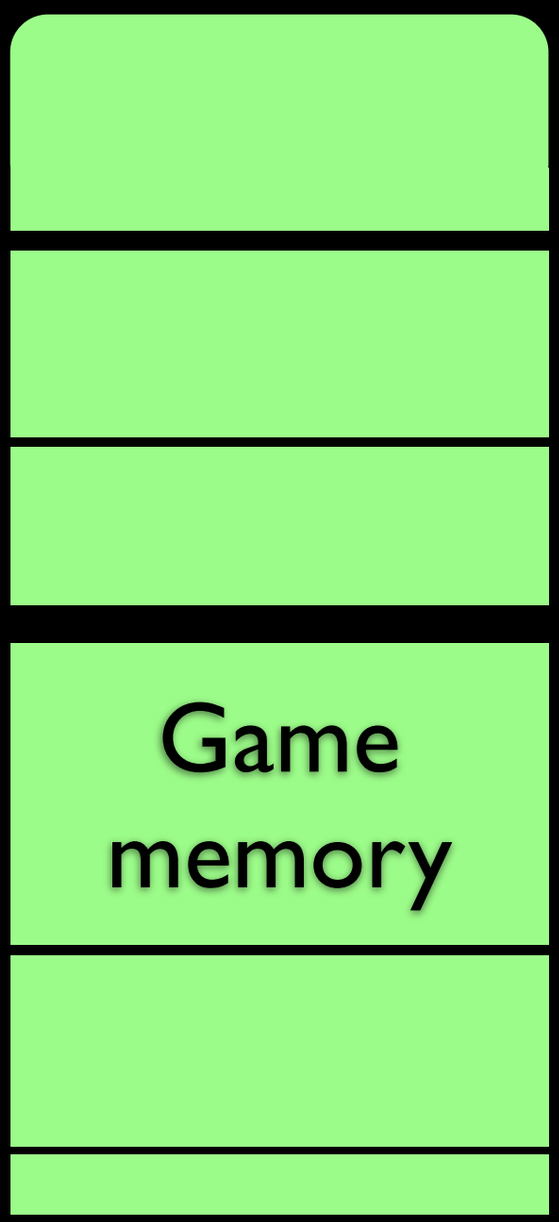


Step 1 play

Step 2 discover

Step 3 play

Reducing memory



Step 1 play

Step 2 discover

Step 3 play

Reducing memory

Acquiring the game's memory

Supreme Commander 2

71

53532 (+17)

99999 (+57)

120/500

01:34:55

MENU

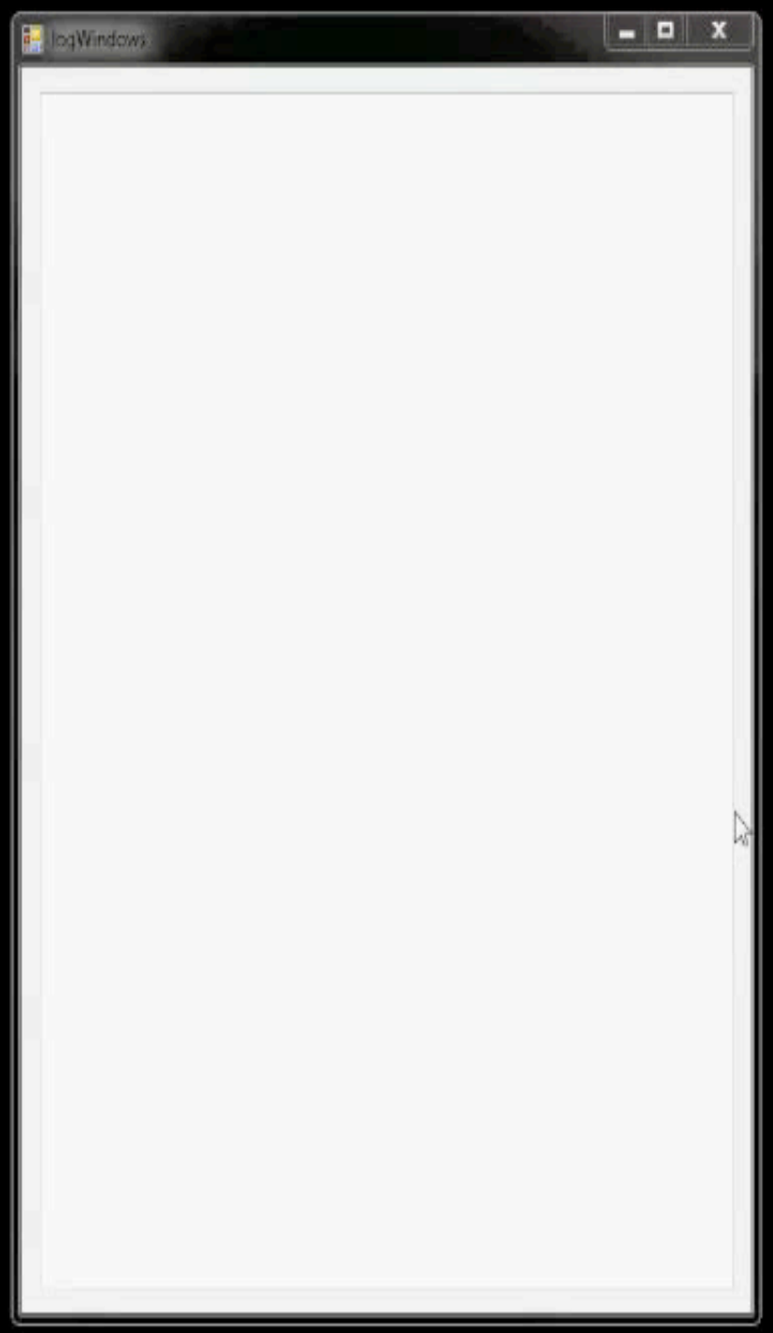
MINIMAP

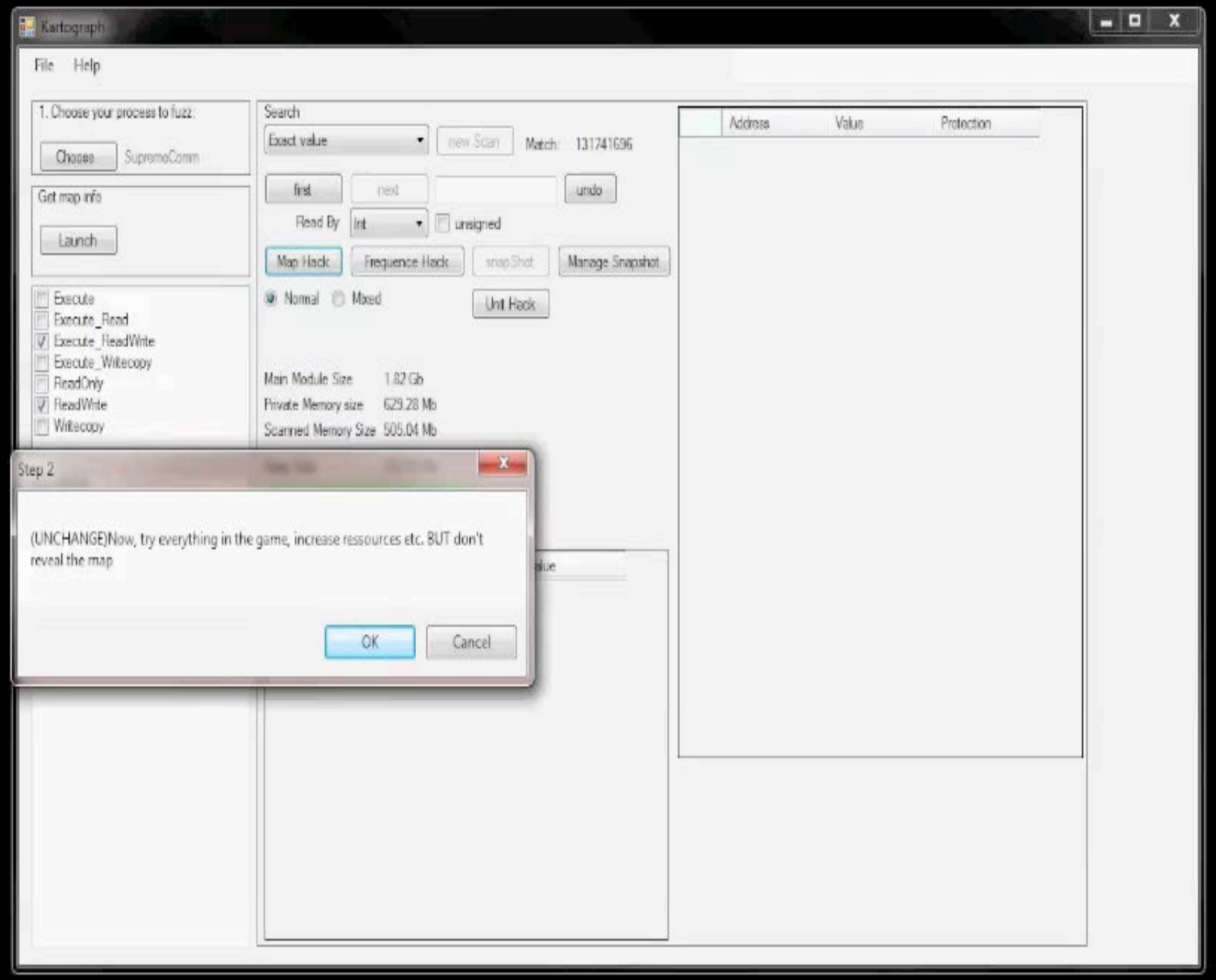
Value

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 SupremoComm

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

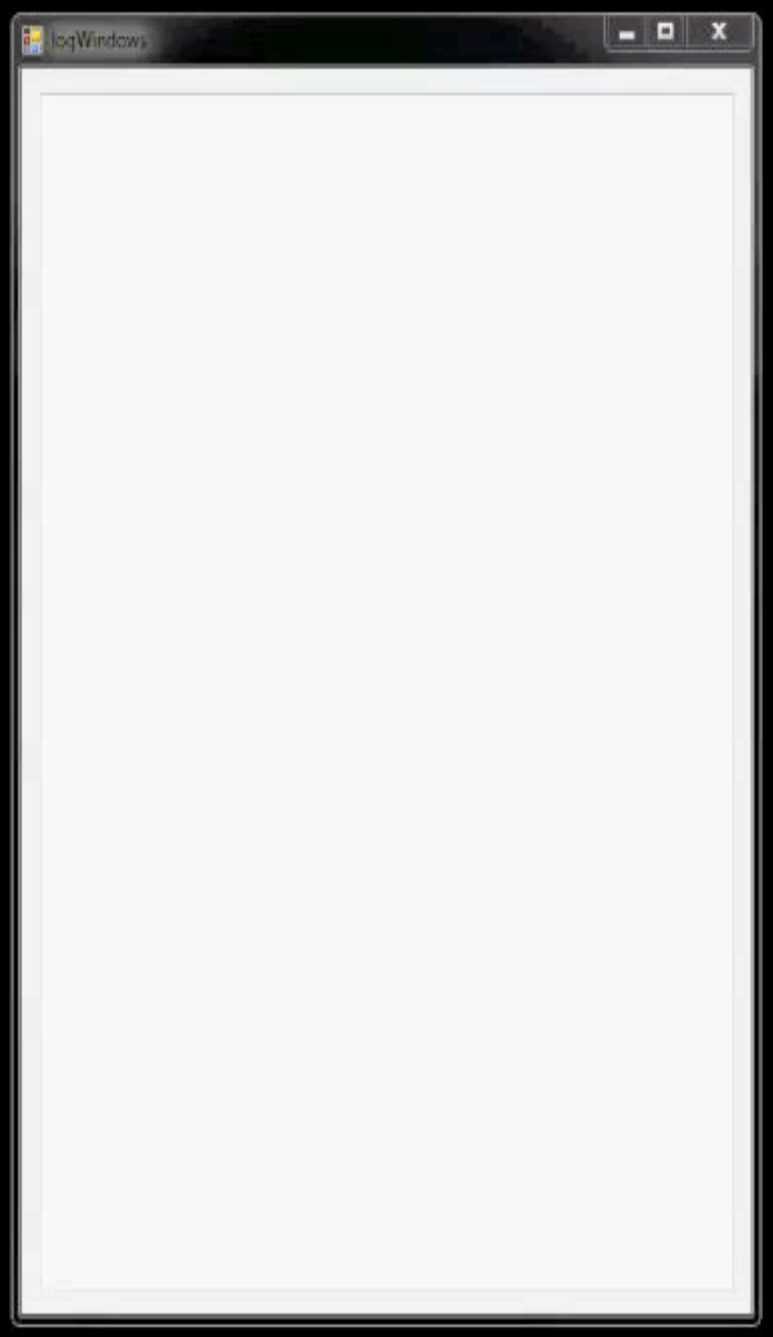
Step 3

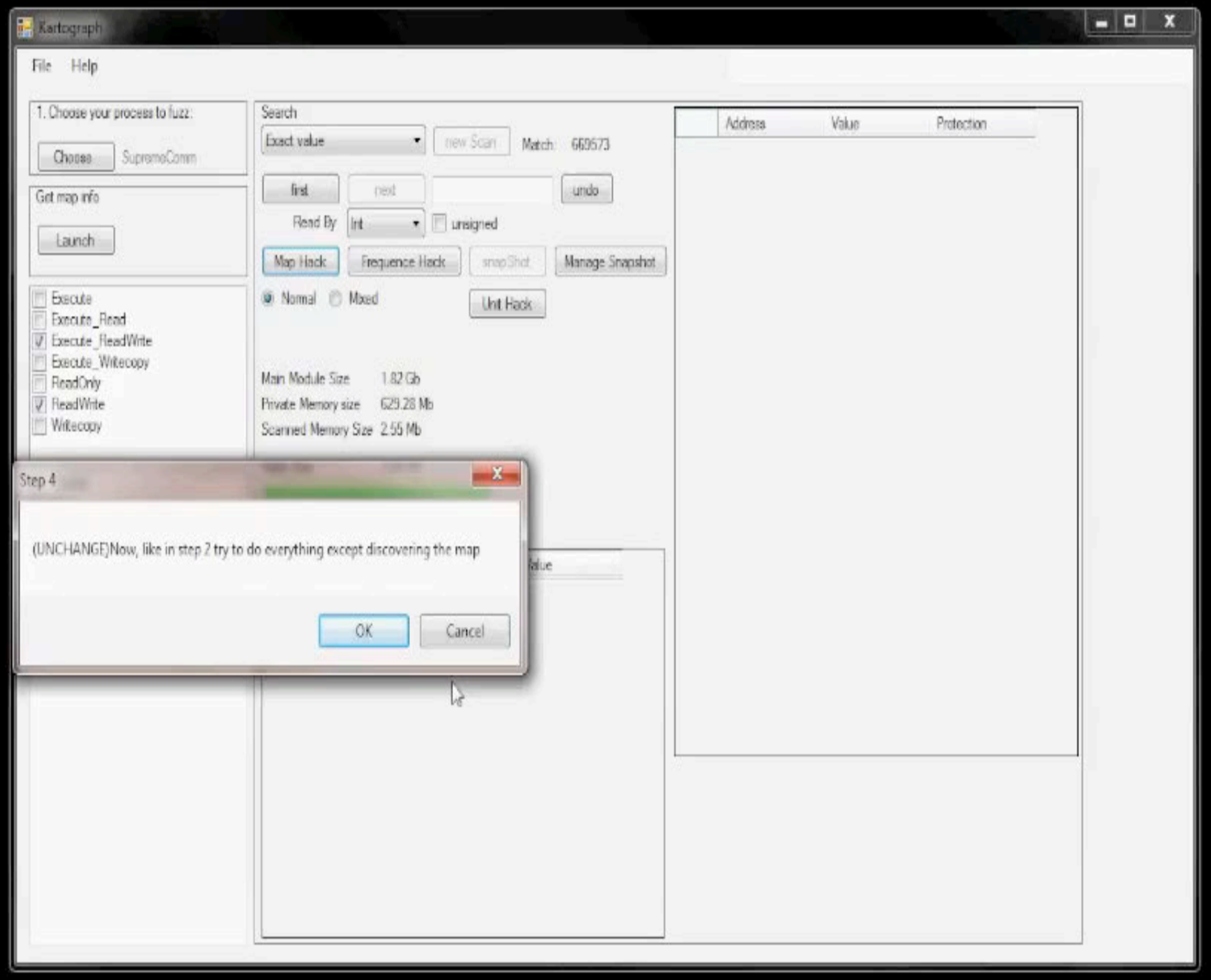
(CHANGE)Now, STOP everything. Use a unit to discover the map. Try to do a square representing 1/4 of the total map

OK Cancel

Step 3

Removing more unrelated memory


logWindows

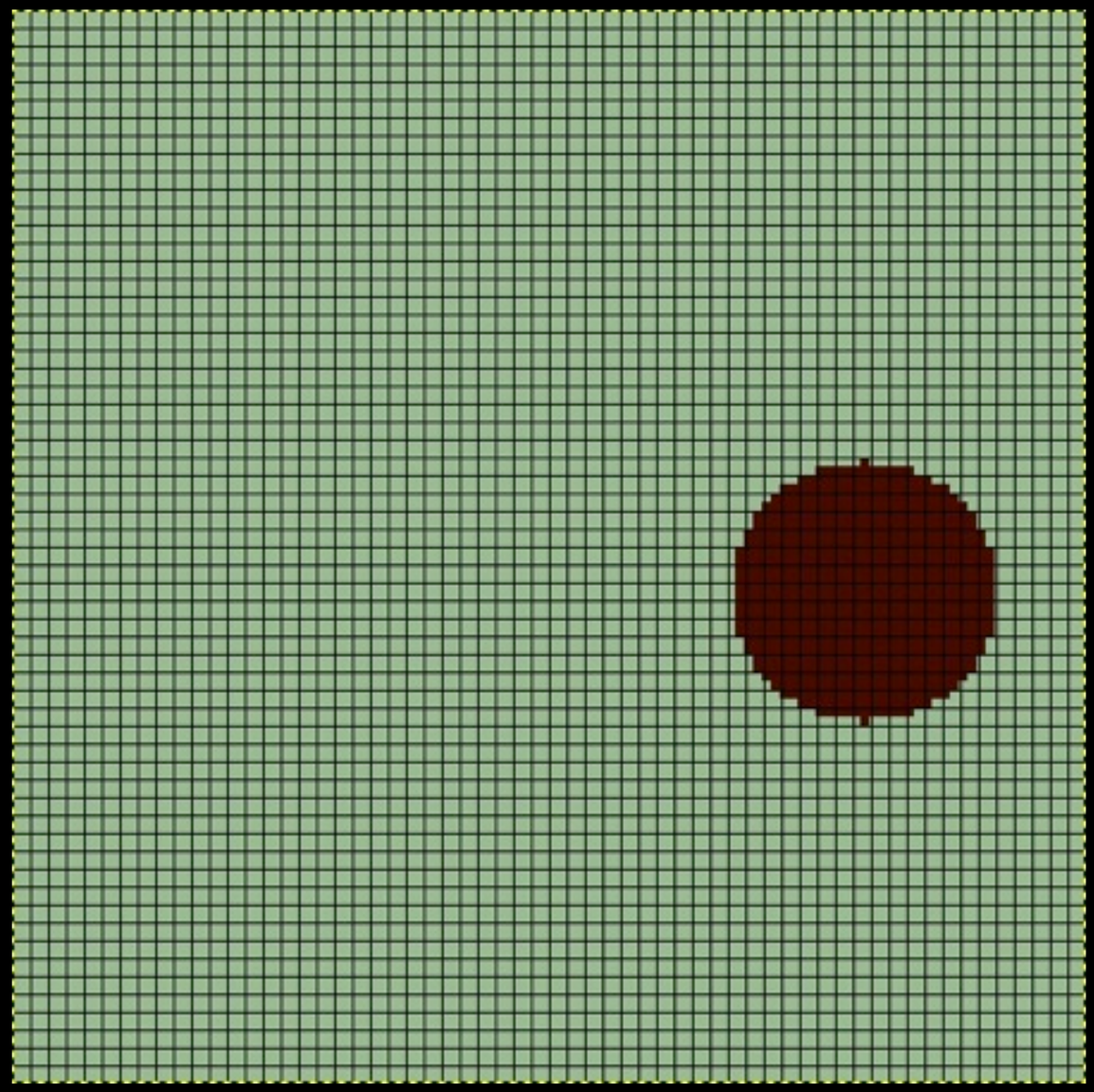

Kartograph
File
Help
1. Choose your process to fuzz:
Choose
SupremoComm
Get map info
Launch
Execute
Execute_Read
Execute_ReadWrite
Execute_Writecopy
ReadOnly
ReadWrite
Writecopy
Search
Exact value
new Scan
Match 660573
first
next
undo
Read By
Int
unsigned
Map Hack
Frequence Hack
snapShot
Manage Snapshot
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

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

Step 5

an other snapshot ?

Yes No

YES

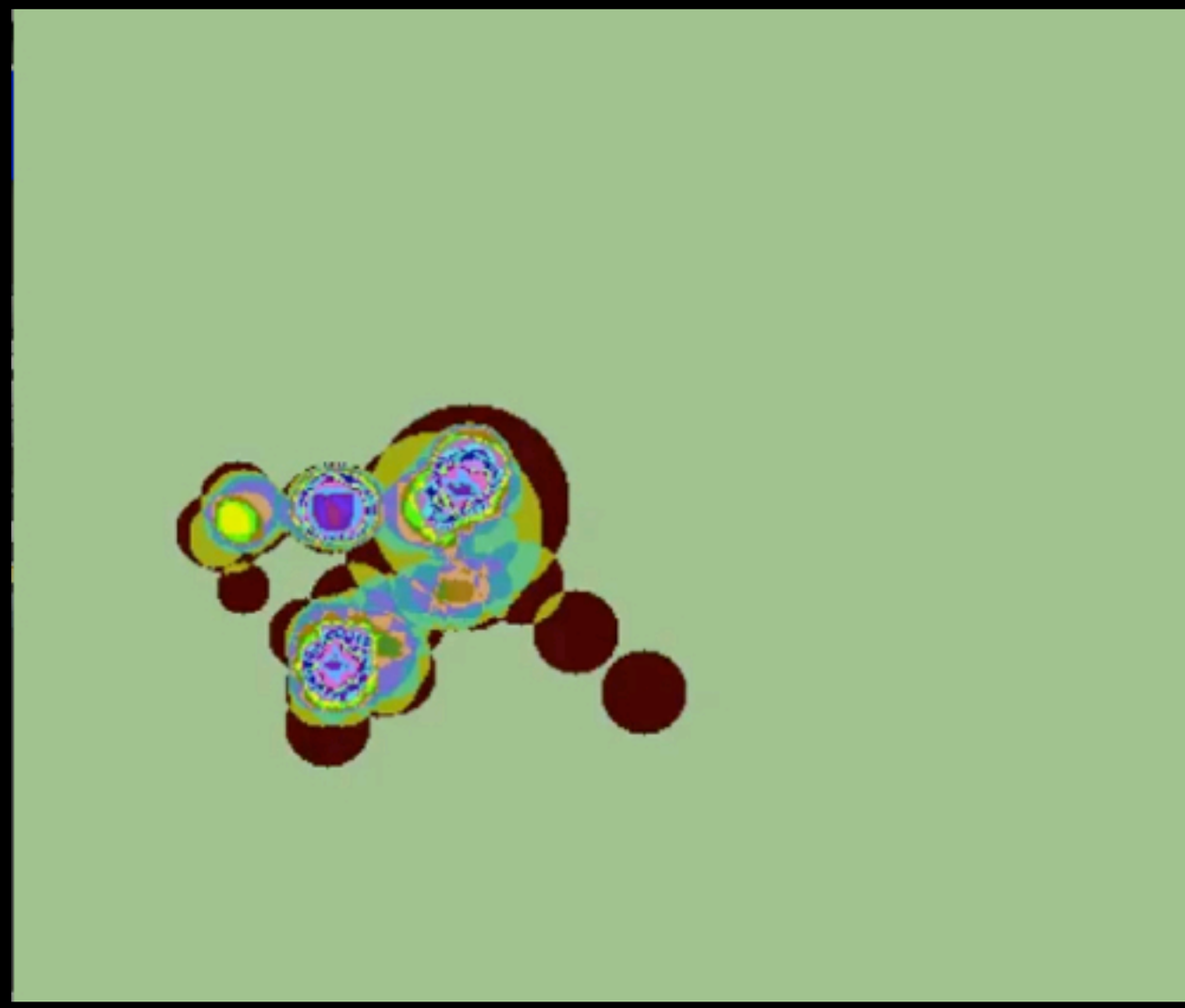
Address Value

Address Value Protection

Step 5

Isolating the potential map

In game



In memory

Step 6

Understanding the map's structure

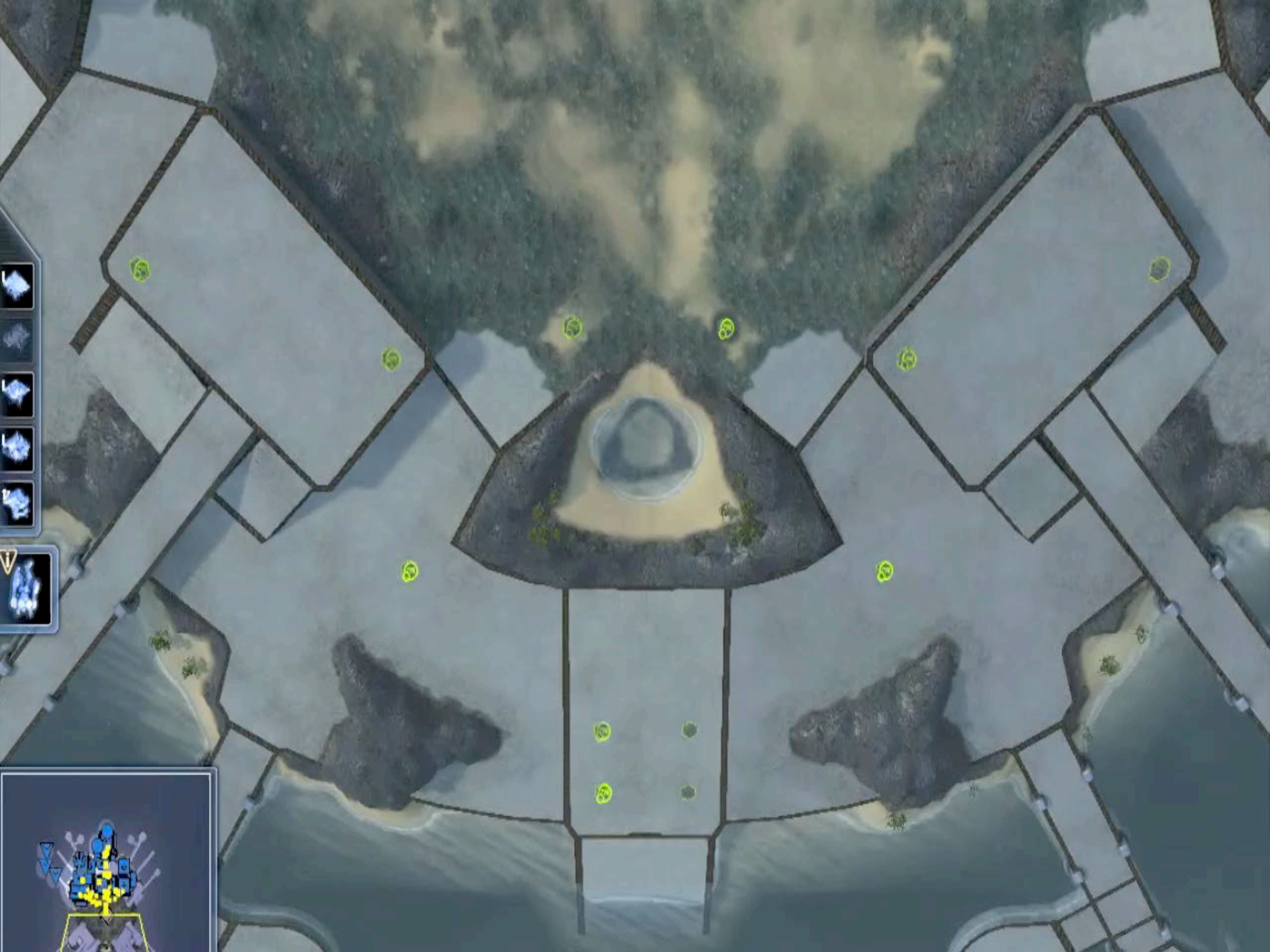
Supreme Commander 2

80 | 56985 (+16) | 99999 (+57) | 121/500 | 01:38:23 | MENU | MINIMAP

Address | Value | Protection

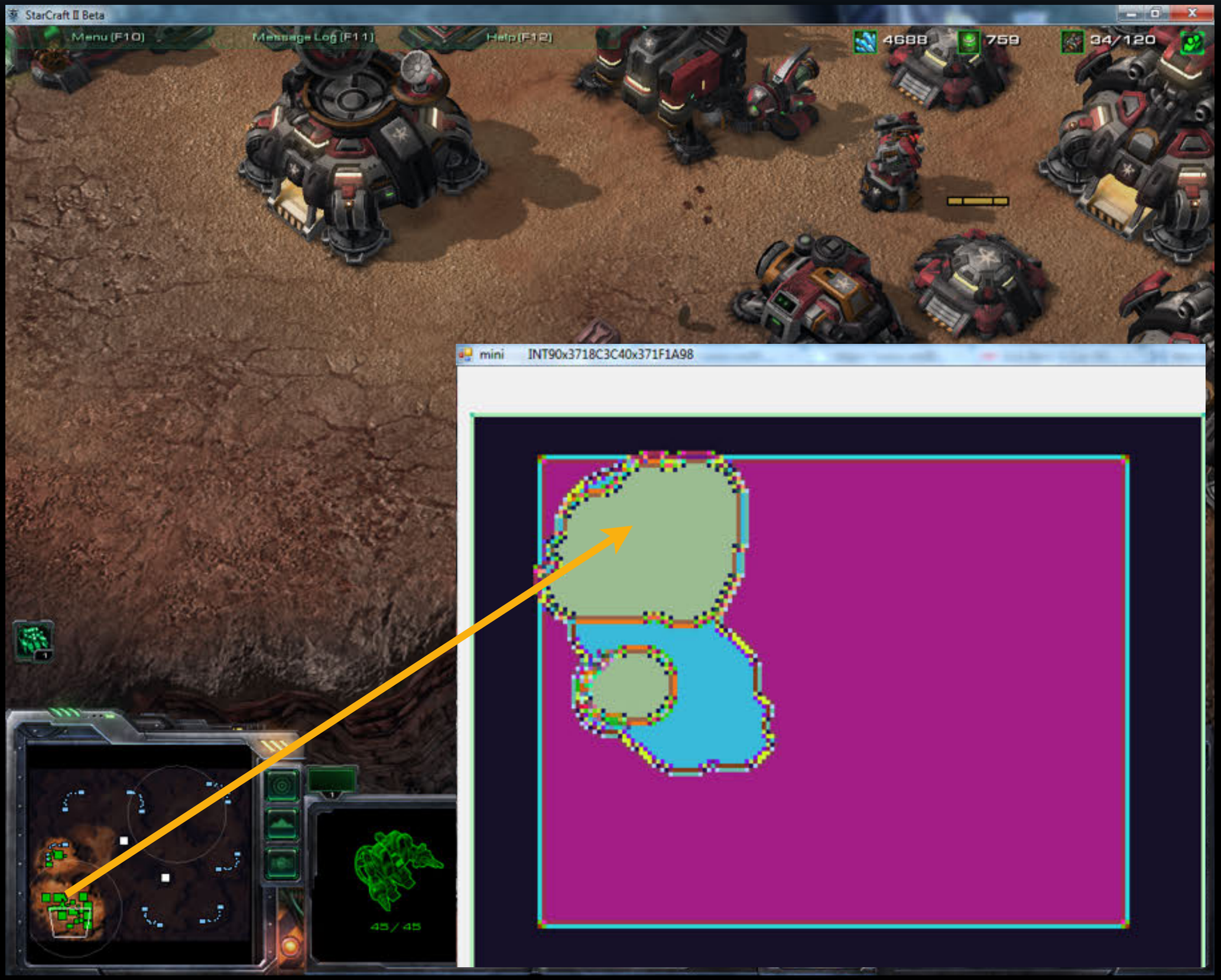
Step 8

Rewriting game memory for fun and profit



Starcraft 2 mini map

Starcraft 2 mini map



Unexpected effects

+88

20

Santa Maria

unit hacks

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

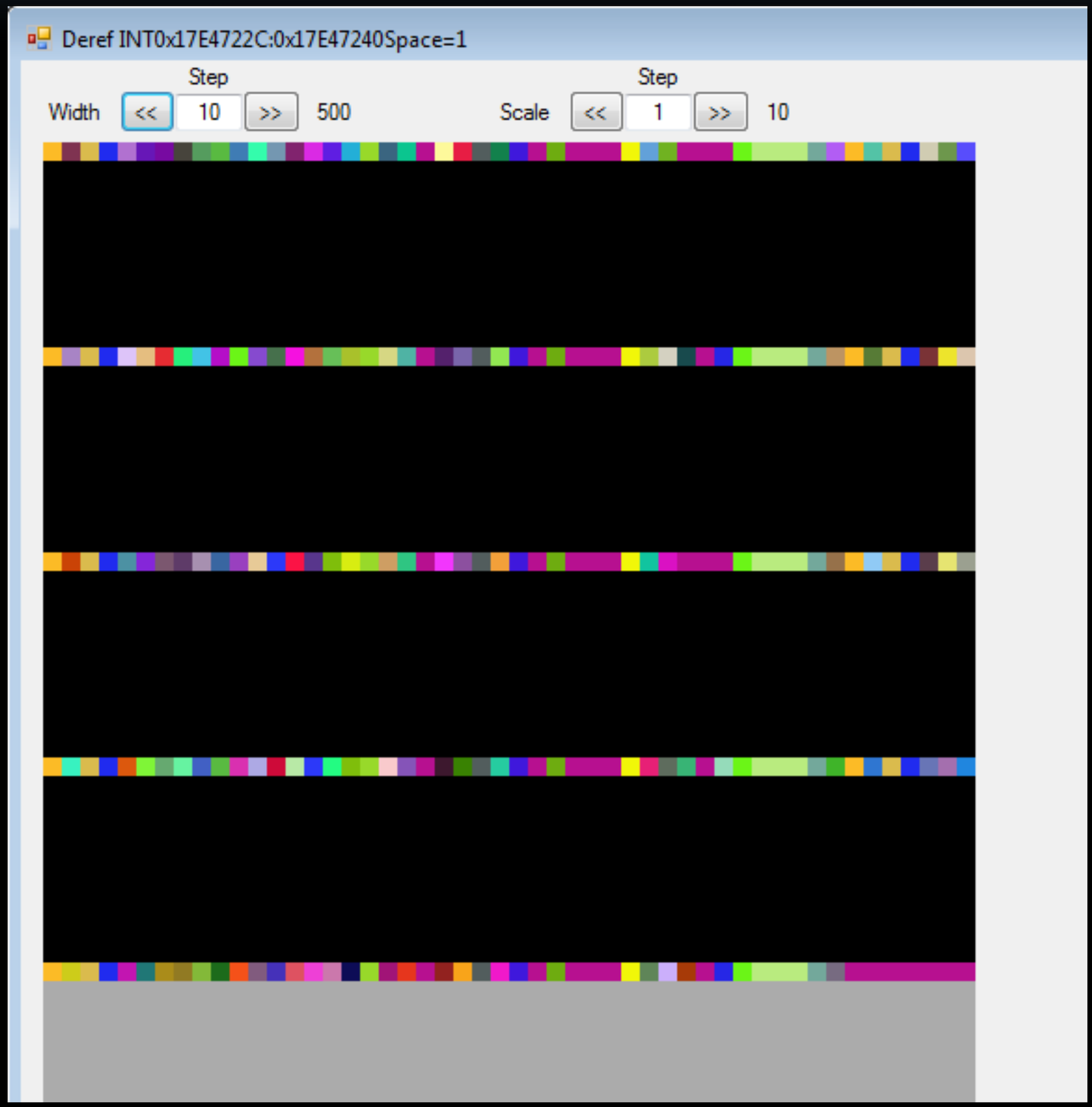
Game memory

Unit hack Step

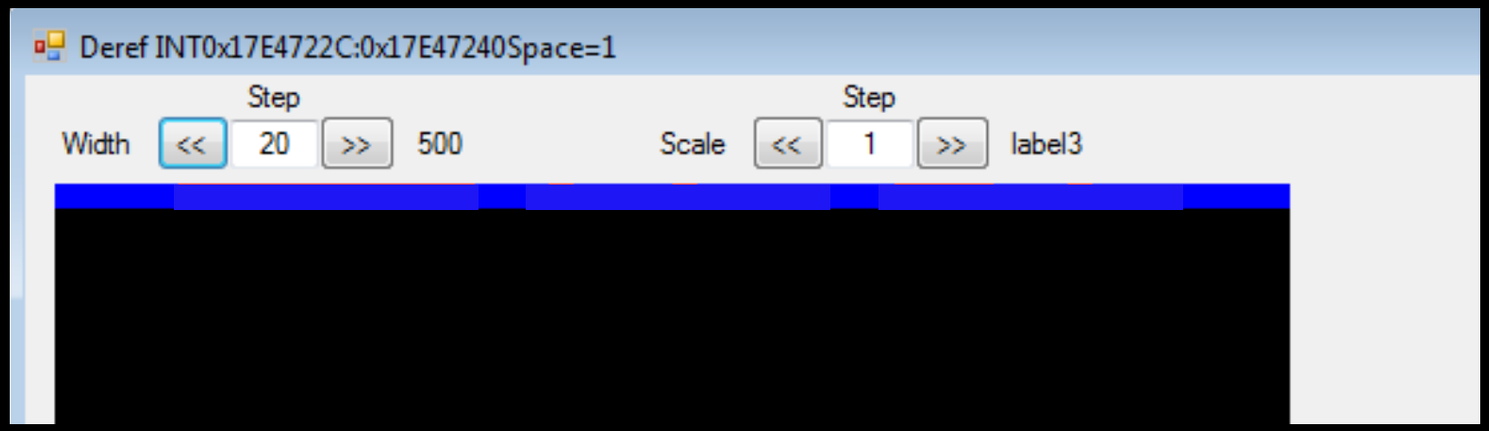
Unit hack Step

Unit hack Step

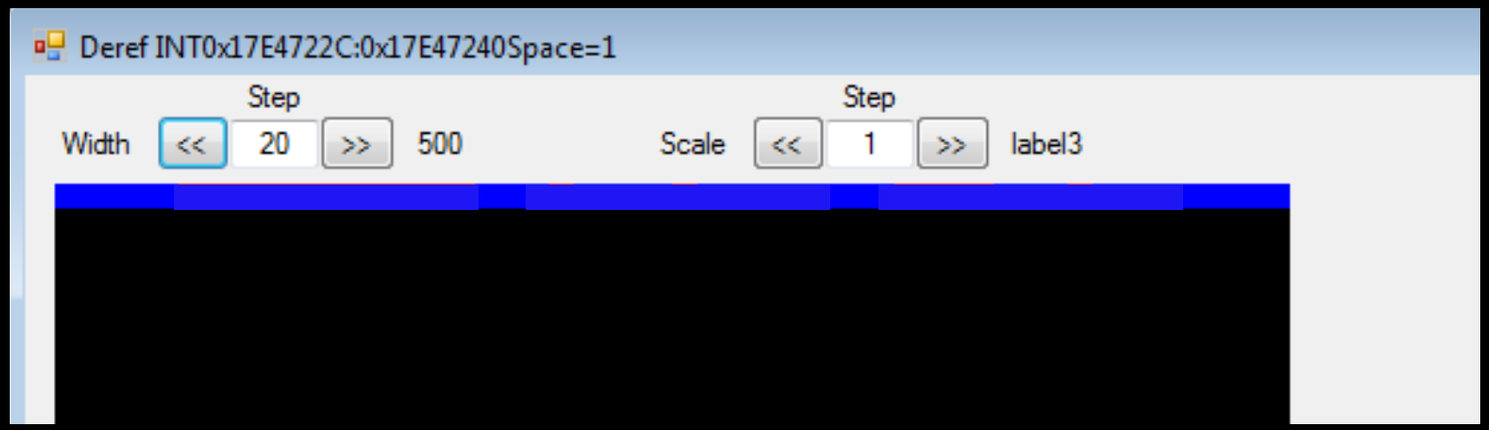
Unit Hack shape



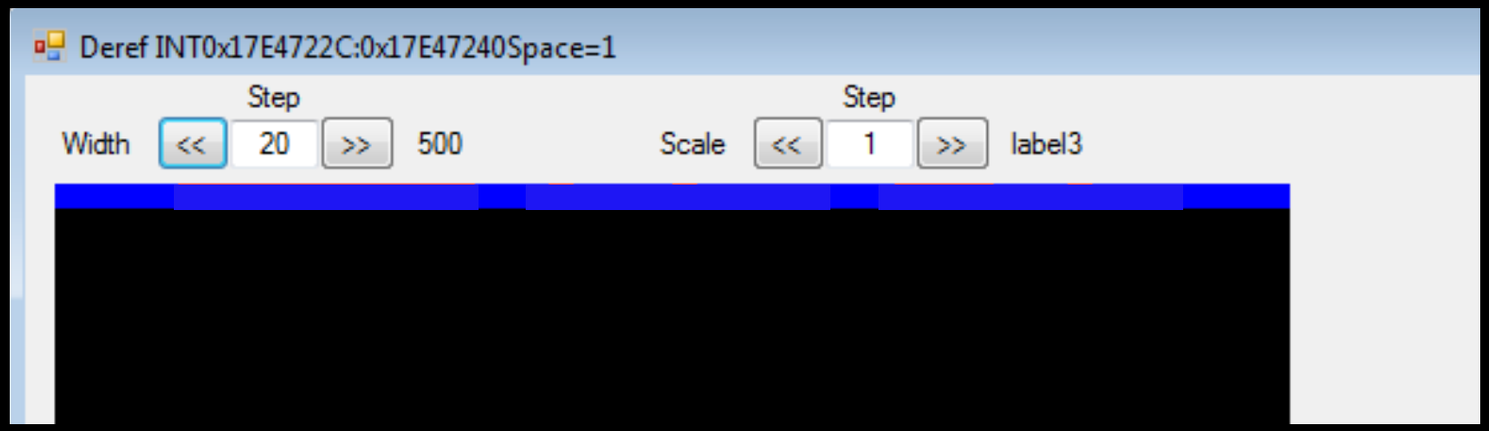
Understanding unit structure

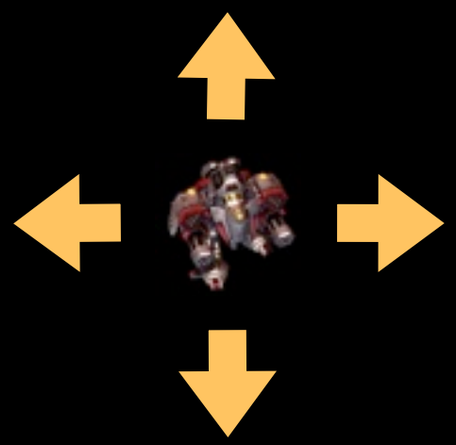


Understanding unit structure



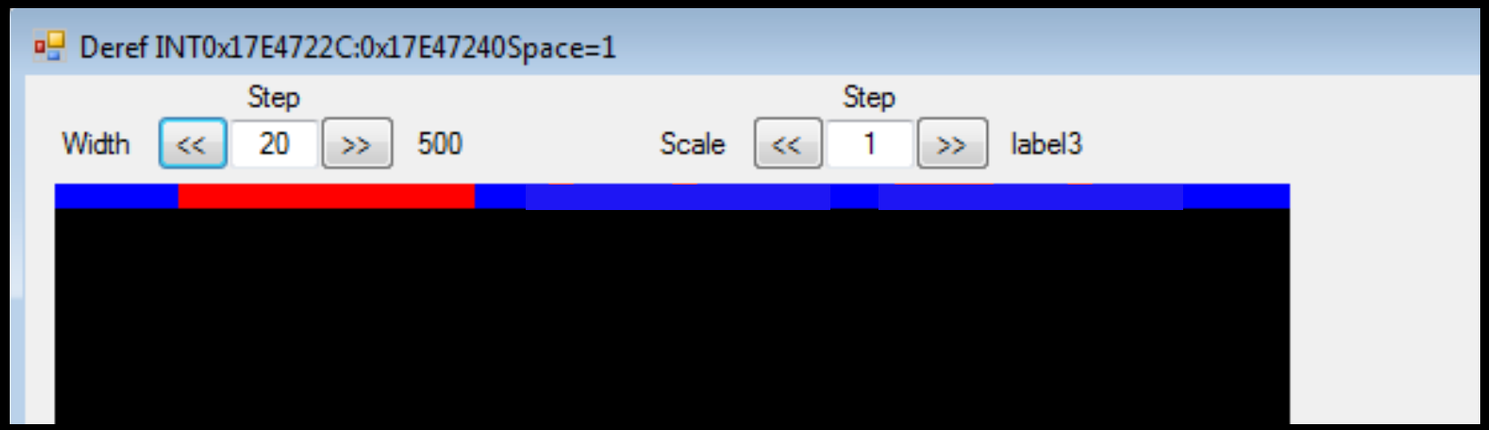
Understanding unit structure

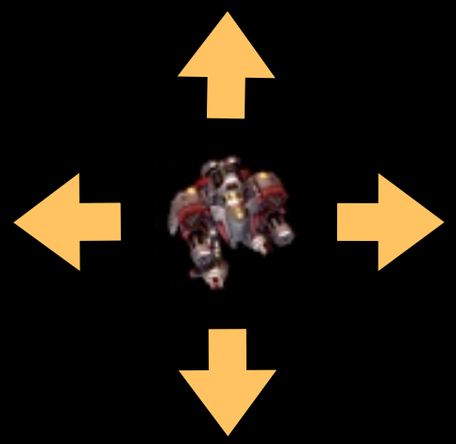




make it move

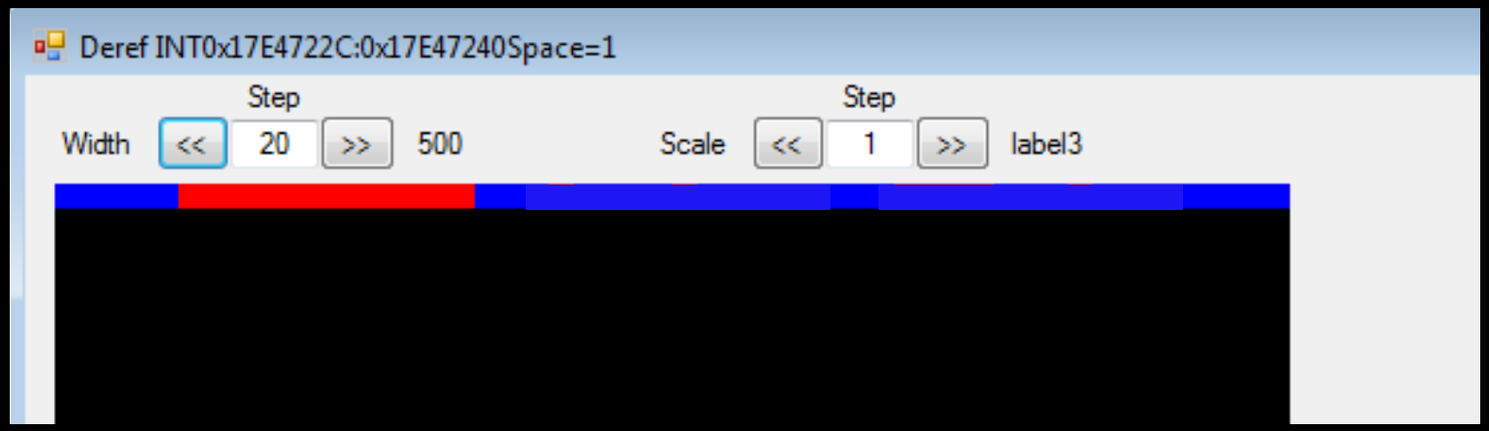
Understanding unit structure

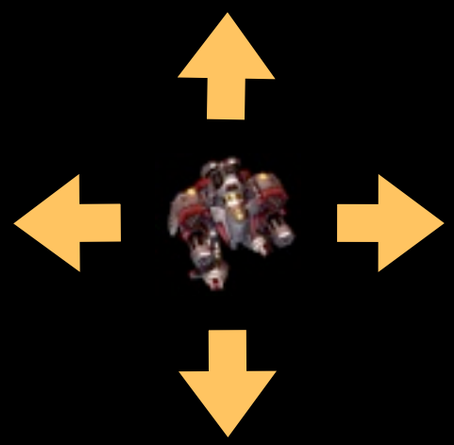




make it move

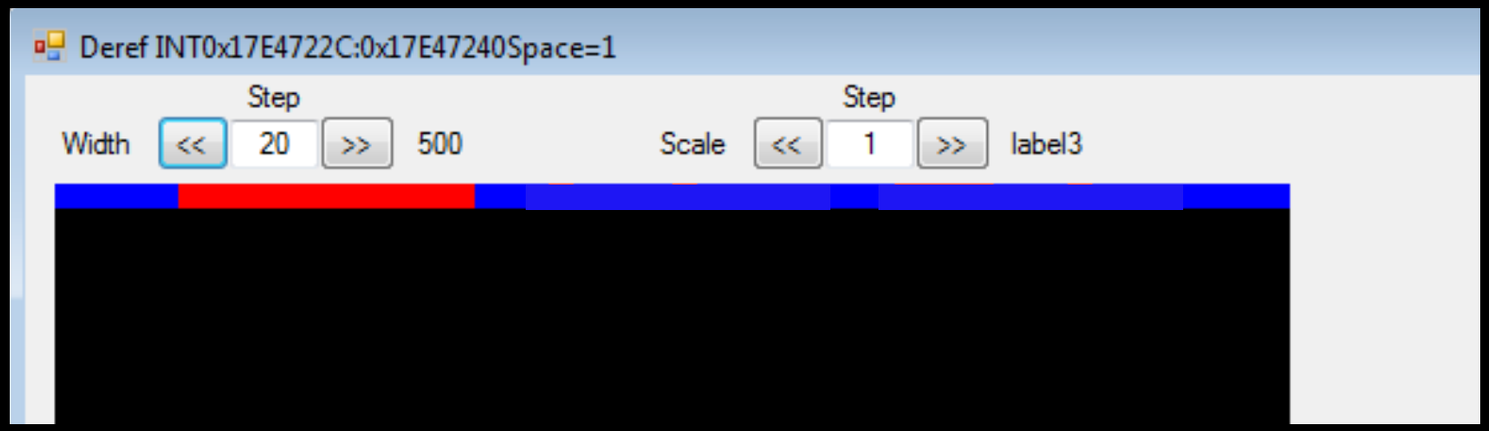
Understanding unit structure

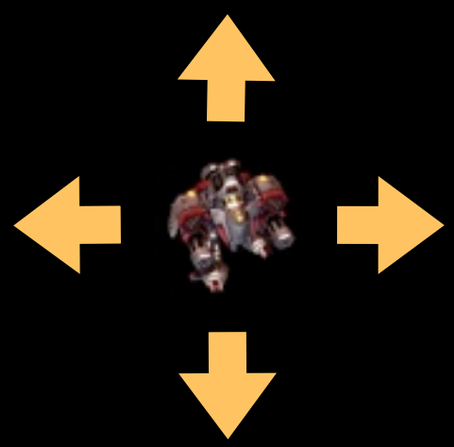




make it move

Understanding unit structure

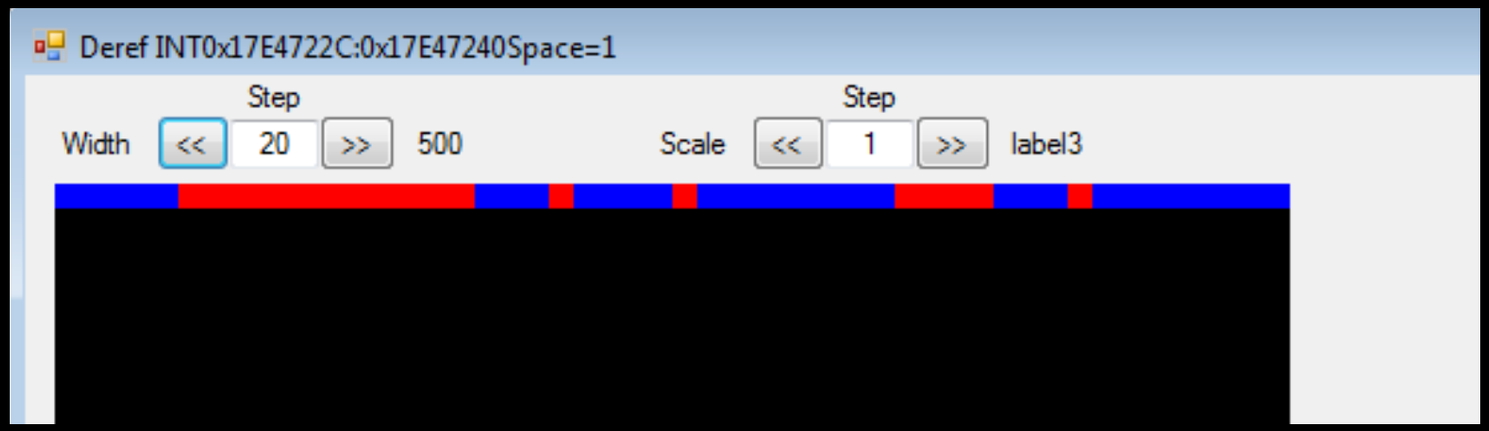


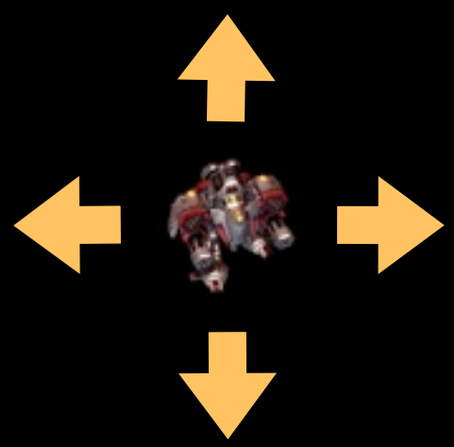


make it move

make it bleed

Understanding unit structure





make it move

make it bleed

V: Imperial Age

Menu

+12

Imperial Nassauer
• Hand infantry

6

10 / 110

2293

1359

925

4

Imperial Espada

Commands

Network

Here is what happen when you are actively cheating

Here is what happen when you are actively cheating

Rewriting network traffic

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

```
Administrator: C:\Windows\System32\cmd.exe - instlsp64.exe  -p

Winsock 32-bit Catalog:
======================
2620 - vlspListener over [RSVP TCP Service Provider]
2621 - vlspListener over [MSAFD Tcpip [TCP/IP]]
2622 - vlspListener over [MSAFD Tcpip [UDP/IP]]
2623 - vlspListener over [MSAFD Tcpip [RAW/IP]]
2624 - vlspListener over [MSAFD Tcpip [TCP/IPv6]]
2625 - vlspListener over [MSAFD Tcpip [UDP/IPv6]]
2626 - vlspListener over [MSAFD Tcpip [RAW/IPv6]]
2627 - vlspListener over [RSVP TCPv6 Service Provider]
2628 - vlspListener over [RSVP UDPv6 Service Provider]
2629 - vlspListener over [RSVP UDP Service Provider]
2630 - vlspListener over [MSAFD Pgm (RDM)]
2631 - vlspListener over [MSAFD Pgm (Stream)]
2632 - vlspListener over [VMCI sockets DGRAM]
2633 - vlspListener over [VMCI sockets STREAM]
1008 - RSVP TCP Service Provider
1001 - MSAFD Tcpip [TCP/IP]
1002 - MSAFD Tcpip [UDP/IP]
1003 - MSAFD Tcpip [RAW/IP]
1004 - MSAFD Tcpip [TCP/IPv6]
1005 - MSAFD Tcpip [UDP/IPv6]
1006 - MSAFD Tcpip [RAW/IPv6]
1007 - RSVP TCPv6 Service Provider
1009 - RSVP UDPv6 Service Provider
1010 - RSVP UDP Service Provider
1011 - MSAFD Pgm (RDM)
1012 - MSAFD Pgm (Stream)
1019 - VMCI sockets DGRAM
1020 - VMCI sockets STREAM
2605 - vlspListener
Press any key to continue...

C:\svn\project\lsp\trunk\lsp\bin>instlsp64.exe -p

Winsock 64-bit Catalog:
======================
2606 - vlspListener over [RSVP TCP Service Provider]
2607 - vlspListener over [MSAFD Tcpip [TCP/IP]]
2608 - vlspListener over [MSAFD Tcpip [UDP/IP]]
2609 - vlspListener over [MSAFD Tcpip [RAW/IP]]
2610 - vlspListener over [MSAFD Tcpip [TCP/IPv6]]
2611 - vlspListener over [MSAFD Tcpip [UDP/IPv6]]
2612 - vlspListener over [MSAFD Tcpip [RAW/IPv6]]
2613 - vlspListener over [RSVP TCPv6 Service Provider]
2614 - vlspListener over [RSVP UDPv6 Service Provider]
2615 - vlspListener over [RSVP UDP Service Provider]
2616 - vlspListener over [MSAFD Pgm (RDM)]
2617 - vlspListener over [MSAFD Pgm (Stream)]
2618 - vlspListener over [VMCI sockets DGRAM]
2619 - vlspListener over [VMCI sockets STREAM]
1008 - RSVP TCP Service Provider
1001 - MSAFD Tcpip [TCP/IP]
1002 - MSAFD Tcpip [UDP/IP]
1003 - MSAFD Tcpip [RAW/IP]
1004 - MSAFD Tcpip [TCP/IPv6]
1005 - MSAFD Tcpip [UDP/IPv6]
1006 - MSAFD Tcpip [RAW/IPv6]
1007 - RSVP TCPv6 Service Provider
1009 - RSVP UDPv6 Service Provider
1010 - RSVP UDP Service Provider
1011 - MSAFD Pgm (RDM)
1012 - MSAFD Pgm (Stream)
1013 - VMCI sockets DGRAM
1014 - VMCI sockets STREAM
2604 - vlspListener
Press any key to continue...
```

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

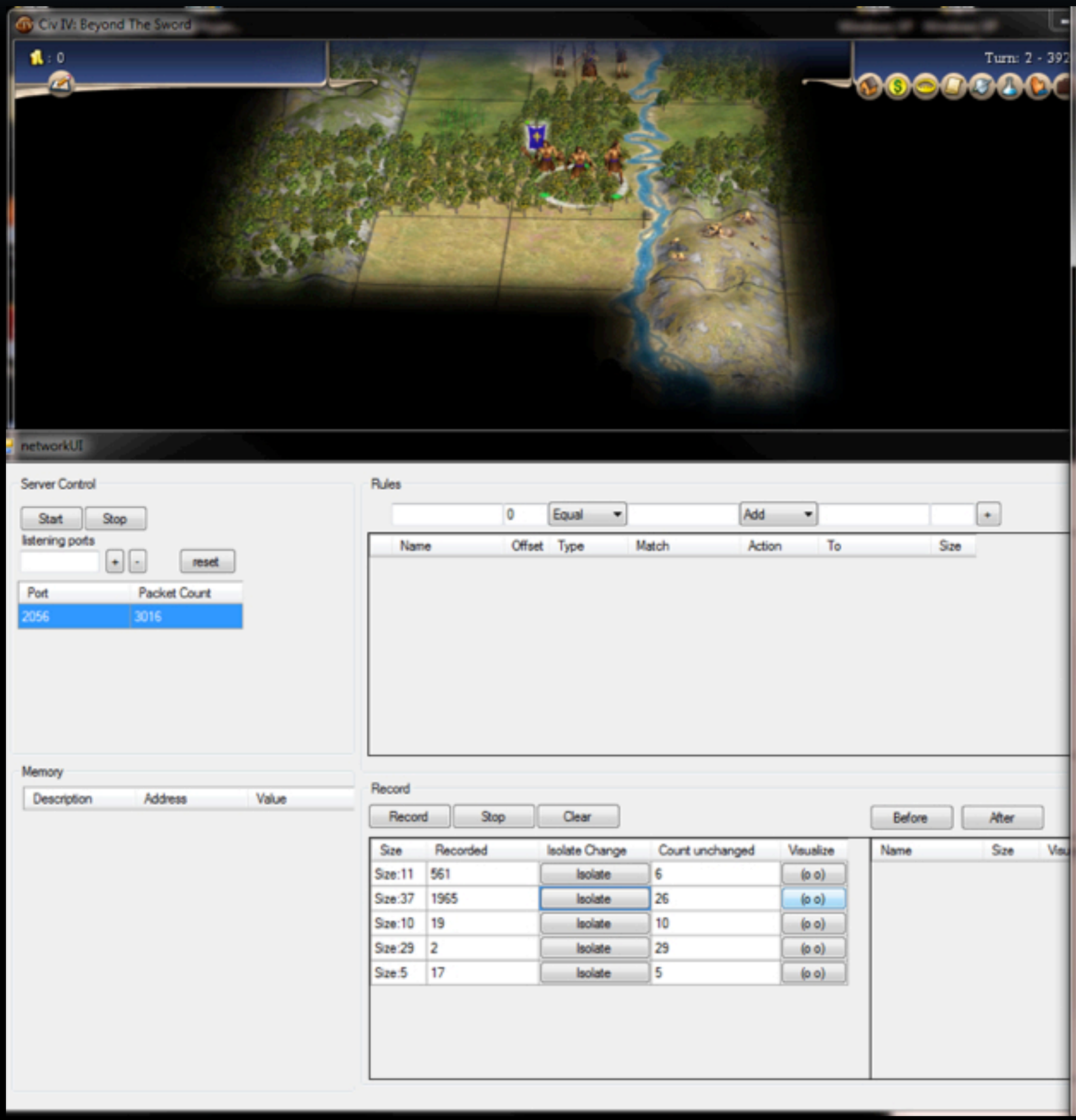
Bucket

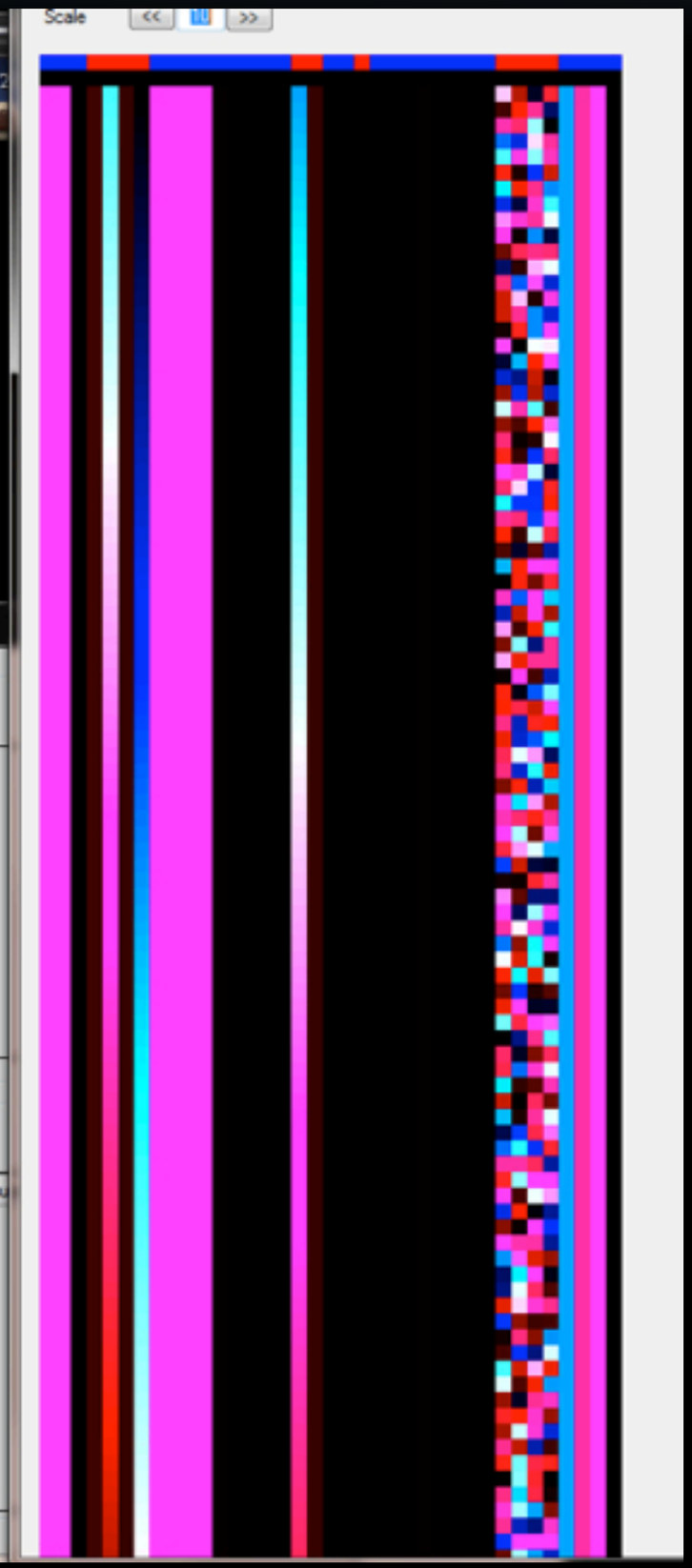
Visualize

Understand

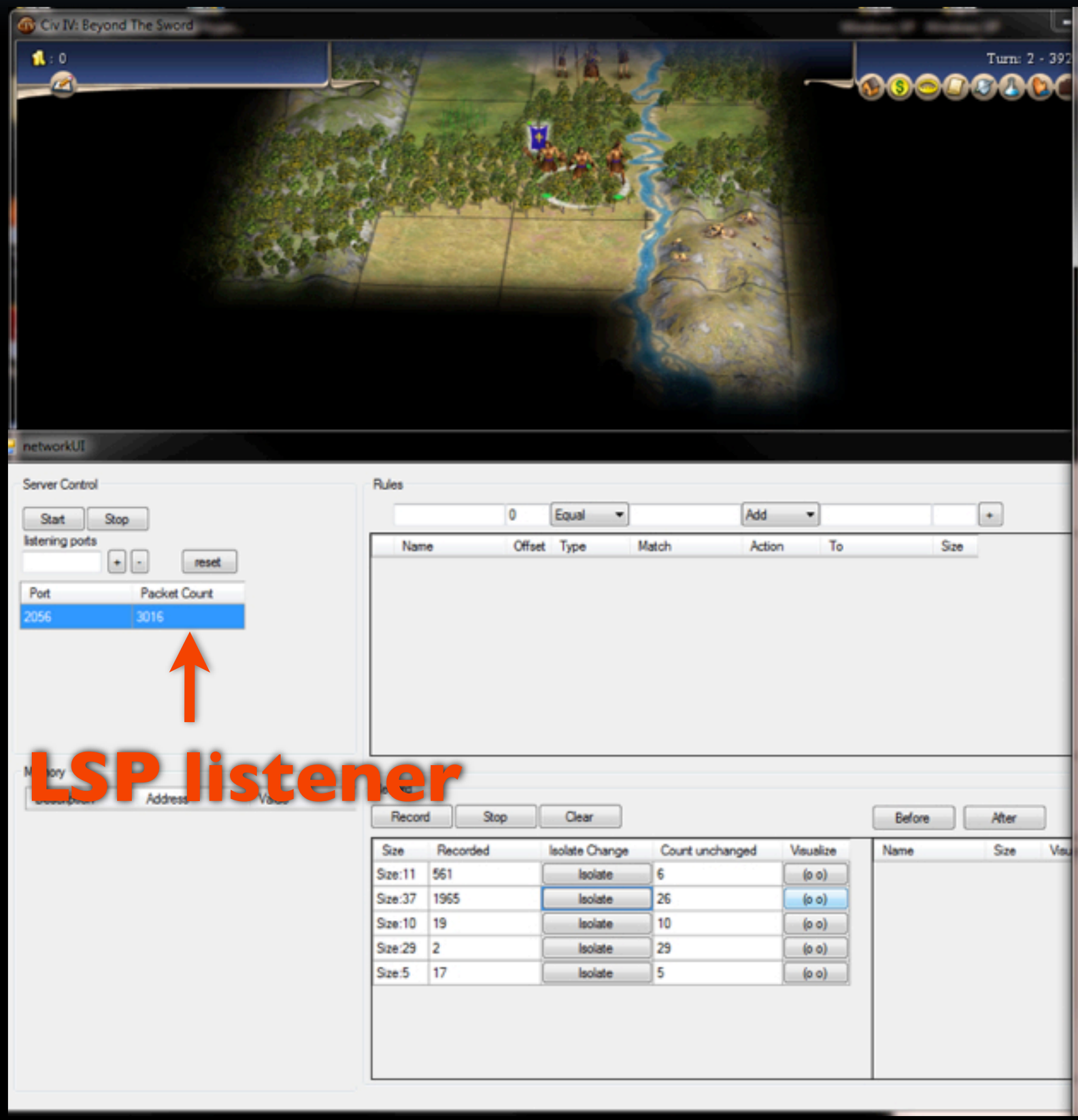
Resync

Civilization 4 vizualization

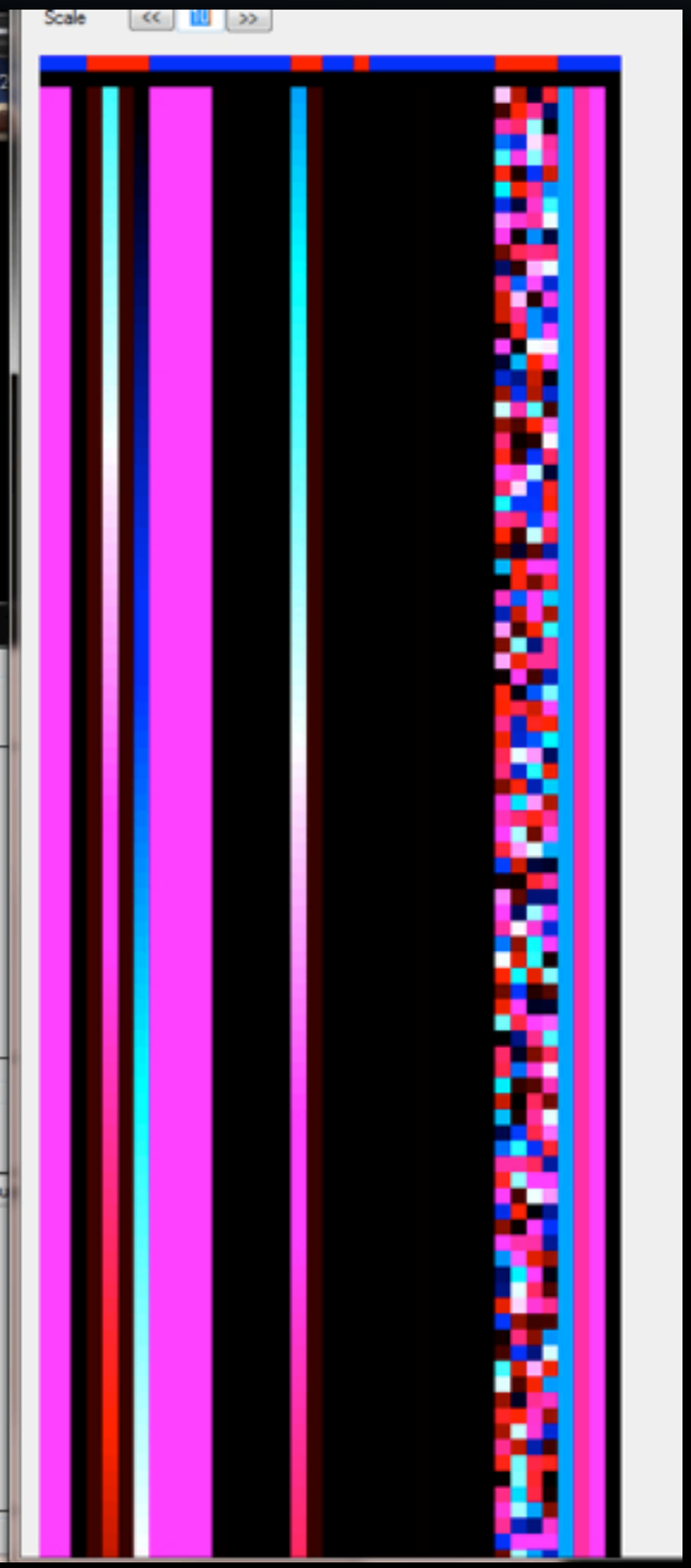




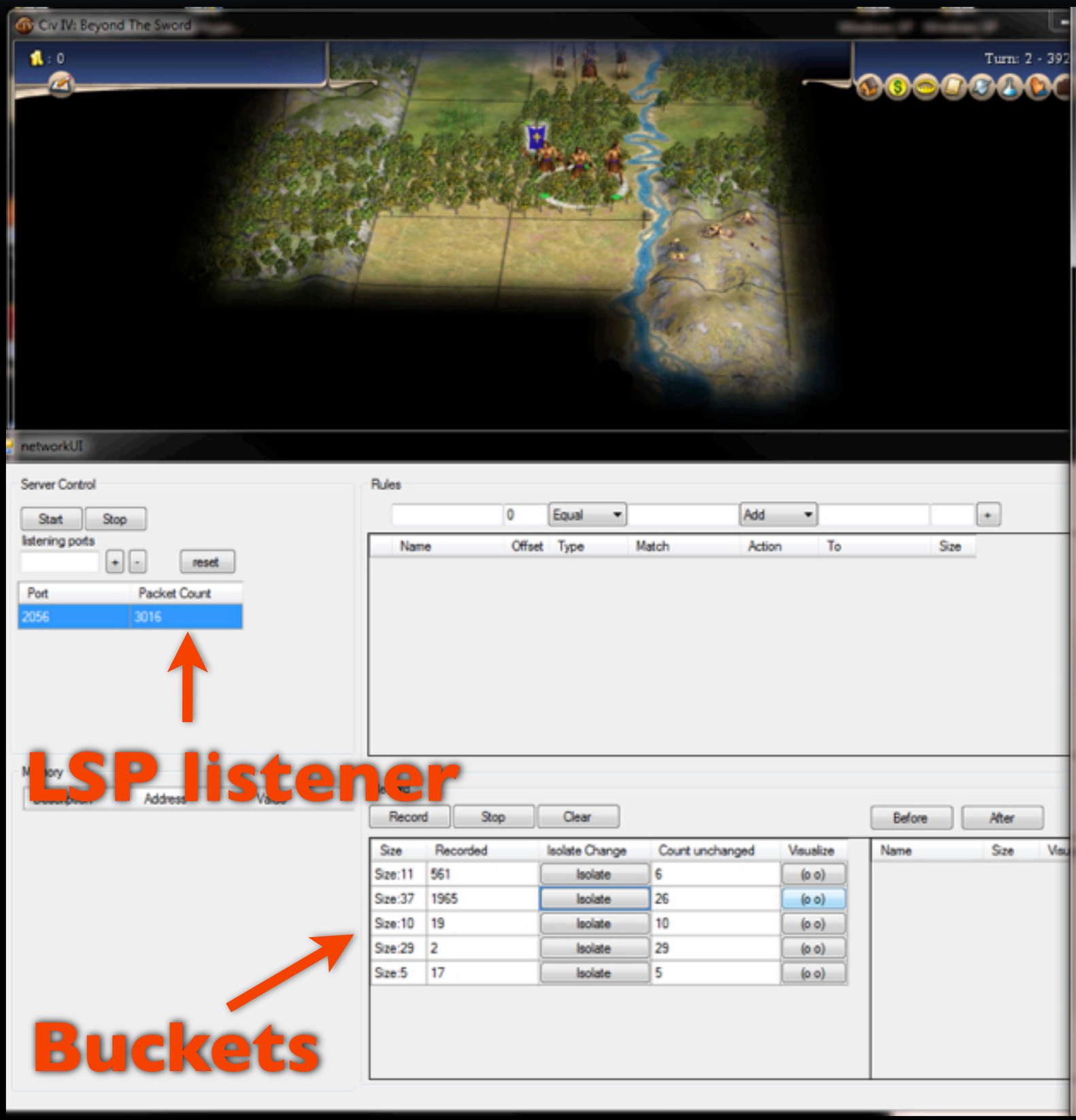
Civilization 4 vizualization

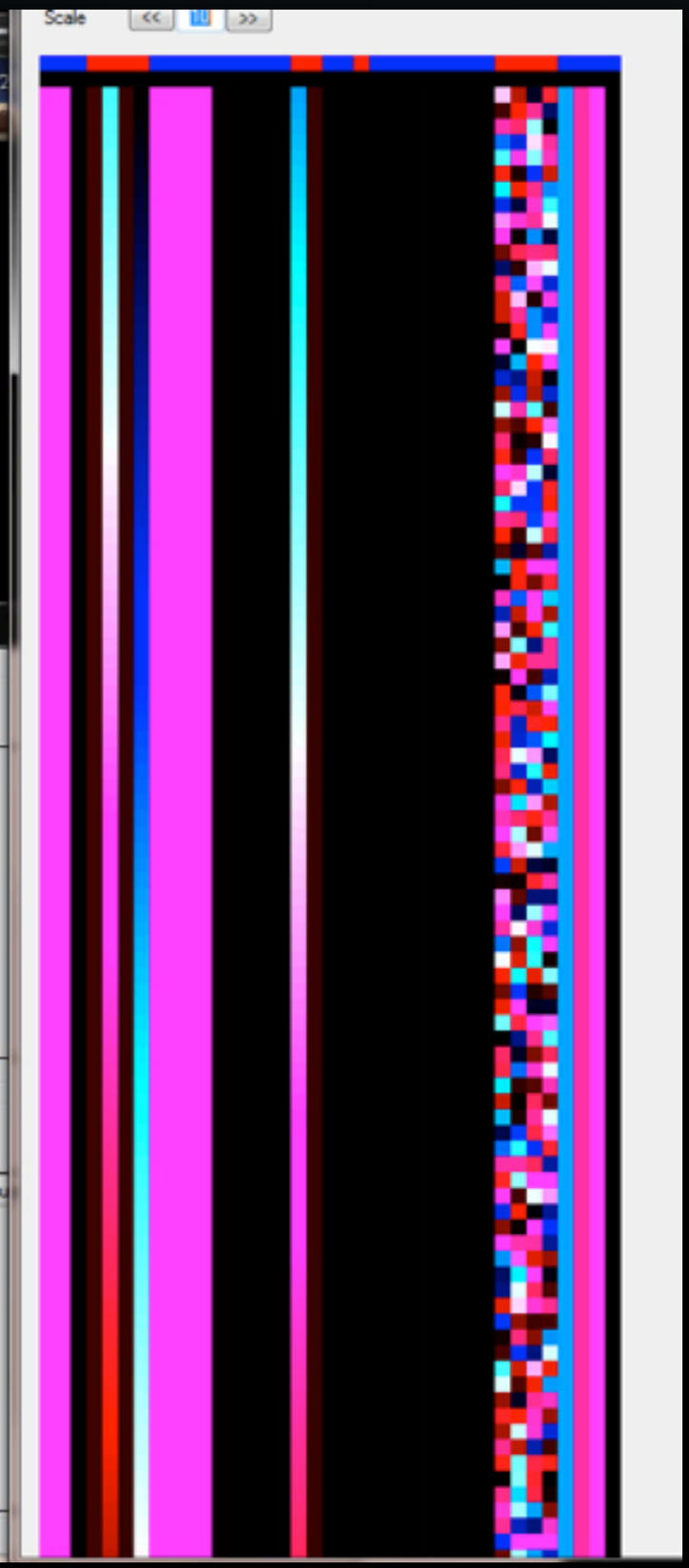


LSP listener

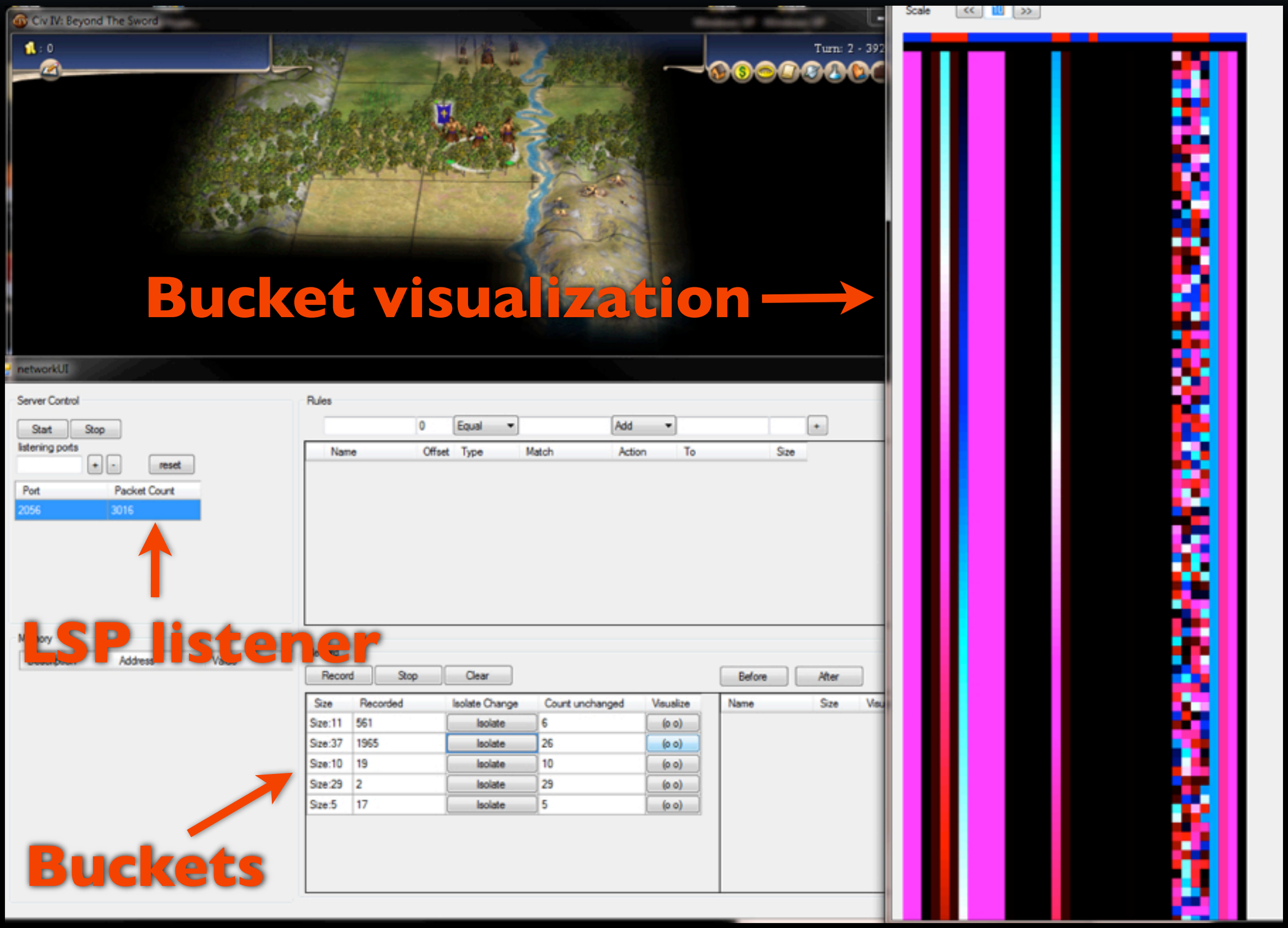


Civilization 4 vizualization

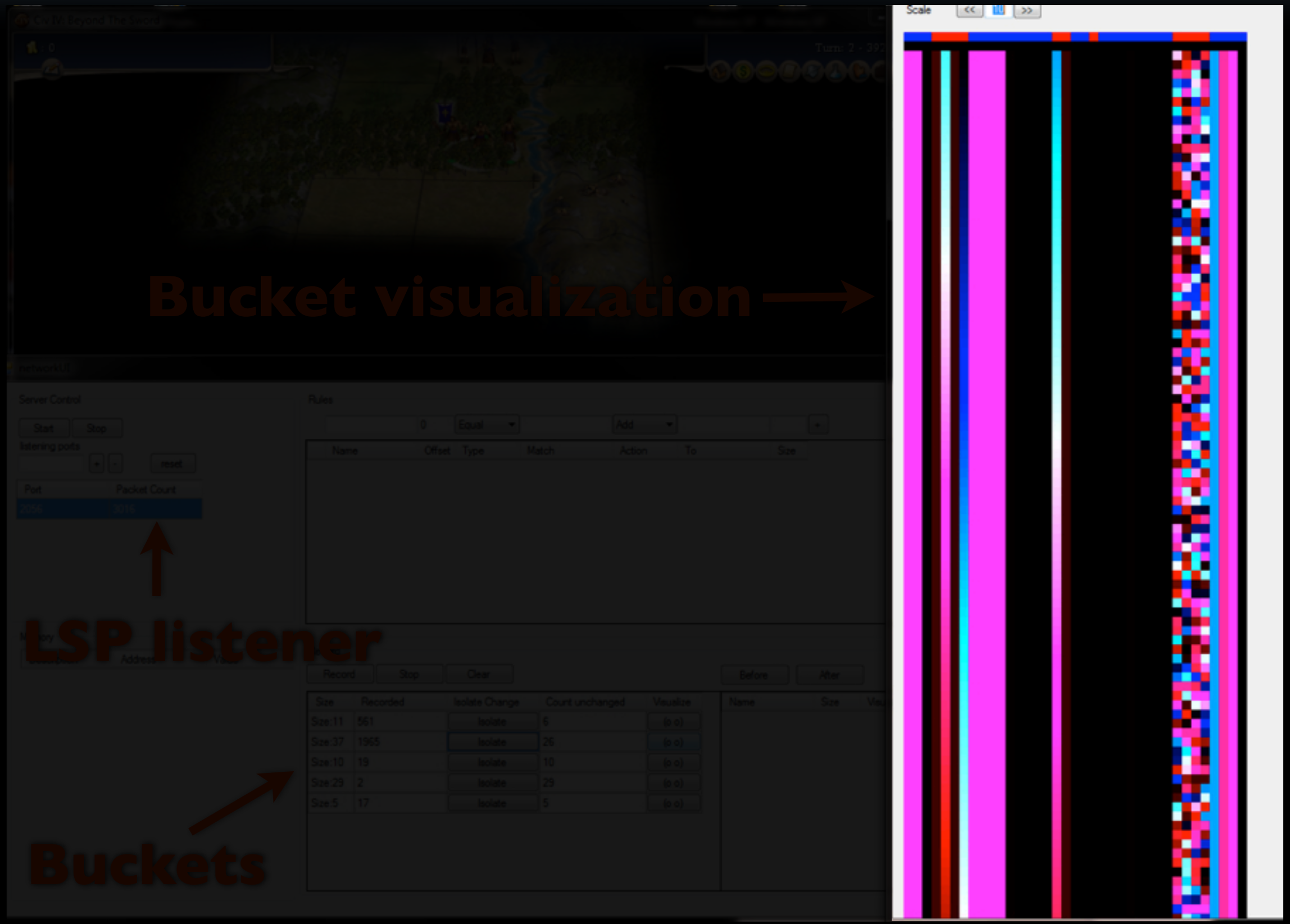




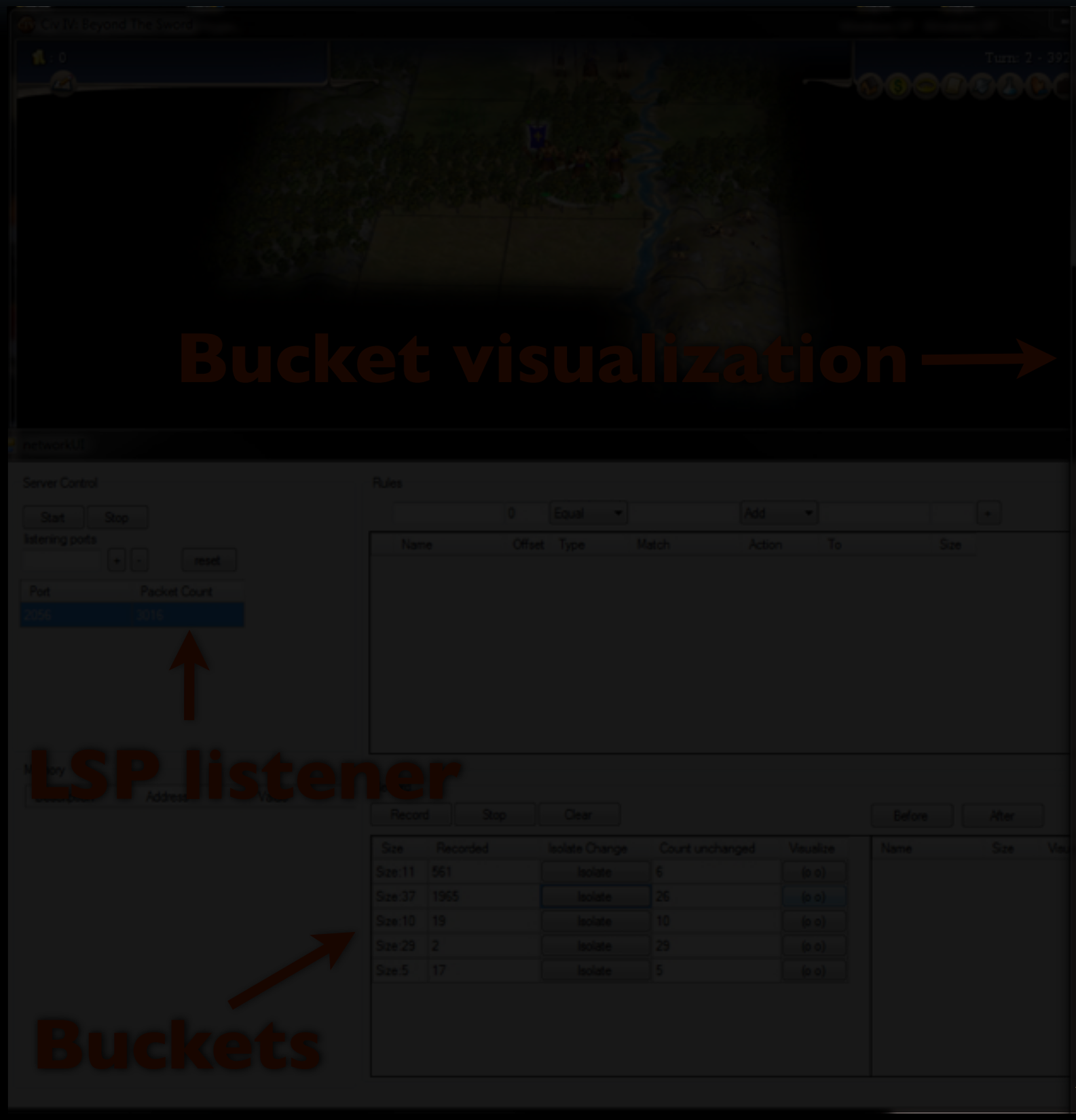
Civilization 4 vizualization

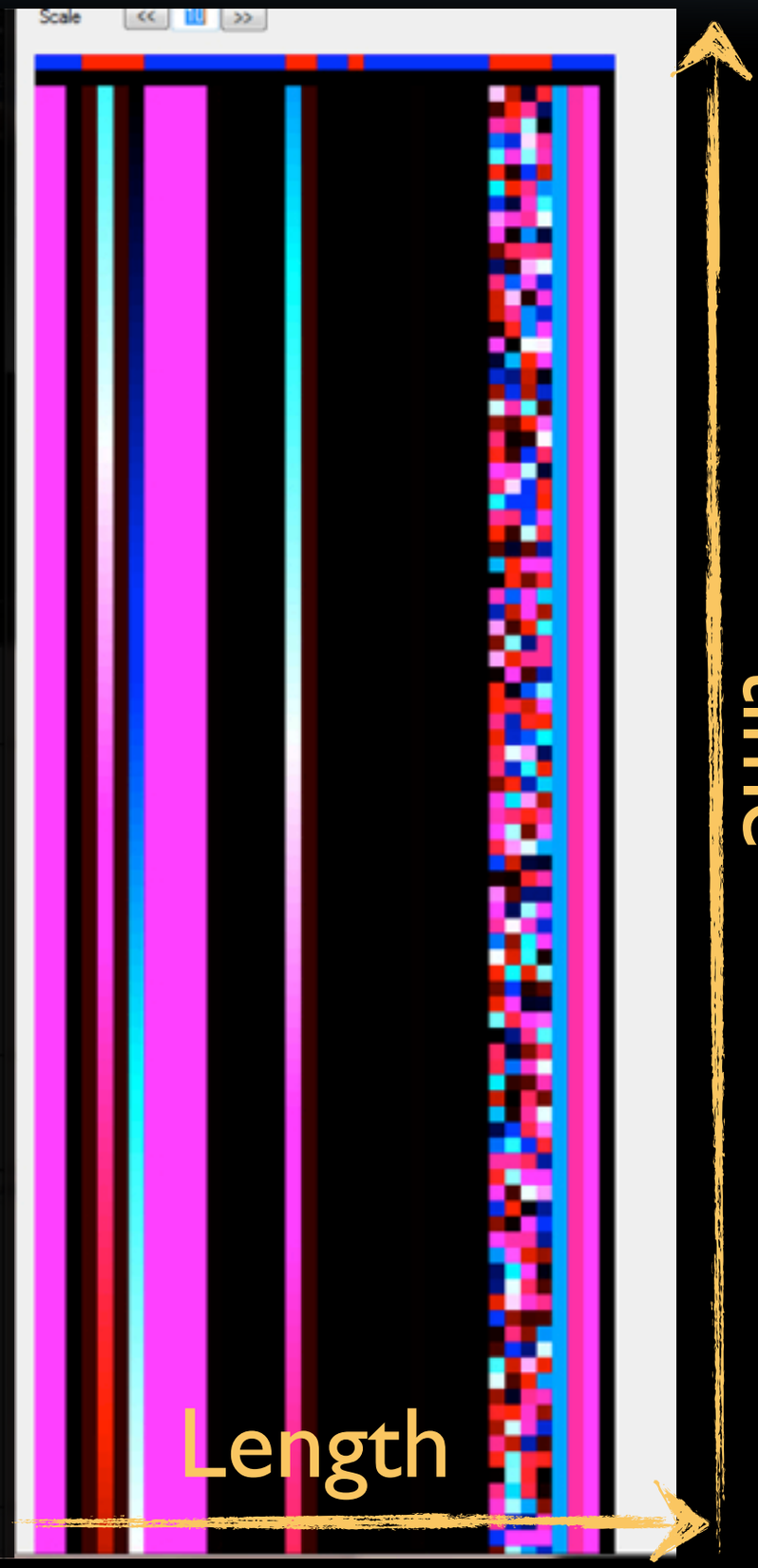


Civilization 4 vizualization



Civilization 4 vizualization





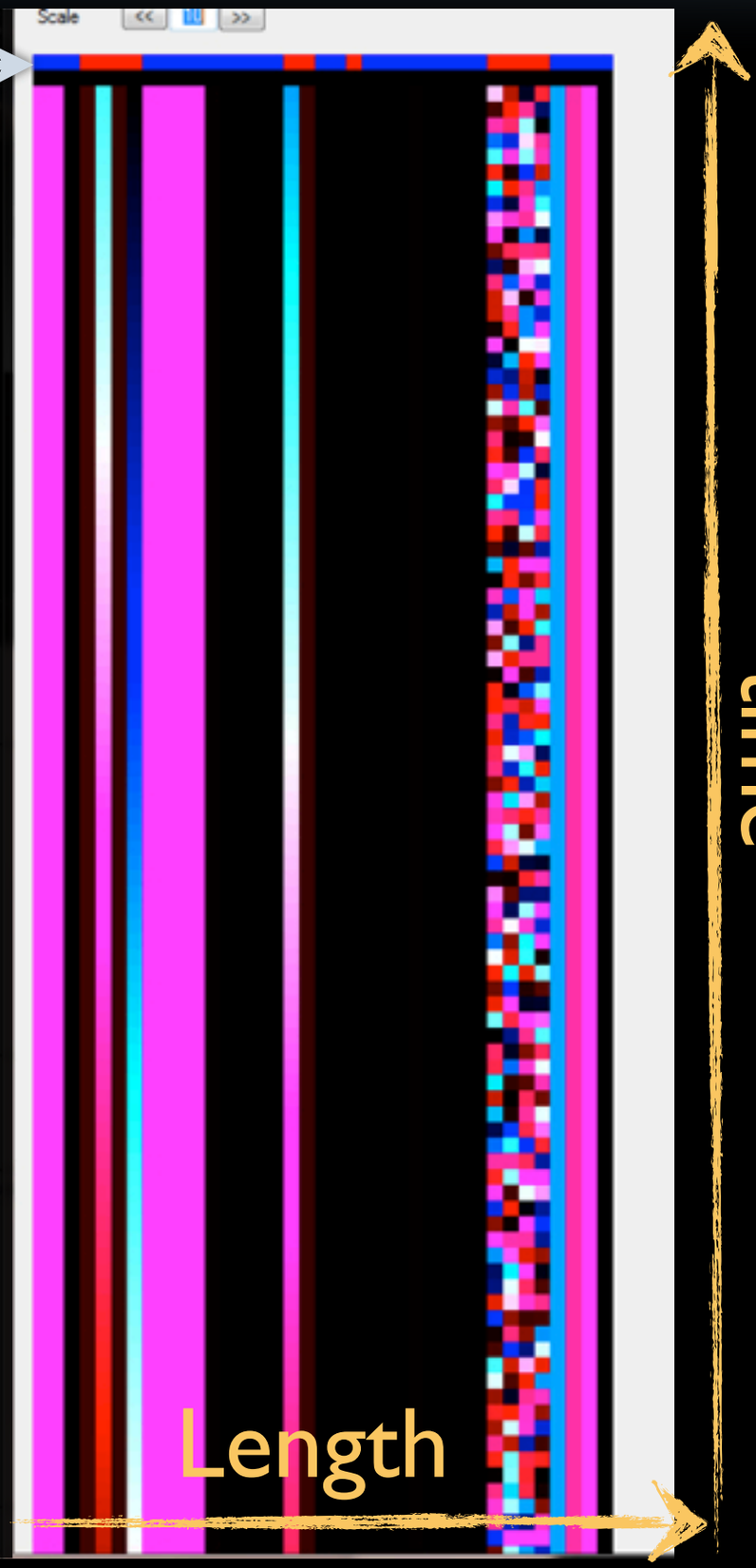
Civilization 4 vizualization

Trace diff map →

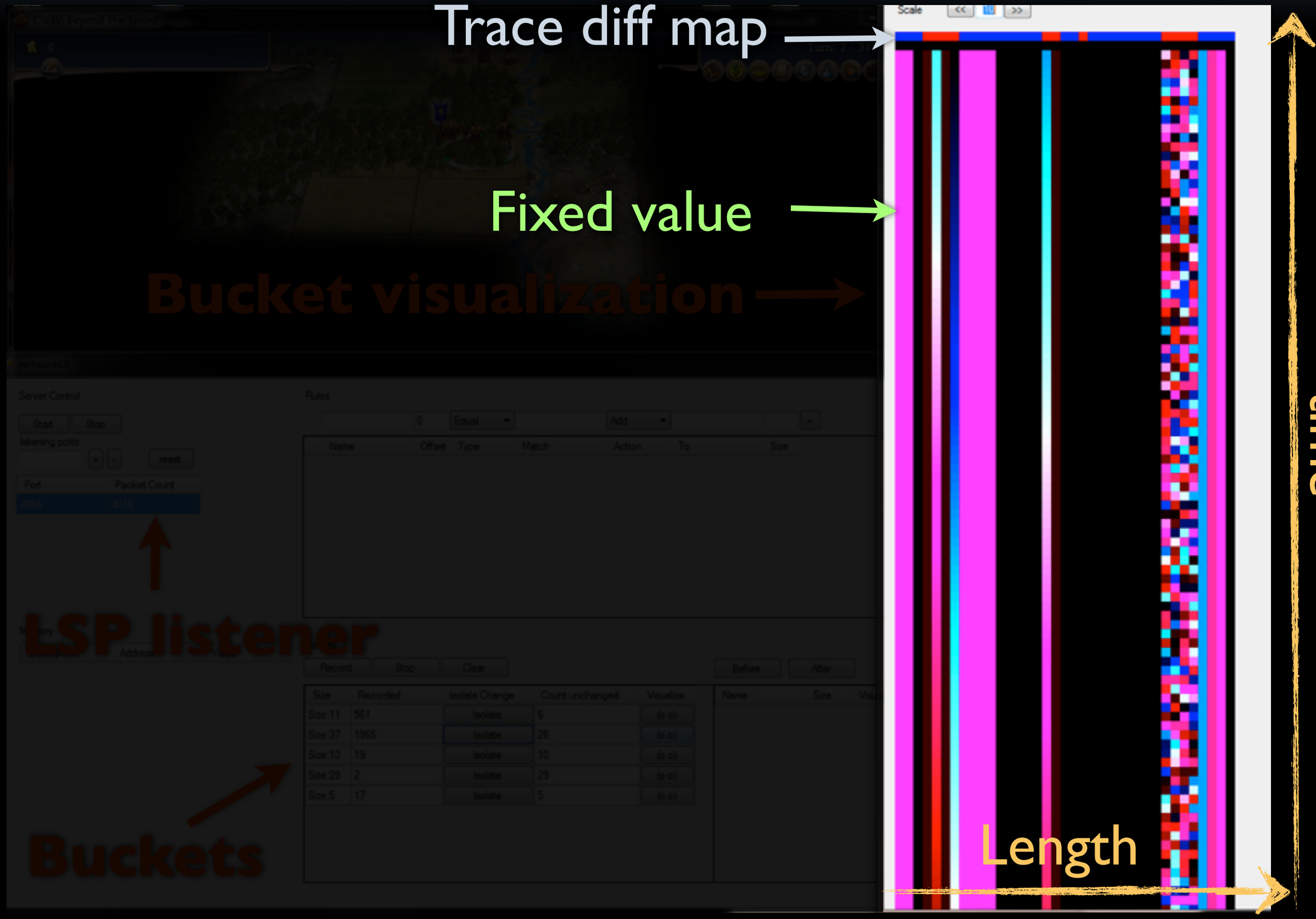
Bucket visualization →

LSP listener

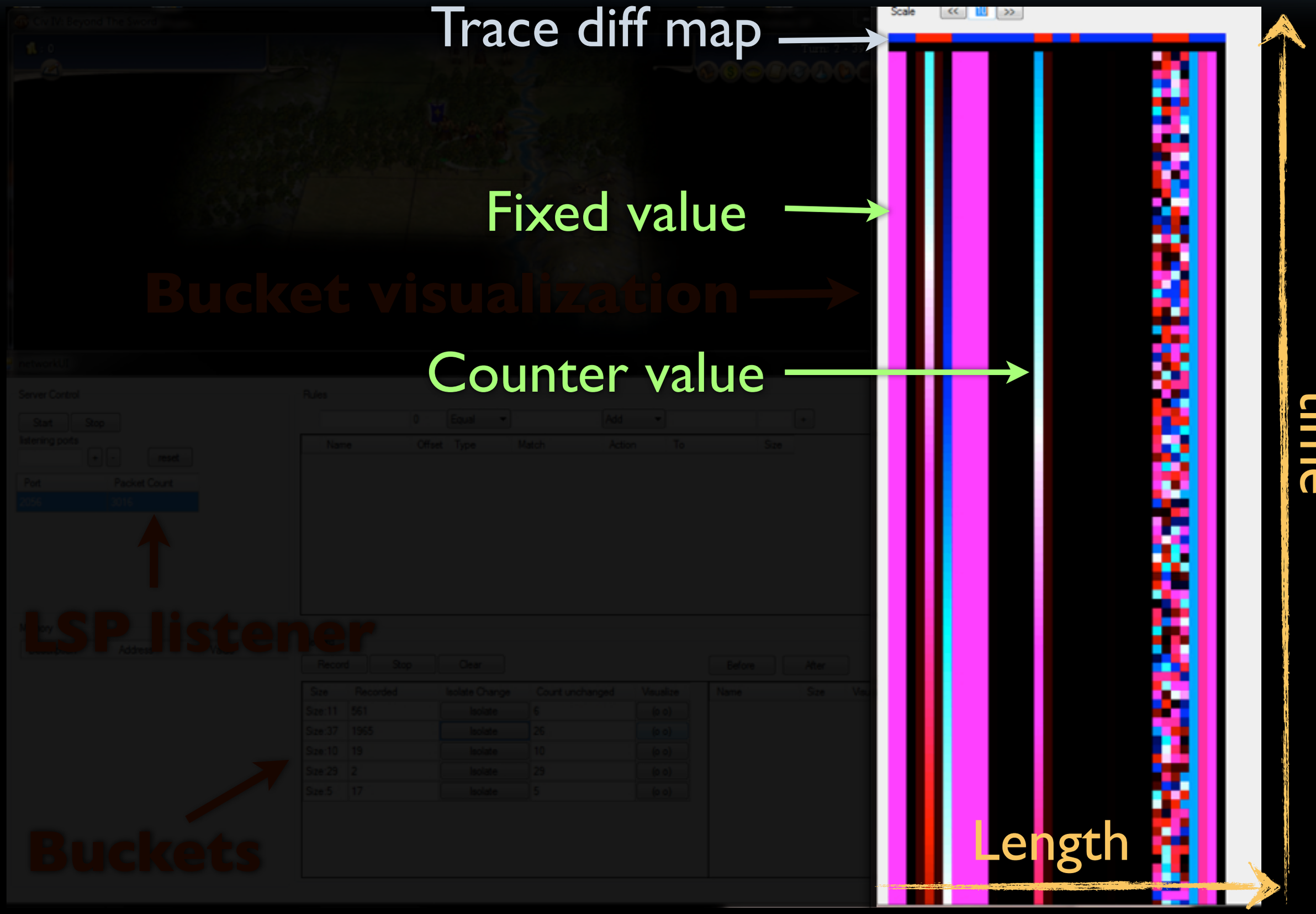
Buckets



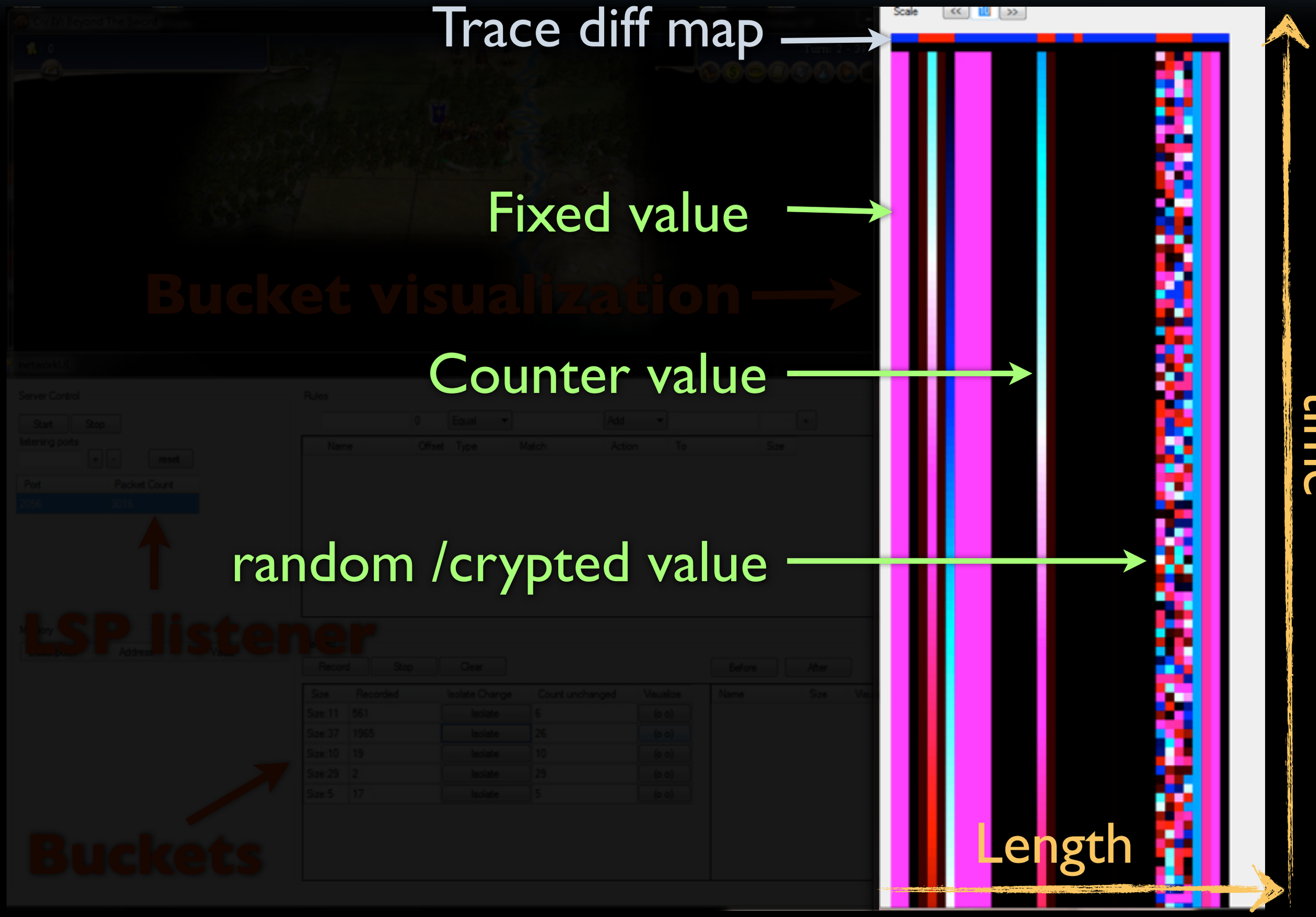
Civilization 4 vizualization



Civilization 4 vizualization



Civilization 4 vizualization



Ongoing work

- A cryptographic lib to improve games
  - Multi-party cryptography against map hack
    - Private Equality Test against synch manipulation
    - Homomorphic encryption for the rest
- A classifier to defend against bots

Get your video and the slides !

We made a video tutorial of Kartograph for you !

http://ly.tl/t10