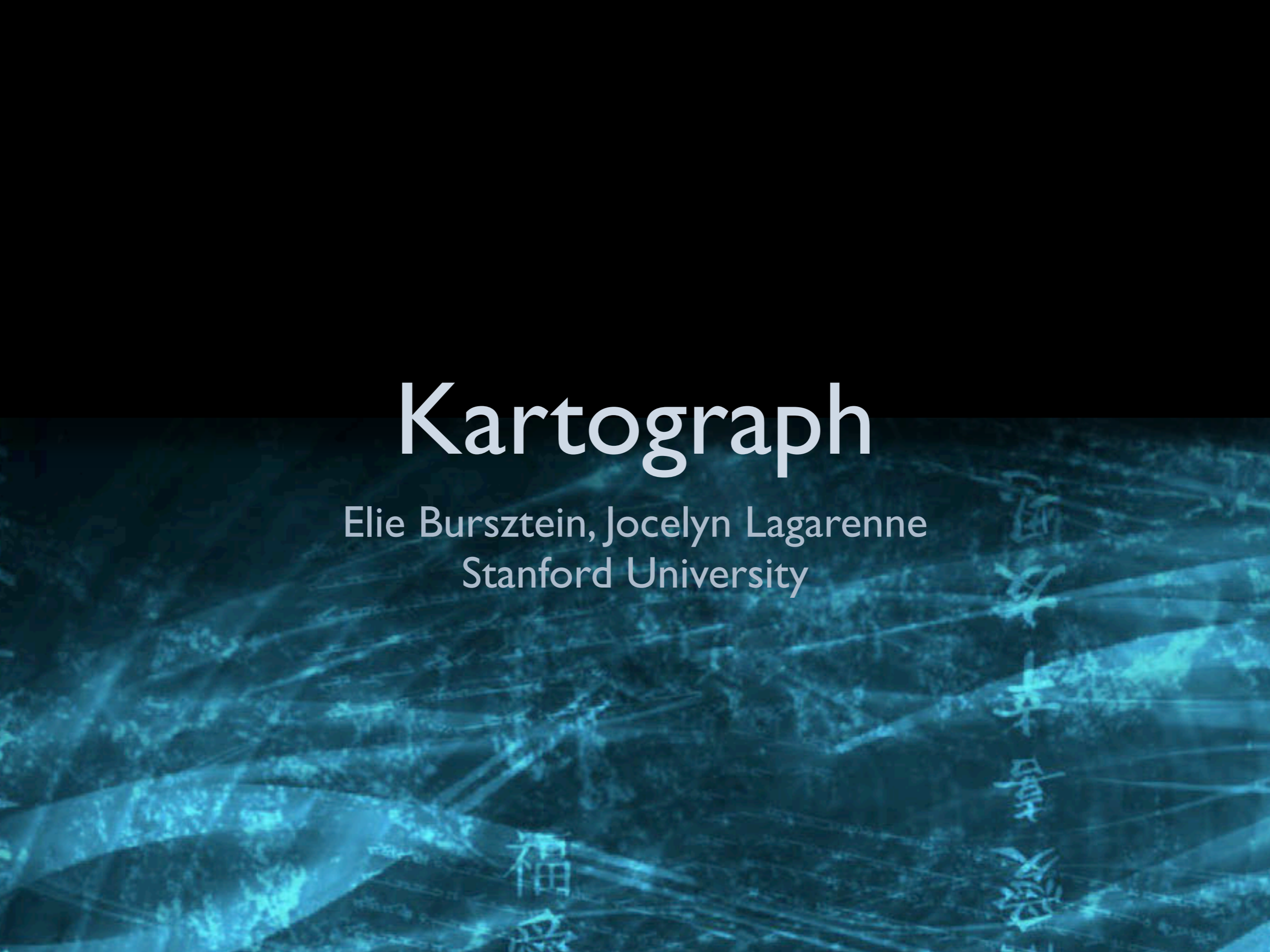


Kartograph

Elie Bursztein, Jocelyn Lagarenne
Stanford University



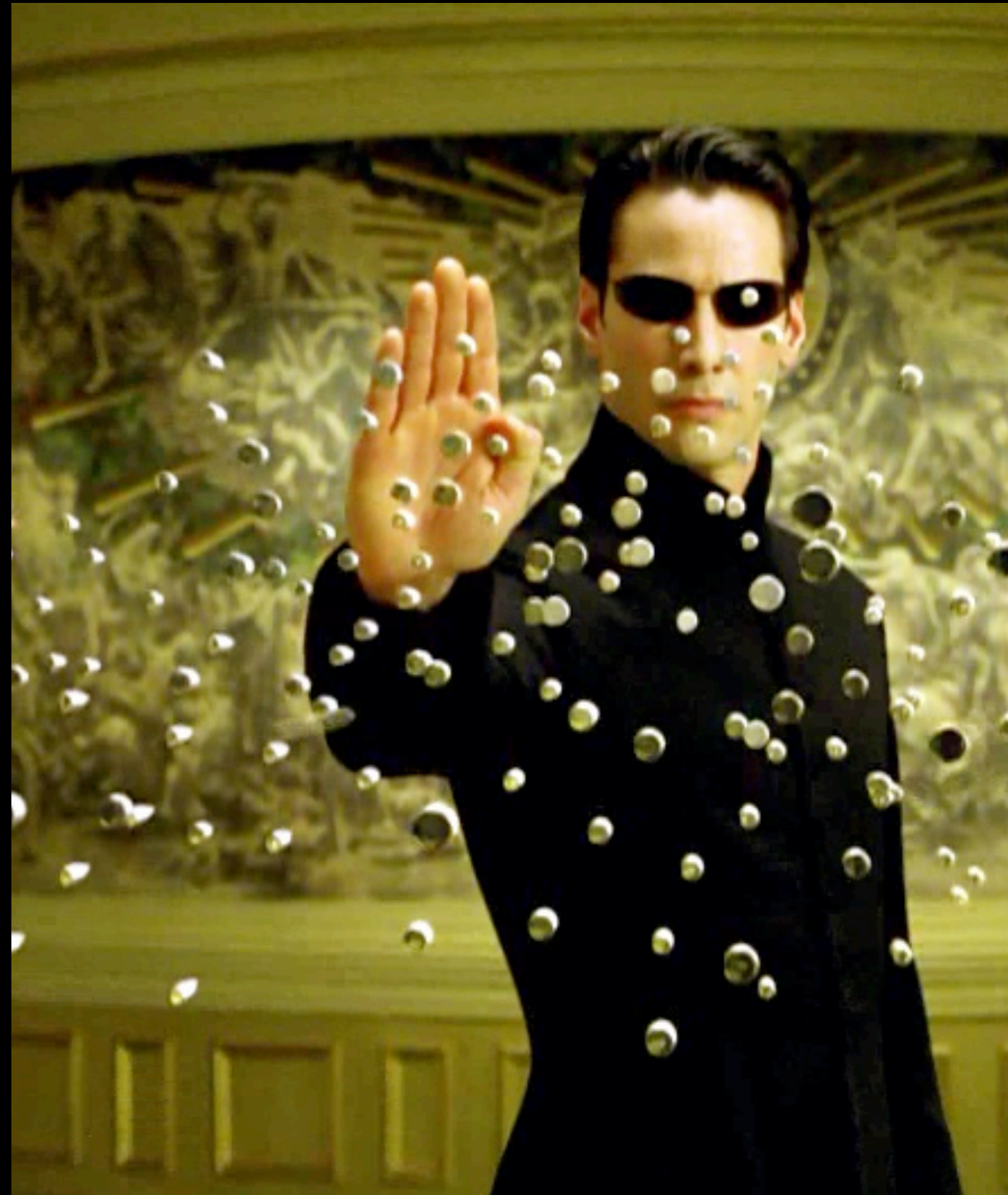


Welcome to the real world

[#kartograph](#)

supernatural powers !

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



Supreme commander 2



Memory based attack



Memory

Memory based attack



Memory

Modification

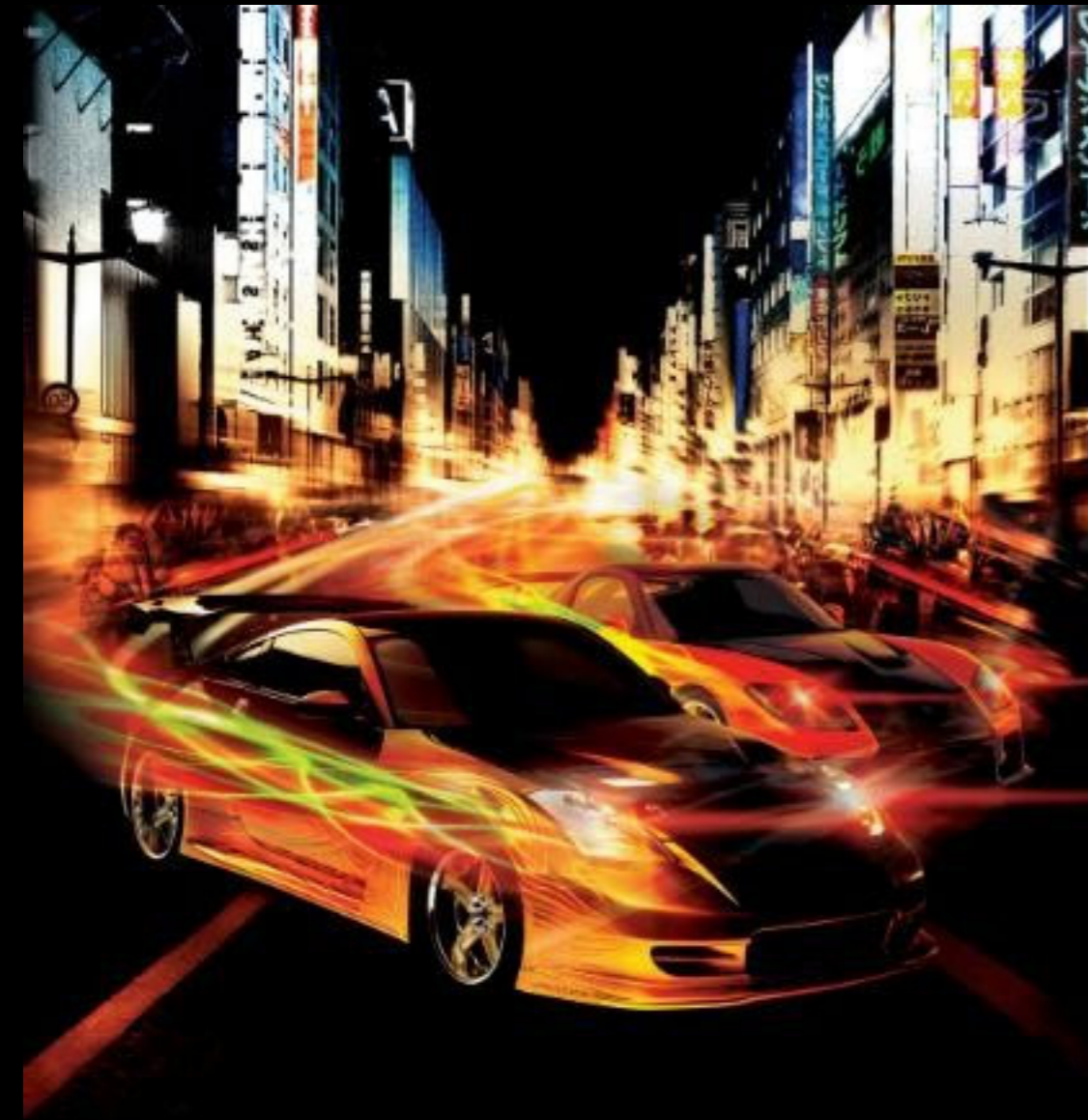
Memory based attack



Memory

Modification

Benefits (fast and furious)

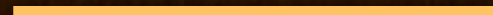


- Generic
- Fast
- Invisible

Drawbacks: Needle in a Haystack



Game memory



Structures



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





Strategy account for **35%** of
the games sold in **2009**





Tankbuster

\$ 300 ⌚ 0:05

Anti-Armor

Steely-cold warriors whose personal plasma-cutter cannons can slice through enemy armor.

Instant Dojo

--	--

Navigation icons: back, forward, search, help



Resources

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

Instant Dojo

--	--

Navigation icons: back, forward, search, help

1

11x 12x 13x



Resources

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

Instant Dojo

--	--

⏪ ⏩ ⏴ ⏵ ⏶ ⏷ ⏸ ⏹ ⏺

Building



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

Instant Dojo

--	--

Navigation buttons: << >> ± × ÷ ?

Zoom level: 1x 12x 13x



Units →

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

Instant Dojo

--	--

⏪ ⏩ ⏴ ⏵ ?

Minimap →



The minimap shows the current game area with a yellow box highlighting the Tankbuster's location. Below the map are icons for a wrench, a dollar sign, a gear, and a shield, along with the resource value 4650. Further down are icons for a house, a shield, a Zergling, a Pylon, a Dragoon, and a Tankbuster.

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

A grid of unit selection icons. The Tankbuster icon is highlighted with a yellow border. Other icons include a Dragoon, a Pylon, a Zergling, a Dragoon, a Dragoon, a Dragoon, a Dragoon, a Dragoon, and a Dragoon.

The Instant Dojo unit selection panel shows the Tankbuster icon highlighted with a yellow border. Below the icons are several control buttons, including a left arrow, a house icon, a Zergling icon, a Pylon icon, and a question mark icon.

A zoom control panel with a circular dial set to 1x, a horizontal bar with 11x, 12x, and 13x markers, and a right arrow button.



Visible

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

Instant Dojo

--	--

⏪ ⏩ ⏴ ⏵ ?

1

11x 12x 13x



Fog of war



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

Instant Dojo

--	--

1

11x 12x 13x

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



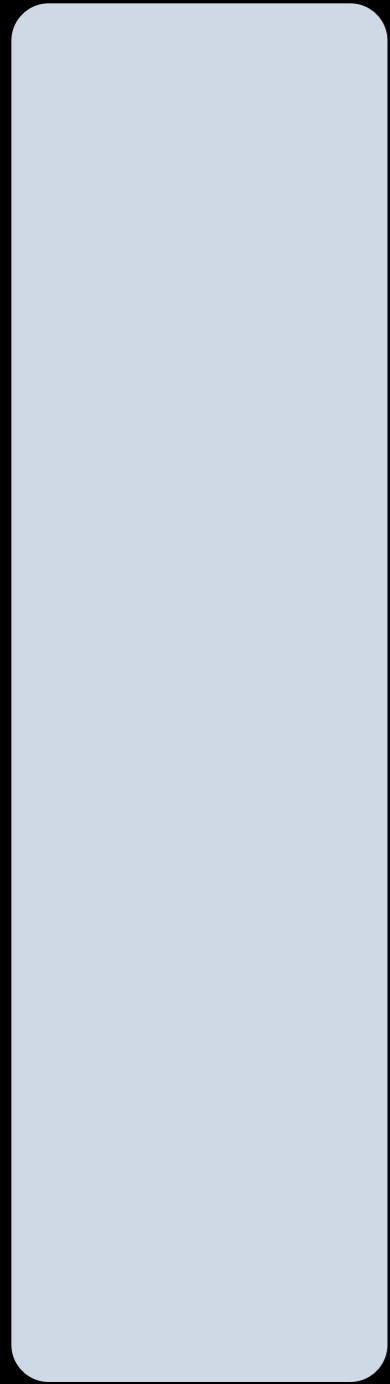


There is no spoon

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



Game
memory



Step | **play**

Reducing memory



Game
memory



Step 1 **play**

Step 2 **discover**

Reducing memory



Game
memory



Step 1 **play**



Step 2 **discover**

Reducing memory



Game
memory



Step 1 **play**



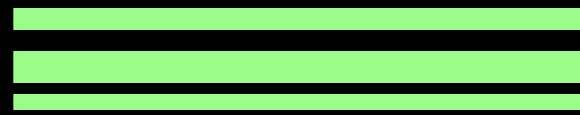
Step 2 **discover**

Step 3 **play**

Reducing memory



Game
memory



Step 1 **play**



Step 2 **discover**

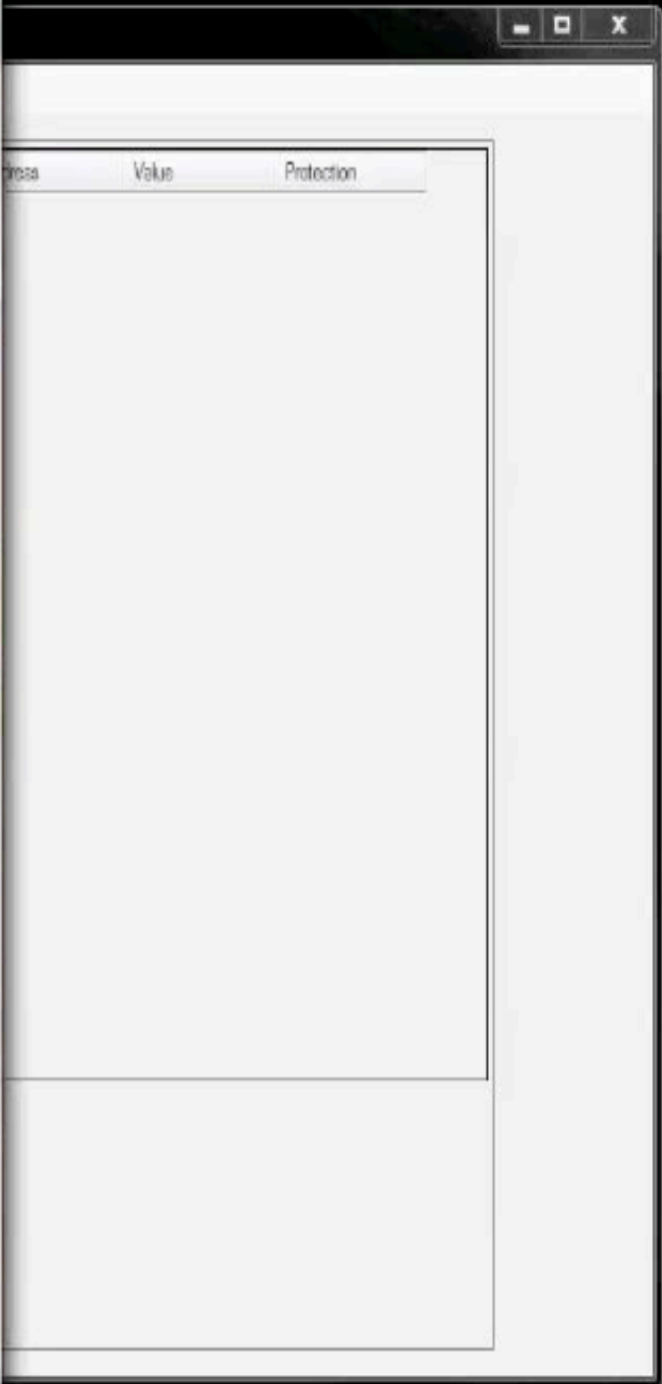
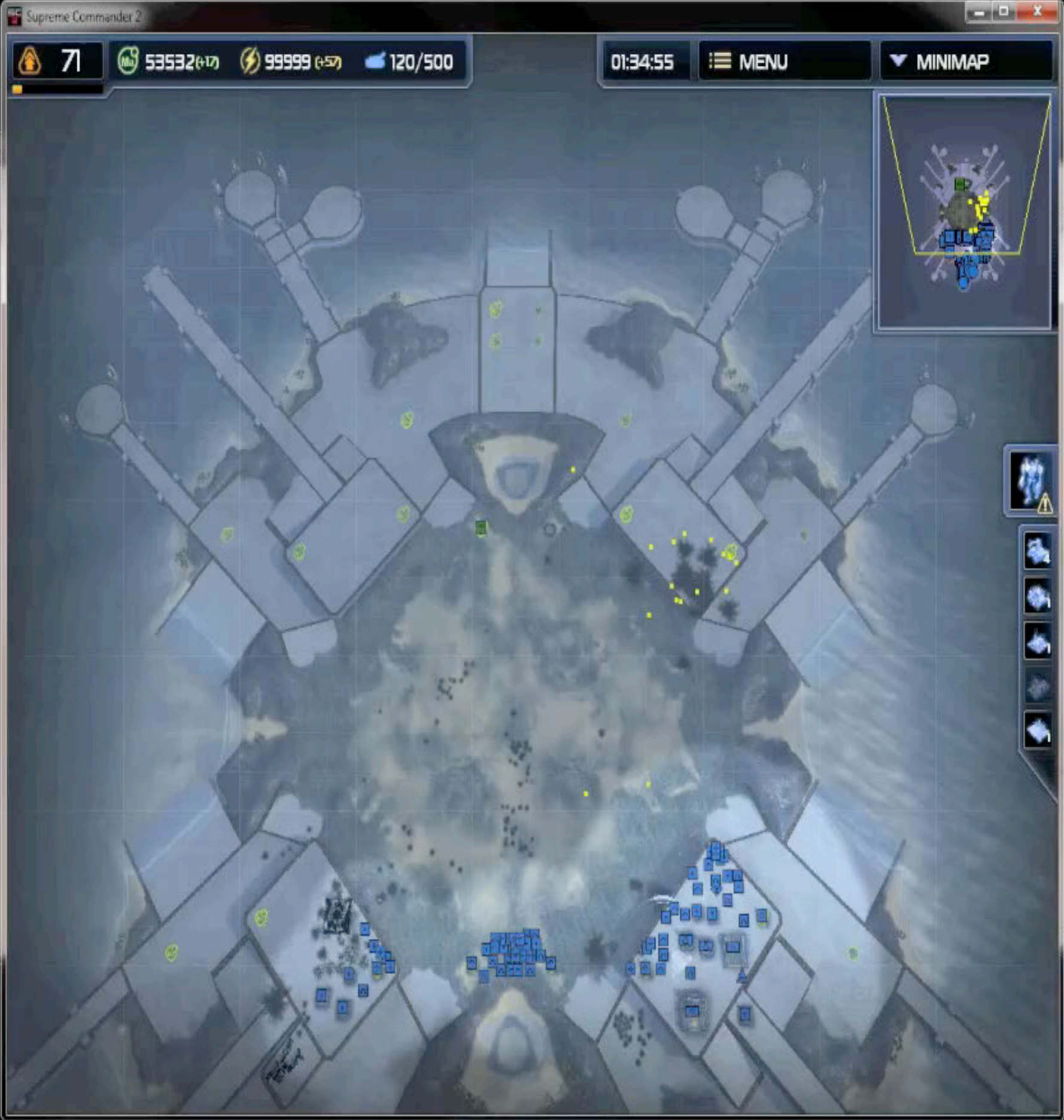


Step 3 **play**

Reducing memory

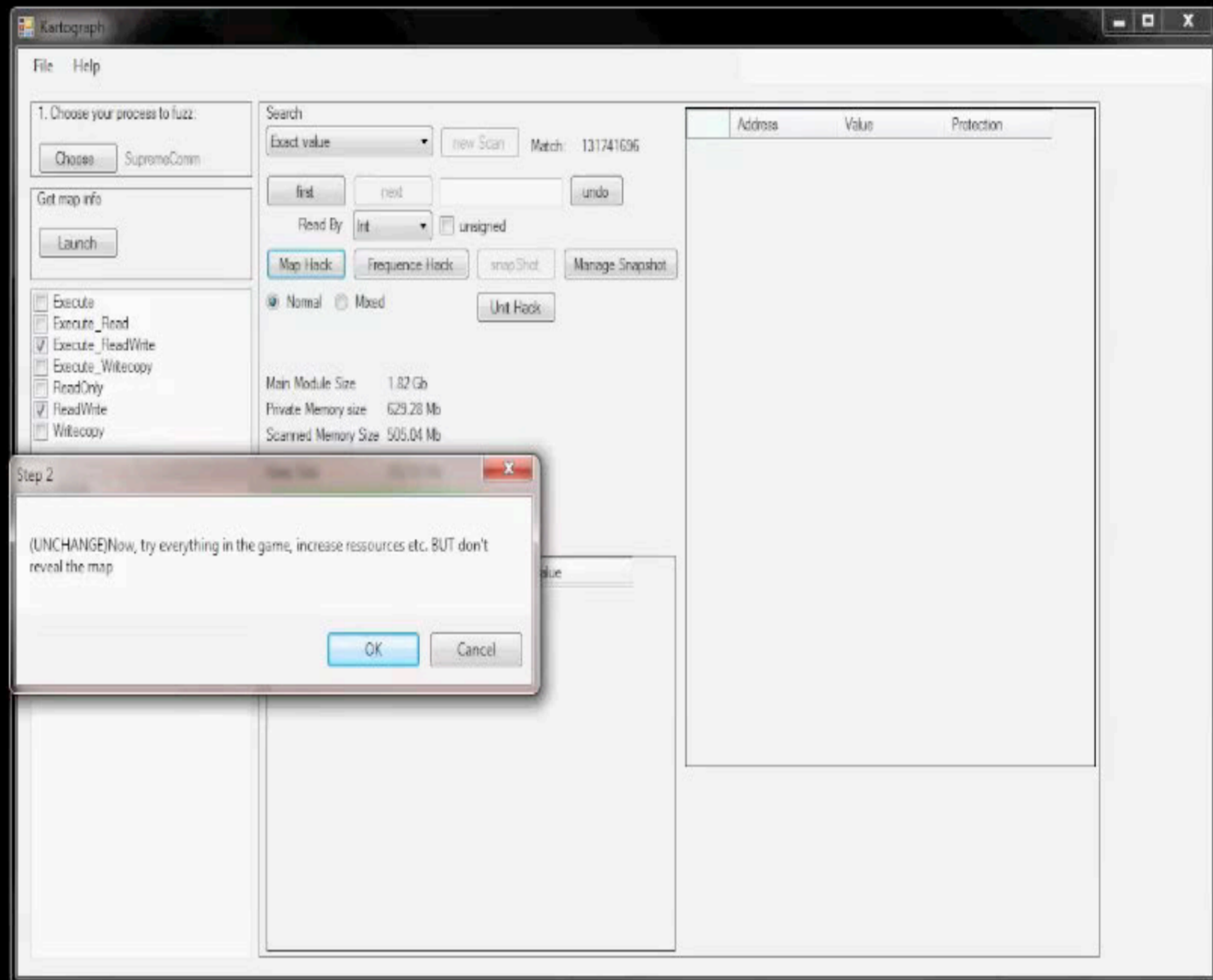
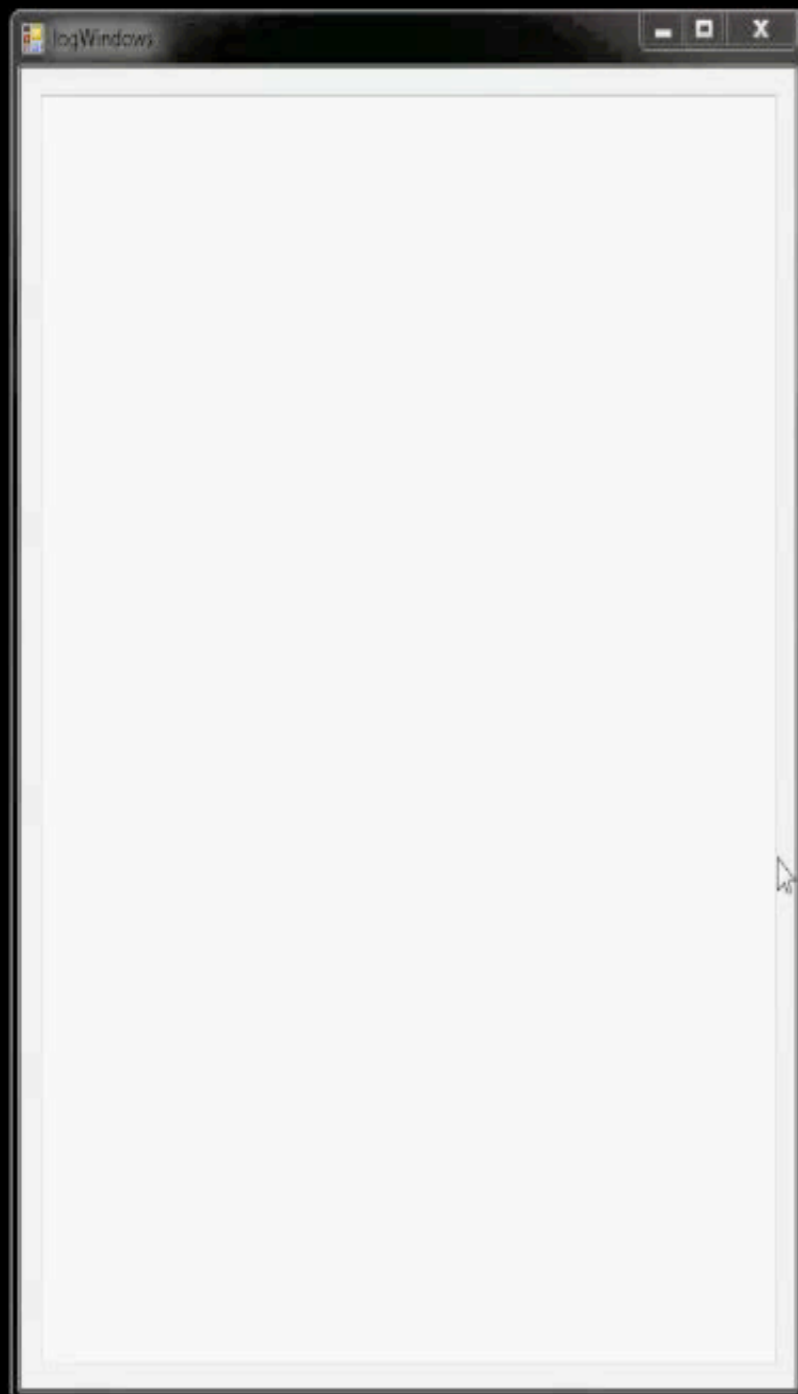


Acquiring the game's memory



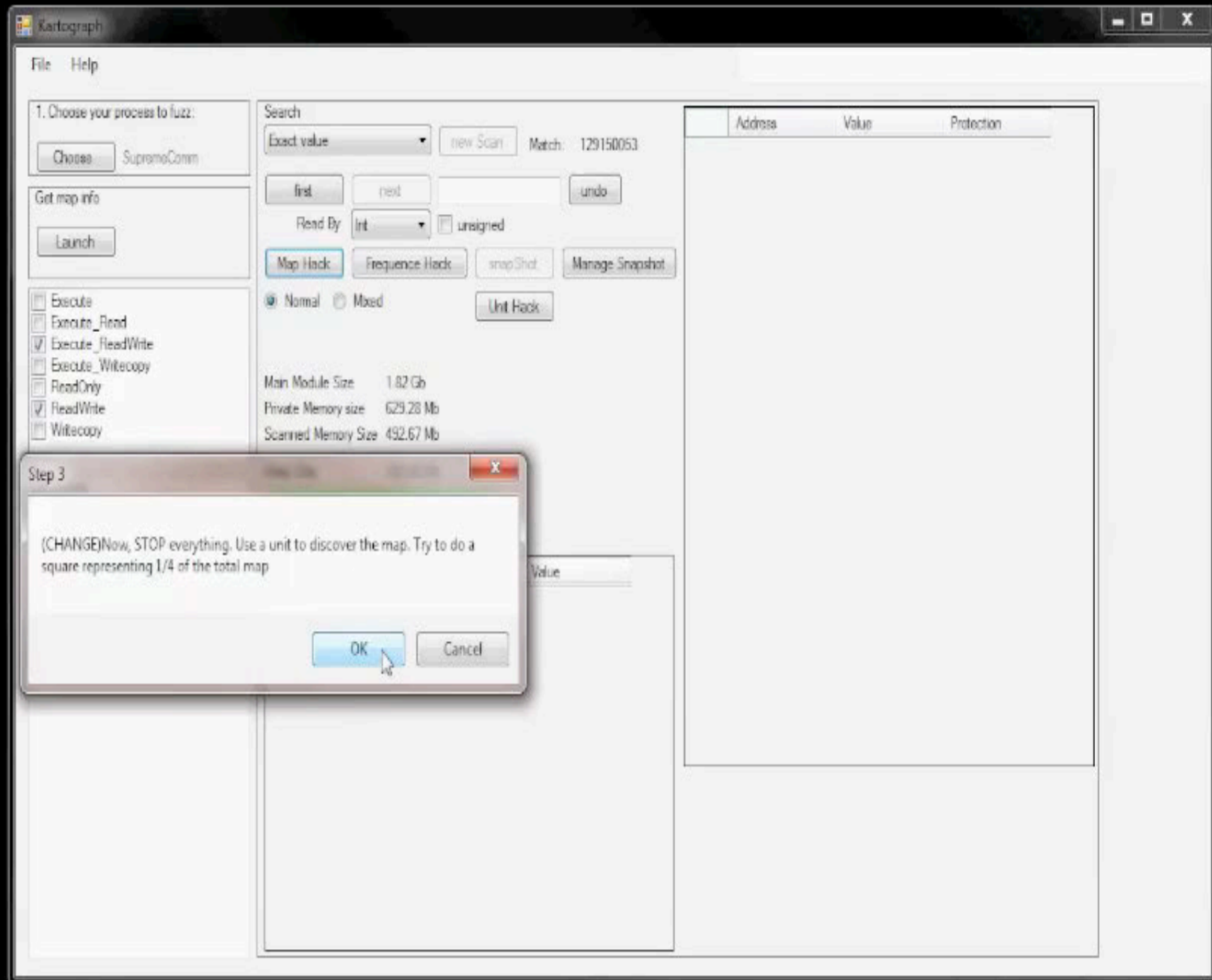
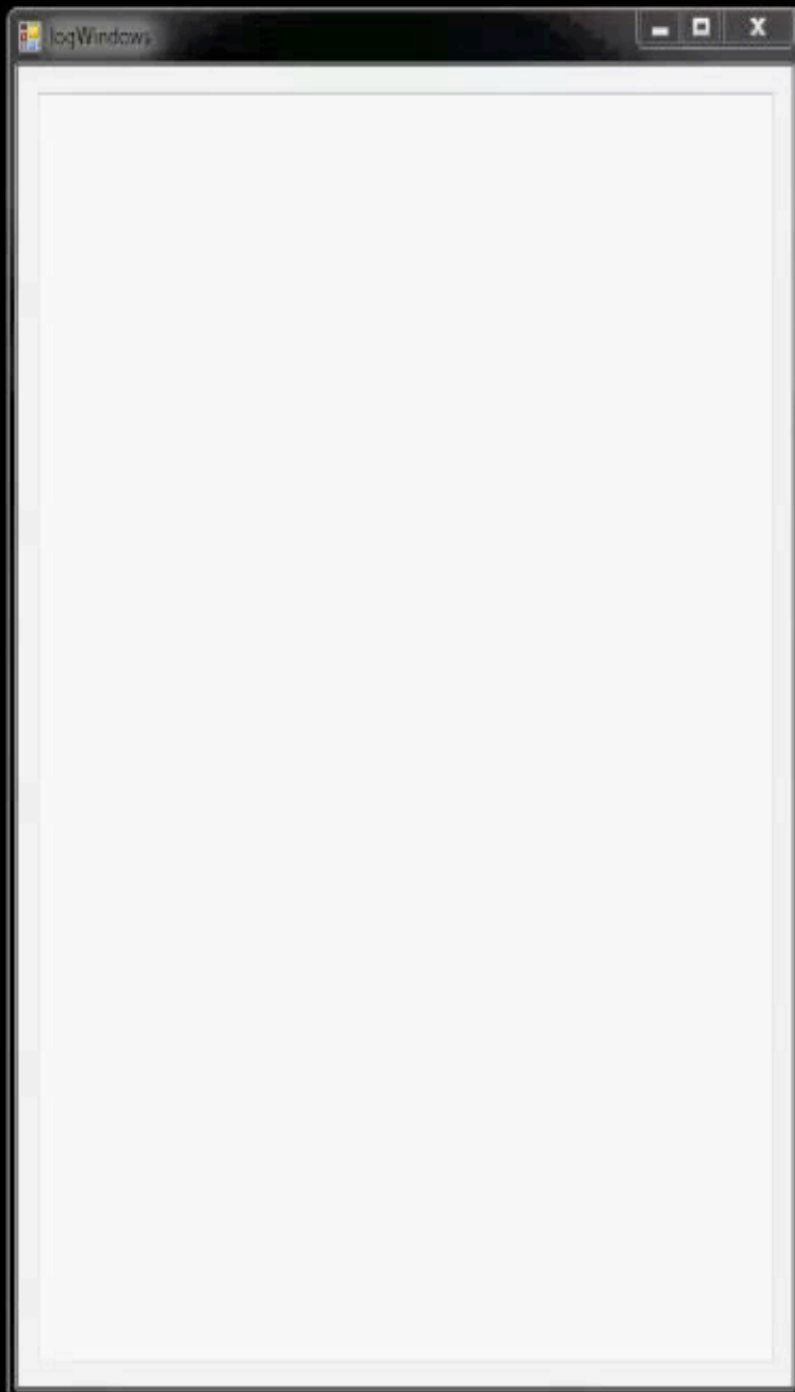
Step 1

Removing unrelated
memory



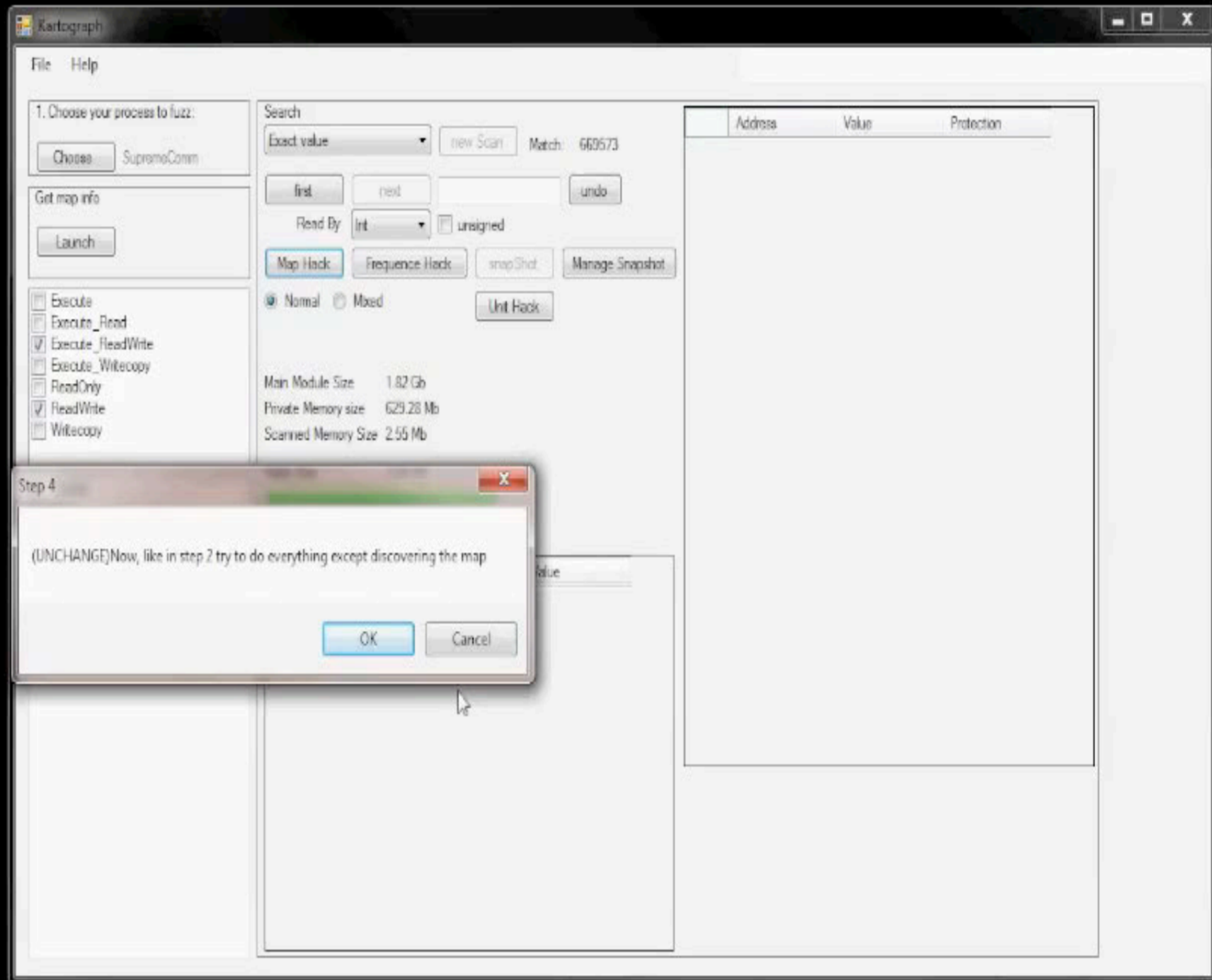
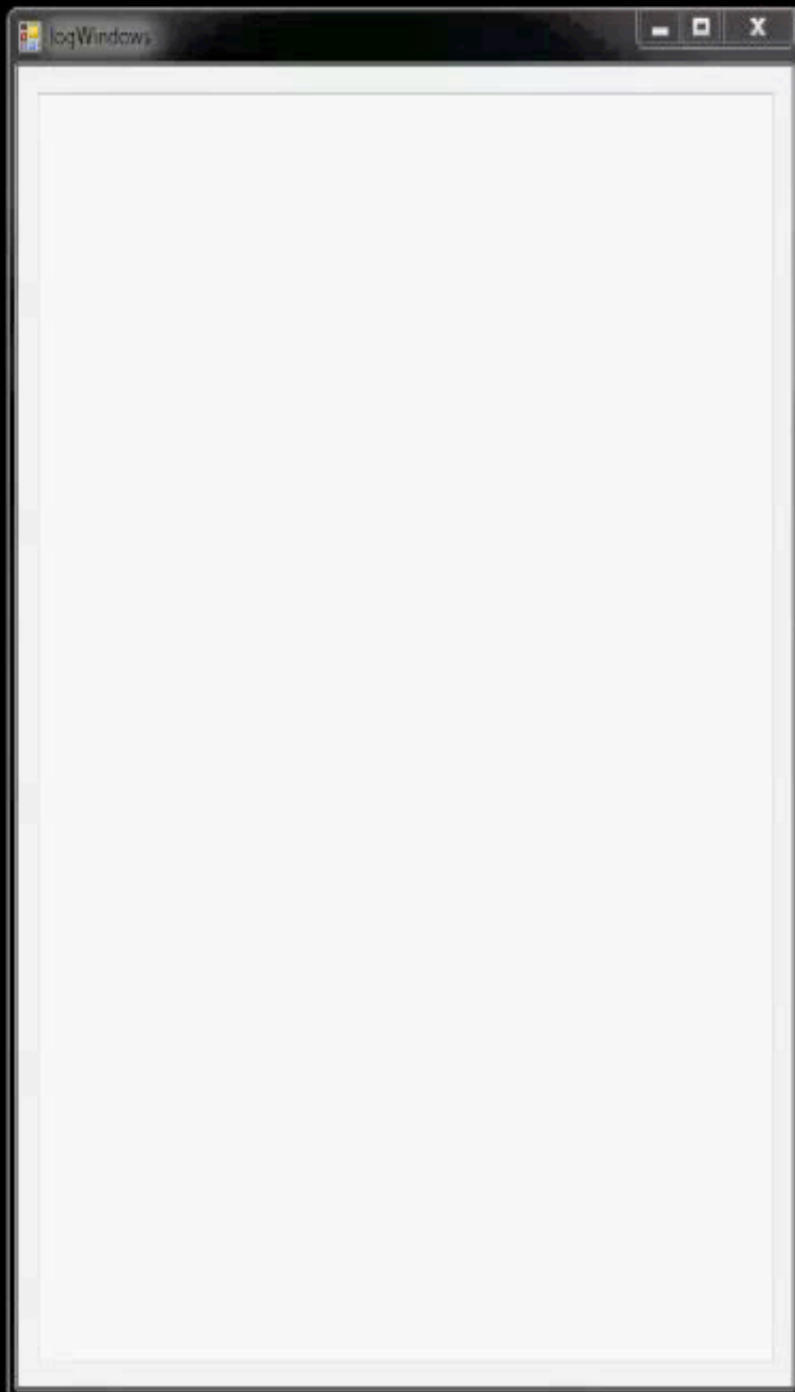
Step 2

Discovering the map and
keeping relevant memory



Step 3

Removing more unrelated
memory



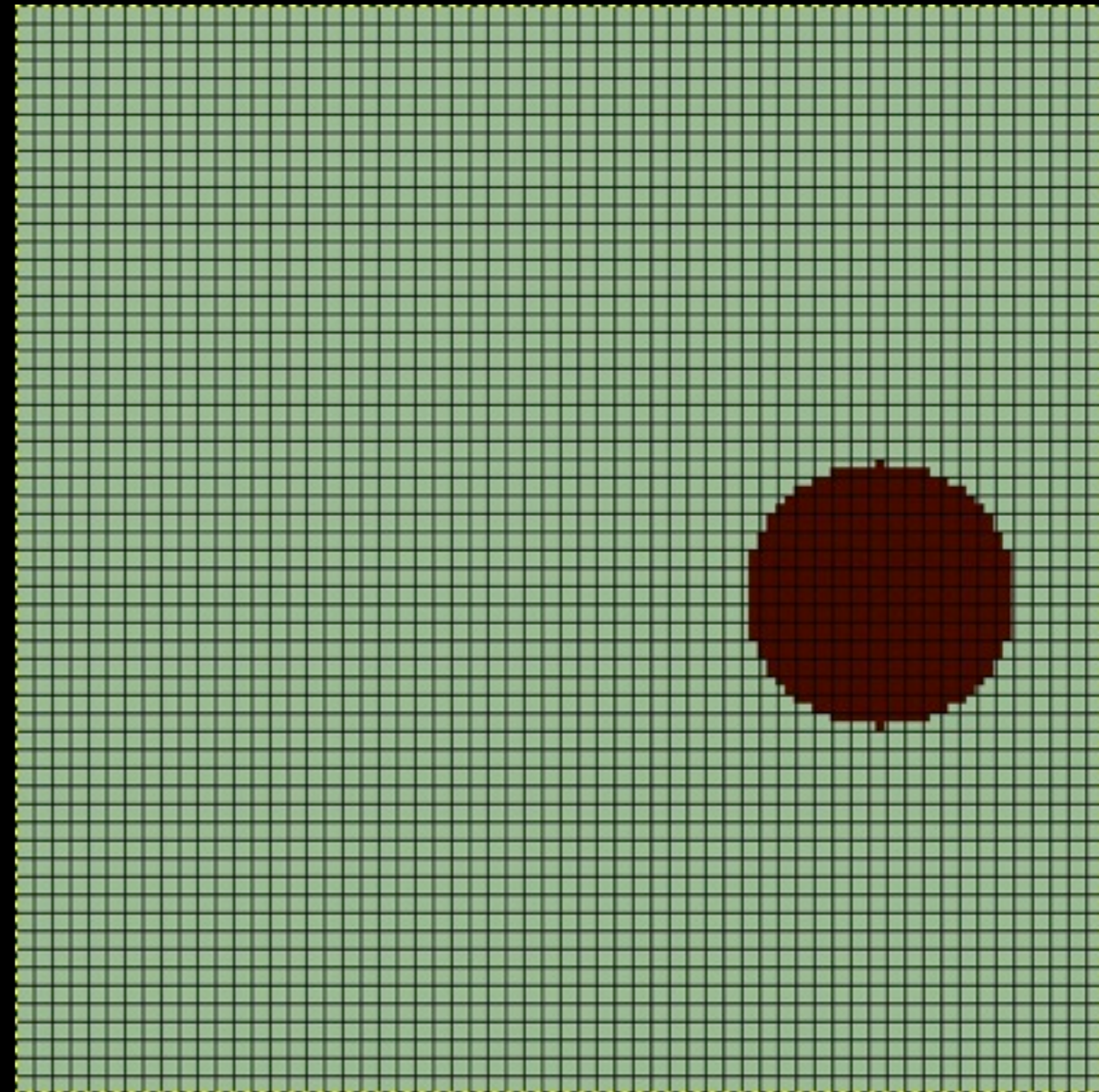
Step 4

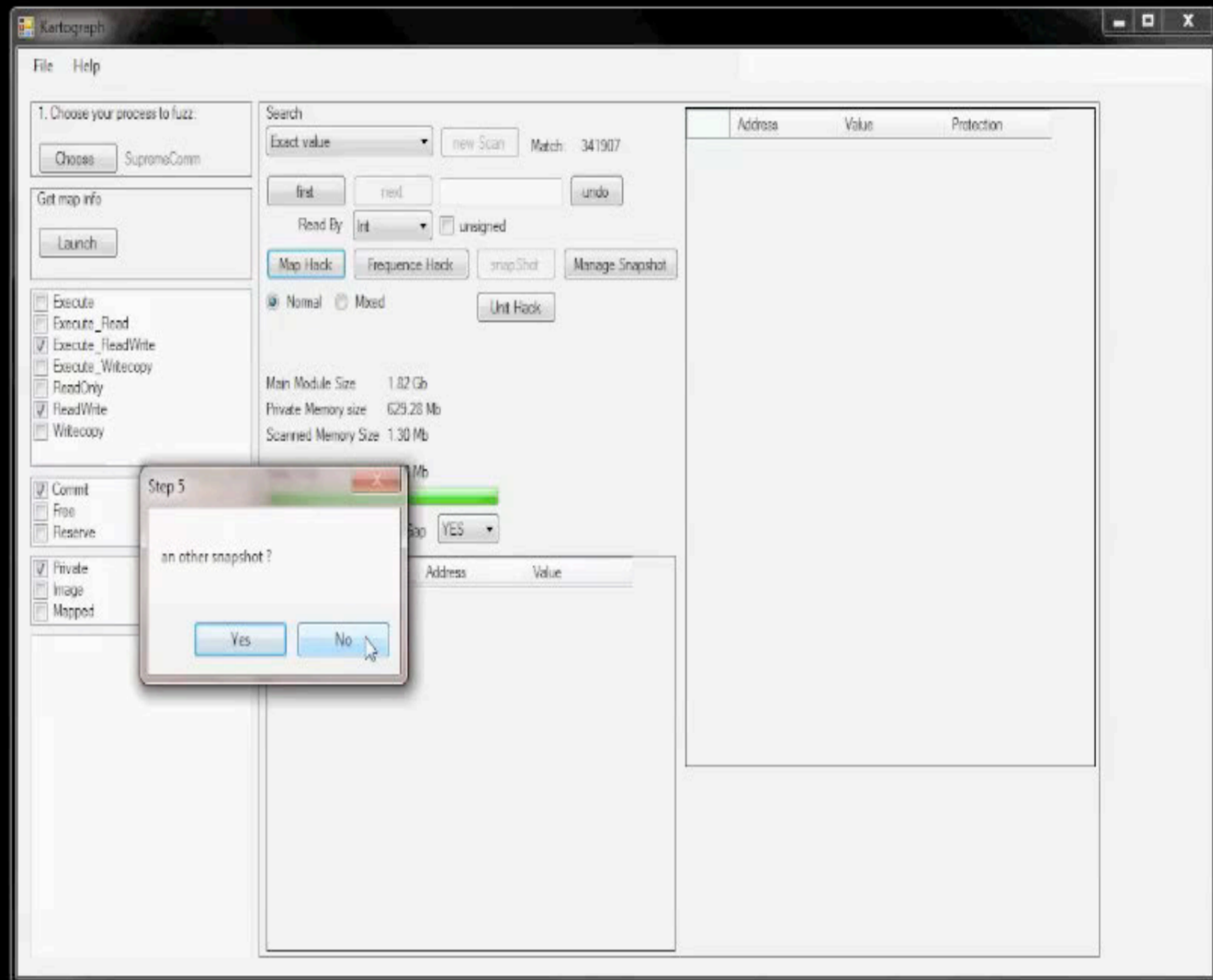
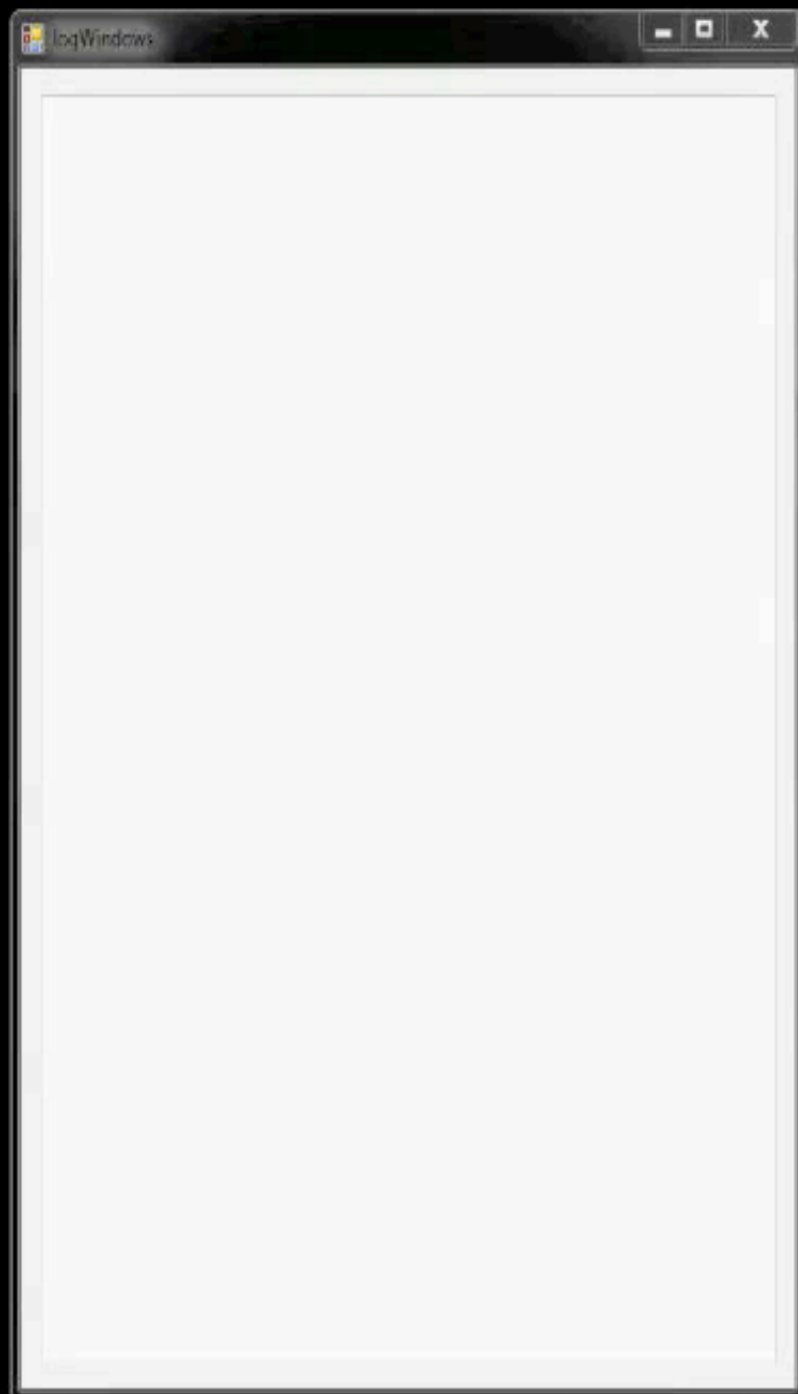
Finding the map in the
remaining memory

Working assumption



Working assumption



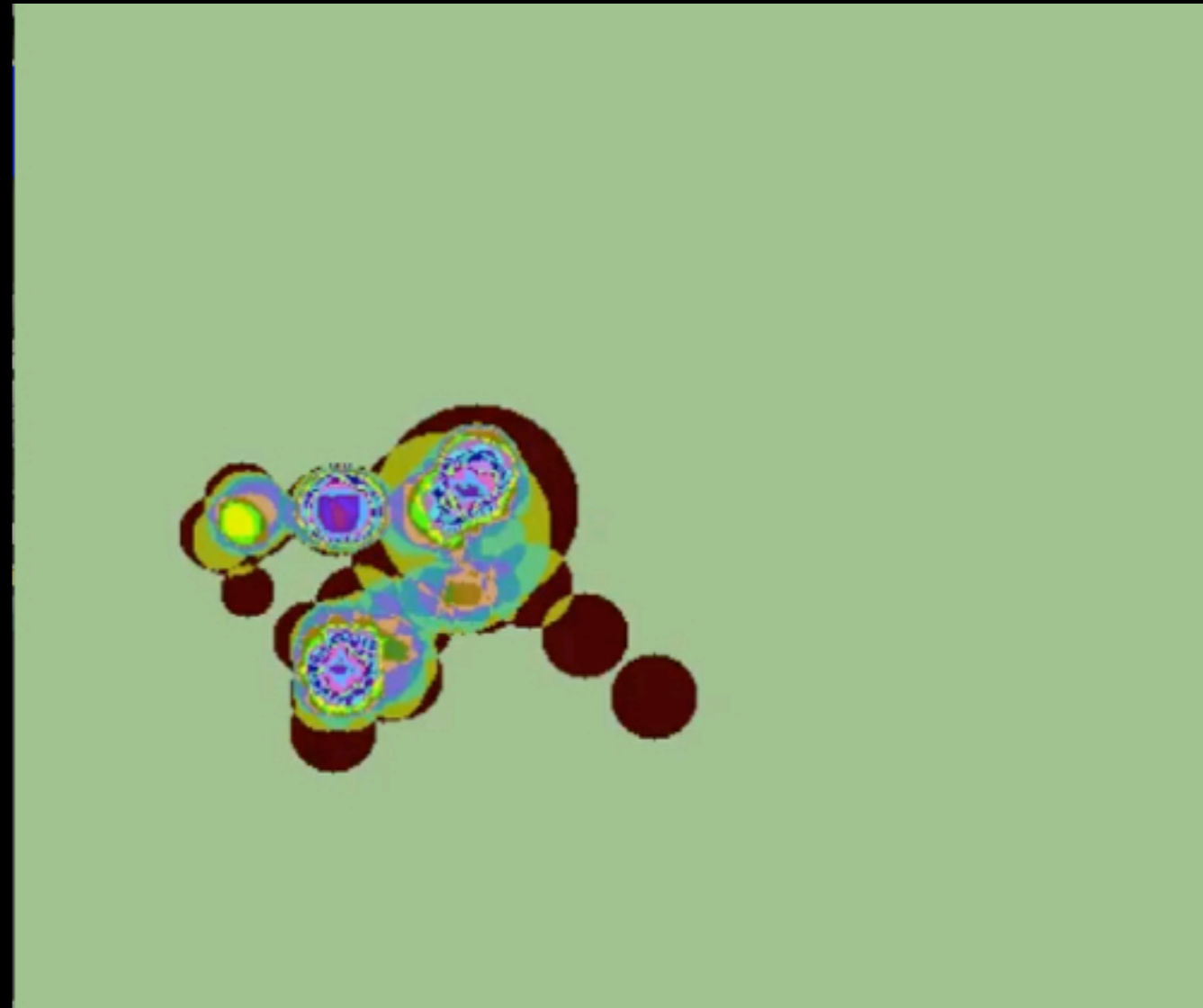


Step 5

Isolating the potential map



In game



In memory

Step 6

Understanding the map's
structure



name

target

read

Address	Value	Protection
---------	-------	------------

Step 8

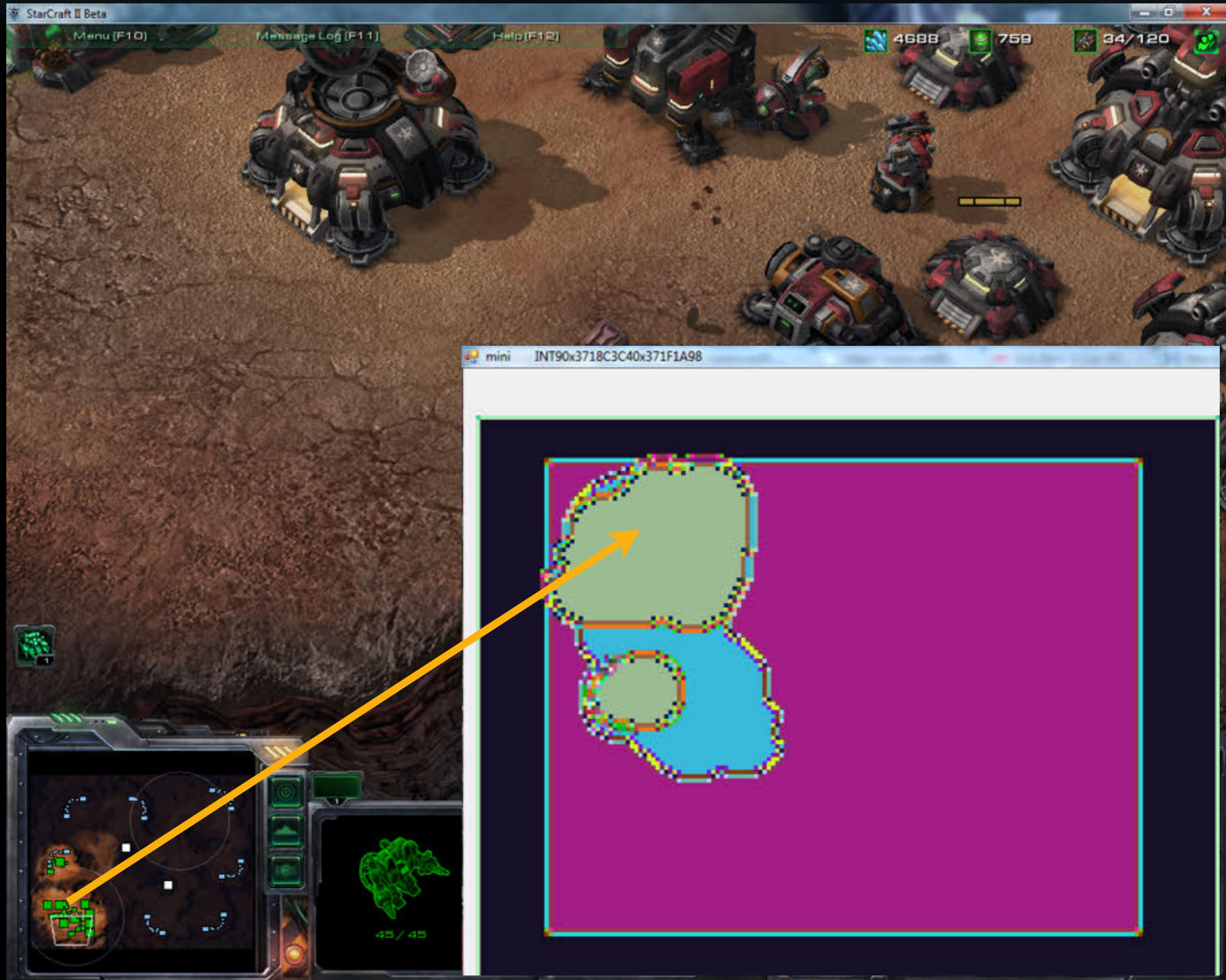
Rewriting game memory
for fun and profit



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

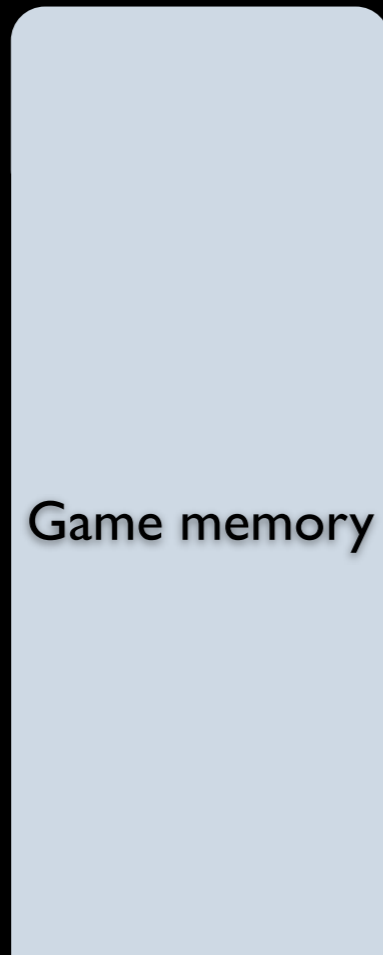
- Only one new integer by unit
- Each integer is a valid pointer

Unit hack Step



Game memory

Unit hack Step



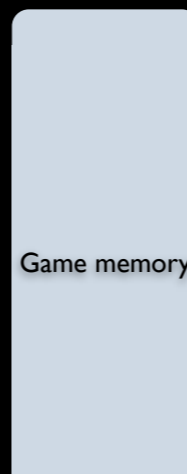
Game memory

Unit hack Step



Game memory

Unit hack Step



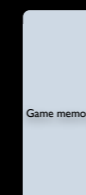
Game memory

Unit hack Step

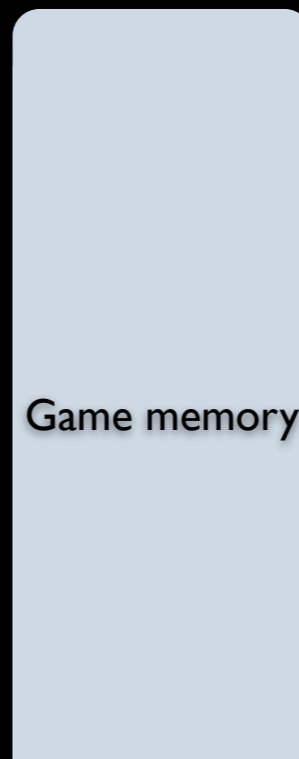


Game memory

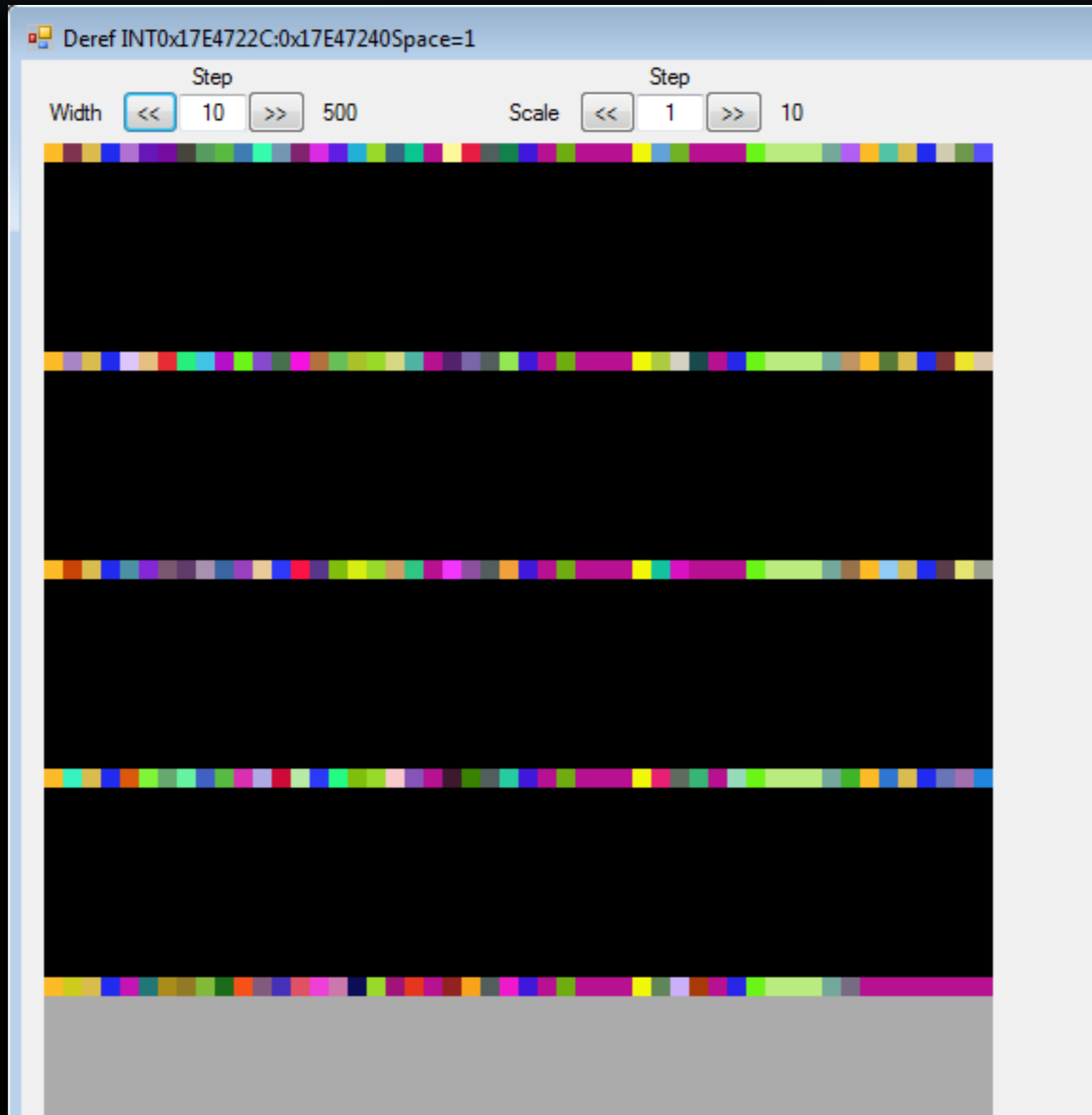
Unit hack Step



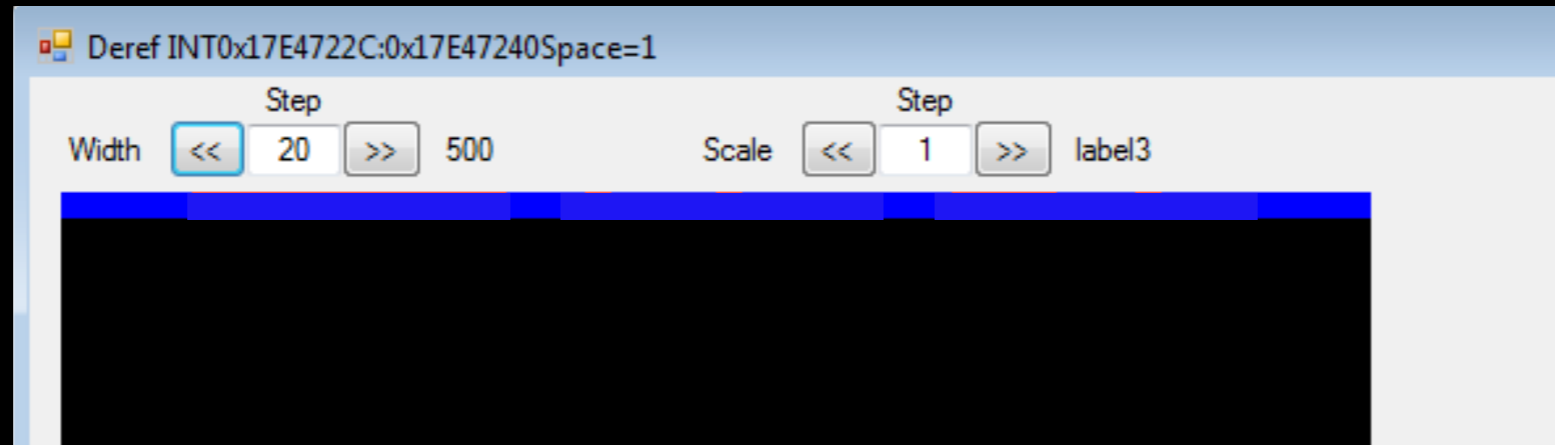
Unit hack Step



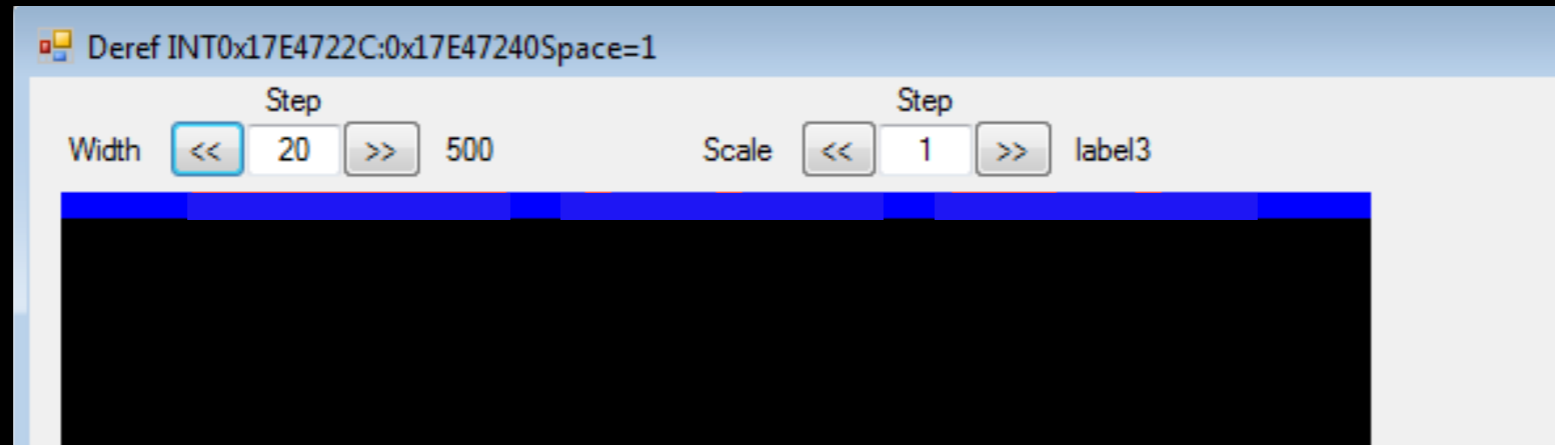
Unit Hack shape



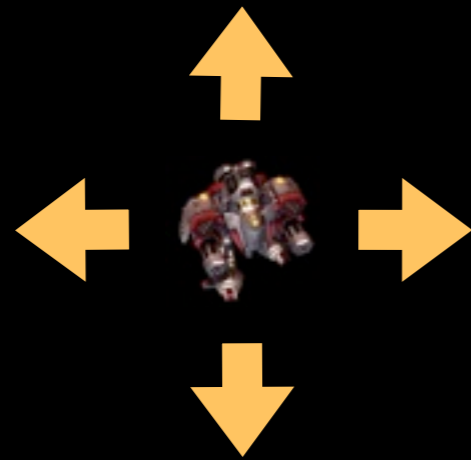
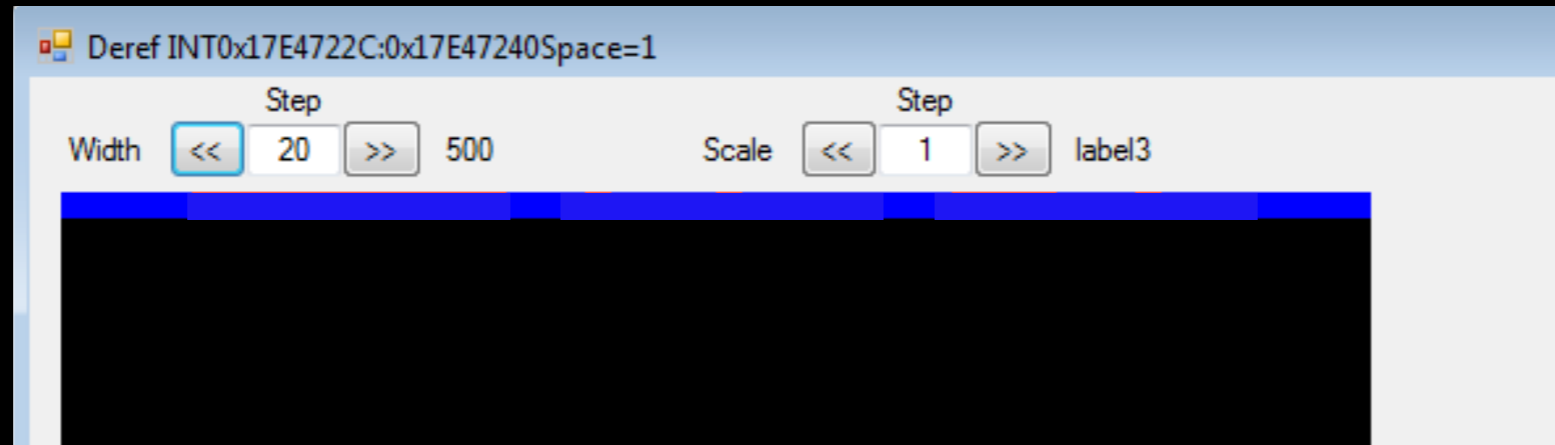
Understanding unit structure



Understanding unit structure

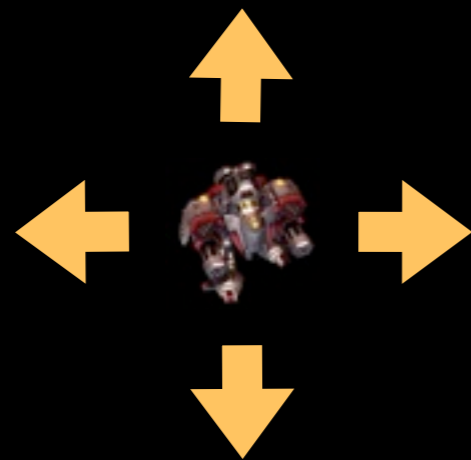
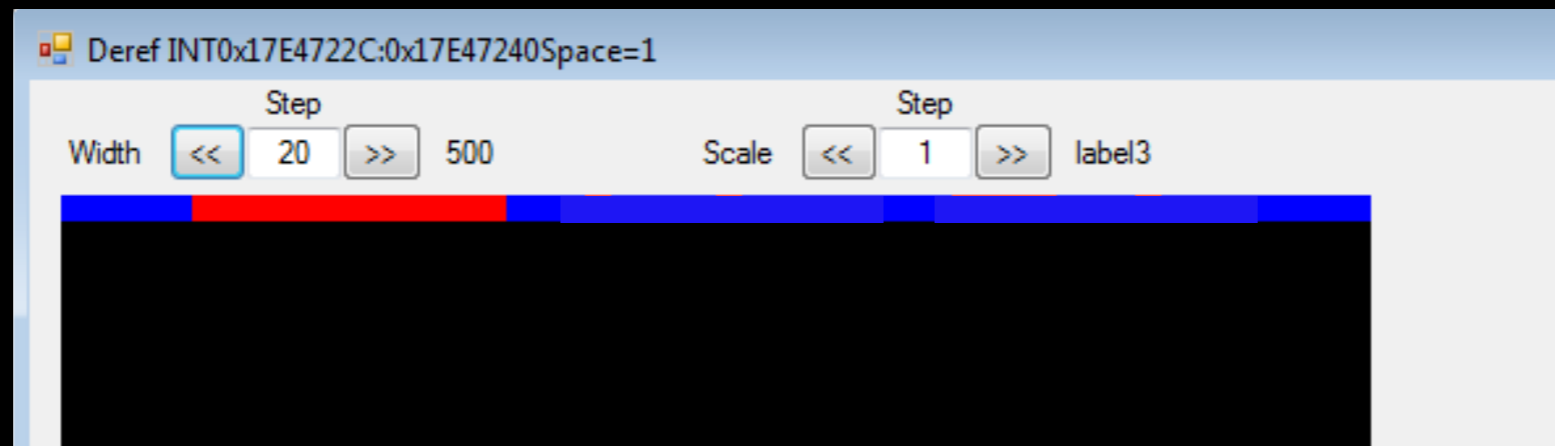


Understanding unit structure



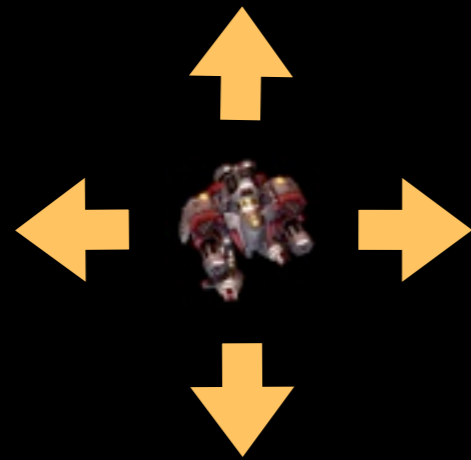
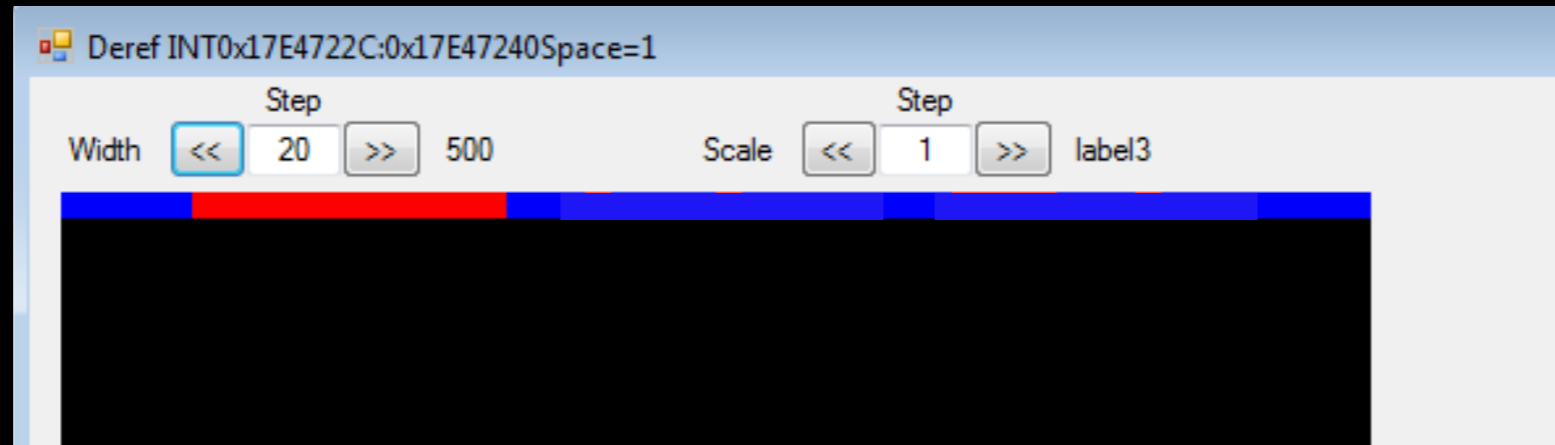
make it move

Understanding unit structure



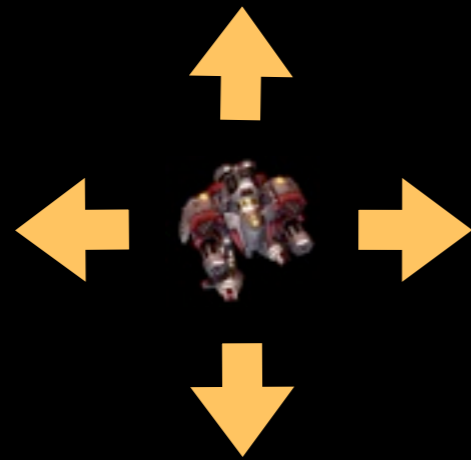
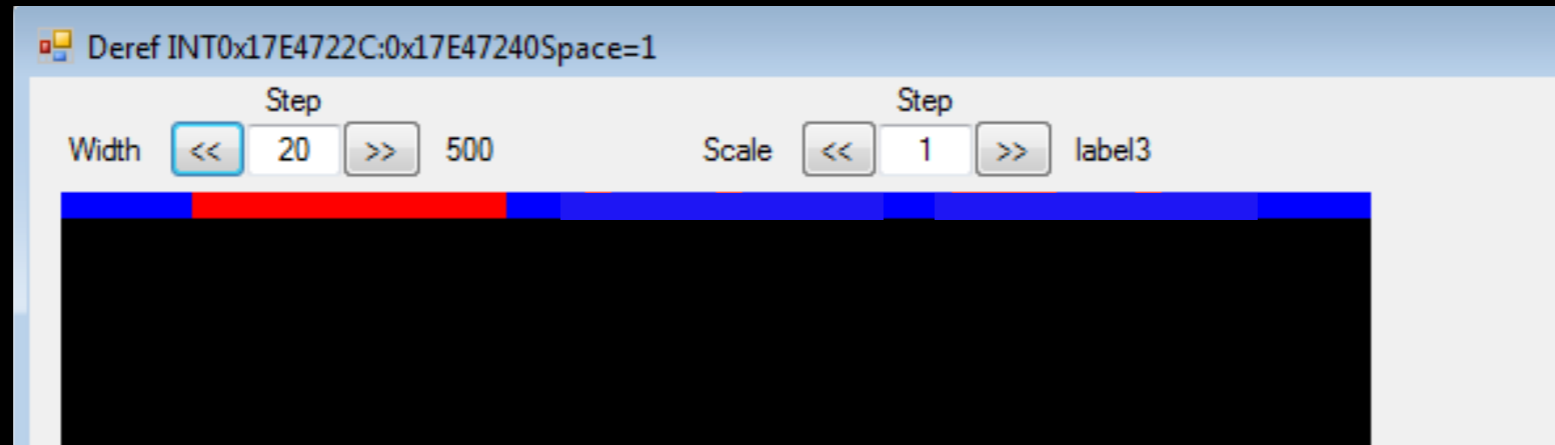
make it move

Understanding unit structure



make it move

Understanding unit structure

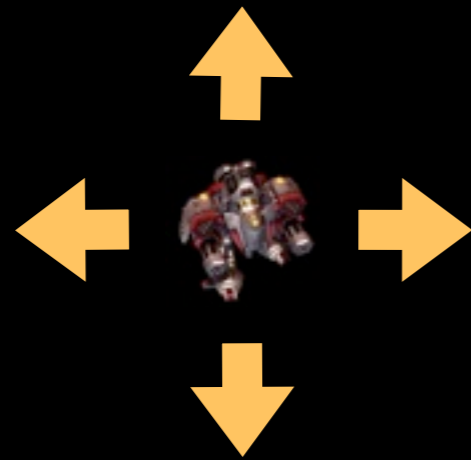
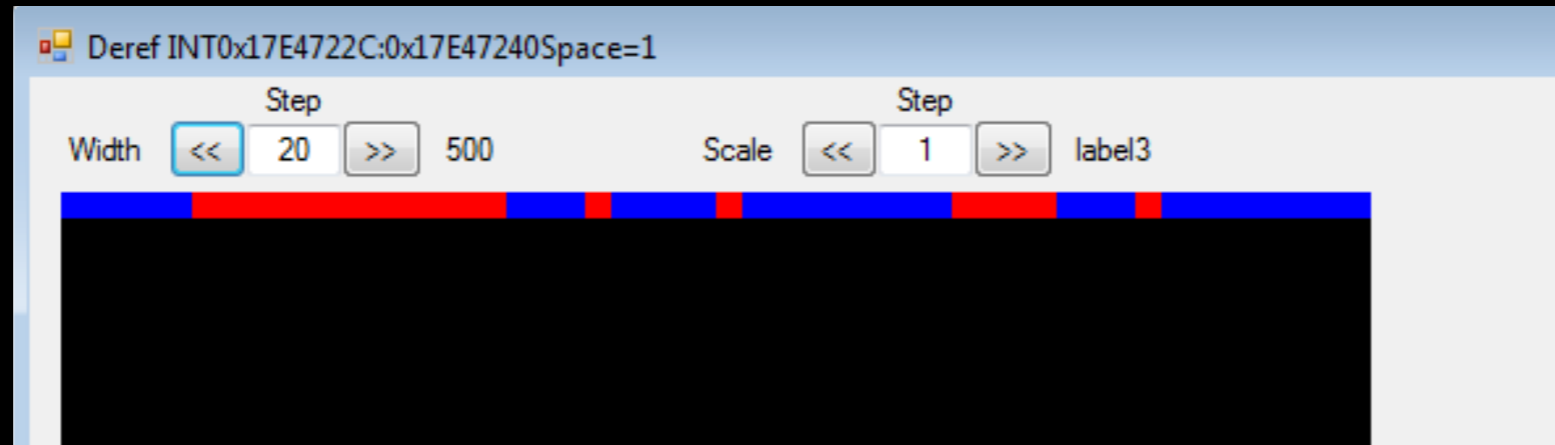


make it move



make it bleed

Understanding unit structure



make it move



make it bleed

V: Imperial Age

Menu



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

Turn: 5 - 3800 BC

The game has gone Out Of Sync.
Please check OOS values (next to scores).
The player with different values should reconnect in order to resync.

30: Joe ? * OOS Values; Sync=656789696; Options=4518537 *
11: [Elie] * OOS Values; Sync=1530118336; Options=4518537 *

Defense Bonus: +25%
Hills/Plains, 2 , 1
Fresh Water

Settler
Movement: 2
Level: 1

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 - vlsplListener over [RSUP TCP Service Provider]
2621 - vlsplListener over [MSAFD Tcpip [TCP/IP]]
2622 - vlsplListener over [MSAFD Tcpip [UDP/IP]]
2623 - vlsplListener over [MSAFD Tcpip [RAW/IP]]
2624 - vlsplListener over [MSAFD Tcpip [TCP/IPv6]]
2625 - vlsplListener over [MSAFD Tcpip [UDP/IPv6]]
2626 - vlsplListener over [MSAFD Tcpip [RAW/IPv6]]
2627 - vlsplListener over [RSUP TCPv6 Service Provider]
2628 - vlsplListener over [RSUP UDPv6 Service Provider]
2629 - vlsplListener over [RSUP UDP Service Provider]
2630 - vlsplListener over [MSAFD Pgm (RDM)]
2631 - vlsplListener over [MSAFD Pgm (Stream)]
2632 - vlsplListener over [UMCI sockets DGRAM]
2633 - vlsplListener over [UMCI sockets STREAM]
1008 - RSUP 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 - RSUP TCPv6 Service Provider
1009 - RSUP UDPv6 Service Provider
1010 - RSUP UDP Service Provider
1011 - MSAFD Pgm (RDM)
1012 - MSAFD Pgm (Stream)
1019 - UMCI sockets DGRAM
1020 - UMCI sockets STREAM
2605 - vlsplListener
Press any key to continue...

C:\svn\project\lsp\trunk\lsp\bin>instlsp64.exe -p
Winsock 64-bit Catalog:
=====
2606 - vlsplListener over [RSUP TCP Service Provider]
2607 - vlsplListener over [MSAFD Tcpip [TCP/IP]]
2608 - vlsplListener over [MSAFD Tcpip [UDP/IP]]
2609 - vlsplListener over [MSAFD Tcpip [RAW/IP]]
2610 - vlsplListener over [MSAFD Tcpip [TCP/IPv6]]
2611 - vlsplListener over [MSAFD Tcpip [UDP/IPv6]]
2612 - vlsplListener over [MSAFD Tcpip [RAW/IPv6]]
2613 - vlsplListener over [RSUP TCPv6 Service Provider]
2614 - vlsplListener over [RSUP UDPv6 Service Provider]
2615 - vlsplListener over [RSUP UDP Service Provider]
2616 - vlsplListener over [MSAFD Pgm (RDM)]
2617 - vlsplListener over [MSAFD Pgm (Stream)]
2618 - vlsplListener over [UMCI sockets DGRAM]
2619 - vlsplListener over [UMCI sockets STREAM]
1008 - RSUP 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 - RSUP TCPv6 Service Provider
1009 - RSUP UDPv6 Service Provider
1010 - RSUP UDP Service Provider
1011 - MSAFD Pgm (RDM)
1012 - MSAFD Pgm (Stream)
1013 - UMCI sockets DGRAM
1014 - UMCI sockets STREAM
2604 - vlsplListener
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

The image displays a network analysis tool interface for Civilization 4. The top portion shows a game map with a river and a city. Below the map is a control panel with 'Server Control' (Start/Stop buttons), 'listening ports' (input field, +, -, reset), and a table of ports. The 'Rules' section contains a dropdown menu set to '0' and 'Equal', and an 'Add' button. The 'Record' section has 'Record', 'Stop', and 'Clear' buttons, and a table of recorded data. The bottom right shows a network visualization with vertical bars of various colors and a detailed pixelated view of a single bar.

Server Control

Start Stop

listening ports

Port Packet Count

2056	3016
------	------

Rules

0 Equal Add

Name	Offset	Type	Match	Action	To	Size
------	--------	------	-------	--------	----	------

Record

Record Stop Clear Before After

Size	Recorded	Isolate Change	Count unchanged	Visualize
Size:11	561	Isolate	6	(o o)
Size:37	1965	Isolate	26	(o o)
Size:10	19	Isolate	10	(o o)
Size:29	2	Isolate	29	(o o)
Size:5	17	Isolate	5	(o o)

Civilization 4 vizualization

The image shows a screenshot of the game Civilization 4: Beyond the Sword. The game window is on top, showing a map with a river and a city. Below the game window is a networkUI overlay. The overlay has a 'Server Control' section with 'Start' and 'Stop' buttons, and a 'listening ports' section with a table showing port 2056 and packet count 3016. An orange arrow points from the text 'LSP listener' below to the '2056' port entry. To the right of the networkUI is a vertical visualization bar with a 'Scale' control at the top. The bar consists of several vertical columns of different colors (magenta, cyan, red, black) and a pattern of small colored squares on the right side.

networkUI

Server Control

Start Stop

listening ports

Port	Packet Count
2056	3016

Rules

0 Equal Add

Name	Offset	Type	Match	Action	To	Size
------	--------	------	-------	--------	----	------

Record Stop Clear

Size	Recorded	Isolate Change	Count unchanged	Visualize
Size:11	561	Isolate	6	(o o)
Size:37	1965	Isolate	26	(o o)
Size:10	19	Isolate	10	(o o)
Size:29	2	Isolate	29	(o o)
Size:5	17	Isolate	5	(o o)

Before After

Name	Size	Visualize
------	------	-----------

LSP listener

Civilization 4 vizualization

The image shows a screenshot of the game Civilization 4: Beyond the Sword. The game window is on the left, showing a map with a river and a city. The networkUI window is overlaid on the bottom. The networkUI window has a 'Server Control' section with 'Start' and 'Stop' buttons, and a 'listening ports' section with a table showing port 2056 and packet count 3016. An orange arrow points from the text 'LSP listener' to the 'listening ports' table. The 'Rules' section has a table with columns: Name, Offset, Type, Match, Action, To, Size. Below it is a 'Record' section with buttons 'Record', 'Stop', 'Clear', 'Before', and 'After'. A table shows recorded data with columns: Size, Recorded, Isolate Change, Count unchanged, Visualize. An orange arrow points from the text 'Buckets' to this table. On the right side of the image, there is a vertical visualization of network traffic, showing a series of colored vertical bars (magenta, cyan, red, black) and a detailed packet capture visualization on the far right.

networkUI

Server Control

Start Stop

listening ports

Port	Packet Count
2056	3016

LSP listener

Rules

Name	Offset	Type	Match	Action	To	Size
------	--------	------	-------	--------	----	------

Record Stop Clear Before After

Size	Recorded	Isolate Change	Count unchanged	Visualize
Size:11	561	Isolate	6	(o o)
Size:37	1965	Isolate	26	(o o)
Size:10	19	Isolate	10	(o o)
Size:29	2	Isolate	29	(o o)
Size:5	17	Isolate	5	(o o)

Buckets

Civilization 4 vizualization

Bucket visualization →

LSP listener

Buckets

Port	Packet Count
2056	3016

Size	Recorded	Isolate Change	Count unchanged	Visualize
Size:11	561	Isolate	6	(o o)
Size:37	1955	Isolate	26	(o o)
Size:10	19	Isolate	10	(o o)
Size:29	2	Isolate	29	(o o)
Size:5	17	Isolate	5	(o o)

Civilization 4 visualization

The image shows a screenshot of a network visualization tool for Civilization 4. The top part of the screenshot is a dark map of the game world. Below the map is a control panel with buttons for 'Start', 'Stop', and 'Reset'. There are also 'Listening ports' and 'Port' fields. A table shows 'Packet Count' for various ports. Below this is an 'LSP listener' section with 'Memory' and 'Address' fields. At the bottom, there is a 'Buckets' section with a table of recorded data and a 'Visualize' button. To the right of the screenshot is a vertical visualization of buckets, showing a series of colored bars (magenta, cyan, red, blue) of varying heights, representing the distribution of data across different buckets.

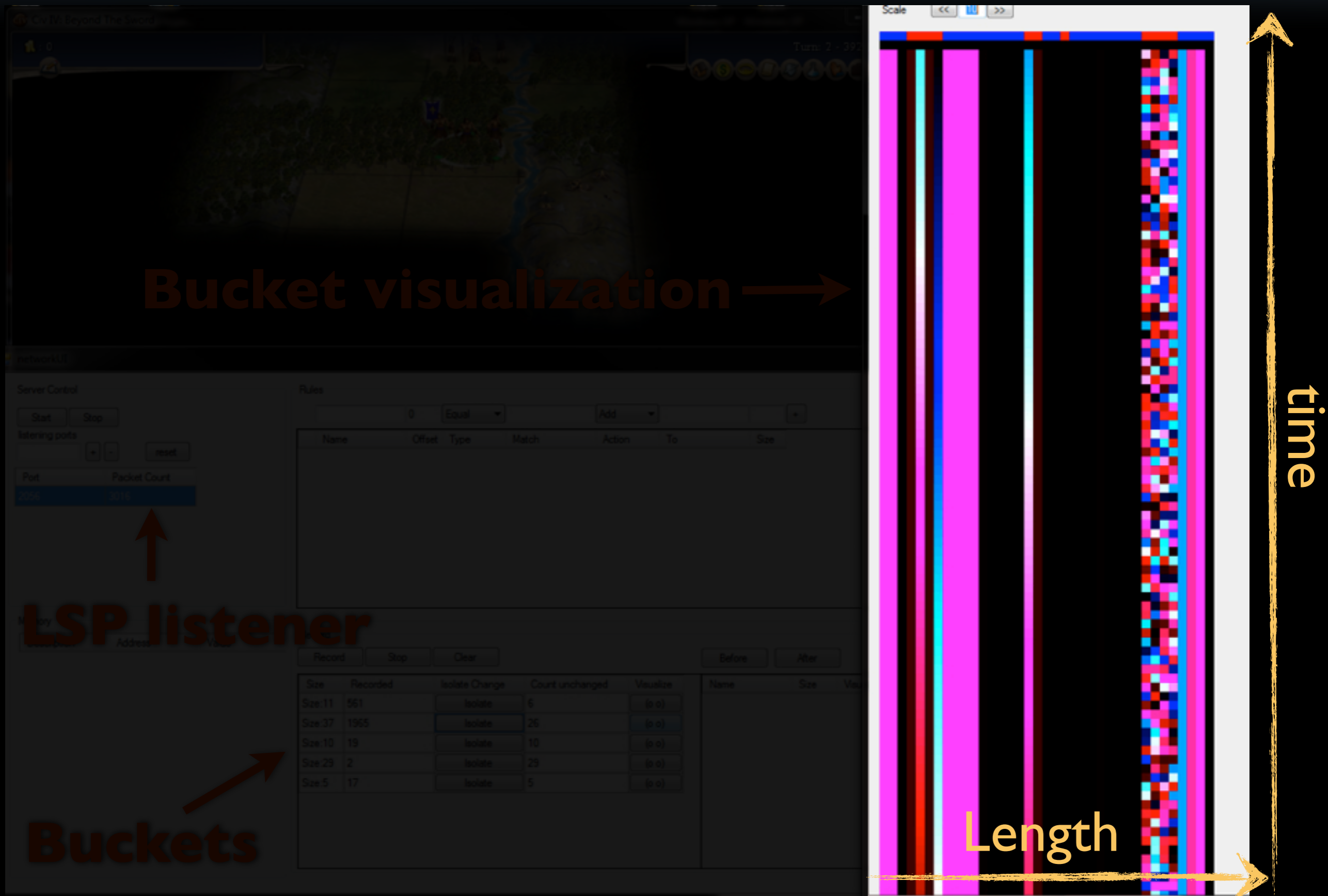
Bucket visualization →

↑ **LSP listener**

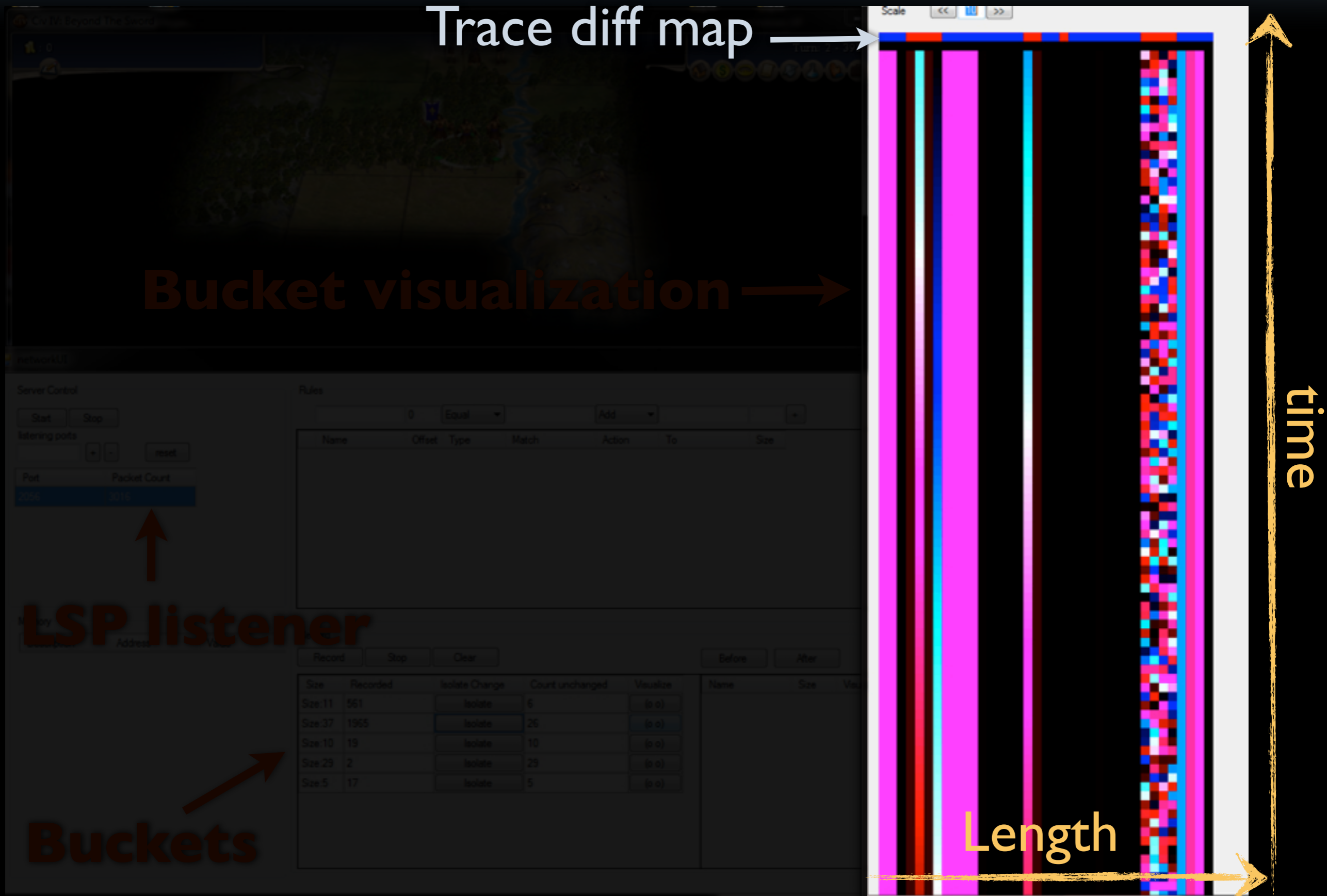
↗ **Buckets**

Size	Recorded	Isolate Change	Count unchanged	Visualize
Size 11	561	isolate	5	(o)
Size 37	1965	isolate	26	(o)
Size 10	19	isolate	10	(o)
Size 29	2	isolate	29	(o)
Size 5	17	isolate	5	(o)

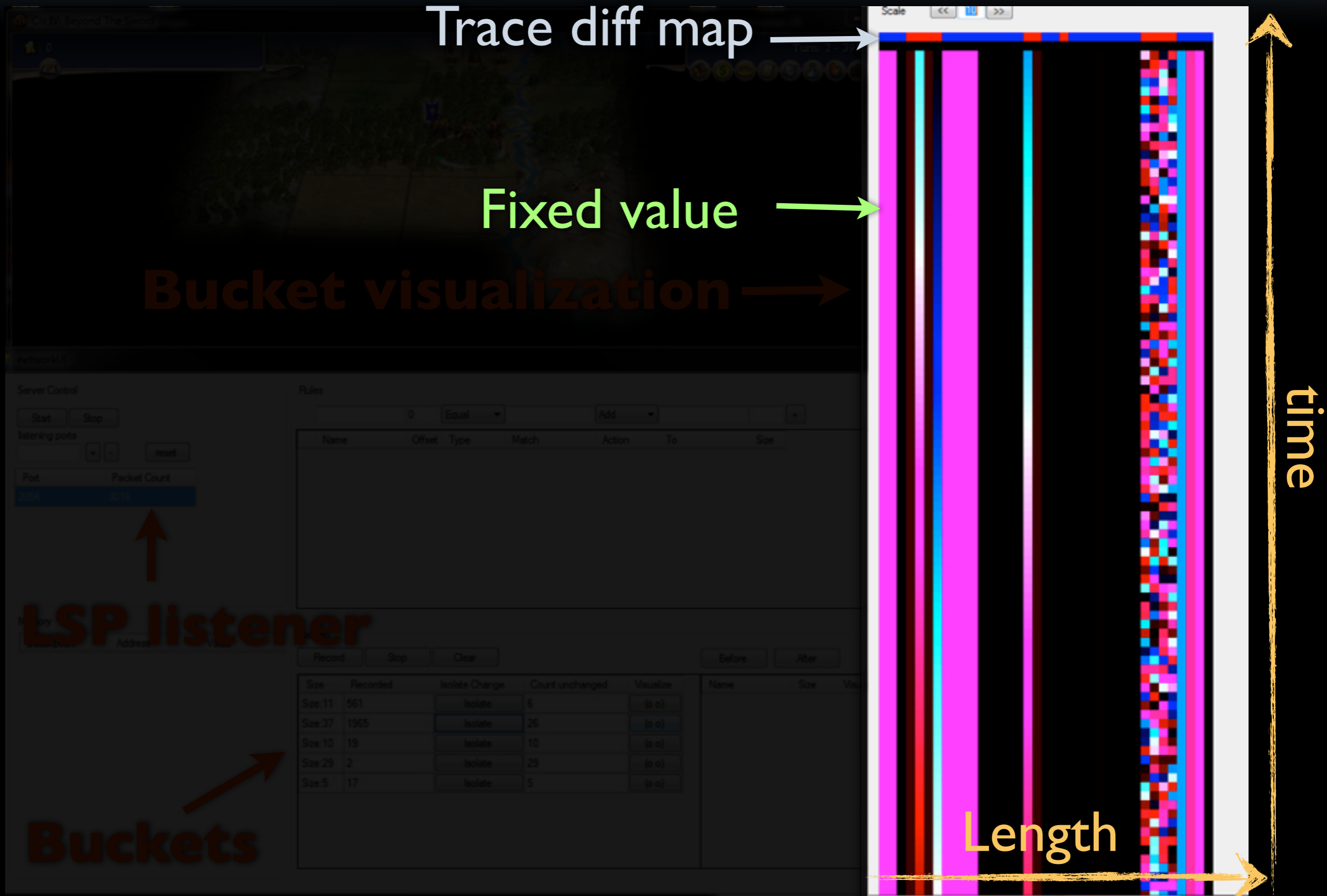
Civilization 4 visualization



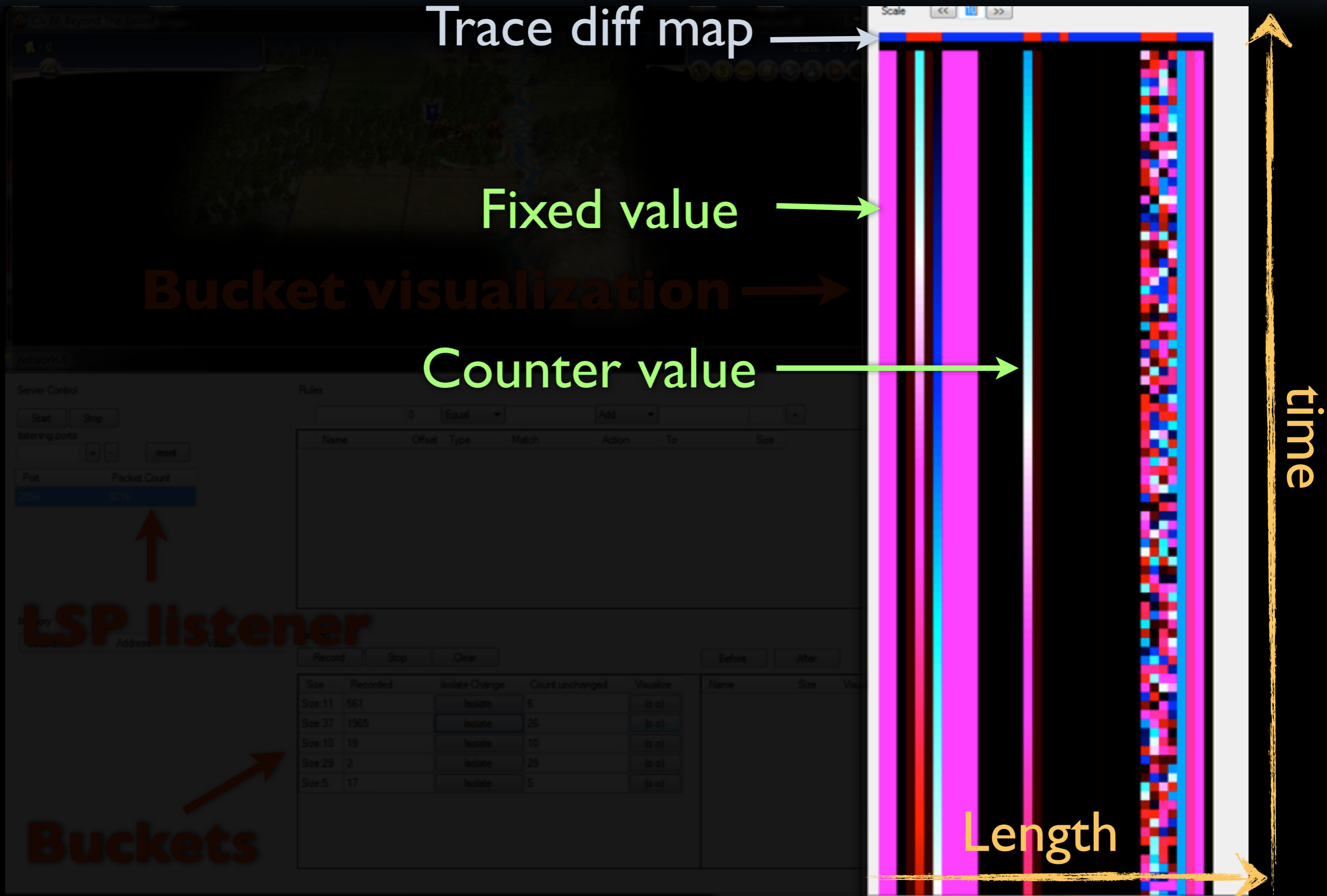
Civilization 4 visualization



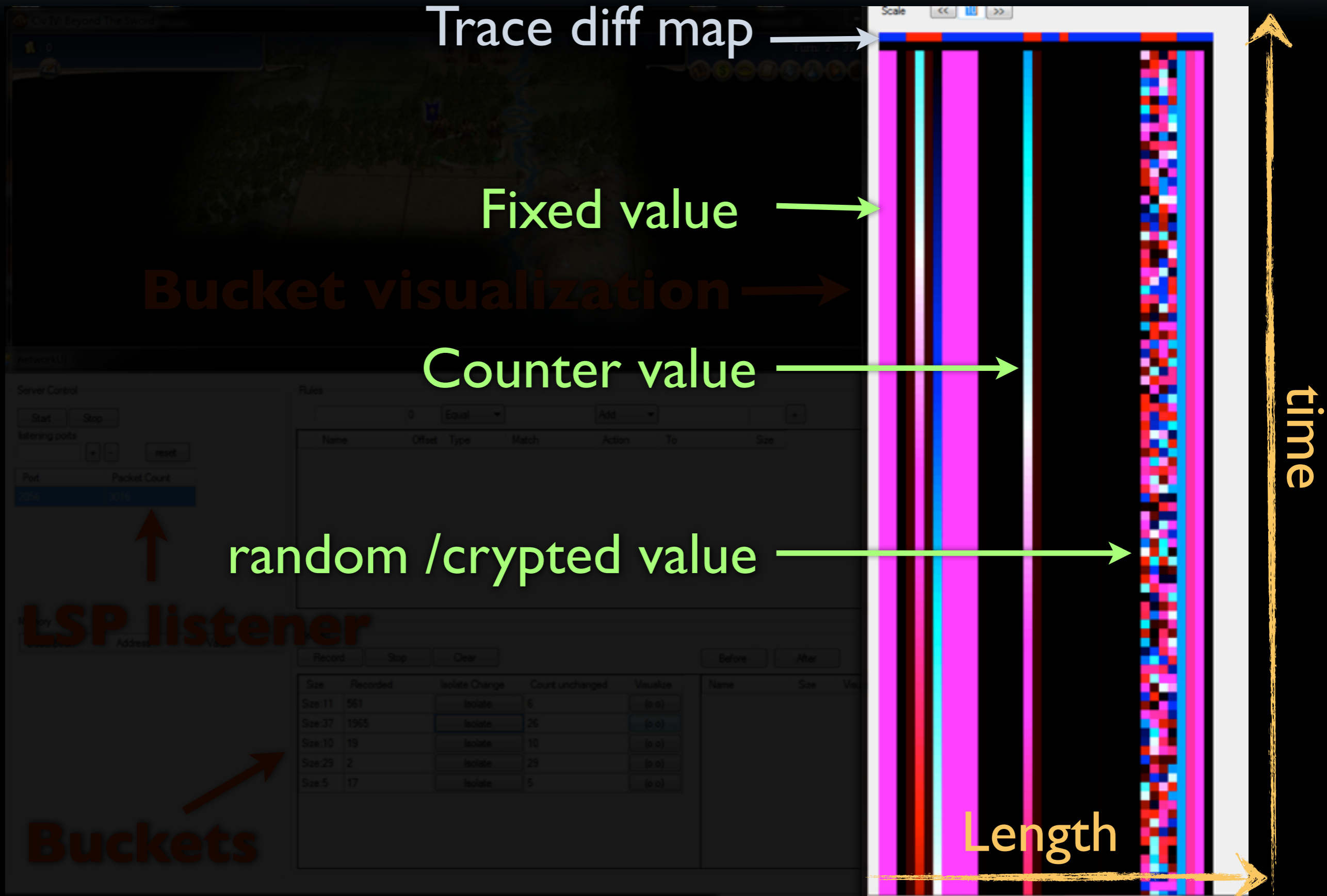
Civilization 4 visualization



Civilization 4 visualization



Civilization 4 visualization



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>

