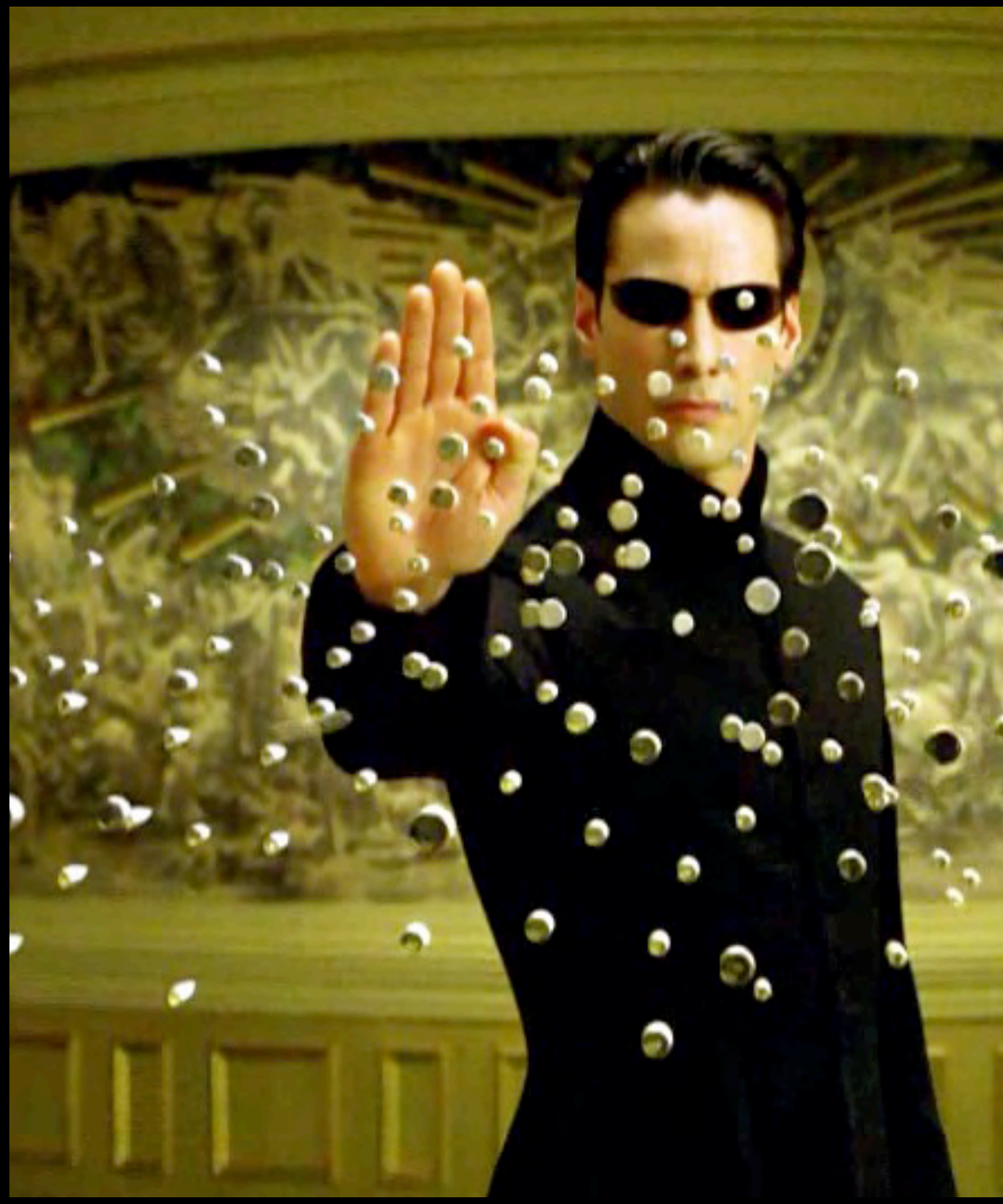
Kartograph

Elie Bursztein and Jocelyn Lagarenne
Stanford University

Welcome to the real world

supernatural powers !

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



God mode illustrated (video)

Memory based attack

Memory

Memory based attack

Memory

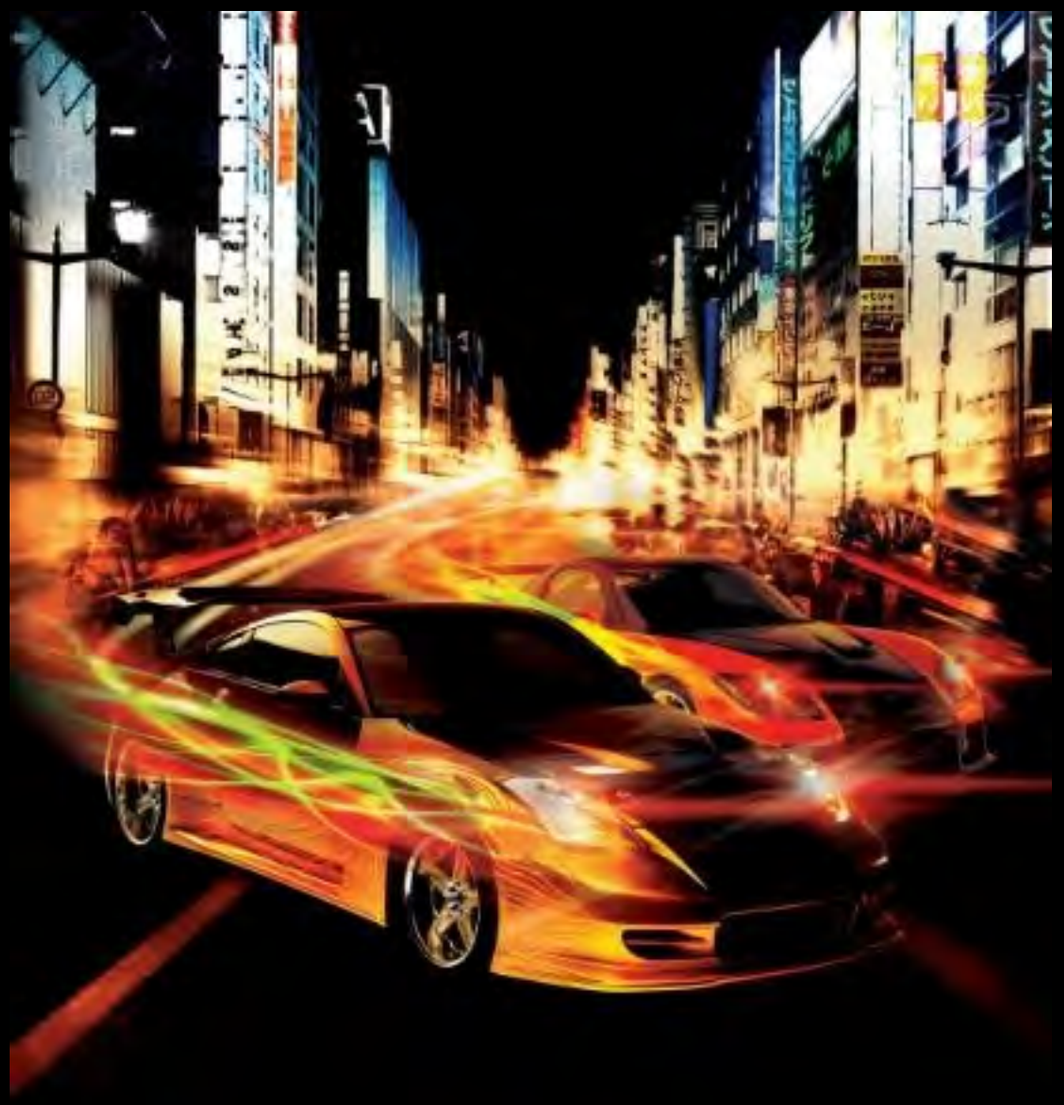
Modification

Memory based attack

Memory

Modification

Benefits (fast and furious)



- Generic
- Fast
- Invisible

Drawbacks

Game memory

Structures

Background

273 Millions games sold in 2009

Game type

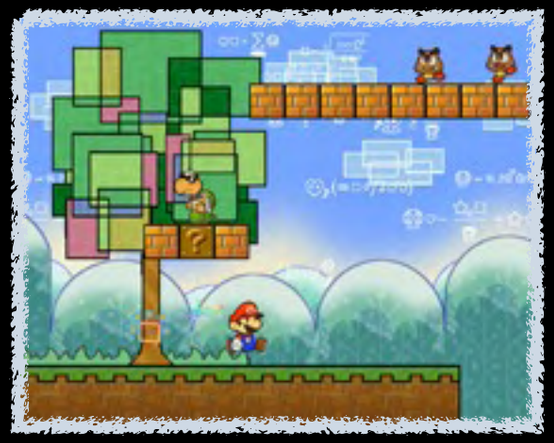
Action

Game type

Action

First person

Game type

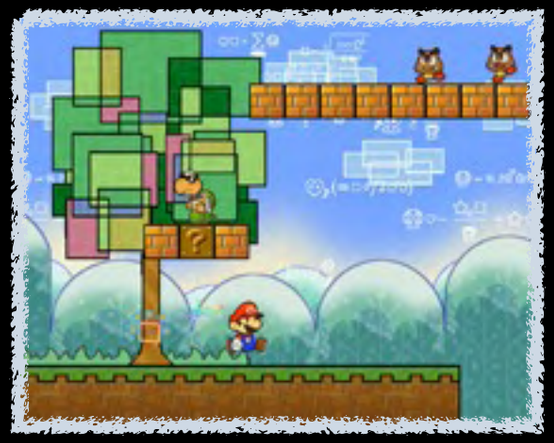


Action

First person

Sport

Game type



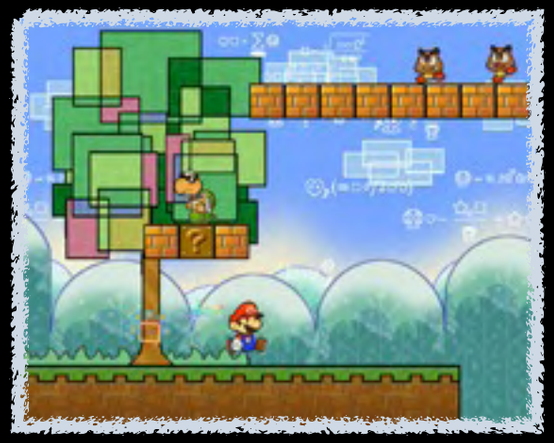
Action

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


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

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

How to do a map hack

How to do a map hack

How to do a map hack

Reduce

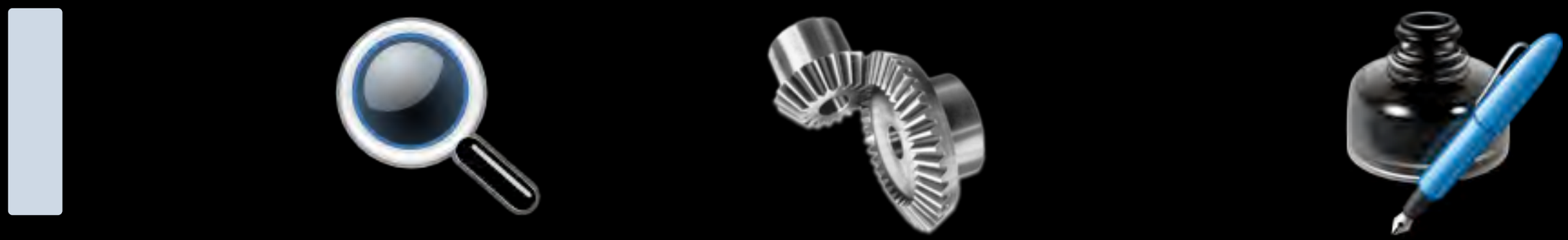
How to do a map hack

Reduce Find

How to do a map hack

Reduce Find Understand

How to do a map hack

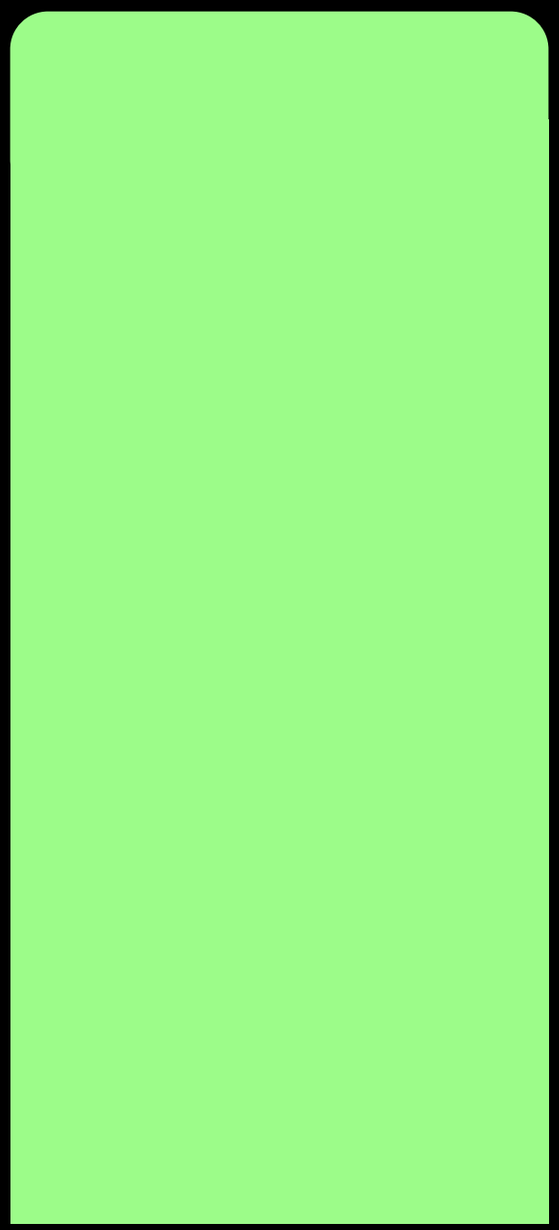


Reduce Find Understand Rewrite

Acquiring game memory

Game memory

Acquiring game memory



How to reduce the search space

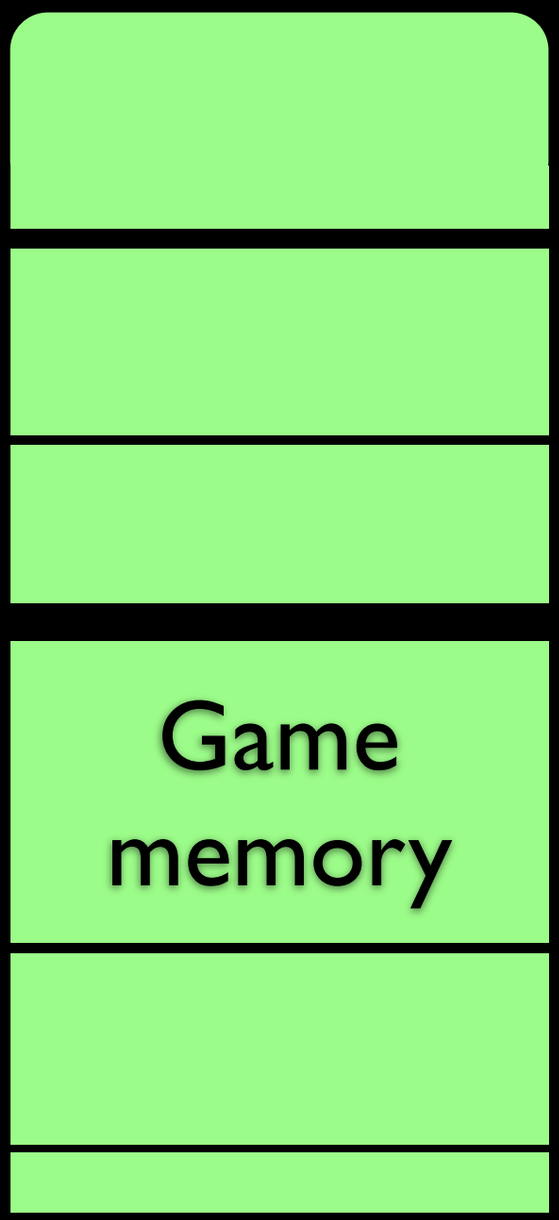
Game memory

Play

Discover

Play more

How to reduce the search space

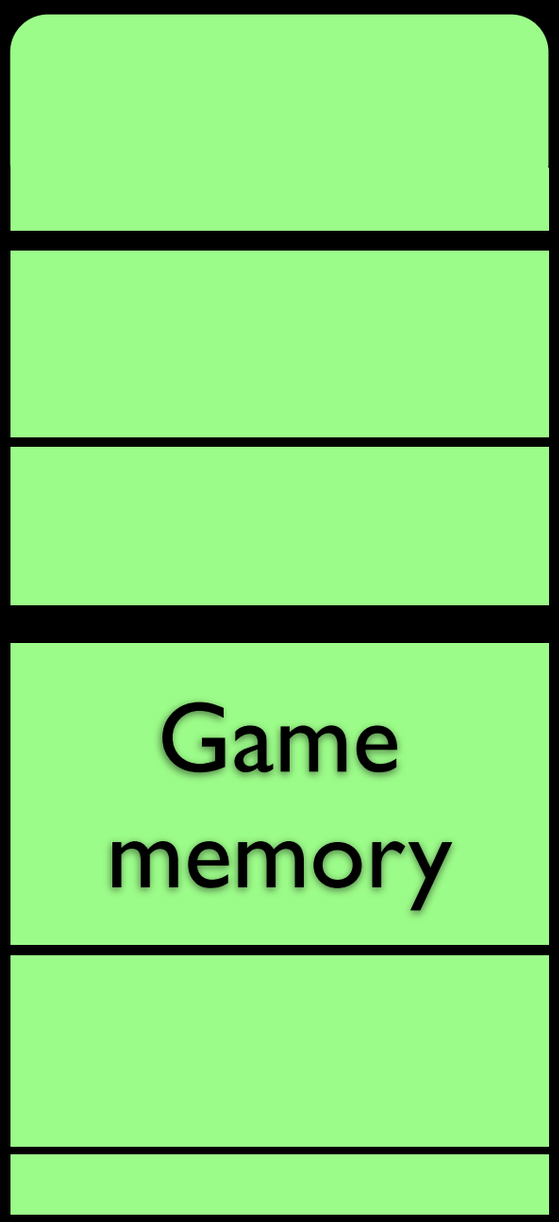


Play

Discover

Play more

How to reduce the search space

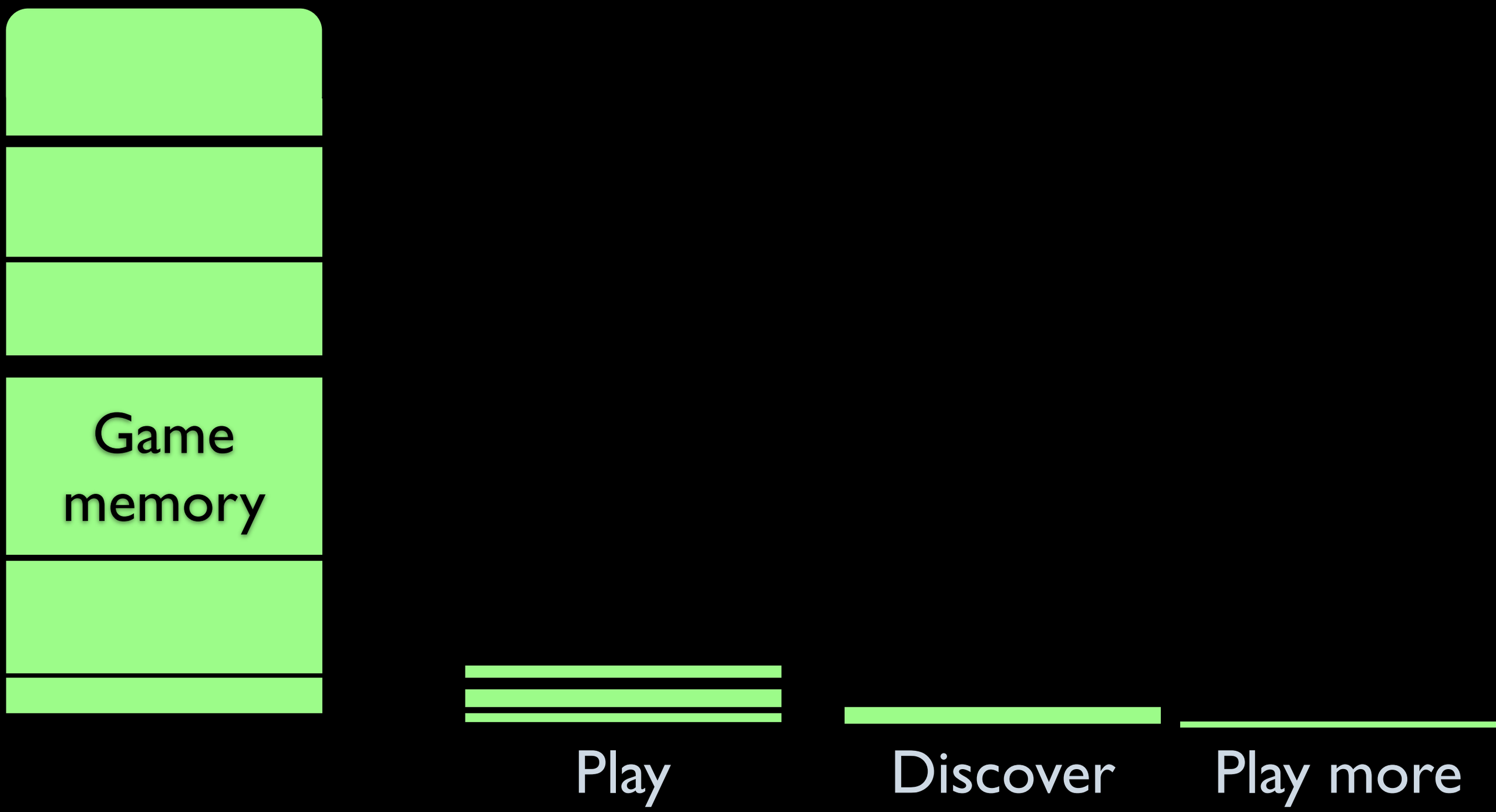


Play

Discover

Play more

How to reduce the search space



How to reduce the search space

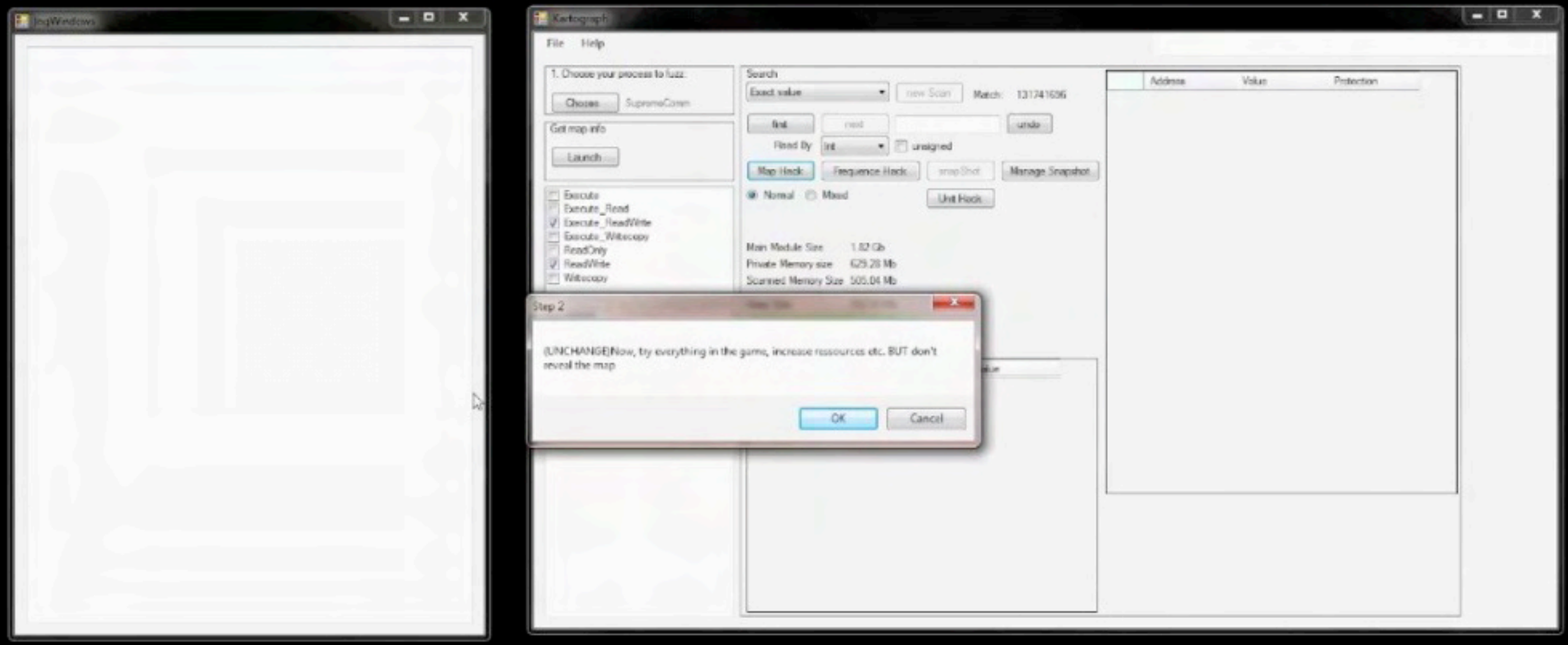
Play Discover Play more

Acquiring the game's memory


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

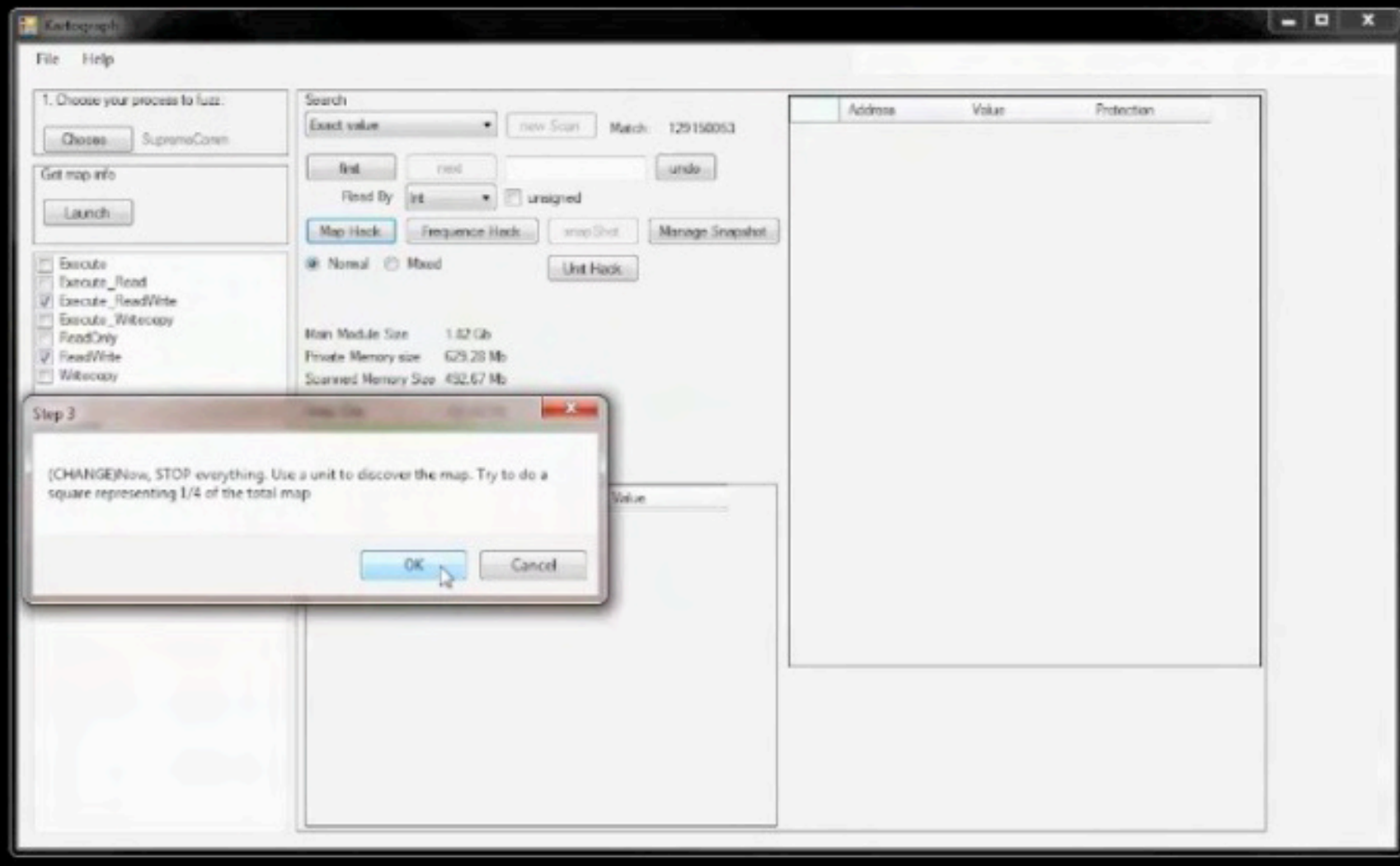
Step 1

Removing unrelated memory


Kartograph
File
Help
1. Choose your process to fuzz:
Choose
SupremaCoren
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

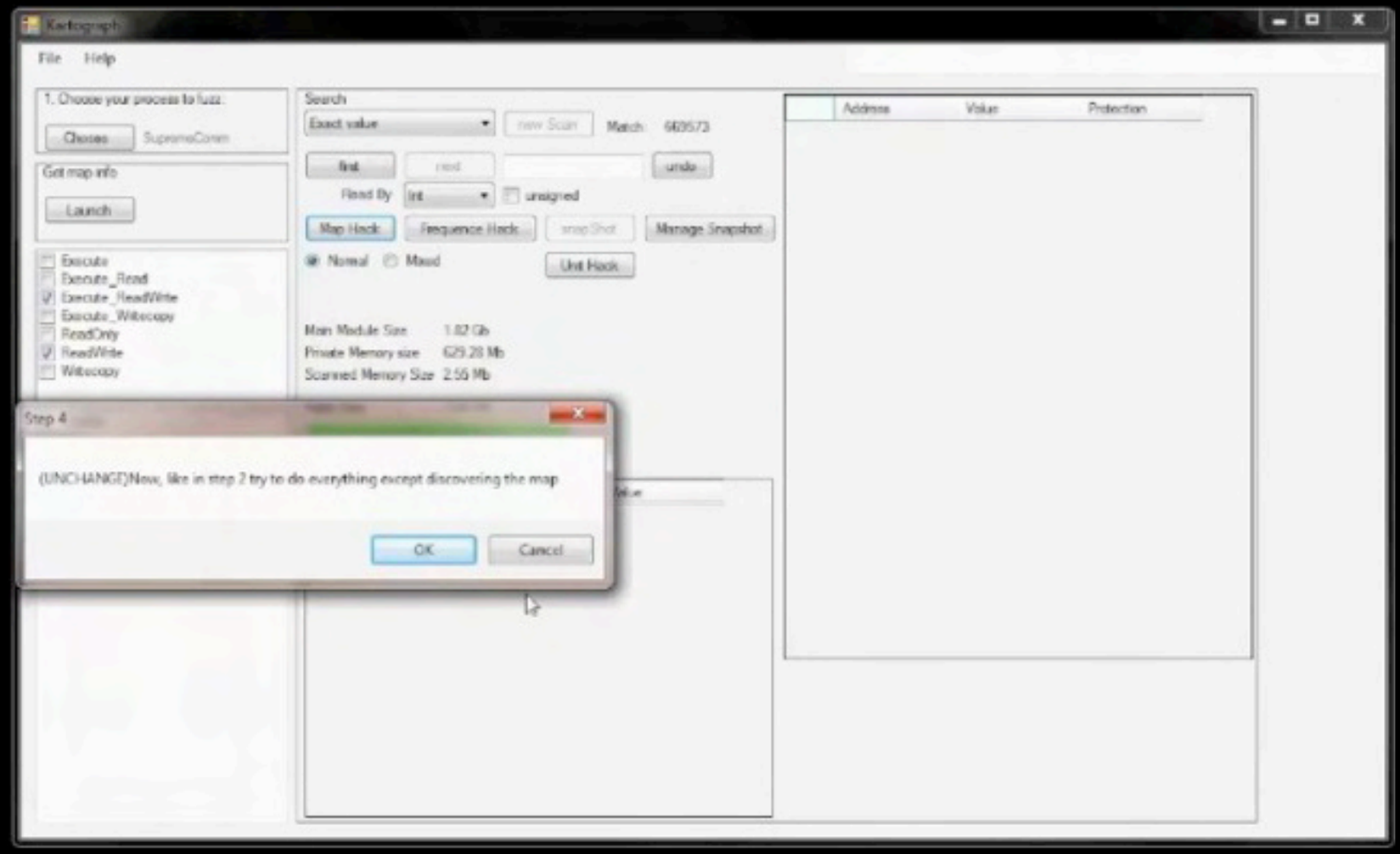
Discovering the map and keeping relevant memory


File Help
1. Choose your process to fuzz:
Choose
SupremoCoren
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 1.42 Gb
Private Memory size 629.28 Mb
Scanned Memory Size 492.67 Mb
Address
Value
Protection
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


TopWindows


Kartograph
File
Help
1. Choose your process to fuzz:
Choose
SupremaComm
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
2.56 Mb
Address
Value
Protection
Step 4
(UNCHANGE)Now, like in step 2 try to do everything except discovering the map
OK
Cancel

Step 4

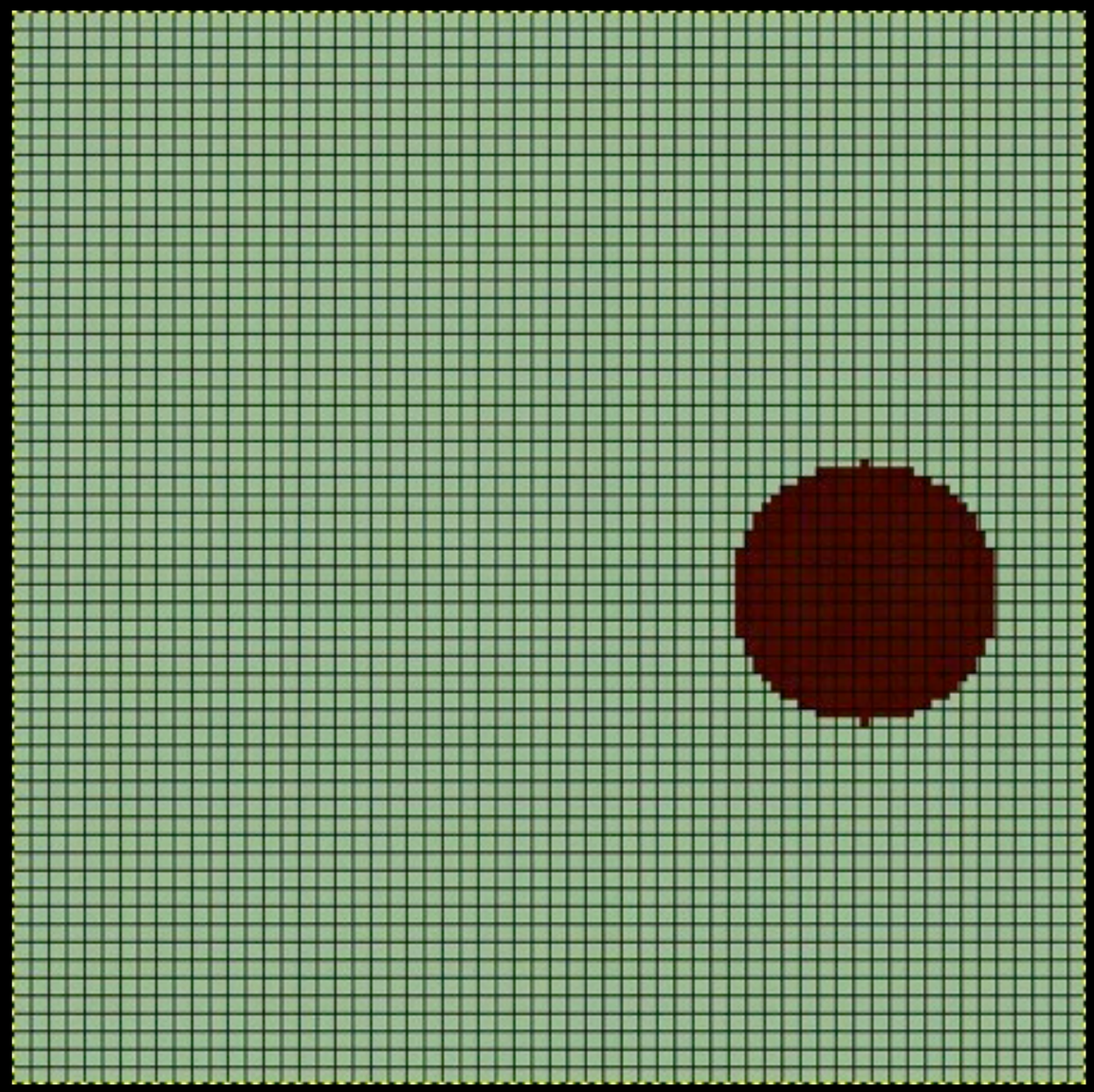
Finding the map in the remaining memory

Working assumption

Maps are stored in 2-D arrays

Working assumption

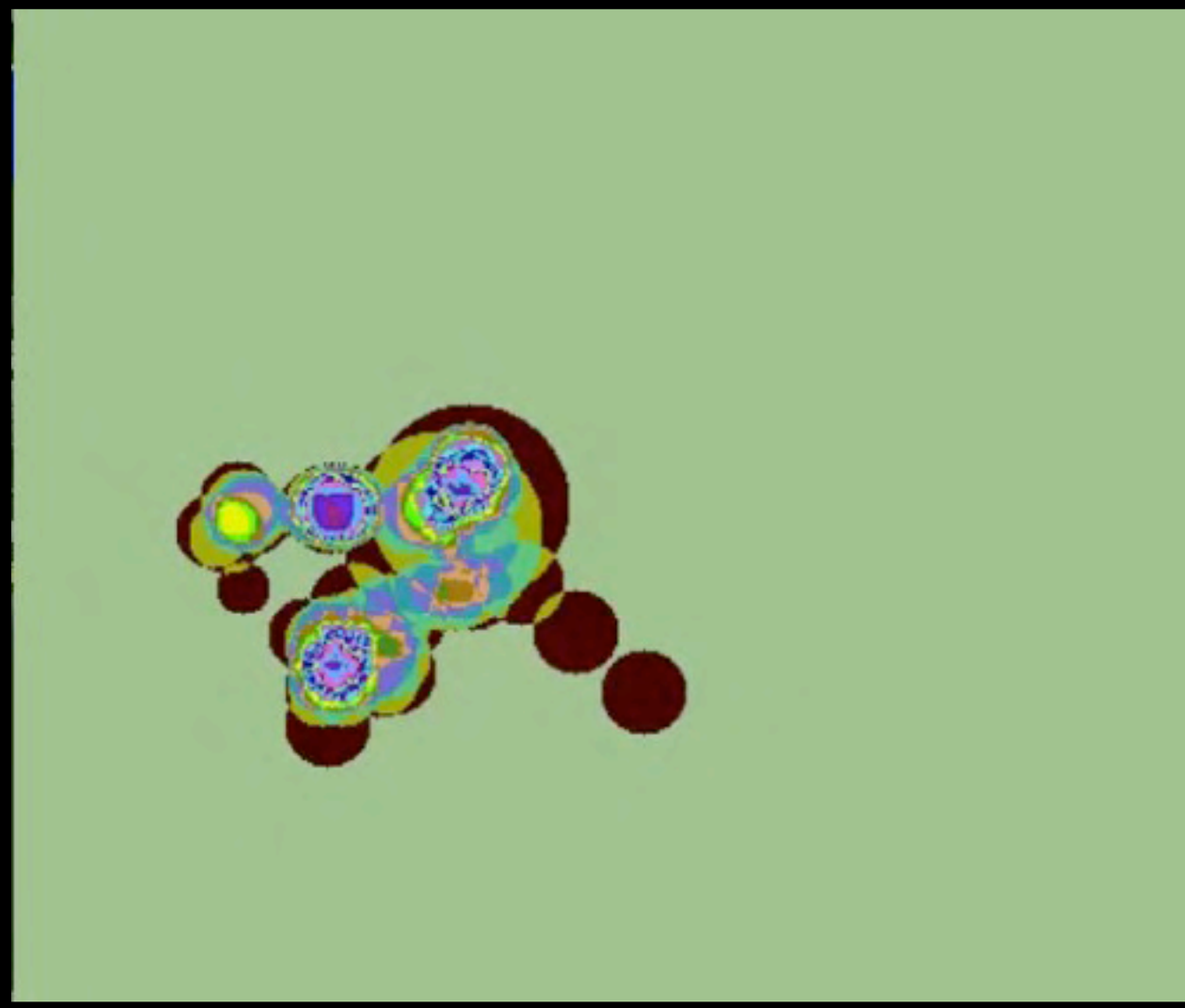
Maps are stored in 2-D arrays



Step 5

Isolating the potential map

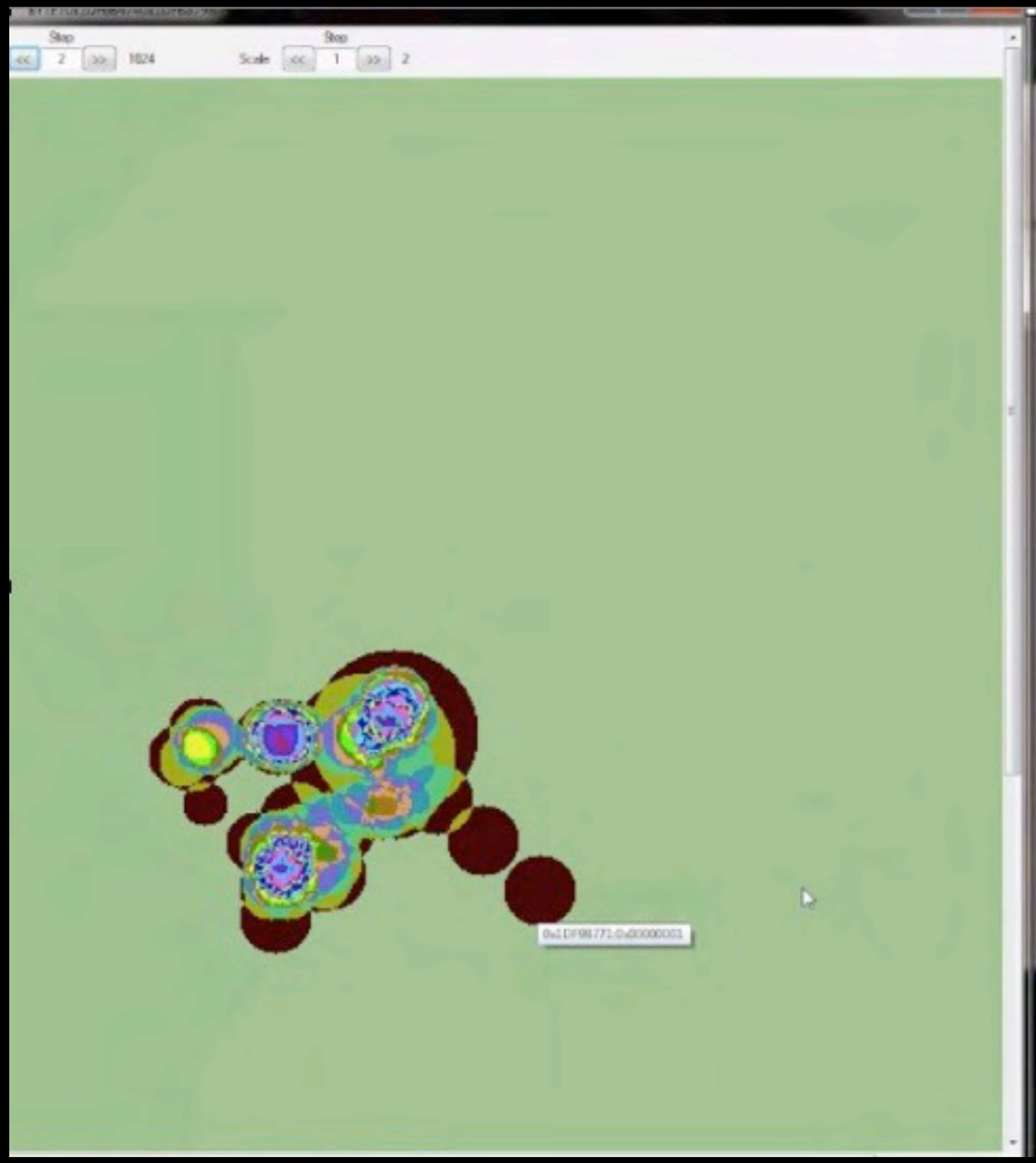
In game

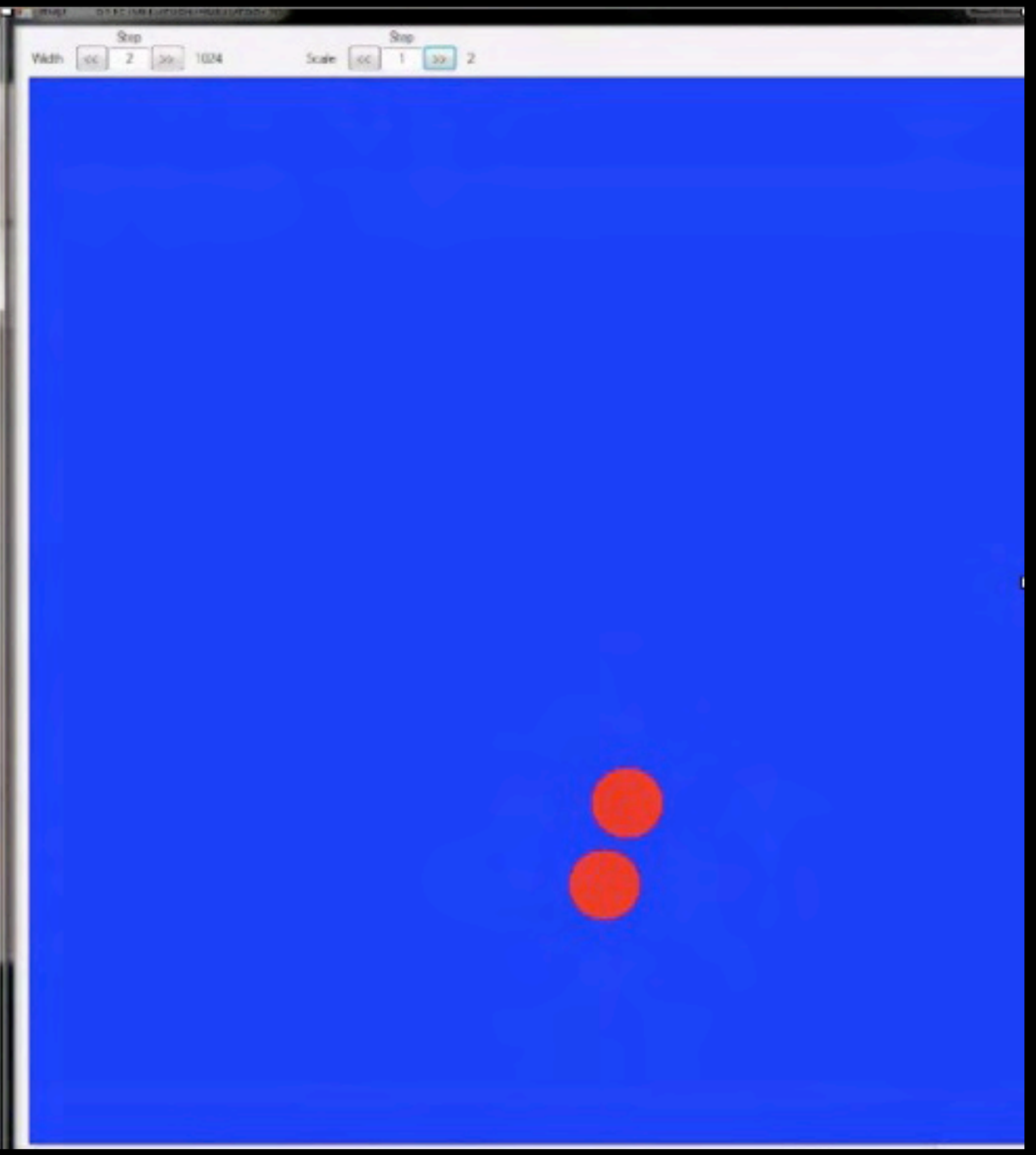


In memory

Step 6

Understanding the map's structure


Step
<< 2 >> 1024
Step
Scale << 1 >> 2


Step
Width << 2 >> 1024
Step
Scale << 1 >> 2

Step 8

Rewriting the memory for fun and profit

Unexpected effects

Unit hacking

Stay tuned for our next episode

Will be available in the online version of the slides

Kartograph Demo

Ongoing work

- Active attack (Network).
- Defense (Multi-parties crypto)

Questions