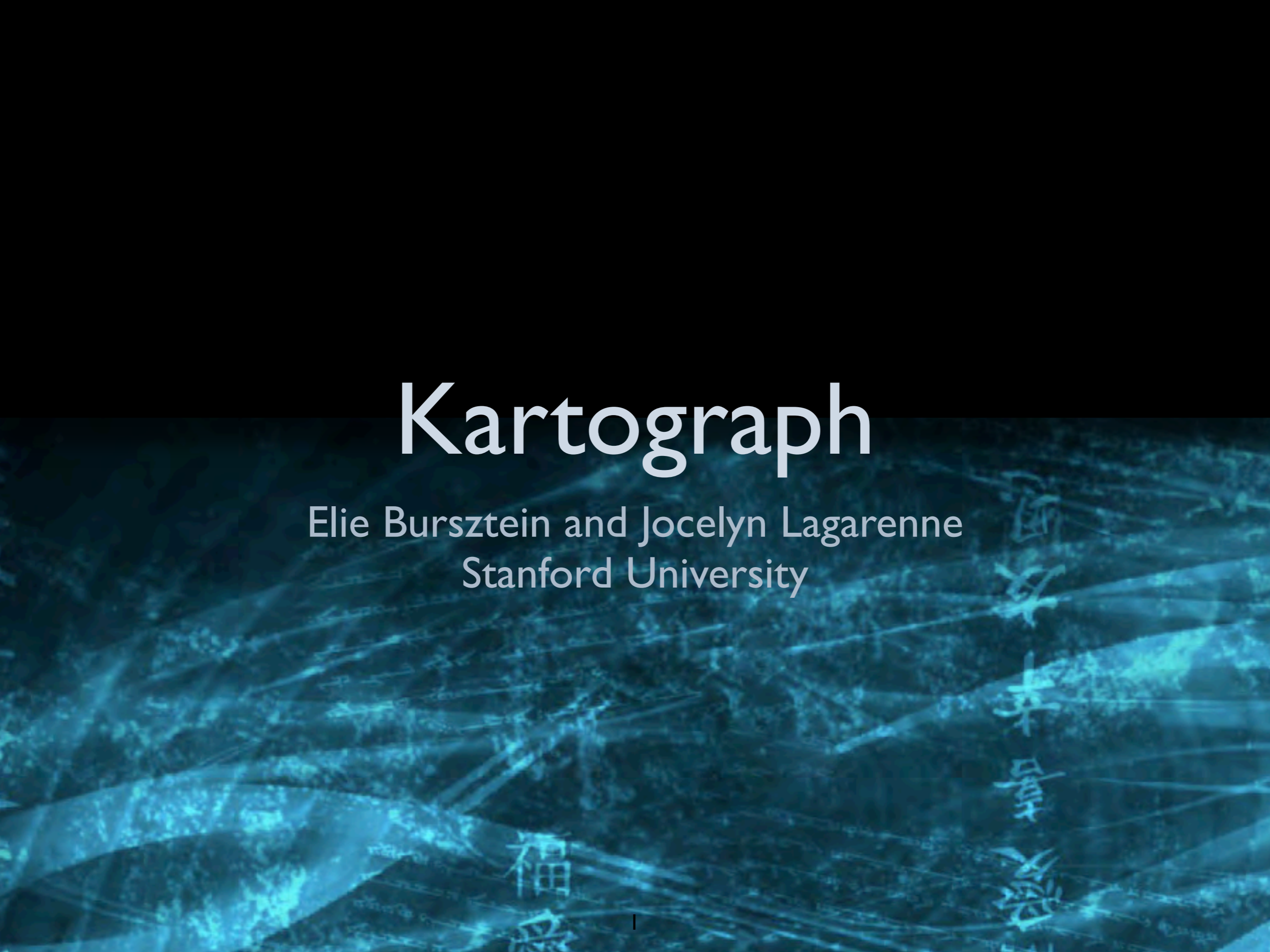


Kartograph

Elie Bursztein and Jocelyn Lagarenne
Stanford University

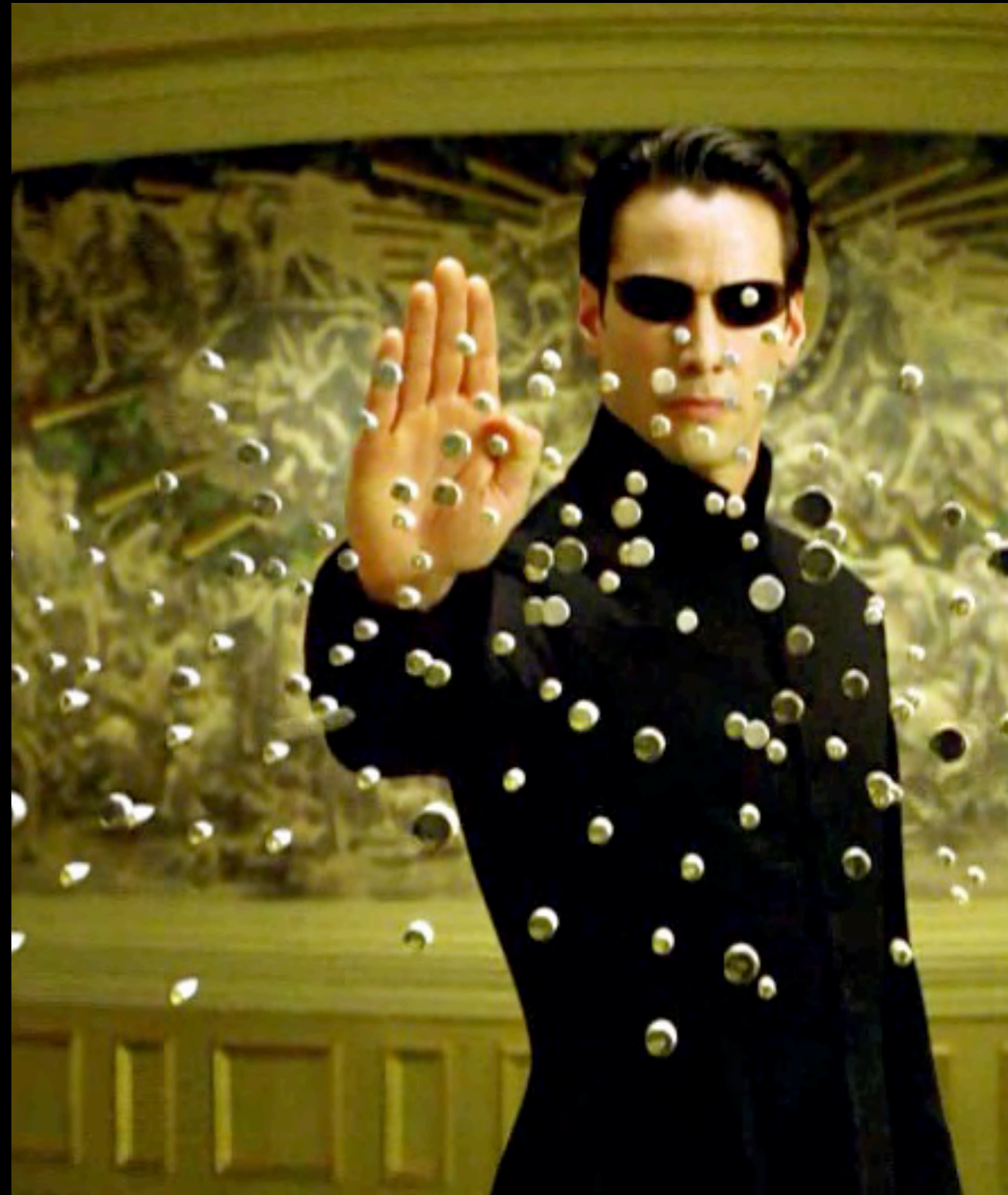




Welcome to the real world

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



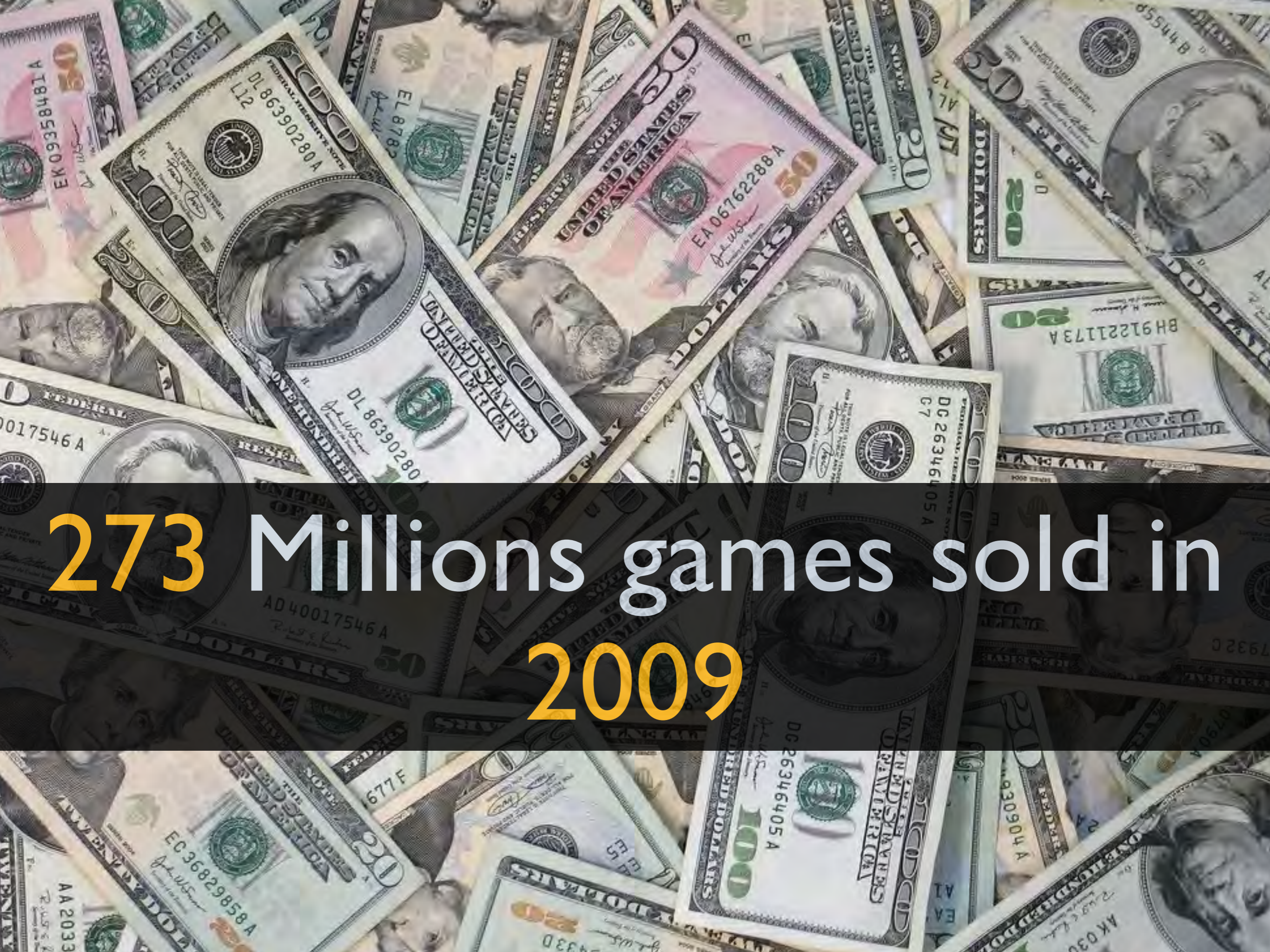
Game memory



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**





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

Instant Dojo

--	--

⏪ ⏩ ⏴ ⏵ ⏶ ⏷ ⏸ ⏹ ⏺



Units →

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

Building



The top right corner of the game interface. It features a mini-map of the current level with a yellow box highlighting the player's location. Below the map are icons for a wrench, a dollar sign, a gear, and a red arrow. To the right of these icons is a currency display showing '4650'. Below the currency are icons for a house, a shield, a robot, and a red arrow.

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

A grid of nine icons representing different units and buildings. The icons include a satellite, a soldier, a tank, a character, a robot, a tank, a character, a robot, and a building.

A panel titled 'Instant Dojo' containing a large icon of the Tankbuster building. Below the icon are several smaller icons, including a robot, a gear, and a question mark.

The bottom left corner of the game interface. It features a circular zoom level indicator showing '1' and a health bar with a red and yellow gradient.



Resources

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

Minimap →

4650

Icons for various game actions: repair, money, power, and unit selection.

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

Instant Dojo

Navigation and action buttons for the Instant Dojo.

1

11x 12x 13x

Zoom and camera controls.



Visible

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

Instant Dojo

--	--

Navigation buttons: back, forward, search, help

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



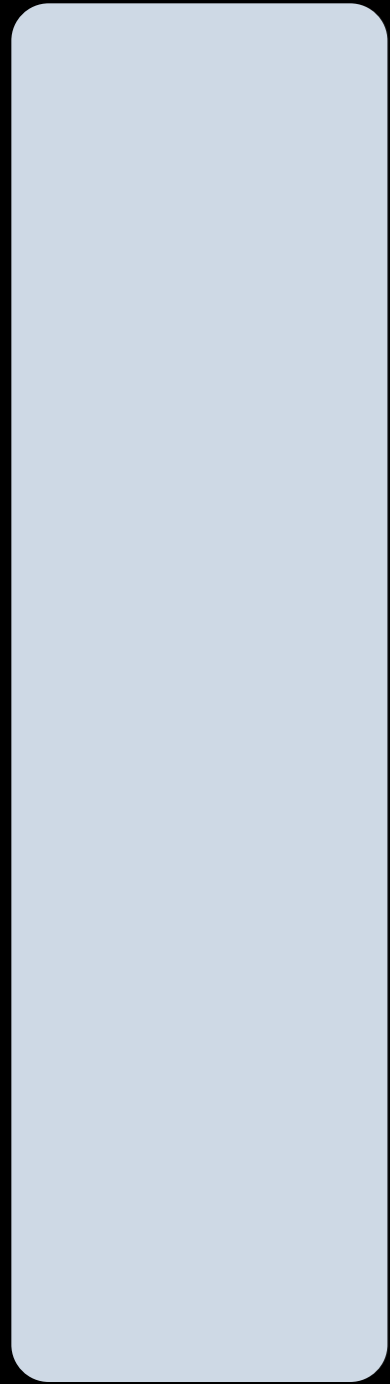


There is no spoon

Maphack

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

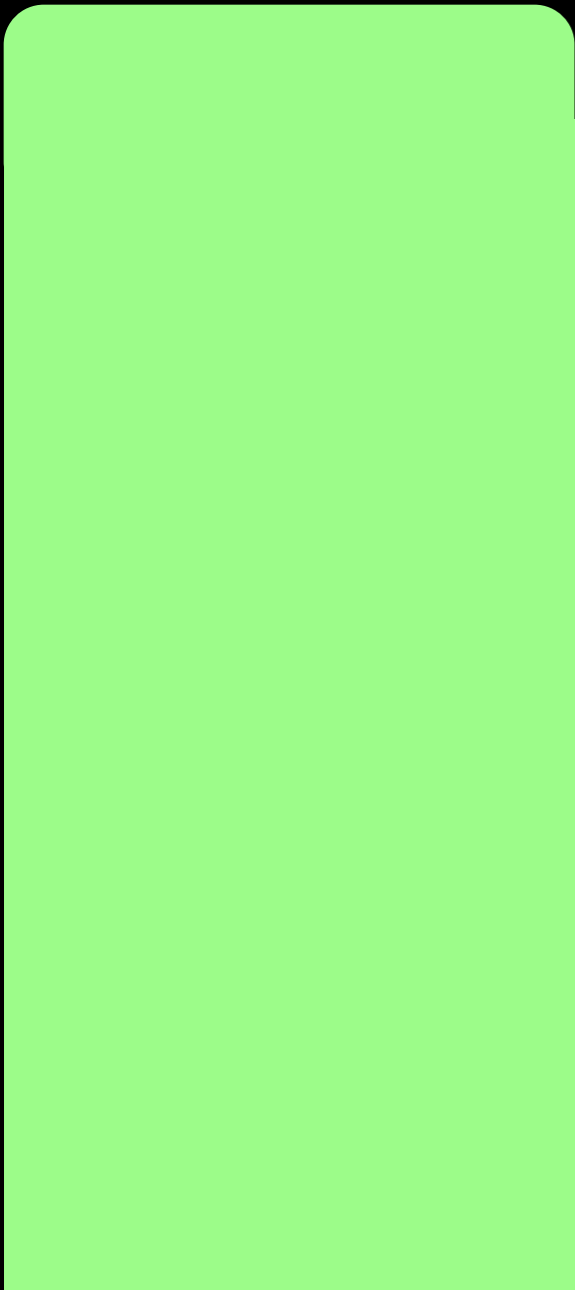
Understand

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



Game
memory

Play

Discover

Play more

How to reduce the search space



Game
memory



Play



Discover

Play more

How to reduce the search space



Game
memory



Play



Discover



Play more

How to reduce the search space

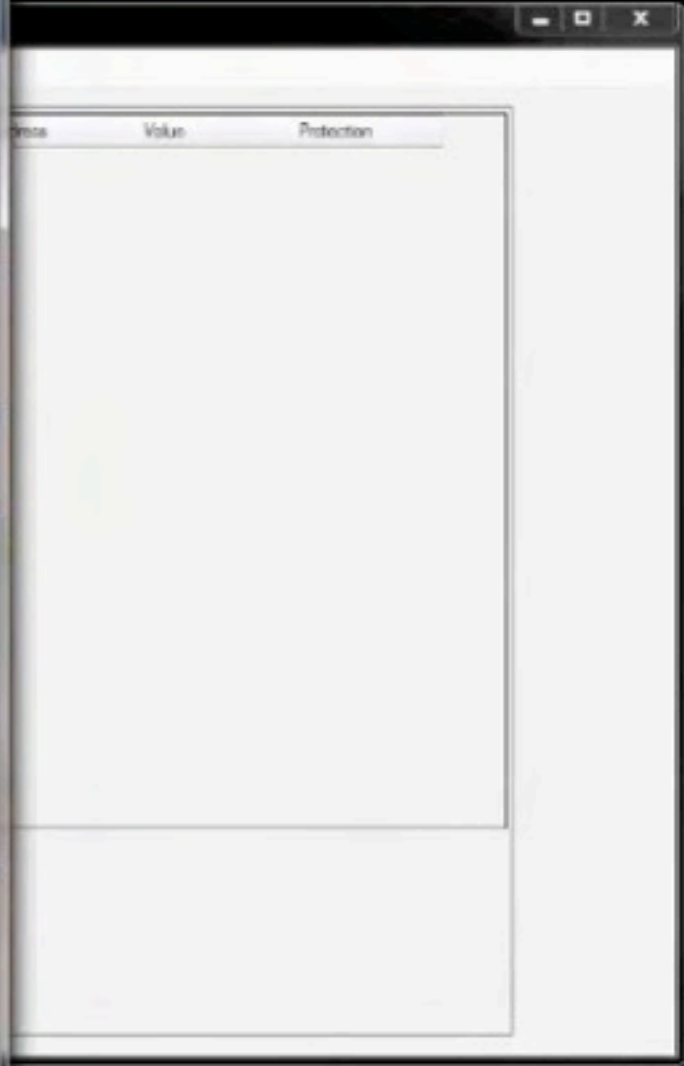


Play

Discover

Play more

Acquiring the game's
memory



Step 1

Removing unrelated
memory



Karograph

File Help

1. Choose your process to fuzz.

Choose SupremeCrown

Get map info

Launch

Execute
 Execute_Read
 Execute_ReadOnly
 Execute_WriteCopy
 ReadOnly
 ReadWrite
 WriteCopy

Search

Exact value new Scan Match: 131741636

find read undo

Read By int unsigned

Map Hook Frequency Hook snapShot Manage Snapshot

Normal Mixed

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 resources etc. BUT don't reveal the map

OK Cancel

Step 2

Discovering the map and
keeping relevant memory



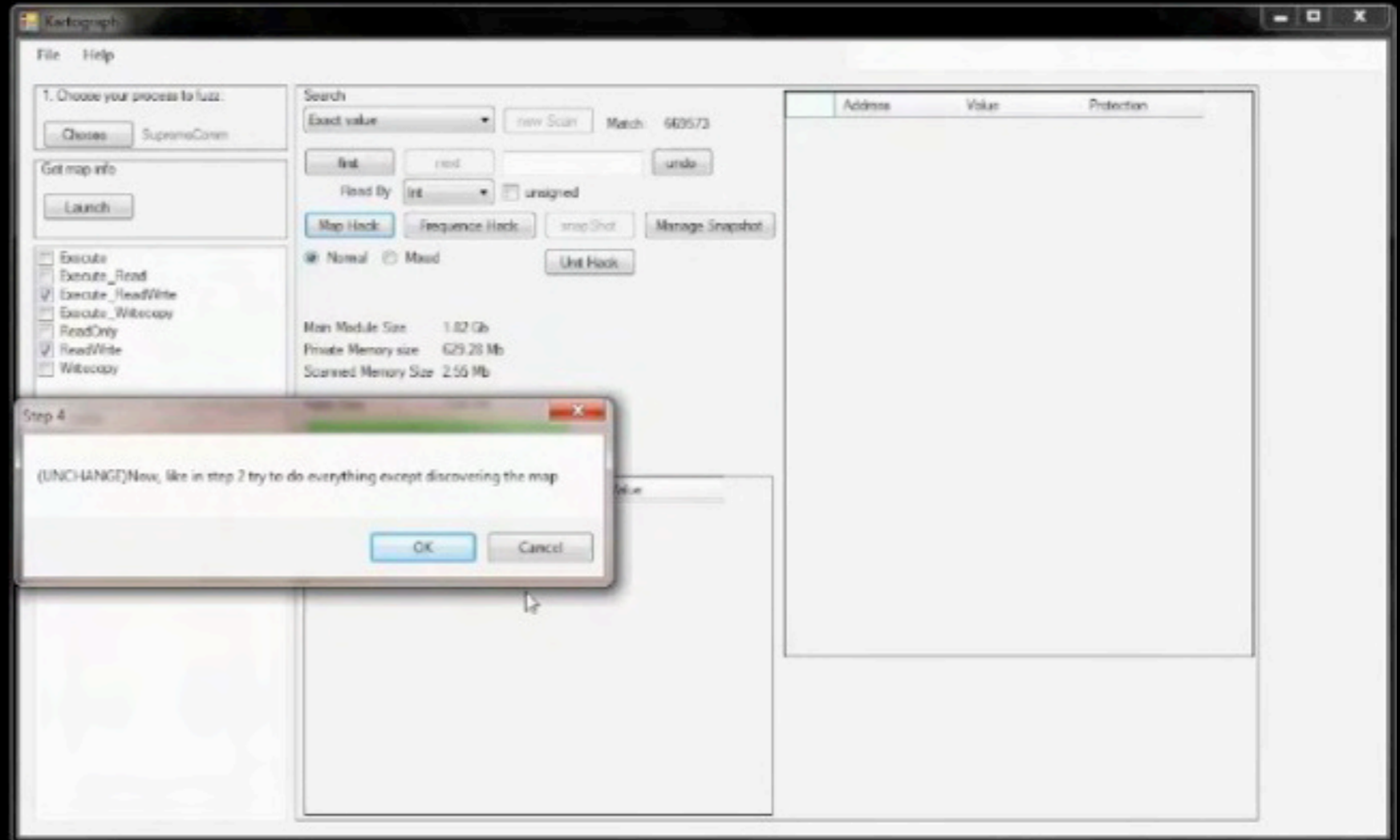
The screenshot shows the 'Kernograph' application window. The interface includes a menu bar with 'File' and 'Help'. The main area is divided into several sections:

- 1. Choose your process to fuzz:** A 'Choose' button is next to 'SupremoCoren'.
- Get map info:** A 'Launch' button.
- Permissions:** A list of checkboxes: Execute, Execute_Read, Execute_ReadWrite, Execute_Writecopy, ReadOnly, ReadWrite, Writecopy.
- Search:** A dropdown menu set to 'Exact value', a 'new Scan' button, and a 'Match: 129150053' label. Below are 'list', 'read', and 'undo' buttons.
- Read By:** A dropdown menu set to 'int' and an 'unsigned' checkbox.
- Buttons:** 'Map Hack', 'Frequency Hack', 'undo Cheat', 'Manage Snapshot', and 'Unit Hack' buttons.
- Radio Buttons:** Normal, Mixed.
- Memory Stats:** 'Main Module Size: 1.82 Gb', 'Private Memory size: 629.28 Mb', and 'Scanned Memory Size: 492.67 Mb'.
- Table:** A table with columns 'Address', 'Value', and 'Protection'.

A dialog box titled 'Step 3' is overlaid on the application. It contains the text: '[CHANGE]Now, STOP everything. Use a unit to discover the map. Try to do a square representing 1/4 of the total map'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Step 3

Removing more unrelated
memory



Step 4

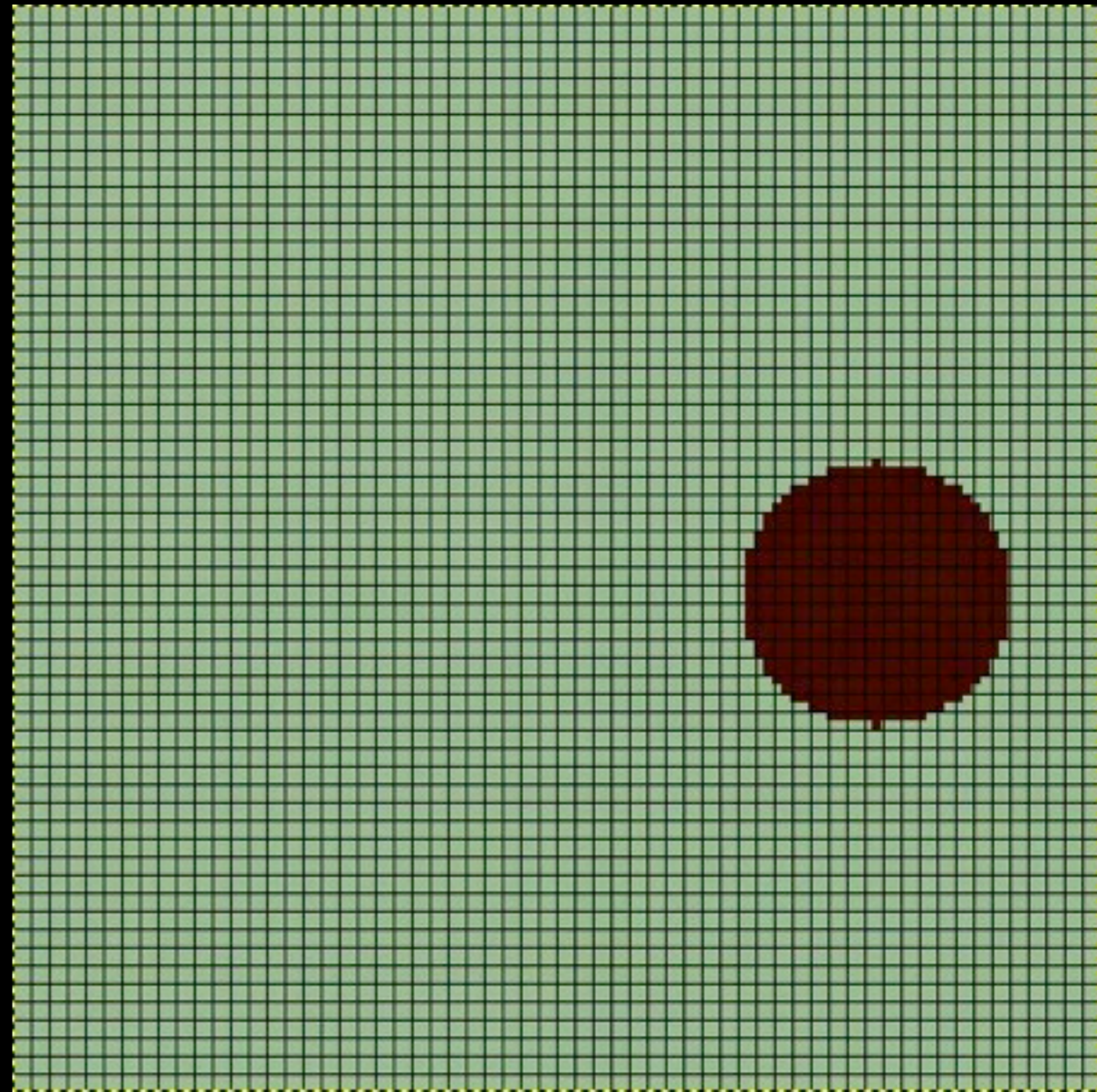
Finding the map in the
remaining memory

Working
assumption
Maps are stored in
2-D arrays



Working
assumption

Maps are stored in
2-D arrays



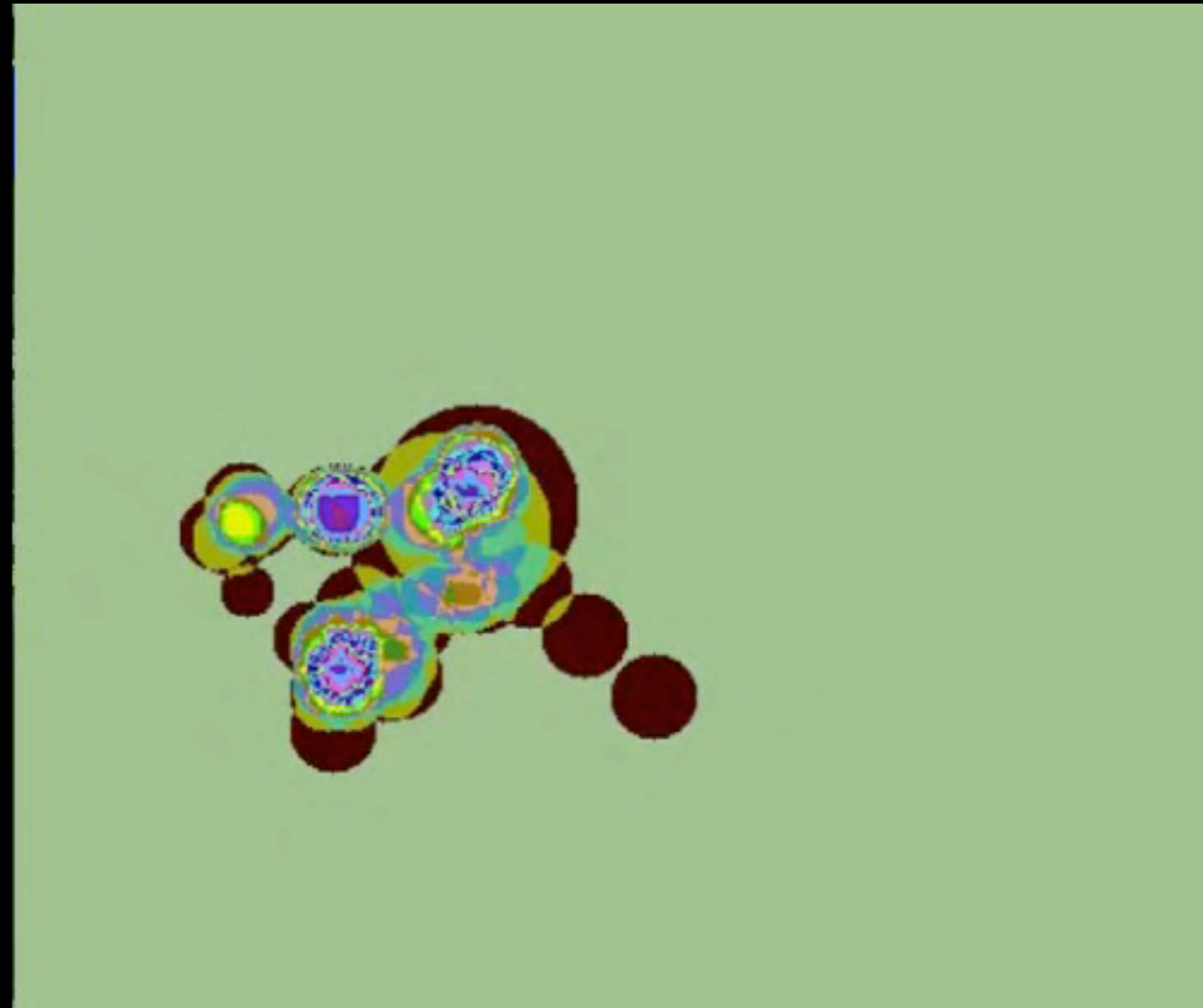


Step 5

Isolating the potential map



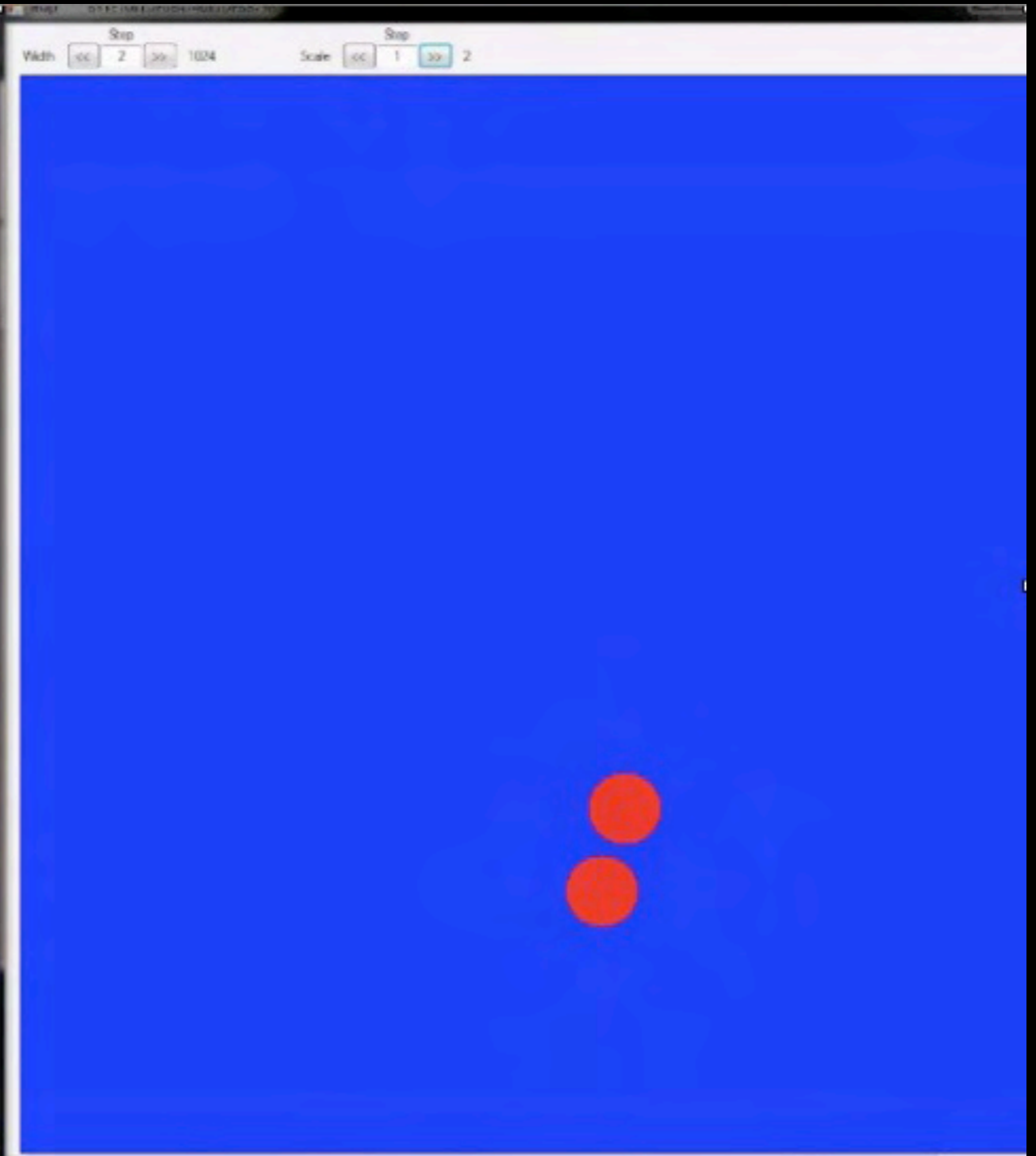
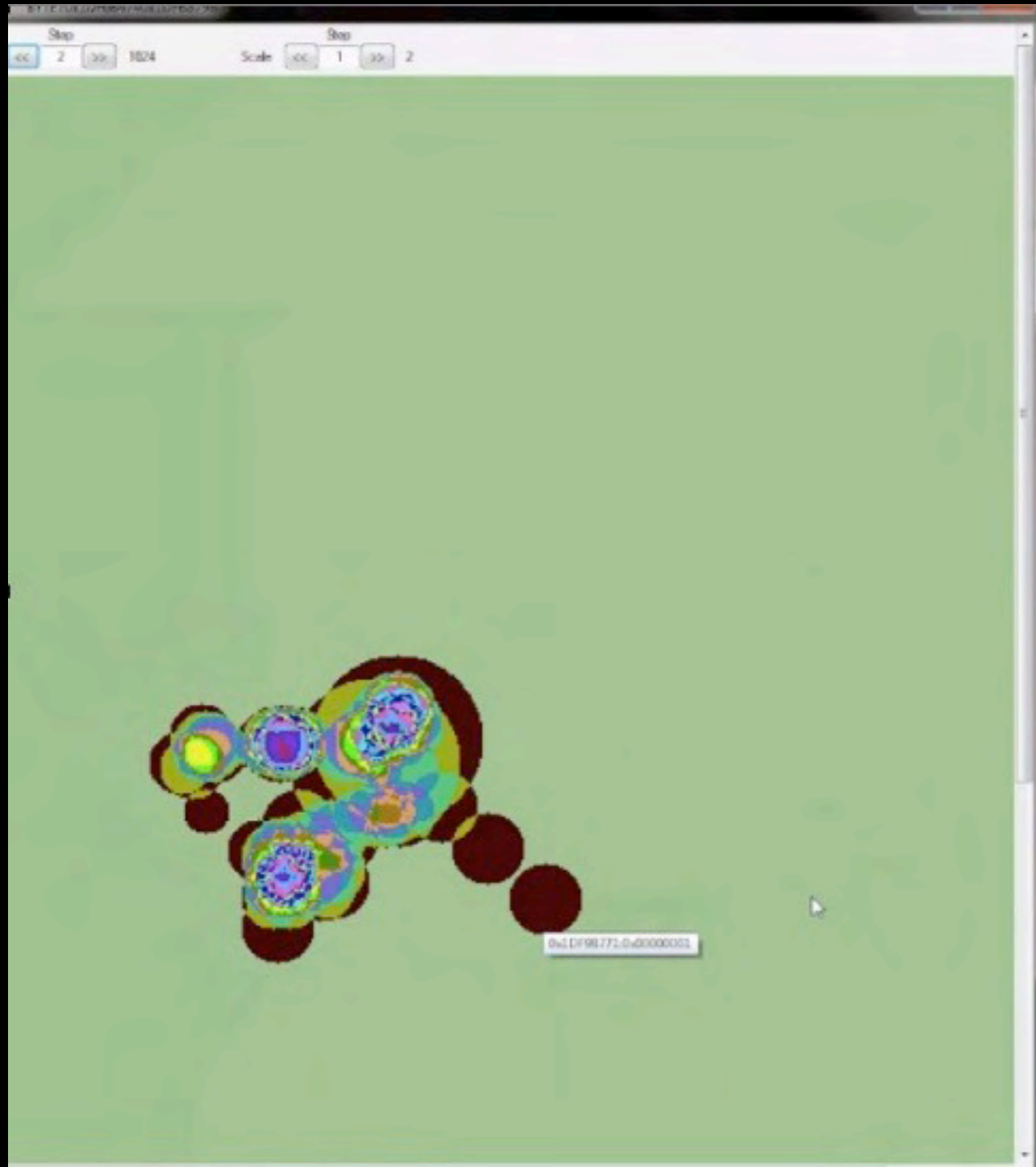
In game



In memory

Step 6

Understanding the map's
structure



Step 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

