

Lets Make Hay!

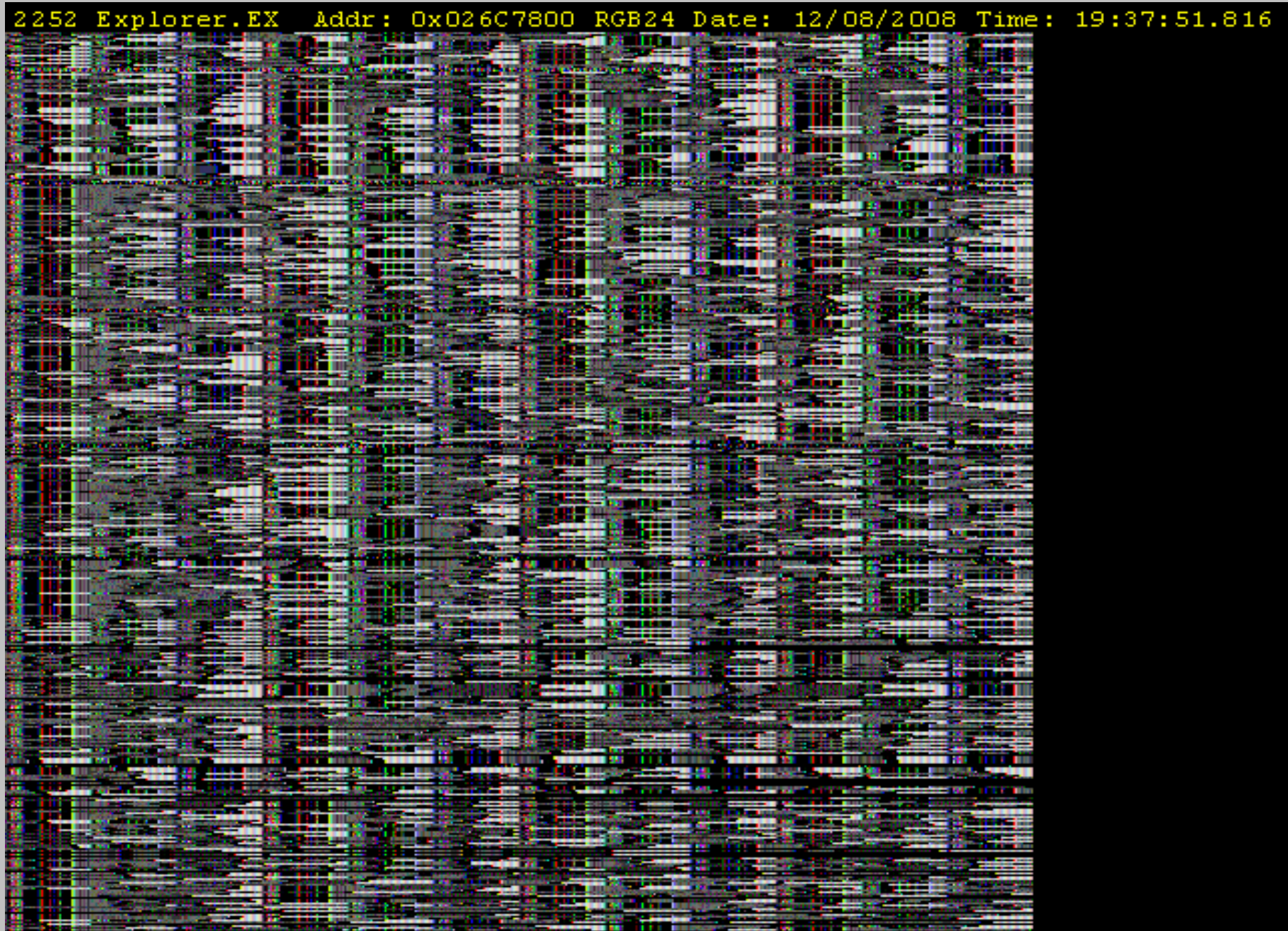
Using the Haystack plugin & the Barn
Burner host application to discover
the hidden world inside your
computer.

What? ... and Why?

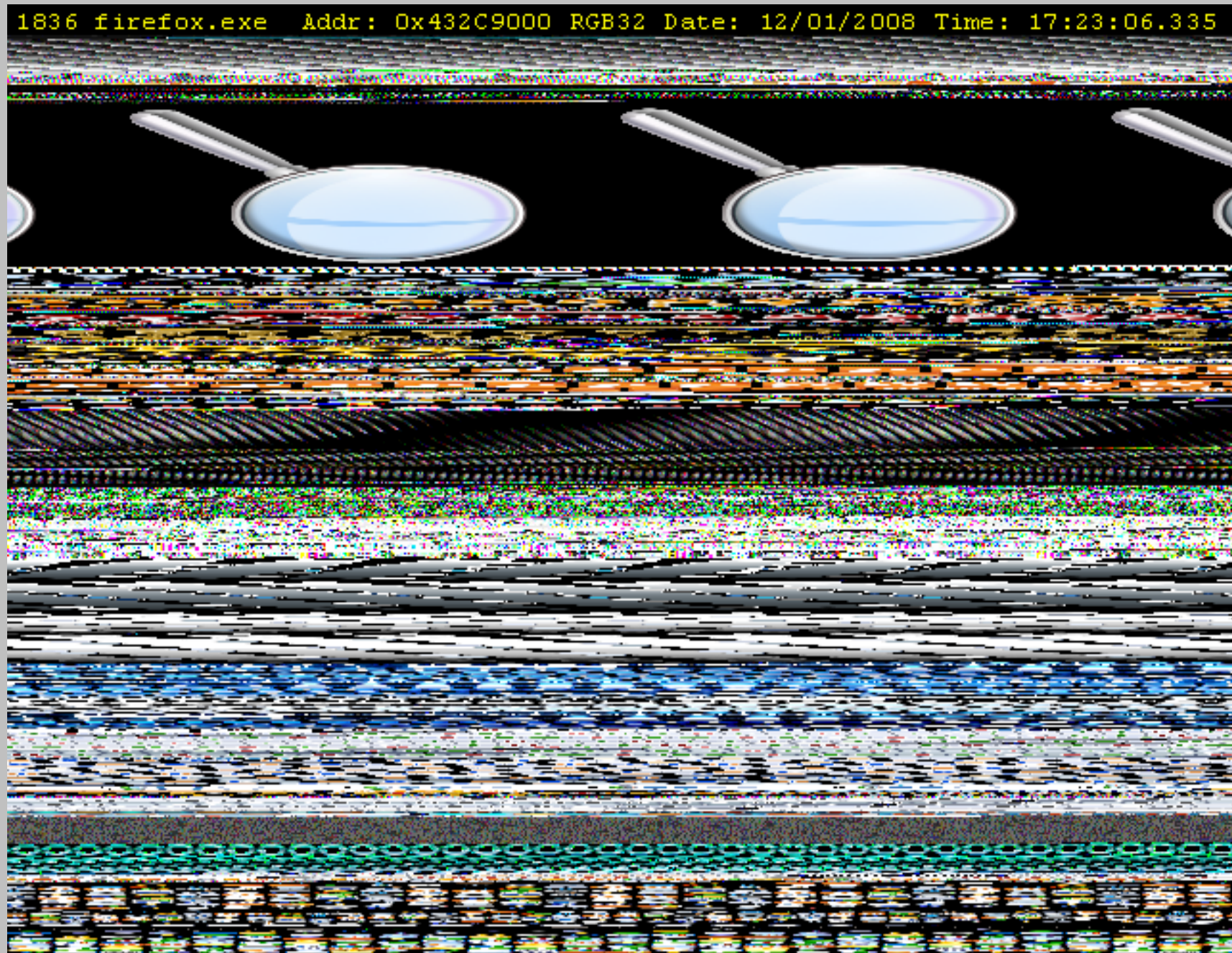
Jamie Fenton developed an unusual video special effects plug-in that dumps memory blocks to video output channels at video frame rates.

This lets you view the actual memory changes taking place inside your computer as they happen.

This can help you understand what your computer is doing and how it does it, and because the images often form intricate and unusual patterns, its fun to explore.

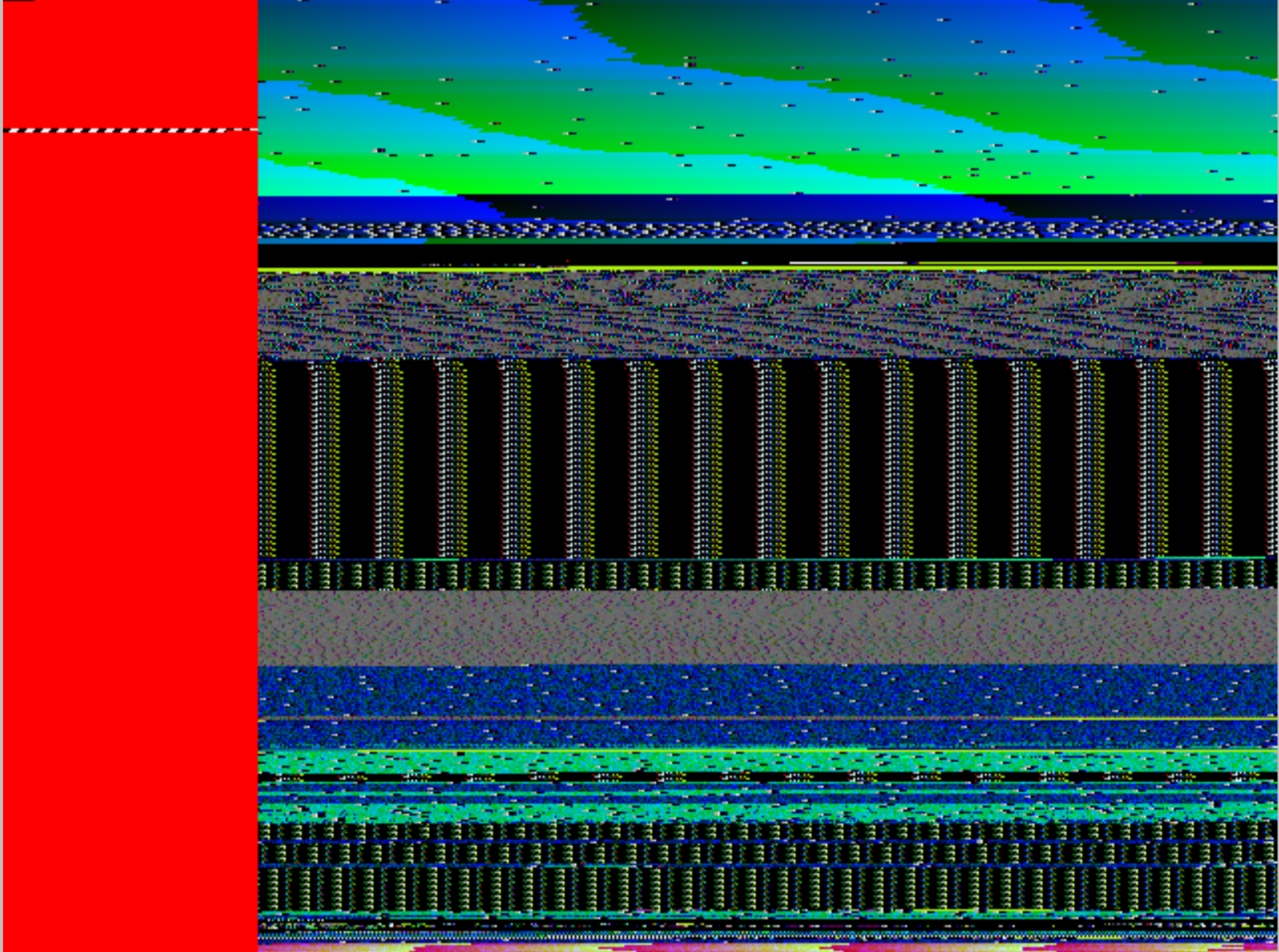


from Explorer.exe (XP desktop GUI)

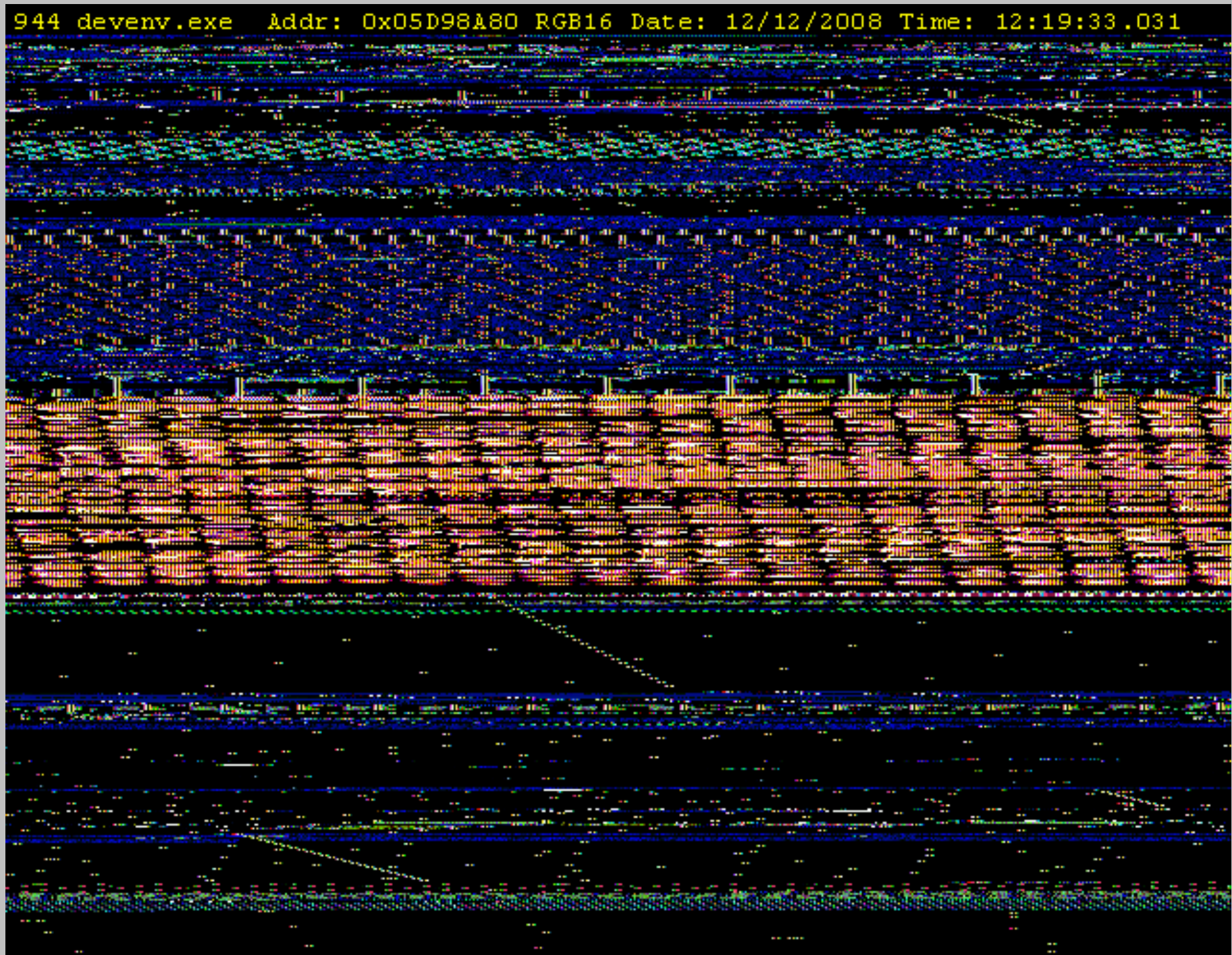


The FireFox Sushi Bar

1560 spoolsv.exe Addr: 0x02080000 RGB32 Date: 12/11/2008 Time: 04:05:57.703



The Print Spooler.



inside Visual Studio 2005



The Lost Legion of the Weasels

How do you "work it"?

Install the program:

Unpack the .ZIP file, and
extract the DLLs, etc,

Read the Read-Me.

Double-click the icon and
stand back!

Memory begins to mutate.

The program opens its frame
and begins refreshing the real
time view pane.

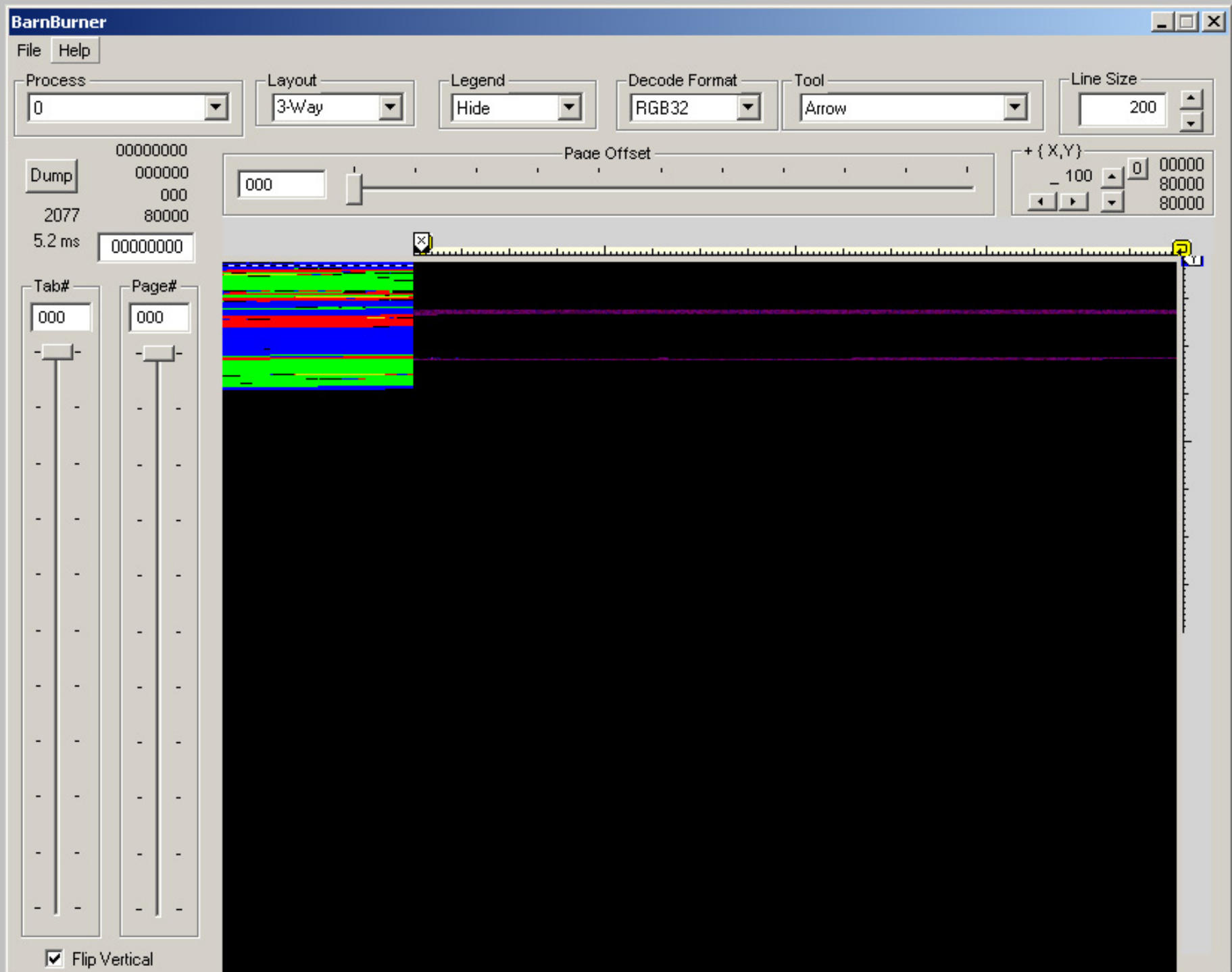
Take the controls and
search around within memory
and note where interesting
patterns appear.

Vary the resolution and size
until really cool stuff pops out.

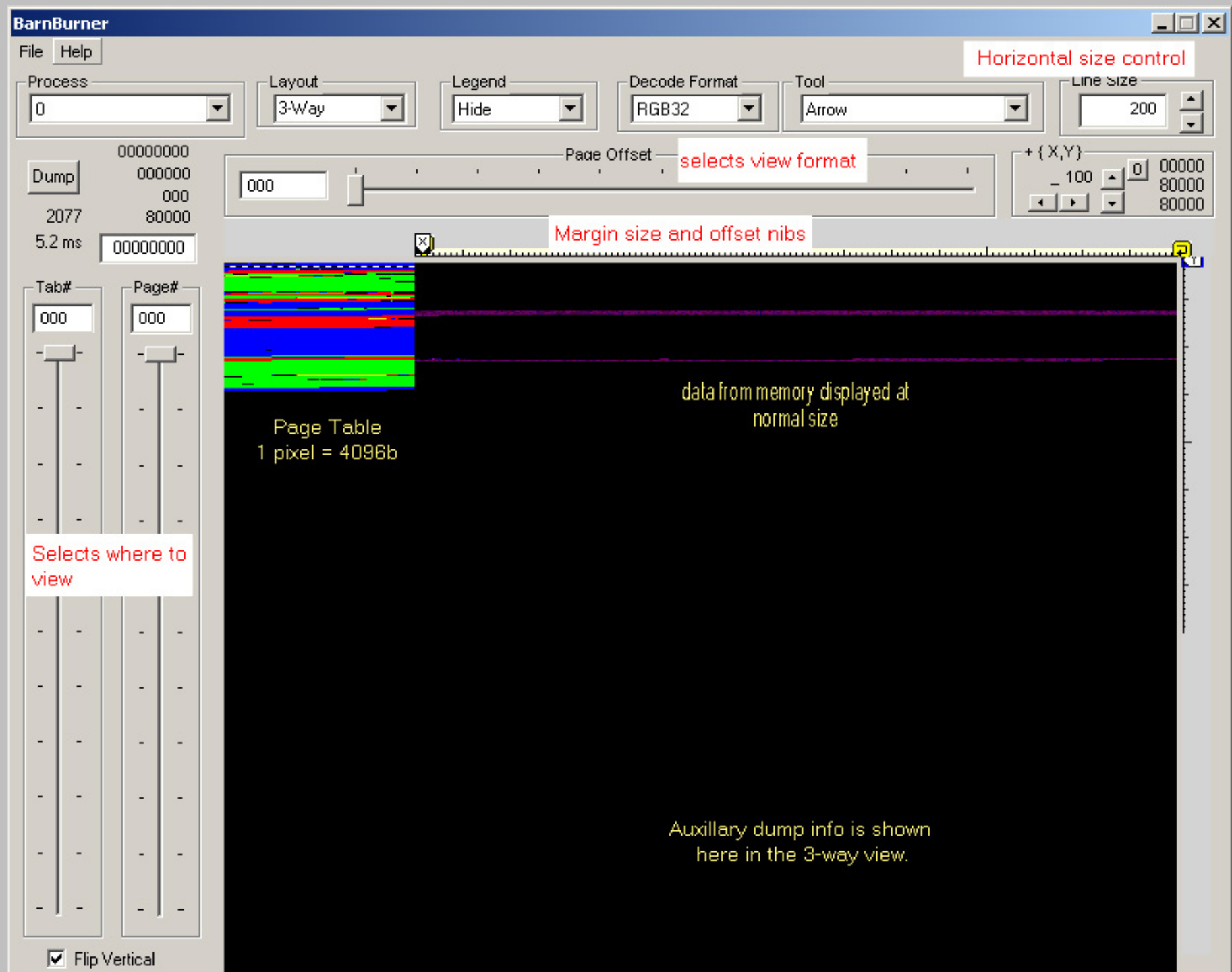
What do those controls do?

They let you position your video gatherer at a precise place in a 4 billion-byte address space.

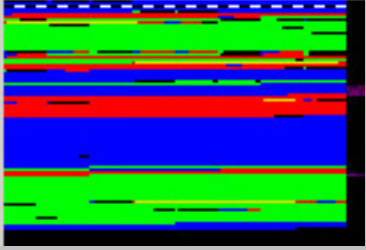
Another group controls the appearance of each element as it is rendered. This includes determining at which point an image skips down a line, the pseudo-color encoding (if any), the size of each symbol generated, and more.



The Barn-burner interface, looking at itself.



...and some of the points of interest...



What is a "Page Table?"

Its that red, green, blue, yellow, white box in the upper left hand corner!

Why is it there in the upper left hand corner?

Its there so you can see the "Big Picture" of what is going on.

Each pixel in the box is a page of computer memory 4096 bytes in size.

Typical personal computers can have several billion bytes of memory, and they all won't fit on one screen. Even when shrunk by a factor of 1024. Each line of the page map represents 128 x 4096 or about half a million bytes.

How do I know where I am and get to where I am going?

Intel & Microsoft figured out a way to keep track of pages in memory.

The system has a thousand tables for one thousand pages each. While its possible to address a million pages with this, the practical limit is around 500,000.

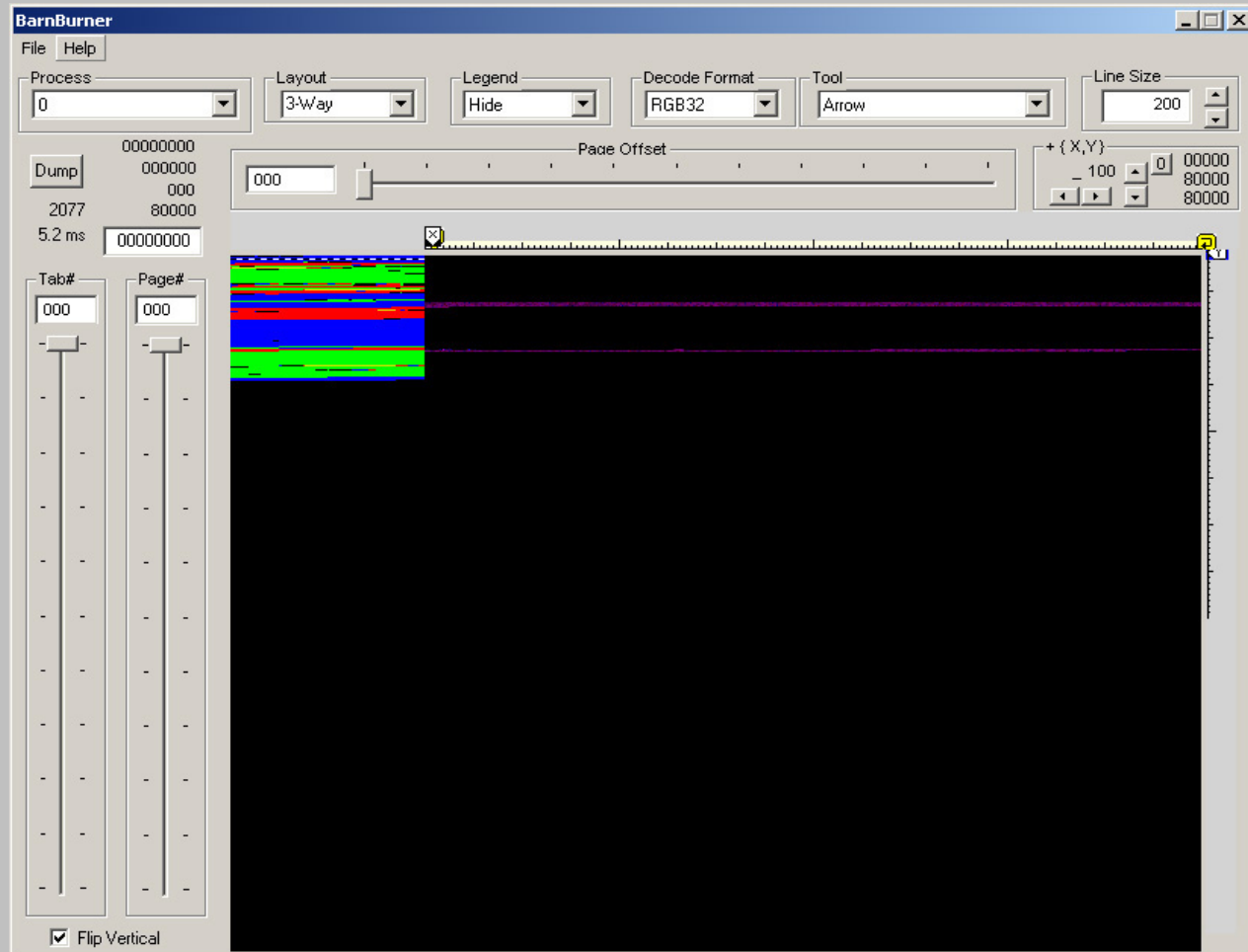
We give you two big sliders to pick which page table you want, and which page in that page table you want.

A third slider, the horizontal one above the screen area, specifies location inside the page.

(You can click and drag inside the window to scroll the view up and down and sometimes left and right.)

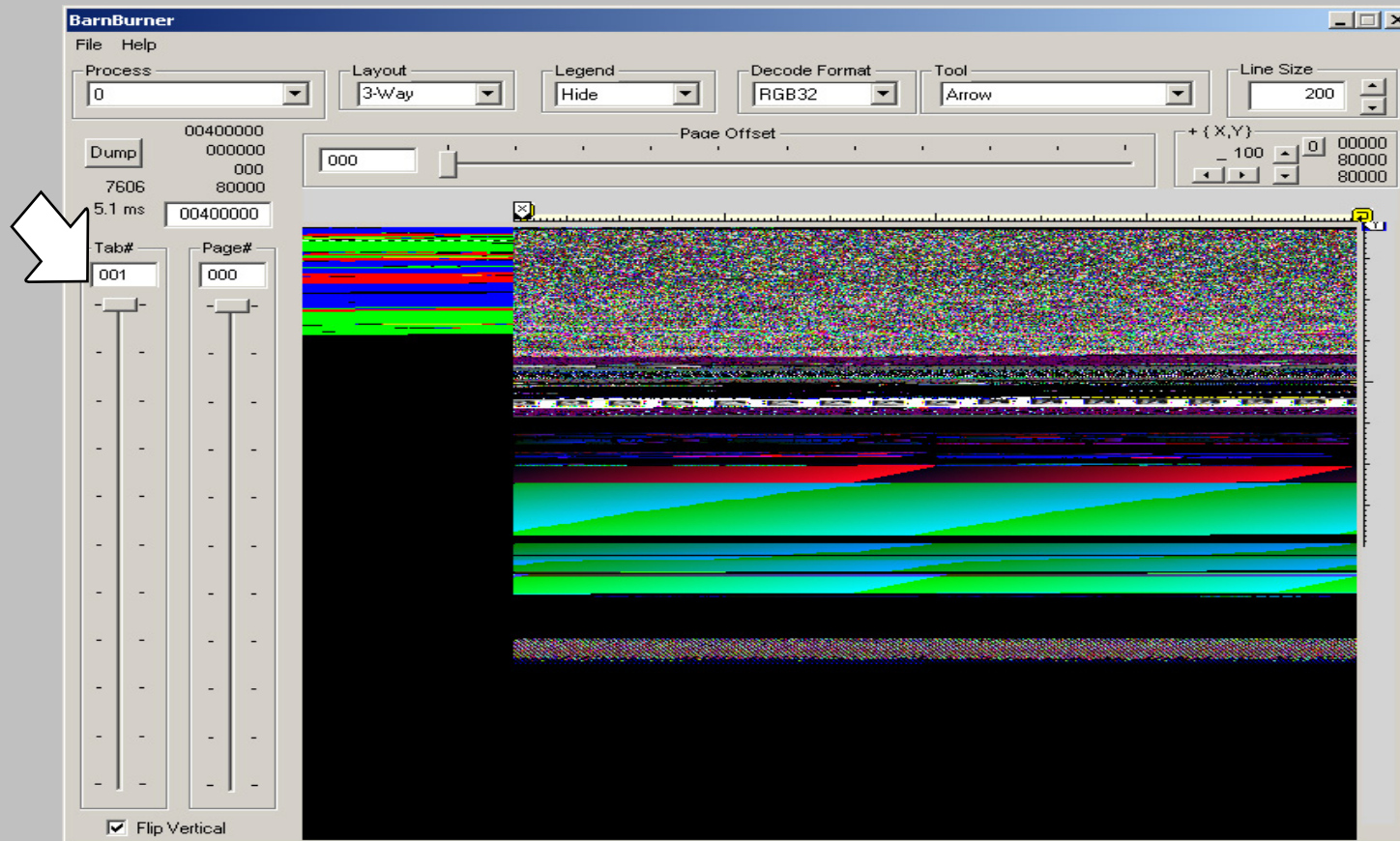
The image shows two vertical sliders side-by-side. The left slider is labeled 'Tab#' at the top and has a small input box at the top containing the number '000'. Below the input box is a vertical track with a slider knob at the top. The right slider is labeled 'Page#' at the top and also has a small input box at the top containing the number '000'. Below the input box is a vertical track with a slider knob at the top. Both sliders have a series of small tick marks along the track, with the top tick mark corresponding to the value in the input box.

Here is an example



you can follow along by starting up BarnBurner, which always starts up looking at itself

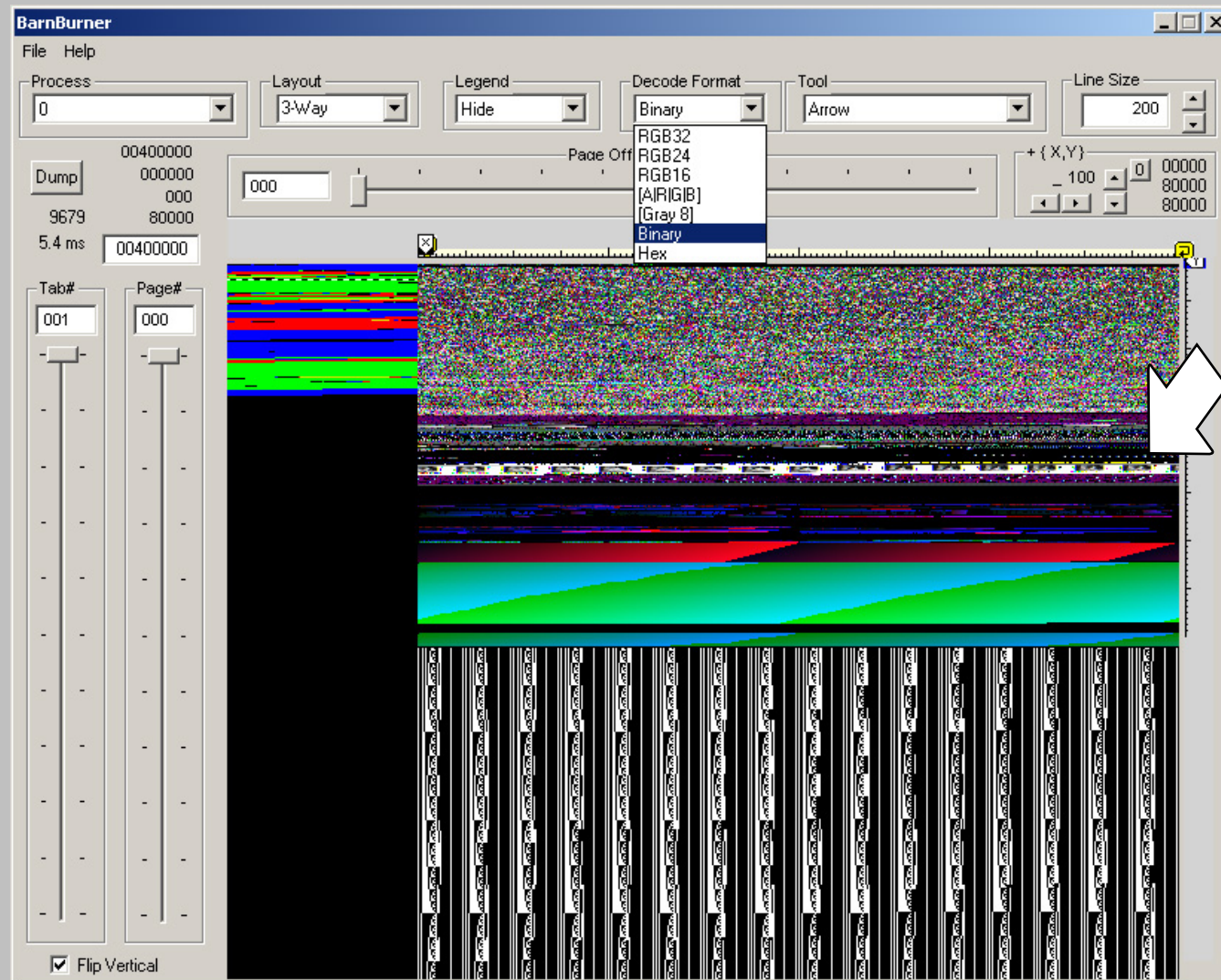
Page table 0 is rather dull, so we will go to page table 1 right away by moving the leftmost slider down a tiny amount. (You can also select the field above it and enter a 1).



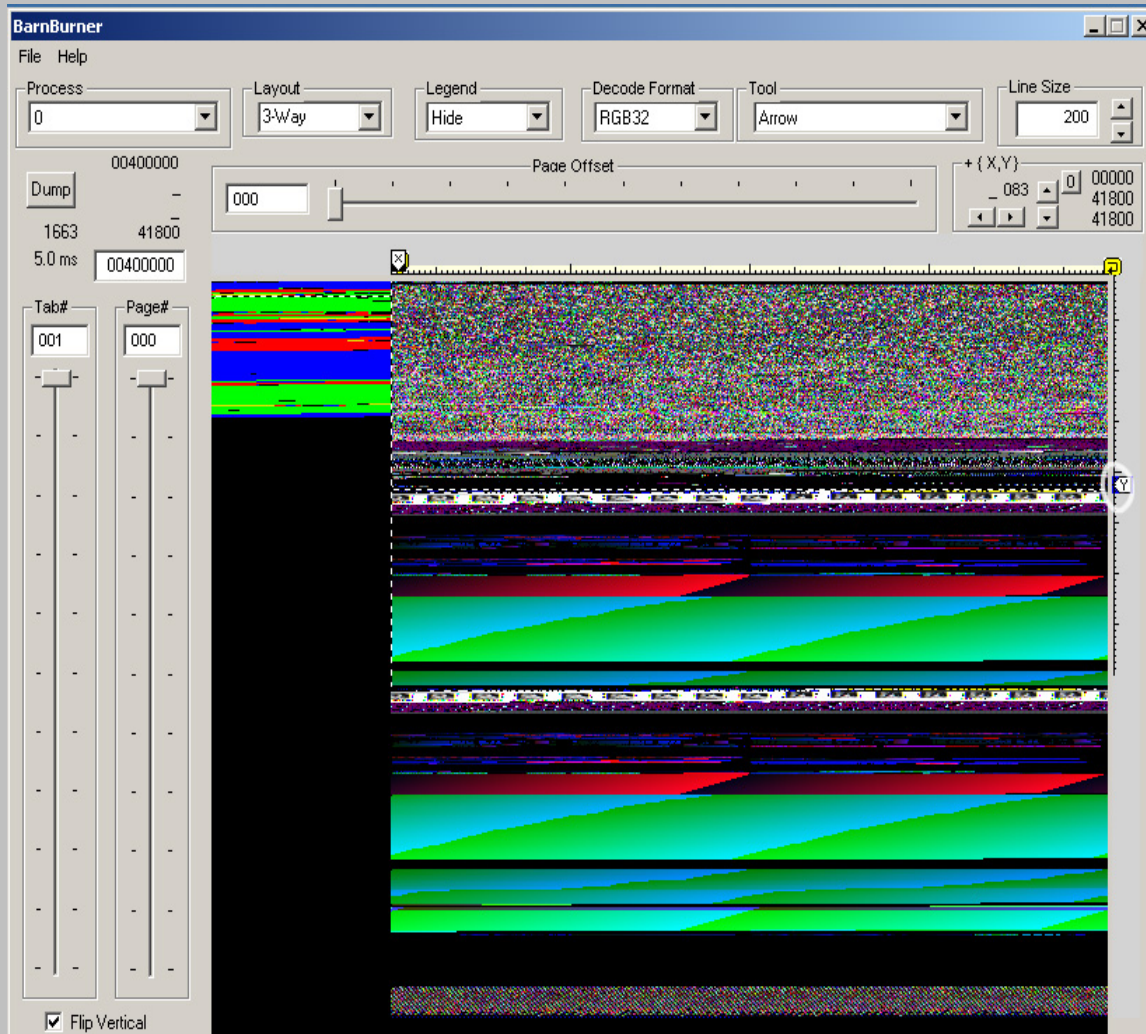
Try out the controls to see what they do. If you get lost, just restart the program again to get found.

The program reads memory but does not write outside of itself, so it is not particularly dangerous (for a Windows program).

For example, you can change the display mode for the screen bottom to binary, which in this case is counting up.



I am curious about the white stripe one third of the way down. So lets investigate.

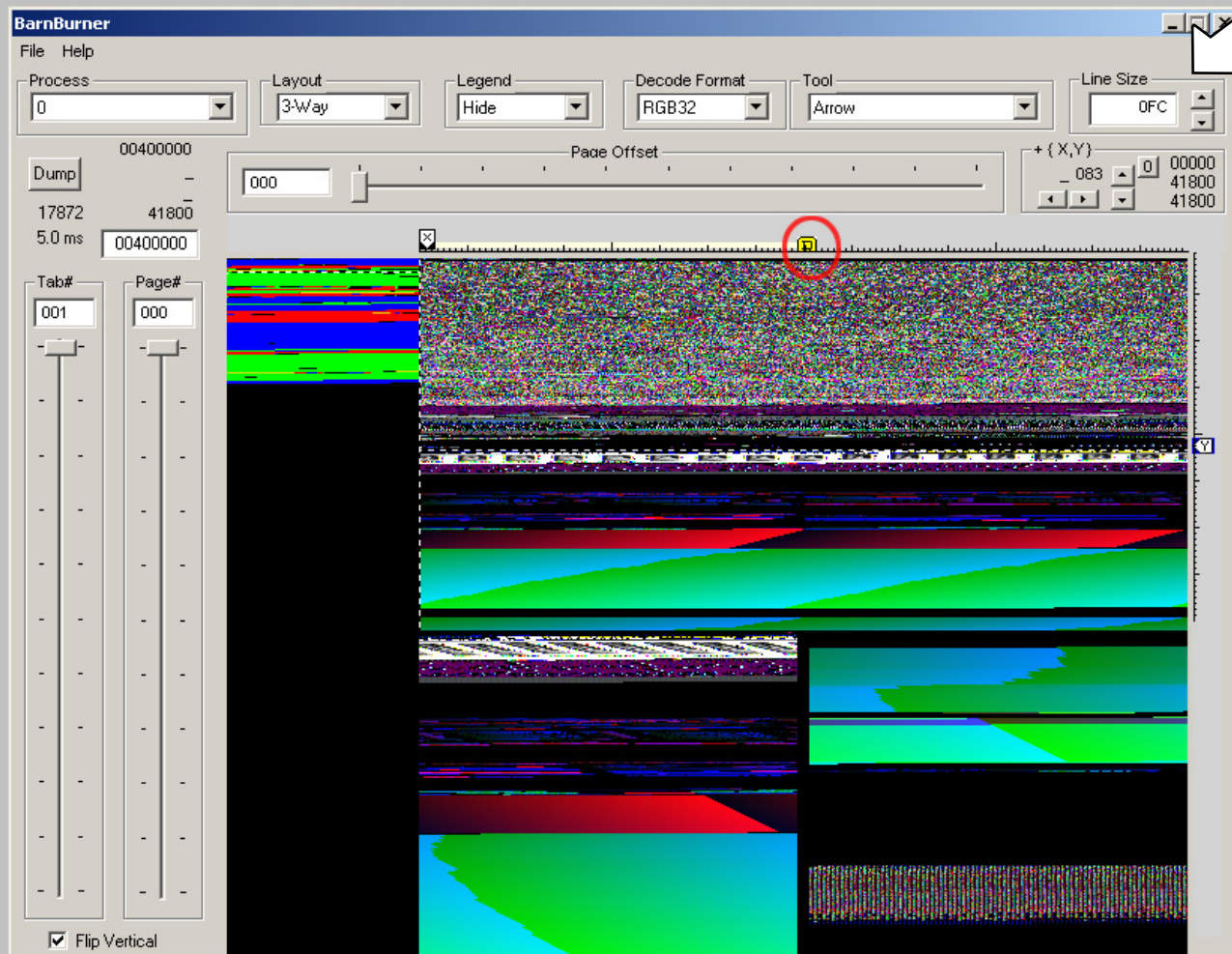


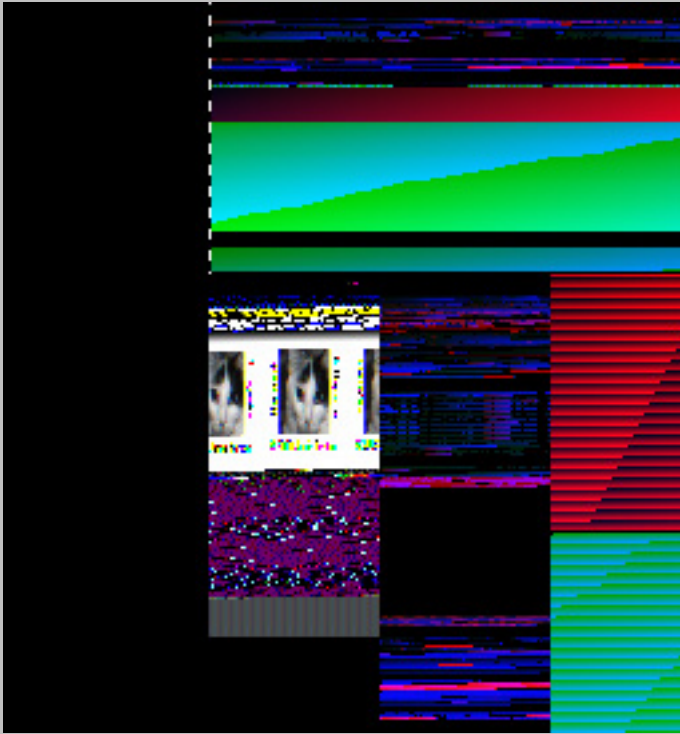
Move the "Y" tab in the right column downward until the "marching ants" are just above the white stripe. Notice that it brings a copy of the image up from the bottom, to just below the split.

The real magic begins on the next slide....

... we grab the yellow "line width" tab and move it to the left. Notice how the display rewraps and eventually, we see two columns. But keep going...

(You can change the line width using this control group, too.)






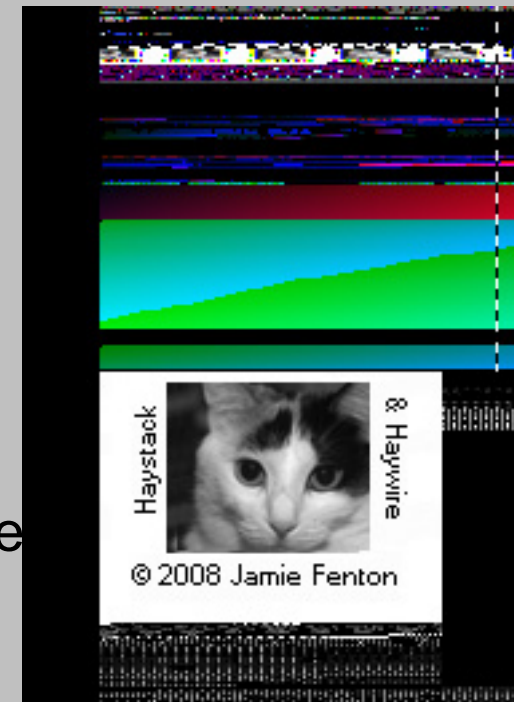
Eventually, the image will snap into sync and start making sense.

To see the image in full glory. change the decode format to [gray 8].

Adjust X & Y sliders as needed to center things up nice,

Congratulations!, you have successfully hunted down a bitmap in memory - the image of a huntress to be exact.

Meet  Calico Katie. She is the most curious cat I have ever known. She is a sweetheart too, I put this entire tutorial together with her in my lap, she has me well trained).



There are many more features to explore

More display formats, other processes running on the system, even operating system kernel memory.

Pressing the "Dump" button takes a screen snapshot.

Changing the mouse tool to "Scan" lets you fling the memory window like a hockey puck, and it speeds up the search through empty areas.

Labels, a magnifying glass, image flipping, & a lot more.

I already have a long list of improvements, and am interested in your suggestions.

Haystack is a standard format video plugin that can be made to run in over 50 video effects programs with full parameter control. It can steal animating bitmaps from the insides of hundreds of thousands more.