This is the first public release (v1) of HeapDraw and HeapTracer

HeapDraw was originally created as a postmortem analysis tool, to see how the heap evolved during the life of a process. The idea is that although we may be used to textual output, like that of ltrace or a malloc/free hooking library, it's much better to see it graphically (in fact I used to make drawings by hand until I realized "WTF am I doing? I have a computer to do it for me!").

HeapTracer is the new name, after it became a runtime analysis tool.

In this first release you can find 4 different versions.

```
$ ls -F
```

Examples and Doc/
Here you'll find Example input files and Doc (for Documentation, not Doctor)

IDA-windows/
This is the source and precompiled version (IDA 5.0/5.1 for windows) of a plugin for IDA. It will hook RtlAllocateHeap, RtlFreeHeap and others, it will open an OpenGL window, and it will draw, on real time, the evolution of the heap (for a specific heap).
Read the readme in this directory for more information.

Linux-native/
This is, erm... the linux native port (actually the original version) of HeapDraw. It does not have a fancy interface, and has rather a set of weird hotkeys (read keystroke() in draw.cpp to know the complete list). This version can read the output of ltrace (for linux) and truss (for Solaris and some others).

python/
This is an unfinished python version... The main problem is that it's too slow right now, even if using psyco as JIT. It may be possible to speed up by using numarray and OpenGL's VertexArrays, but I tried with no luck. Feel free to contribute!

Windows-standalone/
This is a standalone, postmortem version of HeapDraw for windows. Sources are almost the same as that for Linux (except a few include file). It may be very easily unified (it was once), but it's not.

README

USING

```
    . Zoom in selecting an area with the mouse
    . hjkl to move (left, down, up, right)
    . Backspace to go back to previous location and zoom
    . 1 to zoom all
    . press 'x' to turn on/off sub-pixel rendering
    . press 'e' to turn on/off events (breakpoints) rendering
    . press '.' to know the address where the mouse is (see IDAs log window for IDA
plugin)
    . press 'h','j','k','l' to move the window around
    . press 'f' to flip the color scale (alloc time vs. free time)
    . press 'g' to turn on/off auto growing (on runtime, grow to the right on new
blocks)
    . press 'q' to exit
```

CREDITS

HeapDraw was originally created by gera, and it was latter improved with suggestions and ideas from a lot of people from Core Security Technologies. Mainly, credits should go to the first users, Arka and Kato, who contributed with ideas, bug reports and the script for ntsd (kato). Hernan, who contributed with an OllyDbg plugin version which sadly died :-(Lately to alfred and t0p0, who tried it on Windows/IDA and Linux, and helped with some code also. And then, to every other who tried it and contributed with bug reports and ideas.