OpenRCE.org

Unpacking bird's eye view

Ero Carrera
Sabre Security GmbH

The idea

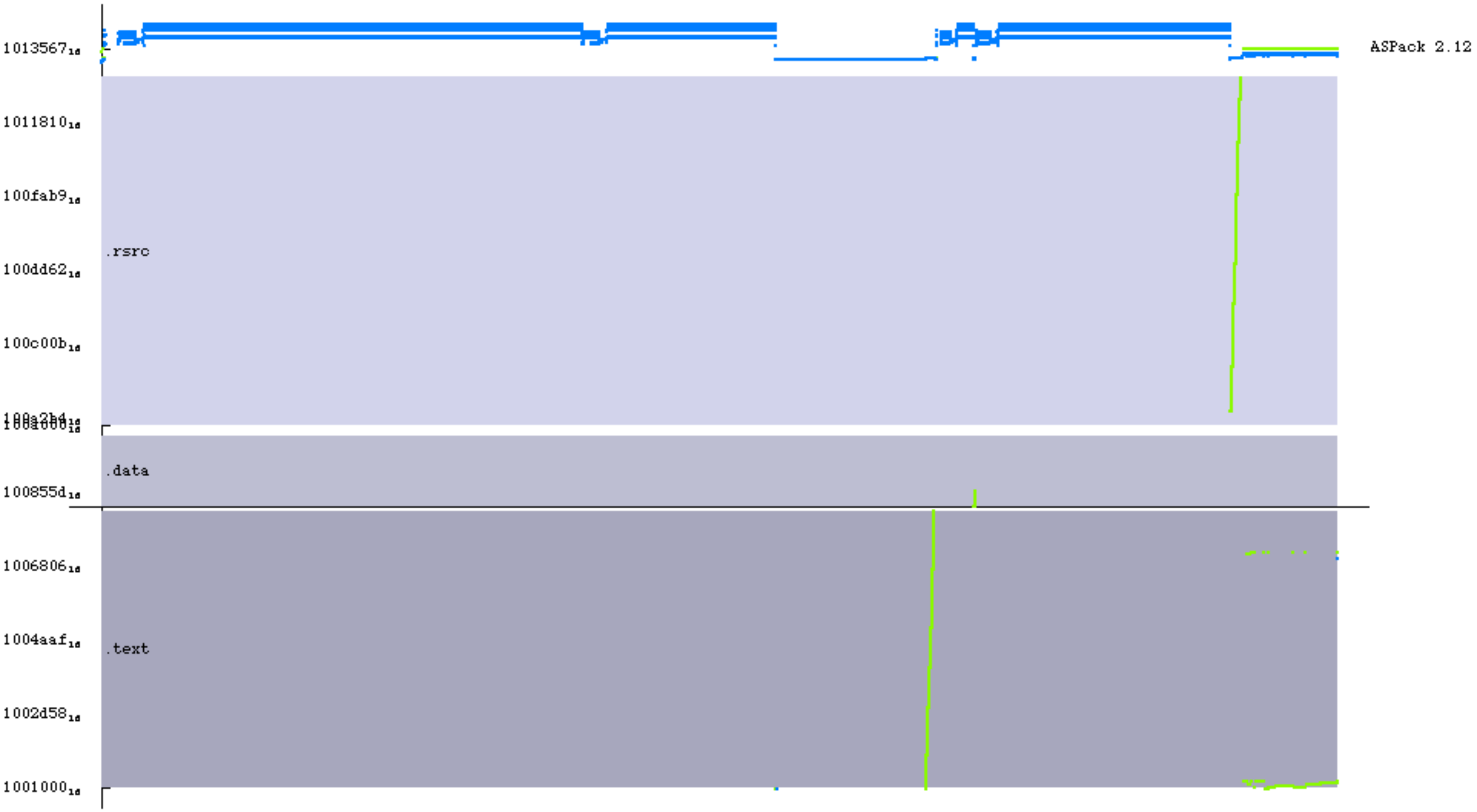
- Thought it would be cool to be able to see how unpacking goes
- as easy as tracing all memory writes and EIP location as the unpacker goes on its way
- i’m a slacker and lame, don’t wanna worry about anti-dbg tricks and the like... then... have write my own tool
- cool thing is, I already had it :)

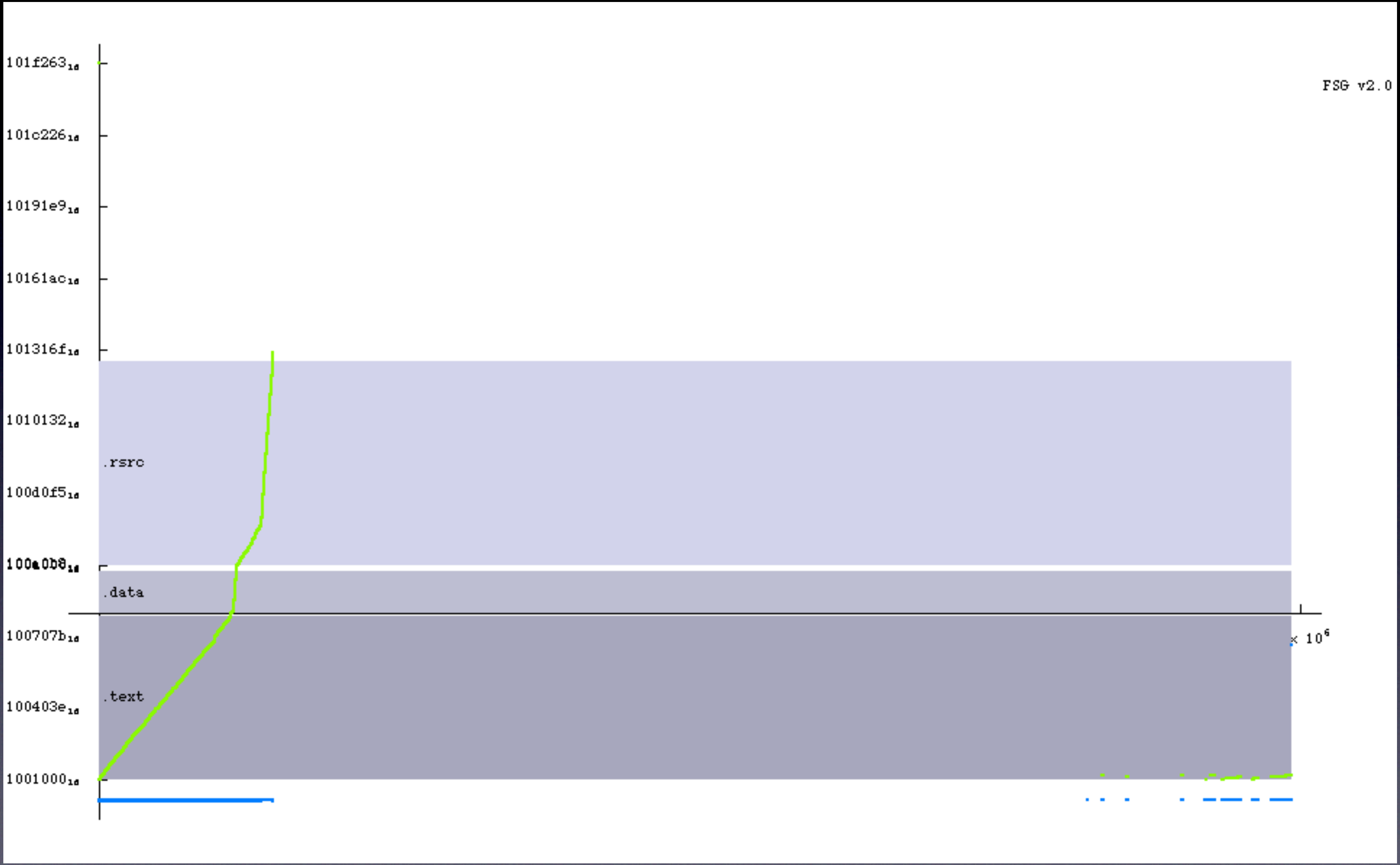
Gather data

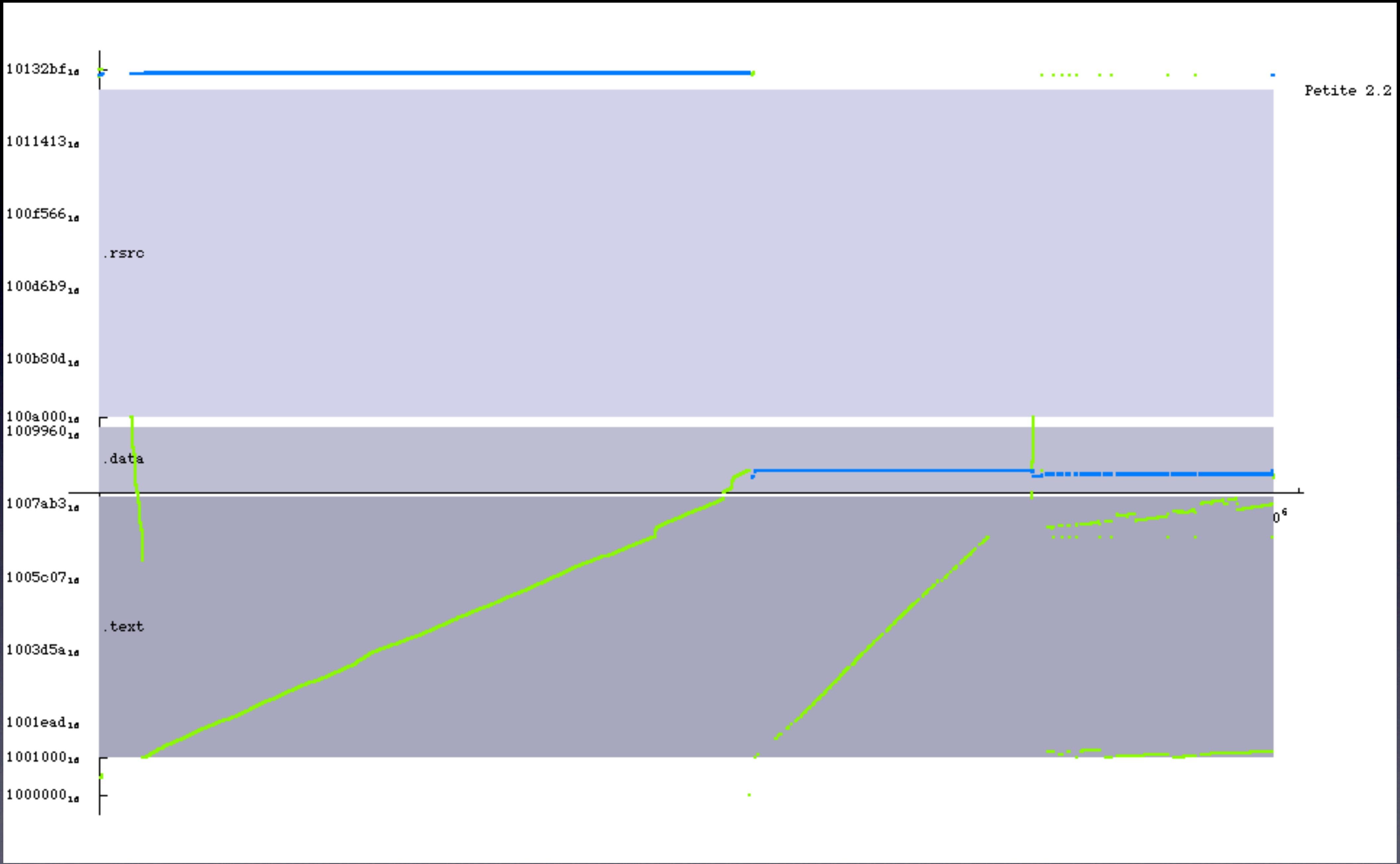
- Run some packers through my black ‘bochs’

Plot data

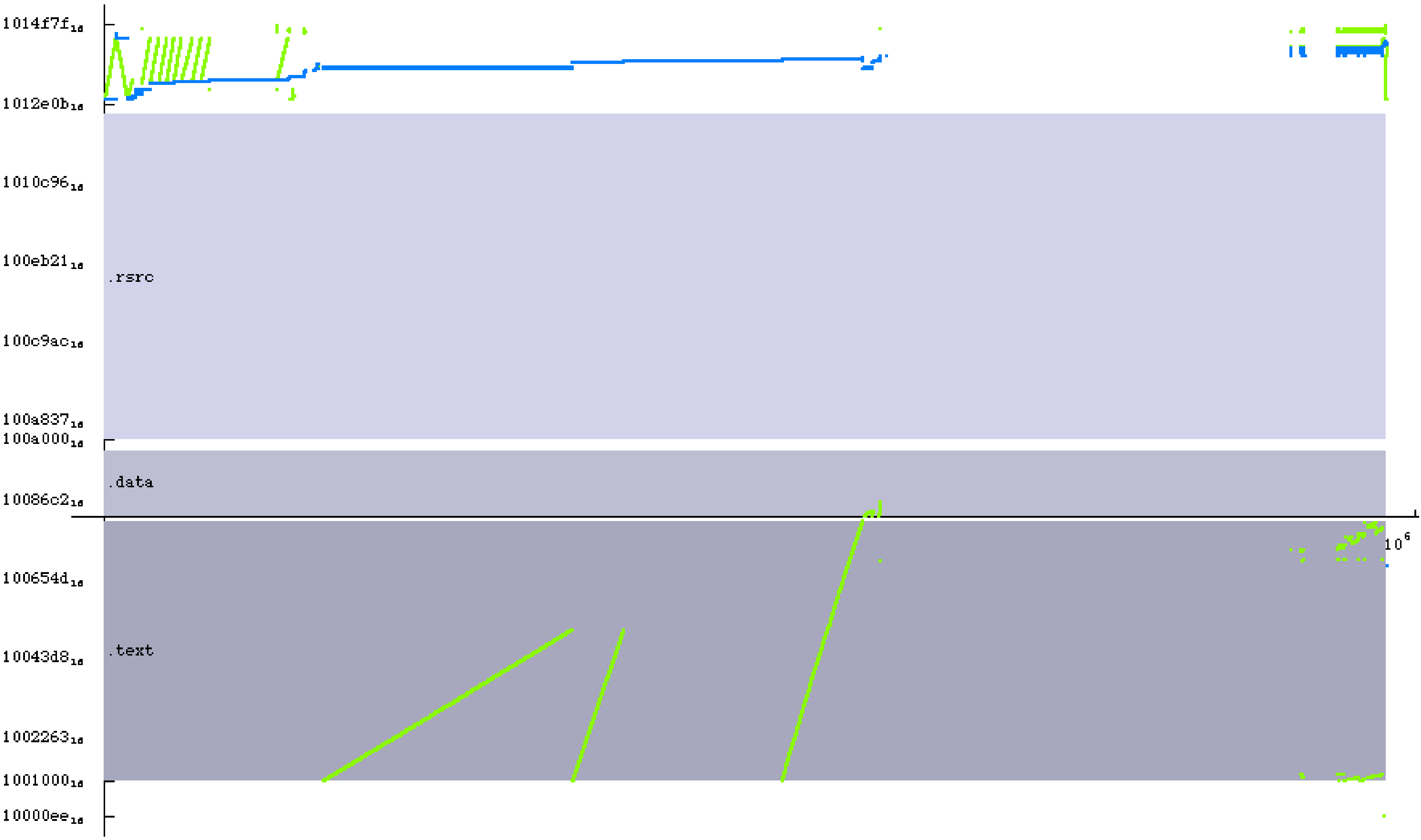
- I plotted most of the packer’s data with Mathematica
- EIP = blue
- Memory writes = green


1013567_{16}
1011810_{16}
$100fab9_{16}$
$100dd62_{16}$
$100c00b_{16}$
$100a2b4_{16}$
$100a000_{16}$
$100855d_{16}$
1006806_{16}
$1004aaf_{16}$
$1002d58_{16}$
1001000_{16}
.rsrc
.data
.text
ASPack 2.12

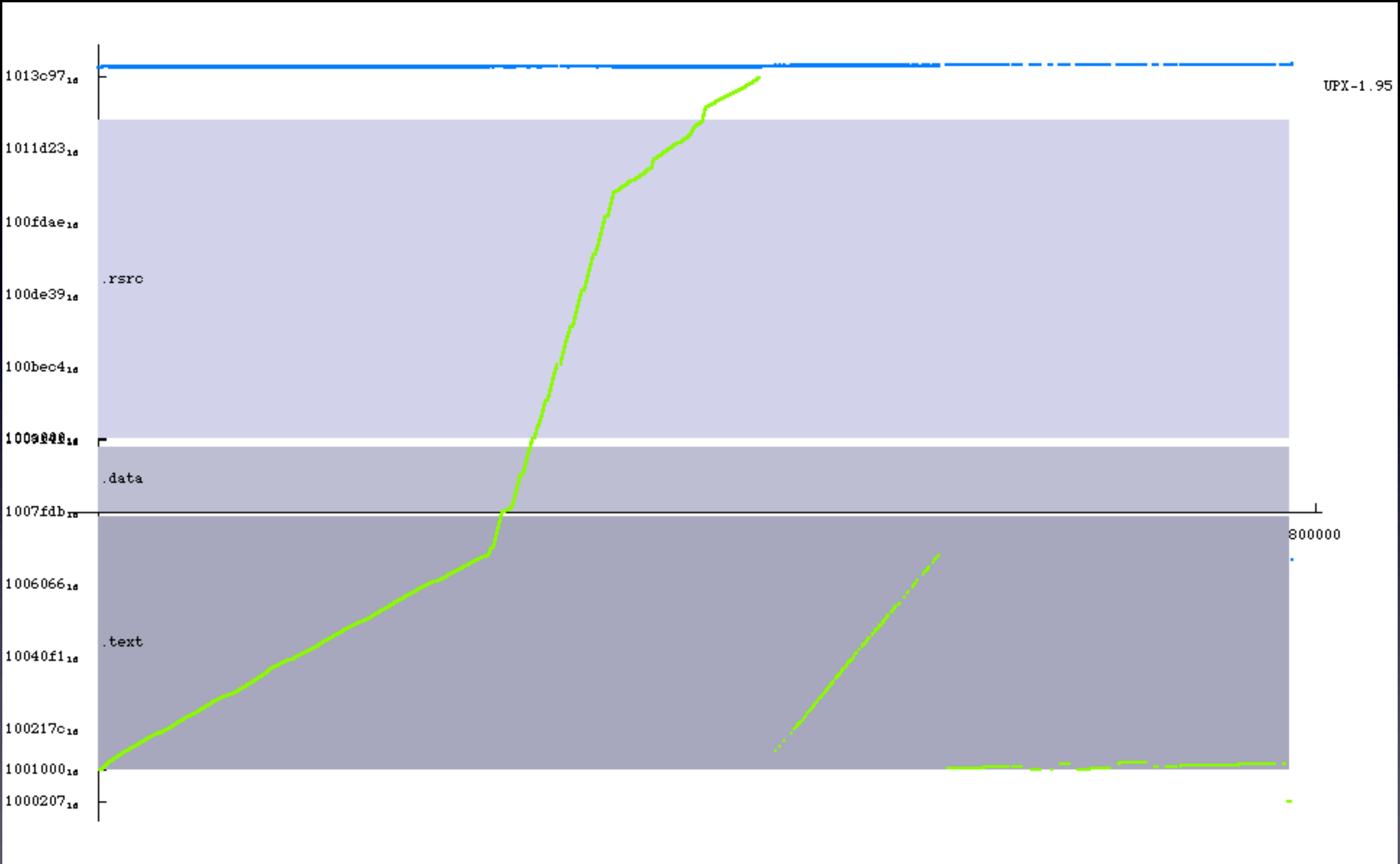

$101f263_{16}$
$101c226_{16}$
$10191e9_{16}$
$10161ac_{16}$
$101316f_{16}$
1010132_{16}
$100d0f5_{16}$
$100a0b8_{16}$
$100707b_{16}$
$100403e_{16}$
1001000_{16}
FSG v2.0
.rsrc
.data
.text
× 10^6

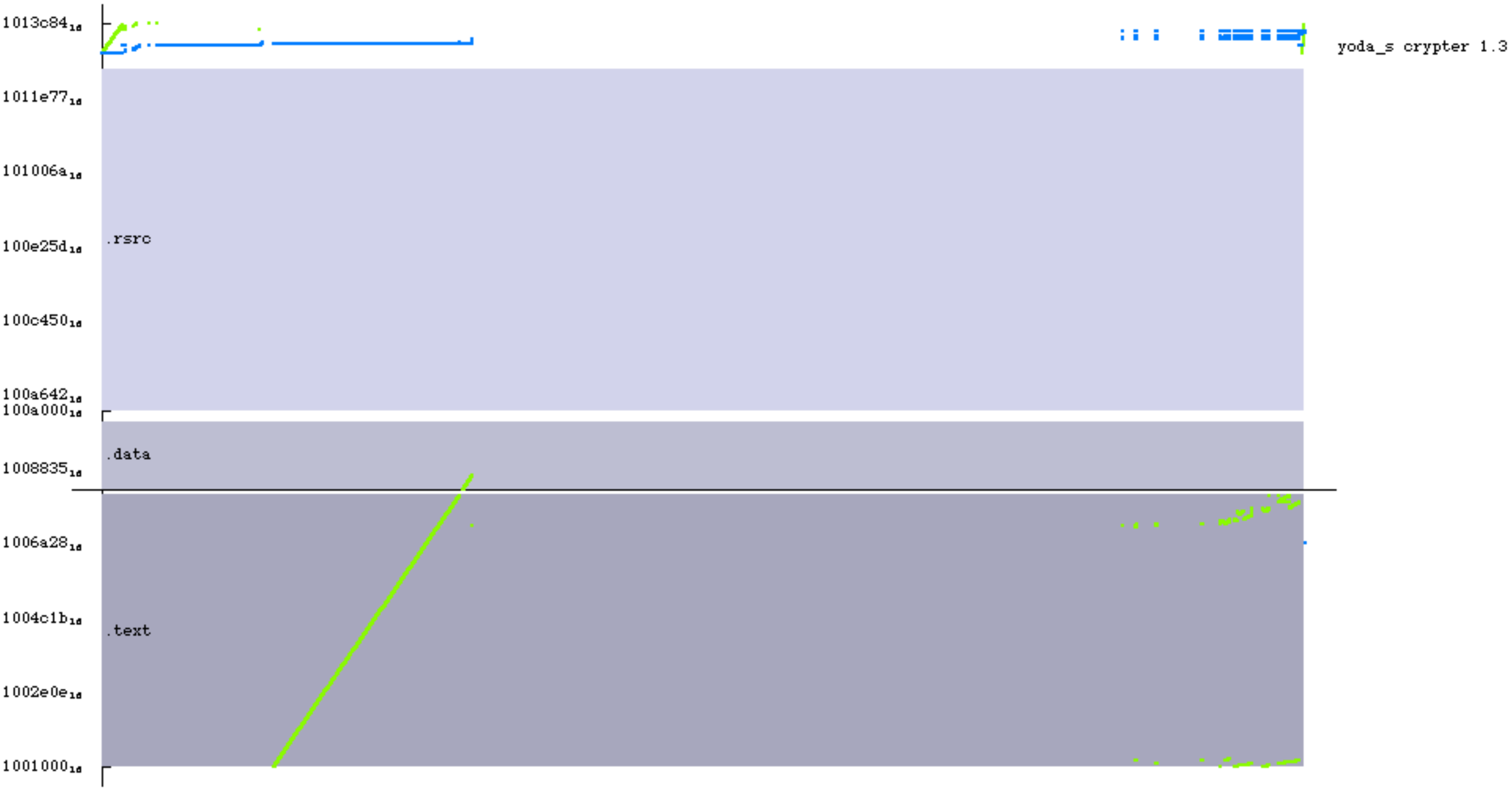


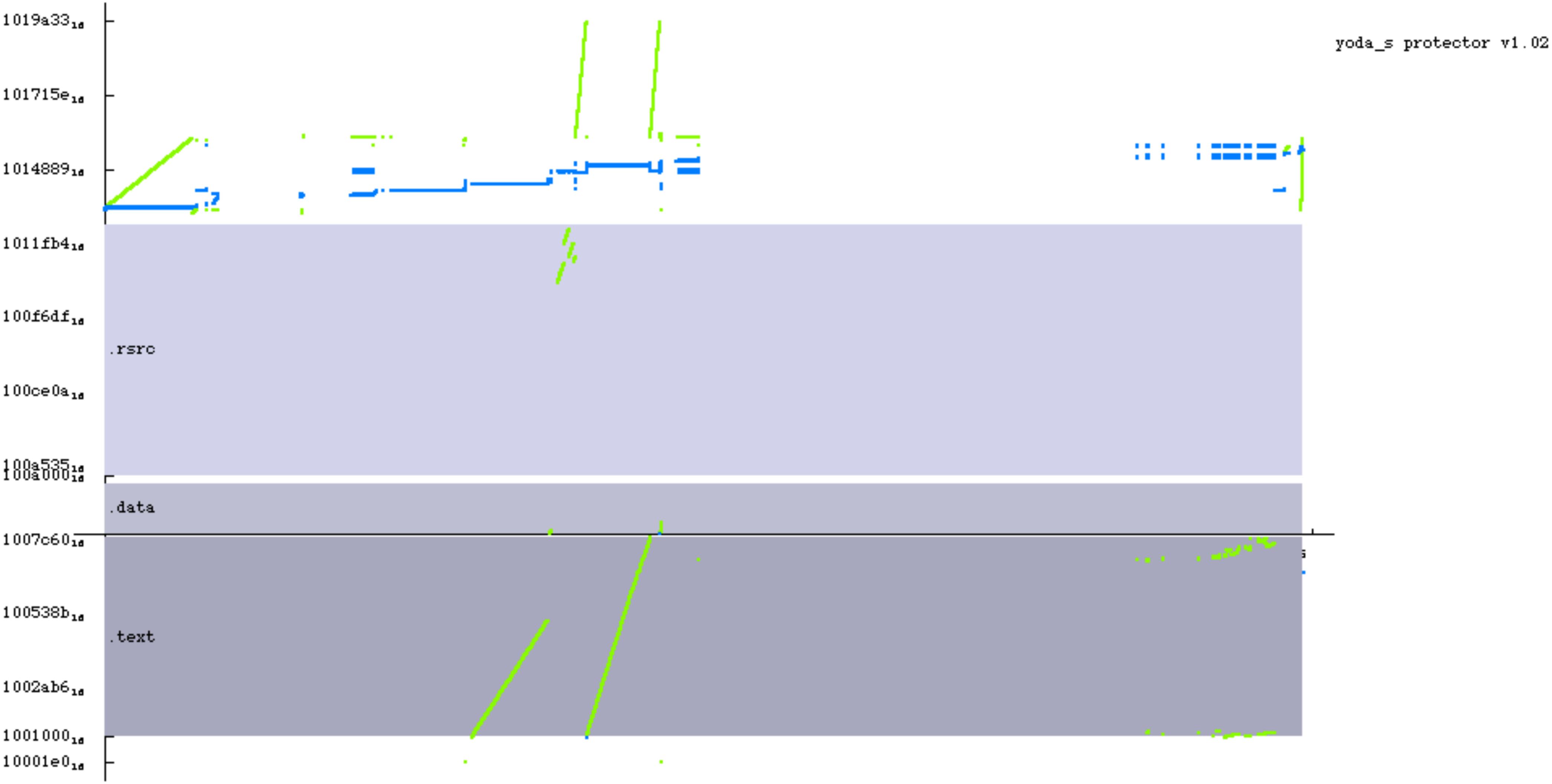
$10132bf_{16}$
1011413_{16}
$100f566_{16}$
$100d6b9_{16}$
$100b80d_{16}$
$100a000_{16}$
1009960_{16}
$1007ab3_{16}$
$1005c07_{16}$
$1003d5a_{16}$
$1001ead_{16}$
1001000_{16}
1000000_{16}
.rsrc
.data
.text
Petite 2.2
0^6


1014f7f$_{16}$
1012e0b$_{16}$
1010c96$_{16}$
100eb21$_{16}$
100c9ac$_{16}$
100a837$_{16}$
100a000$_{16}$
10086c2$_{16}$
100654d$_{16}$
10043d8$_{16}$
1002263$_{16}$
1001000$_{16}$
10000ee$_{16}$
.rsrc
.data
.text
10^6

tElock v0.98


1013c97$_{16}$
UPX-1.95
1011d23$_{16}$
100fdae$_{16}$
.rsrc
100de39$_{16}$
100bec4$_{16}$
.data
1007fdb$_{16}$
800000
1006066$_{16}$
.text
10040f1$_{16}$
100217c$_{16}$
1001000$_{16}$
1000207$_{16}$


1013c84₁₆
1011e77₁₆
101006a₁₆
100e25d₁₆
100c450₁₆
100a642₁₆
100a000₁₆
1008835₁₆
1006a28₁₆
1004c1b₁₆
1002e0e₁₆
1001000₁₆
.rsrc
.data
.text
yoda_s crypter 1.3


yoda_s protector v1.02
1019a33$_{16}$
101715e$_{16}$
1014889$_{16}$
1011fb4$_{16}$
100f6df$_{16}$
100ce0a$_{16}$
100a535$_{16}$
100a000$_{16}$
1007c60$_{16}$
100538b$_{16}$
1002ab6$_{16}$
1001000$_{16}$
10001e0$_{16}$
.rsrc
.data
.text

Questions?