Stack exchange challenge

Alexandre Bergel
Leonel Merino

Reverse Engineering stack exchange

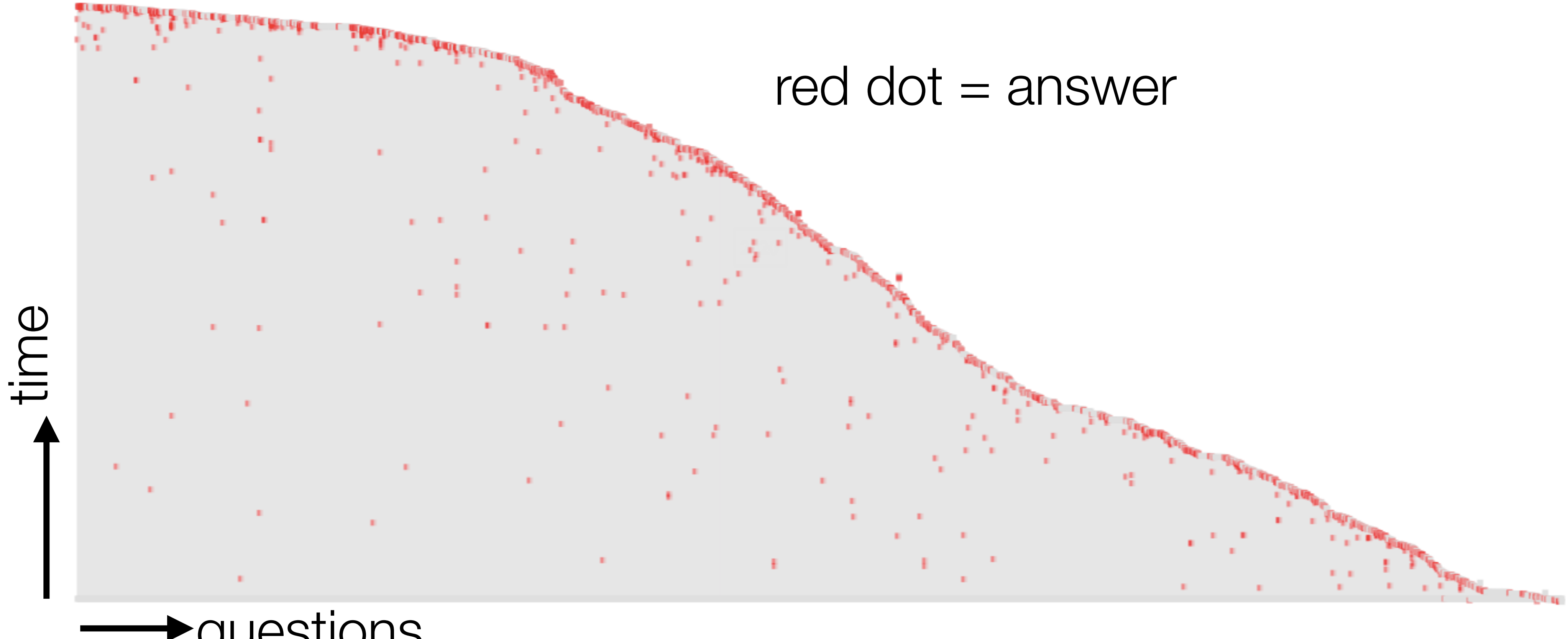
http://reverseengineering.stackexchange.com

2953 posts (1255 questions, 1698 answers)

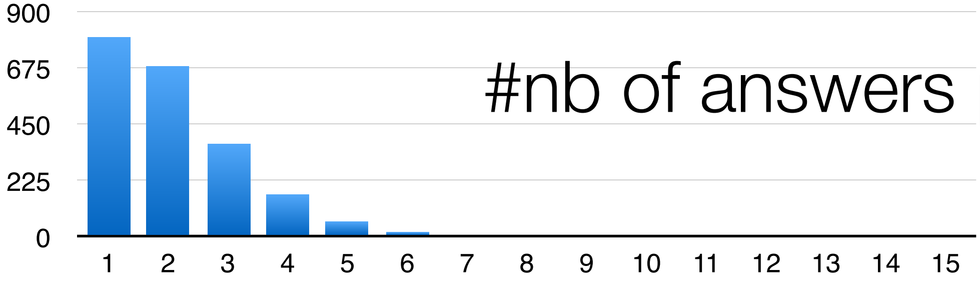
First post was posted in 2013-03-19

4536 users

Question age and #answers

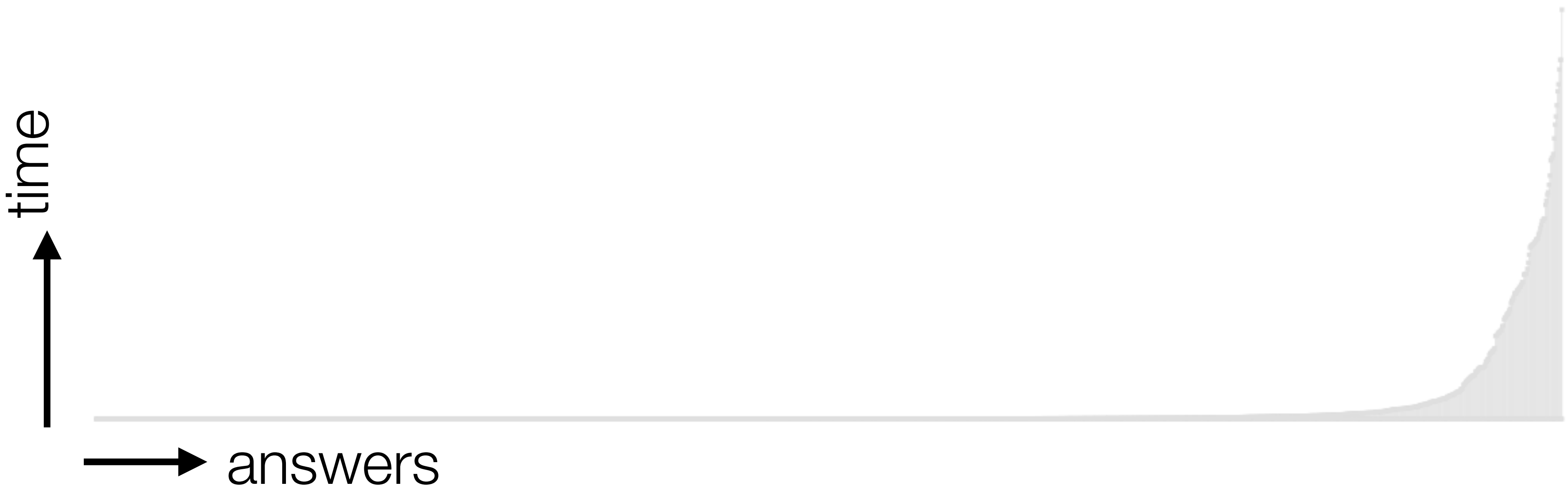


red dot = answer



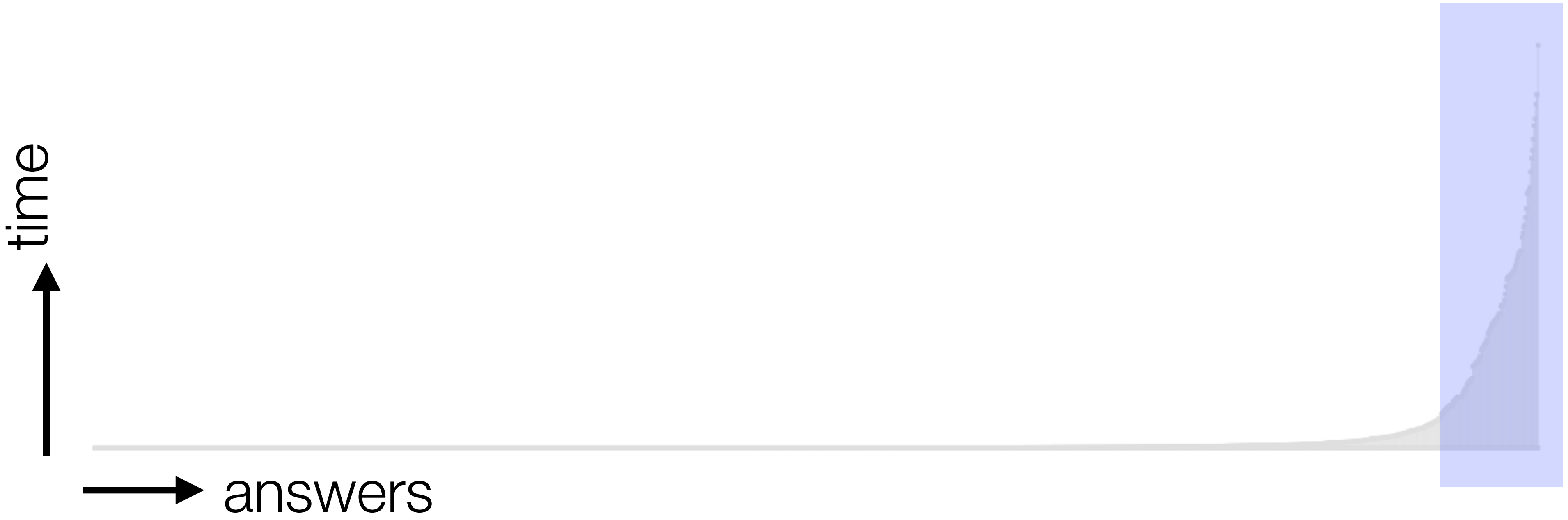
#nb of answers per question

Time to answer



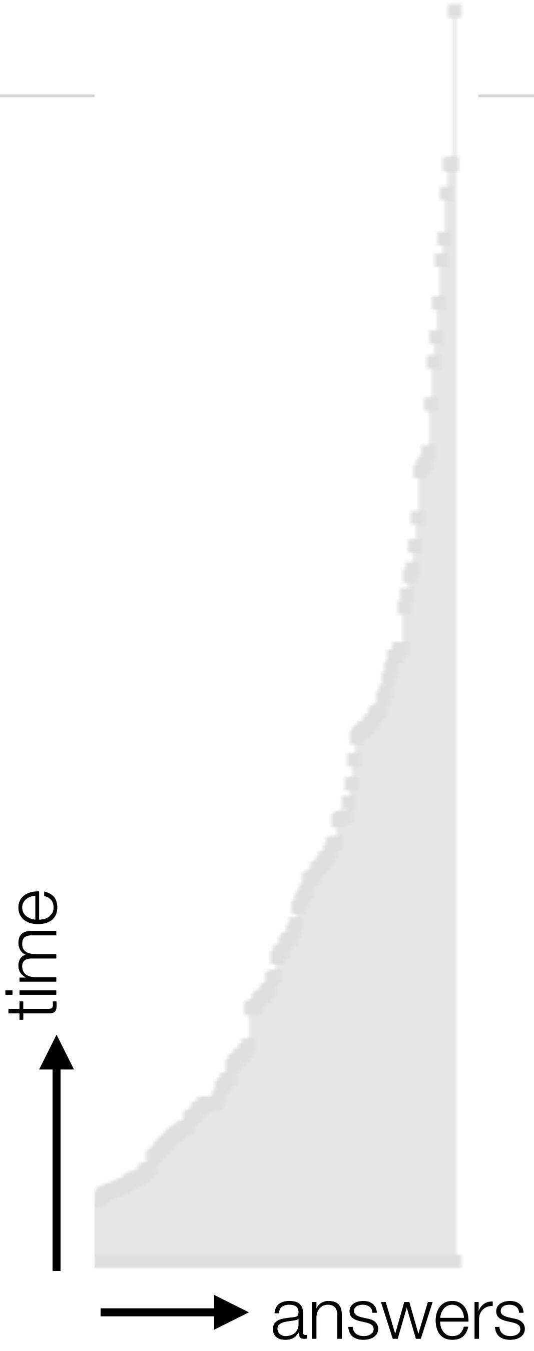
Most of the questions are answered shortly after they are posted

Time to answer

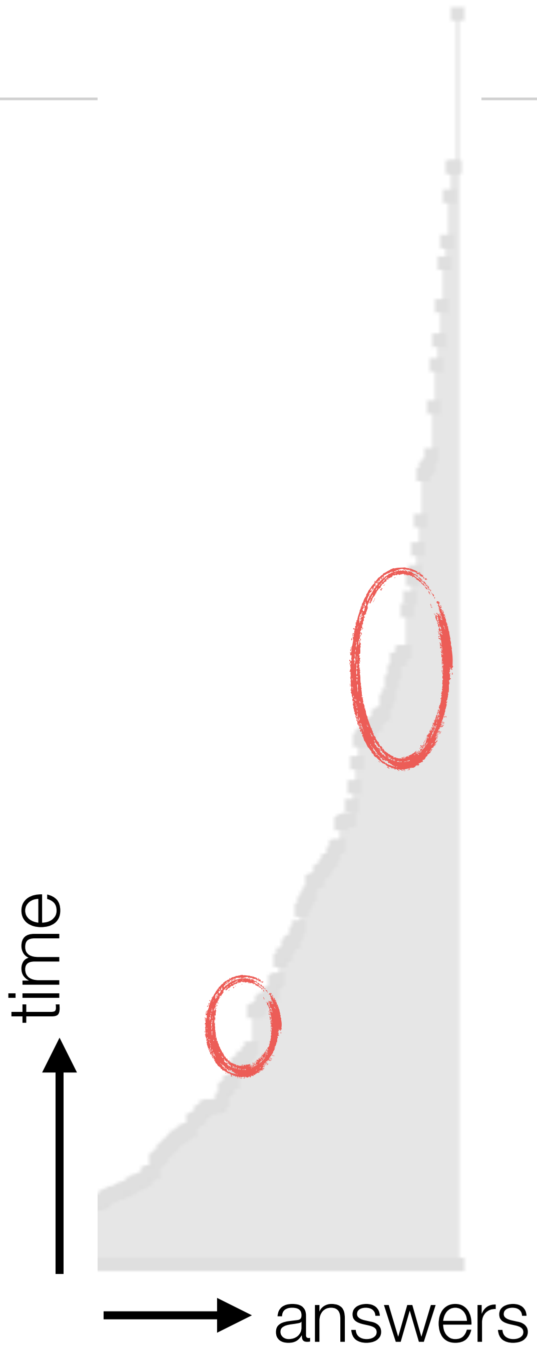


Most of the questions are answered shortly after they are posted

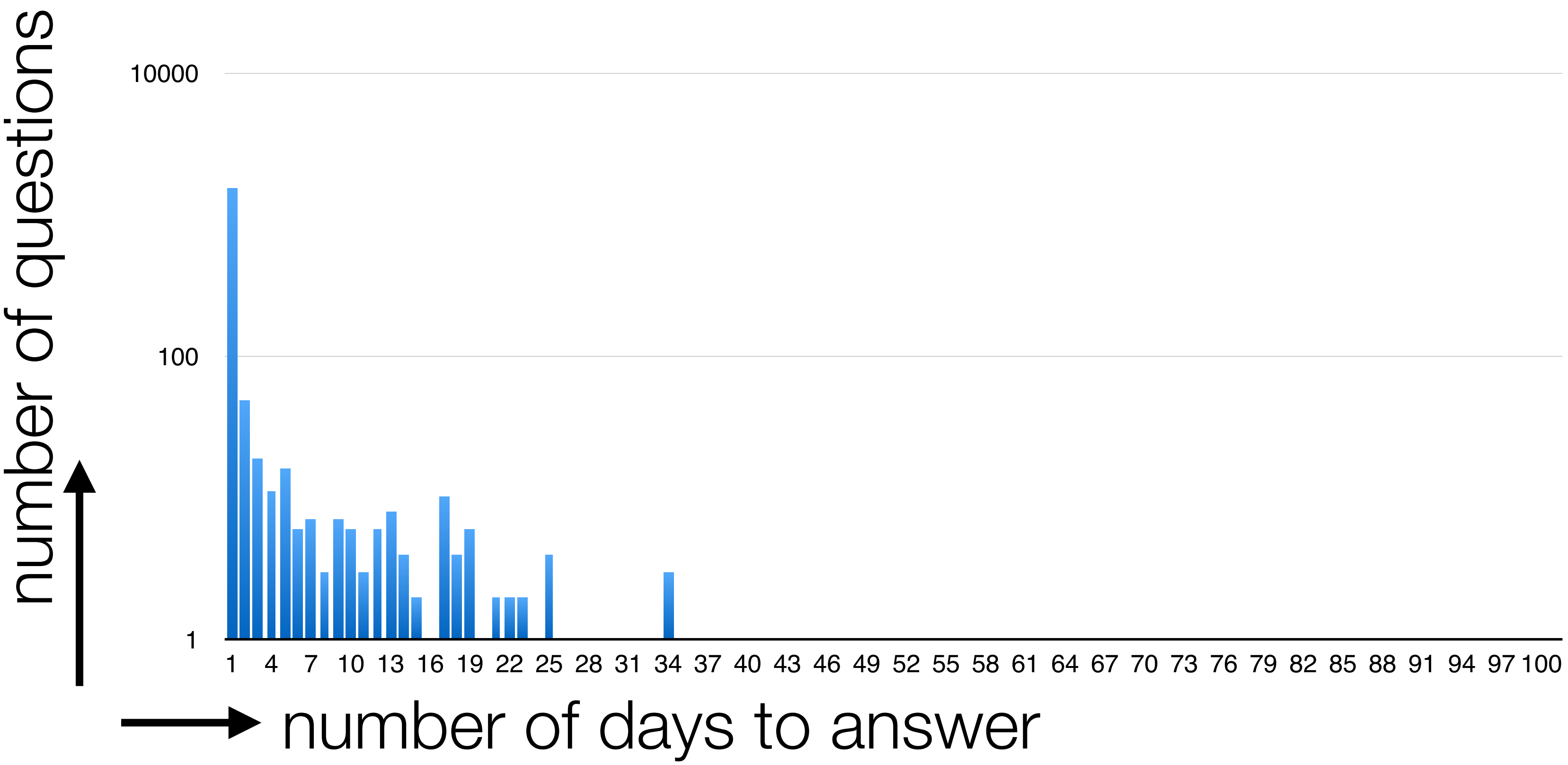
Time to answer



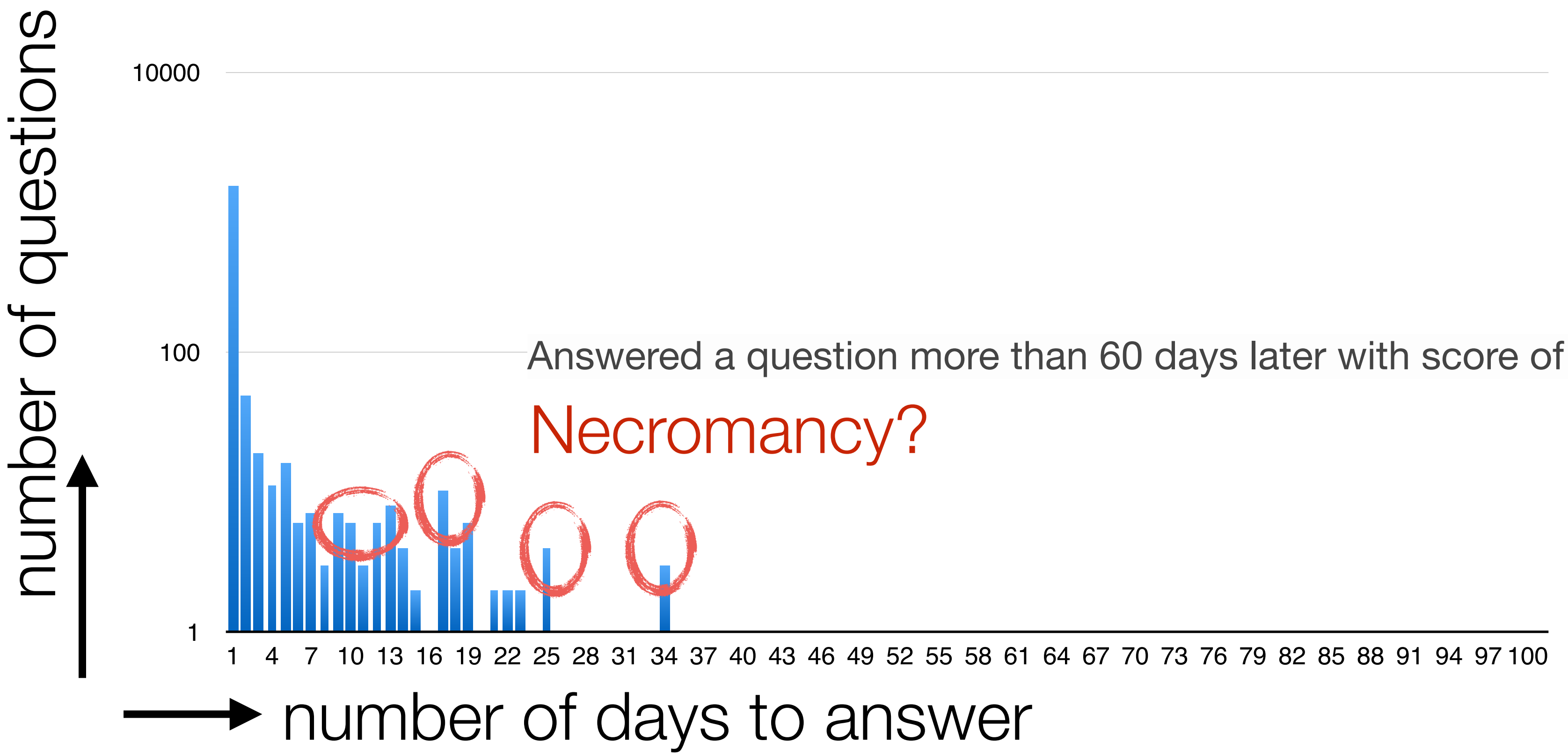
Time to answer



Time to answer



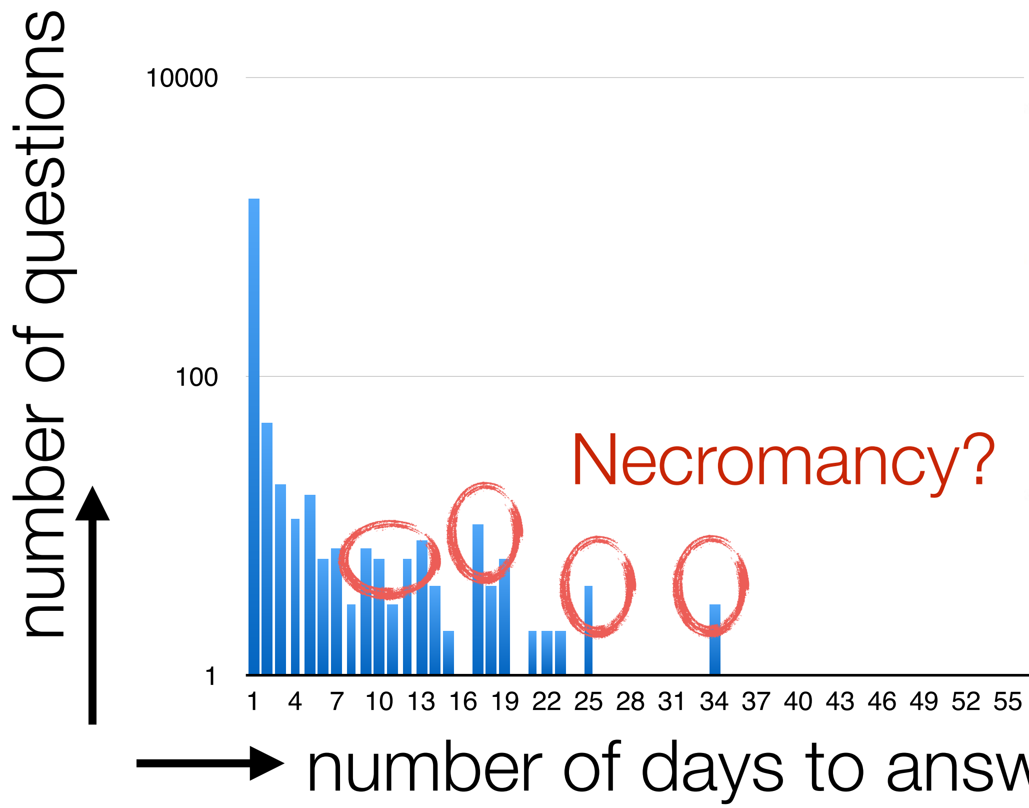
Time to answer



Answered a question more than 60 days later with score of 5 or more

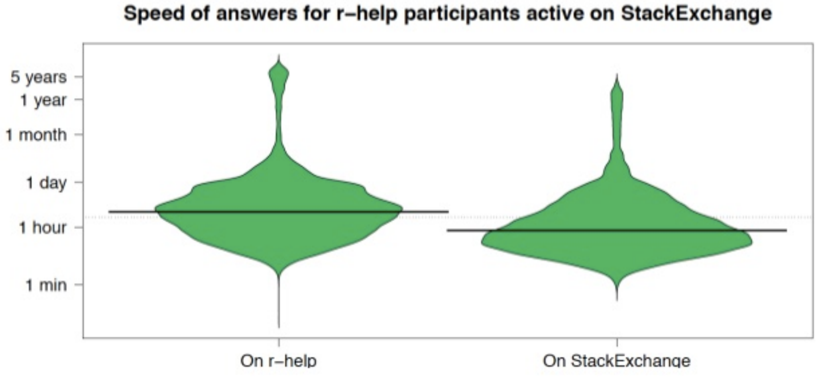
Necromancy?

Time to answer



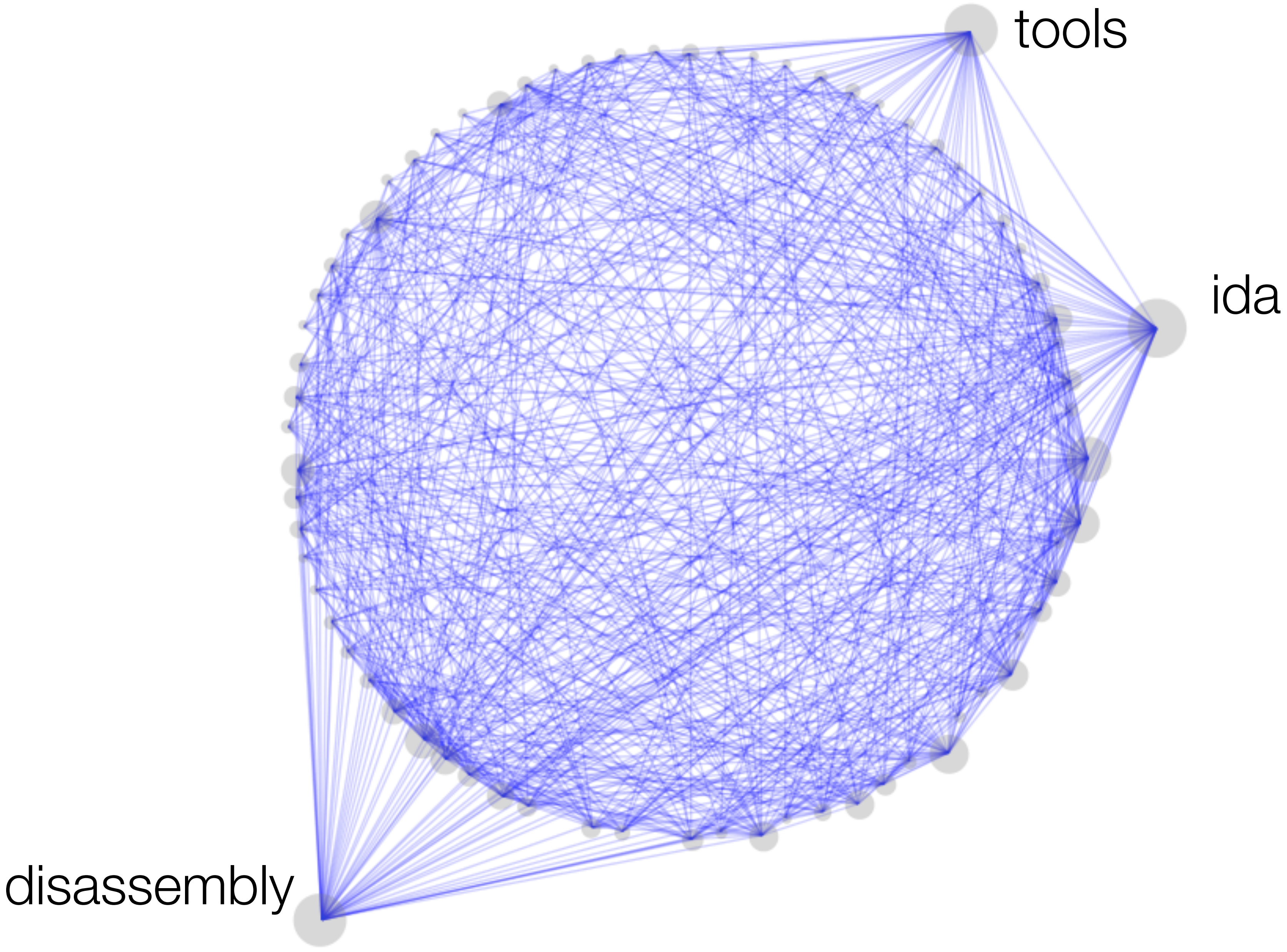
Necromancy?

stack overflow + R help = ♥

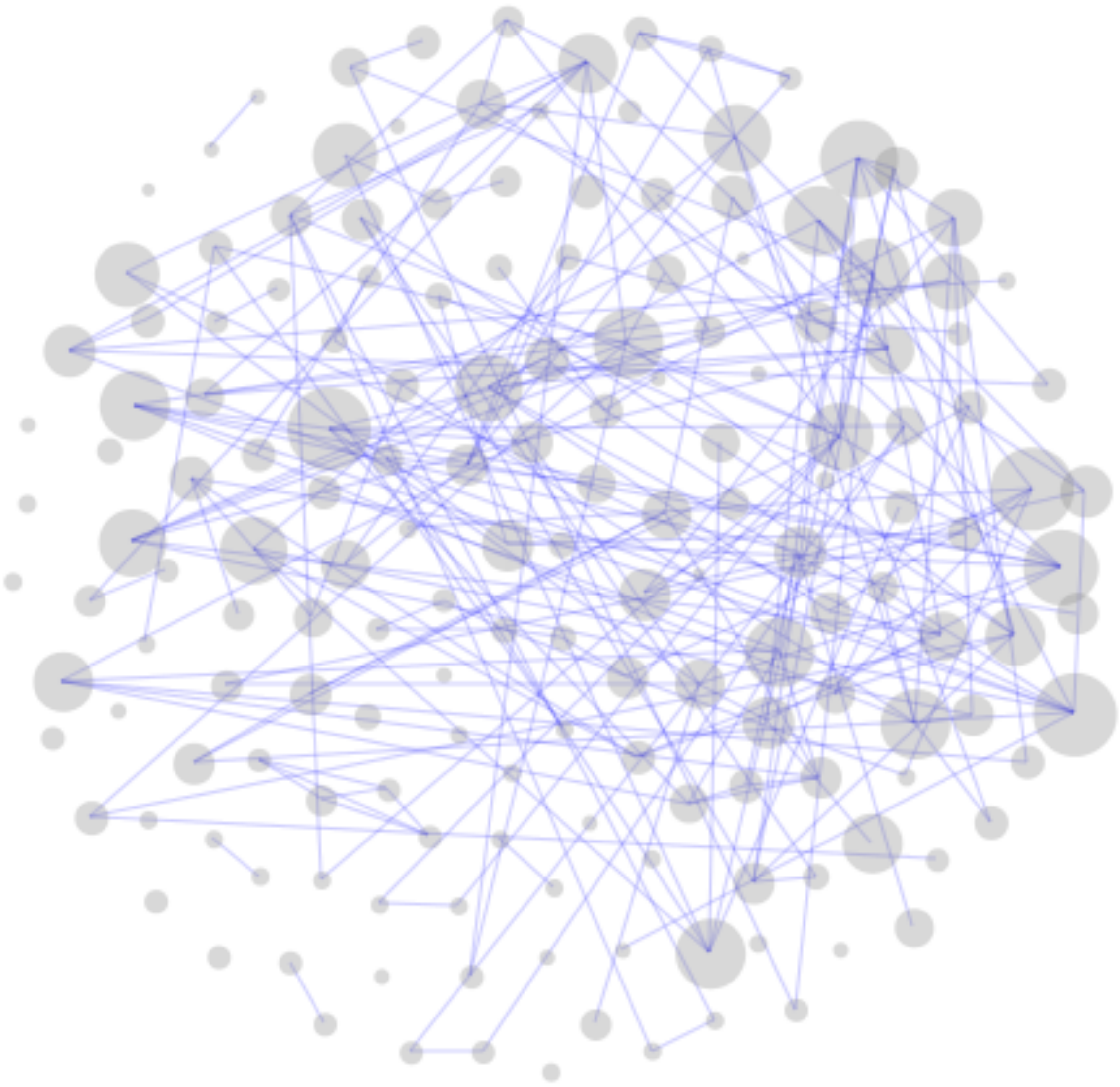


How Social Q&A sites are changing knowledge sharing in open source software communities, Vasilescu, B., Serebrenik, A., Devanbu, P.T. and Filkov, V., In CSCW 2014, ACM.

Tags relations

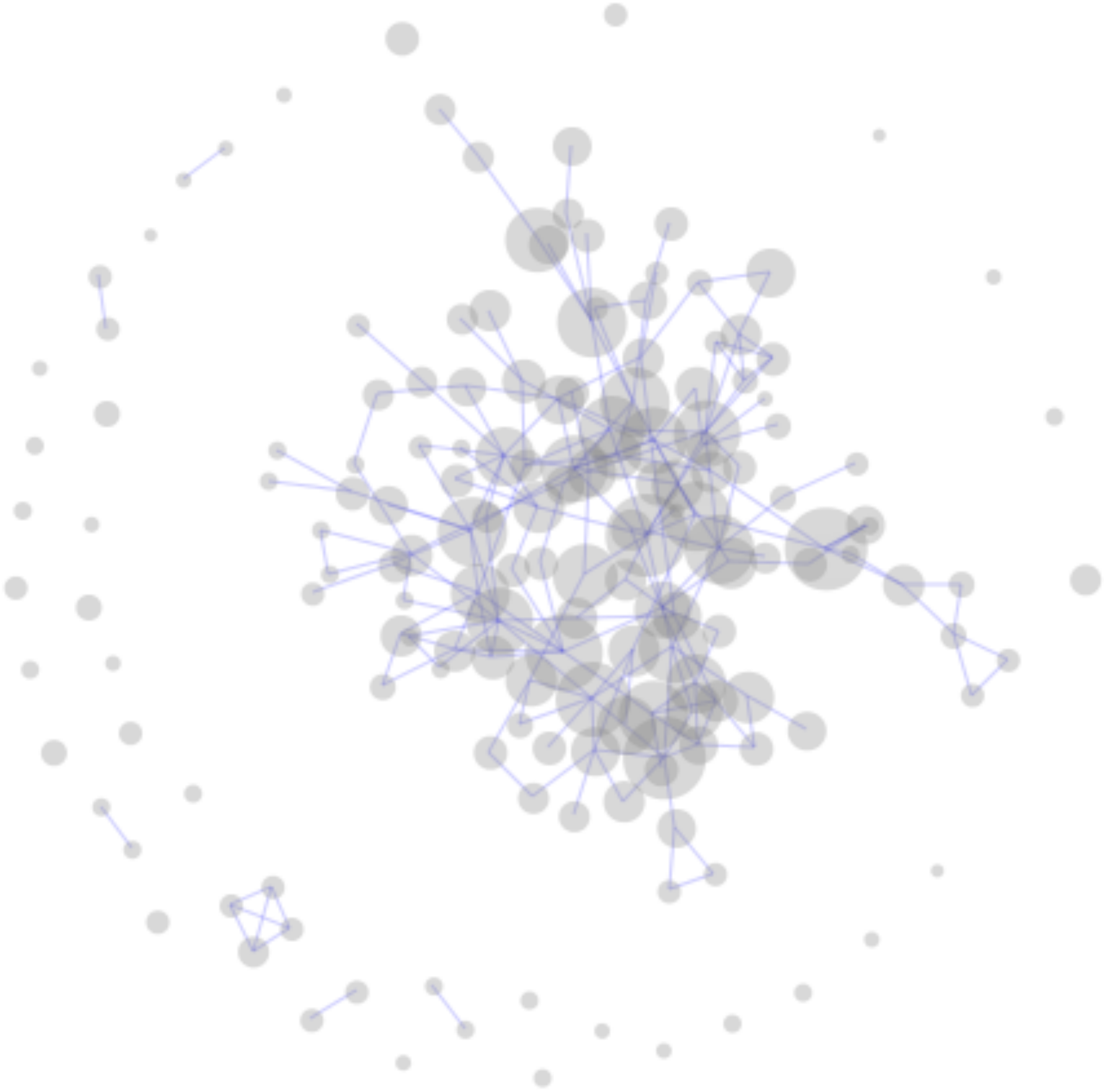


Tags relations



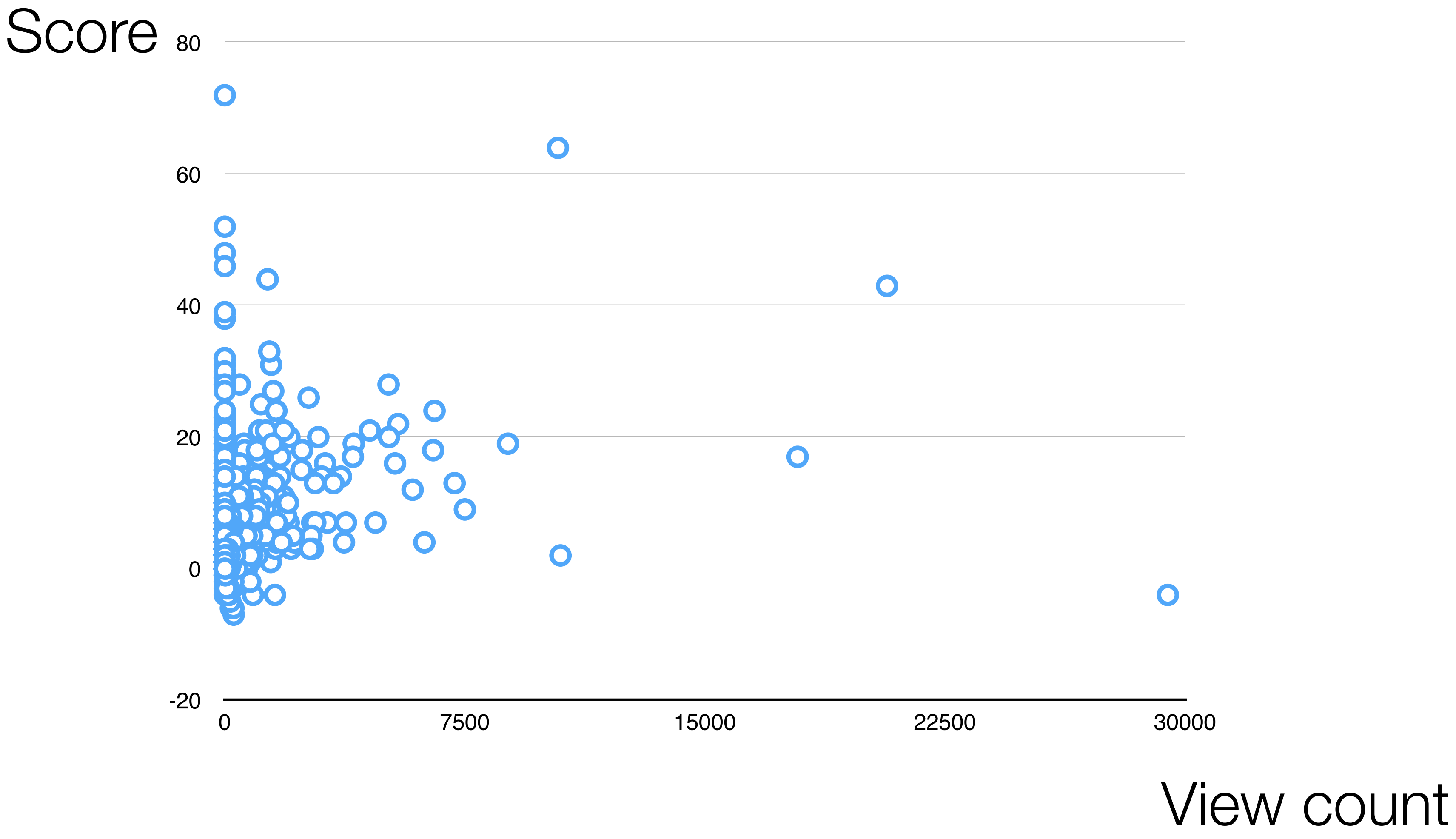
numberOfRelatedTags < 20

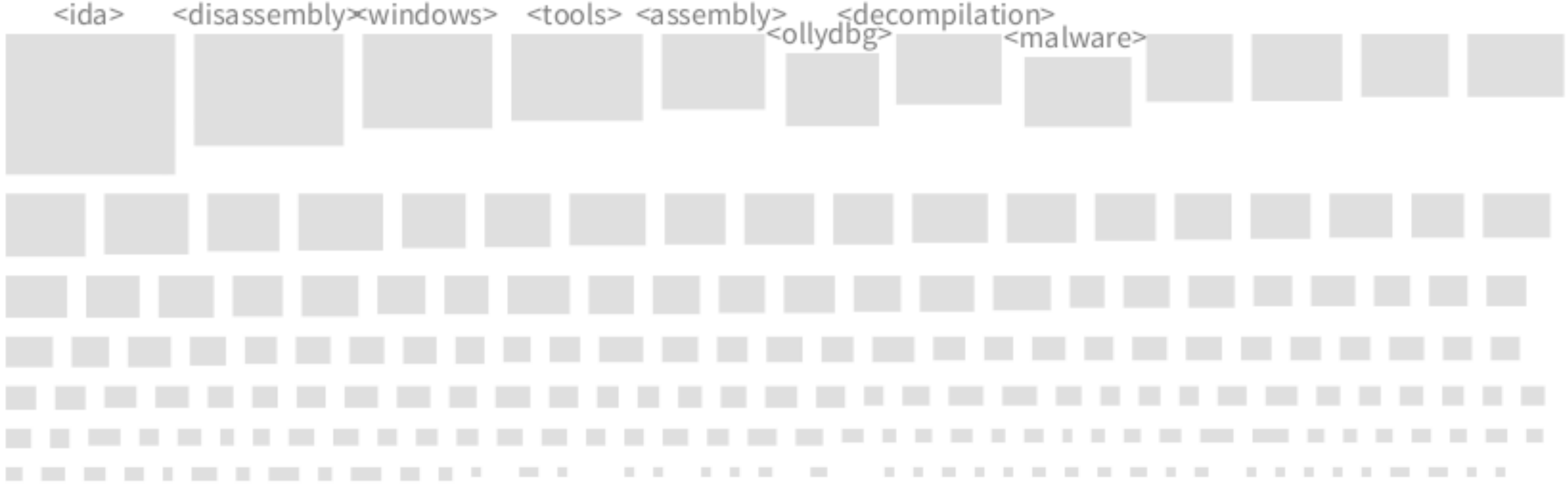
Tags relations



numberOfRelatedTags < 20

Score vs View: No correlation



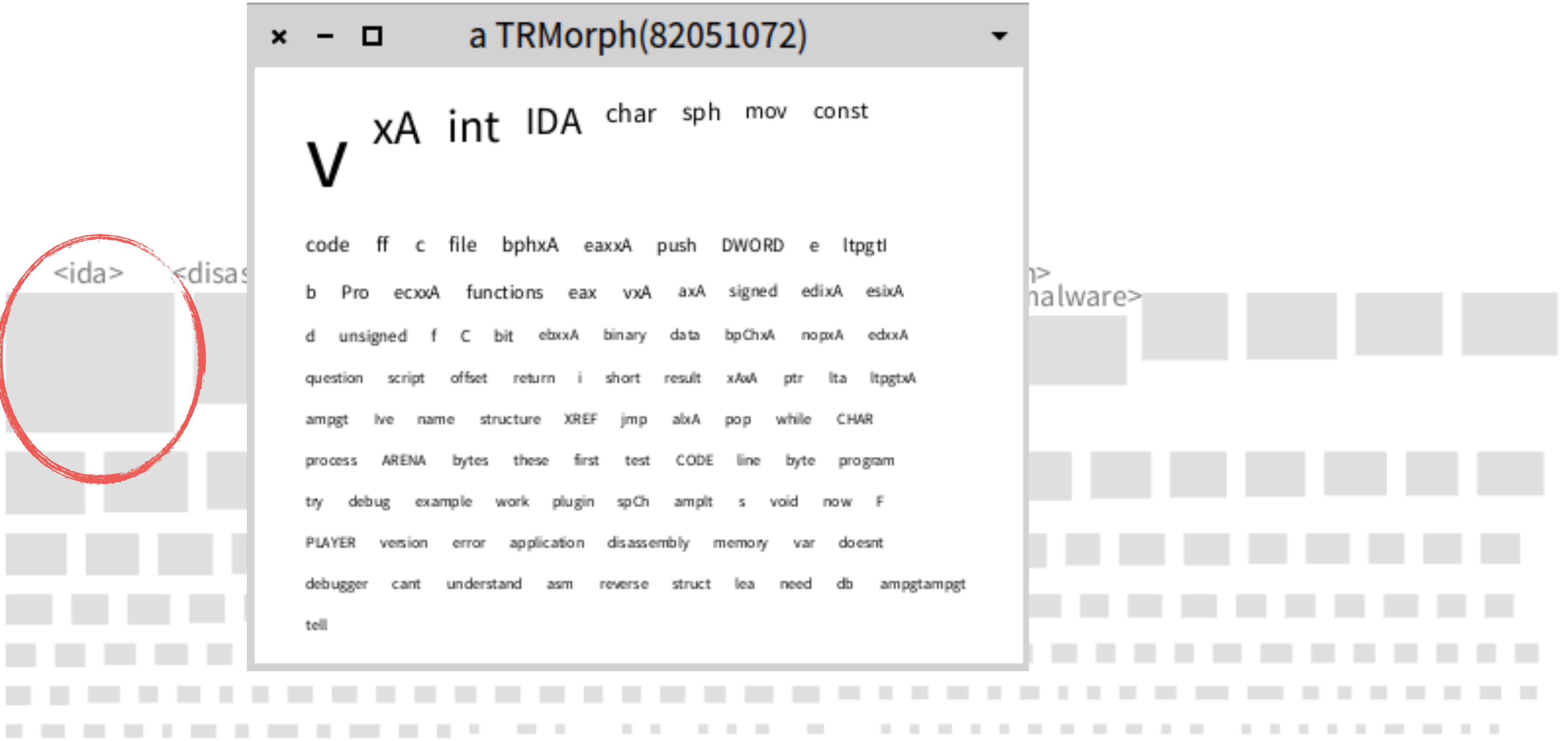


each box is a tag

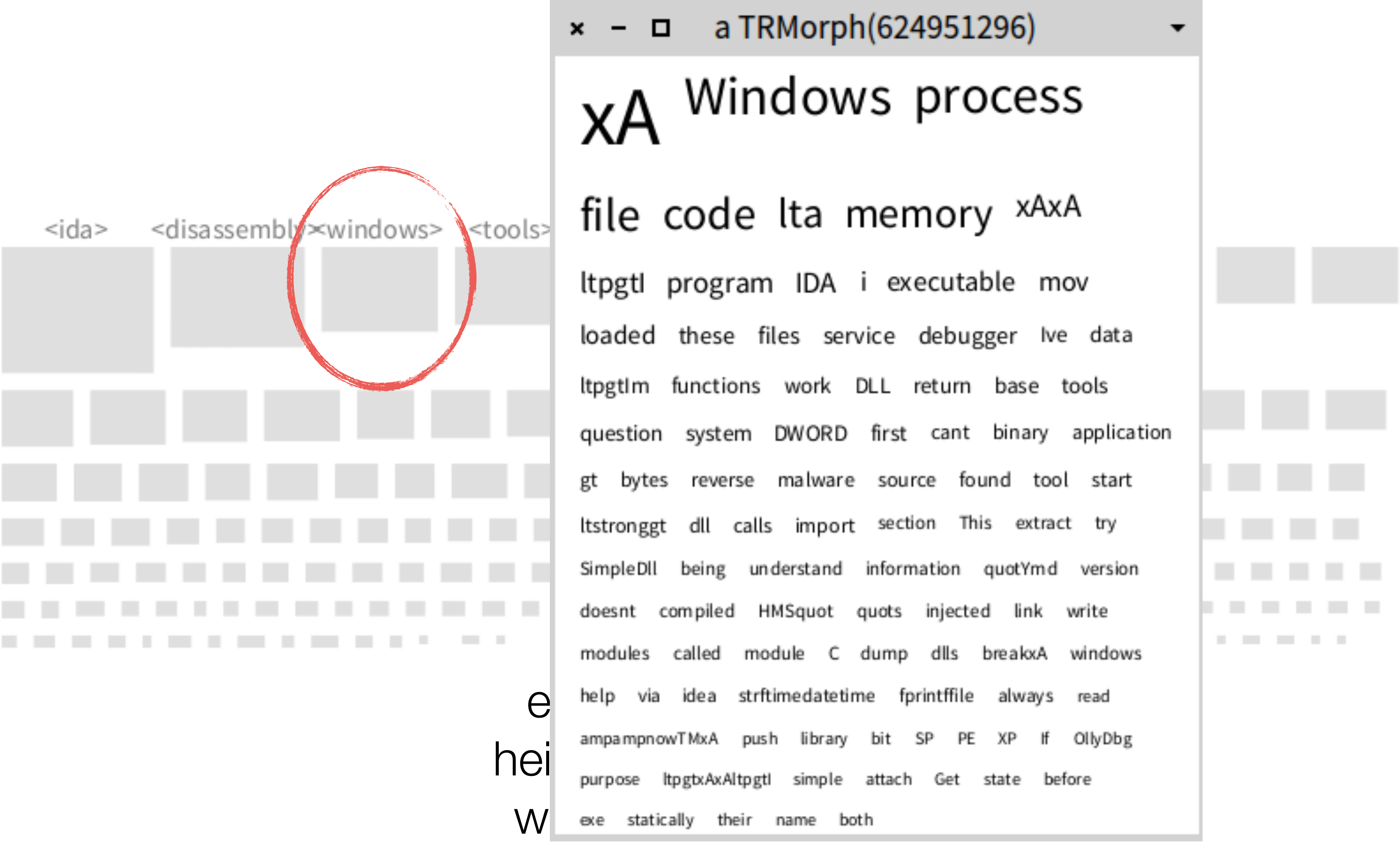
height = # questions

width = # answers

square root transformation


a TRMorph(82051072)
V
xA
int
IDA
char
sph
mov
const
code ff c file bphxA eaxxA push DWORD e ltpgtl
b Pro ecxxA functions eax vxA axA signed edixA esixA
d unsigned f C bit ebxxA binary data bpChxA nopxA edxxA
question script offset return i short result xAxA ptr lta ltpgtxA
ampgt lve name structure XREF jmp alxA pop while CHAR
process ARENA bytes these first test CODE line byte program
try debug example work plugin spCh amplt s void now F
PLAYER version error application disassembly memory var doesnt
debugger cant understand asm reverse struct lea need db ampgtampgt
tell
<ida>
<disas
n>
nalware>

each box is a tag
height = # questions
width = # answers
square root transformation



xA Windows process

file code lta memory xAxA

ltpgtl program IDA i executable mov

loaded these files service debugger lve data

ltpgtlm functions work DLL return base tools

question system DWORD first cant binary application

gt bytes reverse malware source found tool start

ltstronggt dll calls import section This extract try

SimpleDll being understand information quotYmd version

doesnt compiled HMSquot quots injected link write

modules called module C dump dlls breakxA windows

help via idea strftimedatetime fprintffile always read

ampampnowTMxA push library bit SP PE XP If OllyDbg

purpose ltpgtxAxAltpgtl simple attach Get state before

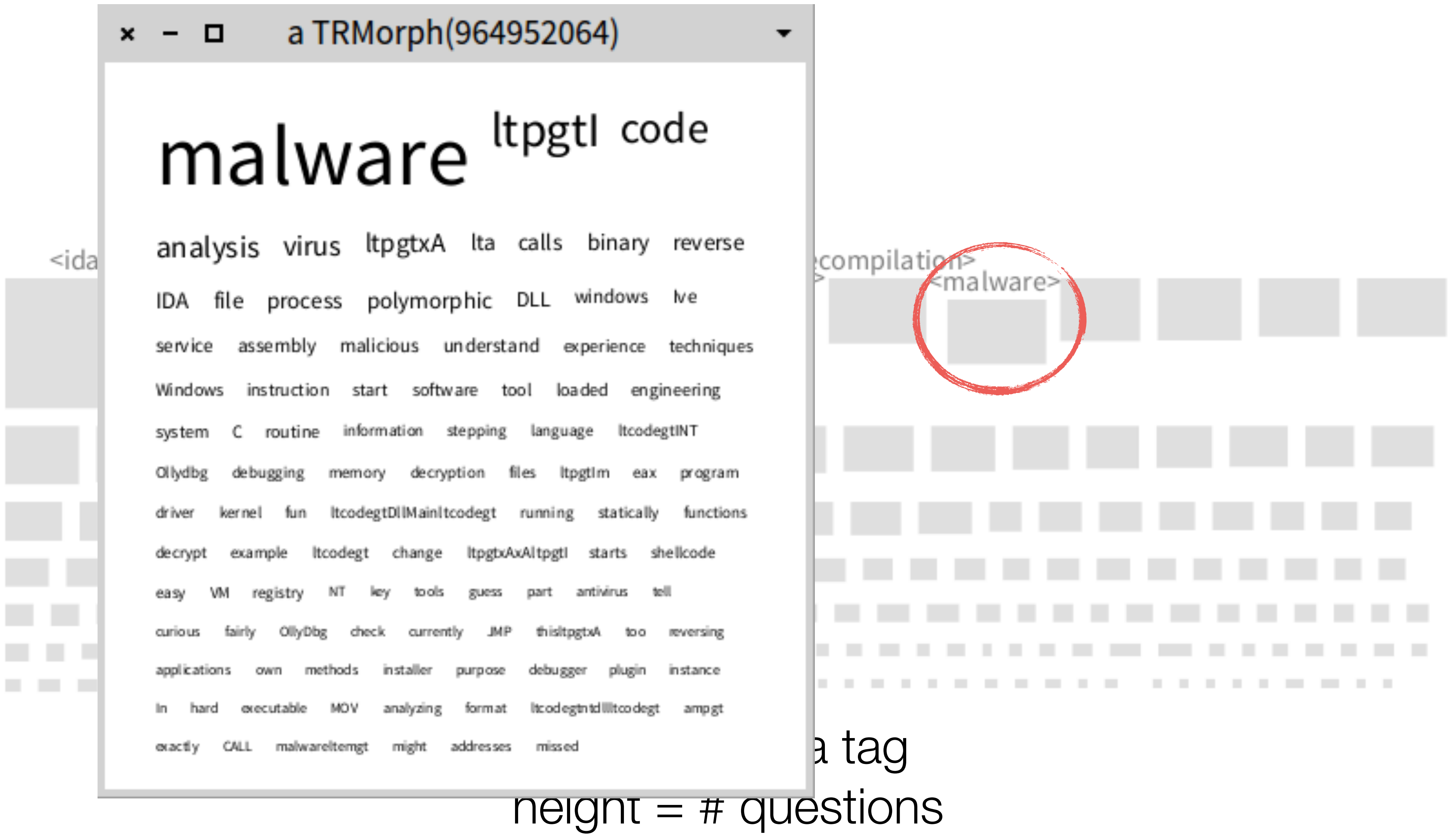
exe statically their name both

e

hei

w

square root transformation



a TRMorph(964952064)

malware ltpgtl code

analysis virus ltpgtxA lta calls binary reverse

IDA file process polymorphic DLL windows lve

service assembly malicious understand experience techniques

Windows instruction start software tool loaded engineering

system C routine information stepping language ltcodegtINT

Ollydbg debugging memory decryption files ltpgtlm eax program

driver kernel fun ltcodegtDllMainltcodegt running statically functions

decrypt example ltcodegt change ltpgtxAxAltpgtl starts shellcode

easy VM registry NT key tools guess part antivirus tell

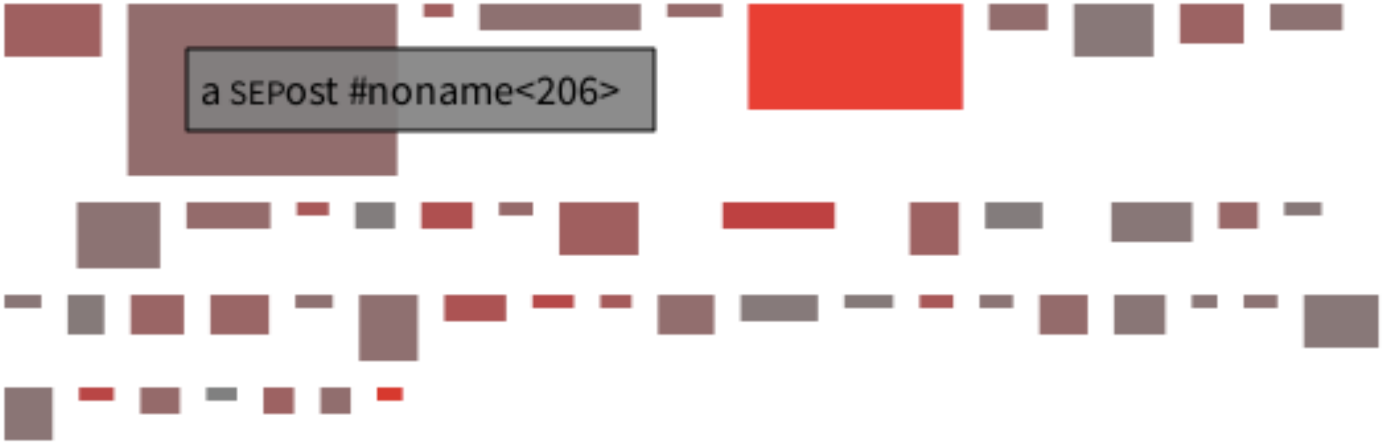
curious fairly OllyDbg check currently JMP thisltpgtxA too reversing

applications own methods installer purpose debugger plugin instance

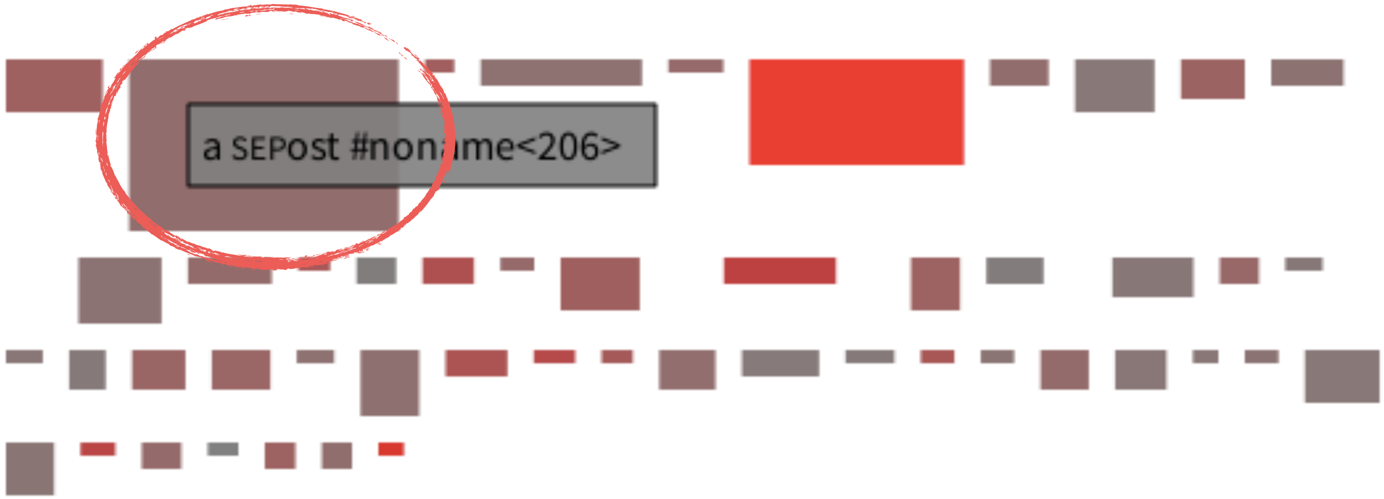
In hard executable MOV analyzing format ltcodegtntdllltcodegt ampgt

exactly CALL malwareltemgt might addresses missed

a tag
height = # questions
width = # answers
square root transformation

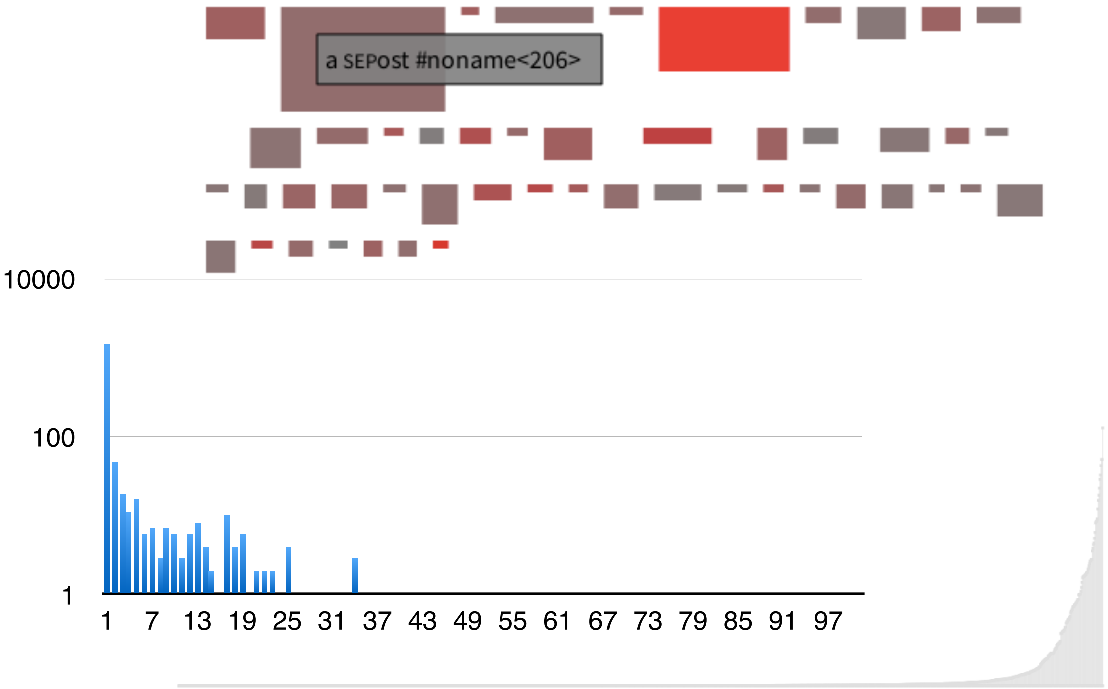


Each box is a post
width = viewCount
height = answerCount
color = body size



Each box is a post
width = viewCount
height = answerCount
color = body size

“It seems that a *popular use of software reverse engineering* skills is to *reverse malicious code in an effort to build better protection* for users. The bottleneck here for people aspiring to break into the security industry through this path seems to be easy access to new malicious code samples to practice on and build heuristics for. Are there any good resources for a person unaffiliated with any organization to download malware in bulk to run analysis on?”



That’s all folk!