Evolution of Binary Code Analysis

Jason Garman
Chief Technology Officer, Kyrus
Why am I here?

• I’ve been analyzing all sorts of binary code for about 8 years
  • For commercial and government entities
  • Mostly malicious code, but also …
    • I’ve lost my source code! How do I read my data?
    • Did he steal my code?
    • … you get the idea

• Now I get to step back and think of new ways to approach the problem

• So… how have I seen the tools & techniques used in code analysis evolve over the years?
In the beginning...
Tools, then and now

(Insert obligatory IDA Pro Screenshots here)
New techniques?

- Volatile memory acquisition & analysis
  - Enables analysis of “live” binaries as running on system
- Focus on automation, less manual static analysis
  - Automated clustering techniques
  - Automated *dynamic sandbox analysis*
- Don’t forget:
  - It takes 10 years for a product to reach “usable” state
  - We are still innovating!
  - Unavoidable subjectivity in analysis
What’s next?