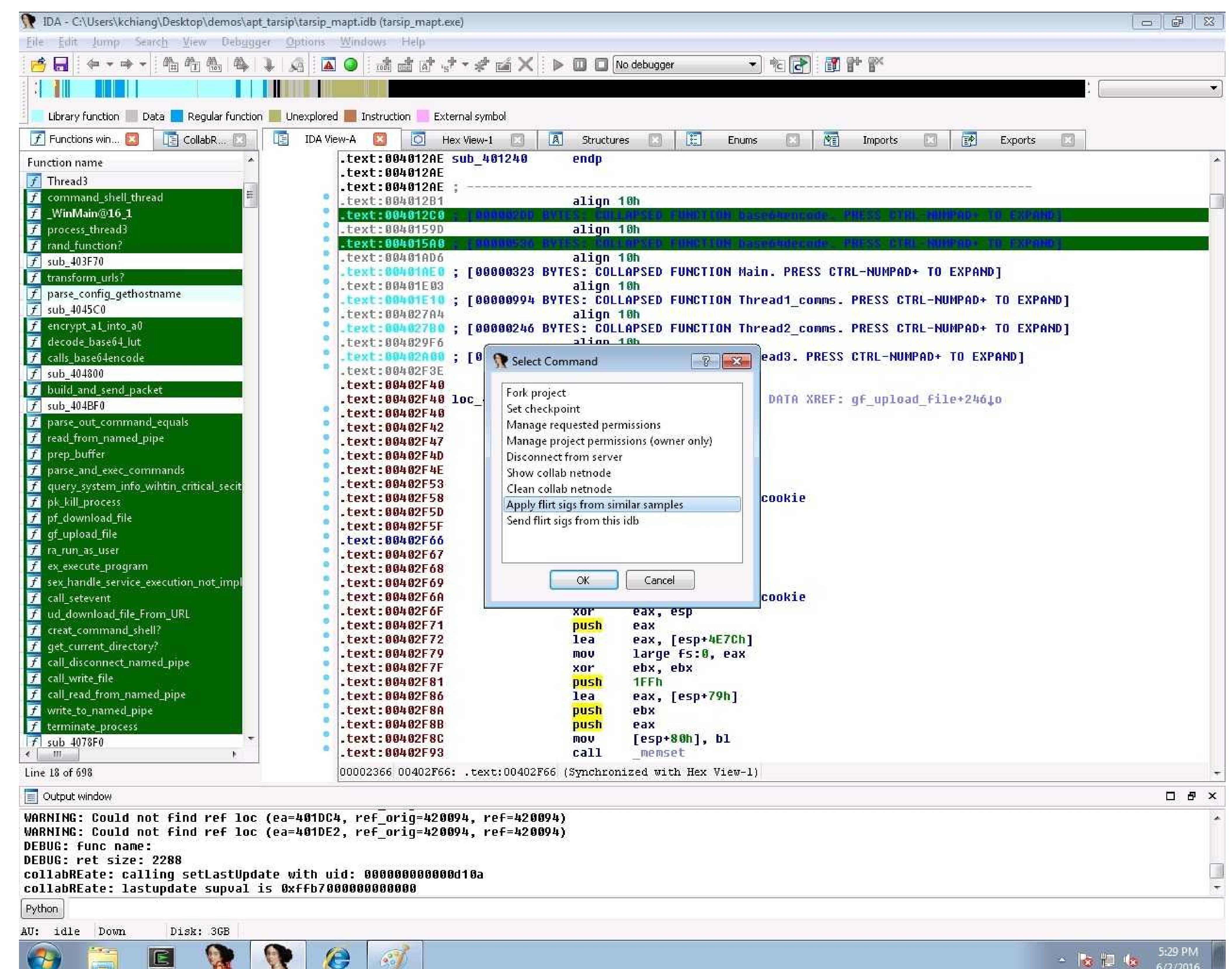


RETRACE

- Increases software reverse engineers' effectiveness and reduces workload
- Identifies and eliminates repetitive and redundant analysis
- Propagates reverse engineering knowledge across IDA Pro databases for identical functions in different binaries
- Extends the functionality of collabREate by Chris Eagle and Tim Vidas

Ken Chiang, Devin Cook, Howard Poston, and Manuel Sanchez



Current Functionality

- Automatic naming of identical functions across differing binaries
- Cross-binary function matching based upon user-configurable thresholds for similarity of binaries

Under Development

- Propagation of code comments contained in identical functions across differing binaries
- Integration of RETRACE with the Forensic Analysis Repository for Malware (FARM) for increased sharing of reverse engineering knowledge

Planned Development

- Cross-binary knowledge sharing for non-code segments of binary (data, structs, enums, etc.)
- Integrated tagging and alerting for user-identified features of interest (C2 functions, encryption S-Boxes, etc.)
- Integrated issue tracking system to allow reverse engineers to request assistance on difficult functions and enable collaboration