OllyDbg

Autor: Oleh Yuschuk

Versiones

- Hubo 10 versiones de la versión 1.x
- La versión 2.0 salió en junio 2010 y fue reescrito desde cero el programa.
- Es shareware, completamente gratis pero hay que registrarse con el autor.
- La última versión de ollydbg aún no puede desarmar binarios compilados en procesadores de 64 bits, pero se ha dicho que se está trabajando en esto.

Aplicación

Ollydbg es un x86 debugger que se enfoca en análisis de código binario.

Mapea registros

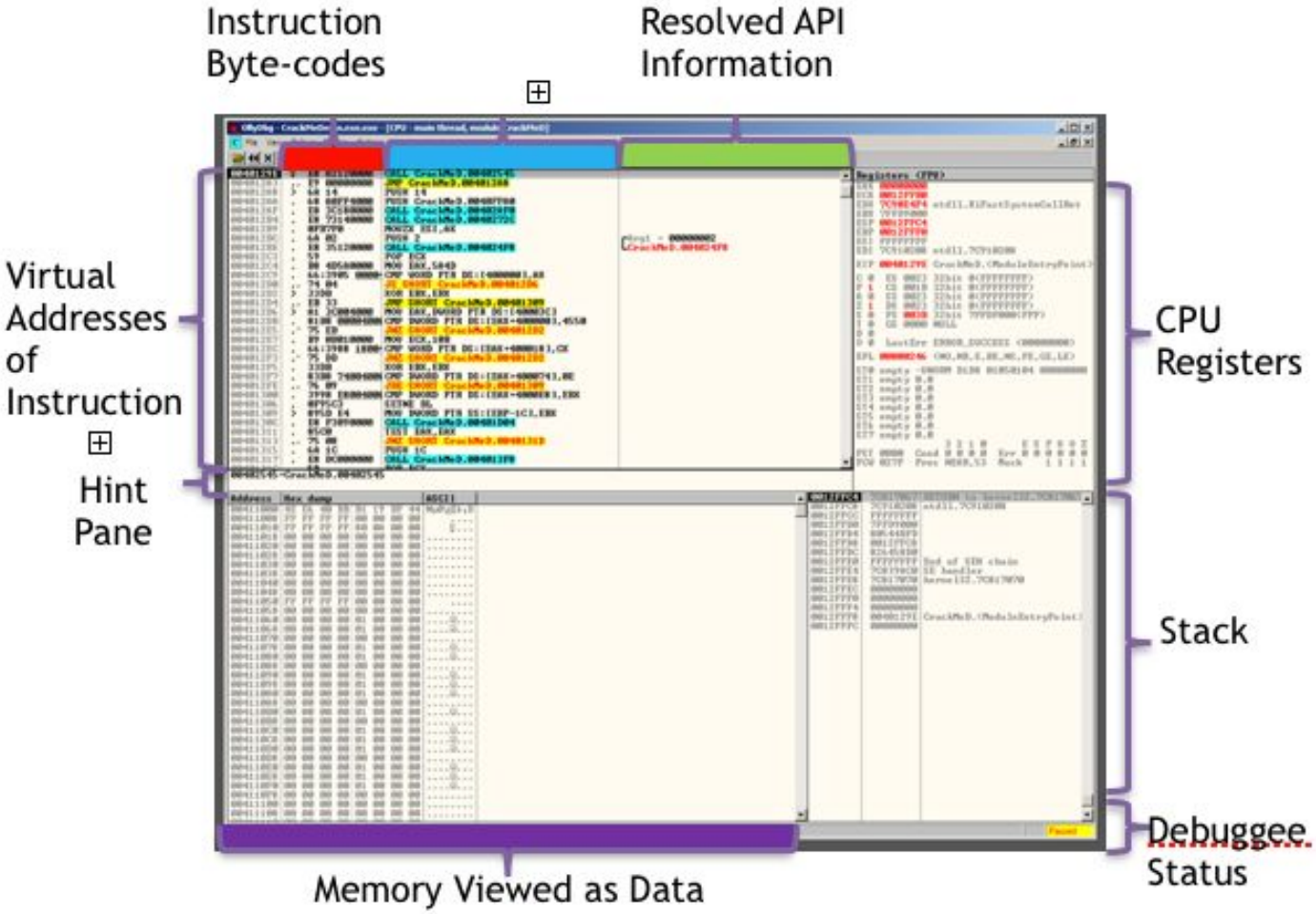
reconoce procedimientos , llamadas a API , switches, tablas , constantes y strings

localiza rutinas de object files y librerías.

Ingeniería inversa

Reverse engineering

OllyDbg is often used for reverse engineering of programs.[3] It is often used by crackers to crack software made by other developers. For cracking and reverse engineering, it is often the primary tool because of its ease of use and availability; any 32-bit executable can be used by the debugger can be edited in bitcode/assembly in realtime.[4] It is also useful for programmers to ensure that their program is running as intended, and for malware analysis purposes.


Instruction Byte-codes
Resolved API Information
Virtual Addresses of Instruction
Hint Pane
CPU Registers
Stack
Debuggee Status
Memory Viewed as Data