Tutorial Olly Debugger

Pentru a putea înțelege mai bine execuția unui program în limbaj de asamblare, sau pentru depistarea erorilor, se folosesc programe de tip debugger. Acestea permit încărcarea unui fișier executabil, execuția acestuia instrucțiune cu instrucțiune, vizualizarea conținutului memoriei și a regiștrilor, la fiecare pas, și chiar modificarea unor instrucțiuni sau date, în timp ce programul rulează.

Debugger-ul folosit la acest laborator va fi Olly Debugger. Lansarea acestuia în execuție se face făcând dublu-click pe executabilul acestuia, numit `ollydbg.exe`. Dacă se utilizează plugin-ul pentru MASM din Notepad++, se poate lansa depanarea programului curent apăsând **F6**.

În Olly Debugger, încărcarea unui program pentru depanare, se va face folosind tasta **F3**. Eventualele argumente cu care trebuie rulat programul se pot specifica în fereastra de dialog care apare. Dacă după încărcarea programului nu apare codul acestuia, se poate ajunge la el, folosind combinația de taste **Ctrl+F9**.

Fereastra debugger-ului arată ca în Figura 1, și este împărțită în 4 zone:

Zona 1 - conține regiștrii procesorului, împreună cu valorile acestora, la momentul curent al execuției. Regiștrii ai căror valori s-au modificat la instrucțiunea anterioară sunt marcați cu roșu, iar restul cu gri. Flag-urile sunt afișate și separat. Tot în această zonă sunt afișați și regiștrii coprocesorului matematic.

Zona 2 - numită și *dump*, poate afișa diverse porțiuni din memoria programului. La începutul execuției, aici se afișează secțiunea de date. Dump-ul este afișat prin 3 coloane. În prima avem adresa de început a liniei, în a doua, conținutul memoriei la adresa respectivă în format hexazecimal, iar în a 3-a, același conținut, în format text. Dacă dorim să vedem conținutul memoriei de la o anumită adresă, care apare în una din cele 4 zone ale debugger-ului, se face click dreapta pe acea adresă, și din meniul apărut se alege opțiunea "Follow in Dump".

Zona 3 - conține stiva programului (zonă de memorie cu o întrebuințare specială, ce va fi dezbătută într-o lucrare viitoare). Pe prima coloană sunt afișate adresele, iar pe a doua valorile, în hexazecimal (câte un `DWORD`). Adresa vârfului stivei este evidențiată. Se poate observa că adresa vârfului stivei este valoarea din registrul `ESP`. Ca și pentru zona de dump, orice adresă ce aparține de stivă poate fi urmărită în aceasta, făcând click dreapta și alegând "Follow in Stack".

Zona 4 - este zona de afișare a codului. În prima coloană se găsesc adresele instrucțiunilor, în hexazecimal. Adresa instrucțiunii următoare este evidențiată. În a doua coloană se găsește codul binar, aferent instrucțiunii de la adresa respectivă. Codurile binare ale instrucțiunilor au lungimi variabile. Pe a 3-a coloană se regăsește codul programului, dezasamblat. Ar trebui să se observe aceleași instrucțiuni ca și în programul sursă, eventual scrise într-o altă ordine.

La depanarea unui program, următoarele comenzi sunt utilizate mai des:

- Step Into - **F7** - trece la instrucțiunea următoare a programului, intrând în funcții, acolo unde se întâlnesc.

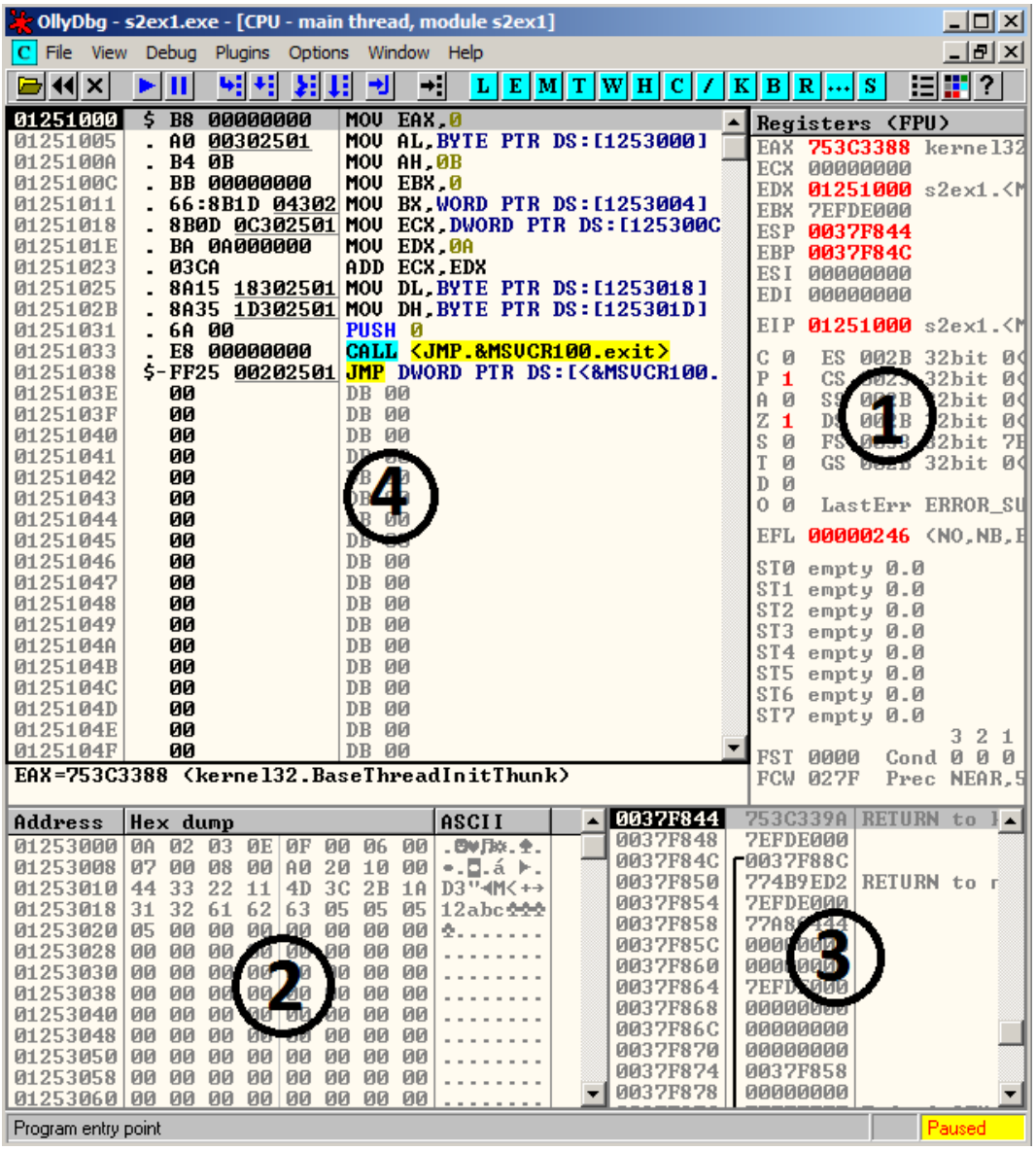

Figura 1: Spațiul de lucru în Olly Debugger

- Step Over - **F8** - trece la instrucțiunea următoare, sărind peste funcții (se execută întreaga funcție, ca și cum ar fi o singură instrucțiune).
- Breakpoint - **F2** - atunci când cursorul se află pe o anumită linie (acea linie este evidențiată prin culoarea gri deschis), se plasează o întrerupere la acea linie. Atunci când programul, în timpul rulării, ajunge la o instrucțiune pe care s-a pus un breakpoint, se va întrerupe execuția.
- Run - **F9** - pornește execuția normală a programului, de la poziția curentă, până la primul breakpoint întâlnit, sau până la final.
- Execute till Return - **Ctrl+F9** - la fel ca Run, dar execuția se oprește și la întâlnirea unei instrucțiuni `RETN`.
- Restart - **Ctrl+F2** - repornește programul depanat.

Instrucțiunile sau datele unui program pot fi modificate în timpul depanării. Se face click pe instrucțiunea sau datele dorite, pentru a poziționa cursorul acolo, apoi se apasă tasta Space. În fereastra de dialog apărută, se pot face modificările.

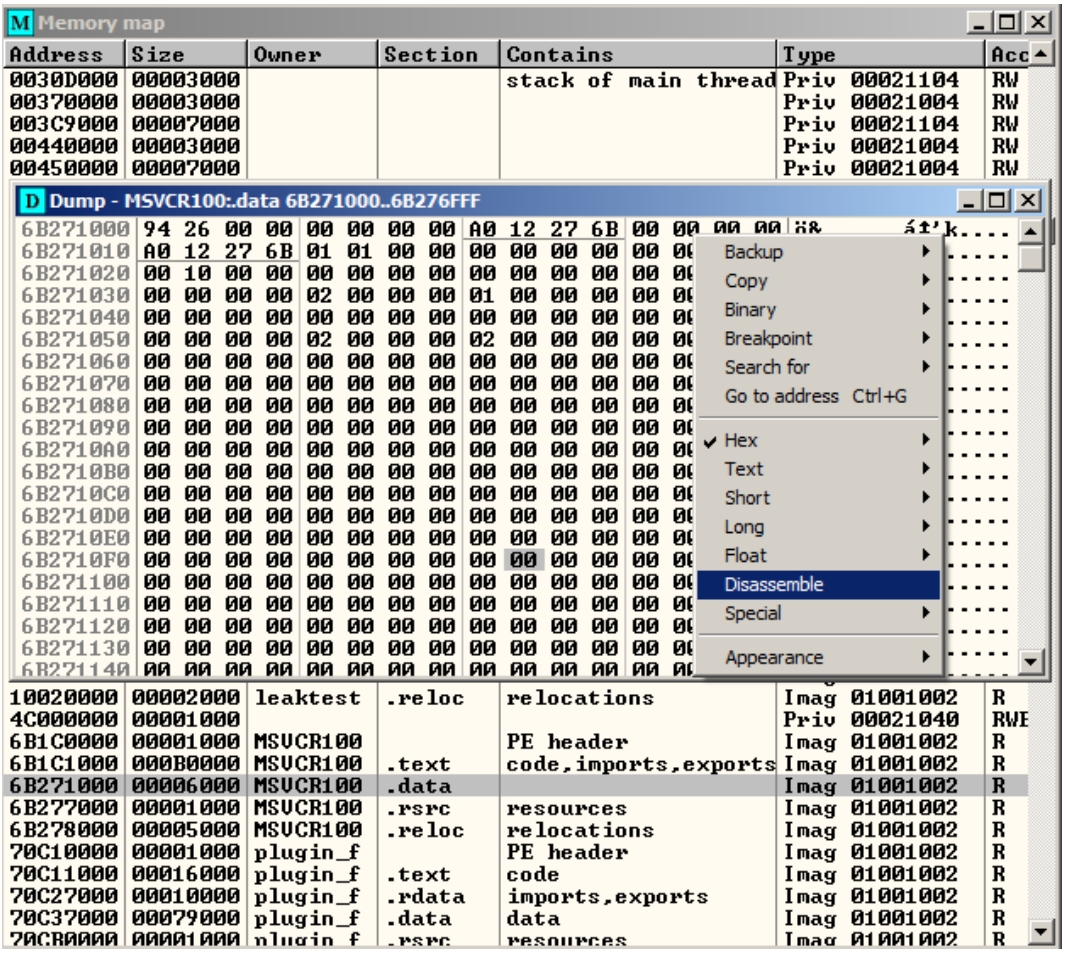

Figura 2: Harta memoriei în Olly Debugger

Pentru a vizualiza întreg conținutul memoriei, se apasă combinația de taste **Alt+M**. În tabelul apărut este descrisă fiecare secțiune. Coloanele *Address* și *Size* indică adresa, respectiv dimensiunea secțiunii. În coloana *Owner*, apare numele modulului ce conține acea secțiune. Modulul principal are același nume ca și numele programului executabil. Coloana *Section* indică numele efectiv al secțiunii, în timp ce coloana *Contains* arată ce se găsește în aceasta.

Făcând dublu-click pe o linie a tabelului, se poate vizualiza conținutul secțiunii respective. Olly Debugger va încerca să "ghicească" tipul de conținut, afișând implicit datele în format hexazecimal și ASCII, respectiv dezasamblând codul. În cazul în care utilizatorul dorește vizualizarea informației în alt format, poate face click dreapta în zona de afișare, și alegerea formatului dorit (ca în Figura 2).

Pentru revenirea în mod CPU (fereastra principală, cu cele 4 zone), se apasă combinația de taste **Alt+C**.