

Reconstruct the top stack frame at breakpoint 1 using output from the various gdb commands (like we did for square.c in the example). Fill in the values in the following template:

| Pointers (Register Addresses) | EBP Offset | Address | Name | Description | Value |
|--|---------------|------------|------------|--|------------|
| ESP -> | ebp - 16 | 0xbffff6e8 | | First empty memory location | |
| | ebp - 12 | 0xbffff6ec | | | |
| | ebp - 8 | 0xbffff6f0 | y | Local variable | 0x421 |
| | ebp - 4 | 0xbffff6f4 | x | Local variable | 0x216 |
| EBP-> | ebp | 0xbffff6f8 | Old EBP | EBP register points here | |
| | ebp + 4 | 0xbffff6fc | Old EIP | Return Instruction Pointer(RIP) | 0xbffff6fc |
| | ebp + 8 | 0xbffff700 | *xp | Parameter for swap_n_add. It is address of a1 | 0xbffff708 |
| Bottom of frame ->(also the previous frame's SP) | ebp + 12 | 0xbffff704 | *yp | Parameter for swap_n_add. It is address of a2 | 0xbffff70c |

4. Reconstruct the top stack frame at breakpoint 2.

| Pointers (Register Addresses) | EBP Offset | Address | Name | Description | Value |
|---|---------------|------------|---------|---------------------------------|-------|
| ESP -> | ebp - 40 | 0xbffff6f0 | | Fir empty memory location | |
| | ebp - 36 | 0xbffff6f4 | | | |
| | ebp - 32 | 0xbffff6f8 | | | |
| | ebp - 28 | 0xbffff6fc | | | |
| | ebp - 24 | 0xbffff700 | | | |
| | ebp - 20 | 0xbffff704 | | | |
| | ebp - 16 | 0xbffff708 | diff | Local variable | 0x20b |
| | ebp - 12 | 0xbffff70c | sum | Local variable | 0x637 |
| | ebp - 8 | 0xbffff710 | a2 | Local variable | 0x216 |
| | ebp - 4 | 0xbffff714 | a1 | Local variable | 0x421 |
| EBP-> | ebp | 0xbffff718 | Old EBP | EBP register | |

| | | | | | |
|---|----------|------------|---------|----------------------------------|--|
| | | | | points here | |
| | ebp + 4 | 0xbffff71c | Old EIP | Return Instruction pointer (RIP) | 0xb7e41a83 |
| | Ebp+8 | 0xbffff720 | argc | Parameter for the main() | 0x1 |
| Bottom of frame ->(also the previous frame's SP) | ebp + 12 | 0xbffff724 | **argv | Parameter for the main() | 0xbffff8d6 -> "/home/user/gdb/swap_n_add" |