HxD:

A picture containing text, screenshot, font, line

Description automatically generated

Disassembly using ndisasm:

A picture containing text, screenshot

Description automatically generated

Notes:

66 55: push ebp

66 89 E5: mov ebp, esp

66 83 EC 10: sub esp, 0x10 - sub because second operand is an immediate value, subtract 16 from esp

66 67 C7 45 04 0B 00 00 00 - mov dword [ebp+0x4], 0xb

66 67 C7 45 08 0D 00 00 00 - mov dword [ebp+0x8], 0xd

66 31 C0 - xor eax, eax - seems like a valid way to clear the eax register

74 01 - jmp

FF: potentially a rogue byte, 66 67 are prefix bytes for the next FF

66 67 FF 75 08 - push word [ebp+0x8]

66 67 FF 75 04 - push word [ebp+0x4]

EB 01: jmp, valid displacement

A0: nop potententially a rogue byte, not needed before 66 BB

66 BB A0 F8 - mov bx, 0xf8a0

FF: nop

BF FF BF 67 FF 1B 66 - mov edi, 0x661bff67

83 C4 08 - add esp, 0x8, add based on second operand

C9 - leave

C3 – ret