Lab 9 Solutions

https://t.me/learningnets

Lab 9 - Disassembly Challenge

The following is a disassembled output of a simple C program. Can you figure out what this program does, and can you translate it back to a pseudocode?

```
mov dword ptr [ebp-4], 16h
mov dword ptr [ebp-8], 5
mov eax, [ebp-4]
add eax, [ebp-8]
mov [ebp-0Ch], eax
mov ecx, [ebp-4]
sub ecx, [ebp-8]
mov [ebp-10h], ecx
```

Solution

The code contains four memory references. First, let's label these addresses - ***ebp-4 = a***, ***ebp-8 = b*** , ***ebp-0Ch = c***, and ***ebp-10H = d***:

```
mov dword ptr [ebp-4], 16h
mov dword ptr [ebp-8], 5
mov eax, [ebp-4]
add eax, [ebp-8]
mov [ebp-0Ch], eax
mov ecx, [ebp-4]
sub ecx, [ebp-8]
mov [ebp-10h], ecx
```

```
mov dword ptr [a], 16h
mov dword ptr [b], 5
mov eax, [a]
add eax, [b]
mov [c], eax
mov ecx, [a]
sub ecx, [b]
mov [d], ecx
```

After translating the code into a high-level language equivalent it looks like the one shown here:

```
mov dword ptr [a], 16h
mov dword ptr [b], 5
mov eax, [a]
add eax, [b]
mov [c], eax
mov ecx, [a]
sub ecx, [b]
mov [d], ecx
```

```
a = 16h
b = 5
eax = a
eax = eax + b
c = eax
ecx = a
ecx = ecx-b
d = ecx
```

Replacing all the register names with their corresponding values on the right side of the = operator (in other words, at ❶), we get the following code:

```
a = 16h
b = 5
eax = a
eax = eax+b ❶
c = eax ❶
ecx = a
ecx = ecx-b ❶
d = ecx ❶
```

```
a = 22
b = 5
eax = a
eax = a+b
c = a+b
ecx = a
ecx = a-b
d = a-b
```

After removing all the entries containing registers on the left side of the = sign at ❷ (because registers are used for temporary calculations), we are left with the following:

```
a = 22
b = 5
eax = a ❷
eax = a+b ❷
c = a+b
ecx = a ❷
ecx = a-b ❷
d = a-b
```

```
a = 22
b = 5
c = a+b
d = a-b
```