National Forensic Sciences University

School of Cyber security and Digital Forensics

Subject: CTMSCS S2 P3 Malware Analysis

(TA-II Assignment)

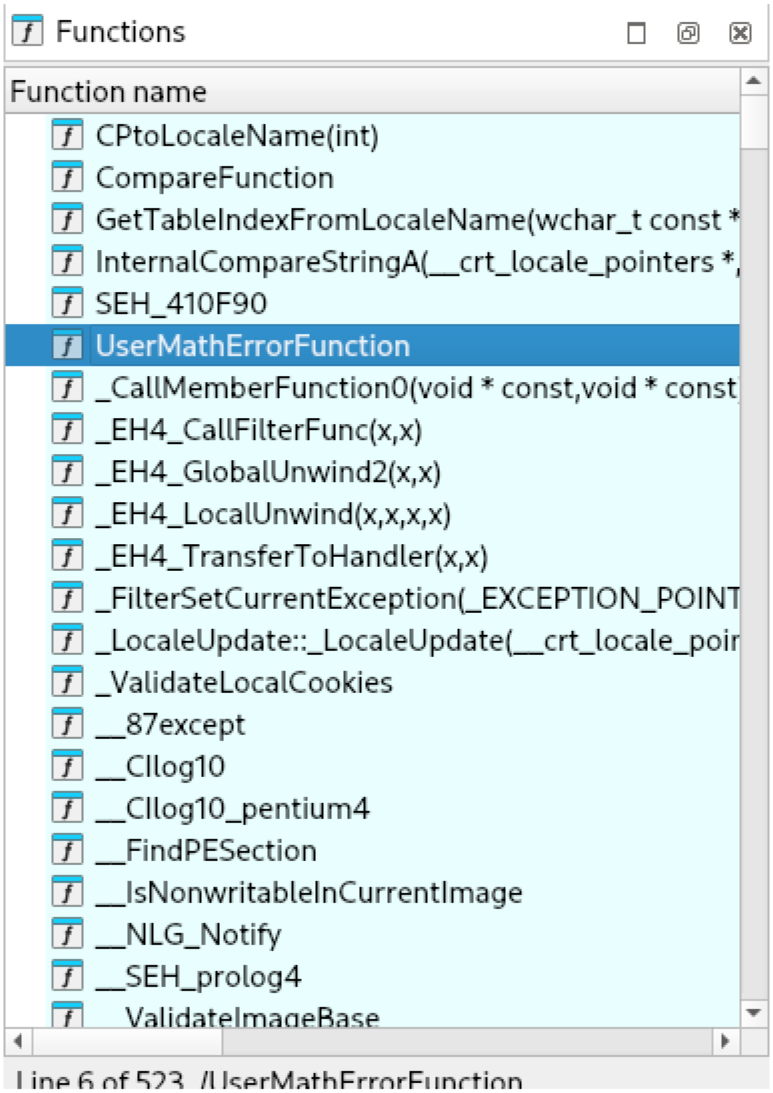
Submitted to: Mr. Dharmesh Dave and Mr. Parag Rughani

Submitted by: Disha Sharma (2401030020014)

Submission Date: 03/04/2025

INDEX

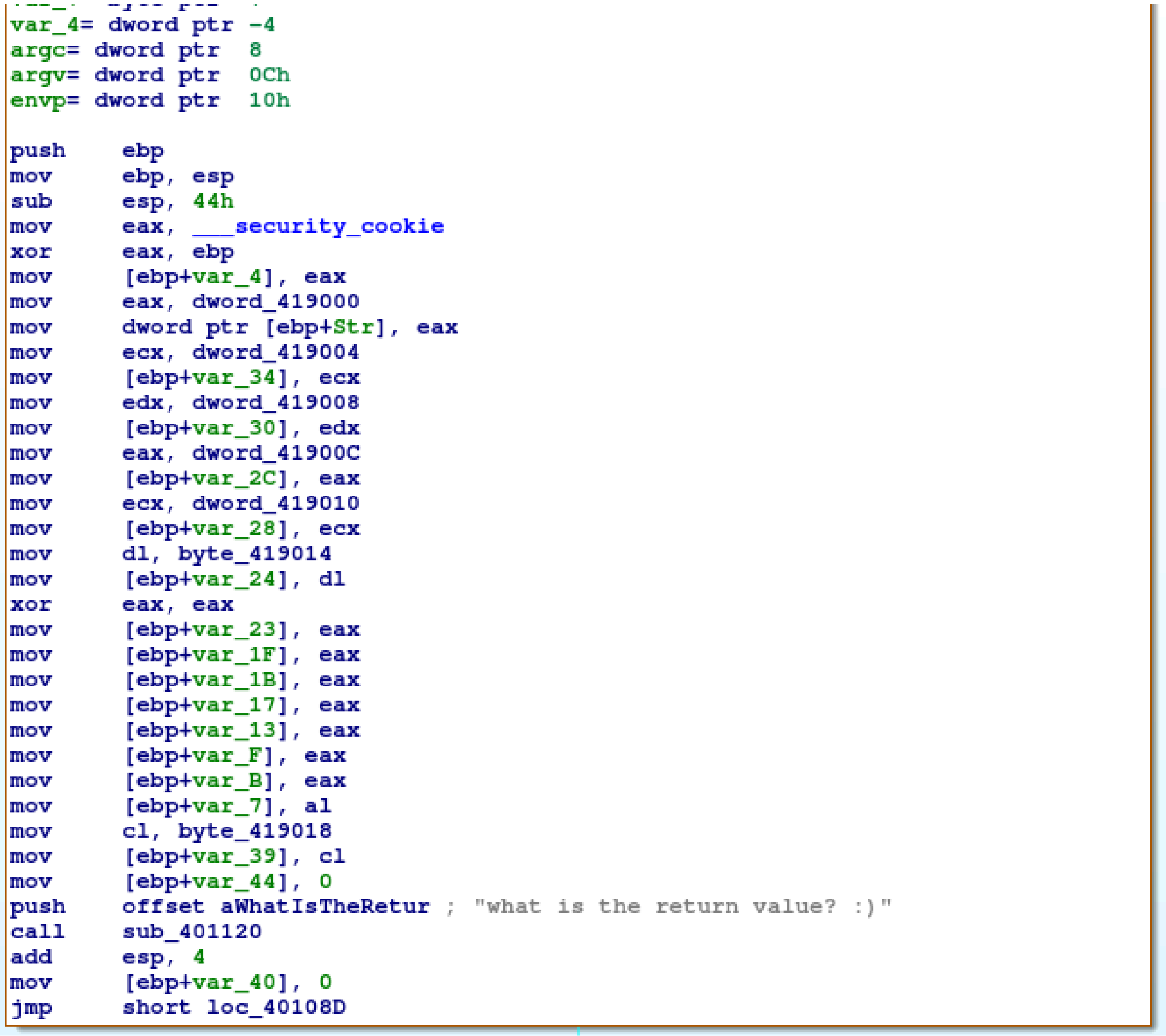
1. How many UDFs are there?



```
CPtoLocaleName(int)
CompareFunction
GetTableIndexFromLocaleName(wchar_t const *
InternalCompareStringA(__crt_locale_pointers *,
SEH_410F90
UserMathErrorFunction
_CallMemberFunction0(void * const,void * const
_EH4_CallFilterFunc(x,x)
_EH4_GlobalUnwind2(x,x)
_EH4_LocalUnwind(x,x,x,x)
_EH4_TransferToHandler(x,x)
_FilterSetCurrentException(_EXCEPTION_POINT
_LocaleUpdate::_LocaleUpdate(__crt_locale_poir
_ValidateLocalCookies
__87except
__CIlog10
__CIlog10_pentium4
__FindPESection
__IsNonwritableInCurrentImage
__NLG_Notify
__SEH_prolog4
__ValidateImageBase
Line 6 of 523, /UserMathErrorFunction
```

One UDF - UserMathErrorFunction can be identified from the functions window.

2. How many variables are there?

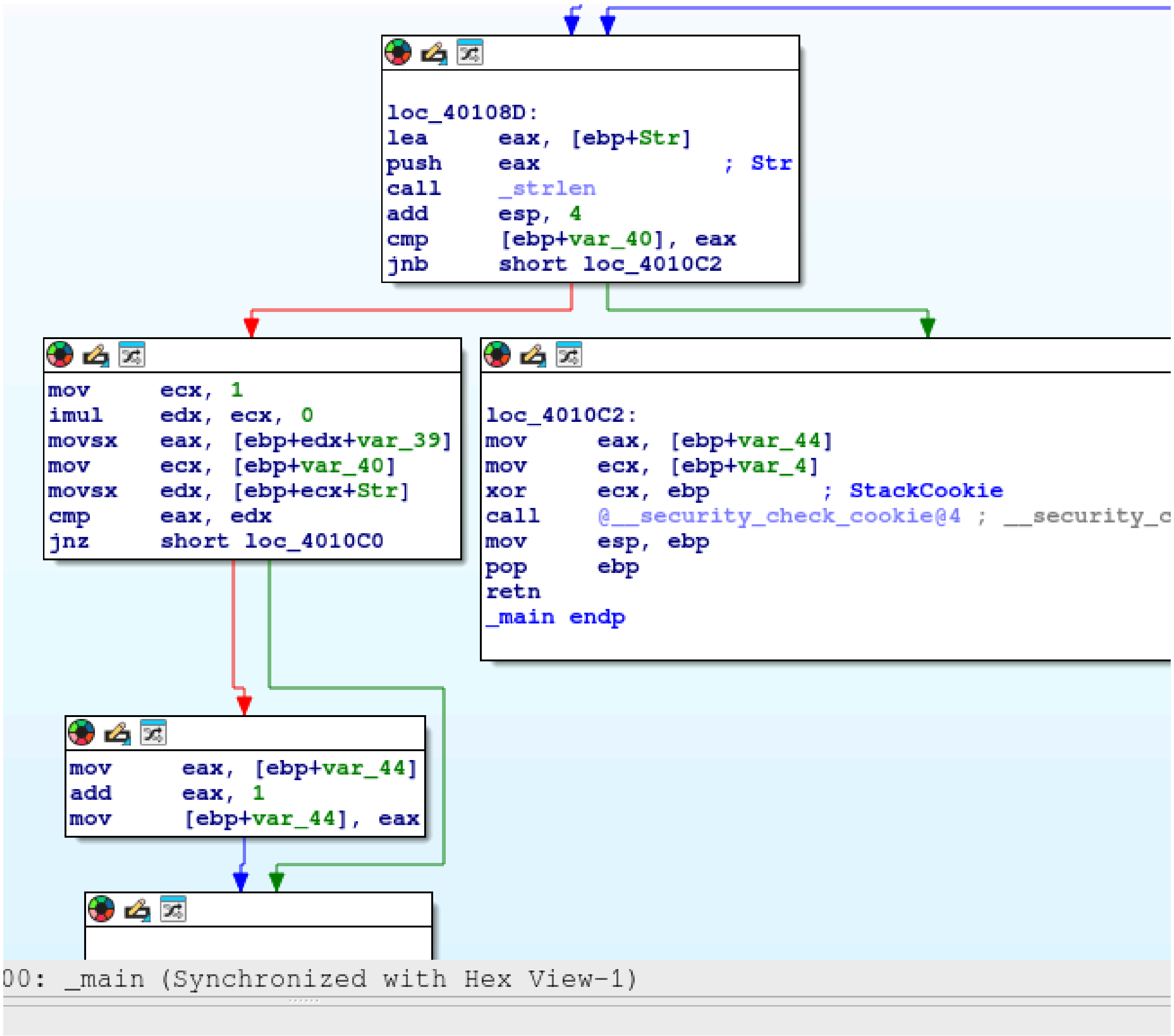


```
var_4= dword ptr -4
argc= dword ptr  8
argv= dword ptr  0Ch
envp= dword ptr  10h

push    ebp
mov     ebp, esp
sub     esp, 44h
mov     eax, ___security_cookie
xor     eax, ebp
mov     [ebp+var_4], eax
mov     eax, dword_419000
mov     dword ptr [ebp+Str], eax
mov     ecx, dword_419004
mov     [ebp+var_34], ecx
mov     edx, dword_419008
mov     [ebp+var_30], edx
mov     eax, dword_41900C
mov     [ebp+var_2C], eax
mov     ecx, dword_419010
mov     [ebp+var_28], ecx
mov     dl, byte_419014
mov     [ebp+var_24], dl
xor     eax, eax
mov     [ebp+var_23], eax
mov     [ebp+var_1F], eax
mov     [ebp+var_1B], eax
mov     [ebp+var_17], eax
mov     [ebp+var_13], eax
mov     [ebp+var_F], eax
mov     [ebp+var_B], eax
mov     [ebp+var_7], al
mov     cl, byte_419018
mov     [ebp+var_39], cl
mov     [ebp+var_44], 0
push    offset aWhatIsTheRetur ; "what is the return value? :)"
call    sub_401120
add     esp, 4
mov     [ebp+var_40], 0
jmp     short loc_40108D
```

A total of 12 variables are noticed. Global variables are identified using memory addresses whereas local variables are identified using stack addresses.
Therefore, 7 global variables and 5 local variables have been identified.

3. Are there any conditional jumps



```
loc_40108D:
lea     eax, [ebp+Str]
push    eax             ; Str
call    _strlen
add     esp, 4
cmp     [ebp+var_40], eax
jnb     short loc_4010C2
```

```
mov     ecx, 1
imul    edx, ecx, 0
movsx   eax, [ebp+edx+var_39]
mov     ecx, [ebp+var_40]
movsx   edx, [ebp+ecx+Str]
cmp     eax, edx
jnz     short loc_4010C0
```

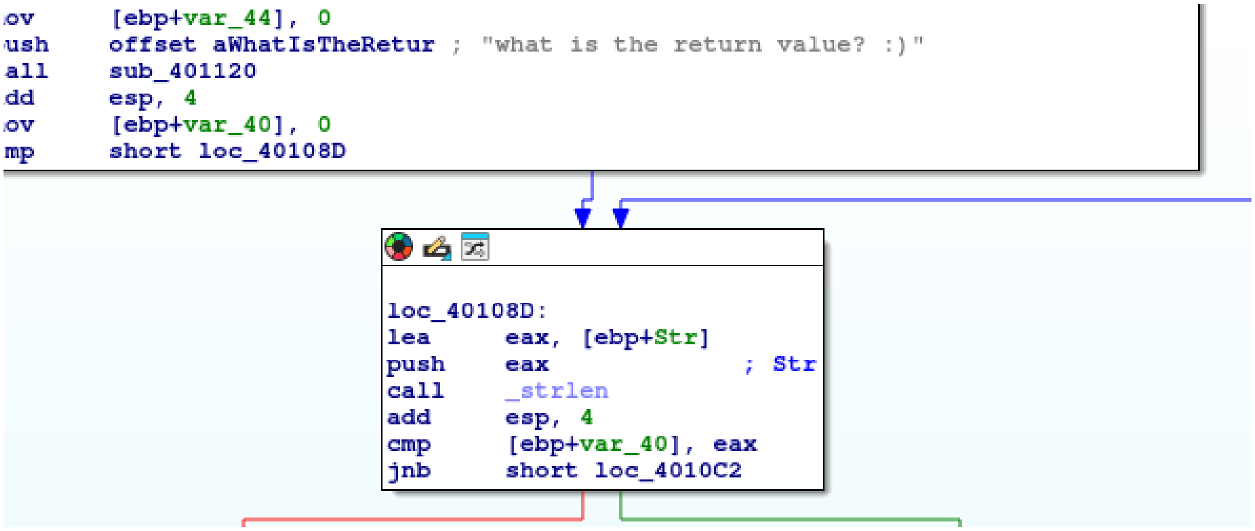
```
loc_4010C2:
mov     eax, [ebp+var_44]
mov     ecx, [ebp+var_4]
xor     ecx, ebp        ; StackCookie
call    @__security_check_cookie@4 ; __security_c
mov     esp, ebp
pop     ebp
retn
_main endp
```

```
mov     eax, [ebp+var_44]
add     eax, 1
mov     [ebp+var_44], eax
```

```
00: _main (Synchronized with Hex View-1)
```

Yes, there is one conditional jump denoted by jnz command as well as red and green arrows. The red arrow suggests if a conditional jump is not taken while the green arrow suggests if a conditional jump has been taken.

4. Are there any unconditional jumps?

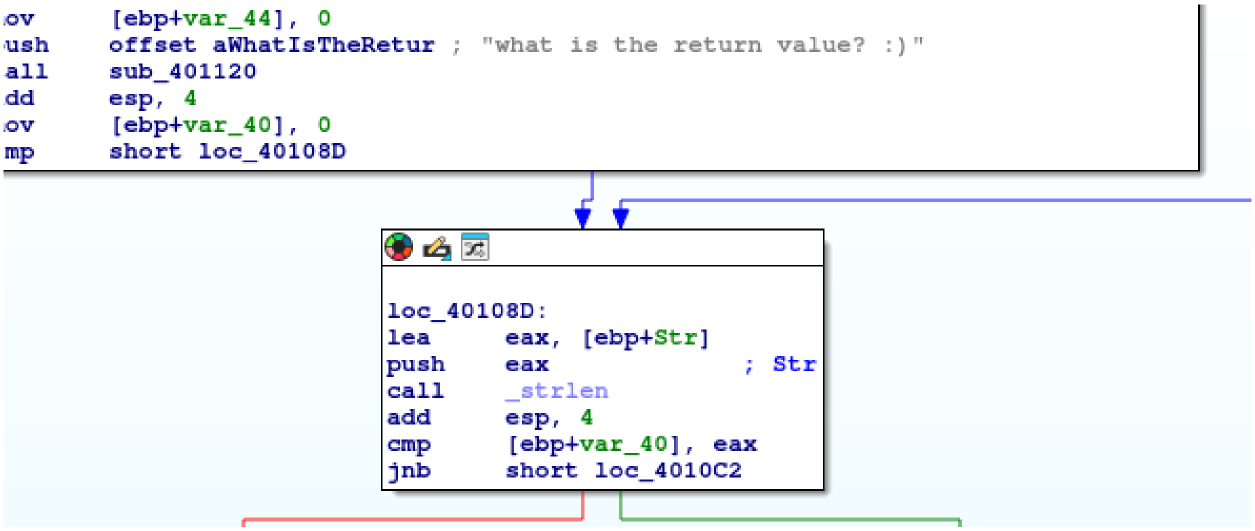


```
ov      [ebp+var_44], 0
ush     offset aWhatIsTheRetur ; "what is the return value? :)"
all     sub_401120
dd      esp, 4
ov      [ebp+var_40], 0
mp      short loc_40108D
```

```
loc_40108D:
lea     eax, [ebp+Str]
push    eax                     ; Str
call    _strlen
add     esp, 4
cmp     [ebp+var_40], eax
jnb     short loc_4010C2
```

Yes, there is one unconditional jump denoted by the command jmp and the blue arrow facing downwards.

5. Are there any loops?



```
ov      [ebp+var_44], 0
ush     offset aWhatIsTheRetur ; "what is the return value? :)"
all     sub_401120
dd      esp, 4
ov      [ebp+var_40], 0
mp      short loc_40108D
```

```
loc_40108D:
lea     eax, [ebp+Str]
push    eax             ; Str
call    _strlen
add     esp, 4
cmp     [ebp+var_40], eax
jnb     short loc_4010C2
```

Yes there is one loop indicated by the blue arrow facing upwards