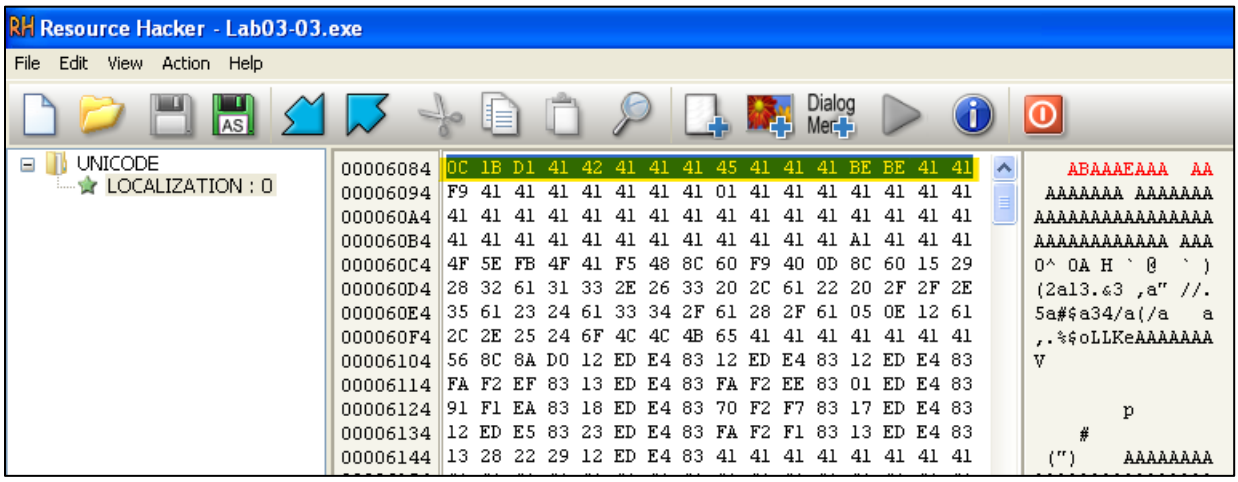
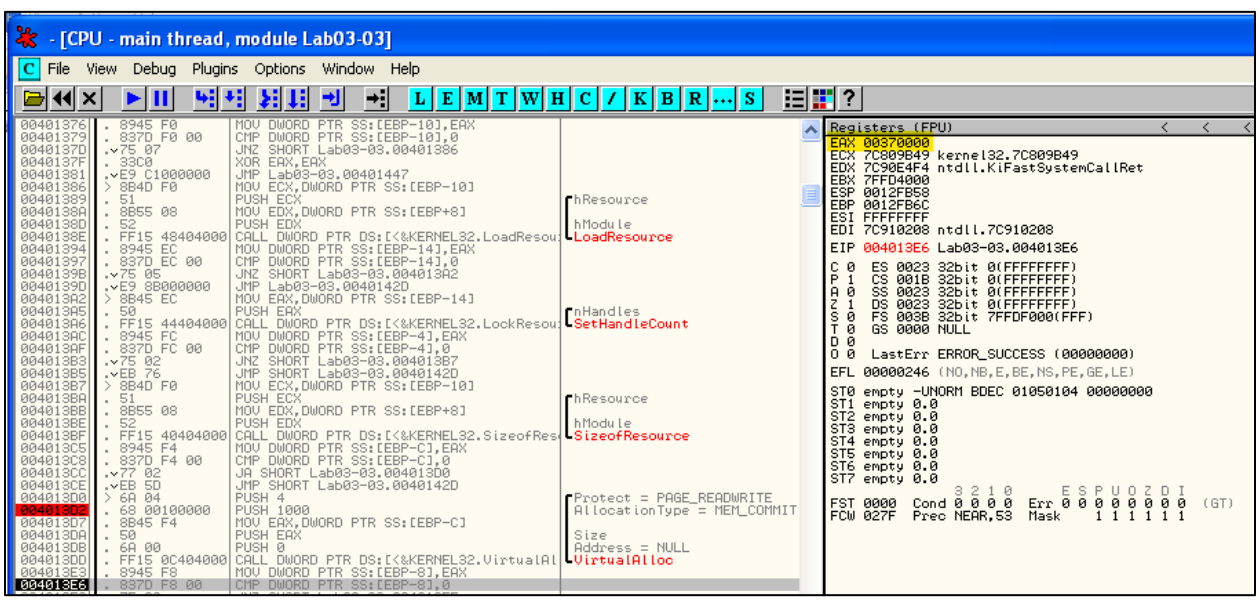
1. Use ResourceHacker to inspect the resources of Lab03-03.exe. What is the name of the resource? What are the first 16 bytes in the resource? Attach a screenshot that shows more details.

Ans. The name of the resource is Localization. The first 16 bytes are highlighted in the screenshot below-



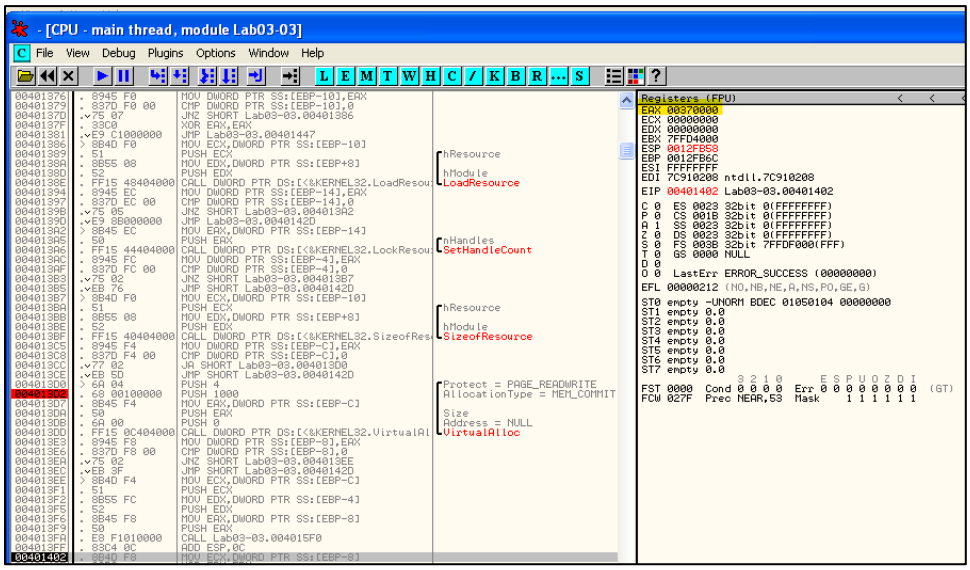
2. When execution reaches instruction 004013E3, what is the value of EAX? Hint: EAX holds the address of a memory buffer.

Ans. When the execution reaches 004013E3, the value of EAX register is 00370000.



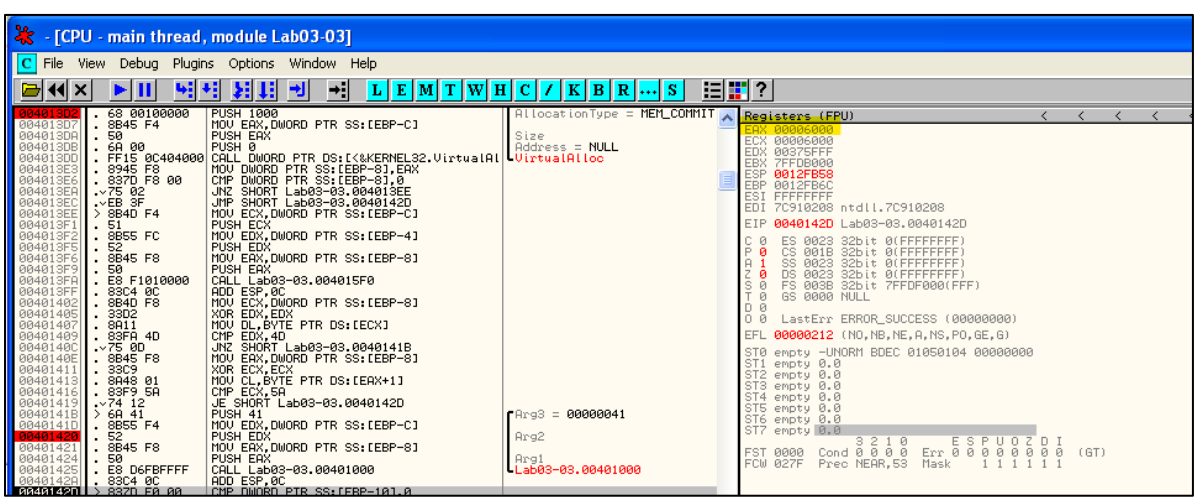
3. When execution reaches instruction 004013FF, what is the content of the memory buffer mentioned in Question 2? Attach a screenshot with more details. When you compare the content of the memory buffer with the screenshot you got in Question 1, what do you think function 004015F0 does?

Ans: When execution reaches instruction 004013FF, the content of the memory buffer mentioned in Question 2 is 00370000.



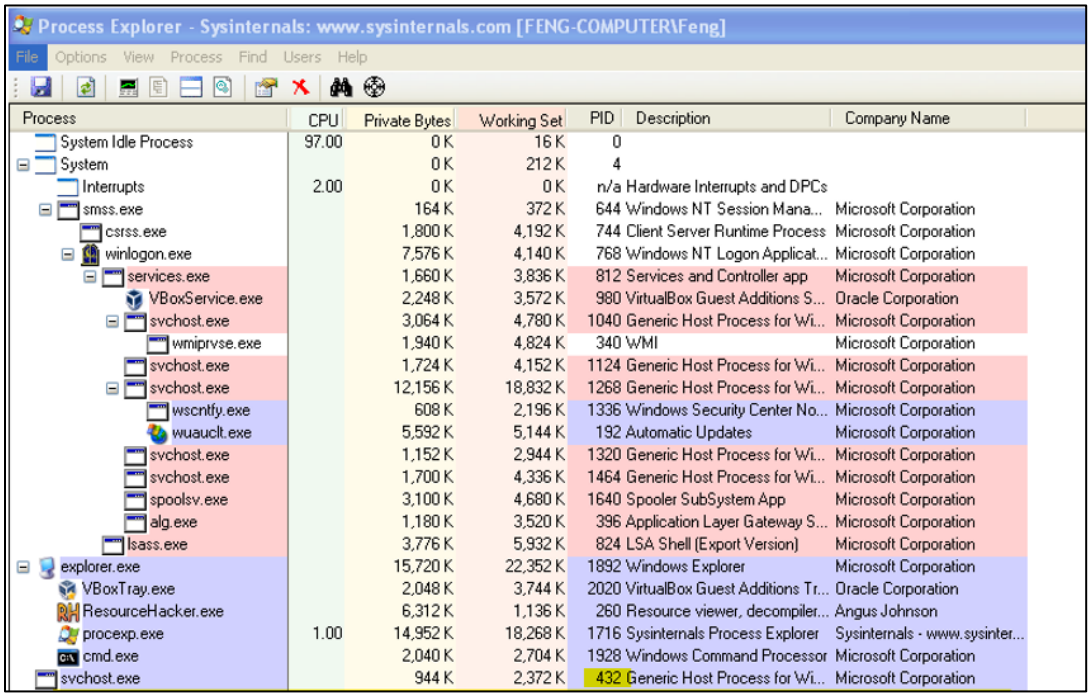
4. When execution reaches instruction 0040142A, what is the content of the above memory buffer? Attach a screenshot with more details. Does the content of this buffer change compared with its content in Question 3?

Ans. When execution reaches instruction 0040142A, the content of the above memory buffer is 00006000. Yes, the content of this memory buffer changed from the value in question 3.



5. Use Process Explorer to find the process ID of svchost.exe created by Lab03-03.exe. Click the “Strings” tab, attach two screenshots: one for “Image” and the other for “Memory.”

Ans. The process ID of svchost.exe was found to be 432.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	97.00	0 K	16 K	0		
System		0 K	212 K	4		
Interrupts	2.00	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		164 K	372 K	644	Windows NT Session Mana...	Microsoft Corporation
csrss.exe		1,800 K	4,192 K	744	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		7,576 K	4,140 K	768	Windows NT Logon Applicat...	Microsoft Corporation
services.exe		1,660 K	3,836 K	812	Services and Controller app	Microsoft Corporation
VBoxService.exe		2,248 K	3,572 K	980	VirtualBox Guest Additions S...	Oracle Corporation
svchost.exe		3,064 K	4,780 K	1040	Generic Host Process for Wi...	Microsoft Corporation
wmiprvse.exe		1,940 K	4,824 K	340	WMI	Microsoft Corporation
svchost.exe		1,724 K	4,152 K	1124	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		12,156 K	18,832 K	1268	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		608 K	2,196 K	1336	Windows Security Center No...	Microsoft Corporation
wuauclt.exe		5,592 K	5,144 K	192	Automatic Updates	Microsoft Corporation
svchost.exe		1,152 K	2,944 K	1320	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,700 K	4,336 K	1464	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe		3,100 K	4,680 K	1640	Spooler SubSystem App	Microsoft Corporation
alg.exe		1,180 K	3,520 K	396	Application Layer Gateway S...	Microsoft Corporation
lsass.exe		3,776 K	5,932 K	824	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe		15,720 K	22,352 K	1892	Windows Explorer	Microsoft Corporation
VBoxTray.exe		2,048 K	3,744 K	2020	VirtualBox Guest Additions Tr...	Oracle Corporation
ResourceHacker.exe		6,312 K	1,136 K	260	Resource viewer, decompiler...	Angus Johnson
procexp.exe	1.00	14,952 K	18,268 K	1716	Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe		2,040 K	2,704 K	1928	Windows Command Processor	Microsoft Corporation
svchost.exe		944 K	2,372 K	432	Generic Host Process for Wi...	Microsoft Corporation

In the following page, screenshot of ‘Strings’ tab is attached-

Image Tab

svchost.exe:432 Properties

Image | Performance | Performance Graph | Disk and Network | Threads | TCP

Printable strings found in the scan:

```
Parameters
System\CurrentControlSet\Services
nServiceMain
ServiceDll
ServiceDllUnloadOnStop
eventlog
ncacn_np
\PIPE\
DefaultRpcStackSize
AuthenticationCapabilities
ImpersonationLevel
AuthenticationLevel
CoInitializeSecurityParam
Software\Microsoft\Windows NT\CurrentVersion\Svchost
\Registry\Machine\System\CurrentControlSet\Control\SecurePipeServers\
VS_VERSION_INFO
StringFileInfo
CompanyName
Microsoft Corporation
FileDescription
Generic Host Process for Win32 Services
FileVersion
5.1.2600.5512 (xpsp.080413-2111)
InternalName
svchost.exe
LegalCopyright
Microsoft Corporation. All rights reserved.
OriginalFilename
svchost.exe
ProductName
Microsoft
Windows
Operating System
ProductVersion
VarFileInfo
Translation
!This program cannot be run in DOS mode.
5Rich
.text
`.data
.rsrc
ADVAPI32.dll
KERNEL32.dll
NTDLL.DLL
RPCRT4.dll
QQV
PWj
WQP
SvchostPushServiceGlobals
ServiceMain
```

(•) Image ( ) Memory

svchost.exe:432 Properties

Image | Performance | Performance Graph | Disk and Network | Threads | TCP/IP | Security | Environment | Strings

Printable strings found in the scan:

```
ServiceMain
Y@PVPVh
VWh@@
SVW
SVW3
PSh
tQj
VVVV
t6PV
t!VV
QSV3
ucj
jwX
Wht@
jdj
QQSVWd
QSV
u-SS
uLV
FFf
!FFf
F$Pj
f9>t f
FFf9>u
tof
tSf
FFf9>u
ShP$
VWh
QRPh
uRS
taj
u:Vj
VVj
PSj
PSSj
PSSj
unj
GPW
FFf
FFf
PWWj
WWj
SVW
HHt
jwX]
SVW
QRPhh2
VWj
VWj
```

Image Memory

svchost.exe:432 Properties

Image | Performance | Performance Graph | Disk and Network | Threads | TCP/IP | Security | Environment | Strings

Printable strings found in the scan:

```
NETAPI32.dll
ole32.dll
Netbios
CoInitializeEx
CoInitializeSecurity
ADVAPI32.dll
KERNEL32.dll
ntdll.dll
RPCRT4.dll
RegQueryValueExW
SetSecurityDescriptorDacl
SetEntriesInAclW
SetSecurityDescriptorGroup
SetSecurityDescriptorOwner
InitializeSecurityDescriptor
GetTokenInformation
OpenProcessToken
OpenThreadToken
SetServiceStatus
RegisterServiceCtrlHandlerW
RegCloseKey
RegOpenKeyExW
StartServiceCtrlDispatcherW
HeapFree
GetLastError
WideCharToMultiByte
lstrlenW
LocalFree
GetCurrentProcess
GetCurrentThread
GetProcAddress
LoadLibraryExW
LeaveCriticalSection
HeapAlloc
EnterCriticalSection
LCMapStringW
FreeLibrary
lstrcpyW
ExpandEnvironmentStringsW
lstrcmpiW
ExitProcess
GetCommandLineW
InitializeCriticalSection
GetProcessHeap
SetErrorMode
SetUnhandledExceptionFilter
RegisterWaitForSingleObject
InterlockedCompareExchange
LoadLibraryA
QueryPerformanceCounter
```

(•) Image ( ) Memory

svchost.exe:432 Properties

Image | Performance | Performance Graph | Disk and Network | Threads | TCP/IP | Security | Environment | Strings

Printable strings found in the scan:

```
GetCommandLineW
InitializeCriticalSection
GetProcessHeap
SetErrorMode
SetUnhandledExceptionFilter
RegisterWaitForSingleObject
InterlockedCompareExchange
LoadLibraryA
QueryPerformanceCounter
GetTickCount
GetCurrentThreadId
GetCurrentProcessId
GetSystemTimeAsFileTime
TerminateProcess
UnhandledExceptionFilter
LocalAlloc
lstrcmpW
DelayLoadFailureHook
NtQuerySecurityObject
RtlFreeHeap
NtOpenKey
wcscat
wcscpy
RtlAllocateHeap
RtlCompareUnicodeString
RtlInitUnicodeString
RtlInitializeSid
RtlLengthRequiredSid
RtlSubAuthoritySid
NtClose
RtlSubAuthorityCountSid
RtlGetDaclSecurityDescriptor
RtlQueryInformationAcl
RtlGetAce
RtlImageNtHeader
wcslen
RtlUnhandledExceptionFilter
RtlCopySid
RpcServerUnregisterIfEx
RpcMgmtWaitServerListen
RpcMgmtSetServerStackSize
RpcServerUnregisterIf
RpcServerListen
RpcServerUseProtseqEpW
RpcServerRegisterIf
I_RpcMapWin32Status
RpcMgmtStopServerListening
RSDS
svchost.pdb
```

(•) Image ( ) Memory

Memory Tab

svchost.exe:432 Properties

Image | Performance | Performance Graph | Disk and Network | Threads | TCP/IP | Security | Environment | Strings

Printable strings found in the scan:

```
!!!!
!This program cannot be run in DOS mode.
RichS
.text
`.rdata
@.data
hPS@
@hTP@
hPW@
hPW@
hPS@
toj
PhPW@
PhPW@
hPW@
hPS@
htP@
hxP@
Glu
GJu
tzVS
Glt%
t/Ku
GKu
SVW
YYh P@
VWu
t9UW
QQS3
VWu
PSSW
PVW
SS@SSPVSS
t#SSUP
t$$VSS
UWV
DSUVWh
SVWUj
SVW
t.;t$$t(
VC20XC00U
SVWU
tEVU
SVW
UAA
Wj@Y3
t7SW
VPj
VPV
VPh
```

Image Memory

svchost.exe:432 Properties

Image | Performance | Performance Graph | Disk and Network | Threads | TCP/IP | Security | Environment | Strings

Printable strings found in the scan:

```
pD#U
SVW
NCu
VWuBh
tPh
SVW
uFWWj
'WWSh
E WW
tfS
tMWWS
WWu
VSh
SVW
PVh
WSV
B~k!C~
C~+wB~
runtime error
TLOSS error
SING error
DOMAIN error
- unable to initialize heap
- not enough space for lowio initialization
- not enough space for stdio initialization
- pure virtual function call
- not enough space for _onexit/atexit table
- unable to open console device
- unexpected heap error
- unexpected multithread lock error
- not enough space for thread data
abnormal program termination
- not enough space for environment
- not enough space for arguments
- floating point not loaded
Microsoft Visual C++ Runtime Library
Runtime Error!
Program:
<program name unknown>
GetLastActivePopup
GetActiveWindow
MessageBoxA
user32.dll
GetModuleHandleA
AllocConsole
CloseHandle
WriteFile
SetFilePointer
CreateFileA
KERNEL32.dll
```

○ Image ◉ Memory

svchost.exe:432 Properties

Image | Performance | Performance Graph | Disk and Network | Threads | TCP/IP | Security | Environment | Strings

Printable strings found in the scan:

```
KERNEL32.dll
UnhookWindowsHookEx
GetMessageA
SetWindowsHookExA
ShowWindow
FindWindowA
CallNextHookEx
GetWindowTextA
GetForegroundWindow
USER32.dll
GetCommandLineA
GetVersion
ExitProcess
TerminateProcess
GetCurrentProcess
UnhandledExceptionFilter
GetModuleFileNameA
FreeEnvironmentStringsA
FreeEnvironmentStringsW
WideCharToMultiByte
GetEnvironmentStrings
GetEnvironmentStringsW
SetHandleCount
GetStdHandle
GetFileType
GetStartupInfoA
HeapDestroy
HeapCreate
VirtualFree
HeapFree
RtlUnwind
HeapAlloc
GetCPInfo
GetACP
GetOEMCP
VirtualAlloc
HeapReAlloc
GetProcAddress
LoadLibraryA
MultiByteToWideChar
LCMapStringA
LCMapStringW
GetStringTypeA
GetStringTypeW
[Window:
ConsoleWindowClass
practicalmalwareanalysis.log
[SHIFT]
[ENTER]
[BACKSPACE]
```

○ Image ◉ Memory

svchost.exe:432 Properties

Image | Performance | Performance Graph | Disk and Network | Threads | TCP/IP | Security | Environment | Strings

Printable strings found in the scan:

```
GetCurrentProcess
UnhandledExceptionFilter
GetModuleFileNameA
FreeEnvironmentStringsA
FreeEnvironmentStringsW
WideCharToMultiByte
GetEnvironmentStrings
GetEnvironmentStringsW
SetHandleCount
GetStdHandle
GetFileType
GetStartupInfoA
HeapDestroy
HeapCreate
VirtualFree
HeapFree
RtlUnwind
HeapAlloc
GetCPInfo
GetACP
GetOEMCP
VirtualAlloc
HeapReAlloc
GetProcAddress
LoadLibraryA
MultiByteToWideChar
LCMapStringA
LCMapStringW
GetStringTypeA
GetStringTypeW
[Window:
ConsoleWindowClass
practicalmalwareanalysis.log
[SHIFT]
[ENTER]
[BACKSPACE]
BACKSPACE
[TAB]
[CTRL]
[DEL]
[CAPS LOCK]
[CAPS LOCK]
Command Prompt
Command Prompt
n to follow
le Lab03-03]
C:\WINDOWS\system32\svchost.exe
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

○ Image ◉ Memory

Launch OllyDbg 1.10 and attach it to the malicious svchost.exe process. If you will see a pop-up window with some error message, just ignore it and continue. Set a breakpoint at 00401226.

6. When execution reaches this breakpoint, press F7, and collect at least three different target addresses (i.e., trigger this breakpoint at least three times). What are the code at those target addresses doing?

Ans. To trigger the breakpoint for 3 times, below method was used

<u>Step 1:</u> After finding the PID from process explorer, OllyDbg was launched and malicious svc.exe process was attached using its PID

<u>Step 2:</u> Once the process was attached, a breakpoint was set at 00401226.

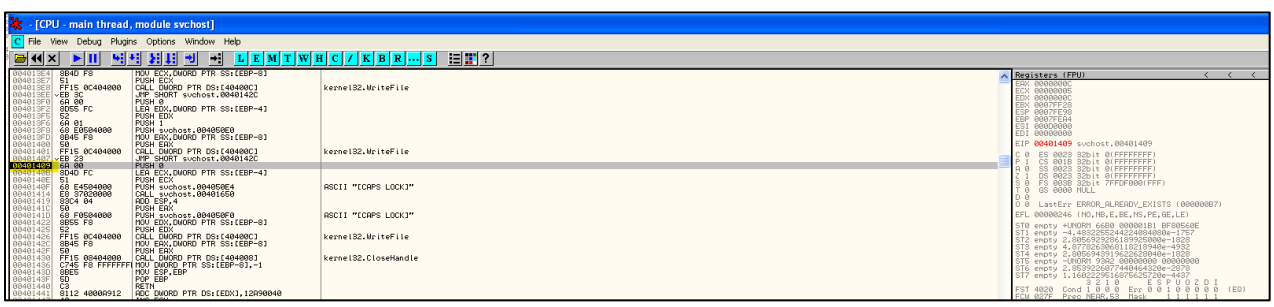
<u>Step 3:</u> After setting the breakpoint, the code was run. Another window was opened, for eg: file explorer, and then Capslock key was pressed.

<u>Step 4:</u> Going back to OllyDbg window F7 key was pressed, which jumped to the address 00401409.

Step 3 and 4 were repeated with 'Enter' and 'Backspace' keys to trigger the break thrice. Below is the screenshot of the target address.

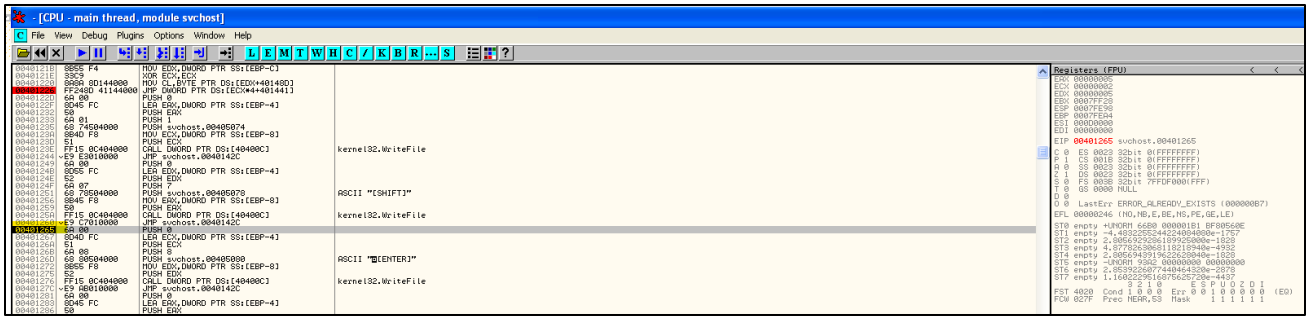
Key Pressed- Capslock, Target Address- 00401409

The code here is writing 'CAPS LOCK' to a file using kernel32.WriteFile. Its recording the CapsLock keystroke.



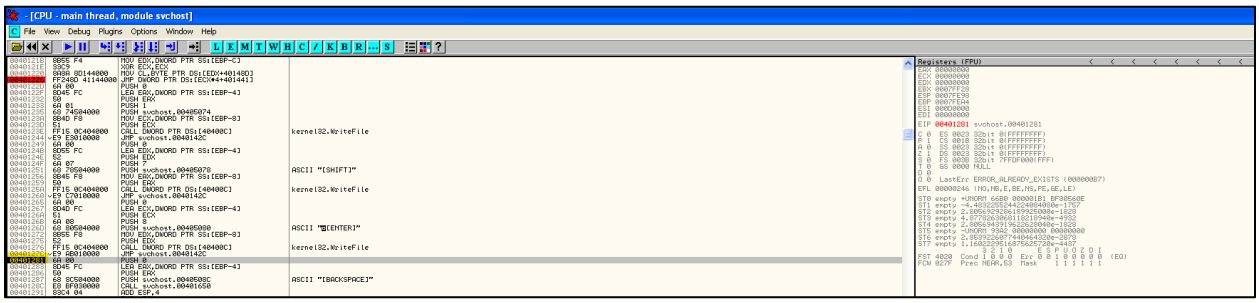
Key Pressed- Enter, Target Address- 00401265

The code here is writing 'Enter' to a file using kernel32.WriteFile. Its recording the Enter keystroke.



Key pressed- Backspace, Target Address- 00401281

The code here is writing ‘Backspace’ to a file using kernel32.WriteFile. Its recording the Backspace keystroke.



7. Specifically, you can leave svchost.exe running and press TAB in another window, which should trigger the breakpoint at 00401226. What is the next address? What is the code there doing?

Ans: The next address is 004012A9. The code here is writing ‘Tab’ to a file using kernel32.WriteFile. Its recording the Tab keystroke.