11: Using OllyDbg to Analyze Lab09-01.exe (Part 1) (15 pts.)

What You Need

- A Windows machine, real or virtual. I tried this on Windows 7, 10, and Server 2008 and it works on them all.

Summary

This is just the beginning of Lab09-01, performing the first run-through.

This analysis shows that if the code is executed as it is, it checks for a certain registry key, and if that key is absent, it deletes itself.

Get OllyDbg 1.10

Get OllyDbg 1.10 here:

http://www.ollydbg.de/download.htm

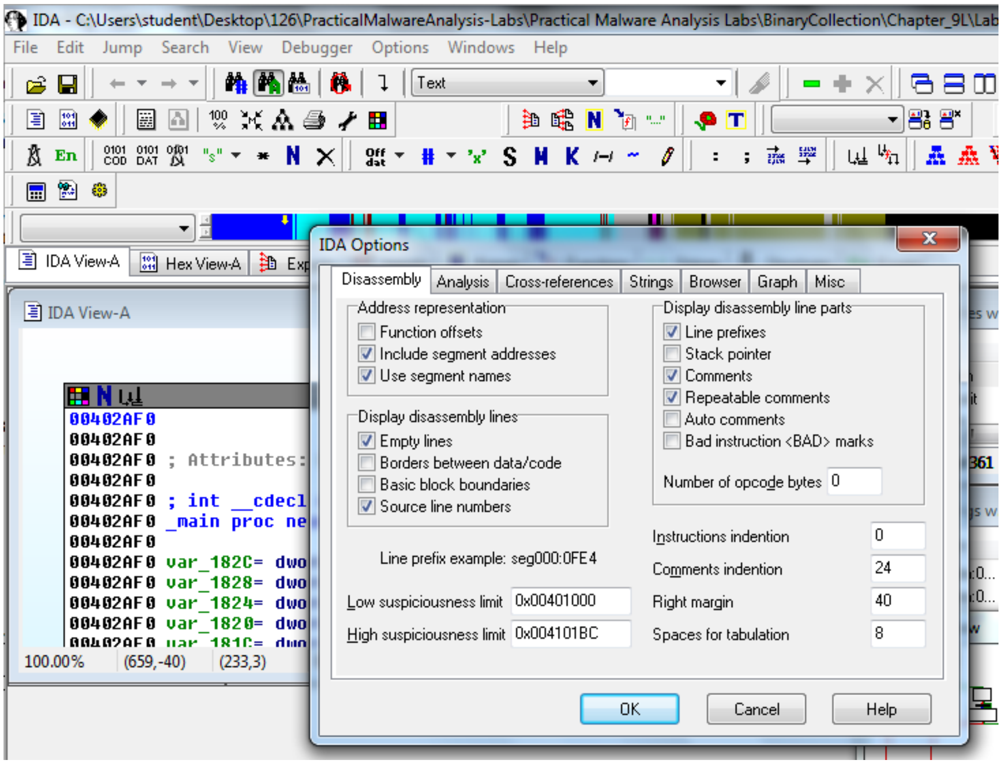
Don't waste your time on OllyDbg 2.00 or 2.01. They are both broken.

Finding the Main Entry Point

Open the Lab09-01.exe file in IDA Pro.

Click **Options**, **General**. Check "**Line Prefixes**", as shown below.

Click **OK**.


IDA - C:\Users\student\Desktop\126\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\BinaryCollection\Chapter_9L\Lab
File Edit Jump Search View Debugger Options Windows Help
Text
IDA View-A
Hex View-A
Exp
IDA View-A
100.00% (659,-40) (233,3)
IDA Options
Disassembly
Analysis
Cross-references
Strings
Browser
Graph
Misc
OK
Cancel
Help

```
00402AF0
00402AF0
00402AF0 ; Attributes:
00402AF0
00402AF0 ; int __cdecl
00402AF0 _main proc ne
00402AF0
00402AF0 var_182C= dwo
00402AF0 var_1828= dwo
00402AF0 var_1824= dwo
00402AF0 var_1820= dwo
00402AF0 var_181C= dwo
```

Address representation
☐ Function offsets
☑ Include segment addresses
☑ Use segment names

Display disassembly lines
☑ Empty lines
☐ Borders between data/code
☐ Basic block boundaries
☑ Source line numbers

Line prefix example: seg000:0FE4

Low suspiciousness limit 0x00401000
High suspiciousness limit 0x004101BC

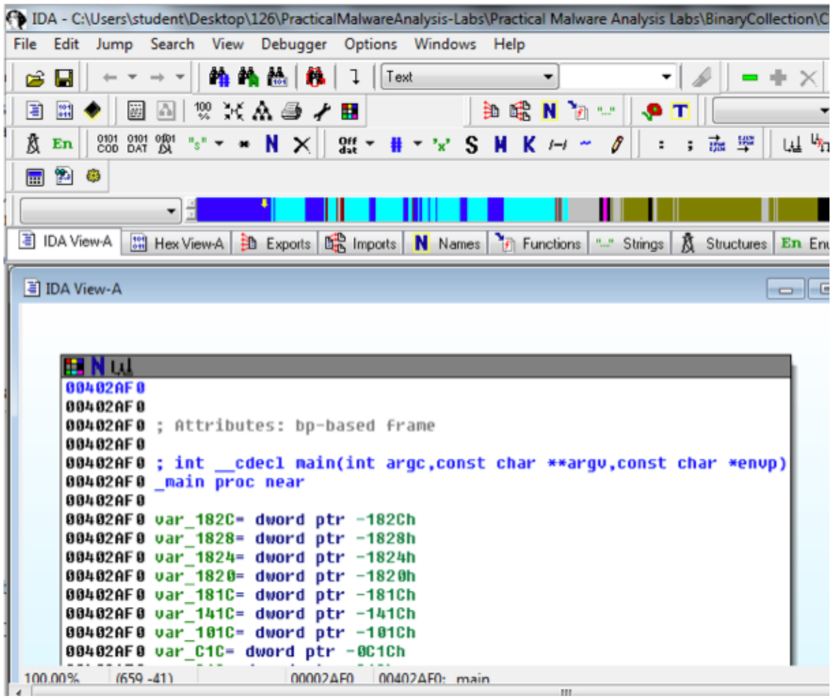
Display disassembly line parts
☑ Line prefixes
☐ Stack pointer
☑ Comments
☑ Repeatable comments
☐ Auto comments
☐ Bad instruction <BAD> marks

Number of opcode bytes 0

Instructions indention 0
Comments indention 24
Right margin 40
Spaces for tabulation 8

Click **Windows**, "**Reset Desktop**".

IDA Pro shows that main starts at 0x402AF0, as shown below:


IDA - C:\Users\student\Desktop\126\PracticalMalwareAnalysis-Labs\Practical Malware Analysis Labs\BinaryCollection\C
File Edit Jump Search View Debugger Options Windows Help
Text
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
En

```
00402AF0
00402AF0
00402AF0 ; Attributes: bp-based frame
00402AF0
00402AF0 ; int __cdecl main(int argc,const char **argv,const char *envp)
00402AF0 _main proc near
00402AF0
00402AF0 var_182C= dword ptr -182Ch
00402AF0 var_1828= dword ptr -1828h
00402AF0 var_1824= dword ptr -1824h
00402AF0 var_1820= dword ptr -1820h
00402AF0 var_181C= dword ptr -181Ch
00402AF0 var_141C= dword ptr -141Ch
00402AF0 var_101C= dword ptr -101Ch
00402AF0 var_C1C= dword ptr -0C1Ch
```

```
100.00%   (659 -41)   00002AF0   00402AF0: main
```

Saving the Screen Image

Make sure you can see the **0x402AF0** address, as shown above.

On your keyboard, press the PrntScrn key.

Click **Start**, type in **PAINT**, and open Paint.

Press **Ctrl+V** to paste in the image of your desktop.

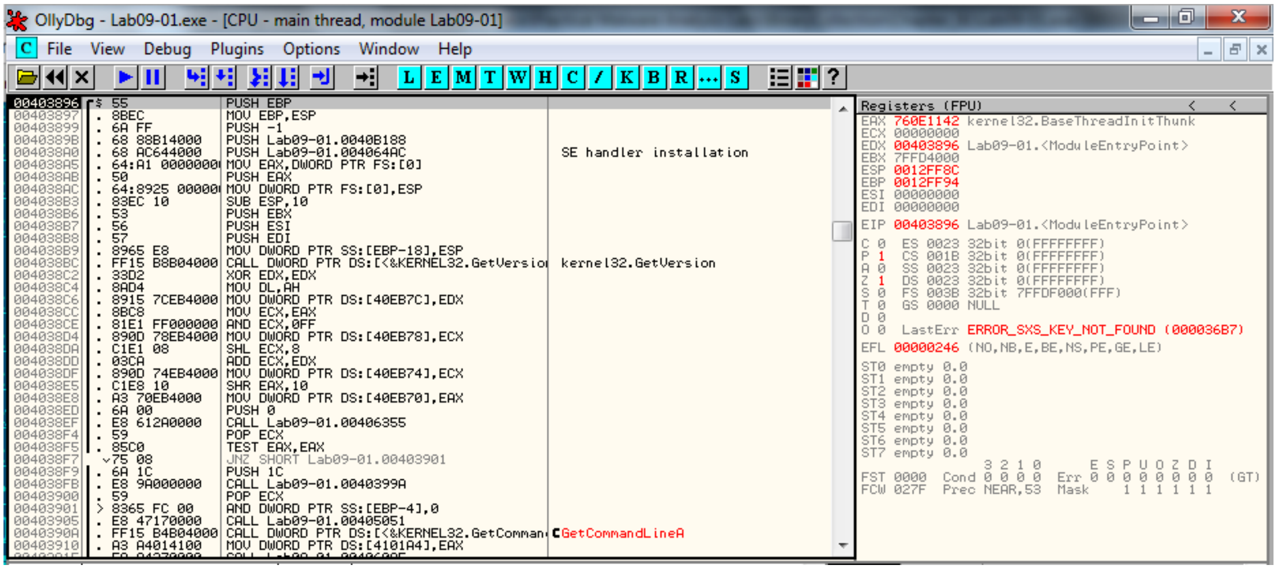
YOU MUST SUBMIT WHOLE-DESKTOP IMAGES TO GET FULL CREDIT.

Save the image with a filename of "**Proj 11a from YOUR NAME**".

Using OllyDbg to Walk Through Quickly

Open Lab09-01.exe in OllyDbg.

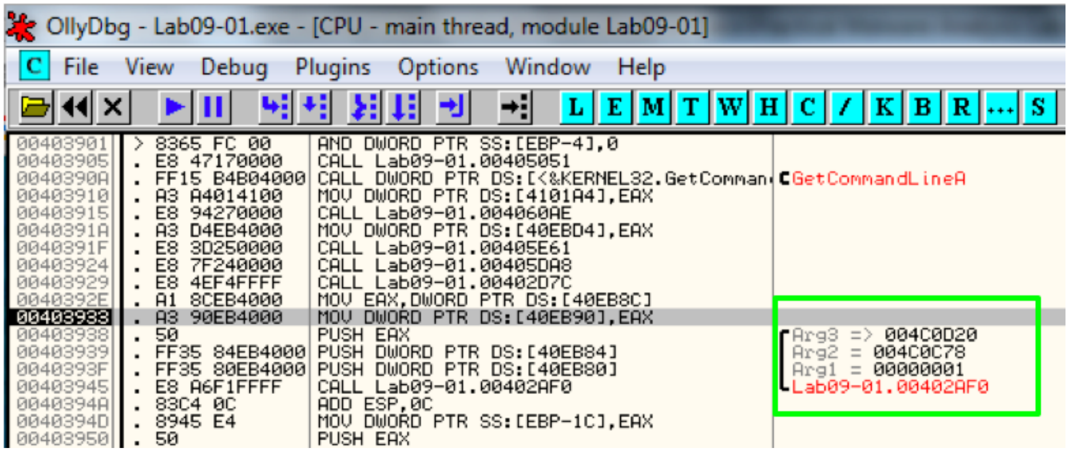
You start at a preamble, which comes before the entry point you saw in IDA Pro, as shown below.


OllyDbg - Lab09-01.exe - [CPU - main thread, module Lab09-01]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S ?

```
00403896 $ 55            PUSH EBP
00403897 . 8BEC          MOV EBP,ESP
00403899 . 6A FF         PUSH -1
0040389B . 68 88B14000   PUSH Lab09-01.0040B188
004038A0 . 68 AC644000   PUSH Lab09-01.004064AC                         SE handler installation
004038A5 . 64:A1 0000000 MOV EAX,DWORD PTR FS:[0]
004038AB . 50            PUSH EAX
004038AC . 64:8925 00000 MOV DWORD PTR FS:[0],ESP
004038B3 . 83EC 10       SUB ESP,10
004038B6 . 53            PUSH EBX
004038B7 . 56            PUSH ESI
004038B8 . 57            PUSH EDI
004038B9 . 8965 E8       MOV DWORD PTR SS:[EBP-18],ESP
004038BC . FF15 B8B04000 CALL DWORD PTR DS:[<&KERNEL32.GetVersio  kernel32.GetVersion
004038C2 . 33D2          XOR EDX,EDX
004038C4 . 8AD4          MOV DL,AH
004038C6 . 8915 7CEB4000 MOV DWORD PTR DS:[40EB7C],EDX
004038CC . 8BC8          MOV ECX,EAX
004038CE . 81E1 FF000000 AND ECX,0FF
004038D4 . 890D 78EB4000 MOV DWORD PTR DS:[40EB78],ECX
004038DA . C1E1 08       SHL ECX,8
004038DD . 03CA          ADD ECX,EDX
004038DF . 890D 74EB4000 MOV DWORD PTR DS:[40EB74],ECX
004038E5 . C1E8 10       SHR EAX,10
004038E8 . A3 70EB4000   MOV DWORD PTR DS:[40EB70],EAX
004038ED . 6A 00         PUSH 0
004038EF . E8 612A0000   CALL Lab09-01.00406355
004038F4 . 59            POP ECX
004038F5 . 85C0          TEST EAX,EAX
004038F7  v75 08         JNZ SHORT Lab09-01.00403901
004038F9 . 6A 1C         PUSH 1C
004038FB . E8 9A000000   CALL Lab09-01.0040399A
00403900 . 59            POP ECX
00403901 > 8365 FC 00    AND DWORD PTR SS:[EBP-4],0
00403905 . E8 47170000   CALL Lab09-01.00405051
0040390A . FF15 B4B04000 CALL DWORD PTR DS:[<&KERNEL32.GetComman  CGetCommandLineA
00403910 . A3 A4014100   MOV DWORD PTR DS:[4101A4],EAX
```

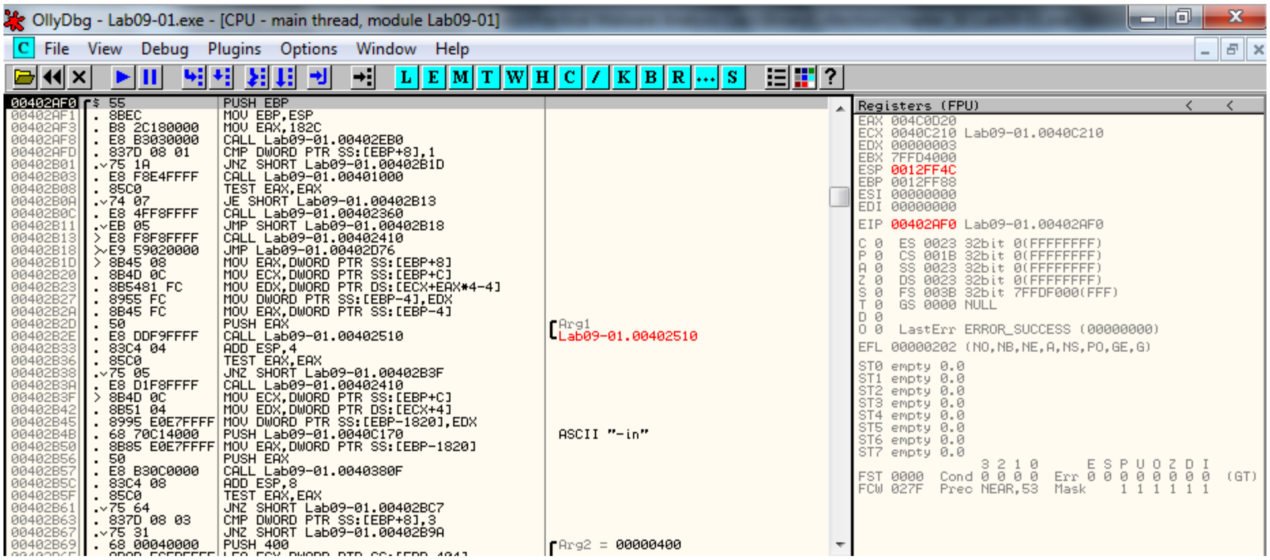
```
Registers (FPU)
EAX 760E1142 kernel32.BaseThreadInitThunk
ECX 00000000
EDX 00403896 Lab09-01.<ModuleEntryPoint>
EBX 7FFD4000
ESP 0012FF8C
EBP 0012FF94
ESI 00000000
EDI 00000000

EIP 00403896 Lab09-01.<ModuleEntryPoint>

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SXS_KEY_NOT_FOUND (000036B7)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

Press F8 forty times, to step over until address 0x403933. In the upper left pane of OllyDbg, scroll down a few lines to show the code that sets the arguments and calls main, as highlighted below.


OllyDbg - Lab09-01.exe - [CPU - main thread, module Lab09-01]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S

```
00403901  > 8365 FC 00      AND DWORD PTR SS:[EBP-4],0
00403905  . E8 47170000     CALL Lab09-01.00405051
0040390A  . FF15 B4B04000   CALL DWORD PTR DS:[<&KERNEL32.GetComman  GetCommandLineA
00403910  . A3 A4014100     MOV DWORD PTR DS:[4101A4],EAX
00403915  . E8 94270000     CALL Lab09-01.004060AE
0040391A  . A3 D4EB4000     MOV DWORD PTR DS:[40EBD4],EAX
0040391F  . E8 3D250000     CALL Lab09-01.00405E61
00403924  . E8 7F240000     CALL Lab09-01.00405DA8
00403929  . E8 4EF4FFFF     CALL Lab09-01.00402D7C
0040392E  . A1 8CEB4000     MOV EAX,DWORD PTR DS:[40EB8C]
00403933  . A3 90EB4000     MOV DWORD PTR DS:[40EB90],EAX
00403938  . 50              PUSH EAX                                 Arg3 => 004C0D20
00403939  . FF35 84EB4000   PUSH DWORD PTR DS:[40EB84]               Arg2 = 004C0C78
0040393F  . FF35 80EB4000   PUSH DWORD PTR DS:[40EB80]               Arg1 = 00000001
00403945  . E8 A6F1FFFF     CALL Lab09-01.00402AF0                   Lab09-01.00402AF0
0040394A  . 83C4 0C         ADD ESP,0C
0040394D  . 8945 E4         MOV DWORD PTR SS:[EBP-1C],EAX
00403950  . 50              PUSH EAX
```

Press F7 five times to load parameters and call main from 0x403945, showing a new section of code starting at 0x402AF0, as shown below.

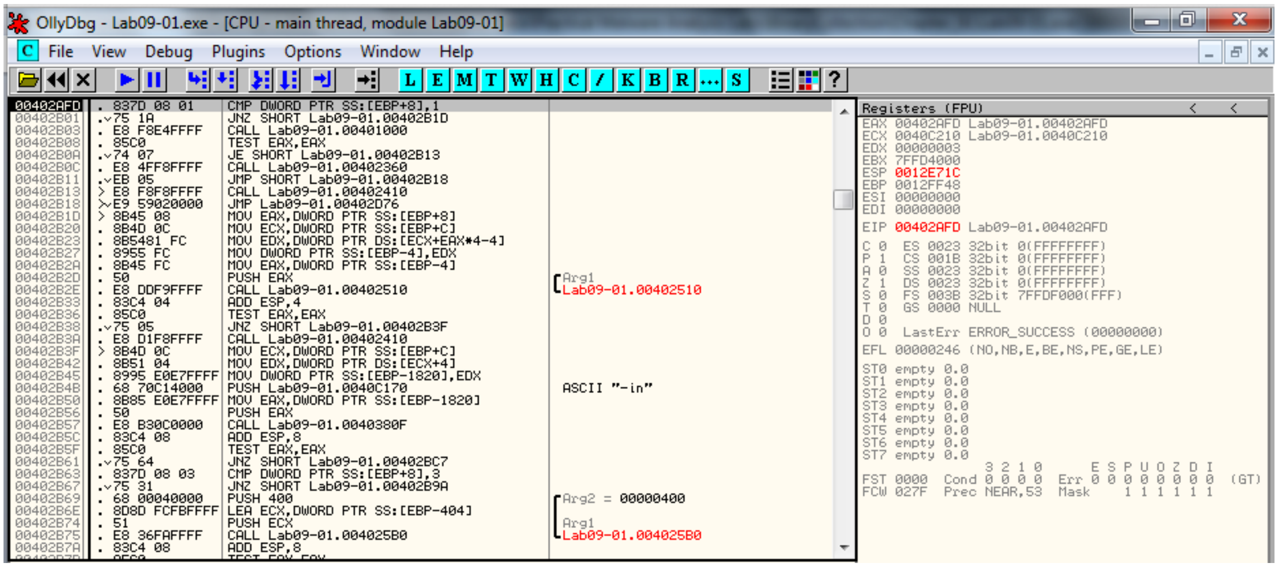

OllyDbg - Lab09-01.exe - [CPU - main thread, module Lab09-01]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S
?

```
00402AF0  $ 55              PUSH EBP
00402AF1  . 8BEC            MOV EBP,ESP
00402AF3  . B8 2C180000     MOV EAX,182C
00402AF8  . E8 B3030000     CALL Lab09-01.00402EB0
00402AFD  . 837D 08 01      CMP DWORD PTR SS:[EBP+8],1
00402B01  .v75 1A           JNZ SHORT Lab09-01.00402B1D
00402B03  . E8 F8E4FFFF     CALL Lab09-01.00401000
00402B08  . 85C0            TEST EAX,EAX
00402B0A  .v74 07           JE SHORT Lab09-01.00402B13
00402B0C  . E8 4FF8FFFF     CALL Lab09-01.00402360
00402B11  .vEB 05           JMP SHORT Lab09-01.00402B18
00402B13  > E8 F8F8FFFF     CALL Lab09-01.00402410
00402B18  >vE9 59020000     JMP Lab09-01.00402D76
00402B1D  > 8B45 08         MOV EAX,DWORD PTR SS:[EBP+8]
00402B20  . 8B4D 0C         MOV ECX,DWORD PTR SS:[EBP+C]
00402B23  . 8B5481 FC       MOV EDX,DWORD PTR DS:[ECX+EAX*4-4]
00402B27  . 8955 FC         MOV DWORD PTR SS:[EBP-4],EDX
00402B2A  . 8B45 FC         MOV EAX,DWORD PTR SS:[EBP-4]
00402B2D  . 50              PUSH EAX                            Arg1
00402B2E  . E8 DDF9FFFF     CALL Lab09-01.00402510              Lab09-01.00402510
00402B33  . 83C4 04         ADD ESP,4
00402B36  . 85C0            TEST EAX,EAX
00402B38  .v75 05           JNZ SHORT Lab09-01.00402B3F
00402B3A  . E8 D1F8FFFF     CALL Lab09-01.00402410
00402B3F  > 8B4D 0C         MOV ECX,DWORD PTR SS:[EBP+C]
00402B42  . 8B51 04         MOV EDX,DWORD PTR DS:[ECX+4]
00402B45  . 8995 E0E7FFFF   MOV DWORD PTR SS:[EBP-1820],EDX
00402B4B  . 68 70C14000     PUSH Lab09-01.0040C170               ASCII "-in"
00402B50  . 8B85 E0E7FFFF   MOV EAX,DWORD PTR SS:[EBP-1820]
00402B56  . 50              PUSH EAX
00402B57  . E8 B30C0000     CALL Lab09-01.0040380F
00402B5C  . 83C4 08         ADD ESP,8
00402B5F  . 85C0            TEST EAX,EAX
00402B61  .v75 64           JNZ SHORT Lab09-01.00402BC7
00402B63  . 837D 08 03      CMP DWORD PTR SS:[EBP+8],3
00402B67  .v75 31           JNZ SHORT Lab09-01.00402B9A
00402B69  . 68 00040000     PUSH 400                            Arg2 = 00000400
```

```
Registers (FPU)
EAX 004C0D20
ECX 0040C210 Lab09-01.0040C210
EDX 00000003
EBX 7FFD4000
ESP 0012FF4C
EBP 0012FF88
ESI 00000000
EDI 00000000

EIP 00402AF0 Lab09-01.00402AF0

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

Press F7 twenty-one times to call a short subroutine and get to 0x402AFD, as shown below.

This CMP operation is testing to see if the number of command-line arguments is 1.


OllyDbg - Lab09-01.exe - [CPU - main thread, module Lab09-01]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S
?

```
00402AFD  . 837D 08 01      CMP DWORD PTR SS:[EBP+8],1
00402B01  .v75 1A           JNZ SHORT Lab09-01.00402B1D
00402B03  . E8 F8E4FFFF     CALL Lab09-01.00401000
00402B08  . 85C0            TEST EAX,EAX
00402B0A  .v74 07           JE SHORT Lab09-01.00402B13
00402B0C  . E8 4FF8FFFF     CALL Lab09-01.00402360
00402B11  .vEB 05           JMP SHORT Lab09-01.00402B18
00402B13  > E8 F8F8FFFF     CALL Lab09-01.00402410
00402B18  >vE9 59020000     JMP Lab09-01.00402D76
00402B1D  > 8B45 08         MOV EAX,DWORD PTR SS:[EBP+8]
00402B20  . 8B4D 0C         MOV ECX,DWORD PTR SS:[EBP+C]
00402B23  . 8B5481 FC       MOV EDX,DWORD PTR DS:[ECX+EAX*4-4]
00402B27  . 8955 FC         MOV DWORD PTR SS:[EBP-4],EDX
00402B2A  . 8B45 FC         MOV EAX,DWORD PTR SS:[EBP-4]
00402B2D  . 50              PUSH EAX                            Arg1
00402B2E  . E8 DDF9FFFF     CALL Lab09-01.00402510              Lab09-01.00402510
00402B33  . 83C4 04         ADD ESP,4
00402B36  . 85C0            TEST EAX,EAX
00402B38  .v75 05           JNZ SHORT Lab09-01.00402B3F
00402B3A  . E8 D1F8FFFF     CALL Lab09-01.00402410
00402B3F  > 8B4D 0C         MOV ECX,DWORD PTR SS:[EBP+C]
00402B42  . 8B51 04         MOV EDX,DWORD PTR DS:[ECX+4]
00402B45  . 8995 E0E7FFFF   MOV DWORD PTR SS:[EBP-1820],EDX
00402B4B  . 68 70C14000     PUSH Lab09-01.0040C170               ASCII "-in"
00402B50  . 8B85 E0E7FFFF   MOV EAX,DWORD PTR SS:[EBP-1820]
00402B56  . 50              PUSH EAX
00402B57  . E8 B30C0000     CALL Lab09-01.0040380F
00402B5C  . 83C4 08         ADD ESP,8
00402B5F  . 85C0            TEST EAX,EAX
00402B61  .v75 64           JNZ SHORT Lab09-01.00402BC7
00402B63  . 837D 08 03      CMP DWORD PTR SS:[EBP+8],3
00402B67  .v75 31           JNZ SHORT Lab09-01.00402B9A
00402B69  . 68 00040000     PUSH 400                            Arg2 = 00000400
00402B6E  . 8D8D FCFBFFFF   LEA ECX,DWORD PTR SS:[EBP-404]
00402B74  . 51              PUSH ECX                            Arg1
00402B75  . E8 36FAFFFF     CALL Lab09-01.004025B0              Lab09-01.004025B0
00402B7A  . 83C4 08         ADD ESP,8
```

```
Registers (FPU)
EAX 00402AFD Lab09-01.00402AFD
ECX 0040C210 Lab09-01.0040C210
EDX 00000003
EBX 7FFD4000
ESP 0012E71C
EBP 0012FF48
ESI 00000000
EDI 00000000

EIP 00402AFD Lab09-01.00402AFD

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

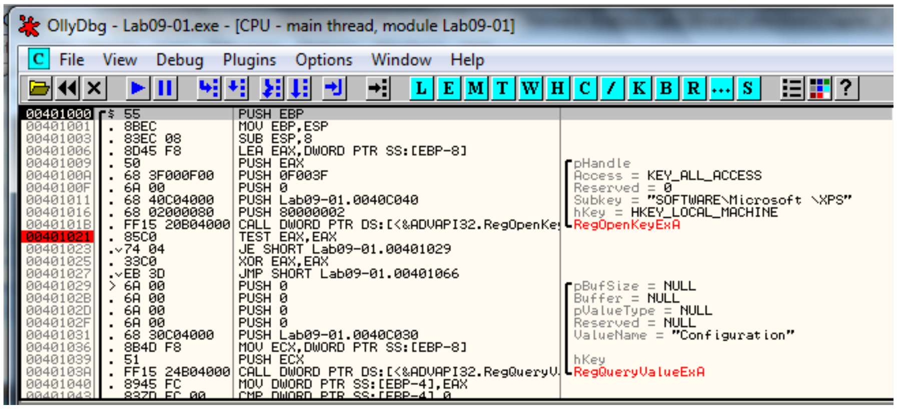
Press F7 three times to pass the test and jump to 0x00401000, as shown below.

Now we are in the routine starting at 0x401000.

It calls RegOpenKeyExA at 0x40101B.

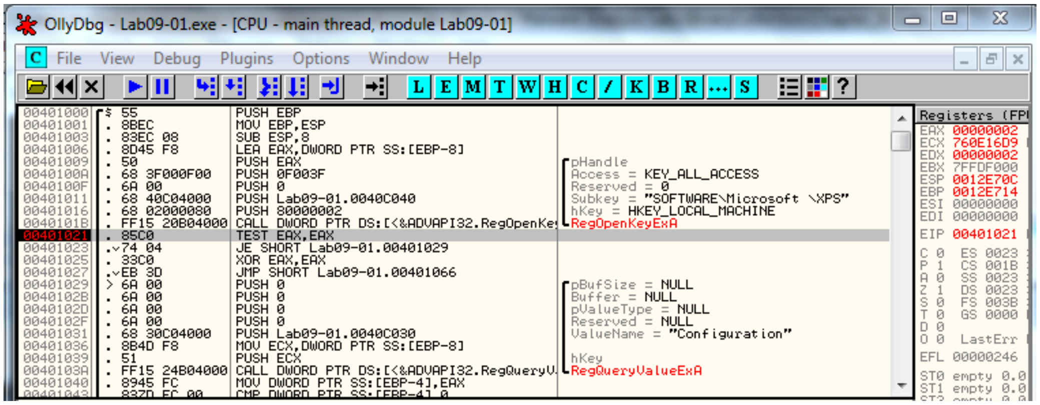
Left-click the line starting with 0x401021 and press F2 to put a breakpoint there. That address turns red, as shown below.

Left-click the line starting with 0x401000. Press F9 to run to the breakpoint.


OllyDbg - Lab09-01.exe - [CPU - main thread, module Lab09-01]
File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S

```
00401000 ┌$ 55             PUSH EBP
00401001 │. 8BEC           MOV EBP,ESP
00401003 │. 83EC 08        SUB ESP,8
00401006 │. 8D45 F8        LEA EAX,DWORD PTR SS:[EBP-8]
00401009 │. 50             PUSH EAX                                   ┌pHandle
0040100A │. 68 3F000F00    PUSH 0F003F                                │Access = KEY_ALL_ACCESS
0040100F │. 6A 00          PUSH 0                                     │Reserved = 0
00401011 │. 68 40C04000    PUSH Lab09-01.0040C040                     │Subkey = "SOFTWARE\Microsoft \XPS"
00401016 │. 68 02000080    PUSH 80000002                              │hKey = HKEY_LOCAL_MACHINE
0040101B │. FF15 20B04000  CALL DWORD PTR DS:[<&ADVAPI32.RegOpenKe    └RegOpenKeyExA
00401021 │. 85C0           TEST EAX,EAX
00401023 │.v74 04          JE SHORT Lab09-01.00401029
00401025 │. 33C0           XOR EAX,EAX
00401027 │.vEB 3D          JMP SHORT Lab09-01.00401066
00401029 │> 6A 00          PUSH 0                                     ┌pBufSize = NULL
0040102B │. 6A 00          PUSH 0                                     │Buffer = NULL
0040102D │. 6A 00          PUSH 0                                     │pValueType = NULL
0040102F │. 6A 00          PUSH 0                                     │Reserved = NULL
00401031 │. 68 30C04000    PUSH Lab09-01.0040C030                     │ValueName = "Configuration"
00401036 │. 8B4D F8        MOV ECX,DWORD PTR SS:[EBP-8]               │
00401039 │. 51             PUSH ECX                                   │hKey
0040103A │. FF15 24B04000  CALL DWORD PTR DS:[<&ADVAPI32.RegQueryV.   └RegQueryValueExA
00401040 │. 8945 FC        MOV DWORD PTR SS:[EBP-4],EAX
00401043 │. 837D FC 00     CMP DWORD PTR SS:[EBP-4],0
```

Look at the upper right to see the registers. EAX now contains 2, as shown below.


OllyDbg - Lab09-01.exe - [CPU - main thread, module Lab09-01]
File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S

```
00401000 ┌$ 55             PUSH EBP
00401001 │. 8BEC           MOV EBP,ESP
00401003 │. 83EC 08        SUB ESP,8
00401006 │. 8D45 F8        LEA EAX,DWORD PTR SS:[EBP-8]
00401009 │. 50             PUSH EAX                                   ┌pHandle
0040100A │. 68 3F000F00    PUSH 0F003F                                │Access = KEY_ALL_ACCESS
0040100F │. 6A 00          PUSH 0                                     │Reserved = 0
00401011 │. 68 40C04000    PUSH Lab09-01.0040C040                     │Subkey = "SOFTWARE\Microsoft \XPS"
00401016 │. 68 02000080    PUSH 80000002                              │hKey = HKEY_LOCAL_MACHINE
0040101B │. FF15 20B04000  CALL DWORD PTR DS:[<&ADVAPI32.RegOpenKe    └RegOpenKeyExA
00401021 │. 85C0           TEST EAX,EAX
00401023 │.v74 04          JE SHORT Lab09-01.00401029
00401025 │. 33C0           XOR EAX,EAX
00401027 │.vEB 3D          JMP SHORT Lab09-01.00401066
00401029 │> 6A 00          PUSH 0                                     ┌pBufSize = NULL
0040102B │. 6A 00          PUSH 0                                     │Buffer = NULL
0040102D │. 6A 00          PUSH 0                                     │pValueType = NULL
0040102F │. 6A 00          PUSH 0                                     │Reserved = NULL
00401031 │. 68 30C04000    PUSH Lab09-01.0040C030                     │ValueName = "Configuration"
00401036 │. 8B4D F8        MOV ECX,DWORD PTR SS:[EBP-8]               │
00401039 │. 51             PUSH ECX                                   │hKey
0040103A │. FF15 24B04000  CALL DWORD PTR DS:[<&ADVAPI32.RegQueryV.   └RegQueryValueExA
00401040 │. 8945 FC        MOV DWORD PTR SS:[EBP-4],EAX
00401043 │. 837D FC 00     CMP DWORD PTR SS:[EBP-4],0
```

```
Registers (FPU
EAX 00000002
ECX 760E16D9
EDX 00000002
EBX 7FFDF000
ESP 0012E70C
EBP 0012E714
ESI 00000000
EDI 00000000

EIP 00401021

C 0  ES 0023
P 1  CS 001B
A 0  SS 0023
Z 1  DS 0023
S 0  FS 003B
T 0  GS 0000
D 0
O 0  LastErr

EFL 00000246

ST0 empty 0.0
ST1 empty 0.0
```

This is a "non-zero error code", as explained here:

http://msdn.microsoft.com/en-us/library/windows/desktop/ms724897(v=vs.85).aspx

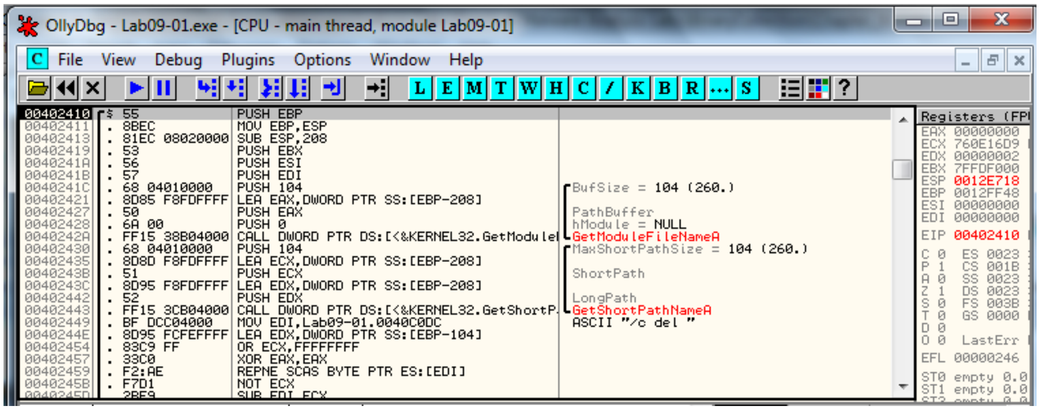
That means the test failed--it did not find the registry key it was looking for.

Press F7 three times to get to location 0x401027.

Press F7 to execute the JMP.

Press F7 three times to step through the subroutine and get to 0x402B08.

Press F7 three times to get to location 0x402410, as shown below:


OllyDbg - Lab09-01.exe - [CPU - main thread, module Lab09-01]
File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S

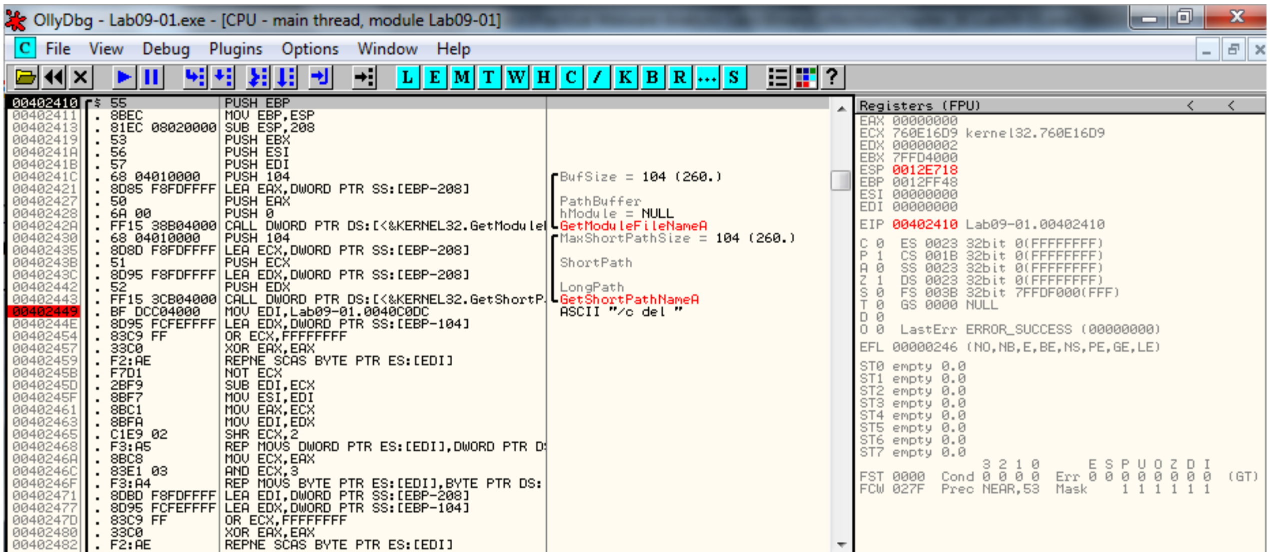
```
00402410 ┌$ 55             PUSH EBP
00402411 │. 8BEC           MOV EBP,ESP
00402413 │. 81EC 08020000  SUB ESP,208
00402419 │. 53             PUSH EBX
0040241A │. 56             PUSH ESI
0040241B │. 57             PUSH EDI
0040241C │. 68 04010000    PUSH 104                                   ┌BufSize = 104 (260.)
00402421 │. 8D85 F8FDFFFF  LEA EAX,DWORD PTR SS:[EBP-208]             │
00402427 │. 50             PUSH EAX                                   │PathBuffer
00402428 │. 6A 00          PUSH 0                                     │hModule = NULL
0040242A │. FF15 38B04000  CALL DWORD PTR DS:[<&KERNEL32.GetModuleI   └GetModuleFileNameA
00402430 │. 68 04010000    PUSH 104                                   ┌MaxShortPathSize = 104 (260.)
00402435 │. 8D8D F8FDFFFF  LEA ECX,DWORD PTR SS:[EBP-208]             │
0040243B │. 51             PUSH ECX                                   │ShortPath
0040243C │. 8D95 F8FDFFFF  LEA EDX,DWORD PTR SS:[EBP-208]             │
00402442 │. 52             PUSH EDX                                   │LongPath
00402443 │. FF15 3CB04000  CALL DWORD PTR DS:[<&KERNEL32.GetShortP.   └GetShortPathNameA
00402449 │. BF DCC04000    MOV EDI,Lab09-01.0040C0DC                   ASCII "/c del "
0040244E │. 8D95 FCFEFFFF  LEA EDX,DWORD PTR SS:[EBP-104]
00402454 │. 83C9 FF        OR ECX,FFFFFFFF
00402457 │. 33C0           XOR EAX,EAX
00402459 │. F2:AE          REPNE SCAS BYTE PTR ES:[EDI]
0040245B │. F7D1           NOT ECX
0040245D │. 2BF9           SUB EDI,ECX
```

```
Registers (FPU
EAX 00000000
ECX 760E16D9
EDX 00000002
EBX 7FFDF000
ESP 0012E718
EBP 0012FF48
ESI 00000000
EDI 00000000

EIP 00402410

C 0  ES 0023
P 1  CS 001B
A 0  SS 0023
Z 1  DS 0023
S 0  FS 003B
T 0  GS 0000
D 0
O 0  LastErr

EFL 00000246

ST0 empty 0.0
ST1 empty 0.0
```

This function uses GetModuleFilename to get the path to the current executable and builds the ASCII string

```
/c del path-to-executable >> NUL
```

To see that, place a breakpoint just after GetShortPathNameA, so its address turns red, as shown below.



OllyDbg - Lab09-01.exe - [CPU - main thread, module Lab09-01]

C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S ?

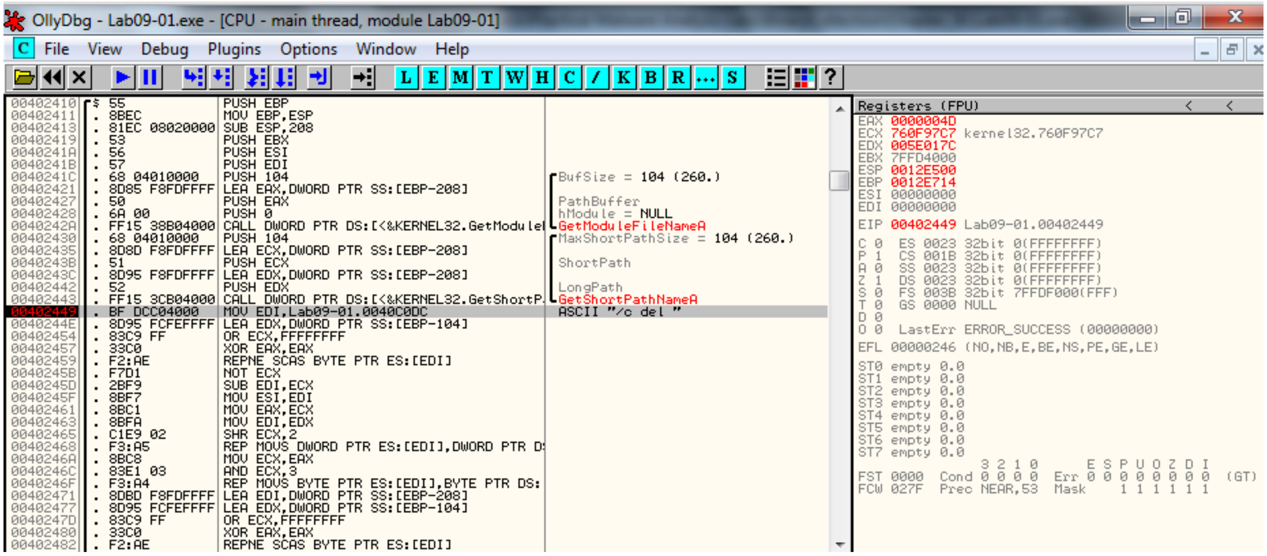
```
00402410 r$ 55             PUSH EBP
00402411  . 8BEC           MOV EBP,ESP
00402413  . 81EC 08020000  SUB ESP,208
00402419  . 53             PUSH EBX
0040241A  . 56             PUSH ESI
0040241B  . 57             PUSH EDI
0040241C  . 68 04010000    PUSH 104                                  rBufSize = 104 (260.)
00402421  . 8D85 F8FDFFFF  LEA EAX,DWORD PTR SS:[EBP-208]            |
00402427  . 50             PUSH EAX                                  |PathBuffer
00402428  . 6A 00          PUSH 0                                    |hModule = NULL
0040242A  . FF15 38B04000  CALL DWORD PTR DS:[<&KERNEL32.GetModulel  LGetModuleFileNameA
00402430  . 68 04010000    PUSH 104                                  rMaxShortPathSize = 104 (260.)
00402435  . 8D8D F8FDFFFF  LEA ECX,DWORD PTR SS:[EBP-208]            |
0040243B  . 51             PUSH ECX                                  |ShortPath
0040243C  . 8D95 F8FDFFFF  LEA EDX,DWORD PTR SS:[EBP-208]            |
00402442  . 52             PUSH EDX                                  |LongPath
00402443  . FF15 3CB04000  CALL DWORD PTR DS:[<&KERNEL32.GetShortP.  LGetShortPathNameA
00402449  . BF DCC04000    MOV EDI,Lab09-01.0040C0DC                 ASCII "/c del "
0040244E  . 8D95 FCFEFFFF  LEA EDX,DWORD PTR SS:[EBP-104]
00402454  . 83C9 FF        OR ECX,FFFFFFFF
00402457  . 33C0           XOR EAX,EAX
00402459  . F2:AE          REPNE SCAS BYTE PTR ES:[EDI]
0040245B  . F7D1           NOT ECX
0040245D  . 2BF9           SUB EDI,ECX
0040245F  . 8BF7           MOV ESI,EDI
00402461  . 8BC1           MOV EAX,ECX
00402463  . 8BFA           MOV EDI,EDX
00402465  . C1E9 02        SHR ECX,2
00402468  . F3:A5          REP MOVS DWORD PTR ES:[EDI],DWORD PTR D:
0040246A  . 8BC8           MOV ECX,EAX
0040246C  . 83E1 03        AND ECX,3
0040246F  . F3:A4          REP MOVS BYTE PTR ES:[EDI],BYTE PTR DS:
00402471  . 8DBD F8FDFFFF  LEA EDI,DWORD PTR SS:[EBP-208]
00402477  . 8D95 FCFEFFFF  LEA EDX,DWORD PTR SS:[EBP-104]
0040247D  . 83C9 FF        OR ECX,FFFFFFFF
00402480  . 33C0           XOR EAX,EAX
00402482  . F2:AE          REPNE SCAS BYTE PTR ES:[EDI]
```

```
Registers (FPU)
EAX 00000000
ECX 760E16D9 kernel32.760E16D9
EDX 00000002
EBX 7FFD4000
ESP 0012E718
EBP 0012FF48
ESI 00000000
EDI 00000000

EIP 00402410 Lab09-01.00402410

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

Click the line starting with 0x402410 to highlight it.

Press F9 to run to the breakpoint.

You should now be at the line ending with "ASCII "/c del ", as shown below.



OllyDbg - Lab09-01.exe - [CPU - main thread, module Lab09-01]

C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S ?

```
00402410 r$ 55             PUSH EBP
00402411  . 8BEC           MOV EBP,ESP
00402413  . 81EC 08020000  SUB ESP,208
00402419  . 53             PUSH EBX
0040241A  . 56             PUSH ESI
0040241B  . 57             PUSH EDI
0040241C  . 68 04010000    PUSH 104                                  rBufSize = 104 (260.)
00402421  . 8D85 F8FDFFFF  LEA EAX,DWORD PTR SS:[EBP-208]            |
00402427  . 50             PUSH EAX                                  |PathBuffer
00402428  . 6A 00          PUSH 0                                    |hModule = NULL
0040242A  . FF15 38B04000  CALL DWORD PTR DS:[<&KERNEL32.GetModulel  LGetModuleFileNameA
00402430  . 68 04010000    PUSH 104                                  rMaxShortPathSize = 104 (260.)
00402435  . 8D8D F8FDFFFF  LEA ECX,DWORD PTR SS:[EBP-208]            |
0040243B  . 51             PUSH ECX                                  |ShortPath
0040243C  . 8D95 F8FDFFFF  LEA EDX,DWORD PTR SS:[EBP-208]            |
00402442  . 52             PUSH EDX                                  |LongPath
00402443  . FF15 3CB04000  CALL DWORD PTR DS:[<&KERNEL32.GetShortP.  LGetShortPathNameA
00402449  . BF DCC04000    MOV EDI,Lab09-01.0040C0DC                 ASCII "/c del "
0040244E  . 8D95 FCFEFFFF  LEA EDX,DWORD PTR SS:[EBP-104]
00402454  . 83C9 FF        OR ECX,FFFFFFFF
00402457  . 33C0           XOR EAX,EAX
00402459  . F2:AE          REPNE SCAS BYTE PTR ES:[EDI]
0040245B  . F7D1           NOT ECX
0040245D  . 2BF9           SUB EDI,ECX
0040245F  . 8BF7           MOV ESI,EDI
00402461  . 8BC1           MOV EAX,ECX
00402463  . 8BFA           MOV EDI,EDX
00402465  . C1E9 02        SHR ECX,2
00402468  . F3:A5          REP MOVS DWORD PTR ES:[EDI],DWORD PTR D:
0040246A  . 8BC8           MOV ECX,EAX
0040246C  . 83E1 03        AND ECX,3
0040246F  . F3:A4          REP MOVS BYTE PTR ES:[EDI],BYTE PTR DS:
00402471  . 8DBD F8FDFFFF  LEA EDI,DWORD PTR SS:[EBP-208]
00402477  . 8D95 FCFEFFFF  LEA EDX,DWORD PTR SS:[EBP-104]
0040247D  . 83C9 FF        OR ECX,FFFFFFFF
00402480  . 33C0           XOR EAX,EAX
00402482  . F2:AE          REPNE SCAS BYTE PTR ES:[EDI]
```

```
Registers (FPU)
EAX 0000004D
ECX 760F97C7 kernel32.760F97C7
EDX 005E017C
EBX 7FFD4000
ESP 0012E500
EBP 0012E714
ESI 00000000
EDI 00000000

EIP 00402449 Lab09-01.00402449

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

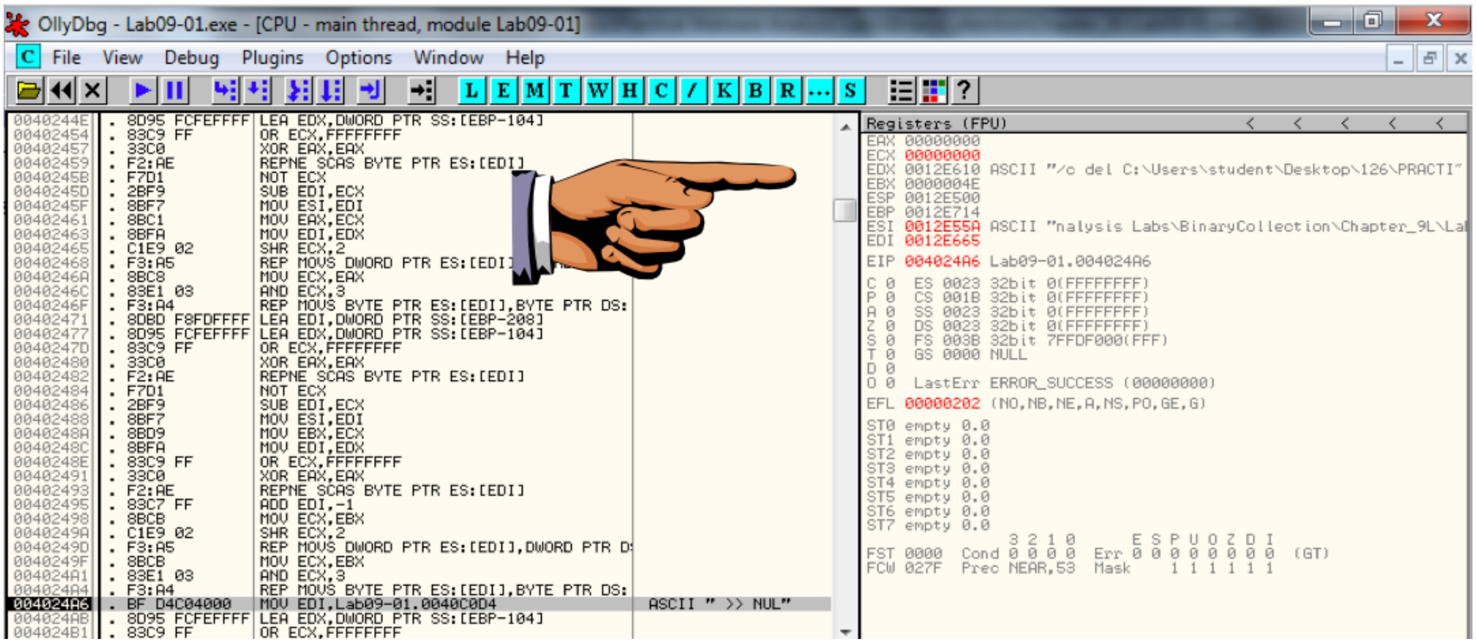
By holding F7 down or tapping it many times, you can play the code forward like a movie in slow motion.

Watch as the code slowly steps through a long path name in EDI. Then the path name flips quickly through several registers, ending up in EDX.

Stop when you see a string in EDX, starting with

ASCII "/c del C:\

as shown below:


OllyDbg - Lab09-01.exe - [CPU - main thread, module Lab09-01]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S
Registers (FPU)

```
0040244E  . 8D95 FCFEFFFF LEA EDX,DWORD PTR SS:[EBP-104]
00402454  . 83C9 FF       OR ECX,FFFFFFFF
00402457  . 33C0          XOR EAX,EAX
00402459  . F2:AE         REPNE SCAS BYTE PTR ES:[EDI]
0040245B  . F7D1          NOT ECX
0040245D  . 2BF9          SUB EDI,ECX
0040245F  . 8BF7          MOV ESI,EDI
00402461  . 8BC1          MOV EAX,ECX
00402463  . 8BFA          MOV EDI,EDX
00402465  . C1E9 02       SHR ECX,2
00402468  . F3:A5         REP MOVS DWORD PTR ES:[EDI]
0040246A  . 8BC8          MOV ECX,EAX
0040246C  . 83E1 03       AND ECX,3
0040246F  . F3:A4         REP MOVS BYTE PTR ES:[EDI],BYTE PTR DS:
00402471  . 8DBD F8FDFFFF LEA EDI,DWORD PTR SS:[EBP-208]
00402477  . 8D95 FCFEFFFF LEA EDX,DWORD PTR SS:[EBP-104]
0040247D  . 83C9 FF       OR ECX,FFFFFFFF
00402480  . 33C0          XOR EAX,EAX
00402482  . F2:AE         REPNE SCAS BYTE PTR ES:[EDI]
00402484  . F7D1          NOT ECX
00402486  . 2BF9          SUB EDI,ECX
00402488  . 8BF7          MOV ESI,EDI
0040248A  . 8BD9          MOV EBX,ECX
0040248C  . 8BFA          MOV EDI,EDX
0040248E  . 83C9 FF       OR ECX,FFFFFFFF
00402491  . 33C0          XOR EAX,EAX
00402493  . F2:AE         REPNE SCAS BYTE PTR ES:[EDI]
00402495  . 83C7 FF       ADD EDI,-1
00402498  . 8BCB          MOV ECX,EBX
0040249A  . C1E9 02       SHR ECX,2
0040249D  . F3:A5         REP MOVS DWORD PTR ES:[EDI],DWORD PTR D:
0040249F  . 8BCB          MOV ECX,EBX
004024A1  . 83E1 03       AND ECX,3
004024A4  . F3:A4         REP MOVS BYTE PTR ES:[EDI],BYTE PTR DS:
004024A6  . BF D4C04000   MOV EDI,Lab09-01.0040C0D4          ASCII " >> NUL"
004024AB  . 8D95 FCFEFFFF LEA EDX,DWORD PTR SS:[EBP-104]
004024B1  . 83C9 FF       OR ECX,FFFFFFFF
```

```
EAX 00000000
ECX 00000000
EDX 0012E610 ASCII "/c del C:\Users\student\Desktop\126\PRACTI"
EBX 0000004E
ESP 0012E500
EBP 0012E714
ESI 0012E55A ASCII "nalysis Labs\BinaryCollection\Chapter_9L\La
EDI 0012E665

EIP 004024A6 Lab09-01.004024A6

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_SUCCESS (00000000)

EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

Troubleshooting

If you press F7 too many times, EDX empties. To return to this point you must do these steps:

- From the Ollydbg menu bar, click **Debug**, **Restart**
- Click **Yes**
- Press **F9** to run to the breakpoint at 0x401021
- Press **F9** to run to the breakpoint at 0x402449
- Hold down or tap **F7** several dozen times to get to the desired point

Saving the Screen Image

Make sure you can see the EDX register with a value starting with **ASCII "/c del C:\** as shown above.

On your keyboard, press the PrntScrn key.

Click **Start**, type in **PAINT**, and open Paint.

Press **Ctrl+V** to paste in the image of your desktop.

YOU MUST SUBMIT WHOLE-DESKTOP IMAGES TO GET FULL CREDIT.

Save the image with a filename of "**Proj 11b from YOUR NAME**".

Turning in Your Project

Email the images to: **cnit.126sam@gmail.com** with a subject line of **Proj 11 From Your Name**, replacing Your Name with your own first and last name. Send a Cc to yourself.

Last Modified: 3-21-16