Reverse Engineering: Towards Malware Analysis

Lecture – IDA Pro

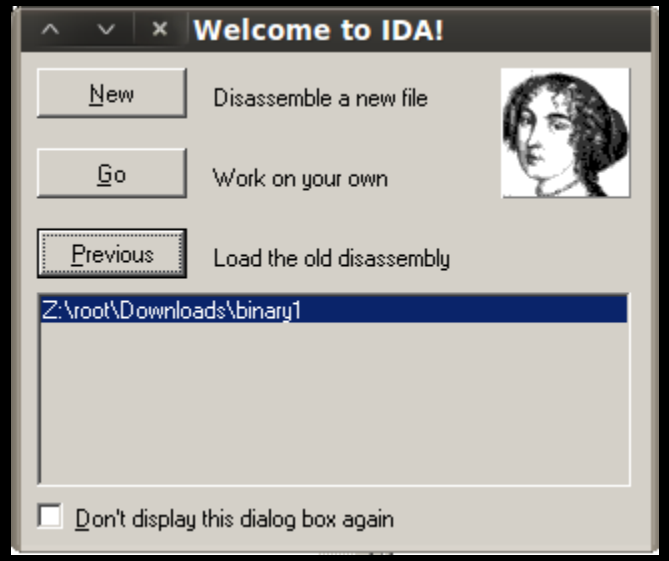
Computer Security Practice

Interactive DisAssembler (IDA)

- 3 versions
  - Free
  - Demo (stay away)
  - Commercial - monies
    - Standard
    - Advanced – x64
- Capable of disassembling
  - Formats
    - PE
    - ELF
  - Architecture
    - x86
    - x64
    - ARM
  - And many, many more
- IDA Pro Free
  - www.hex-rays.com

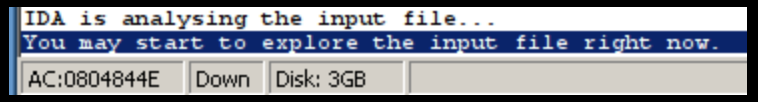
Loading an Executable

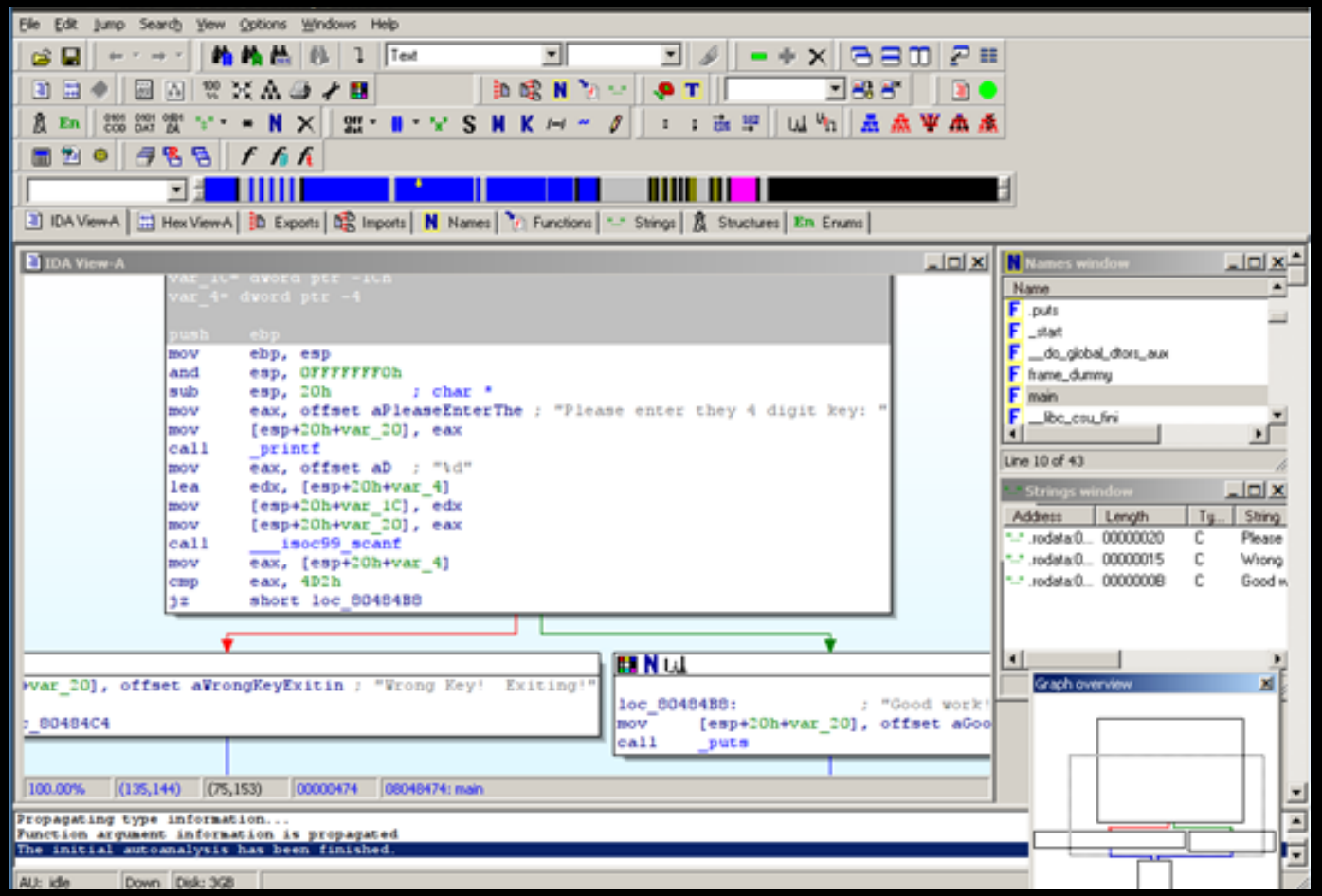
- Drag and drop
- Or open IDA and select “New”
- Start by accepting the defaults
  - Click “OK”



Graph Mode

Give IDA some time to load!

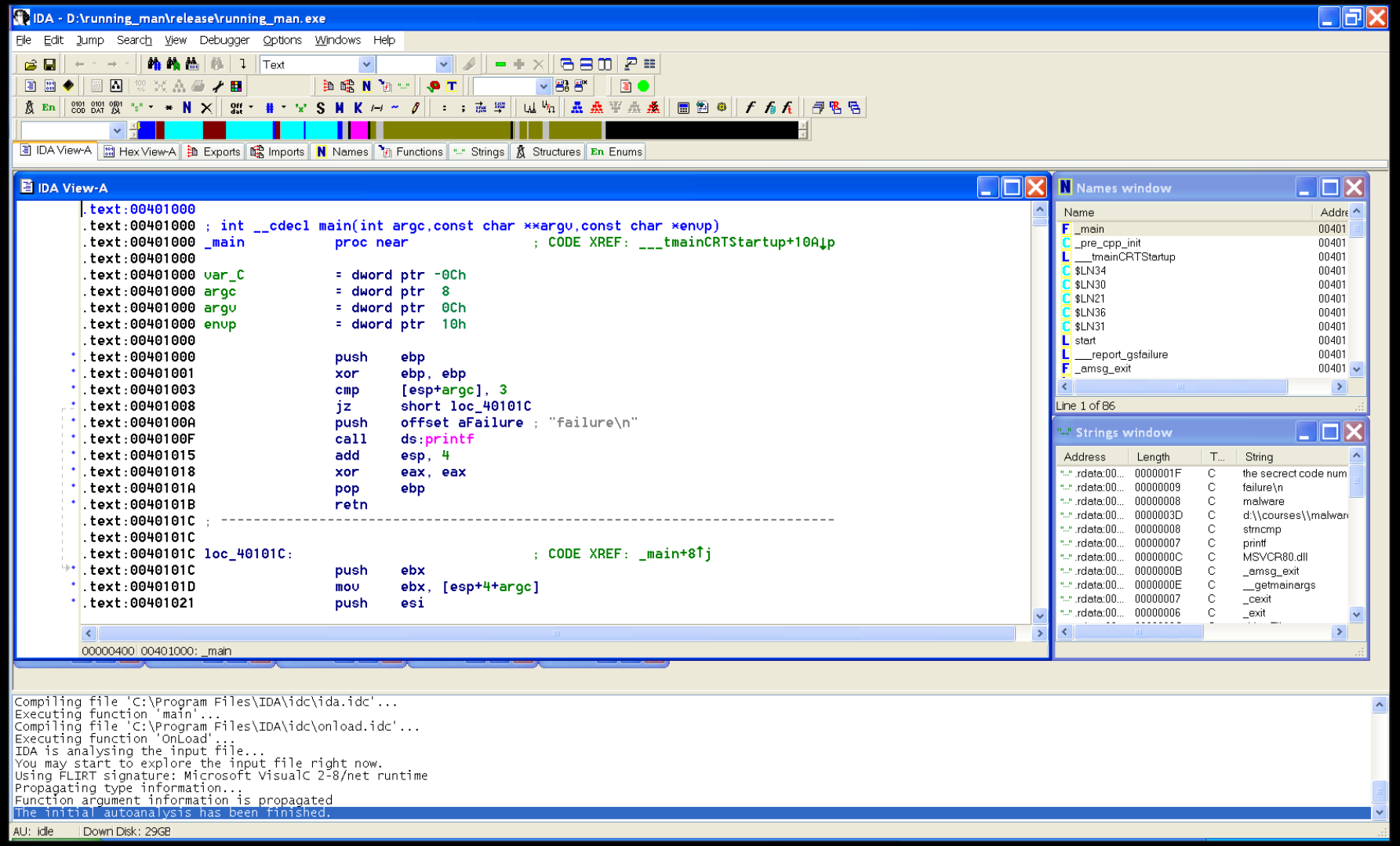




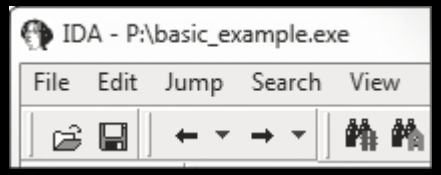
Text Mode

```
.text:00401040
.text:00401040                  sub_401040 proc near                    ; CODE XREF: sub_4010A0+2A↓p
.text:00401040
.text:00401040                  var_18    = dword ptr -18h
.text:00401040                  var_14    = dword ptr -14h
.text:00401040                  var_10    = dword ptr -10h
.text:00401040                  var_C     = dword ptr -0Ch
.text:00401040                  var_8     = dword ptr -8
.text:00401040                  var_4     = dword ptr -4
.text:00401040
.text:00401040 55                       push  ebp
.text:00401041 89 E5                    mov   ebp, esp
.text:00401043 83 EC 18                 sub   esp, 18h
.text:00401046 C7 45 F4 00 00 00+       mov   [ebp+var_C], 0
.text:0040104D C7 45 F0 00 00 00+       mov   [ebp+var_10], 0
.text:00401054 C7 45 FC 64 00 00+       mov   [ebp+var_4], 64h
.text:0040105B
.text:0040105B                  loc_40105B:                             ; CODE XREF: sub_401040+5C↓j
.text:0040105B 83 7D FC 01              cmp   [ebp+var_4], 1
.text:0040105F 7E 3D                    jle   short locret_40109E
.text:00401061 C7 45 F0 00 00 00+       mov   [ebp+var_10], 0
.text:00401068 8B 45 F8                 mov   eax, [ebp+var_8]
.text:0040106B 03 45 FC                 add   eax, [ebp+var_4]
.text:0040106E 89 45 F4                 mov   [ebp+var_C], eax
.text:00401071 83 7D F4 1E              cmp   [ebp+var_C], 1Eh
.text:00401075 75 07                    jnz   short loc_40107E
.text:00401077 C7 45 F0 01 00 00+       mov   [ebp+var_10], 1
.text:0040107E
.text:0040107E                  loc_40107E:                             ; CODE XREF: sub_401040+35↑j
.text:0040107E 83 7D F4 00              cmp   [ebp+var_C], 0
.text:00401082 75 13                    jnz   short loc_401097
.text:00401084 8B 45 FC                 mov   eax, [ebp+var_4]
.text:00401087 89 44 24 04              mov   [esp+18h+var_14], eax
.text:0040108B C7 04 24 20 20 40+       mov   [esp+18h+var_18], offset aPrintNumberD ; "Print Number= %d\n"
.text:00401092 E8 B1 00 00 00           call  printf
.text:00401097
.text:00401097                  loc_401097:                             ; CODE XREF: sub_401040+42↑j
.text:00401097 8D 45 FC                 lea   eax, [ebp+var_4]
.text:0040109A FF 08                    dec   dword ptr [eax]
.text:0040109C EB BD                    jmp   short loc_40105B
.text:0040109E                  ; ---------------------------------------------------------------------------
.text:0040109E
.text:0040109E                  locret_40109E:                          ; CODE XREF: sub_401040+1F↑j
.text:0040109E C9                       leave
.text:0040109F C3                       retn
.text:0040109F                  sub_401040 endp
```

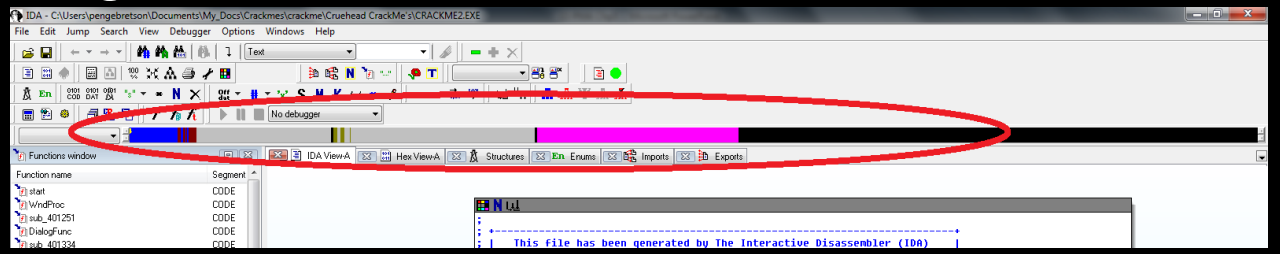
The many IDA Windows



Navigating IDA



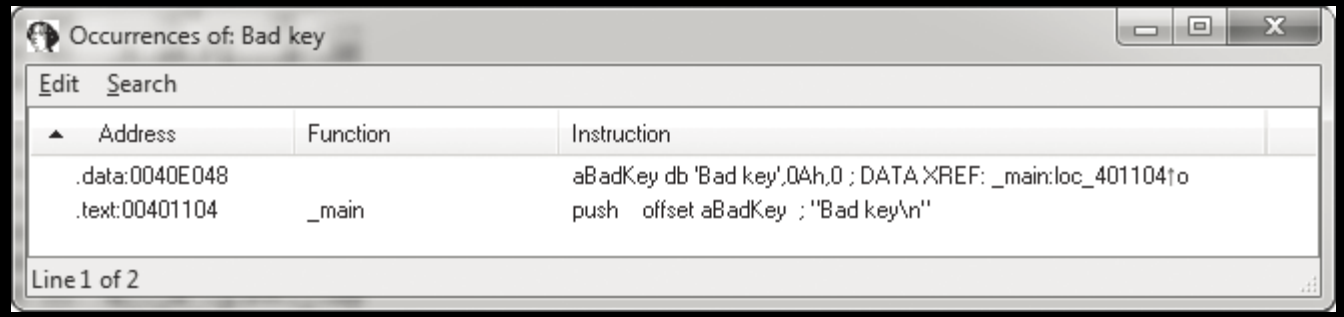
- IDA's Forward & Back buttons
- Navigation Band



  - Focus on the dark blue region…
- Press "G" for…Jump?
  - Jump to location
- Search

Search Example

```
C:\>password.exe
Enter password for this Malware: test
Bad key
```




```
004010E0        push    offset aMab     ; "$mab"
004010E5        lea     ecx, [ebp+var_1C]
004010E8        push    ecx
004010E9        call    strcmp
004010EE        add     esp, 8
004010F1        test    eax, eax
004010F3        jnz     short loc_401104
004010F5        push    offset aKeyAccepted ; "Key Accepted!\n"
004010FA        call    printf
004010FF        add     esp, 4
00401102        jmp     short loc_401118
00401104 loc_401104                     ; CODE XREF: _main+53j
00401104        push    offset aBadKey  ; "Bad key\n"
00401109        call    printf
```

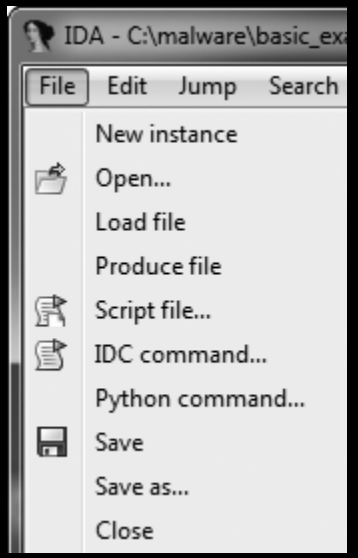
```
C:\>password.exe
Enter password for this Malware: $mab
Key Accepted!
The malware has been unlocked
```

Enhancing Disassembly – so many ways

- You can modify the disassembly to increase the efficiency
  - `Sub_401000` or `DNS_Request`?
  - Can rename function, variable names, and more
- Adding Comments
  - Embed comments throughout your disassembly
  - Use the ";" to create a comment
- Adding Notes
- Standard symbolic constants
- Common structures, runtime functions
- Identifying and Renaming stack variables
- Naming Local Labels
- Imports and Exports

Extending IDA with Plug-ins

- Allow you to expand IDA
- Python / IDAPython
- IDC
- Commercial Plugins
  - HexRays Decompiler
  - BinDiff



More IDA Pro

- Sections
- Code, Data, Undefined
  - (C,D,A,L,F,U)
- Branches and Loops
- Functions
  - Arguments
  - Calling conventions
- Is it data or is it code?
- Cross References
- Suggested options (display opcodes, xrefs)