Reset Desktop
Navigate – Use Search -> Text

IDA auto comments – very useful
Navigate (Links)

```
sub_4015E0 proc near

var_20= dword ptr -20h
var_10= dword ptr -10h
var_8= dword ptr -8
var_4= dword ptr -4

push ebp
mov ebp, esp
and esp, 0FFFFFFF0h
sub esp, 20h ; char *
call sub_401790
mov [esp+20h+var_4], 1
mov [esp+20h+var_8], 2
mov eax, [esp+20h+var_8]
add [esp+20h+var_4], eax
mov eax, [esp+20h+var_4]
mov [esp+20h+var_10], eax
mov [esp+20h+var_20], offset altotal0 ; "total = %d\n"
call printf
mov eax, 0
leave
ret
```

Double Click here

It will redirect you to the sub links

Could be functions

Navigate through history
Navigation Band

Navigation band: colors represent different address space of the binary

See default color in Options->Color->Navigation Band

See other colors in the options

Light blue->lib code

Dark blue->user written code

We should perform our analysis in user written code -> dark blue area
Press “G” key to jump to virtual memory address or named location, tried previous one: sub_401790

Brings us back in here
Using Cross-references

- Cross-reference – tells where a function is called or where a string is used.

Press “X”- windows will list all locations this loc_4012D1 is called.
Analyzing Functions

- IDAPro: recognize functions/local variables/parameters and label them.

IDA discovers local variables for you

Local variables: prefix var_

Parameter: prefix arg_

Dummy name: renaming would make more sense during analysis. But need to understand first.
Graph Views

Play with one of these buttons to see graph views

Cross-reference Graph

Can change to decimal, octal, binary – right click
Redefining Code and Data

Bytes could be occasionally categorized incorrectly.

Both are bit strings.

Code may be defined as data; data defined as code

Indistinguishable.

Press ‘U’Key to undefine functions, code or data -> becomes raw bytes; press ‘C’ to define
In-class homeworks