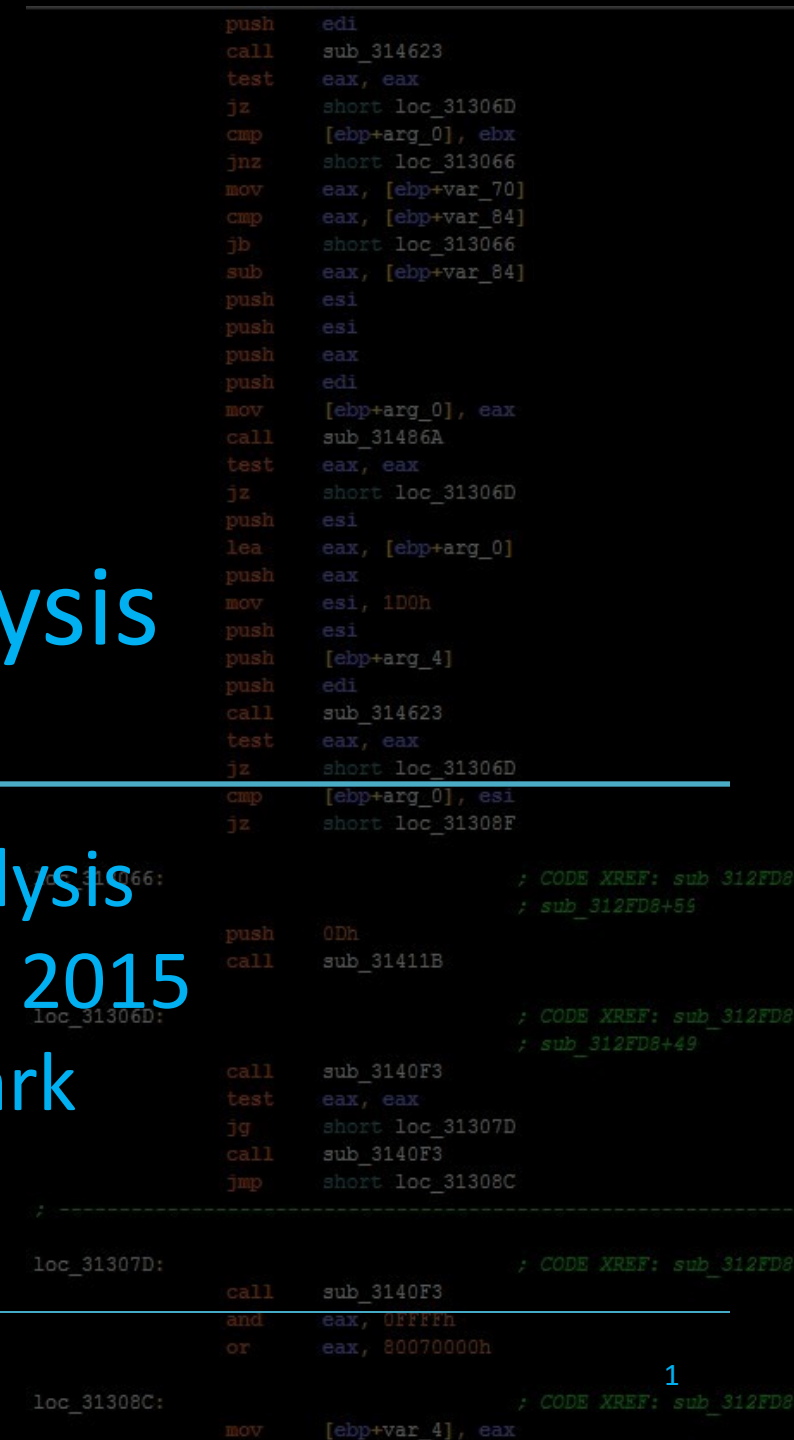
Basic Analysis

Malware Analysis
CSCI 4976 - Fall 2015
Branden Clark

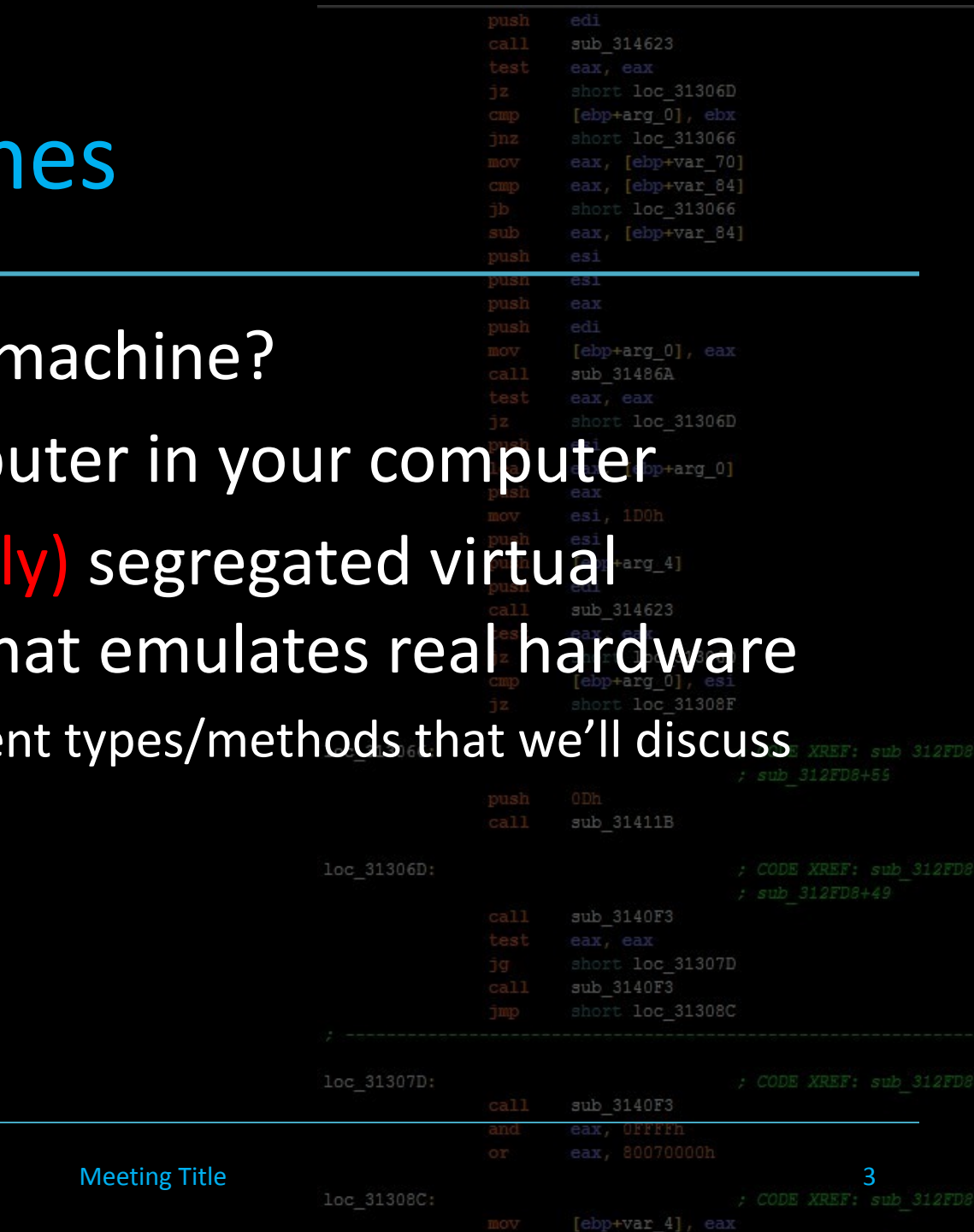


Overview

- Your malware analysis VM
- Static Analysis
- Dynamic Analysis

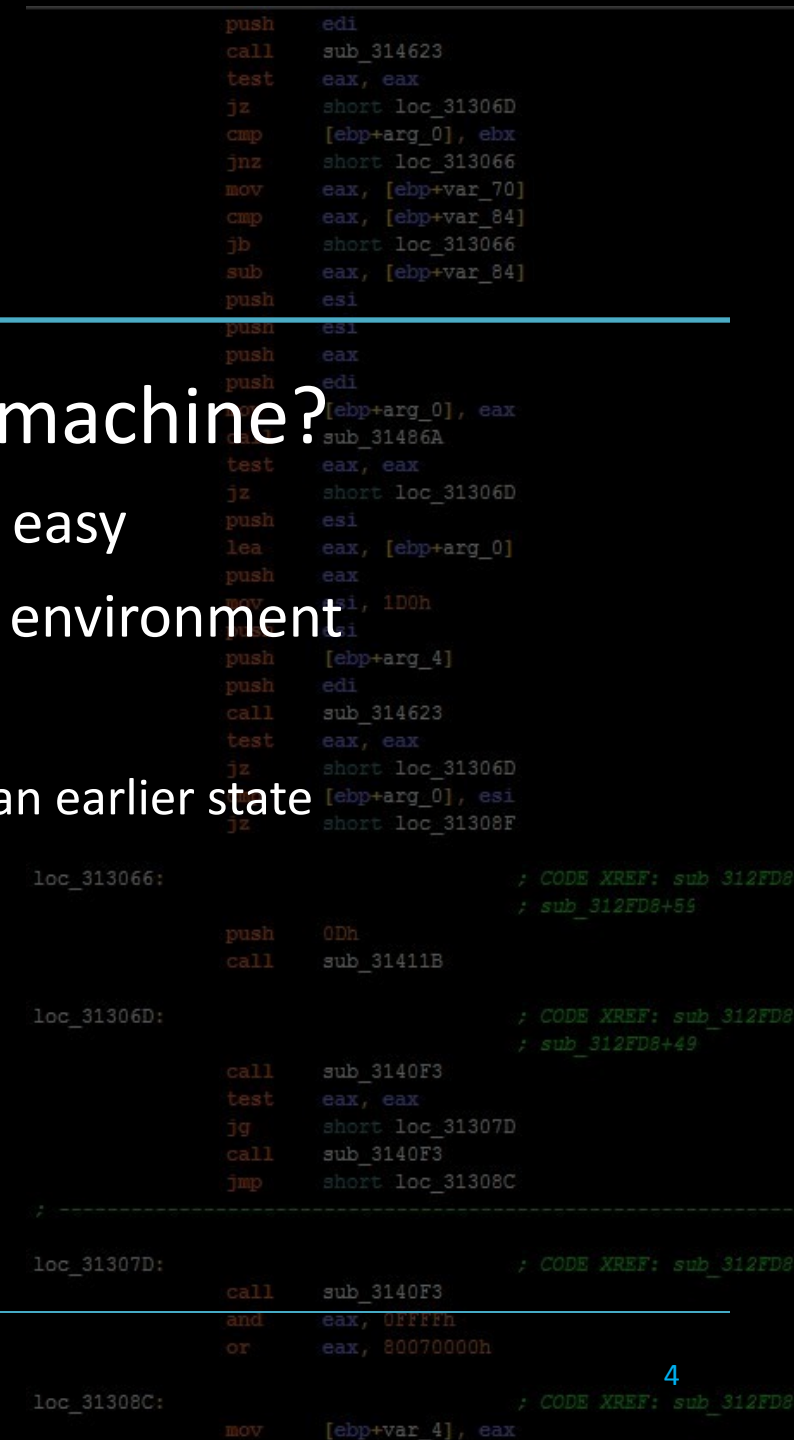
Virtual Machines

- What is a virtual machine?
  - Simply, a computer in your computer
  - Really, a (usually) segregated virtual environment that emulates real hardware
    - There are different types/methods that we'll discuss later



Virtual Machines

- Why are we using a virtual machine?
  - Safety, reliability, consistency, it's easy
  - Keep the malware in a contained environment
  - Snapshots
    - Completely 100% revert the VM to an earlier state
    - If things go bad, no one cares

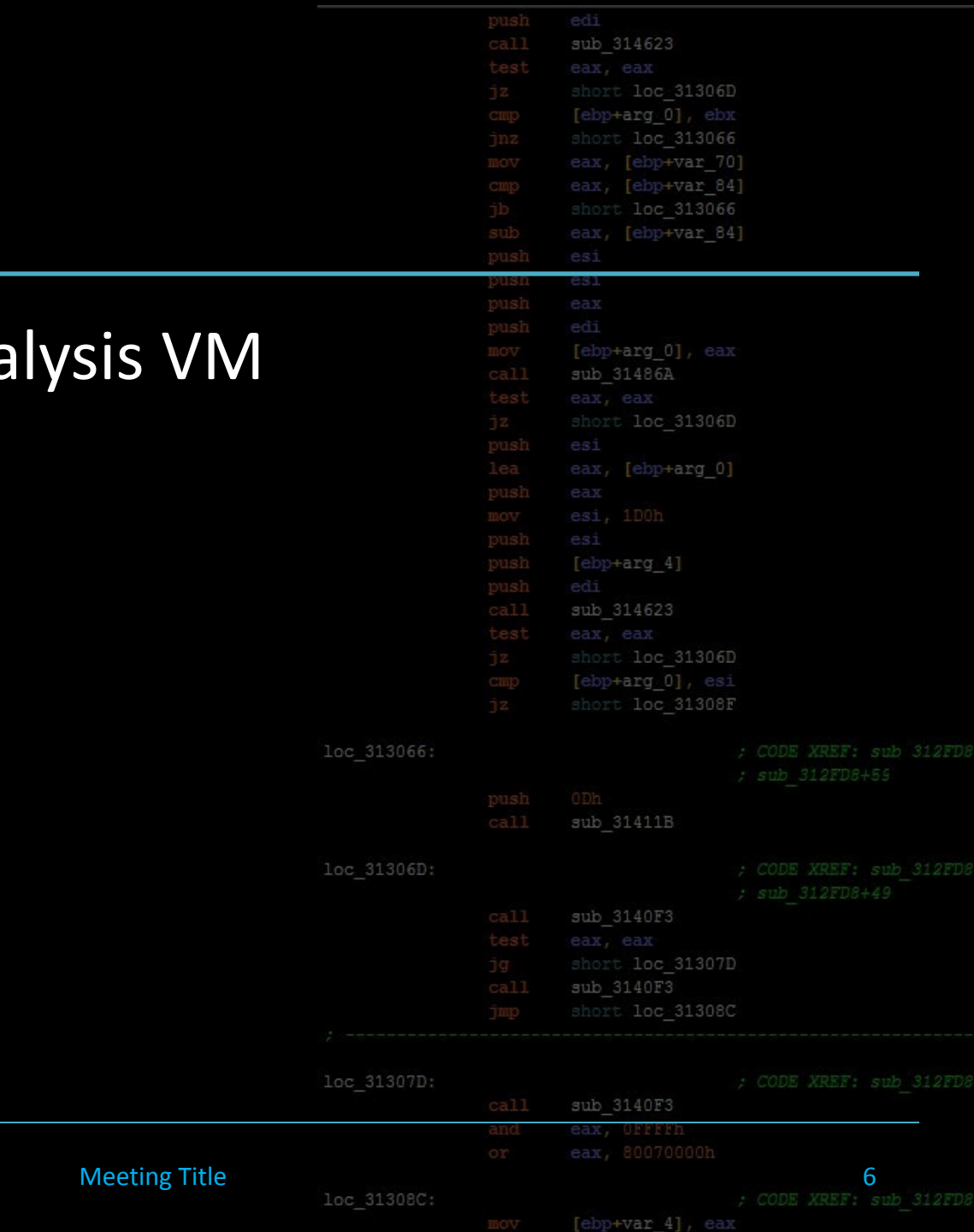


Virtual Machines

- We will be using Windows 7
  - First, find and download an iso
  - The OS is really old, so you'll need to follow the instructions here in order to allow it to update fully
  - Once Windows is updated, you can install all the tools you'll need via the FLARE VM
    - You may need to install powershell V3

Overview

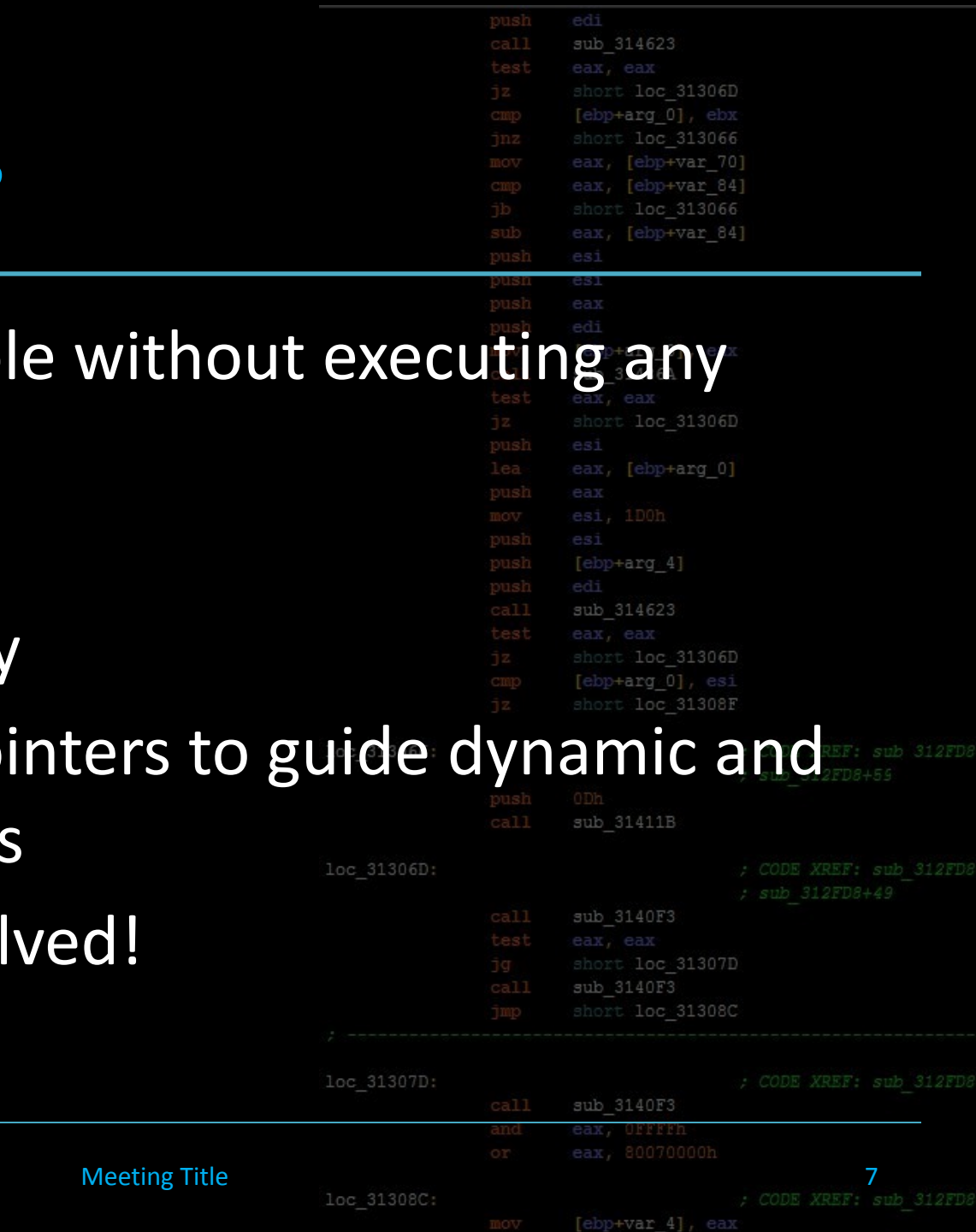
- Your malware analysis VM
- Static Analysis
- Dynamic Analysis



```
                push    edi
                call    sub_314623
                test    eax, eax
                jz      short loc_31306D
                cmp     [ebp+arg_0], ebx
                jnz     short loc_313066
                mov     eax, [ebp+var_70]
                cmp     eax, [ebp+var_84]
                jb      short loc_313066
                sub     eax, [ebp+var_84]
                push    esi
                push    esi
                push    eax
                push    edi
                mov     [ebp+arg_0], eax
                call    sub_31486A
                test    eax, eax
                jz      short loc_31306D
                push    esi
                lea     eax, [ebp+arg_0]
                push    eax
                mov     esi, 1D0h
                push    esi
                push    [ebp+arg_4]
                push    edi
                call    sub_314623
                test    eax, eax
                jz      short loc_31306D
                cmp     [ebp+arg_0], esi
                jz      short loc_31308F

loc_313066:                             ; CODE XREF: sub_312FD8
                                        ; sub_312FD8+55
                push    0Dh
                call    sub_31411B

loc_31306D:                             ; CODE XREF: sub_312FD8
                                        ; sub_312FD8+49
                call    sub_3140F3
                test    eax, eax
                jg      short loc_31307D
                call    sub_3140F3
                jmp     short loc_31308C
; ---------------------------------------------------------------------------

loc_31307D:                             ; CODE XREF: sub_312FD8
                call    sub_3140F3
                and     eax, 0FFFFh
                or      eax, 80070000h

loc_31308C:                             ; CODE XREF: sub_312FD8
                mov     [ebp+var_4], eax
```

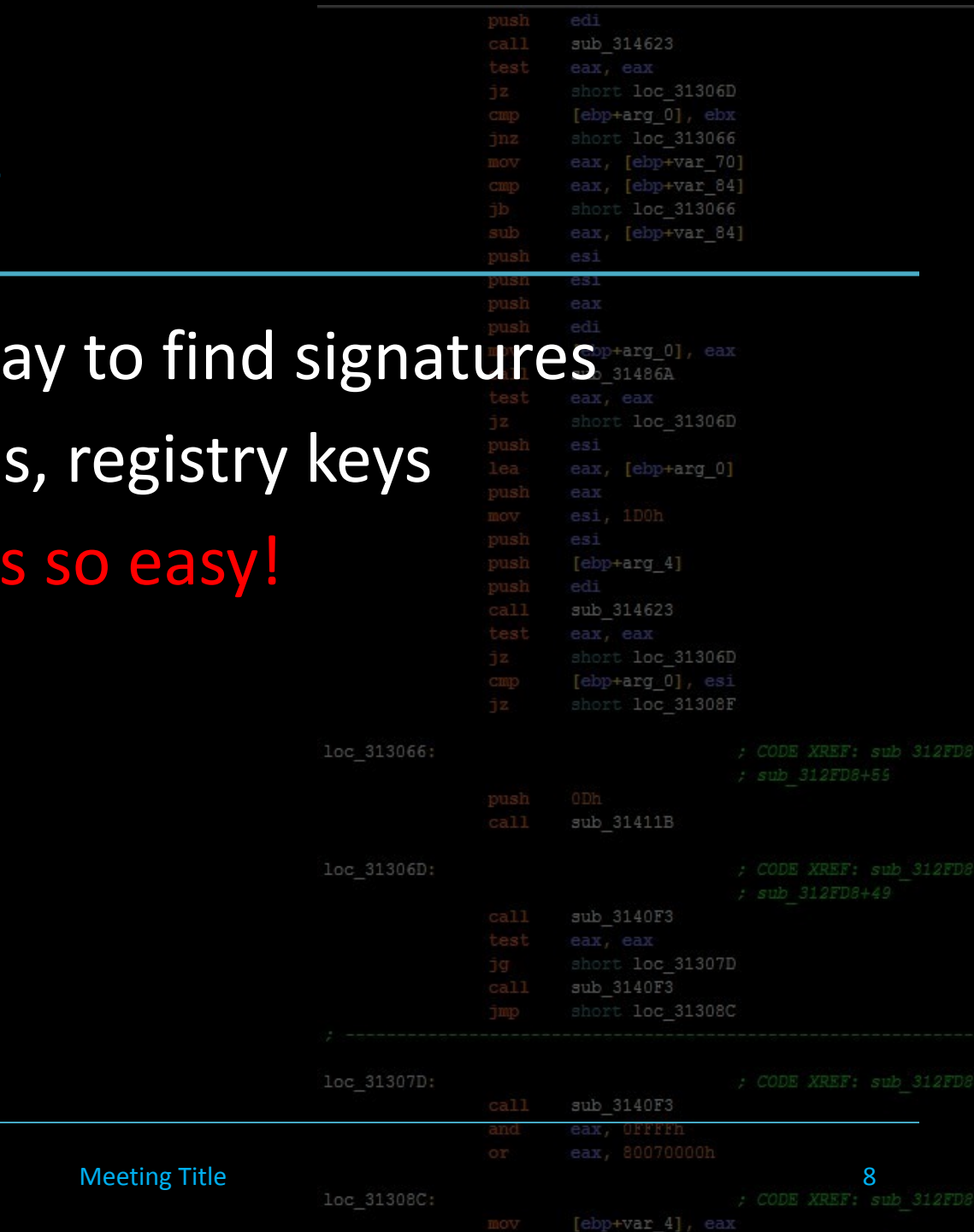
Static Analysis

- Analyzing a sample without executing any code
- Safe(r)
- Infer functionality
- Provides good pointers to guide dynamic and advanced analysis
- Lots of tools involved!



Static Analysis

- Can be an easy way to find signatures
  - URLs, filenames, registry keys
- But it's not always so easy!

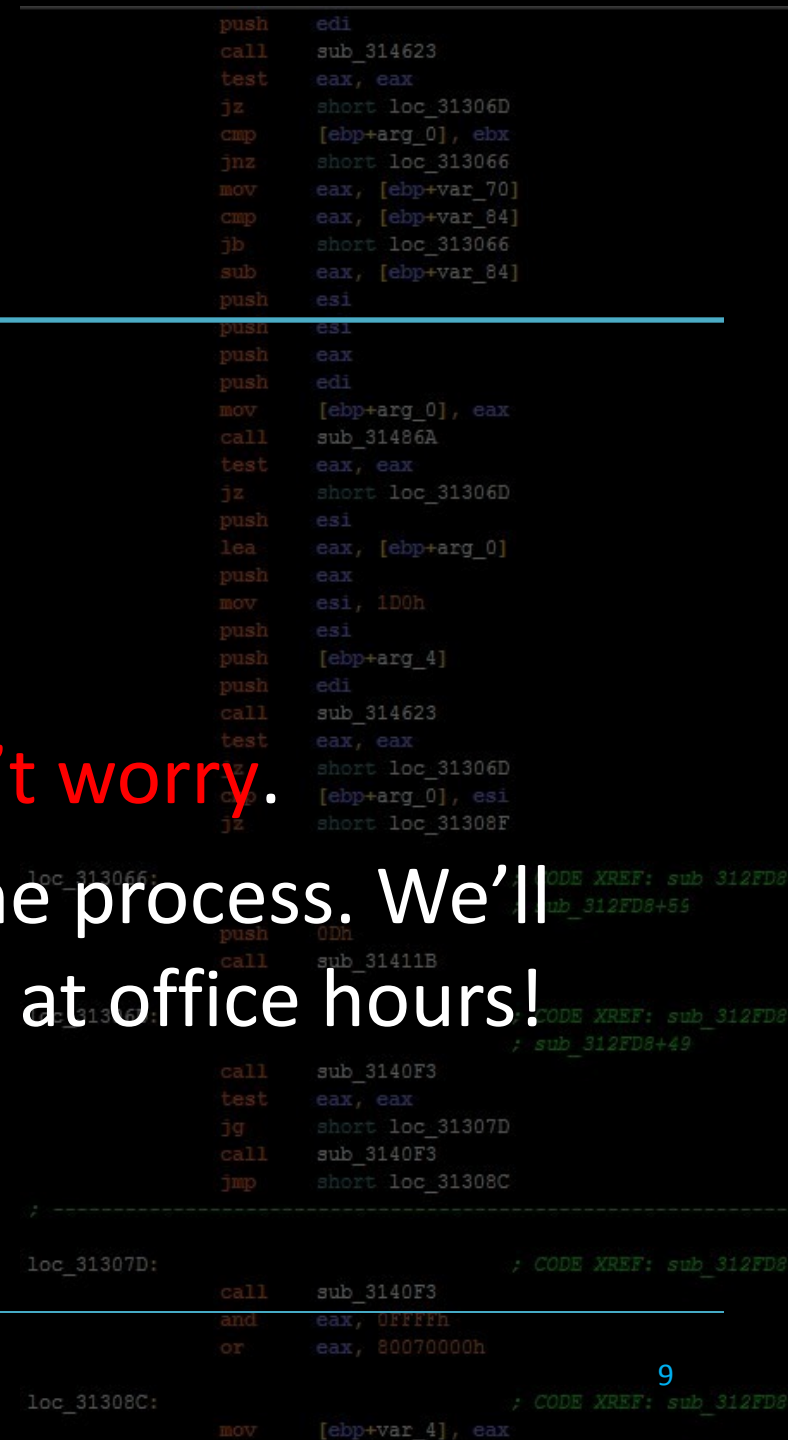


Hands on

- VM time!

If your VM isn't working, don't worry.

Just jot down the tools and the process. We'll resolve any issues and review at office hours!



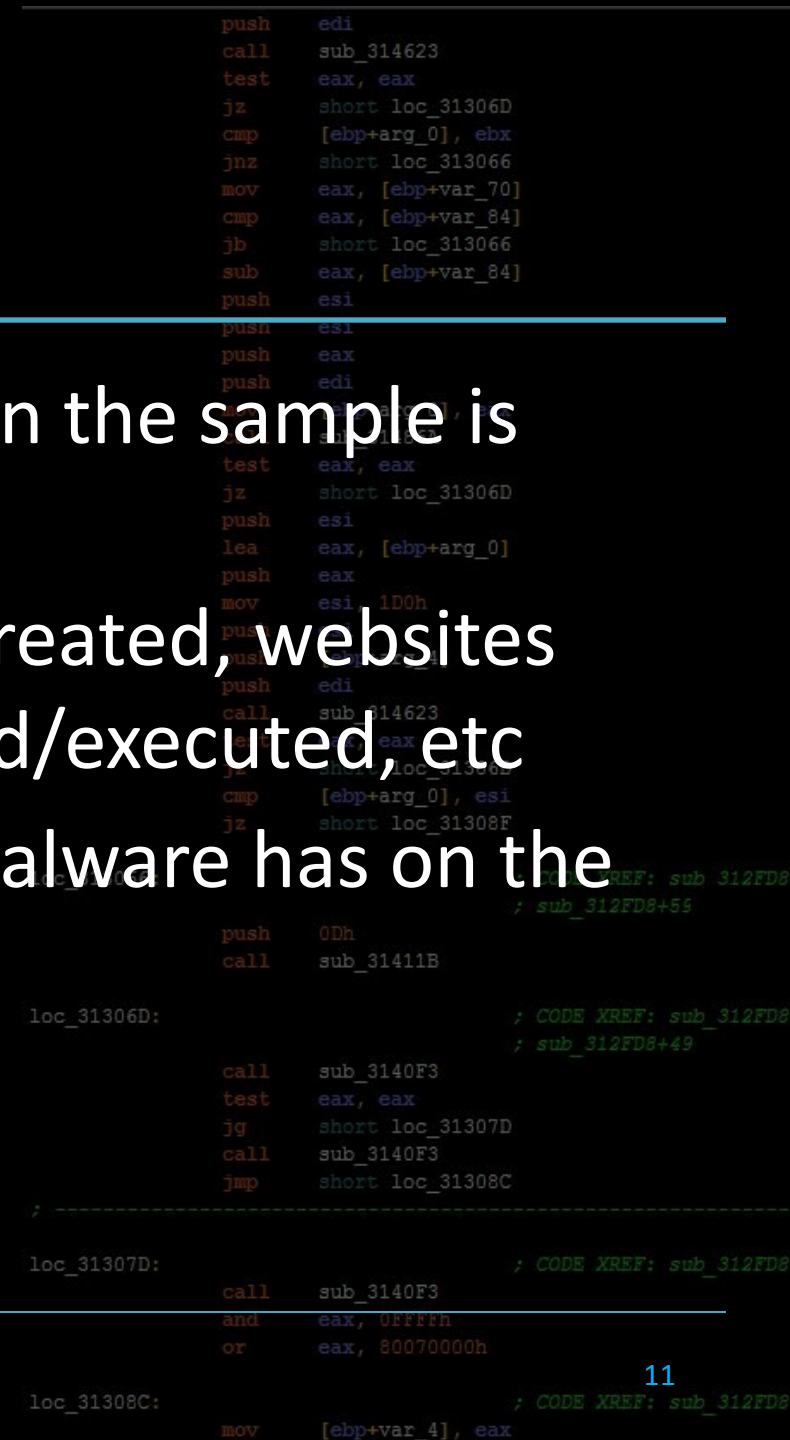
Overview

- Your malware analysis VM
- Static Analysis
- Dynamic Analysis

```
                push    edi
                call    sub_314623
                test    eax, eax
                jz      short loc_31306D
                cmp     [ebp+arg_0], ebx
                jnz     short loc_313066
                mov     eax, [ebp+var_70]
                cmp     eax, [ebp+var_84]
                jb      short loc_313066
                sub     eax, [ebp+var_84]
                push    esi
                push    esi
                push    eax
                push    edi
                mov     [ebp+arg_0], eax
                call    sub_31486A
                test    eax, eax
                jz      short loc_31306D
                push    esi
                lea     eax, [ebp+arg_0]
                push    eax
                mov     esi, 1D0h
                push    esi
                push    [ebp+arg_4]
                push    edi
                call    sub_314623
                test    eax, eax
                jz      short loc_31306D
                cmp     [ebp+arg_0], esi
                jz      short loc_31308F

loc_313066:                             ; CODE XREF: sub_312FD8
                                        ; sub_312FD8+55
                push    0Dh
                call    sub_31411B

loc_31306D:                             ; CODE XREF: sub_312FD8
                                        ; sub_312FD8+49
                call    sub_3140F3
                test    eax, eax
                jg      short loc_31307D
                call    sub_3140F3
                jmp     short loc_31308C
; ---------------------------------------------------------------------------

loc_31307D:                             ; CODE XREF: sub_312FD8
                call    sub_3140F3
                and     eax, 0FFFFh
                or      eax, 80070000h

loc_31308C:                             ; CODE XREF: sub_312FD8
                mov     [ebp+var_4], eax
```

Dynamic Analysis

- Analyze what happens when the sample is executed
- Are files made, processes created, websites contacted, files downloaded/executed, etc
- Shows you the effect the malware has on the system/network

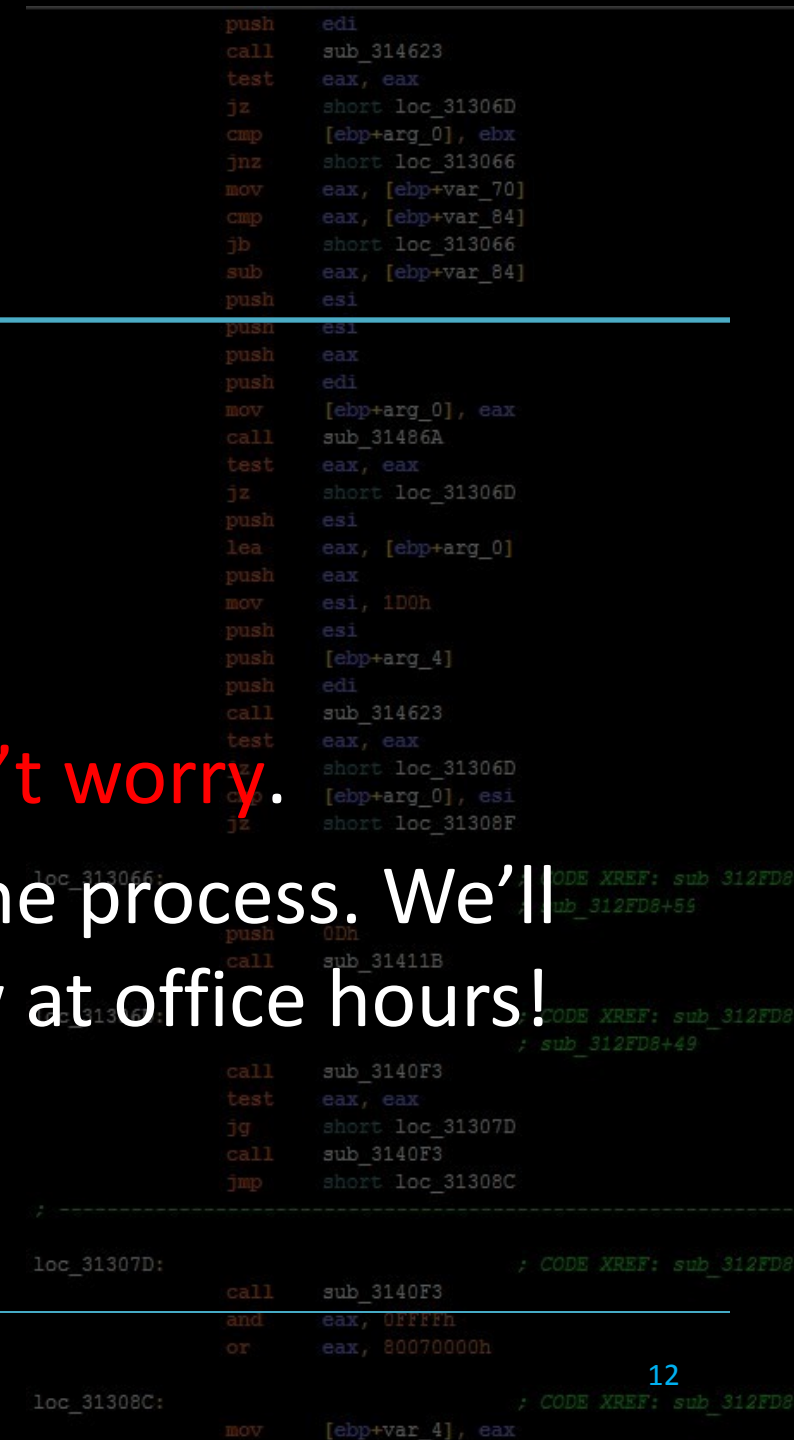


Hands on

- VM time!

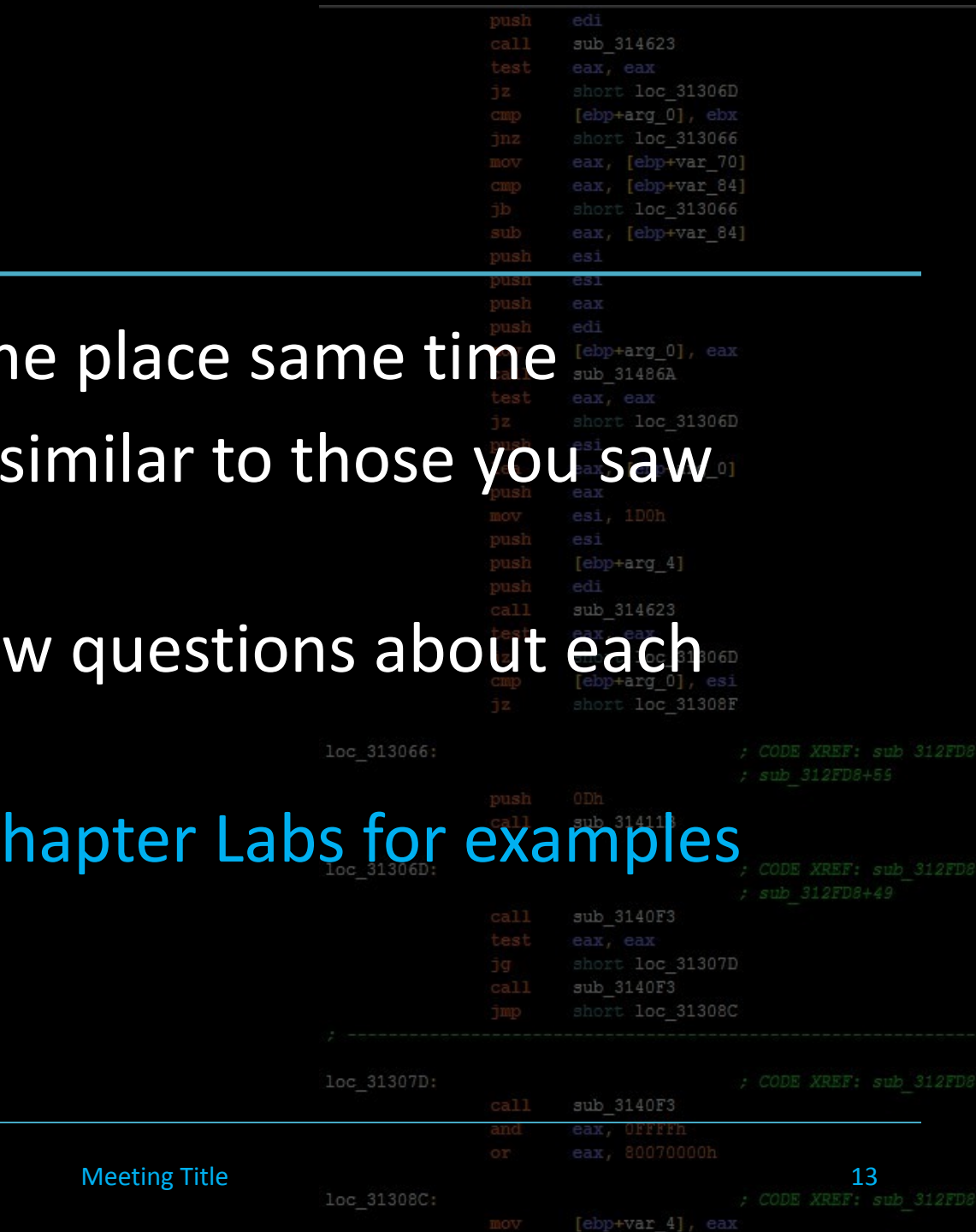
If your VM isn't working, don't worry.

Just jot down the tools and the process. We'll resolve any issues and review at office hours!



Lab

- Friday 09/04, same place same time
- Problems will be similar to those you saw today
- Must answer a few questions about each sample
  - See the PMA Chapter Labs for examples



Additional Material

- Related Readings:
  - Practical Malware Analysis
    - Chapter 1. Basic Static Analysis
    - Chapter 2. Malware Analysis in Virtual Machines
    - Chapter 3. Basic Dynamic Analysis

The chapter outlines make a great reference