Reverse Engineering

AND

Malware Analysis

Introduction to Reverse Engineering

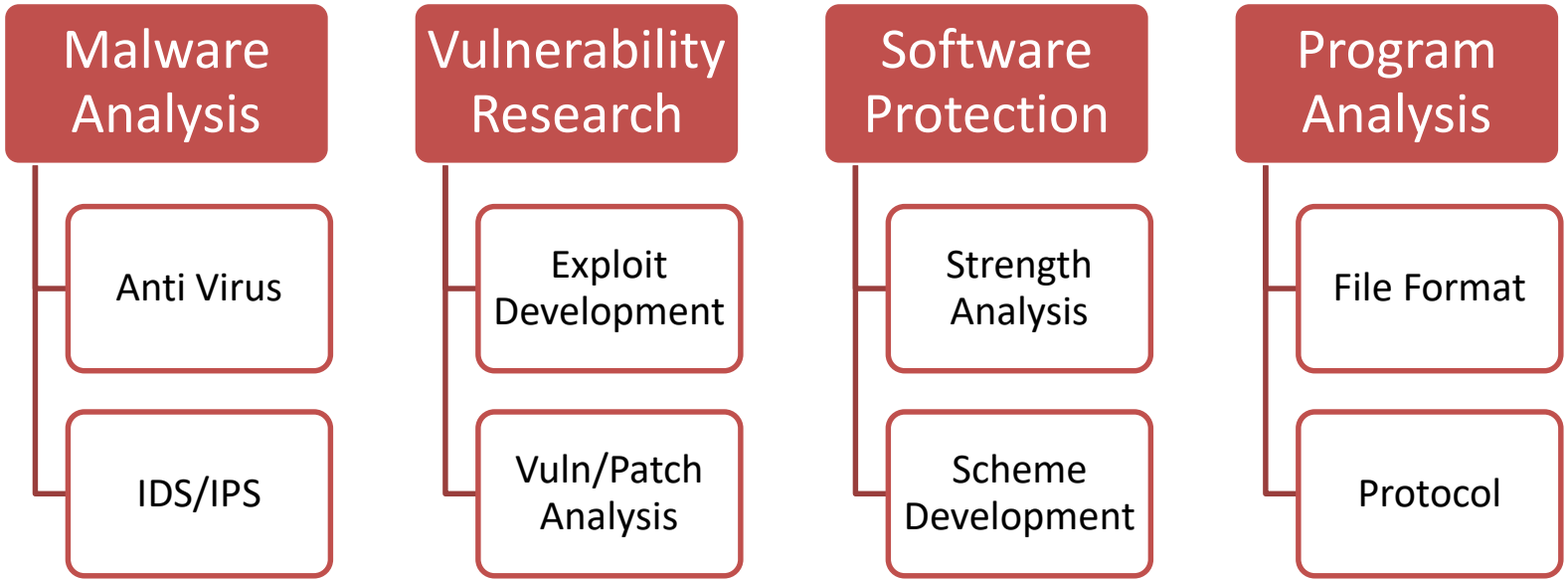
Reverse Engineering (RE): WHAT?

- In general – understanding the inner working of a system or deriving its blue prints from its functional sample can be called Reverse Engineering.

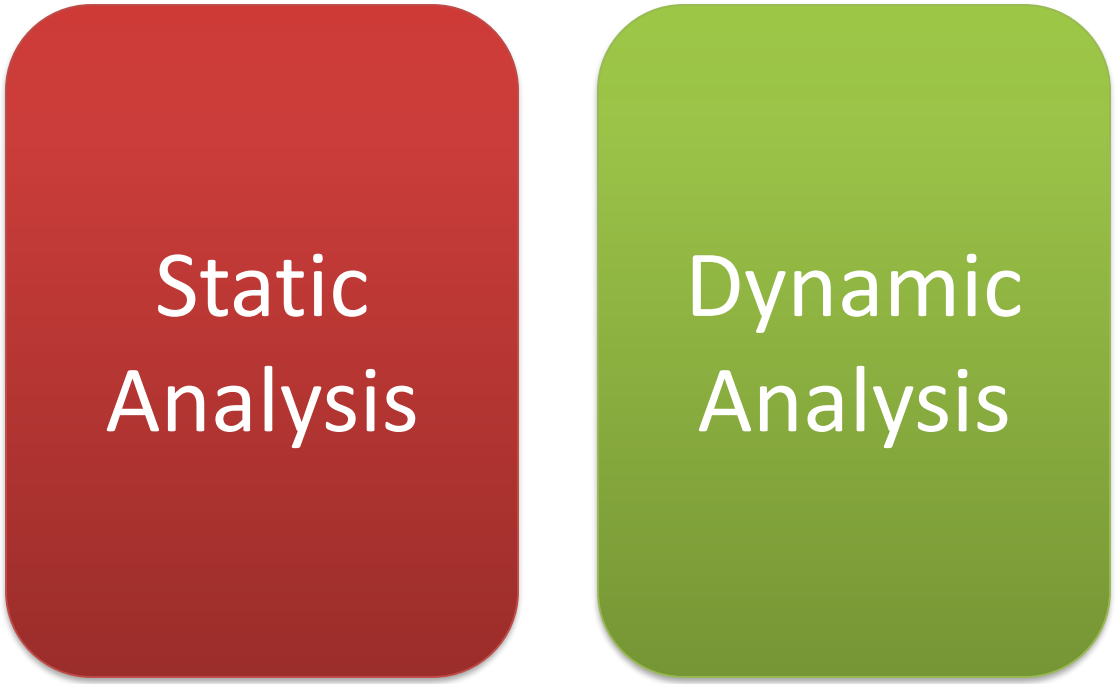
.. alternatively, quoting wikipedia:

- Reverse engineering is the process of discovering the technological principles of a device, object, or system through analysis of its structure, function, and operation.

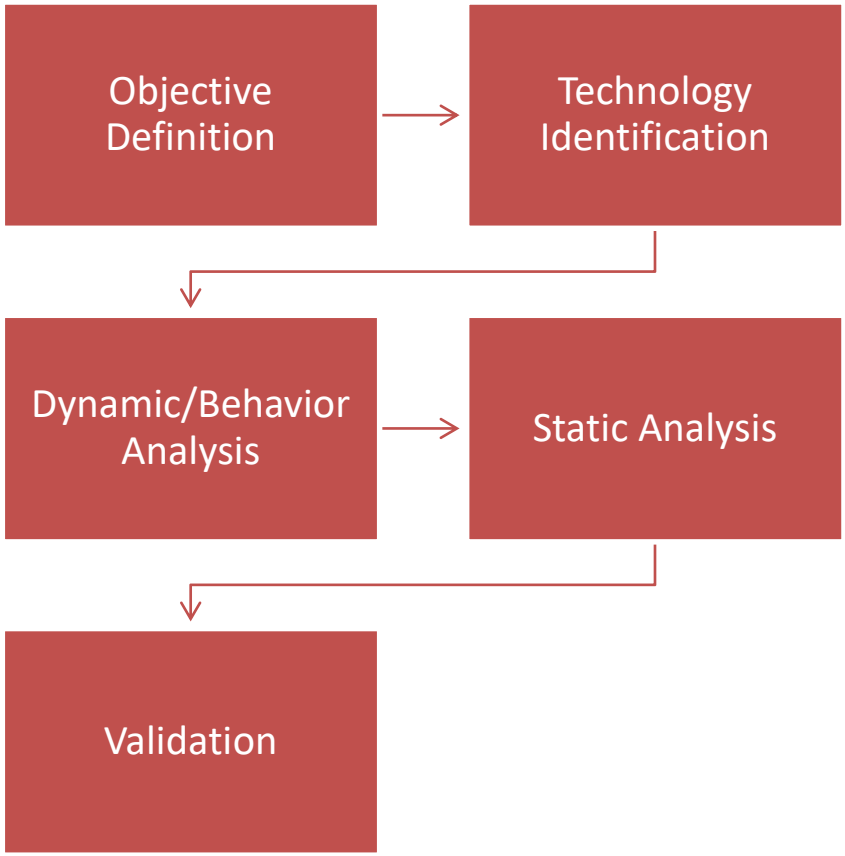
RE: Common Motivation



RE: Methodology



RE: Basic Approach

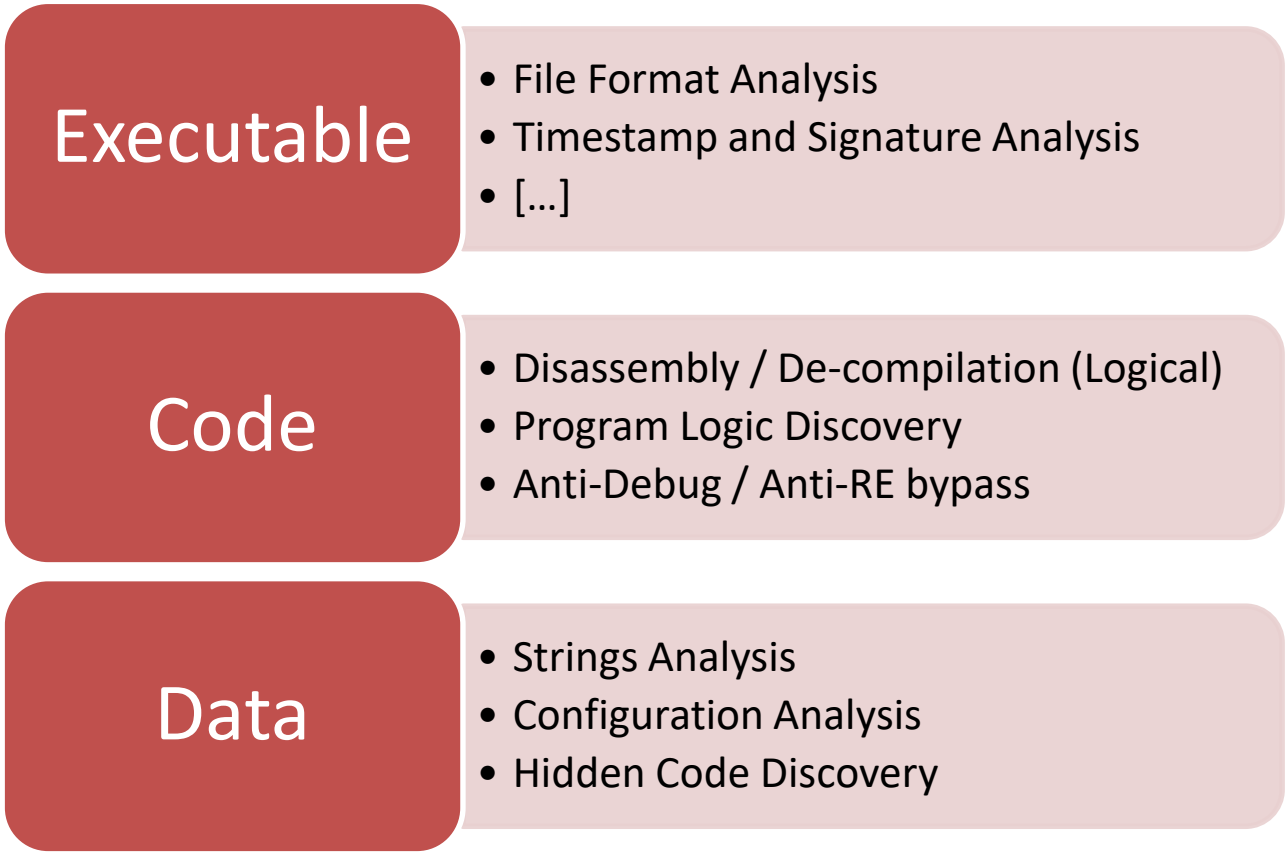


Static Analysis

- The process of identifying the behavior and characteristics of a computer program statically i.e. **without actually executing it**.

  This process is performed usually on the source code of the application or in case the source code is not available, it is subjected on the disassembled machine code of the application.

Static Analysis

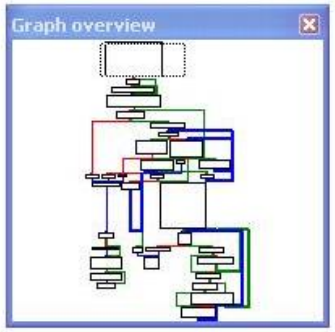


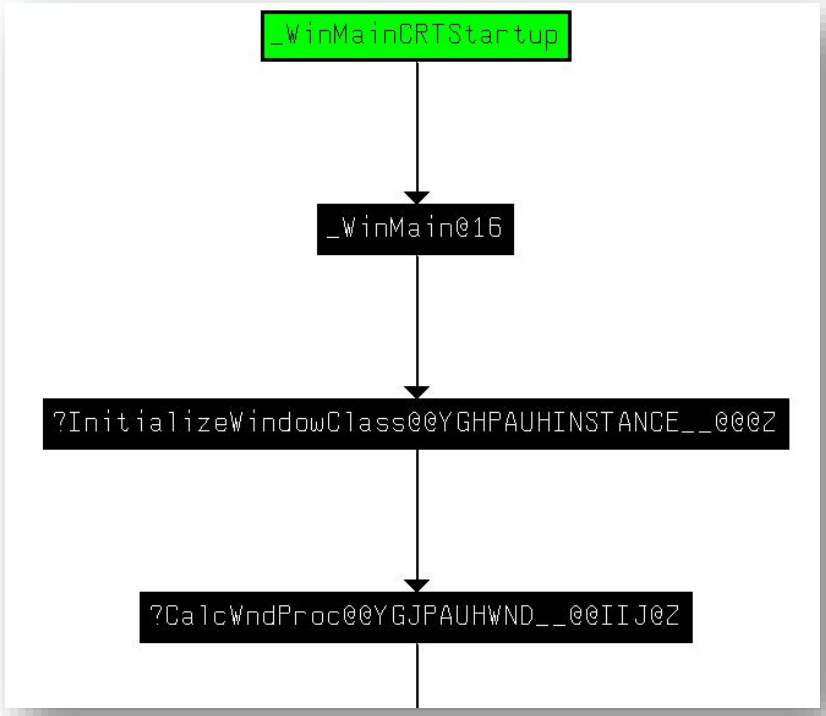
Static Analysis

```
; int __stdcall WinMain(HINSTANCE hInstance,HINSTANCE hPrevInstance,LPSTR
_WinMain@16 proc near

hInstance= dword ptr  4
hPrevInstance= dword ptr  8
lpCmdLine= dword ptr  0Ch
nShowCmd= dword ptr  10h

mov     eax, offset sub_10128EE
call    __EH_prolog
sub     esp, 0F0h
push    ebx             ; wMsgFilterMax
push    esi             ; wMsgFilterMin
push    edi             ; hWnd
mov     [ebp-10h], esp
push    31h
pop     ecx
xor     eax, eax
xor     ebx, ebx
mov     [ebp-0FCh], bx
lea     edi, [ebp-0FAh]
rep stosd
stosw
lea     eax, [ebp-18h]
push    eax             ; lpMsg
call    ds:__imp__GetProcessDefaultLayout@4 ; GetProcessDefaultLayout(x)
test    eax, eax
jz      short loc_1001FA8
```





Dynamic Analysis

- The process of identifying the program logic and behavior of a given application by means of dynamic tracing and/or instrumentation **at runtime during its execution**.

  The process usually involves hooking / intercepting various core platform APIs in order to understand its runtime characteristics.

Dynamic Analysis: Program Trace