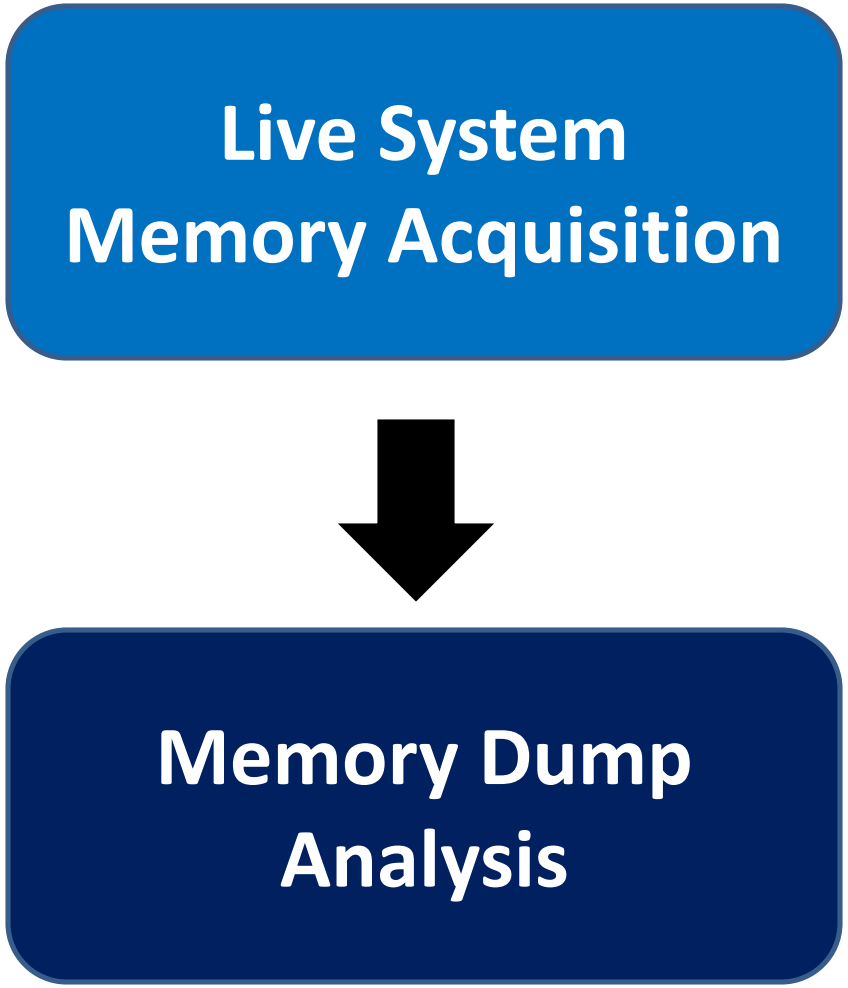
Malware Analysis

Memory Dump Analysis

What will you do if you are analyzing a system infected with **Blue Pill** or **StuxNet** or similar sophisticated malware with **rootkit** capabilities?

Can you **TRUST** your **TOOLS**


Live System
Memory Acquisition
Memory Dump
Analysis

Live System Memory Acquisition

- Virtual Machine Memory Snapshot
  - VMware
  - Virtual Box
- Live Memory Acquisition Tools
  - FastDump
  - **Win32DD** (MoonSols Windows Memory Toolkit)
  - MDD

Memory Dump Analysis

- HBGary Responder
- **Volatility**
- Memoryze
- …

Memory Dump Analysis

- The **Volatility** Project
  - Image Information
    - vol.py –f mem.dmp **imageinfo**
  - Process List
    - vol.py –f mem.dmp –profile=WinXPSP2x86 **psscan**
    - vol.py –f mem.dmp –profile=WinXPSP2x86 **psxview**
  - TCP Connection List
    - vol.py –f mem.dmp –profile=WinXPSP2x86 **connscan**
  - Open Files
    - vol.py –f mem.dmp –profile=WinXPSP2x86 **filescan**
  - Interrupt Descriptor Table
    - vol.py –f mem.dmp –profile=WinXPSP2x86 **idt**
  - Malware Scan
    - vol.py –f mem.dmp –profile=WinXPSP2x86 **malfind**

Lets get real..

HANDS-ON