Practical Malware Analysis

Ch 2: Malware Analysis in Virtual Machines

Dynamic Analysis

- Running malware deliberately, while monitoring the results
- Requires a **safe environment**
- Must prevent malware from spreading to production machines
- Real machines can be **airgapped** –no network connection to the Internet or to other machines

Real Machines

- Disadvantages
  - No Internet connection, so parts of the malware may not work
  - Can be difficult to remove malware, so re-imaging the machine will be necessary
- Advantage
  - Some malware detects virtual machines and won't run properly in one

Virtual Machines

- The most common method
- We'll do it that way
- This protects the host machine from the malware
  - Except for a few very rare cases of malware that escape the virtual machine and infect the host

VMware Player

- Free but limited
- Cannot take snapshots
- VMware Workstation or Fusion is a better choice, but they cost money
- You could also use VirtualBox, Hyper-V, Parallels, or Xen.

Windows XP

- The malware we are analyzing targets Windows XP, as most malware does
- The DVD handed out in class contains a Win XP SP3 virtual machine for you to use

Configuring VMware

- You can disable networking by disconnecting the virtual network adapter
- Host-only networking allows network traffic to the host but not the Internet

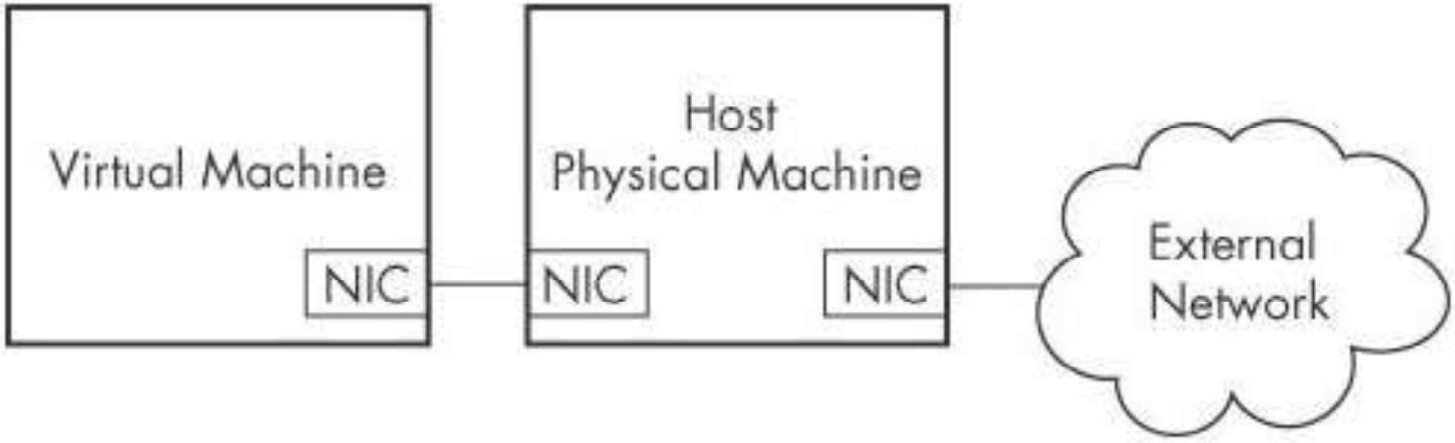


Figure 3-3. Host-only networking in VMware

Connecting Malware to the Internet

- NAT mode lets VMs see each other and the Internet, but puts a virtual router between the VM and the LAN
- Bridged networking connects the VM directly to the LAN
- Can allow malware to do some harm or spread – controversial
- You could send spam or participate in a DDoS attack

Snapshots

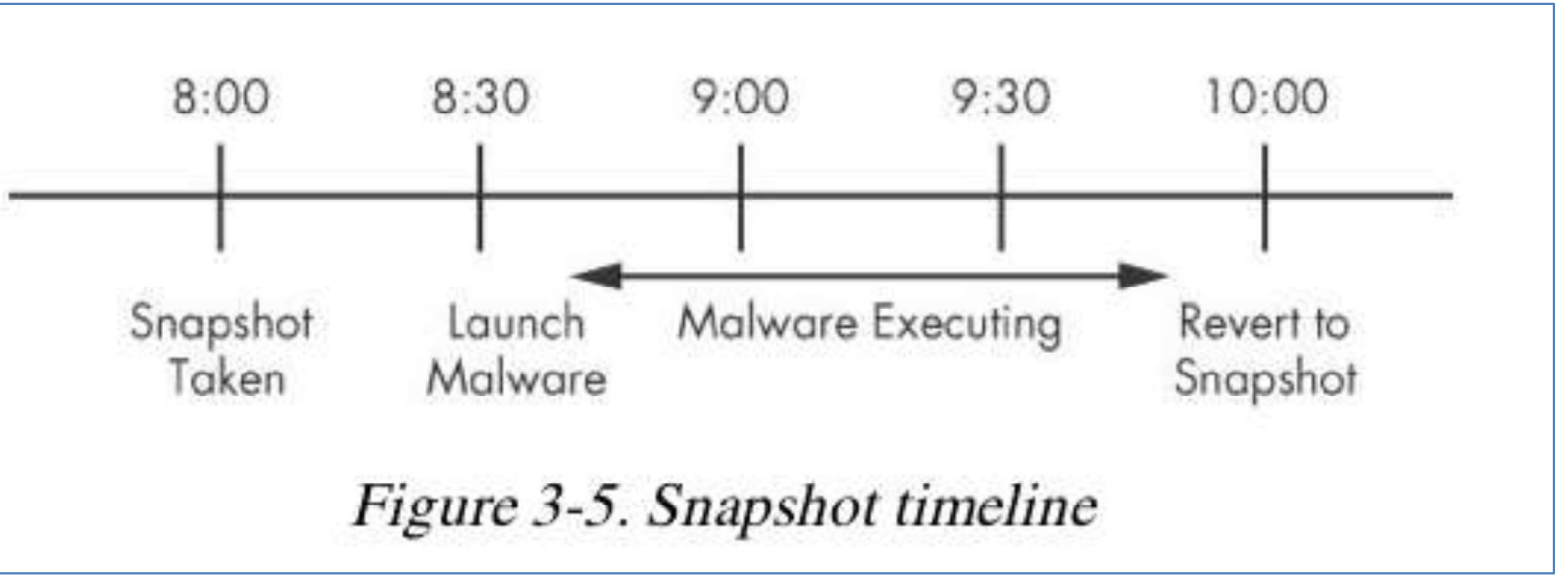


Figure 3-5. Snapshot timeline

Risks of Using VMware for Malware Analysis

- Malware may detect that it is in a VM and run differently
- VMware has bugs: malware may crash or exploit it
- Malware may spread or affect the host – don't use a sensitive host machine
- **All the textbook samples are harmless**

Practical Malware Analysis

Ch 3: Basic Dynamic Analysis

Why Perform Dynamic Analysis?

- Static analysis can reach a dead-end, due to
  - Obfuscation
  - Packing
  - Examiner has exhausted the available static analysis techniques
- Dynamic analysis is efficient and will show you exactly what the malware does

Sandboxes: The Quick-and-Dirty Approach

Sandbox

- All-in-one software for basic dynamic analysis
- Virtualized environment that simulates network services
- Examples: Norman Sandbox, GFI Sandbox, Anubis, Joe Sandbox, ThreatExpert, BitBlaze, Comodo Instant Malware Analysis
- They are expensive but easy to use
- They produce a nice PDF report of results

Running Malware

Launching DLLs

- EXE files can be run directly, but DLLs can't
- Use Rundll32.exe (included in Windows)

  rundll32.exe *DLLname, Export arguments*
- The *Export* value is one of the exported functions you found in Dependency Walker, PEview, or PE Explorer.

Launching DLLs

- Example
  - rip.dll has these exports: **Install** and **Uninstall**

    rundll32.exe rip.dll, Install
- Some functions use **ordinal** values instead of names, like

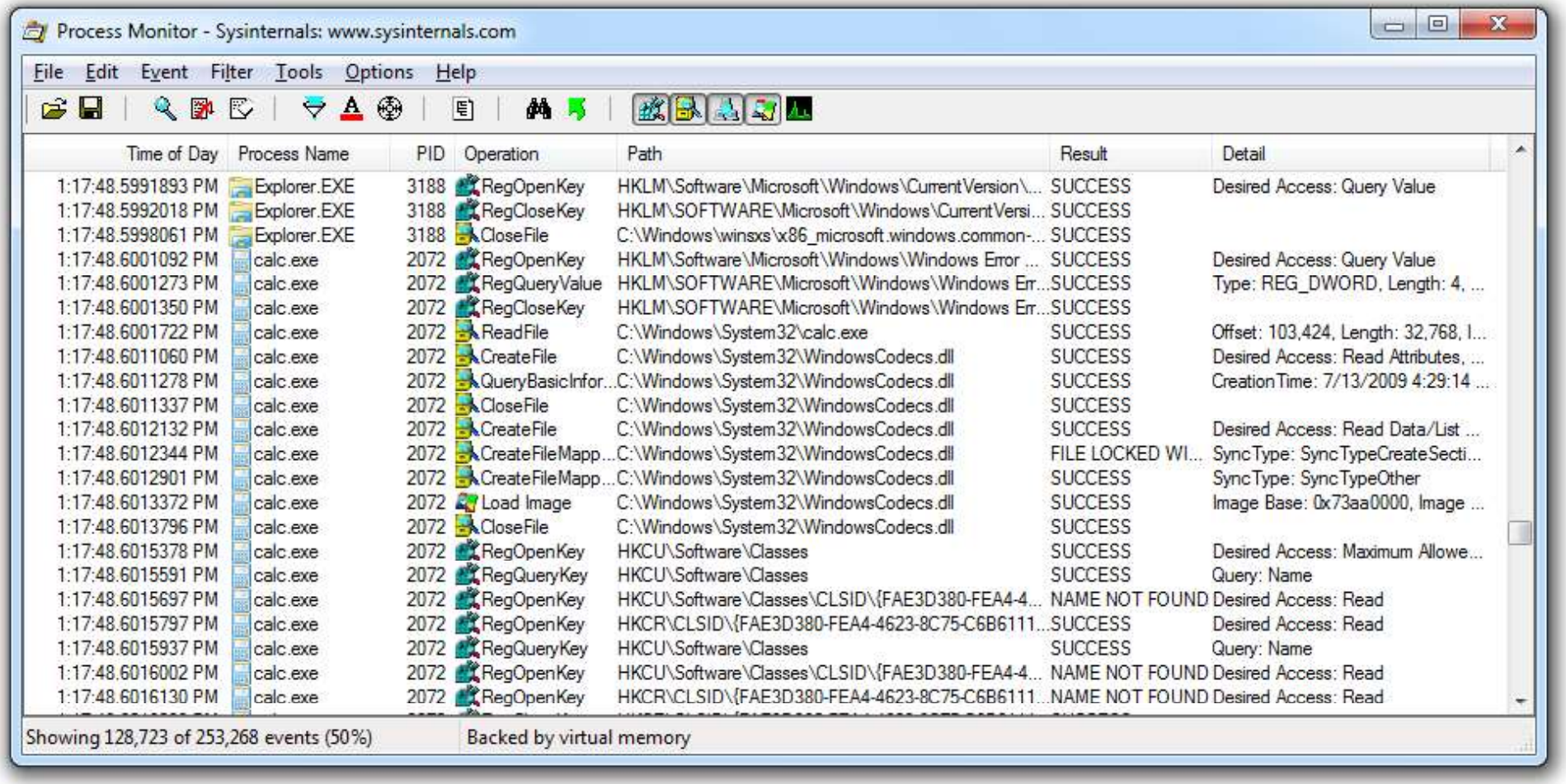
  rundll32.exe xyzzy.dll, #5
- It's also possible to modify the PE header and convert a DLL into an EXE

Monitoring with Process Monitor

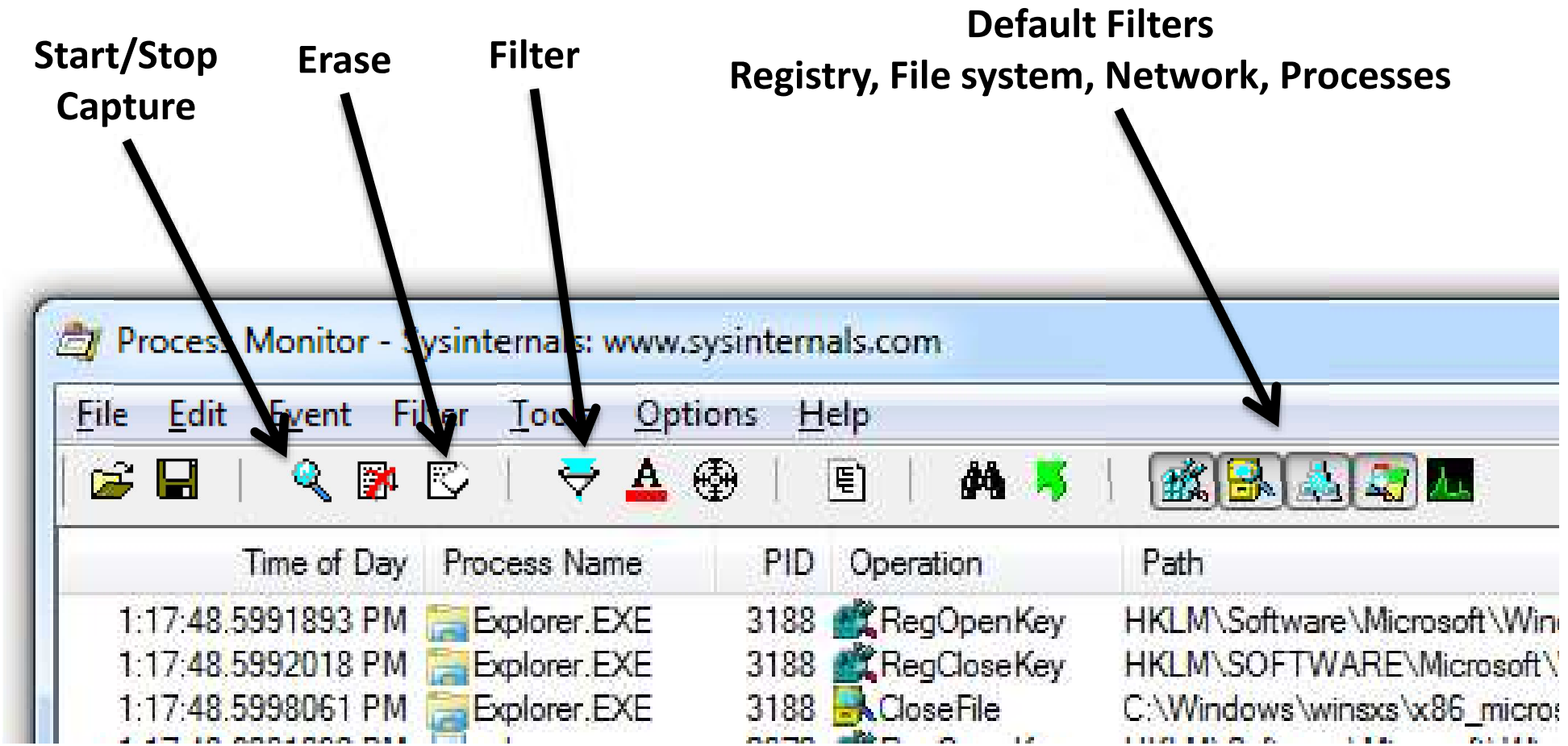
Process Monitor

- Monitors registry, file system, network, process, and thread activity
- All recorded events are kept, but you can filter the display to make it easier to find items of interest
- Don't run it too long or it will fill up all RAM and crash the machine

Launching Calc.exe



Process Monitor Toolbar



Filtering with Exclude

- One technique: hide normal activity before launching malware
- Right-click each Process Name and click **Exclude**
- Doesn't seem to work well with these samples

Filtering with Include

- Most useful filters: Process Name, Operation, and Detail