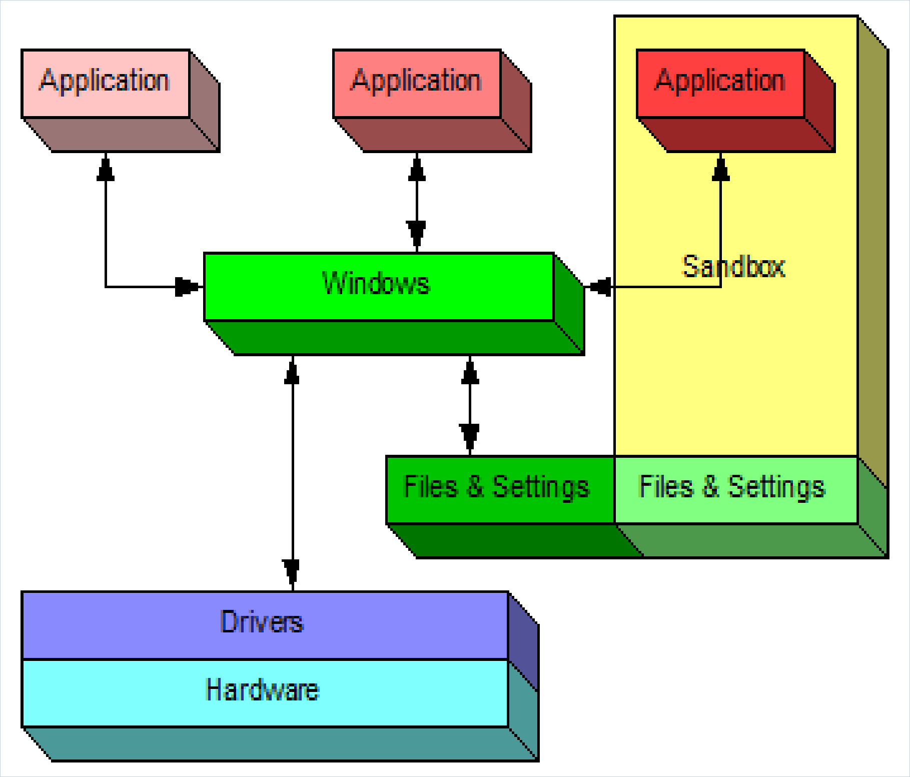
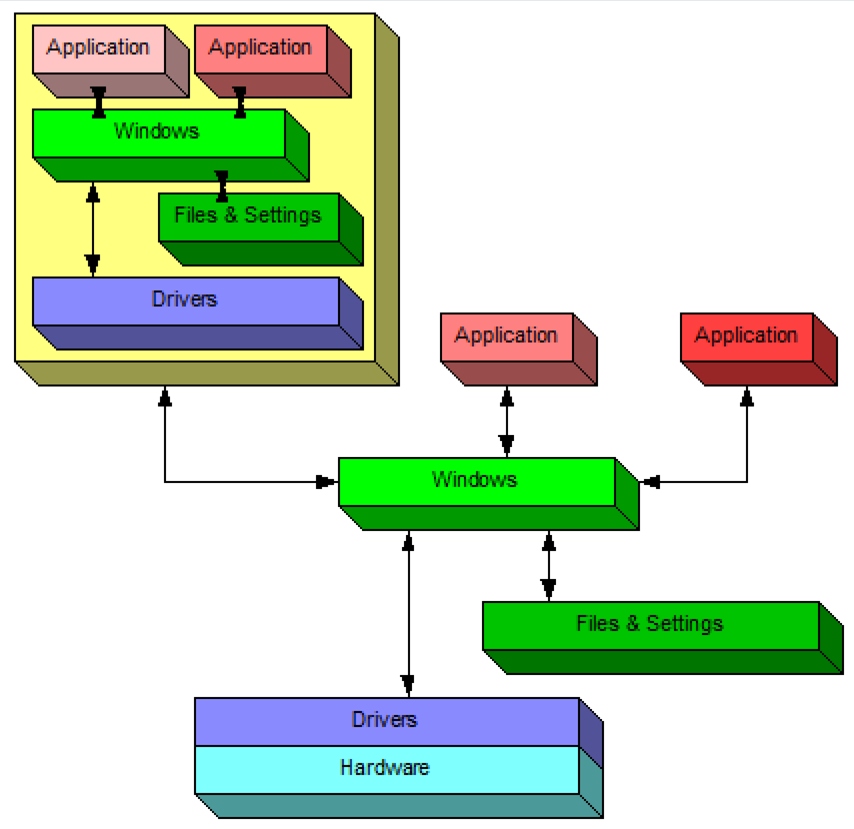
Lab 5: Sandbox Setup and Configuration

Because teaching teaches
teachers to teach

Sandbox vs virtual machine



Sandbox vs virtual machine



Some SandBox

- VirusTotal
- Anubis
- VxStream
- Malwr
- SandSift

SANS Investigative Forensic Toolkit (SIFT) Workstation

- An international team of forensics experts CREATED SIFT Workstation for incident response and digital forensics use. The free SIFT that can match any modern incident response and forensic tool suite.
- It demonstrates that advanced investigations and responding to intrusions can be accomplished using cutting-edge open-source tools that are freely available and frequently updated.

Key new features of SIFT

- Ubuntu LTS 16.04 Base
- 64 bit base system
- Better memory utilization
- Auto-DFIR package update and customizations
- Latest forensic tools and techniques
- VMware Appliance ready to tackle forensics
- Cross compatibility between Linux and Windows
- Option to install stand-alone via (.iso) or use via VMware Player/Workstation
- Online Documentation Project at http://sift.readthedocs.org/
- Expanded Filesystem Support

Two ways to install SIFT

- Download SIFT Workstation VMware Appliance Now - 2.4 GB (https://digital-forensics.sans.org/community/download-sift-kit/3.0)
- Install for yourself (https://github.com/sans-dfir/sift-cli#instructions)

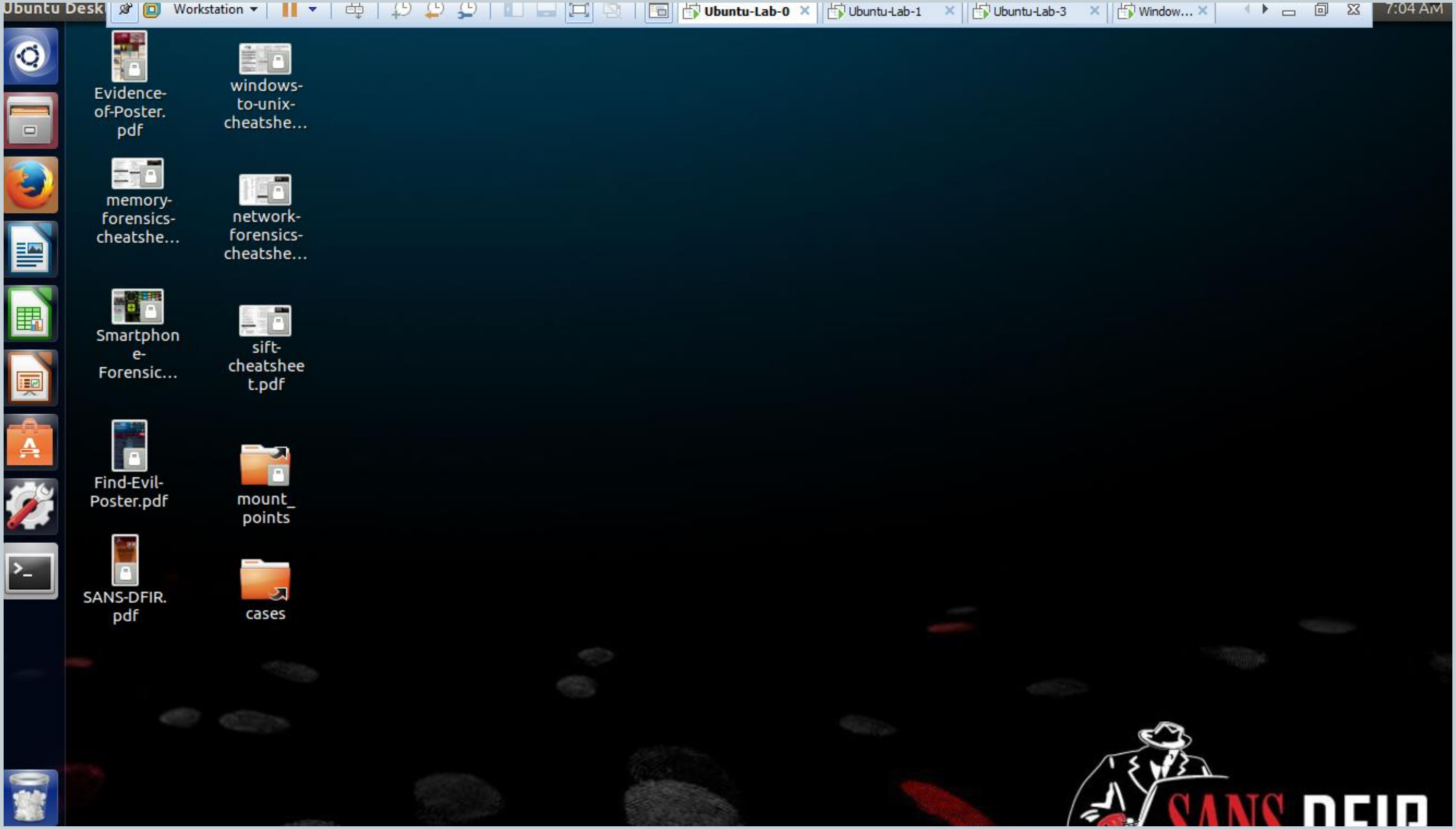
Install for yourself

- Go to the Latest Releases
- Download all the release
  - filessift-cli-linux
  - sift-cli-linux.sha256.asc
- Import the PGP Key - gpg --keyserver pgp.mit.edu --recv-keys 22598A94
- gpg –verify sift-cli-linux.sha256.asc
- shasum -a 256 -c sift-cli-linux.sha256.asc OR sha256sum -c sift-cli-linux.sha256.asc

Install for yourself

- mv sift-cli-linux /usr/local/bin/sift
- chmod 755 /usr/local/bin/sift
- Type sift --help to see its usage
- sift install
- Sift update

Install successfully



Q & A