Intro to Packet Analysis Exercise Requirements

During this class on packet analysis, we will use tcpdump, Wireshark, and several Linux command-line tools for text parsing. All the tools will run natively on Linux, MacOS, or Windows 10 with the Linux Subsystem for Windows. Kali Linux is the preferred OS (either on physical or virtual) since it has all the tools and you can experiment with Scapy using it. No exercises explicitly require its use though. Windows 7 instructions are located at the end of the document.

# Windows 10 Instructions

1. Install the Windows Subystem for Linux (WSL)
   1. Instructions - <https://docs.microsoft.com/en-us/windows/wsl/install-win10>
   2. Use the Windows store to download Debian
   3. Start the Debian application
   4. sudo apt-get update && sudo apt-get install wireshark && sudo apt-get install tcpdump

# Linux Instructions

Linux distributions, such as Kali Linux (https://www.kali.org/downloads/) and Security Onion (https://github.com/Security-Onion-Solutions/security-onion/blob/master/Verify\_ISO.md), already have all necessary software installed.

This will depend upon your distribution. Use your package manager to install tcpdump and wireshark:

-sudo apt-get update && sudo apt-get install wireshark && sudo apt-get install

-sudo yum install wireshark && sudo yum install tcpdump

# MacOSX

Full disclosure, I haven’t tried this but…

<https://theagileadmin.com/2017/05/26/tcpdump-and-wireshark-on-osx/>

# Windows 7 Instructions

If Windows 7 is the available operating system, there are several free ways to acquire the necessary tools. Any of these three options will work, just pick one:

1. VMware Workstation Player
   1. VMWare Workstation Player lets you run a Virtual Machine without disturbing your host operating system.
   2. Instructions - <https://www.pentestingshop.com/how-to-install-kali-linux-in-vmware-player/>
   3. VMWare Workstation Player Download - <https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/14_0>
   4. Kali Linux Download <https://www.kali.org/downloads/>
2. VirtualBox
   1. Virtualbox lets you run a Virtual Machine without disturbing your host operating system. First install Virtualbox and then set up a Kali Virtual Machine.
   2. Instructions - <https://www.blackmoreops.com/2014/04/08/detailed-guide-installing-kali-linux-on-virtualbox/>
   3. VirtualBox Download - <https://www.virtualbox.org/wiki/Downloads>
   4. Kali VirtualBox Image Download - <https://www.kali.org/downloads/>
3. Linux Live Image
   1. This is just Kali Linux on a bootable USB drive. This will not affect your main operating system.
   2. Instructions - <https://docs.kali.org/downloading/kali-linux-live-usb-install>
   3. Kali Download - <https://www.kali.org/downloads/>