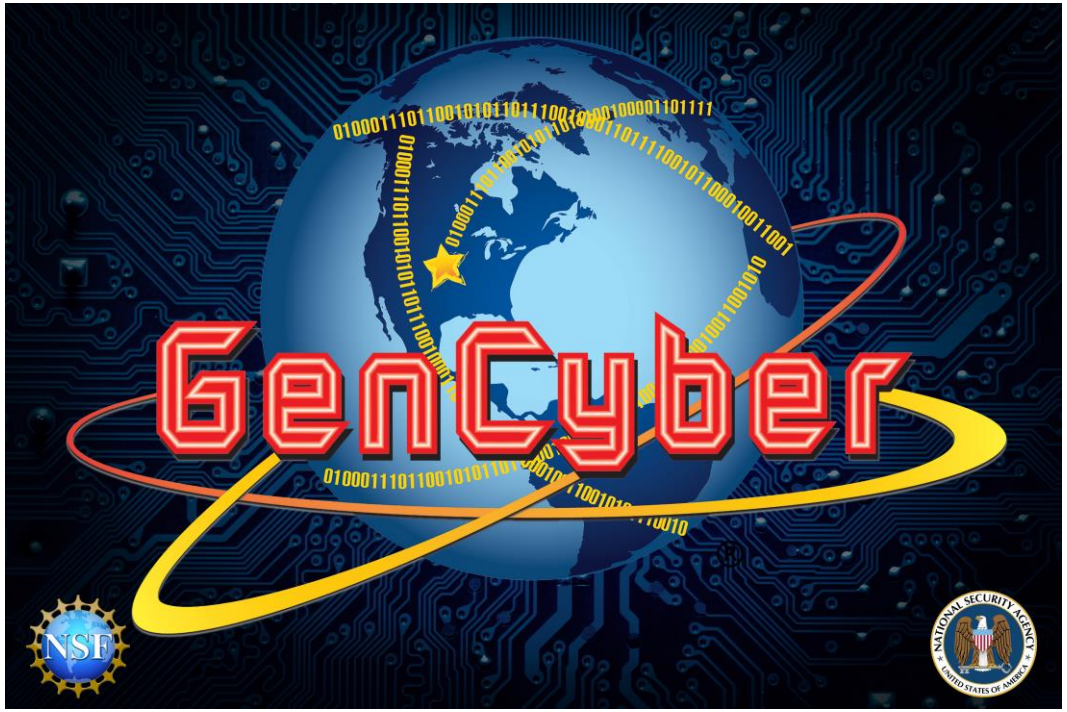


Workshop Agenda

January 2022 – Extension Activity

22 Jan 2022

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

Agenda

- 11-11:15: **Loyce** overview of workshop, the GenCyber program and other UMCG programs, events, degrees, certs for teachers
- 11:15-11:25: **Shannon** - Overview of the day, Agenda review, RPi review, lab kickoff
- 11:30-12:30: **Kim** - Intro to Linux Lab
- 12:30-1:00 - Break for lunch
- 1:00-2:00: **Shannon** - Wireshark lab
- 2:00-2:15 Break
- 2:15-3:15 **Jonathan** and password auditing
- 3:15-3:30 Wrap-up
  - **Team** - answer any outstanding questions
  - **Loyce** - discuss future sessions and requirements for program
  - Thank you's :-)

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

Workshop Overview

Using the Kali OS running on the Raspberry Pi (RPi)

- Introduce the affordable hardware environment of the RPi
- Practice using Kali Linux and Linux commands at a command line interface (CLI)
- Explore a few of the many pre-installed cybersecurity-related programs on Kali Linux

Organization of the Workshop

- Introduction / Practice with Kali
- Network forensics with Wireshark
- Password auditing using John the Ripper

Raspberry Pi 400

- Complete personal computer, built into a compact keyboard
- Purpose-built board based on Raspberry Pi 4
  - Quad-core 64-bit processor
  - 4GB of RAM
  - Wireless networking
  - Dual-display output and 4K video playback
  - 40-pin GPIO header

- This is what you were sent!

https://www.raspberrypi.com/products/raspberry-pi-400/

Overall Setup of Raspberry Pi 400

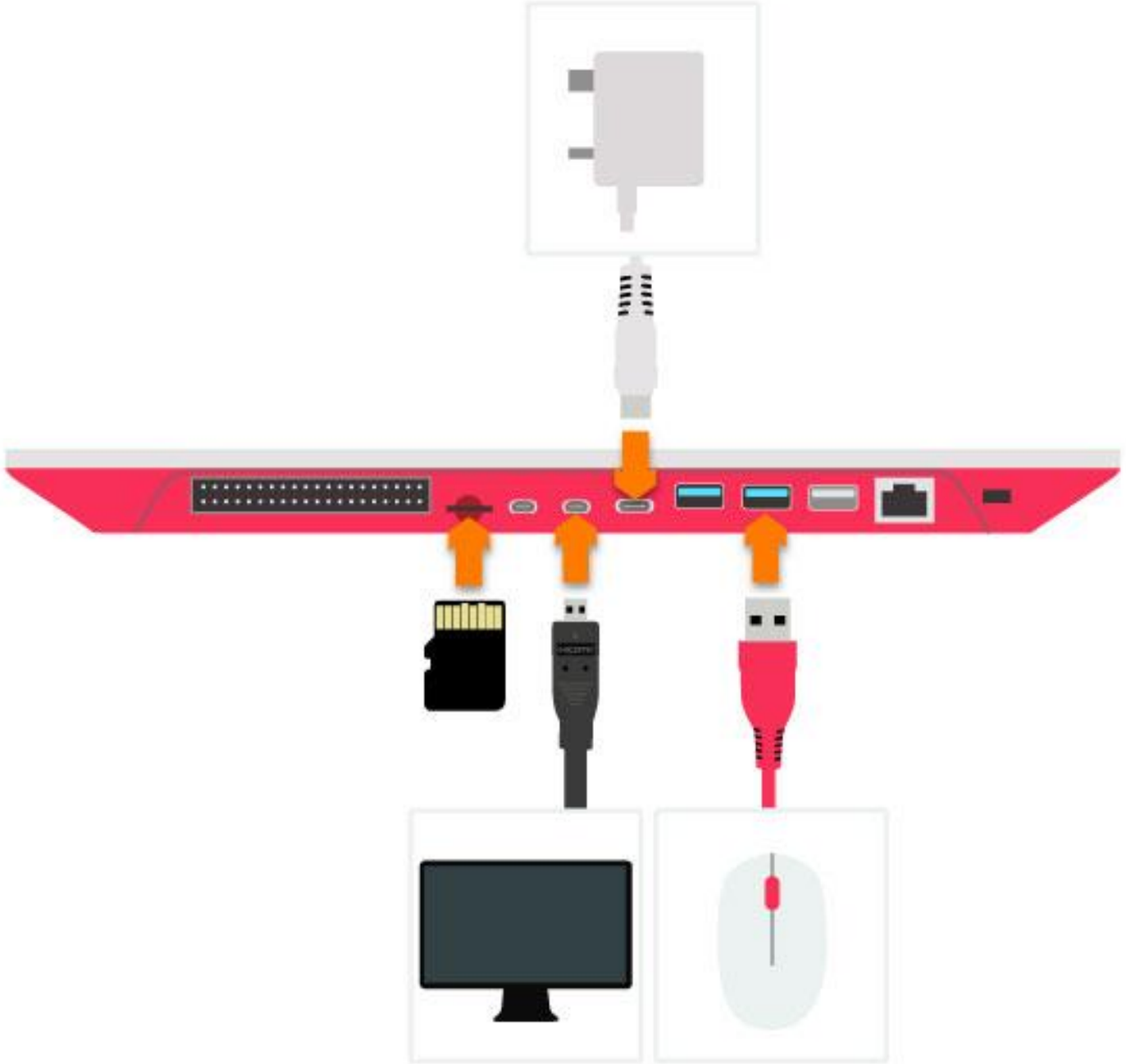
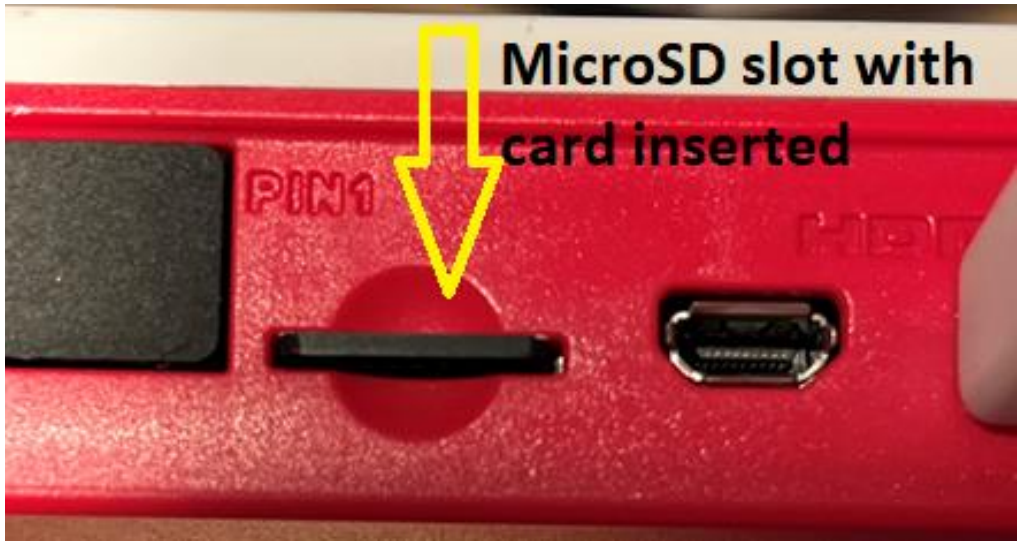


Image from:
https://www.okdo.com/getting-started/get-started-with-raspberry-pi-400/

Rear of Raspberry Pi 400

- All necessary connections made
- Mouse (USB)
- Monitor (microHDMI)
- Power (USB C)

Before Powering Up - Swap the MicroSD Card

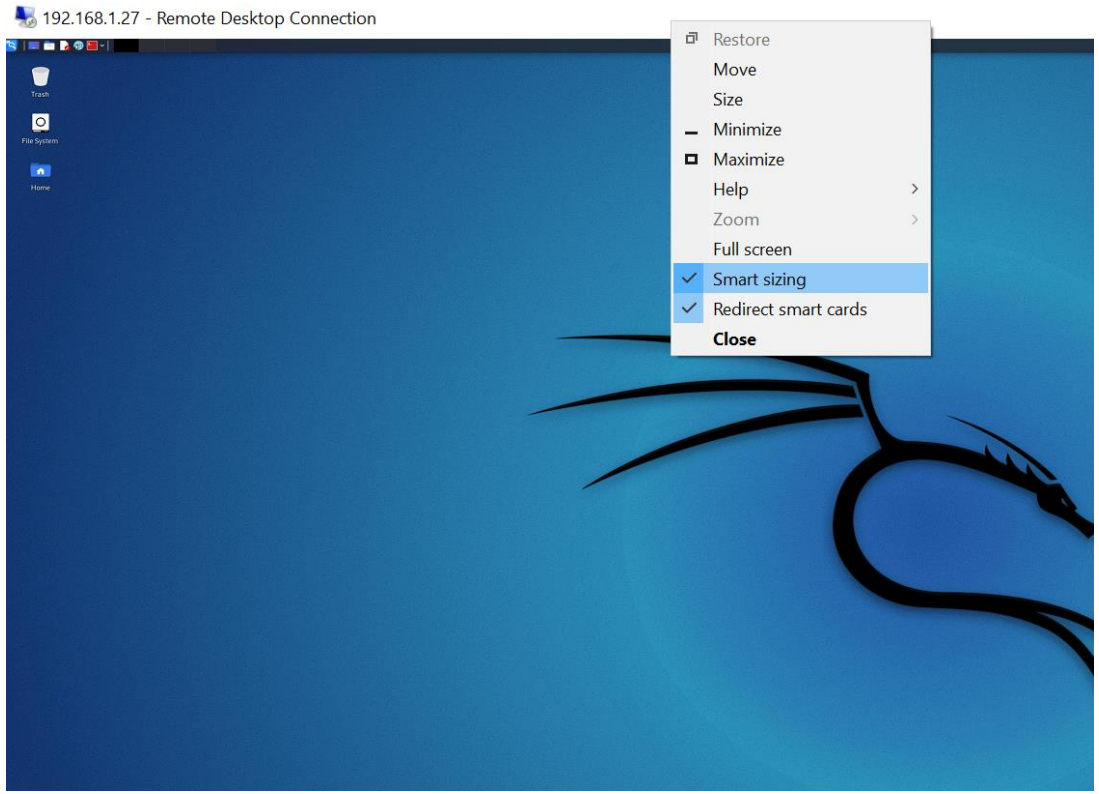


- If you already have a microSD card inserted, replace it with the 32-bit Kali OS for RPi that was shipped to you.
- Push in and when the card pops out, remove it and replace it.
- Be sure the pins are facing toward the bottom of the keyboard *and* that you completely push and lock the microSD card into the slot

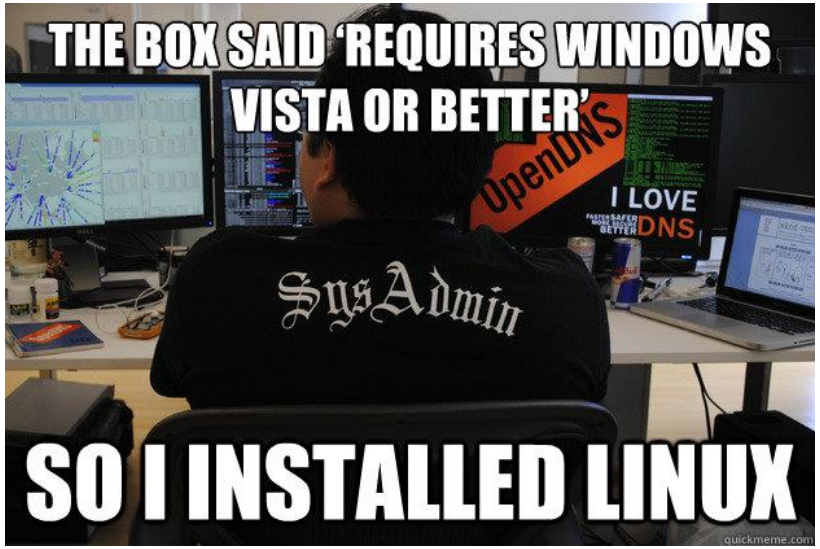
Booting the System

- Turn on your monitor
- Connect the power
- Wait for system to boot
  - Text will roll by – expected!
- Login to system
  - Username: kali
  - Password: kali

- Open a program
  - Such as Internet browser
- Open a command line terminal
  - Run command such as “ls” to list directory contents



Intro to Linux Lab

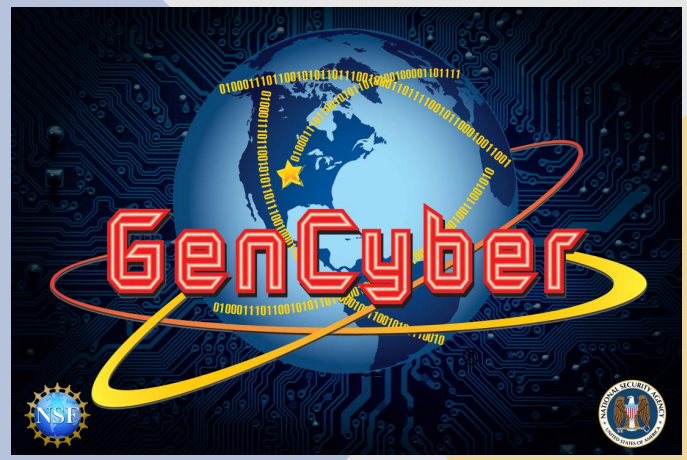


Kim Mentzell

11:30-12:30

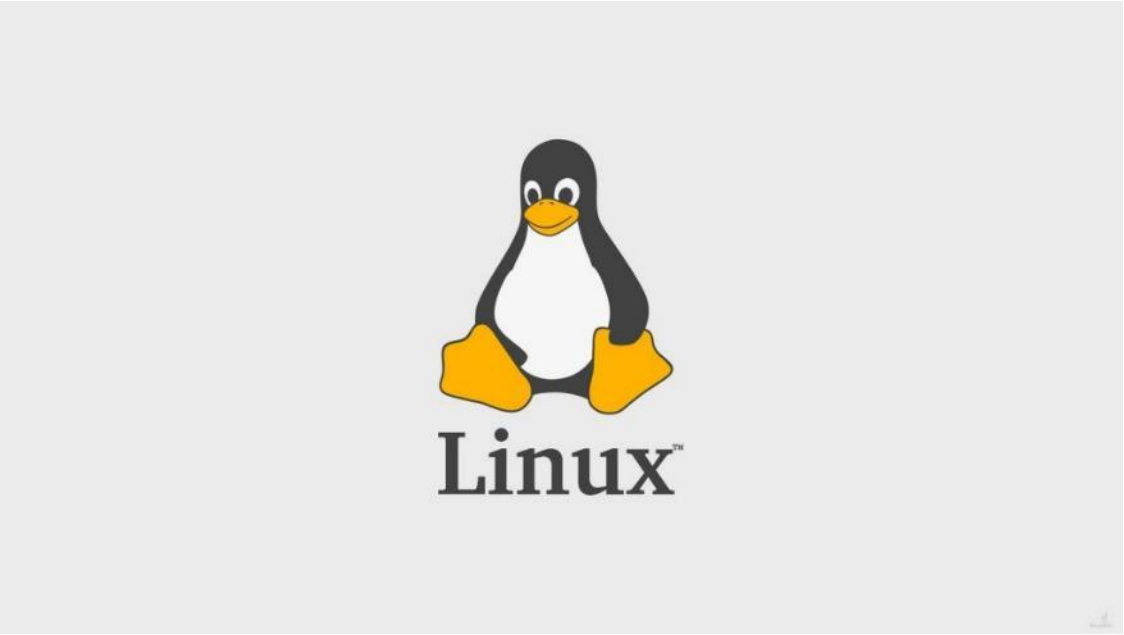
UNIVERSITY OF MARYLAND
GLOBAL CAMPUS

Introduction to Linux



What we are going to cover

- What is Linux?
- How do we use Linux?
- What are Linux Distributions?
- Simple Linux commands
- What can you do with Linux?



UNIVERSITY OF MARYLAND
GLOBAL CAMPUS

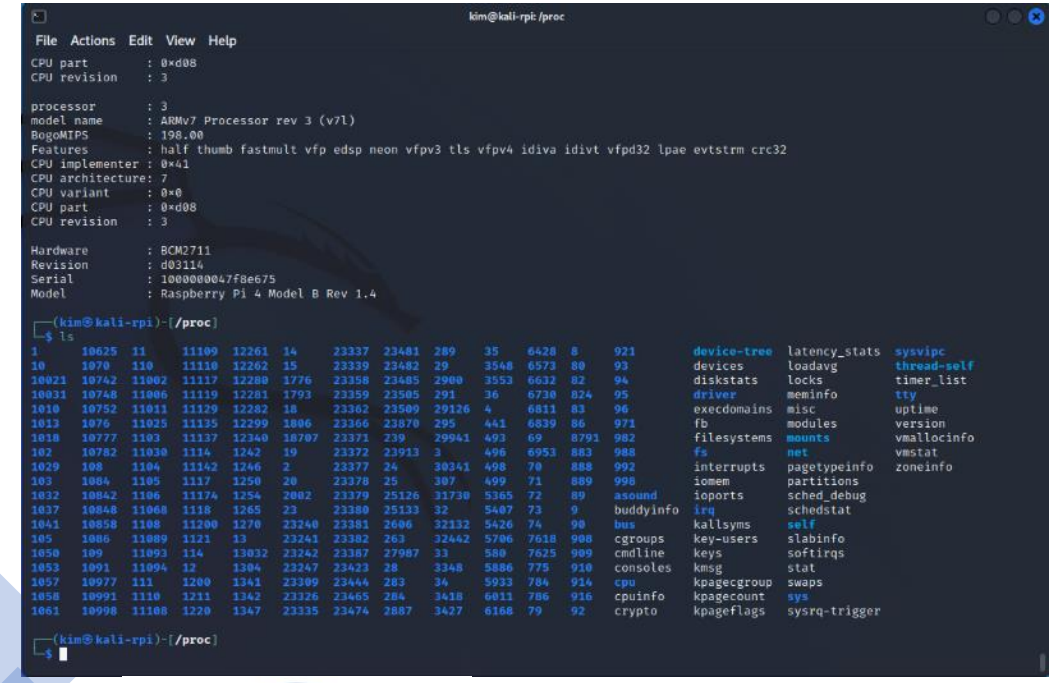
What is Linux?

- Linux is an operating system written by volunteers called contributors
- Linux allows you to use computer hardware to do things
- The Linux ecosystem provides tools to run varied services such as web services or compute modules for advanced AI

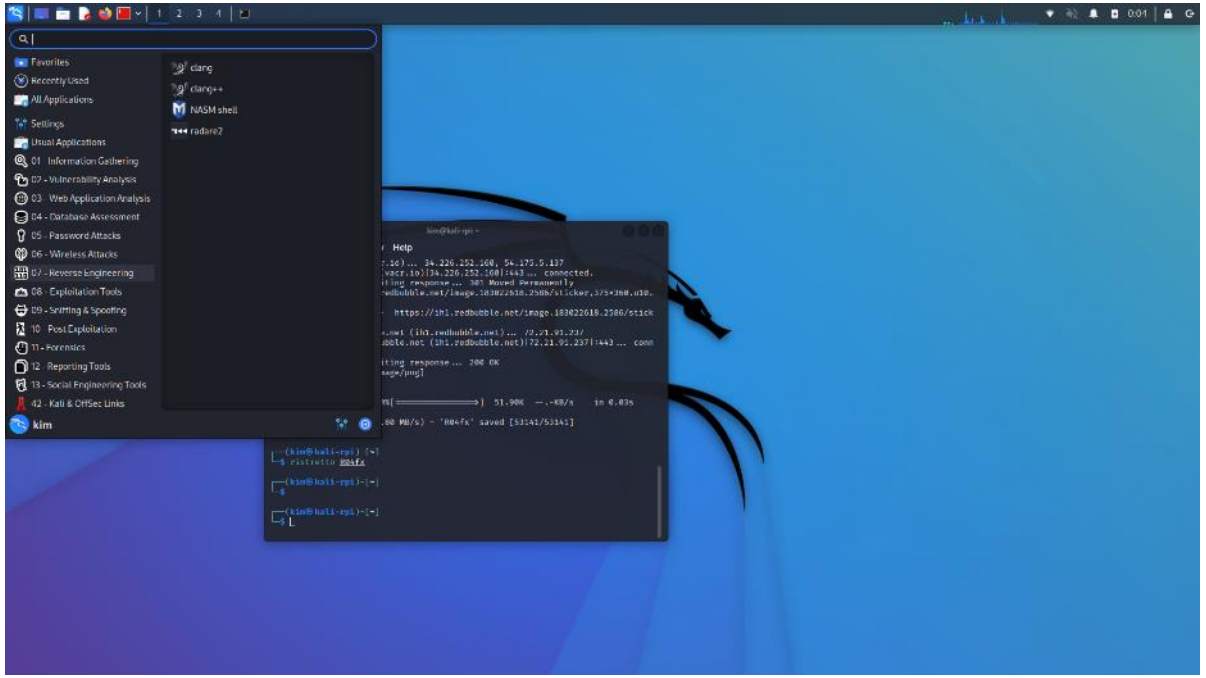
UNIVERSITY OF MARYLAND GLOBAL CAMPUS

How do we use Linux?

Command Line



Graphical User Interface



What is a Linux Distribution?

- A Distribution is a series of packages bundled together by a group of maintainers.
- The packages and the kernel (heart) make up a Distribution.
- Some Distributions are maintained by companies (Debian, Ubuntu, Red Hat, Oracle, SuSE)

Simple Linux Command Reference

- **ls** : Lists the files in a directory
- **cd** : change directory
- **pwd** : shows the present working directory
- **cat** : concatenates a file – or displays it to the screen
- **less / more** : pagination of output
- **tar** : Tape ARchive. Old backup software, now used as a primitive way to package files.
- **cp / rm / mv** : copy, remove and move a file
- **compress / gzip / bzip2 / xv** : compression tools to make files smaller
- **touch** : create a file or change its timestamp
- **useradd** : create users
- **chown / chgrp** : change owner and group permissions on a file
- **awk / sed / grep** : modification of data in files or on the screen
- **echo** : repeats a command to the screen
- **Pipes "|, <, >"** : allow redirection of data between processes

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

What can you do with Linux?

- Android Cell Phones
- Super Computers
- Microcomputers
- Web Services
- Data Processing
- AI/ML
- Cloud Servers
- Databases

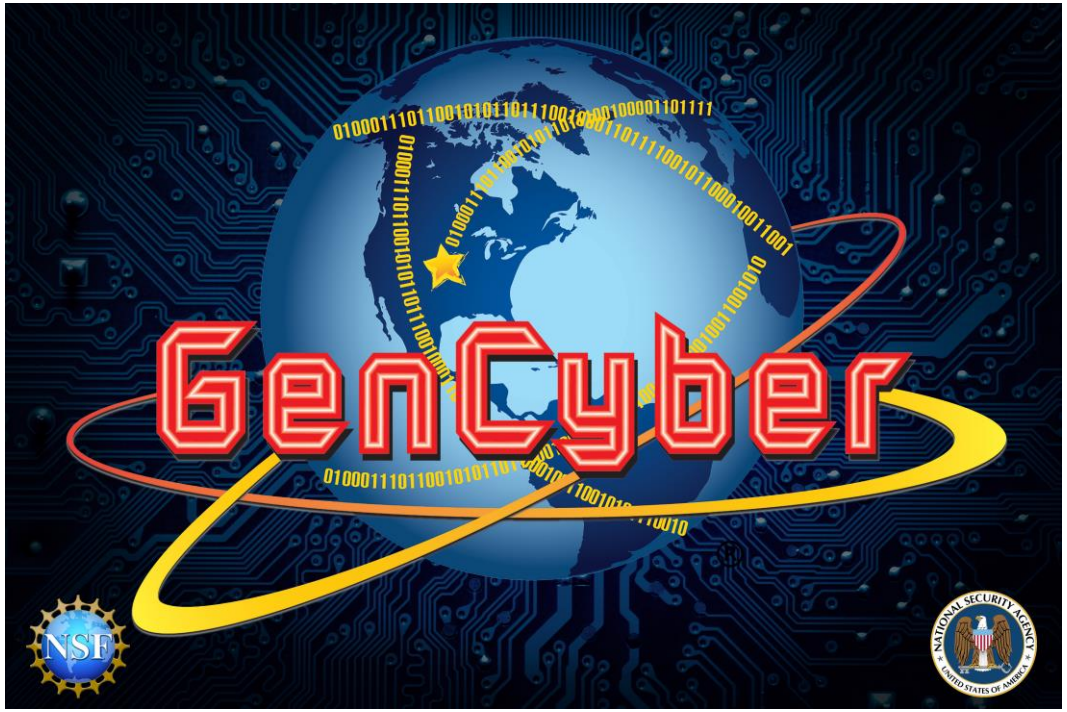
- Game Consoles
- Graphics Design
- Video Authoring
- Embedded Systems

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

Wireshark Lab

Dr. Shannon Beck

1:00 – 2:00

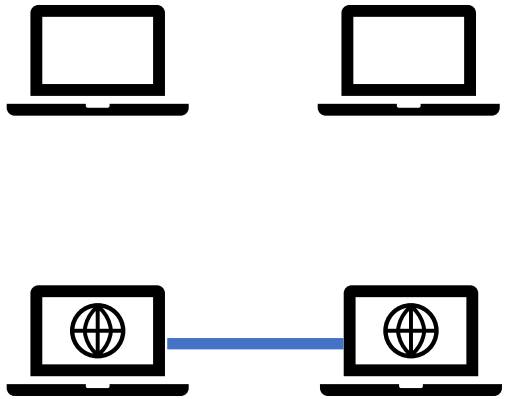


Introduction to Networks and Wireshark

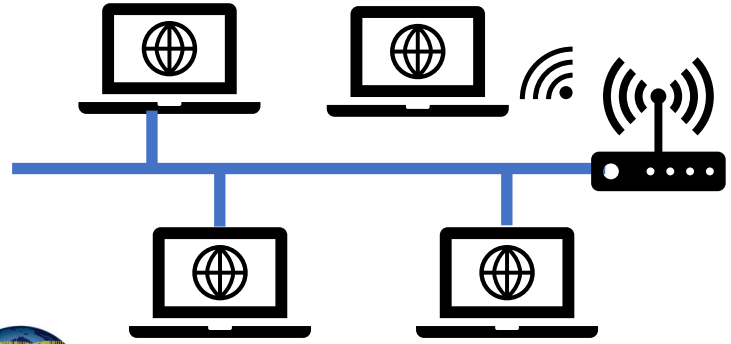
Overview of Networking

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

What is a Network?



- When you connect two or more computers or devices, you have “networked” them together
- **Networks** can use wires and radio waves (wi-fi)



- Usually, you want or need more than two devices talking to each other
  - Introduce more networking hardware to help
  - A **router** symbol shows both wired and wireless network

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

Speaking the Same Language

- Information exchange must be done so that all parties can understand the information being shared
- What happens if you show up to a class and your teacher is speaking Korean and you only know French? How well does that information exchange work?
- There has to be an agreement on the language used for exchanging human information
- Computers are the same – they need to agree on how to exchange information
  - These **network protocols** provide a common "language" for how to communicate

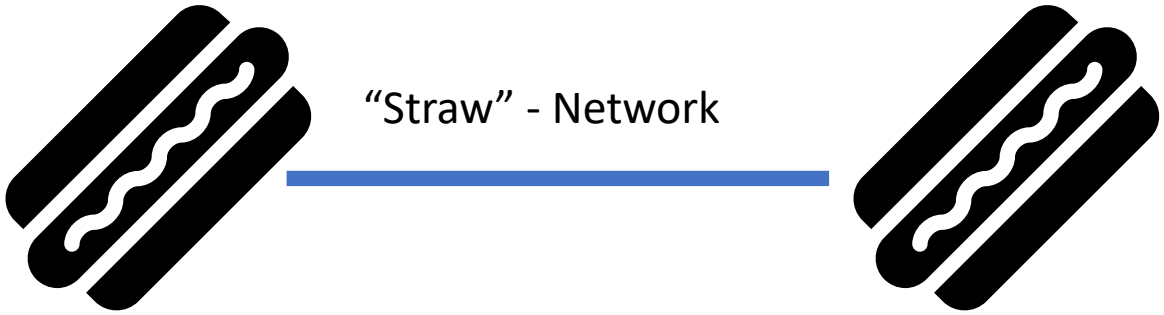
Network Protocols

- Definition: A set of rules that governs the connection of computer systems to the internet (Oxford Dictionary)
- Ever heard of TCP/IP?
  - **TCP** = Transmission Control Protocol
  - **IP** = Internet Protocol
- The two protocols are used together to establish and maintain a network conversation
- TCP focuses on establishing and maintaining a **network connection**
  - Connection-oriented, knows if a packet is missing
- IP defines how computers send **packets** of data to each other

Network Protocols – Continued

- In addition to TCP, there is UDP
  - **UDP** = User Datagram Protocol
  - Unlike TCP, UDP doesn't guarantee that the packets will get to the right destinations.
  - UDP uses **IP** (Internet Protocol) as well
- UDP is connection-less
- UDP is less reliable than TCP
  - Relies on devices in between the sending and receiving computers to correctly get the data where it's supposed to go

Network Traffic



- **Packets** on a network are pieces of a file that sent over the network and re-assembled on the receiving side.
- Imagine the network is a straw and you want to push through a sandwich.
- How do you do it? One small piece (packet) at a time.

Network Data Packets Concept Map

Original Image

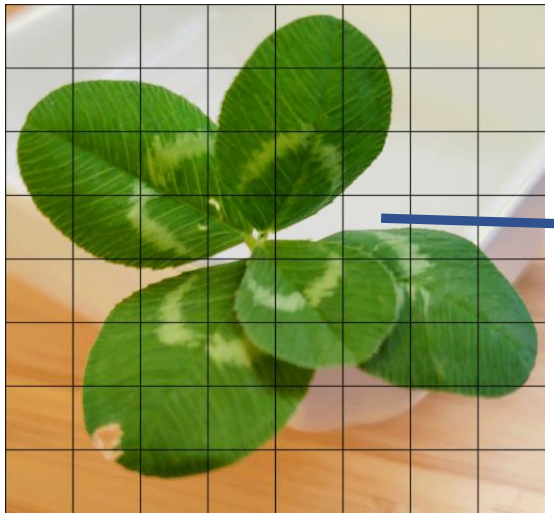
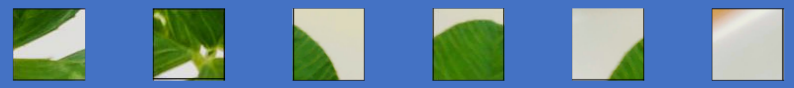


Image divided up into packet-sized data pieces

Individual Packet

IP sends packet to network

Network



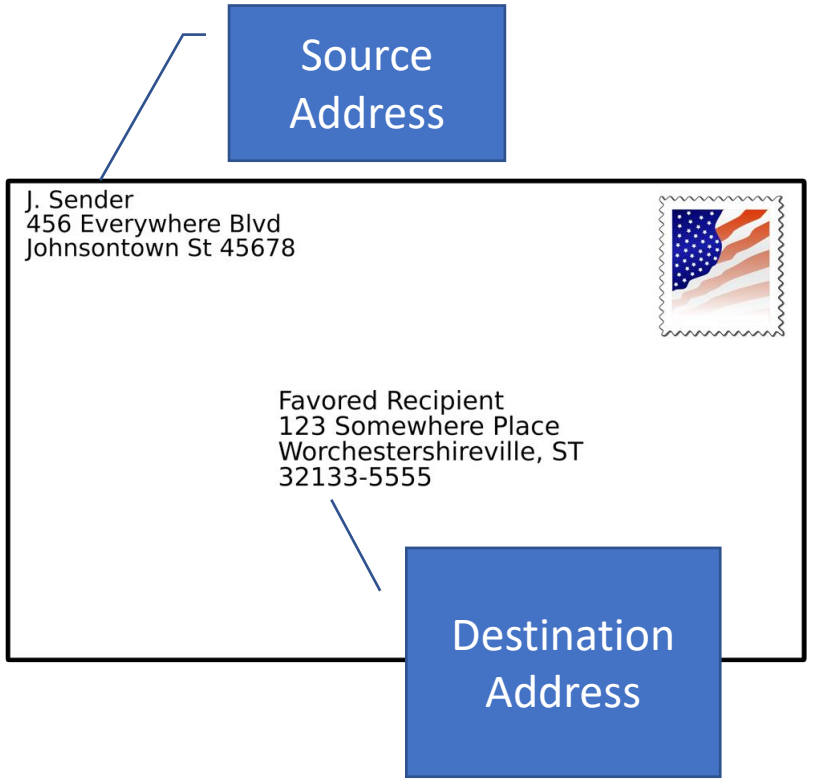
internet

Packets get sent to destination

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

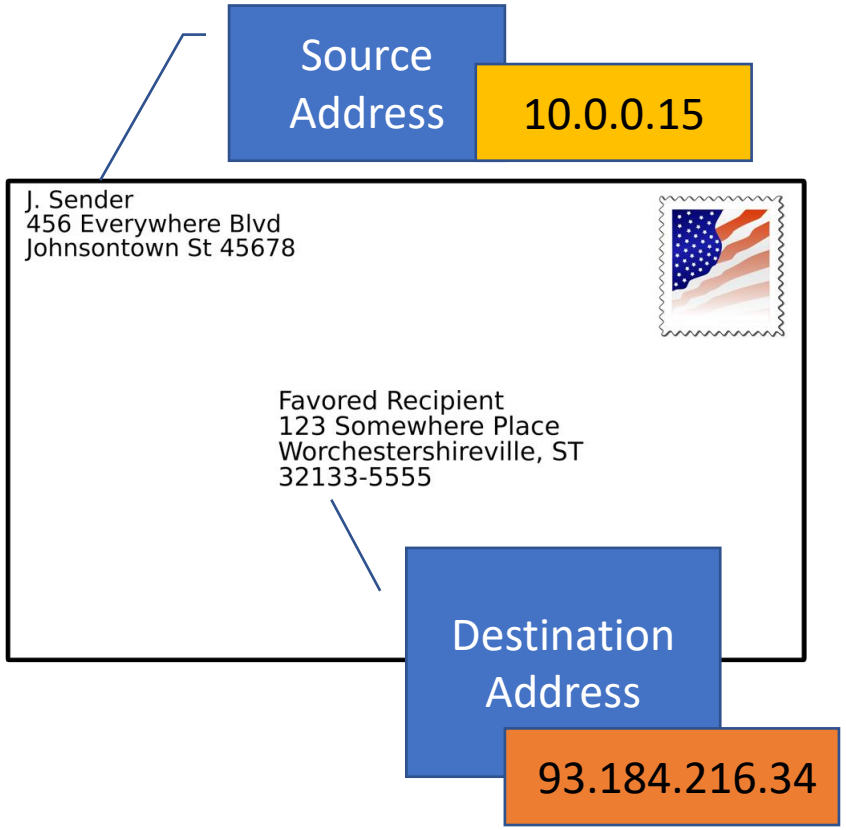
IP Addresses

- How does a packet know where it came from and where it's going to?
- Just like a letter, is uses addresses.
- **Source Address -** the IP address of where it's coming from (like a return address)
- **Destination Address** – the IP address of where it's going to



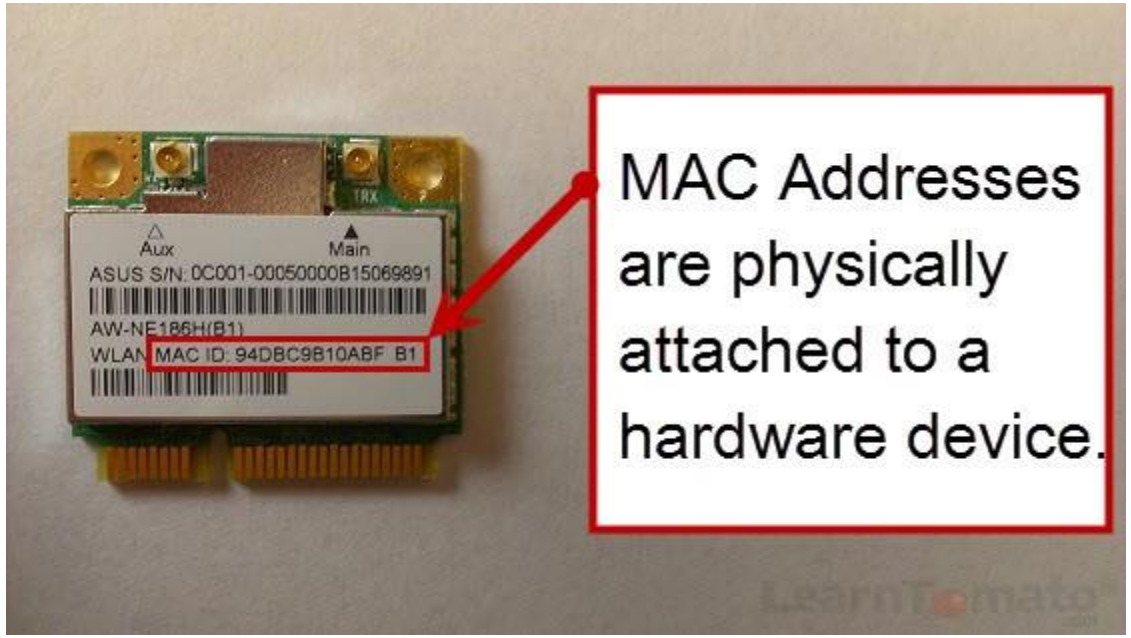
IP Addresses

- How does a packet know where it came from and where it's going to?
- Just like a letter, is uses addresses.
- **Source Address -** the IP address of where it's coming from (like a return address)
- **Destination Address** – the IP address of where it's going to



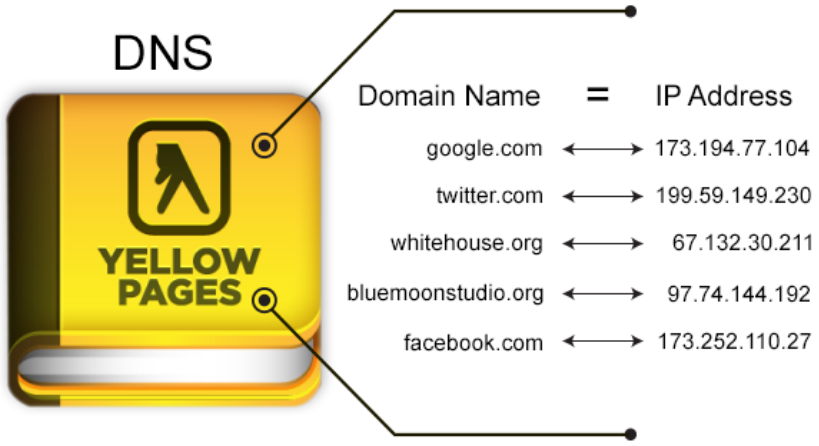
Other Identifiers – The MAC Address

- Computers are assigned IP addresses through software (changeable)
- The hardware has its own identifier, MAC address (non-changeable)
- Assigned at manufacture time, the first three bytes map to manufacturer (OUI listing)
- Can tell information about network hardware connected through the network traffic. The MAC address has (leaks) this information
- MAC addresses can be spoofed (faked), but generally the way to identify a specific physical network device



Not Lost in Translation

- How do you get from “example.com” to the IP address 93.184.216.34?
  - Answer: the **Domain Name System (DNS)**!
- DNS is like a phonebook for domain names mapped to IP addresses.



Ports

- Network ports indicate what type of service it is (email, file transfer, web).
- Typical ports used when browsing the internet
  - Resolving a URL (www.example.com) to an IP address (198.41.0.4) uses the **Domain Name System (DNS)** on port 53
  - Unencrypted website traffic (HTTP) – Port 80
  - Encrypted website traffic (HTTPS) – Port 443

Port Number	Usage
23	Telnet - Remote login service, unencrypted text messages
25	Simple Mail Transfer Protocol (SMTP) E-mail Routing
53	Domain Name System (DNS) service
80	Hypertext Transfer Protocol (HTTP) used in World Wide Web
110	Post Office Protocol (POP3) used by e-mail clients to retrieve e-mail from a server
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol (IMAP) Management of Digital Mail
161	Simple Network Management Protocol (SNMP)
194	Internet Relay Chat (IRC)
443	HTTP Secure (HTTPS) HTTP over TLS/SSL

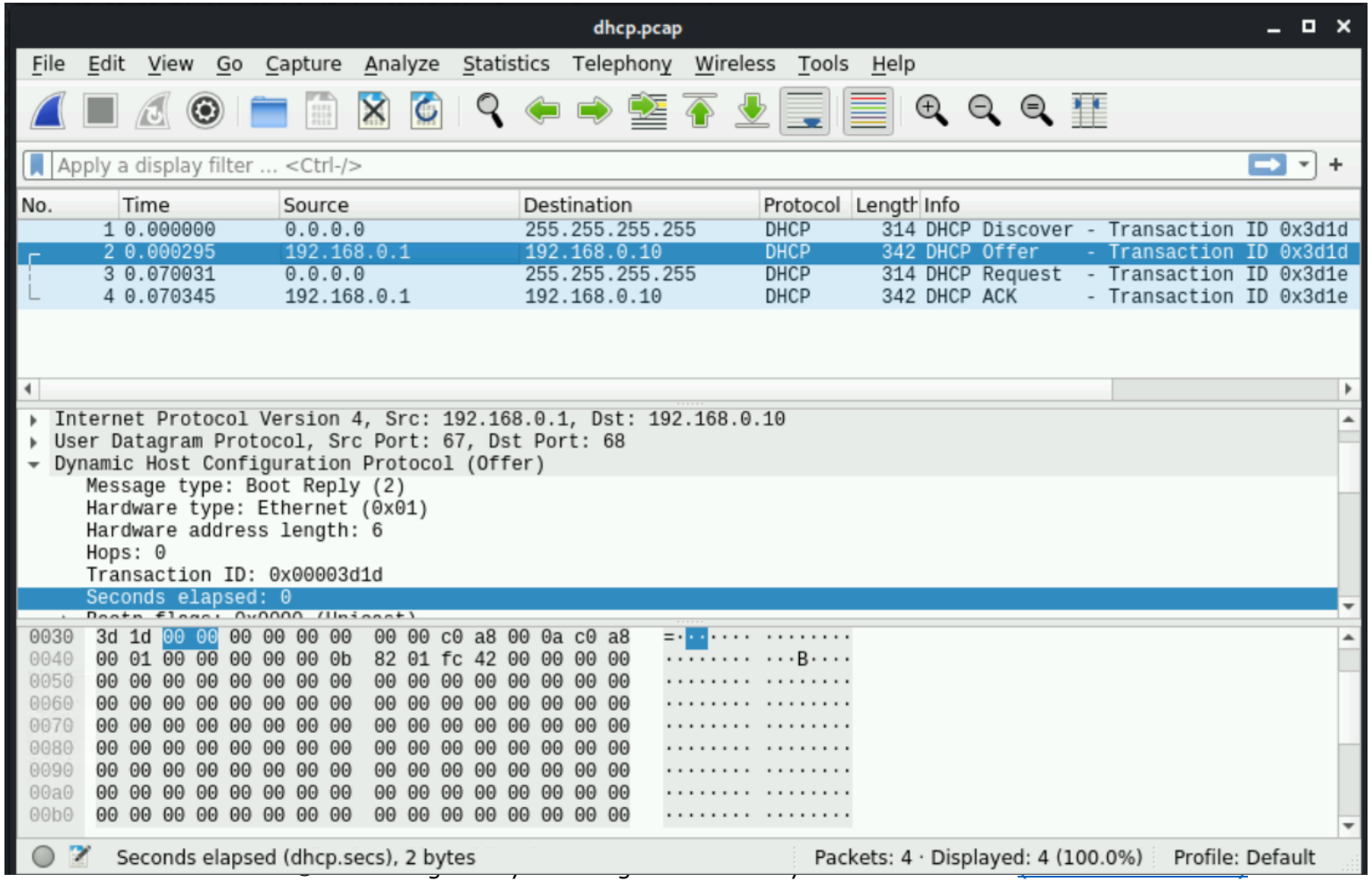
Do you think it’s possible to analyze data sent over the network?

Wireshark

- Wireshark is a powerful analysis software that allows you to not only capture network and device packets, but to analyze them too (i.e., a packet analyzer).
    - Remember - A packet is a fragment of data that is sent over a network from one machine to another. This data usually includes a *source port*, *source IP* address, *destination port*, *destination IP*, and other data that we will see in this lab.
- Wireshark allows a user to analyze the traffic traveling in and out of the machine, which can serve many uses.

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

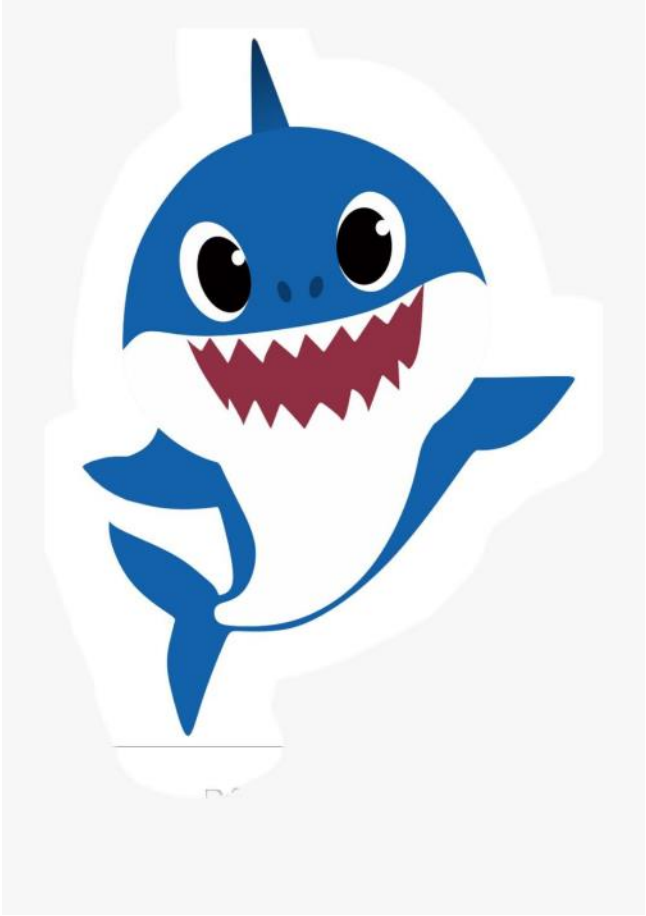
Wireshark



UNIVERSITY OF MARYLAND GLOBAL CAMPUS

Attack of the Sharks

WIRESHARK ≠



UNIVERSITY OF MARYLAND
GLOBAL CAMPUS

Why Use Wireshark?

- Troubleshoot network connections.
- Filter data between two hosts to see a single network “conversation.”
- Comparing all “conversations” to discover bad actors or “bandwidth hogs.”
- Filter captured data to analyze specific protocols and ports being used.
- Analyze specific statistics about the traffic coming in and out of the system.

Wireshark Lab

- Wireshark allows you to view pieces of data (called packets) in real-time as they go in and out of a system and can be saved as packet capture or **pcap files**.

- In this lab, you will be analyzing packet capture files (network forensics).

- The objectives at the end of the lab is understand:
  - Wireshark overview
  - Analyzing DNS Packets
  - Name-to-IP address resolution
  - Wireless access points and identifiers

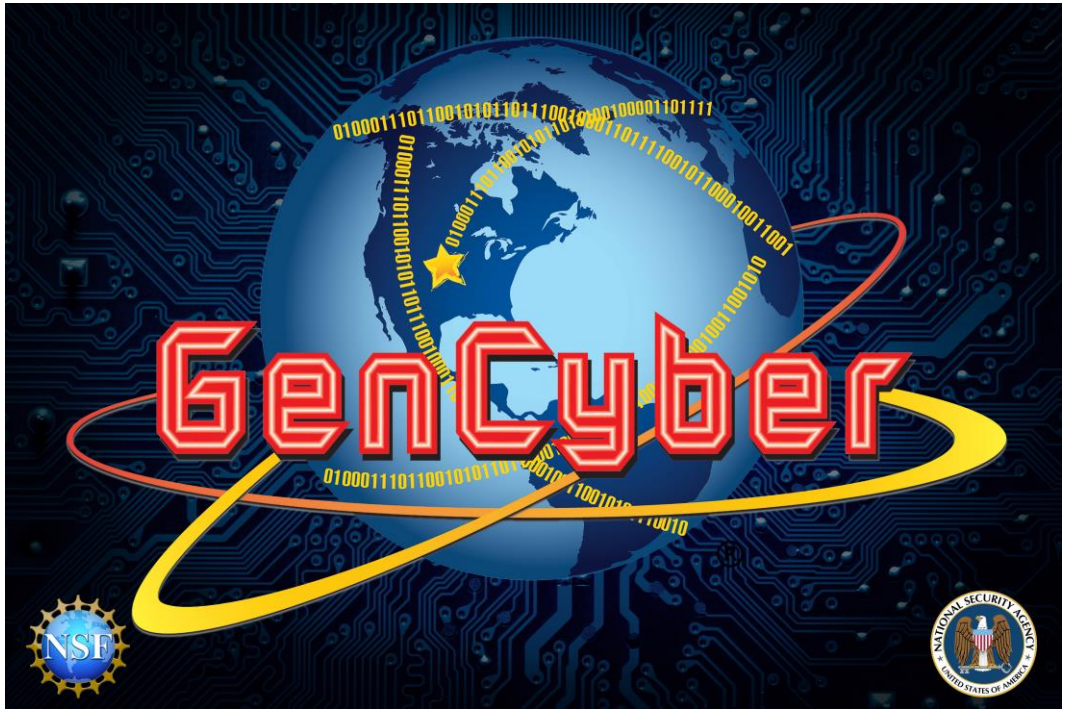
Debrief

UNIVERSITY OF MARYLAND
GLOBAL CAMPUS

Password Auditing Lab

Jonathan Woodward

2:15-3:15



Password Auditing Lab

UNIVERSITY OF MARYLAND
GLOBAL CAMPUS

Authentication and Authorization

- Authenticate – verify ID (you are who you say you are)
  - Something you know (password)*
  - Something you have (SMS phone, RSA key)
  - Something you are (biometrics like fingerprint)
- Authorize – grant access to resources based on authentication
  - R-BAC – based on your role

Password Auditing Lab Objectives

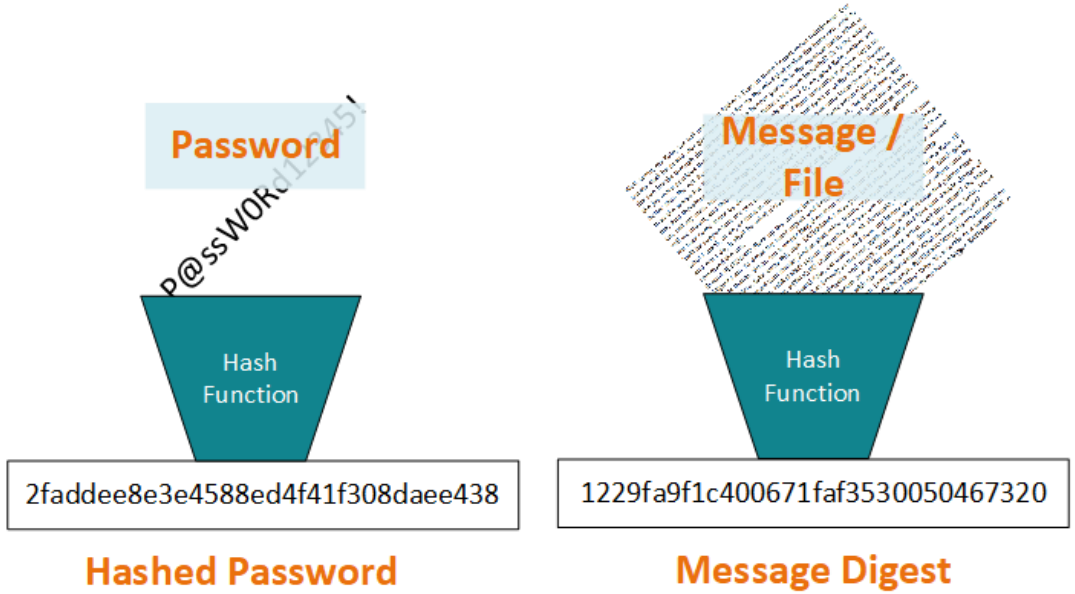
- Understand what makes weak and strong passwords
- Demonstrate creating hashes from plain text passwords
- Demonstrate how to use password cracking tools
- Understand the difference between dictionary and brute force password cracking

Password Auditing*

- Review and learn about password files in Linux
- Using the John the Ripper
  - Free password auditing (cracking) tool
  - Find trivial passwords in a short amount of time
  - Accessible on multiple platforms
    - Can be run from within Metasploit or on its own
  - Takes the entry from salted password hash from `/etc/shadow`:
    - `jsmith:$6$JRF8OgFTYSP1zDeO$2PuYhV7jFxrdY8x.4P73BspAXQZiv2S8Dr.hrFIGNXTWrIt6gdTiwnTr9cTgFurP4NPWT8isXwizoGRqt/iJ./:18659:0:99999:7:::`
    - Reduces it to the password: 12345

- **Hint: be careful where you use the word "hack"*

Background: What is a Hash?



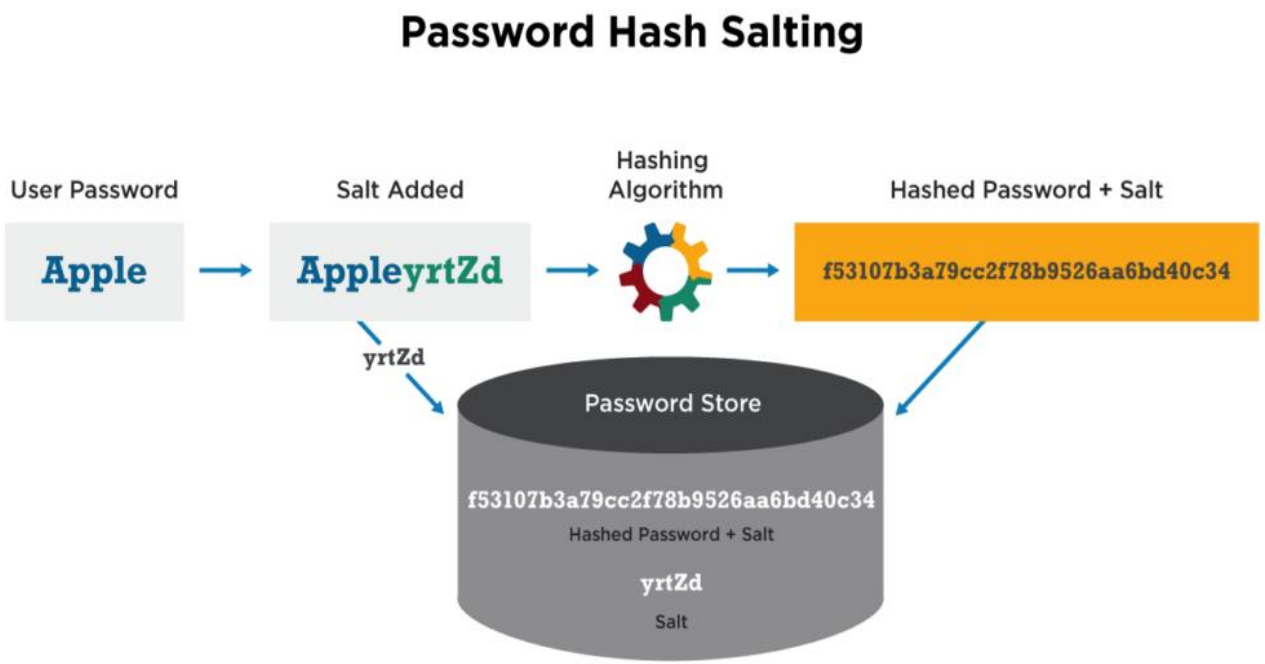
Same cryptographic hash function can be used.

- A hash function maps digital data of arbitrary size to digital data of **fixed size**. The hash is sometimes called a **message digest.**

- A cryptographic hash function is a hash function that is considered practically impossible to reverse (one-way-ness) or find collisions (i.e. two messages with the same hash value)

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

Password Hashing with Salt

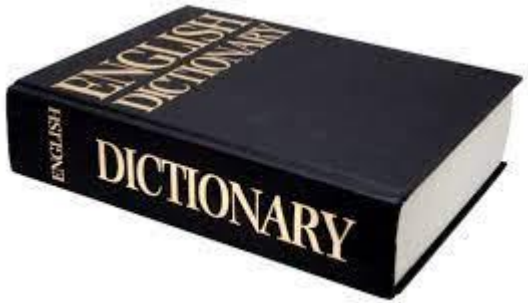


- Passwords aren't stored in plaintext or plain hash, they are salted
- Prevents Rainbow Table Attacks
  - Attack a hashed password in reverse with a table of pre-computed hashes with corresponding passwords
- Adds a layer of security (Defense in Depth)

Image from https://cyberhoot.com/cybrary/password-salting/

UNIVERSITY OF MARYLAND GLOBAL CAMPUS

Dictionaries in John



- Not like the dictionary you think of
  - A list of words to try against the password hashes

Image source: https://images2.minutemediacdn.com/image/upload/c_fill,g_auto,h_1248,w_2220/f_auto,q_auto,w_1100/v1555926333/shape/mentalfloss/166091799.jpg

Custom Dictionaries in John

```
root@kali:~/MyCookbook# john --stdout --wordlist=cewl_WackoPicko.txt
WackoPicko
Users
person
unauthorized
Login
Guestbook
Admin
access
password
Upload
agree
Member
posted
personal
responsible
account
illegal
applications
Membership
profile
words: 20  time: 0:00:00:00 DONE (Sun Jun 21 16:25:22 2015)  w/s: 333  current: profile
```

List 1:
cat
dog
panda
racoon
deer

List 2:
cat
dog
panda
racoon
deer
panther
puma
bear
chicken
corgy
welshcorgy
bordercollie
jump
run
audit
goat
horse
palamino
chestnut
…

Image source: https://static.packt-cdn.com/products/9781784392918/graphics/B04027_Ch02_23.jpg

Custom Dictionary

- If know target (person) attacking, what are some good sources for knowledge and possible passwords?

- Even the Linux built in “dictionary”

Defensive Uses of Password Cracking

- Phishing Investigation

To: david@lawfirm.com

Subject: Case Details Attached

Hi David,

I would also like to share with you some additional information regarding this case. It has a password since it is sensitive information.

The password is 284958934.

Regards,

Stacey Adams
29384 Wall Street
Suite 395
New York, NY 1001

LAW FIRM

Defensive Uses of Password Cracking

- Incident Response

```
  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 17 2020 03:07:47
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # sekurlsa::minidump .\lsass.dmp
Switch to MINIDUMP : '.\lsass.dmp'

mimikatz # sekurlsa::logonpasswords
Opening : '.\lsass.dmp' file for minidump...

Authentication Id : 0 ; 372033 (00000000:0005ad41)
Session           : Interactive from 1
User Name         : Administrator
Domain            : FROG
Logon Server      : AD
Logon Time        : 2021-04-22 11:15:47 PM
SID               : S-1-5-21-2669088251-2370404724-563291528-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : FROG
         * NTLM     : e19ccf75ee54e06b06a5907af13cef42
         * SHA1     : 9131834cf4378828626b1beccaa5dea2c46f9b63
         [00010000] CredentialKeys
         * NTLM     : e19ccf75ee54e06b06a5907af13cef42
         * SHA1     : 9131834cf4378828626b1beccaa5dea2c46f9b63
```

UNIVERSITY OF MARYLAND
GLOBAL CAMPUS

Defensive Uses of Password Cracking

- Password strength auditing

```
Account stats for: domain.local
  Disabled users ____________________________________________________  418 of  5164 (8%)
  Expired users _____________________________________________________   67 of  5164 (1%)
  Active users unused in 1 year _____________________________________  787 of  4679 (17%)
  Active users unused in 90 days ____________________________________ 1240 of  4679 (27%)
  Active users which do not require a password ______________________  156 of  4679 (3%)
  Active users with non-expiring passwords __________________________ 3907 of  4679 (84%)
  Active users with password unchanged in 1 year ____________________ 1006 of  4679 (22%)
  Active users with password unchanged in 90 days ___________________ 1400 of  4679 (30%)
  Active users with Administrator rights ____________________________   63 of  4679 (1%)
  Active users with Domain Admin rights _____________________________   54 of  4679 (1%)
  Active users with Enterprise Admin rights _________________________    0 of  4679 (0%)

  Disabled computer accounts ________________________________________   86 of  1414 (6%)

Password stats for: domain.local
  Active users using LM hashing _____________________________________   40 of  4679 (1%)
  Active users with duplicate passwords _____________________________ 2312 of  4679 (49%)
  Active users with password stored using reversible encryption ______ 4666 of  4679 (100%)
```

UNIVERSITY OF MARYLAND
GLOBAL CAMPUS

Wrap-up

Loyce, Shannon, Kim and Jonathan!

3:15-3:30