Wireshark and CyberChef

By: Bare Minimum Bandits

What is a WIRESHARK ?

- Cross-platform open source network protocol/packet analyzer
- Both GUI and CLI (tshark) based
- Can perform live captures and offline analysis of .pcap files
- Supports more than 2000 network protocols

What is WireShark used for?

First and foremost - Monitoring and troubleshooting tool

Offensive

- Can be used for active hacking e.g. MITM
- Traffic

Defensive

- Network Forensics

What is CyberChef?

- Open source ‘swiss-army knife’ with multiple functions including cryptographic, compression and hashing operations
- Under active development, new functionality added with each update
- Online web app and also desktop based
- Support drag and drop for files up to 500MB and supports breakpoints in the browser
- Can chain series of operations (recipes) together to transform data

Why use CyberChef?

- Extremely useful when you're confronted by different type of encryptions and don't know where to start.
- It's free can be used online or offline.
  - If other tools for cryptography can't be used
    - E.g simple -> ciphers (dcode.fr)
  - Downloadable htm file
- Use operations that use simple to complex encryption
  - Eg. Simple -> XOR or Base64
  - Complex -> AES, hexdumps, calculate hashes and checksums or character encoding

- Write-ups for training for CySCA 2018
  - https://hackmd.io/2ngmHk3USpKbEr1pHsFE-g

Wireshark Demo

CyberChef Demo