- Network Traffic: the amount of data that moves across a network.
- Network Data: the data that's transmitted between devices on a network.
- Indicators of compromise (IOC): observable evidence that suggests signs of a potential security incident.
- Data exfiltration: unauthorized transmission of data from a system.
- Command and control (C2) techniques: used by malicious actors to maintain communications with compromised systems.
- Network Protocol Analyzer (Packet Sniffer): a tool designed to capture and analyze data traffic within a network.
- Packet Capture (P-cap): a file containing data packets intercepted from an interface or network.

Created By: Abdelrahim Alsadiq

- **The fields of IPv4 Header:**
  - Version: the version of the IP being used.
  - Internet Header Length (IHL): the length of IP header + any options.
  - Type of Service (ToS): if certain packets should be treated with different care.
  - Total Length: the length of the entire packet.
  - Identification - Flags - Fragment Offset: deal with information related to fragmentation.
  - Time To Live: determines how long a packet can live before it gets dropped.
  - Protocol: provide a value that specify the protocol used.
  - Header Checksum: used to determine if any error occurred in the header.
  - Source and Destination Addresses.
  - Options: commonly used for network troubleshooting.
- **The fields of IPv6 Header:**
  - Version: similar to IPv4
  - Traffic Class: similar to IPv4 ToS.
  - Flow Label: specifies the length of the data portion of the packet.
  - Next Header: the type of header that follows the IPv6 header
  - Hop Limit: similar to the IPv4 Time to Live field
  - Source and Destination Addresses.