Thesis Statement: To research and monitor network traffic analysis. Specifically, a method known as Packet Sniffing. This is an analysis-based project where I will use a packet sniffer to monitor and capture data packets passing through a computer network.

1. Introduction to Packet Sniffing
2. History behind Packet Sniffing and why it's become popular.
3. Development into prevent packet sniffers.
4. Learning how encryption of hardware and packets makes it tougher for hackers to break into packets with information such as passwords, credit card details, etc.

II. Hardware – Computer Networks, Routers, Encryption Devices

- Breaking down networks to monitor traffic flow, and routing information.
- Checking router software to see if implementation of rerouting information has been implemented.
- Checking for encryption methods on devices such as card readers/etc. Inside of the networking system.

III. Software

- Encryption Software – How we can use this to further keep our packets embedded with security, to prevent thieves from stealing information.
- Penetration Prevention – Stopping a cyber-attack from an external source via methods like keylogging, networking holes, etc.

IV. Preventative Measures

- How to stop packet sniffers from monitoring your network traffic flow on public and private networks.

- How to prevent hackers from implementing software inside of your network to monitor packets via trusted devices.

V. Utilization of Hardware/Software

- How we can intertwine both hardware and software together to make sure everything is in place to keep hackers/packet sniffers/opportunists out of your network.

VI. Resources

- UWRF Resource Database
- Wireshark (Network at home)
- Security Engineering Third Edition: A Guide to Building Dependable Distributed Systems by Ross Anderson
- SolarWinds Network Performance Monitor