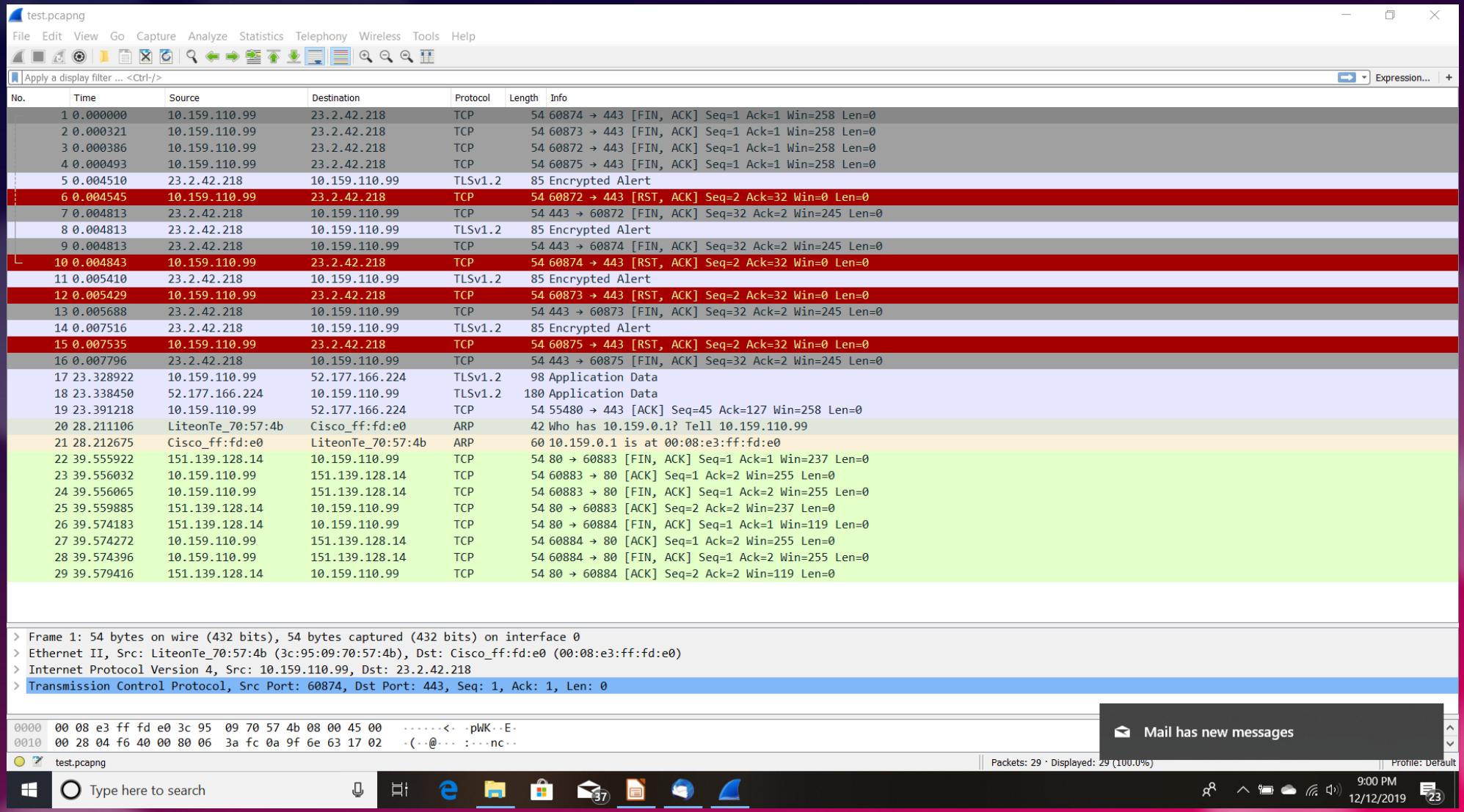
Janus

The goal of the project was to be able to scan a networked environment for potential security violations through a mobile application.

Wireshark Output



Three Parts of The Design

- The first part of the design was a sniffer to collect data and tag the location that the data was collected from.
- The second part was the storage and the analysis of the data for potential security threats.
- The last phase is the ability to take action.

Sniffer

- The sniffer collects the following information:
  - MAC address of the device. (allows for the tracking of the device if it changes locations in the network)
  - GPS location that the device was located at.
  - IP addresses visited.
  - Date/Time

Server

- The server provides the following functions:
  - Stores information in case there is an incident, and the information needs to be reviewed
  - Allows the network administrator to flag potential threats for the next stage.
  - Allows for the data to be fairly anonymous

Action

- This module provides the following functions:
  - Sends a “last known GPS location”, a MAC address and the security violation to be addressed.

Results of the Project

Why No One Else Did This

- In order for this project to reach it full potential the device has to be rooted and the PCAP libraries have to be added to the device.
- Then code has to be added to the App to call a shell on the device and to execute the code for the PCAP libraries.

- The results of these calls then have to be translated back to Android, and then interpreted.
- All of these calls and interpretation have to occur in real time.

What Started This Project

- There is a company called PawnieExpress
- A couple of years back they made the prototype phone for a TV series called “Mr Robot”
- I was wondering how far I could push this design into a real functioning network testing tool.

Summary of the Results

- While a mobile device for the testing of a network may sound appealing, the reality of the design is not.
- The better option is to use a laptop running COTS software packages that have years of testing and research behind them.
- These results can then be passed to the server, and analyzed.
- From this point the results of the analysis could be passed to the mobile devices for remediation

Questions

Better Options for Network Security Testing