Server Monitoring with FPGAs: Snoopy

COEN-4790 Course Project
Students: Tyler Sherman, Anthony Del Toro, Benjamen Palmer, Wajahat Ali
Professor: Dr. Cristinel Ababei (cristinel.ababei@marquette.edu)

Snoopy

OPUS College of Engineering
MARQUETTE UNIVERSITY

Abstract

FPGAs are incredibly useful in applications involving multiple inputs and calculations within a short time period. Snoopy was born out of a curiosity and drive to understand the power of VHDL and FPGAs when combined with security. Using an Ethernet adapter attached to a computer, Snoopy monitors network activity by counting the number of packets coming in and out of a particular server. Due to an FPGA's parallelism, we thought an additional application of mitigating DDoS attacks would be an effective way to increase our product's viability in a market. Thus, Snoopy blocks and rejects requests an IP address that sends requests to a server too rapidly.
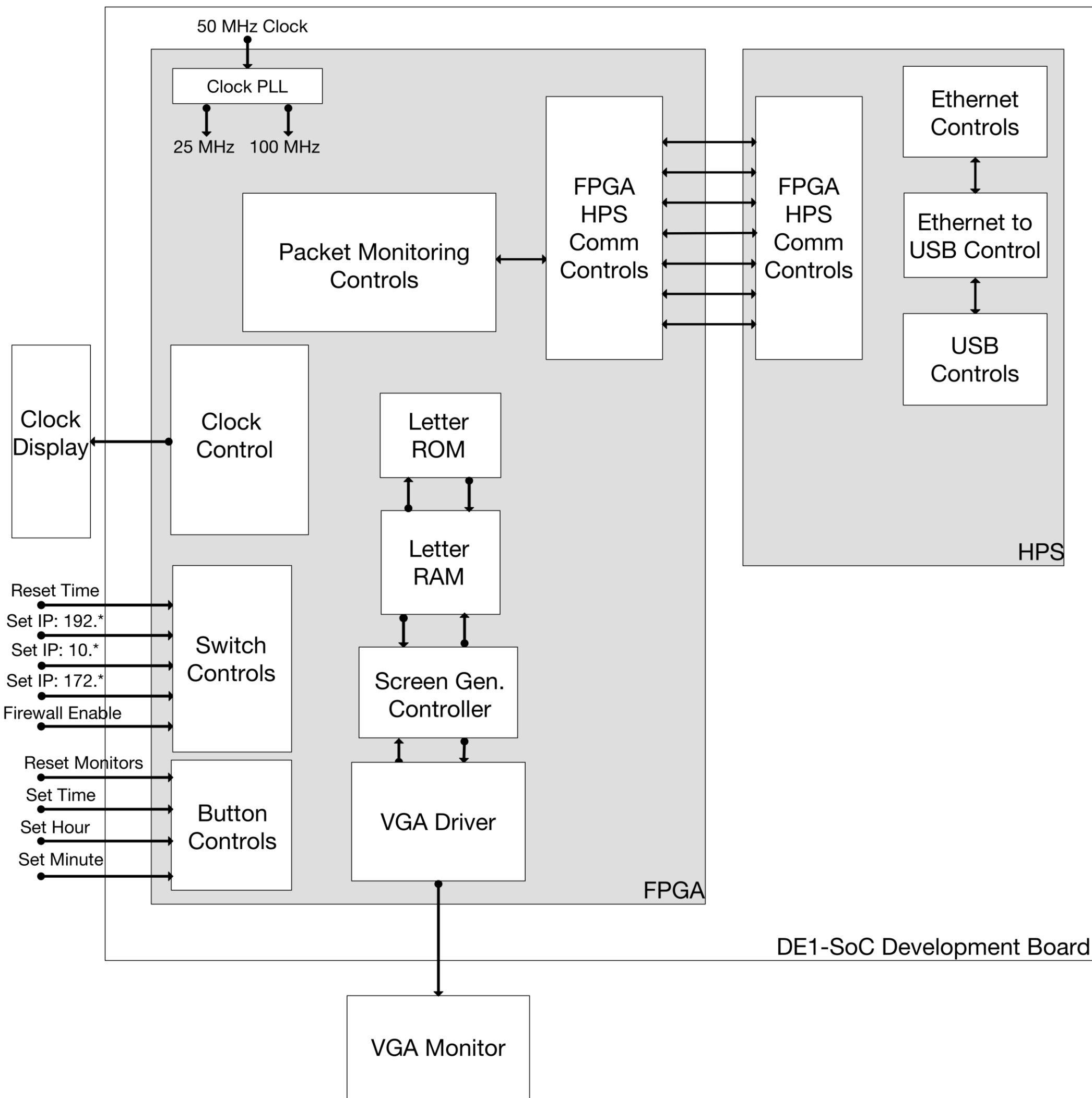
Objectives

Create a product to monitor network traffic to a server.

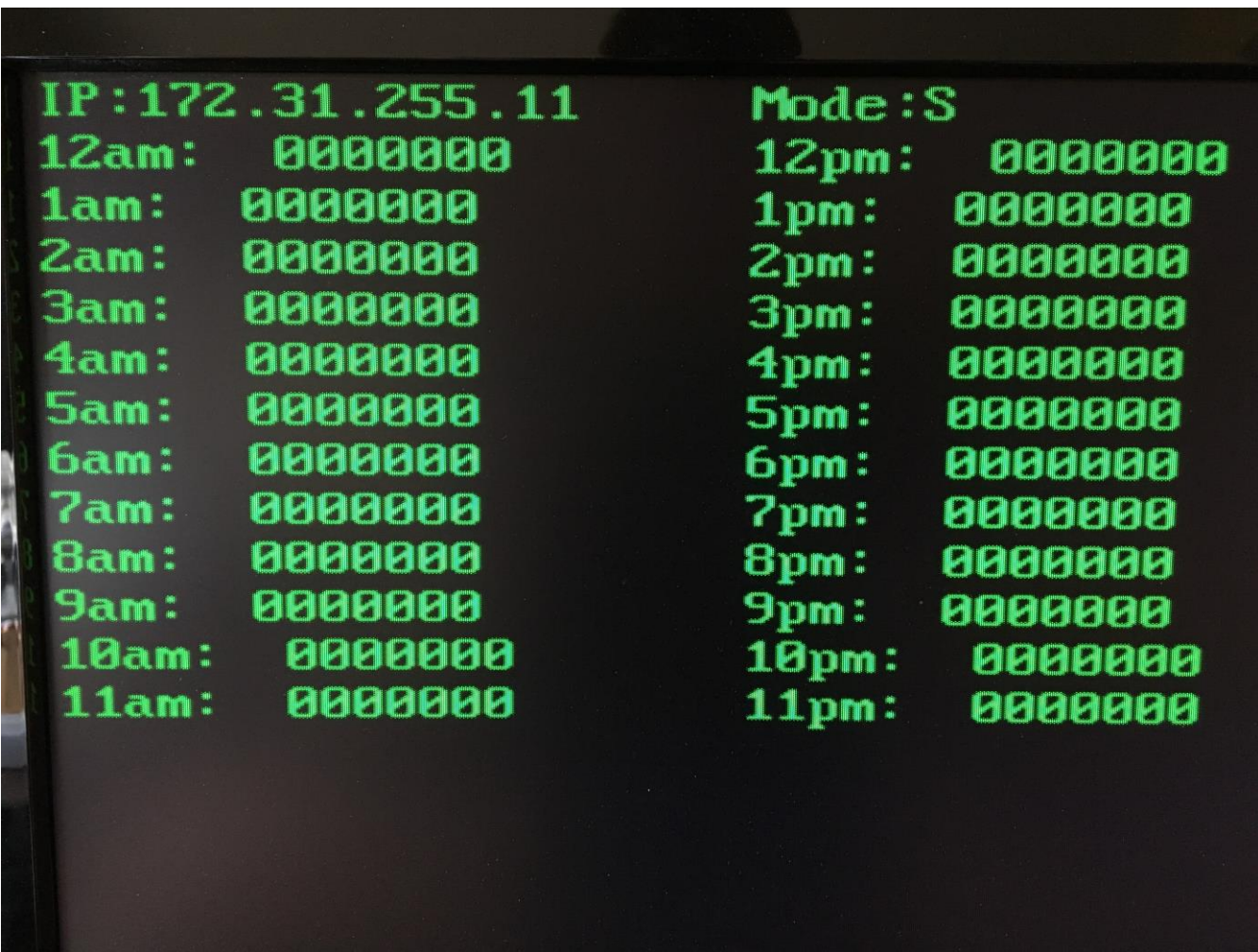Learn about HPS, Linux, Networks, VGA, Ethernet, and Security concepts.

Materials and Methods

Used a DE1-SoC board produced by Terasic, the board contains an Altera Cyclone V FPGA and a dual core HPS system.

An SD card containing Ubuntu to program the HPS side to integrate with the FPGA.
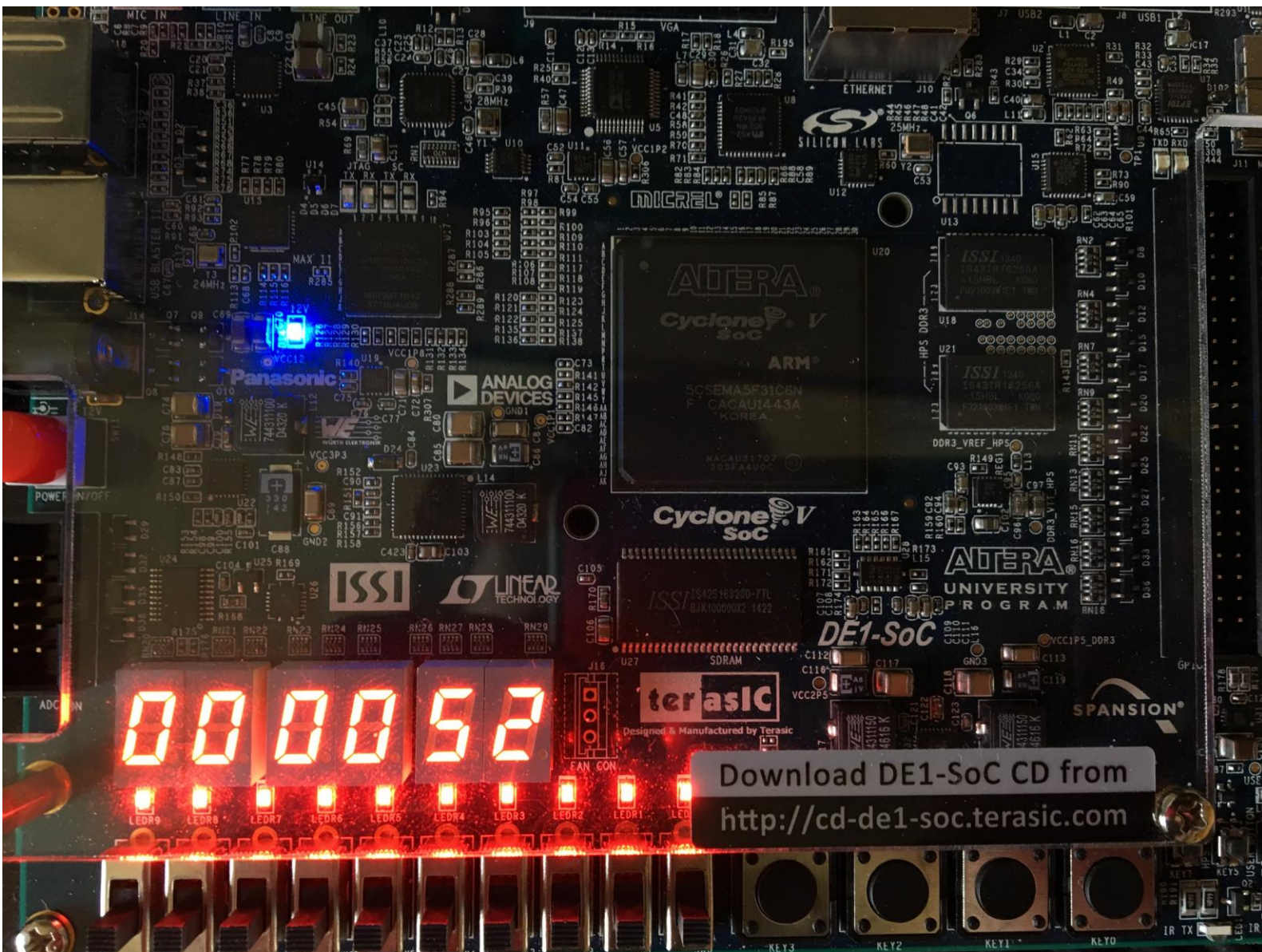
Agile Methodology was used throughout the project.

Simplified Block Diagram

Results

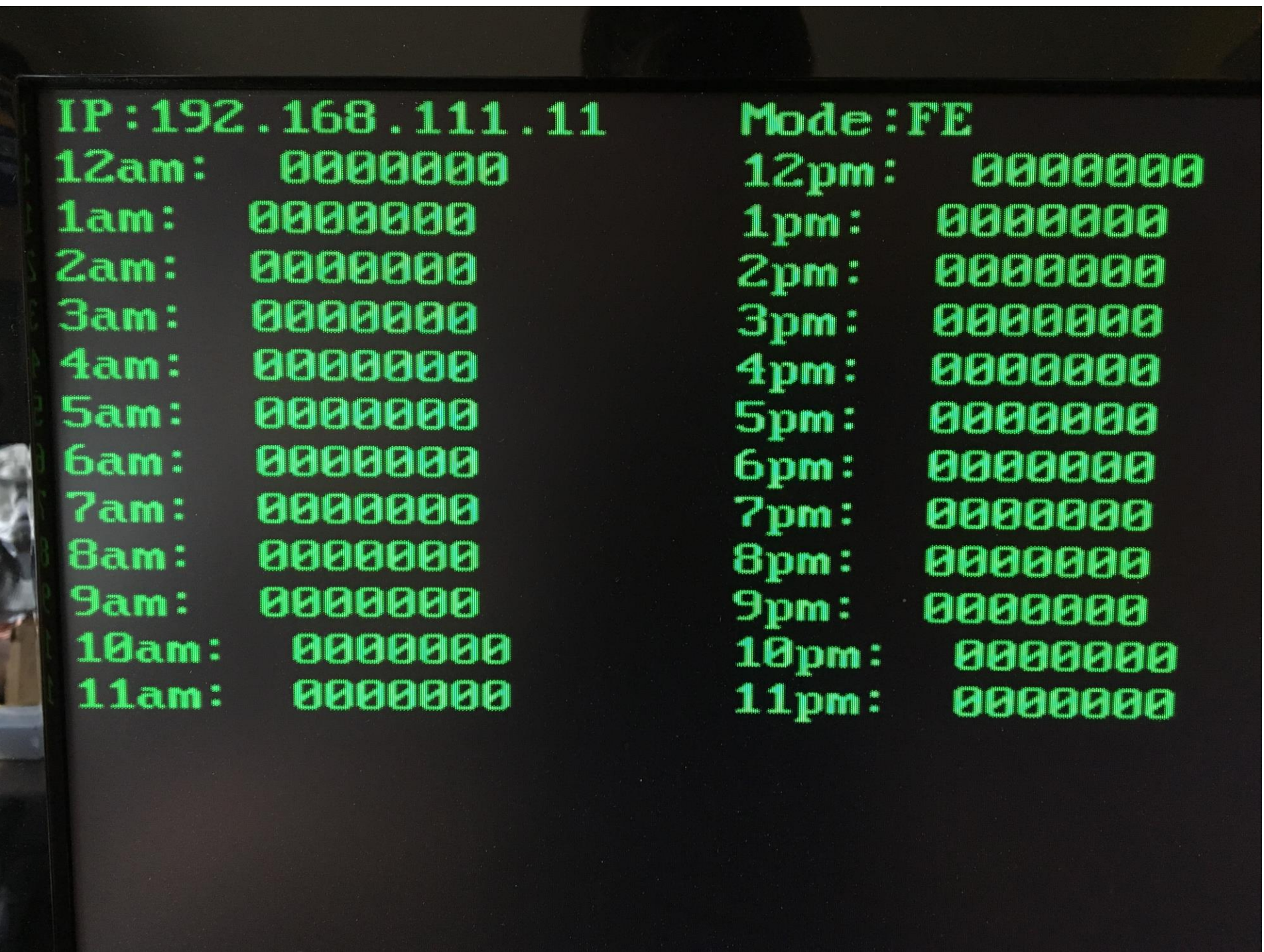
Display with 192.* IP address and Firewall Enabled

Test	Pass/Fail
Able to access server through FPGA	Pass
Traffic is recorded	Pass
Records are accurate	Pass
Information displayed on screen	Pass
Information is accurate	Pass

Monitoring Traffic

Information through VGA connection on display

Clock working on the board (12:00:52 am)

Current/Future Work

There are still different ways that this project can be improved past the Proof of Concept. We would want to further implement a better user interface than what we have created so far. We would want it to include the ability to display graphs and other important information to the user. We would also want to have it store multiple days worth of traffic in memory whereas right now it only stores a signal day before resetting.