*Srinivas Piskala Ganesh Babu – spg349 and N13138339*

# Forensics Project Synopsis

## *"PcapXray"* - A Packet Capture Visualizer/Diagnosis Tool for Network Forensics

As we approach to a more connected world with the Internet and the Cloud, Network has become a tremendous place for all types of Information exchange. In the recent years, a major shift has taken place from information exchanges within drives to a whole new residence, the Network. Information within itself brings about numerous threat and risk vectors. The Internet has become one big digital planet with all the digital life. Threats and Risk accompany everything on the internet.

A great deal of development on Network Forensics Analysis has become a priority. The tool PcapXray would help to visualize and diagnose given a network capture. It would help visualize the network map, devices involved and highlight respective important communication that has taken place. There exist no other tools that provide an offline analysis of the packet capture and map the network with the information that exists as evidence. This project visualizes a Packet Capture offline/online as a Network Diagram including device identification, highlight important communication and file extraction which would immensely reduce the time and effort of the investigator handling the evidence to spot any important findings.

| Objective | Duration | Milestone |
|---|---|---|
| **Recon** – Collect information on what to display with the network diagram | 1 week (Oct 2) | Resources on what/how diagnostic information is collected and shown |
| **Design –** Start with Manual Packet Analysis to plot the network and other information, create a design document | 1 week (Oct 9) | Output a design document, create a block diagram and code flow diagram to support the logic |
| **DiveIn –** Start with a Base code to handle pcap files and decide on the libraries to use, work on examples | 1 week (Oct 16) | Python snippets for example use cases and respective library code usage |
| **UI/UX Design –** Plot a design for the application and output display | 1 week (Oct 23) | Output a good design samples |
| **User Interface –** Create a usable user interface for the application and respective options | 1 week (Oct 30) | create a design framework to use – (FRONTEND) |
| **Backend Development** – Full Fledge Backend Support and Results | 2 week (Nov 6) | Finish all the functionality and features in the code (BACKEND) |
| **Merge** all modules to a final product | 3 week (Nov 20) | Merge all code and review the code for whole app |
| **Test** the Application and **Documentation** | 2 week (Dec 11) | Test- Fix Bugs and Deliver with presentation |