CS6963 Digital Forensics

Professor Marc Budofsky

Amandeep Singh 10/01/2017

Synopsis:

Pcap file contains network data packet created during a live network capture. In Nitroba University Case assignment, we were given a pcap file to analyze and find the suspect of the case using it. In order to efficiently solve the problem, students had to reconstruct the network layout in the pcap file.

In this project I plan to develop a tool that parses a pcap file to construct a network diagram being depicted in the file. In addition to the network diagram, the tool will also facilitate visualization of network traffic between each node and protocols/services utilized by them.

This will be a two-part project. The first part includes developing an algorithm to efficiently analyze and get accurate network details. And the second part of the project involves constructing a visual representation of the network data that we obtained from the first part.

Timeline:

Steps	Timeline	Deliverables
Analyzing different protocols in the pcap file and processing the data	Oct 1 – Oct 29	Python program that processes a pcap file and saves the network architecture data
Getting familiar with Visual representation library in python	Oct29 – Nov 5	--
Develop data processing engine for visualization	Nov 5 – Nov 12	Python tool to construct structure of visual network architecture diagram and protocol details
Integrating both parts to make it an integrated tool	Nov 12 – Nov 26	Final Python tool
Testing	Nov 26 – Dec 3	Error Corrections
Documentation and Reports	Dec 3 – Dec 10	Pdf Report and Presentaion