

# APT Proposal

Title: **Visualization of Security Logs**

Supervisor: Dr. Guillermo Francia, III

Keywords: Visualization, Computer Security, Java, Log Monitoring

Objective:

To implement a portable security log visualization tool using Java as an implementation language.

Description:

Computer forensic is the information that is produced, stored, or transmitted by a computer system or network. It is primarily the evidentiary material that is collected and used in establishing and analyzing digital transactions and activities. Once this data is collected and secured, the analysis and reporting of the data is usually required. The data analysis can be enhanced through visualization, which can be used in recognizing anomalous trends or patterns.

In this APT, the student is required to design and implement a portable visualization system for security log files. The portability requirement of the system entails the utilization of Java as the implementation language and JFreeChart, an open-source charting library, for visualization development. Students will be provided with tutorials on Java-Swing Graphical User Interface (GUI) programming and JFreeChart development.

Timing: (25 days total)

Attend tutorial lectures (3 days)

Research (3 days)

Design (3 days)

Implementation (10 days)

Testing (3 days)

Report and presentation preparation (3 days)

References:

- [1] R. Erbacher and S. Teerlink: "Improving the Computer Forensic Analysis Process through Visualization." Communications of the ACM. February 2006. Vol. 49.,No.2.
- [2] Axelsson, S. and Sands, D. Understanding Intrusion Detection Through Visualization. Springer-Verlag. 2005.
- [3] JFreeChart Website: <http://www.jfree.org/jfreechart/index.html>. Access date: 12/03/2006.
- [4] Deitel, et. al. Java How to Program, 6<sup>th</sup> Edition. Prentice-Hall. 2005