# Virus Analysis

**Techniques, Tools, and Research Issues**

Michael Venable
Arun Lakhotia

University of Louisiana at Lafayette, USA

## Tutorial Objectives

- Provide background to initiate research in malware analysis.
- Initiate discussions on a distributed, collaborative, university-based reverse-engineering team

## What Will Be Discussed

- Introduction to malware
- Description of lab environment and tools
  - Setting up a secure environment
  - Static and dynamic analysis tools
- Techniques for analyzing malware
  - Hands-on analysis of Beagle.J
- Research in virus analysis
  - Survey
  - Distributed virus analysis framework

## Pre-requisites

- Windows and Linux usage
  - Running programs
  - Windows Registry
- Programming background
  - Assembly Language
  - Using debuggers
  - C programming
  - Socket programming
- Networking
  - TCP/UDP communication packets
  - Setting up host tables, DNS queries