



JOHN JAY COLLEGE
THE CITY UNIVERSITY OF NEW YORK
OF CRIMINAL JUSTICE

The Center for Cybercrime Studies

Presents

Visual Forensic Analysis

Speaker: *Greg Conti*

Computer Science Department
United States Military Academy

For decades hex was the common tongue of reverse engineers and forensic analysts, but we can do better. Hex editors are the Swiss Army knives of low level analysis and have evolved significantly, but are now at a local maximum. With the tiny textual window hex provides, it is difficult, if not impossible to understand the big picture context and inner workings of binary objects - files, file systems, process memory, and network traffic. While there are helpful tools to analyze the special case of executable files, little work exists to help address the general case of all types of binary objects. This talk presents visual approaches to improve the art and science of forensic analysis, diffing, and reverse engineering, both in the context independent case where little is known about the raw structure of the binary data and at the semantic level where external knowledge can be used to inform analysis. If you are faced with low level analysis tasks, you should attend this talk.

Greg Conti is an Assistant Professor of Computer Science at the United States Military Academy. His research includes security data visualization and web-based information disclosure. He is the author of Security Data Visualization (No Starch Press) and the forthcoming Googling Security (Addison-Wesley). His work can be found at www.gregconti.com and www.rumint.org.

Date: September 24, 2008
Time: 3:30 PM
Location: Mathematics Conference Room - 4238N
445 West 59th Street, New York City 10019

RSVP: Nicole Daniels at 212-237-8920 or email ndaniels@jjay.cuny.edu.

For additional information please contact Professor Doug Salane, Director of the Center for Cybercrime Studies, at 212-237-8836 or email dsalane@jjay.cuny.edu.

The Center for Cybercrime Studies at John Jay College of Criminal Justice brings together scholars and practitioners to develop and disseminate knowledge, methods and tools needed in the fight against cyber crime.