Digital Artifact Persistence, Extraction, Analysis, and Manipulation

Jim Jones, Ph.D.

Department of Electrical and Computer Engineering

George Mason University

October 24, 2018, 11:00 am-12:00 pm

Research 163

Abstract

Digital data dies an uncertain death. Delete a file today, and the content might be entirely destroyed immediately, or some of it may survive for a few seconds, hours, days, or longer. For a forensic investigator, this is good news – residual fragments of a deleted file might be recoverable days, months, even years after the file was deleted. But why do some fragments persist while others do not, what can we infer from the fragments that we can recover, and can such fragments be artificially created or modified? In this talk, I will discuss our approach, tools, and work to understand the patterns and mechanisms of deleted digital data decay, analysis and interpretation of recovered fragments, and techniques for the manipulation of digital fragments under various circumstances.

Biography

Jim Jones is an Associate Professor in the Digital Forensics and Cyber Analysis program within the ECE Department. Dr. Jones earned his Bachelor's degree from Georgia Tech (Industrial and Systems Engineering, 1989), Master's degree from Clemson University (Mathematical Sciences, 1995), and PhD from George Mason University (Computational Sciences and Informatics, 2008). He has been a cyber security practitioner, researcher, and educator for over 20 years. During that time, he has led and performed network and system vulnerability and penetration tests, led a cyber incident response team, conducted digital forensics investigations, and taught university courses in cyber security, penetration testing, digital forensics, and programming. Past and current funded research sponsors include DARPA, IARPA, DHS, NSF, and DoD. His research interests are focused on digital artifact persistence, extraction, analysis, and manipulation.