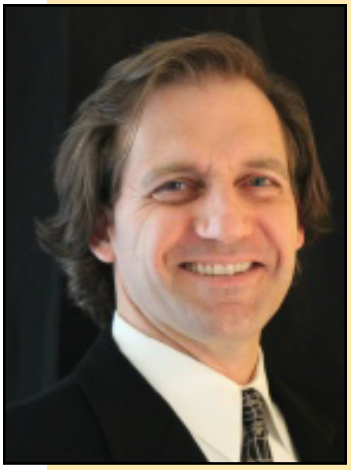

Jim Jones, PhD

Associate Professor, Department of Electrical and Computer Engineering
Director, DHS Center of Excellence for Criminal Investigations and Network Analysis

Education

PhD, Computational Sciences and Informatics, George Mason University

Key Interests

Digital Forensics | Cybersecurity | Digital Artifacts | Cyber Warfare | Digital File Persistence | Digital File Decay | Digital System Manipulation

CONTACT

Phone: 703-993-5599 | Email: jjonesu@gmu.edu
Website: https://cina.gmu.edu/

SELECT PUBLICATIONS

- J. H. Jones & T. M. Khan. A method and implementation for the empirical study of deleted file persistence in digital devices and media. *2017 IEEE 7th Annual Computing and Communication Workshop and Conference* (CCWC), Las Vegas, NV, 2017, 1-7 (2017).
- A.A. Bahjat & J. Jones. Deleted file fragment dating by analysis of allocated neighbors. *Digital Investigation,* 28, S60-S67 (2019).
- J. Jones. Deleted audio file decay on a digital voice recorder: in Audio Engineering Society Conference: 2017 AES International Conference on Audio Forensics. *Audio Engineering Society.* (2017).
- J. Jones. Cyber deception via system manipulation. *International Conference on Cyber Warfare and Security*, 194-201 (2017).

Research Focus

Digital data dies an uncertain death. Delete a file today, and the content might be entirely destroyed immediately, or not - residual fragments of a deleted file might be recoverable days, months, even years after the file was deleted. My research focuses on two questions: (1) What factors drive this decay, and can those factors be understood well enough to predict the decay pattern of different files on different systems and under different circumstances, and (2) What can we say about recovered fragments, such as inferring the past presence of the original file or estimating when the file was deleted. In much the same way that an archaeologist pieces together past events from shards of pottery, or a detective reconstructs a crime from partial fingerprints and chemical traces, we enable investigators and analysts to draw conclusions from the ubiquitous and often ignored digital crumbs and fragments left behind.

Current Projects

- With funding from the DHS, we are developing methods to quickly find partial files on digital media and to associate different entities based on residual file fragments, even if the fragments are not consistent across different media sources.
- With funding from the US Army P3i program, we are developing methods to extract digital data from embedded systems and to identify malware and other indicators of compromise on those systems based on recovered residual fragments.