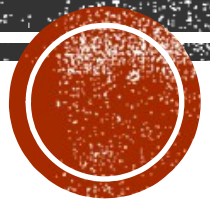
DELETED FILE PERSISTENCE ON DIGITAL MEDIA



Jim Jones, PhD

Associate Professor

Electrical and Computer Engineering

Digital Forensics and Cyber Analysis

George Mason University

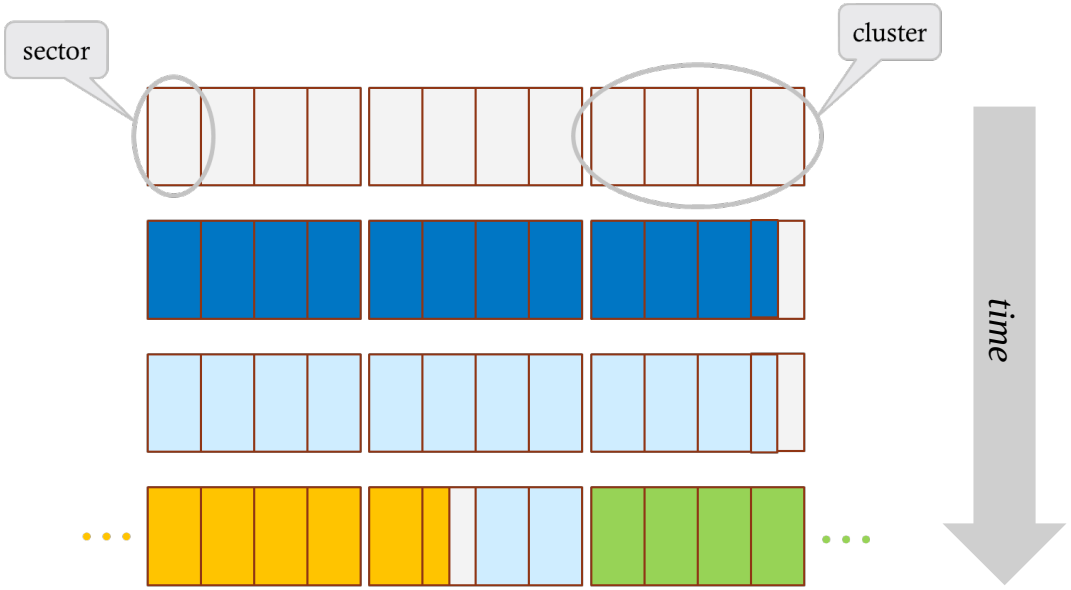
Tahir Khan, PhD

and several others...

George Mason University

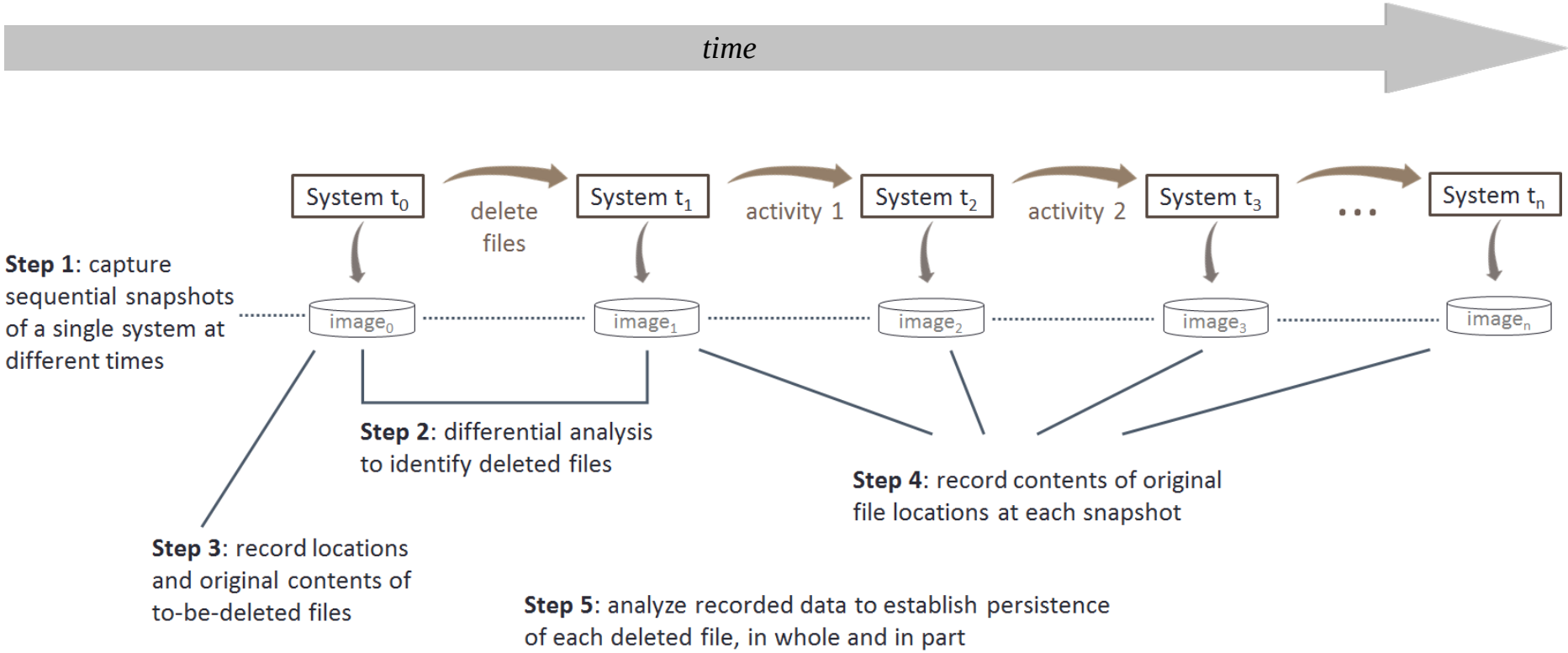
DFRWS 2017

WHAT ARE THE FACTORS THAT AFFECT DIGITAL FILE PERSISTENCE (DECAY)?



- Can a predictive model be constructed?
- Could it be used for triage decisions? to interpret recovered residual fragments? privacy?

WE DEVELOPED TOOLS AND TECHNIQUES TO STUDY THIS QUESTION



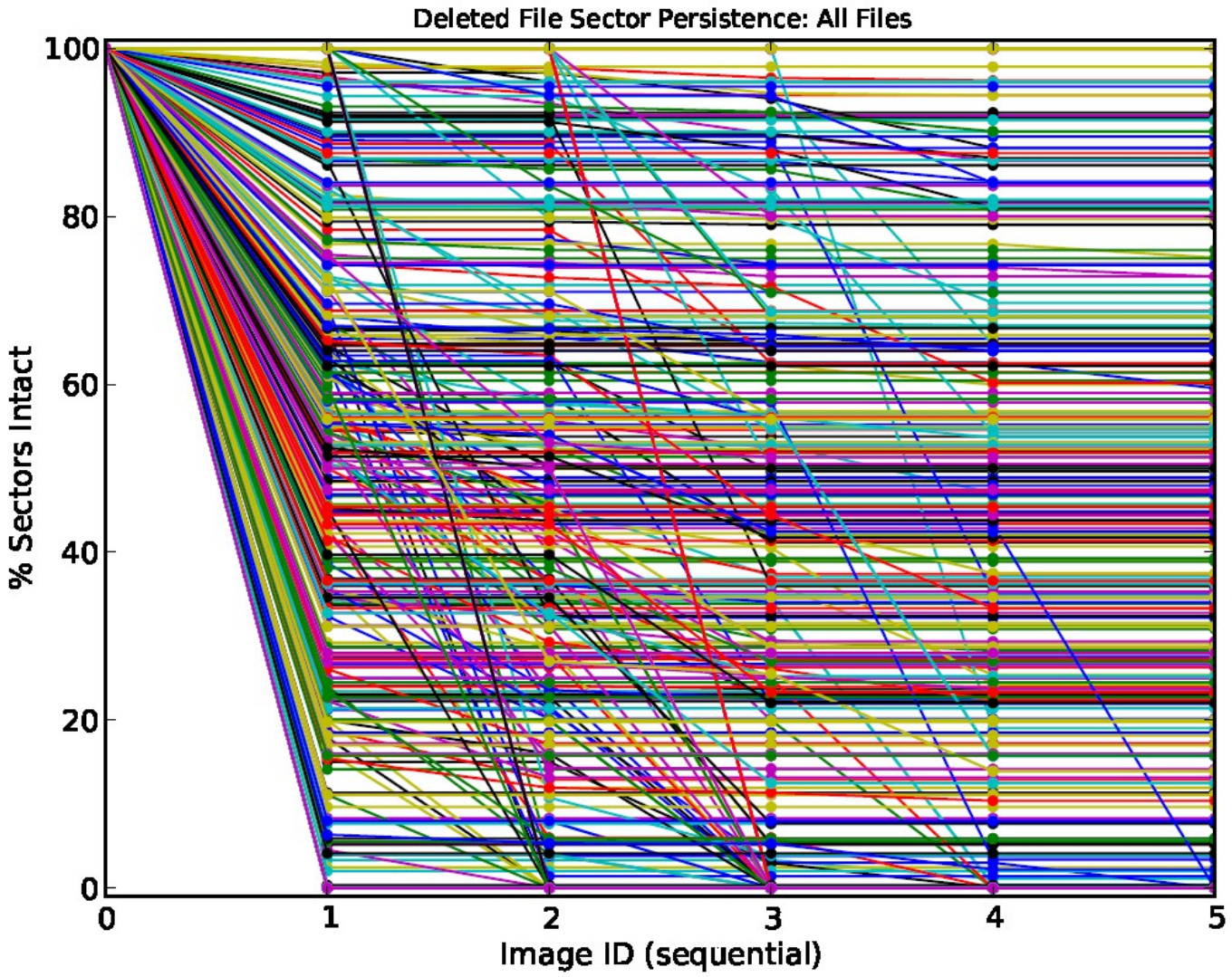
Jones, J. H., & Khan, T. M. (2017, January). A method and implementation for the empirical study of deleted file persistence in digital devices and media. In Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual (pp. 1-7). IEEE.

M57 ADVANCED KEYLOGGER

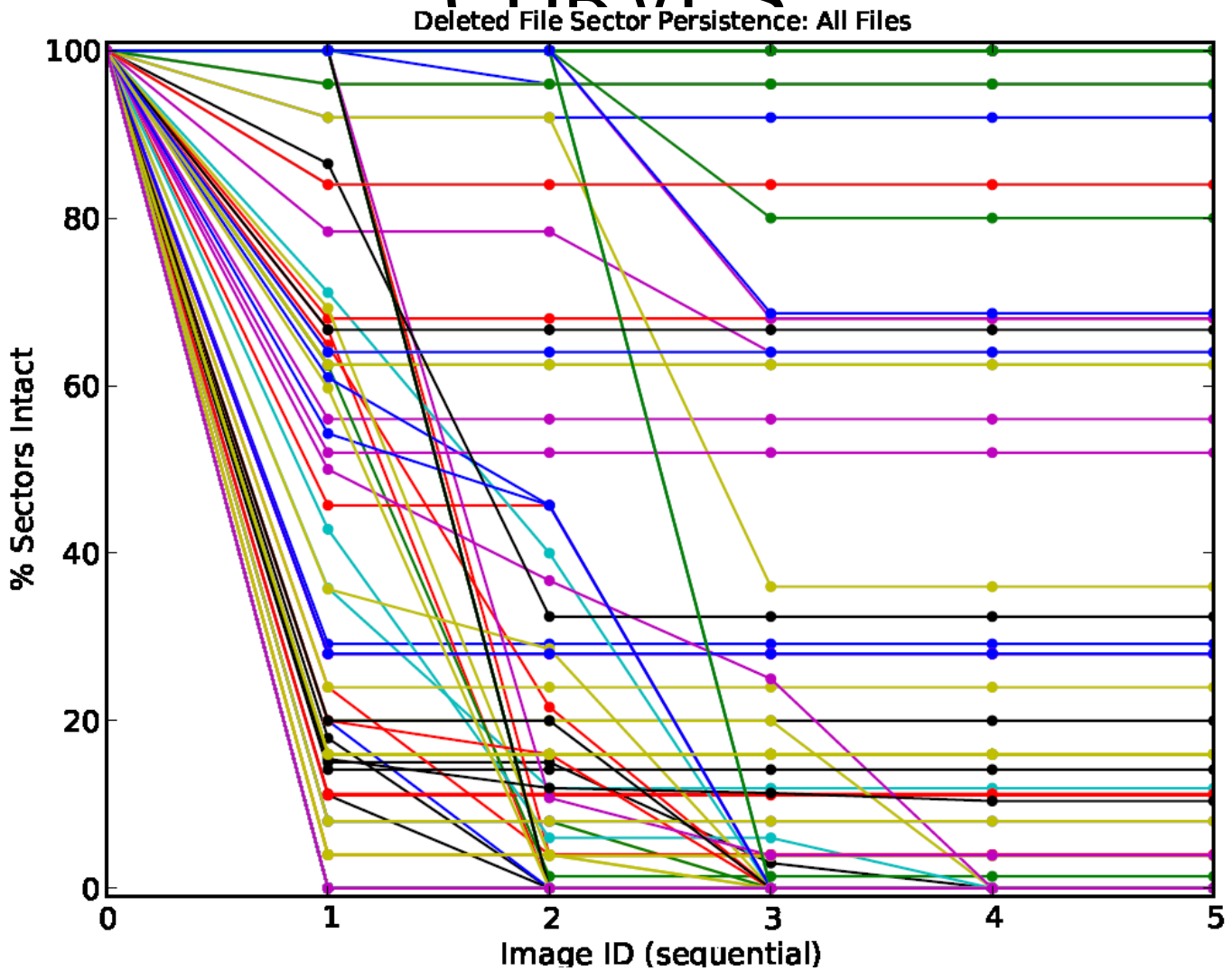
- 17 snapshots over 25 days (11/16 - 12/11)
- Advanced Keylogger installed on machine Pat 12/02 - 12/03
- Uninstalled and files deleted 12/04 - 12/07
  - 1314 files (662,307 sectors) deleted between these images
  - 691 of these files (13,173 sectors) are Advanced Keylogger logs
- Continued use 12/07 - 12/11

Garfinkel, Farrell, Roussev and Dinolt, Bringing Science to Digital Forensics with Standardized Forensic Corpora, DFRWS 2009, Montreal, Canada

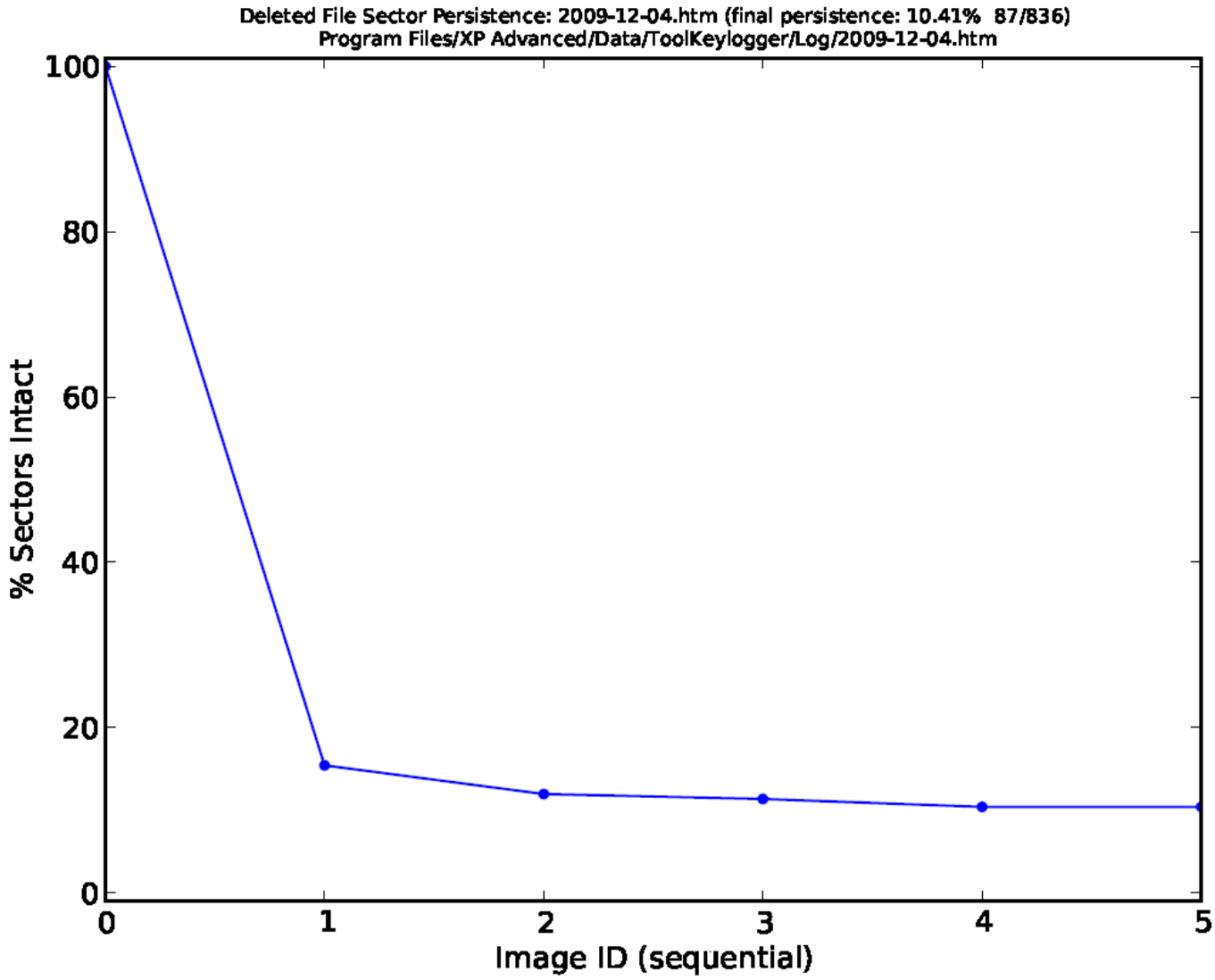
M57 ADVANCED KEYLOGGER: DECAY CURVES



M57 ADVANCED KEYLOGGER: DECAY CURVES



M57 ADVANCED KEYLOGGER: DECAY CURVES



RESULTS: AUDIO FILES

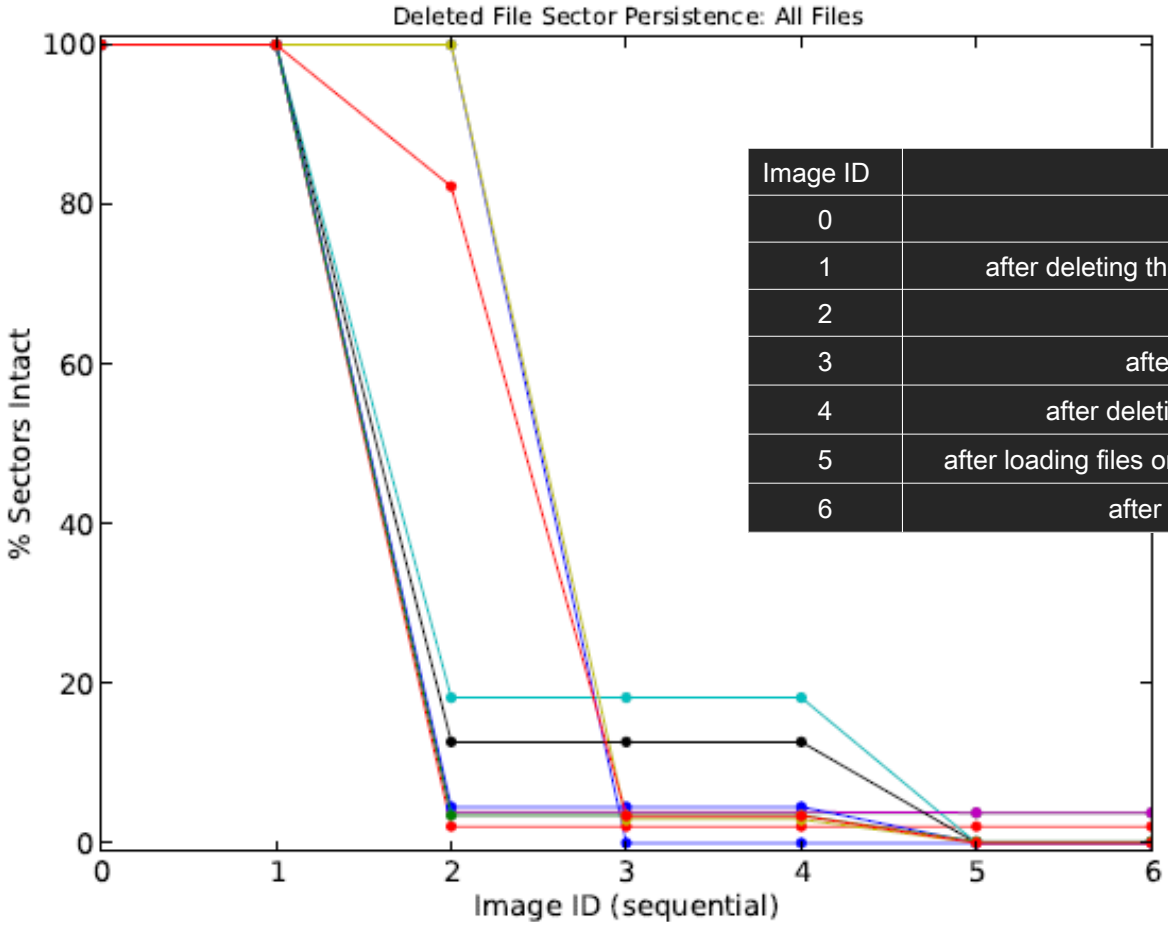
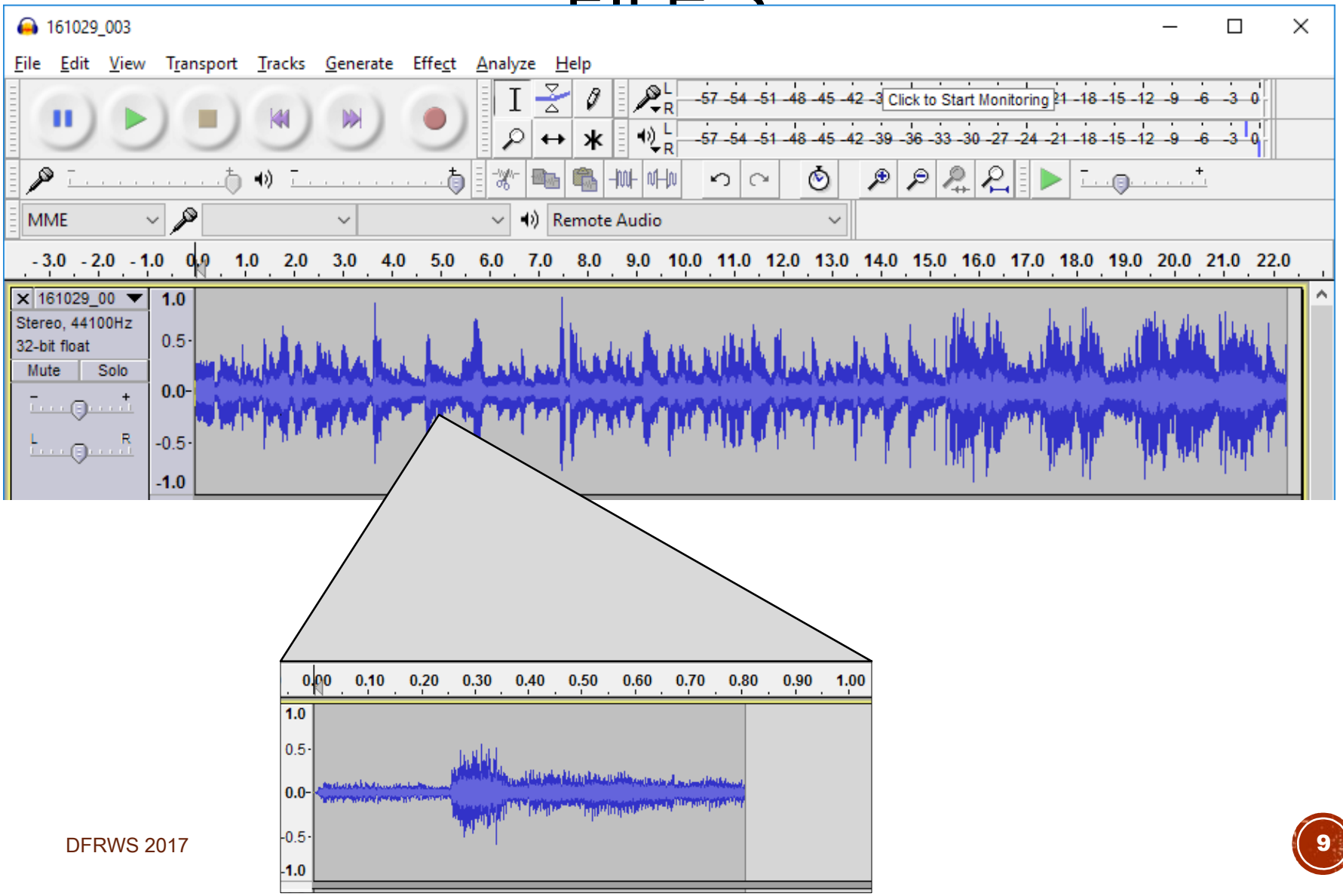


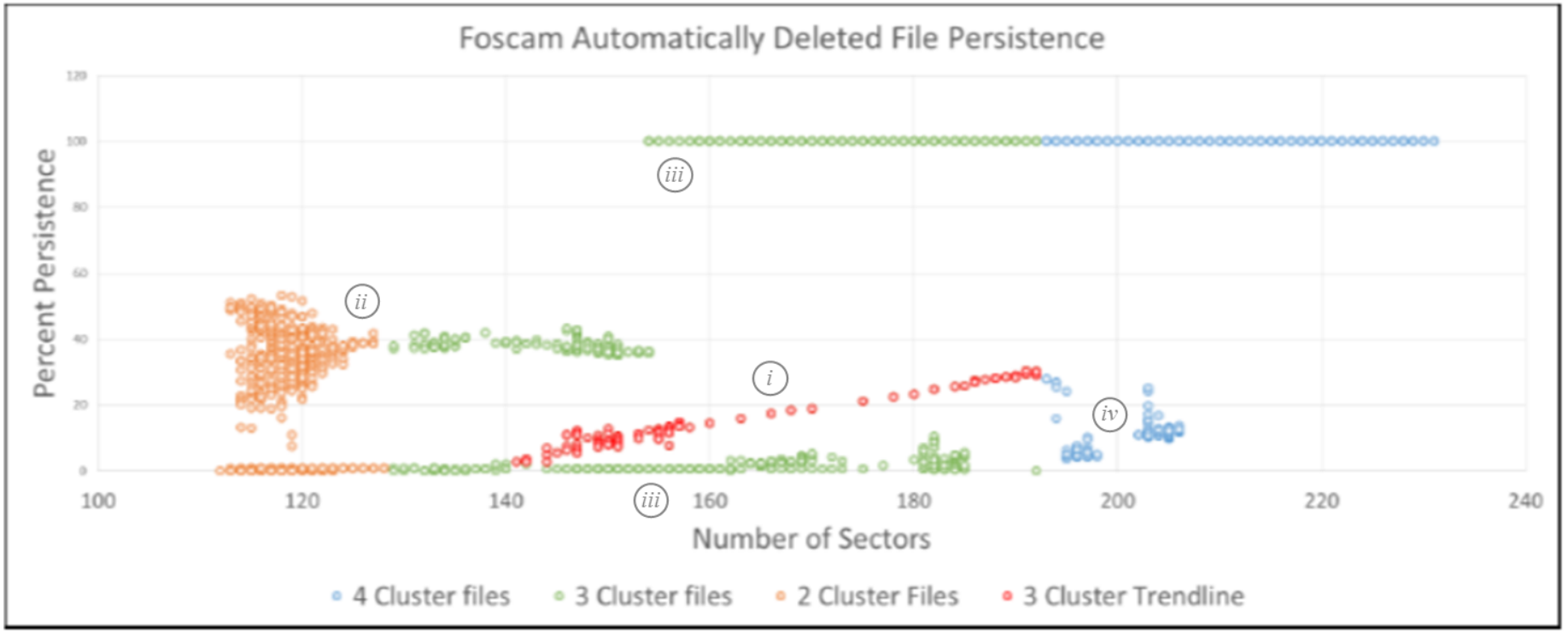
Image ID	Activity
0	after creating 10 audio files
1	after deleting those 10 files manually (via USB connection to PC)
2	after creating nine new audio files
3	after creating seven additional audio files
4	after deleting the newly created (all) files on the device
5	after loading files on the device manually (3GB; to near device capacity)
6	after (quick) reformatting the device storage

Jones, James. "Deleted Audio File Decay on a Digital Voice Recorder." Audio Engineering Society Conference: 2017 AES International Conference on Audio Forensics. Audio Engineering Society, 2017.

RECOVERED AUDIO FRAGMENTS FROM FILE 3

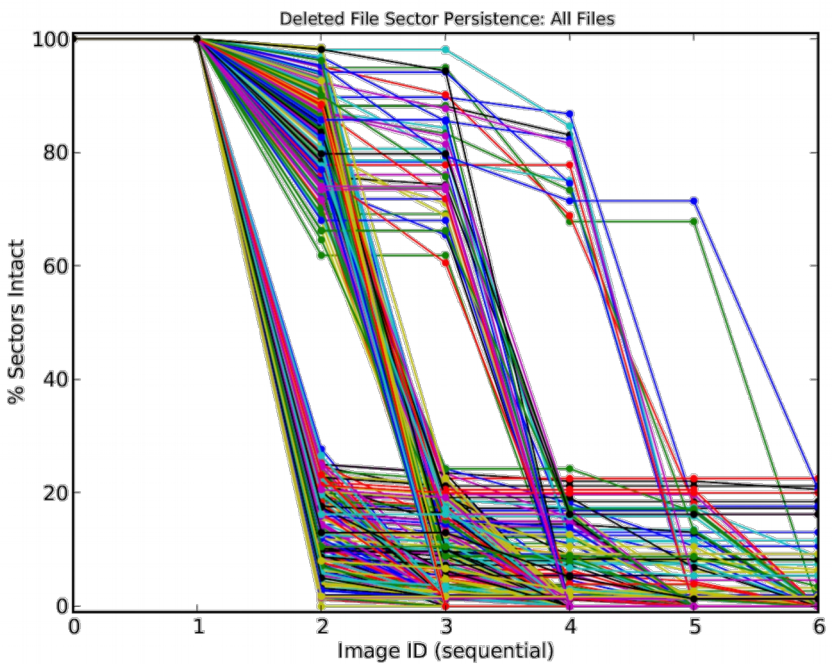


RESULTS: CAMERAS AND SDCARDS

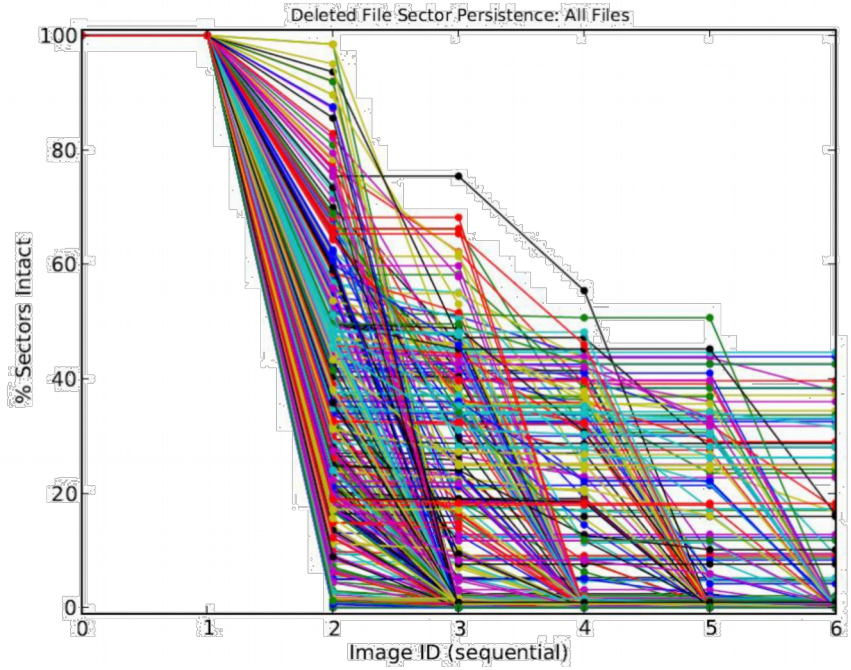


Jones, James H. Jr; Srivastava, Anurag; Mosier, Josh; Anderson, Connor; and Buenafe, Seth, "Understanding Deleted File Decay on Removable Media using Differential Analysis" (2017). Annual ADFSL Conference on Digital Forensics, Security and Law. 13.

SD CARDS: CLUSTER SIZE

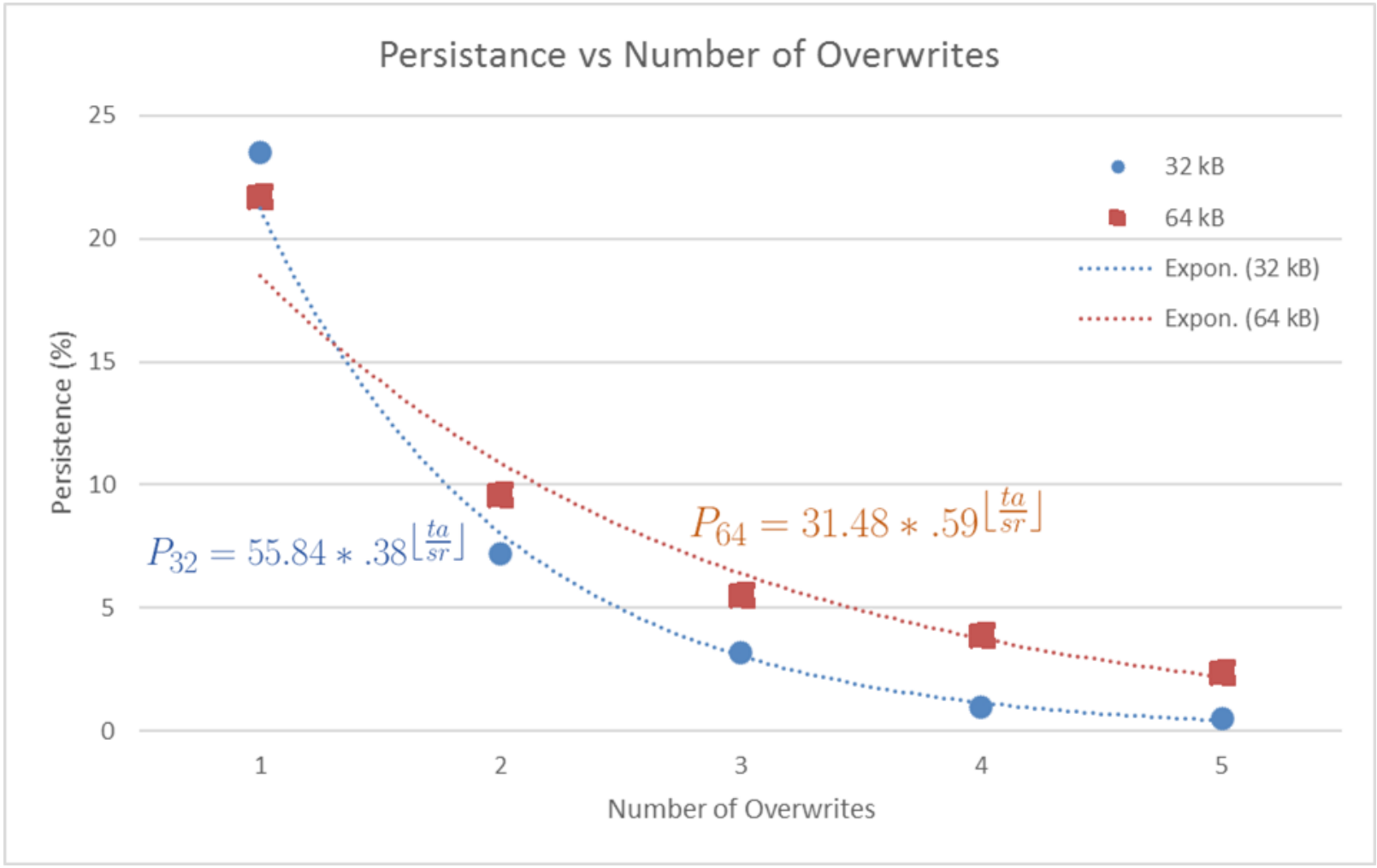


32 kB clusters

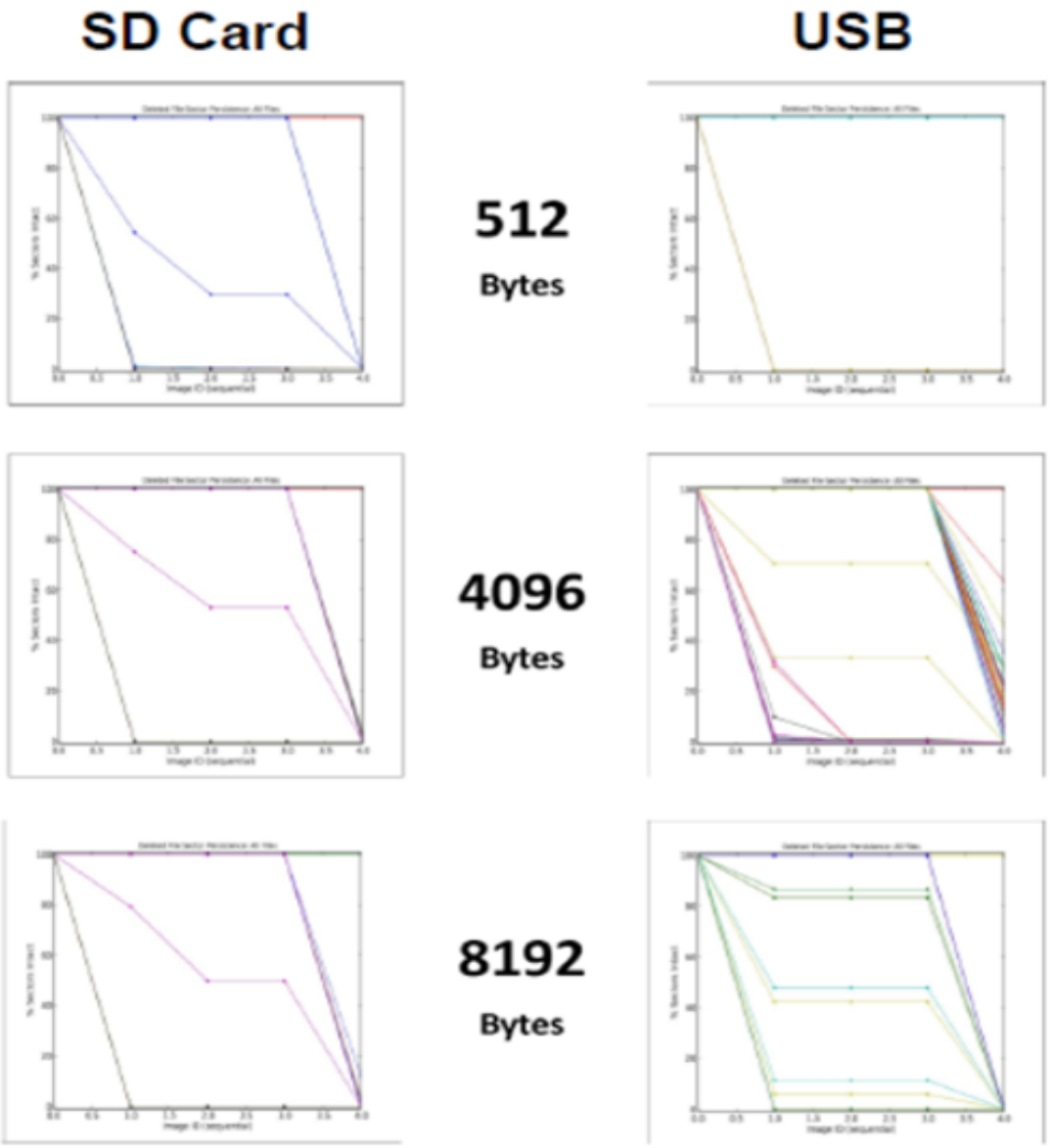


64 kB clusters

SD CARDS: CLUSTER SIZE (CONTINUED)



SD CARDS AND USB STICKS



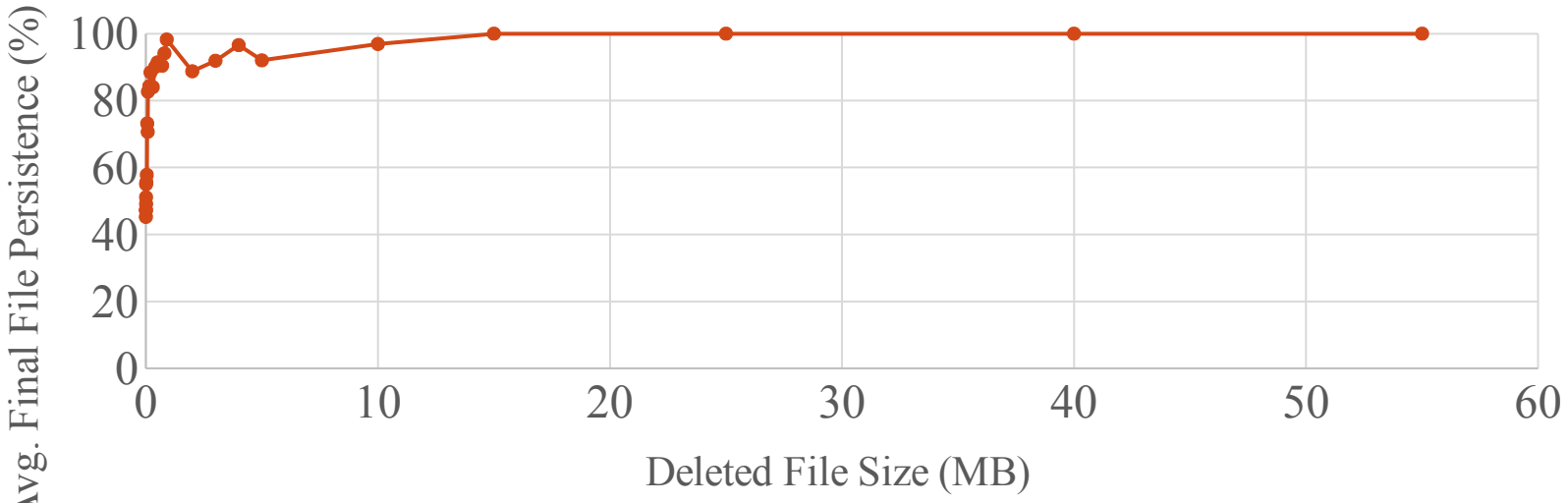
RESULTS: MAGNETIC HARD DISKS

- 12 Disks (3 disk frag levels x 4 disk free levels)
- 9 User Activities, Repeated 3 Times
- 12 x 9 x 3 = 324 experimental runs
- Dataset Includes:
  - Disk Free Bytes
  - Disk Fragmentation
  - User Activity
  - File Characteristics:
    - Source, Path, Image Offset, Extension, Size, Fragmentation
  - Final File Persistence

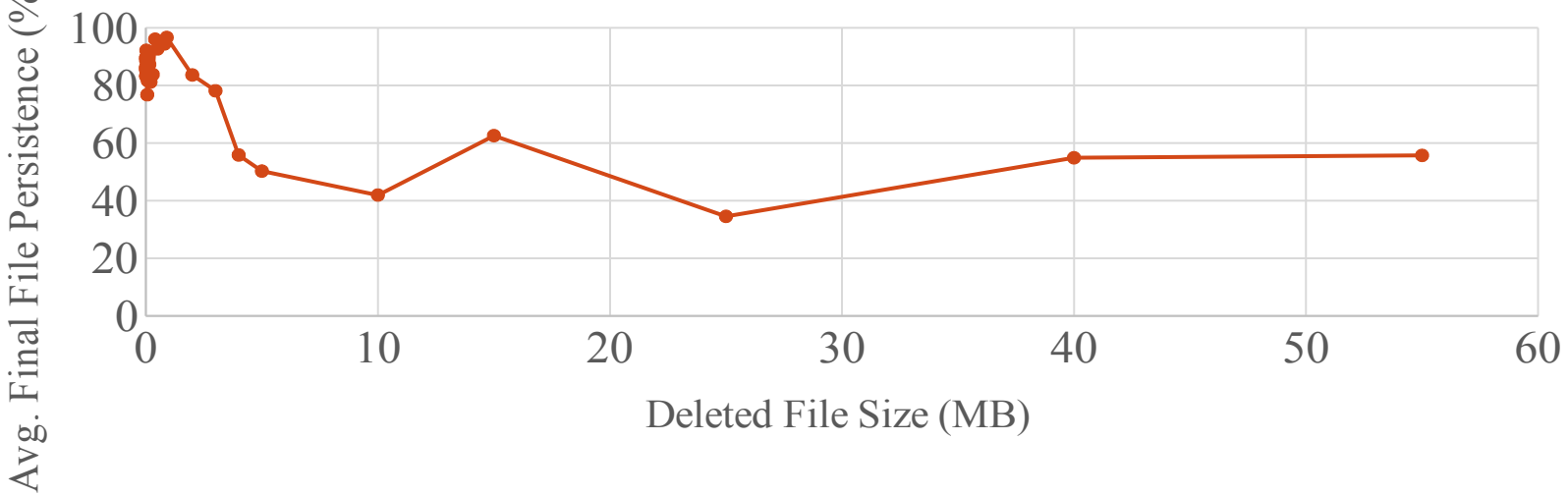
Experimental runs: 324
Tracked deleted files: 1917
Dataset records: 621,108

USER ACTIVITY

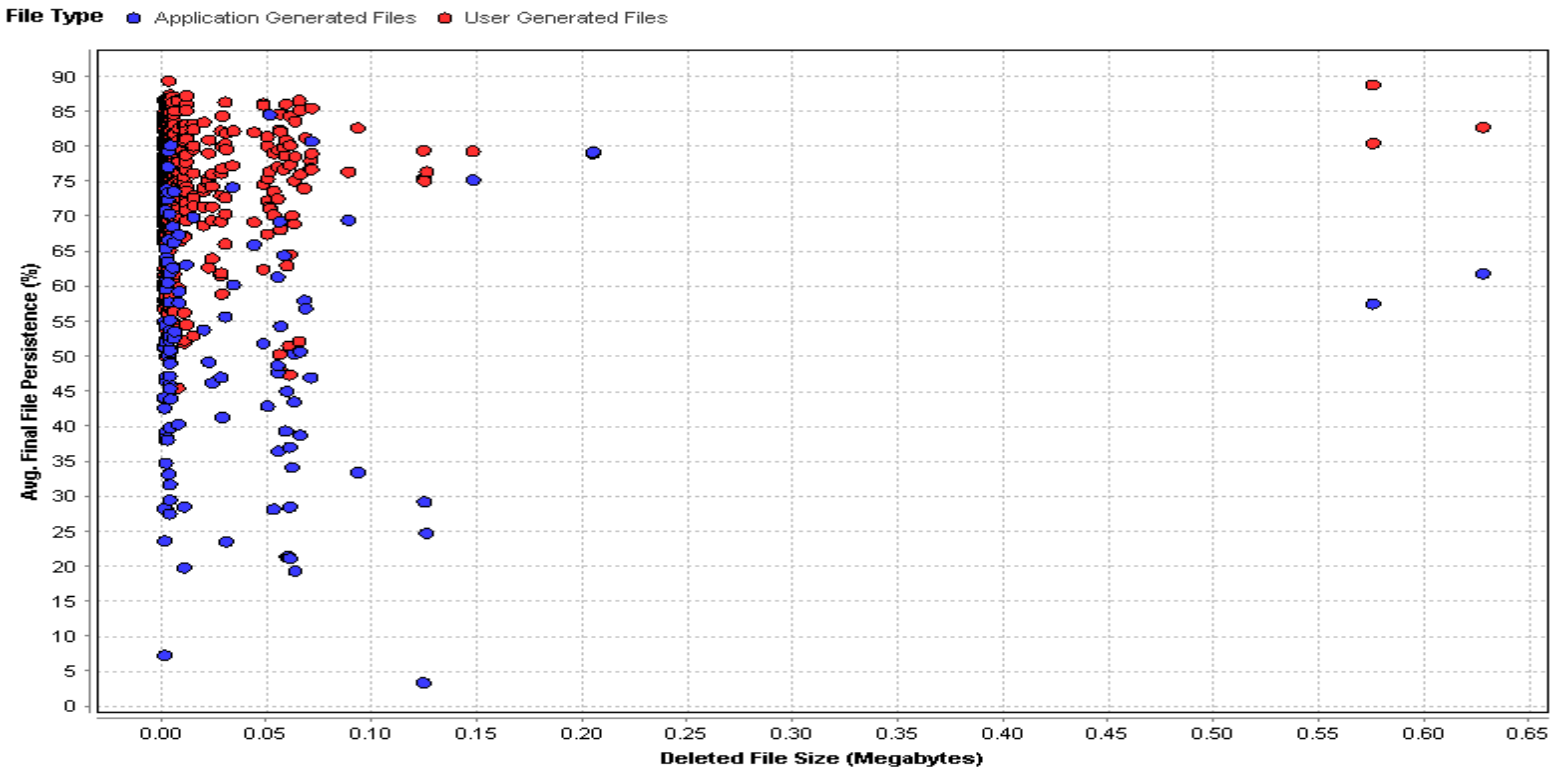
web



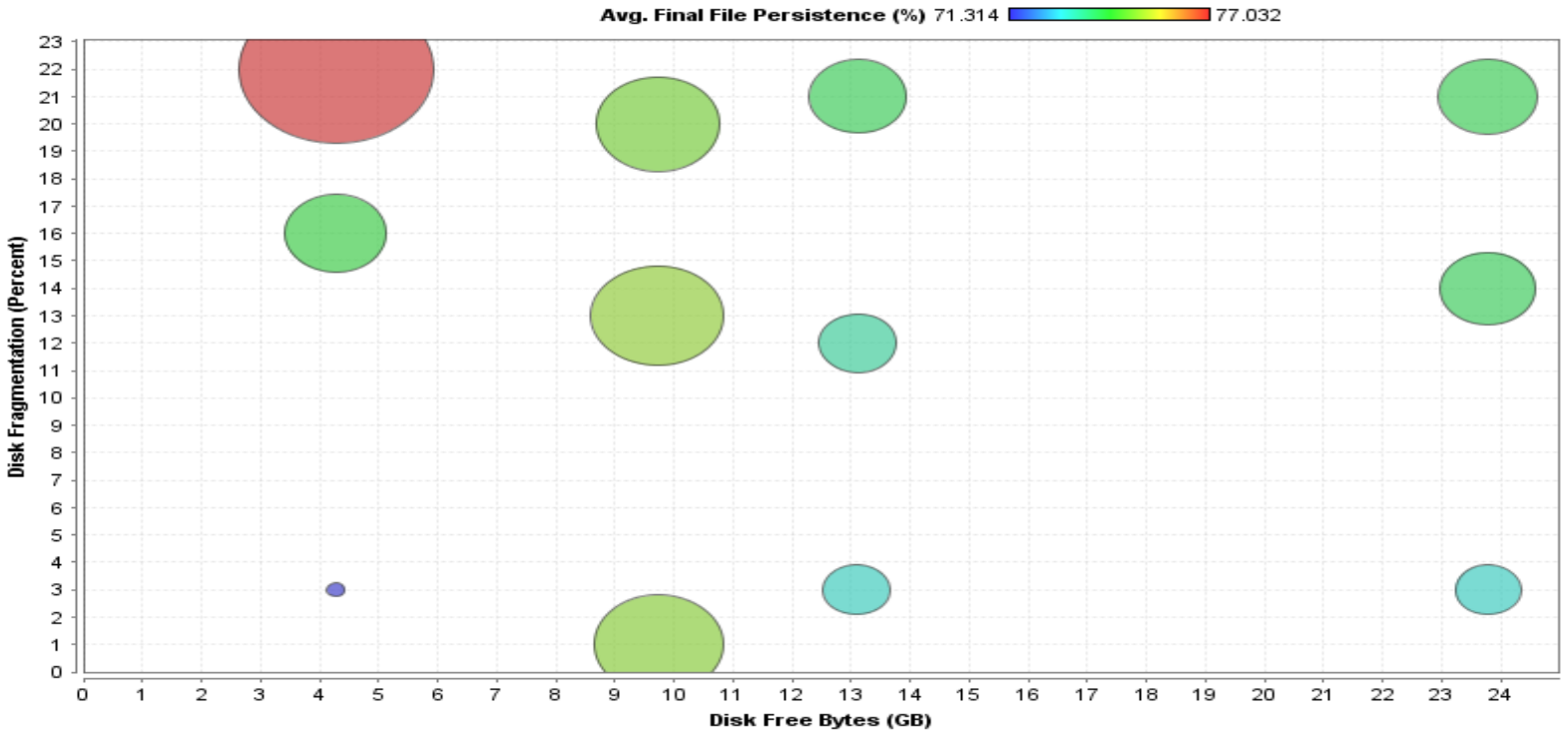
3GB



FILE SOURCE ("WHO" WROTE IT)



DISK FRAGMENTATION AND FREE DISK SPACE



LIMITATIONS AND FUTURE WORK

- Content is copied and moved, but we only track the initial logical location
- Deleted file decay is complicated; depends (at least) on:
  - OS, filesystem, hardware, user and system activity, format, disk usage and fragmentation, file characteristics, ... need to do more work
- Time matters: can we use a model to date the file deletion?
- Other devices, media, and applications:
  - SSDs, mobile, malware, ICS, ...

QUESTIONS?

Jim Jones, PhD
Associate Professor, ECE/DFCA
Nguyen Engineering Bldg., Room 3241
George Mason University, MS 2B5
Fairfax, VA 22030
(o) 703-993-5599
(c) 703-955-1033
(e) jjonesu@gmu.edu
(w) http://ece.gmu.edu/
(w) http://cfrs.gmu.edu/
Github: jjonesu/DeletedFilePersistence

BACKUP

M57 ADVANCED KEYLOGGER