

The Death (and Life) of Deleted File Contents

Jim Jones
George Mason University

October 17, 2017

8th Annual Open Source Digital Forensics Conference

Acknowledgements

- ◆ Tahir Khan (PhD student)
- ◆ Simson Garfinkel and Kevin Fairbanks (ideas and discussions)
- ◆ Alex Nelson (idifference2.py)
- ◆ University of Maryland and MITRE (grant)
- ◆ Multiple students...

Allocation, De-allocation, and Re-use

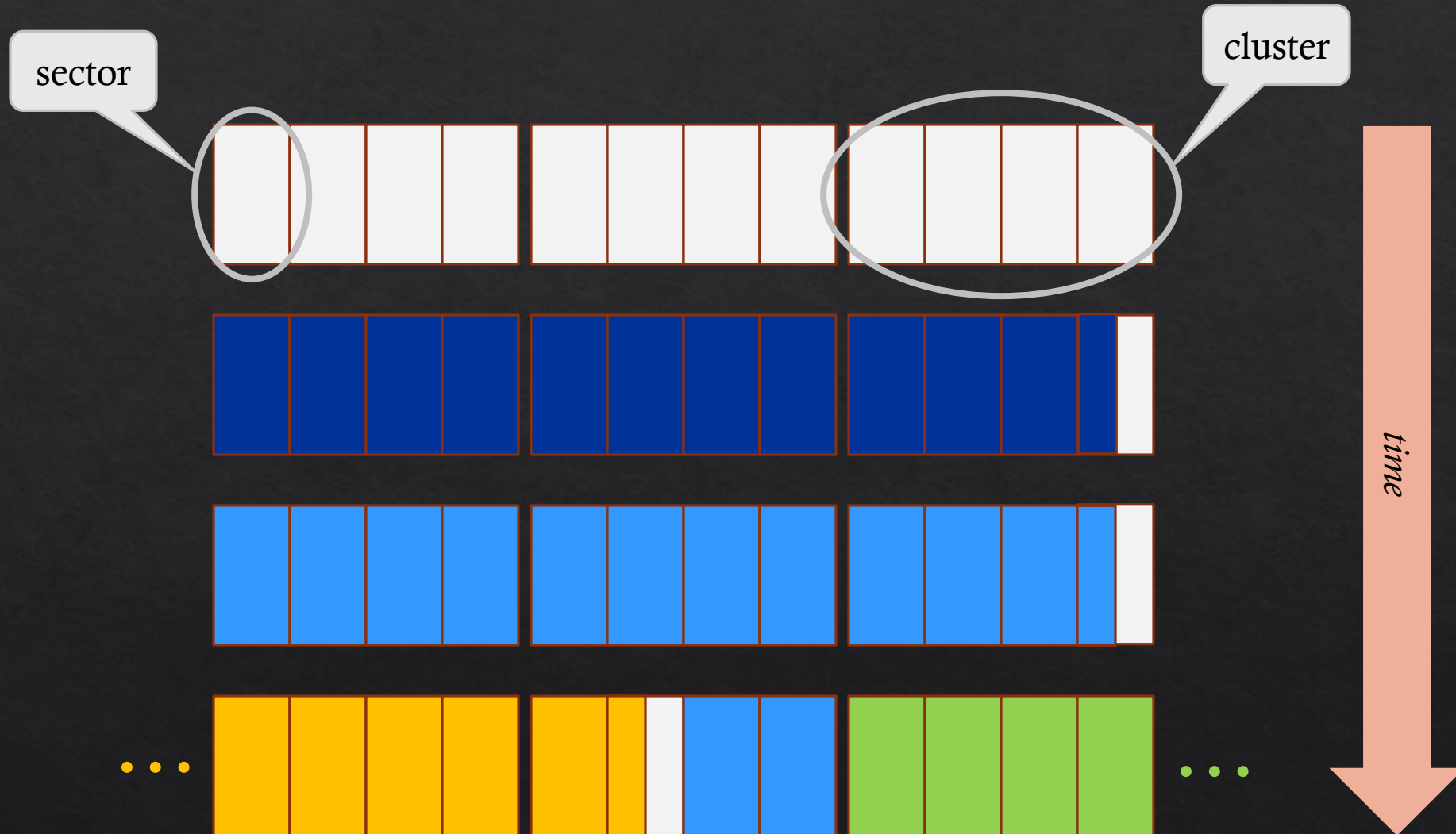
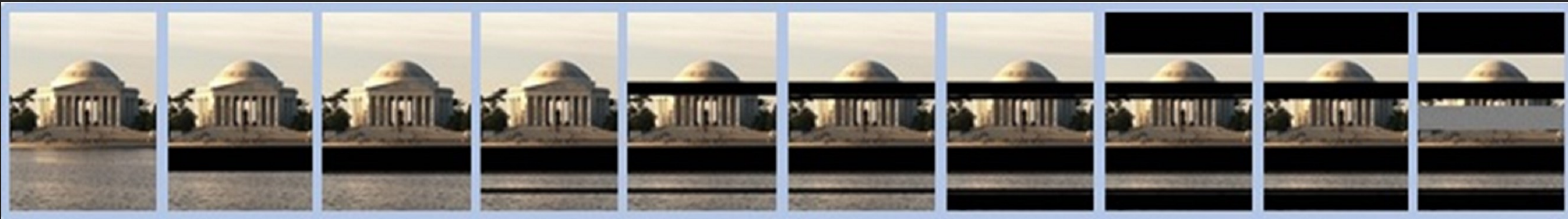
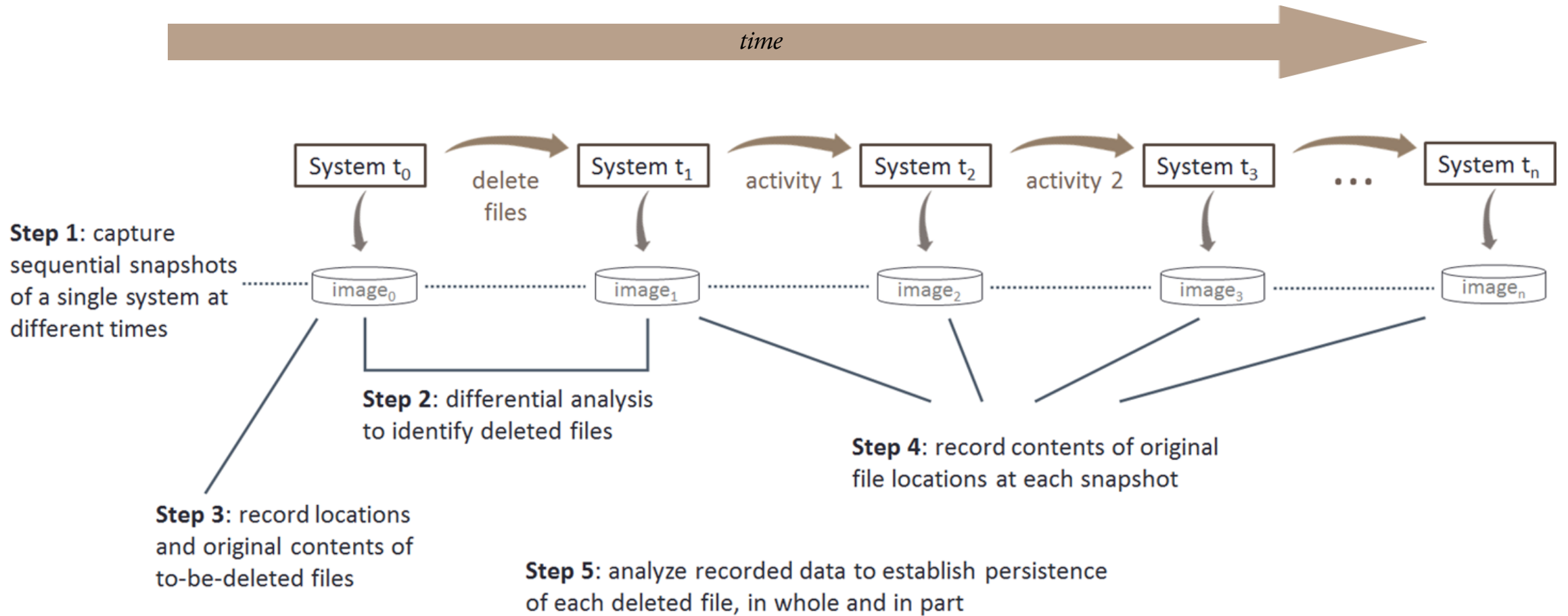


Image file (BMP) example...



Experimental Setup



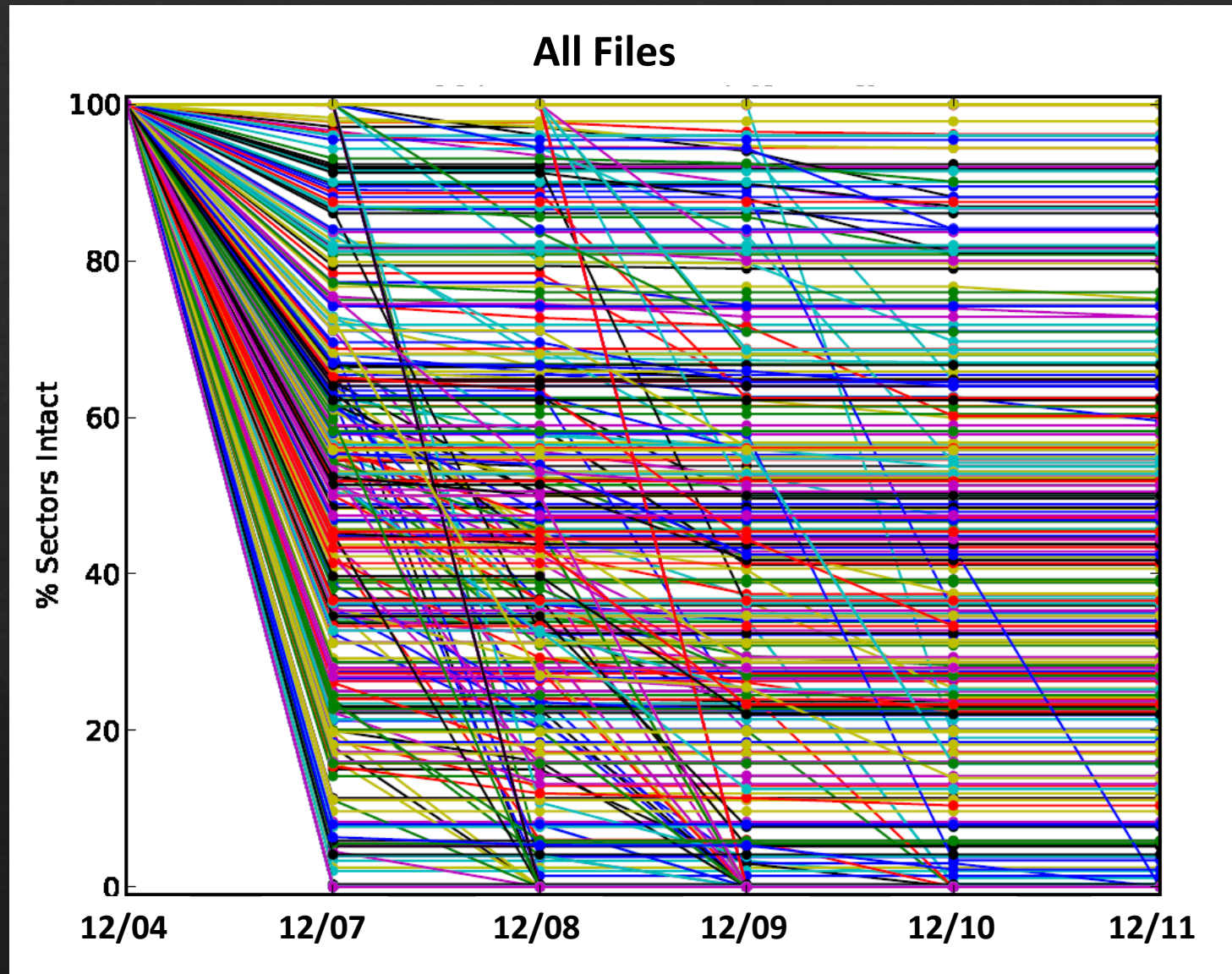
Jones, J. H., & Khan, T. M. (2017, January). A method and implementation for the empirical study of deleted file persistence in digital devices and media. In *Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual* (pp. 1-7). IEEE.

M57 Advanced Keylogger

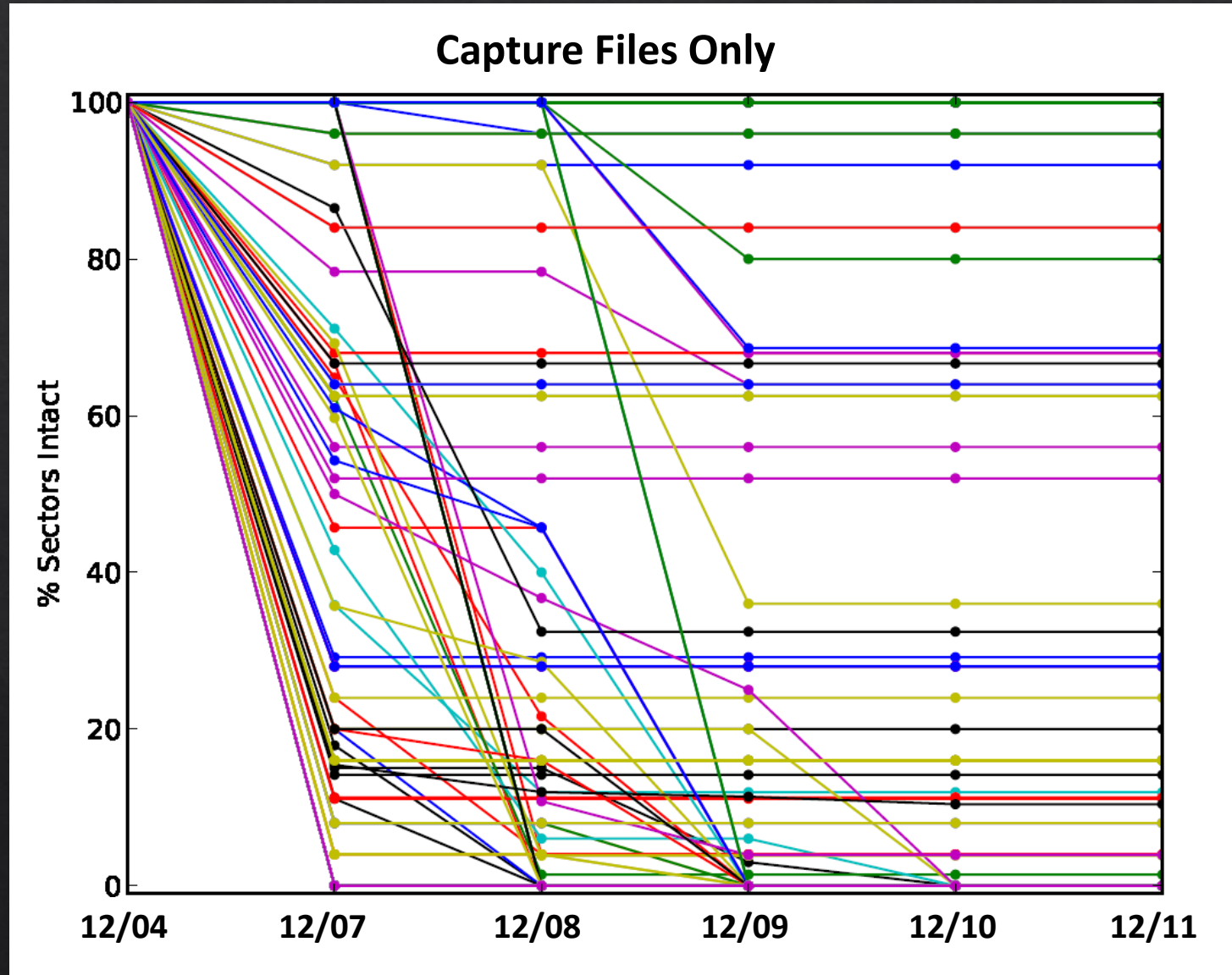
- ◆ 17 snapshots over 25 days (11/16 - 12/11)
- ◆ Advanced Keylogger installed on machine Pat 12/02 - 12/03
- ◆ Uninstalled and files deleted 12/04 - 12/07
 - ◆ 1314 files (662,307 sectors) deleted between these images
 - ◆ 691 of these files (13,173 sectors) are Advanced Keylogger logs
- ◆ Continued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

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

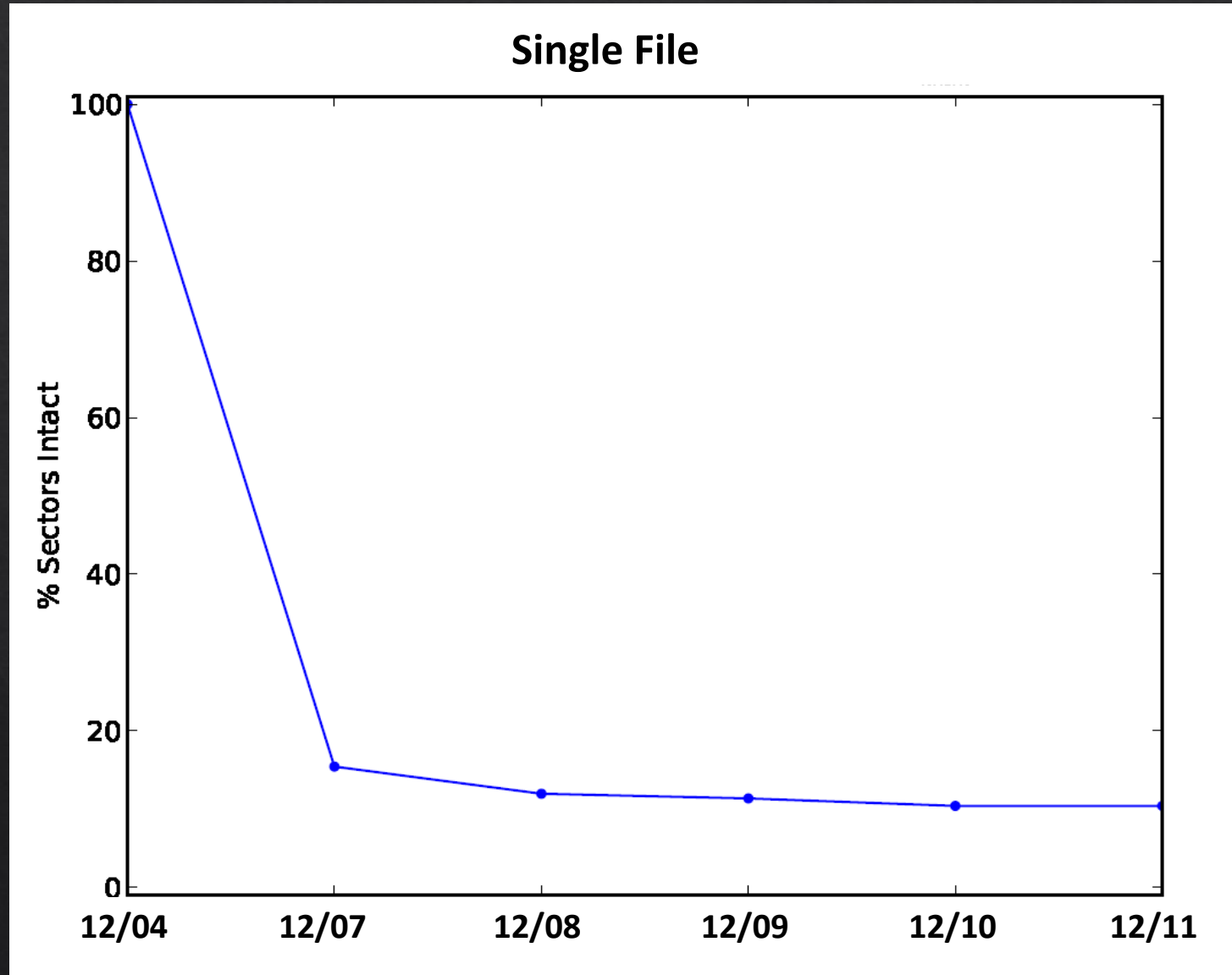
M57 AK: Decay Curves



M57 AK: Decay Curves



M57 AK: Decay Curves



Embedded Flash



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

Embedded Flash: Decay Curves

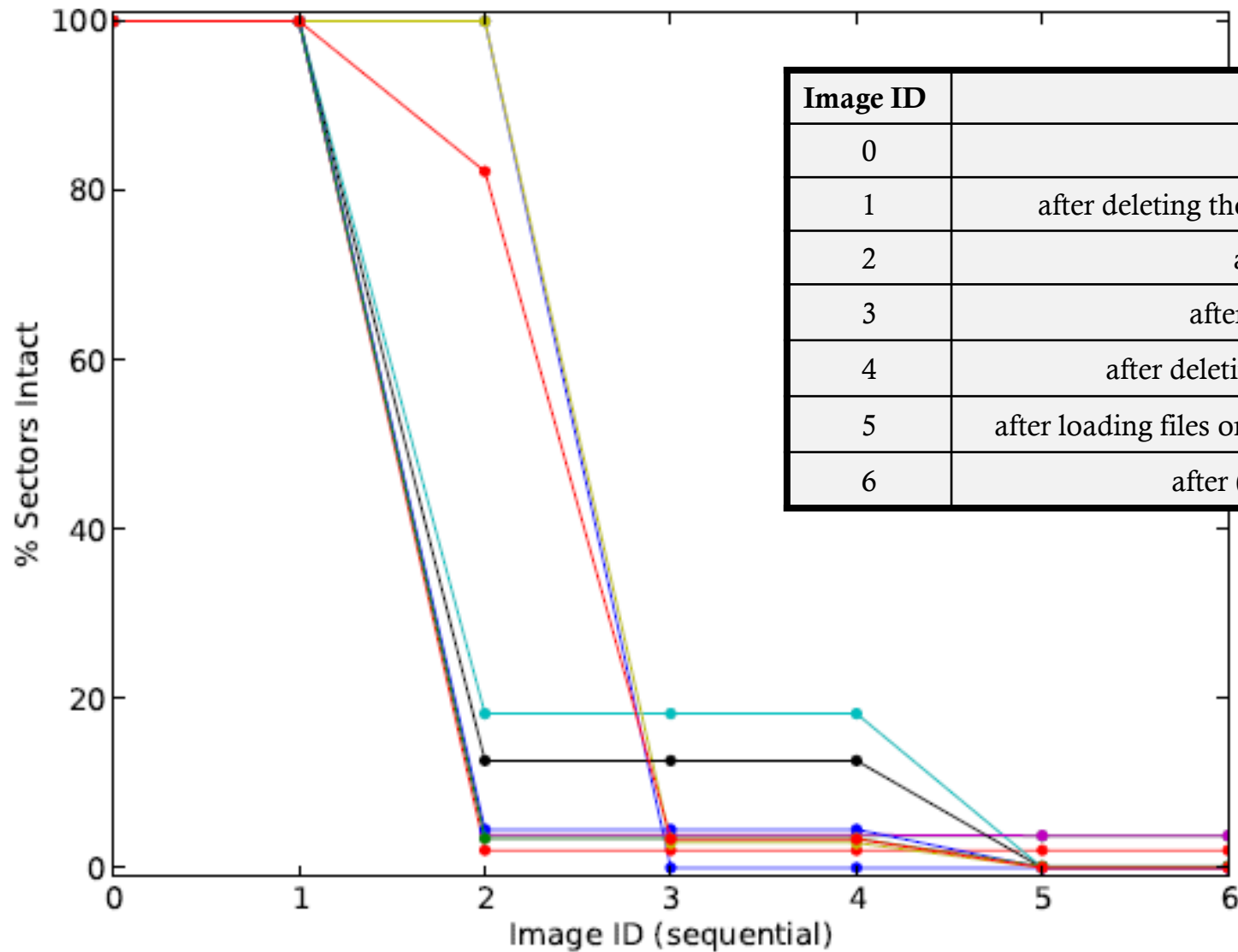


Image ID	Activity
0	after creating 10 audio files
1	after deleting those 10 files manually (via USB connection to PC)
2	after creating nine new audio files
3	after creating seven additional audio files
4	after deleting the newly created (all) files on the device
5	after loading files on the device manually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

Embedded Flash: Persistence Data

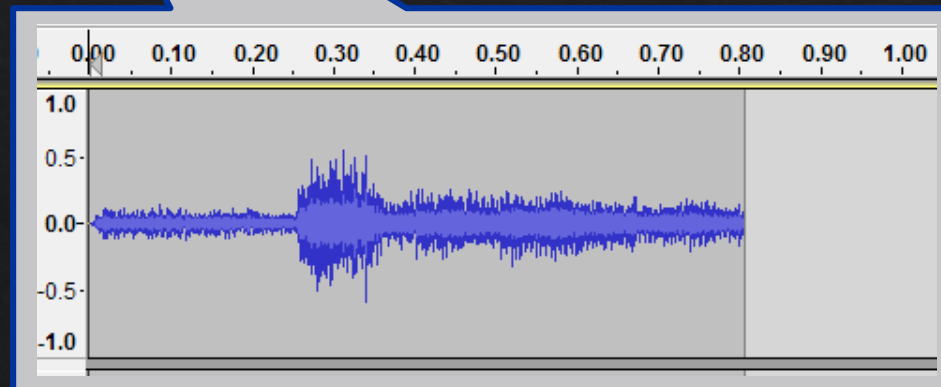
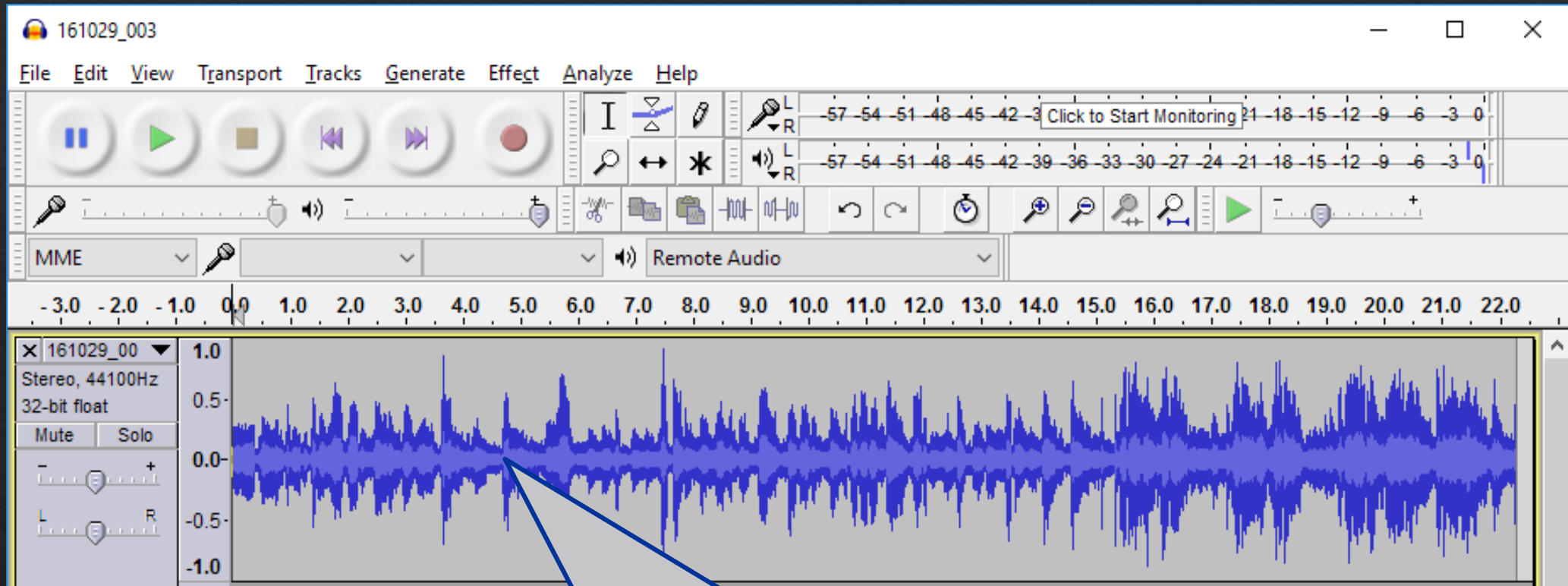
file	sectors	sectors intact at image ID:							final persistence
		0	1	2	3	4	5	6	
0	346	346	346	63	63	63	0	0	0.00%
1	746	746	746	28	28	28	28	28	3.75%
2	1065	1065	1065	22	22	22	22	22	2.07%
3	1055	1055	1055	41	41	41	40	40	3.79%
4	1435	1435	1435	65	65	65	0	0	0.00%
5	2554	2554	2554	88	88	88	5	5	0.20%
6	395	395	395	50	50	50	0	0	0.00%
7	1387	1387	1387	1141	47	47	0	0	0.00%
8	611	611	611	611	0	0	0	0	0.00%
9	1665	1665	1665	1665	49	49	0	0	0.00%

File 3 fragments on final image

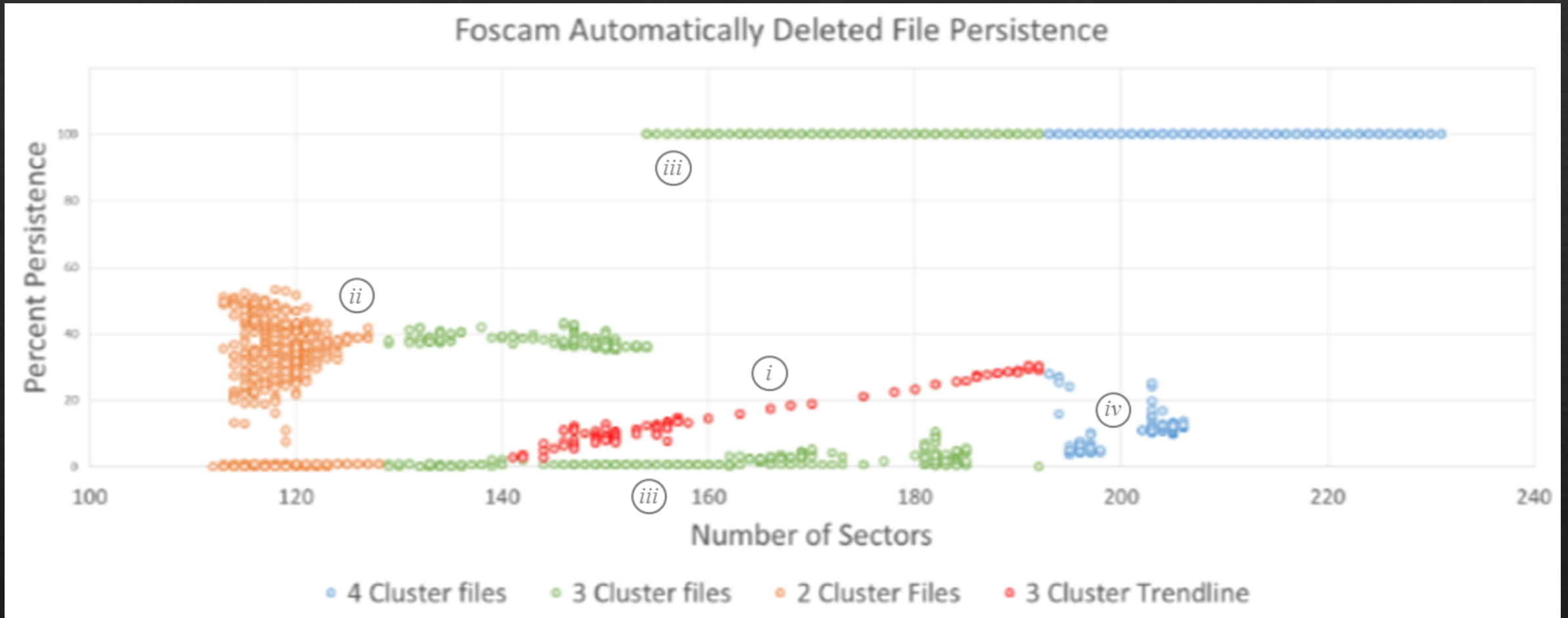
[illegible]

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	
AD	DB	7C	A9	68	2C	1D	B1	4B	9C	78	54	92	BB	F0	33	.Û @h,.+KœxT'»ß3
13	FF	FF	F8	8F	15	E6	A9	0A	7D	76	DD	66	56	D7	A1	.ÿÿœ..æ@.}vÝFV×;ı
17	60	37	3D	47	5A	42	93	36	A2	B9	85	8B	98	40	FE	.˙7=GZB"6œ˙...<~@p
52	97	1D	39	06	88	93	84	50	6E	0E	52	14	3B	92	90	R-.9.ˆˆ„Pn.R.:˙.
09	F1	52	A8	61	B8	AF	D6	7C	0A	24	A1	5F	3E	4C	C9	.ñR"ˆa,ˆÖ .\$.ı>LÉ
29	A6	ED	53	65	3F	06	C1	70	FD	6C	EE	D0	35	9B	F3	)ııİse?.ÁpýlİİĐ5>ó
CD	56	2D	5D	84	17	07	34	F1	FA	30	7E	67	6A	B6	31	İV-]„...4ñú0~gıııı
29	CD	68	5C	E5	8C	61	10	1B	2E	0B	47	60	FC	26	2F	)İh\â&Ea....Gˆüa/
2C	6E	26	5B	78	14	68	D0	A8	33	27	95	5E	E8	07	38	,nâ[x.hĐ"3'•ˆê.8
71	63	D3	0B	45	BA	DD	69	32	3C	69	4D	AA	FB	EC	DD	qcÖ.Eˆıı2<ıMˆüııY
15	A9	15	60	76	67	7A	66	61	6B	3A	3D	39	62	79	EE	ı@.˙vgzfak:ˆ9byİ
46	AD	39	E6	9B	09	FC	AD	2A	EC	EC	05	BD	18	5D	0C	F.9œ>ü.*İı.ıı.].
12	ED	49	05	A8	D7	59	F0	75	53	68	4C	11	86	68	5E	.ııı.˙Y8uShL.thˆ
36	1E	F8	95	42	3C	B5	30	47	06	1C	F2	D2	88	86	D7	6.œˆB<ııÖG..đÖ"ˆt×
B9	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	ııPNG.....ııHDR
00	00	04	32	00	00	02	46	08	02	00	00	00	26	A8	32	...2...F.....&"2
9A	00	00	2E	BC	49	44	41	54	78	DA	ED	DD	09	9C	94	š...ıııDATxÜııY.œ"
85	7D	F0	F1	07	08	97	79	4D	13	49	7C	B5	2A	C6	28	...)đñ..-yM.ııııE(
C6	10	35	82	37	88	88	82	A8	1C	72	0B	72	88	28	F7	E.5,7ˆˆ,˙.r.r.ˆ(÷
15	D0	78	E2	15	9B	A6	49	B4	8D	CD	E1	27	26	4D	B1	.Đxâ.>ııı.İá'âM±
69	93	26	D5	A4	B1	B1	D6	56	73	34	79	13	93	98	80	ı"ˆôœııııÖVs4y.˙"ˆE
78	04	10	03	2C	7B	71	88	1C	BB	B3	CB	39	EF	F3	EC	x...,ııqˆ.˙»ˆE9ııđıı
B3	3B	2C	B3	33	B3	B3	B0	27	FB	FD	7E	FE	AE	BB	B3	˙,˙3˙3˙3˙ıııı~pœ˙3
33	CF	3E	F3	EC	1C	CF	6F	66	76	08	92	87	0B	86	FD	3ıı>đıı.İœfv.'˙ı.ııY
A1	C3	F0	95	E1	04	43	FF	14	CD	0D	AB	AB	67	D4	86	ııÄšˆâ.CŸ.İ.«gÖt
60	EC	C6	E0	E6	C2	60	5A	49	FC	B1	C3	AD	5B	82	69	˙ııEâœÄ`ZııüııÄ.ıııı
9B	83	9B	4B	82	29	9B	A3	4F	A6	D4	CC	C4	AD	C6	98	>f>K,)ıı>ŁııÖııİ.Ê"
76	36	DB	8D	31	ED	68	26	95	1A	63	DA	D1	A4	DF	E3	v6Ü.ııııœ.ııCÜñııBâ
1F	BE	0F	30	3A	9E	A2	E8	E3	B0	92	AA	4F	8A	AA	3E	ıı.0:žœœä"ıı"œÖšˆ>
6C	FF	3C	03	64	8C	3C	F0	D3	0C	6C	00	47	3C			

Recovered fragments from file 3

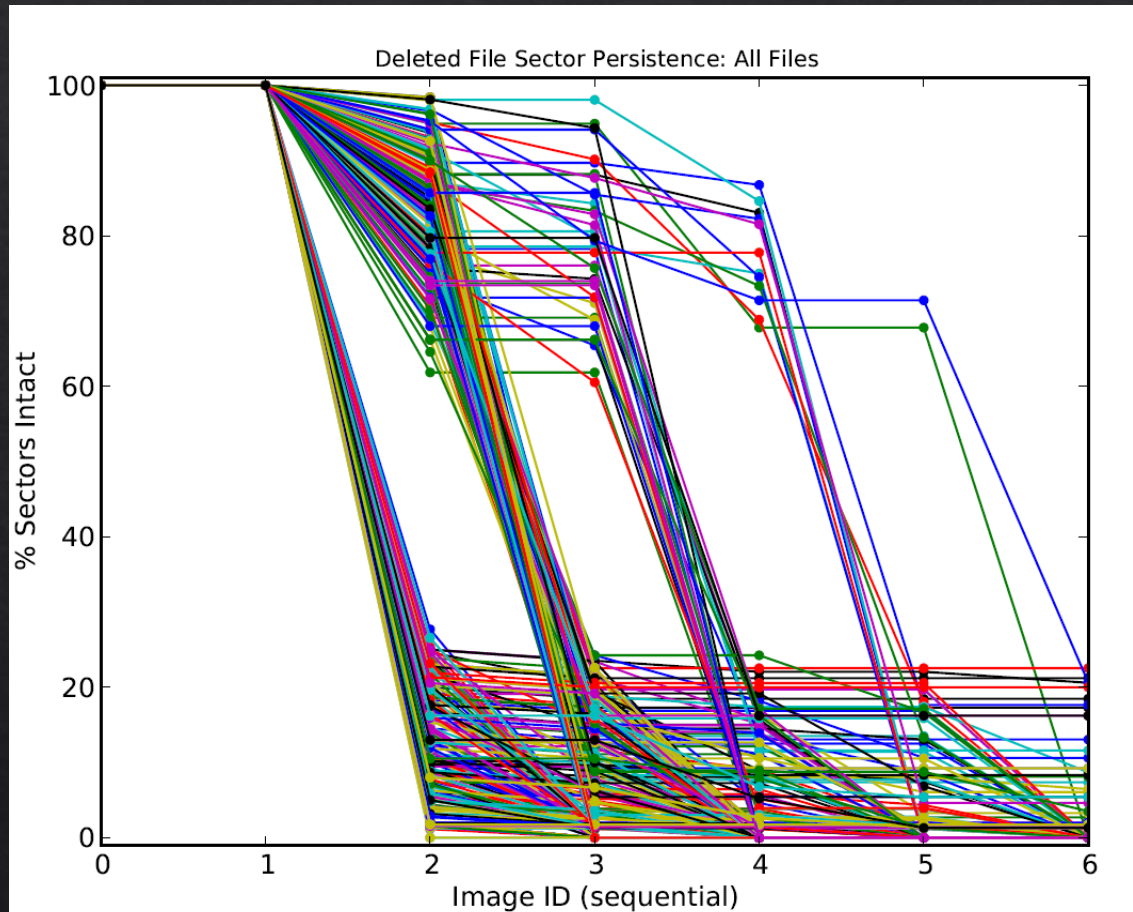


Cameras and SD Cards

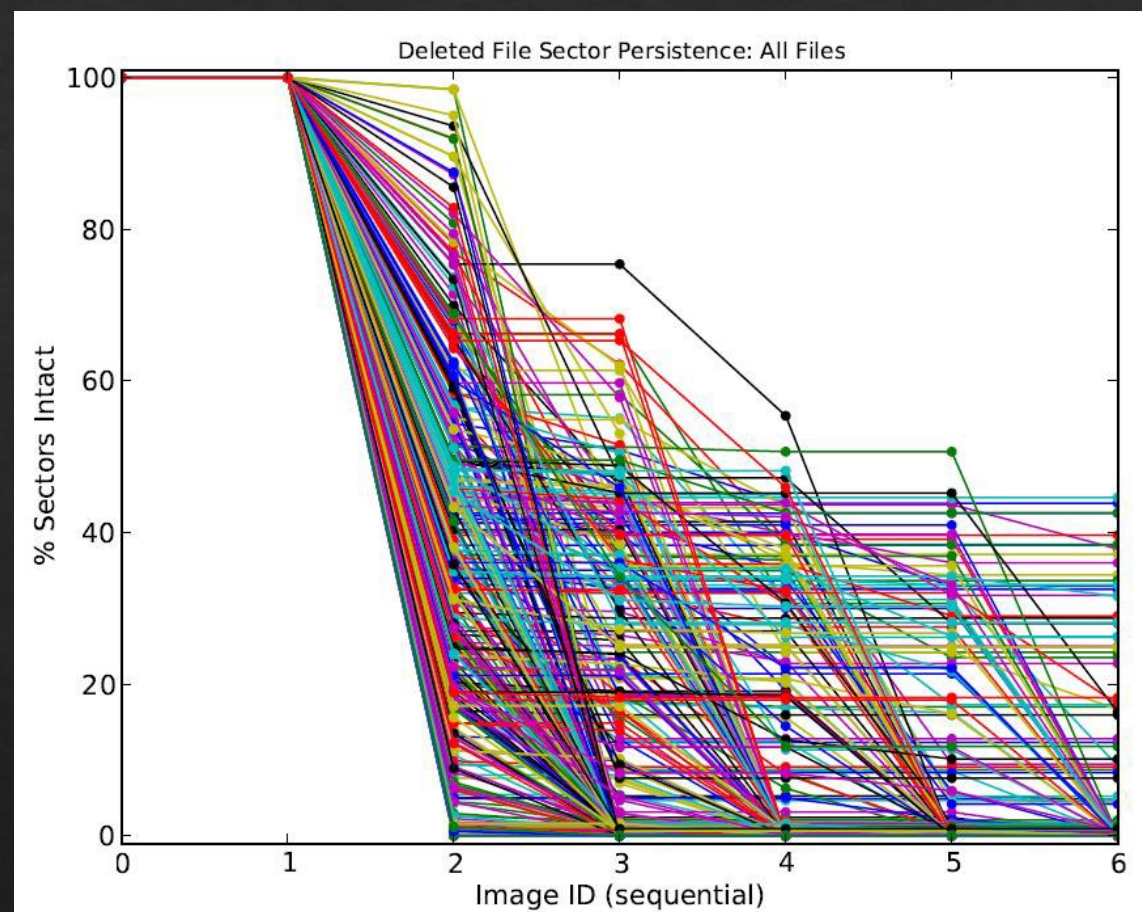


Jones, James H. Jr; Srivastava, Anurag; Mosier, Josh; Anderson, Connor; and Buenafe, Seth, "Understanding Deleted File Decay on Removable Media using Differential Analysis" (2017). Annual ADFSL Conference on Digital Forensics, Security and Law. 13.

SD Cards

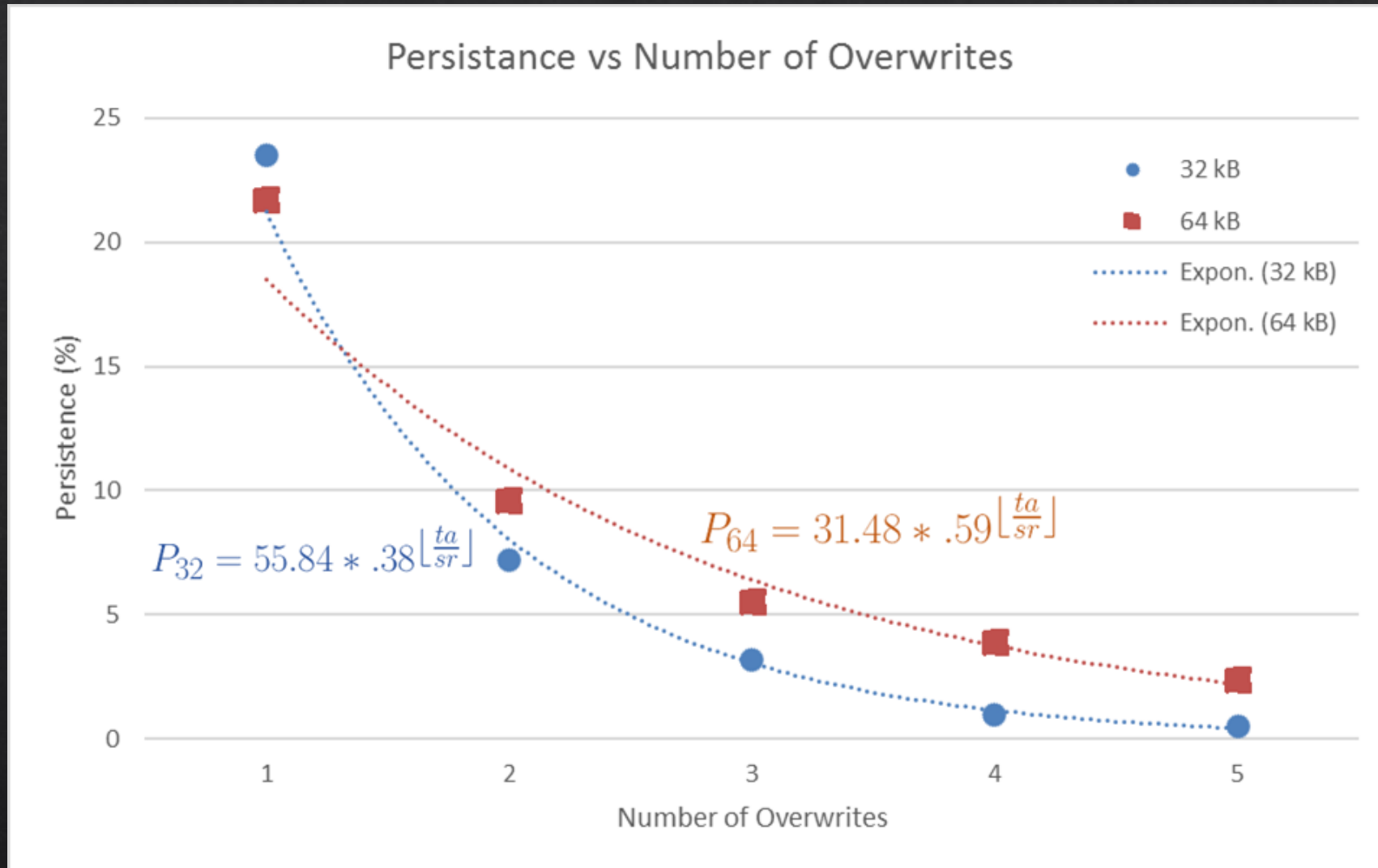


32 kB clusters



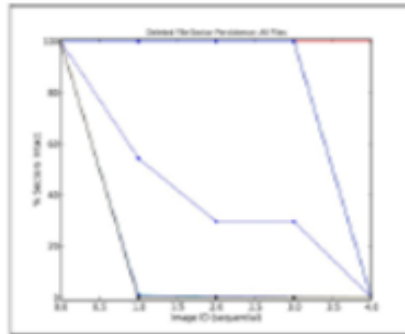
64 kB clusters

SD Cards: cluster size (continued)

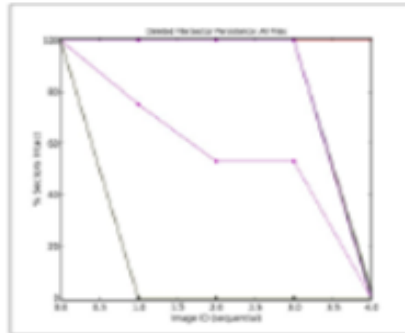


SD Cards and USB sticks

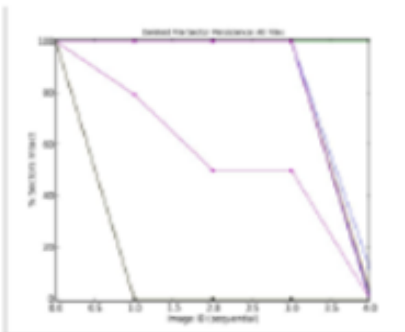
SD Card



512
Bytes

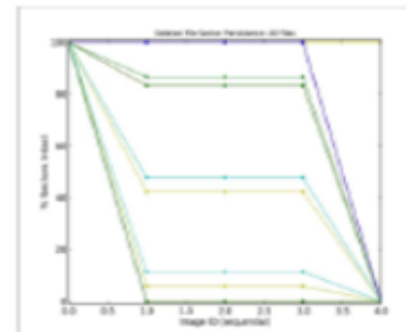
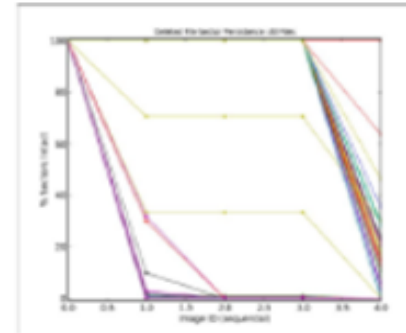
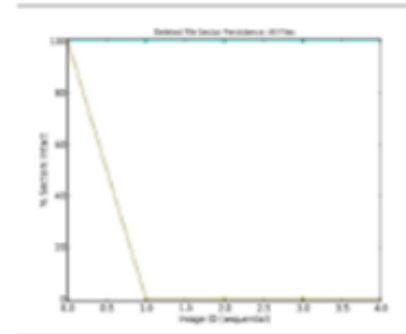


4096
Bytes



8192
Bytes

USB



Magnetic Hard Disks

- ◆ 12 Disks (3 disk frag levels x 4 disk free levels)

- ◆ 9 User Activities, Repeated 3 Times

- ◆ $12 \times 9 \times 3 = 324$ experimental runs

- ◆ Dataset Includes:

 - ◆ Disk Free Bytes

 - ◆ Disk Fragmentation

 - ◆ User Activity

- ◆ File Characteristics:

 - ◆ Source, Path, Image Offset, Extension, Size, Fragmentation

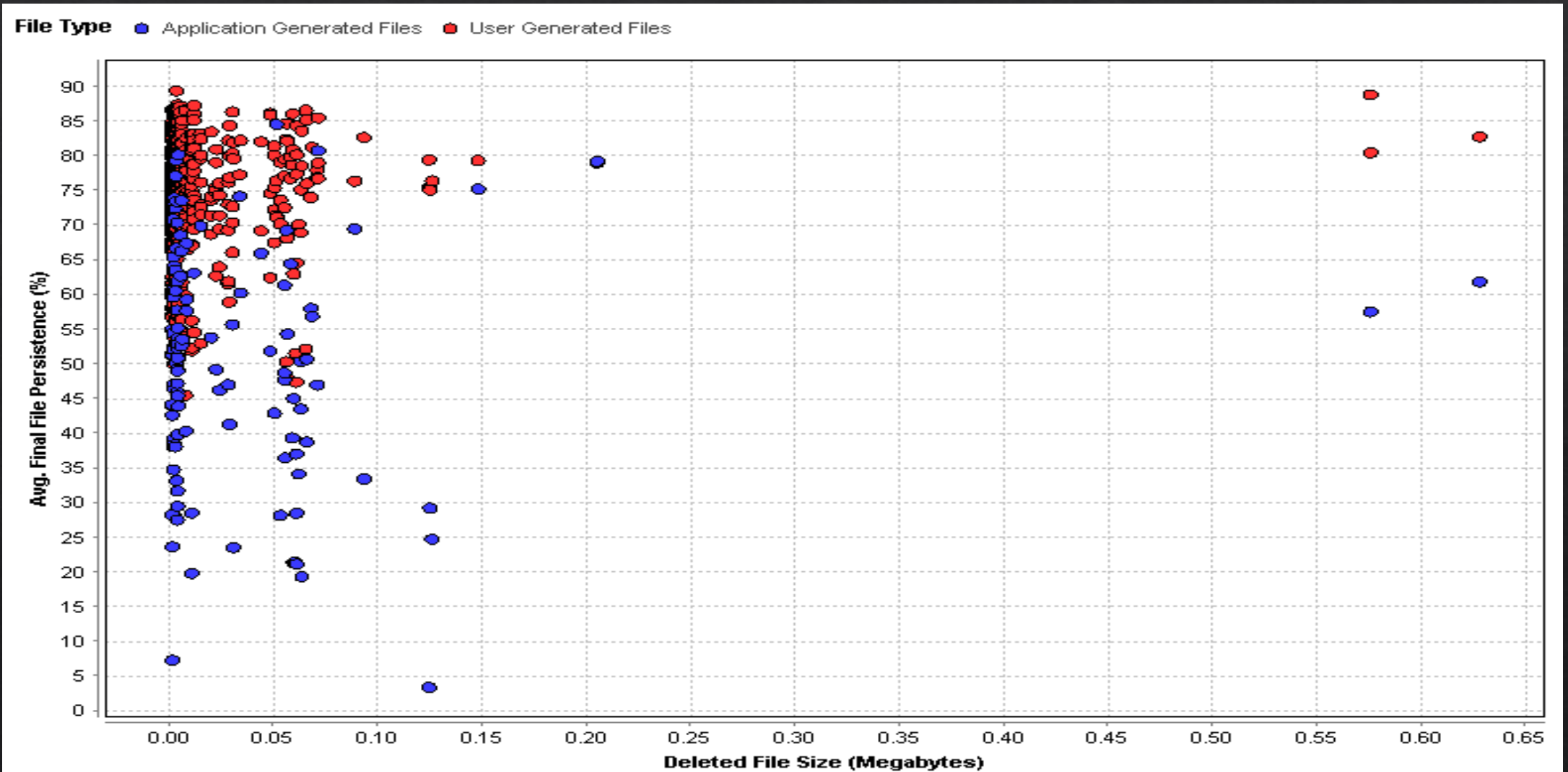
- ◆ Final File Persistence

Experimental runs: 324

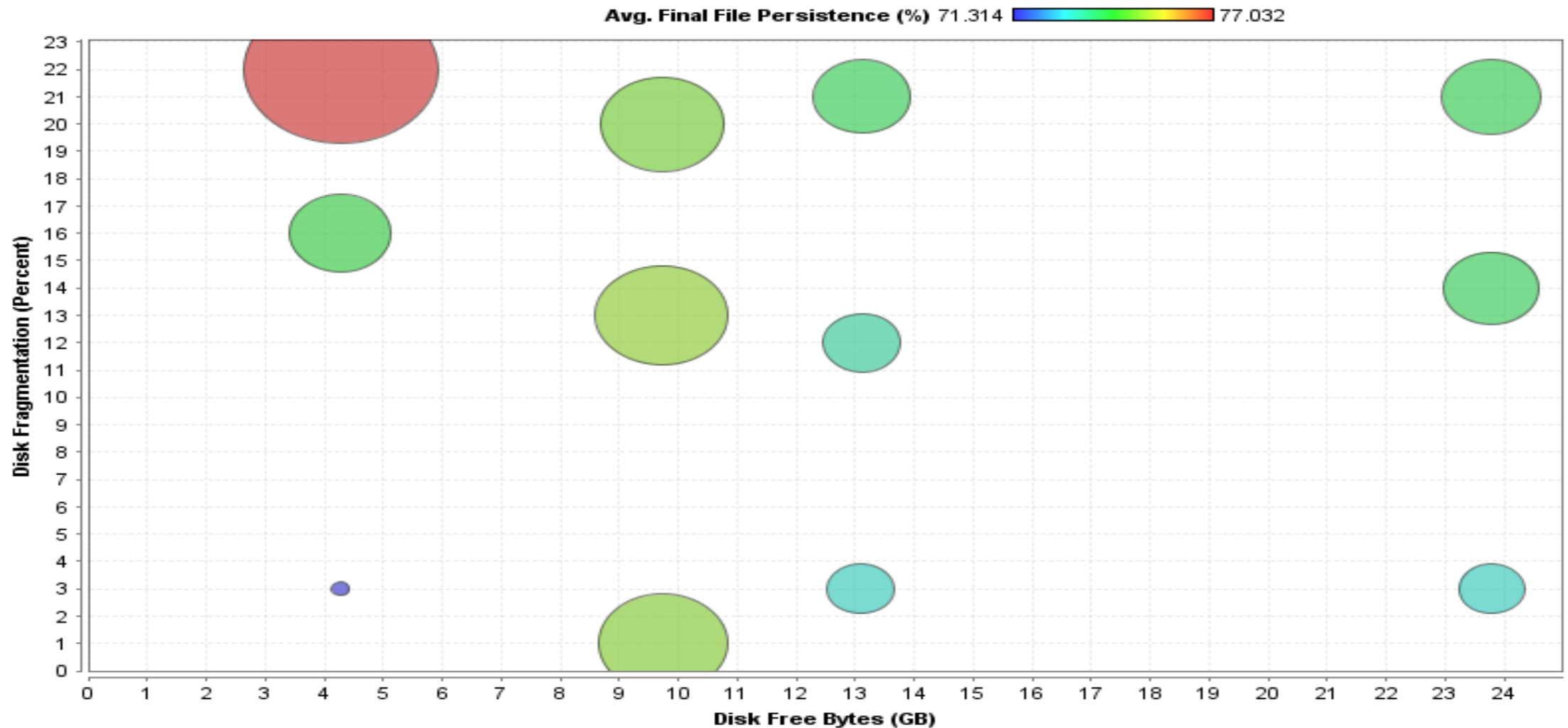
Tracked deleted files: 1917

Dataset records: 621,108

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

Digital Forensics and Cyber Analysis

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/>

<https://github.com/jjonesu/DeletedFilePersistence>

File Decay Patterns

[illegible]

[illegible]

810114560	*	.	.	.	.	.
810115072	*	.	.	.	.	.
810115584	*	.	.	.	.	.
810116096	*	.	.	.	.	.
810116608	*	.	.	.	.	.
810117120	*	.	.	.	.	.
810117632	*	*	*	.	.	.
810118144	*	*	*	.	.	.

848219648	*	.	.	.	.	.
848220160	*	.	.	.	.	.
848220672	*	.	.	.	.	.
848221184	*	.	.	.	.	.
848221696	*	.	.	.	.	.
848222208	*	.	.	.	.	.
848222720	*	.	.	.	.	.
848223232	*	.	.	.	.	.
848223744	*	.	.	.	.	.
848224256	*	.	.	.	.	.
848224768	*	.	.	.	.	.
848225280	*	.	.	.	.	.
848225792	*	.	.	.	.	.
848226304	*	.	.	.	.	.
848226816	*	.	.	.	.	.
848227328	*	.	.	.	.	.
848227840	*	.	.	.	.	.

9163230720	*	.	.	.	.	.
9163231232	*	.	.	.	.	.
9163231744	*	.	.	.	.	.
9163232256	*	.	.	.	.	.
9163232768	*	.	.	.	.	.
9163233280	*	.	.	.	.	.
9163233792	*	.	.	.	.	.
9163234304	*	.	.	.	.	.
9163234816	*	.	.	.	.	.
9163235328	*	.	.	.	.	.
9163235840	*	.	.	.	.	.
9163236352	*	.	.	.	.	.
9163236864	*	*	*	*	*	*
9163237376	*	*	*	*	*	*
9163237888	*	*	*	*	*	*
9163238400	*	*	*	*	*	*
9163238912	*	.	.	.	.	.
9163239424	*	.	.	.	.	.
9163239936	*	.	.	.	.	.
9163240448	*	.	.	.	.	.
9163240960	*	.	.	.	.	.
9163241472	*	.	.	.	.	.
9163241984	*	.	.	.	.	.
9163242496	*	.	.	.	.	.
9163243008	*	.	.	.	.	.

11458395648	*	.	.	.	.	.
11458396160	*	*	*	*	*	*
11458396672	*	*	*	*	*	*
11458397184	*	*	*	*	*	*
11458397696	*	*	*	*	*	*
11458398208	*	*	*	*	*	*
11458398720	*	*	*	*	*	*
11458399232	*	*	*	*	*	*
11458399744	*	*	*	*	*	*
11458400256	*	*	*	*	*	*
11458400768	*	*	*	*	*	*
11458401280	*	*	*	*	*	*
11458401792	*	*	*	*	*	*
11458402304	*	*	*	*	*	*
11458402816	*	*	*	*	*	*
11458403328	*	*	*	*	*	*
11458403840	*	*	*	*	*	*
11458404352	*	*	*	*	*	*
11458404864	*	*	*	*	*	*
11458405376	*	*	*	*	*	*
11458405888	*	*	*	*	*	*
11458406400	*	*	*	*	*	*
11458406912	*	*	*	*	*	*
11458407424	*	*	*	*	*	*
11458407936	*	.	.	.	.	.

11459780096	*	.	.	.	.	.
11459780608	*	.	.	.	.	.
11459781120	*	.	.	.	.	.
11459781632	*	.	.	.	.	.
11459782144	*	.	.	.	.	.
11459782656	*	.	.	.	.	.
11459783168	*	.	.	.	.	.
11459783680	*	.	.	.	.	.
11459784192	*	.	.	.	.	.
11459784704	*	.	.	.	.	.
11459785216	*	.	.	.	.	.
11459785728	*	.	.	.	.	.
11459786240	*	*	*	*	*	*
11459786752	*	*	*	*	*	*
11459787264	*	*	*	*	*	*
11459787776	*	*	*	*	*	*

11459898880	*	.	.	.	.	.
11459899392	*	.	.	.	.	.
11459899904	*	.	.	.	.	.
11459900416	*	.	.	.	.	.
11459900928	*	.	.	.	.	.
11459901440	*	.	.	.	.	.
11459901952	*	.	.	.	.	.
11459902464	*	.	.	.	.	.
11459902976	*	.	.	.	.	.

11458526720	*	.	.	.	.	.
11458527232	*	*	*	*	*	*
11458527744	*	*	*	*	*	*
11458528256	*	*	*	*	*	*
11458528768	*	*	*	*	*	*
11458529280	*	*	*	*	*	*
11458529792	*	*	*	*	*	*
11458530304	*	*	*	*	*	*
11458530816	*	.	.	.	.	.
11458531328	*	.	.	.	.	.
11458531840	*	.	.	.	.	.
11458532352	*	.	.	.	.	.
11458532864	*	.	.	.	.	.
11458533376	*	.	.	.	.	.
11458533888	*	.	.	.	.	.
11458534400	*	.	.	.	.	.
11458534912	*	.	.	.	.	.
11458535424	*	*	*	*	*	*
11458535936	*	*	*	*	*	*
11458536448	*	*	*	*	*	*
11458536960	*	*	*	*	*	*
11458537472	*	*	*	*	*	*
11458537984	*	*	*	*	*	*
11458538496	*	*	*	*	*	*
11458539008	*	.	.	.	.	.

10979188224	*	*	.	.	.	.
10979188736	*	*	.	.	.	.
10979189248	*	*	.	.	.	.
10979189760	*	*	.	.	.	.
10979190272	*	*	.	.	.	.
10979190784	*	*	.	.	.	.
10979191296	*	*	.	.	.	.
10979191808	*	*	.	.	.	.
10979192320	*	*	.	.	.	.
10979192832	*	*	.	.	.	.
10979193344	*	*	.	.	.	.
10979193856	*	*	.	.	.	.
10979194368	*	*	.	.	.	.
10979194880	*	*	.	.	.	.
10979195392	*	*	.	.	.	.
10979195904	*	*	.	.	.	.
10979196416	*	*	.	.	.	.
10979196928	*	*	.	.	.	.
10979197440	*	*	.	.	.	.
10979197952	*	*	.	.	.	.
10979198464	*	*	.	.	.	.
10979198976	*	*	.	.	.	.
10979199488	*	*	.	.	.	.
10979200000	*	*	.	.	.	.

10979311104	*	*	*	*	*	*

[illegible][illegible]

810114560	*	.	.	.	.	.
810115072	*	.	.	.	.	.
810115584	*	.	.	.	.	.
810116096	*	.	.	.	.	.
810116608	*	.	.	.	.	.
810117120	*	.	.	.	.	.
810117632	*	*	*	.	.	.
810118144	*	*	*	.	.	.

848219648	*	.	.	.	.	.
848220160	*	.	.	.	.	.
848220672	*	.	.	.	.	.
848221184	*	.	.	.	.	.
848221696	*	.	.	.	.	.
848222208	*	.	.	.	.	.
848222720	*	.	.	.	.	.
848223232	*	.	.	.	.	.
848223744	*	.	.	.	.	.
848224256	*	.	.	.	.	.
848224768	*	.	.	.	.	.
848225280	*	.	.	.	.	.
848225792	*	.	.	.	.	.
848226304	*	.	.	.	.	.
848226816	*	.	.	.	.	.
848227328	*	.	.	.	.	.
848227840	*	.	.	.	.	.

11459780096	*	.	.	.	.	.
11459780608	*	.	.	.	.	.
11459781120	*	.	.	.	.	.
11459781632	*	.	.	.	.	.
11459782144	*	.	.	.	.	.
11459782656	*	.	.	.	.	.
11459783168	*	.	.	.	.	.
11459783680	*	.	.	.	.	.
11459784192	*	.	.	.	.	.
11459784704	*	.	.	.	.	.
11459785216	*	.	.	.	.	.
11459785728	*	.	.	.	.	.
11459786240	*	*	*	*	*	*
11459786752	*	*	*	*	*	*
11459787264	*	*	*	*	*	*
11459787776	*	*	*	*	*	*

11459898880	*	.	.	.	.	.
11459899392	*	.	.	.	.	.
11459899904	*	.	.	.	.	.
11459900416	*	.	.	.	.	.
11459900928	*	.	.	.	.	.
11459901440	*	.	.	.	.	.
11459901952	*	.	.	.	.	.
11459902464	*	.	.	.	.	.
11459902976	*	.	.	.	.	.

9163230720	*	.	.	.	.	.	.
9163231232	*	.	.	.	.	.	.
9163231744	*	.	.	.	.	.	.
9163232256	*	.	.	.	.	.	.
9163232768	*	.	.	.	.	.	.
9163233280	*	.	.	.	.	.	.
9163233792	*	.	.	.	.	.	.
9163234304	*	.	.	.	.	.	.
9163234816	*	.	.	.	.	.	.
9163235328	*	.	.	.	.	.	.
9163235840	*	.	.	.	.	.	.
9163236352	*	.	.	.	.	.	.
9163236864	*	.	*	*	*	*	*
9163237376	*	.	*	*	*	*	*
9163237888	*	.	*	*	*	*	*
9163238400	*	.	*	*	*	*	*
9163238912	*	.	.	.	.	.	.
9163239424	*	.	.	.	.	.	.
9163239936	*	.	.	.	.	.	.
9163240448	*	.	.	.	.	.	.
9163240960	*	.	.	.	.	.	.
9163241472	*	.	.	.	.	.	.
9163241984	*	.	.	.	.	.	.
9163242496	*	.	.	.	.	.	.
9163243008	*	.	.	.	.	.	.

11458526720	*	.	.	.	.	.
11458527232	*	*	.	*	*	*
11458527744	*	*	.	*	*	*
11458528256	*	.	*	*	*	*
11458528768	*	*	*	*	*	*
11458529280	*	*	.	.	*	*
11458529792	*	*	*	*	*	*
11458530304	*	*	*	*	*	*
11458530816	*	.	.	.	.	.
11458531328	*	.	.	.	.	.
11458531840	*	.	.	.	.	.
11458532352	*	.	.	.	.	.
11458532864	*	.	.	.	.	.
11458533376	*	.	.	.	.	.
11458533888	*	.	.	.	.	.
11458534400	*	.	.	.	.	.
11458534912	*	.	.	.	.	.
11458535424	*	*	*	*	*	*
11458535936	*	*	*	*	*	*
11458536448	*	*	*	*	*	*
11458536960	*	*	*	*	*	*
11458537472	*	*	*	*	*	*
11458537984	*	*	*	*	*	*
11458538496	*	*	*	*	*	*
11458539008	*	.	.	.	.	.

11458395648	*	.	.	.	.	.
11458396160	*	*	*	*	*	*
11458396672	*	*	*	*	*	*
11458397184	*	*	*	*	*	*
11458397696	*	*	*	*	*	*
11458398208	*	*	*	*	*	*
11458398720	*	*	*	*	*	*
11458399232	*	*	*	*	*	*
11458399744	*	*	*	*	*	*
11458400256	*	*	*	*	*	*
11458400768	*	*	*	*	*	*
11458401280	*	*	*	*	*	*
11458401792	*	*	*	*	*	*
11458402304	*	*	*	*	*	*
11458402816	*	*	*	*	*	*
11458403328	*	*	*	*	*	*
11458403840	*	*	*	*	*	*
11458404352	*	*	*	*	*	*
11458404864	*	*	*	*	*	*
11458405376	*	*	*	*	*	*
11458405888	*	*	*	*	*	*
11458406400	*	*	*	*	*	*
11458406912	*	*	*	*	*	*
11458407424	*	*	*	*	*	*
11458407936	*	.	.	.	.	.

10979188224	*	*	.	.	.	.
10979188736	*	*	.	.	.	.
10979189248	*	*	.	.	.	.
10979189760	*	*	.	.	.	.
10979190272	*	*	.	.	.	.
10979190784	*	*	.	.	.	.
10979191296	*	*	.	.	.	.
10979191808	*	*	.	.	.	.
10979192320	*	*	.	.	.	.
10979192832	*	*	.	.	.	.
10979193344	*	*	.	.	.	.
10979193856	*	*	.	.	.	.
10979194368	*	*	.	.	.	.
10979194880	*	*	.	.	.	.
10979195392	*	*	.	.	.	.
10979195904	*	*	.	.	.	.
10979196416	*	*	.	.	.	.
10979196928	*	*	.	.	.	.
10979197440	*	*	.	.	.	.
10979197952	*	*	.	.	.	.
10979198464	*	*	.	.	.	.
10979198976	*	*	.	.	.	.
10979199488	*	*	.	.	.	.
10979200000	*	*	.	.	.	.

10979311104	*	*	*	*	*	*