RAPID RECOGNITION OF BLACKLISTED FILES AND FRAGMENTS

MICHAEL MCCARRIN BRUCE ALLEN



MANY THANKS TO:

- OSDFCon and Basis
- Bruce Allen
- Scott Young
- Joel Young
- Simson Garfinkel

All of whom have helped with this project immensely.

PROBLEM STATEMENT: GIVEN A LIST OF INTERESTING FILES, FIND ALL DEVICES THAT CONTAIN AT LEAST ONE.



A COMMON SOLUTION: HASH EVERYTHING. COMPARE HASHES.

- 1. Keep a database of the hashes of your interesting files.
- 2. Extract files from each new device you see:
 - Overt + undeleted + carved
- 3. Hash extracted files. Look for matches against the database.
- 4. Solved!



MATCH?

THERE ARE MANY COMMON SCENARIOS WHERE FILE HASHING DOESN'T WORK.

- Comparing cryptographic hashes only finds exact matches.
- Flip a bit, the hash changes completely.
- Everybody knows this already.
- Usually it comes up when people are worrying about mildly clever adversaries.
- But... there are many more mundane reasons to worry.

EXAMPLE 1: EXCEL CHANGES FILE CONTENT WHEN YOU SAVE

"GET NEW MD5"

How to get a new MD5 for your Excel file:

- Open your file.
- Click save.
- Complete!

•	••	se	ecret_workbo	ook.xlsx				
9		🖶 🔏 🖻		rch in Shee	t		\square	>>
cali	bri (Body) 🔹 1	12 * B	I ∐ ≣		¢Ao	\$ %	,	≫
1	A Home Lay	yout Table	es Charts	Smar	tArt	>>	~ ¢	ΕŦ
E	dit	Font	Alignmer	nt Nu	mber	F	ormat	
Ê	🖣 🛫 🛛 Calibri (Bo	ody) 🔻 12	• 三 ,	Genera	•			Ъ
	B I	U 💩 - 1		I	% >	Condition	nal ou	2
Pa		; 80	Align		/0 /	Formatti		_
1	A	B			ſ)	E	•
1	Common Poisons	Cost	Pro	-	Con	,	-	
2	Cyanide	\$ 440.	00 effective		cliché			
3	Arsenic	\$ 2,234.0	00 classic		costly			
4	Fruitcake	\$ 11.			too cruel			
5	Hemlock	\$ 78.		ated.	Hard to fin	d		
6	Rat Poison	\$ 99.			none			
7	RAID	\$ 10.0			Probably w			
8	Nitric Acid	\$ 884.	00 Apply topic	ally	kind of che	ating		
9 10								
11								
12	Common Explosive	Cost	Pro		Con			
13	Firecrackers	\$ 11.0			hurt my ea	rs		
14	sparklers		00 sparkly		not that fu			
15	Roman candles		00 really fun		none			
16	Nitro glycerin	\$ 1,000.0		ve	hard to car	ry		
17	Dynamite	\$ 1,200.0			too amusir	-		
18	Nuclear Warheads	+//		-	too thorou	-		
19	Popcorn		00 delicious		too delicio			
20	cherry bombs	\$ 10.			•	d on toilets		
21 22	grenades	\$ 4,546.0	00 exciting		error pron	e		
22								
24								
25								
26								
27								
28								
29								
30								
31								
32 33								
		Poisons	Explosives	s				
	Normal Vie	w Select d	estination and	press ENTER	or choose	Paste	1.1	
								11

HERE'S THE HEX VIEW OF THE CHANGES

	•									sw.he	x (~/Google Drive/NPS	S/gather	rings/OSDF	FCon)	VIM3							
0		+2791 1 0000ae70:											+2791 1 0000ae70									0000 2100 ede7 PK.
	2793	0000									a.r.W! <q [a,0.jK</q 		0000ae80 0000ae90									a.r.W! <q [a,0.jK</q
	2795	0000 D	EF		KE		A	VI		G	0+i+q	2795	0000aea0	Ał	-	E K		A	V I			o+i+q
	2796	0000aec0:	bc64	32fe	83a4	bf01	8888	****	0300	5845	H.8	2796 2797	0000aeb0 0000aec0:	bc64	32fe	83a4	bf01	0000	****	0300	5845	H.8 .d2PK
	2798	0000aed0:	0304	1400	0600	0800	6666	2100	e016	1fa4		2798	0000aed0:	0304	1400	0600	0800	0000	2100	49e5	41fc	
	2799 2800	0000acc0: 0000acf0:									rops/core.xml	2799 2800	0000acc0: 0000acf0:									rops/core.xml
		0000af00: 0000af10:									.(0000af00: 0000af10:									.(
	2803	0000af20:	0000	0000	0000	0000	0000	0000	0000	0000		2803	0000af20:	0000	0000	0000	0000	0000	0000	0000	0000	
		0000af30: 0000af40:											0000af30: 0000af40:									
		+ 5 li	ines:	8000a f	50: 0	0000 0	0000 0	0000 0	000	0000	0000 0000 0000	+ 2806	+ 5 li	ines:	0000af	50: 0	0000	0000	0000	0000	0000	0000 0000 0000
	2811	0000afa0: 0000afb0:										2811 2812	0000afa0: 0000afb0:									
		0000afc0: 0000afd0:											0000afc0: 0000afd0:									
	2815	0000afe0:	0000	0000	0000	6666	6666	6666	0000	9999		2815	0000afe0:	0000	0000	0000	0000	0000	0000	0000	0000	
	2816 2817	0000aff0:									N.0H	2816 2817	0000aff0: 0000b000:				_					QK.0
	2818	00006010:									C.{.8XI*JH	2818	0000b010:	_								C.{u*@e0'
	2819 2820	0000b020: 0000b030:		59f6 81a3							Y6.}{M wf]T.}.	2819 2820	0000b020: 0000b030:		72b7 31f7							.Br4\$.n .1s/).{UG.`
	2821 2822	0000b040: 0000b050:		d125 b728							u%"I."RoJ Z(r.iFC	2821 2822	0000b040: 0000b050:		7489 3d8a							.lt.H40
	2823	00005060:	babc	28b8	albc	b1f0	6c1b	03d6	4b70	5120	(lKpQ	2823	00005060:	aeaf	0a6e	286f	2cbc	d8c6	80f5	125c	1448	n(o,\.H
	2824 2825	0000b070: 0000b080:		b929 d78d							iG.){Clv \$8	2824 2825	0000b070: 0000b080:		6e4a 4d63							.QnJPb Mci0
	2826	00000090:	d2f4	la2b	f04c	30cf	7007	8ccd	4844	07a4	+.L0.pHD	2826	00006090:	34bd	c50a	3c13	cc33	dc01	6333	12d1	1129	4<3c3)
	2827 2828	0000b0a0: 0000b0b0:		d27c 5e0f							.#. ;L. .0^.V.?.ze.TM.	2827 2828	0000b0a0: 0000b0b0:		d783					f60e f407		4c.A
	2829 2830	0000b0c0: 0000b0d0:		77ca 8c90							w .Gm	2829 2830	0000b0c0: 0000b0d0:		9db2 23e4							:wr4.m.
	2831	0000b0e0:	0ea8	2a04	a7dc	02f3	8dad	9692	6f19	d405	*	2831	0000b0e0:	0 <mark>3aa</mark>	0ac1	29b7	c07c	63ab	a5e4	3b06)[c;.u.
	2832 2833	0000b0f0: 0000b100:		bafb a0f5							e8.Zl	2832 2833	0000b0f0: 0000b100:		ee7e 687d						67db acf3	'~5s~.Ng. h}".q
	2834	0000b110:		ae16							? <r2.i.g7.4.< td=""><td>2834</td><td>0000b110:</td><td>c7a7</td><td>d502</td><td>5559</td><td>4a66</td><td>3149</td><td>e3ec</td><td>6e95</td><td>6674</td><td>UYJflIn.ft</td></r2.i.g7.4.<>	2834	0000b110:	c7a7	d502	5559	4a66	3149	e3ec	6e95	6674	UYJflIn.ft
	2835 2836	0000b120: 0000b130:	9398	bdca 5342	28b9	9610	8f80	7843 aac0	411d 675f	a2fa		2835 2836	0000b120:	1273	4a32	4737 4aa6	c413	a02a	6728 f0c5	97a8	7e00	6.7.G7.Wo(.sJ2J*~
	2837 2838	0000b140: 0000b150:	0100	00ff	ff03	0050 e5ba	4b03	8414	0006 005f	0008 0300	PK	2837 2838	0000b140:	0 <mark>000</mark>	ffff 2100	0300 95e5	504b	0304 a701	1400	0600	0880	
	2839	00005160:	0010	0008	0164	6f63	5072	6f70	732f	6170	docProps/ap	2839	0000b160:	1000	0801	646f	6350	726f	7073	2f61	7070	docProps/app
	2840 2841	00005170: 00005180:	782e 0000	786d 0000	6c20 0000	a204 0000	8128 0000	a000 0000	0100 0000	0000	p.xml(2840 2841	00005170: 00005180:	2e78 0000	6d6c 0000	20a2 0000	8481 8888	28a0 0000	0001	0000	0000	.xnl(.
	2042	00001100		0000	0000	0000		0000				2842	0000b190: 0000b1a0:		0000	0000				0000		
SHL	FΤ	ED	FR	O	M		gaaa	0000	0000	0000		2843 2844	0000b1b0:									
							8888 8888	0000	0000	0000	· · · · · · · · · · · · · · · · · · ·	2845 2846	0000b1c0: 0000b1d0:				0000			0000		
ERE	T	ΟΤ	HE	E	N	D	800 6	0000 0	000		0000 6290 0000	+ 2847	+ 3 li	ines:	0000b1	le0: (8000	0000	0000	0000	0000	0000 0000
								0000 0000				2850 2851	00005210: 00005220:									
	(~	1.5	K)_					0000				2852 2853	00005230: 00005240:							0000		
							8000	0000	0000	0000		2854	0000b250:	0000	0000		0000	0000	0000	0000	0000	
	2855 2856	0000b260: 0000b270:	0000	0000	0000	0000	0000	0000	0000 009c	0000 93c1		2855 2856	0000b260: 0000b270:	0000	0000	0000	0000	0000	0000	0000 9c93	0000 c16e	
	2857	0000b280:	6edb	300c	86ef	03fa	8e86	ee8d	dca6	1886	n.0	2857	0000b280:	db30	0c86	ef03	falle	86ee	8ddc	a618	8649	.0
	2858	00000290:	4076	5184	107a	5801	0049	0033	27d3	0150	@VQzXI.3'P	2858	0000b290:	7651	a41d	/a58	D100	49bb	3327	d3b1	5059	VQZXI.3'PY

H

EXAMPLE 2: POWERPOINT EXHIBITS SIMILAR BEHAVIOR

"GET NEW MD5"

- Not as many changes, but one byte is enough.
- Note that the user content is 100% unchanged!

•••	dfrws_befriend.pptx		1
ଂ 🛅 🛒	E 😹 🍐 🔍 Search in Presentation	»	
	$\bullet \bullet B I U S ABC \equiv \Xi$		
A Home	Themes Tables Charts SmartArt	» ∧ ☆•	
Slides	Font	:	
¶ ■ ·	• • A• A• A	= v ¹ / ₃ =	
New Slide	$\begin{bmatrix} \mathbf{B} & I & \underline{\mathbf{U}} & \mathbf{ABG} & \mathbf{A^2} & \mathbf{A_2} & \mathbf{A^V_{\bullet \bullet}} & \mathbf{Aa \bullet} & \underline{\mathbf{A}} & \mathbf{\bullet} & \mathbf{A\bullet} & \mathbf{\bullet} & \bullet$	EE	

Visualizing bulk_extractor Results with Gephi and BEfriend

Michael McCarrin The Naval Postgraduate School

0.0.0

Click to add notes

□ BB □ Normal View

45% -©

 \geq

DIFF OF POWERPOINT HEX DUMPS BEFORE AND AFTER SAVING:

• • •			be_1.hex (~/Google Drive/NP	PS/gatherings/OSDFCon) - VIM3	
+	1 +77421	lines: 00000000: 504b 0304 1400	0 0600 0800 0000 2100 ab70 P	+ 1 +77421 lines: 00000000: 504b 0304 1400 0600 0800 0000 2100 ab70	P m
		6e74 68ef 9393 f43a 1bf0 0e20		77422 0012e6d0: 6e74 68ef 9393 f43a 1bf0 0e20 2df8 de80 nth	
		6ed7 913d d645 e225 6de3 17c7		77423 0012e6e0: 6ed7 913d d645 e225 6de3 17c7 0ecf 23d5 n=.E.%m#	
		addc 13b2 8fd2 a775 6312 a23f		77424 0012e6f0: addc 13b2 8fd2 a775 6312 a23f 8fb6 578cuc?W	
		e613 142a dc68 e195 c657 161a		77425 0012e700: e613 142a dc68 e195 c657 161a a64d f113*.hWM.	
		00a0 81d0 3f7b df36 fde7 f900		77426 0012e710: 00a0 81d0 3f7b df36 fde7 f900 0000 ffff?{.6	
774		0300 504b 0304 1400 0600 0800 0390 fab4 6601 0000 5902 0000		77427 0012e720: 0300 504b 0304 1400 0600 0800 0000 2100PK	•
		646f 6350 726f 7073 2f63 6f72		77429 0012e740: 646f 6350 726f 7073 2f63 6f72 652e 786d docProps/core.x	m
		6c20 a204 0128 a000 0100 0000		77430 0012e750: 6c20 a204 0128 a000 0100 0000 0000 0000 l(
		0000 0000 0000 0000 0000 0000		77431 0012e760: 0000 0000 0000 0000 0000 0000 0000	
		0000 0000 0000 0000 0000 0000		77432 0012e770: 0000 0000 0000 0000 0000 0000 0000	
774	33 0012e780:	0000 0000 0000 0000 0000 0000	0000 0000	77433 0012e780: 0000 0000 0000 0000 0000 0000 0000	
		0000 0000 0000 0000 0000 0000		77434 0012e790: 0000 0000 0000 0000 0000 0000 0000	
		ines: 0012e7a0: 0000 0000 0000 0		+ 77435 + 5 lines: 0012e7a0: 0000 0000 0000 0000 0000 0000 0000	• •
		0000 0000 0000 0000 0000 0000		77448 0012e7f0: 0000 0000 0000 0000 0000 0000 0000	
		0000 0000 0000 0000 0000		77441 0012e800: 0000 0000 0000 0000 0000 0000 0000	
		0000 0000 0000 0000 0000 0000		77442 0012e810: 0000 0000 0000 0000 0000 0000 0000	
		0000 0000 0000 0000 0000 0000		77443 0012e820: 0000 0000 0000 0000 0000 0000 0000	
774		0000 0000 0000 0000 0000 0000		77445 0012e840: 0000 0000 0000 0000 0000 0000 0000	
774		0000 0000 0000 0000 006c 924b		77446 0012e850: 0000 0000 0000 0000 006c 925f 4fc2 3014l. 0.0	
774		84ef 48fc 07cb f7d4 49a1 3ca2		77447 0012e860: c5df 4dfc 0e4d df47 3708 4a96 3112 547cMM.G7.J.1.T	
774		854a 08ca 435c 90bl b78d 85e3		77448 0012e870: 91c4 28fe 892f a6b6 17d6 d075 4d7b 61e0(/uM{a	
774	49 0012e880:	f9f5 3869 09ad e068 cdf8 f3ec	acb3 8b558ihU	77449 0012e880: a7b7 1b38 31fa d89c d35f cf3d b7d9 645781=d	W
774	50 0012e890:	a5c9 129c 57b5 c969 3288 2901		77450 0012e890: 6ab2 05e7 5565 c634 e9c5 9480 1195 5466 jUe.4T	
774		Sca7 4fd3 7174 4689 476e 24d7		77451 0012e8a0: 35a6 4f8b 5934 a2c4 2337 92eb cac0 98ee 5.0.Y4#7	
774		c1d3 8be2 f020 1336 15b5 837b		77452 0012e8b0: c1d3 497e 7e96 099b 8aca c1bd ab2c 3854	
774		c093 4032 3e15 36a7 25a2 4d19		77453 0012e8c0: e049 2019 9f0a 3ba6 05a2 4d19 f3a2 8092 .I;M	
774		fb41 7098 20ce 6a57 710c 4737		77454 0012e8d0: fb5e 7098 202e 2b57 720c 47b7 6296 8b35 .^p+Wr.G.b	
774		3e07 368c e313 5601 72c9 91b3 48b7 4829 7aa4 5d38 dd01 a460		77455 0012e8e0: 5f01 ebc7 f105 2b01 b9e4 c859 038c 6c47+Yl 77456 0012e8f0: a447 a414 1dd2 6e9c 6e01 5230 d050 8241 .Gn.n.R0.P.	
774		9e25 8384 fd7a 115c e5ff bdd0		77456 0012e900: cf92 5ec2 7ebc 08ae f4ff 5e68 9513 67a9	
774		elda 8699 b671 77d9 526c c4de			
774		364d 3368 8eba 1821 7fc2 5e27		77459 0012e920: ebba eed5 8336 46c8 9fb0 d7f9 dd63 3b6a6Fc;	
774		9132 6d57 0268 9149 91a2 420d		77460 0012e930: a44c d395 009a 6752 a4a8 5043 feac fc86 .LgRPC	
774	61 0012e940:	aed5 5768 947c 2cf4 e73b acd0	7181 b523Wh. ,;q#	77461 0012e940: 6bf5 191a 251f 1bbd 7e87 1d3a 2eb0 72e4 k%~:r	
774	62 0012e950:	Øfe0 171a 3d69 1496 e416 6ca9 -	4868 9a5c=il.Hh.∖	77462 0012e950: 01fc 46a3 27b5 c282 dc82 2d14 094d 93e9F.'M.	
774			3809 9b99#3.C5.8	77463 0012e960: cdd2 2930 3263 1da4 a95b 738f f3b0 99a5)02c[s	<u>.</u>
774			d4ba 1d2c)b.D.Ag,	77464 0012e970: 0239 dde7 7325 0a0e 3a63 7fa5 c6ed 60ab .9s%:c	- I
774			ab2d 8a84 U"1zH	77465 0012e980: 9aa5 e649 ebe8 8e21 58db 435a 1e51 248cI!X.CZ.Q\$	
774			8b61 9c8cM.?tL.a.	77466 0012e990: 961e 8af8 965e 0657 d78b 19cd fb71 328c^.Wq2 77467 0012e9a0: 9238 ea5f 2ee2 7e3a 8cd3 ele8 ad09 f51b .8~:	
774			f8ad 0db5 .\$x. ff03 0050 .(?C	77460 0010-010-0017 055- 5-0- 5017 0000 0055 5500 0050	è.
774		4603 0414 0005 0008 0000 0021		77468 0012e9b0: 9067 0ffc fe0c f917 0000 00ff ff03 0050	I
774		dlee 0300 00b3 2400 0028 0000		77470 0012e9d0: d1ee 0300 00b3 2400 0028 0000 0070 7074\$(pp	
774		2f70 7269 6e74 6572 5365 7474		77471 0012e9e0: 2f70 7269 6e74 6572 5365 7474 696e 6773 /printerSetting	
774		2f70 7269 6e74 6572 5365 7474		77472 0012e9f0: 2f70 7269 6e74 6572 5365 7474 696e 6773 /printerSetting	
774	73 0012ea00:	312e 6269 6ee4 59cd 72da 3010	a6b9 c11b 1.bin.Y.r.0	77473 0012ea00: 312e 6269 6ee4 59cd 72da 3010 a6b9 c11b 1.bin.Y.r.0	
774		f4e6 7207 9184 86b4 e390 a110		77474 0012ea10: f4e6 7207 9184 86b4 e390 a110 a6cc 90c4r	
the second se		nes: 0012ea20: 13a0 333d 6514 5			
779		0070 7074 2f70 7265 7350 726f		77925 00130640: 0070 7074 2f70 7265 7350 726f 7073 2e78 .ppt/presProps.	
779		6d6c 504b 0102 2d00 1400 0600		77926 00130650: 6d6c 504b 0102 2d00 1400 0600 0800 0000 mlPK	
7792		2100 7b21 f91a 9a01 0000 6303		77927 00130660: 2100 7b21 f91a 9a01 0000 6303 0000 1100 !.{!	
		0000 0000 0000 0000 0000 0000 7070 742f 7669 6577 5072 6f70		77928 00130670: 0000 0000 0000 0000 0000 59e5 1200Y 77929 00130680: 7070 742f 7669 6577 5072 6f70 732e 786d ppt/viewProps.x	
779		6c50 4b01 022d 0014 0006 0008		77930 00130690: 6c50 4b01 022d 0014 0006 0008 0000 0021 lPK	
		0003 90fa b466 0100 0059 0200		77931 001306a0: 0070 d90c 9a66 0100 0059 0200 0011 0000 .pfY	
779		0000 0000 0000 0000 0000 0022		77932 001306b0: 0000 0000 0000 0000 0000 0022 e712 0064	d

MD5 (PLAN.PDF) = 0E2CDDFF785730F97C93E087A270250A

M57 PATENTS EXTENSION

My Clever Plan

Jo Smith

1 USE MATH

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

$$\begin{aligned} (x+y)^3 &= (x+y)^2(x+y) \\ &= (x^2+2xy+y^2)(x+y) \\ &= (x^3+2x^2y+xy^2) + (x^2y+2xy^2+y^3) \\ &= x^3+3x^2y+3xy^2+y^3 \end{aligned}$$
(1.1)

Phasellus viverra nulla ut metus varius laoreet. Quisque rutrum. Aenean imperdiet. Etiam ultricies nisi vel augue. Curabitur ullamcorper ultricies

1.1 NOW FOR THE CLEVER BIT

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

$$\mathbf{I} = \begin{bmatrix} A_{11} & A_{21} \\ A_{21} & A_{22} \end{bmatrix}$$
(1.2)

Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem.

MD5 (PLAN.PDF) =)4206496CA24F93A75C79186572E8670

M57 PATENTS EXTENSION

My Clever Plan

Jo Smith

1 USE MATH

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

$$(x + y)^{3} = (x + y)^{2}(x + y)$$

= $(x^{2} + 2xy + y^{2})(x + y)$
= $(x^{3} + 2x^{2}y + xy^{2}) + (x^{2}y + 2xy^{2} + y^{3})$
= $x^{3} + 3x^{2}y + 3xy^{2} + y^{3}$ (1.1)

Phasellus viverra nulla ut metus varius laoreet. Quisque rutrum. Aenean imperdiet. Etiam ultricies nisi vel augue. Curabitur ullamcorper ultricies

1.1 NOW FOR THE CLEVER BIT

Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

$$A = \begin{bmatrix} A_{11} & A_{21} \\ A_{21} & A_{22} \end{bmatrix}$$
(1.2)

1

Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem.

1

EXAMPLE 3: TWO "IDENTICAL" PDFS CREATED BY PDFLATEX

AGAIN, HERE IS THE HEX VIEW.

IF YOU LOOK CLOSELY YOU CAN SEE THE TIME STAMP HAS CHANGED

and the second second

0 0																				100					
0 00009228: 6473 7472 6561 6d0e 656e 6d6f 026e 0a33 dstream.endob 0 00009248: 7563 6572 2628 7664 6556 2633 dstream.endob 0 00009248: 7563 6572 2628 7664 6556 558 2d31 244 ucer (pdfTeX-1.4 0 00009248: 7563 5572 2628 7664 6556 558 2d31 244 ucer (pdfTeX-1.4 0 00009268: 5455 5829 0.21 f 372 6561 7469 6f6 4461 TeX) remationBa 234 000009268: 5455 5829 0.21 f 372 6561 7469 6f6 4.611 f 2.2028 4.33 320 3135 3130 3237 3039 te (p:2015162) 0 00009268: 5465 5829 0.21 f 372 6561 7469 6f6 4461 TeX) remationBa 234 000009268: 5465 5829 0.21 f 372 6561 7469 6f6 4.611 f 2.2028 4.33 320 3135 3130 323 708 399 f 2.208 443a 3230 3135 3130 323 708 399 f 2.208 443a 3230 3135 3130 323 708 395 2.208 443a 3230 3135 3130 323 200 at (p:2015162) 0 00009268: 2156 5415 5829 4675 6666 2672 707 006564 2021 4665 46558 (This is pdfTeX) 2346 00009268: 2216 5657 7273 6066 666 6572 772 30664 6654 652 2083 208 31 3529 (TeX Live C18) 0 00009268: 22156 5415 7273 6066 662632 313 2231 313 519									D pl	an1.h	ex (~/Go	oogle	Drive/N	PS/ga	the	rings/OSD	FCon)	- VIM	2		No. of Concession, name				
0 00009228: 6473 7472 6561 6d0e 656e 6d6f 026e 0a33 dstream.endob 0 00009248: 7563 6572 2628 7664 6556 2633 dstream.endob 0 00009248: 7563 6572 2628 7664 6556 558 2d31 244 ucer (pdfTeX-1.4 0 00009248: 7563 5572 2628 7664 6556 558 2d31 244 ucer (pdfTeX-1.4 0 00009268: 5455 5829 0.21 f 372 6561 7469 6f6 4461 TeX) remationBa 234 000009268: 5455 5829 0.21 f 372 6561 7469 6f6 4.611 f 2.2028 4.33 320 3135 3130 3237 3039 te (p:2015162) 0 00009268: 5465 5829 0.21 f 372 6561 7469 6f6 4461 TeX) remationBa 234 000009268: 5465 5829 0.21 f 372 6561 7469 6f6 4.611 f 2.2028 4.33 320 3135 3130 323 708 399 f 2.208 443a 3230 3135 3130 323 708 399 f 2.208 443a 3230 3135 3130 323 708 395 2.208 443a 3230 3135 3130 323 200 at (p:2015162) 0 00009268: 2156 5415 5829 4675 6666 2672 707 006564 2021 4665 46558 (This is pdfTeX) 2346 00009268: 2216 5657 7273 6066 666 6572 772 30664 6654 652 2083 208 31 3529 (TeX Live C18) 0 00009268: 22156 5415 7273 6066 662632 313 2231 313 519	1	+2338 li	ines:	00000	000:	2550	4446	2d31	2e35	0a25	d0d4 c	5 8 0	a33 %P	+	1	+2338 1	ines:	0000	0000:	2550	4446	20.21	2e35	0a25	d0d4 c5d8 0a33
0 00009230: 3120 3020 6f62 6a0a 3:3: 0a27 5072 6f64 1 0 0j.< 753 657 22028 766 656 6558 2031 2:34 ucer pdfTeX-1.4 2240 00009250: 302. 3136 290a 2f43 7265 6174 6f72 2028 0.16) / Creator 734 00009250: 302. 3136 290a 2f43 7265 6174 6f72 2028 0.16) / Creator 00009270: 7465 2028 445a 3230 3135 3130 327 3039 0.10 2015102.00 734 0000926: 545 5829 002f 4372 656 1746 6f2 2028 0.16) / Creator 00009270: 7465 2028 445a 3230 3135 3130 327 3039 0.10 2015102.00 734 00009270: 7465 2028 443a 323 0313 531 3032 0.10 / Creator 00009290: 6444 6174 6520 2844 3a32 3031 3531 3037 2004 4000 4000 4000 00009200: 543 726 1074 6564 451 0.10 / Creator 00009200: 2150 746 566 773 650 7710 307 2004 4000 100 4017 6000 100 4000 100 100 100 100 100 100 100																									
1 00009240: 7563 6572 2028 7064 6654 6558 2d31 2e34 uccr indfTeX-1.4 2341 00009240: 7563 6572 2028 7064 6654 6558 2d31 2e34 uccr (pdfTeX-1.4 0 0009270: 7465 2028 4237 26551 7469 6f6e 4461 TeX). restions 2343 0009270: 7465 2028 4237 326 517 7469 6f6e 4461 vX). restions 0 0009270: 7465 2028 4233 230 3135 313 0312 022 021 4017 4137 0481.46 2344 00009270: 7465 2028 4235 2308 3135 310 2327 0021 4017 4137 0481.46 0 0009270: 7465 2028 4233 230 3135 313 0312 022 021 4017 4137 0481.46 2344 00009270: 7465 2028 4235 320 3135 313 0327 2000 re (0:2015102 200 2000 re (0:201510 200 200 re (0:201510 200 r																									
2 00009220: 3022 3136 290a 2f43 7265 6174 6f72 2028 0.16) Creator (00009270: 7465 2028 443a 3230 3135 3130 3237 3039 40 (D:201510270) 2343 00009260: 5465 5829 0.2f 4372 565 746 6f6 4461 xX)./creatio 00009270: 7465 2028 443a 3230 3135 3130 3237 3039 40 (D:201510270) 2343 00009270: 7465 2028 443a 3230 3135 3130 3237 3039 40 (D:2015102 00009270: 7465 2028 443a 3230 3135 3130 3237 3039 40 (D:201510270) 2344 00009270: 7465 2028 443a 3230 3135 3130 3237 3039 40 (D:2015102 00009270: 7465 2028 443a 3230 3135 3130 3237 3039 40 (D:2015102 00009270: 7465 2028 443a 3230 3135 3130 3237 3039 40 (D:2015102 00009270: 7465 2028 443a 3230 3135 3130 3237 3039 40 (D:2015102 00009270: 7465 2028 443a 3230 3135 3130 3237 3039 40 (D:2015102 00009270: 7465 2028 4463 657 273 3027 290a 70401704 000 00009270: 7455 5445 5824 4657 5666 567 773 506f 5620 322 4136 565 477 4765 2023 438 723 3027 290a 7095745 04 00009270: 7250 5445 5824 4657 5666 5672 777 566 6657 277 566 4654 6574 6576 5677 656 2631 666 6572 /TFEX.Fullbanne 2340 00009270: 3932 3635 2432 2436 2031 243 3135 , Version 3.1415 00009270: 2208 5465 5820 4c69 765 2031 281 3329 (TeX Live 2015) 00009270: 3932 3635 2432 2436 2431 243 3022 3136 3259 (TeX Live 2015) 00009270: 3932 3635 2432 2436 2431 243 3026 3136 9265-2.6-1.40 00009270: 3932 3635 2432 2466 765 2623 381 3329 (TeX Live 2015) 000009270: 3932 3635 2432 2466 765 5627 773 696f fe20 3322 316 313529 (TeX Live 2045) 000099210: 2208 5465 5820 4c69 7655 2032 381 3529 (TeX Live 2045) 00009920: 2407 9666 477 4772 75561 6408 6566 4467 +.endstream.endo 00009910: 626a 0433 3220 3020 6762 5492 3461 542 7655 7273 696f +.endstream.endo 00009910: 626a 0433 3220 3020 6762 5492 5465 773 656 774 657 273 6967 +.endstream.endo 00009910: 7265 0467 4727 2551 6408 455 6120 765 7273 6967 +.endstream.endo 00009910: 7262 0483 3336 0427 4364 658 437 431 748 748 748 748 748 748 748 748 748 748												pdfT	eX-1.4	23											
4 00009270: 7465 2028 443a 3230 3135 3130 3237 3039 .cc (D:2015102) 2344 00009270: 7465 2028 443a 3230 3135 3130 3237 3039 .cc (D:2015102) 5 00002208: 333 334 333 724 333 724 3334 723 3027 2007 40645 401-0400/M0 2346 00009290: 6444 6174 6520 2844 3a32 3031 3531 303; dDate (D:2015102) 7 00003200: 3733 334 333 724 3334 723 3027 2007 40645 401-0400/M0 2346 00009290: 6444 6174 6520 2844 3a32 3031 3531 303; dDate (D:2015102) 7 00003200: 2154 7261 7070 6564 2027 4661 6c7 3568 7.7700//M1 6520 2844 3a32 3031 3531 302; dDate (D:2015102) 0 00003200: 2154 7261 7070 6564 2027 4661 6c7 3568 7.7700//M1 6520 2844 3a32 3031 3531 302; dDate (D:2015102) 0 00003200: 2205 468 6973 2609 7320 7064 6654 6527 7.771 6067 6620 332 3134 3135 , Version 3.1415 0 00003200: 2028 5465 5820 4669 7665 2032 3031 3529 (Trk Live 2015) 2350 000092061; 2228 5465 5820 4c69 7665 2032 3031 3529 (Tek Live 2015) 4 95 Lines: 00009300: 2028 5465 5820 4c69 7665 2032 3031 3529 (Tek Live 2015) 2350 00009300: 2028 5465 6820 4c69 7665 2032 3031 3529 (Tek Live 2015) 0 00009300: 2028 5465 6473 7472 6561 6408 6566 6473 7472 6561 6408 6566 6473 7472 6561 6408 356 6129 7665 7273 6961 90009300: 2028 5465 6820 4659 7665 7273 6961 90009300: 2028 5465 6820 4659 7665 7273 6961 90009920: 5479 7665 2027 5852 6566 6427 4726 765 7273 6961 900099900: 2048 5566 6473 7472 6561 6408 332 666 6120 ref 30 747 1256 6	342	00009250:	302e	3136	290a	2f43	7265	6174	6f72	2028	0.16)	Cre	ator (23	42	00009250:	302e	3136	290a	2f43	7265	6174	6f72	2026	0.16)./Creato
6 000002200: 3438 3117 2d30 3427 3300 7229 0n2f 4665 6410 2346 00002200: 2532 3435 2d30 3427 3300 7229 0n2f 4646 5243 6444 6174 6520 2844 3a32 3031 3531 3032 dDate (D:2015) 0 00009200: 2755 5454 5524 4575 6566 6227 4661 6573 5584 6584 4237 3030 2249 4661 6573 5584 6584 5224 4575 6566 6562 723 6666 6558 (This is pdf 7280 60009202: 2275 5645 5282 4533 4313 , Version 3.1415 2350 00009201: 2363 60002201: 2302 5653 723 6966 6558 (This is pdf 0 00009201: 2285 5455 5282 4665 6528 3233 3333 533 526	343	00009260:	5465	5829	0a2f	4372	6561	7469	6f6e	4461	TeX).	,irea	tionDa	23	43	00009260:	5465	5829	0a2f	4372	6561	7469	6f6e	4461	x)./Creation
6 00000200: 6444 6174 6520 2844 3a32 3031 3531 3032 dDate (D:2015)22 7 00000200: 2750 3034 2730 3027 2900 7044807 2340 00002200: 2740 3034 2730 3027 2900 70002201 2740 00002200: 2750 3244 3322 3031 3531 3032 dDate (D:2015) 000002200: 2755 5445 582e 4675 666c 6572 /PTEX.Fullbanner 2340 00009200: 2720 5665 7273 696f 6627 2747 60009200: 2228 5665 7273 696f 6627 2747 100009200: 2228 5665 7273 696f 6627 2747 100009200: 2228 5655 2243 2230 00009200: 2208 5655 2243 2230 00009200: 2208 5655 2243 2208 2218 00009200: 2208 2218 00009200: 2208 2218 2218 100009200: 2208 2218 <t< th=""><th>344</th><th>00009270:</th><th>7465</th><th>2028</th><th>443a</th><th>3230</th><th>3135</th><th>3130</th><th>3237</th><th>3039</th><th>.e (D</th><th>:2015</th><th>102700</th><th>23</th><th>44</th><th>00009270:</th><th>7465</th><th>2028</th><th>443a</th><th>3230</th><th>3135</th><th>3130</th><th>3237</th><th>3039</th><th>Le (D:2015102)</th></t<>	344	00009270:	7465	2028	443a	3230	3135	3130	3237	3039	.e (D	:2015	102700	23	44	00009270:	7465	2028	443a	3230	3135	3130	3237	3039	Le (D:2015102)
7 800092a0: 2730 3934 3831 372d 3034 2730 3027 2908 7094817-041001 2348 000092a0: 2754 7261 7070 6564 2027 4661 6c73 650a 7778baac 2348 000092a0: 2754 7261 7070 6564 2027 4665 6572 7778baac 2348 000092a0: 2754 5445 5822 4675 6c6c 6261 6c73 650a 7778baac 6c6 7778baac 778bbaac 2348 000092a0: 2759 5445 5822 4675 6c6c 6261 6c6 6572 7778bbaac (This is pdfrex) 2350 000092a0: 2228 5486 6973 2069 7320 7064 6554 773 6967 6c6 773 6967 6c7 6c6 773 7965 6c21 765 723 6967 4c3 6c6 6c6 762<	345													23											
8 00000206: 2154 7261 7070 6564 202f 4661 6C73 658a 7respect / FEX.Fullbanner 0 00000206: 2150 5445 582e 4675 656c 6261 6e6e 6572 /PTEX.Fullbanner 0 00000206: 2028 5468 6973 2069 7320 7064 6554 6558 (This is pdfTeX 0 000009206: 2028 5465 5872 6964 6573 90009206: 2028 5465 7273 696f 620 332e 3134 3135 , Version 3.14 0 00009300: 2028 5465 5820 4c69 7665 7273 696f kp - 95 11es: 00009300: 2028 5465 5820 4c69 7655 7273 696f 6473 772 6561 6473 774 6567 773 696f 6473 772 6561 6473 772 6561 6473 772 6561 6473 772 6561 6473 772 6561 <td< th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></td<>																									
9 000092c0: 2f50 5445 582e 4675 6c6c 6261 6e6e 6572 /PTEX.Fullbanner 2349 000092c0: 2675 5465 582e 4675 6c6c 6261 6e6e 6572 /PTEX.Fullbanner 0 000092d0: 2028 5468 6973 2069 7320 7064 6654 6558 (This is pdfTeX 2350 000092c0: 2028 5468 6973 2069 7320 7064 6654 6558 (This is pdfTeX 0 000092d0: 2028 5465 5820 4c69 7665 2023 32e 3134 3135 y265-2.6-1.40.16 2352 000092c0: 2028 5465 5820 4c69 7665 2032 3031 3529 (TeX Live 2015) 0 00009300: 2028 5465 5820 4c69 7665 2032 3031 3529 (TeX Live 2015) 2353 00009300: 2028 5465 5820 4c69 7665 2032 3031 3529 (TeX Live 2015) 0 00009300: 2028 5465 5820 4c69 7665 2032 3020 6162 6048 332 000 617 468 7365 6120 7665 7273 696f kp + +	347																								
0 0																									
1 000092e0: 2c20 5655 7273 696f 6e20 332e 3134 3135 , Version 3.1415 2 00009210: 2353 0302 23635 2d32 2a36 2d31 2e34 302e 3134 3135 , Version 3.1415 2 00009210: 2265 2d52 2d6 2d31 2e34 302e 3134 3135 , Version 3.1415 2 00009300: 2028 5465 5820 4c69 7665 2032 3031 3529 (Tex Live 2015) 4																									
2 00009216: 3932 3635 2d32 2e36 2d31 2e34 302e 3136 9265-2.6-1.40 3 00009300: 2028 5465 5820 4c69 7665 2032 3031 3529 (Tex Live 2015) 4																									
3 00009300: 2028 5465 5820 4c69 7665 2032 3031 3529 (TeX Live 2015) 2353 00009300: 2028 5465 5820 4c69 7665 2032 3031 3529 (TeX Live 2015) 4																									
4																									
9 00009900: 2b0a 656e 6473 7472 6561 6d0a 656e 6473 7472 6561 6d0a 656e 646f +.endstream.endo 2449 00009900: 2b0a 656e 6473 7472 6561 6d0a 656e 646f +.endstream.endo bj.32 0 obj.< 2450 00009900: 2b0a 6562 6aaa 3.32.0 3220 3626 6626 6aaa 3.32.0 0 obj.< 2450 00009900: 25479 7665 2033 3.50 0a2f 5302 2656 6467 Type /XRef./I 00009930: 7820 5b30 2033 3540 0a2f 526f 3./W_122211./Ro 2450 00009900: 674 2033 3020 3020 3020 3202 3150 0a2f 526f 3./W_122211./Ro 2450 00009900: 3312 2302 3120 3220 3150 0a2f 526 3.1 0.0 R./In 00009900: 3311 2030 2052 0a2f 4343 331 R./In 2450 00009900:																									
0 00009910: 626a 0a33 3220 3020 6f62 6a0a 3c3c 0a2f bj.32 0 obj.< // 2450 000099010: 626a 0a33 3220 3020 6f62 6a0a 3c3c 0a2f bj.32 0 obj.< 1 0000920: 5479 7065 202f 5852 6566 0a2f 496e 6465 Type /XRef./Inde 2451 00009920: 5479 7065 202f 5852 6566 0a2f 496e 6465 Type /XRef./Inde 2 00009940: 330a 2f57 205b 3120 3220 315d 0a2f 526f 3.////////////////////////////////////																									
1 00009920: 5479 7065 202f 5852 6566 0a2f 496e 6465 Type /XRef./Inde 2 0000930: 7820 5b30 2033 335d 0a2f 5369 7a65 2033 x [0 331./Size 3 3 00009940: 330a 2f57 205b 3120 3220 315d 0a2f 526f 3./W 12-2-11./Ro 4 00009960: 6f74 2033 3020 3020 2020 2f49 6e66 6f20 x [0 3./W 12-2-11./Ro 4 00009960: 6f74 2033 3020 3020 3220 315d 3c1 3/A 31 8./L 2453 00009960: 6f74 2033 3020 3c20 4137 31 8./L 11 8./L 12-2-11./L 2455 00009960: 3331 2033 2024 4944 205b 3c20 43./L 12-2-11./L 2455 00009960: 3331 2032 0202 2020 2020 2021 2456 00009960: <th></th>																									
2 00009930: 7820 5b30 2033 335d 0a2f 5369 7a65 2033 x [0 33]./Size 3 3 00009940: 330a 2f57 205b 3120 3220 315d 0a2f 526f 3./W.[1]211./Ro 4 00009950: 6f74 2033 3020 3020 520a 2f49 6e66 6f20 c<30 0 R./Into 2453 00009960: 330a 2f57 205b 3120 3220 315d 0a2f 526f 3./W.[1]2241./Ro 4 00009960: 3331 2030 2052 0a2f 4944 205b 3c3l 3743 31 R./Into 2455 00009960: 3331 2030 2052 0a2f 4444 205b 3c30 4137 31 R./Into 6 00009900: 3137 4345 4845 3444 4534 4534 4534 4534 4234 4246 4442 3731 3631 0A7210C7C349067 6 000099900: 3137 4345 4238																									
3 00009940: 330a 2f57 205b 3120 3220 315d 0a2f 526f 3./W.14=2.11./Ro 2453 00009940: 330a 2f57 205b 3120 3220 315d 0a2f 526f 3./W.14=2.11./Ro 2453 00009950: 6f74 2033 3020 520a 2f49 6e66 6f20 of 30 0 R./Into 2453 00009950: 6f74 2033 3020 520a 2f49 6e66 6f20 of 30 0 R./Into 2453 00009950: 6f74 2033 3020 520a 2f49 6e66 6f20 of 30 0 R./Into 2454 00009950: 3674 2433 343 4334 433 4334 444 205b 3c30 4137 31 0 R./Into 2455 00009960: 3331 2337 4334 444 433 343 4344 433 343 4344 444 243 444 244 4442 244 4442 244 4444 4444 4444 4444 4444 4444																									
4 00009950: 6f74 2033 3020 3020 520a 2f49 6e66 6f20 of 30 0 n./Into 2454 00009950: 6f74 2033 3020 520a 2f49 6e66 6f20 of 30 0 n./Into 2454 00009950: 6f74 2033 3020 520a 2f49 6e66 6f20 of 30 0 n./Into 2454 00009950: 6f74 2033 3020 520a 2f49 6e66 6f20 of 30 0 n./Into 2455 00009950: 6f74 2033 3020 2022 0a2f 4944 205b 3c30 4137 31 0 n./Into 2455 00009960: 3331 2030 2020 20a f494 205b 3c30 4137 31 0 n./Into 2455 00009960: 3331 2032 2454 4033 4337 4333 4434 444 444 4237 3136 3130 423e 2457 00009900: 3641 3739 3231 3043 3743 3344 4																									
5 00009960: 3331 2030 2052 0a2f 4944 205b 3c3l 3743 31 0 R./ID 2455 00009960: 3331 2030 2052 0a2f 4944 205b 3c3l 4137 31 0 R./ID 6 00009970: 4542 3845 3846 3132 3546 3644 4533 4534 EB8E8F125F6DE3E6 2456 00009970: 3932 3130 4337 4333 3439 4436 4645 4344 9210C7C349D6F 7 00009900: 3137 4345 4238 4538 4636 4444 17CEB8E8F125F6DE3E6 2457 00009900: 3041 3739 3231 3043 3743 334 3944 3644 0A79210C7C349D6F 9 00009900: 3650 0a2f 4c65 6e67 7468 2039 3320 2020 >1 /Length 93 2459 000099900: 3654 4242 3731 3631 3042 ECB84ABFDB71610B 00009900: 3e5d 0a2f <t< th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>and the second se</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>and the second sec</th></t<>													and the second se												and the second sec
6 00009970: 4542 3845 3846 3132 3546 3644 4533 4534 EB8E8F125F6DE3E6 2456 00009970: 3932 3130 4337 4333 3439 4436 4645 4342 9210C7C349D6F 7 00009980: 3943 3744 3431 3830 4542 3042 3932 2034 9C7D4180EB0B9> < 2457 00009980: 3834 4142 4644 4237 3136 3130 4232 2031 84ABFDB71610B 8 00009990: 3137 4345 4238 4434 3138 3045 4239 3E69C7D4180EB0B9 2458 00009900: 3041 3739 3231 3043 3743 3344 3944 3644 9210C7C349D6F 9 00009900: 3137 4337 4337 4333 3443 4442 4644 4237 3136 3130 4232 2031 84ABFDB71610B 9 00009900: 3e5d 0a2f 4c55 6e67 7468 2039 3320 2020 2459 000099060:	455	00009960:	3331	2030	2052	0a2f	4944	205b	3c31	3743						00009960:	3331	2030		_			_		31 0 R./ID [<
7 00009980: 3943 3744 3431 3830 4542 3932 2034 9C7D4180EB089 2457 00009980: 3834 4142 4644 4237 3136 3130 4232 2034 84ABFDB71610B 8 00009990: 3137 4345 4238 4538 4631 3235 4636 4444 17CEB8E8F125F6DE 2458 00009990: 3041 3739 3231 3043 3743 3334 3944 3644 84ABFDB71610B 9 00009900: 3453 3639 4337 4434 3138 3045 4239 326907D4180EB0B9 2459 00009900: 3041 3739 3231 3043 3743 3334 3944 3641 8779210C7C349 9 00009900: 3e5d 0a2f 4c65 6e67 7468 2039 3320 2020 2146 90009900: 2020 200a 2f46 696c 7465 7220 2f46 7774 1ateDiade.>>.st 2460 00009900: 6c61 7465 636f 6465 932 <td< th=""><th>456</th><th>00009970:</th><th>4542</th><th>3845</th><th>3846</th><th>3132</th><th>3546</th><th>3644</th><th>4533</th><th>4536</th><th>EB8E8</th><th>F125F</th><th>6DE3E6</th><th></th><th></th><th>00009970:</th><th>3932</th><th>3130</th><th>4337</th><th>4333</th><th>3439</th><th>4436</th><th>4645</th><th>434</th><th>9210C7C349D6FI</th></td<>	456	00009970:	4542	3845	3846	3132	3546	3644	4533	4536	EB8E8	F125F	6DE3E6			00009970:	3932	3130	4337	4333	3439	4436	4645	434	9210C7C349D6FI
8 00009990: 3 137 4345 4238 4538 4631 3235 4636 4445 17CEB8E8F125F6DE 2458 00009900: 3041 3739 3231 3043 3743 3334 3944 364 0A79210C7C349 9 00009900: 3345 3639 4337 4434 3138 3045 4239 3E69C7D4180EB0B9 2459 00009900: 3e5d 0a2f 4c65 6e67 7468 2039 3320 2020 >1./Length 93 2460 00009900: 3e5d 0a2f 4c65 6e67 7468 2039 3320 2020 >1./Length 93 1 00009900: 2020 2020 200a 2f46 696c 7465 7220 2f46	457	00009980:	3943	3744	3431	3830	4542	3042	393e	203	907043	180EB	0B9> <	24	57	00009980:	5834	4142	4644	4237	3136	3130	4236	203	84ABFDB71610B
0000099b0: 3e5d 0a2f 4c65 6e67 7468 2039 3320 2020 >1./Length 93 2460 000099b0: 3e5d 0a2f 4c65 6e67 7468 2039 3320 2020 >1./Length 93 1 000099c0: 2020 200a 2f46 696c 7465 7220 2f46 >1./Length 93 2460 000099b0: 3e5d 0a2f 4c65 6e67 7468 2039 3320 2020 >1./Length 93 2 000099d0: 6c61 7465 4465 636f 6465 0a3e 3e0a 7374 IateDipode.>>.st 2460 000099d0: 6c61 7465 4465 636f 6465 0a3e 3e0a 7374 IateDipode.>>.st 2462 000099d0: 6c61 7465 4465 636f 6465 0a3e 3e0a 7374 IateDipode.>>.st 3 000099e0: 7265 616d 0a78 da15 c9b9 0d80 5010 4341 ream.xP.CA 2463 000099e0: 7265 616d 0a78 da15 c9b9 0d80 5010 4341 ream.xP.CA 4 000099f0: 9bf3 73df 1219 2109 8280 ba68 8302 20a2 s o0z2/ 2465 00009a00: 3e0a 016f 307a 5a2f 80cf 83a3 80a8 a0b6 >o0z2/	458	00009990:	3137	4345	4238	4538	4631	3235	4636	4445	17CEB	8E8F1	25F6DE	24	58	00009990:	3041	3739	3231	3043	3743	3334	3944	364	0A79210C7C349
1 000099c0: 2020 200a 2f46 696c 7465 7220 2f46	459	000099a0:	3345	3639	4337	4434	3138	3045	4230	4239	3E69C	7D418	0EB0B9	24											ECB84ABFDB716
2 000099d0: 6c61 7465 4465 636f 6465 0a3e 3e0a 7374 lateDecode.>>.st 2462 000099d0: 6c61 7465 4465 636f 6465 0a3e 3e0a 7374 lateDecode.>>.st 3 000099e0: 7265 616d 0a78 da15 c9b9 0d80 5010 4341 ream.xP.CA 2463 000099e0: 7265 616d 0a78 da15 c9b9 0d80 5010 4341 ream.xP.CA 4 000099f0: 9bf3 73df 1219 2109 8280 ba65 8302 20a2 .s 2464 000099f0: 9bf3 73df 1219 2109 8280 ba65 8302 20a2 2464 000099f0: 9bf3 73df 1219 2109 8280 ba65 8302 20a2 2465 00009a00: 3e0a 016f 307a 5a2f 80a8 a0b6 o0zZ/ 2465	460	00009960:	3e5d	0a2f	4c65	6e67	7468	2039	3320	2020	>] /Le	ength	93	24	60	000099b0:	3e5d	0a2f	4c65	6e67	7468	2039	3320	202	Length 93
3 000099e0: 7265 616d 0a78 da15 c9b9 0d80 5010 4341 ream.xP.CA 2463 000099e0: 7265 616d 0a78 da15 c9b9 0d80 5010 4341 ream.xP.CA 000099f0: 9bf3 73df 1219 2109 8280 ba65 8302 20a2s!h. 2464 000099f0: 9bf3 73df 1219 2109 8280 ba65 8302 20a2s!h. 5 00009a00: 3e0a 016f 307a 5a2f 80cf 83a3 80a8 a0b6 >o0zZ/	461	000099c0:	2020	2020	200a	2f46	696c	7465	7220	2f46		· rises	cer /F	24	61	000099c0:	2020	2020	200a	2f46	696c	7465	7220	2f/	·/···ter
4 000099f0: 9bf3 73df 1219 2109 8280 ba68 8302 20a2sh 2464 000099f0: 9bf3 73df 1219 2109 8280 ba65 8302 20a2s!h. 5 00009a00: 3e0a 016f 307a 5a2f 80cf 83a3 80a8 a0b6 >o0z2(2465 00009a00: 3e0a 016f 307a 5a2f 80cf 83a3 80a8 a0b6 >o0zZ/														24											
5 00009a00: 3e0a 016f 307a 5a2f 80cf 83a3 80a8 a0b6 >o0z2(2465 00009a00: 3e0a 016f 307a 5a2f 80cf 3a3 80a8 a0b6 >o0zZ/											ream.	×	P.CA	24											
											· · S · · ·	•••••	.h	24											
6 + 6 lines: 00009a10: d249 2d15 efdd b65e 7cf1 e81a bb1b 2925 .I- + 2466 + 6 lines: 00009a10: d249 2#15 efdd b65e 7cf1 e81a bb1b 2925	465	00009a00:	3e0a	016f	307a	5a2f	80cf	83a3	80a8	a0b6	>00	z2/													
	466	+ 6 lin	nes: 0	0009a	10: 0	249 2	2d15 e	efdd b	065e 7	/cf1 e	e81a bb:	1b 29	25 .I-	+ 24	66	+ 6 li	nes: (00009	a10:	d249	2015	efdd	b65e	7cf1	e81a bb1b 2925

FILE ID?

CONCLUSION: MANY APPLICATIONS CHANGE FILE-LAYER CONTENT.

- The point is not that your investigation relies on Excel files or finding PowerPoint presentations.
- The point is: **applications don't care** about forensic integrity.
- The changes above are **transparent** to the user.

COROLLARY: WE MAY BE MISSING EVIDENCE.

Other things you won't find with file hashes:

- Files that are **deleted** and partially overwritten.
- Slightly **edited** files.
- **Corrupted** files in overt space.
- Badly **carved** files.
- Fragments of files in unallocated space.

WORSE: THESE ARE CASES WHERE THE SUSPECT IS NOT EVEN TRYING.

- At most, they require someone to click save or empty the recycling bin.
- The state produced by **default behavior** is much more concerning than any single clever person.
- Many reasons to improve this process, but the most compelling is economic:
 - Solving the problem should be cost less than creating it.

AN ARGUMENT FOR "APPROXIMATE MATCHING" STRATEGIES:

- Not a fancy thing: we often just want to find files with the **exact same** user-level content.
- Fundamentally, the approach is not that different:
 - 1. Cut the object into pieces.
 - 2. Hash the pieces.
 - 3. Count matching hashes.

THIS PROBLEM HAS MANY KNOWN SOLUTIONS.

Numerous sophisticated matching schemes:

- Rabin fingerprinting, ssdeep, sdhash, frag_find, sector hashing...
- Lots of good stuff—we try to build on it.
- A skilled examiner could find everything we mentioned.
- Many groups have in-house solutions.
- Why write a new tool?

REASONS FOR A NEW TOOL

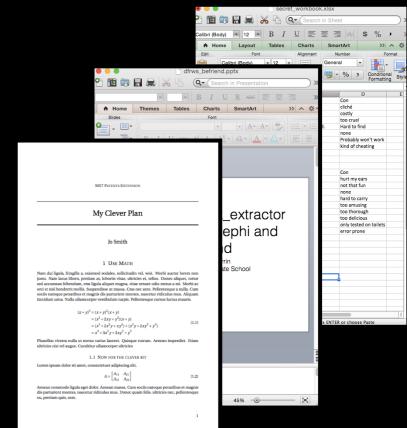
- Nothing on the previous slide will change the economic problem.
- 2. Make already developed techniques more available.
- 3. Getting it right is harder than it first seems.
 - In particular, the feature selection problem has not been solved.

OUR GOALS: TRIVIAL, SCALABLE, COMPREHENSIBLE.

- **Trivial**: It has to be easier to discover targets than it is to obscure them.
- Scalable: Should be able to search for millions of files at once.
- **Comprehensible**: operation of tool and interpretation of results must be intuitive.

SECTORSCOPE DEMO

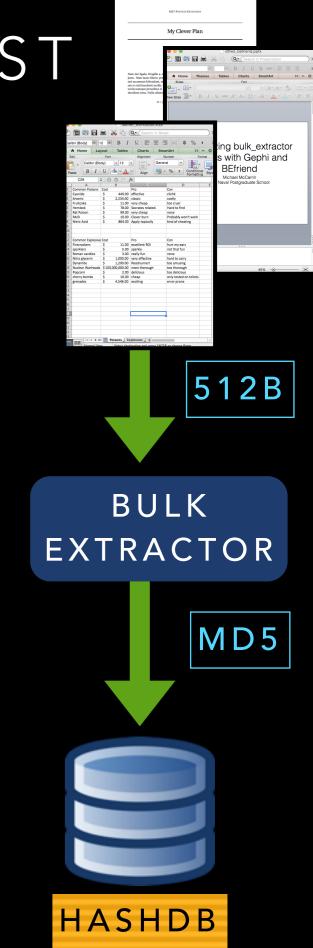
- Target: the 3 files shown above.
- Media: a modified disk image from the m57 patents scenario (exFAT).
 - Files were added to a subfolder on the image then deleted.
 - Subfolder was deleted then replaced so it is not trivially easy to recover through Autopsy / TSK.





STEP 1: CREATE A BLACKLIST

- We store our blacklist in hashdb: a fast, lightweight key-value store we designed for this project.
- Blacklist files are hashed in 512-byte chunks and imported into the database using the hashdb bulk_extractor scanner.
- At the moment, this requires a command line.



STEP 2: SCAN MEDIA

- Could do this at the command line...
- Let's use Autopsy.
- Install SectorScope and the SectorScope plugin.
- Add your disk image to the case.

Ingest Modules	
 Recent Activity Hash Lookup File Type Identification Embedded File Extractor Exif Parser Keyword Search Email Parser Extension Mismatch Detector E01 Verifier Android Analyzer Interesting Files Identifier PhotoRec Carver 	Path to block hash blacklist database: C:\Users\student\data\govdoc_partial_p
NPS-SectorScope	
Process Unallocated Space	Find Blacklist content using a block hash
Start Close	

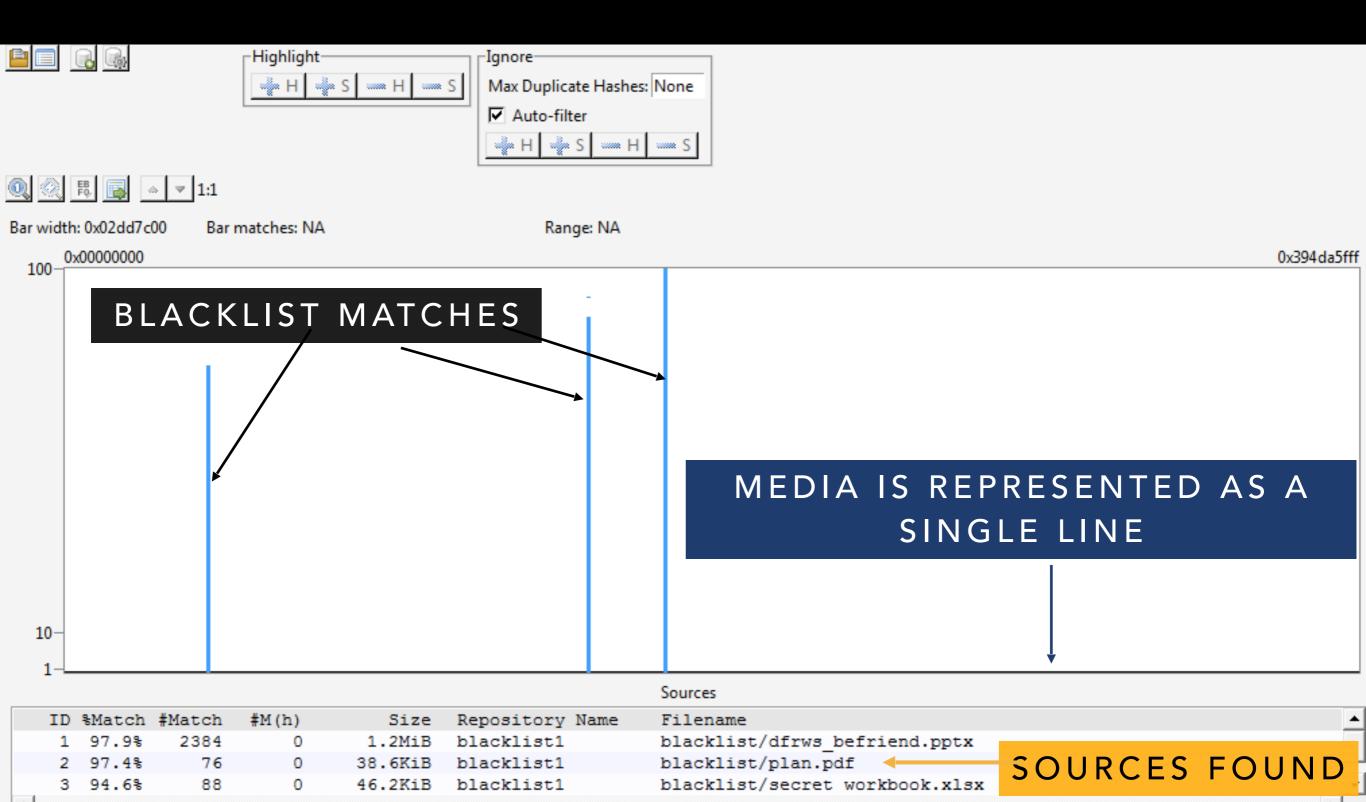
• Run SectorScope ingest module.

STEP 3: ANALYZE THE RESULTS.

Open SectorScope from the Reports listing:

😹 osdfcon_1 - Autopsy 3.1.3					
File View Tools Window Help					
💊 Close Case 🕂 Add Data Source 📗 Ger	nerate Report		<u> </u>	Keyword Lists	Q- Keyword Search
€ →	Directory Listing				
Data Sources	Table Thumbnail				1 Results
vol1 (Unallocated: 0-32255)	Source Module Name	Report Name	Created Time	Report File Path	
vol2 (NTFS / exFAT (0x07): 63-1537 vol3 (Unallocated: 30025485-39218		jo-2009-12-10.E01	2015-10-28 01:40:30 PDT	C:\Users\student\autopsy\osdf	con_1\ModuleOutput\NPS-Sector
 Views Results Extracted Content Keyword Hits Single Literal Keyword Search (0) Single Regular Expression Search (0) 	4		111		
	Hex Strings Metadata	a Results Text Me	dia		
	In the state of th				
	•		111		•

RESULTS FROM OUR 3 FILE BLACKLIST.



PAN AND ZOOM TO NAVIGATE THE MEDIA.

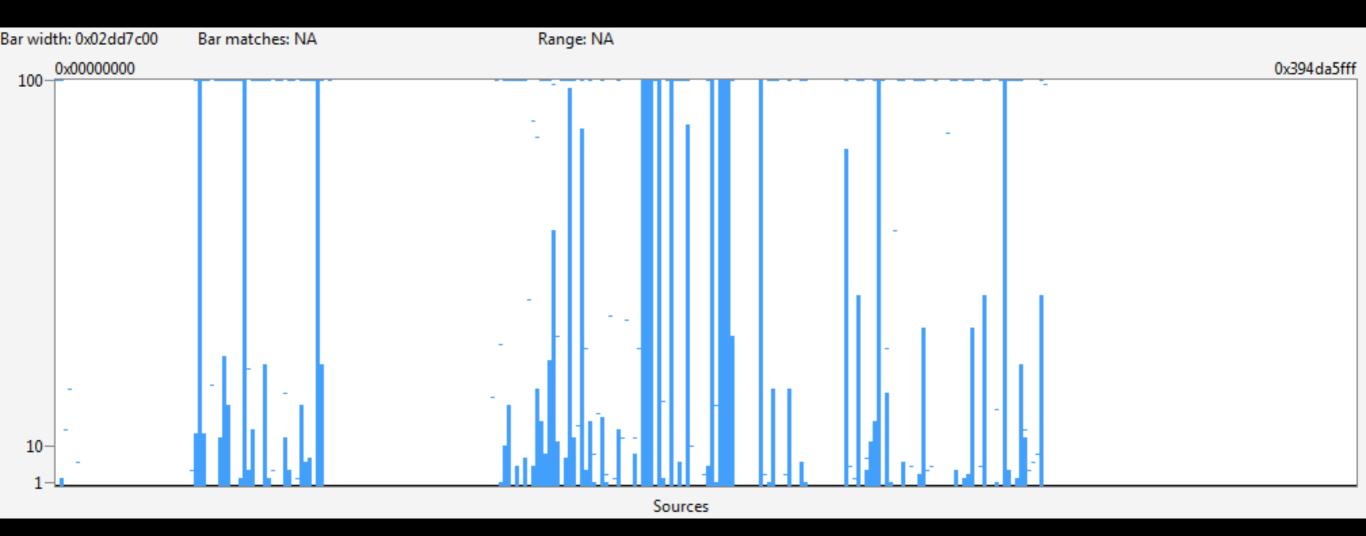
- The list is sorted by percent of file found.
- Highlight a file to see where it is.
- Ignore it to get it off the screen.
- Select a range to see which sources are there.
- Adjust the resolution.
- Open a hex-dump of the data.

LET'S LOOK AT A NON-TRIVIAL EXAMPLE.

THE SCAN RUNS BULK_EXTRACTOR'S HASHDB MODULE TO QUERY THE BLACKLIST.

- Scanning took 109 seconds to scan against 20,772,713 hashes
- Lenovo Thinkpad with 8G of RAM, and a Dual Core i7-5600U CPU (2.6 GHz)
- You can beat this speed with faster hardware
- Compare to 99 seconds to scan against 2,607 hashes: a factor of a thousand takes 10 seconds longer.

THINGS GET MORE COMPLICATED WITH 20 MILLION HASHES.

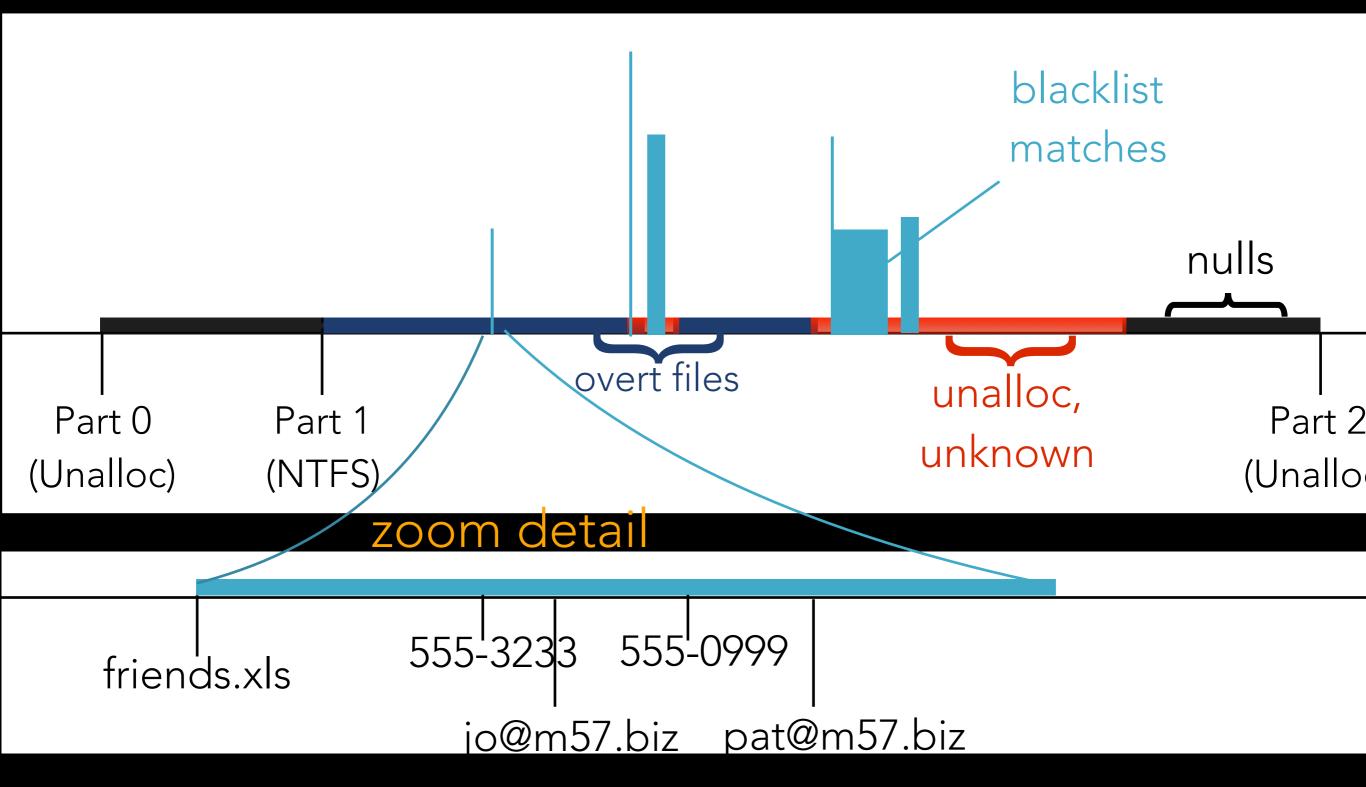


- Added from govdocs—not all high entropy.
- Need to use noise reduction to filter out false positives.

NOISE REDUCTION IS TRICKY

- Down at the level of a 512-byte block, it's not really clear what a "match" tells us.
- Some blocks are extremely rare. (2⁴⁰⁹⁶ is a lot of possibilities).
- Some blocks show up all over the place.
- We use an algorithm published in a recent DFRWS paper: Garfinkel, S. L., & McCarrin, M. (2015). Hash-based carving: Searching media for complete files and file fragments with sector hashing and hashdb. Digital Investigation, 14, S95-S105.

FUTURE WORK: ANNOTATE WITH TSK AND BULK_EXTRACTOR DATA



YOU NEED TO KNOW WHAT YOU DON'T KNOW.

- Few forensics tools will tell you this.
- How much of the image contains data that you know nothing about at all?
- Our end goal is to bring available tools together to map out every sector.

Questions?

Contact: Michael McCarrin mrmccarr@nps.edu

Bruce Allen bdallen@nps.edu

SectorScope on GitHub: https://github.com/NPS-DEEP/NPS-SectorScope