



Graphic Content Ahead: Towards Automated Scalable Analysis of Graphical Images Embedded In Malware

Alex Long, Joshua Saxe, Robert Gove Invincea Labs

8/5/2015

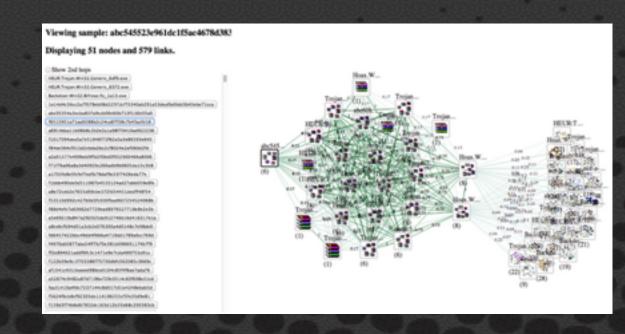
invincea^m





1. The Status Quo of Malware Analysis 2. Hard Problems The Industry is Dealing With 3. Our Approach 4. Two Research Experiments 1. Detecting and Visualizing Image-

Sharing Relationships (Live Demo)



2. Automatically Classifying Images by Their Semantics

Tabura, bena'alda Mada yay	abbe flash	
🕥 alaan_kon/ativina.pg		D 🖻 🖥 🖉 🖸 🔘 🖓 📷 ·
alana_tons/addrinal.pg		8 -10 0 0 -100
nitera (constige tile icon.pag	jpy file fees	õ (h 🔿 👩 🕻 🧈 😨
Section (mail place land page		🔽 🗐 (문 vm 🕑 한 는 📰
advare_tress/advare.pag		
alane, inc./sintex installer pag		≥ ∜ 0 4 ∰b₀0 ĭ
alan, kau/dalan kulallari.pg	vindres installer	
alma, tou, thin intailet py		0
and many terms / stations installerst page		/ (A () () () () () () () () ()
2 album_tona/didon sebeck ion.pg		
The second se		A 12 W 164 05 Y 11 A 116 Y 104 PT 169 163





Status Quo of Malware Analysis

Malware analysis treats malware as just a set of instructions

	Bet +				
A	***SHEH=7				
	/ 1 1 1 1 1 1 1 1 1 1				
and Dimension	D Dearts M Departs N	Names window Manufactors window Mr. Drings window			
text 00421614 text 00421617	lee	edx. [ebptvar_C]			
text 00421617		ecx. [edx]			
text 00421610	mou line	[ebp*ver_4], ecx			
	jep	short loc_0_42163E			
_text:0042161E	-				
_text 0042161E	The A LOUGH	CONT. VIEL, and & approximately	Choose function to jump to	La alio	6 X
_text:0042161E		: CODE AMER : 800_0_421000 483			_
CRUE COMPTEND	lea	eax, [ebp*var_0]	Function name	Segment	
text:00421621	push	eax	No.0 0 42135C	.101	004.
_text 00421622	call	@TRutoArgsDese@GetArgsSxqv_8 TAutoArgsBese GetA	N 16 0 421180	text.	0042
text:00421627	pop	+EX	18 alt 0.42118C	text	0042
_text 00421628	BOU	edx, eex	N 948 0.4211FB	.text	0042
*_text:00421629	807	ecx. ecx	an and 0 421300	Mail I	104.
text 0042162C	800	eax. [ebptvar_4]	1 sub. 0.421340	. host	004;
*_text:0042162F	cell	sub_0_4201E0	1 u.b. 0.4214AD	_box	0044
text 00421634	les	edx, [ebp*var_8]	1 web 0.421418	_boxt	0042
text:00421637	push	edx	No. of the second		-
text 00421638	call	oub_0_415080	No. 0. 42147C	. Most	0042
*_text:00421630	pop	ecx	sub 0.421700	.see	0042
_text 0042163E	4		1 ub 0.421908	304	0042
_text:0042163E	lec_0_42163E:	: CODE XREF: sub_0_421SC0+SCTj	The operators of GLD & GLD &)	_ soc	0042
" _text:0042163E	BOU	ecx, [ebp*var_*]	The set of AzIAzo	.tori	0042
text:00921641	add	ecx, 130h	N GE 0 42LAID	_ NORT	0042
text 00421647	push	ecx	18 Std. 0.421A74		004.
* _text:00921648	leo	eax. [ebp*ver_10]	1 140 0 42180C	_Mol	0042
* _text 00421648	push	esx .	18 sat. 0.421854	_host	0042
* _text:0042164C	cell	sub_0_415050	18 N.D. 0.421804	_text	0042
text 00421651	bbe	esp, B	3 s.e. 0.4218CD		0042
* _text:00421654	leo	edx. [ebp+var_10]	18 sub.0.421010	_bost	0042
* _text:00921657	push	edx		.text	
* _text:00421658	lea	ecx. [ebp=sar_8]	8 s.e. 0.421004	_boxt	0042
* _text:00421658	push	ecx	38 sub_0_421034	_text	0042
* text 0042165C	cell	sub_0_415068	No. 6 4 421040	. sevil	me:
* _text 00421661	edd	esp. 8			
* _text:00421664	test	al. al	OK Cantal Search	100	
text 00421666	jma:	short loc_0_42161E		A Designation of the local division of the l	
			Line 1993 of 1989		

Analysis typically consists of analyzing the disassembled code and/or observing the malware's runtime behavior







Vincea Problems Facing Analysts Today



Malware could be packed or use VM detection tactics

Manual analysis of each sample is intractable given huge numbers of polymorphic variants

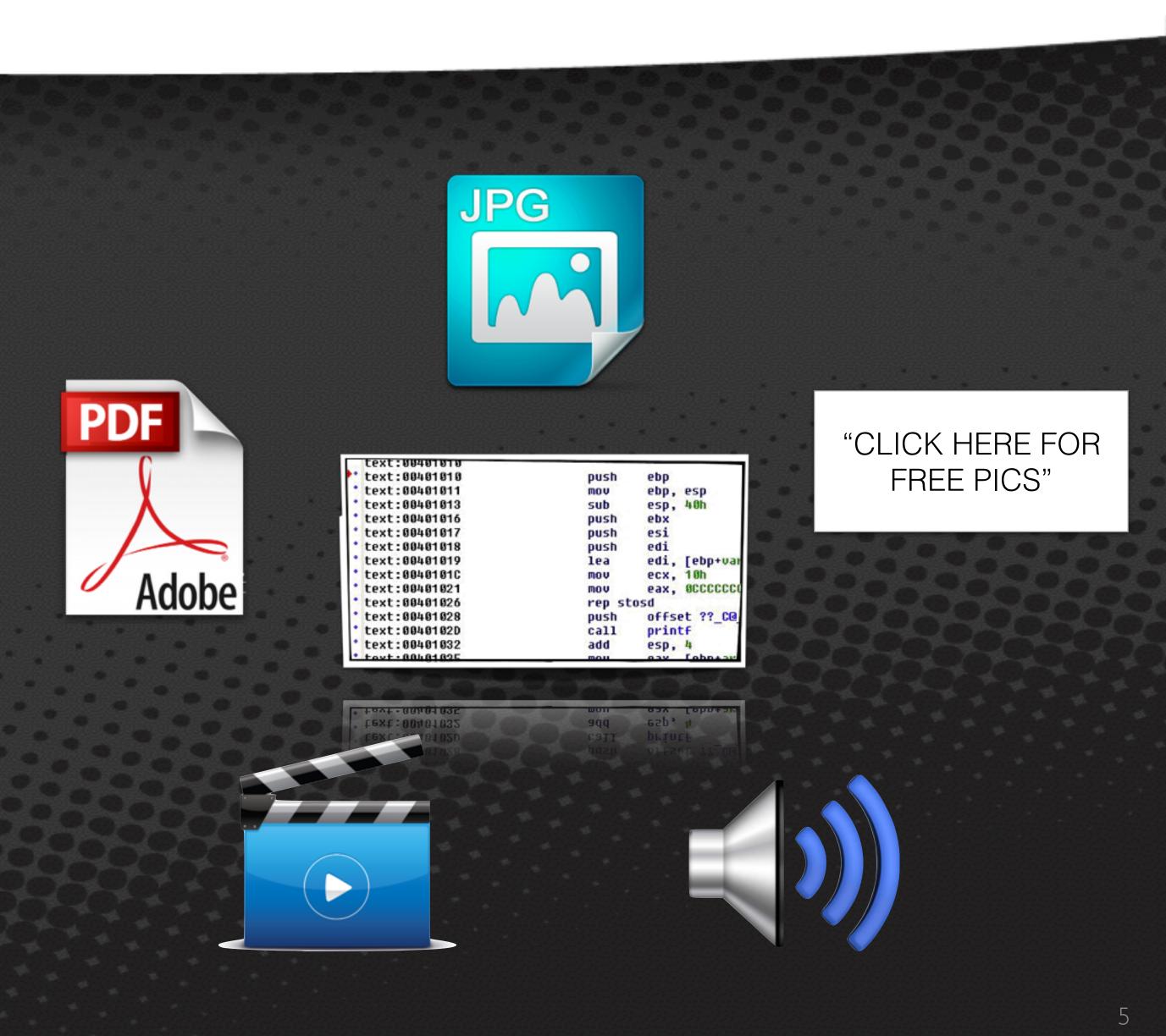






Malware is not just code, it's also

- natural language
- documents
- audio
- video
- images





• **Problem:** Graphical assets are an untapped resource in the malware analysis space; image analysis done manually.

samples without parseable images

Of a collection of 2 million malware samples provided to us by DARPA, over half had at least one image embedded.

samples with parseable images

No images



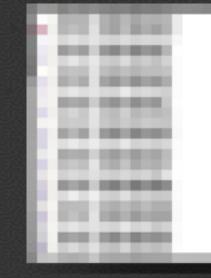
600 400 200 number of samples (in hundreds of thousands)

1 to 10 images 11 to 20 images More than 20 images





A packed Trojan still needs an attractive icon to lure a user into executing it



Images can hint at the ways in which attackers are tricking the user and the purpose of a binary artifact.

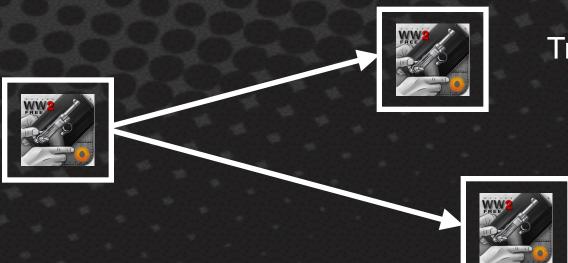




invincea How Image Analysis is Useful



By exploring the malware's "social network" through shared rare images, you can learn about an otherwise hard-to-reverse sample.



Trojan.Win32.VBKrypt...

Trojan.Win32.Swizzor...





Survey of the threat landscape We're seeing an up-tick in malware masquerading as PDFs, let's alert our employees to be on the lookout

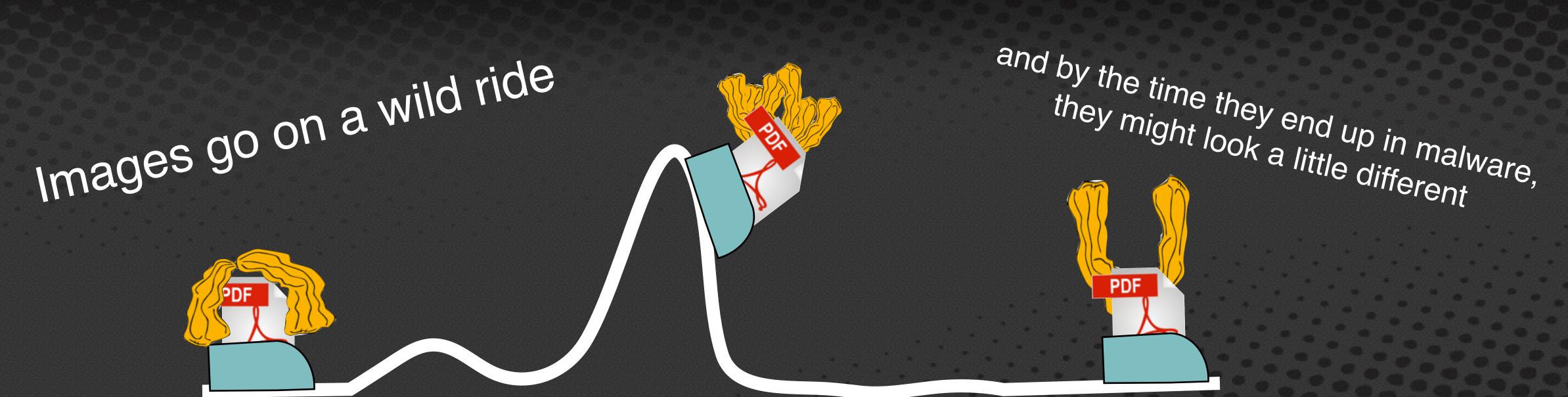
Quick analysis of new samples Our system has found a previously analyzed sample that shares an image with this email attachment

What Automation Makes Possible









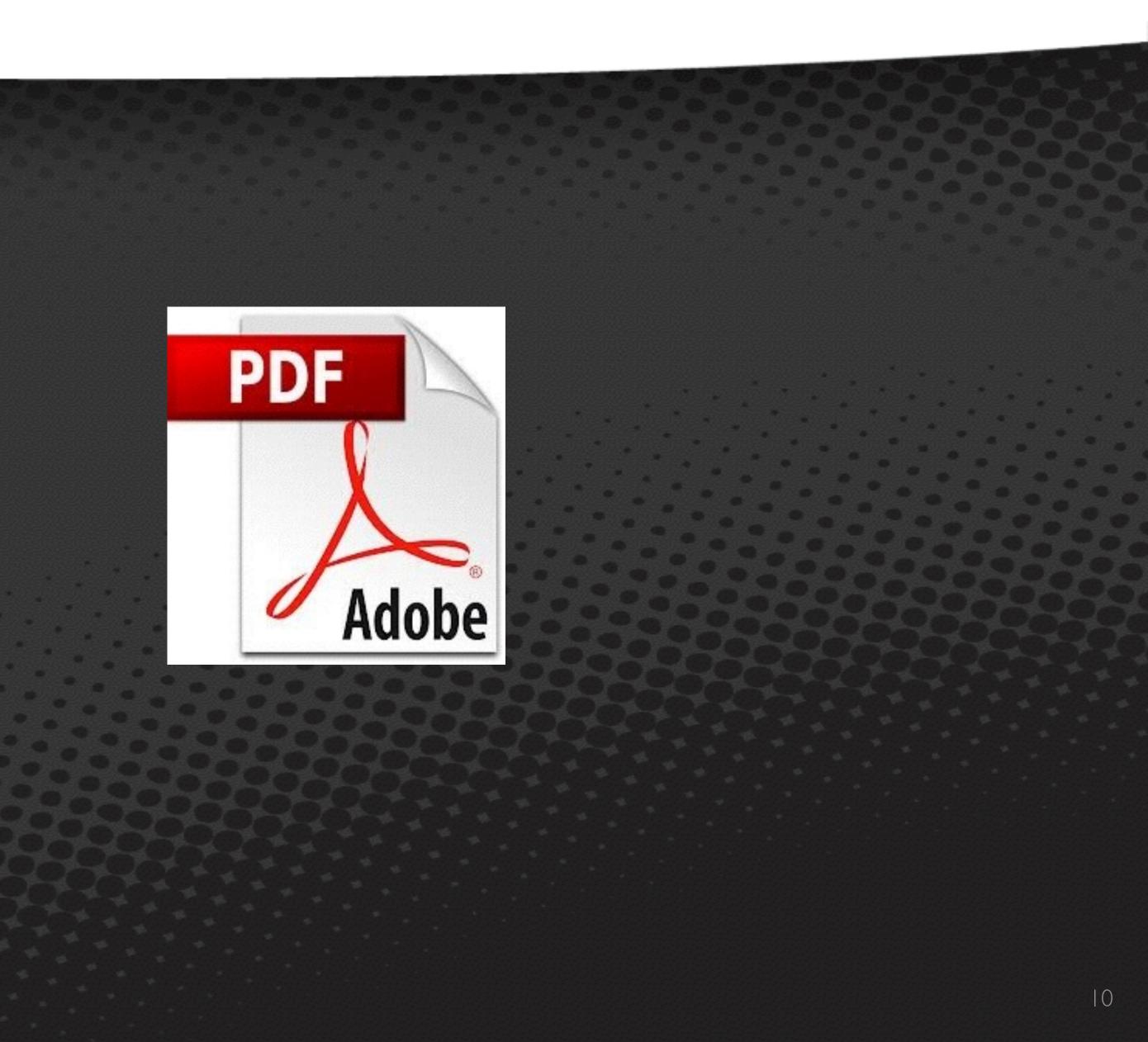
Hash comparison will fail if the image was compressed copied and pasted modified <u>deliberately</u>

Why Not Just Compare Hashes?



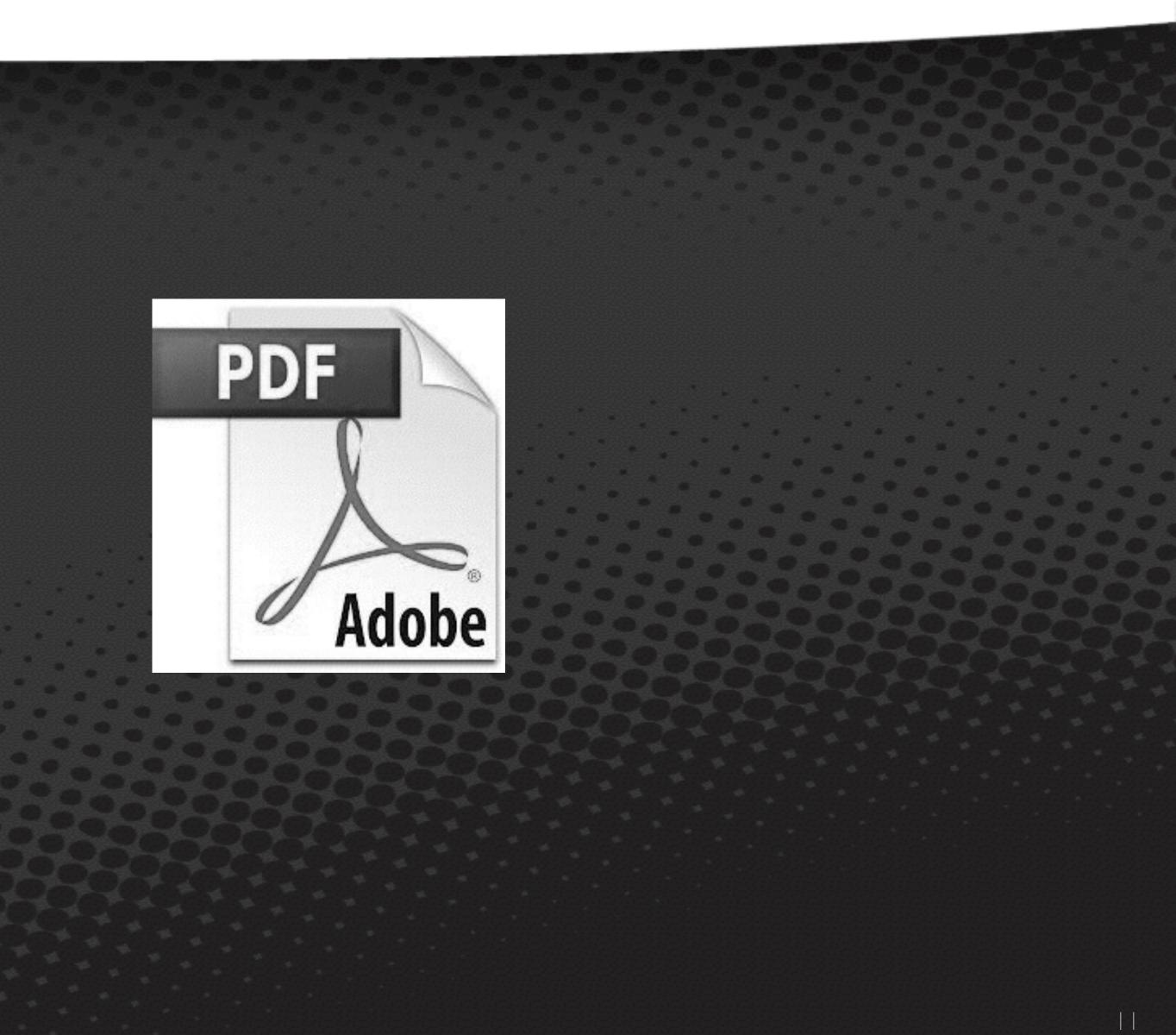


1. Take an image





1. Take an image 2. Reduce to grayscale





1. Take an image 2. Reduce to grayscale 3. Stretch/shrink to 32x32



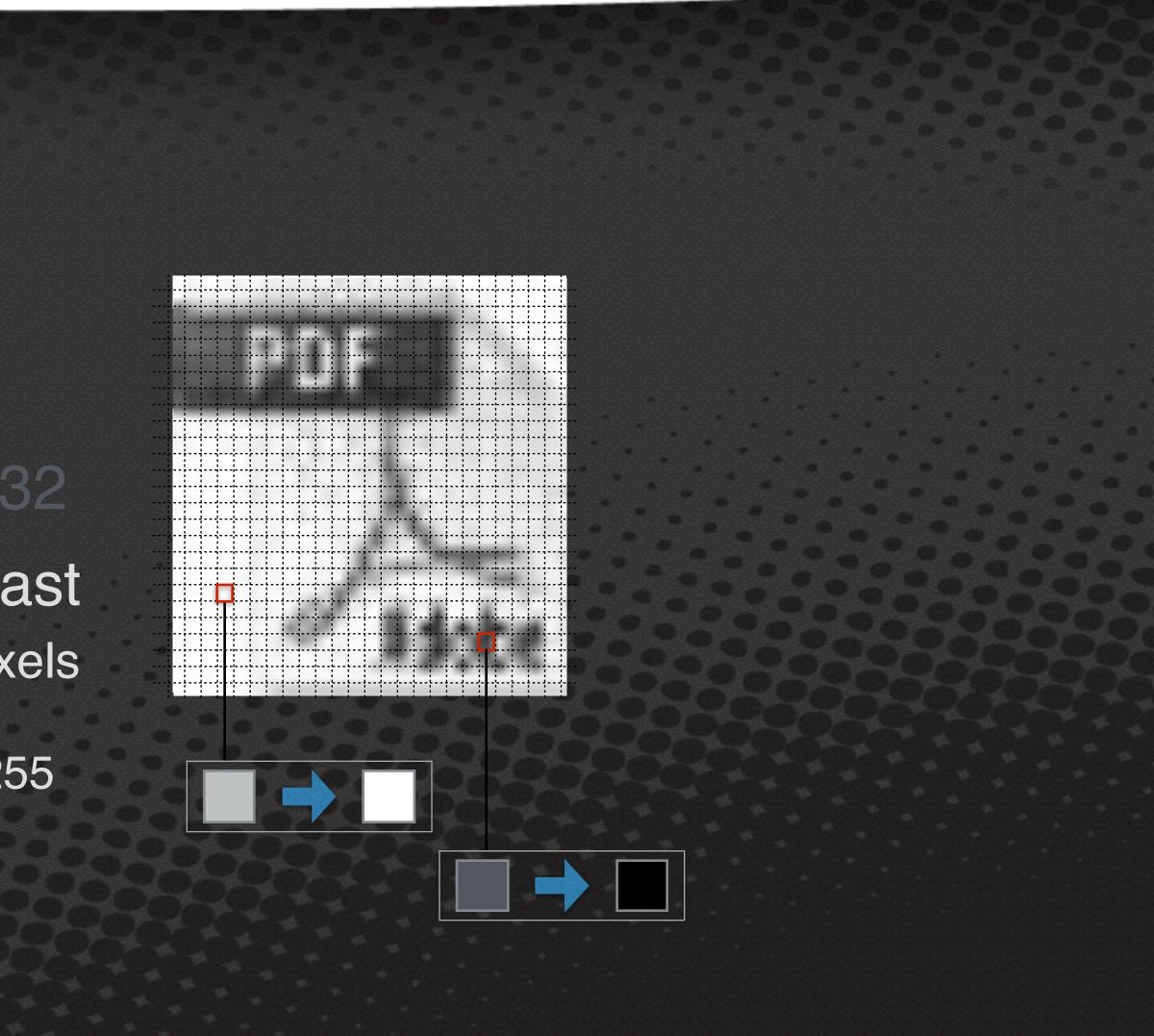


1. Take an image 2. Reduce to grayscale 3. Stretch/shrink to 32x32

4. Convert to high contrast

a. Get average value of pixels b. For each pixel,

> if above average, set to 255 if below average, set to 0







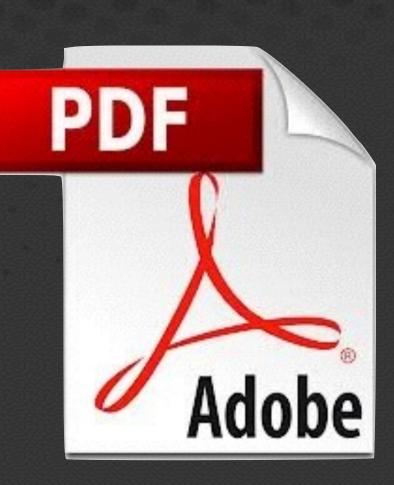
blàck hat

1. Take an image 2. Reduce to grayscale 3. Stretch/shrink to 32x32 4. Convert to binary vector a. Get average value of pixels b. For each pixel, if above average, set to 255 if below average, set to 0









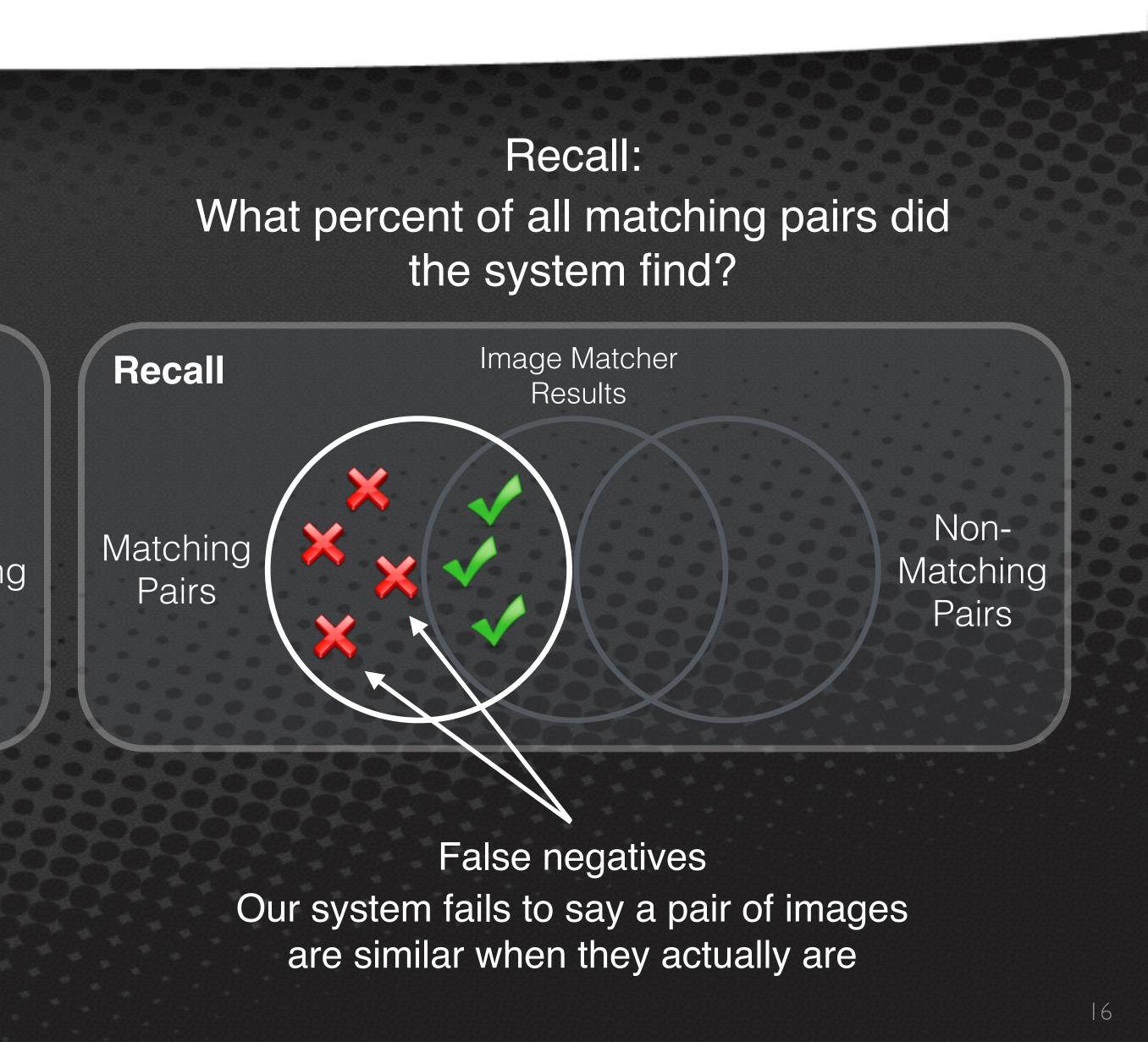




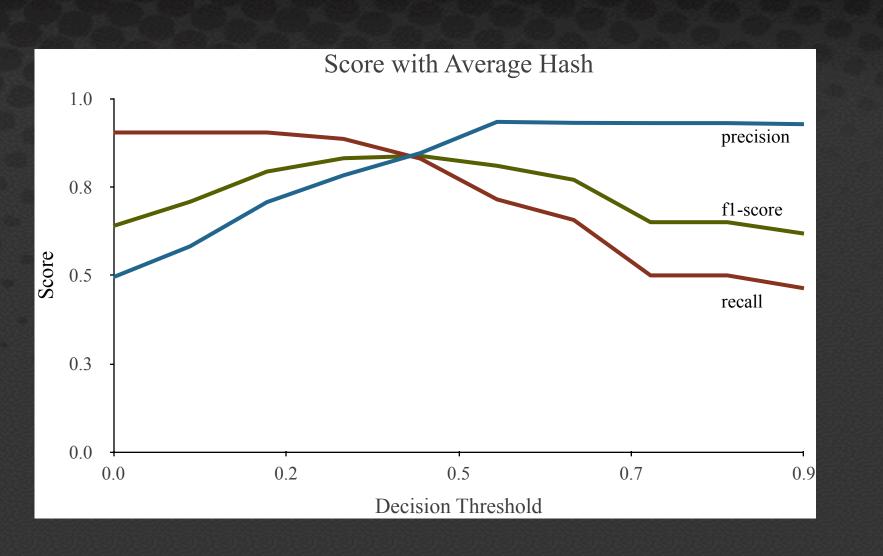


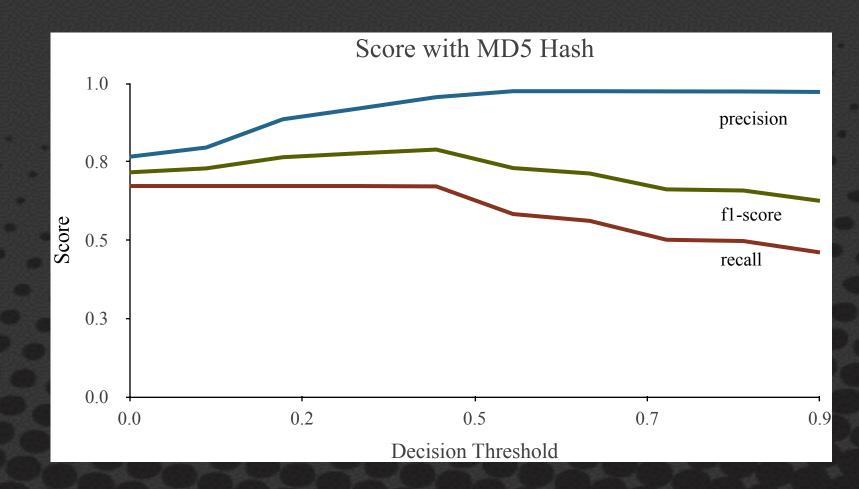
Precision: What percent of the pairs matched by the system actually had similar images? Image Matcher Precision Results Non-Matching Matching Pairs Pairs

False positives Our system says a pair of images are similar that actually are different









- 200 hand clustered samples •
- MD5 wins out in precision •
- Average hash wins in recall •
- Humans can easily detect and ignore images that • don't match (false positives)
- False negatives invisible to user and lost forever
- We'd prefer to have more false positives (lower O precision) in order to have fewer false negatives (higher recall)

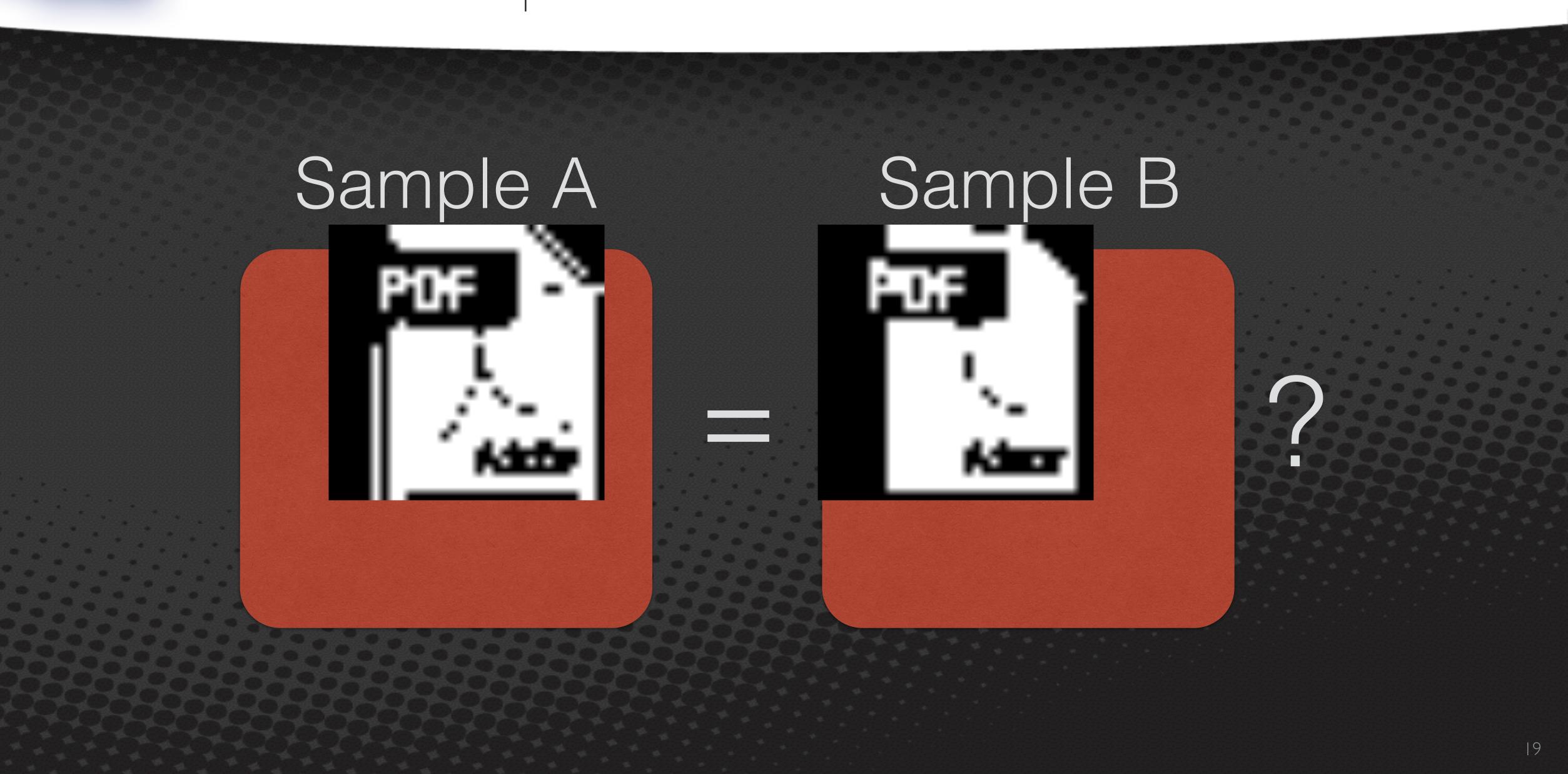






Comparing Sets of Images





Comparing Sets of Images



Comparing Sets of Images



Number of matching pairs (2)

Number of possible matching pairs (3)

= 0.66 similarity















Browser





Document

Solution of Images Automatic Classification of Images

Anti-virus

 Reveal purpose of malware Survey threat landscape Assign risk factor

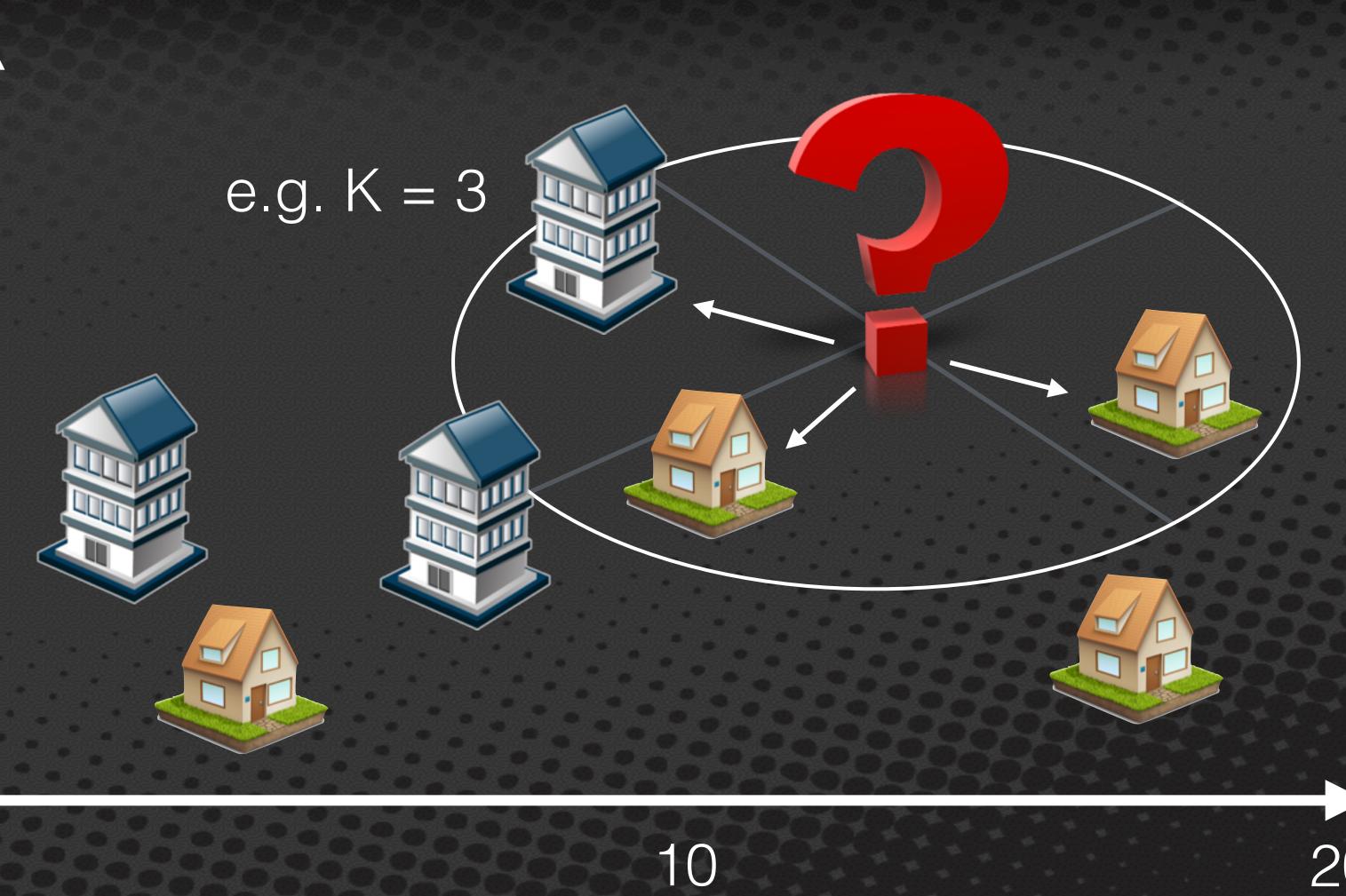




Machine Learning 101: **K** Nearest Neighbors



black hat



Number of rooms

K Nearest Neighbors

- 1. Plot points on graph
- 2. Assign classes to points (e.g. house or apartment)
- 3. Plot point on graph with unknown class
- 4. Pick a number K as appropriate for your data
- 5. Get the top-K nearest neighbors (AKA closest points) to the point with the unknown class
- 6. Classify by majority vote (e.g. if the 3 nearest points are 2 houses and 1 apartment, unknown class is house)

20



23



Image with

unknown class



_	ļ
	_
	/



Q

icons/antivirus.png	wind
icons/antivirus2.png	wine
icons/jpg file icon.png	jþg
icons/real player icon1.png	wind
icons/unknown.png	vmwa
icons/windows installer.png	wine
icons/windows installer1.png	wine





lware icons/windows installer3.png



/windows network icon.png

Classification by Color Histogram





Graphical content of malware is a significantly under-utilized signal in malware analysis

Automation and visualization make this "human" signal accessible at a large scale

Alex Long alex.long@invincea.com



