Nuix Workshop - Introduction to Forensics







WHAT IS COMPUTER FORENSICS?



Computer forensics, also called cyber forensics, is the application of scientific method to computer investigation and analysis techniques in order to gather evidence suitable for presentation in a court of law or legal body. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computer and who was responsible for it.

Computer forensics has become its own area of scientific expertise, with accompanying coursework and certification.

Computer forensics is a science and therefore requires **Scientific Method**....



- The **scientific method** is a recognised body of techniques for investigating incident or occurrence, acquiring new knowledge, or correcting and integrating previous knowledge. To be termed scientific, a method of enquiry must be based on empirical and measurable evidence subject to specific principles of reasoning.
- Scientific method is a model applied to all areas of scientific examination. These elements are valuable to computer forensic science

The Scientific Method Ask a Question Do background research Construct hypothesis / theory **Investigate** through analysis **Draw conclusion** prove hypothesis Report your

results

INDUSTRY GUIDELINES



Principle 1:

No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2:

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3:

An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4:

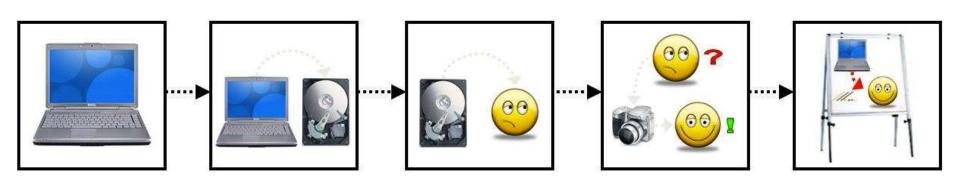
The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

Source http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf

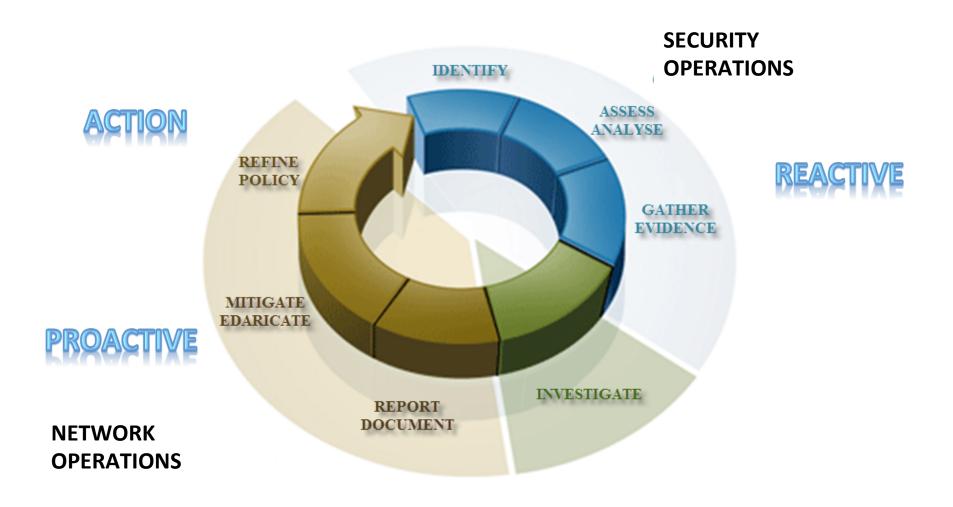


The benefits of the application of digital forensics to computer based investigations underpin the following:

- Security of evidence / incident
- Integrity of investigative steps
- Deeper analysis unallocated space / file slack (The whole story)
- Auditable response
- Repeatability of action
- Best evidence practice







SECURITY OF INCIDENT - DOING NOTHING EVEN CAUSES CHANGES

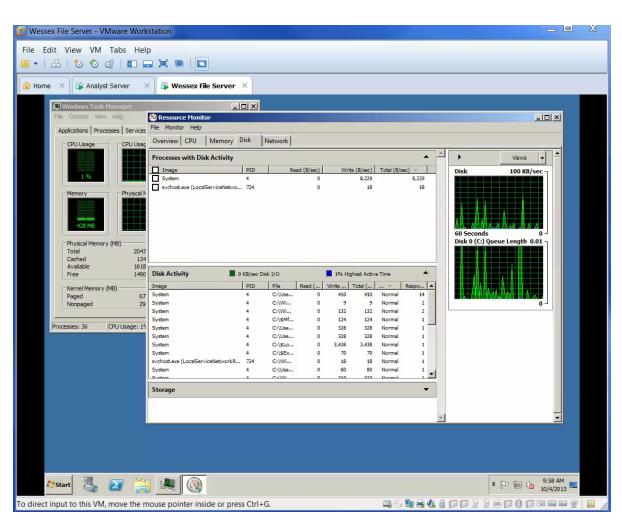


Even at rest a computer is using memory and performing disk writes. This is essential to the operating system.

The capture shows disk activity on a computer with no user activity and no applications running.

Now consider

Malware
Anti forensic applications
Cluster overwrites





The first step in any investigation is the search & seizure of exhibits which may contain crucial evidence!

Decisions that you, make may result in loss of crucial evidence.

Points to consider

- DNA and/or fingerprints
- Prevent tampering & preserve original condition
- Record details & actions paperwork!



Store in a secure location

What is capable of storing data?

Losing data - shutdown or not?



















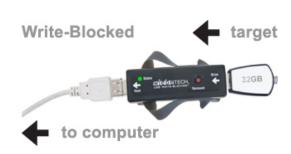
COLLECTING DATA - FORENSIC METHOD



Whether we are considering logical or physical collection we must ensure that we collect data in accordance to industry guidelines and take every step to protect the data from any change due to our action. In accordance to guidelines if this is impractical we must ensure we understand the implications of our actions.

A write blocker is a hardware or software device that prevents ANY write activity to a connected device or resource. We can then use a forensic application or DD command to collect the data into a forensic container.

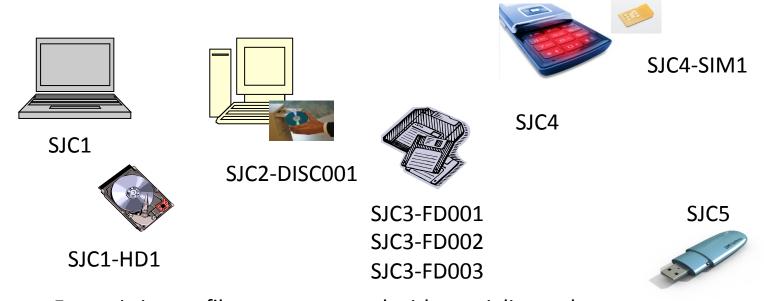




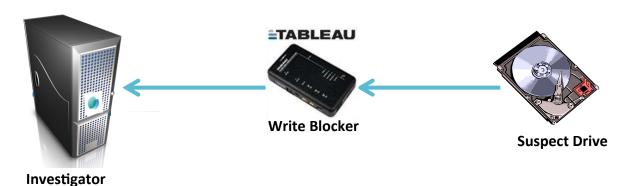


FORENSIC MAGE FILES





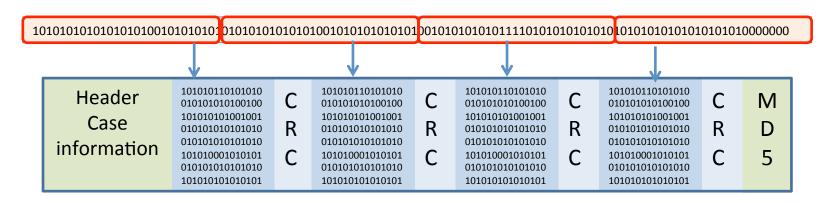
- Forensic image files are generated with specialist tools
- Are an exact 'bit for bit' acquisition of the data
- All devices should be unique referenced



FORENSIC MAGE - CONTAINER



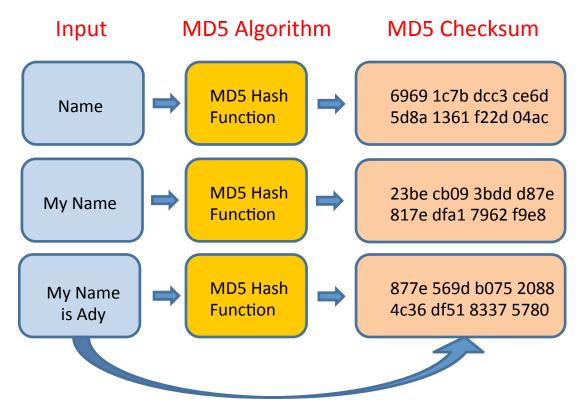
Data is collected from the source device at binary/disk level by pre defined size and each section is checked with a CRC checksum. The whole image is then verified with an MD5 checksum



Should any single value be change then the CRC would fail and the MD5 checksum would present a different value. Therefore verification would fail and the collection process would be undermined.



MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length). The result is as unique to that specific data as a fingerprint is to the specific individual.



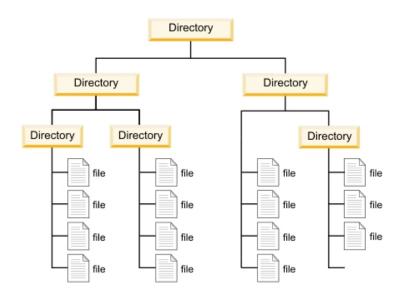
Identical data will provide identical MD5

INVESTIGATIONS - AN INTELLIGENT APPROACH

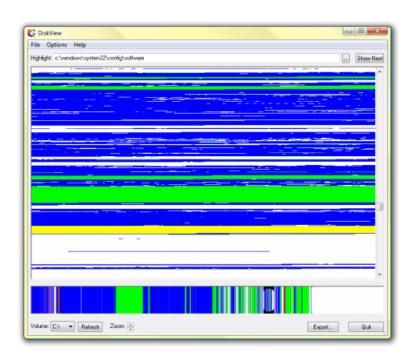


- Investigations frequently involve large numbers of devices including multiple computers, mobile devices and a variety of digital storage media.
- Traditional methods of analysing each data repository individually are immensely time consuming and often ineffective.
- Typical collection of devices for investigation analysis
 - Suspect's personal possessions
 - Apple Mac book Laptop (HFS+)
 - Apple iPhone (iOS)
 - External Hard Drive
 - Company/Employer data relating to suspect
 - Microsoft Windows Desktop PC
 - Microsoft Exchange Mailbox
 - > Folder and files stored on a Windows Network share
 - RIM Blackberry mobile phone
- Nuix is engineered to triage, process, analyze and bring to the surface critical evidence from entire data sets.
- This saves time and effort, freeing investigators to test hypotheses, follow evidence trails and find links between suspects.





Logical application only allows an analyst to investigate live files and folders and whilst investigation is undertaken important attributes are changing



This Sysinternals utility will make a graphical map of a hard drive - we can see all clusters and view information about every single one of them. Capturing the data at disk level in a forensic container ensures no changes can be made to the data



Lets take a look at a simple word document. From a logical view we can see the content and some simple meta data



Now lets take a look at the document from a forensic image

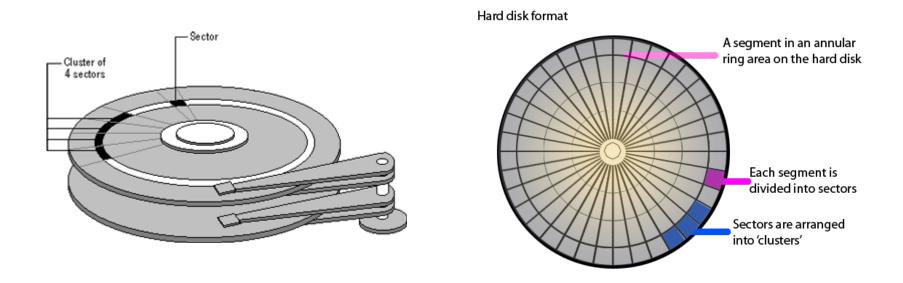
WHAT'S IN A FILE?



0000 <mark>0፲ a'± - q</mark>		ϒϒϔϒϒϔϒϒϒϒϒϒϒϔϒϒϒϒϒϒϒϔϒϒϒϒϒϒϒϒϒϒ	¥ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸ	ŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŸŶŶŶŶŶŶŶŶŸŸŸŸŸŸŸŸŸŶŶŶŶ
00220\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\				
00660 · · · · · · · · · · · · · · · · ·	éő	····é·····£···0·····		ÜÜÜFHH
00880 · H · · · · · · Õ · · · · · · · · · · ·		j		· · · · · · · · · · · · · · · · · · ·
01100 · · · · Ü · · · · · · · · · · · · · ·		····Ü······F····	Actual Content	
01320 · · · · · · · · · · · · · · · · · · ·	···s···0···£·····		Actual Content	
$01760 \cdot 0 \cdot \cdots \cdot 0 \cdot 0$		0000000000000000		000 0000 0000 0000 0000 0000
01980		·····Ö··········Ö·····················	/	
02200		· · · · · · · · · · · · · · · · · · ·	<u></u>	
02420		This is a	simple file	
02640	Dates		**************************************	
File Header		The second of		THE RESIDENCE OF THE PARTY OF T
				,
04400				
$04620 \cdots \cdots$	v · · · v · · · · v · · · · v · · · · v · · · · v	·v···v··6···6···6···6···6···	6666	6 · · · 6 · · · 6 · · · 6 · · · 6 · · · 6 · · · 6 · · · 6 · · · 6 · · · 6 · · · 6
$04840 \\ 6 \\ \cdots \\ 6 \\ $	-6 6 6 6 6 -	··6···6···6···6···6···6···6···h···H···6	6 6 6 6 6	$\cdot e \cdot \cdot \cdot \cdot \cdot \cdot \cdot e \cdot \cdot \cdot \cdot \cdot \cdot e \cdot \cdot \cdot \cdot \cdot e \cdot \cdot$
04620	-6666-	6 6 6 6 6 6 6 6	66666	-666662AĐà
05280	. D ,	Д Д Д	P;p@ A	-8 V ab
05720mH -nH -sH -tHJ`ñÿJU:°N-o-r-m-a-ldgECJ HaJmH -sH -tH -) - A. Òÿ; - D D - e - f - a - u - l - t	- ·P·a·r·a·α·r·a·n·h·	·F·o·n·t····R·i·óÿ*·R······0···T·a·b·l·e· ·N·
05940 o · r · m · a · 1 · · · · · ö · · · 4Ö · · · · · 1 · 4Ö · · · · · · aö · · · · · · · (· k · 6ÿÁ· (· · · · · · · 0 · · · N · o · · · Ē · i · s · t · · · · · · · · · PF	K·····!;,Š≒·ú·	·····[Content_Types].xml¬'ËjÃC	$\cdot \texttt{E} \div \texttt{bfffqor} \circ (\texttt{¥0lcIw}) , \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\$	$\cdot \texttt{ä} \pm -\texttt{j} \mid \text{,'} 4 \text{ £Bwì, P}^{\circ} \cdot -\texttt{t} \# \cdot \texttt{b} \hat{\textbf{I}}^{\text{m}} \{ \texttt{U} \otimes \mid \tilde{\textbf{a}} \cdot \cdot \text{``\'oT\'eU}^{\text{hd}} \} \tilde{\textbf{a}} \text{```\'ou} \hat{\textbf{a}})$
06160 »×*1P·f'¬ô "^××Wåi ·0) ™;Též9<·"1 ##Ü·\$yi}· å·;·À~@‡æ¶(îŒŏÄHœñÄĐuù*·D× zfÈ/OŠÇ° ōûù·\$€"X«Ç3aZoò·Âå				
06380 '\$\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\				
068200c'v·ušžt>-M·ān+it-Øpe@il)'ūše'-Űa+'Øm+a[Ø¥ûū:l Đ °GR'Āx^6Øš->\$·ùāûÿ·@≪*iC··!)0ū^ýriCsñy				
$07040 \grave{h} \dagger \ddot{a} \mathring{*} \grave{o} \cdot \ddot{A} \ddot{A} \mathring{D} \mathring{w} \ddot{Y} \cdot \acute{q} u \boxed{g} \langle Z \circ \P \cdot @ o \sim \mathring{U} \circ Ap \circ x \breve{S} p T 0 - \div \cdot - + [\cdot] \cdot \cdot j \cdot \times \ddot{e} \tilde{o} \cdot \mathring{w} z A \ddot{I} \cdot \circ i f V - 2 \acute{I} F U - 9 \acute{e} \acute{q} \ddot{z} v \cdot \ddot{O} - 5 \setminus [\mathring{w} p \mathring{E} \mathring{u} \mathring{L} - \mathring{u}] \cdot \mathring{u} = 0$				
07260ĐTµ×:S··1£÷êù÷¯ž?EÇ·ž·?øéøáÃā·?ZBΰmœ,åU/¿ýìÏÇ·£?ž~óòÑ·ŐxYÆÿúÃ'¿üüy5·ÒgsĨ‹/ŸüöiÉ‹¯>ýý»G·ðM Geø Æ				y8IÂjæbRÆic XÅ»< ·Ç¿¾I u3·KGñnD·1÷·N··IB·Òsü€
07480 iîrê@u-ú,K>Vè.E·L+M2ׇ'šf<¶i·~~~Vé·bvl³{·u8«Ôz<·°HÈ Ì*"··æñ:ž(·W`·â* ~·«"JĚÁTøe\O*ōtH·GWEHYµæ- 07700»\·ôi¯¹[x'ì·óù c É}Wrbÿ É ″Ïq-′³Ú eW÷¶)6-r4°C·SÆ·jÊÈ išd ûDD‡AbIqbJ‡xÌe°f··6k àê‡*¢A,Sh°ëžá				a ' ·ôäïÊ1£P m·\\9†·øâëÇ·'ô¶·âMØ"²2aûDù],,;Yt ·ö,,·AÛ·V^ô*f··ÌH ín÷ÞÜ-Æ··é"·á€d>Òzïû"nœ"
07920(S ² * 6008 '>ā bu · 6û · 1Ĵāa'> Æ · v² + ÞĀKy · Taya'OB '* ace, AGM Ö\nzĒCiū ' Āa· · ā · 4. uI+Y · C¾ · 610M " Å30¶ ĀŪS "ĀS.			.m.i uata	%&LED/p ;-m;Üâœ%]ùöÊàì8fi,,'r«S4Ïd·7y\È`ÞJâ n
08140 * *åίŠIù ~R¥·Æÿ3Uô~·7·+ ö€·×¸·# ¯m ··q¨BiDý%€ÆÁÔ·^·. <i·*,l6ÿ·9ôÿmîy·&-áàsŏi^·ýhe, =(k&ún!vïö.f< th=""><td>K'e"LD•Ä•©·{D· ·ê·,</td><td>÷v·E·ê¦šdeÀàNÆŸûžeÐ(ÔMN9ßœ·Rì¾6·þé</td><td>fças (embedded)</td><td>\$Y >ÕÈ 3 - 4¶, V-ö) Â9 - Z [±æ4^næÂ -ç5+Á0!Já¾ -é?°ÿQ</td></i·*,l6ÿ·9ôÿmîy·&-áàsŏi^·ýhe, =(k&ún!vïö.f<>	K'e"LD•Ä•©·{D· ·ê·,	÷v·E·ê¦šdeÀàNÆŸûžeÐ(ÔMN9ßœ·Rì¾6·þé	fças (embedded)	\$Y >ÕÈ 3 - 4¶, V-ö) Â9 - Z [±æ4^næÂ -ç5+Á0!Já¾ -é?°ÿQ
08360á3ûeBo~C%·µ·Á‡·M·Ã·oú'm< . vp· ``·'Á¤IYÓf-~¶Z%Y_pS[ð=al-ŪYü}Nc-j™ĒĪĒĀ‹4vfaÇÖvl;@Á''S-†ÆùĀÆ8Æ Ò*□u				rels/themeManager.xml.rels, M Â0·,,+,w·ooó°·
08580 &Ý^Ð-Ô·"ä5 6?\$Qìi ⊗,·.‡a¾™i»— É·c2Þlh²··:é·qšám,ìŽ@R·N%ů;d°·,Žo7i·q°K(M&\$R(.1f·'J°œĐŠTù€®8£ Vä"£ 08800 ypes].xmlPK··-····!·¥ĭŎ\$çÀ··6·······	E¦AE»ÐH÷u} ñ>∶ A޾b	·{O··-Pšÿ³ý8·%g/··]bQAsU·(¢ÆIå#>ªI	-E[°°AB···ŸŸ··PK··-	····!·,Š\u00e4·ú······[Content_T
09020 NIVE theme/theme/ rele/themeManager wml relePV	couml transion=#1 O#	encoding="HTT-9" etandalone="wee"	<pre>/a.clrMan vmlne.a=#1</pre>	http://achemaa.onenymlformata.org/drawingml/2006/
				Hlink="folHlink"/>······
09460 · · · · · · · · · · · · · · · · · · ·	······································	(8 8		······S··ð·····:Ë·····ÿ·········?·····
09680 8 4 5X) U;	, °	y@p@yy	U·n·k·n·o·w·n·ÿÿ·····	
10120 bri-1-A	• " · så" · s · · · · · · · · · ·	U I 3. y acx A		7.
10340 · · · · · · · · · · · · · · · · · · ·				
10560 · · · · · · · · 0 · · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·	2f · · ð · · · ·	üý·····	······HX····· ðÿ····\$P··ā···ÿÿÿ□ÿÿÿ□ÿÿÿ□ÿÿÿ□ÿÿÿ□ÿÿÿ
10780 JŸŸŸ□fXj · · · · · · · · · · · · · · · · · · ·		···· A · d · y · · ·		
11220 þý åÝòùoh «` +' 'ऐo	. xa	· · · · · · _{//} · · · · · · · · · · · · · · · · · ·	Ð	ôä
11440 ddy · · · · · · Normal.dotm · · · · · · · Ady · · · · · · 1 · · · · · · Microsoft Office Word · · · · · · · · · · · · · · · · · ·	··"T5èÀη@···œaÄèÀi	t · · · · · · · · · · · · · · · · · · ·	·····	
11,660				
	File Slack			
	,	xxY1		
2090b - 'ŸŸŸŸŸŸŸY', /Ÿ - 21120 YYYYYYYYYY Y - Y				ŸŸŸŸŸŸ¥¥ŸŸŸŸŸŸŸŸŸŸŸŸ¥ \$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$\$
21340,999999999999999999999999999999999999		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
21560-2003 Document · · · · MSWordDoc · · · · Word.Document . 8 · 69*q · · · · · · · · · · · · · · · · · · ·				
22000			±ε11η	VIAGAMI JOHN VIAGA OND JOE WILLIAM STORE WILLIAM
22000	'(Êæl -!÷ÞŠÉØ¶mÔ'C-Ÿ		-⊾:-10: 0-11:-08:μum¶κ: ÅšZ:ô: à: vT∞:∀>î -vo!	: Muowe-reg:::;uv=regur-ss\ u P*Exk-e a:n"-k#AlE Sr68!="516@°D00000-Y*-*s!:-"1504-f-hi-liftil
22440 ·c ë ·Ä″TIš `«sâ ·P ·%Ï ?Lù · ·ÿÿ · ·PK · · · · · · · · ! · ·çž ·) · · · 0 · · · · · ÿØÿà ·JFIF · · · · ·ÿÜ " · · · · · · · · ·	/#'[··ŌžMp^¥ØŽ ·)ß^	~×I ·m1+"ܤ BàØ¹q~œs}{÷¬ò`',H£§\$°;\$:	:1k@7Sò^\ .\J®×<7ZLE^	-1>}pt[MR£K·ðz -;%YY·"0,,\$-SA),,E±ÖXÁKüi7;IS™^~&]
22660*: E Q:Èyh÷tL-@Újőkő*c×5h-ÀÅ*40S,ôdő8. "&š+\õ 42746'-8 *-+v <y-uçwdc:asy-iè-\$ en"kä"+™i-*5sĕf<="" th=""><td>f e' ·ô··/ zñ· üàÀ·\</td><td>V·oØ%H£D·ýμÂNæô^+I]gôâ*T°NW·—·6□Ï ^</td><td>¥T ·, o≎ %×+w · Þ · aHa@{H"Æ</td><td>fá·ØO"þ·" ,pv¿X·‰ÌQ·Žâ¨UŽDÆ-â%R?□ÔÔ°œÈÜl-·Ö1ñúf //</td></y-uçwdc:asy-iè-\$>	f e' ·ô··/ zñ· üàÀ·\	V·oØ%H£D·ýμÂNæô^+I]gôâ*T°NW·—·6□Ï ^	¥T ·, o≎ %×+w · Þ · aHa@{H"Æ	fá·ØO"þ·" ,pv¿X·‰ÌQ·Žâ¨UŽDÆ-â%R?□ÔÔ°œÈÜl-·Ö1ñúf //
22880ztư œ7·2°++2ka} :Iả°XŸ°ā, ½;ñ,fā'·^·ýfÁŽg¿/¼IáŪÔ4Óý< İy,WVZA0°-à, £98Ó-···°\$ÀU\$@)({· ·.ûy\$··r·l	Io·2@fvy@-<ÄVq·A	'AőSøïfAVÉ·»ÇÆžç:Á€ö·Þ¦f¾×)"z}Sà ·q	2,,ë• ·×; "3Äő»^ß·4îØ·-	; z½÷ A·ív·³ÿÿ··PK······!·0!NZ···bG····
23100wcrd/stylesWithEffects.xmli\8s06 \~8Yp \ PSyJ1%7w-sK >>8ëëäöLËt-< %j' \7ûë \%K-\Fên \ë< \ŠÄ \ \\ \A \\$\\$\doorage \frac{1}{2} \\ \A \\		108.00.1114H	-Vzy z**E, alique . Ageogi z>eez~s+mg, reque . Ageogi	D¤b>MnB vinB vin Thinks Mt< aoq" <z 10<br="" eviog-2xx-ab="" vovs!="" ="">Zja - o « < e Bayos vin Gerall vovs! 20 vinoù mar vin San vinoù mar vinoù ver vin San vinoù ver vin San vinoù ver vin San v</z>
23540/ Y, yvyg TI-co // oay// JEBIJMENDAT # DO ALC # OA : (100AL# 1874\) COLOR		·⟨I; /¾; ·£©‡ { ··¬.··+:·Ü·I	uRŒ oùö"ðžøf•Á‹¥‹X0øb÷	%nE-4°t/.\$&-®xèDô7,-{^vb†ÿ-ãNCÊ7ÅøHÏZo'ÖQ-}
23760Î - A°ÛŎ ÇÇÎ : ÎbÔĀŸĀ : ÀOPG - ÛÛ6j , ŠfŪā -ÅĀ" (; ĪdIsPŸV - 28 -h*-* -Er-t Ö -qÞ _ĀŪþ "Oxû ÍĀo ¿ -p éë ¥ "#;	;5·ž ¾ò>Ì.ZBV®″EQçŠ2	ZÐt®"ÅHçŠZHt®"E@犚Ã;W *ÖC°	FÑ:wf"Ø÷~ ·@ ì`°IO*Ó¥Æùi	·ö°xçÈÂZU» ,WûuFS·éôõd¹Ê·! >·;·ÕY¦î«9ù×0Þ±Ô‡Sy·
23980 P1 - ¿-G·çCáĂňu·è- %8Mx09YÂ%·Ìā; lxáÜóoÊ£ e? ·g¥N· Êötë'yq-9p*"%··lb°éf; ¡ä□ÖSÜfÖj>o0¥K8ɇóf; l·þ.&øü				-·'l÷Až· ô°°Î':A3Á:% :I,-3ø^> +ÏfBÜ(qjik,G-P-Ý P
242000ŮeqX;¥B{····································			DO2S7 XfOM ·VCOhöQ™Sı	mŒ®>e s· X4·y·€†!o·ĐOäM·êOÞÝ Ã`7·Ëš··§-É>·"S1~)7
Tite Acres 1919' A'Pari o'u o phiequatou A boust o 1:0 poqu is Gwl, u os.o.tulge seet 195qu 1sc	nrai alihir eni :	y 1 max. 1000 1, yet/compayingspoor	7 174 GPA	//



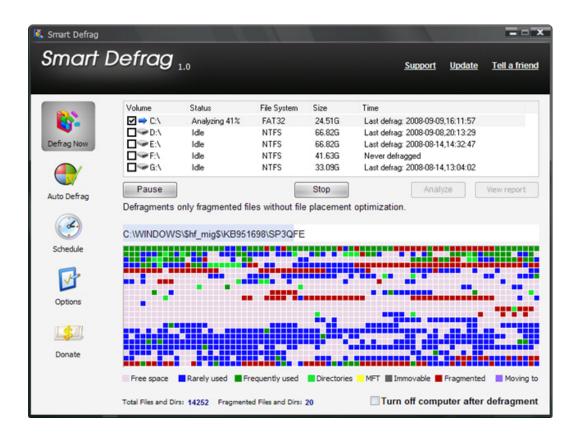
To gain a better understanding of how data is recovered we must appreciate how data is stored and managed by an operating system.



The above example uses a traditional single HDD however the same principle applies to other data medium e.g. USB, Solid State and RAID configuration.

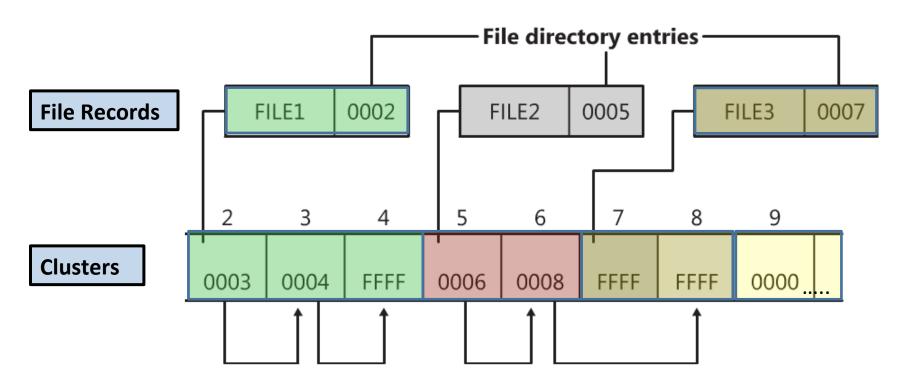


This is sometimes easier to represent and more familiar when we use an application to show the fragmentation of files across the hard drives





The allocation of the sectors and cluster is managed by the operating system. On FAT it is the File Allocation Table and NTFS is the Master File Table. The system records much information about the files it is storing in these tables and this is referred to as Meta Data. The table records the whereabouts of all files on a system and also which clusters are available for future use.



FILE SYSTEMS - HOW IS DATA STORED?



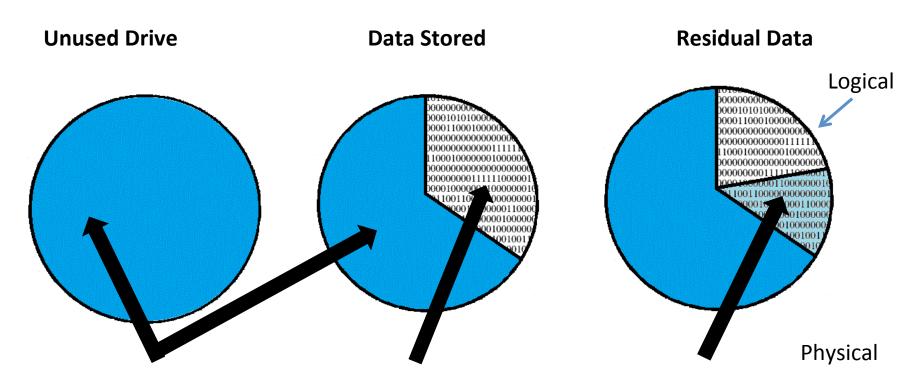
When files are erased or deleted the content of the file is not actually erased. Unless security grade file deletion software is used data from the 'erased file' remains behind in an area called unallocated storage space. The same is true concerning file slack that may have been attached to the file before it was deleted. As a result, the data remains behind for discovery through the use of data recovery and/or computer forensics software utilities.

Unallocated file space and file slack are both important sources of leads for the computer forensics investigator.

Until the first file is written to the data storage area of a computer storage device, the clusters are unallocated by the operating. As files are created by the computer user, clusters are allocated in the file table to store the data. When the file is 'deleted' by the computer user, the clusters allocated to the file are released by the operating system so new files and data can be stored in the clusters when needed. However, the data associated with the 'deleted' file remains behind. This data storage area is referred to as unallocated storage space and it is fragile from an evidence preservation standpoint. However, until the unallocated storage space is reassigned by the operating system, the data remains behind for discovery and extraction by the computer forensics specialist.



As data is deleted through system or user activity then more and more data becomes recoverable from unallocated sectors

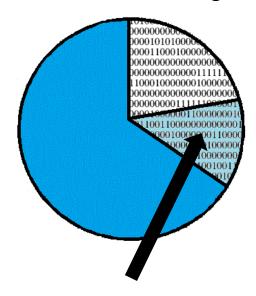


Unused Disk Space (Zero Sectors) Allocated Sectors Residual Data in Unallocated Sectors



Carve file system unallocated space

Data carving, or file carving is a process of reading files without reference to a file system. The technique can be applied to any type if disk that stores data on sector boundaries which includes camera memory, USB devices as well as hard drives. It is based on the fact that most files start with a recognisable data signature



Unallocated Sectors with residual data

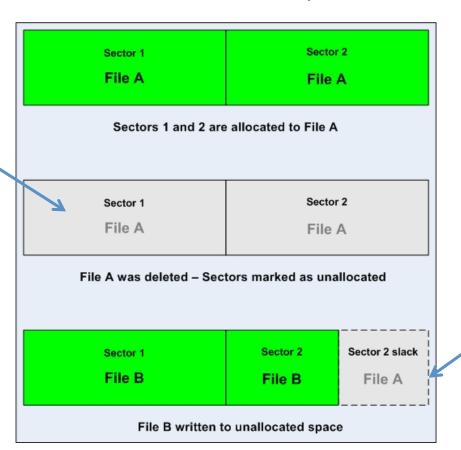


Extract end of-file slack space from disk images

The unused space in a disk cluster. The DOS and Windows file systems use fixed-size clusters. Even if the actual data being stored requires less storage than the cluster size, an entire cluster is reserved for the file. The unused space is called the *slack space*.

Actual data remains on the drive and the sectors are ready to be reused by the file system [File entry is deleted from the file index]

New file written to sectors is smaller than file A



Sector size = 512 bytes

File A = 1024 bytes

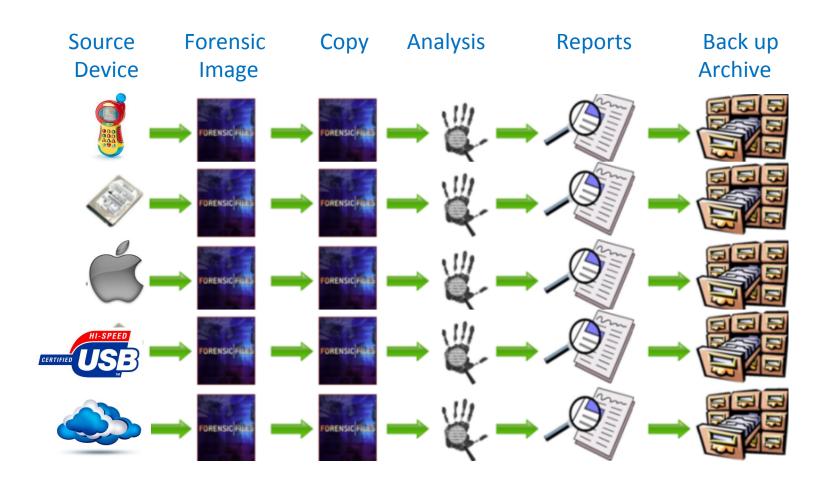
File B = 750 bytes

Slack space = 274 bytes

Residual data recovered by forensic application

CURRENT APPROACH TO FORENSIC INVESTIGATION

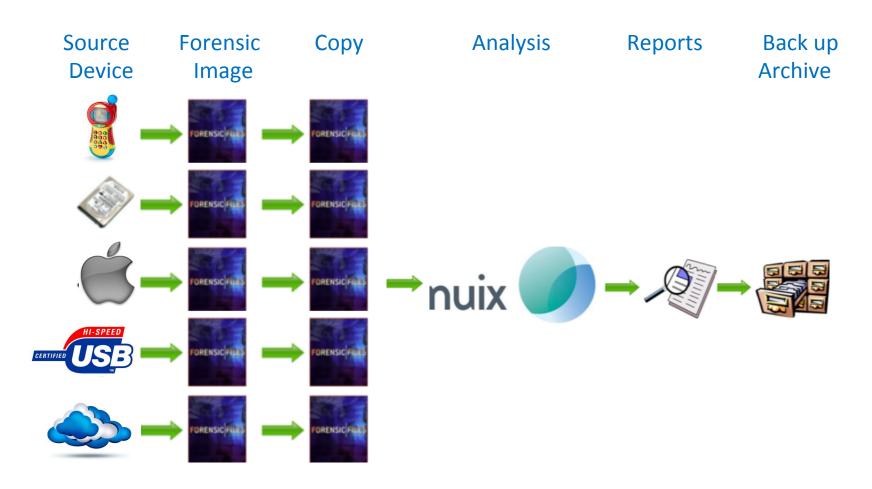




December 9, 2013

A NEW THINKING





Offering a scalable collaborative analysis solution saving time, storage and money

December 9, 2013 25

WHY NUIX?



More power, more precision, more speed

- Speed The ability to react
 - Upwards of 1 TB of data on a single server in 24 hours
- Breadth of supported file types Save the sorting for later
 - As data quantities rise so does the range of file formats encountered for analysis.
- Indexing Get to the detail
 - Fully double-byte Unicode compliant Search in any language, search both file content and metadata, search for special characters
- Ease of deployment Install and go
 - Download and install in under 5 minutes
- Ease of use Quickly realise the value
 - Within minutes, identify IP leaks, transmission of data outside the organization, or run 1000's of queries in an automated fashion



NUIX **S**EARCHABLE INDEXES

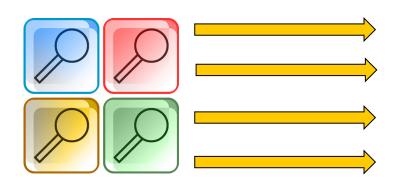
As Nuix processes data it extracts valuable information and places the data into separate searchable indexes which can be searched against in whole or individually.

Powerful dynamic component that allows investigators to be flexible and intuitive in the approach to data management from ECA through analysis.

Allows for the application of specific function to relevant data throughout workflow.

Enable investigators to quickly target and hydrate function to relevant material through ECA and NVA.



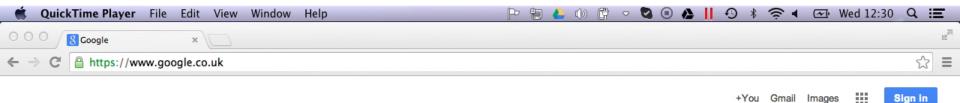


The database architecture of Nuix offers the investigator powerful options in order to get to relevant data very quickly and decreasing false hits from search criteria. We can draw comparison to a well known entity that we use every day - Google



SMART SEARCHING







Advertising Business About New Privacy & Terms Settings Google.com

EXTRACTED ENTITIES



As previously discussed Nuix extracts values of credit cards, money values, IP addresses, emails, company names and countries – these are referred to Extracted Entities. Nuix uses a method of searching for these values by pre defined regular expression.

In computing, a **regular expression** (abbreviated **regex** or **regexp**) is a sequence of characters that form a search pattern.

Unlike MD5 which requires exact matching regular expression allows for rules of sequence to be applied into a search string that can be used to match any entities that meet that rule.

As long as the entity meets a predefined rule then we can use this method to find data

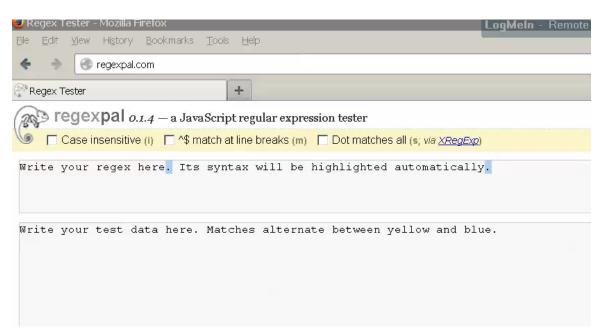
USING REGULAR EXPRESSION TO FIND DATA



This is a simple example of how the use of Regular expression can locate data. All Mastercard numbers start with a 51,52,53,54, or 55 followed by 14 numbers. This rule can be applied to a regular expression as follows:

The number must start with 2 digits that are defined in the expression followed by 14 digits that are between 0 and 9.







Typical collection of devices for investigation analysis

Suspect's personal possessions

Apple Macbook / Laptop (PC/HFS+)
Mobile device Apple iPhone (iOS)
External Hard Drive

Company/Employer data relating to suspect

Microsoft Windows Desktop PC
Microsoft Exchange Mailbox
Folder and files stored on a
Windows Network share
RIM Blackberry mobile phone
USB Devices - Media

Extended range of supported file formats

Forensic Images

Cloud based email

HFS, HFS+ Filesystems

Cellebrite mobile phone images

XRY Mobile device files

Mobile phone backup files

Apple plist files

Apple iWork files types

Apple iPhone/iPad images (iOS)

SQLite files

Entire Exchange databases

Outlook mailstore containers

Lotus Notes mailstore container





Nuix addresses all of the topics we have discussed along with many more and automates them into its process.

Allows the user to feel assured that forensic integrity is maintained and data is presented in a format that is ready to be immediately searched and investigated.

Lets take a look!