



Simple. Powerful. Precise.



Simple. Powerful. Precise.

Nuix Workshop - Introduction to Digital Forensics



- Computer forensics, also called cyber forensics, is the application of scientific method to computer investigation and analysis 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.
- Informática forense, también llamados los forenses cibernéticos, es la aplicación del método científico a la investigación y análisis de la computadora con el fin de reunir las pruebas adecuadas para su presentación en un tribunal de justicia o cuerpo legal. El objetivo de la informática forense es llevar a cabo una investigación estructurada, manteniendo una cadena de evidencia documentada para averiguar exactamente lo que sucedió en un equipo y que era responsable de la misma.
- Informática forense se ha convertido en su propia área de conocimientos científicos, con el acompañamiento de los cursos y la certificación.

- 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



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.

Principio 1: Ninguna acción tomada por las fuerzas del orden o de sus agentes debe cambiar los datos almacenados en un soporte informático o de almacenamiento que posteriormente pueda ser invocada ante los tribunales.

Principio 2: En circunstancias en que una persona se ve obligado a acceder a los datos originales guardados en un ordenador o en medios de almacenamiento, esa persona debe ser competente para ello y ser capaz de prestar declaración explicando la importancia y las implicaciones de sus acciones.

Principio 3: Una pista de auditoría u otro registro de todos los procesos que se aplican a las pruebas electrónicas por computadora deben ser creados y preservados. Un tercero independiente debe ser capaz de examinar los procesos y obtener el mismo resultado.

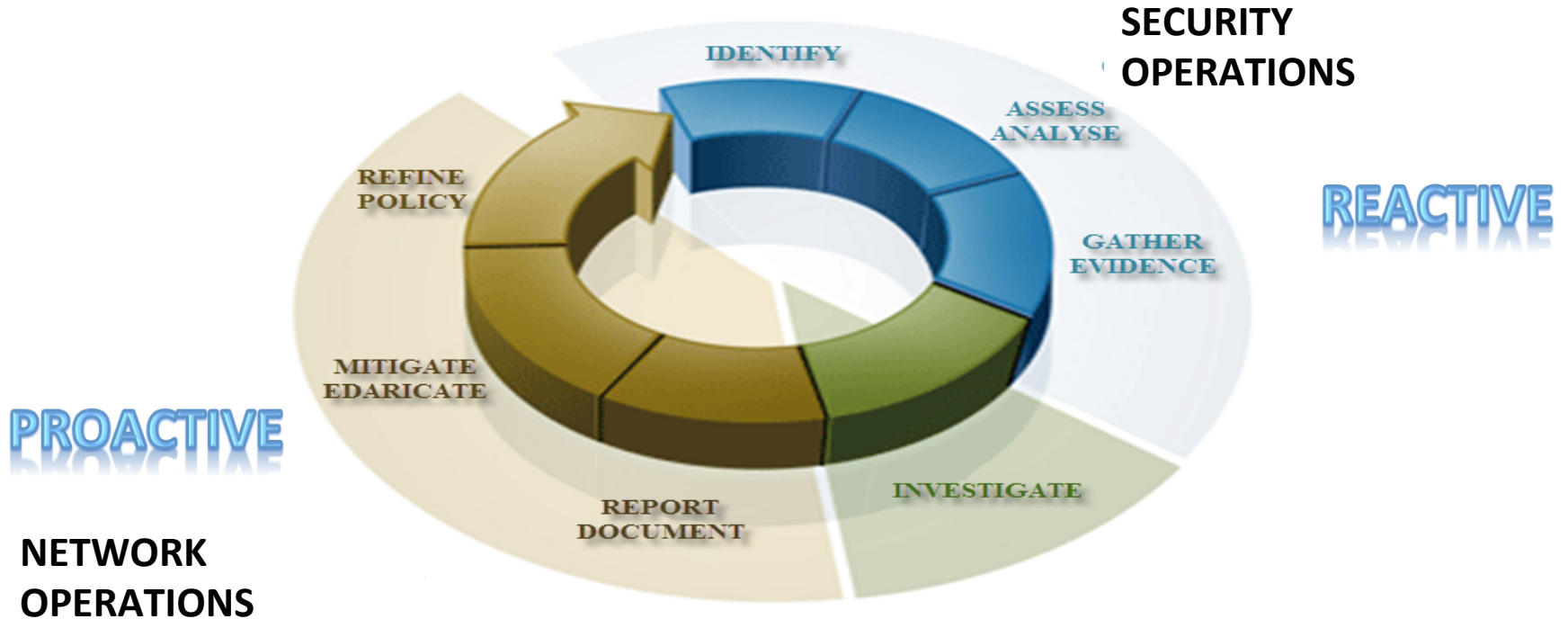
Principio 4: La persona a cargo de la investigación (el oficial de caso) tiene la responsabilidad general de garantizar que las leyes y estos principios se cumplen.

Source <http://www.acpo.police.uk/documents/crime/2011/201103CRIEC114.pdf>

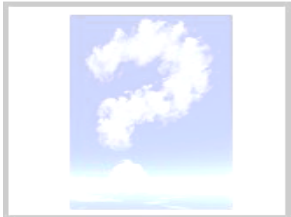
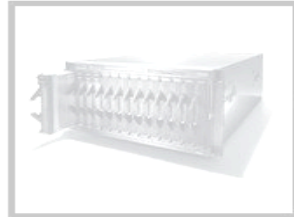
The benefits of the application of digital forensics to computer based investigations underpin the following:

- 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



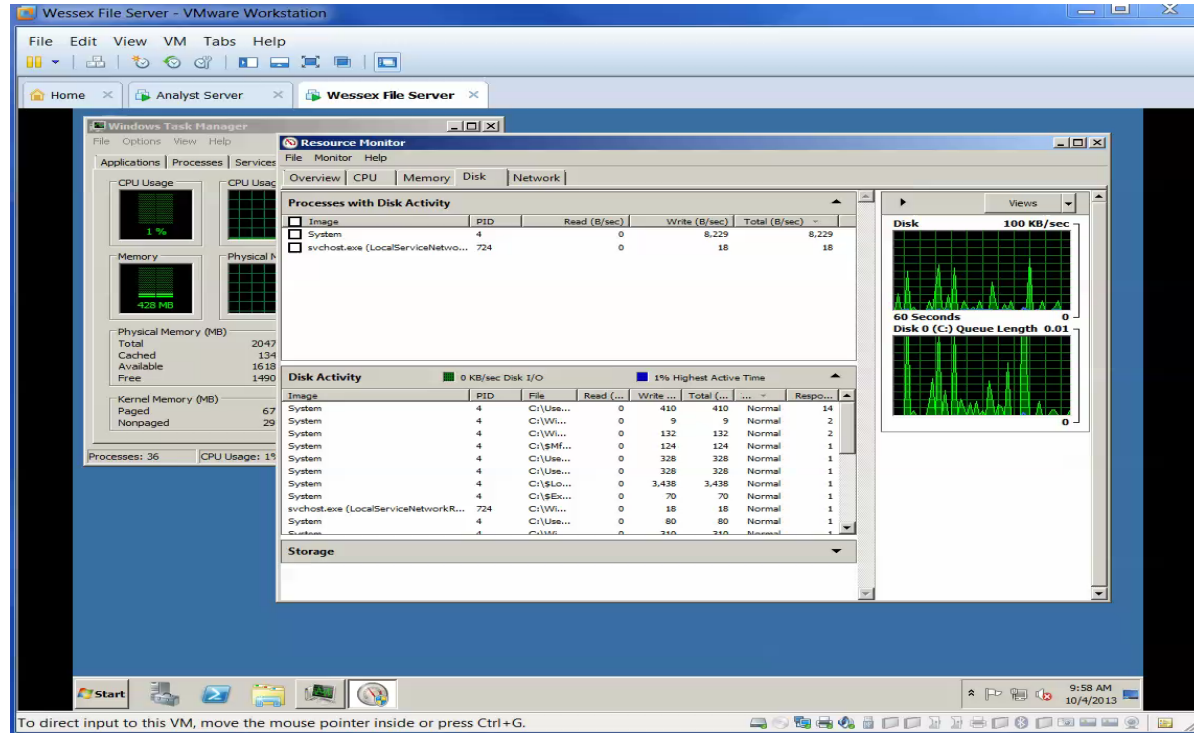


- The first step in any investigation is the search & seizure of exhibits which may contain crucial evidence!
- Decisions that you, make may result in loss of crucial evidence.
- Points to consider
 - DNA and/or fingerprints
 - Prevent tampering & preserve original condition
 - Record details & actions – paperwork!

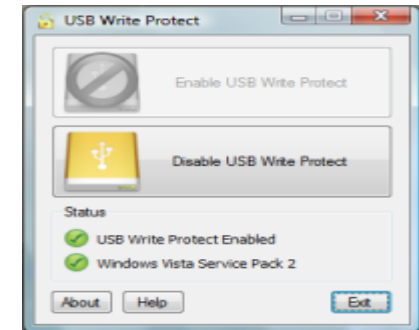


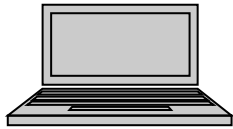
- Store in a secure location
- What is capable of storing data?
- Losing data – shutdown or not?

- 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



- 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.

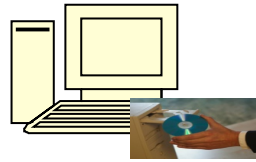




SJC1



SJC1-HD1



SJC2-DISC001



SJC3-FD001

SJC3-FD002

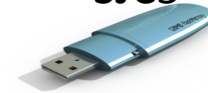
SJC3-FD003



SJC4



SJC4-SIM1



SJC5

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



TABLEAU



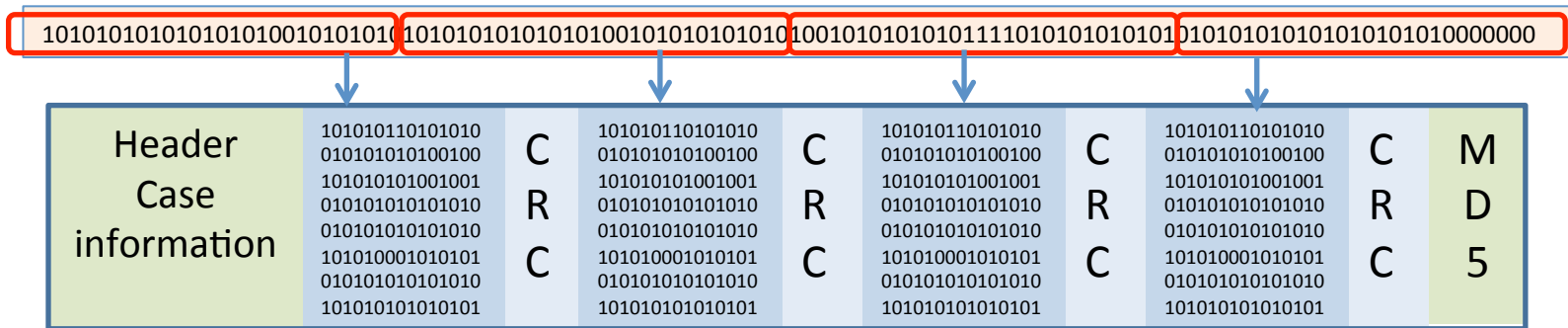
Write Blocker



Suspect Drive

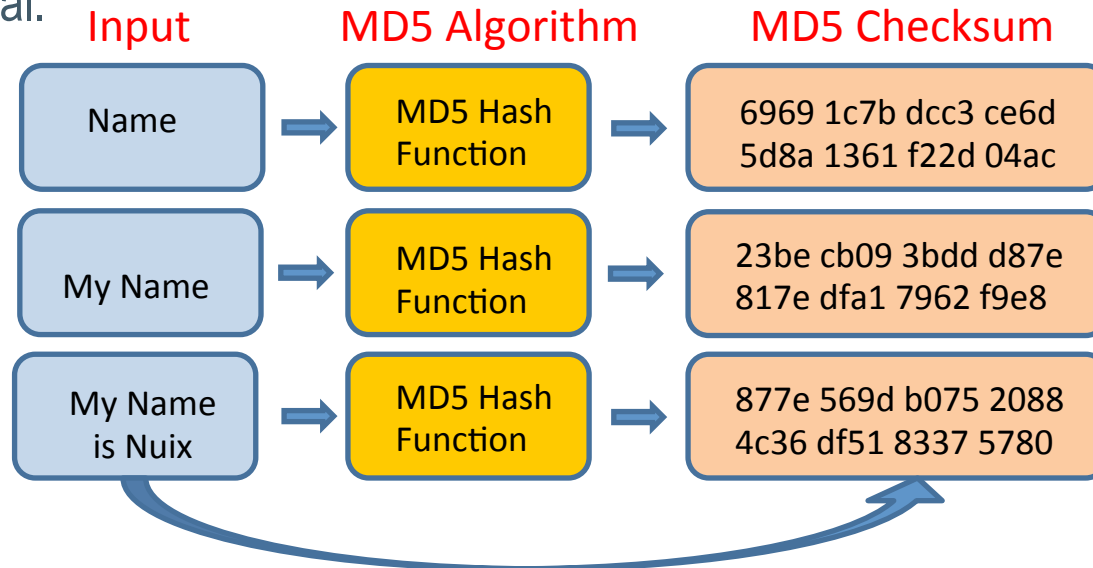


- Data is collected from the source device at binary/disk level by pre defined size and each section is checked with a CRC checksum. The whole image is then verified with an MD5 checksum



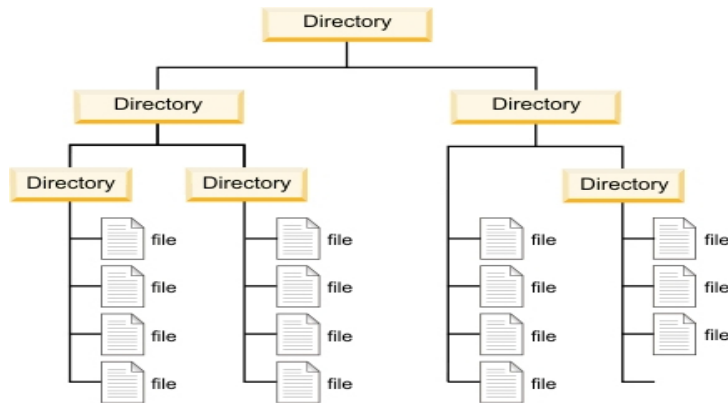
- Should any single value be change then the CRC would fail and the MD5 checksum would present a different value. Therefore verification would fail and the collection process would be undermined.

- 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.

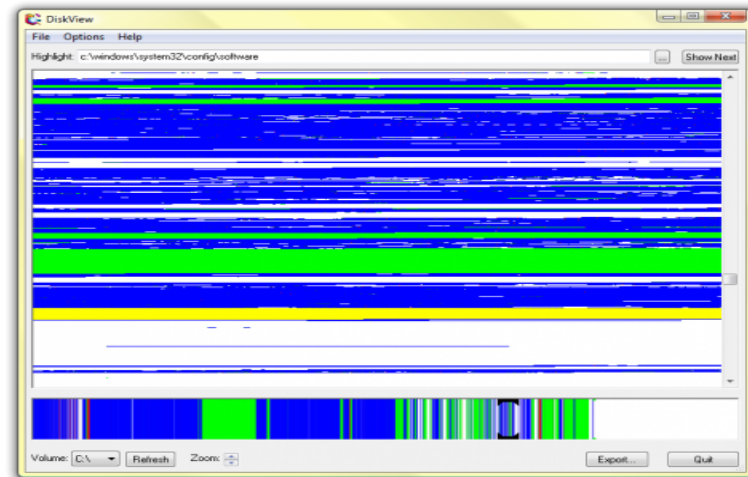


Identical data will provide identical MD5

- Investigations 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.

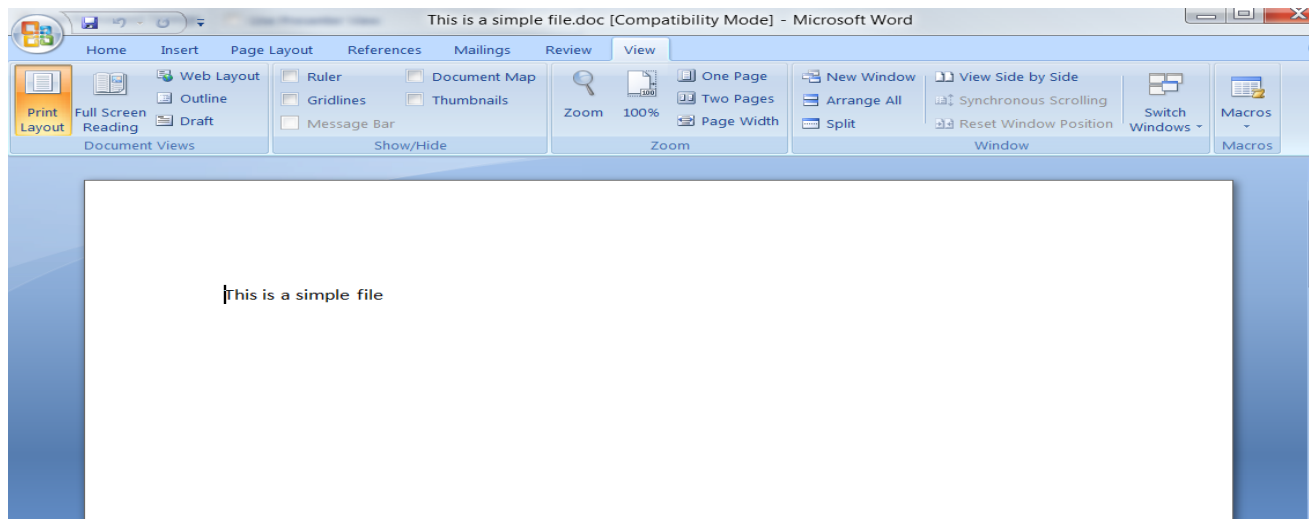


Logical application only allows an analyst to investigate live files and folders and whilst investigation is undertaken important attributes are changing



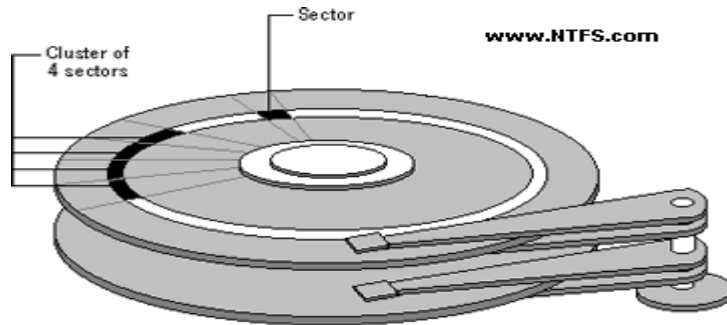
This Sysinternals utility will make a graphical map of a hard drive - we can see all clusters and view information about every single one of them. Capturing the data at disk level in a forensic container ensures no changes can be made to the data

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

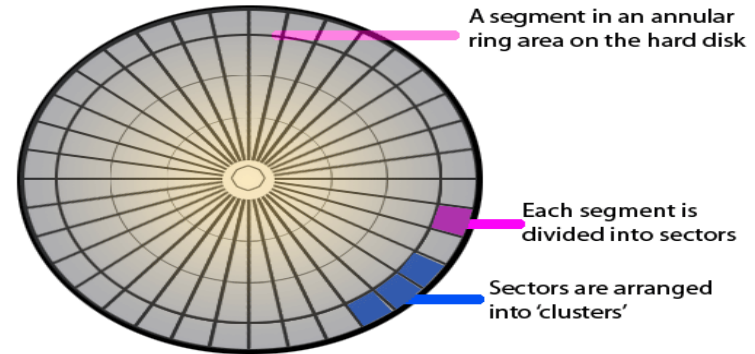


- Now lets take a look at the document from a forensic image

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



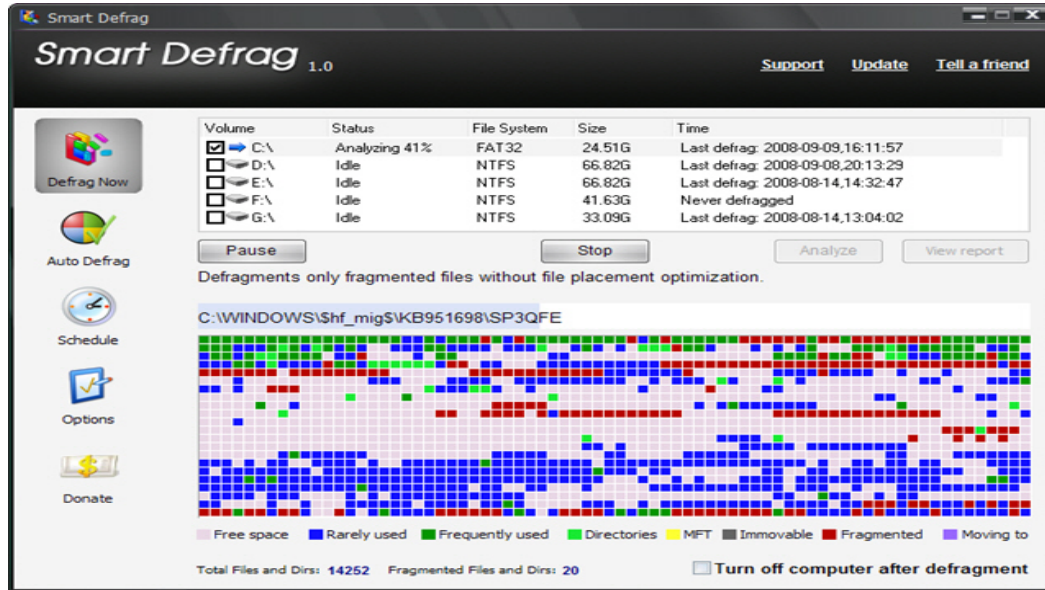
Hard disk format



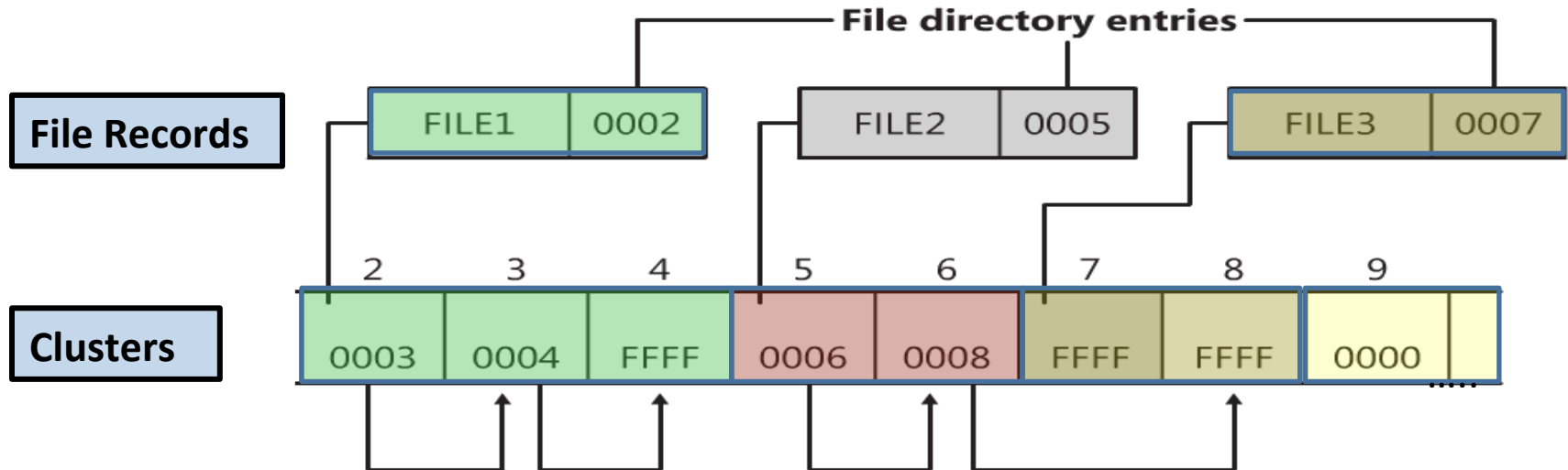
(c) www.teach-ict.com

- 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.

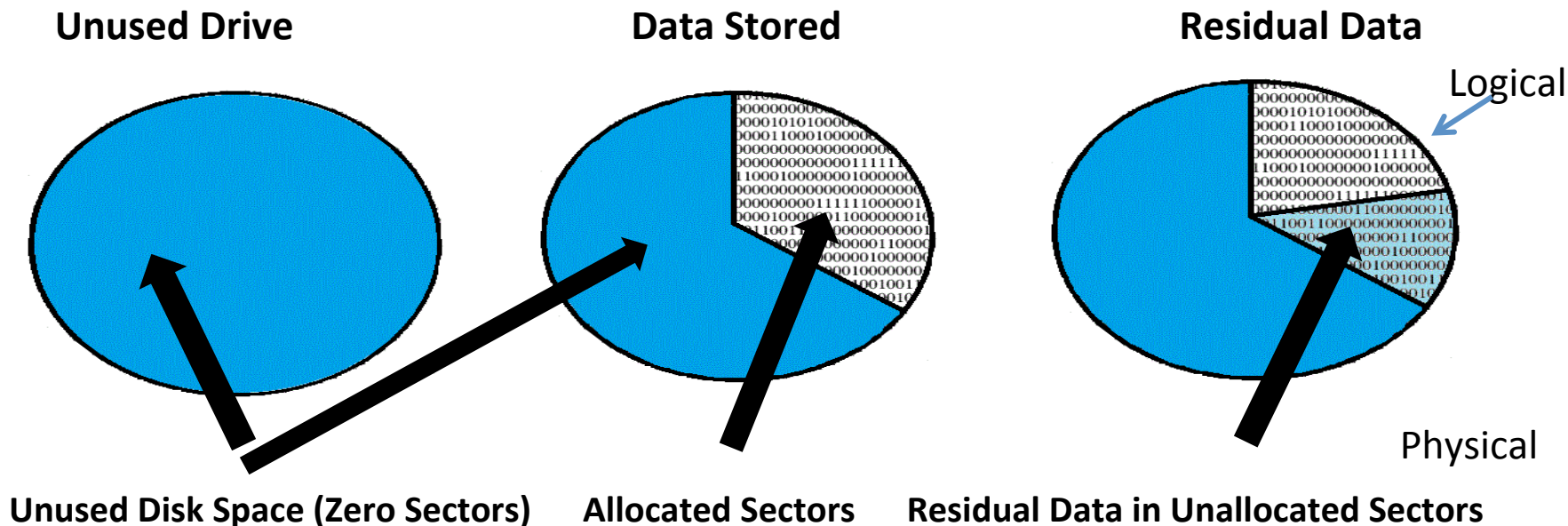


When files are erased or deleted the content of the file is not actually erased. Unless security grade file deletion software is used data from the 'erased file' remains behind in an area called unallocated storage space. The same is true concerning file slack that may have been attached to the file 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.

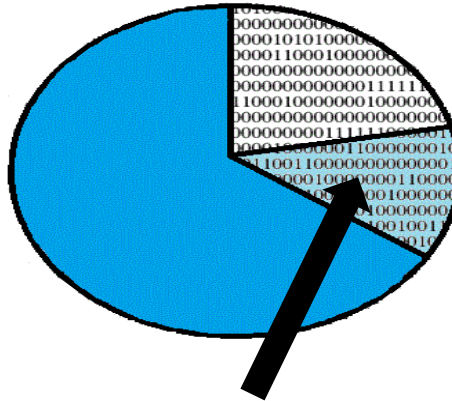
Until the first file is written to the data storage area of a computer storage device, the clusters are unallocated by the operating system. As files are created by the computer user, clusters are allocated in the file table to store the data. When the file is 'deleted' by the computer user, the clusters 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



Carve file system unallocated space

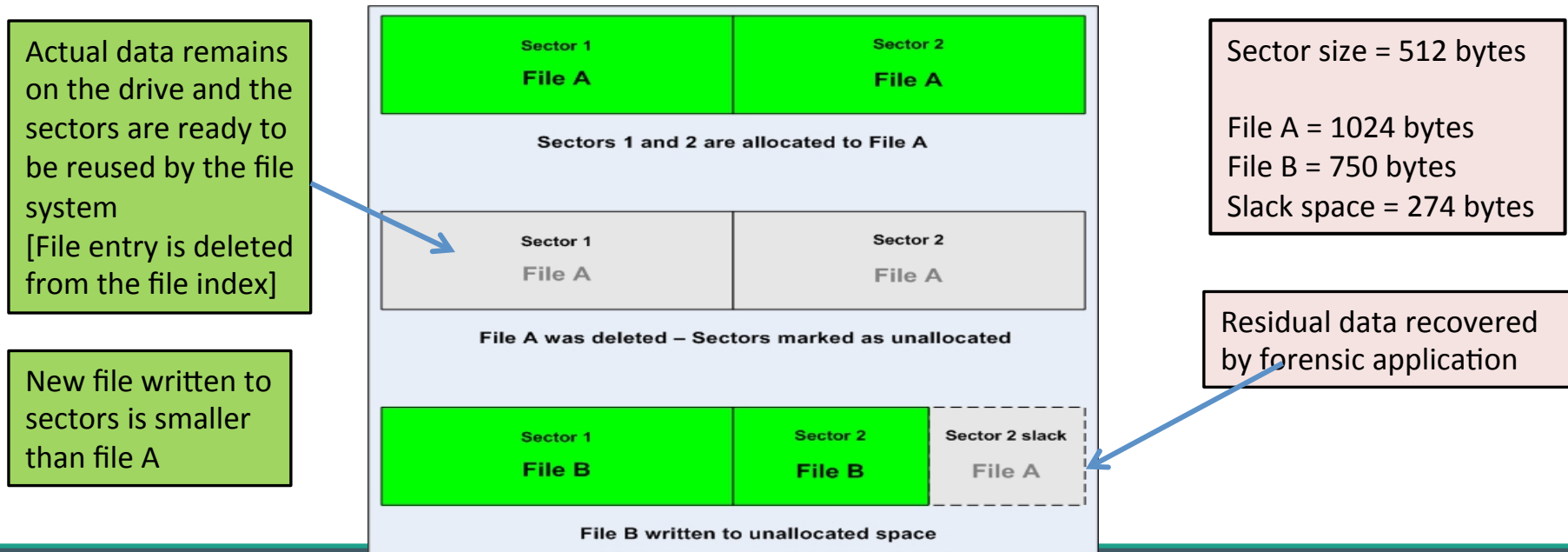
- Data carving, or file carving is a process of reading files without reference to a file system. The technique can be applied to any type of disk that stores data on sector boundaries which includes camera memory, USB devices as well as hard drives. It is based on the fact that most files start with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



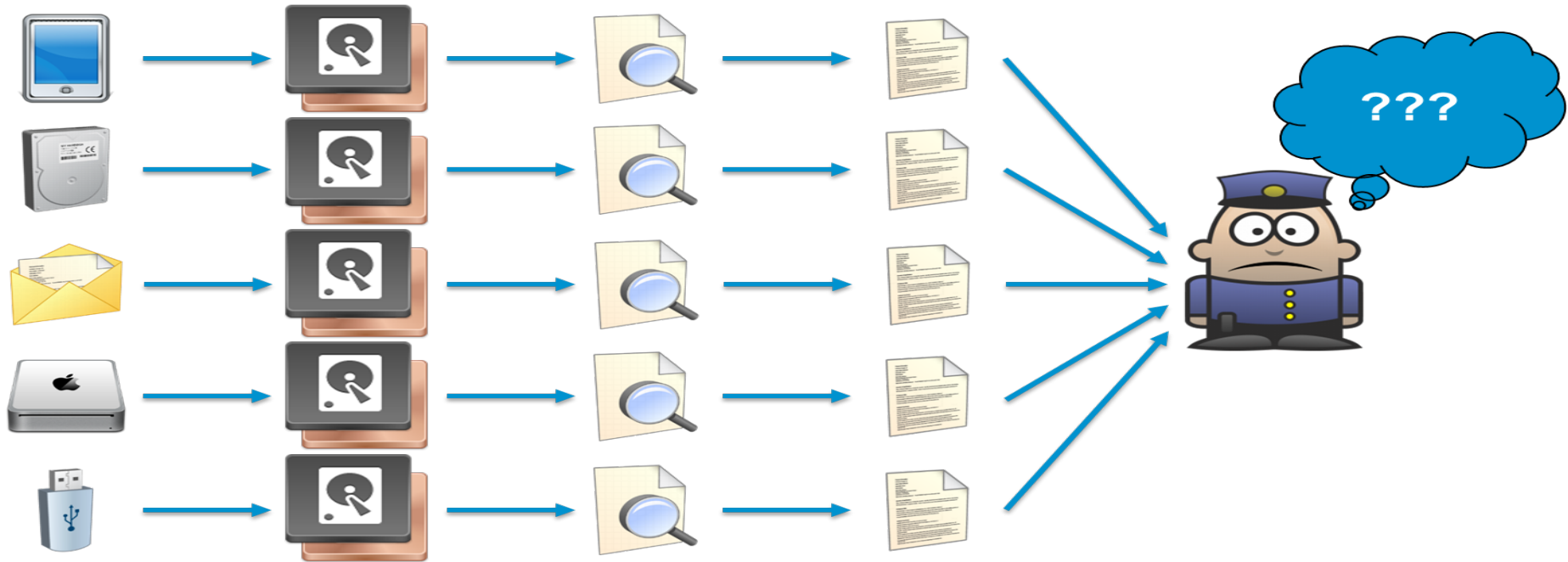
Source device

Forensic image and copy

Analyze

Report

Take action



Source device



Forensic image and copy



Analyze



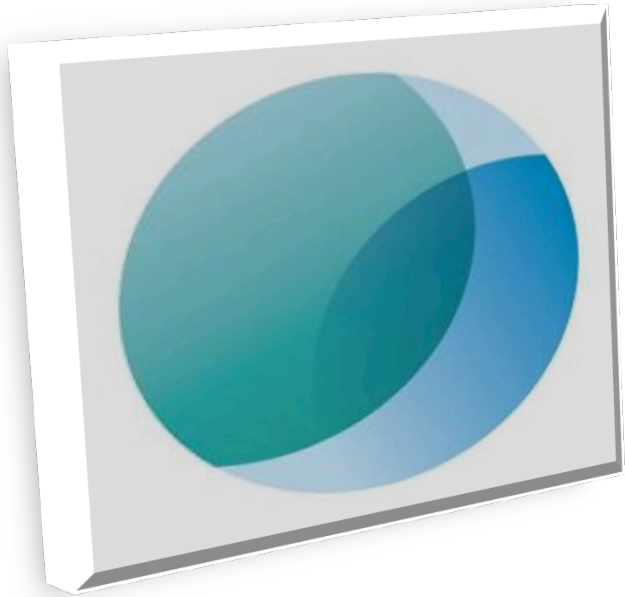
Report



Take action



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



- 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!

More power, more precision, more speed

- ❑ Speed – The ability to react
 - Upwards of 2 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 SEARCHABLE INDEXES

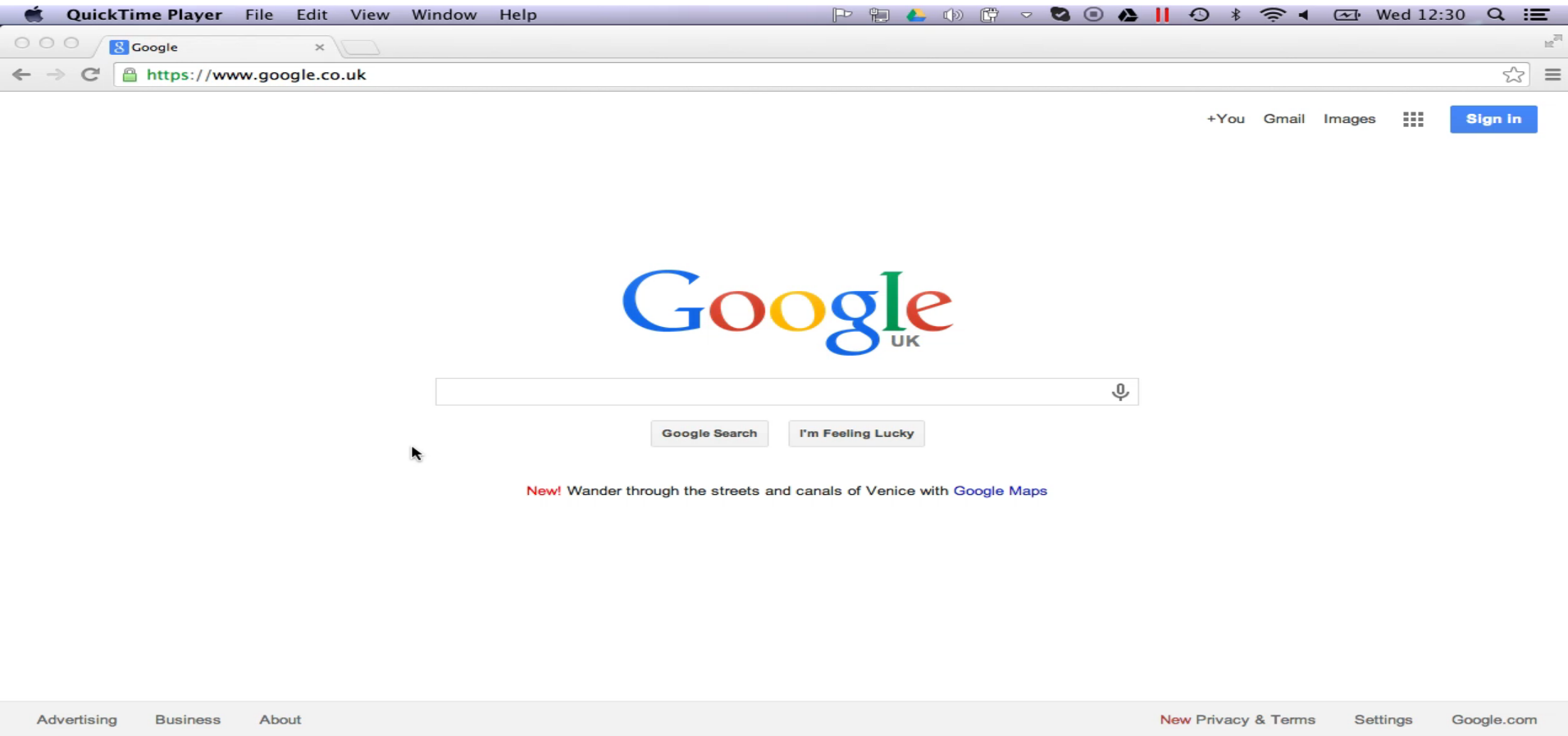
- As Nuix processes data it extracts valuable information and places the data into separate searchable indexes which can be searched against in whole or individually.
- Powerful dynamic component that allows investigators to be flexible and intuitive in the approach to data management from ECA through 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





The image shows a screenshot of a web browser window displaying the Google UK homepage. The browser's title bar reads "QuickTime Player" and the address bar shows "https://www.google.co.uk". The page features the Google logo with "UK" underneath, a search input field, and buttons for "Google Search" and "I'm Feeling Lucky". A notification banner for Google Maps is visible. The footer contains links for "Advertising", "Business", "About", "New Privacy & Terms", "Settings", and "Google.com".

QuickTime Player File Edit View Window Help

Google

https://www.google.co.uk

+You Gmail Images [Sign in](#)

Google

UK

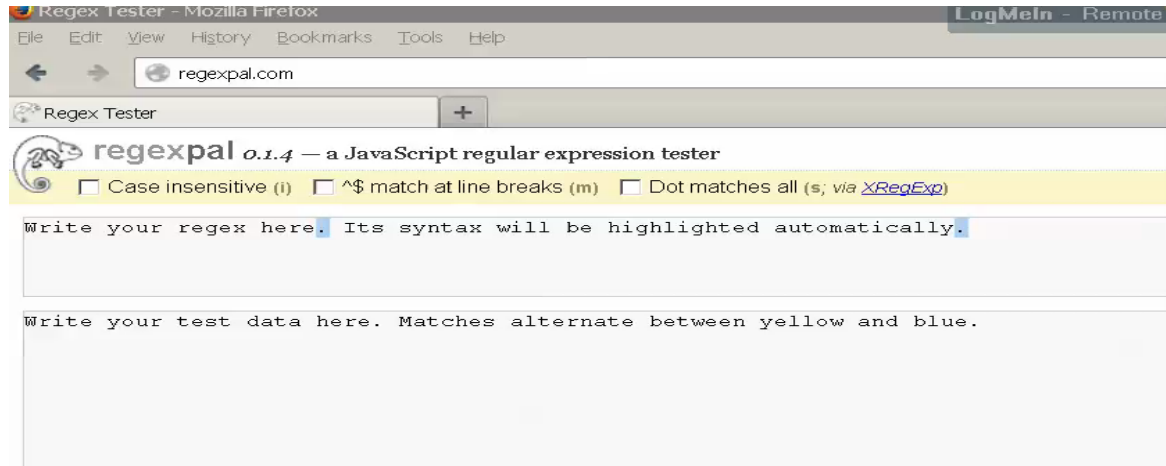
Google Search I'm Feeling Lucky

New! Wander through the streets and canals of Venice with [Google Maps](#)

Advertising Business About [New Privacy & Terms](#) [Settings](#) [Google.com](#)

- 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

- 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.

Online tester <http://regexpal.com/>

- **Typical collection of devices for investigation analysis**

- Suspect's personal possessions

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

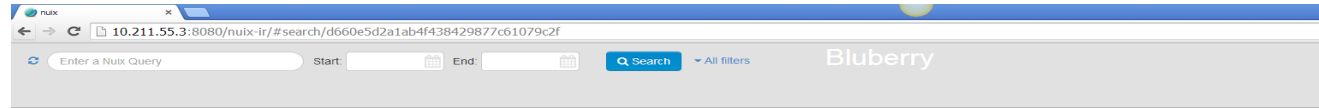
- Company/Employer data relating to suspect

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

- Extended range of supported file formats

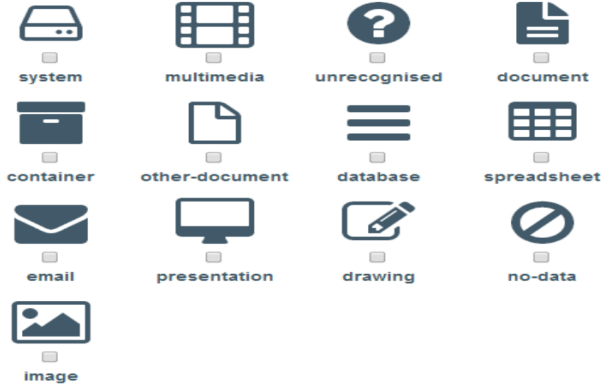
- Forensic Images
 - Cloud based email
 - HFS, HFS+ Filesystems
 - Cellebrite mobile phone images
 - XRY Mobile device files
 - Mobile phone backup files
 - Apple plist files
 - Apple iWork files types
 - Apple iPhone/iPad images (iOS)
 - SQLite files
 - Entire Exchange databases
 - Outlook mailstore containers
 - Lotus Notes mailstore container

- Nuix Web Review allows for a efficient, streamlined review of your case data through the browser interface



- A quick search pane where non-technical users can easily run keywords over the case data

Quickly search by ItemTypes or use the search options to specify your query.



- Easily apply file type filters and date range filters through the browser

- Complex search queries
- Advanced multimedia options

The screenshot displays the Nux search interface. On the left, a sidebar contains search filters: Keywords (credit card), Query Options (None, Stem, Exact, Fuzzy), Fuzz Factor (0.5), Filter By (Any), File Types (system, multimedia, unrecognized, document, container, other-document, database, spreadsheet, email), Multimedia (Skin Tone, Image Color, Image Color Range, Image Size), Languages, and Named Entities. The main area shows a table of search results with columns: File Size, File Type, File Created, File Accessed, File Modified, Item Date, and MD5 Digest. The table lists several Microsoft Outlook notes. A preview window on the right shows the content of a selected note, which is an iPad code for a Naked Wines £40 off £60 deal. The preview includes fields for Name, Path, File Type, and a detailed list of communication details such as To, From, Date, Subject, File Created, File Modified, Item Date, and MD5 Digest.

File Size	File Type	File Created	File Accessed	File Modified	Item Date	MD5 Digest
	Google Chrome History Entry				2014-03-07 12:44:13	
	Microsoft Outlook Note	2014-03-07 12:57:42		2014-03-07 12:57:52	2014-02-12 01:48:05	199d5d770b4d10978b9e66e193560ac3
	Google Chrome History Entry				2014-03-07 12:44:13	
	Microsoft Outlook Note	2014-03-07 12:57:42		2014-03-07 12:57:50	2014-02-19 11:07:15	#6b8d82d3df572f9a036ce7ed4e958f
	Microsoft Outlook Note	2014-03-07 12:43:23		2014-03-07 12:57:22	2014-02-12 01:48:05	199d5d770b4d10978b9e66e193560ac3
	Microsoft Outlook Note	2014-03-07 12:58:28		2014-03-07 12:58:29	2014-03-04 04:38:49	0e79caf0f61149c9f9e38b10f494dcee
	Microsoft Outlook Note	2014-03-07 12:43:23		2014-03-07 12:57:20	2014-02-19 11:07:15	#6b8d82d3df572f9a036ce7ed4e958f
174.147 KB	Plain Text				2014-03-07	588c0859be0998ec4145f888805c9d43

- File preview rendering
- Full metadata exposure

The screenshot displays the Nuix search interface. On the left, there are various filters and options including 'Keywords', 'Query Options', 'Fuzz Factor', 'Filter By', 'File Types', 'Multimedia', and 'Languages'. The main area shows a search results table with columns for File Size, File Type, File Created, File Accessed, File Modified, Item Date, and MD5 Digest. A red box highlights a detailed preview window for a selected file, showing its metadata and content.

File Size	File Type	File Created	File Accessed	File Modified	Item Date	MD5 Digest
	Google Chrome History Entry				2014-03-07 12:44:13	
	Microsoft Outlook Note	2014-03-07 12:57:42		2014-03-07 12:57:52	2014-02-12 01:48:05	199d5d770b4d10978b9e66e193560ac3
	Google Chrome History Entry				2014-03-07 12:44:13	
	Microsoft Outlook Note	2014-03-07 12:57:42		2014-03-07 12:57:50	2014-02-19 11:07:15	#6b8d82d3df572f9a036ce7ed4e958f
	Microsoft Outlook Note	2014-03-07 12:43:23		2014-03-07 12:57:22	2014-02-12 01:48:05	199d5d770b4d10978b9e66e193560ac3
	Microsoft Outlook Note	2014-03-07 12:58:28		2014-03-07 04:38:49	2014-03-05 04:38:49	0e79ca0f61f49c9f9e38b10f494dcee
	Microsoft Outlook Note	2014-03-07 12:43:23		2014-03-07 12:57:20	2014-02-19 11:07:15	#6b8d82d3df572f9a036ce7ed4e958f
174.147 KB	Plain Text				2014-03-07	588c0859be0998ec4145f888805c9d43

No Preview Available

Name iPad code, Naked Wines £40 off £60, hot superfast b'band deal, free eye test, 20 dating tips, free push hand cream, 31mths 0%, mortgage time bomb

Path Name /Bluberry/BluBerry User Folder/BluBerry.ad1/AppData/Local/Microsoft/Outlook/bluberry1988@gmail.com/Gmail/All Mail

File Type Microsoft Outlook Note

Additional Info Duplicate Items Family Items

To <bluberry1988@gmail.com>

From Martin's Money Tips -martinsmoneytips@moneysexperts.com-

Communication Date 2014-02-19 11:07:15

Subject iPad code, Naked Wines £40 off £60, hot superfast b'band deal, free eye test, 20 dating tips, free push hand cream, 31mths 0%, mortgage time bomb

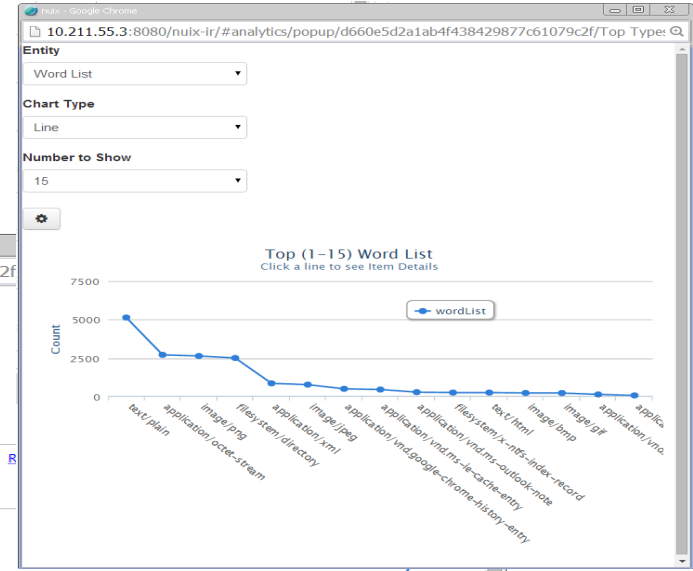
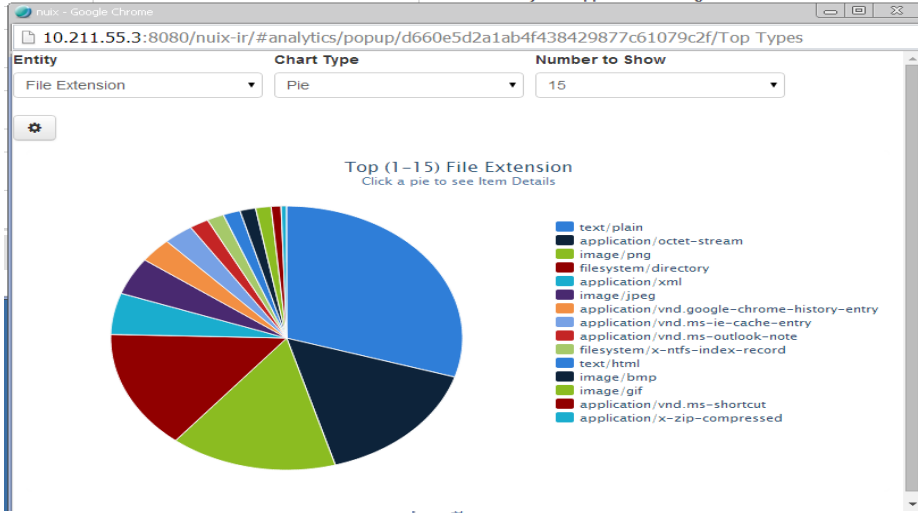
File Created 2014-03-07 12:57:42

File Modified 2014-03-07 12:57:50

Item Date 2014-02-19 11:07:15

MD5 Digest #6b8d82d3df572f9a036ce7ed4e958f

- Full range of visual analytics
- Interactive review & reporting



FIND OUT MORE



twitter.com/nuix



facebook.com/nuixsoftware



linkedin.com/company/nuix



youtube.com/nuixsoftware

www.nuix.com/investigation