

VE&S

Engineering & Services



www.eysglobal.com



CURSO DE INFORMÁTICA FORENSE

Instructor: Juan Esteban Tapias

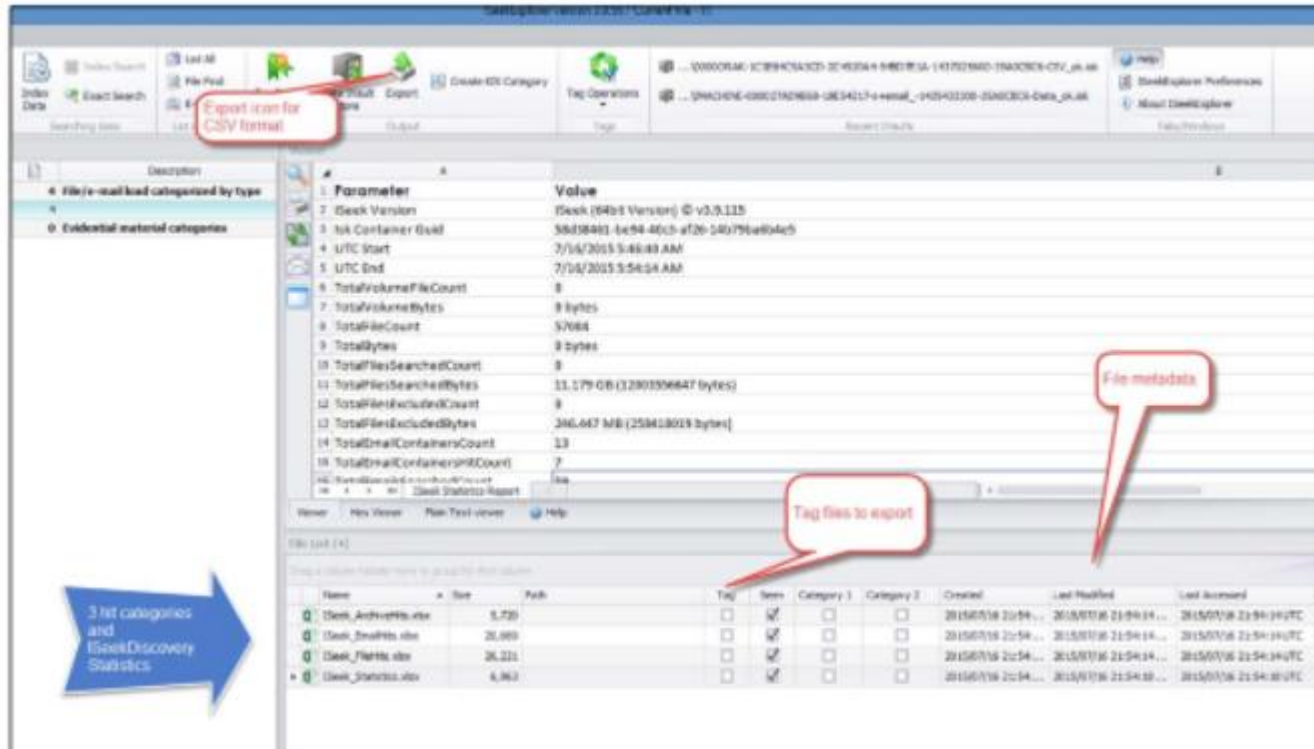


MÓDULO 3

PARTE 2

RECUPERACIÓN DE EVIDENCIA

Evidencias digitales



The screenshot shows the SleuthKit interface with several annotations:

- Export icon for CSV format:** A red callout points to the 'Export' button in the top toolbar.
- File metadata:** A red callout points to the 'Parameter' and 'Value' table.
- Tag files to export:** A red callout points to the 'Tag' column in the file list.
- 3 hit categories and 1500 Discovery Statistics:** A blue arrow points to the 'File/malware categorized by type' and 'Evidential material categories' sections on the left.

Parameter	Value
1. Sleek Version	Sleek (Sleek Version) © v1.9.115
2. Sleek Container Build	58d38401-6e94-40c3-a720-240796a04c5
3. UTC Start	7/14/2015 3:46:43 AM
4. UTC End	7/14/2015 3:54:54 AM
5. TotalVolumeFileCount	0
6. TotalVolumeBytes	0 bytes
7. TotalFileCount	57084
8. TotalBytes	0 bytes
9. TotalFilesSearchedCount	0
10. TotalFilesSearchedBytes	11,179 GB (1200350647 bytes)
11. TotalFilesExcludedCount	0
12. TotalFilesExcludedBytes	346.647 MB (35418019 bytes)
13. TotalEmailContainersCount	13
14. TotalEmailContainersSizeCount	7

Name	Size	Path	Tag	Item	Category 1	Category 2	Created	Last Modified	Last Accessed
Q Sleek_Android.exe	5,720		☐	☒	☐	☐	2015/07/16 21:54...	2015/07/16 21:54:04...	2015/07/16 21:54:04UTC
Q Sleek_Analysis.exe	20,000		☐	☒	☐	☐	2015/07/16 21:54...	2015/07/16 21:54:14...	2015/07/16 21:54:14UTC
Q Sleek_Flirt.exe	26,221		☐	☒	☐	☐	2015/07/16 21:54...	2015/07/16 21:54:14...	2015/07/16 21:54:14UTC
Q Sleek_Scheduler.exe	4,963		☐	☒	☐	☐	2015/07/16 21:54...	2015/07/16 21:54:14...	2015/07/16 21:54:14UTC

Evidencias digitales

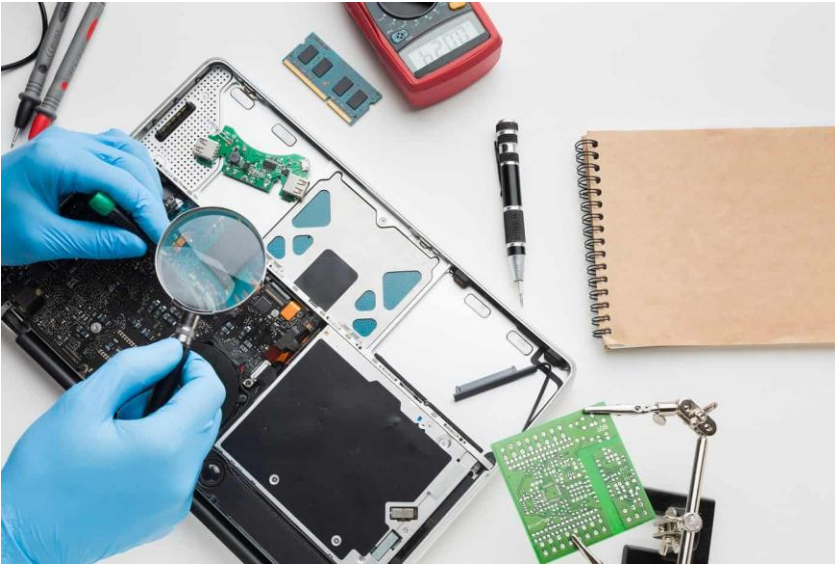
ISearchExplorer Explorer			
Categories			Description
Available FileTypes	39,629	File/e-mail load categorized by type	
Case categories	0	Evidential material categories	
Search Results	3	Previous search results	
fraud: 26/06/2015 8:14:19 PM	566	fraud	
hutchens: 26/06/2015 7:24:...	67	hutchens	
hutchens: 26/06/2015 7:32:...	1,422	hutchens	

Evidencias digitales

Los teléfonos móviles y otros dispositivos de mano no se visualizan de la misma forma que escritorios. El hardware y la interfaz de dispositivos externos, como una computadora forense son diferentes.



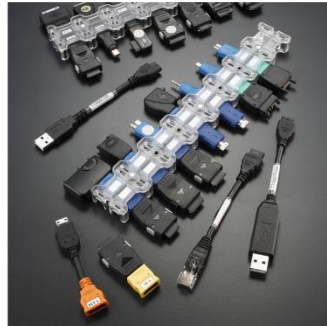
Evidencias digitales



Este software conecta la computadora del examinador al dispositivo móvil, que, a través de una serie de comandos de usuario y algunos pequeños cambios en la configuración del dispositivo, permite la extracción de datos.

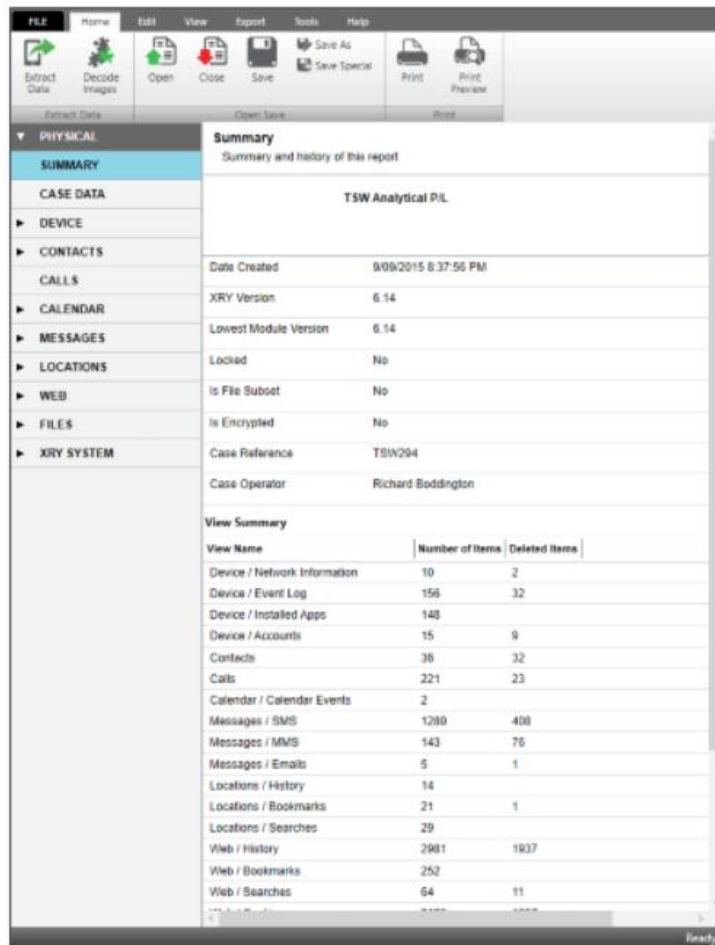
El software ofrece una extracción lógica de la básica información en el dispositivo junto con un registro de las características del dispositivo y un registro de extracción.

Evidencias digitales



Aplicaciones de software líderes, como Cellebrite y XRY de Microsystemation kits, cree un contenedor de evidencia patentado de los datos del dispositivo que se recuperan incluidos los registros de extracción.

Evidencias digitales



The screenshot shows the TSW Analytical P.L. software interface. The left sidebar contains a tree view with categories: PHYSICAL, SUMMARY (selected), CASE DATA, DEVICE, CONTACTS, CALLS, CALENDAR, MESSAGES, LOCATIONS, WEB, FILES, and XRY SYSTEM. The main window displays a 'Summary' report with the following data:

Summary		
Summary and history of this report		
TSW Analytical P.L.		
Date Created	9/9/2015 8:37:56 PM	
XRY Version	6.14	
Lowest Module Version	6.14	
Locked	No	
Is File Subset	No	
Is Encrypted	No	
Case Reference	TSW294	
Case Operator	Richard Boddington	

View Summary		
View Name	Number of Items	Deleted Items
Device / Network Information	10	2
Device / Event Log	156	32
Device / Installed Apps	148	
Device / Accounts	15	9
Contacts	38	32
Calls	221	23
Calendar / Calendar Events	2	
Messages / SMS	1280	408
Messages / MMS	143	76
Messages / Emails	5	1
Locations / History	14	
Locations / Bookmarks	21	1
Locations / Searches	29	
Web / History	2981	1837
Web / Bookmarks	252	
Web / Searches	64	11

Evidencias digitales

A diferencia de las computadoras portátiles y de escritorio, los teléfonos móviles no están completamente bloqueados para escritura protegido por software y herramientas forenses durante la recuperación de datos

