Asignatura	Datos del alumno	Fecha
Análisis forense	Actividad Grupal	10/07/2022
	Ángel Ramón Paz López Blanca Paola Toledo Martínez Braulio David Velasco Castillo	

Actividades

Actividad grupal: Fuga de información

Objetivos

El objetivo de esta actividad es conocer distintos tipos de fuga de información que se pueden dar y practicar las técnicas necesarias para su investigación.

1. ¿Cuál es el hash (SHA1) de las imágenes analizadas? ¿Coincide el valor del hash de la adquisición y el de la verificación?

IMAGEN	SHA1
cfreds_2015_data_leakage_pc.E01	afe5c9ab487bd47a8a9856b1371c2384d44fd785
cfreds_2015_data_leakage_rm#1.E01	f6bb840e98dd7c325af45539313fc3978fff812c
cfreds_2015_data_leakage_rm#2.E01	048961a85ca3eced8cc73f1517442d31d4dca0a3
cfreds_2015_data_leakage_rm#3.E01	471d3eedca9add872fc070829728 4e1960ff44f8

2. ¿Qué Sistema Operativo tenía el equipo instalado? ¿En qué fecha y hora se instaló? ¿Quién es el propietario del sistema?

Sistema Operativo: Windows 7 Ultimate Service Pack 1
Instalado: 22 de marzo del 2015 a las 14:34:26
Propietario: Informant

3. ¿Cuál es el ajuste horario del equipo?

(UTC-05:00) Eastern Time (US & Canada)

4. Enumere todas las cuentas de usuario del sistema (excepto las propias del Sistema Operativo como: Administrator, Guest, etc.)

Admin11
Informant
IteachTeam
temporary

5. ¿Quién fue el último usuario en iniciar sesión en el equipo?

Informant a las 07:06:09 fue el inicio sesión y cerro sesión a las 09:30:58

6. ¿Cuándo fue la última fecha y hora de apagado del equipo?

El 25 de marzo del 2015 a las 9:31:05

7. ¿Cuál fue la última dirección IP asignada al equipo? ¿Se asignó por DHCP?

Asignatura	Datos del alumno	Fecha
Análisis forense	Actividad Grupal Ángel Ramón Paz López Blanca Paola Toledo Martínez Braulio David Velasco Castillo	10/07/2022

IP Address: 10.11.11.129
Subnet Mask: 255.255.255.0
Name Server: 10.11.11.2
Domain: localDomain
Gateway: 10.11.11.2
DHCP Server: 10.11.11.254

8. ¿Qué aplicaciones tenía el equipo instaladas?

Google Chrome
Microsoft Office
Bonjour
Eraser
Apple Software Update
Microsoft SQL Server
Microsoft .Net Framework 4

9. ¿Qué navegadores de Internet se utilizaban?

Google Chrome
Microsoft Internet Explorer versión 9.11.9600.17691

10. ¿A qué sitios web se accedieron y en qué hora?

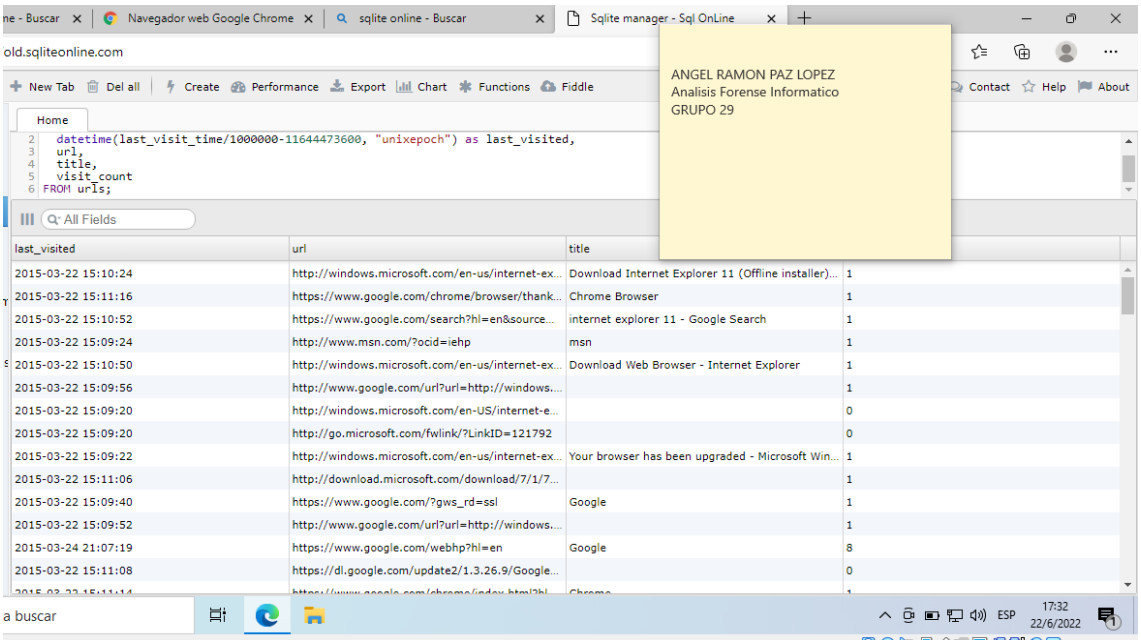
Se busco el archivo de Google Chrome: En C:\Users(nombre de usuario)\AppData\Local\Google\Chrome\User Data\Default, el archivo History, se uso Sqlite manager - Sql OnLine (sqliteonline.com) para abrir el archivo History

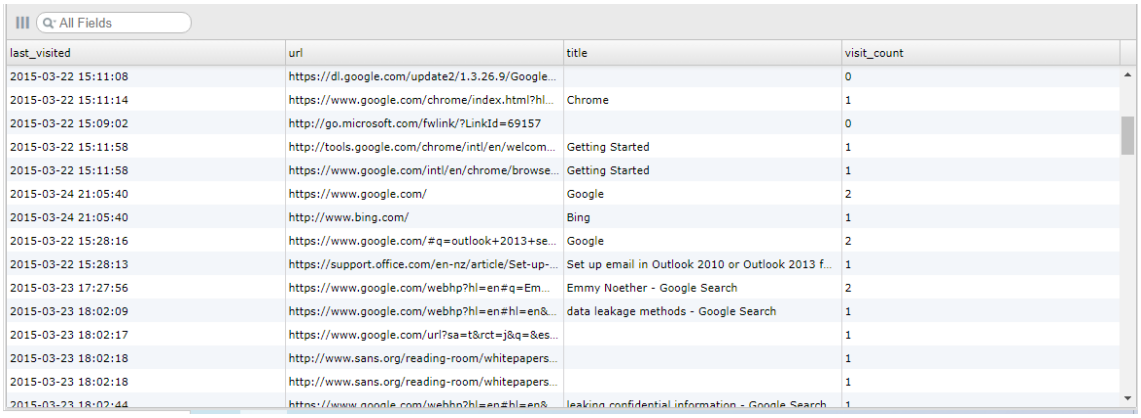
All Fields

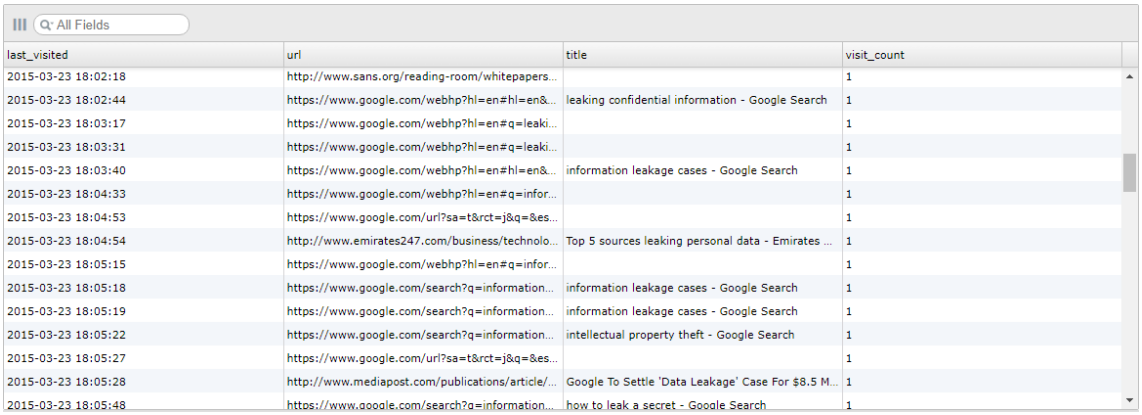
id	url	title	v...	t...	last_visit_time	h
1	http://windows.microsoft.com/en-us/internet-explorer/ie-11-worldwide-languages	Download Internet Explorer 11 (Offline installer) - Internet Explorer	1	0	13071510624000000	0
2	https://www.google.com/chrome/browser/thankyou.html?brand=CHNG&platform=win...	Chrome Browser	1	0	13071510676000000	0
3	https://www.google.com/search?hl=en&source=hp&q=internet+explorer+11&gbv=2&...	internet explorer 11 - Google Search	1	0	13071510652000000	0
4	http://www.msn.com/?ocid=iehp	msn	1	0	13071510564000000	0
5	http://windows.microsoft.com/en-us/internet-explorer/download-ie	Download Web Browser - Internet Explorer	1	0	13071510650000000	0
6	http://www.google.com/url?url=http://windows.microsoft.com/en-us/internet-explorer...		1	0	13071510596000000	0
7	http://windows.microsoft.com/en-US/internet-explorer/products/ie-8/welcome		0	0	13071510560000000	1
8	http://go.microsoft.com/fwlink/?LinkID=121792		0	0	13071510560000000	1
9	http://windows.microsoft.com/en-us/internet-explorer/ie-8-welcome	Your browser has been upgraded - Microsoft Windows	1	0	13071510562000000	0
10	http://download.microsoft.com/download/7/1/7/7179A150-F2D2-4502-9D70-4B59EA1...		1	0	13071510666000000	0
11	https://www.google.com/?gws_rd=ssl	Google	1	0	13071510580000000	0
12	http://www.google.com/url?url=http://windows.microsoft.com/en-us/internet-explorer...		1	0	13071510592000000	0
13	https://www.google.com/webhp?hl=en	Google	8	0	13071704839567844	0
14	https://dl.google.com/update2/1.3.26.9/GoogleInstaller_en.application?appguid%3D%...		0	0	13071510668000000	1

Usamos la siguiente instruccion SQL para que sea legible la fecha SELECT datetime(last_visit_time/1000000-11644473600, "unixepoch") as last_visited, url, title, visit_count FROM urls;

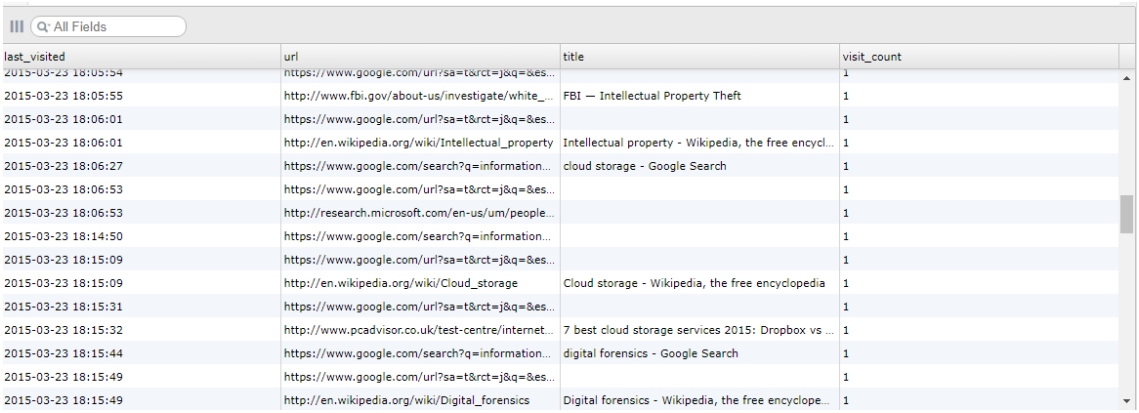
Asignatura	Datos del alumno	Fecha
Análisis forense	Actividad Grupal Ángel Ramón Paz López Blanca Paola Toledo Martínez Braulio David Velasco Castillo	10/07/2022



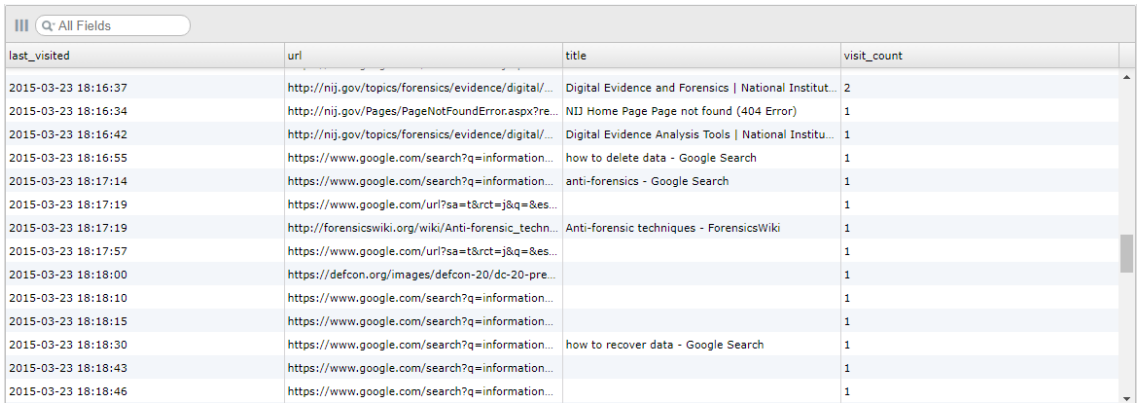




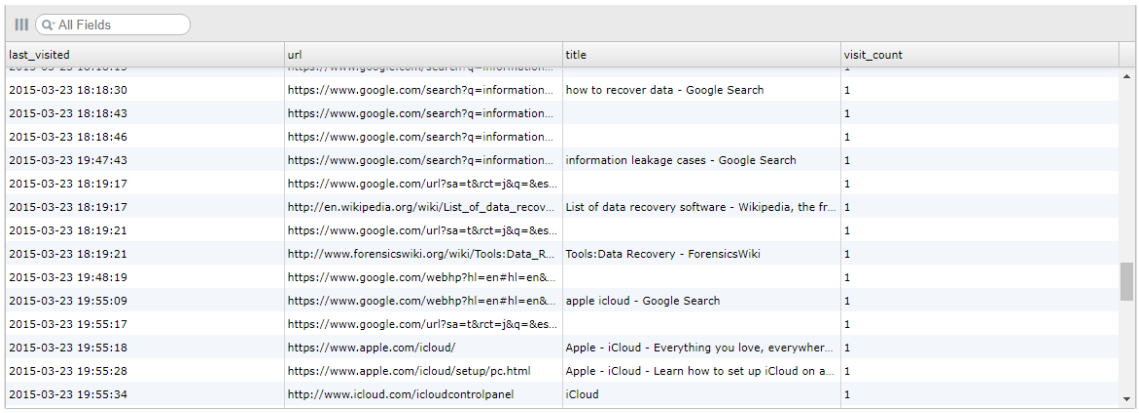
Asignatura	Datos del alumno	Fecha
Análisis forense	Actividad Grupal Ángel Ramón Paz López Blanca Paola Toledo Martínez Braulio David Velasco Castillo	10/07/2022



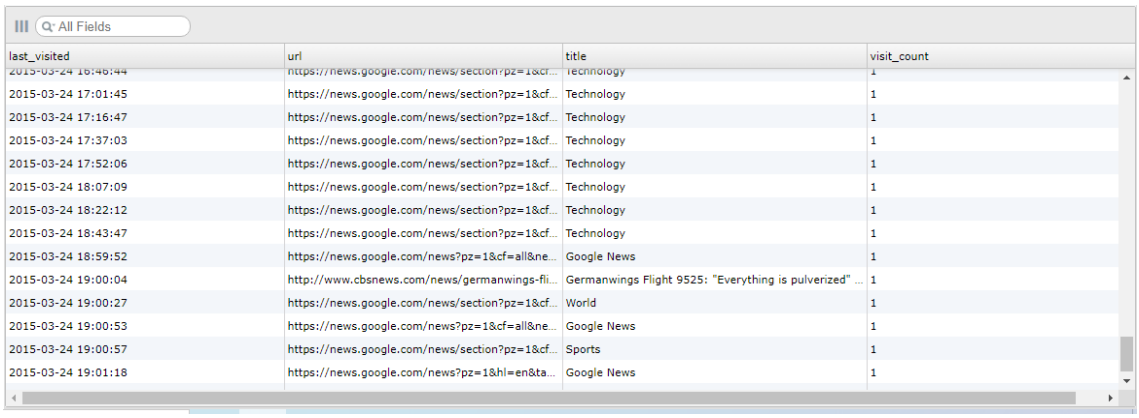
last_visited	url	title	visit_count
2015-03-23 18:05:54	https://www.google.com/url?sa=t&rct=j&q=&es...		1
2015-03-23 18:05:55	http://www.fbi.gov/about-us/investigate/white_...	FBI — Intellectual Property Theft	1
2015-03-23 18:06:01	https://www.google.com/url?sa=t&rct=j&q=&es...		1
2015-03-23 18:06:01	http://en.wikipedia.org/wiki/Intellectual_property	Intellectual property - Wikipedia, the free encycl...	1
2015-03-23 18:06:27	https://www.google.com/search?q=information...	cloud storage - Google Search	1
2015-03-23 18:06:53	https://www.google.com/url?sa=t&rct=j&q=&es...		1
2015-03-23 18:06:53	http://research.microsoft.com/en-us/um/people...		1
2015-03-23 18:14:50	https://www.google.com/search?q=information...		1
2015-03-23 18:15:09	https://www.google.com/url?sa=t&rct=j&q=&es...		1
2015-03-23 18:15:09	http://en.wikipedia.org/wiki/Cloud_storage	Cloud storage - Wikipedia, the free encyclopedia	1
2015-03-23 18:15:31	https://www.google.com/url?sa=t&rct=j&q=&es...		1
2015-03-23 18:15:32	http://www.pcadvisor.co.uk/test-centre/internet...	7 best cloud storage services 2015: Dropbox vs ...	1
2015-03-23 18:15:44	https://www.google.com/search?q=information...	digital forensics - Google Search	1
2015-03-23 18:15:49	https://www.google.com/url?sa=t&rct=j&q=&es...		1
2015-03-23 18:15:49	http://en.wikipedia.org/wiki/Digital_forensics	Digital forensics - Wikipedia, the free encyclope...	1



last_visited	url	title	visit_count
2015-03-23 18:16:37	http://nij.gov/topics/forensics/evidence/digital/...	Digital Evidence and Forensics | National Institut...	2
2015-03-23 18:16:34	http://nij.gov/Pages/PageNotFoundError.aspx?re...	NIJ Home Page Page not found (404 Error)	1
2015-03-23 18:16:42	http://nij.gov/topics/forensics/evidence/digital/...	Digital Evidence Analysis Tools | National Institu...	1
2015-03-23 18:16:55	https://www.google.com/search?q=information...	how to delete data - Google Search	1
2015-03-23 18:17:14	https://www.google.com/search?q=information...	anti-forensics - Google Search	1
2015-03-23 18:17:19	https://www.google.com/url?sa=t&rct=j&q=&es...		1
2015-03-23 18:17:19	http://forensicswiki.org/wiki/Anti-forensic_techn...	Anti-forensic techniques - ForensicsWiki	1
2015-03-23 18:17:57	https://www.google.com/url?sa=t&rct=j&q=&es...		1
2015-03-23 18:18:00	https://defcon.org/images/defcon-20/dc-20-pre...		1
2015-03-23 18:18:10	https://www.google.com/search?q=information...		1
2015-03-23 18:18:15	https://www.google.com/search?q=information...		1
2015-03-23 18:18:30	https://www.google.com/search?q=information...	how to recover data - Google Search	1
2015-03-23 18:18:43	https://www.google.com/search?q=information...		1
2015-03-23 18:18:46	https://www.google.com/search?q=information...		1



last_visited	url	title	visit_count
2015-03-23 18:18:30	https://www.google.com/search?q=information...	how to recover data - Google Search	1
2015-03-23 18:18:43	https://www.google.com/search?q=information...		1
2015-03-23 18:18:46	https://www.google.com/search?q=information...		1
2015-03-23 19:47:43	https://www.google.com/search?q=information...	information leakage cases - Google Search	1
2015-03-23 18:19:17	https://www.google.com/url?sa=t&rct=j&q=&es...		1
2015-03-23 18:19:17	http://en.wikipedia.org/wiki/List_of_data_recov...	List of data recovery software - Wikipedia, the fr...	1
2015-03-23 18:19:21	https://www.google.com/url?sa=t&rct=j&q=&es...		1
2015-03-23 18:19:21	http://www.forensicswiki.org/wiki/Tools:Data_R...	Tools:Data Recovery - ForensicsWiki	1
2015-03-23 19:48:19	https://www.google.com/webhp?hl=en#hl=en&...		1
2015-03-23 19:55:09	https://www.google.com/webhp?hl=en#hl=en&...	apple icloud - Google Search	1
2015-03-23 19:55:17	https://www.google.com/url?sa=t&rct=j&q=&es...		1
2015-03-23 19:55:18	https://www.apple.com/icloud/	Apple - iCloud - Everything you love, everywher...	1
2015-03-23 19:55:28	https://www.apple.com/icloud/setup/pc.html	Apple - iCloud - Learn how to set up iCloud on a...	1
2015-03-23 19:55:34	http://www.icloud.com/icloudcontrolpanel	iCloud	1



last_visited	url	title	visit_count
2015-03-24 16:46:44	https://news.google.com/news/section?pz=1&cf...	Technology	1
2015-03-24 17:01:45	https://news.google.com/news/section?pz=1&cf...	Technology	1
2015-03-24 17:16:47	https://news.google.com/news/section?pz=1&cf...	Technology	1
2015-03-24 17:37:03	https://news.google.com/news/section?pz=1&cf...	Technology	1
2015-03-24 17:52:06	https://news.google.com/news/section?pz=1&cf...	Technology	1
2015-03-24 18:07:09	https://news.google.com/news/section?pz=1&cf...	Technology	1
2015-03-24 18:22:12	https://news.google.com/news/section?pz=1&cf...	Technology	1
2015-03-24 18:43:47	https://news.google.com/news/section?pz=1&cf...	Technology	1
2015-03-24 18:59:52	https://news.google.com/news?pz=1&cf=all&ne...	Google News	1
2015-03-24 19:00:04	http://www.cbsnews.com/news/germanwings-fli...	Germanwings Flight 9525: "Everything is pulverized" ...	1
2015-03-24 19:00:27	https://news.google.com/news/section?pz=1&cf...	World	1
2015-03-24 19:00:53	https://news.google.com/news?pz=1&cf=all&ne...	Google News	1
2015-03-24 19:00:57	https://news.google.com/news/section?pz=1&cf...	Sports	1
2015-03-24 19:01:18	https://news.google.com/news?pz=1&hl=en&ta...	Google News	1

Asignatura	Datos del alumno	Fecha
Análisis forense	Actividad Grupal Ángel Ramón Paz López Blanca Paola Toledo Martínez Braulio David Velasco Castillo	10/07/2022

11. ¿Qué búsquedas se realizaron a través de los buscadores de Internet?

Internet Explorer 11

Download Web Browser

Information leakage cases

Intellectual propierty theft

How to leak a secret

Cloud Storage

Digital forensic

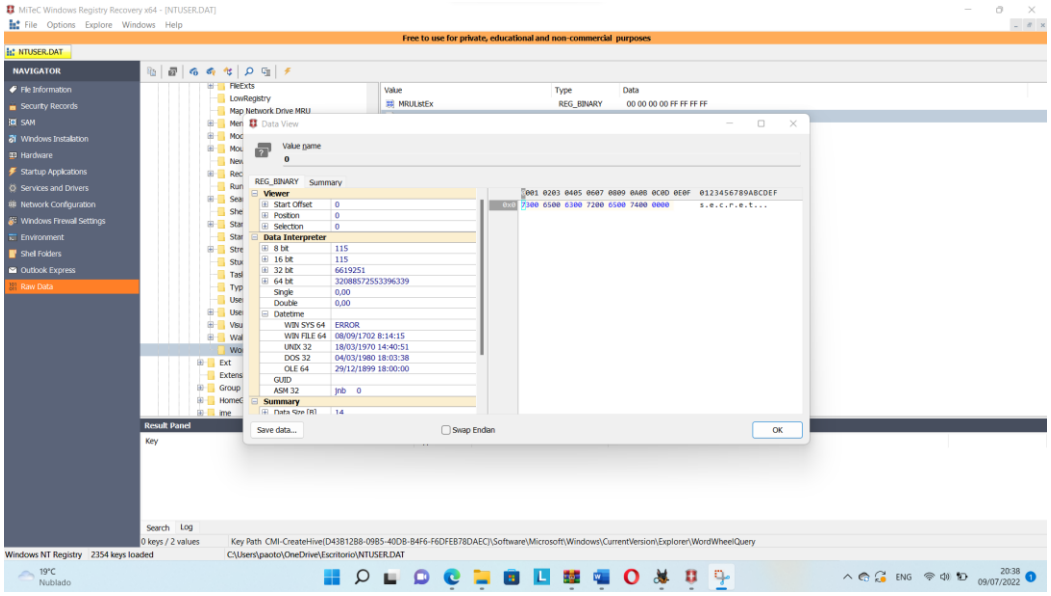
How to delete data

Anti-forensic

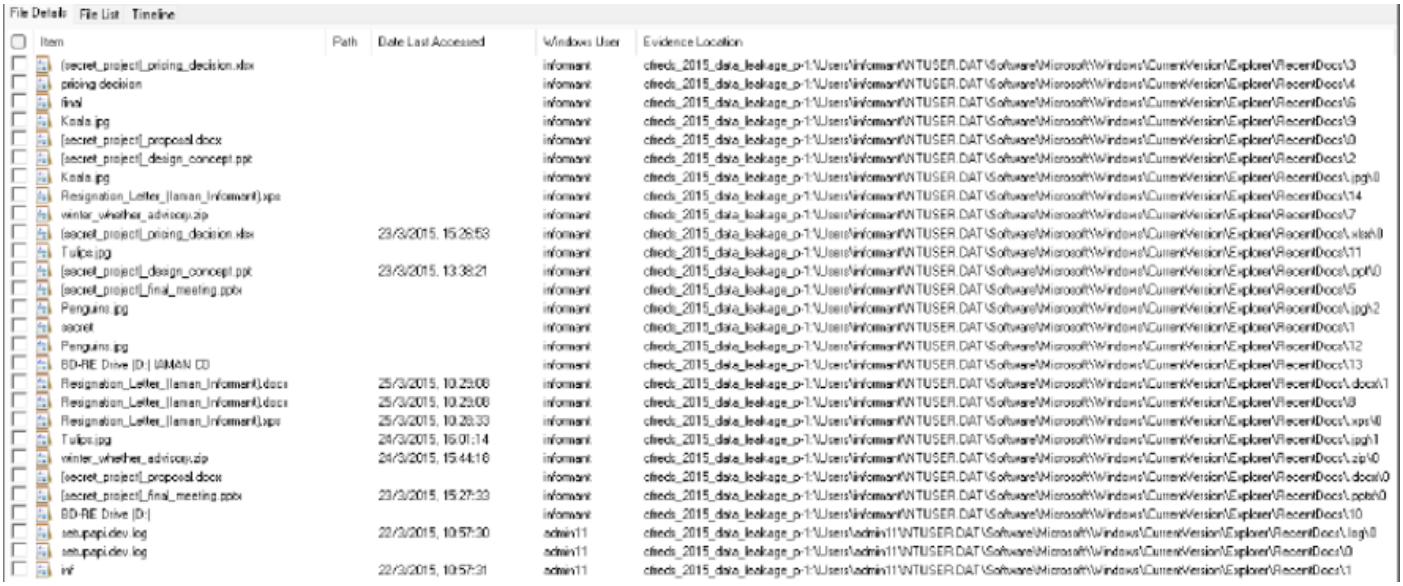
How to recover data

12. ¿Qué búsquedas realizó el usuario a través de la barra de búsqueda del explorador de Windows?

Podemos observar que por medio de la extracción DAT del user informant, la búsqueda que se estaba realizando en el explorador fue con la cadena “secret”



Asignatura	Datos del alumno	Fecha
Análisis forense	Actividad Grupal Ángel Ramón Paz López Blanca Paola Toledo Martínez Braulio David Velasco Castillo	10/07/2022

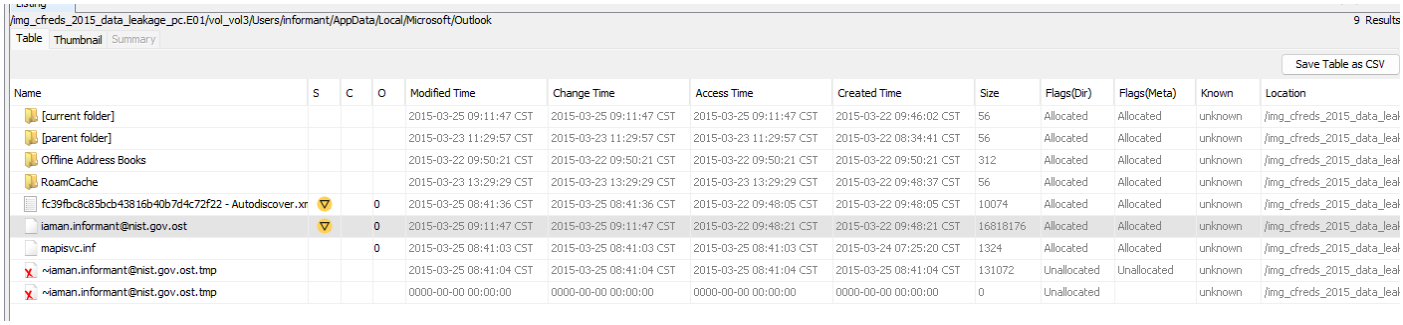


13. ¿Qué aplicación utilizaba para el envío y recepción de correos electrónicos?

Outlook 2013

14. ¿Qué cuentas de correo se encontraban configuradas?

Se identifica la cuenta iaman.informant@nist.gov configurada



15. ¿Qué dispositivos de almacenamiento externo se conectaron al equipo?

Authorized USB – DEVICE ID: 4C530012450531101593 – San Disk

IAMAN $_@ - DEVICE ID: 4C530012550531106550l – San Disk

16. ¿Cuál es la dirección IP de la unidad de red compartida de la empresa?

10.11.11.128

17. Enumere todos los archivos que se abrieron en la unidad de red de la empresa.

\\10.11.11.128\secured_drive\SecretProjectData\final\[secret_project]_final_meeting.pptx

\\10.11.11.128\secured_drive\SecretProjectData\final\[secret_project]_final_meeting.pptx

\\10.11.11.128\secured_drive\Secret Project Data\final

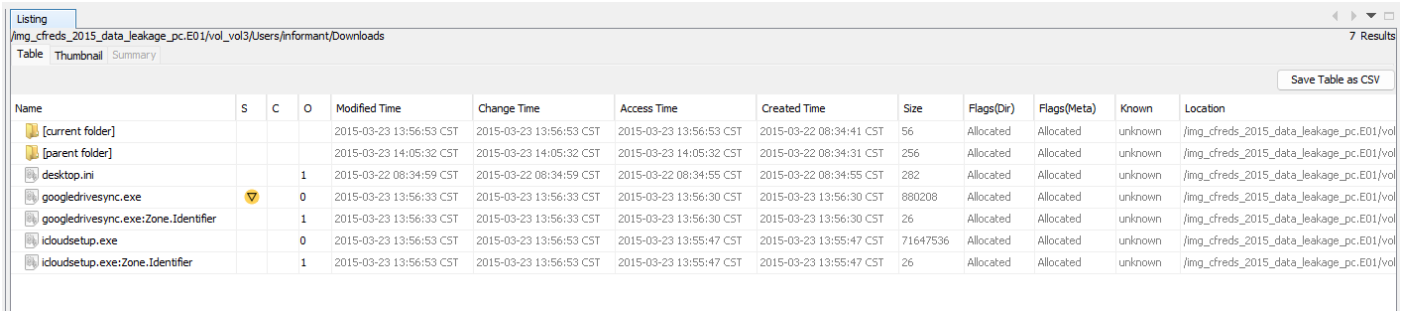
\\10.11.11.128\SECURED_DRIVE\Secret Project Data\pricing decision\(secret_project)_pricing_decision.xlsx

\\10.11.11.128\SECURED_DRIVE\Secret Project Data\pricing decision\(secret_project)_pricing_decision.xlsx

\\10.11.11.128\SECURED_DRIVE\Secret Project Data\pricing decision

18. Encuentre en el PC rastros relacionados con los servicios en la nube (Nombre del servicio, archivos de registro...)

Se encuentran registros de servicios como Google Drive y ICloud


Listing

/img_cfreds_2015_data_leakage_pc.E01/vol_vol3/Users/informant/Downloads

7 Results

Table | Thumbnail | Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2015-03-23 13:56:53 CST	2015-03-23 13:56:53 CST	2015-03-23 13:56:53 CST	2015-03-22 08:34:41 CST	56	Allocated	Allocated	unknown	/img_cfreds_2015_data_leakage_pc.E01/vol
[parent folder]				2015-03-23 14:05:32 CST	2015-03-23 14:05:32 CST	2015-03-23 14:05:32 CST	2015-03-22 08:34:31 CST	256	Allocated	Allocated	unknown	/img_cfreds_2015_data_leakage_pc.E01/vol
desktop.ini			1	2015-03-22 08:34:59 CST	2015-03-22 08:34:59 CST	2015-03-22 08:34:55 CST	2015-03-22 08:34:55 CST	282	Allocated	Allocated	unknown	/img_cfreds_2015_data_leakage_pc.E01/vol
googledrivesync.exe	▽		0	2015-03-23 13:56:33 CST	2015-03-23 13:56:33 CST	2015-03-23 13:56:30 CST	2015-03-23 13:56:30 CST	880208	Allocated	Allocated	unknown	/img_cfreds_2015_data_leakage_pc.E01/vol
googledrivesync.exe:Zone.Identifier			1	2015-03-23 13:56:33 CST	2015-03-23 13:56:33 CST	2015-03-23 13:56:30 CST	2015-03-23 13:56:30 CST	26	Allocated	Allocated	unknown	/img_cfreds_2015_data_leakage_pc.E01/vol
icloudsetup.exe			0	2015-03-23 13:56:53 CST	2015-03-23 13:56:53 CST	2015-03-23 13:55:47 CST	2015-03-23 13:55:47 CST	71647536	Allocated	Allocated	unknown	/img_cfreds_2015_data_leakage_pc.E01/vol
icloudsetup.exe:Zone.Identifier			1	2015-03-23 13:56:53 CST	2015-03-23 13:56:53 CST	2015-03-23 13:55:47 CST	2015-03-23 13:55:47 CST	26	Allocated	Allocated	unknown	/img_cfreds_2015_data_leakage_pc.E01/vol

19. ¿Qué archivos se eliminaron de Google Drive? (Sugerencia: Busca un archivo de registro de transacciones de Google Drive)

C:\\Users\\informant\\Google Drive', name=u'happy_holiday.jpg

C:\\Users\\informant\\Google Drive\\do_u_wanna_build_a_snow_man.mp3

20. Identificar la información de la cuenta utilizada para sincronizar Google Drive

2015/03/23 16:05:32,279 -0400 INFO pid=2576 2828:LaunchThreads common.service.user:64 Initializing User instance with new credentials.

iaman.informant.personal@gmail.com

Las credenciales son iaman.informant.personal@gmail.com

21. ¿Qué *software* se utilizó para grabar el CD?

DVD Maker

22. ¿Cuándo grabó el sospechoso el CD?

2015.03.25 04:18:12 CST

23. Identifique todas las marcas de tiempo relacionadas con un archivo de renuncia (en formato DOCX) en el escritorio de Windows.

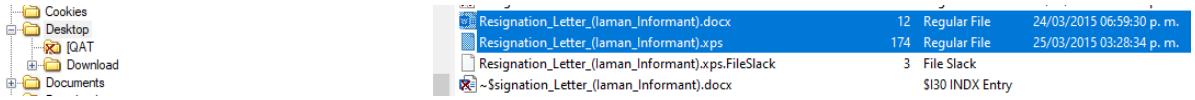
El archivo de renuncia se llama Resignation_Letter_(Iaman_Informant).docx

Creado: 24/03/2015 06:48:40 p. m.

Acceso: 24/03/2015 06:59:30 p. m.

Asignatura	Datos del alumno	Fecha
Análisis forense	Actividad Grupal	10/07/2022
	Ángel Ramón Paz López Blanca Paola Toledo Martínez Braulio David Velasco Castillo	

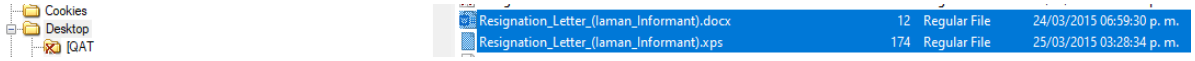
Modificado: 24/03/2015 06:59:30 p. m.



24. ¿Cómo y cuándo imprimió el sospechoso un archivo de renuncia?

En misma ubicación de archivo **Resignation_Letter_(Iaman_Informant).docx** se encuentra el archivo Resignation_Letter_(Iaman_Informant).xps, que corresponde a la impresora por defecto Microsoft XPS Document Writer.

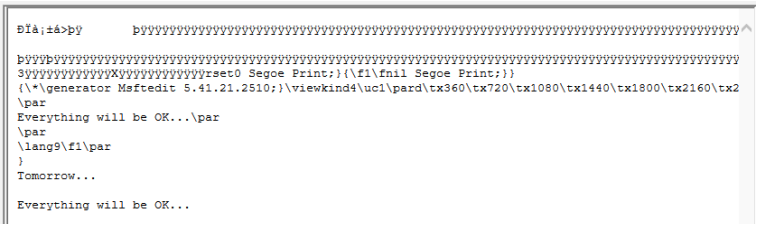
Creado: 24/03/2015 03:28:33 p. m.



25. ¿Dónde se encuentran los archivos de la aplicación Sticky Note (Notas)? Identifique las notas almacenadas.

C:\Users\Informant\AppData\Roaming\Microsoft\Sticky Notes\StickyNotes.snt

Sticky Notes encontradas:



26. ¿Qué acciones se llevaron a cabo para los complicar el análisis forense del equipo el día 25 de marzo de 2015?

Se identifica la descarga e instalación de software que permite el borrado de información para evitar un análisis forense.

CCleaner

Eraser

27. Recupere los archivos borrados de los USB. ¿Hay algún archivo de interés?

[secret_project]_design_concept.ppt

[secret_project]_proposal.docx

28. ¿Qué archivos se copiaron el PC a los USB?

Se realiza la revisión de los archivos detectados, sin encontrar coincidencias de archivos existentes en el PC, por lo que podemos decir que no se copió información a la USB.

29. Recupere los archivos ocultos del CD ¿Hay algún archivo de interés?

f0084376_secret_project_market_shares.xls

Asignatura	Datos del alumno	Fecha
Análisis forense	Actividad Grupal	10/07/2022
	Ángel Ramón Paz López Blanca Paola Toledo Martínez Braulio David Velasco Castillo	

f0061720_secret_project_price_analysis_2.xls

f0199536_secret_project_technical_review_3.doc

f0104472_secret_project_progress_3.doc

f0204148_secret_project_technical_review_3.ppt

f0001308_secret_project_revised_points.ppt

30. Examine la papelera de reciclaje del PC ¿Hay algún archivo de interés?

PATH	TIME DELETED
Chrysanthemum.jpg	2015/03/24 15:11:42
Desert.jpg	2015/03/24 15:11:42
Hydrangeas.jpg	2015/03/24 15:11:42
IE11-Windows6.1-x64-en-us.exe	2015/03/24 15:11:42
Jellyfish.jpg	2015/03/24 15:11:42
Koala.jpg	2015/03/24 15:11:42
Lighthouse.jpg	2015/03/24 15:11:42
Penguins.jpg	2015/03/24 15:11:42
Tulips.jpg	2015/03/24 15:11:42
desktop.ini	2015/03/24 15:11:42

Entrega de la actividad grupal

Indica en la actividad el nombre de todos los componentes del equipo y cumplimenta la siguiente tabla de valoración individual:

	Sí	No	A veces
Todos los miembros se han integrado al trabajo del grupo	X		
Todos los miembros participan activamente	X		
Todos los miembros respetan otras ideas aportadas	X		
Todos los miembros participan en la elaboración del informe	X		
Me he preocupado por realizar un trabajo cooperativo con mis compañeros	X		
Señala si consideras que algún aspecto del trabajo en grupo no ha sido adecuado		X	