Universidad de Alcalá

Seguridad en Sistemas Distribuidos:
Forense

Carlos Javier Hellín Asensio

carlos.hellin@edu.uah.es

Grado en Ingeniería Informática
Curso: 2021-2022

Contenido

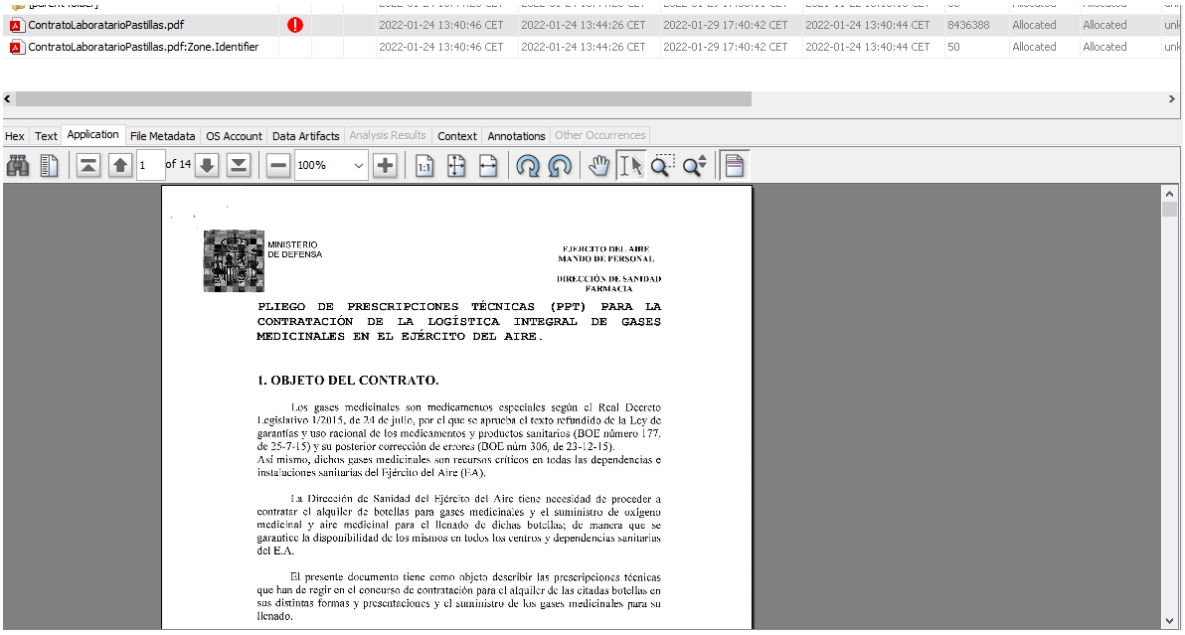
ARCHIVO DD_JF.E01

Archivo de copia de un disco duro con SO Windows, ¿Por dónde se debe empezar a buscar?

Se podría empezar a buscar en la carpeta del usuario, donde normalmente están los documentos, descargas, etc. a partir de ahí habría que mirar en otros sitios como en la papelera o archivos eliminados.

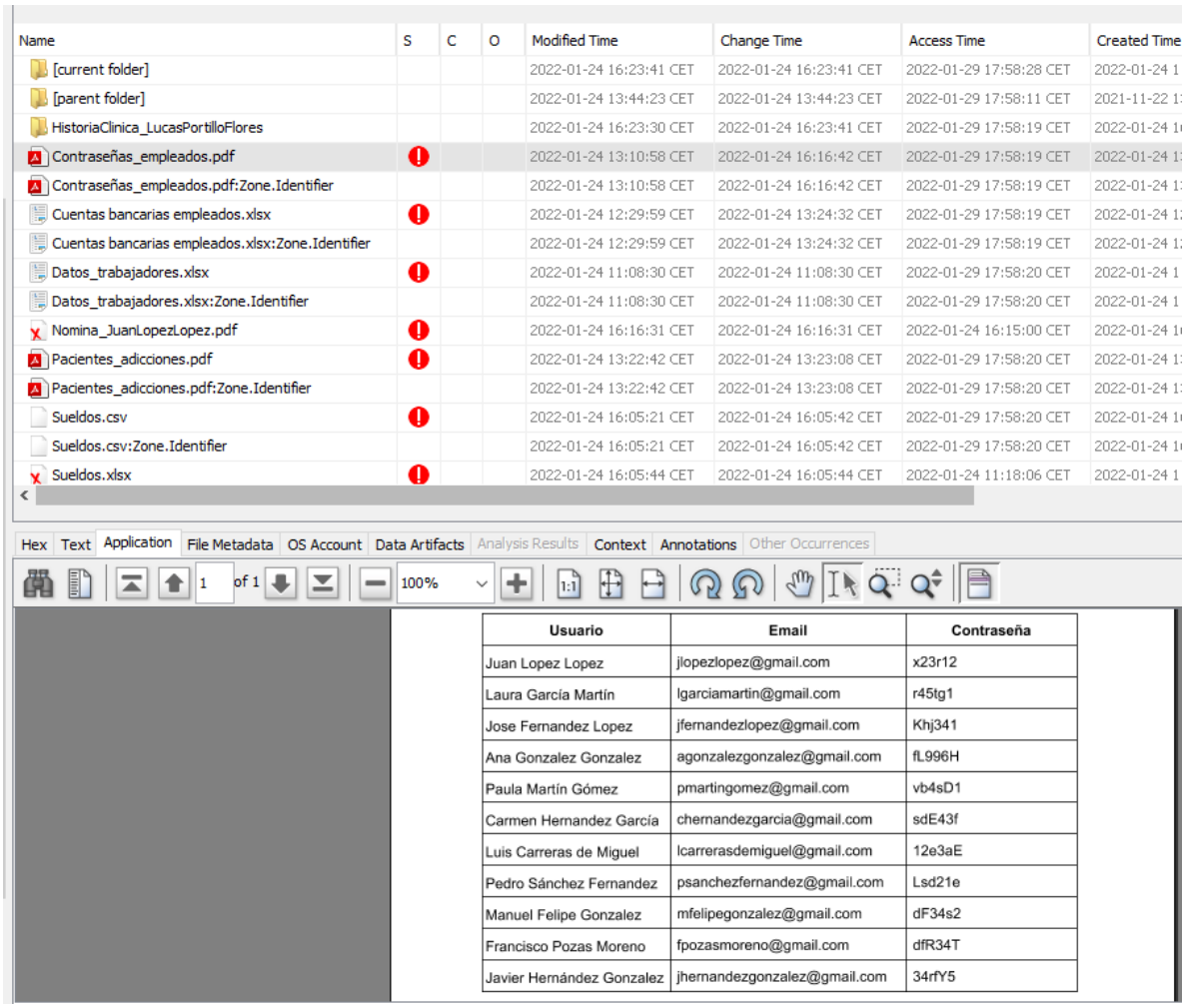
Por ejemplo, en Users/jfgomez/Documents se encuentra lo siguiente:

Contratos con clientes/ContratoLaboratorioPastillas.pdf:



Buscar alguna carpeta que pueda ser sospechosa con posible información relevante para el caso.

Una carpeta sospechosa podría ser la de “Datos confidenciales” que se encuentra en la siguiente ruta: Users/jfgomez/Documents/Datos confidenciales



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2022-01-24 16:23:41 CET	2022-01-24 16:23:41 CET	2022-01-29 17:58:28 CET	2022-01-24 1
[parent folder]				2022-01-24 13:44:23 CET	2022-01-24 13:44:23 CET	2022-01-29 17:58:11 CET	2021-11-22 1
HistoriaClinica_LucasPortilloFlores				2022-01-24 16:23:30 CET	2022-01-24 16:23:41 CET	2022-01-29 17:58:19 CET	2022-01-24 1
Contraseñas_empleados.pdf	!			2022-01-24 13:10:58 CET	2022-01-24 16:16:42 CET	2022-01-29 17:58:19 CET	2022-01-24 1
Contraseñas_empleados.pdf:Zone.Identifier				2022-01-24 13:10:58 CET	2022-01-24 16:16:42 CET	2022-01-29 17:58:19 CET	2022-01-24 1
Cuentas bancarias empleados.xlsx	!			2022-01-24 12:29:59 CET	2022-01-24 13:24:32 CET	2022-01-29 17:58:19 CET	2022-01-24 1
Cuentas bancarias empleados.xlsx:Zone.Identifier				2022-01-24 12:29:59 CET	2022-01-24 13:24:32 CET	2022-01-29 17:58:19 CET	2022-01-24 1
Datos_trabajadores.xlsx	!			2022-01-24 11:08:30 CET	2022-01-24 11:08:30 CET	2022-01-29 17:58:20 CET	2022-01-24 1
Datos_trabajadores.xlsx:Zone.Identifier				2022-01-24 11:08:30 CET	2022-01-24 11:08:30 CET	2022-01-29 17:58:20 CET	2022-01-24 1
Nomina_JuanLopezLopez.pdf	!			2022-01-24 16:16:31 CET	2022-01-24 16:16:31 CET	2022-01-24 16:15:00 CET	2022-01-24 1
Pacientes_adicciones.pdf	!			2022-01-24 13:22:42 CET	2022-01-24 13:23:08 CET	2022-01-29 17:58:20 CET	2022-01-24 1
Pacientes_adicciones.pdf:Zone.Identifier				2022-01-24 13:22:42 CET	2022-01-24 13:23:08 CET	2022-01-29 17:58:20 CET	2022-01-24 1
Sueldos.csv	!			2022-01-24 16:05:21 CET	2022-01-24 16:05:42 CET	2022-01-29 17:58:20 CET	2022-01-24 1
Sueldos.csv:Zone.Identifier				2022-01-24 16:05:21 CET	2022-01-24 16:05:42 CET	2022-01-29 17:58:20 CET	2022-01-24 1
Sueldos.xlsx	!			2022-01-24 16:05:44 CET	2022-01-24 16:05:44 CET	2022-01-24 11:18:06 CET	2022-01-24 1

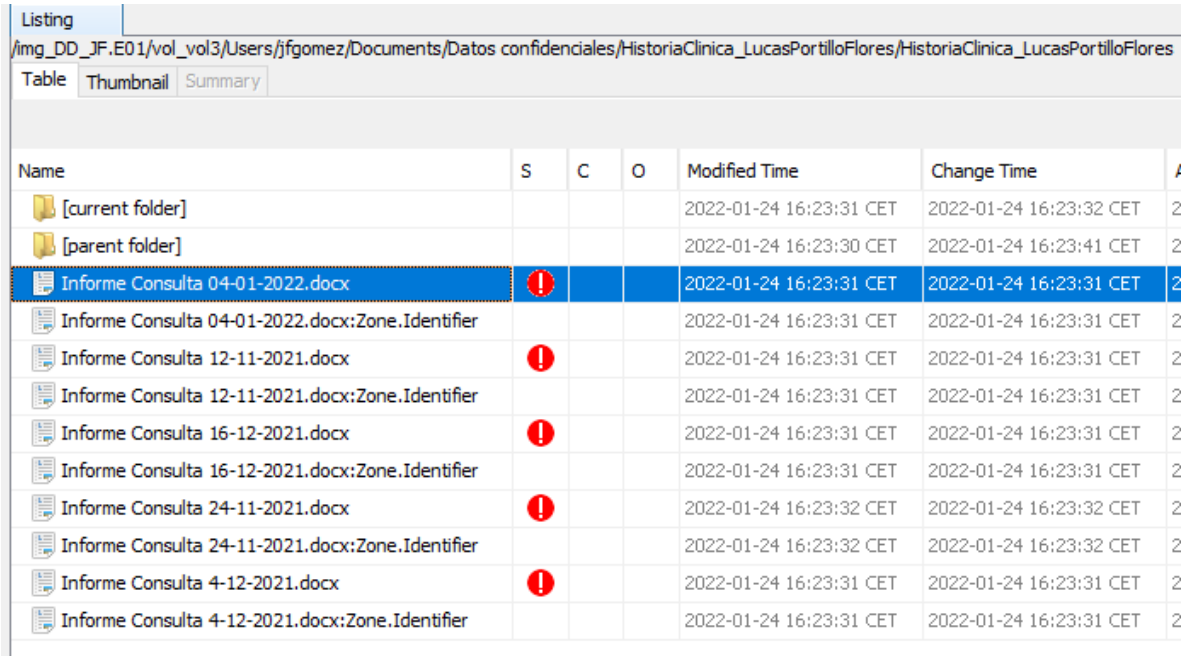
Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

1 of 1 100%

Usuario	Email	Contraseña
Juan Lopez Lopez	jlopezlopez@gmail.com	x23r12
Laura García Martín	lgarciamartin@gmail.com	r45tg1
Jose Fernandez Lopez	jfernandezlopez@gmail.com	Khj341
Ana Gonzalez Gonzalez	agonzalezgonzalez@gmail.com	fL996H
Paula Martín Gómez	pmartingomez@gmail.com	vb4sD1
Carmen Hernandez García	chernandezgarcia@gmail.com	sdE43f
Luis Carreras de Miguel	lcarrerasdemiguel@gmail.com	12e3aE
Pedro Sánchez Fernandez	psanchezfernandez@gmail.com	Lsd21e
Manuel Felipe Gonzalez	mfelipegonzalez@gmail.com	dF34s2
Francisco Pozas Moreno	fpozasmoreno@gmail.com	dfR34T
Javier Hernández Gonzalez	jhernandezgonzalez@gmail.com	34rfY5

En está carpeta, se puede ver ficheros como Contraseñas_empleados.pdf que contiene usuarios, emails y contraseñas. También hay cuentas bancarias de los empleados, nominas, información de las adicciones de los pacientes y sueldos.

En la carpeta “HistoriaClinica_LucasPortiflloFlores” dentro de la carpeta “Datos confidenciales” hay informes de consulta sobre la clínica.



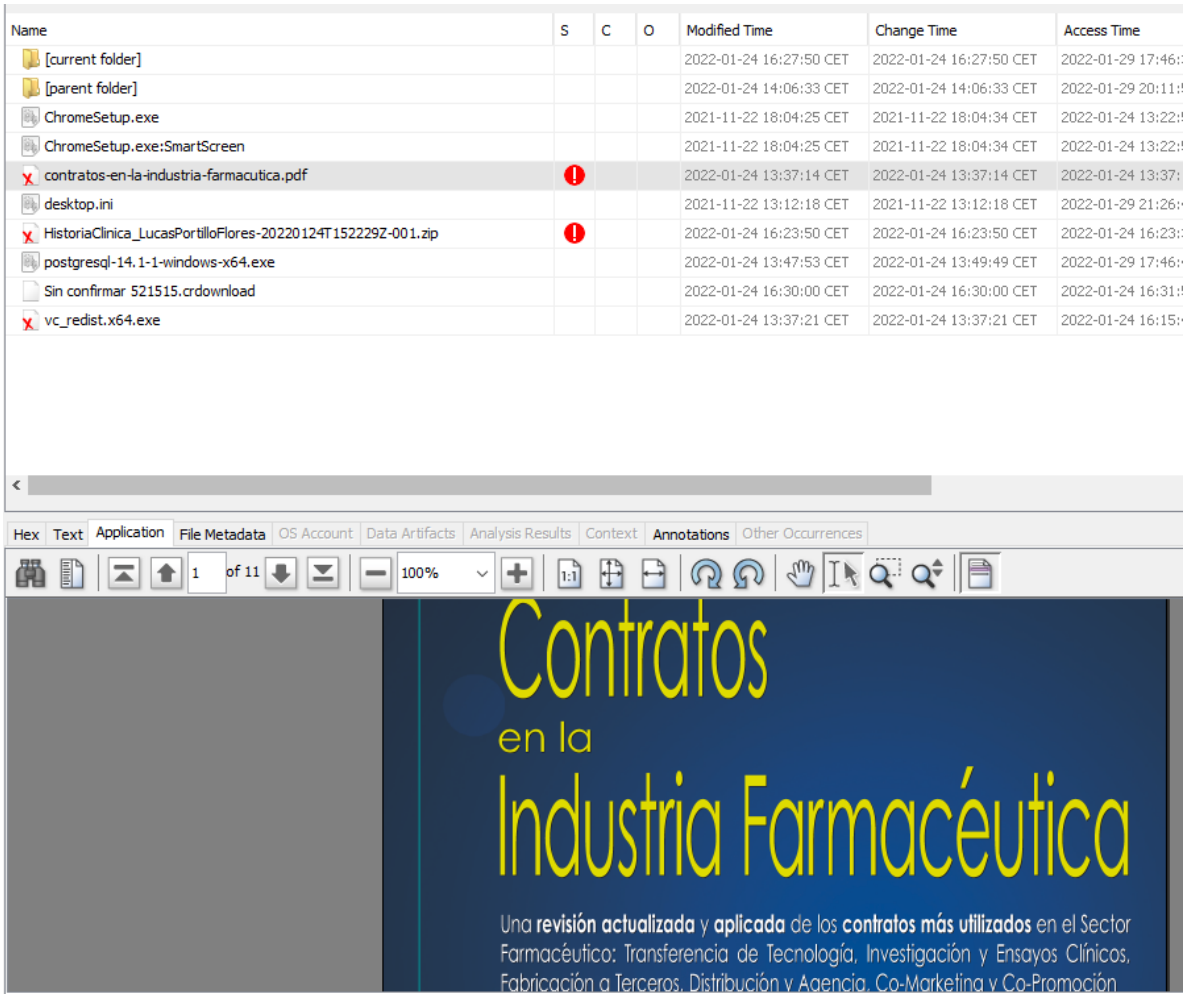
Listing

/img_DD_JF.E01/vol_vol3/Users/jfgomez/Documents/Datos confidenciales/HistoriaClinica_LucasPortilloFlores/HistoriaClinica_LucasPortilloFlores

Table | Thumbnail | Summary

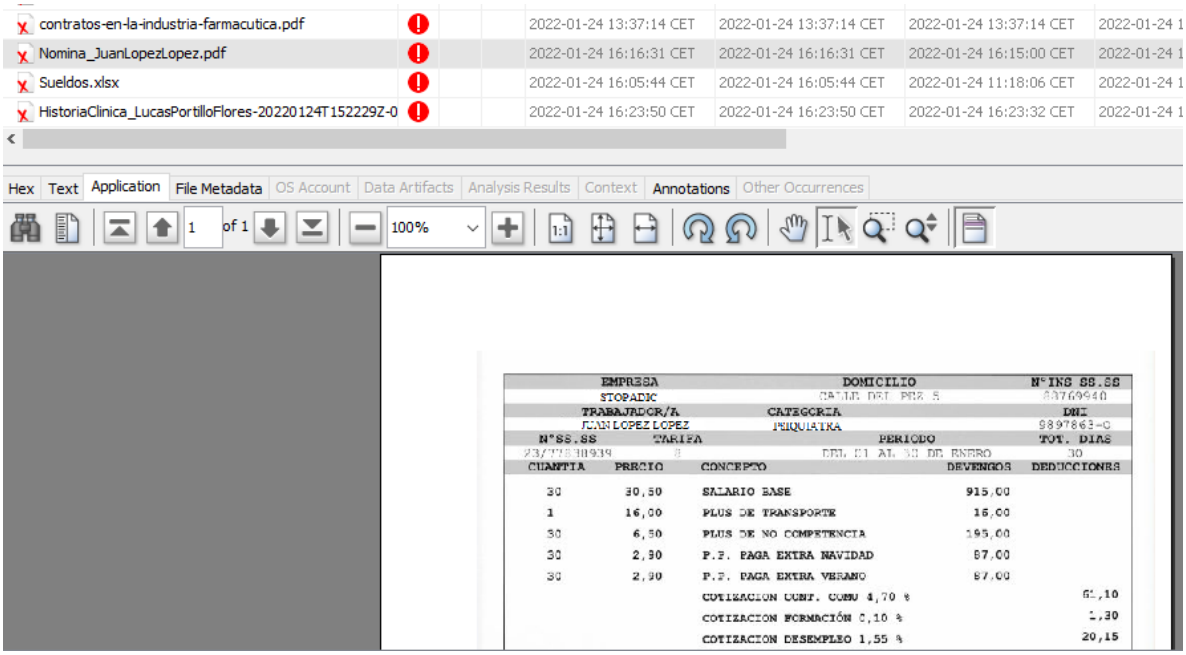
Name	S	C	O	Modified Time	Change Time	A
[current folder]				2022-01-24 16:23:31 CET	2022-01-24 16:23:32 CET	2
[parent folder]				2022-01-24 16:23:30 CET	2022-01-24 16:23:41 CET	2
Informe Consulta 04-01-2022.docx	!			2022-01-24 16:23:31 CET	2022-01-24 16:23:31 CET	2
Informe Consulta 04-01-2022.docx:Zone.Identifier				2022-01-24 16:23:31 CET	2022-01-24 16:23:31 CET	2
Informe Consulta 12-11-2021.docx	!			2022-01-24 16:23:31 CET	2022-01-24 16:23:31 CET	2
Informe Consulta 12-11-2021.docx:Zone.Identifier				2022-01-24 16:23:31 CET	2022-01-24 16:23:31 CET	2
Informe Consulta 16-12-2021.docx	!			2022-01-24 16:23:31 CET	2022-01-24 16:23:31 CET	2
Informe Consulta 16-12-2021.docx:Zone.Identifier				2022-01-24 16:23:31 CET	2022-01-24 16:23:31 CET	2
Informe Consulta 24-11-2021.docx	!			2022-01-24 16:23:32 CET	2022-01-24 16:23:32 CET	2
Informe Consulta 24-11-2021.docx:Zone.Identifier				2022-01-24 16:23:32 CET	2022-01-24 16:23:32 CET	2
Informe Consulta 4-12-2021.docx	!			2022-01-24 16:23:31 CET	2022-01-24 16:23:31 CET	2
Informe Consulta 4-12-2021.docx:Zone.Identifier				2022-01-24 16:23:31 CET	2022-01-24 16:23:31 CET	2

En la carpeta de Descargas, se encuentran los ficheros que seguramente ha descargado de Internet, como contratos en la industria farmacéutica y un zip con el historial de la clínica, cuya carpeta se ha visto anteriormente.



Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2022-01-24 16:27:50 CET	2022-01-24 16:27:50 CET	2022-01-29 17:46:
[parent folder]				2022-01-24 14:06:33 CET	2022-01-24 14:06:33 CET	2022-01-29 20:11:
ChromeSetup.exe				2021-11-22 18:04:25 CET	2021-11-22 18:04:34 CET	2022-01-24 13:22:
ChromeSetup.exe:SmartScreen				2021-11-22 18:04:25 CET	2021-11-22 18:04:34 CET	2022-01-24 13:22:
contratos-en-la-industria-farmacutica.pdf	!			2022-01-24 13:37:14 CET	2022-01-24 13:37:14 CET	2022-01-24 13:37:
desktop.ini				2021-11-22 13:12:18 CET	2021-11-22 13:12:18 CET	2022-01-29 21:26:
HistoriaClinica_LucasPortilloFlores-20220124T152229Z-001.zip	!			2022-01-24 16:23:50 CET	2022-01-24 16:23:50 CET	2022-01-24 16:23:
postgresql-14.1-1-windows-x64.exe				2022-01-24 13:47:53 CET	2022-01-24 13:49:49 CET	2022-01-29 17:46:
Sin confirmar 521515.crdownload				2022-01-24 16:30:00 CET	2022-01-24 16:30:00 CET	2022-01-24 16:31:
vc_redist.x64.exe				2022-01-24 13:37:21 CET	2022-01-24 13:37:21 CET	2022-01-24 16:15:

En los ficheros eliminados se encuentran algunos que podría ser relevantes, pero ya se han visto en otras carpetas.



contratos-en-la-industria-farmacutica.pdf	2022-01-24 13:37:14 CET	2022-01-24 13:37:14 CET	2022-01-24 13:37:14 CET	2022-01-24 1
Nomina_JuanLopezLopez.pdf	2022-01-24 16:16:31 CET	2022-01-24 16:16:31 CET	2022-01-24 16:15:00 CET	2022-01-24 1
Sueldos.xlsx	2022-01-24 16:05:44 CET	2022-01-24 16:05:44 CET	2022-01-24 11:18:06 CET	2022-01-24 1
HistoriaClinica_LucasPortilloFlores-20220124T152229Z-0	2022-01-24 16:23:50 CET	2022-01-24 16:23:50 CET	2022-01-24 16:23:32 CET	2022-01-24 1

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

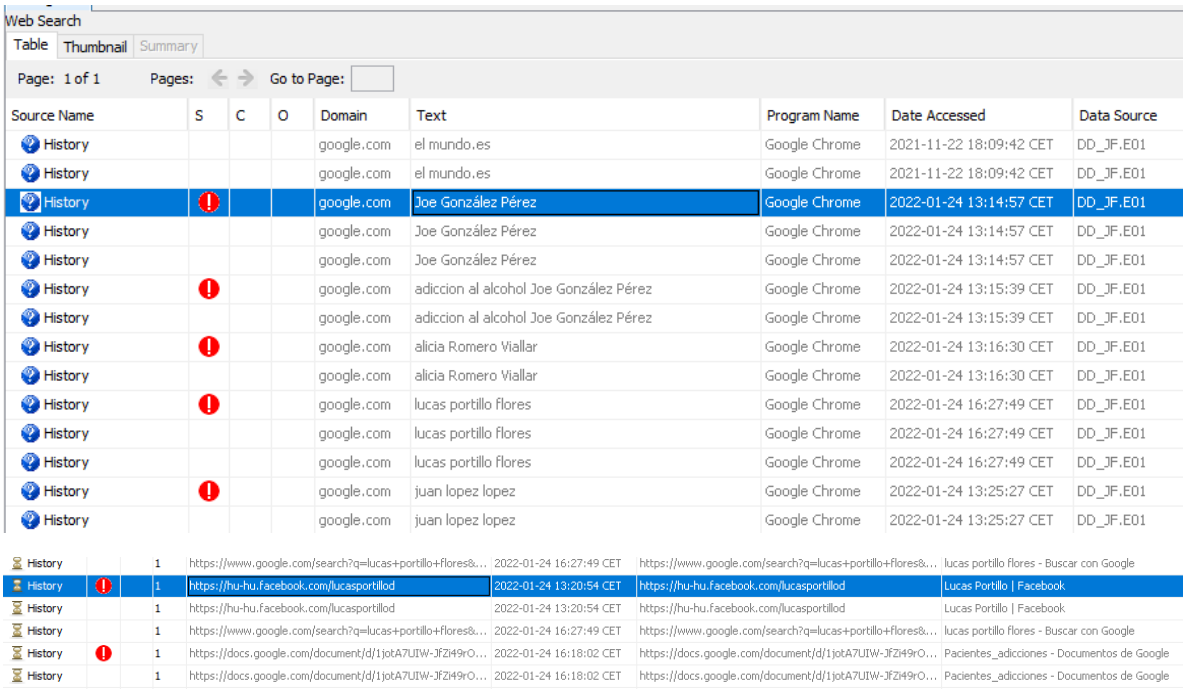
1 of 1 100%

EMPRESA	DOMICILIO	Nº INS SS.SS
STOPADIC	CALLE DEL PEZ 5	08769940
TRABAJADOR/A	CATEGORIA	DNI
JUAN LOPEZ LOPEZ	PSIQUIATRA	9897863-G
Nº SS.SS	TARIFA	PERIODO
23/[illegible]939		DEL 01 AL 30 DE ENERO

TOT. DIAS: 30

CUANTIA	PRECIO	CONCEPTO	DEVENGOS	DEDUCCIONES
30	30,50	SALARIO BASE	915,00	
1	16,00	PLUS DE TRANSPORTE	16,00	
30	6,50	PLUS DE NO COMPETENCIA	195,00	
30	2,90	P.P. PAGA EXTRA NAVIDAD	87,00	
30	2,90	P.P. PAGA EXTRA VERANO	87,00	
		COTIZACION CONT. COMU 4,70 %		61,10
		COTIZACION FORMACIÓN 0,10 %		1,30
		COTIZACION DESEMPLEO 1,55 %		20,15

En cuanto a las búsquedas por Internet, se han realizado varias sobre distintos pacientes de la clínica o sobre sus adicciones. En algunos casos, incluso ha mirado en las redes sociales de los pacientes como Facebook.



Web Search

Table | Thumbnail | Summary

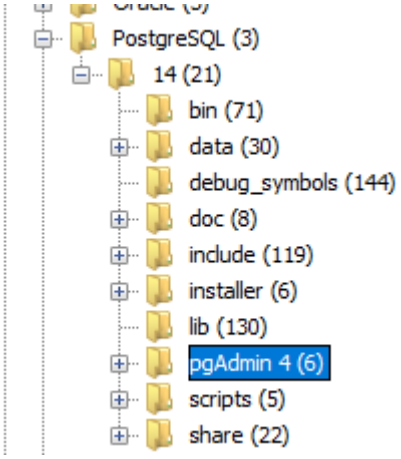
Page: 1 of 1 Pages: Go to Page:

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	el mundo.es	Google Chrome	2021-11-22 18:09:42 CET	DD_JF.E01
History				google.com	el mundo.es	Google Chrome	2021-11-22 18:09:42 CET	DD_JF.E01
History	!			google.com	Joe González Pérez	Google Chrome	2022-01-24 13:14:57 CET	DD_JF.E01
History				google.com	Joe González Pérez	Google Chrome	2022-01-24 13:14:57 CET	DD_JF.E01
History				google.com	Joe González Pérez	Google Chrome	2022-01-24 13:14:57 CET	DD_JF.E01
History	!			google.com	adiccion al alcohol Joe González Pérez	Google Chrome	2022-01-24 13:15:39 CET	DD_JF.E01
History				google.com	adiccion al alcohol Joe González Pérez	Google Chrome	2022-01-24 13:15:39 CET	DD_JF.E01
History	!			google.com	alicia Romero Viallar	Google Chrome	2022-01-24 13:16:30 CET	DD_JF.E01
History				google.com	alicia Romero Viallar	Google Chrome	2022-01-24 13:16:30 CET	DD_JF.E01
History	!			google.com	lucas portillo flores	Google Chrome	2022-01-24 16:27:49 CET	DD_JF.E01
History				google.com	lucas portillo flores	Google Chrome	2022-01-24 16:27:49 CET	DD_JF.E01
History				google.com	lucas portillo flores	Google Chrome	2022-01-24 16:27:49 CET	DD_JF.E01
History	!			google.com	juan lopez lopez	Google Chrome	2022-01-24 13:25:27 CET	DD_JF.E01
History				google.com	juan lopez lopez	Google Chrome	2022-01-24 13:25:27 CET	DD_JF.E01

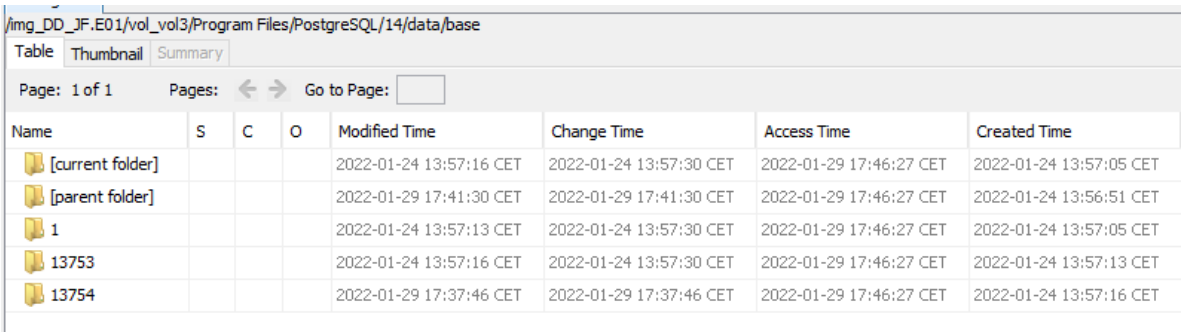
History		1	https://www.google.com/search?q=lucas+portillo+flores&...	2022-01-24 16:27:49 CET	https://www.google.com/search?q=lucas+portillo+flores&...	lucas portillo flores - Buscar con Google
History	!	1	https://hu-hu.facebook.com/lucasportillod	2022-01-24 13:20:54 CET	https://hu-hu.facebook.com/lucasportillod	Lucas Portillo | Facebook
History		1	https://hu-hu.facebook.com/lucasportillod	2022-01-24 13:20:54 CET	https://hu-hu.facebook.com/lucasportillod	Lucas Portillo | Facebook
History		1	https://www.google.com/search?q=lucas+portillo+flores&...	2022-01-24 16:27:49 CET	https://www.google.com/search?q=lucas+portillo+flores&...	lucas portillo flores - Buscar con Google
History	!	1	https://docs.google.com/document/d/1jotA7UIW-JfZi49rO...	2022-01-24 16:18:02 CET	https://docs.google.com/document/d/1jotA7UIW-JfZi49rO...	Pacientes_adicciones - Documentos de Google
History		1	https://docs.google.com/document/d/1jotA7UIW-JfZi49rO...	2022-01-24 16:18:02 CET	https://docs.google.com/document/d/1jotA7UIW-JfZi49rO...	Pacientes_adicciones - Documentos de Google

Indicar información de la aplicación PgAdmin, ¿para qué puede servir? ¿Cuál puede ser su fin?

pgAdmin se encuentra instalado en la carpeta de PostgreSQL:



Se han revisado la carpeta data/base/ donde se almacenan las bases de datos



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2022-01-24 13:57:16 CET	2022-01-24 13:57:30 CET	2022-01-29 17:46:27 CET	2022-01-24 13:57:05 CET
[parent folder]				2022-01-29 17:41:30 CET	2022-01-29 17:41:30 CET	2022-01-29 17:46:27 CET	2022-01-24 13:56:51 CET
1				2022-01-24 13:57:13 CET	2022-01-24 13:57:30 CET	2022-01-29 17:46:27 CET	2022-01-24 13:57:05 CET
13753				2022-01-24 13:57:16 CET	2022-01-24 13:57:30 CET	2022-01-29 17:46:27 CET	2022-01-24 13:57:13 CET
13754				2022-01-29 17:37:46 CET	2022-01-29 17:37:46 CET	2022-01-29 17:46:27 CET	2022-01-24 13:57:16 CET

Y también los logs que genera PostgreSQL.

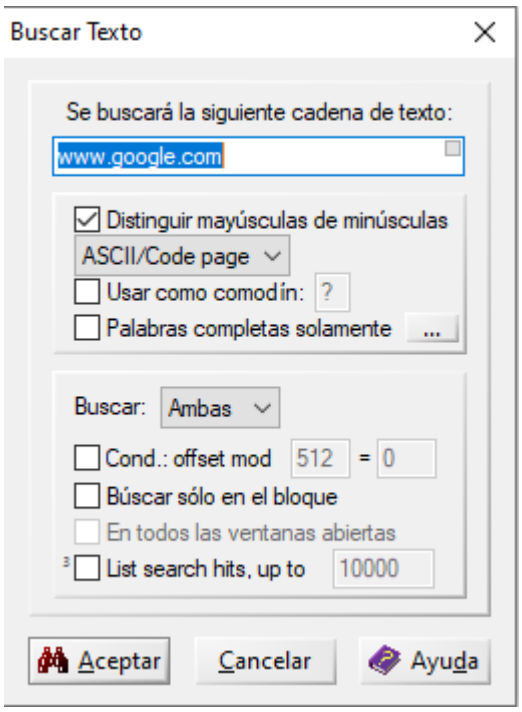
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2022-01-29 17:41:29 CET	2022-01-29 17:41:29 CET	2022-01-29 17:46:27 CET	2022-01-24 13:57:28 CET
[parent folder]				2022-01-29 17:41:30 CET	2022-01-29 17:41:30 CET	2022-01-29 17:46:27 CET	2022-01-24 13:56:51 CET
postgresql-2022-01-24_135735.log				2022-01-24 13:59:53 CET	2022-01-24 13:59:53 CET	2022-01-24 13:59:54 CET	2022-01-24 13:57:35 CET
postgresql-2022-01-24_140434.log				2022-01-24 14:04:34 CET	2022-01-24 14:04:34 CET	2022-01-24 14:04:34 CET	2022-01-24 14:04:34 CET
postgresql-2022-01-29_173741.log				2022-01-29 17:37:46 CET	2022-01-29 17:37:46 CET	2022-01-29 17:37:46 CET	2022-01-29 17:37:41 CET
postgresql-2022-01-29_173840.log				2022-01-29 17:40:49 CET	2022-01-29 17:40:49 CET	2022-01-29 17:40:49 CET	2022-01-29 17:38:40 CET
postgresql-2022-01-29_174129.log				2022-01-29 17:41:30 CET	2022-01-29 17:41:30 CET	2022-01-29 17:41:30 CET	2022-01-29 17:41:29 CET

En ambos casos, no se ha encontrado información de posibles bases de datos que estén importadas en PostgreSQL. El uso de pgAdmin sería para poder importar, conectar y consultar bases de datos en PostgreSQL, cuyo fin seguramente es obtener información confidencial de la clínica.

ARCHIVO memJF.mem

- Búsquedas webs:
    - *Teniendo en cuenta lo encontrado en el disco duro, ¿qué tipo de información buscarías en el ordenador?*

Buscaría información relacionado con la clínica o sus pacientes de lo encontrado en los ficheros del disco duro. También se podría buscar www.google.com usando WinHex para saber qué búsquedas ha realizado:



Y algunos de los resultados serían los siguientes:

```
00119540 | 68 74 74 70 73 3A 2F 2F  77 77 77 2E 67 6F 6F 67 | https://www.goog
00119550 | 6C 65 2E 63 6F 6D 2F 73  65 61 72 63 68 3F 71 3D | le.com/search?q=
00119560 | 6A 6F 65 2B 67 6F 6E 7A  61 6C 65 7A 2B 70 65 72 | joe+gonzalez+per
00119570 | 65 7A 26 72 6C 7A 3D 31  43 31 4F 4E 47 52 5F 65 | ez&rlz=1C1ONGR_e
00119580 | 73 45 53 39 38 31 45 53  39 38 33 26 6F 71 3D 6A | sES981ES983&oq=j
00119590 | 6F 65 2B 67 6F 6E 7A 61  6C 65 7A 2B 70 65 72 65 | oe+gonzalez+pere
001195A0 | 7A 26 61 71 73 3D 63 68  72 6F 6D 65 2E 2E 36 39 | z&aqs=chrome..69
001195B0 | 69 35 37 2E 34 32 34 38  6A 30 6A 37 26 73 6F 75 | i57.4248j0j7&sou
001195C0 | 72 63 65 69 64 3D 63 68  72 6F 6D 65 26 69 65 3D | rceid=chrome&ie=
001195D0 | 55 54 46 2D 38 0A 32 35  36 39 36 30 38 35 37 37 | UTF-8 2569608577
001195E0 | 33 36 38 39 33 32 39 35  34 00 00 00 00 00 00 00 | 368932954
```

```
018650E0  EC 00 00 00 E4 00 00 00  68 74 74 70 73 3A 2F 2F  ì   ä   https://
018650F0  77 77 77 2E 67 6F 6F 67  6C 65 2E 63 6F 6D 2F 73  www.google.com/s
01865100  65 61 72 63 68 3F 71 3D  61 64 69 63 63 69 25 43  earch?q=adicci%C
01865110  33 25 42 33 6E 2B 61 6C  2B 61 6C 63 6F 68 6F 6C  3%B3n+al+alcohol
01865120  2B 6A 6F 65 2B 67 6F 6E  7A 61 6C 65 7A 2B 70 65  +joe+gonzalez+pe
01865130  72 65 7A 26 72 6C 7A 3D  31 43 31 4F 4E 47 52 5F  rez&rlz=1C1ONGR_
01865140  65 73 45 53 39 38 31 45  53 39 38 33 26 6F 71 3D  esES981ES983&oq=
01865150  61 64 69 63 63 69 25 43  33 25 42 33 6E 2B 61 6C  adicci%C3%B3n+al
01865160  2B 61 6C 63 6F 68 6F 6C  2B 6A 6F 65 2B 67 6F 6E  +alcohol+joe+gon
01865170  7A 61 6C 65 7A 2B 70 65  72 65 7A 26 61 71 73 3D  zalez+perez&aqs=
01865180  63 68 72 6F 6D 65 2E 2E  36 39 69 35 37 6A 33 33  chrome..69i57j33
01865190  69 31 36 30 6C 32 2E 31  34 32 31 6A 30 6A 37 26  i1602.1421j0j7&
018651A0  73 6F 75 72 63 65 69 64  3D 63 68 72 6F 6D 65 26  sourceid=chrome&
018651B0  69 65 3D 55 54 46 2D 38  0A 34 35 30 32 37 36 35  ie=UTF-8 4502765
018651C0  33 36 36 37 36 36 35 39  34 34 39 38 00 00 00 00  366766594498
018651D0  36 36 31 2E 37 30 36 38  39 38 35 26 63 6C 65 61  661.7068985&clea
018651E0  72 43 61 63 68 65 3D 31  0A 31 38 32 39 36 39 32  rCache=1 1829692
018651F0  32 33 35 38 36 31 39 32  38 38 38 35 00 00 00 00  235861928885
```

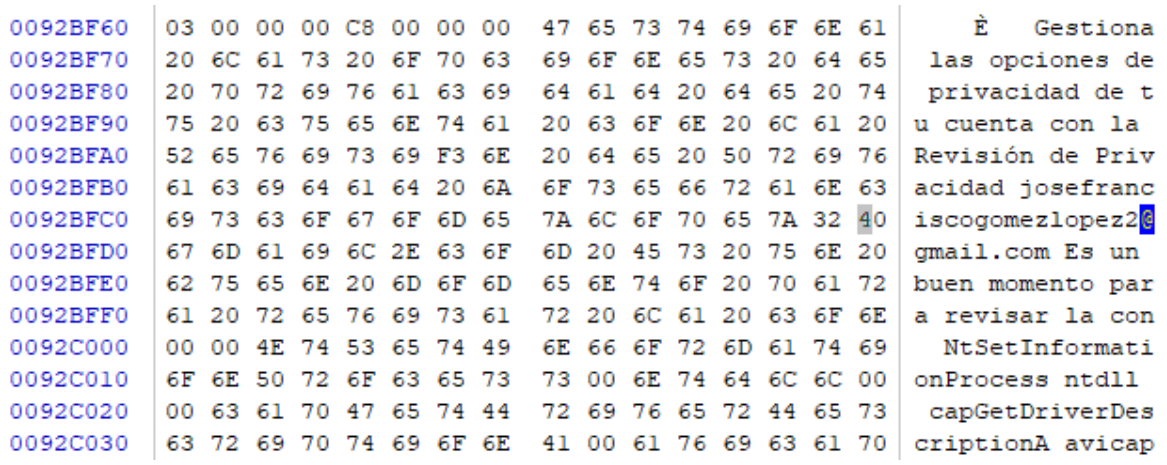
- *¿Qué nombres de los de los ficheros anteriores, puedes encontrar que haya buscado en Internet?*

Se han encontrado ficheros como “Contraseñas_empleados.pdf” y “Cuentas bancarias empleados.xlsx”

```
225F5050  01 00 00 00 19 00 00 00  01 CF 6D 71 43 6F 6E 74          ÏmqCont
225F5060  72 61 73 65 F1 61 73 5F  65 6D 70 6C 65 61 64 6F  raseñas_empleado
225F5070  73 2E 70 64 66 62 30 34  31 34 33 36 63 66 61 66  s.pdfb041436cfaf
225F5080  02 00 00 00 1D 00 00 00  05 2D E1 8B 4D 6F 6E 2C          -á‹Mon,
225F5090  20 31 36 20 4F 63 74 20  32 30 31 37 20 31 37 3A   16 Oct 2017 17:
225F50A0  33 32 3A 35 35 20 47 4D  54 00 00 00 00 00 00 00  32:55 GMT
225F50B0  01 00 00 00 17 00 00 00  39 00 00 00 68 74 74 70          9   http
225F50C0  73 3A 2F 2F 6D 61 69 6C  2E 67 6F 6F 67 6C 65 2E  s://mail.google.
225F50D0  63 6F 6D 61 64 65 72 73  69 61 6C 73 32 37 61 64  comadersials27ad
225F50E0  01 00 00 00 19 00 00 00  01 CF 6D 71 43 6F 6E 74          ÏmqCont
225F50F0  72 61 73 65 F1 61 73 5F  65 6D 70 6C 65 61 64 6F  raseñas_empleado
225F5100  73 2E 70 64 66 20 47 4D  54 74 2D 6F 6E 6C 79 00  s.pdf GMTt-only
225F5110  06 00 00 00 20 00 00 00  05 CD 48 DF 4F 70 63 69          ÍHßOpci
225F5120  6F 6E 65 73 20 64 65 20  6C 61 20 73 65 63 63 69  ones de la secci
225F5130  F3 6E 20 52 65 63 69 62  69 64 6F 73 FF FF 00 00  ón Recibidosÿÿ
225F5140  01 00 00 00 20 00 00 00  01 BF 9E 4D 43 75 65 6E          ¿žMCuen
225F5150  74 61 73 20 62 61 6E 63  61 72 69 61 73 20 65 6D  tas bancarias em
225F5160  70 6C 65 61 64 6F 73 2E  78 6C 73 78 31 FF 00 00  pleados.xlsxlÿ
225F5170  01 00 00 00 01 00 00 00  FF FF 00 00 01 00 00 00          ÿÿ
```

- Correo electrónico:
    - *Hay una cuenta de correo en la memoria, ¿cuál es?*

Al buscar "@gmail.com" se ha encontrado la cuenta josefranciscogomezlopez2@gmail.com del trabajador con el que ha iniciado sesión:



- *Dado el correo del sospechoso proporcionado en el caso, accede al correo e investiga en busca de información que pueda resultar relevante ¿qué email sospechoso puedes ver? (Mirar tanto la carpeta de recibidos como la de enviados)*

Al buscar posibles correos, se ha encontrado el siguiente donde se adjunta documentos confidenciales pidiendo a otra persona que haga una campaña de phishing contra la empresa que ha sido despedido: