



Universidad  
Francisco de Vitoria  
**UFV** Madrid



## Incidentes de ciberseguridad

# Investigación del incidente



Nombre:	Fecha:	Edición:	Firma:
Gonzalo Pascual Romero	25/03/2023	1.0	

# Índice

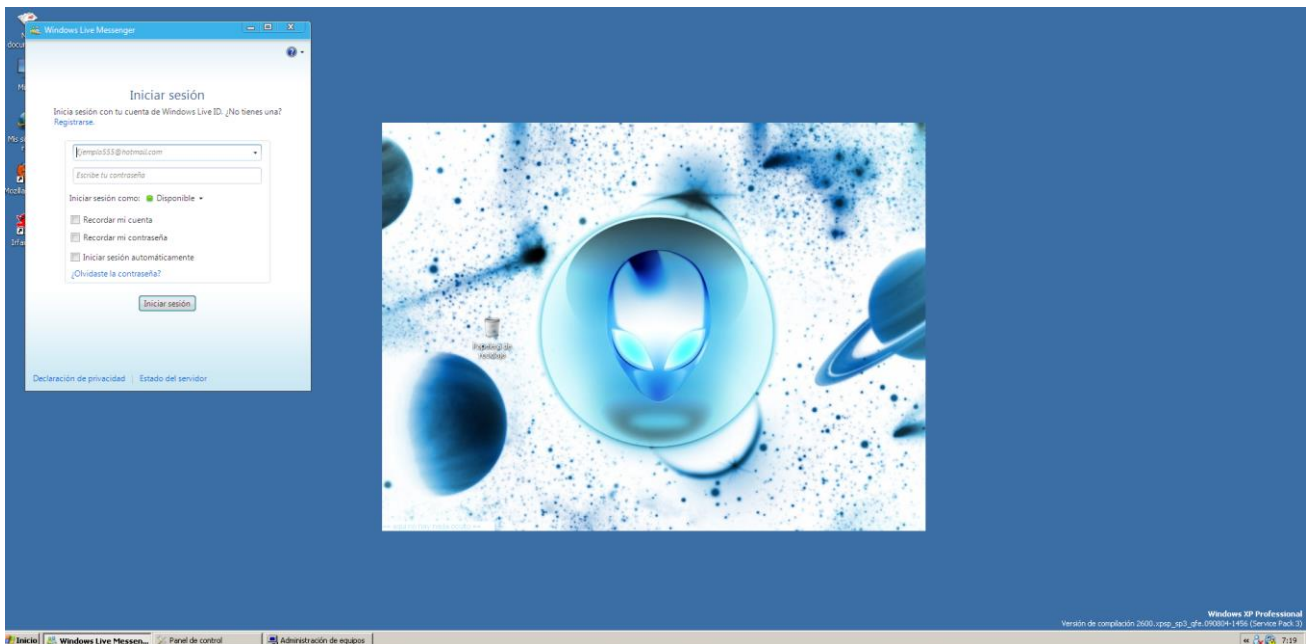
1. Introducción .....	3
2. Investigación .....	3
3. Conclusión.....	8

## Introducción

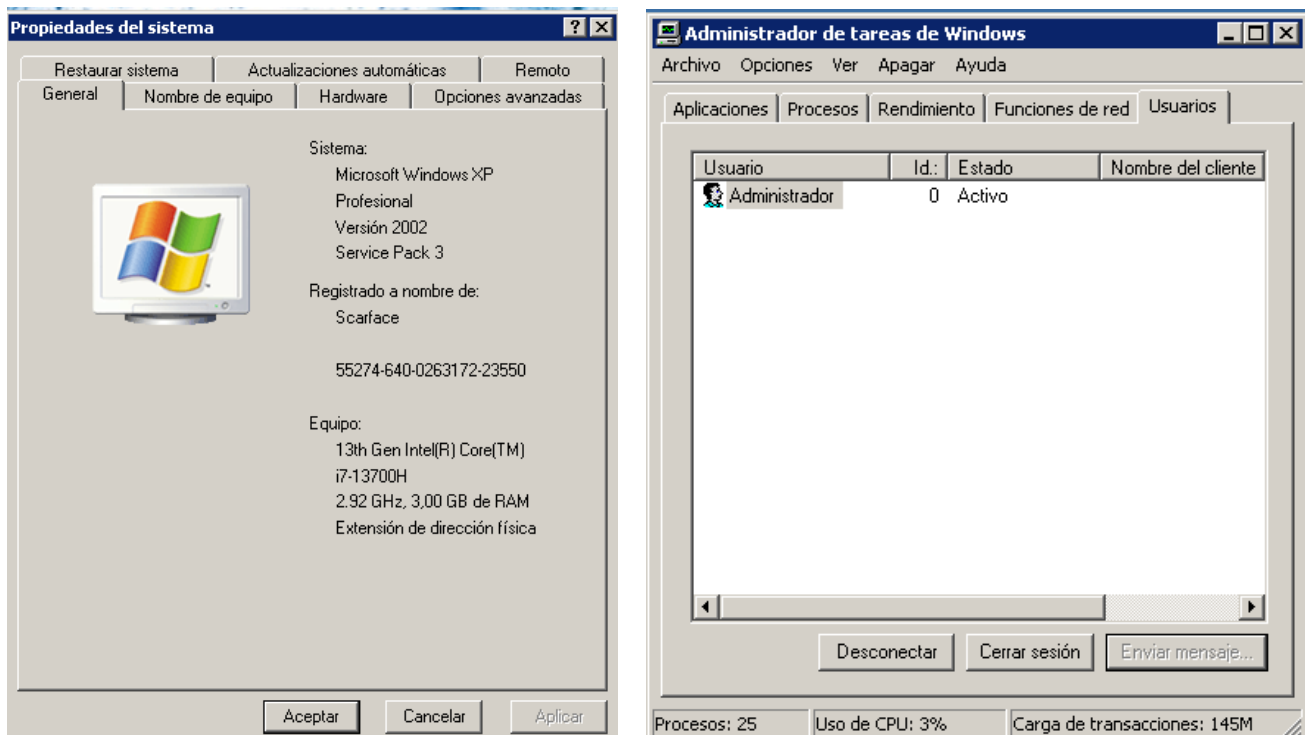
Se me ha sido asignado el estudio de una máquina Windows XP que fue requisada en un caso judicial con el objetivo de investigar y documentar cualquier evidencia digital relevante. No se cuenta con información previa sobre su historial o actividad y se busca identificar y recopilar datos que puedan proporcionar información sobre el uso pasado del sistema, actividades sospechosas o incidentes de seguridad.

## Investigación

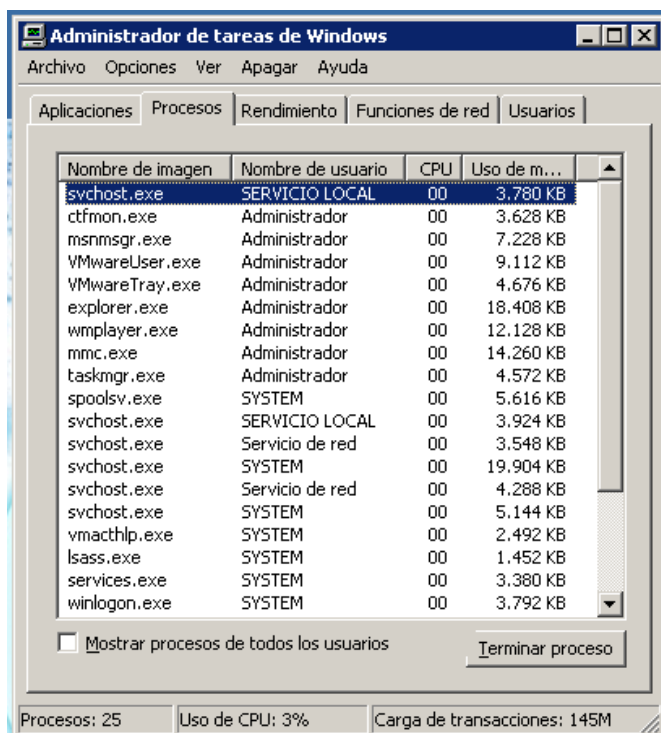
Lo primero que encontramos al encender la máquina es la página de inicio de sesión de Messenger por lo cual el usuario usa esta aplicación.



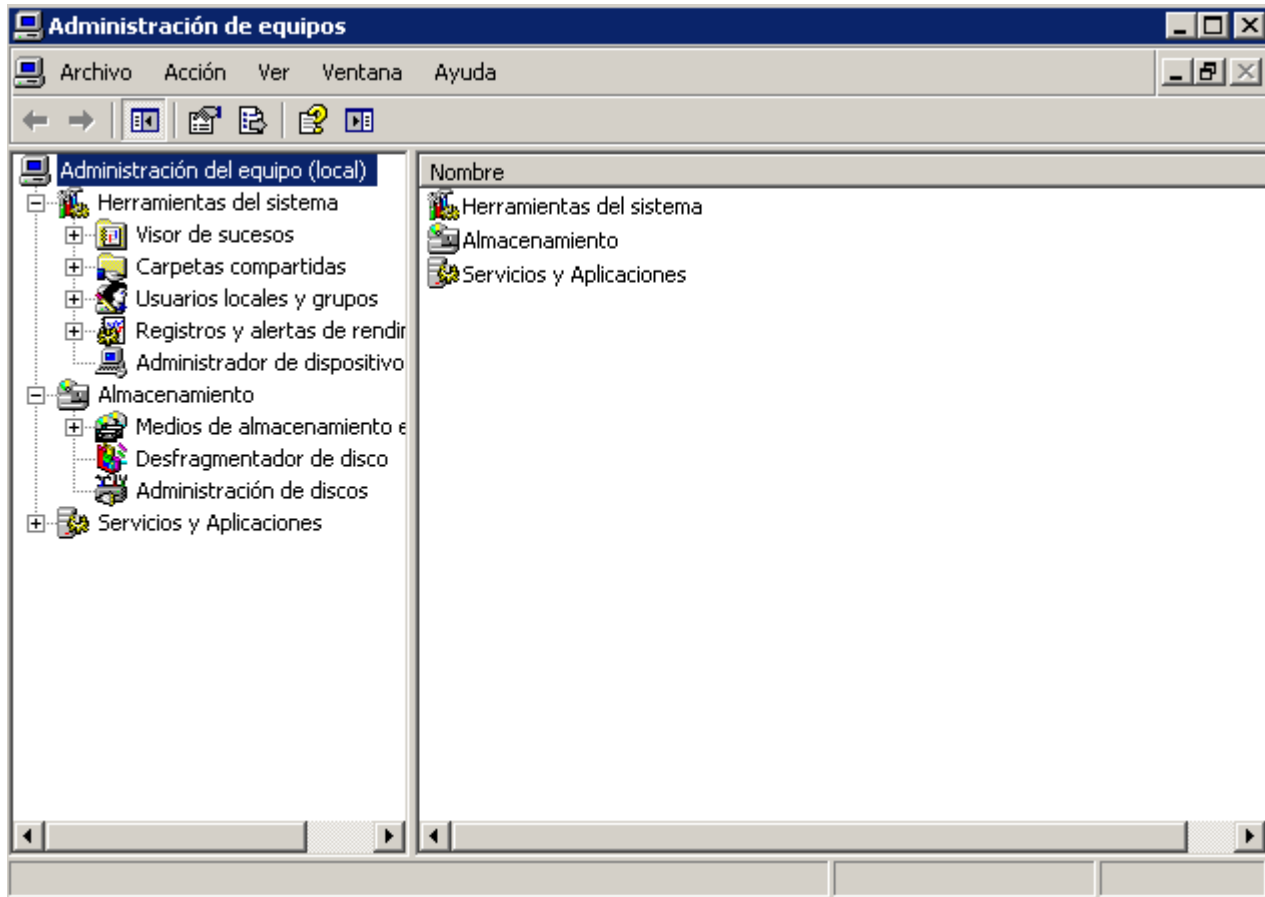
Vemos las propiedades del sistema y los usuarios, en el que solo hay uno que es el administrador.



También miramos el administrador de tareas para comprobar si se están ejecutando procesos extraños o si hay algún tipo de malware, pero no se detecta nada importante.



También examinamos el administrador de equipos y sus diferentes apartados como el visor de sucesos, la administración de discos o carpetas compartidas con el objetivo de identificar y comprender mejor cualquier actividad sospechosa.



Mediante el paquete de herramientas NirLauncher vamos a ejecutar “MyLastSearch” para ver las últimas búsquedas de este usuario.

NirLauncher - NirSoft Utilities

File Edit View Options Launcher Packages Help

Password Recovery Utilities

Internet Related Utilities

Programmer Tools

All Utilities

Network Monitoring Tools

Command-Line Utilities

Disk Utilities

Web Browser Tools

Desktop Utilities

System Utilities


Video/Audio Related Utilities

Outlook/Office Utilities

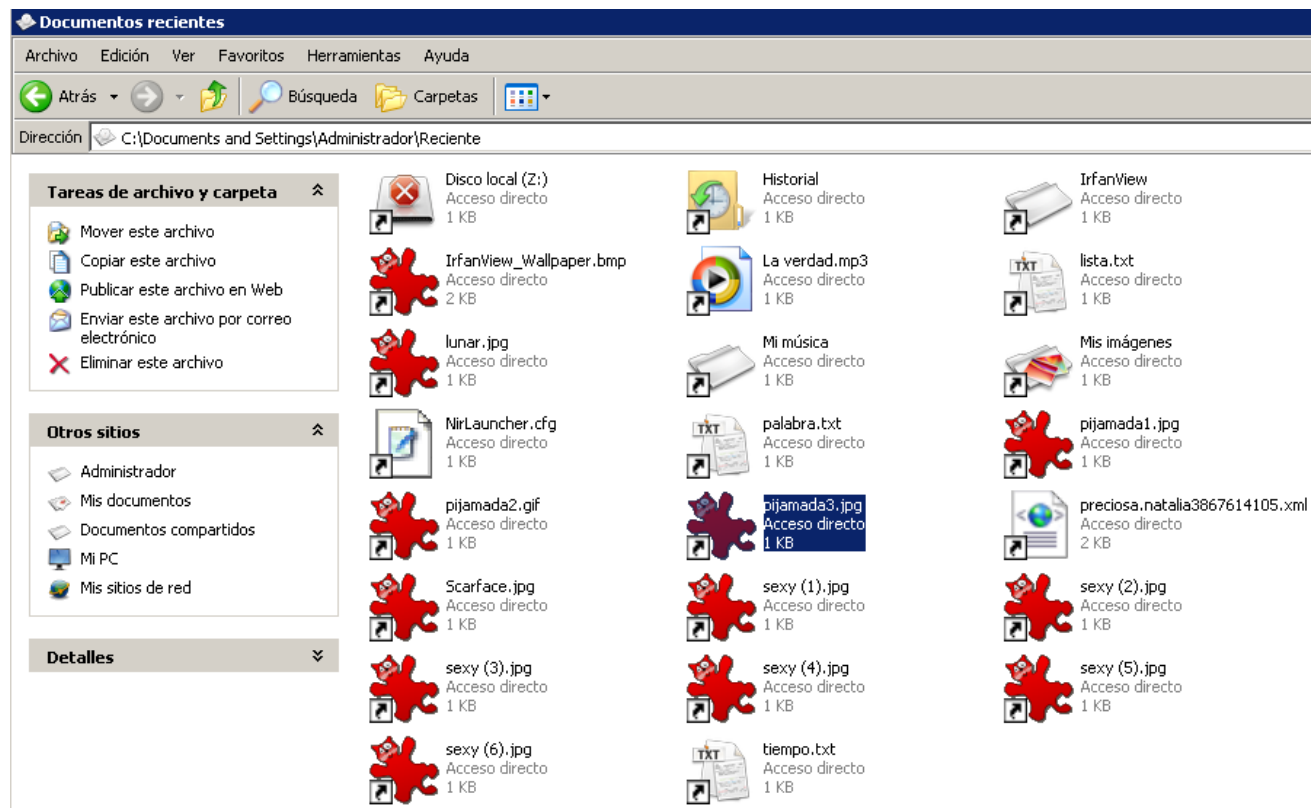
Other Utilities

Name	Description	Version	Updated On	Web Page URL
ImageCacheViewer	Displays images stored in the cache of your Web bro...	1.31	26/02/2024 9:49:30	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
ChromeCookiesView	Alternative to the standard internal cookies viewer of ...	1.76	15/02/2024 6:48:12	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
BrowserAddonsView	Displays the details of all Web browser addons/plugin...	1.29	28/01/2024 16:03:28	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
ChromeCacheView	Chrome Browser Cache Viewer	2.47	13/01/2024 10:53:24	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
WebBrowserBookmarksView	View all bookmarks of Chrome and Firefox Web brows...	1.12	11/01/2024 4:57:46	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
BrowserAutoFillView	View form autofill text stored by Chrome and Firefox ...	1.00	31/12/2023 8:35:12	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
ChromeHistoryView	View the browsing history of Chrome Web browser	1.53	16/11/2023 4:58:32	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
BrowsingHistoryView	View browsing history of popular Web browsers	2.57	11/11/2023 10:28:34	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
BrowserDownloadsView	Displays the details of downloaded files of Chrome an...	1.45	17/08/2023 7:04:04	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
MZCookiesView	alternative to the standard 'Cookie Manager' provided...	1.60	02/11/2022 9:33:06	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
MZCacheView	List all files currently stored in the cache of Firefox/M...	2.21	20/10/2022 4:48:54	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
WebCacheImageInfo	Shows EXIF information of the images stored in Web ...	1.34	05/02/2022 2:19:12	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
FBCacheView	Shows Facebook images stored in the cache of your ...	1.22	24/01/2022 1:57:56	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
MZHistoryView	Displays the list of visited Web sites in Firefox/Mozilla/...	1.70	03/11/2021 6:15:48	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
EdgeCookiesView	Display cookies from new versions of MS-Edge	1.17	17/08/2019 7:56:40	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
FirefoxDownloadsView	Displayed the list of downloaded files in Firefox	1.40	30/03/2019 4:12:46	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
WebCookiesSniffer	Captures Web site cookies and displays them in a sim...	1.30	02/09/2018 18:37:52	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
MyLastSearch	View your latest searches with Google, Yahoo, and MSN	1.65	24/09/2017 6:16:46	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>
IECookiesView	Displays the cookies that Internet Explorer stores on ...	1.79	11/02/2017 5:03:02	<a href="https://www.nirsoft.net/">https://www.nirsoft.net/</a>

Y en esta encontramos unos registros con nombres extraños

MyLastSearch				
File Edit View Options Help				
				
Search Text	Search Engine	Search Type	Search Time	Web Browser
high school musical	Google	General	19/12/2009 22:08:52	Internet Explorer
high school musical	Google	Images	19/12/2009 22:08:55	Internet Explorer
high school musical sexo	Google	General	19/12/2009 22:06:24	Internet Explorer
tbn:-5IcPb9BHKdHqM::imstars...	Google	General	19/12/2009 22:08:52	Internet Explorer
tbn:80FvqNEM_9WzMM::bp0...	Google	General	19/12/2009 22:08:52	Internet Explorer
tbn:cTep-5uhNOxLM::karen1...	Google	General	19/12/2009 22:08:52	Internet Explorer
tbn:erBotj29mgq0sM::fondos...	Google	General	19/12/2009 22:08:52	Internet Explorer
tbn:trRA_vLz1JjRIM::www.ej...	Google	General	19/12/2009 22:08:52	Internet Explorer
wallpapers	Google	General	19/12/2009 20:55:30	Internet Explorer

En documentos recientes encontramos contenido e imágenes con nombres sospechosos de pornografía.



Para tener más detalle vamos a ver el historial que se ha descargado del navegador y este cuenta con archivos sospechosos del mismo carácter que en los archivos recientes

URL	Title	Hits	Modified Date	Expiration Date
<a href="https://login.live.com/login.srf?wa=wsignin1.0&amp;rpsrv=11&amp;check...">https://login.live.com/login.srf?wa=wsignin1.0&amp;rpsrv=11&amp;check...</a>		7	20/12/2009 0:39:18	15/01/2010 0:39:20
<a href="http://login.live.com/ui/logout.srf?lc=3082&amp;id=64855&amp;ru=http://...">http://login.live.com/ui/logout.srf?lc=3082&amp;id=64855&amp;ru=http://...</a>	Cerrar sesión	5	20/12/2009 0:39:15	15/01/2010 0:39:16
<a href="http://login.live.com/ui/logout.srf?lc=3082&amp;id=64855&amp;ru=http://...">http://login.live.com/ui/logout.srf?lc=3082&amp;id=64855&amp;ru=http://...</a>	Cerrar sesión	4	20/12/2009 0:39:15	15/01/2010 0:39:16
<a href="http://login.live.com/logout.srf?ct=1261284067&amp;rver=6.0.5285...">http://login.live.com/logout.srf?ct=1261284067&amp;rver=6.0.5285...</a>	Continuar	9	20/12/2009 0:39:10	15/01/2010 0:39:12
<a href="http://imgsrc.ru/main/login.php?n=1&amp;cnt=/members/album_edit...">http://imgsrc.ru/main/login.php?n=1&amp;cnt=/members/album_edit...</a>	iMG5RC.RU Free photo ho...	7	20/12/2009 0:39:09	15/01/2010 0:39:10
<a href="http://e3.imgsrc.ru/members/album_edit.php?ald=477093&amp;nc=...">http://e3.imgsrc.ru/members/album_edit.php?ald=477093&amp;nc=...</a>	iMG5RC.RU Princesa on sc...	21	20/12/2009 0:39:05	15/01/2010 0:39:06
<a href="http://e3.imgsrc.ru/main/login.php?out=1&amp;cnt=%2Fmembers%...">http://e3.imgsrc.ru/main/login.php?out=1&amp;cnt=%2Fmembers%...</a>		1	20/12/2009 0:39:02	15/01/2010 0:39:04
<a href="http://login.live.com/logout.srf?ct=1261284067&amp;rver=6.0.5285...">http://login.live.com/logout.srf?ct=1261284067&amp;rver=6.0.5285...</a>	Continuar	4	20/12/2009 0:39:00	15/01/2010 0:39:02
<a href="http://bl146w.blu146.mail.live.com/mail/logout.aspx">http://bl146w.blu146.mail.live.com/mail/logout.aspx</a>		3	20/12/2009 0:38:59	15/01/2010 0:39:00
<a href="http://mail.live.com/default.aspx?wa=wsignin1.0">http://mail.live.com/default.aspx?wa=wsignin1.0</a>	Windows Live Hotmail	25	20/12/2009 0:38:49	15/01/2010 0:38:50
<a href="http://e3.imgsrc.ru/main/login.php?out=1&amp;cnt=%2Fmembers%...">http://e3.imgsrc.ru/main/login.php?out=1&amp;cnt=%2Fmembers%...</a>		1	20/12/2009 0:38:45	15/01/2010 0:38:46
<a href="http://e3.imgsrc.ru/members/album_edit.php?ald=477103&amp;nc=...">http://e3.imgsrc.ru/members/album_edit.php?ald=477103&amp;nc=...</a>	iMG5RC.RU Otra Pendeja ...	5	20/12/2009 0:38:42	15/01/2010 0:38:44
<a href="http://e3.imgsrc.ru/members/album_sets.php">http://e3.imgsrc.ru/members/album_sets.php</a>		4	20/12/2009 0:38:39	15/01/2010 0:38:40
<a href="http://e3.imgsrc.ru/members/album_edit.php?id=16307478">http://e3.imgsrc.ru/members/album_edit.php?id=16307478</a>	iMG5RC.RU Otra Pendeja ...	5	20/12/2009 0:37:38	15/01/2010 0:37:40
<a href="http://e3.imgsrc.ru/members/album_upload.php?logged_in=scar...">http://e3.imgsrc.ru/members/album_upload.php?logged_in=scar...</a>		2	20/12/2009 0:37:19	15/01/2010 0:37:20
<a href="file:///Z:/sexy%20(5).jpg">file:///Z:/sexy%20(5).jpg</a>		1	20/12/2009 0:37:15	15/01/2010 0:37:16
<a href="file:///Z:/sexy%20(4).jpg">file:///Z:/sexy%20(4).jpg</a>		1	20/12/2009 0:37:12	15/01/2010 0:37:14
<a href="file:///Z:/sexy%20(3).jpg">file:///Z:/sexy%20(3).jpg</a>		1	20/12/2009 0:37:09	15/01/2010 0:37:10
<a href="file:///Z:/sexy%20(2).jpg">file:///Z:/sexy%20(2).jpg</a>		1	20/12/2009 0:37:06	15/01/2010 0:37:08
<a href="file:///Z:/sexy%20(1).jpg">file:///Z:/sexy%20(1).jpg</a>		1	20/12/2009 0:37:05	15/01/2010 0:37:06

## Conclusión

Tras analizar la máquina virtual con Windows XP, se ha encontrado evidencia de que un usuario tenía contenido e imágenes pornográficas y que las descargaba y traficaba con ellas a través de Messenger. El historial del usuario reveló la presencia de información y archivos de naturaleza delicada, lo que constituye una clara infracción a la ley al poseer y compartir dicho material.



