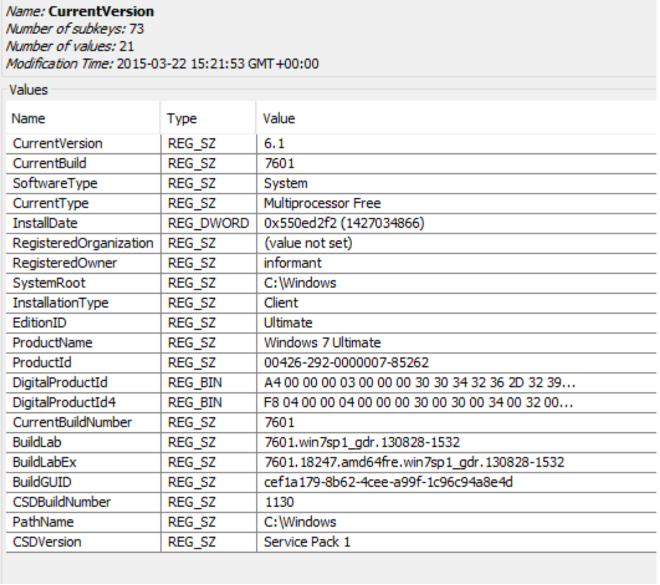
Immune Technology Institute

Informe Forense

9 de Julio del 2023

Cuestionario

1. Explique detalladamente la información del sistema operativo instalado.



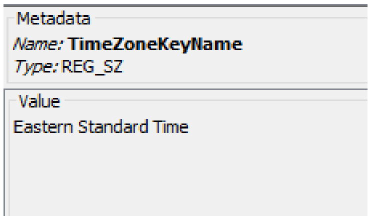
Name: **CurrentVersion**
Number of subkeys: 73
Number of values: 21
Modification Time: 2015-03-22 15:21:53 GMT+00:00

Values

Name	Type	Value
CurrentVersion	REG_SZ	6.1
CurrentBuild	REG_SZ	7601
SoftwareType	REG_SZ	System
CurrentType	REG_SZ	Multiprocessor Free
InstallDate	REG_DWORD	0x550ed2f2 (1427034866)
RegisteredOrganization	REG_SZ	(value not set)
RegisteredOwner	REG_SZ	informant
SystemRoot	REG_SZ	C:\Windows
InstallationType	REG_SZ	Client
EditionID	REG_SZ	Ultimate
ProductName	REG_SZ	Windows 7 Ultimate
ProductId	REG_SZ	00426-292-0000007-85262
DigitalProductId	REG_BIN	A4 00 00 00 03 00 00 00 30 30 34 32 36 2D 32 39...
DigitalProductId4	REG_BIN	F8 04 00 00 04 00 00 00 30 00 30 00 34 00 32 00...
CurrentBuildNumber	REG_SZ	7601
BuildLab	REG_SZ	7601.win7sp1_gdr.130828-1532
BuildLabEx	REG_SZ	7601.18247.amd64fre.win7sp1_gdr.130828-1532
BuildGUID	REG_SZ	cef1a179-8b62-4cee-a99f-1c96c94a8e4d
CSDBuildNumber	REG_SZ	1130
PathName	REG_SZ	C:\Windows
CSDVersion	REG_SZ	Service Pack 1

Sun Mar 22 10:34:26 AM EDT 2015

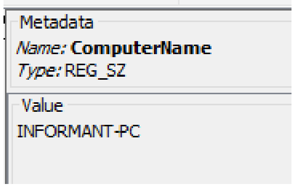
2. ¿Cuál es la configuración de la zona horaria?



Metadata
Name: **TimeZoneKeyName**
Type: REG_SZ

Value
Eastern Standard Time

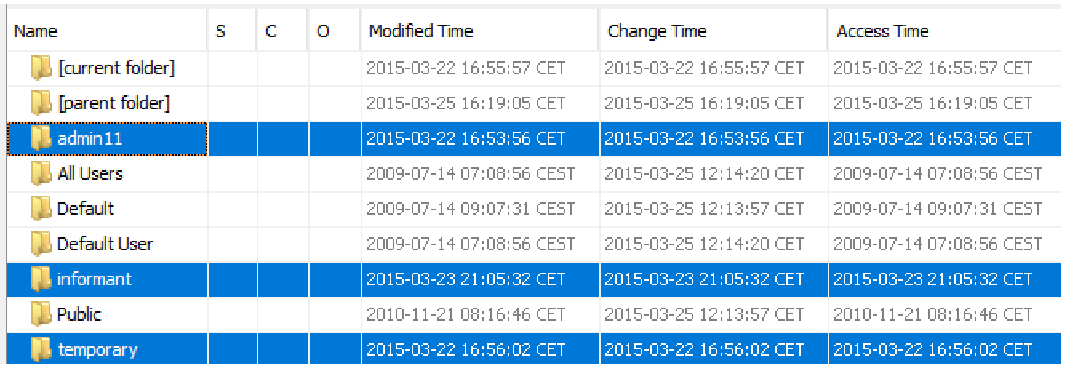
3. ¿Cuál es el nombre de la computadora?



Metadata
Name: **ComputerName**
Type: REG_SZ

Value
INFORMANT-PC

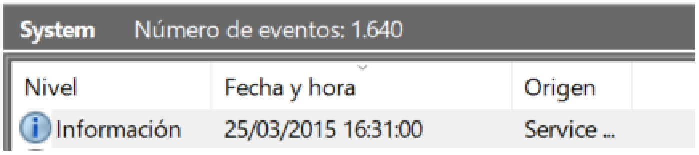
4. Enumere todas las cuentas en el sistema operativo, excepto las cuentas del sistema: Administrador, Invitado, perfil del sistema, Servicio local, Servicio de red. (Nombre de la cuenta, número de inicios de sesión, última fecha de inicio de sesión...)



Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2015-03-22 16:55:57 CET	2015-03-22 16:55:57 CET	2015-03-22 16:55:57 CET
[parent folder]				2015-03-25 16:19:05 CET	2015-03-25 16:19:05 CET	2015-03-25 16:19:05 CET
admin11				2015-03-22 16:53:56 CET	2015-03-22 16:53:56 CET	2015-03-22 16:53:56 CET
All Users				2009-07-14 07:08:56 CEST	2015-03-25 12:14:20 CET	2009-07-14 07:08:56 CEST
Default				2009-07-14 09:07:31 CEST	2015-03-25 12:13:57 CET	2009-07-14 09:07:31 CEST
Default User				2009-07-14 07:08:56 CEST	2015-03-25 12:14:20 CET	2009-07-14 07:08:56 CEST
informant				2015-03-23 21:05:32 CET	2015-03-23 21:05:32 CET	2015-03-23 21:05:32 CET
Public				2010-11-21 08:16:46 CET	2015-03-25 12:13:57 CET	2010-11-21 08:16:46 CET
temporary				2015-03-22 16:56:02 CET	2015-03-22 16:56:02 CET	2015-03-22 16:56:02 CET

5. ¿Quién fue el último usuario que inició sesión en la PC?
informant-PC

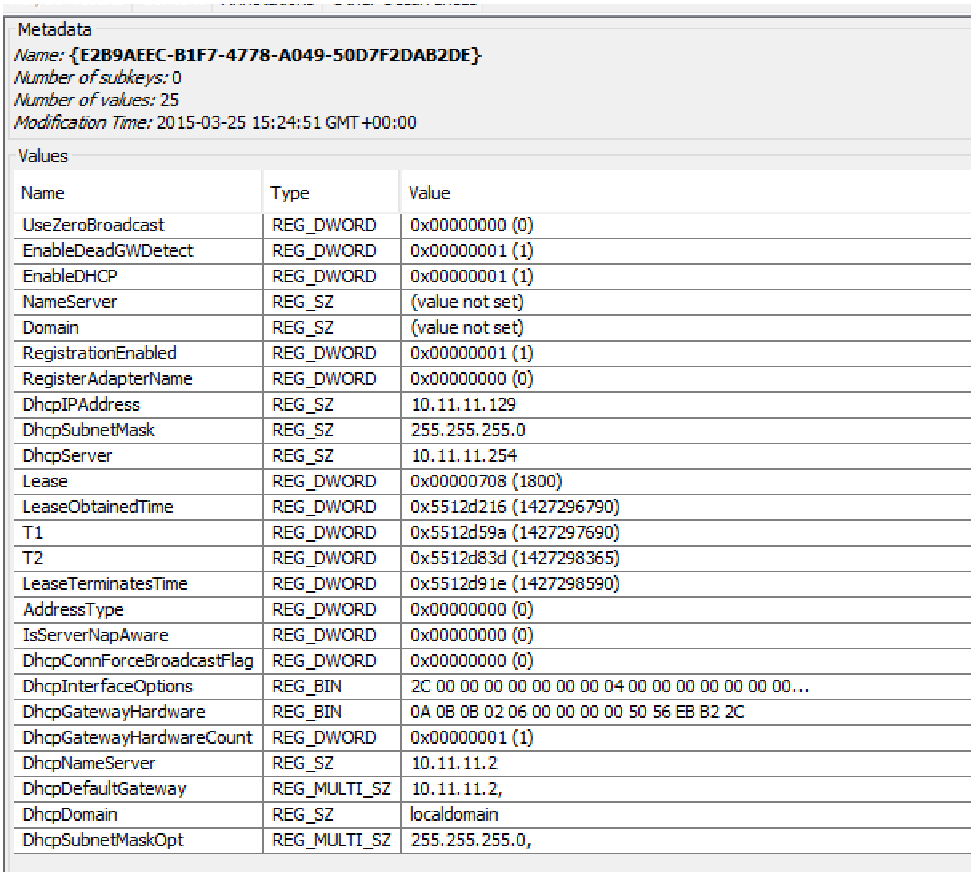
6. ¿Cuándo fue la última fecha/hora de apagado registrada?



System Número de eventos: 1.640

Nivel	Fecha y hora	Origen
Información	25/03/2015 16:31:00	Service ...

7. Explique la información de las interfaces de red con una dirección IP asignada por DHCP.



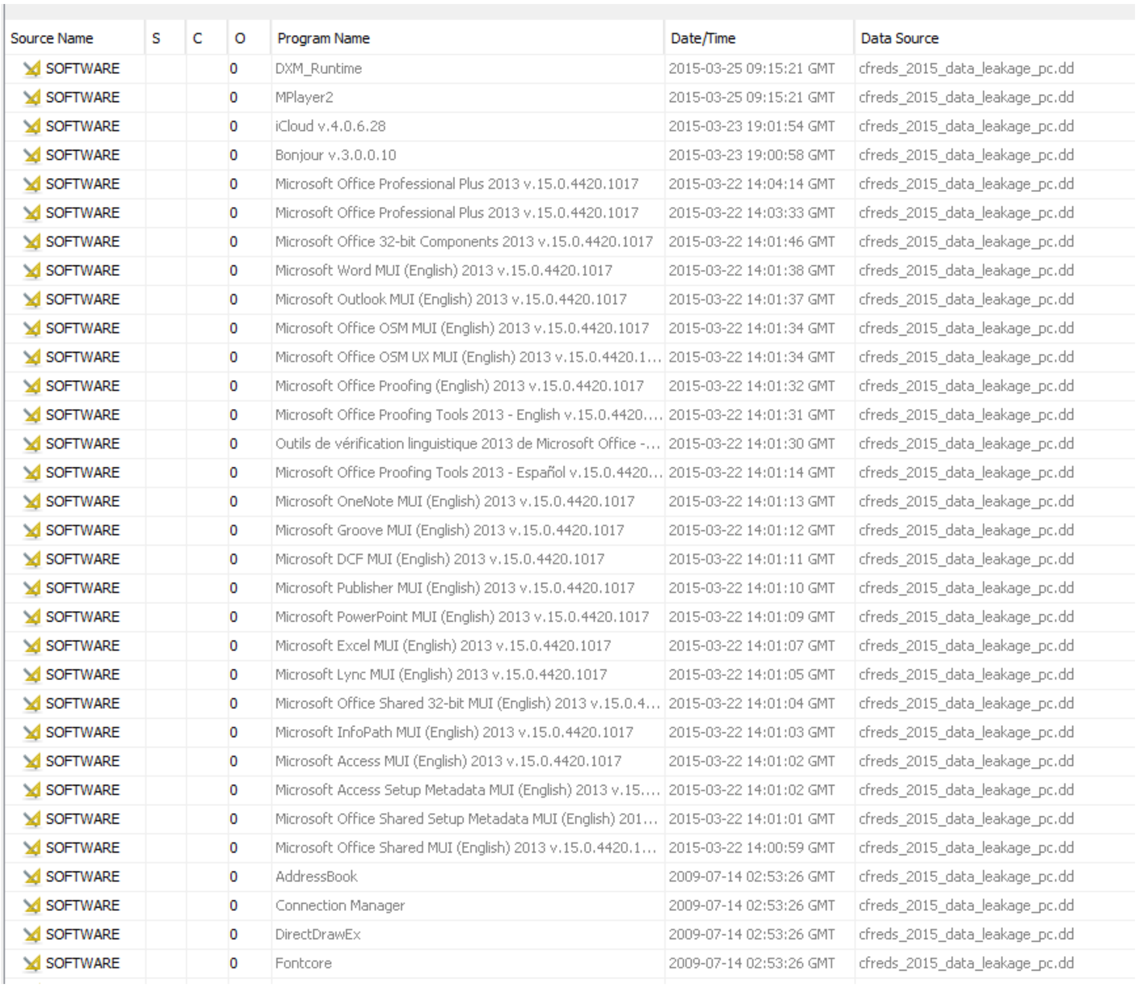
Metadata

Name: **{E2B9AEEC-B1F7-4778-A049-50D7F2DAB2DE}**
Number of subkeys: 0
Number of values: 25
Modification Time: 2015-03-25 15:24:51 GMT +00:00

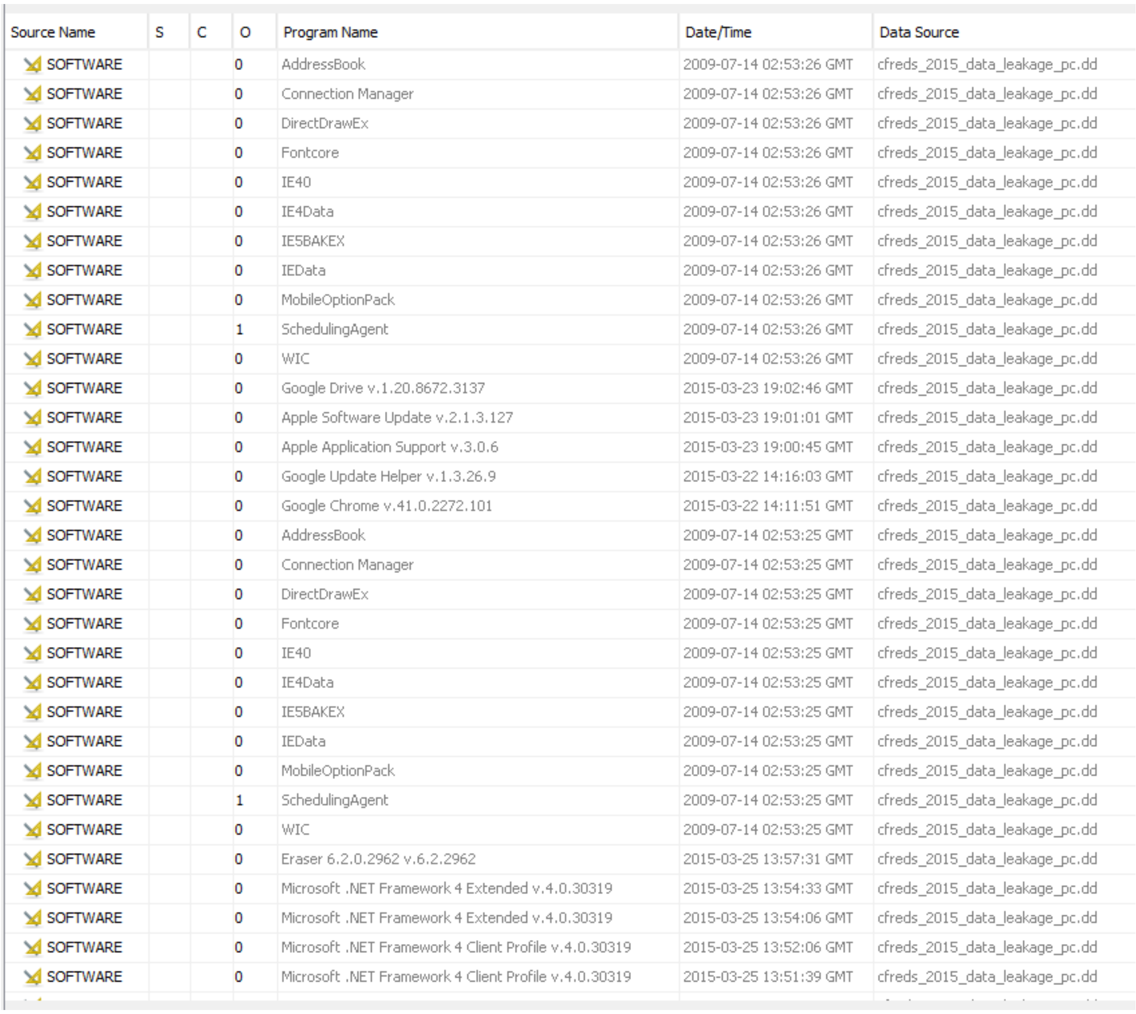
Values

Name	Type	Value
UseZeroBroadcast	REG_DWORD	0x00000000 (0)
EnableDeadGWDetect	REG_DWORD	0x00000001 (1)
EnableDHCP	REG_DWORD	0x00000001 (1)
NameServer	REG_SZ	(value not set)
Domain	REG_SZ	(value not set)
RegistrationEnabled	REG_DWORD	0x00000001 (1)
RegisterAdapterName	REG_DWORD	0x00000000 (0)
DhcpIPAddress	REG_SZ	10.11.11.129
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpServer	REG_SZ	10.11.11.254
Lease	REG_DWORD	0x00000708 (1800)
LeaseObtainedTime	REG_DWORD	0x5512d216 (1427296790)
T1	REG_DWORD	0x5512d59a (1427297690)
T2	REG_DWORD	0x5512d83d (1427298365)
LeaseTerminatesTime	REG_DWORD	0x5512d91e (1427298590)
AddressType	REG_DWORD	0x00000000 (0)
IsServerNapAware	REG_DWORD	0x00000000 (0)
DhcpConnForceBroadcastFlag	REG_DWORD	0x00000000 (0)
DhcpInterfaceOptions	REG_BIN	2C 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00...
DhcpGatewayHardware	REG_BIN	0A 0B 0B 02 06 00 00 00 00 50 56 EB B2 2C
DhcpGatewayHardwareCount	REG_DWORD	0x00000001 (1)
DhcpNameServer	REG_SZ	10.11.11.2
DhcpDefaultGateway	REG_MULTI_SZ	10.11.11.2,
DhcpDomain	REG_SZ	localdomain
DhcpSubnetMaskOpt	REG_MULTI_SZ	255.255.255.0,

8. ¿Qué aplicaciones instaló el sospechoso después de instalar el sistema operativo? (Ruta ejecutable, tiempo de ejecución, conteo de ejecución...)

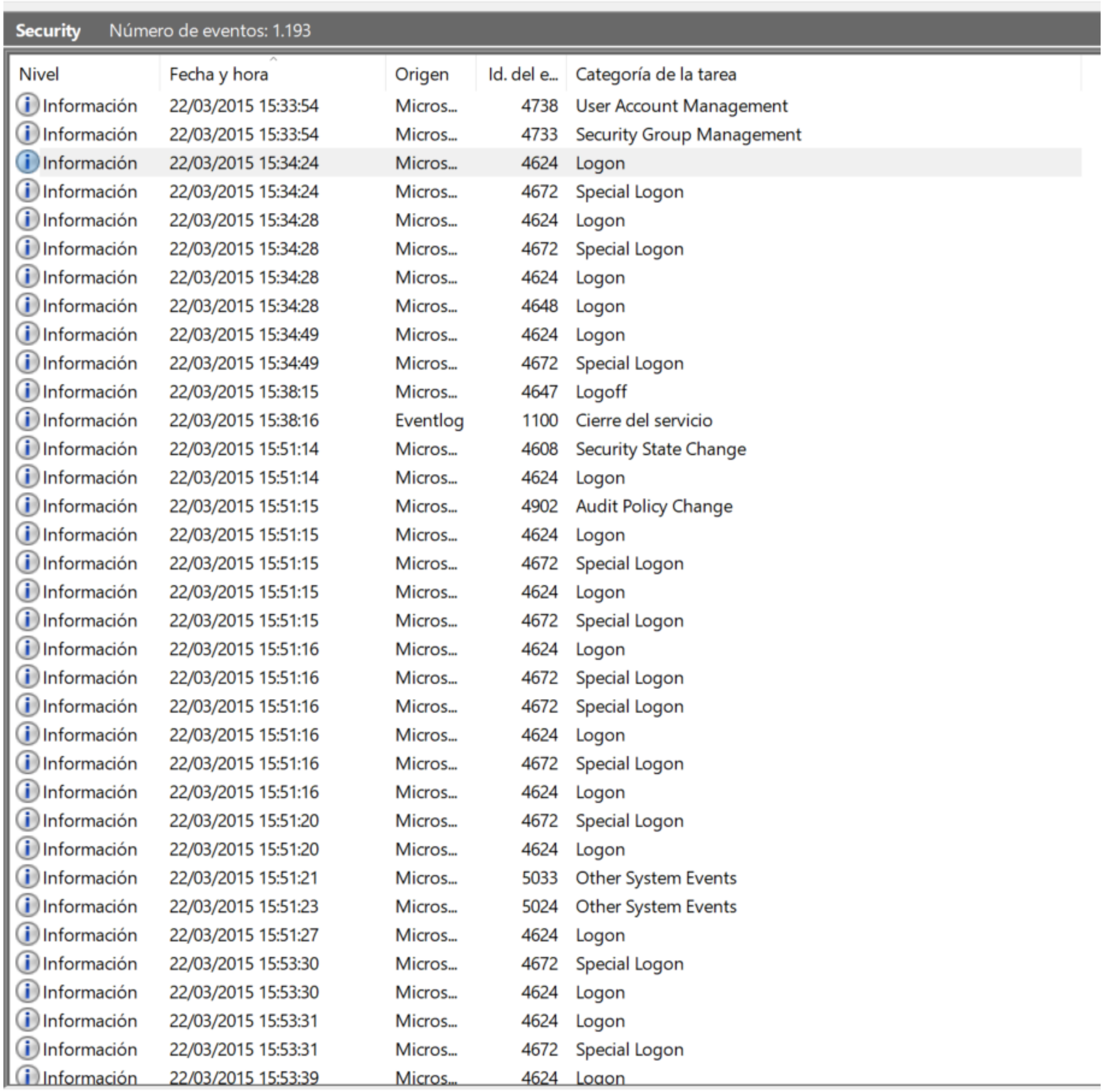


Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	DXM_Runtime	2015-03-25 09:15:21 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	MPlayer2	2015-03-25 09:15:21 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	iCloud v.4.0.6.28	2015-03-23 19:01:54 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Bonjour v.3.0.0.10	2015-03-23 19:00:58 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Office Professional Plus 2013 v.15.0.4420.1017	2015-03-22 14:04:14 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Office Professional Plus 2013 v.15.0.4420.1017	2015-03-22 14:03:33 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Office 32-bit Components 2013 v.15.0.4420.1017	2015-03-22 14:01:46 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Word MUI (English) 2013 v.15.0.4420.1017	2015-03-22 14:01:38 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Outlook MUI (English) 2013 v.15.0.4420.1017	2015-03-22 14:01:37 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Office OSM MUI (English) 2013 v.15.0.4420.1017	2015-03-22 14:01:34 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Office OSM UX MUI (English) 2013 v.15.0.4420.1…	2015-03-22 14:01:34 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Office Proofing (English) 2013 v.15.0.4420.1017	2015-03-22 14:01:32 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Office Proofing Tools 2013 - English v.15.0.4420.…	2015-03-22 14:01:31 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Outils de vérification linguistique 2013 de Microsoft Office -…	2015-03-22 14:01:30 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Office Proofing Tools 2013 - Español v.15.0.4420…	2015-03-22 14:01:14 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft OneNote MUI (English) 2013 v.15.0.4420.1017	2015-03-22 14:01:13 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Groove MUI (English) 2013 v.15.0.4420.1017	2015-03-22 14:01:12 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft DCF MUI (English) 2013 v.15.0.4420.1017	2015-03-22 14:01:11 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Publisher MUI (English) 2013 v.15.0.4420.1017	2015-03-22 14:01:10 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft PowerPoint MUI (English) 2013 v.15.0.4420.1017	2015-03-22 14:01:09 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Excel MUI (English) 2013 v.15.0.4420.1017	2015-03-22 14:01:07 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Lync MUI (English) 2013 v.15.0.4420.1017	2015-03-22 14:01:05 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Office Shared 32-bit MUI (English) 2013 v.15.0.4…	2015-03-22 14:01:04 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft InfoPath MUI (English) 2013 v.15.0.4420.1017	2015-03-22 14:01:03 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Access MUI (English) 2013 v.15.0.4420.1017	2015-03-22 14:01:02 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Access Setup Metadata MUI (English) 2013 v.15.…	2015-03-22 14:01:02 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Office Shared Setup Metadata MUI (English) 201…	2015-03-22 14:01:01 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft Office Shared MUI (English) 2013 v.15.0.4420.1…	2015-03-22 14:00:59 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	AddressBook	2009-07-14 02:53:26 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Connection Manager	2009-07-14 02:53:26 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	DirectDrawEx	2009-07-14 02:53:26 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Fontcore	2009-07-14 02:53:26 GMT	cfreds_2015_data_leakage_pc.dd



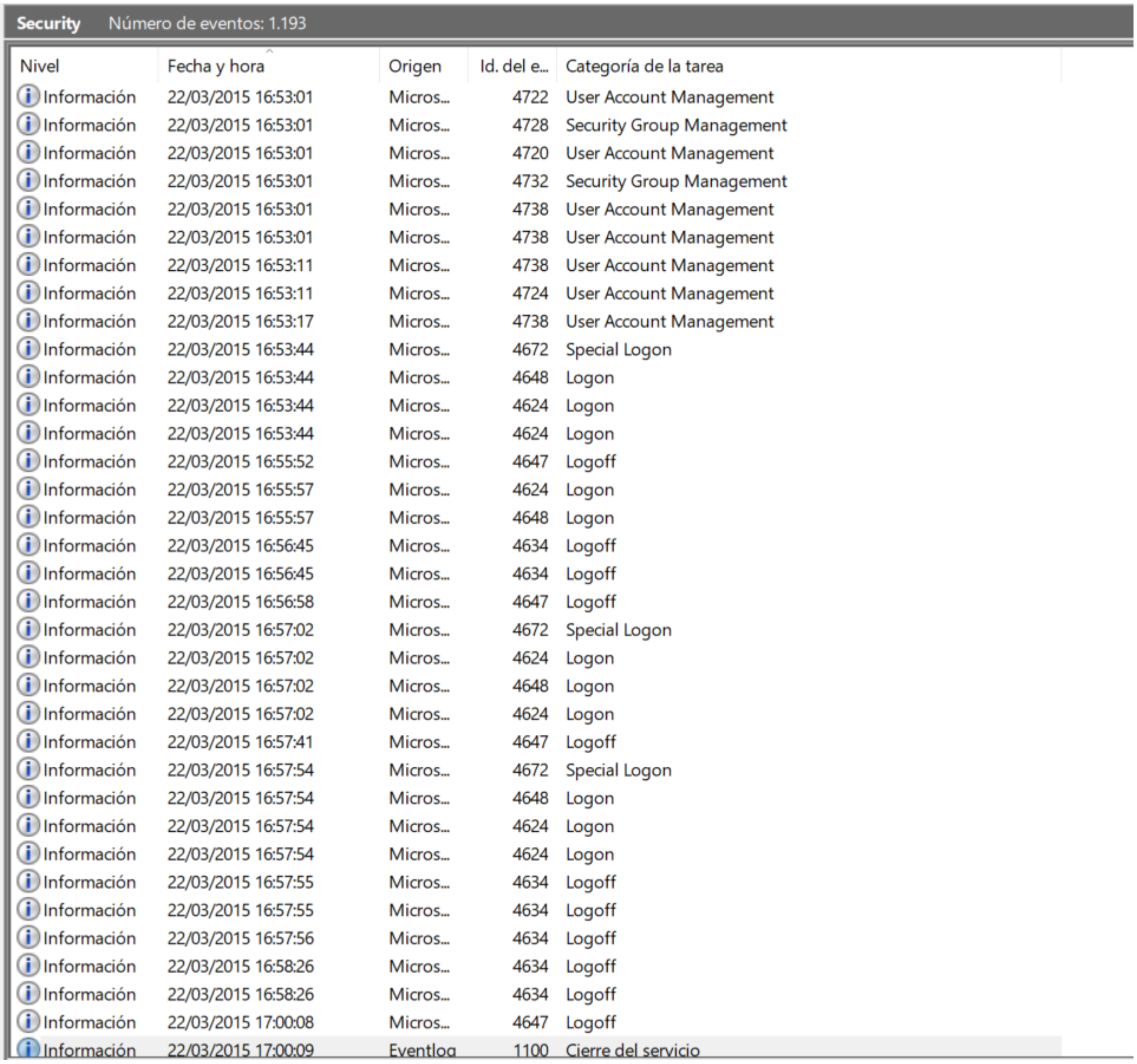
Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	AddressBook	2009-07-14 02:53:26 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Connection Manager	2009-07-14 02:53:26 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	DirectDrawEx	2009-07-14 02:53:26 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Fontcore	2009-07-14 02:53:26 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	IE40	2009-07-14 02:53:26 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	IE4Data	2009-07-14 02:53:26 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	IE5BAKEX	2009-07-14 02:53:26 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	IEData	2009-07-14 02:53:26 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	MobileOptionPack	2009-07-14 02:53:26 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			1	SchedulingAgent	2009-07-14 02:53:26 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	WIC	2009-07-14 02:53:26 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Google Drive v.1.20.8672.3137	2015-03-23 19:02:46 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Apple Software Update v.2.1.3.127	2015-03-23 19:01:01 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Apple Application Support v.3.0.6	2015-03-23 19:00:45 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Google Update Helper v.1.3.26.9	2015-03-22 14:16:03 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Google Chrome v.41.0.2272.101	2015-03-22 14:11:51 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	AddressBook	2009-07-14 02:53:25 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Connection Manager	2009-07-14 02:53:25 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	DirectDrawEx	2009-07-14 02:53:25 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Fontcore	2009-07-14 02:53:25 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	IE40	2009-07-14 02:53:25 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	IE4Data	2009-07-14 02:53:25 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	IE5BAKEX	2009-07-14 02:53:25 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	IEData	2009-07-14 02:53:25 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	MobileOptionPack	2009-07-14 02:53:25 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			1	SchedulingAgent	2009-07-14 02:53:25 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	WIC	2009-07-14 02:53:25 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Eraser 6.2.0.2962 v.6.2.2962	2015-03-25 13:57:31 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft .NET Framework 4 Extended v.4.0.30319	2015-03-25 13:54:33 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft .NET Framework 4 Extended v.4.0.30319	2015-03-25 13:54:06 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft .NET Framework 4 Client Profile v.4.0.30319	2015-03-25 13:52:06 GMT	cfreds_2015_data_leakage_pc.dd
SOFTWARE			0	Microsoft .NET Framework 4 Client Profile v.4.0.30319	2015-03-25 13:51:39 GMT	cfreds_2015_data_leakage_pc.dd

9. Enumere todos los rastros sobre el encendido/apagado del sistema y el inicio/cierre de sesión del usuario.



Security Número de eventos: 1.193

Nivel	Fecha y hora	Origen	Id. del e...	Categoría de la tarea
Información	22/03/2015 15:33:54	Micros...	4738	User Account Management
Información	22/03/2015 15:33:54	Micros...	4733	Security Group Management
Información	22/03/2015 15:34:24	Micros...	4624	Logon
Información	22/03/2015 15:34:24	Micros...	4672	Special Logon
Información	22/03/2015 15:34:28	Micros...	4624	Logon
Información	22/03/2015 15:34:28	Micros...	4672	Special Logon
Información	22/03/2015 15:34:28	Micros...	4624	Logon
Información	22/03/2015 15:34:28	Micros...	4648	Logon
Información	22/03/2015 15:34:49	Micros...	4624	Logon
Información	22/03/2015 15:34:49	Micros...	4672	Special Logon
Información	22/03/2015 15:38:15	Micros...	4647	Logoff
Información	22/03/2015 15:38:16	Eventlog	1100	Cierre del servicio
Información	22/03/2015 15:51:14	Micros...	4608	Security State Change
Información	22/03/2015 15:51:14	Micros...	4624	Logon
Información	22/03/2015 15:51:15	Micros...	4902	Audit Policy Change
Información	22/03/2015 15:51:15	Micros...	4624	Logon
Información	22/03/2015 15:51:15	Micros...	4672	Special Logon
Información	22/03/2015 15:51:15	Micros...	4624	Logon
Información	22/03/2015 15:51:15	Micros...	4672	Special Logon
Información	22/03/2015 15:51:16	Micros...	4624	Logon
Información	22/03/2015 15:51:16	Micros...	4672	Special Logon
Información	22/03/2015 15:51:16	Micros...	4672	Special Logon
Información	22/03/2015 15:51:16	Micros...	4624	Logon
Información	22/03/2015 15:51:16	Micros...	4672	Special Logon
Información	22/03/2015 15:51:16	Micros...	4624	Logon
Información	22/03/2015 15:51:20	Micros...	4672	Special Logon
Información	22/03/2015 15:51:20	Micros...	4624	Logon
Información	22/03/2015 15:51:21	Micros...	5033	Other System Events
Información	22/03/2015 15:51:23	Micros...	5024	Other System Events
Información	22/03/2015 15:51:27	Micros...	4624	Logon
Información	22/03/2015 15:53:30	Micros...	4672	Special Logon
Información	22/03/2015 15:53:30	Micros...	4624	Logon
Información	22/03/2015 15:53:31	Micros...	4624	Logon
Información	22/03/2015 15:53:31	Micros...	4672	Special Logon
Información	22/03/2015 15:53:39	Micros...	4624	Logon

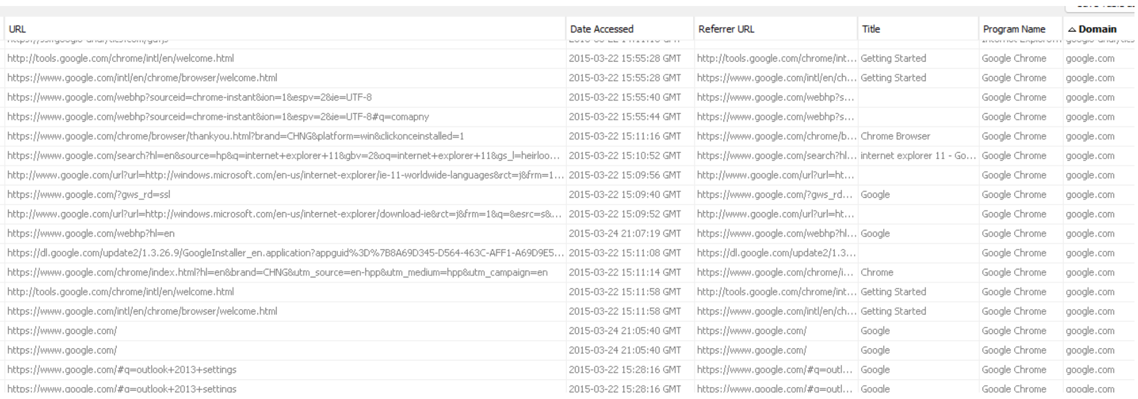


Security Número de eventos: 1.193

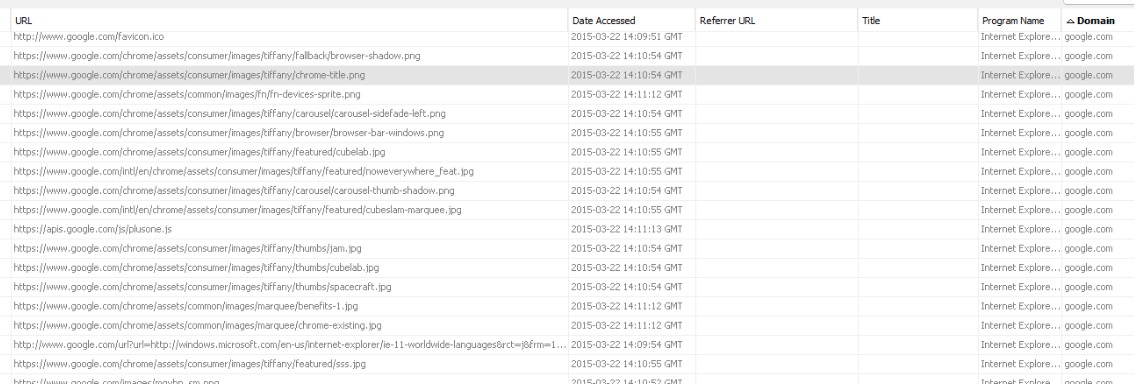
Nivel	Fecha y hora	Origen	Id. del e...	Categoría de la tarea
Información	22/03/2015 16:53:01	Micros...	4722	User Account Management
Información	22/03/2015 16:53:01	Micros...	4728	Security Group Management
Información	22/03/2015 16:53:01	Micros...	4720	User Account Management
Información	22/03/2015 16:53:01	Micros...	4732	Security Group Management
Información	22/03/2015 16:53:01	Micros...	4738	User Account Management
Información	22/03/2015 16:53:01	Micros...	4738	User Account Management
Información	22/03/2015 16:53:11	Micros...	4738	User Account Management
Información	22/03/2015 16:53:11	Micros...	4724	User Account Management
Información	22/03/2015 16:53:17	Micros...	4738	User Account Management
Información	22/03/2015 16:53:44	Micros...	4672	Special Logon
Información	22/03/2015 16:53:44	Micros...	4648	Logon
Información	22/03/2015 16:53:44	Micros...	4624	Logon
Información	22/03/2015 16:53:44	Micros...	4624	Logon
Información	22/03/2015 16:55:52	Micros...	4647	Logoff
Información	22/03/2015 16:55:57	Micros...	4624	Logon
Información	22/03/2015 16:55:57	Micros...	4648	Logon
Información	22/03/2015 16:56:45	Micros...	4634	Logoff
Información	22/03/2015 16:56:45	Micros...	4634	Logoff
Información	22/03/2015 16:56:58	Micros...	4647	Logoff
Información	22/03/2015 16:57:02	Micros...	4672	Special Logon
Información	22/03/2015 16:57:02	Micros...	4624	Logon
Información	22/03/2015 16:57:02	Micros...	4648	Logon
Información	22/03/2015 16:57:02	Micros...	4624	Logon
Información	22/03/2015 16:57:41	Micros...	4647	Logoff
Información	22/03/2015 16:57:54	Micros...	4672	Special Logon
Información	22/03/2015 16:57:54	Micros...	4648	Logon
Información	22/03/2015 16:57:54	Micros...	4624	Logon
Información	22/03/2015 16:57:54	Micros...	4624	Logon
Información	22/03/2015 16:57:55	Micros...	4634	Logoff
Información	22/03/2015 16:57:55	Micros...	4634	Logoff
Información	22/03/2015 16:57:56	Micros...	4634	Logoff
Información	22/03/2015 16:58:26	Micros...	4634	Logoff
Información	22/03/2015 16:58:26	Micros...	4634	Logoff
Información	22/03/2015 17:00:08	Micros...	4647	Logoff
Información	22/03/2015 17:00:09	Eventlog	1100	Cierre del servicio

(Debe considerarse solo durante un intervalo de tiempo entre las 09:00 y las 18:00 en la zona horaria de la Pregunta 4).

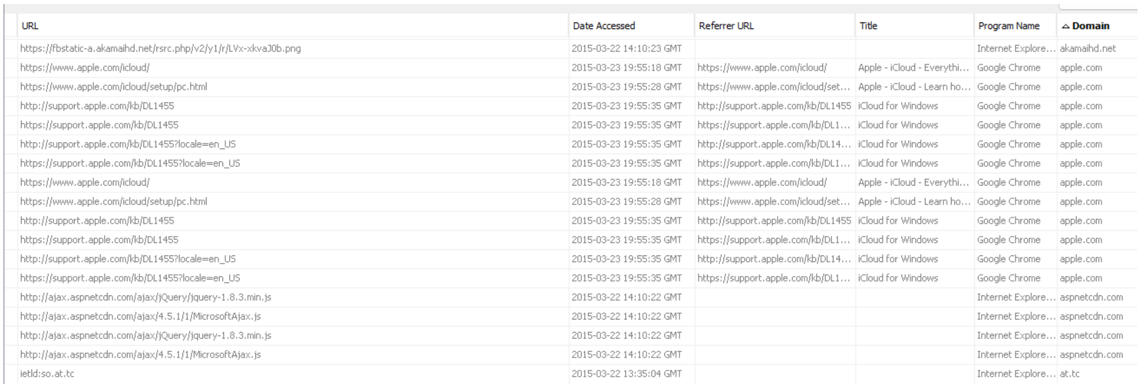
10. ¿A qué sitios web estaba accediendo el sospechoso? (Marca de tiempo, URL...)



URL	Date Accessed	Referrer URL	Title	Program Name	△ Domain
http://tools.google.com/chrome/intl/en/welcome.html	2015-03-22 15:55:28 GMT	http://tools.google.com/chrome/int…	Getting Started	Google Chrome	google.com
https://www.google.com/intl/en/chrome/browser/welcome.html	2015-03-22 15:55:28 GMT	https://www.google.com/intl/en/ch…	Getting Started	Google Chrome	google.com
https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8	2015-03-22 15:55:40 GMT	https://www.google.com/webhp?s…		Google Chrome	google.com
https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=comapny	2015-03-22 15:55:44 GMT	https://www.google.com/webhp?s…		Google Chrome	google.com
https://www.google.com/chrome/browser/thankyou.html?brand=CHNG&platform=win&clickonceinstalled=1	2015-03-22 15:11:16 GMT	https://www.google.com/chrome/b…	Chrome Browser	Google Chrome	google.com
https://www.google.com/search?hl=en&source=hp&q=internet+explorer+11&gbv=2&oq=internet+explorer+11&gs_l=heirloo…	2015-03-22 15:10:52 GMT	https://www.google.com/search?hl…	internet explorer 11 - Go…	Google Chrome	google.com
http://www.google.com/url?url=http://windows.microsoft.com/en-us/internet-explorer/ie-11-worldwide-languages&rct=j&frm=1…	2015-03-22 15:09:56 GMT	http://www.google.com/url?url=ht…		Google Chrome	google.com
https://www.google.com/?gws_rd=ssl	2015-03-22 15:09:40 GMT	https://www.google.com/?gws_rd…	Google	Google Chrome	google.com
http://www.google.com/url?url=http://windows.microsoft.com/en-us/internet-explorer/download-ie&rct=j&frm=1&q=&esrc=s&…	2015-03-22 15:09:52 GMT	http://www.google.com/url?url=ht…		Google Chrome	google.com
https://www.google.com/webhp?hl=en	2015-03-24 21:07:19 GMT	https://www.google.com/webhp?hl…	Google	Google Chrome	google.com
https://dl.google.com/update2/1.3.26.9/GoogleInstaller_en.application?appguid%3D%7B8A69D345-D564-463C-AFF1-A69D9E5…	2015-03-22 15:11:08 GMT	https://dl.google.com/update2/1.3…		Google Chrome	google.com
https://www.google.com/chrome/index.html?hl=en&brand=CHNG&utm_source=en-hpp&utm_medium=hpp&utm_campaign=en	2015-03-22 15:11:14 GMT	https://www.google.com/chrome/i…	Chrome	Google Chrome	google.com
http://tools.google.com/chrome/intl/en/welcome.html	2015-03-22 15:11:58 GMT	http://tools.google.com/chrome/int…	Getting Started	Google Chrome	google.com
https://www.google.com/intl/en/chrome/browser/welcome.html	2015-03-22 15:11:58 GMT	https://www.google.com/intl/en/ch…	Getting Started	Google Chrome	google.com
https://www.google.com/	2015-03-24 21:05:40 GMT	https://www.google.com/	Google	Google Chrome	google.com
https://www.google.com/	2015-03-24 21:05:40 GMT	https://www.google.com/	Google	Google Chrome	google.com
https://www.google.com/#q=outlook+2013+settings	2015-03-22 15:28:16 GMT	https://www.google.com/#q=outl…	Google	Google Chrome	google.com
https://www.google.com/#q=outlook+2013+settings	2015-03-22 15:28:16 GMT	https://www.google.com/#q=outl…	Google	Google Chrome	google.com

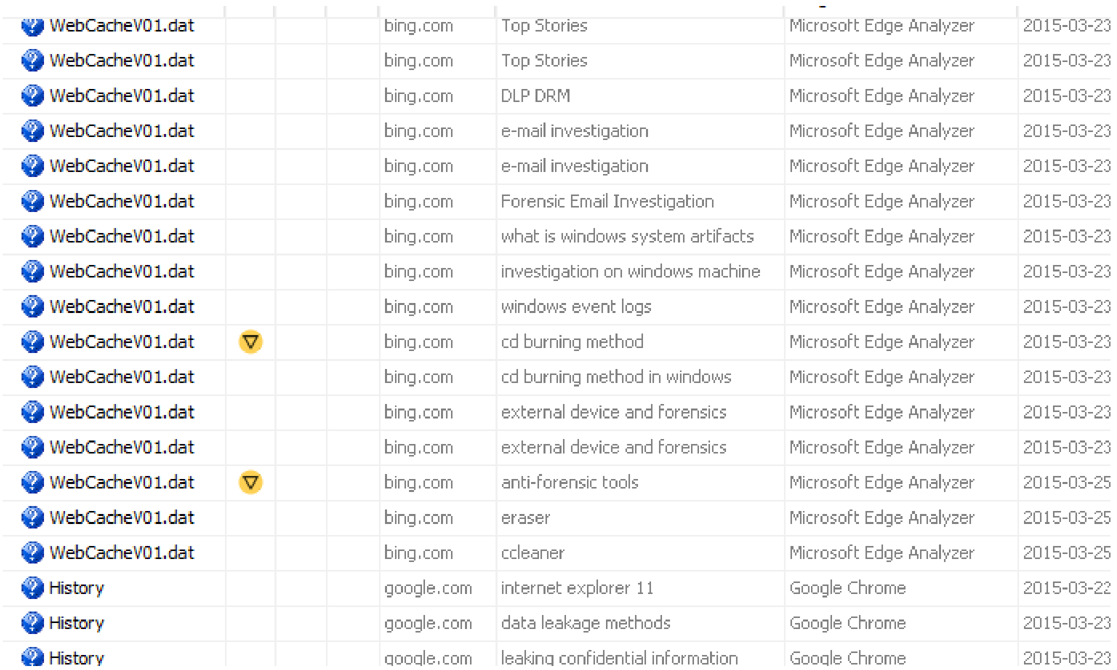


URL	Date Accessed	Referrer URL	Title	Program Name	△ Domain
http://www.google.com/favicon.ico	2015-03-22 14:09:51 GMT			Internet Explore…	google.com
https://www.google.com/chrome/assets/consumer/images/tiffany/fallback/browser-shadow.png	2015-03-22 14:10:54 GMT			Internet Explore…	google.com
https://www.google.com/chrome/assets/consumer/images/tiffany/chrome-title.png	2015-03-22 14:10:54 GMT			Internet Explore…	google.com
https://www.google.com/chrome/assets/common/images/fn/fn-devices-sprite.png	2015-03-22 14:11:12 GMT			Internet Explore…	google.com
https://www.google.com/chrome/assets/consumer/images/tiffany/carousel/carousel-sidefade-left.png	2015-03-22 14:10:54 GMT			Internet Explore…	google.com
https://www.google.com/chrome/assets/consumer/images/tiffany/browser/browser-bar-windows.png	2015-03-22 14:10:55 GMT			Internet Explore…	google.com
https://www.google.com/chrome/assets/consumer/images/tiffany/featured/cubelab.jpg	2015-03-22 14:10:55 GMT			Internet Explore…	google.com
https://www.google.com/intl/en/chrome/assets/consumer/images/tiffany/featured/noweverywhere_feat.jpg	2015-03-22 14:10:55 GMT			Internet Explore…	google.com
https://www.google.com/chrome/assets/consumer/images/tiffany/carousel/carousel-thumb-shadow.png	2015-03-22 14:10:54 GMT			Internet Explore…	google.com
https://www.google.com/intl/en/chrome/assets/consumer/images/tiffany/featured/cubeslam-marquee.jpg	2015-03-22 14:10:55 GMT			Internet Explore…	google.com
https://apis.google.com/js/plusone.js	2015-03-22 14:11:13 GMT			Internet Explore…	google.com
https://www.google.com/chrome/assets/consumer/images/tiffany/thumbs/jam.jpg	2015-03-22 14:10:54 GMT			Internet Explore…	google.com
https://www.google.com/chrome/assets/consumer/images/tiffany/thumbs/cubelab.jpg	2015-03-22 14:10:54 GMT			Internet Explore…	google.com
https://www.google.com/chrome/assets/consumer/images/tiffany/thumbs/spacecraft.jpg	2015-03-22 14:10:54 GMT			Internet Explore…	google.com
https://www.google.com/chrome/assets/common/images/marquee/benefits-1.jpg	2015-03-22 14:11:12 GMT			Internet Explore…	google.com
https://www.google.com/chrome/assets/common/images/marquee/chrome-existing.jpg	2015-03-22 14:11:12 GMT			Internet Explore…	google.com
http://www.google.com/url?url=http://windows.microsoft.com/en-us/internet-explorer/ie-11-worldwide-languages&rct=j&frm=1…	2015-03-22 14:09:54 GMT			Internet Explore…	google.com
https://www.google.com/chrome/assets/consumer/images/tiffany/featured/sss.jpg	2015-03-22 14:10:55 GMT			Internet Explore…	google.com
https://www.google.com/images/mgyhp_sm.png	2015-03-22 14:10:52 GMT			Internet Explore…	google.com



URL	Date Accessed	Referrer URL	Title	Program Name	△ Domain
https://fbstatic-a.akamaihd.net/rsrc.php/v2/y1/r/LVx-xkvaJ0b.png	2015-03-22 14:10:23 GMT			Internet Explore…	akamaihd.net
https://www.apple.com/icloud/	2015-03-23 19:55:18 GMT	https://www.apple.com/icloud/	Apple - iCloud - Everythi…	Google Chrome	apple.com
https://www.apple.com/icloud/setup/pc.html	2015-03-23 19:55:28 GMT	https://www.apple.com/icloud/set…	Apple - iCloud - Learn ho…	Google Chrome	apple.com
http://support.apple.com/kb/DL1455	2015-03-23 19:55:35 GMT	http://support.apple.com/kb/DL1455	iCloud for Windows	Google Chrome	apple.com
https://support.apple.com/kb/DL1455	2015-03-23 19:55:35 GMT	https://support.apple.com/kb/DL1…	iCloud for Windows	Google Chrome	apple.com
http://support.apple.com/kb/DL1455?locale=en_US	2015-03-23 19:55:35 GMT	http://support.apple.com/kb/DL14…	iCloud for Windows	Google Chrome	apple.com
https://support.apple.com/kb/DL1455?locale=en_US	2015-03-23 19:55:35 GMT	https://support.apple.com/kb/DL1…	iCloud for Windows	Google Chrome	apple.com
https://www.apple.com/icloud/	2015-03-23 19:55:18 GMT	https://www.apple.com/icloud/	Apple - iCloud - Everythi…	Google Chrome	apple.com
https://www.apple.com/icloud/setup/pc.html	2015-03-23 19:55:28 GMT	https://www.apple.com/icloud/set…	Apple - iCloud - Learn ho…	Google Chrome	apple.com
http://support.apple.com/kb/DL1455	2015-03-23 19:55:35 GMT	http://support.apple.com/kb/DL1455	iCloud for Windows	Google Chrome	apple.com
https://support.apple.com/kb/DL1455	2015-03-23 19:55:35 GMT	https://support.apple.com/kb/DL1…	iCloud for Windows	Google Chrome	apple.com
http://support.apple.com/kb/DL1455?locale=en_US	2015-03-23 19:55:35 GMT	http://support.apple.com/kb/DL14…	iCloud for Windows	Google Chrome	apple.com
https://support.apple.com/kb/DL1455?locale=en_US	2015-03-23 19:55:35 GMT	https://support.apple.com/kb/DL1…	iCloud for Windows	Google Chrome	apple.com
http://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.8.3.min.js	2015-03-22 14:10:22 GMT			Internet Explore…	aspnetcdn.com
http://ajax.aspnetcdn.com/ajax/4.5.1/1/MicrosoftAjax.js	2015-03-22 14:10:22 GMT			Internet Explore…	aspnetcdn.com
http://ajax.aspnetcdn.com/ajax/jQuery/jquery-1.8.3.min.js	2015-03-22 14:10:22 GMT			Internet Explore…	aspnetcdn.com
http://ajax.aspnetcdn.com/ajax/4.5.1/1/MicrosoftAjax.js	2015-03-22 14:10:22 GMT			Internet Explore…	aspnetcdn.com
ietld:so.at.tc	2015-03-22 13:35:04 GMT			Internet Explore…	at.tc

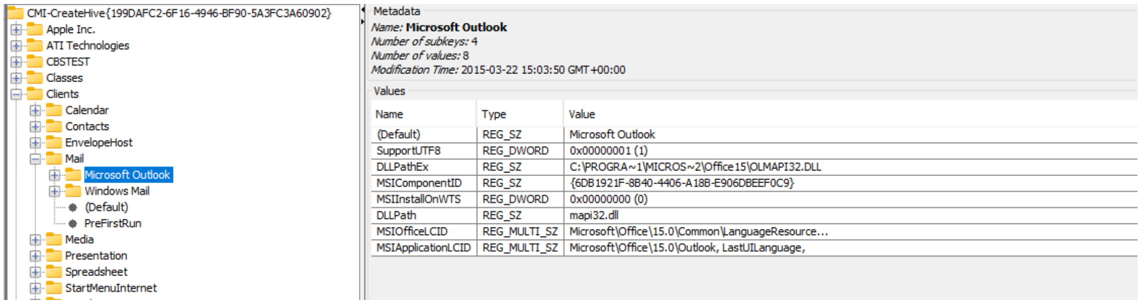
11. Enumere todas las palabras clave de búsqueda utilizando navegadores web. (Marca de tiempo, URL, palabra clave...)



WebCacheV01.dat				bing.com	Top Stories	Microsoft Edge Analyzer	2015-03-23
WebCacheV01.dat				bing.com	Top Stories	Microsoft Edge Analyzer	2015-03-23
WebCacheV01.dat				bing.com	DLP DRM	Microsoft Edge Analyzer	2015-03-23
WebCacheV01.dat				bing.com	e-mail investigation	Microsoft Edge Analyzer	2015-03-23
WebCacheV01.dat				bing.com	e-mail investigation	Microsoft Edge Analyzer	2015-03-23
WebCacheV01.dat				bing.com	Forensic Email Investigation	Microsoft Edge Analyzer	2015-03-23
WebCacheV01.dat				bing.com	what is windows system artifacts	Microsoft Edge Analyzer	2015-03-23
WebCacheV01.dat				bing.com	investigation on windows machine	Microsoft Edge Analyzer	2015-03-23
WebCacheV01.dat				bing.com	windows event logs	Microsoft Edge Analyzer	2015-03-23
WebCacheV01.dat	▽			bing.com	cd burning method	Microsoft Edge Analyzer	2015-03-23
WebCacheV01.dat				bing.com	cd burning method in windows	Microsoft Edge Analyzer	2015-03-23
WebCacheV01.dat				bing.com	external device and forensics	Microsoft Edge Analyzer	2015-03-23
WebCacheV01.dat				bing.com	external device and forensics	Microsoft Edge Analyzer	2015-03-23
WebCacheV01.dat	▽			bing.com	anti-forensic tools	Microsoft Edge Analyzer	2015-03-25
WebCacheV01.dat				bing.com	eraser	Microsoft Edge Analyzer	2015-03-25
WebCacheV01.dat				bing.com	ccleaner	Microsoft Edge Analyzer	2015-03-25
History				google.com	internet explorer 11	Google Chrome	2015-03-22
History				google.com	data leakage methods	Google Chrome	2015-03-23
History				google.com	leaking confidential information	Google Chrome	2015-03-23

12. Enumere todas las palabras clave de los usuarios en la barra de búsqueda del Explorador de Windows. (marca de tiempo, palabra clave)

13. ¿Qué aplicación se utilizó para la comunicación por correo electrónico?



```
CMI-CreateHive{199DAFC2-6F16-4946-BF90-5A3FC3A60902}
  Apple Inc.
  ATI Technologies
  CBSTEST
  Classes
  Clients
    Calendar
    Contacts
    EnvelopeHost
    Mail
      Microsoft Outlook
      Windows Mail
      (Default)
      PreFirstRun
    Media
    Presentation
    Spreadsheet
    StartMenuInternet
```

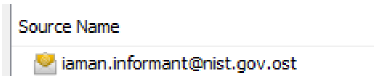
Metadata

Name: **Microsoft Outlook**
Number of subkeys: 4
Number of values: 8
Modification Time: 2015-03-22 15:03:50 GMT+00:00

Values

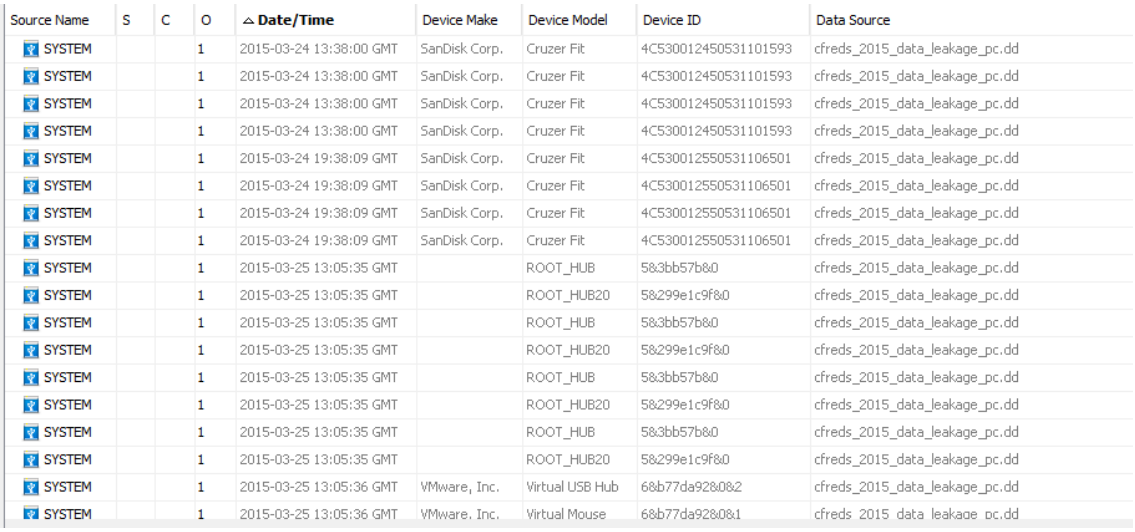
Name	Type	Value
(Default)	REG_SZ	Microsoft Outlook
SupportUTF8	REG_DWORD	0x00000001 (1)
DLLPathEx	REG_SZ	C:\PROGRA~1\MICROS~2\Office15\OLMAPI32.DLL
MSIComponentID	REG_SZ	{6DB1921F-8B40-4406-A18B-E906DBEEF0C9}
MSIInstallOnWTS	REG_DWORD	0x00000000 (0)
DLLPath	REG_SZ	mapi32.dll
MSIOfficeLCID	REG_MULTI_SZ	Microsoft\Office\15.0\Common\LanguageResource...
MSIApplicationLCID	REG_MULTI_SZ	Microsoft\Office\15.0\Outlook, LastUILanguage,

14. ¿Cuál fue la cuenta de correo electrónico utilizada por el sospechoso?



Source Name
iaman.informant@nist.gov.ost

15. Enumere los dispositivos de almacenamiento externo conectados a la PC.

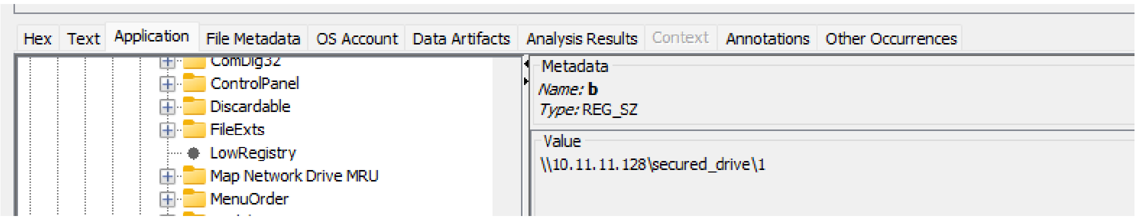


Source Name	S	C	O	△ Date/Time	Device Make	Device Model	Device ID	Data Source
SYSTEM			1	2015-03-24 13:38:00 GMT	SanDisk Corp.	Cruzer Fit	4C530012450531101593	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-24 13:38:00 GMT	SanDisk Corp.	Cruzer Fit	4C530012450531101593	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-24 13:38:00 GMT	SanDisk Corp.	Cruzer Fit	4C530012450531101593	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-24 13:38:00 GMT	SanDisk Corp.	Cruzer Fit	4C530012450531101593	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-24 19:38:09 GMT	SanDisk Corp.	Cruzer Fit	4C530012550531106501	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-24 19:38:09 GMT	SanDisk Corp.	Cruzer Fit	4C530012550531106501	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-24 19:38:09 GMT	SanDisk Corp.	Cruzer Fit	4C530012550531106501	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-24 19:38:09 GMT	SanDisk Corp.	Cruzer Fit	4C530012550531106501	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-25 13:05:35 GMT		ROOT_HUB	5&3bb57b&0	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-25 13:05:35 GMT		ROOT_HUB20	5&299e1c9f&0	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-25 13:05:35 GMT		ROOT_HUB	5&3bb57b&0	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-25 13:05:35 GMT		ROOT_HUB20	5&299e1c9f&0	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-25 13:05:35 GMT		ROOT_HUB	5&3bb57b&0	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-25 13:05:35 GMT		ROOT_HUB20	5&299e1c9f&0	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-25 13:05:35 GMT		ROOT_HUB	5&3bb57b&0	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-25 13:05:35 GMT		ROOT_HUB20	5&299e1c9f&0	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-25 13:05:36 GMT	VMware, Inc.	Virtual USB Hub	6&b77da92&0&2	cfreds_2015_data_leakage_pc.dd
SYSTEM			1	2015-03-25 13:05:36 GMT	VMware, Inc.	Virtual Mouse	6&b77da92&0&1	cfreds_2015_data_leakage_pc.dd

16. Identifique todos los rastros relacionados con el "cambio de nombre" de los archivos en el escritorio de Windows.

(Debe considerarse solo durante un rango de fechas entre 2015-03-23 y 2015-03-24). [Sugerencia: los directorios principales de los archivos renombrados se eliminaron y sus entradas MFT también se sobrescribieron. Por lo tanto, es posible que no pueda encontrar sus rutas completas.]

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

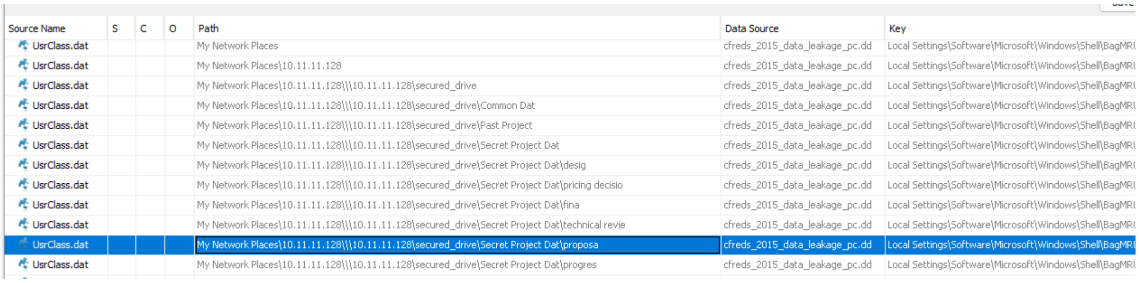


ComDlg32
ControlPanel
Discardable
FileExts
LowRegistry
Map Network Drive MRU
MenuOrder

Metadata
Name: **b**
Type: REG_SZ

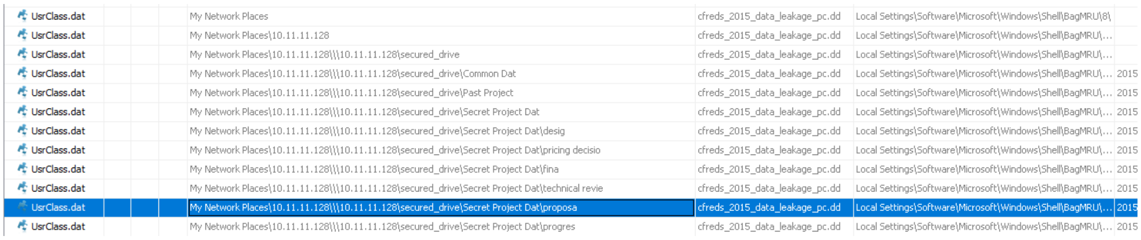
Value
\\10.11.11.128\secured_drive\1

18. Enumere todos los directorios y ficheros que se traspasaron en 'RM#2'.



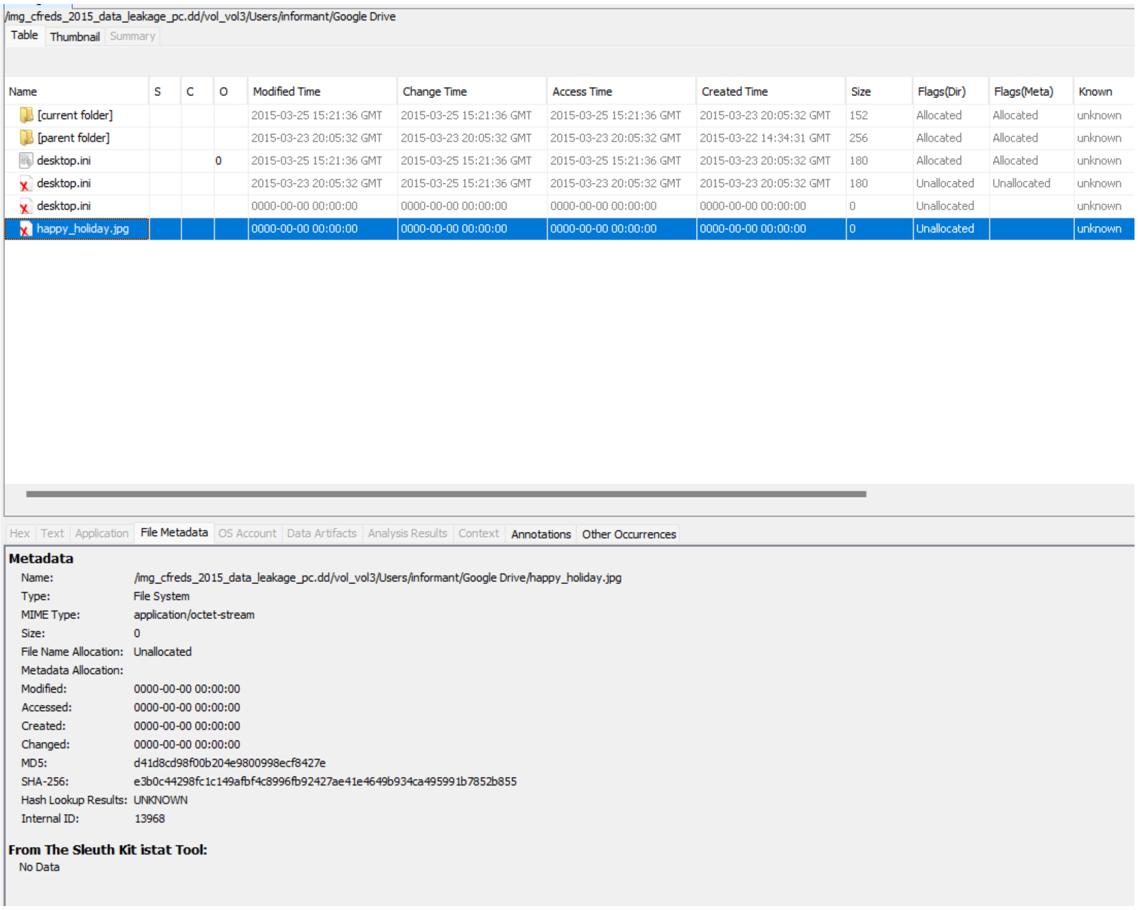
Source Name	S	C	O	Path	Data Source	Key
UsrClass.dat				My Network Places	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU
UsrClass.dat				My Network Places\10.11.11.128	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Common Dat	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Past Project	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Secret Project Dat	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Secret Project Dat\desig	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Secret Project Dat\pricing decisio	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Secret Project Dat\fina	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Secret Project Dat\technical revie	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Secret Project Dat\proposa	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Secret Project Dat\progres	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU

19. Enumere todos los directorios que se traspasaron en la unidad de red de la empresa.



UsrClass.dat				My Network Places	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\8\	
UsrClass.dat				My Network Places\10.11.11.128	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...	
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...	
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Common Dat	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...	2015
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Past Project	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...	2015
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Secret Project Dat	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...	2015
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Secret Project Dat\desig	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...	2015
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Secret Project Dat\pricing decisio	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...	2015
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Secret Project Dat\fina	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...	2015
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Secret Project Dat\technical revie	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...	2015
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Secret Project Dat\proposa	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...	2015
UsrClass.dat				My Network Places\10.11.11.128\\\10.11.11.128\secured_drive\Secret Project Dat\progres	cfreds_2015_data_leakage_pc.dd	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...	2015

20. ¿Qué archivos se eliminaron de Google Drive? Encuentre el nombre de archivo y la marca de tiempo modificada del archivo. [Sugerencia: busque un archivo de registro de transacciones de Google Drive.]



/img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Users/informant/Google Drive

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
[current folder]				2015-03-25 15:21:36 GMT	2015-03-25 15:21:36 GMT	2015-03-25 15:21:36 GMT	2015-03-23 20:05:32 GMT	152	Allocated	Allocated	unknown
[parent folder]				2015-03-23 20:05:32 GMT	2015-03-23 20:05:32 GMT	2015-03-23 20:05:32 GMT	2015-03-22 14:34:31 GMT	256	Allocated	Allocated	unknown
desktop.ini			0	2015-03-25 15:21:36 GMT	2015-03-25 15:21:36 GMT	2015-03-25 15:21:36 GMT	2015-03-23 20:05:32 GMT	180	Allocated	Allocated	unknown
desktop.ini				2015-03-23 20:05:32 GMT	2015-03-25 15:21:36 GMT	2015-03-23 20:05:32 GMT	2015-03-23 20:05:32 GMT	180	Unallocated	Unallocated	unknown
desktop.ini				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown
happy_holiday.jpg				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated		unknown

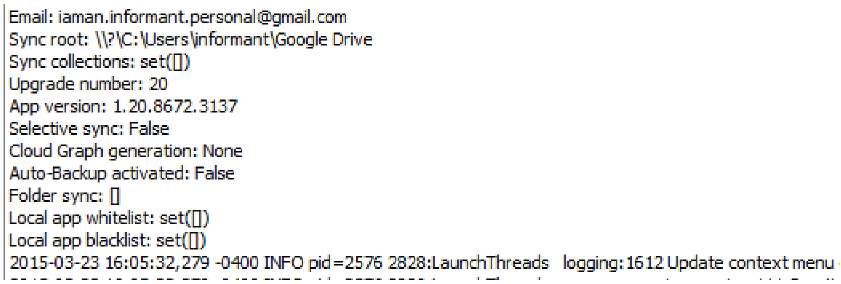
Metadata

```
Name:                  /img_cfreds_2015_data_leakage_pc.dd/vol_vol3/Users/informant/Google Drive/happy_holiday.jpg
Type:                  File System
MIME Type:             application/octet-stream
Size:                  0
File Name Allocation:  Unallocated
Metadata Allocation:
Modified:              0000-00-00 00:00:00
Accessed:              0000-00-00 00:00:00
Created:               0000-00-00 00:00:00
Changed:               0000-00-00 00:00:00
MD5:                   d41d8cd98f00b204e9800998ecf8427e
SHA-256:               e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
Hash Lookup Results:   UNKNOWN
Internal ID:           13968
```

From The Sleuth Kit istat Tool:

No Data

21. Identifique la información de la cuenta para sincronizar Google Drive.



```
Email: iaman.informant.personal@gmail.com
Sync root: \\?\C:\Users\informant\Google Drive
Sync collections: set([])
Upgrade number: 20
App version: 1.20.8672.3137
Selective sync: False
Cloud Graph generation: None
Auto-Backup activated: False
Folder sync: []
Local app whitelist: set([])
Local app blacklist: set([])
2015-03-23 16:05:32,279 -0400 INFO pid=2576 2828:LaunchThreads   logging:1612 Update context menu
```

22. Crea un timeline de los sucesos notables.

- Behavior of the suspect

> 2015-03-22: Normal business works (installation and configuration of apps)

> 2015-03-23: Transferring sample confidential data through the internet

> 2015-03-24: Copying confidential data to storage devices

> 2015-03-25: Trying to do anti-forensics and take storage devices out

- Some traces may be hard to be exactly identified from the images.