1. **Hashing** ([Comandos para hashing](#hashing))

**Los valores estan en las imagenes en la carpeta hash**

¿Cuál es la importancia forense de los hashes?

Los hash o funciones de resumen son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, una contraseña o un archivo, por ejemplo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado (es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos).

Un Hash es un valor único generado por un algoritmo criptográfico. Los valores Hash (funciones) son utilizados en una diversidad de maneras, incluyendo integridad de la evidencia y criptografía. Los valores Hash son comúnmente referidos como una “huella digital” o un “ADN digital”. Cualquier cambio en el dispositivo de almacenamiento, incluso un sólo bit, resultará en valor Hash diferente. Por lo tanto, cualquier alteración o manipulación de la evidencia es fácilmente detectable.

Los algoritmos hash son utilizados en situaciones en las que es necesario o conveniente verificar esta identidad de contenido interno como, por ejemplo, cuando se aporta un fichero en una investigación forense, o cuando alguien se descarga un software o un fichero y se quiere comprobar que es idéntico al que los desarrolladores han liberado en origen, o quizás, para verificar si algún fichero de un Sistema o de un Aplicativo ha sido modificado por un malware introduciéndole una cadena de código malicioso.

¿Cómo se puede mejorar el proceso forense a través del uso de hashes?

En la investigación forense se utiliza el cálculo de los valores hash a nivel global o extendido en las carpetas sobre sus ficheros para poder comparar el contenido de dispositivos frente a otros dispositivos o las carpetas conteniendo ficheros incautados

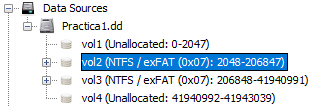
Se utiliza en la fase de adquisición forense de los datos informáticos

* Primero, se aplica un algoritmo a todo el contenido del disco duro original y se obtiene como resultado una primera clave denominada en informática “clave HASH” (o huella digital). La “clave HASH” se genera en función de todos los datos contenidos en el disco duro original y es única para cada contenido de un disco duro. Haciendo un símil, se obtiene el ADN del contenido del disco duro.
* Luego, se aplica idéntico algoritmo (aplicado al contenido del disco duro original) a toda la imagen o copia de datos realizada del disco duro original y se obtiene como resultado una segunda “clave HASH” (o huella digital).
* Finalmente, se comparan las 2 “clave HASH” obtenidas; estas son: la del contenido del disco duro original y la de la imagen o copia realizada. Si ambos valores coinciden, la imagen o copia se ha realizado correctamente; si no coinciden, es necesario repetir todo el proceso de “adquisición forense de los datos informáticos”.

**Particiones del disco duro**

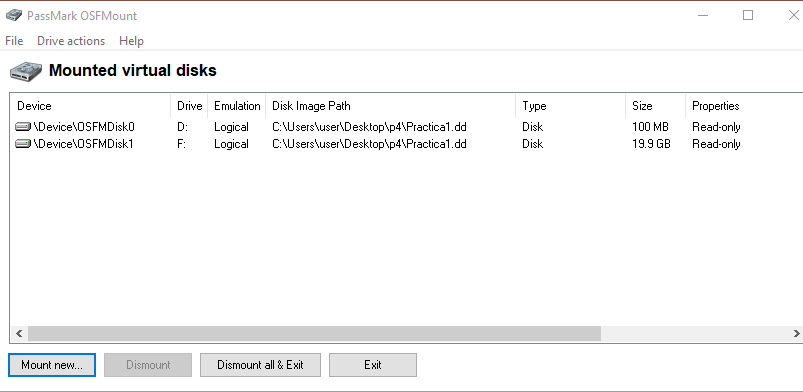
¿Cuantas particiones tiene el disco?

**2**



Vol 2 y vol 3

**¿Cuál partición contiene la información?**



Vol3 /F:

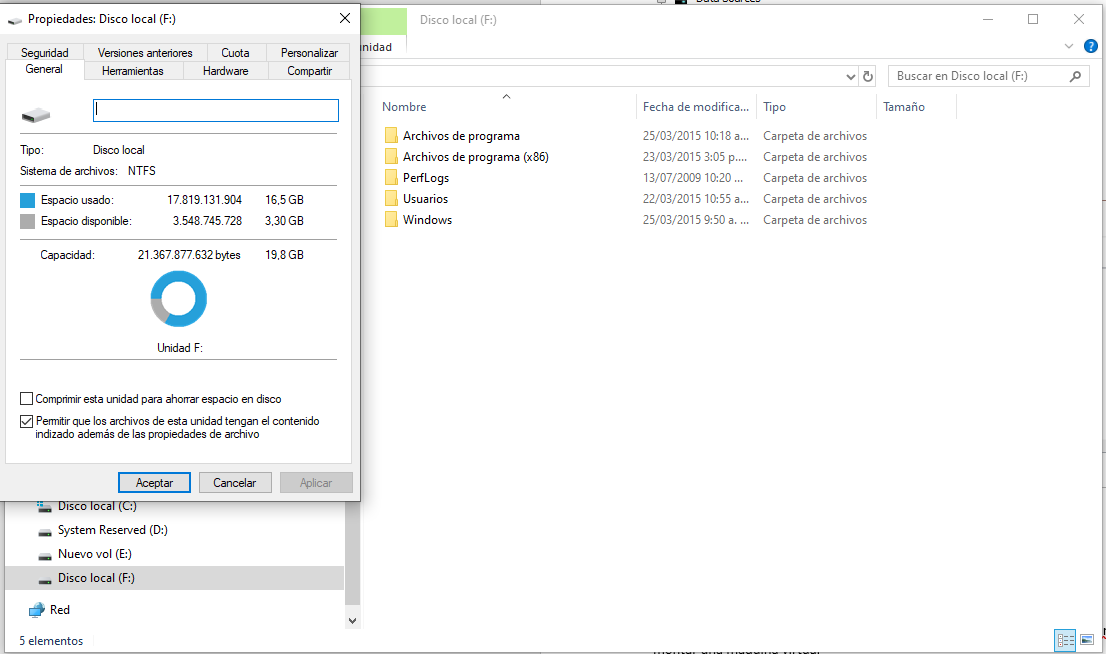
**La partición que contiene la información ¿En qué sector inicia?**

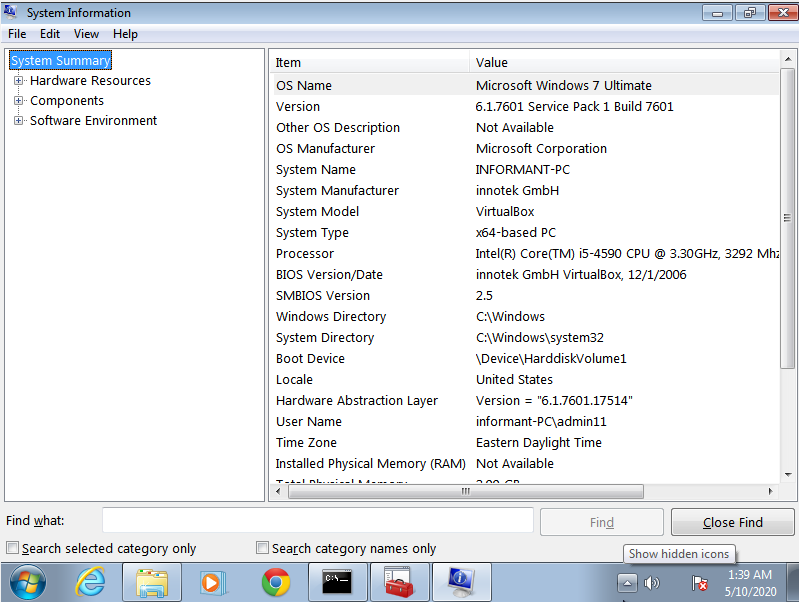


Inicia en 206848

**Identifique si es posible montar la partición de la información**

Si es posible montar la particion , se puede montar con OSFMount, o convirtiendo .dd a .VDI y montar una maquina virtual

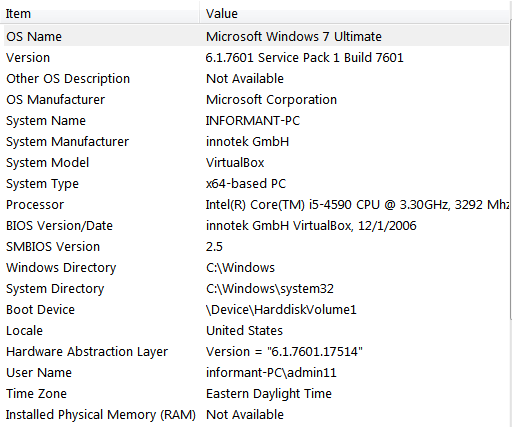




**Información del sistema operativo**

**1**

Identifique con detalle cual es el sistema operativo instalado



2.Nombre del sistema operative

Microsoft Windows 7 Ultimate

3. Versión

6.1.7601 service pack 1 build 7601

4.fecha instalacion



5 registrado a



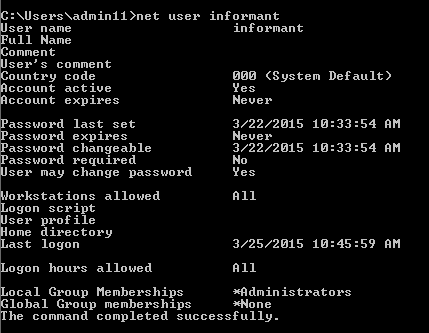
6 nombre del pc



7 time zone

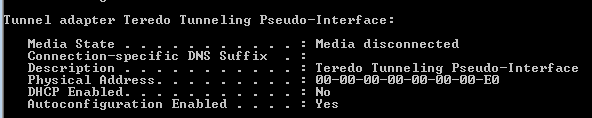


8 ¿Quién inició sesión por última vez?

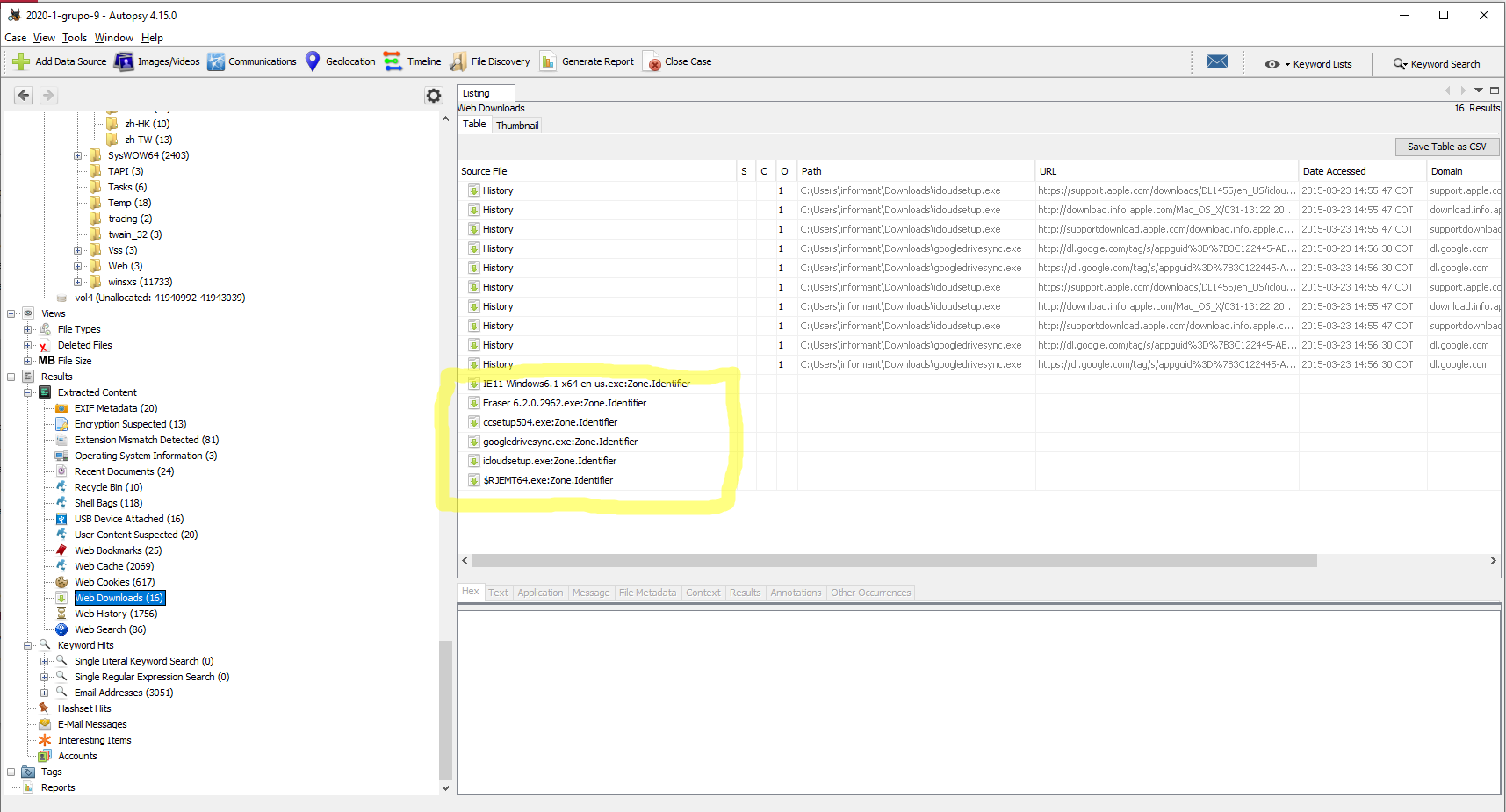


9. Extraiga la información de las interfaces de red





10.¿Qué aplicaciones instaló el sospechoso?



11. Extraiga los logs de uso de las aplicaciones

"Key","Index","Name","Counter","Last","Last UTC","Focus counter?","Focus time?","Flags?"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","44","{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\xpsrchvw.exe","1","3/25/2015 11:28:47 AM","3/25/2015 3:28:47 PM","1","19921","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","25","{6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office\Office15\WINWORD.EXE","4","3/25/2015 11:24:48 AM","3/25/2015 3:24:48 PM","10","844511","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","31","{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Google\Drive\googledrivesync.exe","1","3/25/2015 11:21:30 AM","3/25/2015 3:21:30 PM","0","78265","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","19","{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Google Drive\Google Drive.lnk","1","3/25/2015 11:21:30 AM","3/25/2015 3:21:30 PM","0","1","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","42","{6D809377-6AF0-444B-8957-A3773F02200E}\CCleaner\CCleaner64.exe","1","3/25/2015 11:15:50 AM","3/25/2015 3:15:50 PM","1","22651","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","18","C:\Users\Public\Desktop\CCleaner.lnk","1","3/25/2015 11:15:50 AM","3/25/2015 3:15:50 PM","0","1","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","41","{6D809377-6AF0-444B-8957-A3773F02200E}\Eraser\Eraser.exe","1","3/25/2015 11:12:28 AM","3/25/2015 3:12:28 PM","2","70138","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","17","C:\Users\Public\Desktop\Eraser.lnk","1","3/25/2015 11:12:28 AM","3/25/2015 3:12:28 PM","0","1","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","40","C:\Users\informant\Desktop\Download\ccsetup504.exe","1","3/25/2015 10:57:56 AM","3/25/2015 2:57:56 PM","0","4274","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","38","C:\Users\informant\Desktop\Download\Eraser 6.2.0.2962.exe","1","3/25/2015 10:50:14 AM","3/25/2015 2:50:14 PM","0","2433","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","15","Microsoft.InternetExplorer.Default","5","3/25/2015 10:46:05 AM","3/25/2015 2:46:05 PM","32","1200321","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","11","{9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Internet Explorer.lnk","5","3/25/2015 10:46:05 AM","3/25/2015 2:46:05 PM","0","5","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","37","Microsoft.Windows.MediaPlayer32","1","3/25/2015 10:42:47 AM","3/25/2015 2:42:47 PM","0","2403","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","16","{9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Windows Media Player.lnk","1","3/25/2015 10:42:47 AM","3/25/2015 2:42:47 PM","0","1","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","22","{6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office\Office15\OUTLOOK.EXE","5","3/25/2015 10:41:03 AM","3/25/2015 2:41:03 PM","0","0","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","13","{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Microsoft Office 2013\Outlook 2013.lnk","5","3/25/2015 10:41:03 AM","3/25/2015 2:41:03 PM","0","5","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","18","Chrome","7","3/24/2015 5:05:38 PM","3/24/2015 9:05:38 PM","42","2218756","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","14","{9E3995AB-1F9C-4F13-B827-48B24B6C7174}\TaskBar\Google Chrome.lnk","5","3/24/2015 5:05:38 PM","3/24/2015 9:05:38 PM","0","5","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","15","{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Microsoft Office 2013\Word 2013.lnk","1","3/24/2015 2:32:15 PM","3/24/2015 6:32:15 PM","0","1","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","4","Microsoft.Windows.StickyNotes","13","3/24/2015 2:31:55 PM","3/24/2015 6:31:55 PM","23","371776","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","4","{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Sticky Notes.lnk","13","3/24/2015 2:31:55 PM","3/24/2015 6:31:55 PM","0","13","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","9","::{ED228FDF-9EA8-4870-83B1-96B02CFE0D52}\{00D8862B-6453-4957-A821-3D98D74C76BE}","7","3/24/2015 2:29:07 PM","3/24/2015 6:29:07 PM","0","7","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","35","{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\rundll32.exe","1","3/24/2015 10:16:37 AM","3/24/2015 2:16:37 PM","0","0","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","27","{6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office\Office15\POWERPNT.EXE","2","3/23/2015 4:27:33 PM","3/23/2015 8:27:33 PM","0","15835","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","33","{6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office\Office15\EXCEL.EXE","1","3/23/2015 4:26:50 PM","3/23/2015 8:26:50 PM","0","10359","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","14","{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe","4","3/23/2015 4:10:19 PM","3/23/2015 8:10:19 PM","2","39296","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","12","C:\Users\Public\Desktop\Google Chrome.lnk","2","3/23/2015 1:26:50 PM","3/23/2015 5:26:50 PM","0","2","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","20","{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\slui.exe","3","3/22/2015 11:24:47 AM","3/22/2015 3:24:47 PM","0","9517","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","19","C:\Users\informant\Desktop\Download\IE11-Windows6.1-x64-en-us.exe","1","3/22/2015 11:12:32 AM","3/22/2015 3:12:32 PM","2","331409","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","0","Microsoft.Windows.GettingStarted","14","3/22/2015 10:33:13 AM","3/22/2015 2:33:13 PM","21","420000","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","2","Microsoft.Windows.MediaCenter","13","3/22/2015 10:33:13 AM","3/22/2015 2:33:13 PM","19","380000","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","3","{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\calc.exe","12","3/22/2015 10:33:13 AM","3/22/2015 2:33:13 PM","17","340000","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","5","{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe","10","3/22/2015 10:33:13 AM","3/22/2015 2:33:13 PM","13","260000","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","6","{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe","9","3/22/2015 10:33:13 AM","3/22/2015 2:33:13 PM","11","220000","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","7","Microsoft.Windows.RemoteDesktop","8","3/22/2015 10:33:13 AM","3/22/2015 2:33:13 PM","9","180000","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","8","{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\magnify.exe","7","3/22/2015 10:33:13 AM","3/22/2015 2:33:13 PM","7","140000","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","9","{6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Games\Solitaire\solitaire.exe","6","3/22/2015 10:33:13 AM","3/22/2015 2:33:13 PM","6","102138","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","0","{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Welcome Center.lnk","14","3/22/2015 10:33:13 AM","3/22/2015 2:33:13 PM","0","14","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","2","{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Media Center.lnk","13","3/22/2015 10:33:13 AM","3/22/2015 2:33:13 PM","0","13","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","3","{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Calculator.lnk","12","3/22/2015 10:33:13 AM","3/22/2015 2:33:13 PM","0","12","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","5","{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Snipping Tool.lnk","10","3/22/2015 10:33:13 AM","3/22/2015 2:33:13 PM","0","10","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","6","{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Paint.lnk","9","3/22/2015 10:33:13 AM","3/22/2015 2:33:13 PM","0","9","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","7","{0139D44E-6AFE-49F2-8690-3DAFCAE6FFB8}\Accessories\Remote Desktop Connection.lnk","8","3/22/2015 10:33:13 AM","3/22/2015 2:33:13 PM","0","8","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","8","{A77F5D77-2E2B-44C3-A6A2-ABA601054A51}\Accessories\Accessibility\Magnify.lnk","7","3/22/2015 10:33:13 AM","3/22/2015 2:33:13 PM","0","7","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","1","UEME\_CTLSESSION","","","","","",""

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","10","UEME\_CTLCUACount:ctor","0","","","0","0","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","11","Microsoft.Windows.ControlPanel","0","","","9","295044","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","12","{F38BF404-1D43-42F2-9305-67DE0B28FC23}\explorer.exe","0","","","121","5631069","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","13","Microsoft.Windows.Shell.RunDialog","0","","","8","121664","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","16","{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\GUMBAD6.tmp\GoogleUpdate.exe","0","","","2","1748","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","17","{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Google\Update\GoogleUpdate.exe","0","","","3","61979","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","21","{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\wscript.exe","0","","","0","967","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","23","Microsoft.Office.OUTLOOK.EXE.15","0","","","83","2558835","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","24","Microsoft.Windows.ControlPanel.Taskbar","0","","","0","12386","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","26","{6D809377-6AF0-444B-8957-A3773F02200E}\Microsoft Office\Office15\FIRSTRUN.EXE","0","","","0","1482","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","28","C:\Users\informant\Downloads\icloudsetup.exe","0","","","0","2465","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","29","Microsoft.Windows.WindowsInstaller","0","","","0","890","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","30","{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\GUMA94B.tmp\GoogleUpdate.exe","0","","","3","1155","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","32","{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Common Files\Apple\Internet Services\iCloud.exe","0","","","1","1888","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","34","{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\taskmgr.exe","0","","","0","1607","0"

"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","36","Microsoft.Windows.PhotoViewer","0","","","0","936","0"

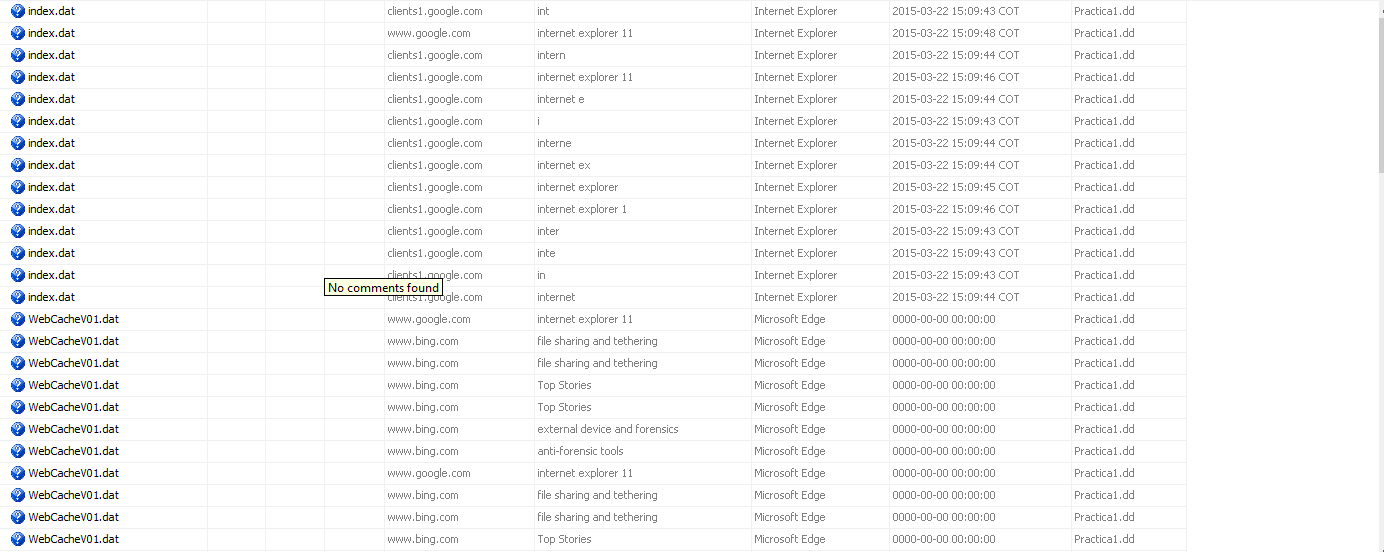
"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","39","C:\Users\informant\AppData\Local\Temp\eraserInstallBootstrapper\dotNetFx40\_Full\_setup.exe","0","","","0","655","0"

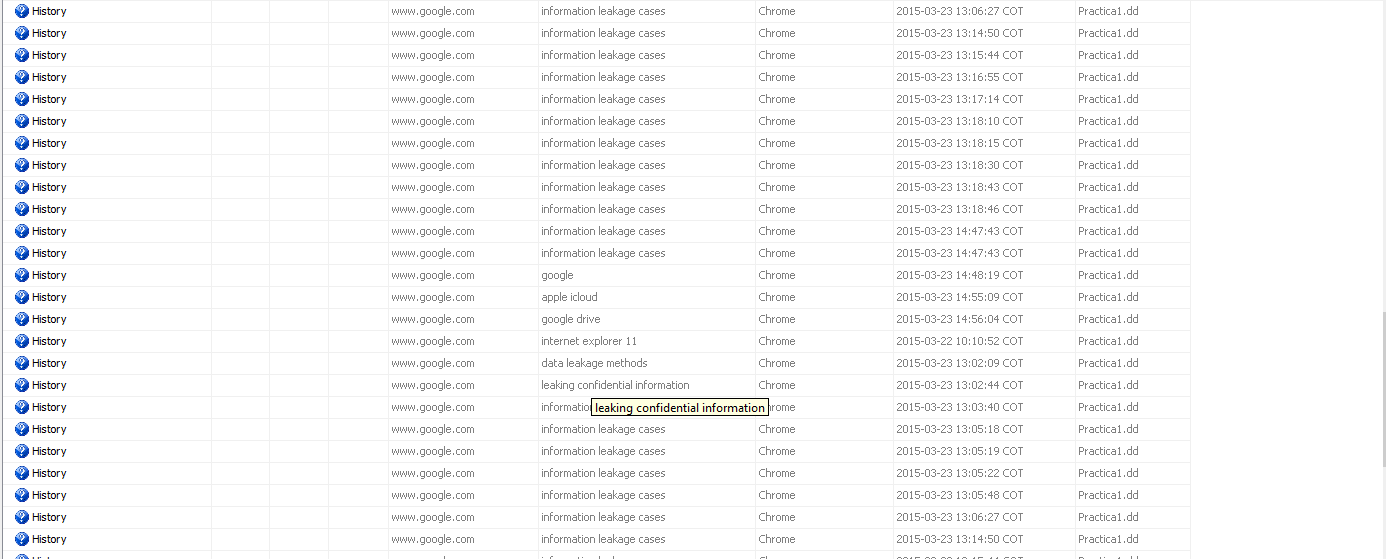
"{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}","43","C:\Users\informant\AppData\Local\Temp\~nsu.tmp\Au\_.exe","0","","","0","12667","0"

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","1","UEME\_CTLSESSION","","","","","",""

"{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}","10","UEME\_CTLCUACount:ctor","0","","","0","0","0"

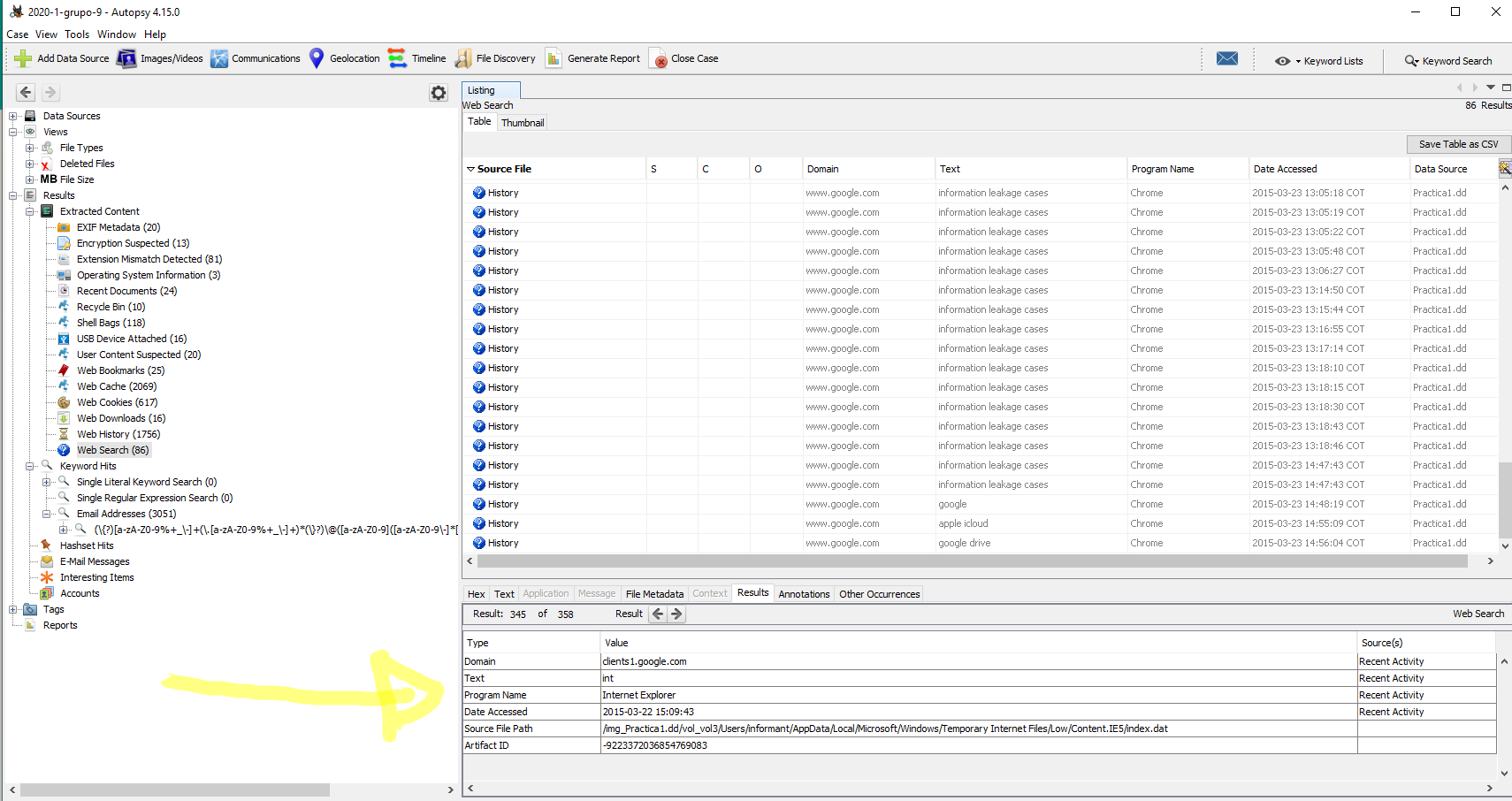
12. ¿Cuáles navegadores fueron usados?

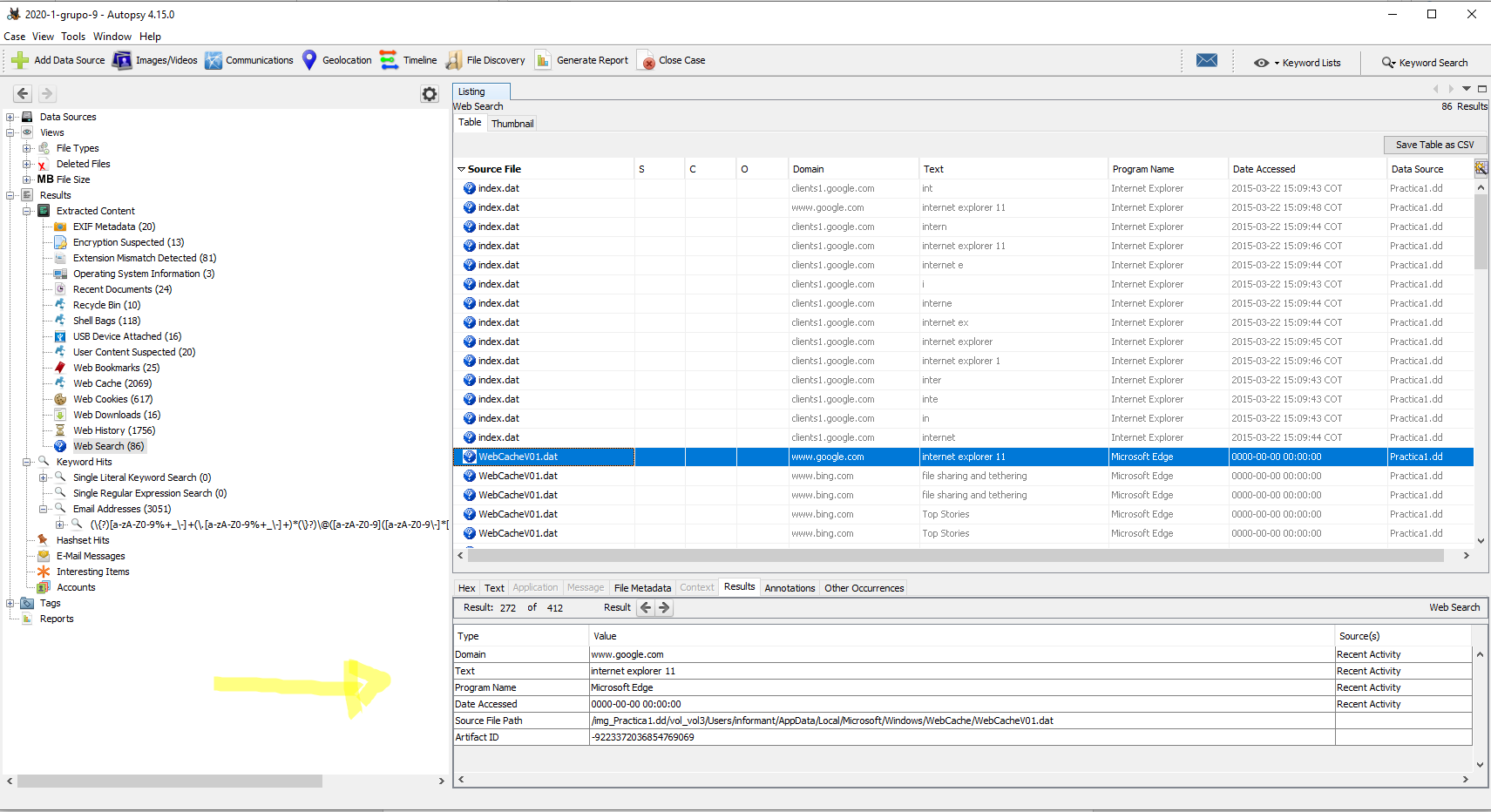


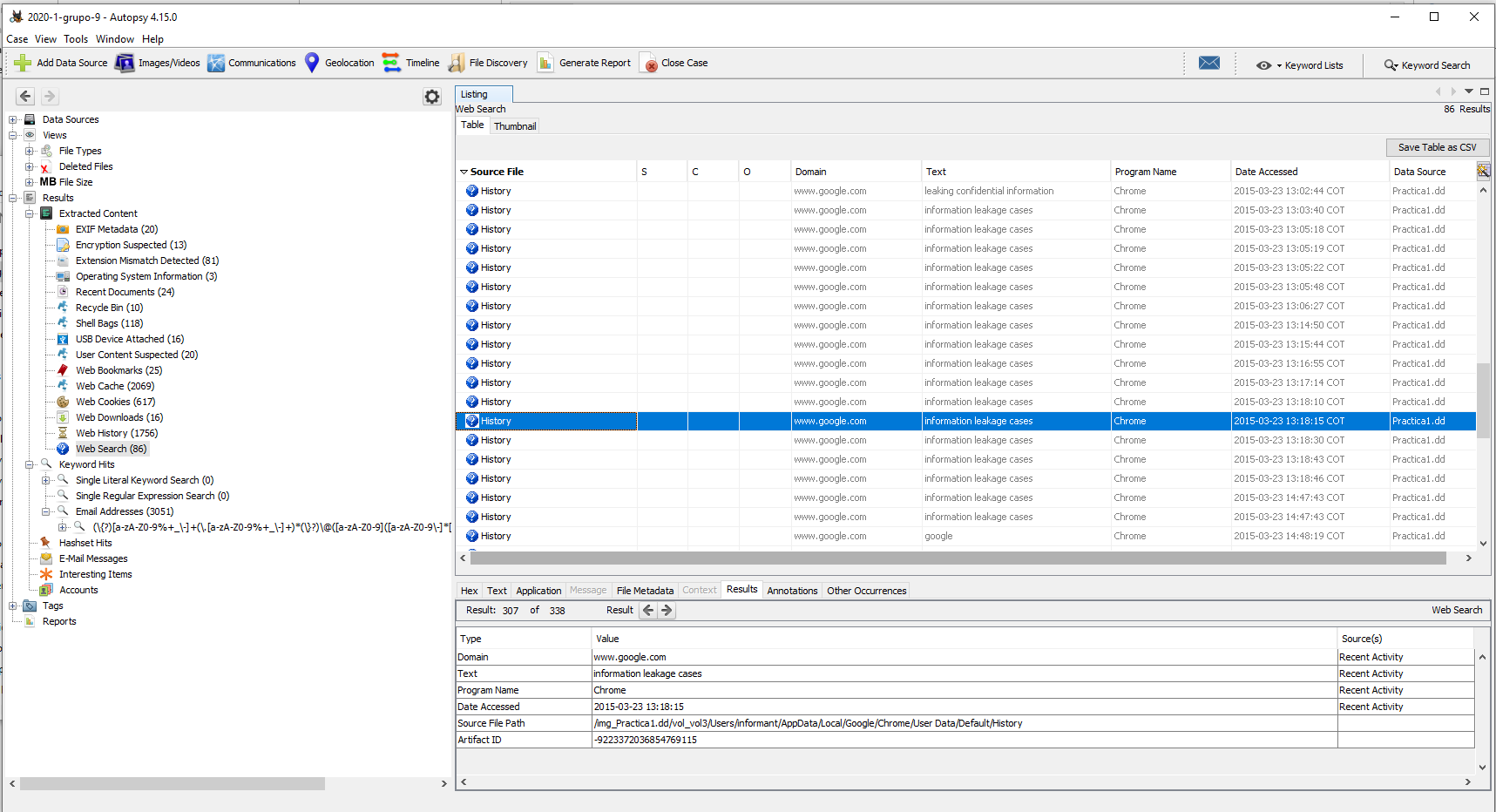


Uso Chrome , internet Explorer , Microsof Edge

13.Liste las ubicaciones en donde se encuentran los historiales de navegación

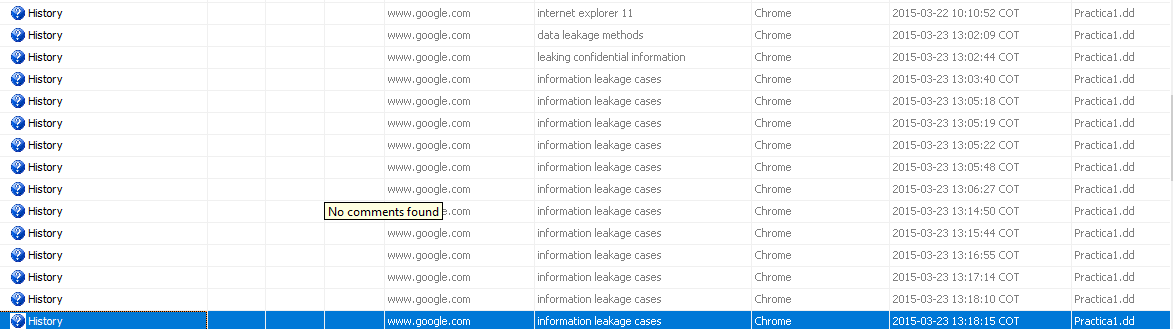




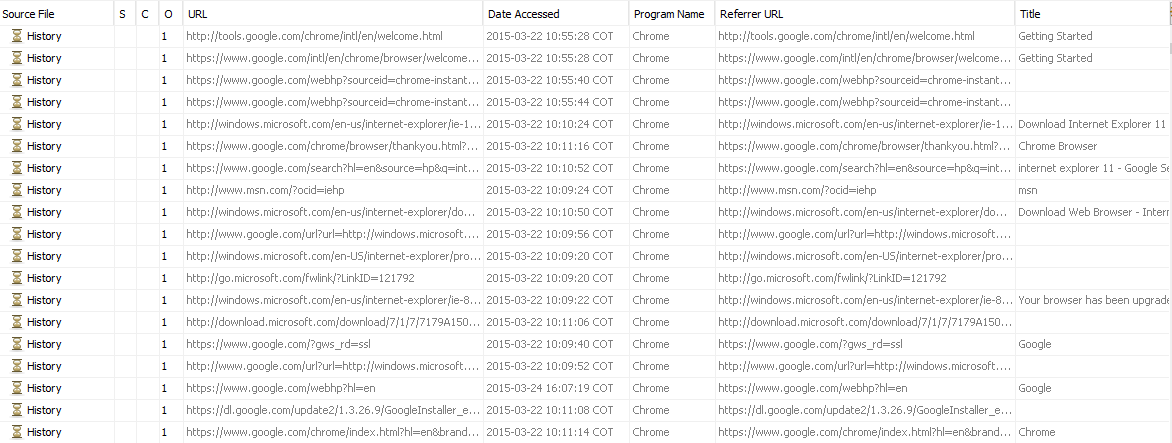


Encuentre evidencia de navegación Web (Internet Explorer y Chrome)

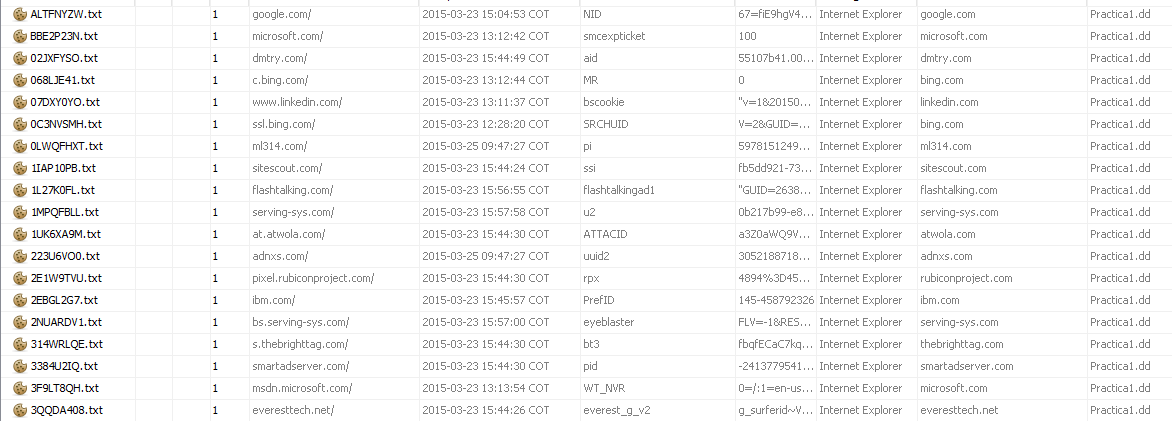
Chrome

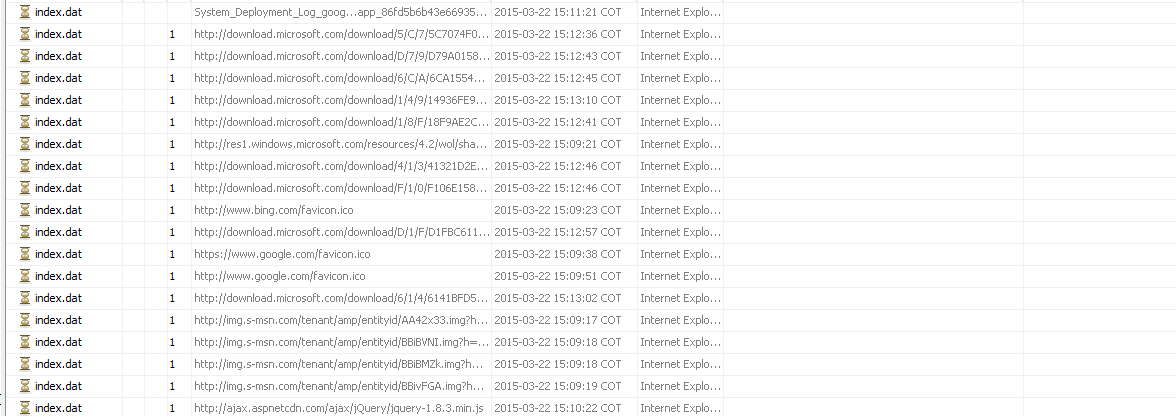






Internet explorer







Encuentre sitios visitados que parezcan sospechosos



<http://eraser.heidi.ie/download.php>



http://www.wired.com/2015/03/stealing-data-computers-using-heat/



http://www.forensicswiki.org/wiki/USB\_History\_Viewing

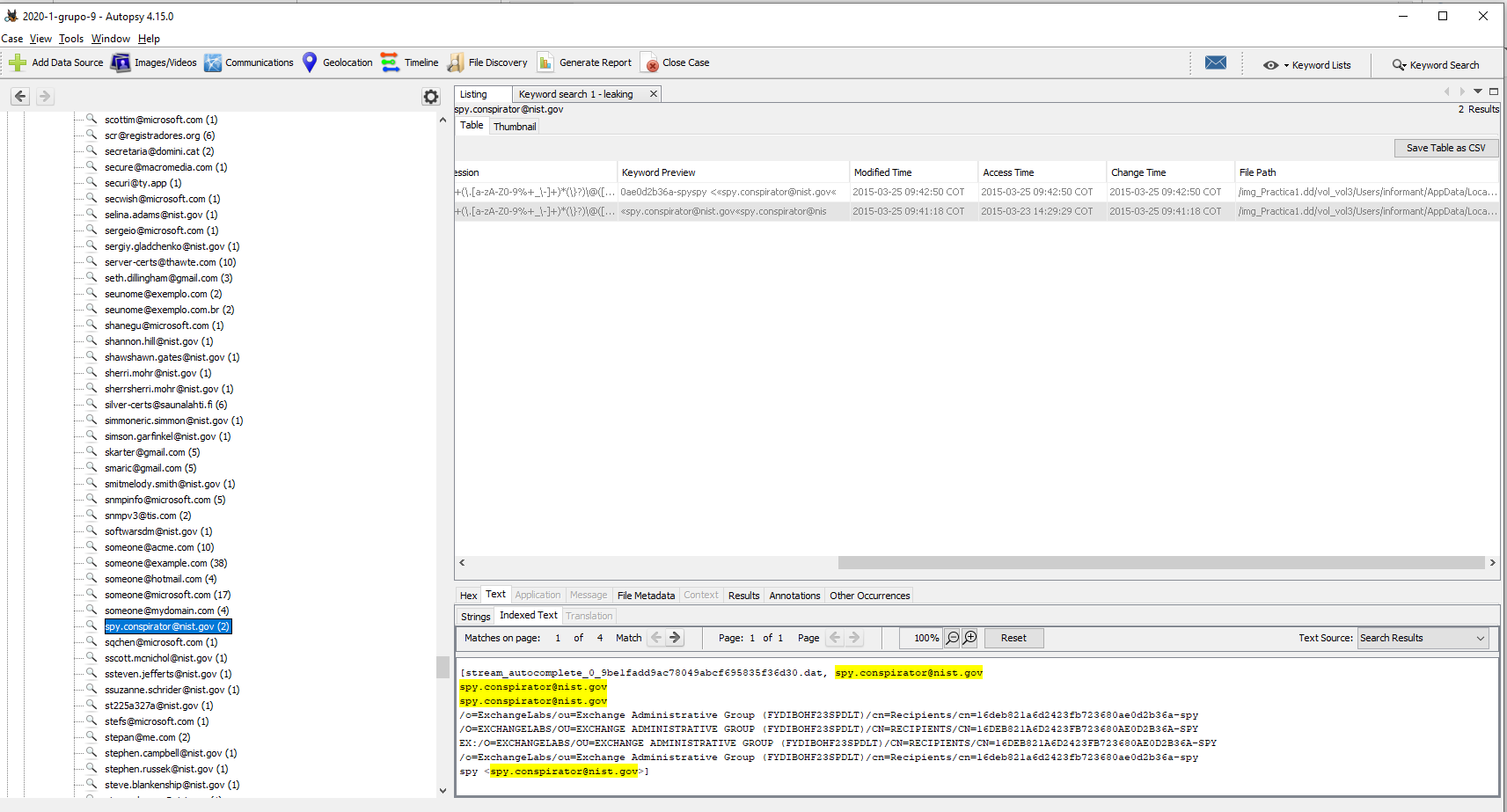
http://www.forensicswiki.org/favicon.ico



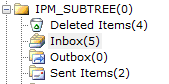
http://www.forensicswiki.org/wiki/Tools:Data\_Recovery

Encuentre direcciones de correo sospechosas

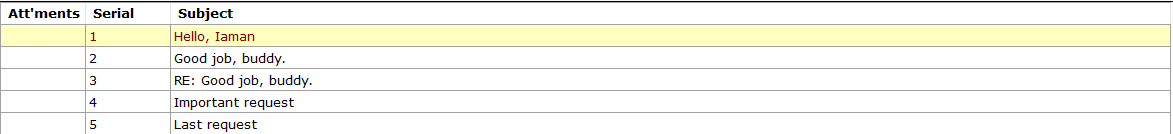
spy.conspirator@nist.gov



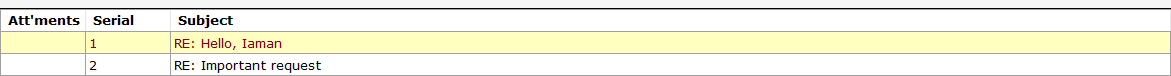
17. Se encuentra un archive .ost y se recupera con bitcover ost



Recibido



Enviados



4. Identifique cuales archivos fueron eliminados del disco duro.



Encuentre evidencias del uso de almacenamiento en la nube





Los archivos elminados de la usb estan una carpeta .