Write-up 2018 Owl (Digital Corpora)

INCIDE - Ref.100100

17 de marzo de 2020

CONFIDENCIAL

Índice general

Capítulo 1

Introducción

Revealer Toolkit 2 (RVT2) es un framework enfocado a investigaciones forenses digitales basado en software libre y escrito en Python 3. El RVT2 se encarga de identificar y automatizar las tareas habituales de una investigación forense, tales como el manejo cuidadoso de imágenes, el parseo de artefactos comunes a todas las investigaciones forenses, o la presentación de los resultados procesados para permitir que un analista dedique su esfuerzo exclusivamente a investigar el caso. El RVT2 se ha desarrollado internamente por INCIDE Digital Data S.L. desde hace una década y durante ese período ha sido empleado en centenares de investigaciones de DFIR reales.

El RVT2 está implementado en base a módulos interconectables, extensibles y personalizables. Entre las capacidades actuales se encuentras las siguientes:

- Interpretación de la salida de herramientas tradicionales como Sleuthkit o Regedit.
- Parseo de artefactos forenses en distintos sistemas operativos: Windows, MacOS, IOS, Android, Linux.
- Acceso y búsqueda en el contenido de miles de tipos de documentos diferentes: ofimática, OCR de PDFs, fotografías, correos, bases de datos...
- Clasificación de documentos utilizando modelos de inteligencia artificial.
- Conexión a servicios remotos de respuesta a incidentes: GRR
- Documentación del análisis y buenas prácticas forenses:
- Búsquedas ciegas de palabras clave
- Acceso solamente a resultados
- Auditoría y replicabilidad del proceso de investigación
- Resultados gráficos:
    - Búsqueda avanzada de documentos: por palabra clave, periodos de tiempo, contexto, búsquedas aproximadas...

- Dashboards gráficos: líneas temporales, eventos de los sistemas, estadísticas...
- Comentarios y etiquetas de los resultados.

- Soporte a laboratorios forenses con múltiples casos abiertos simultáneamente, cada uno de ellos con diversas fuentes e investigados por múltiples analistas.

En este documento se explican las funcionalidades y el manejo del RVT mediante la resolución de un caso tipo *challenge forense* propuesto por *Digital Corpora* llamado owl 2018 (https://digitalcorpora.org/corpora/scenarios/2018-owl). En este caso ficticio se investiga si un sospechoso ha participado en una supuesta compra ilegal de búhos.

Para obtener información relativa al uso detallado de RVT, se puede consultar la documentación oficial del RVT2 en https://portal.incide.es/rvt2-docs/.

1.1. Formato del documento

A lo largo de este documento se utilizarán los siguientes formatos:

Info

Información técnica extra.

Aviso

Avisos para leer con cuidado.

Resultados

Resultados de la investigación.

1.2. Planteamiento del caso y objetivos

En un país donde es ilegal comprar y vender búhos (en inglés, *owls*), dos personas son sospechosas de participar en un intercambio de búhos. La mera tenencia de búhos no es ilegal, pero sí su comercio.

La policía ha identificado a un sospechoso de ser comprador de búhos, y ha adquirido su teléfono móvil Android y su ordenador personal.

Se sospecha que el comprador escogió un búho, acordó un lugar y fecha para hacer la transacción y al acabar envió un mensaje de confirmación de la compra.

El objetivo de la investigación es verificar si realmente se produjo o no esta compra de búhos. El análisis, en consecuencia, se basará en responder a las siguientes preguntas:

Las preguntas que se desean responder son las siguientes:

- ¿Se encuentran documentos relacionados con búhos en los dispositivos adquiridos?
- ¿Hay indicios de búsqueda de información sobre cómo comprar tales animales?
- ¿La persona investigada ha negociado la compra de un búho?
- ¿La persona investigada llegó a finalizar una compra de un búho?
- ¿Cuándo se realizó el intercambio?
- ¿Puede identificarse al vendedor?

Cuando el equipo de CSI se reúne, deciden que para responder a estar preguntar lo más eficiente es centrar sus esfuerzos en:

- Documentos en el ordenador
- Redes sociales en el teléfono móvil

A continuación se irán describiendo los resultados obtenidos del parseo de diferentes artefactos que podrían responder a alguna de las anteriores cuestiones.

Dado que en la mayoría de casos forenses existe la prohibición legal de acceder a contenidos del disco que no sean relevantes para el propósito del caso y puedan contener información personal, el procedimiento de resolución del caso se limitará al análisis de aquellos archivos en los que figure, en nombre o contenido, al menos una de de las palabras clave definidas. Teniendo en cuenta que se trata de un caso de ejemplo, en algunos casos se tomará la licencia de analizar contenido más allá de estas restricciones con el fin de mostrar más extensamente algunas de las capacidades de RVT2.

1.3. Prerrequisitos

Se asumirá que ya se ha realizado la primera etapa de una investigación forense, esto es, la adquisición de las fuentes de información que se utilizan durante la investigación. En este caso, las fuentes de información pueden descargarse en la página web de Digital Corpora: `https://digitalcorpora.org/corpora/scenarios/2018-owl`. En adelante se presupondrá que las dos imágenes del caso han sido guardadas en:

- `/morgue/images/100100-training/100100-07-1.E01`: **PC Windows** (64G)
- `/morgue/images/100100-training/100100-07-2.dd`: **Nexus Android** (30G)

1.4. Resumen del caso y objetivos

En un país donde es ilegal comprar y vender búhos, la policía ha identificado a un sospechoso de ser comprador de búhos, y ha adquirido su ordenador personal Windows y su teléfono móvil Android.

Se desea resolver las siguientes preguntas:

- ¿Se encuentran documentos relacionados con búhos en los dispositivos adquiridos?
- ¿Hay indicios de búsqueda de información sobre cómo comprar tales animales?
- ¿La persona investigada ha negociado la compra de un búho?
- ¿La persona investigada llegó a finalizar una compra de un búho?
- ¿Cuándo se realizó el intercambio?
- ¿Puede identificarse al vendedor?

Capítulo 2

Análisis de la fuente 100100-07-1

La fuente `100100-07-1` se corresponde con la imagen forense del ordenador personal del sospechoso. Según se observa en el informe de adquisición, es un PC Windows de 64GB, aunque estos datos tienen que confirmarse. ¡No sería la primera vez que se analiza la imagen que no es!

Se realizarán los siguientes análisis sobre esta fuente.

- Preparación de la imagen y "preforense":
  - Montaje de la imagen
  - Caracterización
- Análisis de archivos
  - Archivos existentes en el disco
  - Búsqueda ciega de palabras clave
  - Indexación
  - Línea temporal o *timeline* de archivos
  - Journal
  - Clasificación de imágenes
- Análisis del sistema
  - Eventos del sistema
  - Papelera de reciclaje
  - USB
  - Strings
- Análisis de actividad de usuario
  - Navegación en Internet
  - Descargas de archivos
  - Apertura de archivos

- Correo electrónico
- Aplicaciones ejecutadas
- Redes sociales

2.1. Preparación de la imagen y "preforense"

Info

La imagen forense está guardada en un archivo llamado `100100-07-1.E01`. Este prefijo se corresponde con una imagen forense de tipo Encase. Este tipo de imagen forense es uno de los más utilizados en la actualidad.

2.1.1. Montaje

En primer lugar es necesario montar el disco duro de esta fuente. Es decir, reconstruir su sistema de archivos. El comando que se ejecuta es el siguiente.

```
$ sudo rvt2 --casename 100100-training --source 100100-07-1
    -j mount
```

Aviso

Algunas operaciones de RVT2 requieren permisos de administración para ser ejecutadas (como en el caso de montaje de imágenes de disco). En adelante se asume que todas las *jobs* de RVT2 se ejecutan con `sudo`

Info

El RVT2 es capaz de montar imágenes en muchos formatos diferentes: E01, dd, ZIP... Si la imagen está en algún formato no soportado todavía, puede descomprirse su contenido en el directorio `mnt`.

Los sistemas de archivos son montados en la carpeta `mnt` dentro del directorio de la fuente `morgue/100100-training/100100-07-1`. Como se observa han podido ser montadas 5 de las 9 particiones del disco (el directorio `auxdir` sirve de paso intermedio para montar particiones con ciertas restricciones y no se usa para el análisis).

```
$ cd /morgue/100100-training/100100-07-1
$ ls mnt
```

```
auxdir  p04  p06  p07  p08  p09
```

Info

Si bien RVT2 permite la flexibilidad de ejecutarse para distintos casos y fuentes mediante los parámetros *casename* y *source*, para simplificar la ejecución de los comandos puede hacerse dos maneras:

- edición del archivo `rvt2/conf/local.cfg` y añadir, dentro de la sección `[DEFAULT]`, la configuración `casename: 100100-training` y `source: 100100-07-1`.
- `alias rvt2="rvt2 --casename 100100-training"`

En adelante se asumirá que el `casename` ha sido predefinido de esta manera, y no es necesario incluir en cada comando la configuración `--casename 100100-training`.

2.1.2. Caracterización del disco

Uno de los primeros pasos es "caracterizar el disco", es decir, la descripción inicial de qué puede encontrarse en ella. Como sabemos que la imagen se corresponde a un disco Windows, puede ejecutarse el siguiente comando.

```
$ rvt2 --source 100100-07-1 -j windows.characterize
```

Info

La salida de este comando puede encontrarse en el archivo: `analysis/characterize.md`.

La información mostrada por el resultado de esta *job*, en el caso de sistemas operativos windows, muestra:

- Tabla de particiones
- Modelo de disco y serial number (si se tiene el log de la clonadora)
- Nombre, versión, Id y propietario del OS
- Fecha de instalación (o update) del OS
- Fechas de creación y último login/logoff para cada usuario presente
- Número de VolumeShadowSnapshots (sólo Windows)

En el caso *Owl*, el disco presenta una partición principal (identificada por ser la de mayor tamaño) **p06**, con sistema de archivos NTFS con Windows. El contenido íntegro del archivo `characterize.md` es el siguiente:

Disk 100100-07-1 characterization
It is a disk image of size 63.5G and 9 partitions.
Partitions table

Partition	Size	Type	VSS
00	512.0	Safety Table	0
02	512.0	GPT Header	0
03	16.0K	Partition Table	0
04	360.0M	FAT32	0
05	128.0M	Microsoft reserved partition	0
06	448.7G	NTFS_DETECT	2
07	980.0M	NTFS_DETECT	0
08	13.7G	NTFS_DETECT	0
09	2.0G	FAT32	0

Partition 06 description
OS Information

- ProductName: Windows 10 Pro
- ComputerName: = DESKTOP-KLOQJ0V
- ProductId: 00330-50295-68670-AAOEM
- RegisteredOwner: Sarah McAvoy
- RegisteredOrganization: Hewlett-Packard Company
- CurrentVersion: 6.3
- CurrentBuild: 14393
- InstallationType: Client
- EditionID: Professional
- ProcessorArchitecture: AMD64
- TimeZone: Eastern Standard Time (5 hours)
- InstallDate: Fri Jan 27 02:58:47 2017 (UTC)
- ShutdownTime: Mon Jan 30 22:46:43 2017 (UTC)

Users

User	Creation date	Last login/logoff
Administrator [500]	27-01-2017 02:14:33 UTC	27-01-2017 02:06:52 UTC
Guest [501]	27-01-2017 02:14:33 UTC	Never
DefaultAccount [503]	27-01-2017 02:14:33 UTC	Never
Sarah McAvoy [1001]	26-01-2017 23:41:56 UTC	27-01-2017 01:48:12 UTC
Sarah M [1002]	27-01-2017 00:33:10 UTC	02-02-2017 21:24:14 UTC

Ref. 100100, INCIDE, Avda. Diagonal 618, 6E - 08021 Barcelona (Spain) / Tlf. (+34) 93.254.62.77 / www.incide.es

User profiles

User	Creation date	Last login/logoff
Sarah McAvoy	27-01-2017 02:43:59 UTC	27-01-2017 02:44:00 UTC
Sarah M	27-01-2017 02:43:58 UTC	02-02-2017 22:53:22 UTC

Resultados

Entre la información obtenida, se destaca la siguiente:

- El sistema operativo es Windows 10
- El sistema fue instalado el día 27-01-2017
- 2 usuarios presentes: *Sarah McAvoy* y *Sarah M*
- Zona horaria local -5 UTC.

Info

Las fechas mostradas en los arcivos resultantes de las *jobs* de RVT están expresadas en UTC. A menos que no se especifique lo contrario, todas las horas mostradas en este *write_up* se asumen en UTC. La hora equivalente local del dispositivo es *Eastern Standard Time*, de tal manera que para la interpretación de los resultados debe tenerse en cuenta que el investigado realizó las acciones 5 horas antes (localmente) de lo que se expresa en los resultados.

2.2. Análisis de archivos

2.2.1. Archivos existentes

Con el job **allocfiles** se obtiene una lista completa de todos los archivos asignados (*allocated*) (no eliminados) tras el montaje de cada partición.

```
$ rvt2 --source 100100-07-1 -j allocfiles
```

Info

Salida: `output/auxdir/allocfiles.txt`

Además de ser un requerimiento de otras varias *jobs* de RVT2, puede ser usado para una primera búsqueda rápida y sencilla de nombres y tipos de archivo.

```
$ grep -i owl output/auxdir/allocfiles.txt
```

```
100100-07-1/mnt/p06/Users/Sarah M/Desktop/pets/Snowy Owl 2.
    jpg
100100-07-1/mnt/p06/Users/Sarah M/Desktop/pets/Snowy Owl 3.
    jpg
100100-07-1/mnt/p06/Users/Sarah M/Desktop/pets/Snowy Owl 4.
    jpg
100100-07-1/mnt/p06/Users/Sarah M/Desktop/pets/Snowy Owl.
    jpg
100100-07-1/mnt/p06/Users/Sarah M/Documents/New Pet Care/
    Owl_Emergency_Care.pdf
100100-07-1/mnt/p06/Users/Sarah M/Documents/New Pet Care/
    Owl_Keeping.pdf
100100-07-1/mnt/p06/Users/Sarah M/Documents/New Pet Care/
    Snowy Owl Care.pdf
100100-07-1/mnt/p06/Users/Sarah M/Documents/New Pet Care/
    Snowy_Owl.pdf
100100-07-1/mnt/p06/Users/Sarah M/Documents/Owl_Keeping.pdf
100100-07-1/mnt/p06/Users/Sarah M/Downloads/Bibliography -
    Snowy Owl 14 April 2014 - GLOW posting.xls
100100-07-1/mnt/p06/Users/Sarah M/Downloads/
    Owl_Emergency_Care.pdf
```

Resultados

La búsqueda anterior da como resultado el primer indicio de la posesión de documentos (*.pdf, .jpd, .xls*) relacionados con búhos.

Snowy Owl (*Bubo scandiacus*)

Description and Range
Snowy owls are unmistakable, large, white owls. Adult males are almost fully white in appearance and occasionally sport a few dark marks. In contrast, females and juveniles tend to have dark scalloping and spotting. Younger birds are more heavily barred, adults less barred. All snowy owls have striking yellow eyes and a dark bill. Their coloration, thick plumage, and heavily feathered talons make them well-adjusted for life in the Arctic. Snowy owls are the largest (by weight) North American owl, often weighing between 3-6 pounds. Males, on average, are smaller than females.

Snowy owls nest in the Arctic tundra within the northernmost areas of Alaska, Canada and Eurasia. In the winter, snowy owls will often migrate through Canada and northern Eurasia with occasional irruptions occurring further south. Snowy owls are rare winter visitors to Maryland.

Figura 2.1: Muestra del documento 'Snowy Owl Care.pdf'

2.2.2. Búsqueda ciega de palabras clave

Se denomina *búsqueda ciega de palabras clave* a una técnica de análisis forense en la que se seleccionan una serie de clave relevantes para la investigación y se analizan los documentos que contienen alguna de estas palabras.

Las búsquedas ciegas son una de las técnicas más utilizadas en análisis forense por los siguientes motivos:

- Permiten garantizar una técnica probatoria proporcional y asegurando que no se vulneran los derechos fundamentales de los afectados por dicha investigación.
- Permite limitar la cantidad de documentos que se van a analizar.

- Permiten descubrir documentos interesantes que para una investigación para los que el RVT2 aún no tiene un módulo desarrolado.

En este caso se han considerado como palabras clave (incluyendo variaciones semánticas y uso de mayúsculas y minúsculas) las siguientes:

- owl
- bird
- pet
- sale
- delivery
- feather
- egg
- nocturnal

2.2.3. Indexación

El procedimiento seguido en esta fuente para aplicar la técnica de búsqueda cieda de palabras clave parte de la indexación de los archivos:

```
rvt2 --source 100100-07-1 -j indexer.save_directory
```

Este comando analizará todos los archivos en todas las particiones de la fuente, se parsearán con TIKA (un programa de la fundación Apache capaz de convertir a texto centenares de tipos de archivos) y se guardan de una base de datos ElasticSearch.

Info

Por defecto se indexa todo el contenido de `mnt`, pero podría elegirse una partición o carpeta en concreto

Realizando una búsqueda por palabras clave en **RVT_Analyzer** se identifica una selección de documentos y imágenes.

```
query: owl OR bird OR feather OR egg
```

La exploración visual del contenido de esos archivos confirma que, efectivamente, que el usuario *Sarah M* posee documentos relacionados con búhos, tales como guías sobre el cuidado de estos animales o imágenes de los mismos.

https://portal.incide.es/rvt2-analyzer/#/search/100100-07-1

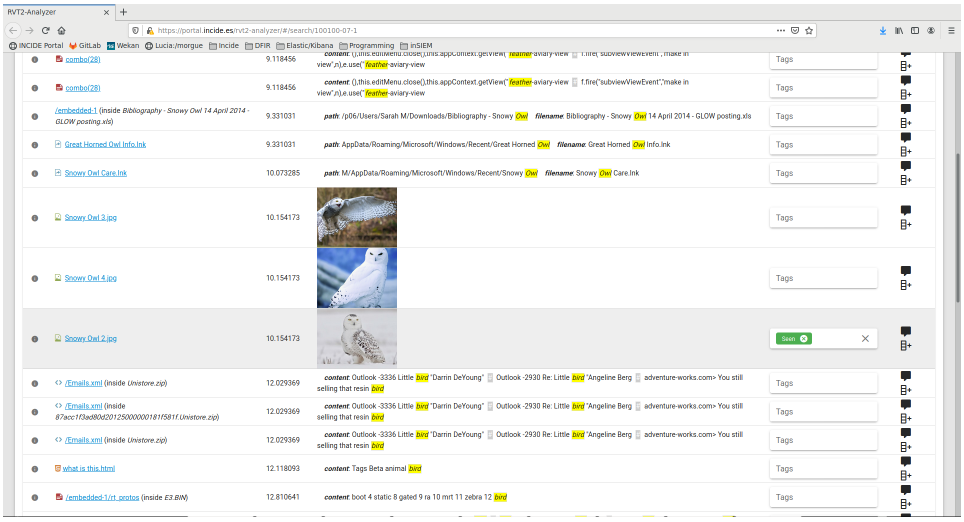

Figura 2.2

Resultados

Se puede afirmar que el investigado posee información específica sobre búhos en al menos uno de sus dipositivos, respondiendo así a la primera de las preguntas planteadas en el caso.

También se detecta coincidencia en archivos relativos a los navegadores `chrome` y `edge`, lo que justifica el parseo que en *Historial de navegación* (apartado 2.4.1, pág. 23) se hará del historial de navegación para poder indagar más sobre la información que pueda encontrarse en ellos.

2.2.4. Línea temporal del sistema de archivos

El contenido de la **MFT**, además de permitir establecer una secuencia temporal de la creación o modificación de los archivos del sistema, podría también en este caso mostrar documentos eliminados que no han sido indexados en el paso anterior. El parseado de la misma es un procedimiento inicial habitual.

```
$ rvt2 --source 100100-07-1 -j fs_timeline
```

Info

Salida: `output/timeline/100100-07-1_BODY.csv`

En este caso no hay ningún archivo eliminado completamente (etiqueta `deleted`) con un nombre que contenga *Owl*. Se verá más adelante que sí

los hay en la papelera de reciclaje (2.3.3 (pág. 18)).

```
$ grep Owl output/timeline/100100-07-1_BODY.csv
...
Date,Size,Type,Mode,UID,GID,Meta,File Name
2017-01-27T17:33:23Z,3496271,.a.b,r/rrwxrwxrwx
    ,0,0,286771-128-3,
"100100-07-1/mnt/p06/Users/Sarah M/Desktop/pets/Snowy Owl
    4.jpg"
2017-02-02T22:00:17Z,593265,.acb,r/rrwxrwxrwx
    ,0,0,286435-128-1,
"100100-07-1/mnt/p06/Users/Sarah M/Documents/New Pet Care/
    Snowy Owl Care.pdf"
...
```

La aplicación gráfica **Kibana** permite observar los períodos de mayor actividad a lo largo del tiempo para la timeline y otros eventos. Entre otras cosas se observa la presencia de muchos archivos propios de Windows modificados en 2015 pero con las otras tres fechas (*acb*) a 27-01-2019. Se trata de un indicador que el sistema fue instalado el 27-01-2019, aunque los archivos de sistema son originarios de 2015.

Los picos de actividad en períodos más cortos pueden verse filtrando el tiempo:

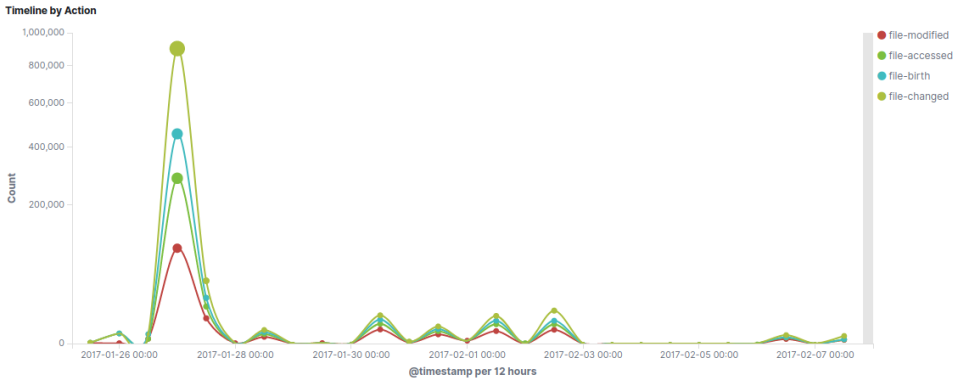

Figura 2.3: Fechas macb entre el 26 de enero y el 7 de febrero de 2017

2.3. Análisis del sistema

2.3.1. Línea temporal de eventos del sistema

RVT2 permite crear una *timeline* que recopila los eventos de los distintos artefactos de Windows. Resulta un herramienta muy útil en casos en los que se necesita investigar la actividad realizada en un dispositivo de

forma cronológica en un espacio de tiempo determinada, por ejemplo para rastrear ataques en un caso de IR (*Incident Response*).

A modo de ejemplo, en el presente caso, se puede observar las últimas acciones realizadas sobre el documento `Snowy Owl Care.pdf` . Concretamente, el día 2 de febrero de 2017, se observa la fecha de creación en el sistema de archivos a las *23:00:17* (UTC +1) y su apertura desde una unidad externa `F:` a través del navegador a las *23:38:35* (UTC +1).

Time	event.module	message	event.dataset
Feb 2, 2017 @ 23:38:36.000	browsers	Url visited: file:///F:/Snowy%20Owl%20Care.pdf	history
Feb 2, 2017 @ 23:38:35.529	usnjrnl	File created: 100100-07-1/mnt/p06/Users/Sarah M/AppData/Roaming/Microsoft/Windows/Recent/Snowy Owl Care.lnk	usnjrnl
Feb 2, 2017 @ 23:38:35.519	registry	Registry value Path set at subkey {C7DADCF6-9E6B-4B8F-8C71-E4C69FE387FE}	ntuser
Feb 2, 2017 @ 23:38:35.519	registry	Registry value DisplayName set at subkey {C7DADCF6-9E6B-4B8F-8C71-E4C69FE387FE}	ntuser
Feb 2, 2017 @ 23:38:35.000	recentfiles	File last opened: F:/Snowy Owl Care.pdf	lnk
Feb 2, 2017 @ 23:38:35.000	recentfiles	File first opened: F:/Snowy Owl Care.pdf	lnk
Feb 2, 2017 @ 23:38:35.000	recentfiles	File last opened: F:/Snowy Owl Care.pdf	jlauto
Feb 2, 2017 @ 23:38:35.000	recentfiles	File last opened: F:/Snowy Owl Care.pdf	jlauto
Feb 2, 2017 @ 23:38:35.000	browsers	Url visited: file:///F:/Snowy%20Owl%20Care.pdf	history
Feb 2, 2017 @ 23:38:35.000	browsers	Url visited: file:///F:/Snowy%20Owl%20Care.pdf	history
Feb 2, 2017 @ 23:38:35.000	filesystem	File birth: 100100-07-1/mnt/p06/Users/Sarah M/AppData/Roaming/Microsoft/Windows/Recent/Snowy Owl Care.lnk	MFT
Feb 2, 2017 @ 23:38:35.000	filesystem	File modified: 100100-07-1/mnt/p06/Users/Sarah M/AppData/Roaming/Microsoft/Windows/Recent/Snowy Owl Care.lnk	MFT
Feb 2, 2017 @ 23:38:35.000	filesystem	File change record: 100100-07-1/mnt/p06/Users/Sarah M/AppData/Roaming/Microsoft/Windows/Recent/Snowy Owl Care.lnk	MFT
Feb 2, 2017 @ 23:38:35.000	filesystem	File access: 100100-07-1/mnt/p06/Users/Sarah M/AppData/Roaming/Microsoft/Windows/Recent/Snowy Owl Care.lnk	MFT
Feb 2, 2017 @ 23:00:17.426	usnjrnl	File created: 100100-07-1/mnt/p06/Users/Sarah M/Documents/New Pet Care/Snowy Owl Care.pdf	usnjrnl
Feb 2, 2017 @ 23:00:17.000	filesystem	File birth: 100100-07-1/mnt/p06/Users/Sarah M/Documents/New Pet Care/Snowy Owl Care.pdf	MFT

Figura 2.4: Eventos relacionados con el archivo `Snowy Owl Care.pdf`

Info

El hallazgo de la misma información en distintos artefactos del sistema es un excelente método de corroborar la veracidad de los datos y detectar posibles manipulaciones en caso que la información sea distinta.

Más adelante se analizarán algunos de los distintos artefactos, pero aquí ya se muestra como la creación de archivos puede detectarse mediante el *UsnJrnl* y el acceso a los archivos mediante los *lnk* y a veces el registro de Windows o las bases de datos de las aplicaciones que abren esos ficheros (en este caso el historial de navegación).

2.3.2. Journal (UsnJrnl)

Resgistra cambios en archivos o directorios.

```
$ rvt2 --source 100100-07-1 -j windows.usnjrnl
```

Info

Salida: `output/windows/usnjrnl`

En este caso, por ejemplo, supone una doble comprobación, junto a la base de datos de `chrome`, de la descarga de imágenes desde `gmail` al sistema de archivos en una fecha específica.

```
Date;Filename;Reason
2017-01-27 17:19:12.222356;Great Horned Owl.jpg.crdownload;
    DATA_EXTEND RENAME_NEW_NAME
2017-01-27 17:19:14.448704;Pygmy Owl.jpg.crdownload;
    RENAME_NEW_NAME
2017-01-27 17:19:18.031882;Snowy Owl.jpg;RENAME_NEW_NAME
```

Recordatorio de la entrada en descargas de `chrome`:

```
"https://mail.google.com/mail/";"C:\Users\Sarah M\Downloads
    \Great Horned Owl.jpg";64476;"2017-01-27 17:19:12"
```

2.3.3. Papelera de reciclaje

Pueden recuperarse los archivos presentes en la papelera y la fecha en la que fueron puestos en ella.

```
rvt2 --source 100100-07-1 -j windows.recycle
```

Info

Salida: `output/windows/recyclebin`

```
$ grep -i owl output/windows/recyclebin/recycle_bin.csv
...
Date;OriginalName;Inode
2017-01-27 17:35:43;C:/Users/Sarah M/Desktop/Great Horned
    Owl.jpg;1122
2017-01-27 17:35:45;94519;C:/Users/Sarah M/Desktop/pets/
    Pygmy Owl.jpg;89702
```

Resultados

La presencia de imágenes relacionadas con búhos podría indicar una intención de deshacerse de cierta información incriminatoria.

En este caso, sin embargo, dada la presencia de múltiples documentos no eliminados relacionados con la temática, parece una hipótesis poco probable.

2.3.4. Dispositivos USB conectados

En el análisis de archivos recientemente abiertos (2.4.6 (pág. 31)) se mencionará la apertura de documentos desde la unidad `F`. Hay 3 artefactos distintos en los que se pueden encontrar los dispositivos USB instalados en el PC:

- En el registro: `rvt2 --source 100100-07-1 -j windows.autorip`
- En setupapi.dev: `rvt2 --source 100100-07-1 -j windows.usb`
- En event_logs: `rvt2 --source 100100-07-1 -j windows.events`

Únicamente se han encontrado dos dispositivos tipo USB en el registro y en el archivo `setupapi.dev`:

- En setupapi.dev:

```
$ cat output/windows/usb/p06_usb_setupapi.csv
...
"Device";"Start";"End";"UMP";"HardwareID";"DevDesc";"
    DrvDesc";"Provider";"Signer";"DrvDate";"Version";"Status
    "
"SWD\WPDBUSENUM\_??_USBSTOR#Disk&Ven_SanDisk&
    Prod_Cruzer_Glide&Rev_1.27#20051739911AEEC1DE29&0#{53
    f56307-b6bf-11d0-94f2-00a0c91efb8b
    }";"2017/02/02";"2017/02/02 16:53:11.225
";"";"wpdbusenum\fs";"WPD FileSystem Volume Driver
    ";"";"";"";"06/21/2006";"10.0.14393.0";"SUCCESS"
"SWD\WPDBUSENUM\_??_USBSTOR#Disk&Ven_General&
    Prod_USB_Flash_Disk&Rev_1100#0315216040016502&0#{53
    f56307-b6bf-11d0-94f2-00a0c91efb8b
    }";"2017/02/07";"2017/02/07 09:02:18.864
";"";"wpdbusenum\fs";"WPD FileSystem Volume Driver
    ";"";"";"";"06/21/2006";"10.0.14393.0";"SUCCESS"
```

- En el registro:

```
$ cat output/windows/hives/05_storage_information_p06.txt
...
mountdev2
```

```
Device: _??_USBSTOR#Disk&Ven_General&Prod_USB_Flash_Disk&
    Rev_1100#0315216040016502&0#{53f56307
-b6bf-11d0-94f2-00a0c91efb8b}
  \DosDevices\F:
  \??\Volume{e826e437-ed3d-11e6-ba92-806e6f6e6963}

Device: _??_USBSTOR#Disk&Ven_SanDisk&Prod_Cruzer_Glide&
    Rev_1.27#20051739911AEEC1DE29&0#{53f563
07-b6bf-11d0-94f2-00a0c91efb8b}
  \??\Volume{01c346bd-e73e-11e6-ba90-a434d955649f}


removdev

Device    : DISK&VEN_SANDISK&PROD_CRUZER_GLIDE&REV_1.27
LastWrite : Thu Feb  2 21:53:11 2017 (UTC)
SN        : 20051739911AEEC1DE29&0
Drive     : F:\

Device    : DISK&VEN_GENERAL&PROD_USB_FLASH_DISK&REV_1100
LastWrite : Tue Feb  7 14:02:18 2017 (UTC)
SN        : 0315216040016502&0
Drive     : PALADIN EDG


usbdevices

VID_0781&PID_5575
LastWrite: Thu Feb  2 21:53:08 2017
  SN       : 20051739911AEEC1DE29
  LastWrite: Thu Feb  2 22:38:09 2017

VID_090C&PID_1000
LastWrite: Mon Feb  6 19:42:05 2017
  SN       : 0315216040016502
  LastWrite: Tue Feb  7 14:01:38 2017


usbstor

Disk&Ven_General&Prod_USB_Flash_Disk&Rev_1100 [Mon Feb  6
    19:42:06 2017]
  S/N: 0315216040016502&0 [Tue Feb  7 14:01:38 2017]
  Device Parameters LastWrite: [Mon Feb  6 19:42:06 2017]
  Properties LastWrite       : [Tue Feb  7 14:01:45 2017]
    FriendlyName    : General USB Flash Disk USB Device

Disk&Ven_SanDisk&Prod_Cruzer_Glide&Rev_1.27 [Thu Feb  2
    21:53:08 2017]
```

```
  S/N: 20051739911AEEC1DE29&0 [Thu Feb  2 21:53:08 2017]
  Device Parameters LastWrite: [Thu Feb  2 21:53:08 2017]
  Properties LastWrite       : [Thu Feb  2 21:53:09 2017]
    FriendlyName    : SanDisk Cruzer Glide USB Device


emdmgmt

Disk&Ven_General&Prod_USB_Flash_Disk&Rev_1100
  LastWrite: Tue Feb  7 14:02:42 2017 Z
  SN: 0315216040016502&0
  Vol Name: PALADIN EDG
  VSN: 1606-2154

Disk&Ven_SanDisk&Prod_Cruzer_Glide&Rev_1.27
  LastWrite: Thu Feb  2 22:38:10 2017 Z
  SN: 20051739911AEEC1DE29&0
  VSN: 80BC-89A2
```

Las distintas fuentes del registro permiten reunir información completa sobre cada dispositivo. En este caso, solo uno de ellos fue instalado con anterioridad a las referencias encontrdas en los archivos recientes (*lnk*), que además es el que figura como asociado a la unidad 'F:'. Sus características son:

- Name: Disk&Ven_SanDisk&Prod_Cruzer_Glide&Rev_1.27
- FriendlyName: SanDisk Cruzer Glide USB Device
- SN: 20051739911AEEC1DE29&0
- VSN: 80BC-89A2
- VID/PID: VID_0781&PID_5575
- Install date: Thu Feb 2 21:53:11 2017 (UTC) o 17/02/02 16:53:11.225
- Last connection: Thu Feb 2 22:38:10 2017 Z

Aviso

Las fechas que aparecen en el registro se corresponden con el momento en que un valor fue escrito, pero no tienen porqué coincidir con exactitud con el momento del evento.

Existe una referencia extra a otro dispositivo en los eventos de System, pero no se puede asociar a otros archivos.

```
$ grep 20001 analysis/events/events.json
...
{"TimeCreated": "2017-01-27T00:55:45.128Z", "EventID":
    "20001", "Provider": "Microsoft-Windows-UserPnp", "
    ProcessID": "7296", "ThreadID": "7940", "Description": "
```

```
    Installation or Update", "DeviceInstanceID": "USB\\
    VID_04CA&PID_7054&MI_00\\6&2FDA0D4&0&0000"}
```

Resultados

Las distintas fuentes de información sobre dispositivos conectados al PC han permitido identifcar un *USB* que ha contenido archivos relacionados con búhos, accedidos desde el PC del investigado.

2.3.5. Strings

Las tareas de búsqueda de `strings` directamente en el contenido del disco, requieren un tiempo considerable y se uso no debería ser indiscriminado. Sin embargo, a veces permiten obtener información de archivos no asignados que no se obtienen mediante la indexación común.

Para obtener resultados de la búsqueda es necesario crear el archivo de configuración `searches_files/keywords` dentro el directorio del caso con el contenido:

```
owl:::\bowl\w*\b
feathers:::\bfeather\w*\b
egg:::\beggs\w*\
```

La tarea de RVT2 a ejecutar es la siguiente:

```
sudo rvt2 --casename 100100-training --source 100100-07-01
    -j strings search_strings
```

Info

Salida: `analysis/searches/*`

Index of /morgue/100100-training/100100-07-1/analysis/searches

Fragmento del resultado de la búsqueda de palabra clave `Nocturnal`, donde se observa una url en un espacio no asignado del disco:

```
Pt: p06; Blk: 59359079; Inode:  Not Allocated; File: -
<...h.t.t.p.:./.b.i.r.d.i.n.g...a.b.o.u.t...c.o.m./.o.d
    ./.
b.i.r.d.i.n.g.g.l.o.s.s.a.r.y./.g./.N.o.c.t.u.r.n.a.l...h.t
    .m.....
```

Para dotar de contexto a esta coincidencia podría realizarse *carving* de los bloques pertinentes. Dado que se trata de un proceso complicado y el

hit detectado no parece establecer conclusiones en relación al caso, se omitirá el posterior análisis.

2.4. Análisis de actividad

2.4.1. Historial de navegación

El historial de navegación, cookies y descargas, se obtiene con:

```
$ rvt2 --source 100100-07-1 -j browsers
```

> **Info**
>
> Salida: `output/browsers/*`

En los archivos `.csv` resultantes, se comprueba el uso de los navegadores `chrome` y `edge` que ya se había advertido con la búsqueda de palabras clave en el indexado (2.2.3 (pág. 14)). En particular el usuario *Sarah M* ha utilizado el navegador `Chrome` y el usuario *Sarah McAvoy* `Edge` . No hay entradas para otros navegadores.

```
$ grep chrome output/browsers/history.csv | wc -l
798
$ grep edge output/browsers/history.csv | wc -l
128
$ grep firefox output/browsers/history.csv | wc -l
0
$ grep safari output/browsers/history.csv | wc -l
0
```

2.4.2. Consultas relacionadas con 'Owl'

En las siguientes búsquedas al historial completo se tendrán en cuenta las línias inmediatamente anteriores y posteriores a los *hits* para dar contexto.

`$ cut -d ';' -f1,2,3 output/browsers/history.csv | grep -B 5 -A 5 -iP "owl|bird"`

Entre el ruido de consultas no relacionadas con la investigación, se observan consultas de información general sobre la temática de búhos. Pueden verse, también, consultas de compra en sitios como **Amazon**, **Craigslist** o **Etsy**.

```
"last_visit";"url";"title"
```

```
"2017-01-27 01:05:34";"https://www.google.com/webhp?
   sourceid=chrome-instant&rlz=1C1CHBD_enUS729US729&ion=1&
   espv=2&ie=UTF-8#q=owls";""
"2017-01-27 01:12:18";"https://www.amazon.com/s/ref=
   nb_sb_noss_2/159-6440290-7542161?url=search-alias%3Daps&
   field-keywords=owl+eggs";"Amazon.com: owl eggs"
"2017-01-27 01:13:06";"https://www.google.com/#q=can+you+
   buy+owl+eggs";"can you buy owl eggs - Google Search"
"2017-01-27 01:13:13";"https://www.google.com/#q=can+you+
   buy+snow+owl+eggs";"can you buy snow owl eggs - Google
   Search"
"2017-01-27 01:13:18";"https://www.reference.com/pets-
   animals/can-buy-snowy-owl-1076a35ab9e3160b";"Can you buy
    a snowy owl? / Reference.com"
"2017-01-27 01:13:32";"http://www.21food.com/products/
   fertile-snowy-owl-eggs-for-sale-355573.html";"Fertile
   Snowy Owl eggs for sale products,Cameroon Fertile Snowy
   Owl eggs for sale supplier"
"2017-01-27 01:14:56";"https://www.google.com/#q=can+you+
   buy+snowy+owl+eggs";"Google"
"2017-01-27 01:16:06";"https://www.google.com/#q=owl+
   wingspans+in+america+pdf";"owl wingspans in america pdf
   - Google Search"
"2017-01-27 01:16:14";"http://www.ncwildlife.org/Portals/0/
   Learning/documents/Profiles/greathornedowl.pdf";"
   greathornedowl.pdf"
"2017-01-27 01:42:37";"https://huntington.craigslist.org/
   search/?sort=rel&query=owls&catAbb=sss";"huntington for
   sale ""owls"" - craigslist"
"2017-01-27 01:43:22";"https://www.reference.com/pets-
   animals/owls-endangered-c769e44150057951";"Are owls
   endangered? / Reference.com"
"2017-01-27 01:44:15";"https://www.googleadservices.com/
   pagead/aclk?sa=L&ai=
   DChcSEwibio_QmeHRAhXeSw0KHUjACGEYABAE&ohost=www.google.
   com&cid=
   CAASIuRosa5aKt26iqTbiExedU5Fda10lb4u1Uop4ZPpMPH4Ukg&sig=
   AOD64_2EE87kpYCqC1V7iXtUFIwsUQg4_Q&q=&ved=0ahUKEwi-
   wYnQmeHRAhXGQCYKHUY0BYIQ0QwIIQ&adurl=";"Northern Spotted
    Owl Continues to Decline - Endangered Listing Needed /
   American Bird Conservancy"
"2017-01-27 17:01:41";"https://www.reference.com/pets-
   animals/snowy-owls-eat-341f14692049578d";"What do snowy
   owls eat? / Reference.com"
"2017-01-27 17:01:46";"https://www.reference.com/pets-
   animals/great-horned-owls-eat-e6741e494bf14e6e?qo=
   contentSimilarQuestions";"What do great horned owls eat?
    / Reference.com"
"2017-01-27 17:02:10";"http://www.birdchick.com/blog
```

```
    /2009/08/big-surprise-snowy-owls-are-not-good-pets";"Big
     Surprise, Snowy Owls Are Not Good Pets! - Birdchick"
"2017-01-27 17:02:19";"http://internationalowlcenter.org/
    owls-humans/owlsaspets";"Owls as Pets"
"2017-01-27 17:02:34";"http://www.defenders.org/snowy-owl/
    what-you-can-do";"Snowy Owl / What You Can Do to Help
    Snowy Owls / Defenders of Wildlife"
"2017-01-27 17:03:30";"http://aboutpetlife.com/pet-animals/
    snowy-owl-pet.php";"Snowy owl as pet - About Pet Life"
"2017-01-27 17:03:50";"https://www.google.com/search?q=
    where+to+keep+a+snowy+owl&rlz=1C1CHBD_enUS729US729&oq=
    where+to+keep+a+snowy+owl&aqs=chrome..69i57.8064j0j4&
    sourceid=chrome&ie=UTF-8";"where to keep a snowy owl -
    Google Search"
"2017-01-27 17:04:04";"https://www.quora.com/How-much-does-
    an-owl-cost";"How much does an owl cost? - Quora"
"2017-01-27 17:04:10";"http://www.internationalowlcenter.
    org/owls-humans/owlsaspets";"Owls as Pets"
"2017-01-27 17:04:30";"http://wildlifeadoption.defenders.
    org/snowyowl";"Adopt a Snowy Owl - Wildlife Adoption and
     Gift Center"
"2017-01-27 17:04:47";"https://www.quora.com/How-can-you-
    own-an-owl-What-are-the-steps";"How to own an owl? What
    are the steps - Quora"
"2017-01-27 17:05:36";"http://exoticpets.about.com/od/birds
    /a/Pet-Owls.htm";"What Should You Know About Having an
    Owl as a Pet?"
"2017-01-27 17:05:58";"https://www.google.com/search?q=
    where+to+keep+a+snowy+owl&rlz=1C1CHBD_enUS729US729&oq=
    where+to+keep+a+snowy+owl&aqs=chrome..69i57.8064j0j4&
    sourceid=chrome&ie=UTF-8#q=purchase+a+snowy+owl+in+the+
    united+states";"how to care for a owl - Google Search"
"2017-01-27 17:06:00";"http://www.barnowltrust.org.uk/
    captive-barn-owls/";"Thinking of keeping a captive Barn
    Owl? - The Barn Owl Trust"
"2017-01-27 17:06:08";"http://www.owl-help.org.uk/page19/
    page21/page21.html";"Keeping Owls as Pets / Suffolk Owl
    Sanctuary"
"2017-01-27 17:06:17";"https://www.youtube.com/watch?v=
    MM_HiXmiwNE";"Take care Baby Owl (kkang-i) - YouTube"
"2017-01-27 17:06:37";"http://audubonportland.org/wcc/
    currentanimals/april18-2014";"Raising a baby owl is hard
     work -- Audubon Society of Portland"
"2017-01-27 17:27:40";"https://www.facebook.com/search/top
    /?q=owls";"owls - Facebook Search"
"2017-01-27 17:29:07";"https://www.facebook.com/search/top
    /?q=snowy%20owl";"snowy owl - Facebook Search"
"2017-01-28 21:46:46";"https://www.youtube.com/results?
    search_query=how+to+care+for+owls";"how to care for owls
```

```
    - YouTube"
"2017-01-28 21:50:55";"https://www.youtube.com/watch?v=1
   Zh50kOKQR0";"What to do if you want a pet owl - YouTube"
"2017-01-28 21:50:55";"https://www.youtube.com/watch?v=
   vV18Vc6quVY";"Owls To You - How it all started! -
   YouTube"
"2017-01-28 22:17:22";"https://www.google.com/#q=falcons+
   birds";"Google"
"2017-01-28 22:18:02";"https://www.google.com/#q=where+can+
   I+learn+falconry";"Google"
"2017-01-28 22:40:03";"https://www.etsy.com/search.php?
   search_query=owls&search_type=all";"owls -- Etsy"
"2017-01-31 19:12:23";"https://www.google.com/#q=snowy+owl+
   care+pdf";"Google"
"2017-01-31 19:14:27";"https://www.google.com/#q=snowy+owl+
   wingspan+xls";"Google"
"2017-01-31 19:21:04";"https://www.google.com/webhp?
   sourceid=chrome-instant&rlz=1C1CHBD_enUS729US729&ion=1&
   espv=2&ie=UTF-8#q=Owl+wingspans+xls";"Owl wingspans xls
   - Google Search"
"2017-01-31 19:26:02";"https://secure.defenders.org/site/
   SPageServer?pagename=wagc_snowyowl&s_src=3WEW1700XXXXX&
   s_subsrc=013117_adopt_block_snowy-owl/basic-facts";"
   Adopt a Snowy Owl - Wildlife Adoption and Gift Center"
"2017-01-31 19:53:32";"https://www.google.com/#q=trippy+owl
   +pictures";"trippy owl pictures - Google Search"
"2017-02-02 22:50:31";"https://www.flickr.com/photos
   /131146257@N07/32454215321";"Grand duc d'Amérique /
   Great Horned Owl / Domaine de Maizere../ Flickr"
"2017-02-02 22:50:43";"https://www.flickr.com/photos
   /131146257@N07/32443981846/in/photostream/";"Chouette é
   pervière / Northern Hawk Owl / Saint-Augustin-de../
   Flickr"
```

Destaca especialmente la visita a la web de venta de aves en UK `http://www.birdtrader.co.uk`, algo que también se observará en el análisis del dispositivo Android (3.2.1 (pág. 47)), con especificaciones sobre ventas (*for sale*) de aves:

```
"2017-01-27 17:00:20";"http://www.birdtrader.co.uk/list-all
   -adverts?sstr=snowy%20owls&ads_dist=5";"All latests
   birds for sale / Birdtrader"
"2017-01-27 17:31:04";"http://www.birdtrader.com/";"Birds
   for sale"
"2017-01-27 17:31:11";"http://www.birdtrader.co.uk/list-all
   -adverts?sstr=owl&ads_dist=5";"All latests birds for
   sale / Birdtrader"
"2017-01-27 17:31:21";"http://www.birdtrader.co.uk/list-all
   -adverts?sstr=owl&ads_dist=5&page=2";"Browse All latests
```

```
     birds for sale / Birdtrader"
"2017-01-27 17:31:35";"http://www.birdtrader.co.uk/list-all
    -adverts?sstr=owl&ads_dist=5&page=3";"Find All latests
    birds for sale / Birdtrader"
"2017-01-27 17:31:50";"http://www.birdtrader.co.uk/owls/
    breeding-pair-ashy-faced/557508";"Breeding pair ashy
    faced for sale in Norfolk, Eastern / Birdtrader"
"2017-01-27 17:31:57";"http://www.birdtrader.co.uk/owls/
    dark-breasted-barn-owls/557507";"Dark Breasted Barn Owls
     for sale in Norfolk, Eastern / Birdtrader"
```

Resultados

La exploración del historial de navegación ha permitido concluir que hay evidencias de búsqueda de información sobre cómo comprar búhos.

2.4.3. Descargas de Internet

En el archivos `csv` de descargas se encuentran documentos e imágenes vistos anteriormente en la búsqueda de palabras clave (2.2.3 (pág. 14)). Ahora se aclara además la procedencia online exacta de esos archivos, así como el momento de finalización de las descargas.

```
$ cut -d ';' -f1,2,3,4 downloads.csv | grep -i owl`
...
"url";"path";"size";"end"
"http://www.ncwildlife.org/Portals/0/Learning/documents/
    Profiles/greathornedowl.pdf";"C:\Users\Sarah M\Downloads
    \Great Horned Owl Info.pdf";355574;"2017-01-27 01:16:49"
"https://mail.google.com/mail/";"C:\Users\Sarah M\Downloads
    \Great Horned Owl.jpg";64476;"2017-01-27 17:19:12"
"https://mail.google.com/mail/";"C:\Users\Sarah M\Downloads
    \Pygmy Owl.jpg";94519;"2017-01-27 17:19:16"
"https://mail.google.com/mail/";"C:\Users\Sarah M\Downloads
    \Snowy Owl.jpg";5948982;"2017-01-27 17:19:18"
"https://mail.google.com/mail/";"C:\Users\Sarah M\Downloads
    \Snowy Owl 2.jpg";10051;"2017-01-27 17:33:22"
"https://mail.google.com/mail/";"C:\Users\Sarah M\Downloads
    \Snowy Owl 3.jpg";74943;"2017-01-27 17:33:24"
"https://mail.google.com/mail/";"C:\Users\Sarah M\Downloads
    \Snowy Owl 4.jpg";3496271;"2017-01-27 17:33:24"
"http://www.owlpages.com/download/Owl_Emergency_Care.pdf";"
    C:\Users\Sarah M\Downloads\Owl_Emergency_Care.pdf
    ";142534;"2017-01-31 19:09:01"
"http://www.owlpages.com/download/Owl_Keeping.pdf";"C:\
    Users\Sarah M\Downloads\Owl_Keeping.pdf
```

```
    ";218461;"2017-01-31 19:09:11"
"";"C:\Users\Sarah M\Desktop\Snowy_Owl.pdf
    ";593265;"2017-01-31 19:12:20"
"https://www.google.com/";"C:\Users\Sarah M\Downloads\
    Bibliography - Snowy Owl 14 April 2014 - GLOW posting.
    xls";396800;"2017-01-31 19:12:44"
"https://www.google.com/";"C:\Users\Sarah M\Downloads\
    Sightings2005.xls";112128;"2017-01-31 19:21:15"
"";"C:\Users\Sarah M\Desktop\Next pet.jpg
    ";44730;"2017-01-31 19:27:24"
```

2.4.4. Visualización de imágenes y pdf desde archivo

En caso que algunas imágenes o documentos locales hayan sido abiertos mediante aplicaciones del navegador, también constan. Particularmente interesante es la constancia de archivos en una unidad `F:` del sistema, que podrían indicar su presencia en dispositivos externos. Tales dispositivos se han detectado en el apartado *Dispositivos USB conectados* (apartado 2.3.4, pág. 19)

```
$ cut -d ';' -f1,2,3 output/browsers/history.csv | grep -iP
    "owl|pet"`
...
"last_visit";"url";"title"
"2017-01-27 T01:06:19Z";"file:///C:/Users/Sarah%20M/
    Downloads/Luna%20Owl.jpg";""
"2017-01-27 T01:16:48Z";"file:///C:/Users/Sarah%20M/
    Downloads/Great%20Horned%20Owl%20Info.pdf";""
"2017-01-27 T17:23:25Z";"file:///C:/Users/Sarah%20M/Desktop
    /pets/Snowy%20Owl.jpg";""
"2017-01-27 T17:23:29Z";"file:///C:/Users/Sarah%20M/Desktop
    /pets/Pygmy%20Owl.jpg";""
"2017-01-27 T17:23:32Z";"file:///C:/Users/Sarah%20M/Desktop
    /pets/Great%20Horned%20Owl.jpg";""
"2017-01-30 T18:51:20Z";"file:///C:/Users/Sarah%20M/Desktop
    /pets/Great%20Horned%20Owl.jpg";""
"2017-01-30 T18:51:20Z";"file:///C:/Users/Sarah%20M/Desktop
    /pets/Pygmy%20Owl.jpg";""
"2017-01-30 T18:51:20Z";"file:///C:/Users/Sarah%20M/Desktop
    /pets/Snowy%20Owl.jpg";""
"2017-01-30 T18:51:20Z";"file:///C:/Users/Sarah%20M/
    Downloads/Great%20Horned%20Owl%20Info.pdf";""
"2017-01-30 T18:51:20Z";"file:///C:/Users/Sarah%20M/
    Downloads/Luna%20Owl.jpg";""
"2017-01-31 19:10:30";"file:///C:/Users/Sarah%20M/Documents
    /New%20Pet%20Care/Owl_Emergency_Care.pdf";"
    Owl_Emergency_Care.pdf"
```

```
"2017-02-02 T22:00:42Z";"file:///C:/Users/Sarah%20M/
    Documents/New%20Pet%20Care/My%20New%20Pet.jpg";""
"2017-02-02 T22:38:25Z";"file:///F:/My%20New%20Pet.jpg";""
"2017-02-02 T22:38:35Z";"file:///F:/Snowy%20Owl%20Care.pdf
    ";""
"2017-02-02 T22:38:39Z";"file:///F:/Snowy_Owl.pdf";""
"2017-02-02 T22:39:08Z";"file:///C:/Users/Sarah%20M/
    Documents/New%20Pet%20Care/Owl_Emergency_Care.pdf";""
```

2.4.5. Correo electrónico

A través del historial de navegación se detecta el uso de la cuenta `mcavoys87@gmail.com`. Es posible observar la fecha de consulta y el asunto de los mails en el correo, así como la fecha de composición de nuevos correos. En concreto se observa que el asunto de un correo del día 27 de enero de 2017 hace referencia a la venta de búhos.

Aviso

Para poder ver datos como la primera entrada registrada en `gmail` o la asociación a una cuenta de `twitter` se ha consultado el historial sin filtrar por palabra clave. Esta no es una buena práctica forense, porque entra en la intimidad de la persona investigada sin el filtro objetivo de las palabras clave.
El RVT2 permite hacer búsquedas solo en aquellos documentos y eventos que hayan dado positivo en una búsqueda ciega de palabras clave. No consideraremos por ahora esta opción.

```
$ cut -d ';' -f1,2,3 history.csv | grep gmail`
...
"2017-01-27 17:06:52";"https://www.google.com/gmail/about
    /";"Gmail - Free Storage and Email from Google"
"2017-01-27 17:07:50";"https://mail.google.com/mail/#inbox
    /159d73b41b53f2e8";"Confirm your Twitter account, Sarah
    McAvoy - mcavoys87@gmail.com - Gmail"
"2017-01-27 17:08:12";"https://mail.google.com/mail/#inbox
    /159d0e02b296fde4";"Sarah, get more out of your new
    Android device - mcavoys87@gmail.com - Gmail"
"2017-01-27 17:08:17";"https://mail.google.com/mail/#inbox?
    compose=new";""
"2017-01-27 17:19:46";"https://mail.google.com/mail/#inbox
    /159e0e81a1cf3d48?projector=1";""
"2017-01-27 17:33:07";"https://mail.google.com/mail/#inbox
    /159e0e81a1cf3d48";"Owls for Sale - mcavoys87@gmail.com
    - Gmail"
```

```
"2017-01-28 22:28:20";"https://mail.google.com/mail/#inbox
    ";"Inbox (1) - mcavoys87@gmail.com - Gmail"
"2017-01-28 22:28:28";"https://mail.google.com/mail/#inbox
    /159e72c5eb387e4f";"Please verify your account -
    mcavoys87@gmail.com - Gmail"
"2017-01-28 22:28:28";"https://mail.google.com/mail/#inbox
    /159e72c5eb387e4f";"Please verify your account -
    mcavoys87@gmail.com - Gmail"
"2017-02-02 22:23:43";"https://mail.google.com/mail/u/0/#
    inbox/15a00bc1020b358d";"(no subject) - mcavoys87@gmail.
    com - Gmail"
"2017-02-02 21:29:50";"https://mail.google.com/mail/u/0/#
    inbox?compose=15a00bbbae3ab77e";""
"2017-02-02 21:53:21";"https://mail.google.com/mail/u/0/#
    inbox?compose=new";""
```

Resultados

La presencia de un correo con asunto `Owls for Sale` visitado el día 27 de enero de 2017 reafirma el interés en la compra de estos animales por parte del investigado

El historial de navegación solo guarda una información limitada de los correos: el título de la página web (que se corresponde con el asunto del correo) y poco más. No hay información sobre emisores, receptores o fechas de envío. Aunque en el pasado era posible recuperar parte de esta información de la caché del navegador, Google y los demás operadores de correo electrónico a través de la web ya no permiten que esta información se cachée, para proteger a sus usuarios. Podría ser posible acceder a parte de esta información analizado la memoria RAM del ordenador o el archivo `hybernate`, que guarda la memoria RAM cuando el ordenador entra en hibernación. Por ahora, este análisis está fuera de los objetivos de este write-up.

Dado que el usuario ha accedido al correo GMail a través del navegador y no mediante una aplicación de gestión de correo como Outlook o Thunderbird, no se hallan archivos propios de estas aplicaciones que con los que podría recuperarse el contenido y cabezeras de los correos (`pst`, `ost`, `mbox`, ...)

Info

RVT2 permite parsear archivos `eml`, así como los propios de aplicaciones de gestión de correo, para obtener el contenido de los correos, extraer estadísticas relevantes y adverarlos.

2.4.6. Archivos recientes (Lnk, Jumplists)

Los archivos **lnk** permiten identificar la fecha de último acceso a documentos y es uno de los pocos indicadores de la presencia de archivos en unidades remotas (USB, discos externos)

```
rvt2 --source 100100-07-1 -j windows.recentfiles
```

Info

Salida: `analysis/recentfiles/`, `output/windows/recentfiles/`

Se demuestra el acceso (*open file*) a los siguientes archivos con la palabra clave `owl` abiertos en el PC analizado:

```
$ cut -d ';' -f1,2,3,4,6,7 analysis/recentfiles/recentfiles
    .csv | grep -iP "owl|pet"
```

```
last_open_date;first_open_date;application;path;drive_type;
    drive_sn
2017-01-27T01:16:48Z;;Google Chrome 9.0.597.84 /
    12.0.742.100 / 13.0.785.215 / 26 / 48.0.2564.116;
C:/Users/Sarah M/Downloads/Great Horned Owl Info.pdf;Fixed
    ;0x14412537
2017-01-27T01:06:19Z;2017-01-27T01:06:19Z;;C:/Users/Sarah M
    /Downloads/Luna Owl.jpg;Fixed;0x14412537
2017-01-27T01:16:48Z;2017-01-27T01:16:48Z;;C:/Users/Sarah M
    /Downloads/Great Horned Owl Info.pdf;Fixed;0x14412537
2017-01-27T01:16:48Z;;Google Chrome 9.0.597.84 /
    12.0.742.100 / 13.0.785.215 / 26 / 48.0.2564.116;C:/
    Users/Sarah M/Downloads/Great Horned Owl Info.pdf;Fixed
    ;0x14412537
2017-01-27T17:21:49Z;;Microsoft Paint (built-in Win7);C:/
    Users/Sarah M/Desktop/pets/Great Horned Owl.jpg;Fixed;0
    x14412537
2017-01-27T17:22:22Z;;Edge Browser;;;
2017-01-27T17:23:03Z;;Photos Microsoft 16.526.11220.0 (
    Windows 10);C:/Users/Sarah M/Desktop/pets/Great Horned
    Owl.jpg;Fixed;0x14412537
2017-01-27T17:23:25Z;2017-01-27T17:23:25Z;;C:/Users/Sarah M
    /Desktop/pets/Snowy Owl.jpg;Fixed;0x14412537
2017-01-27T17:23:25Z;;Photos Microsoft 16.526.11220.0 (
    Windows 10);C:/Users/Sarah M/Desktop/pets/Snowy Owl.jpg;
    Fixed;0x14412537
2017-01-27T17:23:25Z;;Quick Access;C:/Users/Sarah M/Desktop
    /pets/Snowy Owl.jpg;Fixed;0x14412537
```

```
2017-01-27T17:23:29Z;2017-01-27T17:23:29Z;;C:/Users/Sarah M
    /Desktop/pets/Pygmy Owl.jpg;Fixed;0x14412537
2017-01-27T17:23:29Z;;Photos Microsoft 16.526.11220.0 (
    Windows 10);C:/Users/Sarah M/Desktop/pets/Pygmy Owl.jpg;
    Fixed;0x14412537
2017-01-27T17:23:32Z;2017-01-27T17:21:49Z;;C:/Users/Sarah M
    /Desktop/pets/Great Horned Owl.jpg;Fixed;0x14412537
2017-01-31T19:08:59Z;;Google Chrome 9.0.597.84 /
    12.0.742.100 / 13.0.785.215 / 26 / 48.0.2564.116;C:/
    Users/Sarah M/Downloads/Owl_Emergency_Care.pdf;Fixed;0
    x14412537
2017-01-31T19:08:59Z;;Quick Access;C:/Users/Sarah M/
    Downloads/Owl_Emergency_Care.pdf;Fixed;0x14412537
2017-01-31T19:09:10Z;2017-01-31T19:09:10Z;;C:/Users/Sarah M
    /Downloads/Owl_Keeping.pdf;Fixed;0x14412537
2017-01-31T19:09:10Z;;Google Chrome 9.0.597.84 /
    12.0.742.100 / 13.0.785.215 / 26 / 48.0.2564.116;C:/
    Users/Sarah M/Downloads/Owl_Keeping.pdf;Fixed;0x14412537
2017-01-31T19:09:10Z;;Quick Access;C:/Users/Sarah M/
    Downloads/Owl_Keeping.pdf;Fixed;0x14412537
2017-01-31T19:10:30Z;;Google Chrome 9.0.597.84 /
    12.0.742.100 / 13.0.785.215 / 26 / 48.0.2564.116;C:/
    Users/Sarah M/Documents/New Pet Care/Owl_Emergency_Care.
    pdf;Fixed;0x14412537
2017-01-31T19:15:03Z;;Google Chrome 9.0.597.84 /
    12.0.742.100 / 13.0.785.215 / 26 / 48.0.2564.116;C:/
    Users/Sarah M/Desktop/Snowy_Owl.pdf;Fixed;0x14412537
2017-01-31T19:15:03Z;;Quick Access;C:/Users/Sarah M/
    Documents/New Pet Care/Snowy_Owl.pdf;Fixed;0x14412537
2017-01-31T19:27:24Z;2017-01-31T19:27:24Z;;C:/Users/Sarah M
    /Desktop/Next pet;Fixed;0x14412537
2017-02-02T22:00:42Z;;Photos Microsoft 16.526.11220.0 (
    Windows 10);C:/Users/Sarah M/Documents/New Pet Care/My
    New Pet.jpg;Fixed;0x14412537
2017-02-02T22:00:42Z;;Quick Access;C:/Users/Sarah M/
    Documents/New Pet Care/My New Pet.jpg;Fixed;0x14412537
2017-02-02T22:38:25Z;2017-02-02T21:53:32Z;;F:/My New Pet.
    jpg;Removable;0x80bc89a2
2017-02-02T22:38:25Z;;Photos Microsoft 16.526.11220.0 (
    Windows 10);F:/My New Pet.jpg;Removable;0x80bc89a2
2017-02-02T22:38:25Z;;Quick Access;F:/My New Pet.jpg;
    Removable;0x80bc89a2
2017-02-02T22:38:35Z;2017-02-02T22:38:35Z;;F:/Snowy Owl
    Care.pdf;Removable;0x80bc89a2
2017-02-02T22:38:35Z;;Edge Browser;F:/Snowy Owl Care.pdf;
    Removable;0x80bc89a2
2017-02-02T22:38:35Z;;Quick Access;F:/Snowy Owl Care.pdf;
    Removable;0x80bc89a2
2017-02-02T22:38:39Z;2017-01-31T19:12:19Z;;F:/Snowy_Owl.pdf
```

```
    ;Removable;0x80bc89a2
2017-02-02T22:39:08Z;2017-01-31T19:08:59Z;;C:/Users/Sarah M
    /Documents/New Pet Care/Owl_Emergency_Care.pdf;Fixed;0
    x14412537
2017-02-02T22:39:08Z;2017-01-31T19:10:23Z;;C:/Users/Sarah M
    /Documents/New Pet Care;Fixed;0x14412537
2017-02-02T22:39:08Z;;Edge Browser;C:/Users/Sarah M/
    Documents/New Pet Care/Owl_Emergency_Care.pdf;Fixed;0
    x14412537
2017-02-02T22:39:08Z;;Quick Access;C:/Users/Sarah M/
    Documents/New Pet Care/Owl_Emergency_Care.pdf;Fixed;0
    x14412537
2017-02-02T22:39:08Z;;Windows Explorer Windows 8.1+;C:/
    Users/Sarah M/Documents/New Pet Care;Fixed;0x14412537
```

Algunos han sido abiertos desde otros dispositivos (*drive_type=Removable*) y pueden relacionarse con el USB detectado en el apartado *Dispositivos USB conectados* (apartado 2.3.4, pág. 19).

El uso de aplicaciones en la nube como `OneDrive` podría implicar el intercambio de archivos relevantes por tales medios. Sin embargo no es posible acceder a los datos de esa aplicación pues se guardan en la nube.

```
last_open_date;first_open_date;application;path;drive_type;
    drive_sn
2017-01-26T23:47:58Z;2017-01-26T23:47:11Z;;C:/Users/Sarah
    McAvoy/AppData/Local/Microsoft/OneDrive/OneDrive.exe;
    Fixed;0x14412537
2017-01-31T18:52:35Z;2017-01-27T00:36:12Z;;C:/Users/Sarah M
    /AppData/Local/Microsoft/OneDrive/OneDrive.exe;Fixed;0
    x14412537
```

Se detecta también la ejecución de software relacionado con redes sociales como `Skype`, `Pidgin` o `yahoomessenger`:

```
last_open_date;first_open_date;application;path;drive_type;
    drive_sn
2017-01-26T23:47:58Z;2017-01-26T23:47:11Z;;C:/Users/Sarah
    McAvoy/AppData/Local/Microsoft/OneDrive/OneDrive.exe;
    Fixed;0x14412537
2017-01-27T01:48:36Z;2017-01-27T01:48:36Z;;C:/Program Files
     (x86)/Skype/Phone/Skype.exe;Fixed;0x14412537
2017-01-30T18:47:49Z;2017-01-30T18:47:49Z;;C:/Program Files
     (x86)/Skype/Phone/Skype.exe;Fixed;0x14412537
2017-02-01T17:00:22Z;2017-02-01T17:00:22Z;;C:/Users/Sarah M
    /AppData/Roaming/Microsoft/Windows/Pidgin/pidgin.exe;
    Fixed;0x14412537
2017-02-02T22:25:24Z;2017-02-02T22:49:01Z;;C:/Users/Sarah M
    /AppData/Local/yahoomessenger/Update.exe;Fixed;0
```

```
    x14412537
```

En el apartado *Redes sociales* (apartado 2.4.9, pág. 35) se ampliará la información.

2.4.7. Shellbags

En algunos casos los `shellbags` permiten corroborar la existencia de directorios que actualmente no constan en el sistema de archivos. Están incluidos en el resultado del parseo del registro de Windows.

```
$ rvt2 --source 100100-07-1 -j windows.autorip
```

Info

Solo algunas de las entradas del registro serán tratadas en este *write up* para dar una muestra.

```
less output/windows/hives/15_user-account-file-access-
    activity_p06.txt
```

15_user-account-file-access-activity_p06.txt
En este caso no aportan información relevante para la investigación.

2.4.8. Ejecutables (Prefetch, RFC, BAM)

Prefetch permite identificar las fechas de ejecución de cada aplicación. Puede usarse en este caso para encontrar el uso de aplicaciones que permitan conversaciones online.

```
rvt2 --source 100100-07-1 -j windows.exec
```

Info

Salida: `output/windows/execution`

Para ver la primera y última fechas de uso de los ejecutables:

```
$ cut -d ';' -f 2,4,5 /morgue/100100-training/100100-07-1/
    output/windows/execution/prefetch_p06.csv
...
Executable;Birth time;Run time 0
SKYPE.EXE;2017-01-30T18:48:00Z;2017-01-31 20:01:41
PIDGIN.EXE;2017-02-01T17:01:24Z;2017-02-02 21:25:05
```

```
YAHOO MESSENGER.EXE;2017-02-02T22:25:35Z;2017-02-02
    22:26:09
MICROSOFT.PHOTOS.EXE;2017-01-27T17:30:55Z;2017-02-02
    22:05:31
MICROSOFTEDGE.EXE;2017-01-27T17:22:27Z;2017-02-02 22:39:08
ONEDRIVE.EXE;2017-01-27T16:57:35Z;2017-02-02 21:24:36
EXPLORER.EXE;2017-01-27T16:54:23Z;2017-02-01 16:55:08
CHROME.EXE;2017-01-27T16:58:06Z;2017-02-02 22:49:15
MSPAINT.EXE;2017-01-27T17:21:51Z;2017-01-27 17:21:49
```

Se detecta el uso de ciertas aplicaciones como *skype*, *edge*, *onedrive*, *chrome*, *cmd*, *pidgin*, . . .

Si las fechas de modificación coinciden, puede usarse para asociarlas a la manipulación de ciertos archivos .

2.4.9. Redes sociales

Para tratar de averiguar si se ha realizado contacto mediante chat con posibles vendedores, se puede analizar qué aplicaciones de redes sociales son utilizadas en el dispositivo.

Algunas de estas aplicaciones ya han sido identificadas en los `lnk` (2.4.6 (pág. 31)) y en el `prefetch` (2.4.8 (pág. 34))

En el historial de navegación se presencian múltiples logins y acciones en sitios web que requieren usuario registrado y que podrían usarse para comunicarse con otros:

Aviso

Se realiza otra vez una búsqueda sin filtro. Tener en cuenta la finalidad práctica y no judicial de este *write up*

`$ cut -d ';' -f1,2,3 history.csv` * Cuenta en **instagram**

```
"2017-01-27 01:11:10";"https://www.instagram.com/accounts/
    login/";"Login - Instagram"
```

- Cuenta en **youtube**

```
"2017-01-27 17:07:25";"https://accounts.youtube.com/
    accounts/SetSID?ssdc=1&sidt=
    ALWU2cv14UuCFSD5CVkN0ss0fZahkmqmrohbWzfqZi1HHCXab2YyveRRuBiwTMI0GHZL3kMS5YaG
    %2BUJAWmRCK18CexOfv4t8dsK7KWf7H9eMS4bzcr2BFqlnPoj%2
    FqLXWvJOr%2Fx4hj8OaII5EVdqfdpJxaY1CD86%2
    BO6i6uqTgCMe2xurQFMKoeSK7dEHApUV%2BtSw%2FNbNRTVu2iqsY1g
    %2F2ZHBXm7hmVsUVXrLQGDWT0Wy6qOWT7c%2
```

```
    BD6LqSIHeiV1981kuA3fg05PyClWeheSoNMKEejhrRzohF1A%3D%3D&
    continue=https%3A%2F%2Fmail.google.com%2Fmail%2F%3Fpli%3
    D1%26auth%3DRAR7vC-
    uDEffHcaLoOj2ZACUJDq0ki8mkrnn0trua3AVM_kUrtmbSloouy-5
    HPv7S21MlA.";"Gmail"
"2017-01-28 22:28:07";"https://accounts.youtube.com/
    accounts/SetSID?ssdc=1&sidt=ALWU2cv3dSmxt5jfLSEVIhYLBiV
    %2Bh6R66KvPqx55c584n55LLUtPdTSFKtmyz6A%2
    FhqOZVUkbdU1JZn8xcnMH0Z0jPHq5851rus67mdMy0f8BT0FQkskFbOq56JTKbSZxtgdvcjjIqCG1
    %2FK%2BYC8rq0mn9KRiuH7cRHw%2Fh8g8RJK8%2
    Fnv82JKBdg407sbEIg7huhGme9szzYMtWkME3A3kU0bashNg09rKLf15RUaHNbgcd
    %2Bc4V6Q6VdmQWLGFg%3D%3D&continue=https%3A%2F%2Faccounts
    .google.com%2FManageAccount";"My Account"
```

- Cuenta en **Twitter**

```
"2017-01-27 17:07:52";"https://twitter.com/account/access
    ";""
```

- Cuenta en **facebook**

```
"2017-01-27 17:15:24";"https://www.facebook.com/search/top
    /?q=terry%20bunch";"terry bunch - Facebook Search"
"2017-01-27 17:16:05";"https://www.facebook.com/profile.php
    ?id=100013220888470&ref=br_rs";"Monica Neff"
"2017-01-27 17:17:55";"https://www.facebook.com/profile.php
    ?id=100013119909406&pnref=lhc.friends";"Isaiah Dashner"
"2017-01-27 17:18:02";"https://www.facebook.com/profile.php
    ?id=100013119909406&lst=100015073810863%3
    A100013119909406%3A1485537474&sk=friends&source_ref=
    pb_friends_tl";"Isaiah Dashner"
"2017-01-27 17:42:56";"https://www.facebook.com/sarah.
    mcavoy.9638#";"(2) Sarah Mcavoy"
"2017-01-27 17:45:22";"https://www.facebook.com/logout.php
    ";"Facebook - Log In or Sign Up"
"2017-02-01 17:12:58";"https://www.facebook.com/sarah.
    mcavoy.9638";"Sarah Mcavoy"
"2017-02-01 17:12:58";"https://www.facebook.com/sarah.
    mcavoy.9638";"Sarah Mcavoy"
"2017-02-01 17:13:11";"https://www.facebook.com/settings";"
    General Account Settings"
"2017-02-01 17:13:42";"https://www.facebook.com/settings?
    tab=account&section=password&view";""
```

- Cuenta en **pottermore**

```
"2017-01-27 01:04:18";"https://my.pottermore.com/account/
    join";"Join - Pottermore"
"2017-01-27 01:04:28";"https://www.pottermore.com/";"
    Pottermore - The digital heart of the Wizarding World"
```

- Cuenta en **pidgin**, relacionada con **facebook**

```
"2017-02-01 17:21:33";"http://askubuntu.com/questions
    /714573/how-to-grant-application-access-for-facebook-
    account";"empathy - How to grant application access for
    Facebook account - Ask Ubuntu"
"2017-02-01 17:21:48";"https://pidgin.im/pipermail/support
    /2010-February/020326.html";"Facebook XMPP with Pidgin"
"2017-02-01 17:21:58";"https://www.google.com/webhp?
    sourceid=chrome-instant&rlz=1C1CHBD_enUS729US729&ion=1&
    espv=2&ie=UTF-8#q=how+to+get+facebook+xmpp";"Google"
```

- Cuenta en **tumblr** asociada a **mcavoys87_gmail.com**, con publicación de un blog

```
"2017-01-28 22:20:02";"https://www.tumblr.com/openid/
    register";"Yahoo"
"2017-01-28 22:22:12";"https://login.yahoo.com/account/
    challenge/recaptcha?intl=us&src=tumblr&altreg=&specId=
    usernameRegFreeformGender&context=reg&done=https%3A%2F%2
    Flogin.yahoo.com%2Faccount%2Ftumblr-migration%3Fcombine
    %3D0%26done%3Dhttps%253A%252F%252Fapi.login.yahoo.com
    %252Foauth2%252Frequest_auth%253Fresponse_type%253Dcode
    %2526redirect_uri%253Dhttps%25253A%25252F%25252Fwww.
    tumblr.com%25252Fopenid%25252Fconnect%2526client_id%253
    Ddj0yJmk9eDczSEtQeDc5WG9pJmQ9WVdrOVJUSm9aVmxVTjJVbWNHbzlNQS0tJnM9Y29uc3VtZXJz
    --%2526nonce%253D9618d1b06d54884bf7e448c1fc5b61a9%2526
    state%253D843b1db42dee82058cb32309c7764fdc%2526scope%253
    Dopenid%252Bsdpp-w&supress=1&authMechanism=reg&
    authCredentialsType=WyJjb29raWVzIl0%3D&yid=mcavoys87%40
    gmail.com&dname=mcavoys87%40gmail.com&s=QQ--&c=9meVuHP.2
    YI2zP8.c1qa5rCNpuZ91JEcDQ9Th7Unpgw.
    mmxGlcpAMm5860i4_BtphVY7e7Fpn6ejk.
    zcMK_mIVTun3eau7Y9tozHCvSMpSoniQVHudCtiNiiUa2uw7CzSWB82h18i1BBIlLRIE5gkYSKufI
    .5VxsdR8sBSQAHUYjKA4FJ6KPXw-~A&crumb=fYuXyZUBA61&acrumb=
    WqhERlA5";"Tumblr"
"2017-01-28 22:22:12";"https://login.yahoo.com/account/
    create/success?intl=us&src=tumblr&altreg=&specId=
    usernameRegFreeformGender&context=reg&done=https%3A%2F%2
```

```
    Flogin.yahoo.com%2Faccount%2Ftumblr-migration%3Fcombine
    %3D0%26done%3Dhttps%253A%252F%252Fapi.login.yahoo.com
    %252Foauth2%252Frequest_auth%253Fresponse_type%253Dcode
    %2526redirect_uri%253Dhttps%25253A%25252F%25252Fwww.
    tumblr.com%25252Fopenid%25252Fconnect%2526client_id%253
    Ddj0yJmk9eDczSEtQeDc5WG9pJmQ9WVdrOVJUSm9aVmxVTjJVbWNHbzlNQS0tJnM9Y29uc3VtZXJz
    --%2526nonce%253D9618d1b06d54884bf7e448c1fc5b61a9%2526
    state%253D843b1db42dee82058cb32309c7764fdc%2526scope%253
    Dopenid%252Bsdpp-w&supress=1&authMechanism=reg&
    authCredentialsType=WyJjb29raWVzIl0%3D&yid=mcavoys87%40
    gmail.com&dname=mcavoys87%40gmail.com&crumb=jQIjg%2
    FvUg62&acrumb=WqhERlA5&mWait=1&scrumb=RCOm7lmNG5M";"
    Tumblr"
"2017-01-28 22:22:12";"https://www.tumblr.com/register/pick
    -a-name";"Tumblr"
"2017-01-28 22:28:51";"https://login.yahoo.com/account/
    security";"Security - Yahoo Account Settings"
"2017-01-28 22:29:00";"https://www.tumblr.com/settings/blog
    /sarahmcavoyblog";"Blog Settings / Tumblr"
"2017-01-28 22:29:12";"https://sarahmcavoyblog.tumblr.com
    /";"Untitled"
"2017-02-02 22:49:18";"https://www.tumblr.com/";"Sign up /
    Tumblr"
"2017-02-02 22:49:24";"https://www.tumblr.com/login";"Log
    in / Tumblr"
"2017-02-02 22:49:39";"https://www.tumblr.com/openid/
    connect";"Yahoo - login"
"2017-02-02 22:49:59";"https://www.tumblr.com/dashboard";"
    Tumblr"
"2017-02-02 22:49:59";"https://www.tumblr.com/openid/
    connect?code=dsupy7w&state=207076
    c8117b5c52bf15d7348d6b35c5";"Tumblr"
```

- Cuenta en **yahoo messenger**

```
"2017-01-28 22:28:36";"https://login.yahoo.com/account/
    action/verify?t=9
    CmexxS9Nl4WzzthRZ5EW1YIduFAJWPb1MpdQou7uyafbGl42XvKPUlmRpn0hRQJnPKQqiEy2ddhkc
    .wOFgx3rw--&.scrumb=LB.3gE3h5AD&.scrumb2=EOIjnsekeMN";"
    Yahoo Account Settings"
"2017-02-02 22:24:05";"https://www.google.com/url?sa=f&rct=
    j&url=https://messenger.yahoo.com/&q=&esrc=s&ei=
    gLGTWPqPOMmlmwHlnKWYCQ&usg=
    AFQjCNGqqA6bzFEYpXrcIXnOYVK67NOnQQ";""
"2017-02-02 22:24:06";"https://messenger.yahoo.com/";""
"2017-02-02 22:24:58";"http://login.yahoo.com/config/login?
    logout=1&.direct=1&.done=https%3A%2F%2Fmessenger.yahoo.
    com%3Fstatus%3D";"Logging out..."
```

- Cuenta en **skype**

```
"2017-01-30 T18:51:20Z";"https://login.live.com/ppsecure/
    post.srf?client_id=00000000480BC46C&scope=service%3A%3
    Alw.skype.com%3A%3AMBI_SSL&response_type=token&
    redirect_uri=https%3A%2F%2Flogin.live.com%2
    Foauth20_desktop.srf&state=999&locale=en&cobrandid
    =90010&lw=1&fl=phone2&client_flight=hsu%2
    CReservedFlight33%2CReservedFlight67&psi=skype&username=
    McavoyS87%40gmail.com&contextid=BE0071BCD6554B93&bk
    =1485802252&uaid=9e17ab7629980397d73a93c08272ead3&pid
    =15216";""
"2017-01-31 T19:01:02Z";"https://login.live.com/ppsecure/
    post.srf?client_id=00000000480BC46C&scope=service%3A%3
    Alw.skype.com%3A%3AMBI_SSL&response_type=token&
    redirect_uri=https%3A%2F%2Flogin.live.com%2
    Foauth20_desktop.srf&state=999&locale=en&cobrandid
    =90010&lw=1&fl=phone2&client_flight=hsu%2
    CReservedFlight33%2CReservedFlight67&psi=skype&username=
    McavoyS87%40gmail.com&contextid=40D811C97F8D893B&bk
    =1485889249&uaid=154287b990a556c255f6735711425171&pid
    =15216";""
"2017-01-31 T19:01:02Z";"https://login.live.com/ppsecure/
    post.srf?client_id=00000000480BC46C&scope=service%3A%3
    Alw.skype.com%3A%3AMBI_SSL&response_type=token&
    redirect_uri=https%3A%2F%2Flogin.live.com%2
    Foauth20_desktop.srf&state=999&locale=en&cobrandid
    =90010&lw=1&fl=phone2&client_flight=hsu%2
    CReservedFlight33%2CReservedFlight67&psi=skype&username=
    McavoyS87%40gmail.com&contextid=40D811C97F8D893B&bk
    =1485889249&uaid=154287b990a556c255f6735711425171&pid
    =15216";""
"2017-01-30 T18:51:20Z";"https://login.live.com/ppsecure/
    post.srf?client_id=00000000480BC46C&scope=service%3A%3
    Alw.skype.com%3A%3AMBI_SSL&response_type=token&
    redirect_uri=https%3A%2F%2Flogin.live.com%2
    Foauth20_desktop.srf&state=999&locale=en&cobrandid
    =90010&lw=1&fl=phone2&client_flight=hsu%2
    CReservedFlight33%2CReservedFlight67&psi=skype&username=
    McavoyS87%40gmail.com&contextid=BE0071BCD6554B93&bk
    =1485802252&uaid=9e17ab7629980397d73a93c08272ead3&pid
    =15216";""
"2017-01-31 T19:01:02Z";"https://login.live.com/ppsecure/
    post.srf?client_id=00000000480BC46C&scope=service%3A%3
    Alw.skype.com%3A%3AMBI_SSL&response_type=token&
    redirect_uri=https%3A%2F%2Flogin.live.com%2
```

```
    Foauth20_desktop.srf&state=999&locale=en&cobrandid
    =90010&lw=1&fl=phone2&client_flight=hsu%2
    CReservedFlight33%2CReservedFlight67&psi=skype&username=
    McavoyS87%40gmail.com&contextid=40D811C97F8D893B&bk
    =1485889249&uaid=154287b990a556c255f6735711425171&pid
    =15216";""
"2017-01-31 T19:01:09Z";"https://apps.skype.com/home/?
    uiversion=7.31.80.104&language=en";""
"2017-01-31 T19:01:10Z";"https://apps.skype.com/adcontrol/
    prelogic.html";""
"2017-01-31 T19:01:15Z";"https://apps.skype.com/
    chatadwidget/?containerType=LER";""
```

- **Hangouts**

```
"2017-02-01 17:22:45";"https://clickserve.dartsearch.net/
    link/click?lid=43700015211414201&ds_s_kwgid
    =58700001981446618&&ds_e_adid=156893041869&
    ds_e_matchtype=search&ds_e_device=c&ds_e_network=g&&
    ds_url_v=2&ds_dest_url=https://gsuite.google.com/intl/
    en_us/products/hangouts/?utm_source=google&utm_medium=
    cpc&utm_campaign=na-US-all-en-dr-bkws-all-all-trial-e-na
    &utm_content=text-ad-none-any-DEV_c-CRE_156893041869-
    ADGP_[*Adgroup*]-KWID_[*TrackerID*]&utm_term=KW_google
    %20talk-ST_[*searchterm*]&gclid=
    CjwKEAiAq8bEBRDuuOuyspf5oyMSJAAcsEyWMUPQ2IZdfi3N7O_lj_KE5OPu_qLqo4dE7xzmf3Qok
    ";"Google Hangouts -- Video Conferencing & Meetings for
    Business"
"2017-02-01 17:23:56";"https://hangouts.google.com/";"
    Google Hangouts"
```

- **Google talk**

```
"2017-02-01 17:23:28";"https://www.google.com/#q=google+
    talk";"Google"
"2017-02-01 17:23:50";"https://support.google.com/talk/?hl=
    en";"Talk Help"
```

Del historial de navegación, se puede observar la descarga de archivos de instalación de aplicaciones *social media* con posible relevancia:

```
"url";"path";"size";"end"
"https://www.skype.com/en/download-skype/skype-for-windows/
    downloading/";"C:\Users\Sarah M\Downloads\SkypeSetupFull
    .exe";43918808;"2017-01-27 01:48:01"
```

```
"https://sourceforge.net/projects/pidgin/files/Pidgin
    /2.11.0/pidgin-2.11.0.exe/download?accel_key=62%3
    A1485968327%3Ahttps%253A//www.pidgin.im/%3Aff296d95
    %244400ae35fb0e6cb1cabd9f9c879ebf0d9c178170&click_id=
    b27b7e92-e89f-11e6-bb41-0200ac1d1d90&source=accel";"C:\
    Users\Sarah M\Downloads\pidgin-2.11.0.exe
    ";9256224;"2017-02-01 16:59:35"
"https://messenger.yahoo.com/?status=";"C:\Users\Sarah M\
    Downloads\yahoo-messenger-0.8.288-win32.exe
    ";46966800;"2017-02-02 22:25:08"
"https://messenger.yahoo.com/?status=";"C:\Users\Sarah M\
    Downloads\yahoo-messenger-0.8.288-win32.exe
    ";46966800;"2017-02-02 22:25:08"
```

Info

La variedad de aplicaciones específicas de redes sociales requiere de herramientas particulares y puestas al día para parsear sus bases de datos. RVT2 tiene incorporados plugins para procesar los datos de aplicaciones de amplio uso como `Skype` o `Whatsapp`. Sin embargo, otras aplicaciones requerirán de un tratamiento específico dependiendo del caso de análisis.

A pesar del número de aplicaciones localizadas, ninguna ha dado positivo en la búsqueda por palabras clave, con lo que no se analizarán en detalle.

2.4.10. Clasificación de imágenes

Entre las funcionalidades de RVT se incluye la classificación de imágenes mediante algoritmos de inteligencia artificial. Esto permite permite realizar una importante criba entre todas las imágenes encontradas en el disco para destacar únicamente aquellas sospechosas de tener un contenido relevante para la investigación.

Info

En este caso se usará el modelo genérico `Inception V3` que classifica imágenes en un elevado número de categorías. Para casos que impliquen la búsqueda de contenido pornográfico, es recomendable usar modelos predictivos más especicos como `nudenet` o `nsfw_detect`

```
$ rvt2 --source 100100-07-1 -j ai.classify --params model=
    IV3
```

El resultado desvela imágenes que podrían haber pasado por alto mediante palabras clave.

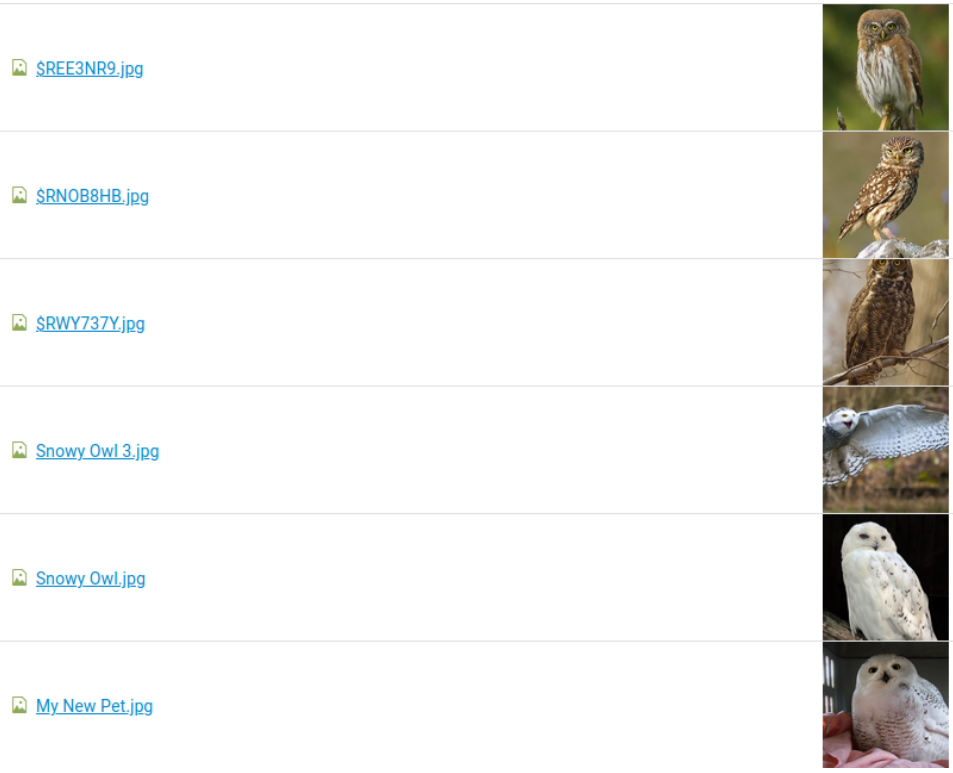

Figura 2.5: Imágenes reconocidas por la inteligencia artificial

Resultados

La classificación de imágenes por IA ha permitido identificar imágenes en localizaciones como la papelera de reciclaje o la caché del navegador Chrome que no contienen ninguna palabra clave en su título o metadatos.

Capítulo 3

Análisis de la fuente 100100-07-2

La fuente `100100-07-2.dd` se corresponde con una imagen forense dispositivo Android del sospechoso. En esta sección se completará la investigación realizada, explorando aquellos detalles que no se podían resolver únicamente con el análisis de la fuente Windows de la sección *Análisis de la fuente 100100-07-1* (apartado 2, pág. 7).

Aviso

En la actualidad, pocas veces se puede analizar una imagen forense de un dispositivo móvil porque tanto Android como iPhone impiden realizarlas.
Las herramientas comerciales como Cellebrite aprovechan errores y exploits del sistema para poder "rootear" el dispositivo y poder hacer una imagen forense. Estas herramientas son caras y no siempre funcionarán.
En la mayor parte de los casos, lo que se va a obtener es una copia lógica (archivo ZIP) con el contenido de la tarjeta SD del móvil, y algunos datos especiales de algunas de las aplicaciones instaladas.

Info

Actualmente, RVT2 solo dispone de unos pocos módulos específicos para Android, aunque pueden definirse nuevos si se desea parsear artefactos o bases de datos de esta plataforma.
Esta sección analiza alguna de las bases de datos específicas de Android, pero basa sus resultados sobretodo en técnicas generales como "strings" y "palabras clave" que pueden aplicarse sobre cualquier imagen forense.

Se realizarán los siguientes análisis sobre esta fuente:

- Preparación de la imagen y “preforense”:
  - Montaje de la imagen
  - Caracterización
  - Búsquedas ciegas
- Actividad de usuario
  - Actividad de navegadores
  - Actividad en redes sociales
  - Mensajería SMS
  - Aplicaciones instaladas
  - Mapas

3.1. Preparación de la imagen y “preforense”:

Info

La imagen forense está guardada en un archivo llamado `100100-07-2.dd`. Este sufijo `dd` se corresponde con una imagen forense de tipo “imagen DD” o “imagen RAW”. Este tipo de imagen forense es también muy común. Su desventaja principal con respecto al E01 de la sección anterior es que no está comprimida.

3.1.1. Montaje y caracterización

Los comandos relevantes para preparar la fuente y hacer la primera caracterización de la misma ya fueron introducidos en la sección anterior.

```
$ rvt2 --source 100100-07-2 -j mount
$ rvt2 --source 100100-07-2 -j characterize
```

La imagen de Android presenta un elevado número de particiones, condición característica de los dispositivos Android. El RVT2 solo monta aquellas que son relevantes, en nuestra experiencia pasada. En este caso, las particiones relevantes son: p04 (FAT16), p19 (EXT4), p28 (EXT4), p30 (EXT4) y especialmente la partición principal p31 (EXT4), de **27,2GB**.

El contenido resultada de la caracterización se puede encontrar en `analysis/characterize`. Se presenta a continuación, aunque no contiene información relevante para los objetivos de esta investigación.

Disk 100100-07-2 characterization

It is a disk image of size 29.1G and 32 partitions. * Model: * SerialNumber:

Partitions table

Partition	Size	Type	VSS
00	512.0	Safety Table	0
02	512.0	GPT Header	0
03	4.0K	Partition Table	0
04	64.0M	FAT16	0
05	1.0M	sbl1	0
06	512.0K	rpm	0
07	512.0K	tz	0
08	512.0K	sdi	0
09	512.0K	aboot	0
10	2.0M	pad	0
11	1.0M	sbl1b	0
12	512.0K	tzb	0
13	512.0K	rpmb	0
14	512.0K	abootb	0
15	3.0M	modemst1	0
16	3.0M	modemst2	0
17	512.0K	metadata	0
18	16.0M	misc	0
19	16.0M	EXT4	0
20	3.0M	imgdata	0
21	22.0M	laf	0
22	22.0M	boot	0
23	22.0M	recovery	0
24	3.0M	fsg	0
25	512.0K	fsc	0
26	512.0K	ssd	0
27	512.0K	DDR	0
28	1.0G	EXT4	0
29	30.0M	crypto	0
30	700.0M	EXT4	0
31	27.2G	EXT4	0
32	5.5K	grow	0

3.1.2. Búsquedas de palabras clave

Para poder buscar de forma eficiente en el contenido de los archivos del disco y facilitar el uso de palabras clave, se parsea con **Tika** y se indexa en **ElasticSearch**.

```
rvt2 --source 100100-07-2 -j indexer.save_directory
```

Una vez indexado, se puede buscar la palabra clave `owl` en Elastic utilizando **RVT-Analyzer**.

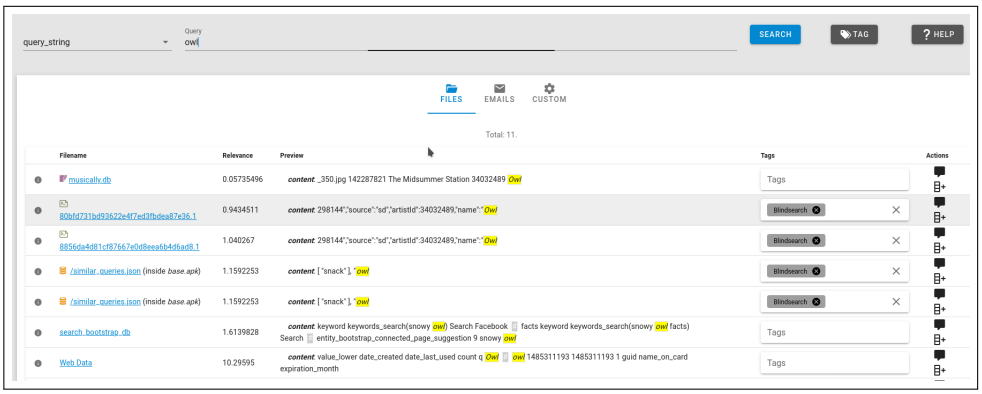

Figura 3.1: Rsultados de buscar owl en la indexación de la fuente 100100-07-2

Se identitifican los siguientes archivos como relevantes, que tras una inspección se comprueba que son correspondientes a las aplicaciones `chrome`, `snapchat` y `musically`.

- `100100-07-2/mnt/p31/data/com.android.chrome/cache/Cache/eb0c8a5b990aece7_0`
- `100100-07-2/mnt/p31/data/com.zhiliaoapp.musically/cache/HttpCache/8856da4d81cf87667e0d8eea6b4d6ad8.1`
- `/similar_queries.json (inside 100100-07-2/mnt/p31/app/com.snapchat.android-1/base.apk)`

Si bien por si mismos son difíciles de interpretar, permiten situar el foco de la búsqueda en esas aplicaciones, que se analizan en los secciones *Snapchat* (apartado 3.2.2, pág. 49), *Historial de navegación* (apartado 3.2.1, pág. 47) y *Musically* (apartado 3.2.3, pág. 50) de este informe.

Otra palabra clave que da resultados interesantes en este dispositivo es `delivery`, que señala a las siguientes bases de datos, todas ellas encargadas de almacenar los mensajes *sms* del dispositivo.

- `/data/com.android.providers.telephony/databases/mmssms.db`

- data/com.google.android.talk/databases/babel0.db
- data/com.google.android.gms/databases/icing_mmssms.db

Estos archivos se analizarán en la sección *Mensajes SMS* (apartado 3.2.5, pág. 53).

Resultados

Mediante búsqueda de palarbras clave, se han identificado archivos que contienen las palabras “owl” y “delivery” relacionados con SnapChat, Chrome, Musically y SMS.

3.2. Análisis de actividad de usuario

3.2.1. Historial de navegación

Parseando los navegadores mediante:

```
$ rvt2 --source 100100-07-2 -j browsers
```

Se pueden observar visitas a webs de supuesta venta de aves.

```
$ grep -iP owl output/browsers/history.csv
...
"last_visit";"url";"title";"visit_count";"visit_type";"
    type_description";"visit_duration";"visit_date";"
    modified";"last_checked";"redirect_urls";"browser";"
    partition";"user"
"2017-01-25 02:10:46";"http://internationalowlcenter.org/
    owls-humans/owlsaspets";"Owls as Pets";1;0;"User clicked
     a link";7760769;"2017-01-25 02:10:46";"";"";"";"chrome
    ";"p31"
;""
"2017-01-25 02:10:56";"https://www.reference.com/pets-
    animals/can-buy-owl-570e816192eb539b";"Where can I buy
    an owl? / Reference.com";1;0;"User clicked a link
    ";0;"2017-01-25 0
2:10:56";"";"";"";"chrome";"p31";""
"2017-01-25 02:20:22";"https://www.quora.com/Where-can-you-
    find-baby-owls-for-sale-Are-owls-legal-to-keep-as-pets
    ";"Where can you find baby owls for sale? Are owls legal
     to ke
ep as pets? - Quora";2;0;"User clicked a link
    ";0;"2017-01-25 02:20:20";"";"";"";"chrome";"p31";""
"2017-01-25 02:22:44";"http://m.birdtrader.co.uk/owls/tawny
    -owls-for-sale/557493";"tawny owls for sale for sale in
```

```
    Londonderry, Northern Ireland / Birdtrader";1;0;"User
    clicke
d a link";0;"2017-01-25 02:22:44";"";"";"";"chrome";"p31
    ";""
"2017-01-25 02:22:57";"http://m.birdtrader.co.uk/owls/
    bonding-pair-asian-wood-owls/558006";"BONDING PAIR ASIAN
     WOOD OWLS for sale in Northamptonshire, East Midlands /
     Birdtrad
er";1;0;"User clicked a link";0;"2017-01-25
    02:22:57";"";"";"";"chrome";"p31";""
"2017-01-25 02:23:10";"http://m.birdtrader.co.uk/birds-of-
    prey-for-sale?sstr=Baby+owl&type_id=5&ads_cid=43&
    ads_place_name=&ads_place_lat=0&ads_place_long=0&
    ads_dist=5";"Owls f
or Sale / Birdtrader / Birdtrader";1;7;"A form the user has
     submitted values to";0;"2017-01-25 02:23:10";"";"";"";"
    chrome";"p31";""
"2017-01-25 02:23:27";"http://m.birdtrader.co.uk/owls/barn-
    owls-for-sale/557933";"Barn Owls for sale for sale in
    Lincolnshire, East Midlands / Birdtrader";1;0;"User
    clicked a
link";0;"2017-01-25 02:23:27";"";"";"";"chrome";"p31";""
"2017-01-25 02:25:20";"http://m.birdtrader.co.uk/birds-of-
    prey-for-sale/owls?sstr=Baby%20owl&ads_dist=5";"Owls for
     Sale / Birdtrader / Birdtrader";2;7;"A form the user
    has sub
mitted values to";0;"2017-01-25 02:25:20";"";"";"";"chrome
    ";"p31";""
"2017-01-25 02:26:34";"http://exoticanimalsforsale.net/
    search.asp?q=Owl";"Search Exotic Animals";1;7;"A form
    the user has submitted values to";41145335;"2017-01-25
    02:26:34";"
";"";"";"chrome";"p31";""
"2017-01-30 22:06:18";"https://www.amazon.com/gp/aw/s/ref=
    is_s_ss_i_0_5/166-5905978-4816857?k=bird+feeder&sprefix=
    bird+";"Amazon.com: bird feeder";3;0;"User clicked a
    link";0;
"2017-01-30 22:06:18";"";"";"";"chrome";"p31";""
"2017-01-30 22:06:46";"https://www.amazon.com/gp/aw/s/ref=
    is_s_ss_i_0_9/166-5905978-4816857?k=bird+bedding&sprefix
    =bird+bedd";"Amazon.com: bird bedding";9;0;"User clicked
     a link";0;"2017-01-30 22:06:31";"";"";"";"chrome";"p31
    ";""
"2017-01-30 22:10:25";"http://images5.fanpop.com/image/
    photos/31400000/Owl-owls-31450189-1600-1200.jpg";"Owl-
    owls-31450189-1600-1200.jpg (1600×1200)";1;0;"User
    clicked a link";0;"2017-01-30 22:10:25";"";"";"";"chrome
    ";"p31";""
"2017-02-03 17:20:32";"https://www.google.com/search?q=
```

```
    snowy+owl&oq=snowy&aqs=chrome.1.69i57j0l2j5.5212j0j4&
    client=ms-android-google&sourceid=chrome-mobile&espv=1&
    ie=UTF-8#img
rc=973zsz59Q3Z4BM:";"";1;0;"User clicked a link
    ";0;"2017-02-03 17:20:32";"";"";"";"chrome";"p31";""
```

Se identifican también descargas relevantes:

```
$ grep -i owl output/browsers/downloads.csv
...
"url";"path";"size";"end";"start";"modified";"date_added"
"https://www.google.com/";"/storage/emulated/0/Download/220
    px-Snowy_Owl_-_Schnee-Eule.jpg";22062;"2017-02-03
    17:20:30";"2017-02-03 17:20:30"
"https://www.google.com/";"/storage/emulated/0/Download/220
    px-Snowy_Owl_Barrow_Alaska.jpg";15191;"2017-02-03
    17:20:44";"2017-02-03 17:20:44"
```

Resultados

En este dispositivo se confirma el interés en la compra de búhos por parte del investigado ya que el día 25 de enero de 2017 visitó páginas con URLs o título como, entre otras:

- birdtrader.co.uk
- “Where can I buy an owl?”
- “Barn Owls for sale for sale in Lincolnshire”
- “Where can you find baby owls for sale?”

Además, el 30 de enero de 2017 visitó páginas sobre cómo mantener a un búho.

Aviso

En una investigación real, en este punto procede asegurar inmediatamente el contenido de estas páginas web. El RVT2 no va a ayudar en este sentido, y deben utilizarse o bien fedatarios públicos, o bien servicios como eGarante.

3.2.2. Snapchat

Una revisión del archivo coincidente, revela que se trata de un documento *.json* encargado de agilizar el proceso de búsquedas en la aplicación. Dado que este archivo almacena gran cantidad de palabras comunes y fuera de contexto, encontrar en él palabras clave no supone ningún indicio en la investigación.

Adicionalmente, las bases de datos asociadas a la aplicación se encuentran vacías de contenido, indicando que no se ha dado uso a la aplicación.

Es necesario explorar otras vías, pues la aplicación `snapchat` resulta ser una vía muerta en el caso.

3.2.3. Musically

Si bien no existe un módulo predefinido para esta aplicación concreta en RVT2, en una exploración de la estructura de carpetas de `musically` (`mnt/p31/data/com.zhiliaoapp.musically/`) destacan las bases de datos `databases/musically.db` y `databases/127174731128320_facebook_emmsg.db`.

Una query simple tal como `select datetime(msgtime/1000,'unixepoch'), msgbody from chat` en la base de datos `127174731128320_facebook_emmsg.db` permite observar una conversación llevada a cabo entre los usuarios con *nickname* **sarahmcavoy** y **layster82**:

> **Info**
>
> El resultado de la query ha sido posteriormente tratado para poder mostrar un mejor resultado

```
date;from;to;message
"2017-01-30 22:55:18";127174731128320_facebook";"
    n_190723800861179904"","Hi Layla I accidentally deleted
    the string of emails we sent so I lost your contact. do
    you. are to send me your email again sorry for the
    inconvenience. also if it's easier you can send me
    information through here as well""
"2017-01-30 22:56:28";n_190723800861179904
    ";"127174731128320_facebook"",""The email is
    Layster82gmail"
"2017-01-30 22:56:56";n_190723800861179904
    ";"127174731128320_facebook"","/storage/emulated/0/
    Android/data/com.zhiliaoapp.musically/musically#
    musically/127174731128320_facebook/image/66560c50-e73f
    -11e6-be73-fff3b1707aec"
"2017-01-30 22:57:25";n_190723800861179904
    ";"127174731128320_facebook"",""How do you like him"
"2017-01-30 22:59:01";127174731128320_facebook";"
    n_190723800861179904"","is that an image of the exact
    one you have or is it a photo of what it will look like
    ?"
```

```
"2017-01-30 23:03:24";n_190723800861179904
    ";"127174731128320_facebook"","Exact one"
"2017-01-30 23:03:49";127174731128320_facebook";"
    n_190723800861179904"","OK what is the age and gender of
     it "
"2017-01-30 23:07:24";n_190723800861179904
    ";"127174731128320_facebook"","1.5 year old female"
"2017-01-30 23:08:32";127174731128320_facebook";"
    n_190723800861179904"","OK she's very pretty could you
    possibly do 4500 "
"2017-01-30 23:09:35";n_190723800861179904
    ";"127174731128320_facebook"","She's pretty and 5000
    take it or leave it"
"2017-01-30 23:10:16";127174731128320_facebook";"
    n_190723800861179904"","OK could you meet me at Harris
    river front park?"
"2017-01-30 23:11:27";n_190723800861179904
    ";"127174731128320_facebook"","Yes that's fine"
```

Esta ilustrativa conversación representa la evidencia de la negociación para la compra de un búho, uno de los objetivos principales de la investigación.

En el directorio de imágenes de la aplicación se encuentra una única imagen: `100100-07-2/mnt/p31/media/0/Android/data/com.zhiliaoapp.musically/musically#musically/127174731128320_facebook/image/th66560c50-e73f-11e6-be73-fff3b1707aec` con fecha de creación idéntica a la registrada en la conversación. Se trata del búho presuntamente implicado en la transacción.

Figura 3.2: Imagen enviada desde layster82 *a* sarahmcavoy *a través de la aplicación* musically

Resultados

El día **30 de enero de 2017** se pacta la compra de un búho por parte de **sarahmcavoy**, usuaria principal de la aplicación `musically` en el dispositivo Android analizada y coincidente en nombre con le usuario del PC Windows. El animal pertene al usuario **layster82**, de nombre Layla, identificador de aplicación *n_190723800861179904* y email **Layster82gmail**. El precio de compra se acuerda en un valor de **5000** y se fija una reunión presencial en la localización **Harris river front park**.

3.2.4. Información de contactos

A la vista de la información obtenida en el apartado anterior, se ha obtenido una nueva palabra clave: *Layster82*. Así pues, aplicando en filtro *Layster82* en *ElasticSearch* da como único resultado ajeno a la aplicación *musical.ly* el archivo `/data/com.google.android.gms/databases/pluscontacts.db`.

Este archivo se incluye entre las bases de datos habituales de Android que parsea RVT2, y guarda información en relación a los contactos del propietario del dispositivo.

```
$ rvt2 --source 100100-07-2 -j android.databases
```

La salida de este comando puede observase en `output/android/*`,

Una búsqueda en los resultados del parseo de las bases de datos de contactos revela el contacto *Layster82@gmail.com*:

```
$ grep Layster82 output/android/contacts*.csv
```

```
"contact_id";"display_name";"value";"last_updated"
"1f3503d78d1f621b";"Layla Aster";"Layster82@gmail.com
    ";"2017-01-27 17:26:54"
```

Resultados

Se identifica el email *Layster82@gmail.com* entre los contactos del dispositivo del investigado, y puede asociarse al nombre **Layla Aster**, uno de los autores del intercambio. Este contacto se actualizó el día **27 de enero de 2017**.

3.2.5. Mensajes SMS

La base de datos `/data/com.android.providers.telephony/databases/mmssms.db`, que da coincidencia con la palabra clave *delivery*, ha sido tambien parseada por RVT2 con el job “android.databases”, ejecutado en la sección anterior.

Filtrando los mensajes *sms* se encuentra un mensaje de contenido sospechoso:

```
$ grep -B 5 -A 5 -i "delivery" output/android/sms.csv
```

```
"date";"address";"person";"read";"seen";"message";"
    service_center"
"2017-01-30 23:01:48";"32665103";"";0;1;"Monica Neff
    commented on your post.
https://fb.com/l/2dDxjpfetYcMa72
Can't wait to hear about it!!!!!!!!

Reply with your comment or ""like"".";"+12404492167"
"2017-02-01 00:41:15";"+13045184333";"";1;1;"Sarah, the
    delivery is today 7 tonight the confirmation will come
    later through pidgin";"+12404492167"
"2017-02-01 00:41:45";"+13045184333";"";1;0;"Thank you!";""
```

Dado que la fecha del mensaje (2017-02-01 00:41:15 UTC) se sitúa apenas 1 hora y media después del último mensaje de la conversación por `musical.ly` (2017-01-30 23:11:27 UTC), resulta razonable asociar la entrega mencionada por *sms* con la acordada previamente relativa a la compra de búhos.

Resultados

Se identifica la recepción de un mensaje *sms* procedente del número de teléfono **+13045184333** en el que se especifica la hora de la entrega a las **7 PM del día 1 de febrero de 2017**.

Si bien no se ha encontrado otra referencia a dicho número de teléfono en ninguno de los dos dispositivos del sospechoso, puede, por contexto, asociarse ese número de teléfono a la persona que realiza la venta, Layla Aster.

Dada la referencia textual a la aplicación **pidgin** en el mensaje, se ha procedido a intentar recuperar los mensajes de esta aplicación en ambos dispositivos.

3.2.6. Aplicaciones instaladas

En la carpeta de salida de RVT `output/android` se encuentra el archivo `applications_state.csv` del que relata las fechas de instalación

y *update* de las aplicaciones del dispositivo. Las primeras (más recientes) entradas de este archivo muestran las aplicaciones descargadas:

```
cut -d';' -f1,2,3,4 output/android/applications_state.csv
| head -10
```

```
"package_name";"title";"version";"first_downloaded"
"com.cmcm.locker";"CM Locker-AppLock,ScreenLock
    ";45043237;"2017-01-30 22:16:09"
"com.cleanmaster.security";"CM Security AppLock AntiVirus
    ";30245023;"2017-01-30 22:14:26"
"com.zhiliaoapp.musically";"musical.ly
    ";2017020301;"2017-01-30 21:59:54"
"com.google.android.play.games";"Google Play Games
    ";39080038;"2017-01-25 20:50:21"
"com.skype.raider";"Skype - free IM & video calls
    ";119604041;"2017-01-25 02:18:55"
"com.enflick.android.TextNow";"TextNow - free text + calls
    ";11192;"2017-01-24 15:51:40"
"com.twitter.android";"Twitter";6110047;"2017-01-24
    15:51:01"
"com.snapchat.android";"Snapchat";1025;"2017-01-24
    15:49:52"
"com.facebook.katana";"Facebook";48723175;"2017-01-24
    15:47:53"
"com.google.android.gms";"Google Play
```

Si bien se observan diversas aplicaciones dedicadas a la comunicación, dado que no han dado resultados positivos en la búsqueda de palabras clave, no se realizará el parseo de sus datos.

Info

Destaca la descarga de aplicaciones de antivirus y protección de pantalla, manifestando una preocupación del usuario por la seguridad y privacidad en el uso del terminal. Su utilización tardía (son las últimas aplicaciones descargadas), podría sugerir un interés o necesidad nacido de las actividades que son objeto de la investigación.

No se observa rastro de la instalación de la aplicación *pidgin* en este dispositivo. Esto puede ser consultado también en otras bases de datos que no se incluyen en este *write up*.

Por ello, y como ejemplo de que la evolución de los casos forenses obliga a revisar fuentes anteriormente analizadas con otra perspectiva, se ha buscado *pidgin* en la fuente `100100-07-1` del caso. La aplicación de escritorio en el PC guarda sus archivos en la ubicación `Users/Sarah M/AppData/Roaming/.purple`. No obstante, no hay rastro de la carpeta `logs` en la que deberían guardarse los mensajes.

Info

Aunque un análisis de memoria podría permitir recuperar tal información, en estos momentos RVT no dispone de plugins específicos para esta tarea.

3.2.7. Mapas

La aplicación *Google Maps* (`com.google.android.apps.maps`) guarda información de las localizaciones buscadas o guardadas, así como las rutas solicitadas. Aunque el formato en el que estan implementadas las bases de datos no es sencillo de parsear y no está incorporado en estos momentos a RVT2, sí se puede hacer una exploración de *strings* del archivo `data/com.google.android.apps.maps/databases/gmm_storage.db-journal`.

```
$ srch_strings mnt/p31/data/com.google.android.apps.maps/databases/gmm_storage.db-journal | less
```

Buscando la referencia de localización *Harris river front park* citada en los mensajes de `musical.ly`, se destaca lo siguiente:

```
http://maps.google.com/?q=Harris+Riverfront+Park+loc:+
    Veterans+Memorial+Blvd,+Huntington,+WV+25701&gl=US&sll
    =38.423656,-82.442845:
```

```
Harris Riverfront Park is a great asset to the city of
    Huntington, however, it's hidden behind the flood-wall
    so it is easily overlooked.
There is a nice, small, playground plus a pleasant walking
    path with interesting placards posted that can teach you
     about local flora and fauna.  There is also a new,
    small, skate park that has long been needed within
    Huntington.
The city is currently working on a public-private
    partnership for redevelopment around the park which
    should make it an even better place to hangout and enjoy
     the Ohio river.
Finally, the park is host to a variety of cool events
    throughout the year including the areas premiere beer
    tasting festival - Rails and Ales.
```

Las coordenadas mencionadas se corresponden efectivamente con el parque **Harris Riverfront Park** en **Huntington**

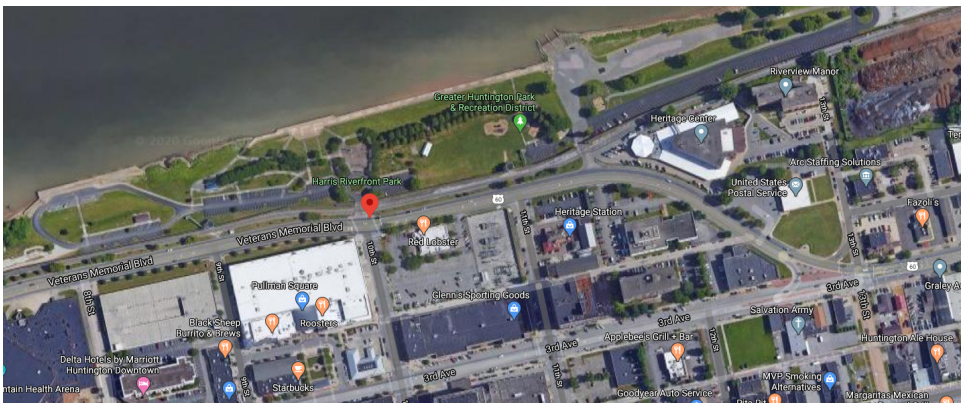

Figura 3.3: Reconstrucción del lugar mencionado en los mensajes

Se incluyen también indicaciones diversas sobre cómo llegar al destino.

```
"You should arrive around 12:27 PM.
```

Resultados

Existen indicios de que la persona investigada realizó un trayecto hasta el parque **Harris Riverfront Park** en **Huntington**, lugar de la supuesta transacción.

Capítulo 4

Documentación

Una vez obtenidos todos los indicios, se da por acabada la etapa de investigación y comienza la documentación, o preparación del informe. El RVT2 no puede ayudar durante esta fase.

El objetivo de la fase de documentación es:

- Ordenar todos los indicios recogidos durante la investigación.
- Preparar un documento en el que aparezcan los resultados que ayuden a conseguir los objetivos marcados para la investigación.

Documentar el proceso de una investigación necesita de sus propias habilidades y experiencia. No es necesario incluir todos los resultados obtenidos, ni el detalle de cómo se obtuvieron. Sí deben mencionarse en suficiente detalle como para que otra persona pueda replicar y validar la investigación y llegar a las mismas conclusiones. En particular, la parte contraria es posible que tenga su propia explicación para todos los indicios identificados.

En este informe se ha documentado a la vez que hacía la investigación. Aunque este documento no es un informe pericial, sí que permite tomar decisiones ejecutivas y planificar los siguientes pasos para realizar. En nuestro caso, acusar formalmente a la persona investigada de haber comprado un búho a Layla Aster a las 7:00 PM del día 1 de febrero de 2017 en el parque Harris Riverfront Park en Huntington.

Capítulo 5

Conclusiones

- Se han identificado numerosos documentos relacionados con búhos en los dispositivos analizados.
- Tanto en el ordenador analizado como en el teléfono móvil se han encontrado rastros de búsquedas en Internet relacionadas con la compra de búhos.
- Se conectó al ordenador un dispositivo *USB* que ha contenido archivos relacionados con búhos, accedidos desde el ordenador del investigado.
- En el ordenador se han encontrado rastros de correos electrónicos relacionados con la compra de búhos.
- El día **30 de enero de 2017** se pacta la compra de un búho por parte de **sarahmcavoy**, usuaria principal de la aplicación `musically` en el dispositivo Android analizado y coincidente en nombre con el usuario del PC Windows. El animal pertenece al usuario **layster82**, de nombre Layla y email **Layster82gmail**.
- El precio de compra se acuerda en un valor de **5000** y se fija una reunión presencial en la localización **Harris river front park**.
- El punto de encuentro mencionado en la conversación de compra-venta, ubicado en **Huntington**, fue buscado en la aplicación *Google Maps*, así como las indicaciones sobre cómo llegar hasta allí.
- Se identifica la recepción de un mensaje *sms* procedente del número de teléfono **+13045184333** en el que se especifica la hora de la entrega a las **7 PM**.
- Se identifica el email *Layster82@gmail.com* entre los contactos del dispositivo del investigado, y puede asociarse al nombre **Layla Aster**.