

Informática Forense y Auditoría

Grado en Ingeniería Informática del Software

Escuela de Ingeniería Informática de Oviedo

Práctica 5a: Ejercicios de Práctica Forense IV

Introducción

Esta práctica tiene tres vertientes:

- Por un lado, se pone el foco en las herramientas forenses incorporadas a CAINE 11 que le permitirán realizar una forensia en vivo de una máquina Windows. También aprenderá a realizar un volcado de memoria RAM así como examinar dicho volcado buscando trazas de malware.
- Aplicar técnicas y herramientas que permiten la obtención de información de fuentes abiertas (OSINT), enfocadas a la realización de investigaciones forenses.
- Introducción a la forensia de redes locales y análisis de trazas en telefonía móvil.

Objetivos

- Utilizar los comandos incorporados a Windows que le permiten obtener información forense, así como explorar las utilidades forenses incorporadas al CD de CAINE 11 que le permitirán realizar la adquisición de evidencias forenses en vivo.
- Realizar un volcado de memoria con FTKImagerLite así como examinar dicho volcado con Volatility.
- Utilizar herramientas de investigación en OSINT.
- Análisis de cabeceras de email.
- Introducción a la forensia de redes con Wireshark y análisis de movilidad en redes de telefonía móvil.

Instrucciones comunes a todos los ejercicios

- **Realice los ejercicios 1 a 28 (inclusive) en la máquina anfitrión.**
- **Los ejercicios de aplicación de técnicas OSINT podrá realizarlos, en algunos casos, bien en la máquina anfitrión o bien en las máquinas virtuales que preparó en la primera práctica del curso.**

- Deberá justificar la realización de los siguientes ejercicios con capturas de pantalla donde quede patente la autoría de los mismos, así como los comandos empleados en su resolución y aquellas explicaciones que considere oportunas.

Aplicación de técnicas de forensia en vivo a una máquina Windows

1. Descargue del campus virtual la imagen ISO del CD de CAINE 11 (**Recursos Prácticas - Práctica 5**). Monte en su máquina física la imagen ISO de dicho CD/DVD. Localice en el CD/DVD de CAINE la aplicación WinAudit. Ejecute dicha aplicación. Realice los siguientes pasos.
 - a) En el menú de herramientas seleccione Opciones y marque todas las categorías de inventario posible.
 - b) Inicie el proceso de recolección de evidencias.
 - c) Una vez finalizado, explore la información obtenida en cada categoría.
 - d) Explore las diferentes formas de guardar la información obtenida y exporte la misma en formato HTML al medio de recolección de evidencias de que disponga.
2. Registra la fecha y la hora del sistema. Comprueba si hay alguna variación con respecto a la hora oficial de España. Para realizar esto último, si tienes conexión a Internet, puedes utilizar la página web <https://time.is/es/Spain> donde puedes encontrar la hora actual de España y compararla con la hora de tu PC. Realiza una captura donde se observe la desviación existente entre dichas horas, si es que existe.
3. Averigüe las interfaces de red presentes en el sistema y la configuración de cada una de ellas. Almacene dicha información en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.
4. Antes de realizar el ejercicio, abre una ventana y conéctate desde ella a la página web del campus virtual de la asignatura y no cierre dicha ventana. Busca, entre las utilidades que proporciona Nirsoft, aquellas que te permiten obtener las conexiones de red existentes con los puertos de red abiertos y los ejecutables a la escucha en dichos puertos. Almacene dicha lista en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia. Compruebe que en dicho listado aparece el ejecutable del navegador en el que tiene abierta la conexión al campus virtual y realice una captura de pantalla donde se pueda apreciar el puerto local y el puerto remoto para dicha conexión, así como la dirección IP o el FQDN del destino. Realice de nuevo el ejercicio, pero esta vez utilizando el comando del sistema con las opciones adecuadas que permite averiguar dicha información.

5. Obtenga el contenido de la tabla de rutas del sistema intervenido. Almacene dicha información en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.
6. Busque la asociación existente entre MACs e IPS en la caché ARP del sistema para el interfaz de red activo en el sistema. Almacene dicha información en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.
7. Obtenga el estado de la caché DNS que permita averiguar los dominios recientes accedidos desde el equipo. Con la utilidad apropiada de Nirsoft, obtenga los registros A, CNAME, MX, NS, SOA, TEXT y PTR para el dominio **asturias.es**. Almacene la información recopilada en este ejercicio en ficheros en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.
8. Enumere los servicios activos en el sistema. Almacene dicha información en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.
9. Enumere la lista de procesos en ejecución en formato CSV. Almacene dicha información en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.
10. Realice un volcado de la memoria. Inténtelo a través de la aplicación FTKImagerLite. En caso de que no pueda debido a que necesite privilegios para ello, averigüe la ubicación más habitual del fichero de volcado de memoria en caso de querer producir un “crashdump” para luego poder localizarlo en la imagen de disco.
11. Suponga que se ha encontrado abierto el navegador. Si queremos estudiar las contraseñas que ha usado el usuario que estaba utilizándolo para navegar, puede ser una buena idea realizar un volcado de la memoria del proceso y almacenarla en un fichero. Averigüe cómo puede realizar un archivo de volcado de la memoria del proceso y realice el volcado para todas las instancias del proceso correspondientes al navegador. Salve luego cada copia del volcado en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.

12. Obtenga la prueba de los usuarios que tienen cuenta en el equipo y el estado en el que se encuentran dichas cuentas para acceder al sistema. Almacene dicha información en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.
13. Obtenga la prueba de las carpetas compartidas por el sistema en el momento actual. Realice dicha operación utilizando tanto la información proporcionada por el propio Sistema Operativo como utilizando alguna utilidad que proporcione Nirsoft. Almacene dicha información en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.
14. Con la utilidad apropiada de Nirsoft, explore el vecindario de su red descubriendo las máquinas presentes en la misma. Exporte dicha lista en formato csv y almacénela en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.
15. En caso de realizar la investigación en un equipo que tenga tarjeta de red inalámbrica, busque y ejecute la/s utilidad/es de Nirsoft que le permitan escanear la red inalámbrica y obtener la lista de redes y dispositivos actualmente conectados a la misma. Almacene dicha información en ficheros en formato csv en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia. En el caso de que no pueda realizar el ejercicio por no disponer el equipo de tarjeta de red inalámbrica, localice simplemente la utilidad de Nirsoft que le permitiría realizarlo.
16. En caso de realizar la investigación en un equipo que que tenga tarjeta de red inalámbrica, busque y ejecute la utilidad de Nirsoft que le permita obtener el historial de conexiones a redes inalámbricas de su equipo. Almacene dicha información en ficheros en formato csv en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia. En el caso de que no pueda realizar el ejercicio por no disponer el equipo de tarjeta de red inalámbrica, localice simplemente la utilidad de Nirsoft que le permitiría realizarlo.
17. Con cada conexión de un dispositivo USB al sistema se crea su correspondiente entrada en el registro donde se almacena información del mismo como el fabricante o su número identificativo único. Esta información se encuentra disponible en las siguientes claves de registro: **HKLM\System\CurrentControlSet\Enum\USBSTOR**,

HKLM\System\CurrentControlSet\Enum\USB y HKLM\System\MountedDevices.

Averigüe qué información registra cada una y salve la información de cada clave en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.

18. Busque y ejecute la utilidad de Nirsoft que le permita obtener la información sobre los dispositivos USBs que están conectados actualmente al sistema así como los que se han usado recientemente. Almacene dicha información en formato csv en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.
19. Busque y ejecute la utilidad de Nirsoft que le permita obtener la información sobre los períodos de tiempo en los que el sistema estuvo encendido. Almacene dicha información en formato csv en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.
20. Busque y ejecute la utilidad de Nirsoft que le permita obtener la información sobre los últimos inicios de sesión de usuario en el sistema y a través de dicha aplicación averigüe la hora en la que inició sesión en el sistema con la cuenta actual. Almacene dicha información en formato csv en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.
21. Busque y ejecute la utilidad de Nirsoft que le permita obtener la información sobre los ejecutables y enlaces abiertos frecuentemente por el usuario actual. Almacene dicha información en formato csv en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.
22. Busque y ejecute la utilidad de Nirsoft que le permita obtener la información sobre los ficheros abiertos recientemente por el usuario con el cual está logueado. Almacene dicha información en formato csv en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.
23. Busque y ejecute la utilidad del CD de CAINE que le permita recuperar ficheros de una unidad mediante técnicas de Carving. Previamente a la realización del ejercicio, en un lápiz de memoria de su propiedad, realice el borrado de diversos ficheros de tipo docx, xlsx, pdf y jpg en diferentes carpetas. Aplique la utilidad de recuperación de archivos (pista, el nombre de la utilidad parece que indica que solamente está

diseñada para recuperar fotografías) y compruebe y documente que los archivos por ud. borrados han sido recuperados.

24. Para realizar el siguiente ejercicio deberá disponer de un lápiz de memoria o tarjeta SD. Borre las particiones que se encuentren en dicho lápiz. Una vez hecho esto, busque y ejecute la utilidad de Photorec que le permita recuperar particiones que han sido borradas. Compruebe y documente que las particiones borradas han sido convenientemente recuperadas y que los archivos que contenían dichas particiones siguen existiendo.
25. Busque y ejecute la utilidad de Nirsoft que le permita obtener la información sobre el contenido de la caché del navegador Google Chrome. Almacene dicha información en formato csv en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.
26. Busque y ejecute la utilidad de Nirsoft que le permita obtener la información sobre el historial de páginas visitadas con el navegador Mozilla Firefox. Almacene dicha información en formato txt en un fichero en la carpeta del medio externo en la que recolecta las evidencias con un nombre identificable y con la fecha y la hora a la que fue obtenida dicha evidencia.

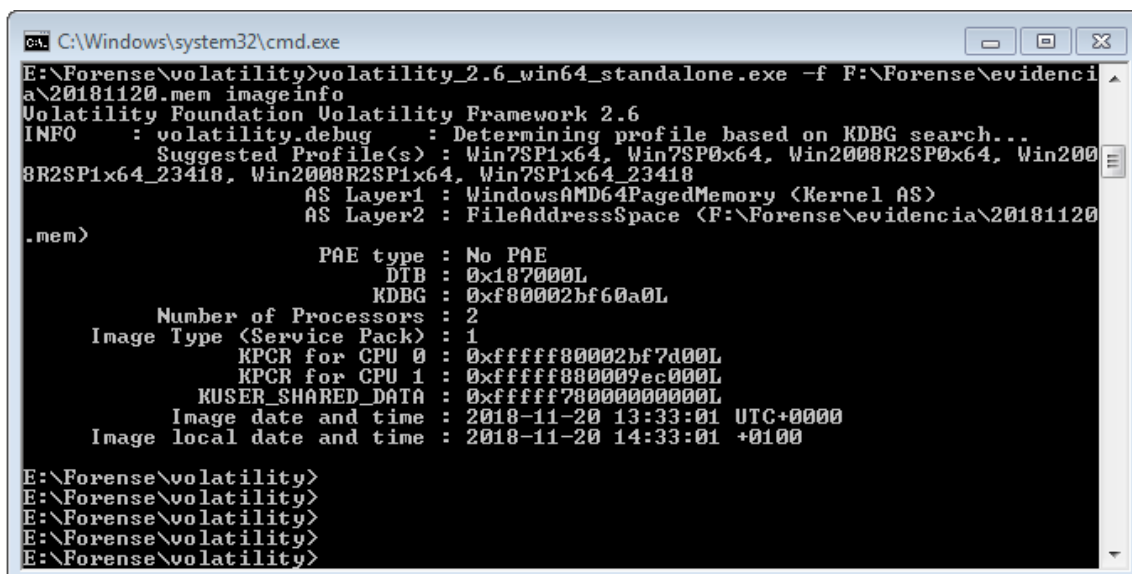
Análisis de un volcado de memoria RAM y búsqueda de trazas de malware con Volatility

27. Descargue de la página web de BelKasoft la herramienta forense Live Ram Capturer. Esta es una herramienta forense que le permitirá realizar una captura de la memoria RAM de su equipo. En la memoria RAM se pueden encontrar trazas de contraseñas, sitios web accedidos recientemente, así como información sobre los procesos que estaban corriendo en el momento de realizar la captura y trazas de malware, entre otros. Realice una captura de la memoria RAM de su máquina virtual en la que ha instalado Windows 7 y almacene dicha captura en un fichero denominado imagenRAMW7.dmp en el medio externo que utilice para la recolección de evidencias. Descargue la herramienta Volatility la cual encontrará en la siguiente URL (<https://www.volatilityfoundation.org/26>). Como puedes ver, puedes descargarla tanto para Windows (como ejecutable independiente), como para Linux. Descárgala para ejecutarla en el SO Windows 10 de los puestos base de las aulas. Una vez descargado, descomprímalo en una carpeta. Lance una ventana de comandos y navegue hasta la carpeta donde ha descomprimido la versión

standalone de Volatility. Desde esta ventana de comandos realizará las siguientes acciones:

Para poder utilizar adecuadamente Volatility sobre un fichero de imagen de captura de RAM, en primer lugar hay que averiguar el tipo de perfil del Sistema Operativo que debemos elegir posteriormente para investigar la información proporcionada por la imagen de memoria. Para ello ejecute el comando volatility de la siguiente manera:

```
$>volatility -f nombre_fichero_imagen imageinfo
```



```
C:\Windows\system32\cmd.exe
E:\Forense\volatility>volatility_2.6_win64_standalone.exe -f F:\Forense\evidencia\20181120.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory <Kernel AS>
AS Layer2 : FileAddressSpace <F:\Forense\evidencia\20181120.mem>

PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf80002bf60a0L
Number of Processors : 2
Image Type <Service Pack> : 1
KPCR for CPU 0 : 0xfffff80002bf7d00L
KPCR for CPU 1 : 0xfffff800009ec000L
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2018-11-20 13:33:01 UTC+0000
Image local date and time : 2018-11-20 14:33:01 +0100

E:\Forense\volatility>
E:\Forense\volatility>
E:\Forense\volatility>
E:\Forense\volatility>
E:\Forense\volatility>
```

La información proporcionada por este comando le indicará el tipo de perfil que tiene que seleccionar para examinar el fichero de volcado de memoria en función de la información extraída de los KDB (Kernell Debugging Blocks) localizados en dicha imagen.

Una vez localizado el perfil del Sistema Operativo del que se ha realizado la imagen de memoria, ejecute el siguiente comando para obtener información de los diferentes pluggins incorporados a la herramienta Volatility:

```
$>volatility -f nombre_fichero_imagen --profile=nombre_perfil_so -h
```

Una vez haya visto las capacidades que permite la herramienta a través de volatility, ejecute el comando pasándole el nombre del plugging que le permite obtener la lista de procesos que se encontraban en ejecución en el momento de realizar la captura de la RAM (incluso los procesos ya finalizados).

```
$>volatility -f nombre_fichero_imagen --profile=nombre_perfil_so psslist
```

Repita el comando anterior pero utilizando el plugin **psscan** y compare el número de procesos obtenidos con el proporcionado por el anterior plugging.

```
$>volatility -f nombre_fichero_imagen --profile=nombre_perfil_so psscan
```

Observe que uno de los procesos que más aparece en la lista obtenida es el correspondiente al **svchost.exe**. Compruebe que todas las instancias de este proceso tienen como proceso padre al **services.exe** ya que, en caso contrario, **eso sería un indicativo de posible malware**. Compruebe también que no hay instancias del proceso svchost.exe mal escritas o con letras cambiadas.

Ejecute el comando volatility una vez más con el plugging que le permite descubrir el árbol de procesos y compruebe que todos los procesos svchost.exe tienen como ancestro inmediato a services.exe

```
$>volatility -f nombre_fichero_imagen --profile=nombre_perfil_so pstree
```

Cuando los procesos svchost.exe no son descendientes del proceso services.exe, sino que lo son, por ejemplo, de explorer.exe, pueden ser sospechosos de malware. También puede resultar sospechoso encontrar varias instancias del proceso **lsass.exe** o bien que estas no sean hijas del proceso **winlogon.exe** (haz una comprobación de dichas instancias en la imagen de memoria que estas examinando). En esos casos se puede extraer la memoria del proceso particular para examinarla en busca de artefactos de malware e incluso someterla a servicios de inspección online como **VirusTotal** (<https://www.virustotal.com/gui/>). Vamos a simular que uno de los procesos svchost encontrados en su volcado de memoria es sospechoso de malware y queremos extraer la memoria de dicho proceso particular. Para ello, desde la línea de comando de volatility ejecute:

```
$>volatility -f nombre_fichero_imagen --profile=nombre_perfil_so procdump -p  
pid_proceso --dump-dir=ruta_carpeta_volcado
```

Una vez extraído el contenido de la memoria del proceso, podemos realizar entre otras cosas, búsqueda de cadenas (por ejemplo, con el comando **strings** de SysInternals) o bien aplicarle un antivirus.

Otra operación interesante que podemos realizar es, no sólo obtener el contenido de la memoria RAM asociada al proceso, sino cualquier contenido almacenado en disco vinculado a dicho proceso. Para ello, desde la línea de comando de volatility ejecute:

```
$>volatility -f nombre_fichero_imagen --profile=nombre_perfil_so memdump -p  
pid_proceso --dump-dir=ruta_carpeta_volcado
```

De la misma manera, con el fichero generado podremos hacer búsqueda de patrones o bien someterlo a una herramienta antivirus.

También podemos encontrar trazas de malware buscando drivers que están ocultos. Para ello ejecute volatility de la siguiente manera:

```
$>volatility -f nombre_fichero_imagen --profile=nombre_perfil_so modscan
```

Esto nos puede ayudar en la búsqueda de procesos que no tienen asociado un fichero en disco y que por tanto pueden suponer un caso de inyección de procesos, lo cual puede ser indicativo de malware.

Si queremos ver las conexiones de red establecidas, a la escucha o bien finalizadas en el momento de realizar el volcado de memoria, también lo podremos hacer con el plugin netscan.

```
$>volatility -f nombre_fichero_imagen --profile=nombre_perfil_so netscan
```

Volatility cuenta con una enorme cantidad de pluggins que nos permiten extraer información de la actividad del usuario (userassist, shellbags, etc.) así como crear líneas de tiempo (timeliner) de eventos ocurridos en el sistema, ...

28. Descargue del campus virtual (**Recursos Prácticas->Práctica 5**) el fichero denominado **windowsram.zip**. Se trata de una captura de la memoria RAM de una máquina Windows. Descomprima dicho archivo. Vamos a intentar buscar en la captura de memoria trazas de malware. Utilice la herramienta Volatility y realice los siguientes apartados sobre dicha imagen:
- a) ¿A qué perfil/es de sistema operativo corresponde dicha imagen de memoria RAM?
 - b) Obtenga la lista de procesos que se encontraban en ejecución cuando se obtuvo el volcado de memoria. ¿Son todos los procesos **svchost.exe** hijos del proceso **services.exe**?
 - c) Obtenga las conexiones establecidas entre la máquina y otros sistemas. Si no puede utilizar el comando **netscan** investigue en la ayuda de Volatility a qué es debido y elija de todos los comandos de networking, aquel que se aplique al perfil de sistema operativo investigado y que permita obtener tanta información de conexiones activas y conexiones finalizadas como sea posible.
 - d) Indique la/s direcciones IPs de la/s máquina/s remotas con las cuales existían conexiones abiertas.
 - e) ¿A qué puerto/s remoto/s se dirigían dicha/s conexión/es?
 - f) ¿Qué PID/s tenían el/los proceso/s que había establecido dichas conexiones?
 - g) ¿Corresponde/n dichos procesos a navegadores web?
 - h) Compruebe si la/s IP/s del apartado d) se encuentran en una blacklist. Utilice para ello la página <https://www.ipvoid.com/ip-blacklist-check/>.
 - i) Suponga que alguna de las IPs detectadas en el apartado d) se encuentra en una blacklist. Si el equipo está infectado por un Troyano, es normal que éste haya

añadido una clave al registro de Windows para asegurarse de que se ejecutará en cada reinicio del sistema. Busque información sobre el comando **printkey** y aplíquelo para buscar información sobre la clave del registro "**Microsoft\Windows NT\CurrentVersion\Winlogon**"

- j) Si ha realizado con éxito el apartado anterior, fíjese en el segundo valor de la subclave UserInit. Busque en internet información sobre ese ejecutable.
- k) Haga un volcado de los procesos que detectó en el apartado f) que no se correspondan con navegadores web. Utilice para ello el comando de volatility que permite extraer no solo el contenido de la memoria sino cualquier contenido en disco asociado a dicho proceso.
- l) Obtenga la firma hash de el/los fichero/s donde ha almacenado el volcado de/los proceso/s. Utilice para ello HashMyFiles que puede encontrar en la subcarpeta Nirsoft del CD de Caine.
- m) Compruebe en la página Web de VirusTotal (<https://www.virustotal.com/gui/home/search>) si se reconoce la firma hash del/los fichero/s volcados como software malicioso.
- n) Los mutex son variables de exclusión mútua que se utilizan para serializar el acceso a una sección crítica en programación concurrente. Hay software malicioso que crea mutex con nombre para asegurarse que una sola instancia del programa malicioso se está ejecutando en el sistema. Utilice el comando **mutant** de Volatility para obtener todos los objetos **KMUTANT** pertenecientes a mutex con nombre.
- o) Observe la lista de mutex con nombre que aparecen en la salida del comando de la opción anterior. Muestre solamente las líneas en las que aparece la palabra **AVIRA**.
- p) Busque en internet información sobre aquellas cadenas en las que figure AVIRA como subcadenas. ¿De qué tipo de software malicioso se trata?
- q) Compruebe si el FireWall está deshabilitado ya que o bien lo tenía deshabilitado el usuario o bien fue deshabilitado por un software malicioso. Para ello compruebe el valor de la clave de registro "**ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile**". ¿Estaba el FireWall de Windows deshabilitado?

Herramientas para investigación de fuentes abiertas (OSINT)

29. Crea un buscador personalizado de ejemplo para una serie de dominios de medios de prensa (ej.: el Comercio digital, el Mundo, el País, etc.) y añádelo a la lista de marcadores a través de su URL pública. Para realizar este ejercicio deberá disponer de una cuenta en Google.
30. Descargue del campus virtual (**Recursos Prácticas->Práctica 5**) el fichero denominado **imagenesP5.zip**. Descomprima dicho archivo. Para responder a las siguientes cuestiones utilice la técnica OSINT denominada búsqueda inversa de imágenes aplicándola al fichero **imagen8.jpg**, para lo cual podrá utilizar bien Google Images, el buscador Yandex o bien TinEye. Responda a las siguientes preguntas:
- ¿Dónde se encuentra el cartel de bienvenida que aparece en la imagen?
 - ¿En qué país se encuentra la ciudad?
 - ¿Cómo se llamaba originalmente la ciudad en la que se encuentra dicho cartel?
 - ¿Cómo se llama la Universidad que se encuentra en la ciudad donde se ubica dicho cartel?
31. En el mes de junio de 2018, Donald Trump adoptó una serie de medidas frente a los menores indocumentados que cruzan la frontera con sus padres. Utilizando la técnica de búsqueda inversa de imágenes a través de Google Images, Yandex o TinEye, determinar la **veracidad de la información** publicada por el perfil de **Twitter: @PabloPardo1**: <https://twitter.com/pablopardo1> , concretamente el **Tweet**: <https://twitter.com/PabloPardo1/status/1008923855954567170> Investigar la veracidad de la información asociada a la imagen que se encuentra asociada a dicho Tweet.
32. Existen otros buscadores especializados cuyo uso principal es la identificación de tecnologías vulnerables (servidores sin parche de seguridad, recursos no protegidos, etc.). Estos buscadores se basan en la captura de banners (datos que los servidores y dispositivos IoT) envían al cliente. Entre los más utilizados se encuentra Shodan (<https://www.shodan.io/>) el cual se puede utilizar tanto en investigaciones forenses como en auditorías informáticas en busca de vulnerabilidades. Este buscador permite utilizar diversos filtros en la cadena de búsqueda como los siguientes:
- Ciudad —> apache **city:Oviedo**
 - País —> apache **country:es**
 - Dominio —> **hostname:uniovi.es**
 - Red o rango —> **net: 156.35.160.135**
 - SO —> **os:windows**
 - Puerto —> **port:445**
 - Título —> **title:"SCADA"**

- OR —> |

En base a lo anterior, regístrate en la plataforma **Shodan** y realiza varias pruebas con los filtros anteriores. Una vez hayas entendido su funcionamiento, investiga el host **88.151.18.120** y responde a las siguientes cuestiones:

- ¿En qué país y ciudad se encuentra ubicado el equipo?
- ¿Qué puertos son accesibles desde el exterior?
- ¿A qué servicios está asociado cada uno de los puertos anteriores?
- ¿Qué versión de Servidor Web está corriendo en dicha máquina?
- ¿Cuándo fue la última vez que se actualizó la página web por defecto de dicho servidor?
- Indique cuántas y qué códigos de vulnerabilidad pueden afectar al sistema indicado.
- ¿A qué empresa/organización corresponde la IP?
- ¿Qué ASN tiene dicho ISP?
- ¿Cuántos sistemas están activos en la organización?
- ¿Cuántos sistemas de dicho ASN están ubicados en España?
- ¿Cuántos están en el extranjero?
- ¿Cuántos de esos sistemas están ejecutando un servidor OpenSSH?
- ¿Qué IP tiene el primer equipo que tiene instalado el servicio OpenSSH?
- ¿Qué versión de OpenSSH se está ejecutando en dicha máquina?
- ¿En qué puerto está corriendo dicho servicio?
- ¿Cuántas vulnerabilidades pueden afectar a dicho servicio?

33. En muchas investigaciones es necesario conocer información sobre la información de registro de un dominio o bien la geolocalización de una IP. Para ello disponemos de diversas herramientas entre las que se encuentran las siguientes:

- **DomainTools:** <https://whois.domaintools.com/>
- **MXToolBox:** <https://mxtoolbox.com/>
- **ViewDNS.info:** <https://viewdns.info/>
- **IP2Location:** <https://www.ip2location.com/>

Explore las herramientas anteriores y responda a las siguientes preguntas relacionadas con el dominio **uniovi.es**:

- ¿Qué dirección IP está asociada al dominio **uniovi.es**?
- ¿A qué país y ciudad corresponde dicha IP?
- ¿La máquina a la que corresponde la IP a la que se resuelve dicho dominio se corresponde con un servidor dedicado o está alojada en un servidor compartido?
- ¿Cuántas direcciones IP, incluida la actual, han estado vinculadas históricamente a este dominio?
- ¿Cuántos servidores de nombres son capaces de resolver el dominio?

- f) ¿Cuál o cuáles de ellos figuran como SOA para dicho dominio?
- g) ¿Cómo se llama la persona que figura como responsable de la administración del dominio? ¿Qué teléfono tiene? ¿Cuál es su dirección de email?
- h) ¿Tiene la universidad registrados bien directamente o bien a través de terceros otros dominios relacionados con uniovi? Indique sus nombres.

34. En este ejercicio vamos a tratar de obtener los metadatos de las fotografías existentes en los ficheros **imagenXX.jpg** resultado de descomprimir el fichero **imagenesP5.zip (Recursos Prácticas->Práctica 5)**. Para cada una de dichas imágenes trate de obtener la siguiente información:

- Fecha en la que fue tomada la imagen.
- Ubicación. En caso de que dicha información no esté presente en los metadatos, trate de averiguarla a través de la búsqueda inversa de imágenes.
- Marca de la cámara.
- Modelo de la cámara.
- Modelo del teléfono en caso de haberse realizado con un Smartphone.
- Año de lanzamiento del teléfono.
- Características de la imagen:
 - Dimensión (ancho x alto) de la imagen en pixels.
 - Resolución.
 - Bits de color por pixel.
- Tamaño del archivo.

Para obtener los metadatos EXIF de dichas imágenes puede utilizar bien la herramienta EXIFToolGUI o bien desde la página <http://metapicz.com/>.

35. En este ejercicio vamos a tratar de obtener los metadatos existentes en los ficheros resultado de descomprimir el archivo **ficherosP5.zip (Recursos Prácticas->Práctica 5)**. Para obtener dichos metadatos utilice la página información que le proporcionará la página Web <https://www.metadata2go.com/>. Para cada uno de los ficheros indicados, trate de obtener la siguiente información:

- Aplicación con la que se creó el archivo.
- Versión de la aplicación con la que se creó el fichero.
- Autor.
- Empresa/organización donde se crea el documento.
- Fecha/hora de creación.
- Fecha/hora modificación.
- Fecha/hora modificación metadatos.
- Número de páginas.
- Tamaño del archivo.

36. Utilice las opciones de búsqueda avanzada de X (antes Tweeter) para averiguar cuántos Tweets (retweets incluidos) se han publicado desde la cuenta oficial del Gobierno del Principado de Asturias que incluyan las palabras **altas temperaturas** entre el 1 de mayo y el 15 de agosto de 2022. Indique la fecha de publicación del tweet más antiguo que incluya dichas palabras y la fecha del más reciente.
37. Utilice las opciones de búsqueda avanzada de X (antes Tweeter) para averiguar cuántos Tweets (retweets excluidos) se han publicado desde la cuenta oficial de Ministerio de Transición Ecológica y Reto Demográfico del Gobierno de España que incluyan las palabras **“temperatura”** entre el 1 de mayo y el 28 de agosto de 2022. Indique, dentro de ese rango, la fecha de publicación del tweet más antiguo que incluya dichas palabras y la fecha del más reciente.
38. Utilice las opciones de búsqueda avanzada de X (antes Tweeter) para averiguar cuántos Tweets (**retweets excluidos**) se han publicado en **idioma inglés** desde la cuenta oficial de la Comisión Europea que incluyan las palabras **“fossil fuels”** entre el 1 de enero y el 28 de agosto de 2022. Indique, dentro de ese rango, la fecha de publicación del tweet más antiguo que incluya dichas palabras y la fecha del más reciente.
39. Utilice las opciones de búsqueda avanzada de X (antes Tweeter) para averiguar cuántos Tweets (**retweets excluidos**) se han publicado en **idioma español** desde la cuenta oficial de la AEMET de la Comunidad Valenciana que incluyan las palabras **“Nivel máx naranja”** entre el 26 de octubre y el 28 de octubre de 2024. Indique, dentro de ese rango, la fecha de publicación del tweet más antiguo que incluya dichas palabras y la fecha del más reciente.

Análisis de cabeceras de email

40. Analice las cabeceras de correo que se encuentran en el fichero **CabecerasMensajeSospechoso-1.txt** el cual puedes descargar desde **Recursos Prácticas->Práctica 5**. Para analizar las cabeceras puedes utilizar la página tanto la página web <https://mha.azurewebsites.net/> como <https://mxtoolbox.com/public/tools/emailheaders.aspx>. Averiguar las IPs (<https://centralops.net/co/>, <https://viewdns.info/>, <https://research.domaintools.com/>) de los servidores de correo que aparecen en las cabeceras por los cuales ha pasado el mensaje y comprueba si se trata de IPs de sitios calificados como maliciosos (<https://www.abuseipdb.com>). Para averiguar si la dirección del remitente del mensaje ha sido comprometida utilice el siguiente URL

<https://Haveibeenpwned.com>. En base a su investigación, responda a las siguientes preguntas:

- a) ¿Desde qué dirección IP se envió el mensaje?
- b) ¿Qué ISP gestiona el rango de IPs en el que está incluida dicha IP?
- c) ¿Quién aparentemente es el remitente del correo?
- d) ¿Puede haber sido comprometida la dirección de correo que figura como remitente del mensaje?
- e) Comprueba si existe la dirección de correo del remitente del mensaje. Utiliza para ello bien la página <https://tools.emailhippo.com/> o bien la página <https://verify-email.org/>.
- f) ¿A qué organización pertenece el dominio de la cuenta de correo?
- g) ¿Cuál es el primer MTA que recibe el mensaje?
- h) ¿Por cuántos servidores de correo intermedios (MTA) pasó el mensaje?
- i) ¿Cuál fue el último de los servidores de correo por el que pasó el mensaje?
- j) ¿Cuál fue la fecha/hora local del momento de envío del mensaje?
- k) ¿Cuánto tiempo tardó en entregarse el mensaje desde el origen hasta el servidor de correo de destino?
- l) En vista de los retardos en la transmisión del mensaje entre los diferentes MTAs por los que ha pasado, ¿se puede decir que ha sido manipulado?
- m) ¿El mensaje cumple con el mecanismo de autenticación DMARC?

41. Analice las cabeceras de correo que se encuentran en el fichero **CabecerasMensajeSospechoso-4.txt** el cual puedes descargar desde **Recursos Prácticas->Práctica 5**. Para analizar las cabeceras puedes utilizar la página tanto la página web <https://mha.azurewebsites.net/> como <https://mxtoolbox.com/public/tools/emailheaders.aspx>. Averiguar las IPs (<https://centralops.net/co/>, <https://viewdns.info/>, <https://research.domaintools.com/>) de los servidores de correo que aparecen en las cabeceras por los cuales ha pasado el mensaje y comprueba si se trata de IPs de sitios calificados como maliciosos (<https://www.abuseipdb.com>). Para averiguar si la dirección del remitente del mensaje ha sido comprometida utilice el siguiente URL <https://Haveibeenpwned.com>. En base a su investigación, responda a las siguientes preguntas:

- a) ¿Desde qué dirección IP se envió el mensaje?
- b) ¿Qué ISP gestiona el rango de IPs en el que está incluida dicha IP?
- c) ¿Quién aparentemente es el remitente del correo?
- d) ¿Puede haber sido comprometida la dirección de correo que figura como remitente del mensaje?
- e) Comprueba si existe la dirección de correo del remitente del mensaje.

- f) ¿A qué organización pertenece el dominio de la cuenta de correo?
- g) ¿Cuál es el primer MTA que recibe el mensaje?
- h) ¿Por cuántos servidores de correo **intermedios** (MTA) pasó el mensaje?
- i) ¿Cuál fue el último de los servidores de correo por el que pasó el mensaje?
- j) ¿Cuál fue la fecha/hora local del momento de envío del mensaje?
- k) ¿Cuánto tiempo tardó en entregarse el mensaje desde el origen hasta el servidor de correo de destino?
- l) En vista de los retardos en la transmisión del mensaje entre los diferentes MTAs por los que ha pasado, ¿se puede decir que ha sido manipulado?
- m) ¿El mensaje cumple con el mecanismo de autenticación DMARC?
- n) ¿Qué conclusión saca tras las pruebas anteriores respecto al correo cuyas cabeceras ha analizado?

42. Analice las cabeceras de correo que se encuentran en el fichero **CabecerasMensajeSospechoso-2.txt** el cual puedes descargar desde **Recursos Prácticas->Práctica 5**. Para analizar las cabeceras puedes utilizar la página tanto la página web <https://mha.azurewebsites.net/> como <https://mxtoolbox.com/public/tools/emailheaders.aspx>. Averiguar las IPs (<https://centralops.net/co/>, <https://viewdns.info/>, <https://research.domaintools.com/>) de los servidores de correo que aparecen en las cabeceras por los cuales ha pasado el mensaje y comprueba si se trata de IPs de sitios calificados como maliciosos (<https://www.abuseipdb.com>). Para averiguar si la dirección del remitente del mensaje ha sido comprometida utilice el siguiente URL <https://Haveibeenpwned.com>. En base a su investigación, responda a las siguientes preguntas:

- a) ¿Desde qué dirección IP se envió el mensaje?
- b) ¿Qué ISP gestiona el rango de IPs en el que está incluida dicha IP?
- c) Averigüe a qué IPs estuvo vinculado el dominio desde el que se envió originalmente el correo.
- d) ¿Cuántos dominios figuran vinculados a dicha IP en el momento actual? ¿Figura el dominio desde el cual se envió el correo entre ellos?
- e) ¿A qué organización está asociada la IP que hace de hosting del dominio investigado?
- f) ¿Dónde está radicada el ISP correspondiente a la red anterior?
- g) ¿Quién aparentemente es el remitente del correo?
- h) ¿Puede haber sido comprometida la dirección de correo que figura como remitente del mensaje?
- i) Comprueba si existe la dirección de correo del remitente del mensaje.

- j) ¿A qué organización pertenece el dominio de la cuenta de correo?
- k) ¿Cuál es el primer MTA que recibe el mensaje?
- l) ¿Por cuántos servidores de correo **intermedios** (MTA) pasó el mensaje?
- m) ¿Cuál fue el último de los servidores de correo por el que pasó el mensaje?
- n) ¿Cuál fue la fecha/hora local del momento de envío del mensaje?
- o) ¿Cuánto tiempo tardó en entregarse el mensaje desde el origen hasta el servidor de correo de destino?
- p) En vista de los retardos en la transmisión del mensaje entre los diferentes MTAs por los que ha pasado, ¿se puede decir que ha sido manipulado?
- q) ¿El mensaje cumple con el mecanismo de autenticación DMARC?
- r) ¿Qué conclusión saca tras las pruebas anteriores respecto al correo cuyas cabeceras has analizado?

43. Analice las cabeceras de correo que se encuentran en el fichero **CabecerasMensajeSospechoso-3.txt** el cual puedes descargar desde **Recursos Prácticas->Práctica 5**. Para analizar las cabeceras puedes utilizar la página tanto la página web <https://mha.azurewebsites.net/> como <https://mxtoolbox.com/public/tools/emailheaders.aspx>. Averiguar las IPs (<https://centralops.net/co/>, <https://viewdns.info/>, <https://research.domaintools.com/>) de los servidores de correo que aparecen en las cabeceras por los cuales ha pasado el mensaje y comprueba si se trata de IPs de sitios calificados como maliciosos (<https://www.abuseipdb.com>). Para averiguar si la dirección del remitente del mensaje ha sido comprometida utilice el siguiente URL <https://Haveibeenpwned.com>. En base a su investigación, responda a las siguientes preguntas:

- a) ¿Desde qué dirección IP se envió el mensaje?
- b) ¿Qué ISP gestiona el rango de IPs en el que está incluida dicha IP?
- c) Averigüe a qué IPs estuvo vinculado el dominio desde el que se envió originalmente el correo.
- d) ¿Cuántos dominios figuran vinculados a dicha IP en el momento actual?
- e) ¿Figura el dominio desde el cual se envió el correo entre ellos?
- f) ¿A qué organización está asociada la IP del dominio desde la cual se remite en primera instancia el correo investigado?
- g) ¿Dónde está radicada el ISP correspondiente a la red anterior?
- h) ¿Quién aparentemente es el remitente del correo?
- i) ¿Puede haber sido comprometida la dirección de correo que figura como remitente del mensaje?

- j) Comprueba si existe la dirección de correo del remitente del mensaje. Utiliza para ello bien la página <https://tools.emailhippo.com/> o bien la página <https://verify-email.org/>.
- k) ¿A qué organización pertenece el dominio de la cuenta de correo?
- l) ¿Cuál es el primer MTA que recibe el mensaje
- m) ¿Por cuántos servidores de correo **intermedios** (MTA) pasó el mensaje?
- n) ¿Cuál fue el último de los servidores de correo por el que pasó el mensaje?
- o) ¿Cuál fue la fecha/hora local del momento de envío del mensaje?
- p) ¿Cuánto tiempo tardó en entregarse el mensaje desde el origen hasta el servidor de correo de destino?
- q) En vista de los retardos en la transmisión del mensaje entre los diferentes MTAs por los que ha pasado, ¿se puede decir que ha sido manipulado?
- r) ¿El mensaje cumple con el mecanismo de autenticación DMARC?
- s) ¿Qué conclusión saca tras las pruebas anteriores respecto al correo cuyas cabeceras has analizado?

Introducción a la forensia de redes con Wireshark y análisis de movilidad en redes de telefonía móvil

44. En muchas investigaciones forenses o auditorías de seguridad es necesario capturar tráfico de red y almacenarlo en un archivo para averiguar posteriormente qué está pasando. Una buena herramienta para ello es el analizador de protocolos **Wireshark** (<https://www.wireshark.org/download.html>) el cual nos permite analizar el contenido de los paquetes que se transmiten por la red. Realiza a continuación las siguientes acciones que te permitirán manejar alguna de sus características y comprender el intercambio de información que se produce cuando se visita una página web.

- a) Descarga e instala en la máquina virtual **IFA-WIN-XX** la versión adecuada del programa Wireshark.
- b) Descarga desde **Recursos Prácticas->Práctica 5** el archivo denominado **capturaHTTP.pcap**.
- c) Abre el archivo anterior en Wireshark y verás en el primer panel 13 tramas que son las que se han tenido que intercambiar entre la máquina del navegador y la máquina del servidor web para que el navegador reciba el contenido de la página web.
- d) Utiliza un filtro para mostrar solo los paquetes pertenecientes al protocolo HTTP. Selecciona el primer paquete de la lista filtrada.
- e) En el panel intermedio, pulsa sobre la línea correspondiente al protocolo HTTP para seleccionar sus bytes y después pulsa sobre el símbolo + que hay a la izquierda de HyperText Transfer Protocol. Si vamos pulsando sobre cada una de las líneas que nos han aparecido, podemos ver en el panel inferior qué bytes son los que proporcionan esa información. Podemos comprobar cómo el navegador web envía bastante información adicional al servidor web además de la ruta del fichero a obtener.
- f) ¿Qué navegador se ha usado para realizar la petición?
- g) ¿Qué sistema operativo ejecutaba la máquina del navegador?
- h) ¿Cuál era el contenido de la página enviada por el servidor?
- i) Vamos a descender un poco en la pila de protocolos. Pulsa de nuevo sobre el primer paquete que nos muestra Wireshark (debería ser el paquete con la petición GET). Si en el panel intermedio hay algún campo expandido, pulsa en los botones - para compactarlos. En el segundo panel, pulsa en cualquier sitio de la línea que pone "Transmission Control Protocol". pulsa en el panel intermedio de Wireshark en el + que hay a la izquierda del campo "Transmission Control Protocol".
- j) ¿Cuál es el puerto de origen (en decimal) de la petición?
- k) ¿Cuál es el puerto de destino (en decimal) de la petición?

- l) De nuevo descenderemos en la pila de protocolos al nivel del protocolo IP. En el panel superior del analizador de protocolos selecciona el primer paquete. Pulsa el botón - de todos los campos en el panel intermedio.
 - m) Pulsa sobre las palabras "Internet Protocol" y pulsa sobre + en el panel intermedio para expandir los campos del protocolo IP.
 - n) ¿Cuál es la dirección IP de origen del paquete? ¿Cuál es la dirección IP de destino del paquete?
 - o) Descenderemos de nuevo un nivel más hasta la capa física. Selecciona la trama número 1. Oculta pulsando sobre - todos los campos que pudieran estar expandidos en el panel intermedio. En el panel intermedio, selecciona la segunda línea, la que comienza con la palabra Ethernet. Expande la información correspondiente al protocolo Ethernet pulsando en el símbolo + que hay a la izquierda de la palabra Ethernet.
 - p) Averigua cuáles son las MAC de las máquinas origen y destino de la trama.
 - q) ¿Quién es el fabricante de la tarjeta de red origen de la trama en función de su MAC?
45. Este ejercicio trata de la trazabilidad de un dispositivo móvil, en términos de su actividad y posicionamiento en determinadas fechas, lo cual puede resultar de gran utilidad en ciertas investigaciones, auditorías y actividades de soporte técnico. No obstante, la información disponible o accesible puede ser sólo parcial debido a las circunstancias de los datos en los repositorios del proveedor de servicio o a cuestiones legales que amparen su obtención. El fichero **p5_tr_cell.csv** incluye varias líneas con datos relativos a los registros posicionales y de comunicaciones de un dispositivo móvil. Es habitual que, a instancias judiciales, estos datos se soliciten a los proveedores de servicio para dar curso a las correspondientes diligencias (atestados, peritaciones de parte, etc.) o, directamente, se realicen intervenciones de la línea desde los medios con los que cuente una administración competente. Analizar el fichero indicado, importándolo con separación de punto y coma y convirtiendo a texto las columnas A, B, H e I. A continuación, responder a las siguientes preguntas:
- a) Identificación única internacional de la línea móvil (país y proveedor del servicio de origen y número de línea).
 - b) ¿Cuántos terminales móviles distintos aparecen registrados?
 - c) Identificación única internacional del terminal o terminales móviles utilizados (modelo, fabricante y si está incluido en la Blacklist de España).
 - d) Indicar el soporte, especificado por el fabricante, en términos de tecnologías de acceso móvil 2G, 3G, 4G y 5G, para el terminal o terminales móviles implicados.
 - e) Enumerar los países en los que se ha registrado la línea móvil junto con los proveedores de servicio implicados en cada uno de ellos.
 - f) Indicar si se ha producido roaming, nacional o internacional, y los países implicados.

- g) Indicar el recorrido posicional, en sentido temporal creciente e identificando con la máxima precisión posible dicha localización, que se ha registrado para la línea móvil entre el 23 de junio y el 29 de junio, ambos inclusive y correspondientes al año 2018.
- h) Indicar la última posición, en sentido temporal y con la máxima precisión posible, que se ha registrado, para la línea móvil.
- i) Indicar la tecnología de acceso móvil (2G, 3G, 4G o 5G) que se corresponde con la célula 7480787217862.
- j) Indicar la fecha y hora local del registro correspondiente al 2018-06-29 05:01:00 (GMT)

46. Con el mismo contexto de inicio que indica el ejercicio anterior analizar el fichero **p5_tr_cell_bis.xlsx** y responder a las siguientes preguntas.

- a) Identificación única internacional de la línea móvil (país y proveedor del servicio de origen y número de línea).
- b) Indicar si la línea móvil se encontró, en algún momento, en situación de roaming; en caso afirmativo, indicar también si fue nacional o internacional.
- c) Indicar, a la vista de los registros, si se trata de un servicio SIM o multi SIM. Razónese la respuesta.
- d) Indicar las ternas IMSI/IMEI/ICC que resultan distinguibles
- e) Indicar si en algún momento se utilizaron redes 4G
- f) Indicar, si en algún momento, se ha producido portabilidad de terminal en la línea móvil -cambio de terminal-
- g) Razonar la posible causa por la que los registros correspondientes a las filas 2 y 3 del fichero incluyen distintos datos de localización.
- h) Examinar las referencias de localización -todos los registros- correspondientes al área 361 y estimar su ubicación general y alcance. **Nota: un área, en el caso de España, suele corresponder habitualmente a parte de una ciudad si ésta supera los 100.000 habitantes. En otros casos, suele corresponder a parte de una provincia. En todo caso, es una aproximación pues dependerá de las estrategias de despliegue del proveedor de servicio al optimizar el plano de control del segmento de acceso de la red.**
- i) Indicar el desplazamiento geográfico, en términos provinciales y secuencia temporal creciente, que corresponde a todos los registros incluidos en el fichero para el IMEI 862551036005121.
- j) Expresar en GMT la referencia de fecha y hora que corresponden al registro de la fila 15 del fichero.
- k) Razonar por qué son posibles los registros, con diferente localización pero muy próximos en fecha y hora, para línea móvil investigada que se corresponden a las filas 11 y 14 del fichero.

47. Trazabilidad posicional y celular de un dispositivo móvil. Analiza el fichero **p5_tr_cell_3.xlsx** y responde a las siguientes preguntas:

- a) Identificación única internacional de la línea o líneas móviles que aparecen en los registros (país y proveedor del servicio de origen y número de línea).
- b) A la vista de los resultados obtenidos en el apartado anterior y las referencias temporales de los registros asociados, razonar la circunstancia que se ha producido con la línea o líneas móviles investigadas.
- c) Identificar el fabricante y el modelo de todos los terminales móviles que aparecen en los registros (indicar, en cada caso, si se trata de smartphone, feature phone u otro tipo de dispositivo).
- d) Indicar los distintos LACs que se registran en 3G.
- e) Considerar las referencias posicionales y temporales de la totalidad de los registros e indicar si se ha producido algún desplazamiento que comporte zonas de distinto huso horario, en caso afirmativo indicar los husos horarios en cuestión.
- f) Indicar, con una precisión al menos de localidad, el recorrido geográfico completo seguido en sentido temporal creciente durante el mes de septiembre de 2023.
- g) Conjeturar el motivo más probable por el que todos los registros de 2G y 4G se corresponden, respectivamente, a una única área de localización.
- h) Indicar cuantas células distintas de 2G aparecen en los registros.
- i) Indicar el trayecto seguido en sentido temporal creciente correspondiente al 27/08/2023, conjeturar las circunstancias de transporte que hicieron posible el trayecto.
- j) Expresar en UTC la referencia de hora y día correspondiente al registro en el que aparece la célula 230897160.