



GRADO EN INGENIERÍA INFORMÁTICA

DEPARTAMENTO DE INGENIERÍA INFORMÁTICA

SEGURIDAD EN LOS SISTEMAS INFORMÁTICOS

Práctica 3: Recolección de información en fuentes abiertas - Parte II

Autores:

Juan Boubeta Puig, Jesús
Lagares Galán y Pedro
José Navas Pérez

Fecha:

29 de octubre de 2024

Índice

1. Objetivo	3
2. Técnicas para el reconocimiento especializado	3
2.1. Registros DNS y resoluciones de dominio	3
2.1.1. DNSDumpster	3
2.1.2. Ejercicio 1	5
2.1.3. DNS Trails	5
2.1.4. Ejercicio 2	7
2.1.5. Whois Lookup	7
2.1.6. Ejercicio 3	7
2.2. Tecnologías web	8
2.2.1. Wappalyzer	8
2.2.2. Ejercicio 4	9
3. Búsqueda y reconocimiento a través de redes sociales	10
3.1. Namecheck	10
3.1.1. Ejercicio 5	11
3.2. Phonebook.cz	12
3.2.1. Ejercicio 6	13
4. Otras herramientas OSINT	13
4.1. Ejercicio 7	14

Índice de figuras

1.	Mapa de subdominios generado por DNSdumpster	4
2.	Colocamos nuestra búsqueda en el buscador de DNS Trails	5
3.	DNS actuales de uca.es	6
4.	Subdominios actuales de uca.es	6
5.	Buscamos el dominio del Diario de Cádiz en whoislookup	7
6.	Información provista del dominio diariodecadiz.es por Whois Lookup	8
7.	Hacemos clic en el botón que ha aparecido en Wappalyzer	9
8.	Tecnologías encontradas en la web del Ministerio de Sanidad	10
9.	Realizamos la búsqueda dentro de Namecheck	11
10.	Disponibilidad, proporcionada por Namecheck, sobre un nombre de usuario entre diferentes redes sociales	11
11.	Seleccionamos la opción <i>Email Addresses</i> en la herramienta Phone- book.cz	12
12.	Direcciones de correo asociadas al dominio de la UCA	13
13.	Observamos las páginas web que han citado a la dirección de correo electrónico del CEIMAR	14
14.	Encontramos más información sobre una de las páginas web que han citado la dirección del CEIMAR	14

1. Objetivo

Dentro de esta segunda parte de la práctica 3 se aprenderán técnicas para el reconocimiento especializado, como la utilización de los registros *Domain Name System* (DNS) o el uso de aplicaciones como Wappalyzer [2], técnicas para el reconocimiento de páginas web y técnicas para el reconocimiento a través de redes sociales.

Dichas técnicas se pondrán en práctica a través de pequeños ejercicios dentro de cada sección.

2. Técnicas para el reconocimiento especializado

En nuestro proceso de recolección de información podemos querer obtener información más especializada. Algunos ejemplos de este tipo de información son los registros DNS o la tecnología que utiliza una determinada web de la que estemos recolectando información. Para estos propósitos existen técnicas y herramientas especializadas como veremos a continuación.

2.1. Registros DNS y resoluciones de dominio

Las empresas utilizan normalmente subdominios propios para mantener diversas aplicaciones bajo un mismo dominio. Para poder acceder a estos normalmente se habilita un registro DNS que permite acceder a este subdominio mediante su resolución.

Si bien existen herramientas que prueban mediante fuerza bruta la existencia de subdominios, en este caso nos centraremos en buscadores diseñados para esta tarea.

2.1.1. DNSDumpster

El primero que trataremos será **DNSdumpster**, una interfaz web para la herramienta del mismo nombre que se encuentra alojada en <https://dnsdumpster.com/>

De las tres herramientas que vamos a tratar en esta práctica es probablemente la más sencilla de usar, pero a su vez la más limitada, aunque cuenta con una funcionalidad que no posee el resto y es la de generar un mapa visual de los subdominios hallados (véase Figura 1).

Para usarla bastará con acceder a la página y escribir un dominio en la barra de búsqueda, por ejemplo: `uca.es`



Figura 1: Mapa de subdominios generado por DNSdumpster

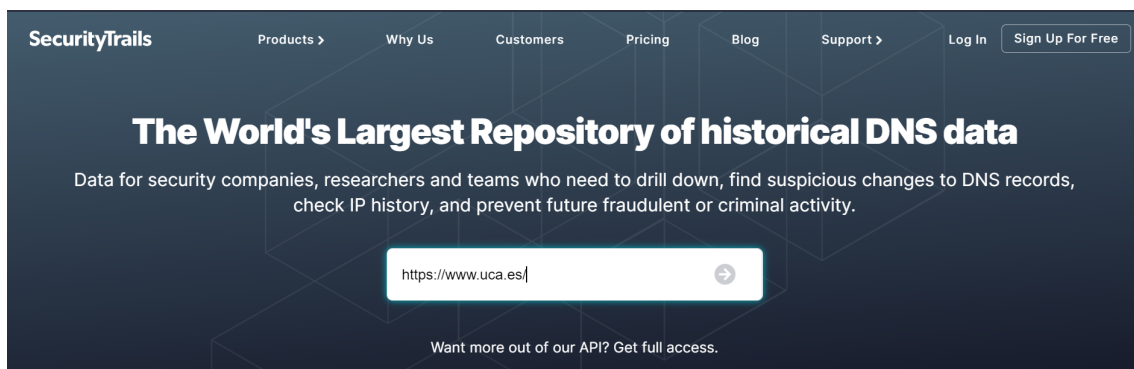


Figura 2: Colocamos nuestra búsqueda en el buscador de DNS Trails

2.1.2. Ejercicio 1

Usando DNSDumpster haga un análisis de los subdominios de *cadiz.es*

- (a) ¿Qué ISP aloja la mayoría de las webs?
- (b) ¿Qué gestor de contenidos utilizan varios de los subdominios?
- (c) ¿Qué sistema operativo es el más probable que use el servidor que aloja el subdominio *ftp.cadiz.es*? ¿Por qué?

2.1.3. DNS Trails

Otra opción a utilizar será **DNS Trails**. DNS Trails es el mayor repositorio mundial de información sobre DNS a nivel histórico. Es decir, gracias a esta herramienta no solo podremos obtener información sobre los registros DNS actuales de un dominio, sino que podremos acceder a los cambios de registros que ha tenido dicho dominio a lo largo de su historia. Mediante la capacidad de comprobar el histórico de direcciones IP y registros DNS, podremos prevenir o detectar actividad criminal.

Su funcionamiento comienza al acceder a su web oficial [5] e insertar un nombre de dominio, dirección IP o palabra clave en el buscador (véase Figura 2). Una vez introducido, la herramienta comenzará a trabajar y nos devolverá los registros DNS actuales (véase Figura 3). Si navegamos por el menú que aparecerá a nuestra izquierda podemos acceder a más información como el histórico de datos —aunque para ello tendremos que crearnos una cuenta— o los subdominios detectados, como podemos ver en Figura 4.

www.uca.es current DNS records

A records

Centro Informatico Cientifico de Andalucia - CICA
[150.214.80.210](#) 513

AAAA records

NO RECORDS

CNAME records pointed here 1

[celama.upo.es](#)
[View more www.uca.es CNAME records](#)

Figura 3: DNS actuales de uca.es

www.uca.es subdomains

1 - 4 of 4 results

Domain	Rank	Hosting Provider	Mail Provider
blog.www.uca.es		Centro Informatico Cientifico de Andalucia - CICA	-
shop.www.uca.es		Centro Informatico Cientifico de Andalucia - CICA	-
www.uca.es		Centro Informatico Cientifico de Andalucia - CICA	-
www.www.uca.es		Centro Informatico Cientifico de Andalucia - CICA	-




Figura 4: Subdominios actuales de uca.es

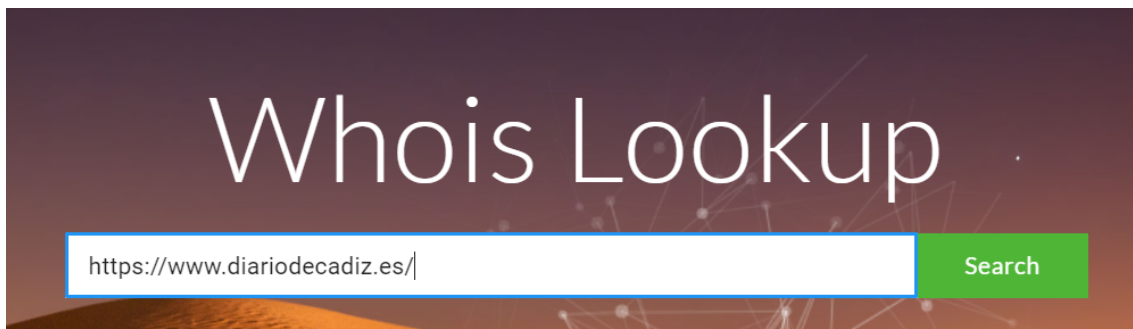


Figura 5: Buscamos el dominio del Diario de Cádiz en whoislookup

2.1.4. Ejercicio 2

Usando la herramienta DNS Trails liste los subdominios de *diariodecadiz.es* y responda a las siguientes preguntas:

- (a) ¿Cuántos subdominios encontramos?
- (b) ¿Quién provee el *hosting* a la página principal?
- (c) ¿Qué subdominio es una redirección a un panel de *login*?

2.1.5. Whois Lookup

Whois Lookup [4] es una herramienta provista por DomainTools capaz de entregarnos información variada sobre el dominio que estemos investigando. Gracias a esta aplicación web podremos saber, por ejemplo, el número de cambios que ha habido en el *hosting* donde se encuentra alojada la web, o ver capturas de pantalla del dominio. También podremos descargar un informe con toda la documentación, aunque esto solo será posible con una cuenta de pago. Para comenzar a probar esta herramienta necesitaremos un dominio sobre el que investigar.

Una vez que sepamos el dominio sobre el que queremos recolectar información, deberemos introducirlo en la barra de búsqueda de la página de inicio de Whois Lookup [4] (véase la Figura 5). La herramienta realizará la búsqueda y nos entregará información del dominio como el nombre de los servidores, la dirección IP del servidor, la dirección física estimada del servidor, el histórico de cambios, el número de imágenes y enlaces, etc. (véase Figura 6).

2.1.6. Ejercicio 3

Haciendo uso de Whois Lookup, conteste a las siguientes preguntas:

The screenshot shows the DomainTools Whois Lookup interface. At the top, there's a navigation bar with 'DOMAINTOOLS', 'PROFILE', 'CONNECT', 'MONITOR', 'SUPPORT', and a 'Whois Lookup' search bar. On the right, there are links for 'LOGIN', a shopping cart icon, and a 'Sign Up' button. The main content area is titled 'Whois Record for Diariodecadiz.es'. It is divided into two sections: 'Domain Profile' and 'Website'. The 'Domain Profile' section includes fields for Registrar Status (taken), Name Servers (DNS33.SERVIDORESDNS.NET and DNS34.SERVIDORESDNS.NET), Tech Contact (none), IP Address (51.81.243.73), IP Location (Oregon - Hillsboro - OvH Us Llc), ASN (AS16276 OVH, FR), and Hosting History (1 change on 2 unique name servers over 4 years). The 'Website' section includes Website Title (None given), Terms (2,303), Images (24), and Links (347). On the right side, there are promotional banners for 'DomainTools Iris' and 'Preview the Full Domain Report', followed by a 'Tools' section with links to 'Hosting History', 'Monitor Domain Properties', 'Reverse IP Address Lookup', 'Network Tools', and 'Visit Website'. At the bottom right, there is a small thumbnail of the website's content.

Figura 6: Información provista del dominio diariodecadiz.es por Whois Lookup

- (a) ¿Qué información podemos obtener sobre el dominio *cadizturismo.com*?
- (b) ¿Quién es el registrador de *cadiz.com*?

2.2. Tecnologías web

Otra forma de obtener información de interés en cualquier reconocimiento a un activo sería indagar sobre las diferentes tecnologías que utiliza su página web. En muchas ocasiones, las tecnologías utilizadas no son versiones únicas, sino que son partes o productos de una empresa de *software* que va actualizando sus aplicaciones o creando parches de actualización para sus productos. Estos parches o actualizaciones comienzan a desarrollarse, en la gran mayoría de ocasiones, por alguna falla en el código detectada que genera una amenaza para la aplicación.

Teniendo esto en cuenta, si conseguimos información sobre la tecnología que utiliza una determinada página web, podremos encontrar vulnerabilidades activas dentro de dicha web.

Para este propósito, existen herramientas especializadas como **Wappalyzer**.

2.2.1. Wappalyzer

Wappalyzer es un *software* que recopila datos de forma anónima de un sitio web a través del navegador. Se presenta en forma de extensión de navegador de código abierto y descubre las tecnologías utilizadas por los sitios web. Es capaz de identificar

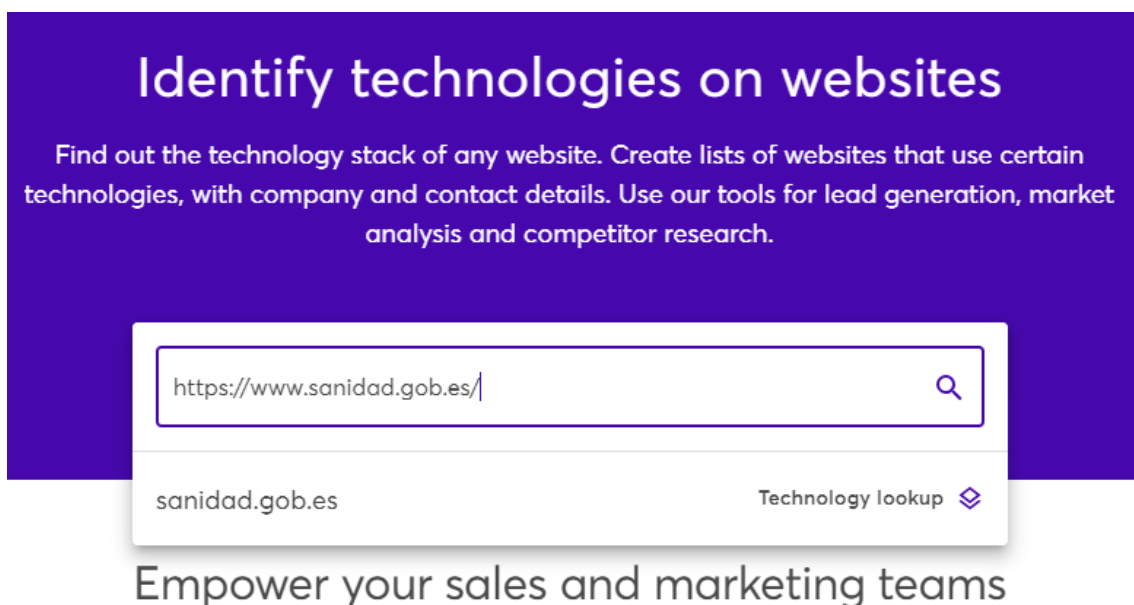


Figura 7: Hacemos clic en el botón que ha aparecido en Wappalyzer

1.222 tecnologías en 65 categorías diferentes. Detecta patrones únicos en el código fuente de la página web, encabezados, variables de *script* y herramientas de análisis con las que cuente la web, entre otros.

Para comenzar a utilizar Wappalyzer podemos descargar la extensión de navegador disponible en [1] o acceder a su web oficial [2]. En este ejemplo de uso utilizaremos la web oficial. Una vez en la web realizaremos una búsqueda (dentro del cuadro de búsqueda) para identificar las tecnologías de la web que queramos. En este caso utilizaremos la web del Ministerio de Sanidad (<https://www.sanidad.gob.es/>). Una vez introducida la dirección a buscar, pulsamos en el botón *technology lookup* que habrá aparecido abajo del cuadro de búsqueda (véase Figura 7). La herramienta comenzará a trabajar y, al terminar, nos mostrará las tecnologías detectadas en la web buscada, como podemos comprobar en Figura 8.

2.2.2. Ejercicio 4

Haciendo uso de la información encontrada a través de la extensión Wappalyzer, conteste a las siguientes preguntas:

- (a) ¿Qué versión de Apache se usa en *directorio.uca.es*?
- (b) ¿Qué versión de PHP se usa en *formulagades.com*?
- (c) ¿Qué *proxy* está usando *biblioteca.uca.es*?

The screenshot displays the website **sanidad.gob.es**. It is divided into two main sections: **Technology stack** and **About**.

Technology stack section:

- Programming languages:** Java
- Maps:** Google Maps
- Web frameworks:** JavaServer Pages (2.1), Java Servlet
- UI frameworks:** (empty)

About section:

- Get Plus for \$10/mo:** Sign up for **Plus** to include company and contact details in technology lookups. **Sign up** button.
- Metadata:**
 - Title:** Ministerio de Sanidad
 - Description:** Sitio Web del Ministerio de Sanidad
- Company information:** (with a **PLUS** button)

Figura 8: Tecnologías encontradas en la web del Ministerio de Sanidad

3. Búsqueda y reconocimiento a través de redes sociales

Además de toda la información que podemos encontrar gracias a los buscadores de Internet, también podemos continuar nuestra recolección de datos en las redes sociales. Cada vez son más los usuarios que tienen redes sociales como Facebook o Instagram, con la consecuente adquisición de los datos que los mismos comparten por partes de terceros. La mayoría de estos datos permanecen ocultos y son solo accesibles por parte de la empresa que hay detrás de cada red social. No obstante, todavía podemos acceder a todos los otros datos que las aplicaciones hacen visibles para los usuarios. Además, si hacemos uso de herramientas que utilicen la interfaz de programación de aplicaciones (API) de cada red social, la tarea se facilita enormemente.

A continuación, describiremos dos ejemplos de este tipo de herramientas: **Namecheck** y **Phonebook.gz**.

3.1. Namecheck

Namecheck [3] es una página web muy útil si queremos comprobar si un determinado nombre, para una cuenta o marca, está disponible en Internet. Namecheck realizará búsquedas en docenas de sitios web y bases de datos, devolviéndonos en un solo clic un informe con la disponibilidad del nombre a buscar en dominios y redes sociales.

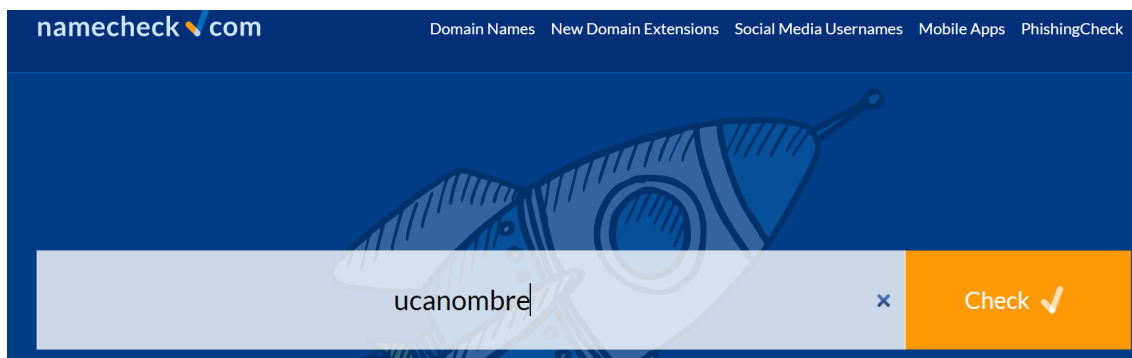


Figura 9: Realizamos la búsqueda dentro de Namecheck

Social Media Usernames [learn more](#)

facebook	already taken	View
twitter	already taken	View
linkedin	already taken	View
instagram	already taken	View
tumblr	available	Register
pinterest	available	Register
youtube	already taken	View
flickr	already taken	View

Figura 10: Disponibilidad, proporcionada por Namecheck, sobre un nombre de usuario entre diferentes redes sociales

Para comenzar a utilizar esta herramienta debemos acceder a su web oficial [3]. Una vez dentro introducimos en el cuadro de búsqueda el nombre cuya disponibilidad queramos consultar, y pulsamos en el botón de *check* (véase Figura 9). Namecheck realizará la búsqueda pertinente y nos devolverá la disponibilidad del nombre a buscar entre nombres de dominio, usuarios de redes sociales, y aplicaciones móviles, como podemos ver en Figura 10. Además, si pulsamos en el botón *view* que aparece a la izquierda de cada red social, seremos redireccionados hacia la URL del usuario.

3.1.1. Ejercicio 5

Haciendo uso de Namecheck, conteste a la siguiente pregunta:

- (a) Según este servicio, ¿en qué redes sociales se encuentra registrado el medio de comunicación *vivacadiz*? ¿Cuáles no son falsos positivos?

3.2. Phonebook.cz

Phonebook.cz [6] es una herramienta web capaz de listar todos los dominios, correos electrónicos asociados y enlaces provenientes de un dominio entregado como *input*.

No es una herramienta para recolectar información de redes sociales de una forma directa, pero es el complemento perfecto a la recolección que podamos hacer. Para utilizar esta herramienta tan solo necesitaremos un dominio web. Por ejemplo, utilizamos las redes sociales para encontrar una empresa sobre la que queramos obtener información, y una vez tengamos su nombre, lo buscamos en Google y llegamos hasta su dominio web. Con su dominio web en nuestras manos, podremos comenzar a utilizar esta poderosa herramienta.

Accedemos a su web oficial [6] e ingresamos el dominio sobre el que queramos recolectar información en su cuadro de búsqueda. Para realizar el ejemplo, utilizaremos la dirección de la UCA (*uca.es*). También deberemos seleccionar entre *Domains*, *Email Addresses* y *URLs* del dominio a buscar, como podemos ver en Figura 11. En este ejemplo, seleccionaremos la opción *Email Addresses* para ver todos los correos asociados a dicho dominio. Una vez seleccionado, pulsamos en el botón *Submit*.

Phonebook.cz

Phonebook lists all domains, email addresses, or URLs for the given input domain. Wildcards such as *.gov.uk are allowed. You are searching 34 billion records.



uca.es Submit

Try: [cia.gov](#), [cnn.com](#), [netflix.com](#), [*.ru](#), [*.gov.uk](#), [solarwinds.com](#)

☐ Domains
☒ Email Addresses
☐ URLs

Figura 11: Seleccionamos la opción *Email Addresses* en la herramienta Phonebook.cz

La herramienta comenzará a trabajar y nos devolverá un listado con todos las direcciones de correo electrónico que logre encontrar (véase Figura 12). Si pulsamos en cualquiera de las direcciones, la web nos mostrará en qué otras páginas web han sido citadas dichas direcciones de correo electrónico, como podemos observar en Figura 13. Por último, si hacemos clic en cualquiera de los enlaces encontraremos más información sobre dicha página web (véase Figura 14).

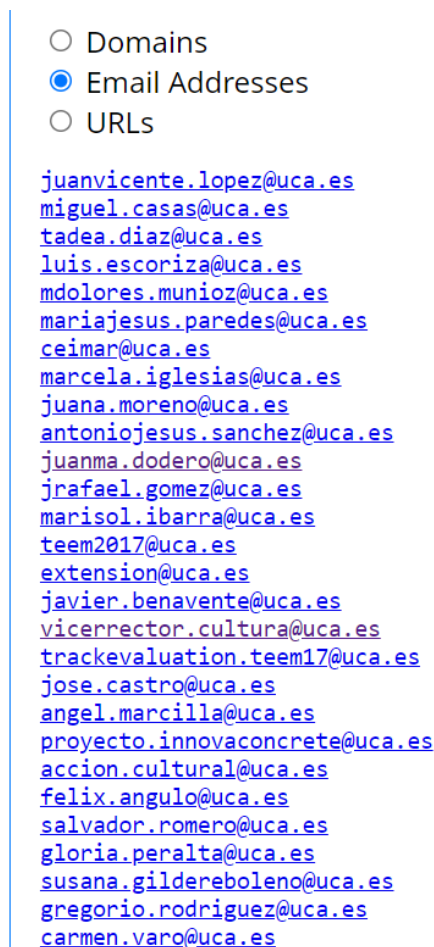


Figura 12: Direcciones de correo asociadas al dominio de la UCA

3.2.1. Ejercicio 6

Haciendo uso de Phonebook.cz, conteste a las siguientes preguntas:

- Obtenga una lista de los subdominios que encuentra la herramienta para el dominio *juntadeandalucia.es*
- ¿Cuántos correos que contengan la palabra *bonilla* aparecen en el apartado de direcciones de correo para el dominio *juntadeandalucia.es*?

4. Otras herramientas OSINT

En esta sección analizaremos otras muchas herramientas OSINT disponibles en la actualidad.

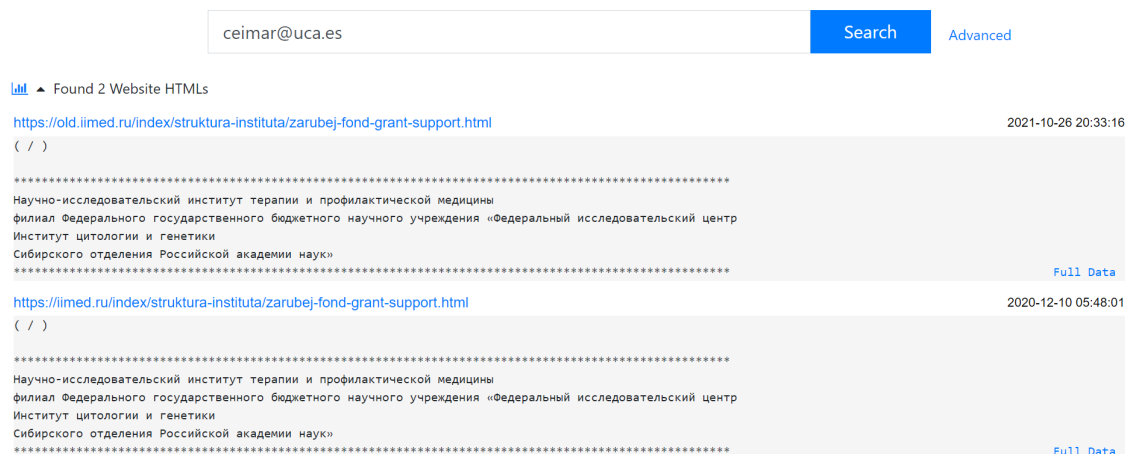


Figura 13: Observamos las páginas web que han citado a la dirección de correo electrónico del CEIMAR

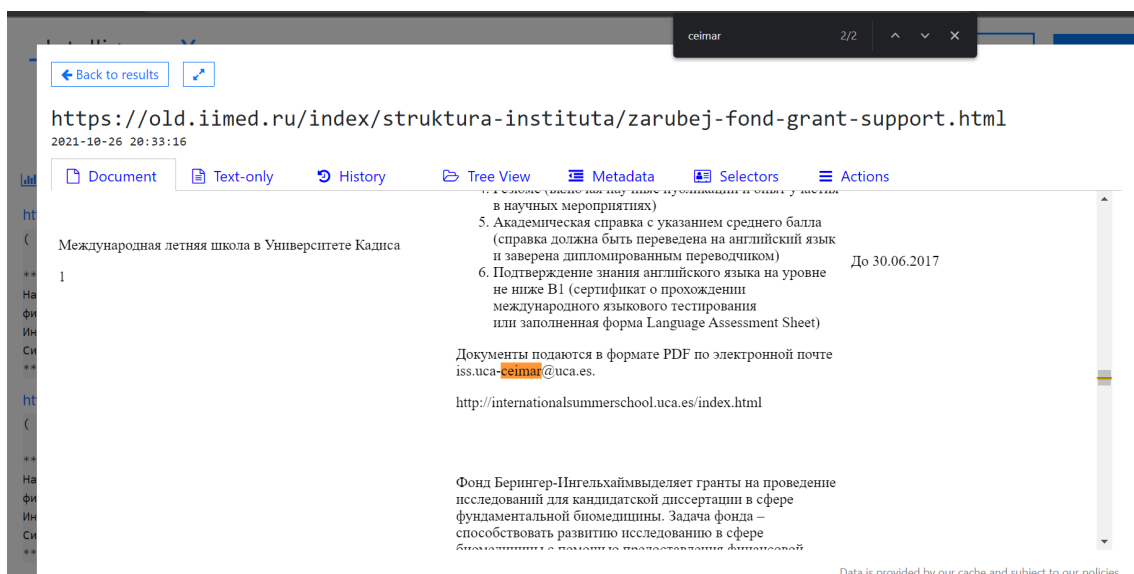


Figura 14: Encontramos más información sobre una de las páginas web que han citado la dirección del CEIMAR

4.1. Ejercicio 7

Conteste a las siguientes preguntas:

- (a) Acceda a la siguiente web: <https://osintframework.com/> ¿Qué información proporciona esta web?

- (b) De todas las herramientas proporcionadas en esta web (<https://osintframework.com/>), seleccione una que le resulte interesante y que no se haya explicado a lo largo de este guion de prácticas. Entonces explique brevemente en qué consiste la herramienta, pruébela con un ejemplo y muestre los resultados que ha obtenido.
- (c) Acceda a la siguiente web: <https://ciberpatrulla.com/links/> ¿Qué información proporciona esta web?
- (d) Entre todos los buscadores listados en esta web (<https://ciberpatrulla.com/links/>), figura el buscador DuckDuckGo (<https://duckduckgo.com/>). Realice una búsqueda cualquiera en Google y la misma búsqueda en DuckDuckGo. ¿Qué diferencias aprecia en los resultados obtenidos?
- (e) Acceda a la siguiente web: <https://inteltechniques.com/tools/index.html> ¿Qué información proporciona esta web?
- (f) De todas las herramientas proporcionadas en esta web (<https://inteltechniques.com/tools/index.html>), seleccione una que le resulte interesante y que no se haya explicado a lo largo de este guion de prácticas. Entonces explique brevemente en qué consiste la herramienta, pruébela con un ejemplo y muestre los resultados que ha obtenido.
- (g) Acceda a la siguiente web: <https://ciberpatrulla.com/guias/> ¿Qué información proporciona esta web?
- (h) De todas las guías proporcionadas en esta web (<https://ciberpatrulla.com/guias/>), seleccione una que le resulte interesante. Entonces haga uso de una de las herramientas explicadas en esa guía, pruébela con un ejemplo y muestre los resultados que ha obtenido.
- (i) ¿Para qué tipos de búsqueda son útiles las siguientes webs?:
 - <https://osint.industries/>
 - <https://epieos.com/>
 - <https://github.com/sundowndev/PhoneInfoga>
 - <https://ciberpatrulla.com/como-saber-quien-numero-telefono/>

Referencias

- [1] Elbert Alias: *Wappalyzer Extension*. <https://chrome.google.com/webstore/detail/wappalyzer/gppongmhjkpfnbhagpmjfkannfbllamg?hl=es>. [Última consulta: 2024-10-29].
- [2] Elbert Alias: *Wappalyzer Web Oficial*. <https://www.wappalyzer.com/>. [Última consulta: 2024-10-29].
- [3] united domains: *Namecheck web oficial*. <https://www.namecheck.com/>. [Última consulta: 2024-10-29].
- [4] DomainTools: *Whois Lookup web oficial*. <https://whois.domaintools.com/>. [Última consulta: 2024-10-29].
- [5] SecurityTrails: *DNS Trails Web Oficial*. <https://securitytrails.com/>. [Última consulta: 2024-10-29].
- [6] Intelligence X: *Phonebook.cz Web Oficial*. <https://phonebook.cz/>. [Última consulta: 2024-10-29].