ESTUDIO DE SEGURIDAD INFORMATICA DE LOS METADATOS CONTENIDOS EN ARCHIVOS PUBLICADOS EN LAS WEB DE LAS ORGANIZACIONES: ALCALDIA DE PAMPLONA, CAMARA DE COMERCIO DE PAMPLONA, GOBERNACION DE NORTE DE SANTANDER, DIARIO LA OPINION Y LA DIAN

JESUS ANTONIO DURAN ACEVEDO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
PROGRAMA DE ESPECIALIZACION EN SEGURIDAD INFORMATICA
PAMPLONA
2017

ESTUDIO DE SEGURIDAD INFORMATICA DE LOS METADATOS CONTENIDOS EN ARCHIVOS PUBLICADOS EN LAS WEB DE LAS ORGANIZACIONES: ALCALDIA DE PAMPLONA, CAMARA DE COMERCIO DE PAMPLONA, GOBERNACION DE NORTE DE SANTANDER, DIARIO LA OPINION Y LA DIAN

Monografía de Investigación

Para optar el título de:

Especialista en Seguridad Informática

Presentado Por:
JESUS ANTONIO DURAN ACEVEDO

Director
ING. FRANCISCO NICOLAS SOLARTE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA (UNAD)
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
PROGRAMA DE ESPECIALIZACION EN SEGURIDAD INFORMATICA
PAMPLONA
2017

Nota de aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

_____

Ciudad y Fecha de entrega

TABLA DE CONTENIDO

Pag.

LISTA DE IMÁGENES

LISTA DE TABLAS

LISTA DE ANEXOS

INTRODUCCION

Los metadatos son datos que proporcionan datos acerca de otros datos, es información organizada que describe, localiza y hace más fácil recuperar objetos digitales: Comenzaron como fichas de catalogación en las bibliotecas y ahora se utiliza principalmente en forma digital. Los metadatos están en todas partes, páginas web, archivos, software, estos describen, cuándo fue creado, de qué tamaño es, el autor, en general todo lo que se necesita saber para encontrar la información de manera eficiente.

Los metadatos proporcionan un medio de indexación, el acceso, la conservación, y la manera de encontrar recursos digitales. El volumen de información digital disponible a través de redes electrónicas ha creado una necesidad apremiante para los estándares que aseguren el uso correcto, la interpretación de los datos por parte de sus propietarios y usuarios, así como la seguridad y protección.

La gestión eficiente de los metadatos es crucial, especialmente para las grandes empresas, entidades y organizaciones, pues de no ser así, colocan en riesgo la información y pueden ser víctimas de ataques informáticos, especialmente de hackers que pueden utilizar diferentes métodos y técnicas de penetración utilizando la información obtenida y extraída de los metadatos encontrados muy fácilmente en diferentes tipos de archivos, como documentos, imágenes, audio, video, presentaciones, etc.

En este trabajo se va realizar un estudio de la seguridad informática de los metadatos, analizando las vulnerabilidades, amenazas, riesgos, y la manera de prevenir y mitigar los problemas de seguridad que se puedan encontrar, todo esto se hará de manera teórica y práctica, analizando los metadatos de archivos de diferentes fuentes y utilizando distintas herramientas y recursos informáticos.

1. PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

Es relevante el valor de los metadatos a nivel personal, institucional y organizacional, pues genera relaciones entre recursos, archivos, usuarios, repositorios y aplicaciones, realizando un seguimiento de todo el ciclo de vida del contenido digital de la información, incluyendo los procesos y procedimientos por los que han pasado desde su creación.

Figura 1. Qué son los metadatos

Fuente: http://es.slideshare.net/noticiasmias2002/modulo6-31190786

La información que contienen los metadatos es significativa y muy valiosa, describe y revela datos sobre un objeto informático, proporcionando datos y pistas precisas sobre su contenido, fecha de creación, usuario que lo creo, equipo donde se creó, impresoras predeterminadas, servidores web, servidores de almacenamiento, geo localización, entre otros.

Por lo tanto es de vital importancia gestionar adecuadamente los metadatos de cada objeto digital creado, y asegurar su información para que no vaya a llegar a manos inescrupulosas y malignas, que causen graves problemas, a nivel de seguridad informática como: Ataques phising, DDos, pharming, malware, carding, todas estas vulnerabilidades asociadas a metadatos.

1.2 DESCRIPCION DEL PROBLEMA

Las personas y organizaciones no han caído en cuenta de lo fundamental que son los metadatos en la seguridad informática y protección de la información, pues con los datos que se pueden extraer de un objeto digital, es posible realizar ataques informáticos y causar daños a todo nivel.

Un archivo (Objeto digital) de cualquier formato, que una empresa haya compartido por internet para que el público en general lo visualice, a parte del contenido, este posee una información que no se ve a primera vista, pero con las herramientas adecuadas se puede ver.

Una fotografía compartida en internet, aparte de contener la imagen como tal, contiene unos datos ocultos que describen la fotografía: resolución, tamaño, orientación, marca y modelo del dispositivo con la que se realizó la fotografía, el software del dispositivo, fecha y hora de creación, geo localización, entre otros.

Con esta información un hacker podría buscar los exploits apropiados para realizar un ataque, de igual manera con los datos de geo localización de una fotografía, un criminal que quiera hacer daño a una persona puede saber el lugar exacto donde se tomó la foto y analizando otras imágenes puede establecer el recorrido que está realizando y conseguir su cometido.

Un documento creado en Word y compartido en internet de igual manera se le pueden extraer lo metadatos, como: usuario autor, usuarios que lo han visualizado o editado, número de páginas, nombre del archivo, tamaño, equipo donde se creó el documento, impresora determinada del equipo, servidor en donde está instalada la impresora, equipos y servidores en el cual se ha compartido el archivo, entre otros.

Estos datos son suficientes, para que un cibercriminal encuentre las vulnerabilidades de la red informática donde se aloja el archivo, y se convierta en una amenaza para el sistema informático, pues se pueden presentar ataques cibernéticos que coloquen el riesgo de la seguridad de la información.

Lo anterior demuestra lo importante que son los metadatos en la seguridad informática de las organizaciones y de las personas en general, y si no se gestionan de una manera apropiada y eficaz, colocan en riesgo la confidencialidad, integridad y disponibilidad de la información.

1.3 FORMULACIÓN DEL PROBLEMA

¿Cómo el estudio de seguridad de los metadatos permitirá minimizar el impacto y probabilidad de ocurrencia de las vulnerabilidades, amenazas y riesgos de seguridad informática en las organizaciones y personas en general?

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Minimizar el impacto y probabilidad de ocurrencia de las vulnerabilidades, amenazas y riesgos de seguridad informática, en las organizaciones: Alcaldía de Pamplona, Cámara de Comercio de Pamplona, Gobernación de Norte de Santander, Diario La Opinión y La Dian, a través de un estudio de seguridad en los metadatos de los archivos publicados en sus respectivas web.

2.2 OBJETIVOS ESPECIFICOS

- ✓ Recolectar y organizar la información obtenida en los metadatos mediante el uso de software que permita la extracción de los metadatos, de los objetos digitales publicados por las empresas en estudio, utilizando diferente software.

- ✓ Analizar la información de los metadatos para determinar las vulnerabilidades, amenazas y riesgos de seguridad.

- ✓ Proponer y determinar alternativas de solución para proteger los metadatos.

- ✓ Elaborar un informe final sobre los resultados del análisis de los metadatos de la investigación

3. JUSTIFICACION DEL PROYECTO

Los metadatos son "los datos de los datos" y muestran parámetros, conexiones y acciones. Su conocimiento puede afectar la privacidad, a través de ellos se puede obtener más información que del mismo contenido de un documento, imagen o mensaje.

Figura 2. Metadatos de un archivo

Fuente: http://www.gitsinformatica.com/metadatos.html

Es fundamental analizar de forma teórica y práctica, la manera como los metadatos pueden incidir en la seguridad informática de las organizaciones y sociedad en general.

En la actualidad, a los metadatos no se les ha dado la importancia que se merece a la hora de diseñar planes de seguridad informática en las empresas. El personal encargado de la seguridad, no ha tenido en cuenta este elemento de información, que, aunque contiene datos ocultos son muy relevantes e importantes cuando se extraen.

Estos datos dan información detallada sobre los objetos digitales de una organización (Archivos), y de esta manera encontrar vulnerabilidades y amenazas que coloquen en riesgo la seguridad de la información. Solo con saber el nombre de un usuario que haya manipulado un archivo, es una vulnerabilidad para el sistema informático, y mucho más si se saben cosas, como: nombres de servidores, direcciones IP, DNS, nombre de impresoras, etc.

Toda la información que suministran los metadatos, debe ser gestionada en a cuanto a seguridad de una manera eficaz, pues de otra forma sería muy fácil utilizar esos datos para ocasionar daño a sistemas informáticos y personas.

Por lo anterior, esta investigación quiere dar a conocer los peligros que corre una organización al no gestionar y proteger los metadatos y a la vez crear conciencia sobre la importancia de asegurar la información de los metadatos, con el fin de minimizar las vulnerabilidades, amenazas y así reducir los riegos de ataques informáticos.

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

Este estudio se llevará a cabo extrayendo y analizando los metadatos de diferentes tipos de archivos públicos, compartidos en internet por algunas empresas y entidades públicas a nivel local, regional, nacional e internacional, escogidas, están son:

A nivel local:
Cámara de comercio de Pamplona, Alcaldía de Pamplona

A nivel Regional:
Diario la Opinión, Gobernación de Norte de Santander

A nivel Nacional:
DIAN

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

5.1.1 Investigación resalta importancia de los metadatos en la seguridad.

Un estudio de estudiantes del doctorado en ciencias de cómputo de la Universidad de Stanford, reveló que se utilizaron los metadatos de los teléfonos móviles para dar a conocer información sensible de los usuarios con el fin de alertar a la comunidad sobre los riesgos de no asegurar la información contenida en los metadatos.

Ellos usaron Metaphone (es un algoritmo fonético, un algoritmo para indexar palabras por su sonido al ser pronunciadas en inglés), para el Android para obtener los registros del dispositivo.

Con los datos obtenidos, se concluyó lo siguiente:

LA DATA

“Nos equivocamos, hemos encontrado que los metadatos de los teléfonos son inequívocamente sensibles, incluso en una población pequeña y haciendo un seguimiento de corto tiempo. Hemos sido capaces de deducir condiciones médicas, la propiedad de armas de fuego, y más, utilizando únicamente los metadatos del móvil”, indicó el grupo investigador.

Los metadatos contenidos en los números de teléfono del remitente y el destinatario, el número de serie de los teléfonos que utilizan, la hora y la duración de la llamada, y la ubicación física de las personas que llaman, puede ser extraída y vista.

La investigación demuestra la importancia de los metadatos y la información sensible que ocultan.

(@cdperiodismo, 2014)

5.1.2 Que Papel Juegan Los Metadatos Dentro De Una Evidencia?

El informe Blair

Se trata del caso que se presentó en el primer capítulo relativo al documento sobre la guerra de Irak que el gobierno de Tony Blair utilizó para justificar la participación de Gran Bretaña en el conflicto armado.

Cuando el ejecutivo británico es interrogado en el Parlamento sobre la autoría del documento y la implicación del gabinete de Blair en su elaboración, el primer ministro y su equipo niegan cualquier manipulación del archivo. No obstante, alguien analizó los metadatos de la versión Word del dos (@cdperiodismo, 2014)ier que el gobierno publicó en el sitio web de Downing Street y pudo demostrar que Blair y su equipo habían mentido.

Se pudo demostrar mediante el análisis de los metadatos del documento, que este fue modificado por varios autores, cuyos nombres de usuario corresponden con miembros del gabinete de Tony Blair, y puede incluso comprobarse que en algún momento el archivo se copió a un disquete. (A:).

5.1.3 La metadata en el centro de la investigación periodística

Actualmente los periodistas están prevenidos a la hora de enviar o publicar algún documento pues se están capacitando sobre la importancia y como proteger la información oculta de los documentos. Cuando se envía un documento, además de su contenido, se está dando a conocer información sobre el equipo que procesó, su sistema operativo, el software con que se creó el documento.

Cuando se envía un correo electrónico además de enviar el contenido también se está mostrando patrones de comportamiento, maneras de relacionarse con otras personas.

Un estudio demostró que quienes tengan a acceso a comunicaciones por Gmail, podrán entender rápidamente los grupos, las relaciones, los amigos, los contactos y todo aquello relacione el comportamiento de estos datos.

(Mariano, 2013)

5.2 MARCO HISTORICO

La historia de los metadatos se remonta desde la época A.C.

5.2.1 Año 280 A.C.

Se registró por primera vez el uso de metadatos, en la biblioteca de Alejandría, una pequeña etiqueta era colgada al final de cada rollo de pergamino, la cual tenía información del autor, título y tema del documento consultado. De esta manera los documentos podían ser consultados más fácilmente y puesto de vuelta a la zona de clasificación de forma sencilla y rápida.

5.2.2 Año 400 - 600 A.C. Edad Media

Manuscritos medievales tenían generalmente iluminaciones en cada capítulo, siendo a la vez una especie de firma para del autor y un anclaje de sección pictórica para los analfabetos en el momento.

5.2.3 Mediados de la década de 1800 – 1810

Con la aparición de la fotografía, los fotógrafos marcaban las fotografías, con el nombre, el lugar y fecha en que se realizó la foto, describiendo el contenido de las imágenes.

5.2.4 Año 1876

Se utilizó el Sistema de Clasificación Decimal Dewey (DDC), para clasificar todos los materiales de las bibliotecas. El DDC fue creado en 1876 por Melville Dewey.

5.2.5 Año 1960. Conversión al sistema digital

Se creó un estándar legible por máquina, eran un conjunto de formatos digitales para la descripción de los elementos catalogados por las bibliotecas. Fue desarrollado por Henriette Avram en los registros de la Biblioteca del Congreso de

Estados Unidos, podían ser utilizados por los ordenadores y compartidos entre las bibliotecas.

5.2.6 Año 1968

El término "metadatos" es utilizado por Philip Bagley en su libro, "Extensión de los conceptos del lenguaje de programación."

5.2.7 Año 1979

La compañía International Press Telecommunications Council (IPTC), crea y establece para salvaguardar los intereses de telecomunicaciones de la prensa, y desarrollar estándares para el intercambio de noticias, el primer conjunto de atributos de metadatos que se aplican a las imágenes.

5.2.8 Año 1980

Se desarrollaron sistemas de software para la gestión de documentos en papel. Estos sistemas registraban información de los documentos y de fotografías, y la clasificaban.

5.2.9 Año 1991

Un nuevo estándar, el "intercambio de información Modelo" (IIM), es creado por el IPTC para gestionar sus activos de imágenes digitales con metadatos codificados como datos binarios dentro del archivo.

5.2.10 Año 1993

Martiijn Koster desarrolla ALIWEB, el primer meta motor de búsqueda.

5.2.11 Año 1995

MetaCrawler, un metabuscador, hace su debut en el mercado. Esta nueva generación de motores de búsqueda fusiona los primeros resultados de búsqueda web de Google, Yahoo!, Live Search, Ask, About.com, MIVA, LookSmart y otros sistemas populares.

5.2.12 Año 2000

Con el uso generalizado de sistemas de información, surge la necesidad de la conceptualización de metadatos. Un conjunto de metadatos es desarrollado para los registros y propiedades de los archivos.

5.2.13 Año 2001

Music Genome Project, crea un complejo algoritmo para describir las canciones, mediante atributos y casi 400 metadatos.

5.2.14 Año 2009

Funcionarios del Departamento de Justicia de Estados Unidos reconocen que la Agencia Nacional de Seguridad (NSA) había participado en la recaudación indiscriminada de registros de metadatos de millones de ciudadanos de Estados Unidos.

5.2.15 Año 2013

Netflix financia la televisión, sobre la base de un análisis minucioso de los hábitos televisivos de sus 44 millones de suscriptores en todo el mundo, utilizando metadatos.

5.3 MARCO TEORICO

5.3.1 LOS METADATOS

Los metadatos son datos de un dato, proporcionan la información mínima necesaria para identificar un recurso, la definición de metadato se obtiene de las ciencias de la computación, son comprensibles para el hombre y reconocibles para los sistemas informáticos.

Constituyen un mecanismo para caracterizar datos y servicios de manera que los usuarios puedan encontrarlos, permiten describir un conjunto de datos y acceder a ellos, incluyen información descriptiva sobre contexto, la calidad y condición del dato.

La importancia de los metadatos, es que su documentación sirve de soporte para quienes utilicen la información de un determinado proyecto, incrementan la accesibilidad a los datos, permite establecer condiciones de acceso y uso de los datos.

Mediante los metadatos un usuario puede evaluar si los datos le son útiles para lo que necesita, revisar su valor potencial y sus limitaciones.

5.3.2 CARACTERIATICAS DE LOS METADATOS

- ✓ Resume el significado de los datos.
- ✓ Permite la búsqueda
- ✓ Determina si el dato es el que se necesita.
- ✓ Recupera y usa una copia del dato
- ✓ Muestra instrucciones de cómo interpretar un dato.
- ✓ Obtiene información sobre las condiciones de uso (derechos de autor)
- ✓ Aporta información acerca de la vida del dato.
- ✓ Ofrece información relativa del propietario o creador.
- ✓ Indica relaciones con otros recursos.
- ✓ Controla la gestión.

5.3.3 FUNCIONES DE LOS METADATOS:

- ✓ Descubrimiento de recursos
- ✓ Organización de recursos electrónicos
- ✓ Facilitar la interoperabilidad
- ✓ Identificación digital
- ✓ Archivo y preservación

5.3.4 TIPOS DE METADATOS

Hay tres tipos principales de metadatos:

Tabla 1. Tipos de Metadatos

Tipo	Objetivo	Elementos de muestra
Metadatos Descriptivos	Describen un recurso para propósitos tales como el descubrimiento y la identificación	Puede incluir elementos como título, resumen, autor y palabras clave.
Metadatos Estructurales	indica cómo los objetos y recursos compuestos se juntan	Por ejemplo, cómo se ordenan las páginas para formar capítulos
Metadatos Administrativos	Proporciona información para ayudar a gestionar un recurso.	Por ejemplo, cuándo y cómo se creó, tipo de archivo y otra información técnica, y quién puede acceder a ella.

Fuente: El autor

5.3.5 IMPORTANCIA DE LOS METADATOS

Un archivo de texto puede contener entre sus metadatos multitud de información relacionada con su procedencia, como datos sobre su autor, su fecha de creación y modificación, qué otros usuarios han manipulado el documento o el software utilizado para su redacción, por ejemplo, una fotografía, podría incorporar información en sus metadatos sobre la marca y el modelo de la cámara utilizada, la profundidad de color, su resolución, o las coordenadas de posicionamiento GPS desde la que se realizó dicha fotografía.

Los metadatos resultan muy útiles para catalogar la información y para facilitar su localización, ya que la información que incorporan se utiliza para optimizar las búsquedas, y son utilizados de forma masiva por los Sistemas de Gestión

Documental de las compañías y por los motores de búsqueda de Internet. Los metadatos de los ficheros almacenados por estos sistemas simplifican el desarrollo de filtros para, por ejemplo, localizar los documentos creados por un determinado usuario o acotar una búsqueda para discriminar documentos en función de su fecha de creación.

Los metadatos además son la base de la Web semántica, una ampliación de la Web en la que, idealmente, las aplicaciones podrán interactuar sin intervención humana porque conocerán el significado de los datos y las relaciones existentes entre ellos, por lo que es necesario que la información esté autodocumentada.

5.3.6 HERRAMIENTAS PARA LA EXTRACCION DE METADATOS

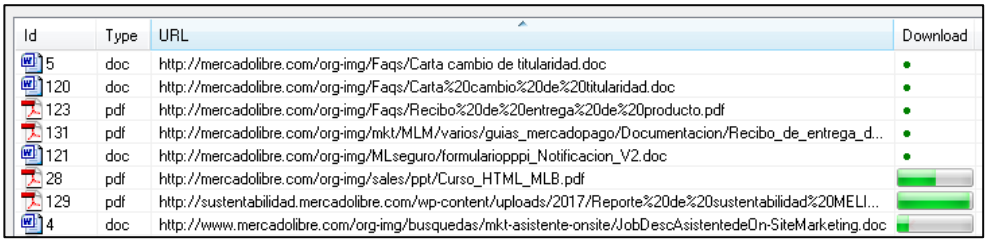
5.3.6.1 Foca

Le herramienta FOCA es una utilidad pensada por pentesters que hacen pentesting. Esto hace que esta herramienta esté llena de opciones muy útiles al momento de realizar una auditoría de seguridad a un sitio web o la red de una empresa. FOCA está basada en la recolección de información de fuentes abiertas OSINT, hoy día es muy popular en el mundo de la seguridad informática.

Posee opciones para el análisis de metadatos, descubrimiento de red, técnicas de fingerprinting y búsqueda de vulnerabilidades.

FOCA es una herramienta muy conocida por la extracción y análisis de metadatos en diferente tipo de documento, esa es la principal función de esta interesante y poderosa herramienta.

Figura 3. Descarga de archivos con FOCA



Id	Type	URL	Download
5	doc	http://mercadolibre.com/org-img/Faqs/Carta cambio de titularidad.doc	
120	doc	http://mercadolibre.com/org-img/Faqs/Carta%20cambio%20de%20titularidad.doc	
123	pdf	http://mercadolibre.com/org-img/Faqs/Recibo%20de%20entrega%20de%20producto.pdf	
131	pdf	http://mercadolibre.com/org-img/mkt/MLM/varios/guias_mercadopago/Documentacion/Recibo_de_entrega_d...	
121	doc	http://mercadolibre.com/org-img/MLseguro/formulariopppi_Notificacion_V2.doc	
28	pdf	http://mercadolibre.com/org-img/sales/ppt/Curso_HTML_MLB.pdf	
129	pdf	http://sustentabilidad.mercadolibre.com/wp-content/uploads/2017/Reporte%20de%20sustentabilidad%20MELI...	
4	doc	http://www.mercadolibre.com/org-img/busquedas/mkt-asistente-onsite/JobDescAsistentedeOn-SiteMarketing.doc	

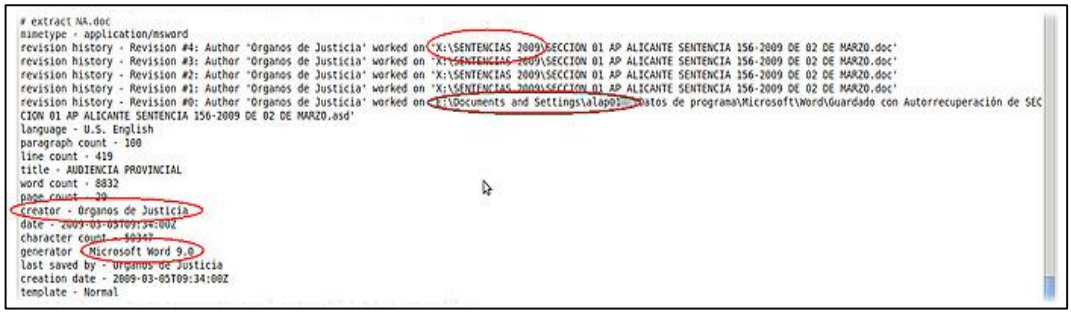
Fuente: El autor

5.3.6.2 Extract

Esta herramienta fue creada para trabajar en sistemas operativos Linux, su objetivo es buscar, encontrar y dar a conocer la información oculta en los documentos, es decir extrae y muestra la información de los metadatos que se encuentra en los documentos y ficheros que se requieran analizar.

De la información extraída se puede obtener información importante como, nombres de usuarios, nombres de servidores, rutas de directorios, nombres de impresoras, sistemas operativos, etc, como se puede apreciar en la siguiente figura:

Figura 4. Uso de herramienta Extract



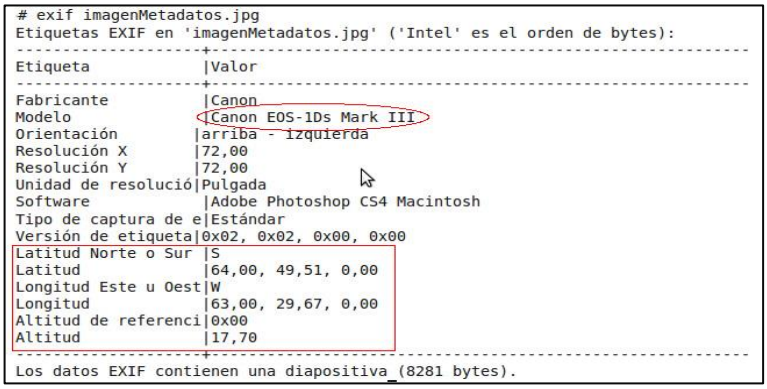
Fuente: http://tonytomisoniii.com/2015/08/11/mtool-a-utility-to-extract-document-metadata-from-m-files/

5.3.6.3 Regex Exif

Esta Herramienta trabaja online, y su función principal es extraer los metadatos EXIF de fotografías.

Hoy día las cámaras digitales, teléfonos inteligentes y escáner al momento de capturar una imagen graban información en el fichero de la fotografía, en esos datos se puede encontrar información como: marca y modelo de la cámara, geolocalización, tamaño de la imagen, exposición, apertura, lente usado, distancia focal, resolución, software y otros datos. Como se puede apreciar en la siguiente figura:

Figura 5. Extracción de Metadatos con REGEX EXIF



```
# exif imagenMetadatos.jpg
Etiquetas EXIF en 'imagenMetadatos.jpg' ('Intel' es el orden de bytes):
--------------------+------------------------------------------------------------
Etiqueta            |Valor
--------------------+------------------------------------------------------------
Fabricante          |Canon
Modelo              |Canon EOS-1Ds Mark III
Orientación         |arriba - izquierda
Resolución X        |72,00
Resolución Y        |72,00
Unidad de resolució|Pulgada
Software            |Adobe Photoshop CS4 Macintosh
Tipo de captura de e|Estándar
Versión de etiqueta|0x02, 0x02, 0x00, 0x00
Latitud Norte o Sur |S
Latitud             |64,00, 49,51, 0,00
Longitud Este u Oest|W
Longitud            |63,00, 29,67, 0,00
Altitud de referenci|0x00
Altitud             |17,70
--------------------+------------------------------------------------------------
Los datos EXIF contienen una diapositiva (8281 bytes).
```

Fuente: http://geeksroom.com/2014/07/regex-exif-fotografia/86913/

Es muy importante dejar en la imagen o fotografía la información necesaria que queremos que se publique, y así evitar que se propague información privada.

Figura 6. Información obtenida de los metadatos con la Herramienta REGEX EXIF

From Web / From File Image URL: View Image At Url [CLEAR IMAGE]

Basic Image Information

Target file: IM0_0748.JPG

Camera:	Canon PowerShot SD1400 IS
Lens:	5 - 20 mm Shot at 20 mm (shot wide open)
Exposure:	Auto exposure, 1/202 sec, f/5.9, ISO 80
Flash:	Auto, Did not fire
Focus:	Single, Face Detect, with a depth of field of from 65.53 m to infinity. AF Area Mode: Multi-point AF or AI AF
Date:	**October 1, 2012** 1:03:56AM (timezone not specified) (1 year, 9 months, 7 days, 19 hours, 47 minutes, 17 seconds ago, assuming image timezone of US Pacific)
File:	**3,240** × **4,320** JPEG (**14.0** megapixels)
Color Encoding:	WARNING: Color space tagged as sRGB, without an embedded color profile. **Windows and Mac browsers and apps treat the colors randomly.** Images for the web are most widly viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for

Extracted **160** × **120** 8.0-kilobyte "CompositeThumbnailImage" JPG
Displayed here at 200% (1/1.82 the area of the original)

Click image to isolate; click this text to show histogram

Main JPG image displayed here at 10% width (1/5.2 the area of the original)

Fuente: http://geeksroom.com/2014/07/regex-exif-fotografia/86913/

5.3.6.4 Exif Tool

ExifTool es un programa gratuito y de código abierto para leer, escribir y manipular metadatos de imagen, audio, video y PDF. ExifTool implementa su propio formato de metadatos abierto. Está diseñado para encapsular meta información de muchas fuentes, en forma binaria o textual, y agruparlo junto con cualquier tipo de archivo.

Características:

- ✓ Lee / escribe metadatos en una amplia variedad de archivos
- ✓ Soporta muchos tipos diferentes de metadatos incluyendo EXIF, IPTC y XMP
- ✓ Incluye la aplicación de línea de comandos más bibliotecas Perl
- ✓ Geotags imágenes de registros de seguimiento GPS
- ✓ Cambia los valores de fecha y hora para fijar las marcas de tiempo en las imágenes
- ✓ Copia metadatos de un archivo a otro
- ✓ Procesa todo el árbol de directorios
- ✓ Renombra / organiza imágenes basadas en metadatos
- ✓ Paquetes de distribución para Unix, Windows y Mac

El sitio de alojamiento de imágenes Flickr utiliza ExifTool para analizar los metadatos de las imágenes subidas.

5.3.6.5 Grampus Project

Creado para los usuarios que requieren automatizar sus tareas de auditorías web. Creado para sistema operativo Linux, es una alternativa semejante a la herramienta FOCA.

El proyecto Grampus se divide en los siguientes componentes:

- ✓ **Forensic Grampus:** Forensic Grampus es una herramienta forense que pretende extraer y analizar los metadatos encontrados en documentos, imágenes , archivos, aplicaciones.

- ✓ Está totalmente programado en Python por lo que es la perfecta alternativa multiplataforma para Forensic FOCA superando a esta con creces en cuanto a extensiones soportadas.

- ✓ **Anti-Forensic Grampus:** Anti Forensic Grampus es una herramienta ANTI forense que pretende eliminar o modificar aquellos metadatos encontrados en documentos, imagenes, archivos, aplicaciones.

- ✓ Está totalmente programada en Python por lo que es una buena alternativa a Metashield Protector proporcionando protección contra las mismas extensiones que podemos analizar en Forensic Grampus.

- ✓ **Grampas:** Grampus es una herramienta para la automatización de procesos fingerprinting en los trabajos de auditoria web sumándole a esto la posibilidad

de extraer y analizar los documentos públicos encontrados en la propia página a la que se le realiza la auditoria.

- ✓ **Anti-Grampus:** Anti Grampus es una herramienta creada para evitar exponer datos o credenciales que puedan ser de utilidad en ese proceso de fingerprinting volviendo así a nuestro sitio más seguro.

  Está totalmente programado en Python así como las otras 3 herramientas y a diferencia de las demás esta surge como contramedida y no como una alternativa.

5.4 MARCO CONCEPTUAL

5.4.1 Metadato: Es el dato de un dato, proporciona la información mínima necesaria para identificar un recurso.

5.4.2 Dato: Es cualquier conjunto de caracteres que se ha recopilado y traducido para algún propósito, por lo general el análisis. Puede ser cualquier carácter, incluyendo texto y números, imágenes, sonido o vídeo. Si los datos no se ponen en contexto, no hace nada a un humano o una computadora.

5.4.3 Atributo: Permite definir el valor de los metadatos que forman la información de un objeto digital.

5.4.4 Etiqueta: Señal**,** marca**,** rótulo o marbete que se adhiere a un objeto digital para su identificación, clasificación o valoración.

5.4.5 Privacidad: Parte más interior o profunda de la vida de una persona, que comprende sus sentimientos, vida familiar o relaciones de amistad.

5.4.6 Descripción: Explicar, de manera detallada y ordenada, los atributos de un objeto.

5.4.7 Objeto digital: Elemento en formato digital destinado a un proceso.

5.4.8 Categoría: Clase que resulta de una clasificación de objetos según un criterio o jerarquía.

5.4.9 Geo localización: Es la capacidad para obtener la ubicación geográfica real de un objeto

5.4.10 Identificación: Reconocer o establecer los datos e información principal sobre un objeto digital.

5.4.11 Sintaxis: Es el conjunto de normas que regulan y coordinan las distintas variables y su asociación.

5.4.12 Vector de ataque: Un vector de ataque es el método que utiliza una amenaza para atacar un sistema.

5.4.13 Vulnerabilidad: Estado de un sistema informático que deja abierta la posibilidad de una posible explotación o ataque.

5.4.14 Amenaza: Es una posible situación en que un sistema informático se puede ver amenazado o afectado por una acción que puede ser realizada intencionalmente para causar daño a los sistemas informáticos y hacer peligrar la seguridad de la información.

5.4.15 Imagen Digital: La imagen digital es la representación bidimensional de una imagen empleando bits, unidad mínima de información compuesta por dígitos binarios (1 y 0), que se emplea a instancias de la informática y cualquier dispositivo de tipo digital. *(Definición ABC, 2009)*

5.4.16 Documento digital: Contiene información codificada en forma de dígitos binarios que puede ser capturada, almacenada, analizada, distribuida y presentada por medio de sistemas informáticos. *(Calameo, 2010)*

5.4.17 Archivo Digital: Un archivo digital, también denominado Fichero, es una unidad de datos o información almacenada en algún medio que puede ser utilizada por aplicaciones de la computadora.

Cada archivo se diferencia del resto debido a que tiene un nombre propio y una extensión que lo identifica. *(wordpress.com, 2013)*

5.4.18 Exif Data: Es un estándar que especifica los formatos de imágenes, sonido y etiquetas auxiliares utilizados por las cámaras digitales, teléfonos inteligentes, escáneres y otros sistemas de manejo de imágenes y archivos de sonido Grabados por cámaras digitales. Este formato tiene etiquetas estándar para información de ubicación. A partir de 2014 muchas cámaras y la mayoría de los teléfonos móviles tienen un receptor GPS integrado que almacena la información de la ubicación en la cabecera Exif cuando se toma una fotografía. *(data, 2011)*

5.5 MARCO LEGAL

5.5.1 Ley estatutaria 1266 del 31 de diciembre de 2008

Normas especiales de Hábeas Data y se reglamenta la gestión de la información que se encuentre en bases de datos personales, financiera, crediticia, comercial, de servicios y la que se obtenga de otros países, y además de otras disposiciones.

5.5.2 Ley 1273 del 5 de enero de 2009

Esta ley reforma el Código Penal, creando un nuevo bien jurídico llamado; “protección de la información y de los datos” y ampara totalmente los sistemas que usen las tecnologías de la información y las comunicaciones, además de otras disposiciones.

Dentro de esta ley se encuentran estipulados los siguientes artículos que se relacionan con el proyecto:

5.5.3 Artículo 269A: Acceso abusivo a un sistema informático.

El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

5.5.4 Artículo 269C: Interceptación de datos informáticos.

El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

5.5.5 Artículo 269E: Uso de software malicioso.

El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

5.5.6 Artículo 269F: Violación de datos personales.

El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

5.5.7 Artículo 269G: Suplantación de sitios web para capturar datos personales.

El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. *(igac, 2014)*

5.5.8 Decreto 1377 de 2013

Esta nueva Ley impone a las empresas que usen datos personales que hayan almacenado antes de este decreto, solicitar permiso y autorización a los ciudadanos por medio de canales de comunicación como; correos electrónicos, correos certificados, llamadas telefónicas, mensajes de texto y su vez les dejó fijar publicidad en diferentes medios masivos.

6 DISEÑO METODOLOGICO

6.1 METODOLOGIA DE INVESTIGACION

Para este estudio se ha definido utilizar el enfoque cualitativo, pues nos permite analizar de una manera real y detallada, todas las observaciones y experiencias que se van a realizar con respecto a la seguridad informática de los metadatos, y de este modo obtener resultados, puntos de vista y conclusiones más globales sobre la problemática.

6.2 TIPO DE INVESTIGACION

El tipo de investigación que se va utilizar en el proyecto es la Descriptiva, ya que permite describir las situaciones, eventos y el comportamiento del tema en estudio, en este caso la seguridad informática de los metadatos.

6.3 METODOLOGIA DE DESARROLLO

6.3.1 Recolectar y organizar la información obtenida en los metadatos.

Este proceso se realiza mediante el uso de software que permita la extracción de los metadatos, de los objetos digitales publicados por las empresas en estudio, utilizando diferente software.

- ✓ Ingresar a cada URL de las entidades que se va analizar y descargar diferentes tipos de archivos publicados de libre acceso, y clasificarlos por organización y tipo de formato.

- ✓ Utilizando distintos software, se extraen los metadatos de los archivos descargados y se clasifica la información.

✓ Realizar un consolidado general de la información obtenida de los metadatos, unificarla y clasificarla por tipo de archivo y por atributo.

6.3.2 Analizar la información de los metadatos para determinar las vulnerabilidades, amenazas y riesgos de seguridad.

- ✓ Analizar la información sensible respecto a seguridad informática encontrada en los metadatos.

- ✓ Determinar las vulnerabilidades, amenazas y riesgos de seguridad informática, de acuerdo a la información obtenida de los metadatos.

6.3.3 Proponer y determinar alternativas, para proteger los metadatos.

- ✓ Realizar un consolidado general de vulnerabilidades, amenazas y riesgos de seguridad informática.

- ✓ Relacionar cada vulnerabilidad, amenaza y riesgo, con los atributos de los metadatos.

- ✓ Proponer medidas de seguridad de los metadatos para mitigar y prevenir cada vulnerabilidad, amenaza y riesgo de seguridad informática.

6.3.4 Elaborar el informe final de la investigación

- ✓ Realizar el informe final del estudio, previo análisis de los resultados.

6.4 FUENTES DE RECOLECCION DE INFORMACION

Para recolectar la información se usarán métodos empíricos: La observación, consultas y el experimento.

Las principales fuentes para la recolección de la información, son artículos y documentos relacionados con los Metadatos.

Otra fuente fundamental para la investigación son los informes de las herramientas que extraen metadatos, esa información es indispensable para el análisis de los metadatos.

6.5 RECURSOS PARA DESARROLLAR EL PROYECTO

6.5.1 Talento Humano

El estudio será desarrollado solo por un profesional en Seguridad Informática, capaz de analizar y evaluar cada vulnerabilidad, amenaza y riesgos de los metadatos, y determinar sus respectivos controles, en este caso será desarrollado por mi persona.

6.5.2 Recursos Físicos

Solo es necesario tener un espacio cómodo (Oficina), dotado de una un buen escritorio, silla y buena iluminación.

6.5.3 Recursos Tecnológicos

- ✓ 1 Computador
- ✓ Acceso a Internet
- ✓ Navegadores Web
- ✓ Paquete de Ofimática
- ✓ Software de extracción de metadatos.
- ✓ Software Pentesting

6.6 UNIVERSO Y MUESTRA

La muestra del estudio se realizará a 27 organizaciones escogidas previamente:

6.6.1 A nivel local:

Cámara de comercio de Pamplona, Alcaldía de Pamplona.

6.6.2 A nivel Regional:

Diario la Opinión, Gobernación de Norte de Santander.

6.6.3 A nivel Nacional:

DIAN

6.7 PRODUCTO A ENTREGAR

Al terminar la investigación se elaborará un informe sobre toda la realización del estudio, como se hizo, la metodología utilizada, el análisis de los resultados, recomendaciones y conclusiones.

7 EJECUCION

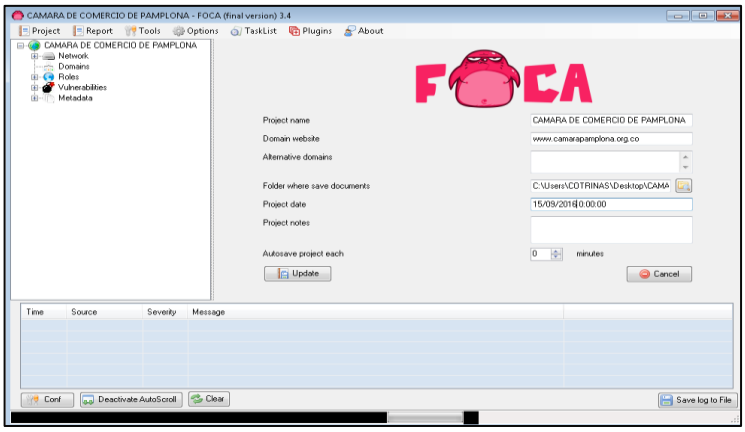
7.1 FASE 1: RECOLECTAR Y ORGANIZAR LA INFORMACIÓN DE LOS METADATOS.

De la URL de cada entidad y empresa en estudio, se descargan los archivos públicos contenidos en cada web, luego se procede a la extracción de los metadatos y posterior análisis, estas 3 acciones se realizan utilizando la herramienta FOCA Versión 3.4.

7.1.1 Descarga de archivos, extracción y análisis de metadatos de la Cámara de Comercio de Pamplona. URL: www.camarapamplona.org.co

El nuevo proyecto se crea con el nombre de la entidad en este caso Cámara de Comercio de Pamplona, se coloca el WebSite: www.camarapamplona.org.co, y la ubicación en donde va quedar almacenados toda la información y documentos del proyecto.

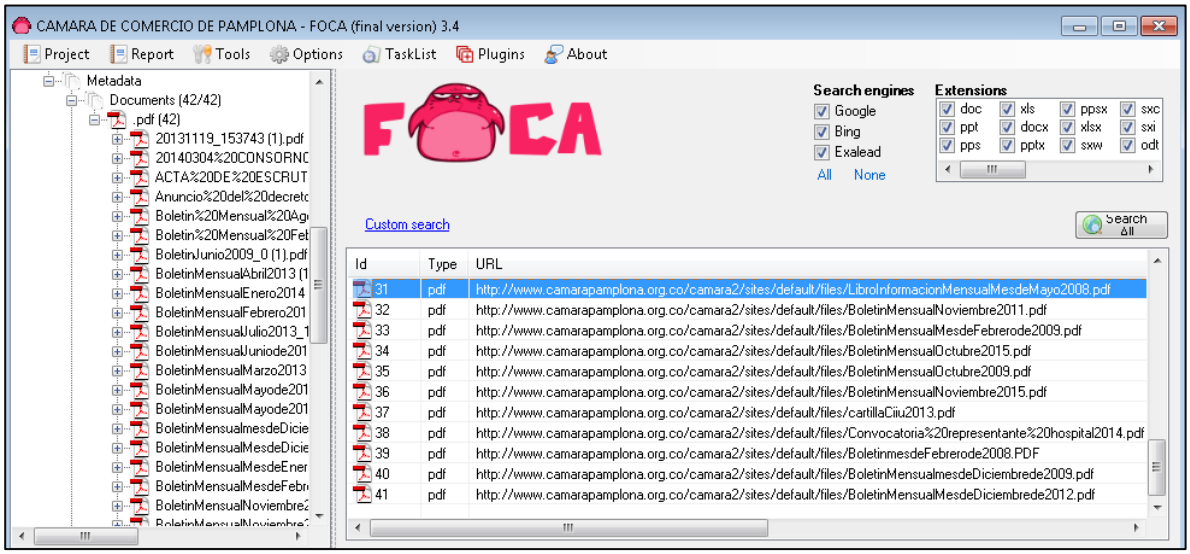
Figura 7. Creación del Proyecto análisis de metadatos de www.camarapamplona.org.co



Fuente: El autor

Utilizando los Buscadores Google, Bing, Exalead, FOCA encuentra 42 documentos públicos en formato pdf.

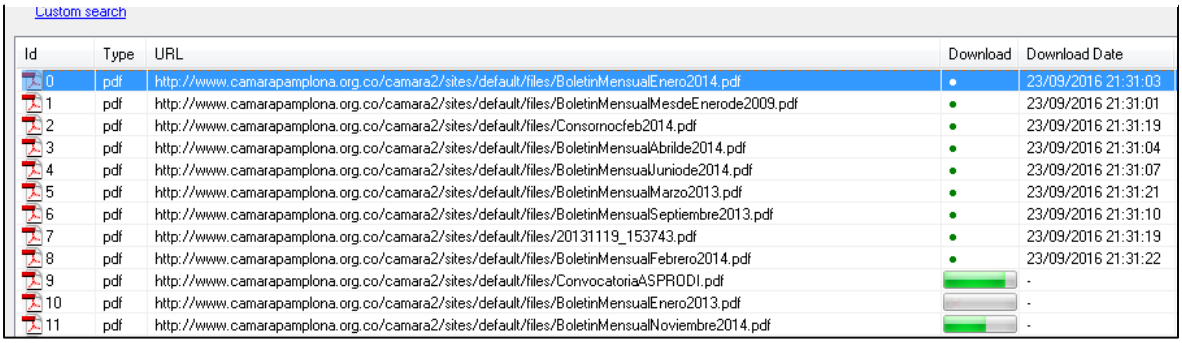
Figura 8. Búsqueda de Archivos Públicos en www.camarapamplona.org.co



Fuente: El autor

Se procede a descargar todos los archivos encontrados en la URL (42 en total).

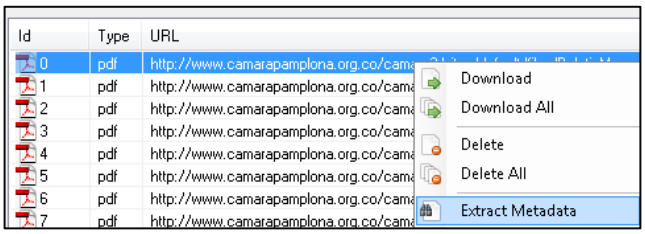
Figura 9. Descarga de los archivos públicos encontrados en www.camarapamplona.org.co



Fuente: El autor

Posteriormente se extraen los metadatos de todos los archivos.

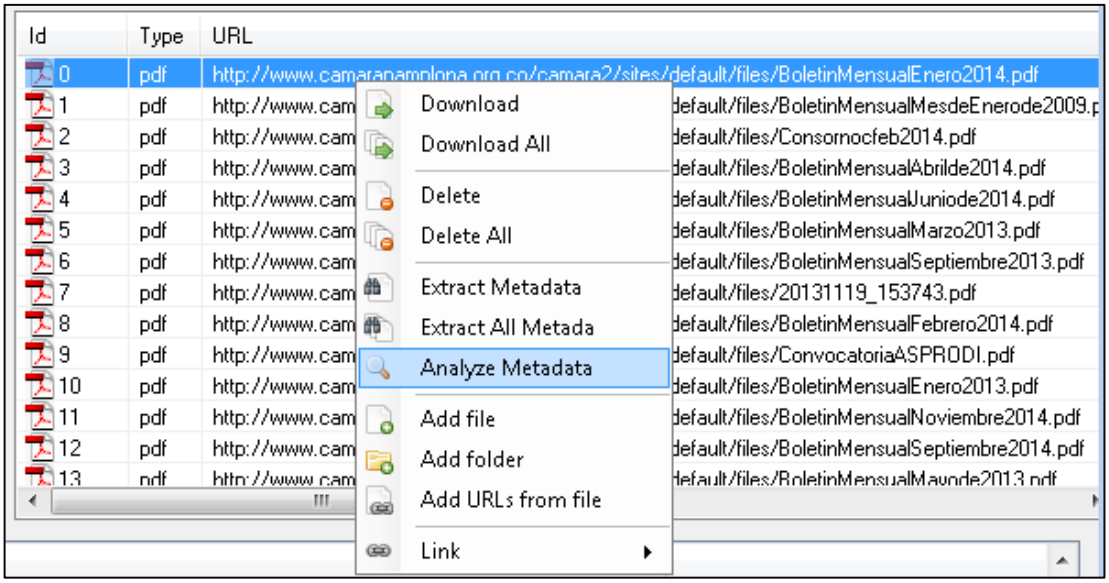
Figura 10. Extracción de metadatos de los archivos públicos descargados de www.camarapamplona.org.co



Fuente: El autor

El siguiente paso es analizar los metadatos de todos los archivos públicos descargados.

Figura 11. Análisis de todos los metadatos



Fuente: El autor

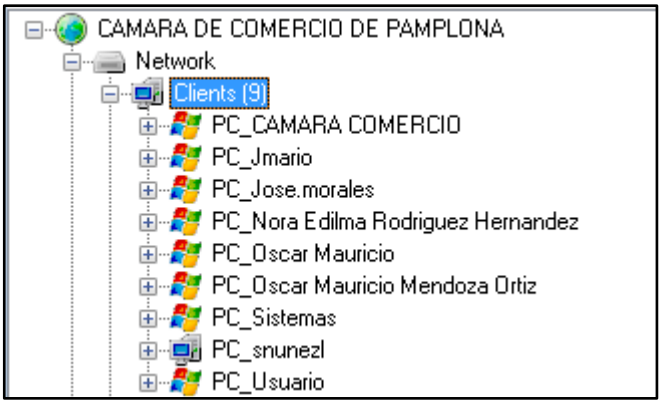
7.1.1.1 Resultado del análisis de los metadatos

Después del análisis de los metadatos realizado por FOCA a los 42 documentos públicos descargados de la URL: www.camarapamplona.org.co, se obtuvieron los siguientes resultados:

7.1.1.2 Red

Se encontró información de 9 usuarios cliente que tienen acceso al sistema.

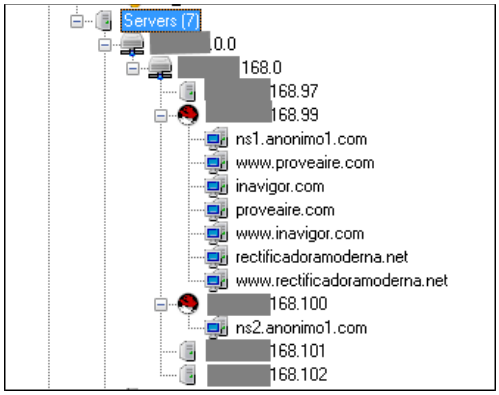
Figura 12. Usuarios cliente encontrados



Fuente: El autor

Se encontró información de 7 Direcciones IP de Servidores que pertenecen a la red informática, en la IP: 138.128.168.99 se observan URL's a las cuales se ha ingresado desde ese servidor.

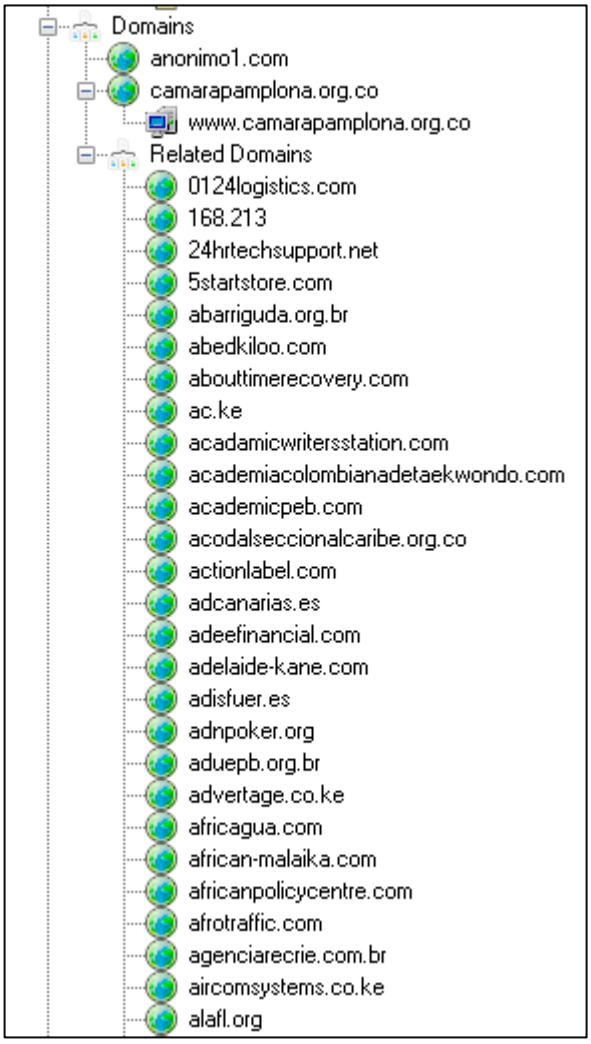
Figura 13. Servidores encontrados



Fuente: El autor

Se encuentra un listado con los dominios con los que ha tenido relación el Servidor.

Figura 14. Lista de Dominios relacionados con el Servidor



Fuente: El autor

Lista completa de los dominios:

anonimo1.com
camarapamplona.org.co
www.camarapamplona.org.co
Related Domains
0124logistics.com
168.213
24hrtechsupport.net
5startstore.com
abarriguda.org.br
abedkiloo.com
abouttimerecovery.com
ac.ke
acadamicwritersstation.com
academiacolombianadetaekwondo.com
academicpeb.com
acodalseccionalcaribe.org.co
actionlabel.com
adcanarias.es
adeefinancial.com
adelaide-kane.com
adisfuer.es
adnpoker.org
aduepb.org.br
advertage.co.ke
africagua.com
african-malaika.com
africanpolicycentre.com
afrotraffic.com
agenciarecrie.com.br
aircomsystems.co.ke
alafl.org
algominetech.co.ke
allegrocasamusical.com
allinongold.com

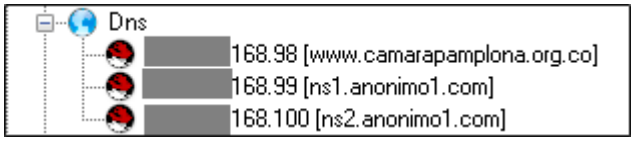
alonsofotografia.com
altagracia.es
altavistafuerteventura.com
alujansoberlivinghomes.com
alyciadebnamcarey.com
amas.co.ke
amcremodelingco.com
anamariarezkrezk.com
anaphilaxys10.net
anaphylaxis10.com
anonimo1.com
apiariolaesperanza.com.co
apnf.com.br
appletreeseries.com
aptoproperties.com
aptoschiropractor.com
aptotest.com
aquamarinebw.com
aramacaoporcolombia.com
ark-tents.com
artedecorativopinares.com
artesaniamaderafuerteventura.com
artlight.co.ke
asonlife.com.co
atfirst.co.ke
atshu.org
autosportbodyworks.com
autotallerlaantigua.com
autotallerlaantigua.es
avansis.com.co
avvygroup.com
axlr8.co.ke
beancity.co.ke
bellegroup.es
besteczemaremedies.com
betterpoolservices.com
biginsurancefraud.com
billgarten.com
bimotos.com
blackriverhealth.org
blchapaypintura.com
bonnieparkerinteriors.com
boomerangrent.com
breathe-africa.com
budachambertx.com
buyusessays.com
cabanaanna.com
cabotinvestments.com
cakebows.com
cakevilla.co.ke
camarafuerteventura.org
camarapamplona.org.co
campbrick.net
campinaimoveis.com.br
capecodcoverings.com
cargoplanmovers.co.ke
caribbeanfrp.com
carneslahacienda.com
cauchosygomas.com
cbhoustonrealestate.com
cdfiltros.com.br
cecconic.com.br
centralcaliforniarehab.com
centrionstaffingsolutions.com
centroeducacionalmoderno.com.br
certifiedslings.com
cflautos.com
charlestonharbortours.net
chcapital.mx
chepthemovie.com
cheruiyotecosystem.com
chgcontabil.com.br
chicagogreenhab.com
childrenscornerofwilmingtonnc.com
chocolatesrivera.com
chukaunicu.org
chunchuwala.com
ciedso.org
cirugiaplasticasanrafael.com
citizenparticipationinsecurity.org
cityhouseinm.com
ciunoa.com
classicafricantours.com
clean4health.com
clearvapors.com
clickplus.net
clinicadelacne.co
clinicadentaltezonco.com
club.org.mx
clubdeindustriales.org.mx
co.ke
co.uk
colaborar.org.co
com.br
com.co
com.mx
comoensucasa.com
compucelibague.com
concordialegal.net
construclay.com.br
cooperas.com.co
corounidotenerife.org
correodelanochebogotasabana.com
cotelcobogota.com
cozycottagesvt.com
cpt.org.co
cribb.com.br
criweb.net.br
criwebhost.com.br
crossairservice.com
crosscenturydiscounts.co.ke
crossfirenc.com
crystalbuildingsystems.co.ke
curtisjohnston.com
dafinaconsultants.co.ke
dalanews.com
danielle-panabaker.com
datalabsoftware.com
daystarinstituteafrica.org
ddayeventos.com
debracolombia.org
delmorediversified.com
denalimountainworks.com
dentistryatthepark.com
deportetolimense.com
destinyisaacbundi.com
dietasin.com
digitalferrer.com
dijitohomeenterprises.co.ke
disfarmed.com.co
distrilifecolombia.com
distrivalvulas.com
djstardachamp.com
dlc.co.ke
doctorsbroker.com
doctorsvaluation.com
dodoworld.com
dolficode.com
dollhousestripclub.com
donfullerinsurance.com
doz.com.co
drguillermorojas.com
drumhorseassociation.com
eavchgold.com
eco.br
ecomontana.com.co
edgemagazine.co.ke
edificiodiariodelotun.com
edu.co
educationnews.co.ke
edumotos.es
ejcarpetcleaning.com
elandcrackertours.com
elasecomodas.com.br
eldonvillas.com
elegantcakery.com
eletroluz.com.br
elkinospinanumerologia.com
emadskate.com
embracedkurves.com
emparnat.com
empirefoods.com
epiceventsmgt.co.ke
ersnellroofing.com
escaladaserramar.com.br
esomake.co.ke
esquire.com.co
eventosdelcafe.com
executta.com
exiletattoo.net
exploretoursandtravel.com
extremeboyz.com
faaliyaha24.com
fairwaysafaris.com
falcaolocacoes.com
fandaco.com
fandgcargo.com
fansitegalleries.com
farmaciadermosalud.com
fashionbrandmarketing.com
fashionstylemogul.com
fasrokenya.org
fcxphotography.com
felicityjones.us
felixmaiko.com
fencycurtains.com
fesbalimited.com
fichuzi.com
financeinwords.com
firtsdiesel.com
floridalegion.org
fobaccounting.com
foreverlivingproductskenya.co.ke
forrestglick.com
foundationofhealingandcaring.org
foxpanda.com
frikinoticias.com
fuencalientevisiondefuturo.com
fuencalientevisiondefuturo.es
fuertehost.com
fuerteventuratarfaya.com
fullblownautomotiverepair.com
fundaciondivinaeucaristia.org
fundaciontedeum.org
funkydeco.co.ke
futuregrad.com
gakuyorealestate.co.ke
galaxysystems.co.ke
garymoffatt.com
gaybondagemodeling.com
gaypornmodeling.com
gddassociates.com
generaciondelcambio.com
generationtechnologies.co.ke
georginaecheverria.com
gestaoterapia.com.br
gestarch.com
getmarriednc.com
giksecurity.com
glasseyedesign.net
gloads.com.br
globalmusicpool.com
gloshelter.com
gocryofit.com
goldenpearlcommunications.com
gomasycauchos.com
gossipmouthpiece.com
graduatefarmer.co.ke
grcitconsulting.com
greatfulsafaris.com
gridbranding.co.ke
gru-mex.com
gsmibague.com
guardauto.es
guitarjax.com
gustavorinconacore2016-2018.org
gygconsultinggroup.com
hak.com.br
happypeoplekenya.com
harubede.com.br
havencruiselines.com
heartofromania.com
hegranjalerida.org
hendersonvilleprivateinvestigator.com
hermosasmodeloscolombianas.com
hillhousehotel.co.ke
hmo-consultores.com
homefixt.com
homestarprotection.com
hostdime.com.br
hostland.com.br
hotelsiar.com
hotmail.com
hsentglobal.com
ht7.mx
hyperwings.com
icontec.org
idevelopertechnologies.co.ke
iem-sa.com
iglesiaevangelicatenerife.org
ihome.co.ke
iickenya.com
imovast.com.br
i-movies.co.ke
impropharma.co
impunidadcero.org
imultipla.com.br
inavigor.com
in-business.net
indicadores.org
infotelegraph.com
inoxidablesdominguez.com
institutoflordelotus.com.br
insurance-real-life.com
interiorsfu.com
interiorviewsstudio.com
int-optimum.com
inversa.com.co
invictafitness.com.br
ipic.co
ipsroadsafety.org
irevista.co
iscwilmington.org
ishacaasimada.com
iynac.org
jacobmacharia.com
jaimebuitrago.com
jaimegarzon.com
jardinbotanicosanjorge.org
jasoncarlsondds.com
javamy.co.ke
javimarubea.com
jayfm.org
jciproductionsinc.com
jeromeclaxton.com

jflmetalroofing.net
jimasudi.com
joheartyarns.com
josatronic.com
josatronics.com
jovesa.com.br
jrpublish.net
juanpablofranco.com
julianaimoveisnf.com
jungleartsandflora.com
jurassic-movies.com
kamukunjiyouths.org
katzaravamaria.com
kawe-kenya.org
kegeco.co.ke
kentexaed.com
kenyaoffershub.co.ke
keysgetaways.com
khenephanceltd.com
kijohphotography.com
kikisaacademy.com
knotsnblooms.com
kondomini.com.br
kountykonnect.com
lacarpafuerteventura.com
laultimadietadetuvida.com
lawyersattorney.org
lebedevesq.com
legacymotorsllc.com
lelcargas.com.br
letrudthtorque.com
lganimacion.com
liceobilinguecideb.com
liceolatinoamericano.edu.co
limurucheshirehome.org
linkvrs.com
liquidsmokevaporshop.com
logichomeinspections.com
lonjadeltolima.com.co
lovahcc.org
lyncentventures.com
maan-bile.com
maasaitrailseastafrica.com
macgriff.com
maggie.mx
mamamiasonline.net
mammadssmokehouse.com
managecom.co.ke
manduk.co.ke
margliv.com
marurahospital.co.ke
masomoportal.co.ke
matemagicas.co
maternalyjicucli.com
maxgolfperformance.com
mdec-sd.com
medianorth.co.ke
melissabenoistsource.com
mellitadistributorsltd.com
menezesandpartners.com
mercymax.com
meshecoincubators.com
mexigastronom.com
mexpayonline.com
mexplayonline.com
miguelsalazarnumerologia.net
milhanaccesscapital.com
millicentmugadi.com
misioncristianamoderna.com
misioncristianamoderna.org
misionmoderna.com
mnousa.com
moiprimaryschoolthika.com
montanhacup.com.br
montanhasports.com.br
monteirorentacar.com.br
monthal.com.br
mosacco.com
mrgroup.com.br
mudancasergipana.com.br
mueblesdonbrico.com
mueblesjhonny.com
muestramed.com
mukisacco.co.ke
multilabsystems.com
multiplacultural.com.br
mumincaraudio.co.ke
mundoimagenes10.com
murinaco.com
muryadventure.com.br
museodearteabstracto.com
museodeartedeltolima.com
museodeartedeltolima.org
mwalimutech.com
mwananchisupermarket.com
mydistrictattorney.com
myellacampaign.com
myinimini.com
naibiz.com
nairobass.com
nairobiselfdrive.com
ncftpc.com
net.br
nhpo.us
nigol.co.uk
nilm.org
nonnaginas.com
normasgraficas.com
novaindustriesltd.com
novarexofficial.com
npi.co.ke
nutrifit.co.ke
nutriflex.co.ke
oakislandnc.biz
oceanislevacations.net
onemassmedia.com
onspot.co.ke
opusau.com.br
or.ke
ordenatech.com
ordenatech.es
org.br
org.co
org.mx
orlandoautoupholstery.com
osabuena.com
ourwhitehouse.org
owagaadvocates.com
paintballnc.com
paintherapywilmington.com
palaciodedios.com
palaciodedios.org
pannapomodoro.com
paradisecanarias.com
paradisefuerteventura.com
passarosdefriburgo.com.br
patacon.com.co
pei-sas.com
personalizedtoursandsafaris.com
pharmacybrokers.com
phfamsafrica.co.ke
phowadsolution.com
pielarte.com
piso3asistencia.com
playlife.co
plusplustutoring.com
pointzerocoffee.com
politecnicoamericano.edu.co
portaldelmimbre.com.co
portium.com.br
portiumhost.com
pousadaartedeviver.com.br
praisecentermbale.org
preferredsecurityoh.com
primepropertyclub.com
primewave-logistics.com
privatedanceryachtcharters.com
productosgourmetdelmar.com
propertykalli.co.ke
proroot.co.ke
protea.edu.co
proveaire.com
proyectoagro.com
publicidad247.com
qtroent.com
questqualitycleaners.com
quickpharmacy.co
quintadacolina.com.br
quintetoclasico.com
quirkyville.com
rachels.com
radiodigitalamerica.com
radiointeractiva.com
ramiroparias.com
rampapublicidad.com
razorbackoutfitters.com
rcsk8.com
rectificadoramoderna.net
redesuperlegaldesupermercados.com
redesuperlegaleshow.com.br
refugiolaesperanza.com
rejuvenecimientocolombia.com
remymotorsltd.co.ke
reneeanduze.com
reneesoya.com
rent-a-dude.com
reproductivelawsolutions.com
resortjumuia.com
restaurantelamarquesina.com
restaurantetiobernabe.com
restaurantetiobernabe.es
revistacomercioexterior.com
revistadigital.co
revistaeventus.com.br
riayngroup.com
ricdzgn.com
ricky-tech.com
riverwoodveterinaryclinic.com
rk7agencia.net
rockspirit.es
romaccointegratedservices.com
rootkenya.co.ke
rough2refinedgemstones.com
rustylung.com
rzinfo.com.br
sacredgcollective.com
sad.com.co
samchi.co.ke
samosafestival.com
samucomtrading.com
sanboni.edu.co
sandraorjuelacordoba.com
saranik.com
sarcemholding.co.ke
satelittex.com
scnf.org.br
screencapped.net
screencapped.org
seasalesliquidation.com
secrpay.com
serradosilicio.com.br
servicios.in
sharpimagecreative.co.ke
sheppardfirm.com
shupav.com
signaturedevelopers.co.ke
silcapital.co.ke
silmiyahbey13.com
simbapakasafaris.com
simitechnologies.co.ke
sirensensorusa.com
sirfelo.co.ke
skyboundconstructions.com
smartgroupproperties.com
smartinvestor.co.ke
smashthroughlimits.com
smileandstile.org
snickersdirect.be
snickersdirect.co.uk
snickersdirect.com
snickersdirect.ie
snickersdirect.it
snickersdirect.ru
social-bit.com
sokotrip.co.ke
solidaridadporcolombia.org
solubox.com.mx
sommerpropertyinvestments.com
sonrident.com
sorcihomesolutions.com
spiralheights.com
splashme.com
sportpesafestival.com
starcardsindia.com
starcomss.co.ke
starsorlando.com
sternideas.co.ke
stim.com.br
storyofmylife.co.ke
structuredsettlementguide.org
styllussemijoias.com.br
sunrayswebcreations.com
sunstarhotelnairobi.com
surfschulefuerteventura.net
surfshopfuerteventura.com
sustainableeconomicdev.org
swchost.com
sweetwatertexas.org
tahiyagroup.com
taichifuerteventura.com
taikansecurity.com
talstales.com
tamacc.org
tarfayaexpress.com
teamsmart.cc
teatrolobatinho.com.br
tec-innovation.co.ke
tenerfe.info
tenerfe.net
tenerfe.org
teresasvacationrentals.com
testdemetabolismo.com
thebeautyofregret.com
thecodepot.com
thecorporate-weekly.com
thegreatpelicanlodge.com
thekenyanoline.com
themadartist.org
thencbla.org
thepoolstoreoflemongrove.com
thepriceisrightasheville.com
thesaharan.com
thesellgroup.com
thetreesrvpark.com
threadocs.com
tiendadelmotero.com

tiffsenterprise.com
tingcreations.co.ke
titcolombia.com
titecnologiainformatica.com
topqc.com
topvideoshd.xyz
torrescapacita.mx
torresdesign.mx
torresdesignmexico.com
touchofglassusa.com
touristhotelbungoma.com
travel-with-pulse.com
tridentcolleges.org
triplecreativity.co.ke
triplerenterprises.org
trueroadtz.com
tsartistry.com
turismovacaciones.co
tusmotraveltours.com
tuviajehoy.com
tvmagharibi.com
uexternado.co
uniformeslanaval.com.mx
uniquetracking.co.ke
unitycollegeofprofessionalstudies.com
vashnaroses.com
verdeaurora.com
viandvi.mx
vicodec.org
victorbinge.com
victorpeace.com
viromed-ea.com
vivirbien.org.mx
vmecotravel.co.ke
wallacenart.com
walshchicagoplumbing.com
websiteduka.co.ke
westerninternationalsecurityservice.com
windycityrooter.com
winesroutelimited.com
wisephyk.co.ke
worktic.com.co
yarnsofwilmington.com
yogaatladaka.com
yourdreamgadget.com
yvonnedavid.com
zelareimoveis.com.br

Se encontraron 3 direcciones DNS

Figura 15. DNS encontrados

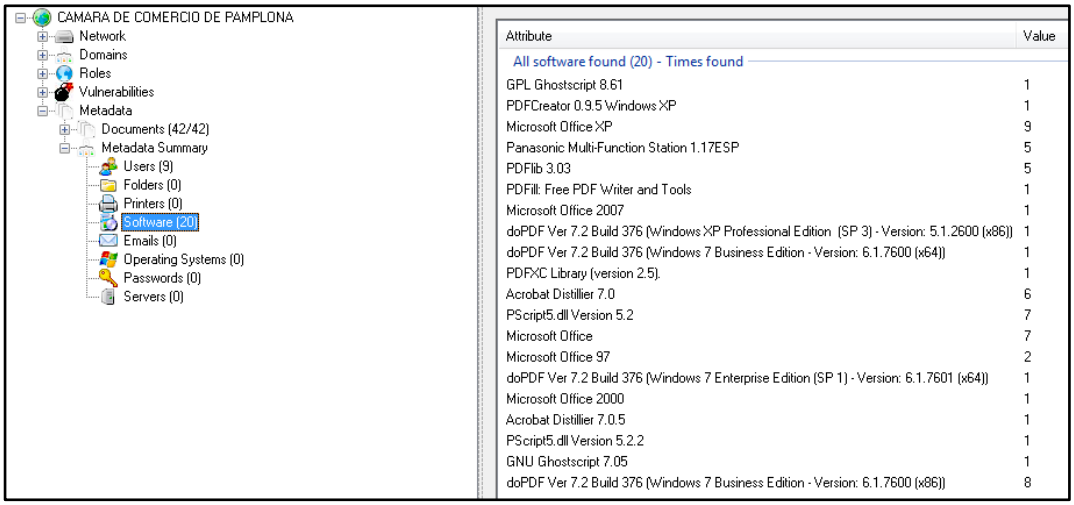


Fuente: El autor

7.1.1.3 Software

Se ha encontrado información de 20 tipos de Software, que se relacionan con los documentos.

Figura 16. Software encontrado relacionado con los documentos



Fuente: El autor

7.1.2 Descarga de archivos, extracción y análisis de metadatos de la Alcaldía de Pamplona. URL: http://pamplona-nortedesantander.gov.co

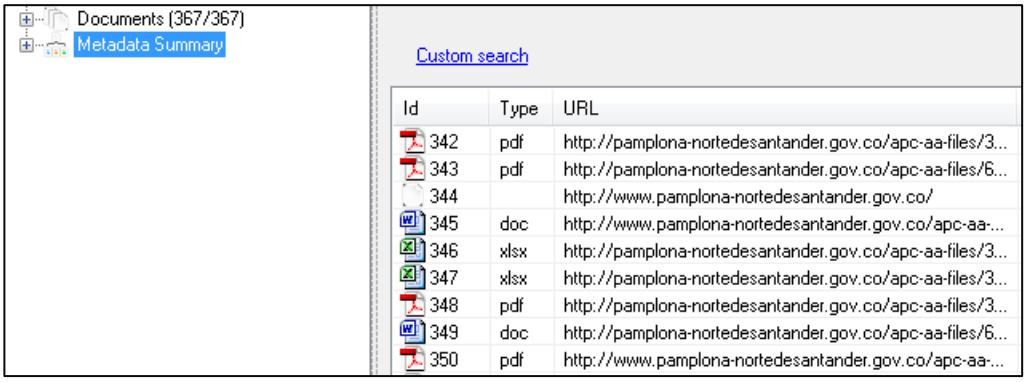
Se realizan los mismos pasos del proyecto anterior.

Figura 17. Creación del Proyecto análisis de metadatos de http://pamplona-nortedesantander.gov.co

Fuente: El autor

Utilizando los Buscadores Google, Bing, Exalead, FOCA encuentra 367 documentos públicos, clasificados de la siguiente manera por tipo de archivo:

Figura 18. Búsqueda de Documentos Públicos http://pamplona-nortedesantander.gov.co



Fuente: El autor

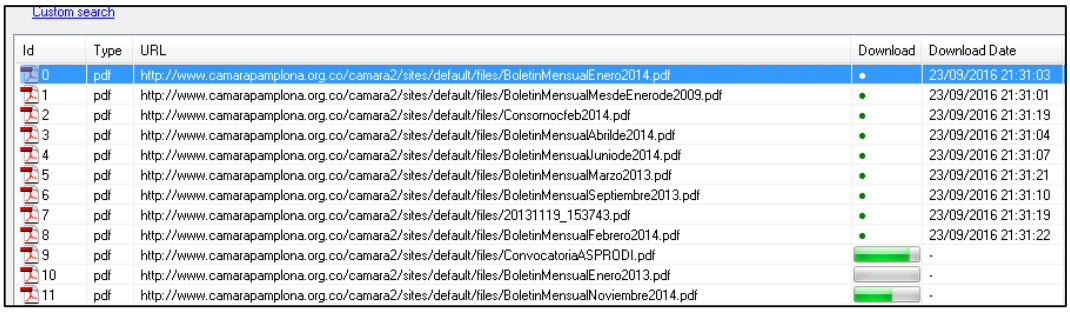
Tabla 2. Documentos Públicos encontrados en http://pamplona-nortedesantander.gov.co

Cantidad	Tipo de Archivo
310	.pdf
37	.doc
10	.docx
4	.ppt
1	.pptx
1	.xls
3	.xlsx
1	Desconocido
367	**Total**

Fuente: El autor

Se procede a descargar los archivos encontrados en la URL (Solo 87 se lograron descargar en total).

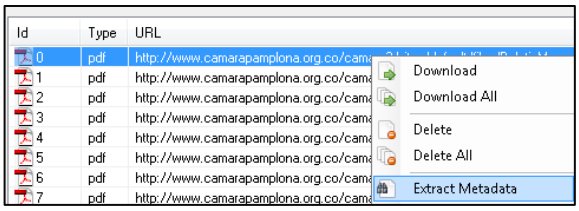
Figura 19. Descarga de los archivos públicos encontrados en http://pamplona-nortedesantander.gov.co



Fuente: El autor

Posteriormente se extraen los metadatos de todos los archivos.

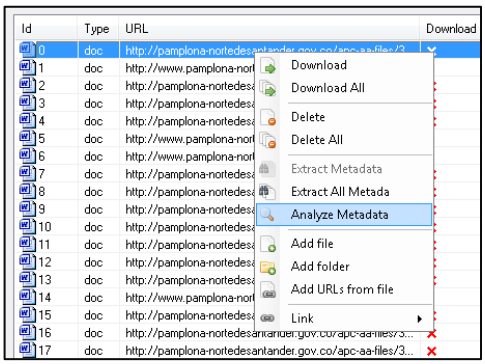
Figura 20. Extracción de metadatos de los archivos públicos descargados de http://pamplona-nortedesantander.gov.co



Fuente: El autor

El siguiente paso es analizar los metadatos de todos los archivos públicos descargados.

Figura 21. Análisis de todos los metadatos



Fuente: El autor

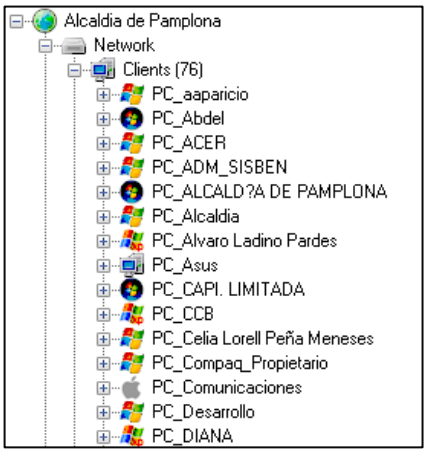
7.1.2.1 Resultado del análisis de los metadatos

Después del análisis de los metadatos realizado por FOCA a los 42 documentos públicos descargados de la URL: http://pamplona-nortedesantander.gov.co, se obtuvieron los siguientes resultados:

7.1.2.2 Red

Se encontró información de 76 usuarios cliente que tienen acceso al sistema.

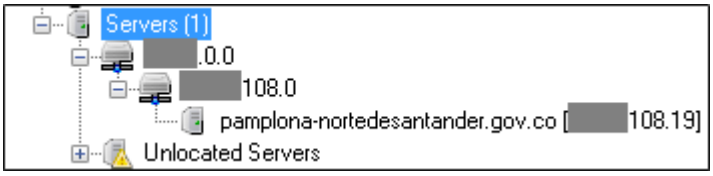
Figura 22. Usuarios cliente encontrados



Fuente: El autor

Se encontró información de 1 Servidor (190.7.0.0), que pertenece a la red informática, en la IP: 138.128.168.99 se observan URL's a las cuales se ha ingresado desde ese servidor

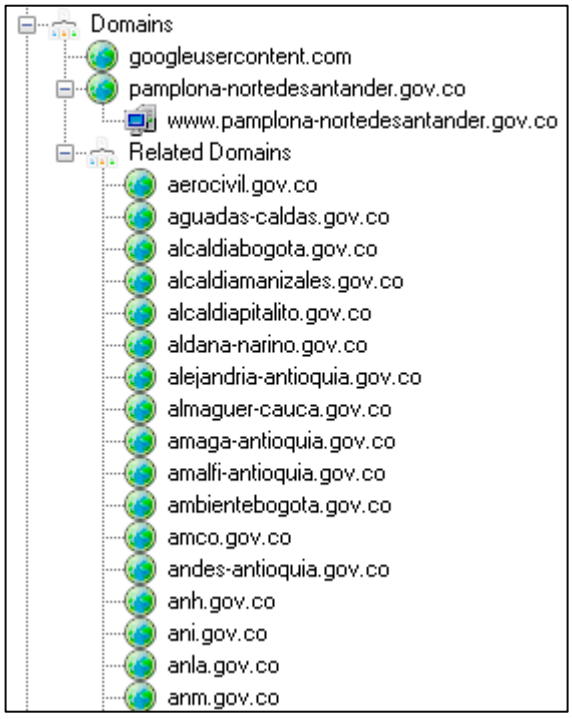
Figura 23. Servidor localizado



Fuente: El autor

Se encuentra un listado de urls con dominios con los que ha tenido relación el Servidor.

Figura 24. Lista de Dominios relacionados con el Servidor



Fuente: El autor

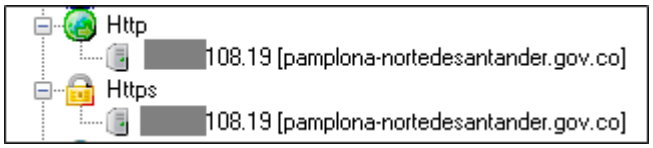
Lista completa de los dominios:

aerocivil.gov.co
aguadas-caldas.gov.co
alcaldiabogota.gov.co
alcaldiamanizales.gov.co
aldana-narino.gov.co
alejandria-antioquia.gov.co
almaguer-cauca.gov.co
amaga-antioquia.gov.co
amalfi-antioquia.gov.co
ambientebogota.gov.co
amco.gov.co
andes-antioquia.gov.co
anh.gov.co
ani.gov.co
anla.gov.co
anm.gov.co
antioquia.gov.co
anza-antioquia.gov.co
apccolombia.gov.co
atlantico.gov.co
bancadelasoportunidades.gov.co
bancoagrario.gov.co
bancoldex.gov.co
banrep.gov.co
barbosa-santander.gov.co
barranquilla.gov.co
belen-narino.gov.co
betulia-antioquia.gov.co
biblored.gov.co
bogota.gov.co
bogotaturismo.gov.co
bucaramanga.gov.co
cali.gov.co
camara.gov.co
canalcapital.gov.co
cancilleria.gov.co
car.gov.co
carder.gov.co
cardique.gov.co
caroycuervo.gov.co
cartagena.gov.co
cco.gov.co
centrodememoriahistorica.gov.co
chigorodo-antioquia.gov.co
chima-santander.gov.co
chip.gov.co
choachi-cundinamarca.gov.co
choco.gov.co
cna.gov.co
cne.gov.co
cnsc.gov.co
colciencias.gov.co
coljuegos.gov.co
colpensiones.gov.co
comisionseptimasenado.gov.co
conalpe.gov.co
concejodecali.gov.co
concejodeibague.gov.co
concejo-raquira-boyaca.gov.co
conciliacion.gov.co
concursouniversitarioddhh.gov.co
consulado.gov.co
contaduria.gov.co
contraloriabogota.gov.co
contraloriagen.gov.co
contraloriameta.gov.co
contraloriavalledelcauca.gov.co
contratacionbogota.gov.co
contratos.gov.co
copacabana.gov.co
corantioquia.gov.co
cordoba.gov.co
cornare.gov.co
corponarino.gov.co
corponor.gov.co
corteconstitucional.gov.co
cortolima.gov.co
cpae.gov.co
cra.gov.co
crautonoma.gov.co
crc.gov.co
crcom.gov.co
creg.gov.co
crq.gov.co
culturantioquia.gov.co
culturarecreacionydeporte.gov.co
cundinamarca.gov.co
dadiscartagena.gov.co
dafp.gov.co
dane.gov.co
defensoria.gov.co
dian.gov.co
dlspereira.gov.co
dnp.gov.co
dssa.gov.co
duitama-boyaca.gov.co
durania-nortedesantander.gov.co
educacioninicialtolima.gov.co
elzulia-nortedesantander.gov.co
empitalito.gov.co
enjambre.gov.co
envigado.gov.co
eru.gov.co
esecerrosanantonio.gov.co
esechdntumaco.gov.co
eselavirginia.gov.co
esenuevocolonboyaca.gov.co
eserafaeluribe.gov.co
esesantaclara.gov.co
esesuba.gov.co
esetitiribi.gov.co
espasantamarta.gov.co
findeter.gov.co
floresta-boyaca.gov.co
fogafin.gov.co
fonade.gov.co
fondoadaptacion.gov.co
funcionpublica.gov.co
funes-narino.gov.co
gama-cundinamarca.gov.co
genova-quindio.gov.co
gestiondelriesgo.gov.co
girardota.gov.co
giron-santander.gov.co
gobiernobogota.gov.co
gobiernoenlinea.gov.co
gov.co
guayabaldesiquima-cundinamarca.gov.co
guepsa-santander.gov.co
haplmanaure.gov.co
hflleras.gov.co
hospitalgigante.gov.co
hospitalmanuelabeltran.gov.co
hospitalsanandresese.gov.co
hospitalsanjose.gov.co
hospitalsuesca.gov.co
hospitalsur.gov.co
hrplopez.gov.co
huila.gov.co
ibague.gov.co
ica.gov.co
icbf.gov.co
icetex.gov.co
icfes.gov.co
icfesinteractivo.gov.co
idartes.gov.co
ideam.gov.co
idermeta.gov.co
idpc.gov.co
idrd.gov.co
idu.gov.co
igac.gov.co
imdri.gov.co
incoder.gov.co
indeportesantioquia.gov.co
inder.gov.co
inderba.gov.co
indersantander.gov.co
inpec.gov.co
ins.gov.co
insor.gov.co
integracionsocial.gov.co
invima.gov.co
ipes.gov.co
juegosdelvalle.gov.co
juegosfuncionpublica.gov.co
labateca-nortedesantander.gov.co
lapaz-santander.gov.co
lasceibas.gov.co
magangue-bolivar.gov.co
manizales.gov.co
medellin.gov.co
megabus.gov.co
metropol.gov.co
metrosabanas.gov.co
metrovivienda.gov.co
migracioncolombia.gov.co
minagricultura.gov.co
minambiente.gov.co
mincit.gov.co
mincultura.gov.co
mindefensa.gov.co
mineducacion.gov.co
minhacienda.gov.co
mininterior.gov.co
minminas.gov.co
minproteccionsocial.gov.co
minsalud.gov.co
mintic.gov.co
mintransporte.gov.co
minvivienda.gov.co
modernizacionsecretarias.gov.co
moniquira-boyaca.gov.co
neira-caldas.gov.co
nemocon-cundinamarca.gov.co
onsm.gov.co
parquesnacionales.gov.co
participacionbogota.gov.co
personeriarmenia.gov.co
policarpa-narino.gov.co
policia.gov.co
popayan.gov.co
popayan-cauca.gov.co
portalmaritimocolombiano.gov.co
positiva.gov.co
presidencia.gov.co
procuraduria.gov.co
puertogaitan-meta.gov.co
puertorico-meta.gov.co
quindio.gov.co
ramajudicial.gov.co
redempleo.gov.co
registraduria.gov.co
reintegracion.gov.co
risaralda.gov.co
rivera-huila.gov.co
saludcapital.gov.co
sanandres.gov.co
sanandres-santander.gov.co
sancristobal-bolivar.gov.co
sanjeronimo-antioquia.gov.co
sanjosedelguaviare-guaviare.gov.co
sanluis-antioquia.gov.co
santacruzdelorica-cordoba.gov.co
santahelenadelopon-santander.gov.co
santamargarita.gov.co
santamaria-huila.gov.co
santander.gov.co
satena.gov.co
sdmujer.gov.co
sdp.gov.co
secretariasenado.gov.co
sedbarranquilla.gov.co
sedbolivar.gov.co
sedboyaca.gov.co
sedcaqueta.gov.co
sedcartagena.gov.co
sedcasanare.gov.co
sedcauca.gov.co
sedguajira.gov.co
sedmagdalena.gov.co
sednarino.gov.co
sednortedesantander.gov.co
sedquindio.gov.co
seduca.gov.co
semduitama.gov.co
semgiron.gov.co
semitagui.gov.co
sempalmira.gov.co
sempopayan.gov.co
serviciocivil.gov.co
sgr.gov.co
shd.gov.co
si3ea.gov.co
sic.gov.co
sire.gov.co
sistemamatriculas.gov.co
sitp.gov.co
sonson-antioquia.gov.co
ssf.gov.co
suan-atlantico.gov.co
sucre.gov.co
superfinanciera.gov.co
supernotariado.gov.co
superservicios.gov.co
supersociedades.gov.co
supersolidaria.gov.co
supertransporte.gov.co
supervigilancia.gov.co
tabio-cundinamarca.gov.co
tlc.gov.co
tolima.gov.co
toro-valle.gov.co
transcaribe.gov.co
transitoarmenia.gov.co
transitobarrancabermeja.gov.co

transitopereira.gov.co	tribunalsuperiorarmenia.gov.c	umv.gov.co	valledelcauca.gov.co
transmilenio.gov.co	o	unidadvictimas.gov.co	veeduriadistrital.gov.co
transparenciabogota.gov.co	uaesp.gov.co	upme.gov.co	versalles-valle.gov.co
	umng.gov.co	upra.gov.co	villarica-cauca.gov.co

Se encontró una dirección de un servidor web, en donde se utilizan conexiones http y https.

Figura 25. IP Servidor WEB encontrado



Fuente: El autor

7.1.2.3 Software

Se ha encontrado información de 47 tipos de Software, que se relacionan con los documentos.

Figura 26. Software encontrado relacionado con los documentos

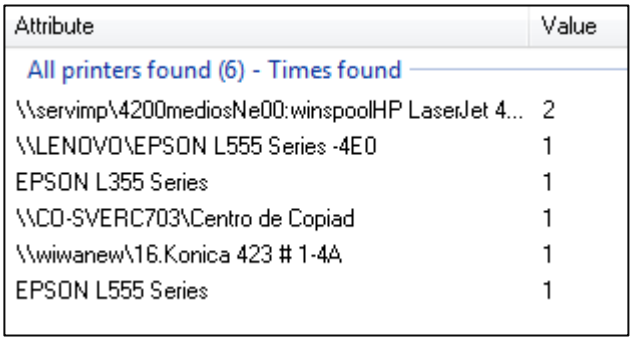
Attribute	Value
All software found (47) - Times found	
Microsoft Office 2007	117
Microsoft Office XP	51
Microsoft Office 2000	5
GPL Ghostscript 8.71	21
PDFCreator 1.0.1Windows	21
OpenOffice	2
Writer	4
LibreOffice 4.1	3
Microsoft Office	58
PScript5.dll Version 5.2	5
GPL Ghostscript 8.15	13
Acrobat Distillier 6.0	2
Acrobat Distillier 8.1.0	6
Microsoft Office 97	7
Calc	1

Fuente: El autor

7.1.2.4 Impresoras

Se encontraron 6 impresoras utilizadas

Figura 27. Impresoras encontradas



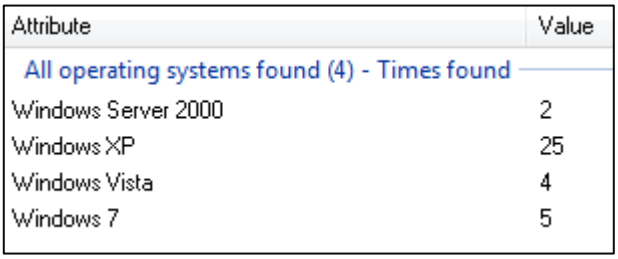
Attribute	Value
All printers found (6) - Times found	
\\servimp\4200mediosNe00:winspoolHP LaserJet 4...	2
\\LENOVO\EPSON L555 Series -4E0	1
EPSON L355 Series	1
\\CO-SVERC703\Centro de Copiad	1
\\wiwanew\16.Konica 423 # 1-4A	1
EPSON L555 Series	1

Fuente: El autor

7.1.2.5 Sistemas Operativos

Se encontraron 4 sistemas operativos utilizados.

Figura 28. Sistemas Operativos encontrados



Attribute	Value
All operating systems found (4) - Times found	
Windows Server 2000	2
Windows XP	25
Windows Vista	4
Windows 7	5

Fuente: El autor

7.1.3 Descarga de archivos, extracción y análisis de metadatos de la Gobernación de Norte de Santander. URL: http://www.nortedesantander.gov.co

Se realizan los mismos pasos del análisis anterior.

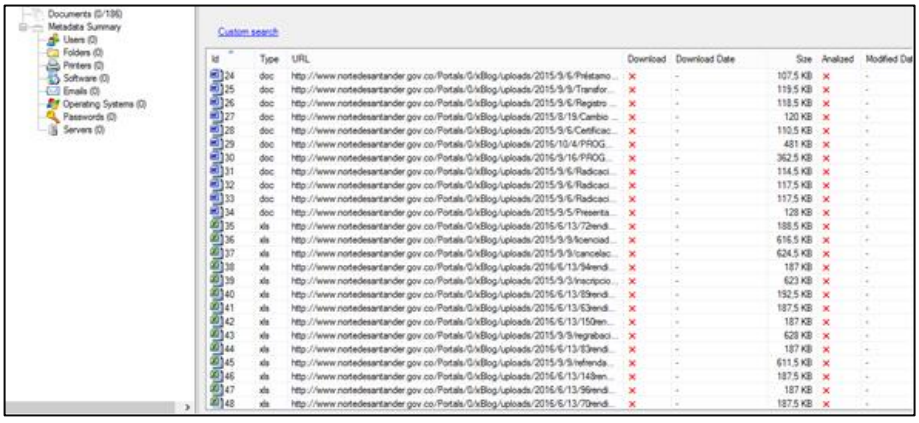
Figura 29. Creación del Proyecto análisis de metadatos de http://www.nortedesantander.gov.co

Figura 29. Creación del Proyecto análisis de metadatos de http://www.nortedesantander.gov.co

Fuente: El autor

Utilizando los Buscadores Google, Bing, Exalead, FOCA encuentra 186 documentos públicos, clasificados de la siguiente manera por tipo de archivo:

Figura 30. Búsqueda de Documentos Públicos http://www.nortedesantander.gov.co



Fuente: El autor

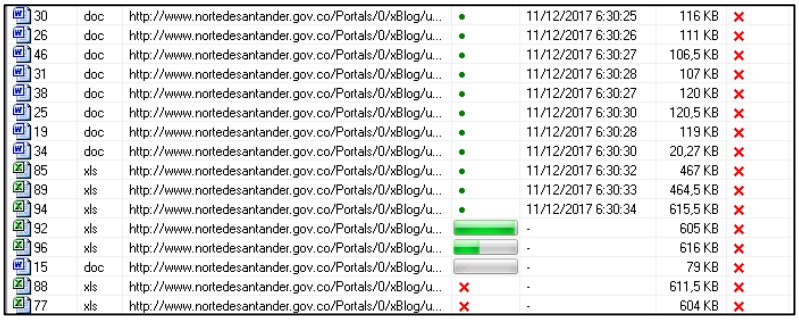
Tabla 3. Documentos Públicos encontrados en http://www.nortedesantander.gov.co

Cantidad	Tipo de Archivo
35	.doc
47	.xls
104	.pdf
186	**Total**

Fuente: El autor

Se procede a descargar los archivos encontrados en la URL.

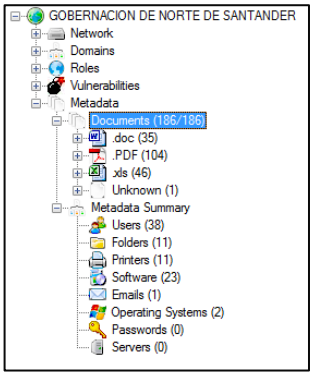
Figura 31. Descarga de los archivos públicos encontrados en http://www.nortedesantander.gov.co



Fuente: El autor

Posteriormente se extraen los metadatos de todos los archivos.

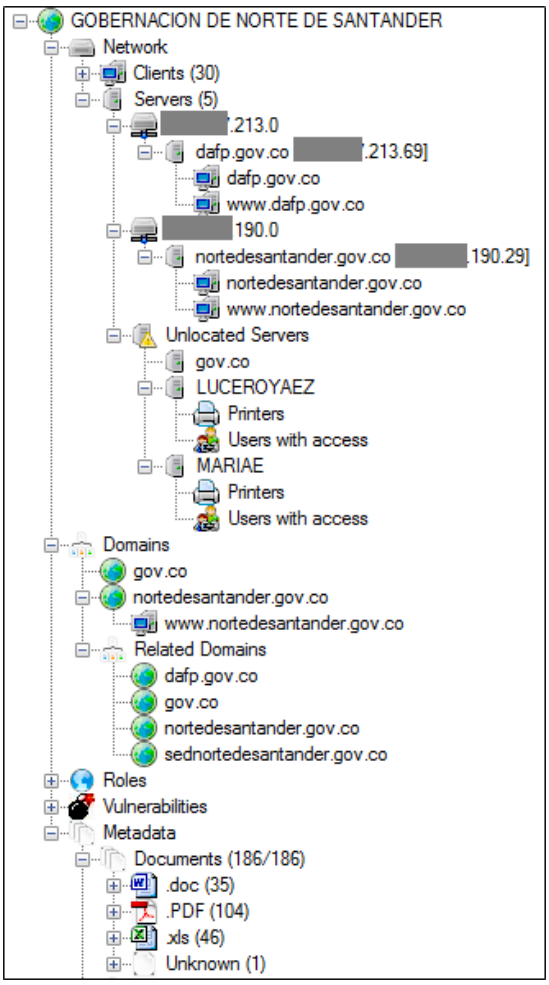
Figura 32. Extracción de metadatos de los archivos públicos descargados de http://www.nortedesantander.gov.co



Fuente: El autor

El siguiente paso es analizar los metadatos de todos los archivos públicos descargados.

Figura 33. Análisis de todos los metadatos



Fuente: El autor

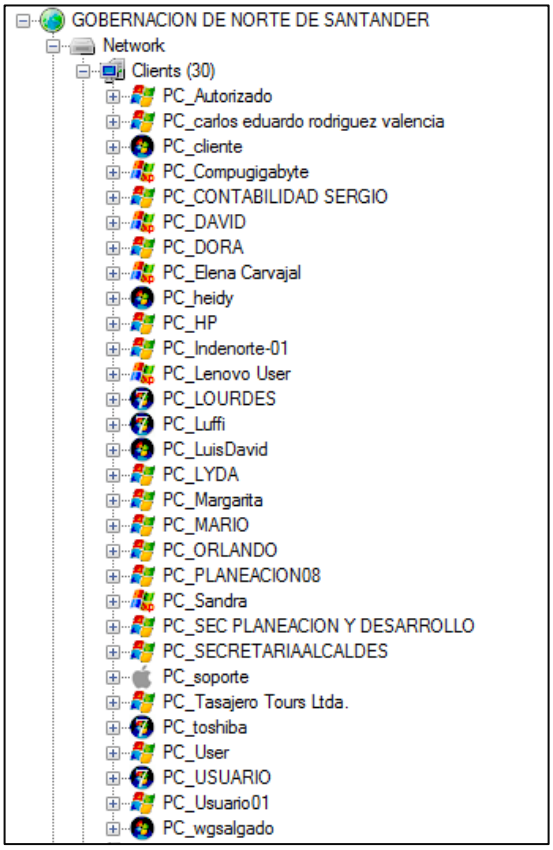
7.1.3.1 Resultado del análisis de los metadatos

Después del análisis de los metadatos realizado por FOCA a los 186 documentos públicos descargados de la URL: http://www.nortedesantander.gov.co, se obtuvieron los siguientes resultados:

7.1.3.2 Red

Se encontró información de 30 usuarios cliente que tienen acceso al sistema.

Figura 34. Usuarios cliente encontrados



Fuente: El autor

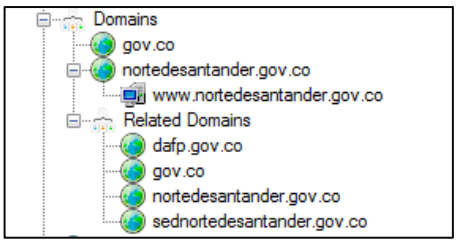
Se encontró información IP de 4 Servidores que pertenece a la red informática.

Figura 35. Servidores localizados

Fuente: El autor

Se encontraron los siguientes dominios:

Figura 36. Dominios relacionados con el Servidor



Fuente: El autor

Se encontró información de 10 impresoras utilizadas.

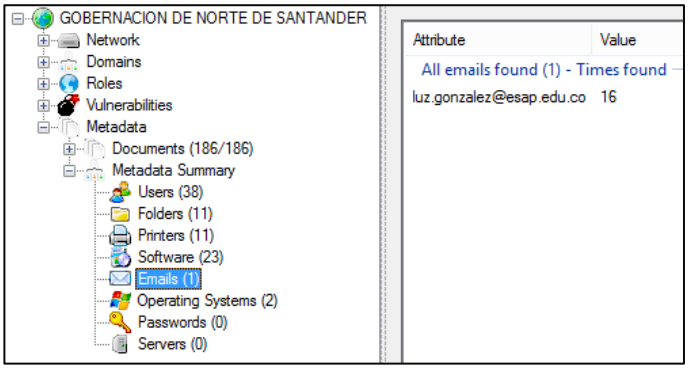
Figura 37. Impresoras encontradas

Attribute	Value
All printers found (10) - Times found	
Xerox Phaser 3435 PCL 6	3
Xerox Phaser 3425 PCL 6(0000F0	16
TinyPDF	5
PDF995	1
Kyocera Mita FS-1920 KX	25
hp LaserJet 1320 PCL 6 (1)	3
HP Deskjet 3050 J610 series	2
\\LUCEROYAEZ\Xerox Phaser 343	11
\\LUCEROYAEZ\Xerox Phaser 342	5
\\192.168.0.30\Samsung ML-1640	1

Fuente: El autor

Se encontró una dirección de correo electrónico.

Figura 38. Correo Electrónico encontrado

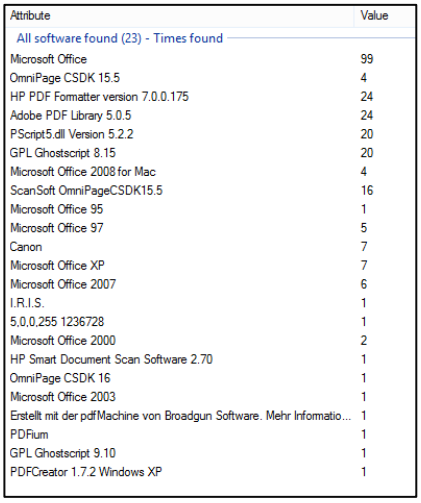


Fuente: El autor

7.1.3.3 Software

Se ha encontrado información de 23 tipos de Software, que se relacionan con los documentos.

Figura 39. Software encontrado relacionado con los documentos



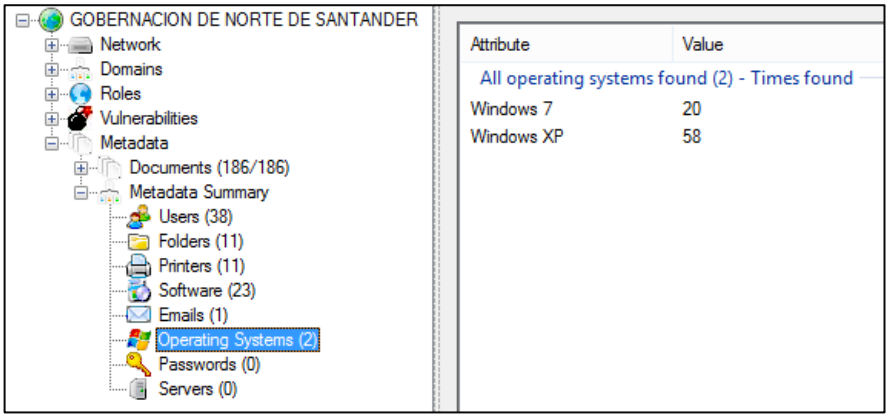
Attribute	Value
All software found (23) - Times found	
Microsoft Office	99
OmniPage CSDK 15.5	4
HP PDF Formatter version 7.0.0.175	24
Adobe PDF Library 5.0.5	24
PScript5.dll Version 5.2.2	20
GPL Ghostscript 8.15	20
Microsoft Office 2008 for Mac	4
ScanSoft OmniPageCSDK15.5	16
Microsoft Office 95	1
Microsoft Office 97	5
Canon	7
Microsoft Office XP	7
Microsoft Office 2007	6
I.R.I.S.	1
5,0,0,255 1236728	1
Microsoft Office 2000	2
HP Smart Document Scan Software 2.70	1
OmniPage CSDK 16	1
Microsoft Office 2003	1
Erstellt mit der pdfMachine von Broadgun Software. Mehr Informatio...	1
PDFium	1
GPL Ghostscript 9.10	1
PDFCreator 1.7.2 Windows XP	1

Fuente: El autor

7.1.3.4 Sistemas Operativos

Se hallaron 2 sistemas operativos utilizados.

Figura 40. Sistemas Operativos encontrados



Fuente: El autor

7.1.4 Descarga de archivos, extracción y análisis de metadatos del diario La Opinión de Cúcuta. URL: http://www.laopinion.com.co

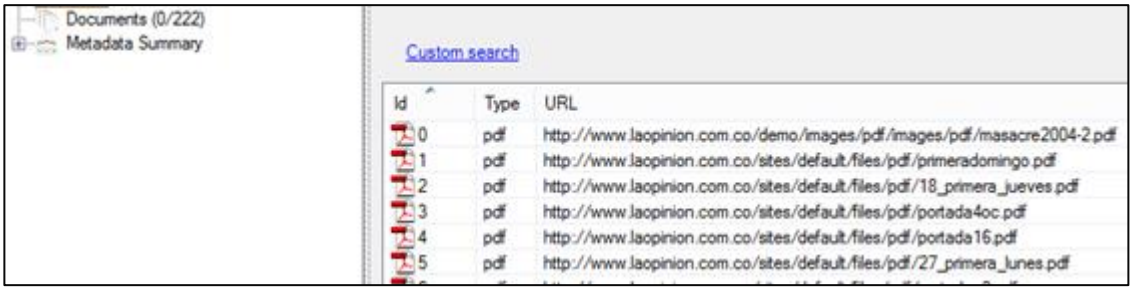
Se realizan los mismos pasos del análisis anterior.

Figura 41. Creación del Proyecto análisis de metadatos de http://www.laopinion.com.co

Fuente: El autor

Utilizando los Buscadores Google, Bing, Exalead, FOCA encuentra 222 documentos públicos, clasificados de la siguiente manera por tipo de archivo:

Figura 42. Búsqueda de Documentos Públicos http://www.laopinion.com.co



Fuente: El autor

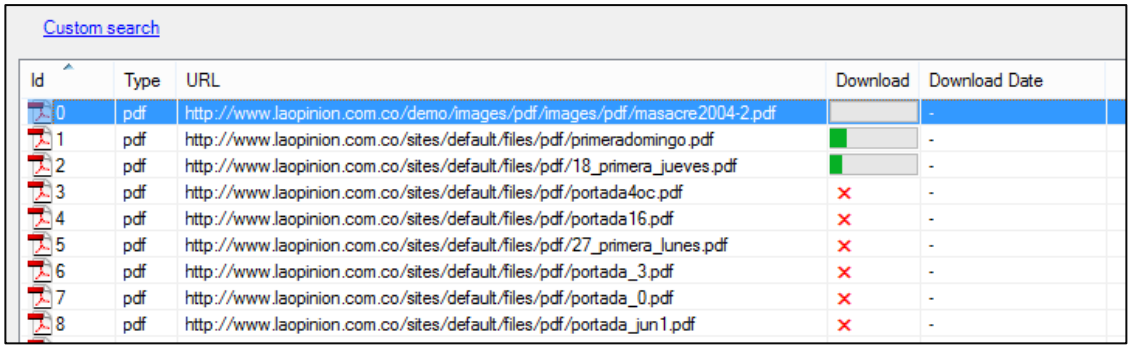
Tabla 4. Documentos Públicos encontrados en http://www.laopinion.com.co

Cantidad	Tipo de Archivo
221	.pdf
1	Desconocido
222	**Total**

Fuente: El autor

Se procede a descargar los archivos encontrados en la URL.

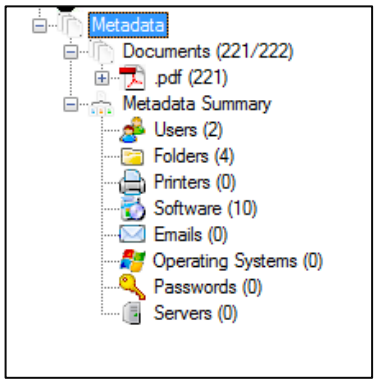
Figura 43. Descarga de los archivos públicos encontrados en http://www.laopinion.com.co



Fuente: El autor

Posteriormente se extraen los metadatos de todos los archivos.

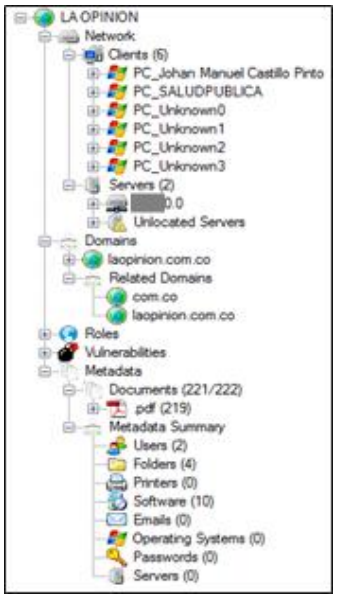
Figura 44. Descarga de los archivos públicos encontrados en http://www.laopinion.com.co



Fuente: El autor

El siguiente paso es analizar los metadatos de todos los archivos públicos descargados.

Figura 45. Análisis de todos los metadatos



Fuente: El autor

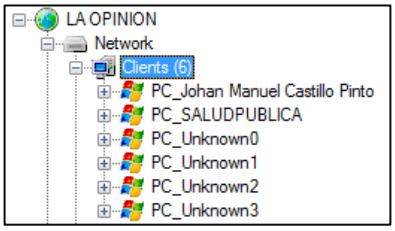
7.1.4.1 Resultado del análisis de los metadatos

Después del análisis de los metadatos realizado por FOCA a los 186 documentos públicos descargados de la URL: http://www.laopinion.com.co, se obtuvieron los siguientes resultados:

7.1.4.2 Red

Se encontró información de 6 usuarios cliente que tienen acceso al sistema.

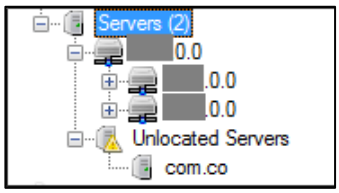
Figura 46. Usuarios cliente encontrados



Fuente: El autor

Se encontró información IP de 2 Servidores, que pertenece a la red informática.

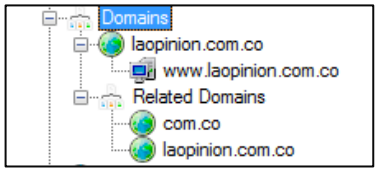
Figura 47. Servidores localizados



Fuente: El autor

Se encontraron los siguientes dominios:

Figura 48. Dominios relacionados con el Servidor

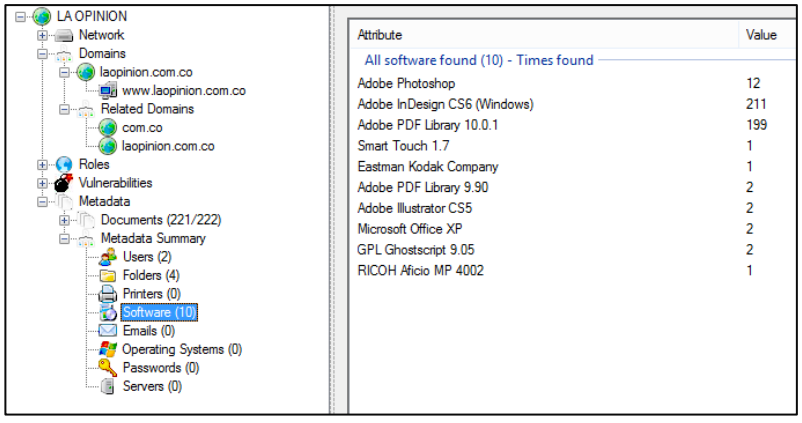


Fuente: El autor

7.1.4.3 Software

Se ha encontrado información de 10 tipos de Software, que se relacionan con los documentos.

Figura 49. Software encontrado relacionado con los documentos



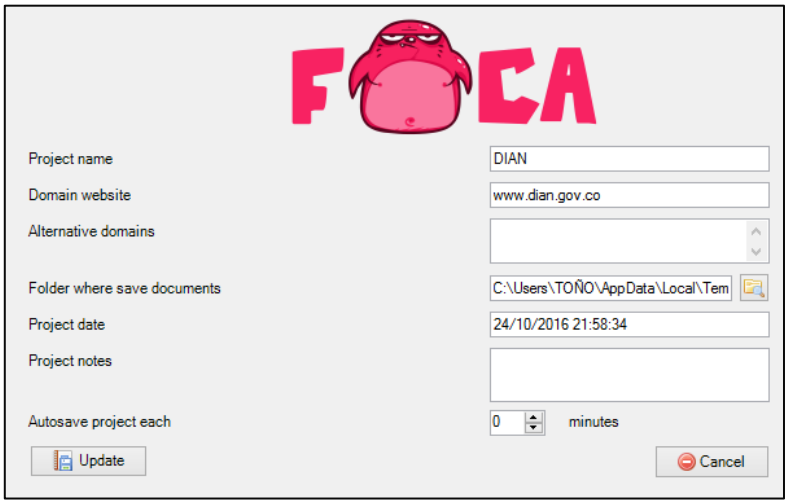
Fuente: El autor

7.1.5 Descarga de archivos, extracción y análisis de metadatos de la DIAN.

URL: http://www.dian.gov.co

Se realizan los mismos pasos del análisis anterior.

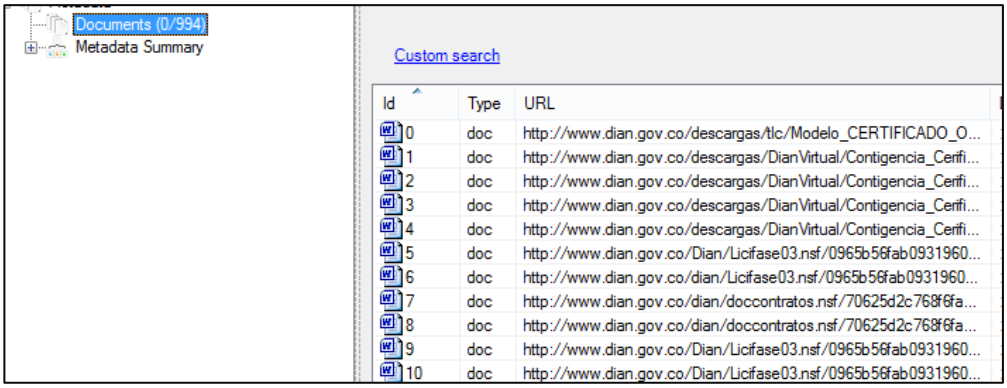
Figura 50. Creación del Proyecto análisis de metadatos de http://www.dian.gov.co



Fuente: El autor

Utilizando los Buscadores Google, Bing, Exalead, FOCA encuentra 994 documentos públicos, clasificados de la siguiente manera por tipo de archivo:

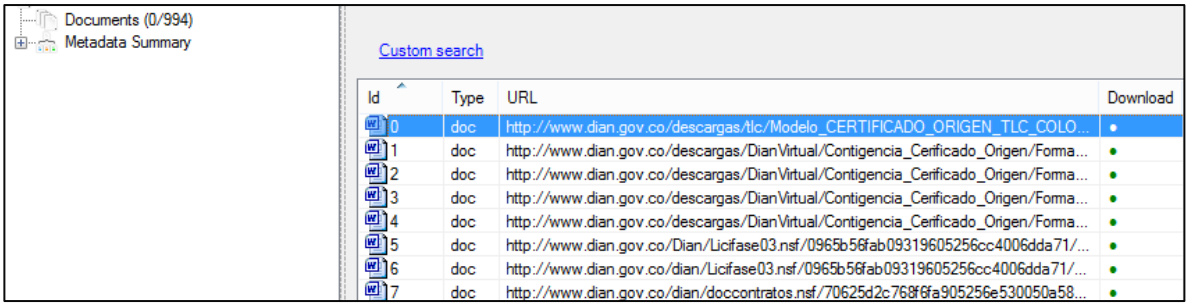
Figura 51. Búsqueda de Documentos Públicos http://www.dian.gov.co



Fuente: El autor

Se procede a descargar los archivos encontrados en la URL.

Figura 52. Descarga de los archivos públicos encontrados en http://www.dian.gov.co



Fuente: El autor

En total se descargaron 980 documentos:

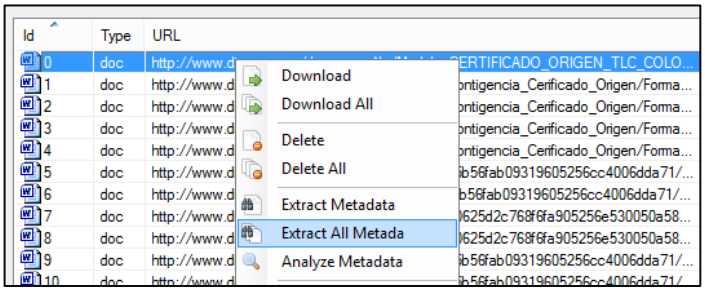
Tabla 5. Documentos Públicos encontrados en http://www.dian.gov.co

Cantidad	Tipo de Archivo
41	.doc
7	.docx
316	.xls
53	.xlsx
551	.dpf
1	.pps
1	.ppsx
4	.ppt
6	Desconocido
980	**Total**

Fuente: El autor

Posteriormente se extraen los metadatos de todos los archivos.

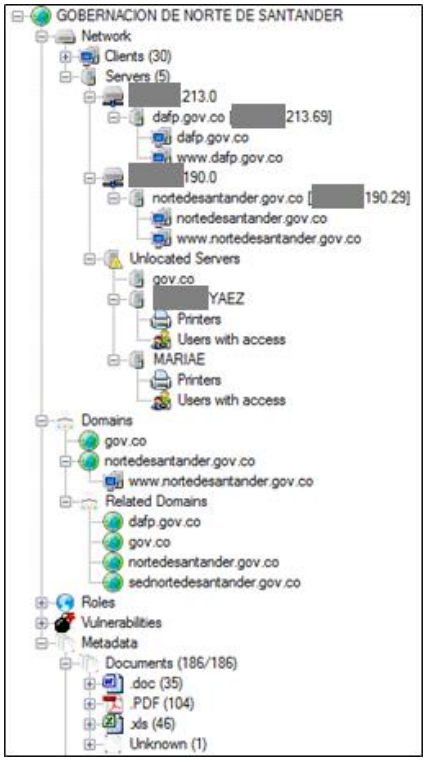
Figura 53. Extracción de metadatos de los archivos públicos descargados de http://www.dian.gov.co



Fuente: El autor

El siguiente paso es analizar los metadatos de todos los archivos públicos descargados.

Figura 54. Análisis de todos los metadatos



Fuente: El autor

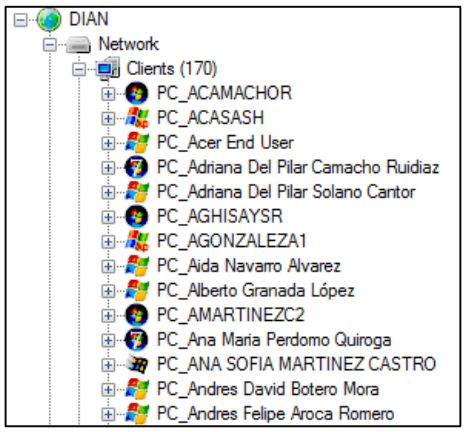
7.1.5.1 Resultado del análisis de los metadatos

Después del análisis de los metadatos realizado por FOCA a los 186 documentos públicos descargados de la URL: http://www.nortedesantander.gov.co, se obtuvieron los siguientes resultados:

7.1.5.2 Red

Se encontró información de 170 usuarios cliente que tienen acceso al sistema.

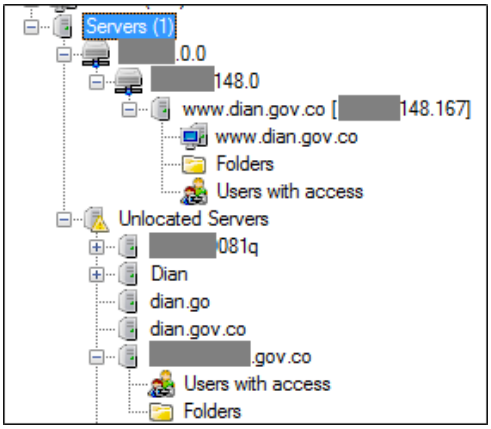
Figura 55. Usuarios cliente encontrados



Fuente: El autor

Se encontró información de 1 Servidor principal (190.24.0.0), que pertenece a la red informática.

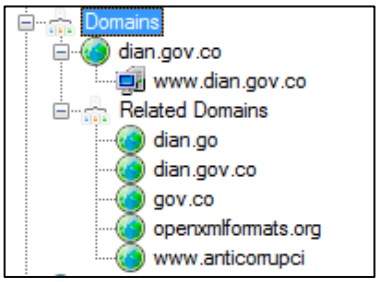
Figura 56. Servidores localizados



Fuente: El autor

Se encontraron los siguientes dominios:

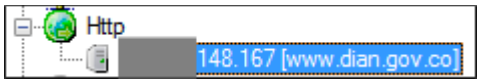
Figura 57. Dominios relacionados con el Servidor



Fuente: El autor

Se encontró una dirección IP (190.24.148.167) de un servidor web, en donde se utilizan conexiones http.

Figura 58. IP Servidor WEB encontrado



Fuente: El autor

Se encontró información de 123 impresoras utilizadas.

Figura 59. Impresoras encontradas

Attribute	Value
All printers found (123) - Times found	
HP LaserJet 1200 Series PCL 5e	2
\\X00070021007\HP LaserJet 4000	7
\\S000SIST008\I000REFI001	111
HP LaserJet 4240 PCL 6	10
\\srv00-001\I000OFEE001	6
Ricoh Aficio MP 4000 PCL	2
\\10.255.30.2\HP LaserJet 4350	4
\\K0006870003\HP DeskJet 820Cxi	2
\\S000sist008\I000CONTR001	21
hp deskjet 960c series	1
\\S000SIST008\I000PLAN001	2
\\s000sist008\I000OPUB002	8
\\srv00-001\I000OPUB002	2
HP DeskJet 680C	2
Lexmark Optra S 1625 (MS)	1
Lexmark Optra S 1625	2
\\w000sgr012\HP	1
Kyocera FS-4000DN	1
\\s000sist008\I000OFEE002	2
\\srv00-001\I000CINT001	1
\\K0006870021005\HP LaserJet 4000 Series PCLNe00:winspoolH...	2

Fuente: El autor

Se hallaron 24 direcciones de correo electrónico.

Figura 60. Correo Electrónico encontrado

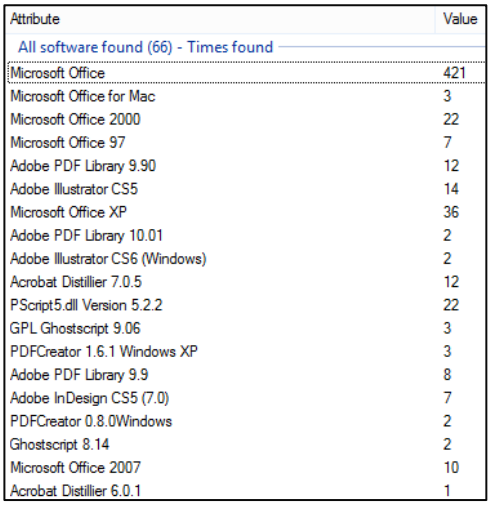
Attribute	Value
All emails found (24) - Times found	
lwilliansonl@dian.gov.co	2
rbernalb@dian.gov.co	5
CDIAZC4@DIAN.GOV.CO	2
DVILLAMILR@dian.gov.co	2
XRENJIFO@DIAN.GOV.CO	3
mguioc@dian.gov..co	1
iarandah2@dian.gov.co	1
respinosae@dian.gov.co	2
ggonzalezg3@dian.gov.co	1
asilvam@dian.gov.co	1
NSANCHEZM@dian.gov.co	1
CCEBALLOSM@dian.gov.co	2
MROAP@dian.gov.co	7
MGUTIERREZC1@dian.gov.co	1
importaciones@cimafemme.com	1
PGONZALEZV@DIAN.GOV.CO	3
LREYESP1@DIAN.GOV.CO	3
asistenciainterna@dian.gov.co	2
administrativa@hangar.com.co	2
kelly.posada@comfenalcoantioquia.com	2
SMEDINAG@DIAN.GOV.CO	1
GRODRIGUEZT@dian.gov.co	1
GESPANOLA@DIAN.GOV.CO	1
JCANONB@DIAN.GOV.CO	3

Fuente: El autor

7.1.5.3 Software

Se ha encontrado información de 66 tipos de Software, que se relacionan con los documentos.

Figura 61. Software encontrado relacionado con los documentos



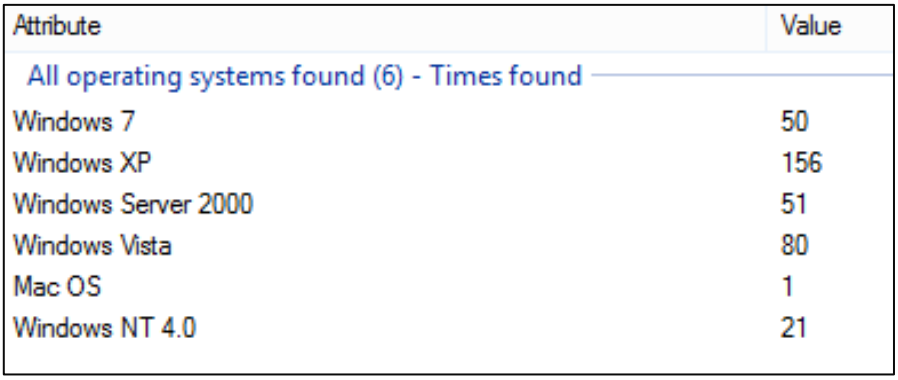
Attribute	Value
All software found (66) - Times found	
Microsoft Office	421
Microsoft Office for Mac	3
Microsoft Office 2000	22
Microsoft Office 97	7
Adobe PDF Library 9.90	12
Adobe Illustrator CS5	14
Microsoft Office XP	36
Adobe PDF Library 10.01	2
Adobe Illustrator CS6 (Windows)	2
Acrobat Distillier 7.0.5	12
PScript5.dll Version 5.2.2	22
GPL Ghostscript 9.06	3
PDFCreator 1.6.1 Windows XP	3
Adobe PDF Library 9.9	8
Adobe InDesign CS5 (7.0)	7
PDFCreator 0.8.0Windows	2
Ghostscript 8.14	2
Microsoft Office 2007	10
Acrobat Distillier 6.0.1	1

Fuente: El autor

7.1.5.4 Sistemas operativos

Se hallaron 6 sistemas operativos utilizados.

Figura 62. Sistemas Operativos encontrados



Attribute	Value
All operating systems found (6) - Times found	
Windows 7	50
Windows XP	156
Windows Server 2000	51
Windows Vista	80
Mac OS	1
Windows NT 4.0	21

Fuente: El autor

7.2 FASE 2. DETERMINAR LAS VULNERABILIDADES, AMENAZAS Y RIESGOS DE SEGURIDAD

Después de realizar la extracción de metadatos y su respectivo análisis a los archivos públicos descargados en la URL de cada organización en estudio, se pudo determinar lo siguiente:

7.2.1 Cámara de comercio de pamplona. (http://camarapamplona.org.co)

En el análisis de metadatos se encontró lo siguiente:

7.2.1.1 Datos Sensibles

Tabla 6. Información sensible encontrada en http://camarapamplona.org.co

Cantidad	Datos Sensibles
9	Nombres de Usuario
7	Ip de Servidores
77	Dominios relacionados con camarapamplona.org.co
3	Direcciones DNS
9	Documentos PDF creados bajo Sistema Operativo XP.
20	Tipos de Software utilizados en la edición de los documentos

Fuente: El autor

7.2.1.2 Determinar vulnerabilidades, amenazas y riesgos.

Ingeniería Social: Consiste en conseguir información de la empresa o del sistema informático, utilizando habilidades sociales y engaños. Esta amenaza se podría explotar conociendo el nombre de un usuario o empleado de la empresa y teniendo la dirección de un correo electrónico, o números de teléfono, en este caso no se encontró ningún correo electrónico en los metadatos, pero de la url se obtiene el email y números telefónicos de contacto, como se observa en la siguiente imagen:

Figura 63. Email y números telefónicos de contacto

> Para Comunicarse con algun Funcionario de la Cámara de Comercio de Pamplona puede llamar al Telefono: (097) 5682047, (097) 5680993 o (097) 5684696; también puede escribir al correo electronico ccpamplona@camarapamplona.org.co

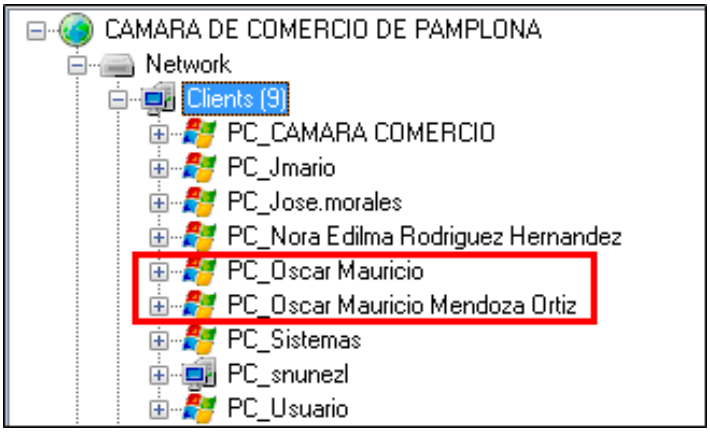
Fuente: http://camarapamplona.org.co/camara2/node/371

Ahora se debe seleccionar un usuario; analizando la información de los equipos cliente se puede apreciar que existen 2 equipos con los siguientes nombres:

PC_Oscar Mauricio y PC_Oscar Mauricio Medoza Ortiz

Y con igual nombre de usuario respectivamente.

Figura 64. Nombres de usuarios iguales



Fuente: El autor

Al parecer este usuario tiene acceso a 2 equipos de la empresa y puede manejar información importante y sensible de la misma. Por consiguiente, puede ser un candidato adecuado para realizarle la ingeniería Social.

Como ya se tiene el nombre completo del usuario y un correo electrónico de la empresa, se puede enviar un email solicitando un contacto directo con la persona, y de ahí en adelante toda la información que se obtenga depende de las habilidades engañosas del atacante.

Phishing: Con la información obtenida de la ingeniería Social, se pueden realizar acciones de pesca o robo de información, enviando un correo electrónico simulando una organización o institución de confianza, al ya tener un nivel de confianza el usuario o empleado de la Cámara de Comercio de Pamplona, puede enviar datos importantes a un posible atacante y este realizar fraudes o falsificaciones de diferente índole.

7.2.2 Alcaldía de pamplona (www.pamplona-nortedesantander.gov.co)

En el análisis de metadatos se encontró lo siguiente:

7.2.2.1 Datos Sensibles

Tabla 7. Información sensible encontrada en www.pamplona-nortedesantander.gov.co

Cantidad	Datos Sensibles
76	Nombres de Usuario
1	IP de Servidor
296	Dominios relacionados con camarapamplona.org.co
1	Servidor Web
6	Impresoras en Total
4	Impresoras conectadas en red
9	Documentos PDF creados bajo Sistema Operativo XP.
4	Sistemas Operativos(Windows Server 2000, Windows XP, Windows Vista, Windows 7)
1	Dirección de correo electronica

Fuente: El autor

7.2.2.2 Determinar vulnerabilidades, amenazas y riesgos.

7.2.2.2.1 Métodos HTTP inseguros

Dentro de las especificaciones del protocolo HTTP con el que se comunican clientes y servidores se definen una serie de verbos o métodos para dialogar con el servidor web y así poder solicitar determinados comportamientos dependiendo de las necesidades de cada situación. Así, además métodos GET y POST para solicitar un fichero situado en una dirección URL concreta o enviar datos a un programa en formato de texto plano, existe una completa lista de verbos definidos en el estándar y mecanismos especiales para que cualquiera pueda extender y crear nuevos verbos HTTP.

Sin embargo, algunas aplicaciones web habilitan los métodos para la manipulación de ficheros en el servidor, tales como DELETE, MOVE, COPY o PUT. El método PUT permite subir ficheros al servidor o, incluso, reemplazar archivos existentes, ya que, si se sube un fichero con PUT y éste existe, entonces se sobrescribiría el anterior. Estos comportamientos pueden suponer un riesgo para la seguridad de un sitio si se dejan habilitados en directorios públicos, aunque, por supuesto. a pesar de que está habilitado el verbo PUT o DELETE, el usuario con que corre el pool de la aplicación debería tener

permisos para poder escribir en el sistema ficheros. Si así fuera, subir una WebShell en PHP, ASP, JSP o lo que soporte el sistema sería trivial.

Para agilizar el proceso de detección de servidores vulnerables, FOCA implementa esta búsqueda para cada dominio web que se descubre, se genera una lista de URLs detectadas en los buscadores. Estas URLs pueden venir de la búsqueda de documentos, de la búsqueda de servidores del descubrimiento de la red, buscando las tecnologías utilizadas en el dominio o, directamente, buscando todos los links en los buscadores relativos a ese dominio.

Con el objetivo de detectar que ubicaciones tienen algún método que pudiera ser potencialmente inseguro para el sitio web, FOCA extrae todos los directorios y realiza una comprobación para saber cuáles son todos los verbos habilitados en él, usando para ello una petición con el método OPTIONS. Si aparece algún método potencialmente inseguro, como DELETE, PUT o TRACE, la herramienta alertará sobre esto, como se observa en la figura siguiente:

Figura 65. Alerta sobre Métodos Inseguros

Fuente: El autor

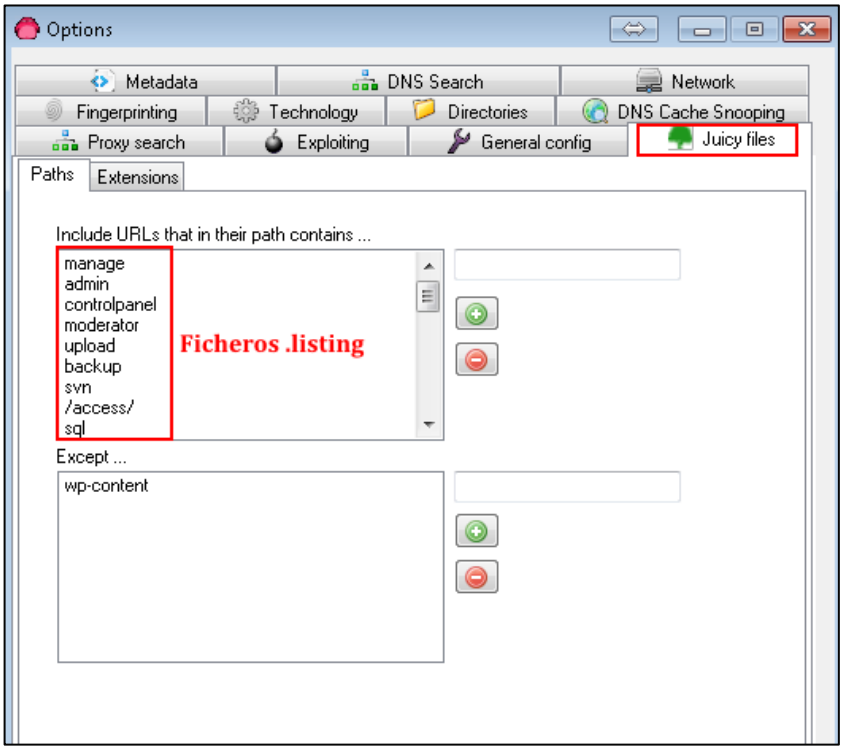
7.2.2.2.2 Juicy files

Los juicy files son aquellos tipos de ficheros que suelen contener datos muy llamativos e importantes para la realización de una auditoría, es decir, aquellos de los que se suele extraer mucha. Información. Los ficheros que FOCA cataloga como juicy files son aquellos que tienen una extensión sospechosa de contener información interesante, como los .bak o los .old, los archivos que por su extensión puedan resultar interesantes, o los servidores en los que se localizan puertos abiertos diferentes al 80, como el puerto 8080, por ejemplo.

Así, en la pestaña juicy files de las opciones de FOCA, se puede configurar el programa (con una lista blanca y una lista negra) para que incluya ficheros que, bien por la ruta en la que se encuentran, 0 bien por su extensión, se considere que merecen un análisis más detallado.

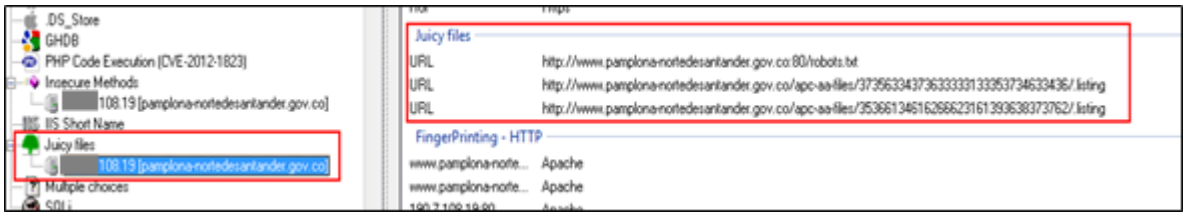
Para localizar todos estos ficheros, FOCA no sólo usa Google Crawling y Bing Crawling, sino que aprovecha la información que aparece en los ficheros .listing, descritos a continuación, busca los directorios que permiten un listado de archivos, aprovecha el contenido de los archivos robots.txt y busca puertos inusuales en los servidores del dominio objetivo.

Figura 66. Configurando lista blanca y negra. Juice Files



Fuente: El autor

Figura 67. Vulnerabilidad Juice Files detectada



Fuente: El autor

7.2.3 Gobernación de norte de Santander [http://www.nortedesantander.gov.co)](http://www.nortedesantander.gov.co)

En el análisis de metadatos se encontró lo siguiente:

7.2.3.1 Datos Sensibles

Tabla 8. Información sensible encontrada en http://www.nortedesantander.gov.co

Cantidad	Datos Sensibles
30	Nombres de Usuario
4	Ip de Servidores
10	Nombres de Impresoras en total
1	Dirección de correo electrónico
23	Tipos de Software utilizados en la creación y edición de los documentos
2	Sistemas operativos utilizados. (Win 7, Win XP)

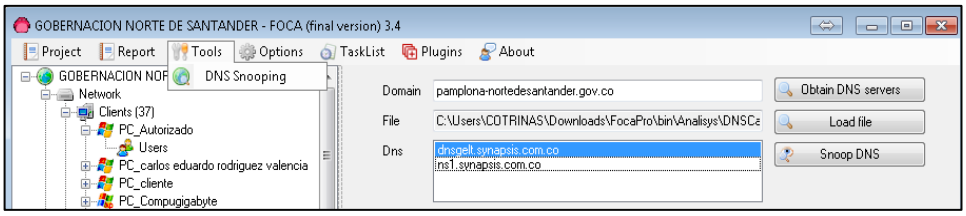
Fuente: El autor

7.2.3.2 Determinar vulnerabilidades, amenazas y riesgos.

7.2.3.2.1 DNS Spoofing Caché

Otra de las vulnerabilidades que busca FOCA es la de servidores DNS que tienen configurado un sistema de Caché, lo que puede ser una fuga de información muy importante para una organización. Cada vez que un usuario quiere resolver un nombre de dominio, éste pregunta al servidor DNS que tiene configurado. Si el servidor tiene activada la Caché, entonces, antes de solicitar la resolución por medio de un sistema de consultas recursivas, mira primero si tiene una resolución no caducada de ese nombre en su Caché.

Figura 68. Vulnerabilidad DNS Spoofing



Fuente: El autor

7.2.4 Diario la opinión (http://www.lapinion.com.co)

En el análisis de metadatos se encontró lo siguiente:

7.2.4.1 Datos Sensibles

Tabla 9. Información sensible encontrada en http://www.lapinion.com.co

Cantidad	Datos Sensibles
6	Nombres de Usuario
2	Ip de Servidores
10	Tipos de Software utilizados en la creación y edición de los documentos

Fuente: El autor

7.2.4.2 Determinar vulnerabilidades, amenazas y riesgos.

De la información extraída de los metadatos de los documentos públicos descargados de http://www.lapinion.com.co, se determina que las vulnerabilidades detectadas son la ingeniería Social y el Phishing, su manera de explotación es similar a la explicada en el numeral 11.2.1.

7.2.5 La Dian (http://www.dian.gov.co)

En el análisis de metadatos se encontró lo siguiente:

7.2.5.1 Datos Sensibles

Tabla 10. Información sensible encontrada en http://www.dian.gov.co

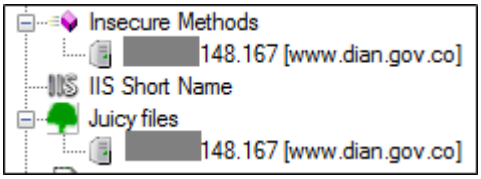
Cantidad	Datos Sensibles
170	Nombres de Usuario
1	Ip de Servidores
66	Tipos de Software utilizados en la creación y edición de los documentos
123	Impresoras encontradas
24	Direcciones de Correo
6	Sistemas Operativos (win 7, Win XP, Win Server 2000, Win Vista, Mac OS, Win NT 4.0)

Fuente: El autor

7.2.5.2 Determinar vulnerabilidades, amenazas y riesgos.

De la información extraída de los metadatos de los documentos públicos descargados de http://www.dian.gov.co, se determina que las vulnerabilidades detectadas son la ingeniería Social, el Phishing, métodos inseguros http y Juicy Files, su explicación y la manera de explotación es similar a la explicada en el numeral 11.2.1 y numeral 11.2.2 respectivamente.

Figura 69. Vulnerabilidad Metodos Inseguros – Juicy Files



Fuente: El autor

7.3 FASE 3. ALTERNATIVAS DE PROTECCION

7.3.1 Limpieza de documentos.

La limpieza de metadatos consiste en borrar y retirar de los documentos información oculta (metadatos), esta limpieza se realiza siempre y cuando el destinatario no necesite esa información.

Esto es muy importante realizarlo sobre todo cuando los documentos se van a compartir en la web de manera masiva, o a destinatarios no conocidos.

No tener en cuenta esta medida, puede hacer daño a:

- ✓ La confidencialidad de información.
- ✓ La seguridad de la información de la organización.
- ✓ La imagen de la organización, pues sería responsable de las consecuencias que pueda ocasionar no tener en cuenta la limpieza y seguridad de los metadatos.

7.3.2 Eliminación de metadatos

Hay procedimientos y herramientas que pueden utilizarse para eliminar los metadatos, para que los documentos publicados en sitios web u otros tipos de repositorios públicos no contengan información que pueda perjudicar a la entidad productora de la información.

Para poner de manifiesto las ventajas e inconvenientes de los diferentes métodos disponibles, se ha establecido una división entre las técnicas de eliminación y edición de metadatos que requieren de acciones por parte de los usuarios y que, por tanto, se han catalogado como técnicas manuales, y aquellas que, de forma automática, realizan los pasos necesarios para que la información publicada no contenga información no deseada.

Existen varias herramientas para eliminar los metadatos en documentos y fotografías, de igual manera Microsoft Office trae incorporada esa función.

Herramientas para eliminar metadatos:

- ✓ **MetaShield Protector:** Es una herramienta comercial que evita la fuga de información en documentos ofimáticos a través de su publicación en sitios web. El documento será limpiado en memoria automáticamente por el componente, quedando una copia totalmente limpia de metadatos e información oculta.

- ✓ **MetaStripper:** Esta herramienta elimina los metadatos en las imágenes y fotografías. Puede eliminar toda la información guardada en varias fotografías al mismo tiempo.

- ✓ **Doc Strubber:** Elimina metadatos e información oculta de documentos Word.

- ✓ **Metadata Cleaner:** Es una herramienta de eliminación de metadatos que protege a las organizaciones de fugas de información y metadatos accidentales. Las fugas no intencionales tienen el potencial de afectar negativamente la seguridad de la información de las organizaciones.

  Metadata Cleaner permite seleccionar el documento y limpiarlo. Le permite limpiar todas las propiedades incorporadas y personalizadas de estos archivos. Puede seleccionar varios archivos y limpiarlos simultáneamente en un solo clic, se puede ejecutar sin necesidad de instalarlo.

- ✓ **Limpiar metadatos con Word:** La herramienta de office para la limpieza de documentos Microsoft Offíce utiliza la opción de Inspeccionar un documento que se encuentra en las versiones de Microsoft Office superiores a 2007. Esta herramienta realiza una búsqueda de información oculta en los documentos, desde el momento de su creación, edición, modificación y envíos, encuentra datos sobre los usuarios, impresoras, directorios, unidades de almacenamiento y cualquier información oculta relacionada con el documento.

  Con esta opción se puede eliminar toda o parte de la información oculta que no se quiera incluir al compartir el documento.

  Ejemplo:

  Para este ejemplo se ha tomado un archivo en Word descargado de la url http://pamplona-nortedesantander.gov.co:

  026___VIERNES_27_DE_AGOSTO.docx

  Este archivo será analizado por FOCA.

  De ese análisis se obtuvo la siguiente información:

Figura 70. Extracción de metadatos archivo .docx

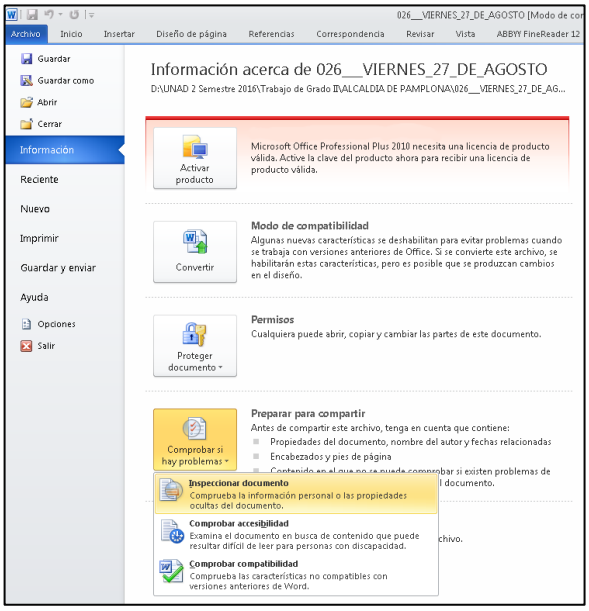
Attribute	Value
File Information	
URL	D:\UNAD 2 Semestre 2016\Trabajo de Grado II\ALCALDIA DE PAMPLONA\026___VIERNES_27_DE_AGOSTO.docx
Local path	D:\UNAD 2 Semestre 2016\Trabajo de Grado II\ALCALDIA DE PAMPLONA\026___VIERNES_27_DE_AGOSTO.docx
Download	Yes
Analized	Yes
Download date	28/11/2016 14:38:48
Size	831,75 KB
Users	
Username	ZADIZA
Username	usuario
Dates	
Creation date	11/07/2010 11:05:00
.docx date	11/07/2010 11:03:00
Modified date	11/07/2010 11:05:00
Other Metadata	
Application	Microsoft Office 2007
Revisions	2
Edition time	00:00:00.0000002
Software	
Microsoft Office 2007	

Fuente: El autor

La ubicación, fecha de descarga, tamaño, nombres de usuario, fecha de creación, fecha de modificación, Software con el cual se creó, número de revisiones.

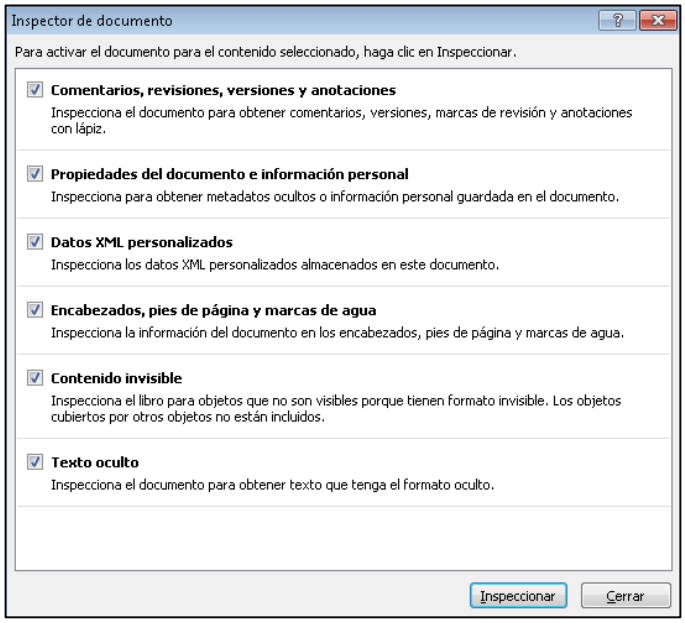
El paso siguiente es borrar los metadatos del archivo con Word.

Figura 71. Paso 1 Borrar Metadatos con Word Office 2010.docx



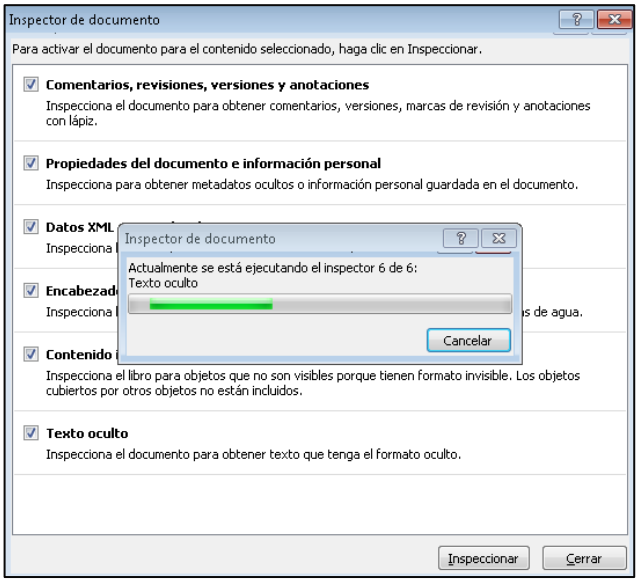
Fuente: El autor

Figura 72. Paso 2 Borrar Metadatos con Word Office 2010.docx



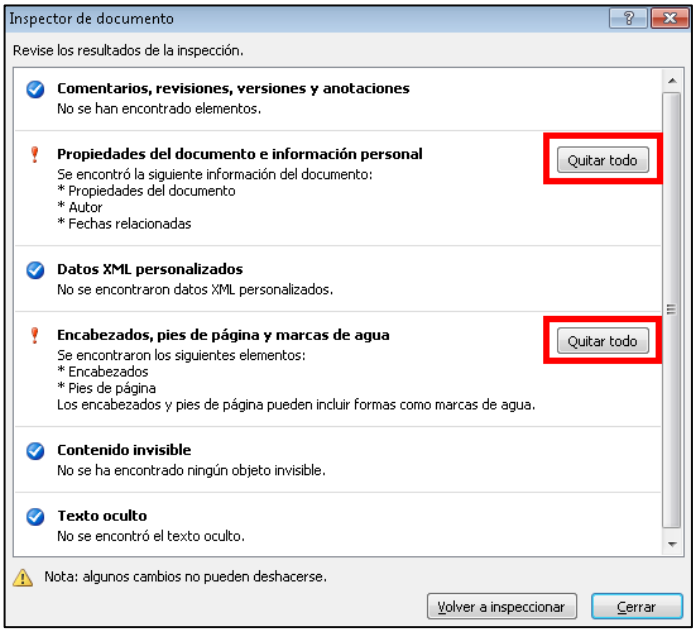
Fuente: El autor

Figura 73. Paso 3 Borrar Metadatos con Word Office 2010.docx



Fuente: El autor

Figura 74. Paso 4 Borrar Metadatos con Word Office 2010.docx



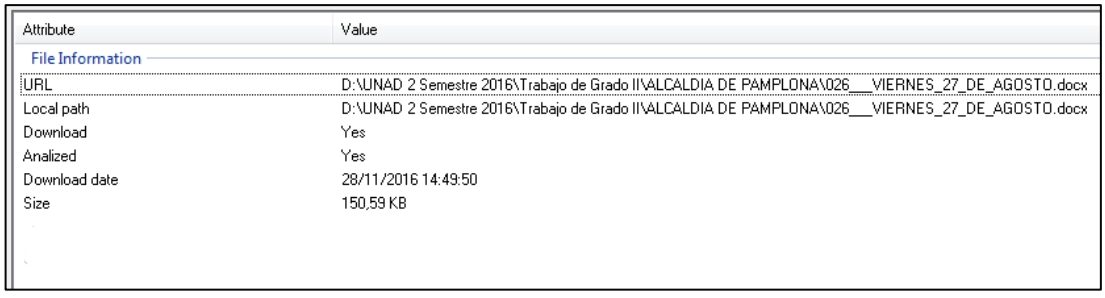
Fuente: El autor

Después se vuelve analizar el archivo con FOCA y estos son los resultados:

La ubicación, fecha de descarga, tamaño.

La información más sensible de los metadatos fue borrada como se observa en la siguiente imagen:

Figura 75. Prueba de la eliminación de los metadatos



Fuente: El autor

7.4 FASE 4. ELABORAR UNINFORME FINAL SOBRE LOS RESULTADOS DEL ANÁLISIS DE LOS METADATOS DE LA INVESTIGACIÓN

El estudio realizado a los metadatos que se encuentran en los documentos públicos de las entidades y organizaciones analizadas, da como resultado lo siguiente:

En total se analizaron los metadatos de 1797 documentos públicos de 5 entidades, estos documentos son de diferente tipo, repartidos de esta manera:

Tabla 11. Total de documentos públicos analizados

Tipo de documento	Cantidad	%
.pdf	1228	68.33
.doc	113	6.28
.docx	17	0.94
.ppt	8	0.44
.pptx	1	0.05
.xls	364	20.42
.xlsx	56	3.11
.pps	1	0.05
.ppsx	1	0.05
Imágenes	0	0
Desconocidos	8	0.44
Total	**1797**	**100**

Fuente: El autor

De la extracción y análisis de los metadatos de los 1797 documentos se encontró la siguiente información sensible:

Tabla 12. Total de datos sensibles encontrados

Datos sensibles	Cantidad	%
Nombres de usuario	291	29.6
Ip de Servidores	16	1.62
Tipos de Software	119	12.10
Nombres de Impresoras	139	14.14
Direcciones de Correo electrónico	26	2.64
Sistemas Operativos	12	1.22
Dominios relacionados	373	37.94
Impresoras en red	4	0.40
Direcciones DNS	3	0.30
Total	**983**	**100**

Fuente: El autor

CONCLUSIONES

- ✓ Es mucha la información oculta que se obtuvo en los documentos analizados y que pueden ocasionar graves problemas de seguridad en la información de las entidades estudiadas.

- ✓ Las entidades en estudio no están siendo cuidadosas con la información que publican en sus respectivos portales web, pues no tienen en cuenta los datos ocultos que se encuentran en los documentos que ofrecen al público.

  Se puede evidenciar que las entidades en estudio no están teniendo en cuenta los metadatos en su plan de seguridad informática, lo que ocasiona un riesgo en la protección de la información confidencial.

- ✓ Es necesario que estas entidades tengan en cuenta la seguridad de los metadatos en cada documento creado, recibido o modificado en sus redes informáticas.

  En las políticas de seguridad de la información de estas entidades se debe incluir la seguridad de los metadatos, creando un protocolo el cual verifique que los documentos no posean información sensible oculta.

  Se debe aplicar las técnicas de borrado y eliminación de los metadatos antes de publicar los documentos al público.

- ✓ Los metadatos podrían convertirse en un riesgo potencial para el creador de la información si, al distribuir o publicar documentos en Internet, no son gestionados de forma adecuada.

BIBLIOGRAFIA

Universidad Nacional Sede Amazonía. “Metadatos”.{En línea}. [Citado el 15 de agosto de 2016]Disponible en internet: http://www.unal.edu.co/siamac/sig/metadatos1.html

Marilin, Gonzalo.”Qué son tus metadatos y por qué pueden ser tan importantes como el contenido de tu email”.{ En línea}.{28 de octubre de 2013}[Citado el 18 de Agosto de 22016]. Disponible en internet: http://www.eldiario.es/turing/vigilancia_y_privacidad/metadatos-pueden-importantes-contenido-email_0_190731401.html

Méndez, Eva. “Introducción a los metadatos, Estándares y Aplicación”.{En Línea}.{2004}. [Citado el 20 de septiembre de 2016].Disponible en Internet: http://www.sedic.es/autoformacion/metadatos/tema2.htm

GITS. “Cyber Seguridad. Metadatos”.{En Línea}.{2003}. [Citado el 25 de Septiembre de 2016].Disponible en internet: http://www.gitsinformatica.com/metadatos.html

Rios, Valeria. “La PGR miente: los metadatos de una foto sí pueden editarse”.{En Línea}.{28 de abril de 2016}[Citado el 1 de octubre de 2016].Disponible en Internet:: http://hipertextual.com/2016/04/metadatos-alterables

W3C.”Comprender los metadatos”.{En Linea}.{2010}.[Citado el 5 de Octubre de 2016] Disponible en Internet: http://www.sidar.org/traducciones/wcag20/es/comprender-wcag20/appendixC.html

SEDIC.”Herramientas y aplicaciones para la creación y gestión de metadatos”{En Linea}.{2016}.[Citado el 25 de Octubre de 2016] Disponible en Internet: http://www.sedic.es/autoformacion/metadatos/tema10.html

Universidad de Antioquia.”Herramientas para metadatos”.{En línea}.{30 de abril de 2016}.[Citado el 1 de noviembre de 2016]. Disponible en Internet: http://aprendeenlinea.udea.edu.co/lms/moodle/mod/resource/view.php?id=3339

Bautista del Viejo, Hipolito.”Cómo utilizar FOCA, extrae metadatos y analiza archivos”.{En línea}.{25 agosto 2013}.[Citado el 10 de Noviembre de 2016]. Disponible en Internet:
http://rootear.com/seguridad/foca-metadatos-archivos

ANEXOS

Anexo 1. Tarjeta de Divulgación

CUIDADO CON LOS METADATOS

Qué son los metadatos ?

Los metadatos son datos que describen otros datos, resumen la información básica sobre los datos, lo que facilita la búsqueda y el trabajo con instancias particulares de datos. Por ejemplo, autor, fecha de creación y fecha de modificación y tamaño de archivo son ejemplos de metadatos .

Además de los archivos de documentos, los metadatos se utilizan para imágenes, videos, hojas de cálculo y páginas web. El uso de metadatos en páginas web puede ser muy importante. Los metadatos de las páginas web contienen descripciones del contenido de la página, así como palabras clave vinculadas al contenido. Estos se expresan normalmente en forma de metatags . Los metadatos que contienen la descripción y resumen de la página web a menudo se muestran en los resultados por los motores de búsqueda, lo que hace que su precisión y detalles sean muy importantes ya que puede determinar si un usuario decide visitar el sitio o no.

Imagen Tomada de: http://www.avantic.net/typo3temp/pics/8cb95cb023.png

Imagen tomada de : https://cdn.tecnologia.net/wp-content/uploads/2015/05/C%C3%B3mo-borrar-los-metadatos-de-una-imagen-o-fotograf%C3%ADa.jpg

Los metadatos pueden crearse manualmente o mediante un procesamiento automatizado de la información. La creación manual tiende a ser más precisa, permitiendo al usuario ingresar cualquier información que consideren relevante o necesaria para ayudar a describir el archivo. La creación automatizada de metadatos puede ser mucho más elemental, normalmente sólo muestra información como el tamaño del archivo, la extensión del archivo, cuando se creó el archivo y quién creó el archivo.

Porque proteger los metadatos ?

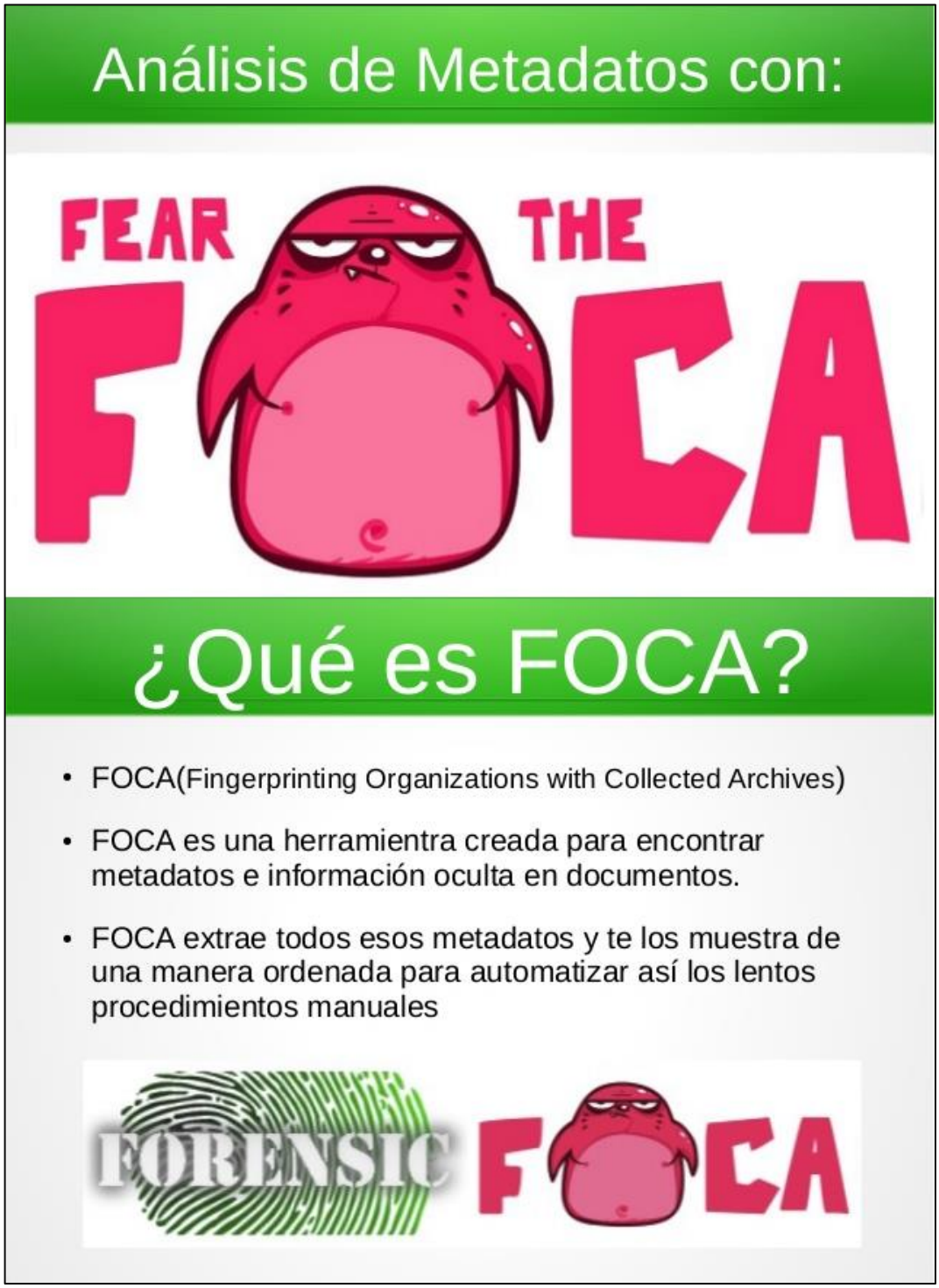
Los metadatos son información oculta incrustada en muchas aplicaciones electrónicas, incluyendo WordPerfect, Microsoft Word, PowerPoint y Excel. Estos datos pueden contener información confidencial, que no se desea revelar a terceros. Gran parte de esta información es invisible para los usuarios de rutina, se crea automáticamente y no se puede prevenir.

Incluso si un documento está protegido por contraseña, se puede discernir una cantidad significativa de metadatos aunque el documento en sí no pueda abrirse. Un abogado de litigios civiles puede utilizar los metadatos como una herramienta eficaz de examen cruzado.

Imagen Tomada de: https://www.cloudseguro.co/metadatos-en-el-mundo-digital/

Fuente: El autor

Anexo 2. Herramienta toma de Información



Fuente: http://image.slidesharecdn.com/presentacin-121222210826-phpapp02/95/anlisis-de-metadatos-con-la-foca-1-638.jpg?cb=1356210716