



Toma de huellas automáticas de una organización utilizando FOCA

FOCA (organizaciones de toma de huellas dactilares con archivos recopilados) es una herramienta que revela metadatos y datos ocultos. Estos archivos pueden estar en las páginas del sitio, y pueden descargarse y diseccionarse con FOCA

Objetivos del laboratorio

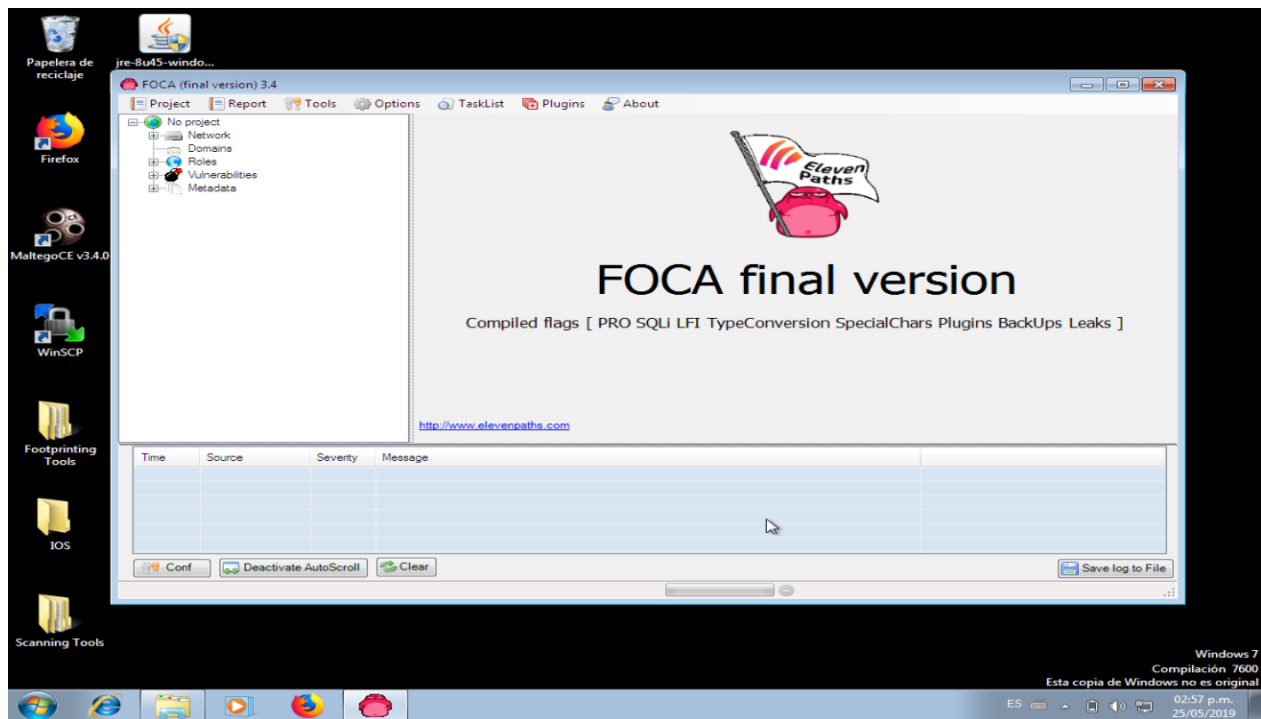
El objetivo de este laboratorio es demostrar cómo extraer documentos e información de dominio utilizando FOCA. Los estudiantes aprenderán a realizar:

- Extracción de metadatos
- Análisis de red
- Snooping DNS
- Buscar archivos comunes
- Archivos jugosos
- Búsqueda de proxies
- Tecnologías de identificación
- Toma de dedos
- fugas
- Búsqueda de copias de seguridad
- Error forzando
- Abrir directorios de búsqueda

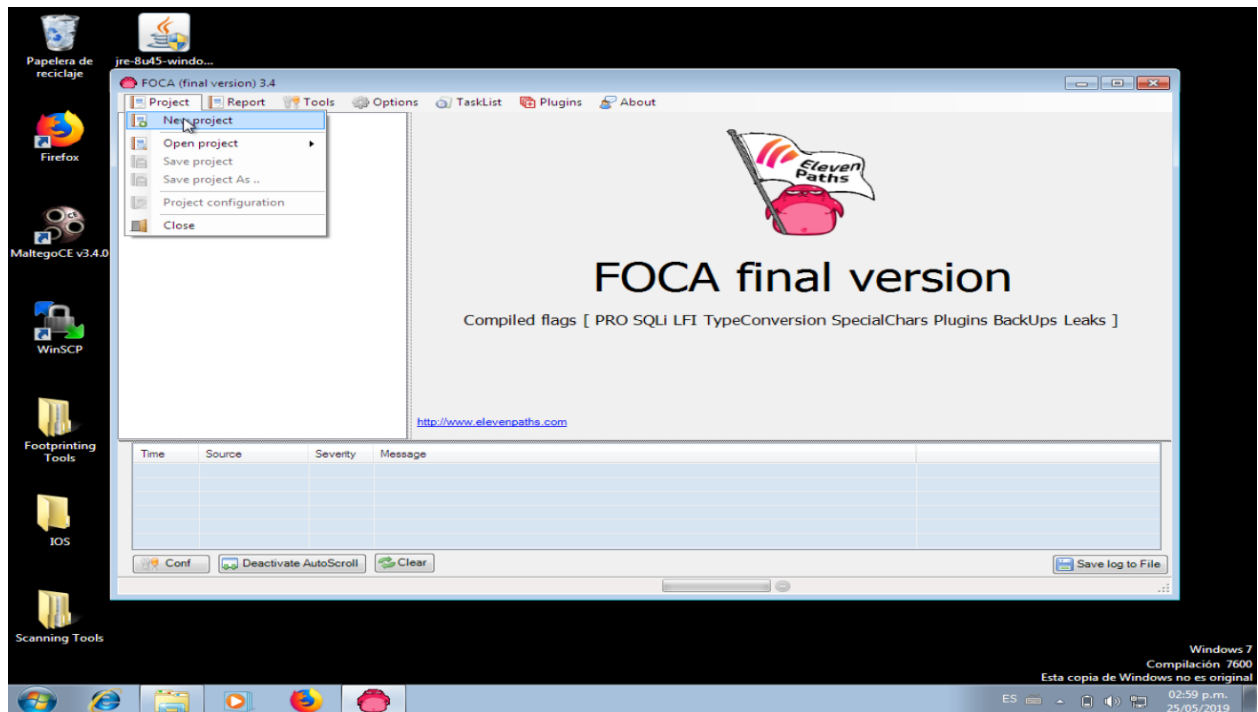
Tareas del laboratorio

1. Para lanzar FOCA dirígete al directorio donde tengas los programas que se ocuparan en este modulo y da doble click al archivo .exe
2. Si aparece la ventana emergente Abrir archivo - Advertencia de seguridad, haga clic en **Ejecutar**.

3. Aparece la ventana principal de FOCA, como se muestra en la siguiente figura.

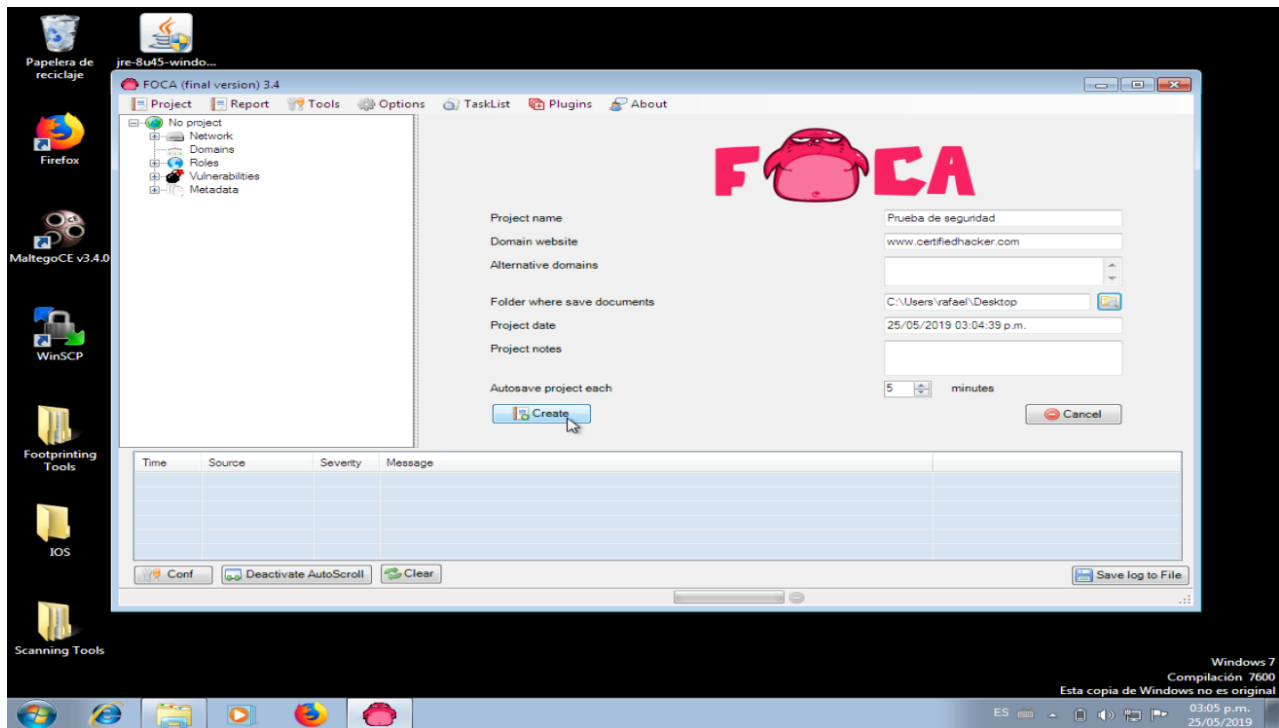


4. Cree un nuevo proyecto navegando a **Proyecto** y haga clic en **Nuevo proyecto** en la barra de menú.

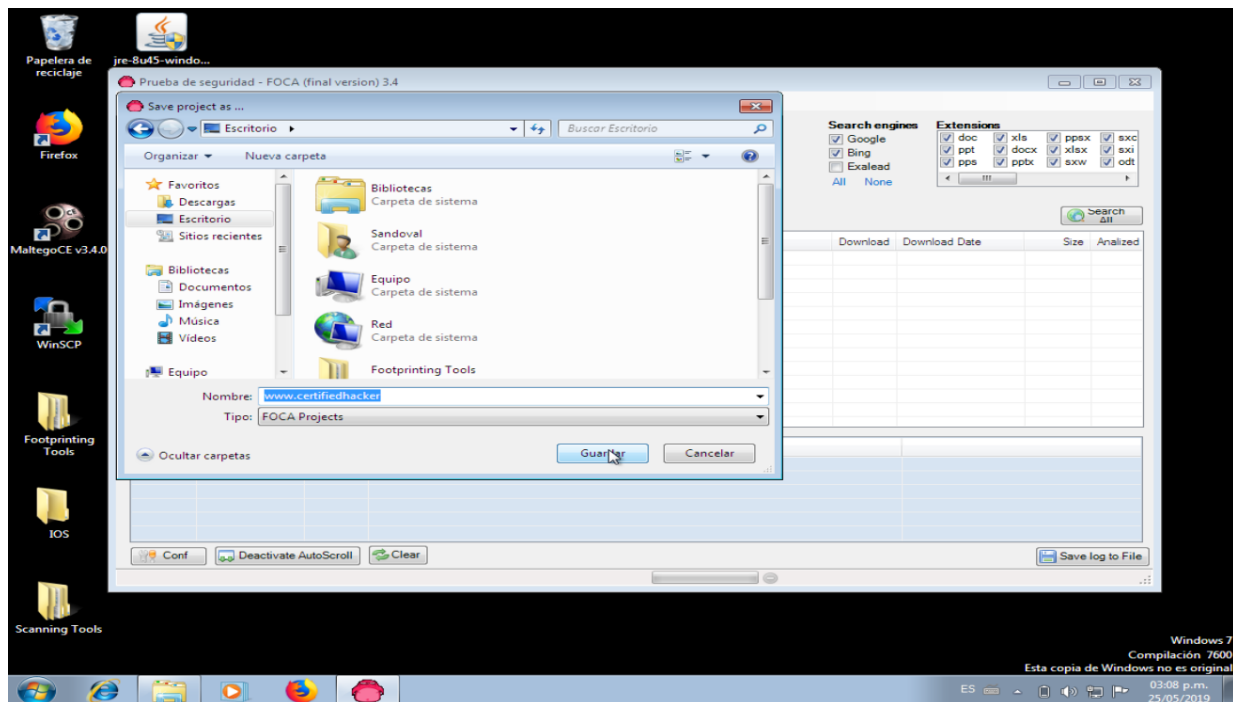


5. El asistente de nuevCaptura de pantalla de 2019-05-25 16-17-16o proyecto de FOCA aparece como se muestra a continuación:

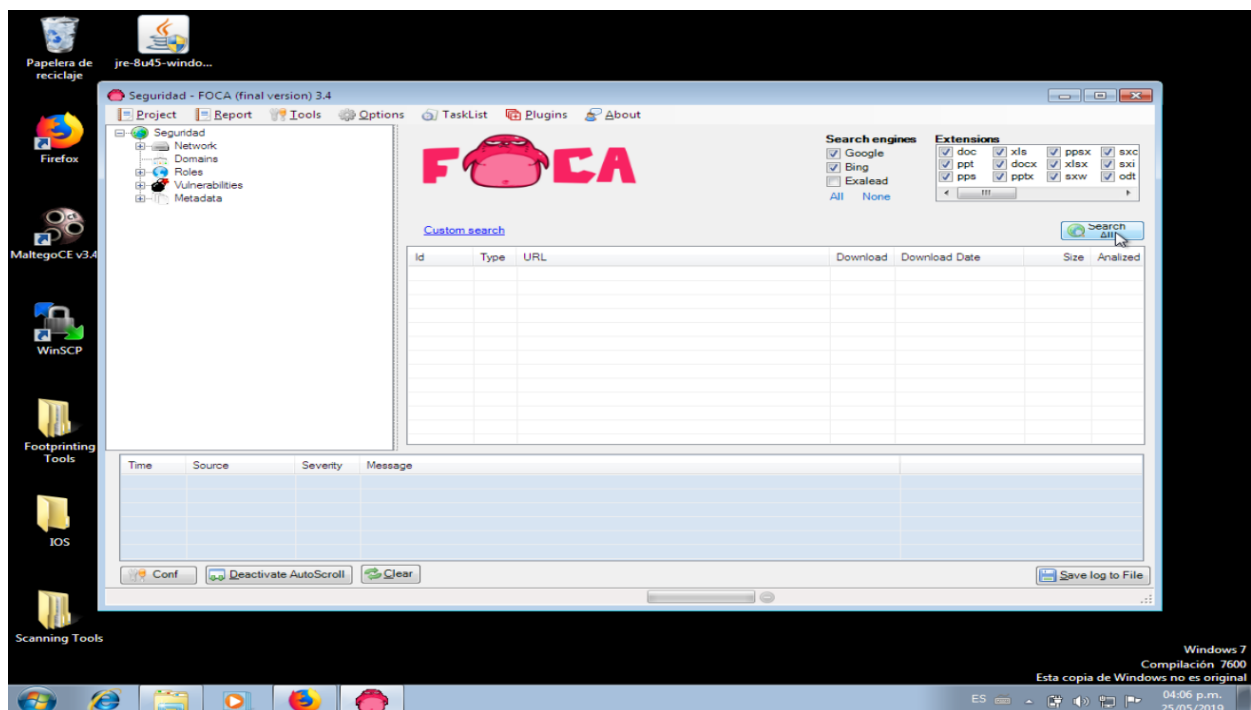
- Ingrese un nombre de proyecto en el campo Nombre de proyecto,
 - Introduzca el sitio web del dominio en el campo Sitio web del dominio
 - Puedes dejar los dominios alternativos opcionales vacíos.
6. Haga clic en **Carpeta** para guardar el documento que **FOCA** extrae en la **carpeta donde se guardan los documentos**, deje las otras configuraciones predeterminadas y haga clic en **Crear**.



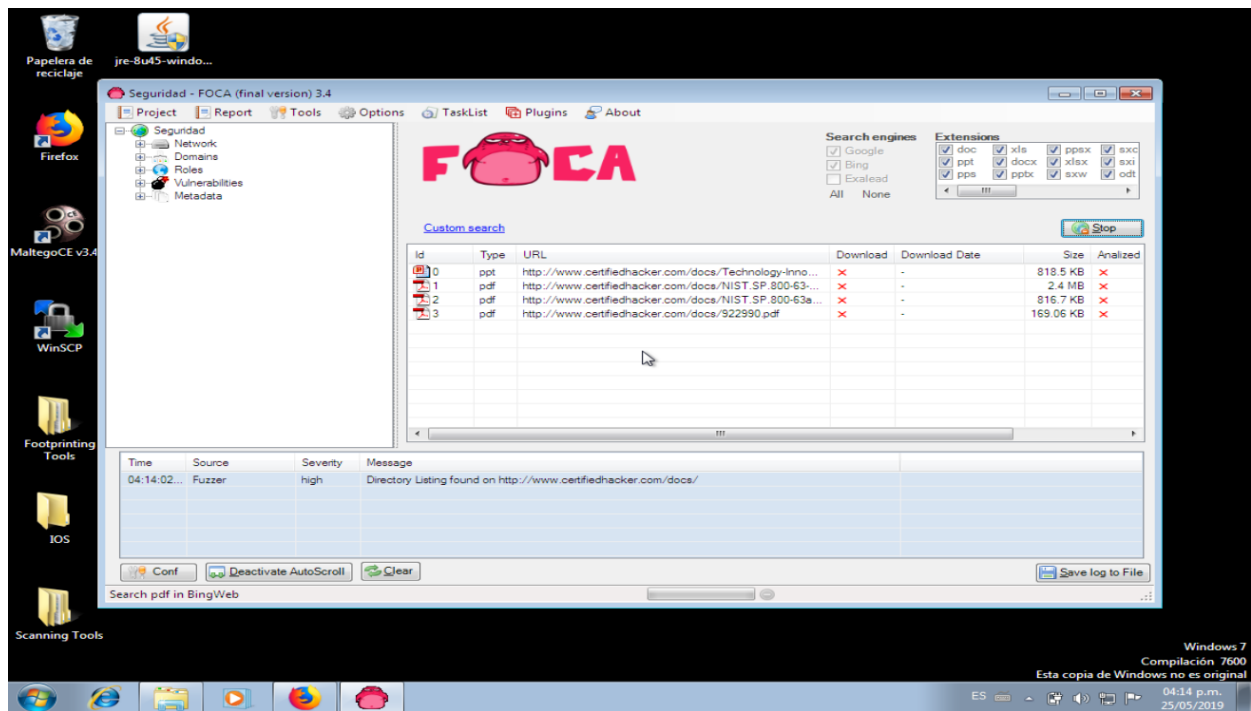
7. El proyecto Guardar como aparece la ventana proporciona la ubicación deseada para guardar el proyecto FOCA y escribir el nombre del archivo en el campo **Nombre de archivo** y hacer clic en Guardar.



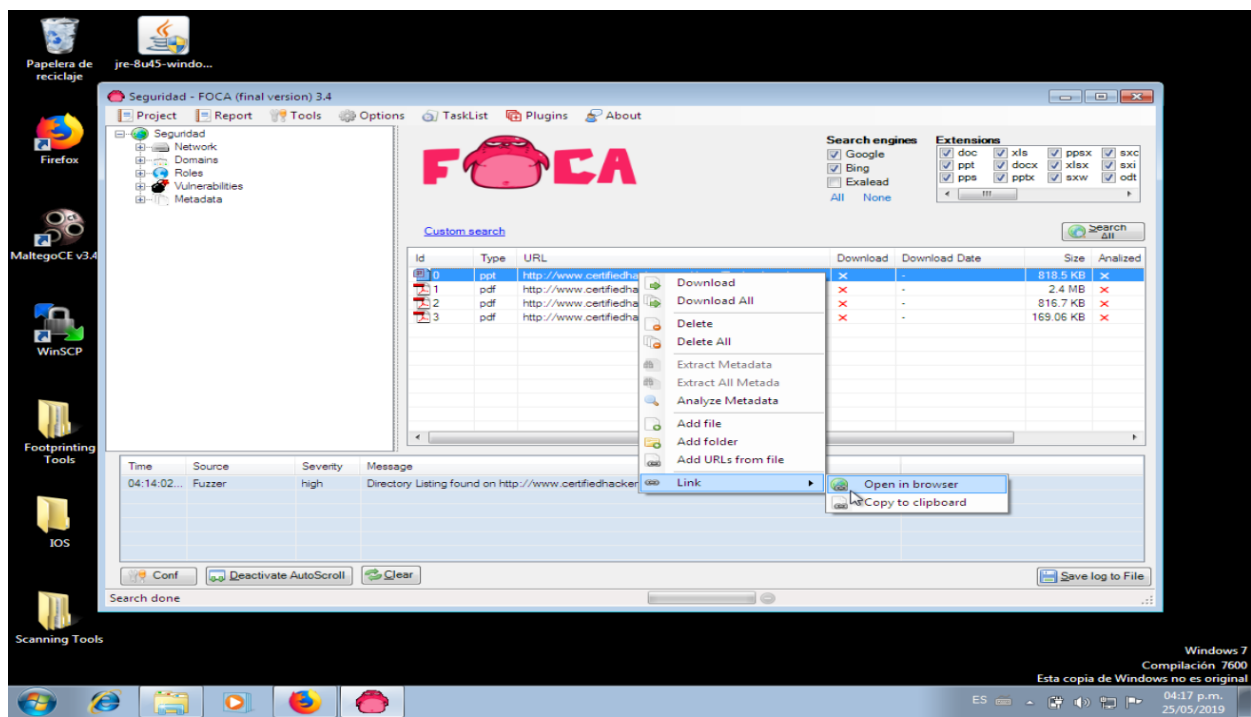
8. Aparece la ventana emergente Guardar proyecto con éxito, haga clic en **Aceptar**.
9. Para extraer la información del dominio apuntado, haga clic en Buscar todo.



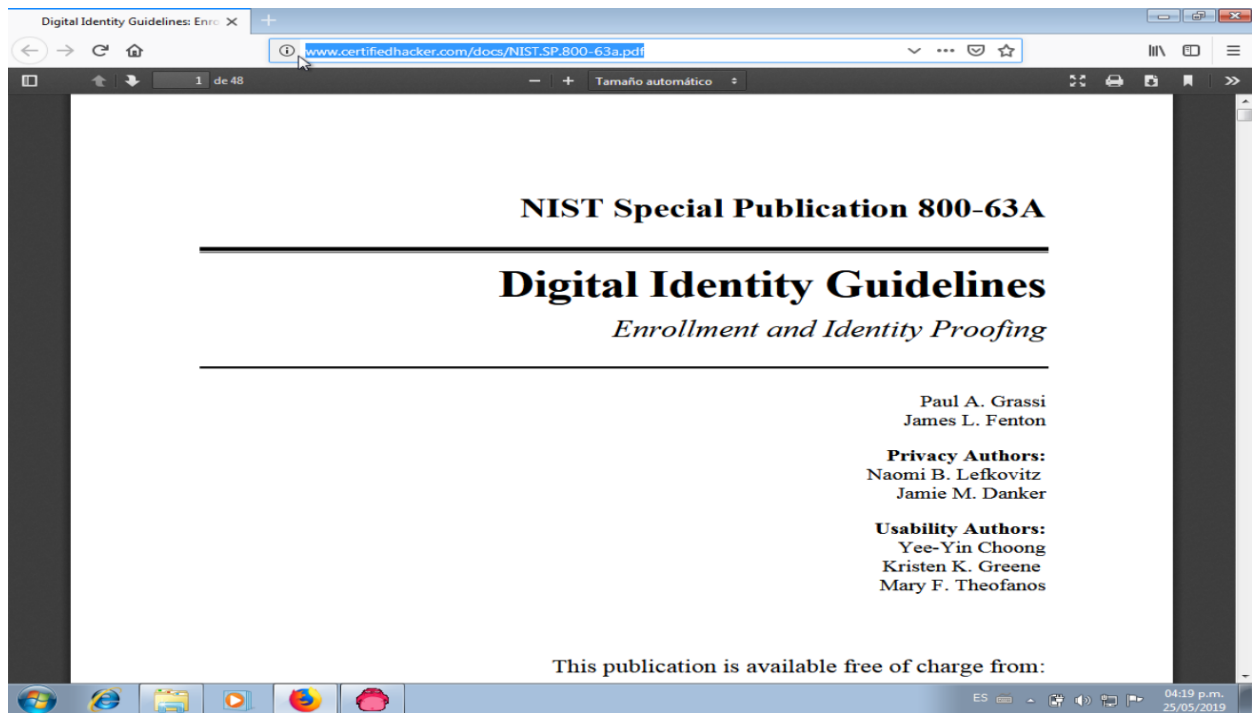
10. El botón **Buscar todos** alterna automáticamente el botón Detener y puede ver el resultado en los paneles inferiores.



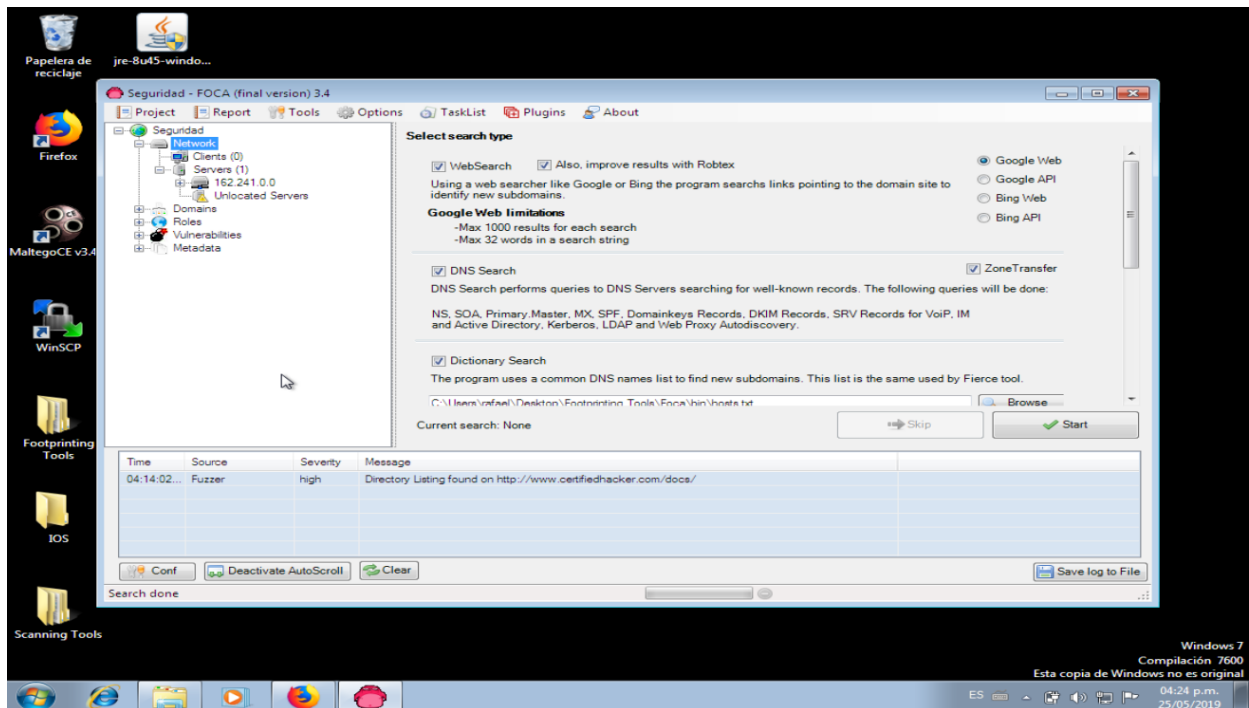
11. Ahora que la información del archivo está almacenada en el dominio, puede verla. Para ver la información, haga clic con el botón derecho en el archivo y haga clic en **Enlace-> Abrir en el navegador** desde el menú contextual.



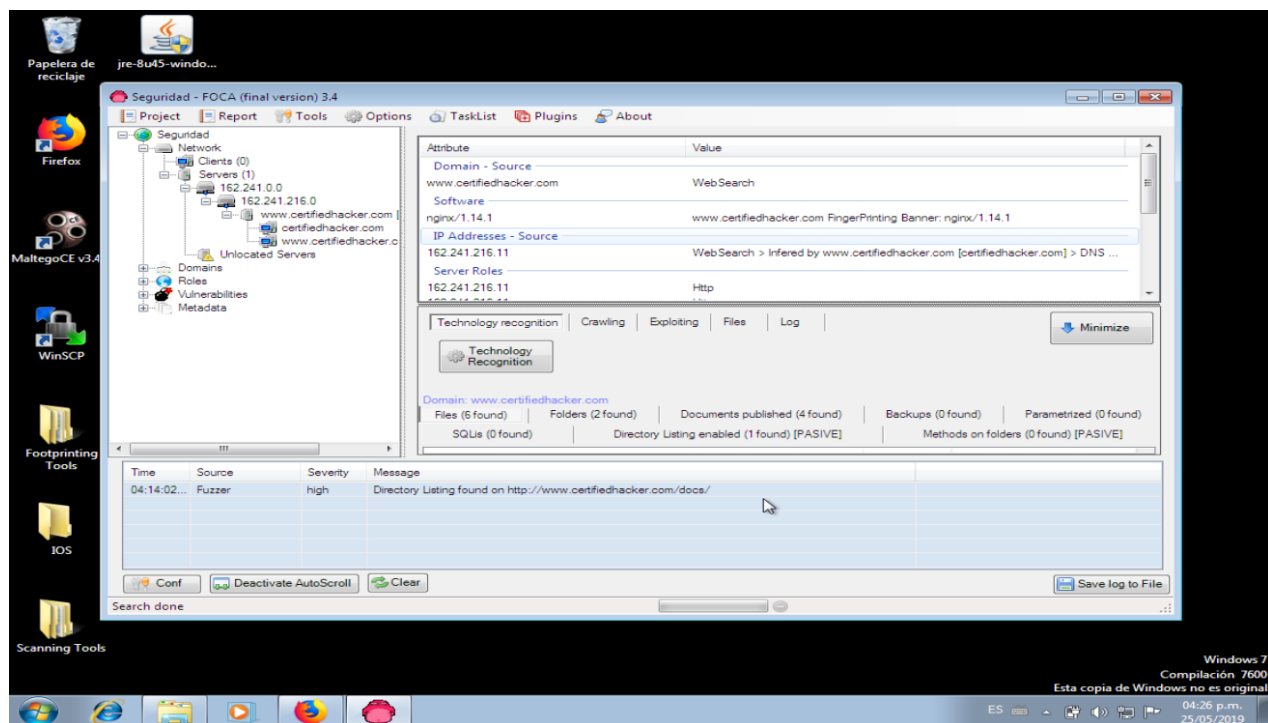
12. Ahora ha extraído los archivos del dominio utilizando FOCA.



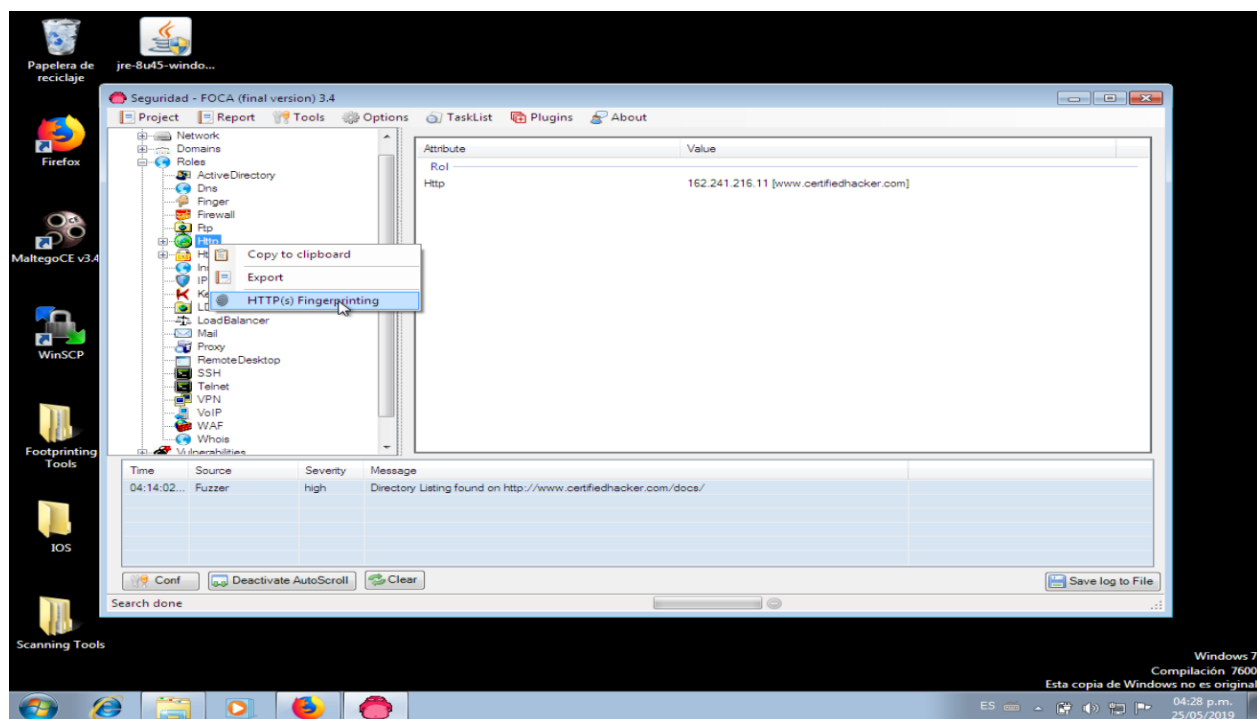
13. Haga clic en **nodo de red** en el panel izquierdo de la ventana para ver la estructura de la red.



14. Expande el nodo **Dominios** y muestra la dirección IP del dominio.



15. Expanda el nodo Roles, haga clic con el botón derecho en Http y haga clic en Huellas dactilares de HTTP en el menú contextual para tomar las huellas dactilares del sitio o dominio.



16. Expanda el nodo Https y haga clic en **Dominio** para ver la versión de IIS instalada en el servidor en el panel derecho.

