PRÁCTICA 4: Evidencias en los Navegadores Web

El análisis forense del navegador es un área de especialización grande e independiente.

Los navegadores web se usan en dispositivos móviles, tabletas, netbooks, computadoras de escritorio, etc., y a menudo se pueden usar no solo para navegar por la web, sino también para navegar a través del sistema de archivos del dispositivo. La memoria caché del navegador web puede contener imágenes, videos, documentos, archivos ejecutables y scripts descargados. Los navegadores web también pueden contener datos ingresados en formularios: consultas de búsqueda, inicios de sesión y contraseñas para cuentas de correo electrónico web, redes sociales, otros sitios web e información financiera (por ejemplo, números de tarjetas de crédito). Los favoritos y las búsquedas pueden dar al investigador una idea de los intereses del propietario del dispositivo.

El análisis forense de navegadores es principalmente de importancia en la respuesta a incidentes para comprender cómo comenzó un ataque a una computadora o red de computadoras y encontrar la fuente del compromiso de seguridad

Las principales fuentes de malware / spyware / adware son los correos electrónicos (incluidos los correos web), las redes sociales y otros sitios comprometidos. Normalmente, un usuario accede a todas estas fuentes (correos electrónicos web, redes sociales, sitios) mediante navegadores web.

Uno de los navegadores web más famosos es Internet Explorer. Este navegador es un componente del sistema operativo Windows y, a menudo, se utiliza como navegador web predeterminado. En Windows 10, Microsoft reemplazó Internet Explorer con Microsoft EDGE. Microsoft EDGE es un navegador web que contiene nuevas funciones. Microsoft planea reemplazar Internet Explorer con Microsoft EDGE en todos los dispositivos, incluidos los dispositivos móviles Android e iOS. Internet Explorer y Microsoft EDGE pueden funcionar en modo InPrivate, sin almacenar información sobre los recursos web visitados por el usuario.

Otro navegador web popular es Google Chrome. Tiene las siguientes características:

- Integración con los servicios de Google.
- Sincronización de contraseñas de usuarios entre dispositivos.
- La capacidad de utilizar extensiones y complementos.
- Operación rápida.
- Recopila datos del usuario.
- Consume gran cantidad de memoria.
- Google Chrome puede funcionar en modo incógnito, lo que evita que el navegador almacene permanentemente información del historial, cookies, datos del sitio o entradas de formularios.

Los desarrolladores de terceros han creado una gran cantidad de navegadores web basados en Chrome Engine, como: 360 Extreme Explorer, Avast SafeZone, Chromium, Comodo Dragon, CoolNovo, Cốc Cốc, Epic Browser, Flock, Vivaldi, Rockmelt, Sleipnir,

SRWare Iron, Titan Browser, Torch Browser, Yandex.Browser, Opera, Orbitum, Breach, Nihrome, Perk, QIP Surf, Baidu Spark, Uran, Chromodo, Sputnik, Amigo, etc.

Todos estos navegadores tienen una funcionalidad similar a Google Chrome y producen artefactos de navegador web como Google Chrome. Estos navegadores son compatibles con la mayoría de extensiones y complementos de Google Chrome.

Uno de los navegadores web más famosos con el motor de Google Chrome es Opera. Opera fue el primero en introducir características que adoptaron otros navegadores web: marcación rápida, bloqueo de ventanas emergentes, reapertura de páginas cerradas recientemente, navegación privada y navegación con pestañas. Además, Opera contiene un servicio gratuito de red privada virtual (VPN), que permite a los usuarios navegar por la web de forma anónima.

Firefox es un navegador web bastante popular, con artefactos que se pueden encontrar en los dispositivos bajo investigación. Este navegador web tiene las siguientes características:

- Más seguro (en comparación con otros navegadores).
- Modo incógnito avanzado, que inhabilita el seguimiento de las ubicaciones y los anuncios del usuario.
- Tiene sus propias extensiones.

Gecko es un motor de navegador desarrollado por Mozilla. Se utiliza en el navegador Firefox, el cliente de correo electrónico Thunderbird y muchos otros proyectos.

Basado en Gecko, los desarrolladores externos han creado varios navegadores web: Firefox, Waterfox, Cyberfox, SeaMonkey, Netscape Navigator, CometBird, BlackHawk, IceCat, IceDragon, Pale Moon, Flock, K-Meleon, Galeon, FlashFox, Orfox, Vega.

Parte de los datos de los navegadores web están cifrados (por ejemplo, contraseñas de sitios web). Internet Explorer en Microsoft EDGE utiliza la interfaz de programación de aplicaciones de protección de datos. El mecanismo DPAPI apareció en Windows 2000 y se utiliza para proteger las contraseñas almacenadas y la información confidencial en la computadora. Este mecanismo incluye las funciones de cifrado y descifrado de datos y RAM.

Necesita una contraseña de usuario para descifrar los datos cifrados. Si la contraseña está registrada en su cuenta usando el nombre de usuario y la contraseña, el sistema operativo usa el hash de la contraseña para descifrar los datos encriptados.

Como regla general, el cifrado de datos se lleva a cabo utilizando el algoritmo SHA1, sin embargo, en algunos casos, los datos se cifran utilizando un algoritmo menos resistente a la criptografía.

Un perito forense a menudo puede tener las siguientes dificultades al analizar navegadores web:

- Muchos navegadores, muchos datos

- Diferentes datos
- Cifrado utilizado para proteger los datos del usuario
- Uso del usuario del modo privado (o modo incógnito), en el que la computadora examinada no tiene artefactos del navegador web.

Por supuesto, cada navegador web deja sus propios artefactos individuales en el sistema operativo. Los tipos de artefactos del navegador web pueden variar según la versión del navegador web. Normalmente, al investigar artefactos de navegadores web, puede extraer los siguientes tipos de artefactos:

- Historial de navegación
- Ficheros en el directorio cache
- Cookies
- URL escritas
- Sesiones
- Sitios más visitados
- Capturas de pantalla
- Valores de formulario (búsquedas, autocompletar)
- Archivos descargados (Descargas)
- Favoritos

(Fuente: An Overview of Web Browser Forensics | Digital Forensics | Computer Forensics | Blog)

Objetivos principales de la práctica:

- **Identificar dónde se localizan las evidencias que generan los navegadores web y aprender a analizar las mismas utilizando diversas herramientas.**

Software a utilizar:

A. Explorador de archivos
B. Diversas herramientas que ofrece Nirsoft.

La práctica consiste en extraer todas las evidencias que se han citado anteriormente en la introducción (historial, descargas, cookies, cache, sesiones y datos de los formularios).

Se pide:

1. Utilizar el sistema operativo de tu propio equipo y/o alguna máquina virtual donde tengas instalados los navegadores más frecuentes: firefox, chrome e internet explorer.

2. Investigar las rutas de directorios donde cada uno de los navegadores guardan las evidencias.

3. Descargar y probar las distintas herramientas que ofrece Nirsoft para analizar y procesar las evidencias obtenidas en el apartado 2.