ANÁLISIS FORENSE

Unidad 5. Actividad 1

13 DE MAYO DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

RELACION DE EJERCICIOS T05

Ejercicio 1 (2 puntos) Describe que elementos debemos tener en cuenta a la hora de realizar una investigación en un coche.

Hay que tener en cuenta los siguientes elementos:

- Memoria USB: Las memorias usb que conectamos al coche, se pueden usar para actualizar el firmware de elementos no vitales para la seguridad, como el nevegador gps, la radio digital DAB+, el reproductor multimedia, los protocolos de conexión con el móvil, así como el firmware del aire acondicionado

- Conexión por bluetooth: El bluetooth del coche siempre está activo desde del momento que encendemos el motor, y no podemos desactivarlo a mano como el del móvil, eso puede dar lugar en ciudad a ataques de tipo Man in the Middle que permiten modificar las rutas que el usuario ha grabado en el gps. Algunas app gratuitas para coche permiten que el móvil, sin el conocimiento del usuario, actúe como una herramienta al servicio de los ciberdelincuentes para copiar las claves de acceso al coche y el arranque del motor.

- Llaves electrónicas: Las llaves de apertura por proximidad son muy codiciadas por los ciberdelincuentes, pues mediante un móvil normal y la app programada por ellos, en una cafetería podemos obtener los códigos de acceso, modelo y marca de estas llaves con situarnos cerca de los usuarios.

- Puerto OBD2: El puerto ODB2 es el conector estandar de los coches de obligado uso en todo el territorio de la Unión Europea, y se usa para acceder a todo el software del coche, sobre todo al software crítico como el que controla los frenos abs, el esp, el control del motor, etc.

- Sistemas de asistencia al conductor (ADAS): Los sistemas ADAS, como el control de crucero adaptativo, el frenado de emergencia automático y la asistencia de mantenimiento de carril, están cada vez más presentes en los vehículos modernos. Investigar su efectividad, precisión y posibles mejoras es crucial para la seguridad vial.

- Integración de dispositivos móviles: La integración de smartphones con el sistema de infoentretenimiento del automóvil permite funciones como la reproducción de música, la navegación y el uso de aplicaciones específicas. Investigar la interoperabilidad, la seguridad y la usabilidad de estas integraciones es importante para garantizar una experiencia de conducción segura y conveniente.

- Sistemas de propulsión alternativa: Con el aumento de los vehículos eléctricos y otras formas de propulsión alternativa, es importante investigar su eficiencia energética, autonomía, tiempos de carga y su impacto ambiental en comparación con los vehículos de combustión interna.

- Seguridad cibernética del vehículo: Los vehículos modernos están cada vez más conectados, lo que los hace vulnerables a ataques cibernéticos. Investigar las vulnerabilidades de seguridad y desarrollar medidas para proteger los sistemas críticos del vehículo contra intrusiones maliciosas es esencial para garantizar la seguridad del conductor y los pasajeros.

- Sensores y sistemas de monitoreo: Los vehículos modernos están equipados con una variedad de sensores y sistemas de monitoreo, como sensores de presión de neumáticos,

cámaras de visión trasera y sistemas de monitoreo de punto ciego. Investigar la precisión y la confiabilidad de estos sistemas, así como su capacidad para mejorar la seguridad y la comodidad del conductor, es importante para su desarrollo y mejora continua.

- Diseño ergonómico del interior del vehículo: El diseño del interior del vehículo, incluidos los controles, la disposición de los asientos y la accesibilidad de los compartimentos de almacenamiento, puede afectar la comodidad y la seguridad del conductor y los pasajeros. Investigar el diseño ergonómico del interior del vehículo y realizar pruebas de usabilidad puede ayudar a identificar áreas de mejora para proporcionar una experiencia de conducción más cómoda y segura.

Ejercicio 2 (2 puntos)

Describe como podemos acceder al modo de servicio de los últimos modelos de smart tv de Samsung, LG y Philips, y que información importante para una investigación podemos encontrar allí.

Samsung Smart TV:

Para acceder al modo de servicio en una Smart TV de Samsung, puedes seguir estos pasos:

Enciende la Smart TV y asegúrate de que esté en modo de espera.

En el control remoto, presiona secuencialmente las teclas: "Info", "Menú", "Mute", "Encendido".

Esto debería abrir el modo de servicio, mostrando un menú con opciones avanzadas y ajustes técnicos.

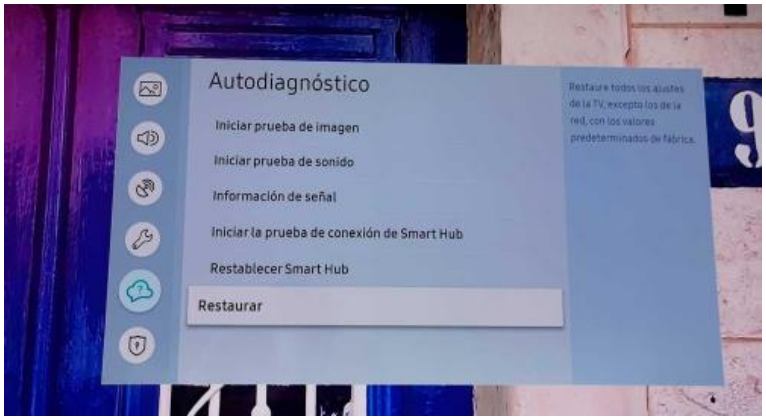
Una vez dentro del modo de servicio de Samsung, puedes encontrar información como:

Detalles sobre el firmware y el software del televisor, incluyendo la versión y la fecha de lanzamiento.

Configuración de la pantalla, como la temperatura de color, el brillo, el contraste, etc.

Información del hardware, como el modelo del panel, la capacidad de procesamiento, etc.

Registros de errores y diagnósticos del sistema que pueden proporcionar pistas sobre problemas técnicos.



LG Smart TV:

Para acceder al modo de servicio en una Smart TV de LG, puedes seguir estos pasos:

Enciende la Smart TV y asegúrate de que esté en modo de espera.

En el control remoto, presiona secuencialmente las teclas: "Settings" o "Configuración", "6", "5", "4", "3", "2", "1".

Esto debería abrir el modo de servicio de LG, mostrando un menú con opciones avanzadas y ajustes técnicos.

Dentro del modo de servicio de LG, puedes encontrar información similar a la de Samsung, incluyendo:

Detalles sobre el firmware y el software del televisor.

Configuración de la pantalla y del sonido, así como opciones avanzadas de calibración.

Información detallada sobre el hardware y los registros de errores del sistema.

Philips Smart TV:

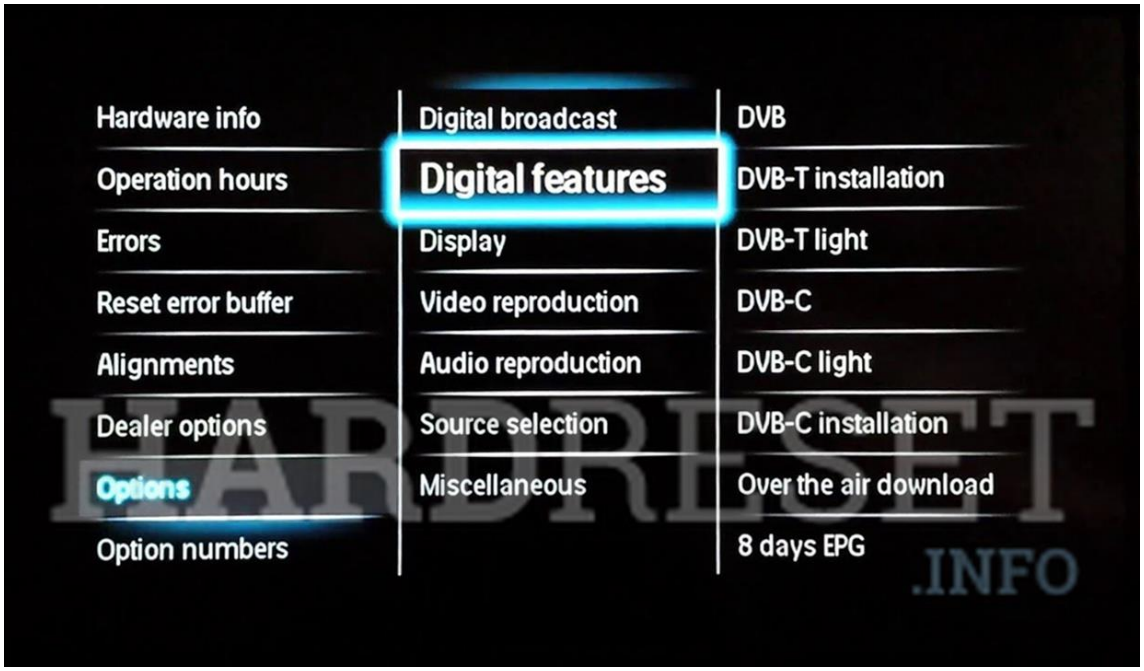
Acceder al modo de servicio en una Smart TV de Philips puede variar según el modelo, pero generalmente implica presionar una combinación específica de teclas en el control remoto o en el panel del televisor.

Una vez dentro del modo de servicio de Philips, puedes encontrar información similar a la de Samsung y LG, incluyendo:

Detalles sobre el firmware y el software del televisor.

Configuración de la pantalla y del sonido, así como opciones avanzadas de calibración.

Información sobre el hardware y los registros de errores del sistema.



Ejercicio 3 (6 puntos) Basándote en el documento sobre drones, redacta tu propio manual para realizar una investigación forense en un incidente con cualquier tipo de dron.

Seguridad inicial y preservación de la escena:

- Antes de entrar en la escena del incidente, evalúa los posibles riesgos y asegúrate de tener el equipo de protección adecuado.

- Delimita la escena del incidente utilizando cintas o barreras para evitar la contaminación de evidencia y asegurar la seguridad de las personas presentes.

- Si el incidente involucra lesiones personales o daños graves, coordina con las autoridades pertinentes, como la policía o los servicios de emergencia, antes de comenzar la investigación.

Documentación y recopilación de información:

- Registra meticulosamente la fecha, hora y ubicación exactas del incidente, así como cualquier condición climática o ambiental relevante.

- Toma fotografías y vídeos de la escena del incidente desde diferentes ángulos para documentar el contexto y cualquier daño visible.

- Entrevista a testigos presenciales para recopilar información sobre lo que observaron antes, durante y después del incidente.

Recopilación de evidencia física:

- Si es posible, recupera el dron involucrado en el incidente y manéjalo con cuidado para evitar daños adicionales o contaminación de evidencia.

- Examina el dron en busca de cualquier daño físico, como roturas, deformaciones o signos de impacto, y documenta estos hallazgos de manera detallada.

Extracción de datos del dron:

- Conecta el dron a un equipo de extracción de datos forenses utilizando cables y software especializados.

- Extrae y copia los datos almacenados en el dron, como registros de vuelo, imágenes y vídeos, asegurándote de mantener la integridad de la evidencia y la cadena de custodia en todo momento.

Análisis de los datos:

- Examina los registros de vuelo para reconstruir la trayectoria del dron antes, durante y después del incidente, identificando cualquier cambio inesperado de altitud, velocidad o dirección.

- Analiza las imágenes y vídeos almacenados en el dron para identificar posibles causas del incidente, como obstáculos, condiciones climáticas adversas o errores de pilotaje.

Entrevistas y análisis de testigos:

- Realiza entrevistas detalladas con cualquier persona que pueda tener información relevante sobre el incidente, incluyendo al operador del dron, testigos presenciales y cualquier persona afectada por el incidente.

- Corroborar la información obtenida durante las entrevistas con la evidencia física y los datos del dron para verificar su precisión y consistencia.

Informe forense:

- Documenta todos los hallazgos de la investigación en un informe forense exhaustivo, que incluya una descripción detallada del incidente, los datos recopilados, el análisis realizado y las conclusiones alcanzadas.

- Presenta el informe forense de manera clara y objetiva, utilizando gráficos, tablas y otros medios visuales para respaldar tus conclusiones y recomendaciones.

Cooperación con autoridades y partes interesadas:

- Colabora estrechamente con las autoridades pertinentes, como la policía, la aviación civil o los reguladores de drones, para proporcionar información relevante y apoyar cualquier investigación adicional que sea necesaria.

- Mantén una comunicación abierta y transparente con otras partes interesadas, como propietarios de propiedades afectadas o compañías de seguros, para garantizar una respuesta coordinada y eficaz al incidente.

Recomendaciones y prevención de futuros incidentes:

- Basándote en los hallazgos de la investigación, proporciona recomendaciones específicas para prevenir futuros incidentes similares, como la implementación de medidas de seguridad adicionales, la capacitación del personal o la revisión de las regulaciones y políticas existentes sobre el uso de drones en la zona afectada.

Seguimiento y revisión:

- Realizar un seguimiento de cualquier acción tomada como resultado de la investigación y revisa regularmente las medidas de seguridad y prevención implementadas para garantizar su eficacia a largo plazo.

- Mantener informado sobre los avances en la tecnología de drones y las mejores prácticas de seguridad para adaptar y mejorar continuamente tus procedimientos de investigación forense.