Guia de seguridad operacional para la comunidad de analistas forenses

Esta sección consolida la guía de seguridad operacional para quienes hacen adquisición en campo y analistas forenses que utilizan AQF y MVT como herramientas de forense consensual.

Preparación de la estación de trabajo

Dispositivo dedicado para adquisición:

Utiliza un dispositivo de propósito único para la adquisición (como una laptop dedicada, Raspberry Pi o similar). Nunca uses una máquina personal o de trabajo que contenga otros datos sensibles o credenciales de infraestructura organizacional.

Cifrado completo del disco:

Obligatorio en las estaciones de trabajo tanto de adquisición como de análisis. Esta es la principal defensa frente al escenario de Incautación Física. Usá LUKS en Linux, FileVault en macOS o BitLocker en Windows. Asegurate de que la máquina esté apagada (no solo en suspensión) cuando no esté en uso.

Aislamiento por caso

Directorio de trabajo nuevo por caso:

Nunca reutilices directorios de salida entre casos. Verificá que el directorio de salida esté vacío antes de iniciar la adquisición o el análisis.

Verificación manual del paquete:

Tras la adquisición, verifica que el paquete contiene los artefactos esperados (`packages.json` , `getprop.txt` , `bugreport.zip` , `files.json` , `dumpsys.txt` , etc.). Un archivo faltante o vacío podría indicar que la recolección falló silenciosamente.

Nota: si la salida de adquisición fue cifrada usando la clave pública de un tercero, no es posible descifrar el paquete para realizar esta verificación.

Cifrado y gestión de claves

Cifra siempre durante la adquisición:

Colocá una clave pública age válida en `key.txt` junto al binario de AQF. Nunca transportes paquetes en texto plano entre las etapas de adquisición y análisis. Si el cifrado no está disponible, trata el paquete en texto plano como altamente sensible y transfiérelo al analista mediante un canal cifrado; luego elimina de forma segura la copia local.

Verifica que el cifrado esté activo:

Usa AQF con el indicador `-v` (verbose) para verificar que el cifrado está habilitado y funcionando correctamente.

Separación de claves:

Almacena la clave privada (la contraparte de la clave pública usada como `key.txt` durante la adquisición) en un medio físico diferente al del paquete (distinto USB, distinto dispositivo). Nunca almacenes la clave privada en la estación de trabajo de adquisición. Si la estación es incautada, el paquete cifrado es inútil sin la clave.

Si no se necesita acceso a los registros en texto plano durante la adquisición, considera usar la clave pública del analista para el cifrado, para evitar retener capacidad de descifrado innecesaria. Tené en cuenta que esto impide que el responsable de adquisición verifique el contenido del paquete, por lo que los errores de recolección podrían pasar desapercibidos hasta el análisis.

Higiene de adquisición

Deshabilita las Opciones de Desarrollador tras la adquisición:

Deshabilita inmediatamente las Opciones de Desarrollador en el dispositivo de la persona defensora, tras completar la adquisición. AQF ya muestra este recordatorio, pero es fácil pasarlo por alto si hay presión de tiempo.

Higiene de la clave de autorización ADB:

Cuando el dispositivo pregunte «Allow USB debugging?», no marques «Always allow from this computer.». Optar por la confianza persistente almacena la clave pública RSA de ADB de la estación de adquisición en el dispositivo de la persona defensora. El operador deberá estar atento a ventanas emergentes de autorización adicionales en el teléfono durante la adquisición.

Transferencia y entrega de muestras

Canal de transferencia cifrado:

Transfiere muestras únicamente a través de canales cifrados. Por ejemplo, un archivo cifrado con age enviado por Signal, OnionShare o plataformas de terceros de confianza con cifrado de extremo a extremo.

Integridad de la muestra

Use el indicador -H:

Ejecuta MVT con `--hashes` (`-H`) para calcular los hashes SHA256 del paquete de entrada y registrarlos en `info.json` . Esto crea un registro independiente de exactamente qué fue analizado.

Gestión de datos post-análisis

Elimina de forma segura el material en texto plano:

Tras comunicar los hallazgos, elimina de forma segura los paquetes en texto plano, las muestras descifradas y los resultados del análisis de la estación de trabajo. Usa `shred` en Linux o herramientas equivalentes de eliminación segura. En SSDs, asegurate de habilitar el cifrado completo del disco, ya que la eliminación segura a nivel de archivo es poco fiable.

Conserva solo copias cifradas:

Si se necesita almacenamiento a largo plazo, conserva únicamente el paquete cifrado. El analista puede no necesitar conservar el paquete sin procesar tras producir los hallazgos.

Documenta una política de retención de datos:

Por cada encargo, definí: qué se conserva, por cuánto tiempo, dónde se almacena y quién tiene acceso. Comunicá esta política a la persona defensora cuyo dispositivo fue adquirido, para obtener su consentimiento.

Preparación ante incautación física

Asume que la incautación es posible:

La pregunta no es ¿ocurrirá?, sino ¿qué podrían encontrar?. Diseña tu configuración operacional de modo que una estación de trabajo incautada no proporcione nada utilizable.

Cifrado completo del disco:

Obligatorio en las estaciones de trabajo tanto de adquisición como de análisis. Esta es la principal defensa frente al escenario de Incautación Física. Usa LUKS en Linux, FileVault en macOS o BitLocker en Windows. Asegúrate de que la máquina esté apagada (no solo en suspensión) cuando no esté en uso.

Aprovecha el cifrado age de las muestras:

Si el paquete está cifrado con age y la clave privada se almacena en otro lugar (distinto USB, distinto dispositivo, con otra persona), una estación incautada contendrá únicamente datos cifrados opacos.

Prácticas operacionales adicionales

Verifica la integridad del binario de AQF antes de usarlo:

AQF se distribuye como un binario independiente desde los lanzamientos de GitHub. El responsable de adquisición debe verificar el checksum SHA256 del binario contra los hashes publicados en la versión antes de utilizarlo.

Compartimenta las estaciones de trabajo de adquisición y análisis:

Si es posible, utiliza máquinas físicas separadas para la adquisición y el análisis. La estación de adquisición se conecta a dispositivos potencialmente comprometidos mediante USB/ADB, mientras que la estación de análisis opera únicamente sobre archivos de paquetes.