

# Documentación de los procedimientos de análisis Forense de Computadores

Por: Jhon J. Barbara

Hay examinadores de trabajo en algunos organismos policiales que NO han documentado la técnica de Procedimientos Operativos Estándar, en inglés standard operating procedures (SOP) para el análisis de los medios digitales. Lo más probable es que no existen Prácticas de Garantía de Calidad, en inglés Quality Assurance Practices (QAP) y no están siguiendo los Sistemas de Aseguramiento de la Calidad, en inglés Quality Assurance Systems (QAS) en estos organismos para la supervisión. Uno de los requisitos de un QAS es el desarrollo de un Manual de Garantía de Calidad, en inglés Quality Assurance Manual (QAM). El QAM incluiría la afirmación de que los SOP deben estar documentados y disponibles para los examinadores de uso. SOP podrían incorporarse en el propio QAM o documentados en un sistema autónomo del manual. Es inaceptable para cualquier investigador que analiza los medios digitales no tener una QAS, una QAM, y la documentación SOP. Sin estos tres componentes fundamentales, no hay garantías para demostrar que las QAPs existen y que se utilizan para proporcionar resultados que son precios, repetibles y confiables en juicios. Cuando un examinador se hace consciente de que se necesita documentarse con SOP en general, él o ella hace dos preguntas: "¿Qué tipo de esquema o formato debo utilizar?" Y "¿Cuánto detalle debo poner mi hoja técnica SOP?". El uso de ese esbozo, una política y un procedimiento para el análisis de las unidades de disco duro extraíble, se muestra a continuación. No se pretende que se incluyan a todas las partes y debe considerarse como una guía técnica para redactar SOP.

Informática forense manual de operaciones:

1. Nombre de la Política: imágenes de los discos duros removibles
2. Política Número / Versión: 1,0
3. Asunto: Imágenes y análisis de las pruebas de las unidades de disco duro extraíble.
4. Propósito: Documento para el procedimiento de imágenes y el análisis de diferentes tipos de pruebas, las unidades de disco duro removido de las computadoras de escritorio o portátil.
5. Control de documentos: Aprobado Por / Fecha:

Fecha de Revisión / Número de revisiones:

6. Autoridad Responsable: El Director de Calidad (o su designado).

7. Las normas relacionadas con la / Estatutos / Referencias:

- A) ASCLD / LAB normas legales 1.4.2.5, 1.4.2.6, 1.4.2.7, 1.4.2.8, 1.4.2.11, y 1. 4.2.12.
- B) ASCLD / LAB Requisitos suplementarios internacionales: 3 (Términos y definiciones), 4.13.2.4, 5.4.1.1, 5.4.1.2, 5.4.2.1.
- C) ISO / IEC 17025:2005 cláusulas: 4.1.5 (f, g, h, i) de 4.2.1, 4.2.2 (d) 4.2.5, 4.3.1, 4.15.1, 5.3.2, 5.4.1, 5.4.4, 5.4.5.2, 5.4.7.2 (a-c), Todos de 5,5, todos de 5,8, y 5.9.1 (una).8. Ámbito de aplicación: las imágenes y el examen de los diferentes tipos de unidades de disco duro (SATA, SCSI y IDE) removido de los ordenadores de sobremesa y portátiles.

9. Declaración de política:

A) No se realizó el análisis sin autorización legal (orden de registro o formulario de consentimiento). Si no se han presentado, el examinador debe ponerse en contacto con el investigador para obtener la necesaria autoridad legal. (Fiscal, Juez, Etc.)

B) Las computadoras a examinar no están conectadas a la Red o Internet.

C) Todos los archivos forenses creados y los datos recuperados en los exámenes se consideran pruebas.

D) Los cambios a este procedimiento pueden hacerse solo en caso de ser aprobada por el Director de Calidad, en el documento de los cambios y garantizar que el procedimiento revisado sea validado, en caso necesario, antes de su utilización en la tramitación de casos.

10. Procedimiento:

A) Responsabilidades

1. Supervisor

- a) Sólo examinadores capacitados se asignan al caso.
- b) Personal administrativo y técnico revisa el expediente.

2. Examinadores

- a) Informe directamente al supervisor.
- b) Deben estar familiarizados con todos los tipos de unidades de disco duro que se pueden encontrar como prueba.
- c) Responsables del registro de la cadena de custodia, manipulación de pruebas, pruebas y marcado de seguridad, y el análisis de las pruebas.
- d) Generar informes y ser dar su testimonio ante los tribunales. (Como expertos o peritos)

## B) Exámen de las pruebas

1. Autoridad Legal: Los examinadores deben revisar la orden de registro o el formulario de consentimiento para determinar el alcance del examen. Póngase en contacto con el investigador o policia para obtener una lista de palabras clave, si ésta no existe.

2. Cadena de Custodia: Todas transferencias de las pruebas son documentadas en el sistema de seguimiento de la evidencia. (escrito para su seguimiento)

3. Seguridad: Aplicable a todas las partes de la agencia de seguridad y el manual de la unidad de "Manejo de Medios Digitales" la política y el procedimiento que se siguió en su caso. (esto con el fin de no perder nada)

### 4. Equipo y Materiales:

- a) Lapíz marcador, Icinta adhesiva, material de envasado y embalaje antiestático, hojas de trabajo, etc
- b) Computadoras Forenses
- c) Software aprobado para uso forense
- d) Nuevos y esterilizados medios digitales (CD, DVD, discos duros, etc)
- e) La Verificación / validación de hardware y de las interfaces de los bloqueadores de escritura
- f) Cruce de cables
- g) Esamble / desmontaje de herramientas
- h) Cámara digital
- i) Disco duro adecuado a las normas y controles

### 5. Consideraciones Especiales

- a) Si las unidades de disco duro no se eliminan o una configuración RAID existe, se refieren a "Cable Imaging", "RAID Imaging," y / o "imagen DOS" procedimiento (s).
- b) Los discos duros pueden ser protegidos por contraseña. Refiérase a Procedimiento de "Rompiendo contraseñas".

### 6. Prueba de documentación, manipulación, y de Inventario:

- a) Fotografíe e imprima las imágenes de las pruebas para el expediente del caso.
- b) Inventarie / describa las pruebas. Guarde los números de serie en el archivo del caso.
- c) Marque las pruebas de acuerdo al "manual de manipulación de evidencia digital"

### C) Análisis del Disco Duro:

1. Seleccione apropiadamente el disco duro estándar, el control y la interfaz / escritura bloqueador.
2. Registre en el computador forense el POST en el equipo.
3. Imagen de la unidad de disco duro estándar y control. Registre el valor en tanto del instrumento diario a bordo y el archivo del caso.
4. Complete la "Hoja de Documentación de hardware."
5. Remueva la evidencia del disco duro (s).
6. Obtenga la información de la BIOS desde el computador forense.
7. Adjunte las pruebas del disco duro (s) para las interfaces adecuadas y / o bloqueadores de escritura y de la imagen en el disco duro borrado (s).
8. Verifique los valores de hash y cree un archivo(s) forense en un medio digital no modificable de comunicación siempre que sea posible.
9. Examine la imagen usando un software (s) de verificación.
10. Complete la "hoja de trabajo de análisis."
11. Exporte los datos probatorios a soportes digitales (CD y DVD, discos duros, etc.)
12. Prepare el informe y presente el expediente a revisión, reenvase las pruebas y regrese a la cadena de custodia.

La política y procedimiento de ejemplo está escrito en un esquema de formato y referencias a hojas de trabajo y otros procedimientos. Los organismos policiales pueden decidir utilizar un estilo narrativo e incorporar procedimientos de la que se hace referencia en un procedimiento detallado. Esa sería su elección. Independientemente de la cantidad de detalles incluidos, la consideración más importante es que todos los procedimientos normales de operación técnica, debe documentarse.

John J. Barbara is a Crime Laboratory Analyst Supervisor with the Florida Department of Law Enforcement (FDLE) in Tampa, FL. John J. Barbara es un Delito Laboratory Analyst Supervisor con la Florida Departamento de Aplicación de la Ley (FDLE), en Tampa, FL. An ASCLD/LAB inspector since 1993, John has conducted inspections in several forensic disciplines including Digital Evidence.

**Definiciones:**

Procedimientos Operativos Estándar, en inglés standard operating procedures (SOP)

Prácticas de Garantía de Calidad, en inglés Quality Assurance Practices (QAP)

Sistemas de Aseguramiento de la Calidad, en inglés Quality Assurance Systems (QAS)

Manual de Garantía de Calidad, en inglés Quality Assurance Manual (QAM)