Ing. Esp. LUIS FERNANDO BARAJAS ARDILA
Especialista en Seguridad Informática
Magister c Seguridad Informatica Universidad de la Rioja-España
EnCase Certified Examiner - EnCE
AccessData Certified Examiner - ACE
Perito en Informática Forense
Docente Unab – UDI
Formador United States Department Of Justice ICITAP - OPDAT

Antiterrorism Assistance Program Bureau of Diplomatic Security (A.T.A)
United States Department Of Justice, International Criminal Investigative Training Assistance Program – ICITAP-USA

febarajas@gmail.com - @ferchoweb

EVIDENCIA DÍGITAL

Evidencia Digital

La evidencia digital es única, cuando se le compara con otras formas de "evidencia documental". A comparación de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es identica al original. Otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizo una copia. Esta situación genera problemas con respecto al robo de información comercial "secretos Industriales".

Se debe tener en cuenta que los datos digitales adquiridos de copias no se deben alterar de los originales del disco, porque automáticamente se invalidaría la evidencia. Es por esta razón que los investigadores deben revisar constantemente sus copias, y que sean exactamente igual a la original. CHECKSUM ó HASH

Evidencia Digital

La IOCE (International Organization On Computer Evidence) define los siguientes puntos como los principios para el manejo y recolección de evidencias computacional:

- Sobre recolectar evidencia digital, las acciones tomadas no deben cambiar por ningún motivo ésta evidencia.
- Cuando es necesario que una persona tenga acceso a evidencia digital original, esa persona debe ser un profesional forense.
- Toda la actividad referente a la recolección, el acceso y el almacenamiento, o a la transferencia de la evidencia digital, debe ser documentada completamente preservada y disponible para la revisión.
- Un individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital mientras que esté en su posesión.
- Cualquier agencia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.

Evidencia Digital

Además definen que los principios desarrollados para la recuperación estandarizada de evidencia computacional se debe gobernar bajo las siguientes premisas:

- ✓Consistencia con todos los sistemas legales.
- ✓Permitir el uso de un lenguaje común.
- ✓Durabilidad.
- ✓Capacidad de cruzar límites internacionales.
- ✓Capacidad de Ofrecer confianza en la integridad de las evidencias.
- ✓Aplicabilidad a todas las evidencias forenses.

UNIVERSITARIA
DE INVESTIGACIÓN
Y DESARROLLO

Evidencia Digital

CADENA DE CUSTODIA

UDI UNIVERSITARIA DE INVESTIGACIÓN Y DESARROLLO

CADENA DE CUSTODIA (Artículos 254 y 265 CPP)

Es un sistema documentado que se aplica a los EMP y EF por las personas responsables del manejo de los mismos, desde el momento en que se encuentran o aportan a la investigación hasta su disposición final, lo que permite no solo garantizar su autenticidad, sino demostrar que se han aplicado los procedimientos estandarizados para asegurar las condiciones de identidad, integridad, preservación, seguridad, continuidad y registro.

UDI UNIVERSITARIA DE INVESTIGACIÓN Y DESARROLLO

Cadena de Custodia

Autenticidad del EMP o EF

Identidad: Es la individualización de los EMP y EF mediante la descripción completa y detallada de todas las características, teniendo en cuenta los pasos de descripción objetiva de cada elemento o sustancia como: color, peso, forma, cantidad, medida, volumen, tipo de construcción y estado, entre otras.

Integridad: Determina que el EMP o EF allegado a la investigación conforme al debido proceso es el mismo que se utiliza para tomar la decisión judicial.

Preservación: Es asegurar las condiciones adecuadas de conservación e inalterabilidad de los EMP y EF de acuerdo con su clase o naturaleza.

UDI UNIVERSITARIA DE INVESTIGACIÓN Y DESARROLLO

Cadena de Custodia

Autenticidad del EMP o EF

Seguridad: Esta a cargo de los custodios, quienes deberán mantener libres y exentos de todo riesgo y peligro a los EMP y EF.

Almacenamiento: Es la acción o efecto de guardar los EMP y EF bajo condiciones adecuadas para garantizar su preservación y protección.

Continuidad y Registro: Es la secuencia ininterrumpida de todos los traslados y traspasos de los EMP y EF entre custodios, garantizada mediante el registro único de cadena de custodia.

ROTULO ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA - FPJ - 07-

Versión 2 - Resolución F.G.N.

1. CODIGO UNICO DE CASO

6 1	0 0	1	6 0	0 0 0 1 3	2 0 0 6	0 0 0 0 1
DPTO	MUNICIPIO	ENTIDAD	UNIDAD	AÑO	CONSECUTIVO	

2. FECHA Y HORA RECOLECCION

FORMATO MILITAR

D D	M M	A A	

3. MUESTRA

NUMERO DE HALLAZGO

CANTIDAD

UNIIDAD DE MEDIDA

4. SITIO O LUGAR DE HALLAZGO DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA

DESCRIPCIÓN

NOMBRES Y APELLIDOS DE LA PERSONA A QUIEN SE LE ENCONTRO EL ELEMENTO

DELITO A INVESTIGAR:

5. DESCRIPCION DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA

6. RECOLECCION DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA

NOMBRES Y APELLIDOS	CEDULA CIUDADANIA	ENTIDAD	CARGO	FIRMA

UNIVERSITARIA
DE INVESTIGACIÓN
Y DESARROLLO

REGISTRO DE CADENA DE CUSTODIA FPJ – 08

Versión 2 - Resolución F.G.N.

UBICACION EN LA BODEGA (*)

Número

1. CODIGO UNICO DE CASO

DPTO	MUNICIPIO	ENTIDAD	UNIDAD	AÑO	CONSECUTIVO

2. HISTORIA CLINICA (**)

Número

3. DOCUMENTACION DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA

H	R	E	NOMBRES Y APELLIDOS	CEDULA DE CIUDADANIA	ENTIDAD	CARGO	FIRMA

4 TIPO DE EMBALAJE

Cantidad Bolsa Plástica ☐ ___ De papel ☐ ___	Cantidad Frasco ☐ ___ Caja ☐ ___	Otro ☐ Cantidad Cual ? _____ _____ _____

5. DESCRIPCION DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA

_____

_____

_____

Convenciones:

(*) Para ser diligenciado exclusivamente por la Bodega General de Evidencias de la Fiscalía General de la Nación, con la posición que le correspondió a la evidencia al interior de la Bodega.

(**) Para ser diligenciado por la Entidad Prestadora de Salud que recolecte el Elemento Material Probatorio o Evidencia Física.

H = Marque con una X si corresponde a quien HALLÓ el Elemento Materia de Prueba o Evidencia Física.

R = Marque con una X si corresponde a quien RECOLECTÓ el Elemento Materia de Prueba o Evidencia Física.

E = Marque con una X si corresponde a quien EMBALÓ el Elemento Materia de Prueba o Evidencia Física.

Se puede marcar una o varias opciones para un mismo nombre, según sea el caso.

6. REGISTRO DE CONTINUIDAD DE LOS ELEMENTOS MATERIA DE PRUEBA O EVIDENCIA

UNIVERSITARIA DE INVESTIGACIÓN Y DESARROLLO

FECHA	HORA MILITAR	NOMBRES Y APELLIDOS DE QUIEN RECIBE EL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA	CEDULA DE CIUDADANIA	ENTIDAD	CALIDAD EN LA QUE ACTUA (Custodio, Perito, Transportador)	PROPOSITO DEL TRASPASO O TRALADO (Entrega Almacén, Almacenamiento, Análisis, Presentación Audiencia, Consulta, Disposición Final)	OBSERVACIONES AL ESTADO EN QUE SE RECIBE EL EMBALAJE O CONTENEDOR DEL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA	FIRMA
D D M M A A								
D D M M A A								
D D M M A A								
D D M M A A								
D D M M A A								
D D M M A A								
D D M M A A								
D D M M A A								
D D M M A A								

7. PARA SER DILIGENCIADO POR EL TECNICO EN PRUEBA DE IDENTIFICACION PRELIMINAR HOMOLOGADA "PIPH"

PRACTICO PRUEBA PRELIMINAR ?	CANTIDAD DE MUESTRAS TOMADAS	ROTULOS Nos.:
SI ☐ NO ☐	_____	_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

NOTA:

1) NUNCA INTERRUMPA EL REGISTRO DE CADENA DE CUSTODIA.
2) EL REGISTRO DE CADENA DE CUSTODIA SIEMPRE DEBE ACOMPAÑAR AL ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FISICA
3) SI ESTA HOJA NO ALCANZA PARA DILIGENCIAR LOS REGISTROS DE CONTINUIDAD DE CADENA DE CUSTODIA, SE PUEDE UTILIZAR TANTAS HOJAS ADICIONALES SEAN NECESARIO. DE SER ASI, EN LA PARTE SUPERIOR DERECHA DE CADA HOJA SE INDICARA EL NUMERO UNICO DEL CASO Y EL DE LA HOJA A QUE CORRESPONDE DEL TOTAL DE HOJAS QUE CONFORMAN EL REGISTRO DE CONTINUIDAD.

REGISTRO DE CONTROL DE IMÁGENES DE EVIDENCIA DIGITALES

1. CODIGO UNICO DE CASO

1	1	0	0	1	6	0	0	0	0	1	3	2	0	0	6	0	0	0	0	1
DPTO		MUNICIPIO			ENTIDAD		UNIDAD					AÑO				CONSECUTIVO				

DESCRIPCIÓN DE LA EVIDENCIA DIGITAL

FECHA	*HORA*	*FUNCIONARIO*	*ENTIDAD*	*FIRMA*

K I T

UNIVERSITARIA
DE INVESTIGACIÓN
Y DESARROLLO

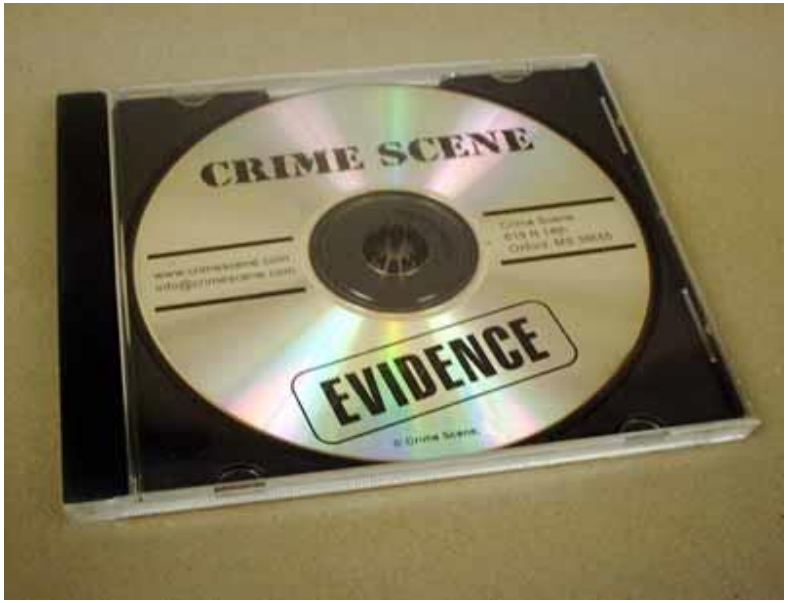
Elementos Necesarios Para Manejo de Evidencias Digitales

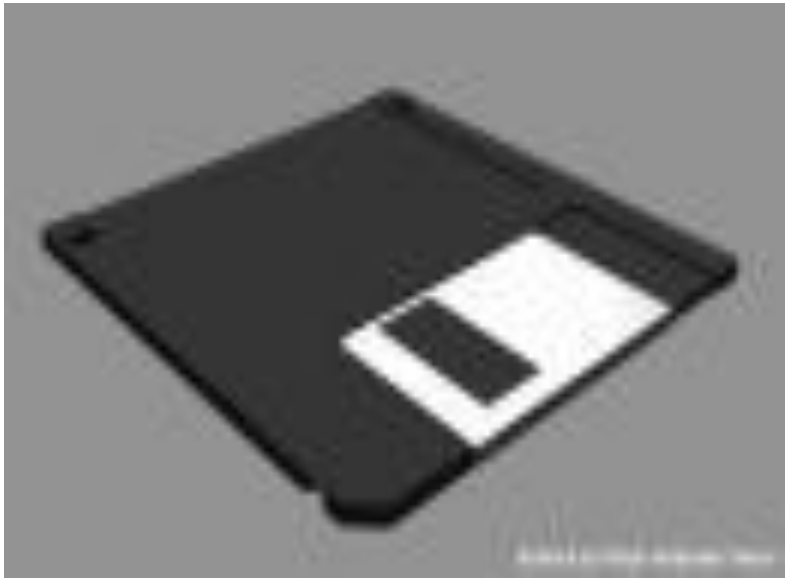
Manilla Antiestática

UNIVERSITARIA
DE INVESTIGACIÓN
Y DESARROLLO

Elementos Necesarios Para Manejo de Evidencias Digitales

CD ROM - DISQUETE





Elementos Necesarios Para Manejo de Evidencias Digitales

Bloqueadores Conectores

UNIVERSITARIA
DE INVESTIGACIÓN
Y DESARROLLO

Elementos Necesarios Para Manejo de Evidencias Digitales

Kit de Herramientas

UNIVERSITARIA
DE INVESTIGACIÓN
Y DESARROLLO

Elementos Necesarios Para Manejo de Evidencias Digitales

Portátil - Discos Duros

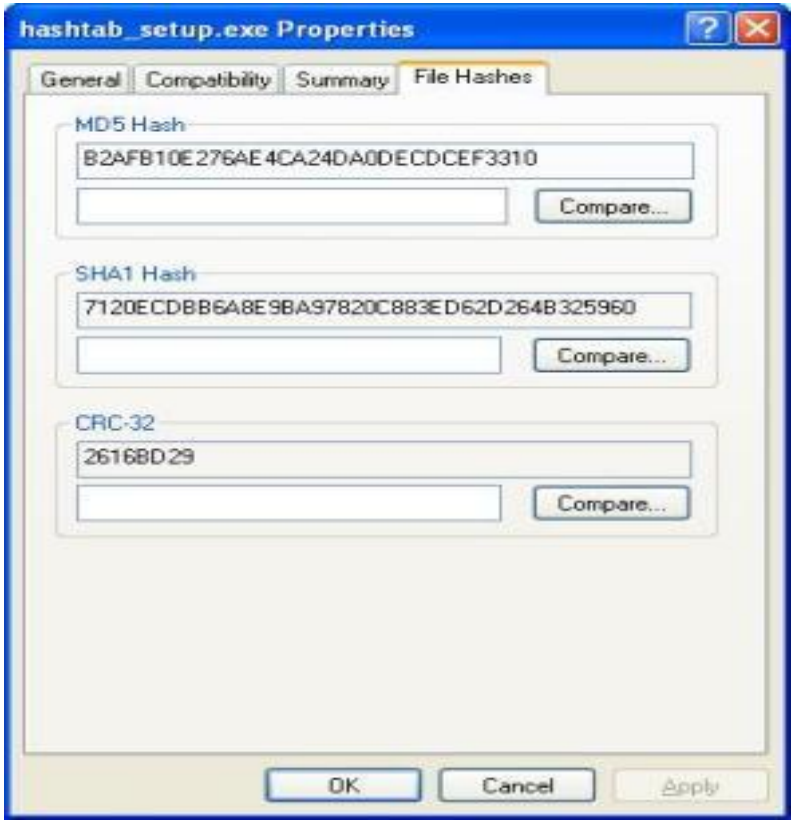
UNIVERSITARIA
DE INVESTIGACIÓN
Y DESARROLLO

Elementos Necesarios Para Manejo de Evidencias Digitales

Programas para realizar borrado seguro

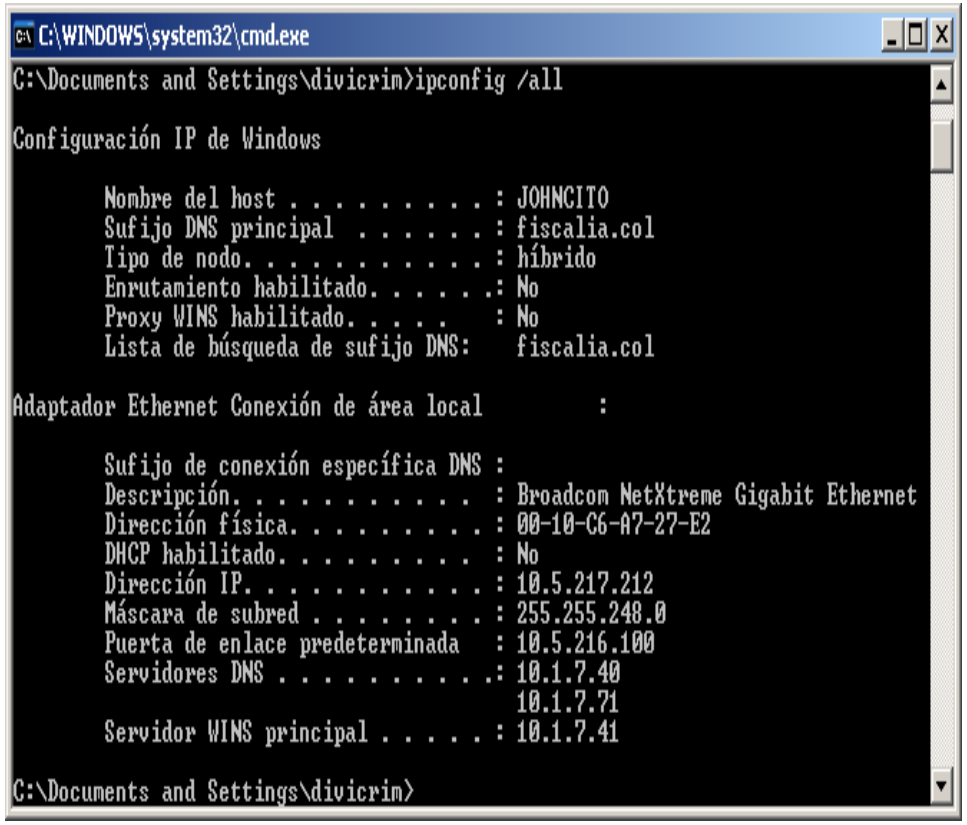
Elementos Necesarios Para Manejo de Evidencias Digitales

Programas para extraer huellas digitales



Elementos Necesarios Para Manejo de Evidencias Digitales

PROGRAMAS PARA EXTRAER DATOS VOLÁTILES



Elementos Necesarios Para Manejo de Evidencias Digitales

PROGRAMAS PARA EXTRAER IMÁGENES FORENSES

Guidance™ Software

AccessData

UDI UNIVERSITARIA DE INVESTIGACIÓN Y DESARROLLO

INFORMÁTICA FORENSE Y SUS PROCEDIMIENTOS

UNIVERSITARIA
DE INVESTIGACIÓN
Y DESARROLLO

Investigaciones Relacionadas con Sistemas de Información

Reacción al Incidente informático.

Manejo del lugar de la escena (escena virtual).

Recolección de las evidencias digitales.

Análisis de la información recopilada vs. EMP.

Exposición de los resultados.

Testimonio en juicio.

UDI UNIVERSITARIA DE INVESTIGACIÓN Y DESARROLLO

INVESTIGACIONES RELACIONADAS CON SISTEMAS DE INFORMACIÓN

PROCEDIMIENTO UTILIZADO

***S**e realiza un análisis del procedimiento utilizado por la organización en donde ocurrió el fraude, ejemplo: Robo a través del departamento de ventas.*

***D**etermina como interviene el sistema de información en el proceso, ejemplo: los datos que se ingresan en cada proceso.*

***E**studia los mecanismos de seguridad que posee el sistema de información para preservar la integridad, confidencialidad y seguridad de los datos.*

***S**olicita todos los EMP o EF que se requieren para determinar la ocurrencia del hecho, y la responsabilidad del indiciado.*

***L**os resultados, producto del análisis de la información recopilada, que en últimas son los EMP y EF hallados, recogidos y embalados.*

UNIVERSITARIA
DE INVESTIGACIÓN
Y DESARROLLO

INVESTIGACIONES RELACIONADAS CON ANÁLISIS A MEDIOS DE ALMACENAMIENTO MAGNÉTICO

Reacción al Incidente informático.

Manejo del lugar de la escena (escena virtual).

Recolección de las evidencias digitales.

Análisis de los EMP.

Exposición de los resultados.

Testimonio en juicio.

UNIVERSITARIA
DE INVESTIGACIÓN
Y DESARROLLO

INVESTIGACIONES RELACIONADAS CON ANÁLISIS A MEDIOS DE ALMACENAMIENTO MAGNÉTICO

PROCEDIMIENTO UTILIZADO

S*e hallan recogen los datos volátiles de la maquina en caso de estar encendida, y posteriormente se hace una descripción de equipo detallando todo lo encontrado.*

P*roceso de cadena de custodia.*

S*e realiza una imagen al medio de almacenamiento magnético.*

L*os resultados, producto del análisis de la información recopilada, que en últimas son los EMP y EF hallados, recogidos y embalados.*

UNIVERSITARIA
DE INVESTIGACIÓN
Y DESARROLLO

Investigaciones Relacionadas con Internet

Reacción al Incidente informático.

Manejo del lugar de la escena (escena virtual).

Recolección de las evidencias digitales.

Análisis de la información recopilada vs. EMP.

Exposición de los resultados.

Testimonio en juicio.

UNIVERSITARIA
DE INVESTIGACIÓN
Y DESARROLLO

INVESTIGACIONES RELACIONADAS CON INTERNET (correos electrónicos)

PROCEDIMIENTO UTILIZADO

Se cita a la persona que coloco la denuncia con el propósito de ingresar a su cuenta electrónica, y así extraer los mensajes de carácter amenazante, injurioso o extorsivos.

Se ingresa al correo electrónico de la persona, en donde es ella quien digita su usuario y contraseña. Es importante resaltar que para fijar estas acciones se utiliza la función PrintScreen, con la finalidad de documentar el proceso paso a paso.

Se buscan los mensajes producto de la denuncia, y se configura la presentación del correo electrónico, de tal forma que nos permita ver los encabezados de direccionamiento IP.

Se extraen los mismos como Elementos Materiales Probatorios mediante una impresión y de ser posible se guardan en un medio de almacenamiento magnético para que hagan parte del caso como evidencias físicas.

Se realiza todo el proceso de cadena de custodia.

Con el encabezado de direccionamiento IP se obtiene el ISP, a quien se le solicita la información de datos biográficos de la persona que tiene adjudicada esa dirección IP.

UNIVERSITARIA
DE INVESTIGACIÓN
Y DESARROLLO

INVESTIGACIONES RELACIONADAS CON INTERNET (Páginas Web)

PROCEDIMIENTO UTILIZADO

Se ingresa a la página web con el fin de determinar su existencia.

Una vez se comprueba su disponibilidad en la red, se procede a extraer mediante la función PrintScreen el contenido de la misma, tal como la esta presentando en ese momento.

Se trata de determinar algún tipo de contacto a través del contenido.

Posteriormente, mediante la instrucción ping se determina la dirección IP que posee la misma en la red Internet.

Determina el país de origen, y el ISP que provee el servicio de conectividad a la gran red.

Se envía solicitud al ministerio de comunicaciones para que bloquee el ingreso de esa página a Colombia.