Parámetros Generales para el Examen en Sistemas Windows

***Preparar*:**
_____Revisar Orden de Registro
_____Revisar Caso
_____Notar Fecha y Horas de CMOS
_____Preparar hoja de examen MECTF

Preparación del Caso
_____Preparar el Disco Forense—borrar, verificar, partición, formatear, nombrar "Forensic"
_____Crear una carpeta Imagen
_____Crear una carpeta para Caso Analizado
_____ENCASE—Preparación de Nuevo Caso, preparar carpetas de favoritos (editar el formato del texto)
_____Grabar el nuevo caso
_____Añadir Dispositivo—bloqueada la escritura
_____Adquirir disco—reemplazar disco de origen
Si el disco es adquirido con FTK, asegurarse de que los archivos eo1.txt sean movido a la carpeta de reporte del caso.

Administración Interna
_____Reconstruir la biblioteca de Hash—si se utilizó
_____Palabras clave—escoger/introducir

Primero
_____1) Barrer—Empezar la Exportación de caso a Excel—ponerlo en HTML, Linux Sweep
_____2) Partition Finder EnScript Favorito como "VBR" (Vaya a favorito, visión del disco, offset @—Click derecho—añadir partición)
_____3) Recuperar carpetas perdidas—click derecho sobre cada volumen
_____4) Modificar la zona horaria en la medida en que sea necesario
_____5) Mount (ver estructura de los archivos)—thumbs.db, zip, rar
_____6) Correr File Signature, Hash, Búsqueda inicial por palabras clave
_____7) Barrer el Registro

*****CP Caso—Correr el barrido de File Finder, SPL Sweep*****

Revisar las particiones para cada medio adquirido

_____Subraye el disco físico—exporte el volumen y los registros del dispositivo

_____Revise la tabla de partición en MBR—ver disco, sector físico 0 offset del archivo 446, 64 Bytes—marcar como favorito la tabla de partición—seleccionar 64 bytes y en vista de favoritos el número de registro (cualquiera con cero u oculto)

_____Exportar reportes sobre la estructura de las carpetas

Barridos

_____Correr **EFS**—el resultado es el almacenamiento seguro

_____Archivos **Info2**

_____Papelera de **reciclaje**

_____File Finder—**Gráficos** en espacio no-asignado—añadir al caso

Gráficos en File Slack—añadir al caso

_____Archivos **Link**

_____Direcciones de correos electrónicos

_____Visor **Exif**—memoria flash

_____HTML Carver

_____EDS Registry Parser

_____Script de Tarjeta de Crédito

_____Chat Parser

_____Información AOL IM

_____Registros Kazaa

_____Archivo de IM—MSN & Yahoo

_____Barrido SPL—Archivos Spool

Vista a través

_____Programas para inicializar el barrido—¿tipos específicos de archivos?

_____Marcar como favorito: como terminado

_____Papelera de reciclaje (resaltar empezando con la C:)

_____Green Home Plate—Visor de gráficos para todos los gráficos, archivos SPL, thumbs.db

_____Aciertos de búsquedas por palabras clave (EMF—destaca 41 bytes de B4, sí en columna pix, ordenar nombre de archivo y offset del archivo—ver)

_____Lengüeta de Correo electrónico—favorito, reporte

_____Lengüeta de historial de Internet

_____Lengüeta de Caché de Internet

_____Firmas—¿problemas?

_____Archivos de registros

_____Archivos DAT

Index.dat—usa un programa de análisis de red

_____Carpeta de Documents and Settings específica al usuario

Condiciones
_____DOC, TXT, etc.

Malware—asegurarse de tener actualizaciones en el computador forense
_____Subir y buscar—Gargoyle, spybot, adaware, antivirus

FTK
_____Revisar Registros—NTUser.dat

_____Hacer Hash de nuevo al archivo de imagen como última verificación de que nada ha cambiado

Reporte del Caso
_____Exportar Reportes
_____Combinar