COMPUTER FORENSIC EXAMINATION FORM

EXAM ADMINSTRATION INFORMATION

Case #: _____ Case Title: _____

Examiner: _____ Case Agent: _____

Date Evidence Seized: _____/_____/_____ Location Seized: _____

_____

Date Exam Started: _____/_____/_____ Location of Exam: _____

Date Exam Ended: _____/_____/_____ _____

EVIDENCE DETAILS

	Evid # / File #	Manufacturer	Model	Serial Number
CPU				
Monitor				
Keyboard / Mouse				
HDD 1 IDE SCSI MA SL CS		Capacity		
HDD 2 IDE SCSI MA SL CS		Capacity		
HDD 3 IDE SCSI MA SL CS		Capacity		
Floppy Disks				
ZIP Disks				
CD-ROM's				
Other				

COMPUTER FORENSIC EXAMINATION FORM

PRE-ACQUISITION

Initialed / Dated Evidence ☐ Yes ☐ No

All Evidence Write-Protected? ☐ Yes ☐ No

Control Boot Disk Created? ☐ Yes ☐ No

Current Date: _____/_____/_____ Current Time: _____

CMOS Date: _____/_____/_____ CMOS Time: _____

CMOS ☐ Orig Boot Seq: _____ ☐ Access Seq: _____

☐ Changed Boot Seq to:: _____ ☐ Reconfigured Boot Seq to Original

Evidence Connection to Forensic System

☐ IDE Cable ☐ SCSI Cable ☐ Parallel Cable ☐ I/O Card Inside CPU

☐ Floppy Disk Drive ☐ ZIP Disk Drive ☐ CD-ROM Drive ☐ Other

Acquisition Image File Names: _____

ACQUISITION

NOTES:

Verification Conducted? ☐ Yes ☐ No

Errors During Imaging? ☐ Yes ☐ No If Yes, Explain: _____

COMPUTER FORENSIC EXAMINATION FORM

MILESTONES

☐ **Sit down with case agent to determine scope of examination!!!**
- Identify legal authority to search the media (court order, consent, other….)
- Obtain explanation of the case
- Determine evidence expected on media

☐ **Create Destination Folder on Forensic Computer / Analysis Hard Drive**
- Identify which drive will hold the image file of the evidence hard drive
- Create a folder on this hard drive to save the image (normally the slave internal forensic hard drive)
- Inside this folder, create two additional folders (***Export*** and ***Trash***)

☐ **Start EnCase and Open New Case**
- Initiate under ***File*** and then select ***New***
- Fill in Create New Case window fields
  - ⇒ Identify Default Export Folder (using the drop-down menu button, identify the ***Export*** folder created at the beginning of this process)
  - ⇒ Identify Temporary Folder (using the drop-down menu button, identify the ***Trash*** folder created at the beginning of this process)
- Fill in Create New Case window fields

☐ **Add Evidence File**
- Initiate under ***File*** and then select ***Add*** and ***Evidence File***
- Select evidence file created during acquisition process

☐ **Recover Lost Folders**
- Click on the volume you want to search with your **right** mouse button (each volume must be searched separately)
- Select ***Recover Folders***
- Review resulting information listed in the Recovered Folders virtual folder located at the bottom of the volume directory

☐ **Compute Hash Values / Signatures** (**used to filter out known files**)
- Initiate under ***Tools*** and then select ***Search***
- Select ***Verify Signature Files*** and ***Compute Hash Value***, then ***Begin Analysis***
- Review resulting information listed in ***Table*** window in EnCase

☐ **Run Keyword / GREP Searches**
- Found in the ***Keywords*** section of the EnCase program
- Typically used to identify occurrences of:
  - ⇒ Victims' names
  - ⇒ Suspects' names
  - ⇒ SSN's
  - ⇒ Credit card numbers
  - ⇒ Telephone numbers
  - ⇒ Other miscellaneous identifiers

COMPUTER FORENSIC EXAMINATION FORM

☐ **Run E-Script Searches**
- Designed to obtain hidden, deleted or unallocated information
- Common files that require E-Script searches:
  - ⇒ .EMF files (previously printed documents no longer visible in the normal file structure of an operating system)
  - ⇒ Deleted image files (.BMP, .JPG, etc…)
  - ⇒ Internet history / links (obtained from Internet .DAT files)
  - ⇒ E-mail addresses (will identify e-mail addresses with 2- or 3-level domain name e-mail addresses)

☐ **Gallery View Searches**
- Useful in quickly identifying image files on smaller storage media

☐ **Complete Text Index (using FTK)**
- ***NOTE:*** Do not run while initially adding evidence to a case file (will lock up forensic CPU)
- FTK has the capability of indexing every text string located on a storage media
- Allows an examiner to conduct instantaneous string searches

☐ **Search E-mail Files (using FTK)**
- FTK has a strong native ability to recover complete e-mails from storage media (much stronger capability than Encase)

POST-EXAMINATION

Evidence CD-ROM Created? ☐ Yes ☐ No

Copy to Agent _____/_____/_____ Copy to File _____/_____/_____

Exam Report Created _____/_____/_____

Exam Report Sent to ECB _____/_____/_____

Exam Report Sent to Squad _____/_____/_____

Evidence Image Files Burned to CD-ROM _____/_____/_____