

# Computer Evidence Worksheet

Case Number: \_\_\_\_\_ Exhibit Number: \_\_\_\_\_

Laboratory Number: \_\_\_\_\_ Control Number: \_\_\_\_\_

## Computer Information

Manufacturer: _____		Model: _____	
Serial Number: _____			
Examiner Markings: _____			
Computer Type:	Desktop <input type="checkbox"/>	Laptop <input type="checkbox"/>	Other: _____
Computer Condition:	Good <input type="checkbox"/>	Damaged <input type="checkbox"/> (See Remarks)	
Number of Hard Drives: _____	3.5" Floppy Drive <input type="checkbox"/>	5.25" Floppy Drive <input type="checkbox"/>	
Modem <input type="checkbox"/>	Network Card <input type="checkbox"/>	Tape Drive <input type="checkbox"/>	Tape Drive Type: _____
100 MB Zip <input type="checkbox"/>	250 MB Zip <input type="checkbox"/>	CD Reader <input type="checkbox"/>	CD Read/Write <input type="checkbox"/>
DVD <input type="checkbox"/>	Other: _____		

## CMOS Information

Not Available ☐

Password Logon:	Yes <input type="checkbox"/>	No <input type="checkbox"/>	Password = _____
Current Time:	_____ AM <input type="checkbox"/>	_____ PM <input type="checkbox"/>	Current Date: _____ / _____ / _____
CMOS Time:	_____ AM <input type="checkbox"/>	_____ PM <input type="checkbox"/>	CMOS Date: _____ / _____ / _____

## CMOS Hard Drive #1 Settings

Auto ☐

Capacity: _____	Cylinders: _____	Heads: _____	Sectors: _____
Mode: LBA <input type="checkbox"/>	Normal <input type="checkbox"/>	Auto <input type="checkbox"/>	Legacy CHS <input type="checkbox"/>

## CMOS Hard Drive #2 Settings

Auto ☐

Capacity: _____	Cylinders: _____	Heads: _____	Sectors: _____
Mode: LBA <input type="checkbox"/>	Normal <input type="checkbox"/>	Auto <input type="checkbox"/>	Legacy CHS <input type="checkbox"/>

Sub Exhibits Split From This Computer

Sub Number	Type	Where Found

Remarks

# Hard Drive Evidence Worksheet

Case Number: \_\_\_\_\_ Exhibit Number: \_\_\_\_\_

Laboratory Number: \_\_\_\_\_ Control Number: \_\_\_\_\_

Hard Drive #1 Label Information [Not Available ☐Hard Drive #2 Label Information [Not Available ☐

Manufacturer: _____ Model: _____ Serial Number: _____ Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____ Controller Rev. _____ IDE <input type="checkbox"/> 50 Pin SCSI <input type="checkbox"/> 68 Pin SCSI <input type="checkbox"/> 80 Pin SCSI <input type="checkbox"/> Other <input type="checkbox"/> Jumper: Master <input type="checkbox"/> Slave <input type="checkbox"/> Cable Select <input type="checkbox"/> Undetermined <input type="checkbox"/>	Manufacturer: _____ Model: _____ Serial Number: _____ Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____ Controller Rev. _____ IDE <input type="checkbox"/> 50 Pin SCSI <input type="checkbox"/> 68 Pin SCSI <input type="checkbox"/> 80 Pin SCSI <input type="checkbox"/> Other <input type="checkbox"/> Jumper: Master <input type="checkbox"/> Slave <input type="checkbox"/> Cable Select <input type="checkbox"/> Undetermined <input type="checkbox"/>
---	---

## Hard Drive #1 Parameter Information

DOS FDisk <input type="checkbox"/> PTable <input type="checkbox"/> PartInfo <input type="checkbox"/> Linux FDisk <input type="checkbox"/> SafeBack <input type="checkbox"/> EnCase <input type="checkbox"/> Other: _____				
Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____ LBA Addressable Sectors: _____ Formatted Drive Capacity: _____ Volume Label: _____				
<b>Partitions</b>				
Name:	Bootable?	Start:	End:	Type:
	<input type="checkbox"/>			
	<input type="checkbox"/>			
	<input type="checkbox"/>			
	<input type="checkbox"/>			

## Hard Drive #2 Parameter Information

DOS FDisk <input type="checkbox"/> PTable <input type="checkbox"/> PartInfo <input type="checkbox"/> Linux FDisk <input type="checkbox"/> SafeBack <input type="checkbox"/> EnCase <input type="checkbox"/> Other: _____				
Capacity: _____ Cylinders: _____ Heads: _____ Sectors: _____ LBA Addressable Sectors: _____ Formatted Drive Capacity: _____ Volume Label: _____				
<b>Partitions</b>				
Name:	Bootable?	Start:	End:	Type:
	<input type="checkbox"/>			
	<input type="checkbox"/>			
	<input type="checkbox"/>			
	<input type="checkbox"/>			

**Image Archive Information**Archive Method: Direct to Tape ☐ NTBackup ☐ Tar ☐ Other :\* \_\_\_\_\_ Compressed? ☐*Attach appropriate worksheet for backup method used.*Tape Type: DAT 24 ☐ Dat 40 ☐ DLT ☐\* Other \*: \_\_\_\_\_ Number Used: \_\_\_\_\_*\*Requires Lab Director Approval***Analysis Platform Information**Operating Systems Used: DOS ☐ Windows ☐ Mac ☐ \*nix ☐ Other: \_\_\_\_\_

Version: \_\_\_\_\_

Analysis Software Base: I-Look ☐ EnCase ☐ DOS Utilities ☐ \*nix Utilities ☐ Other:\*

Version: \_\_\_\_\_

**Restored Work Copy/Image Validated:** Yes ☐ No ☐**List of utilities used other than base**

Utility	Version	Purpose

**Analysis Milestones**

Milestone	Remarks	Initials
Run Anti-Virus Scan		
Full File List with Meta Data		
Identify Users/Logons/ISP Accounts, etc.		
Browse File System		
Keyword/String Search		
Web/E-mail Header Recovery		
Recover & Examine Free/Slack Space		
Examine Swap		
Unerase/Recover Deleted Files		
Execute Programs as Needed		
Examine/Recover Mail/Chat		
Crack Passwords		