ITU Session Two:

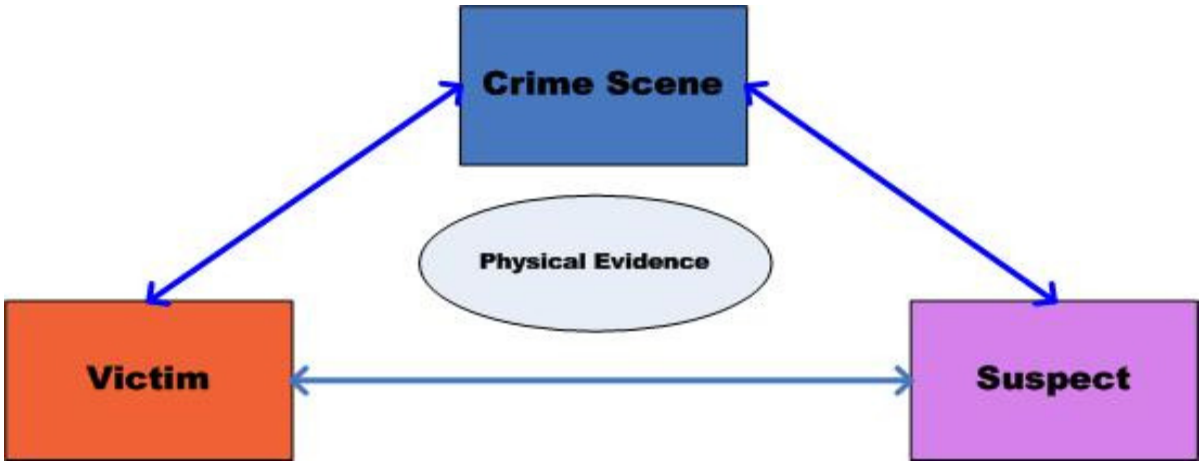
Conduct a "forensically safe" investigation

Mounir Kamal
Mkamal@Qcert.org
Q-CERT

The Importance of Crime Scene

- One of the main goals in an investigation is to attribute the crime to its perpetrator by uncovering compelling links between the offender, victim, and crime scene.

- According to Locard's Exchange Principle, anyone, or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave.



Computer Crime Categories

- **The computer as a target** The attack seeks to deny the legitimate users or owners of the system access to their data or computers. A Denial-of-Service (a.k.a., DOS or DDOS) attack or a virus that renders the computer inoperable would be examples of this category.
- **The computer as an instrument of the crime** The computer is used to gain some other criminal objective. For example, a thief may use a computer to steal personal information.
- **The computer as incidental to a crime** The computer is not the primary instrument of the crime; it simply facilitates it. Money laundering and the trading of child pornography would be examples of this category.
- **Crimes associated with the prevalence of computers** This includes crimes against the computer industry, such as intellectual property theft and software piracy.

What is the Electronic Evidence

Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device.

Electronic Evidence:

- Is often latent in the same sense as fingerprints or DNA evidence.
- Can transcend borders with ease and speed.
- Is fragile and can be easily altered, damaged, or Destroyed.
- Is sometimes time-sensitive.

The Fragility of Digital Evidence

- Once a crime scene has been secured, the evidence of a traditional crime such as fingerprints or firearms tends to obey The Dead Body Theorem ("It's not going anywhere").

- When a computer is involved in the crime scene, however, the situation is not as clear. The very existence of evidence may not be obvious upon initial examination. There are no bullet holes to show where an intruder has gained unauthorized access nor blood stains to show where information has been destroyed.

Types of Fragile Evidence

- **Transient data** - Information that will be lost at shutdown, such as open network connections, memory resident programs, etc.
- **Fragile data** - Data that is stored on the hard disk, but can easily be altered, such as last accessed time stamps.
- **Temporarily accessible data** - Data that is stored on the disk, but for a period of time only

In order to preserve fragile data, it has to be transported to a non-volatile medium as quickly as possible without disrupting any other part of the system (Live Response)

The Law Enforcement Response to Electronic Evidence

- **The law enforcement** response to electronic evidence requires that officers, investigators, forensic examiners, and managers all play a role.
- **A first responder** may be responsible for the recognition, collection, preservation, transportation, and/or storage of electronic evidence.
- **Officers** may encounter electronic devices during their day-to-day duties.
- **Investigators** may direct the collection of electronic evidence, or may perform the collection themselves.
- **Forensic examiners** may provide assistance at crime scenes and will perform examinations on the evidence.

How Is Electronic Evidence Handled at the Crime Scene?

Handling electronic evidence at the crime scene normally consists of the following steps:

1-Recognition and identification of the evidence

2-Documentation of the crime scene.

3-Collection and preservation of the evidence.

4-Packaging and transportation of the evidence.

Seizing Evidence Processes and Documentation

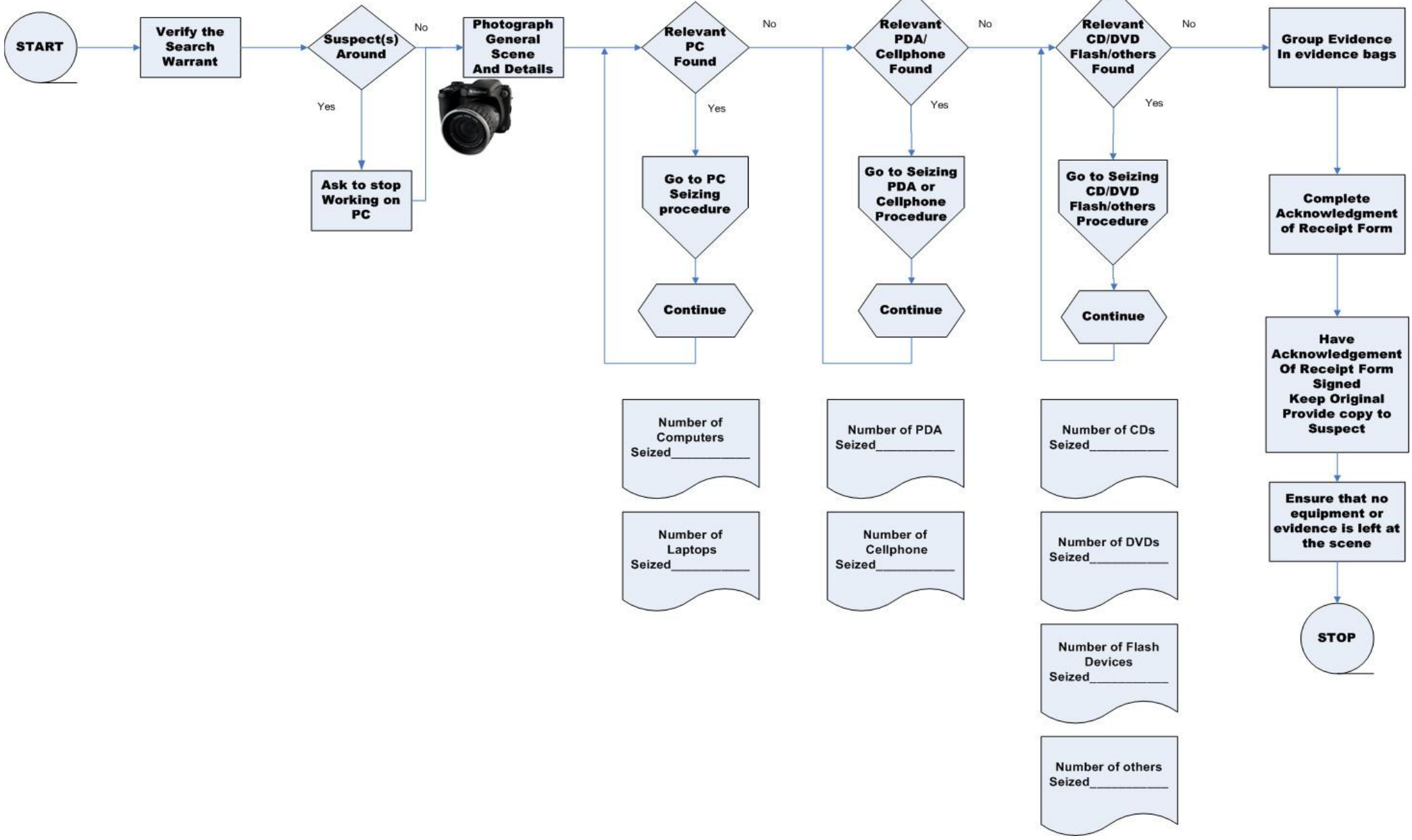
- Examples of Process to follow at Electronic Evidence Scene.

- Seizing PC Procedure
- Seizing PC Hard disk Form

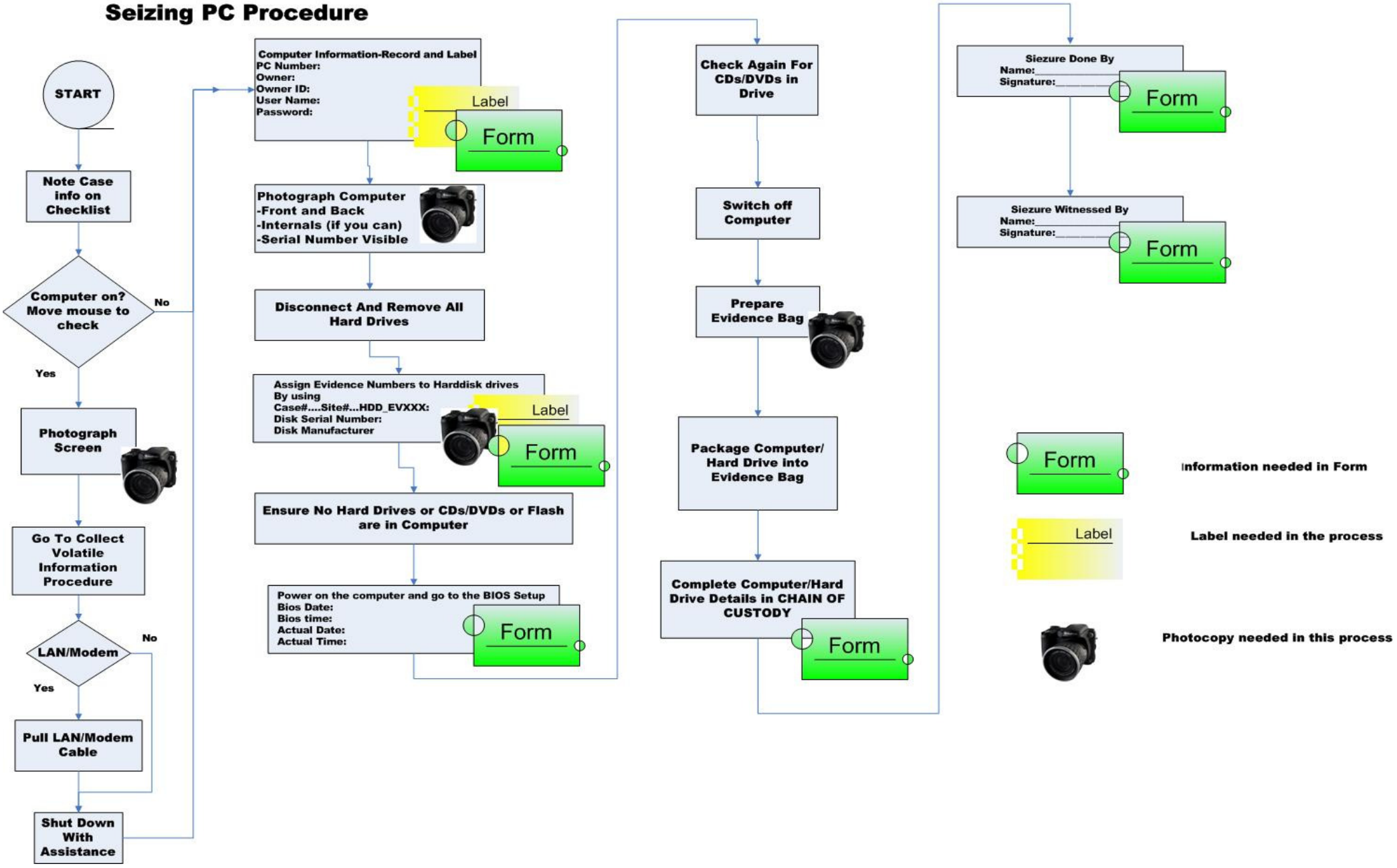
- Seizing PDA/Cell Phone Procedure
- Seizing PDA/Cell Phone Form

- Seizing CDs, DVDs, Flash Memory, and Others Procedure
- Seizing CDs, DVDs, Flash Memory and Others Form

PROCESS TO FOLLOW AT AN ELECTRONIC EVIDENCE SCENE



Seizing PC Procedure



Seizing Computer Hard Disks Form

Case No.		Exhibit Ref. No.	
PC Name		Owner	
Owner ID Number		Computer Serial No	
User Name		Password	

Evidence Number to Hard Disks

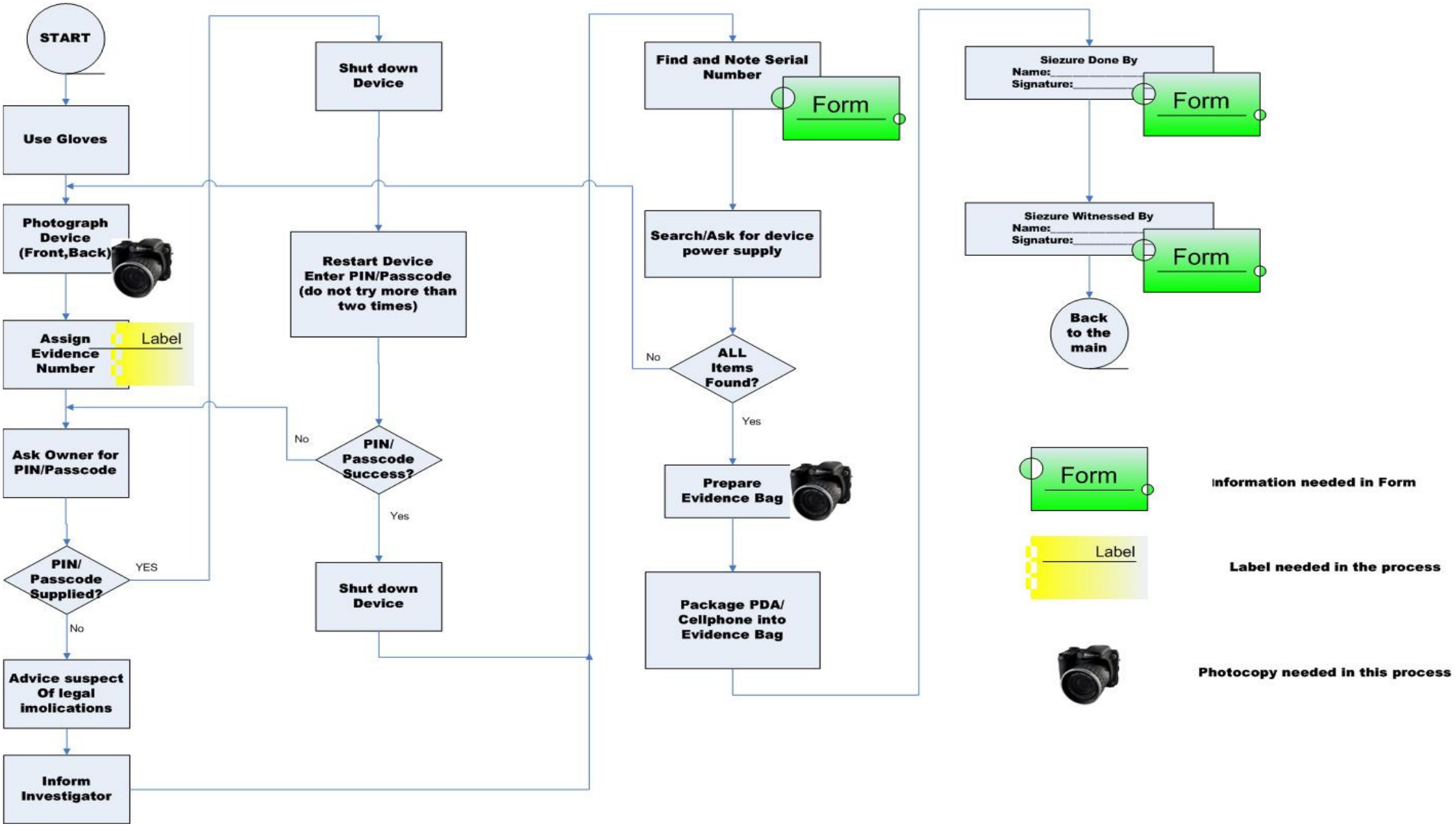
CASE#____SITE#_____HDD_EVXXXXX	Disk Serial Number	Disk Manufacturer

BIOS SETUP Information

BIOS DATE:	
BIOS TIME:	
ACTUAL DATE:	
ACTUAL TIME:	

SEIZURE done by		SEIZURE witnessed by	
NAME:		NAME:	
Signature:		Signature:	

Seizing PDA/CELLPHONE Procedure

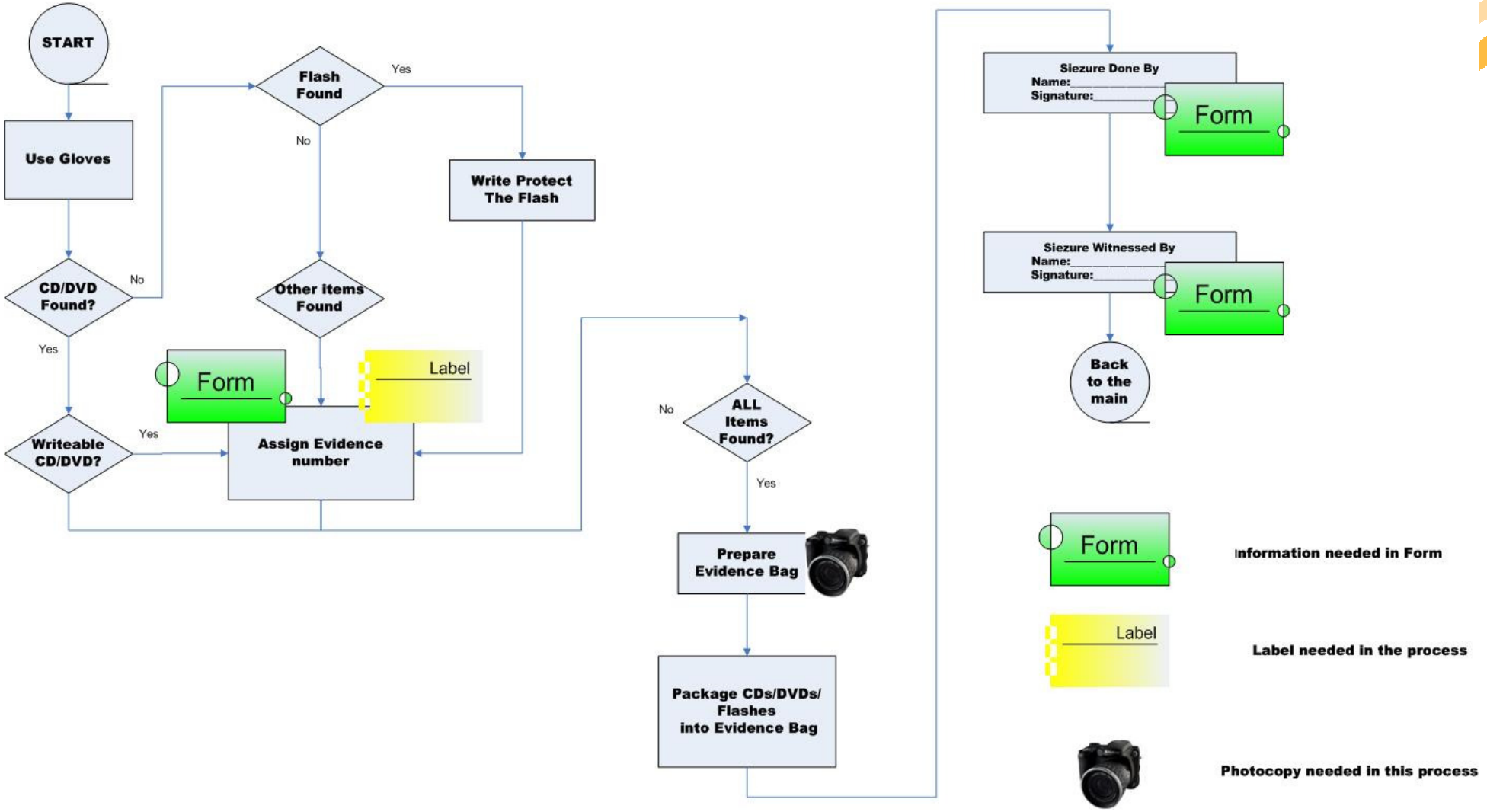


Seizing PDA/Cell Phones Form

CASE#....SITE#....XXX-EV-YYYY	Serial Number	Password/PI N	Owner	Owner ID

SEIZURE done by		SEIZURE witnessed by	
NAME:		NAME:	
Signature:		Signature:	

Seizing CDs/DVDs/Flash/Others Procedure



Seizing CDs/DVDs/Flash/Others Form

CASE#....SITE#....XXX-EV-YYYY	Type Of Item(CD/DVD/Flash/Others)	Info on Label/Manufacturer	Placed Found

SEIZURE done by		SEIZURE witnessed by	
NAME:		NAME:	
Signature:		Signature:	

REFERNCES

- Electronic Crime Scene Investigation (US . Department of Justice)

  “www.ojp.usdoj.gov/nij/pubs-sum/187736.htm “

- The Collection of Digital Evidence “http:// icsa.cs.up.ac.za”

- Digital Evidence and Computer Crime-Forensic Science

Thank You