

Evidence Collection

Section 1: Details of the Organization

Organization Name:	
Contact Number:	
Website:	
Address:	
<i>Additional Contact Information:</i>	

Section 2: Details of the First Responder

Date of Incident:		Date Report Processing Began:	
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, If Applicable, Extension:			
Brief Details of the Incident:			
<i>Additional Details (If any):</i>			

Section 3: Approval Authority Details

Authority Name:	
Designation:	
Department:	
Date of Approval:	
Contact Number & Email:	
Authorized To:	
Additional Details (If any):	

Details of Collected Evidence

☐ Collecting Evidence from Powered-On Computers

Techniques/tools used _____

Results obtained:

[Photograph the screen and document the running programs, open files or data of evidentiary value, etc.]

☐ Collecting Evidence from Powered-Off Computers

Techniques/tools used _____

Results obtained:

[If the computer is switched off, leave it OFF, disassemble and package it as per procedure, etc.]

❑ Collecting Evidence from Networked Computers

Techniques/tools used _____

Results obtained:

[Unplug the network cable from the router and modem in order to prevent further attacks, photograph all devices connected to the victim's computer, such as the router, modem, printer, scanner, etc., from different angles, if the computer is turned OFF, leave it in that state and follow the procedure for its disassembly, if the computer is turned ON, photograph the screen, and follow the steps for powered-on computers, etc.]

❑ Collecting Evidence from Open Files and Startup Files

Techniques/tools used _____

Results obtained:

[Open any recently created document, document the date and time of the files, examine the open files, search for unusual MAC, etc.]

❑ Collecting Evidence from Smart Phones or Other Handheld Devices

Techniques/tools used _____

Results obtained:

[Do not turn the device ON if it is OFF, collect and label the power cables and package the device, collect and label the power cables and package the device, etc.]

❑ Collecting Evidence from Other Sources, Specify _____

Techniques/tools used _____

Results obtained: