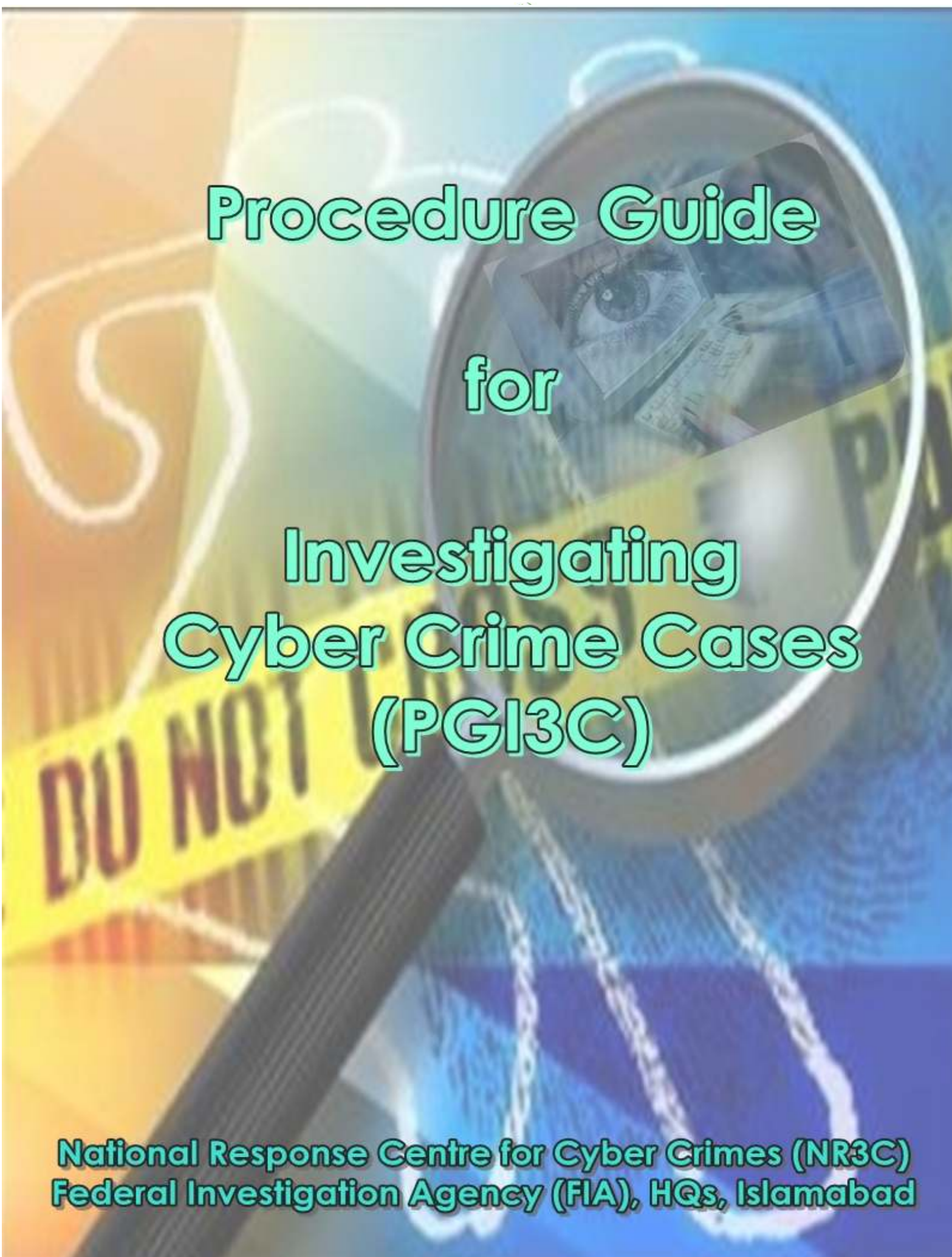

Procedure Guide
for
Investigating
Cyber Crime Cases
(PGI3C)
DO NOT
National Response Centre for Cyber Crimes (NR3C)
Federal Investigation Agency (FIA), HQs, Islamabad

Prepared By:

1. Mehmood ul Hassan, Forensic Expert
2. Amir Nazir Choudhry, Forensic Expert
3. Khurram Shahzad, Technical Writer

The purpose of this guide is to train the law enforcement officers of Pakistan to combat cyber crimes/cyber terrorism and to maintain the integrity of electronic evidence by standard operating procedures (sops).

This guide is specially designed for the first responders, who are the responsible for protecting an electronic crime scene and for the recognition, collection and preservation of electronic evidence.

Note:

Without having the necessary skills and training, no responder should attempt to explore the contents or recover data from a computer (e.g. Do not touch the keyboard or click the mouse) or other electronic device other than to record what is visible on its display.

Procedures Guide for Investigating Cyber Crimes

About NR3C 01

Investigation Tools and Equipment 02

Toolkit for Collecting Digital Evidence 03

Preliminary Interviews 03

Search and Seizure Digital Evidence 05

Introduction 06

Grounds for obtaining search and arrest warrants 06

Powers to Search, Seizure and Arrest 06

Collection of Digital Evidence 09

Procedure for Search, Seizure and Arrest 11

Investigation summary form 12

Form for the Collection of Electronic Evidence 13

Form for Receiving thee Evidence 14

Check list for crime scene analysis 15

Check list for computer system analysis 16

Packaging, Transportation & Storage of Digital Evidence 17

Introduction 18

Policy 18

Packaging Procedure 18

Transportation Procedure 19

Storage Procedure 19

Examination and Analysis of Digital Evidence 21

Introduction 22

Presumption 22

Analysis & Recovery 22

Evidence Examination Procedure 22

Analysis 23

About National Response Center for Cyber Crimes (NR3C)

It has been observed that criminals are using latest technology to execute their plans. These criminals are involved in financial matters, information stealing, online internet frauds, and email threats and at times even in terrorism. To effectively counter such activities it was felt that there must be an organization in the country that should be able to monitor, track and prosecute all such criminals. Keeping this in view National Response Center for Cyber Crimes (NR3C) has been established under Federal Investigation Agency to deal with such types of Crimes.

NR3C is providing single point of contact for all local and foreign organizations on all matters related to cyber crimes. NR3C is imparting trainings and related information system security education to persons of government/semi-government and private sector organizations. An effort is being made to develop a working liaison with international organizations especially against online internet frauds, email threats, plastic money frauds and other financial crimes. NR3C is committed to build local capabilities in incident handling and security intelligence. When this capability is achieved it will be integrated internationally to monitor global security issues.
The Prevention of Electronic Crime Ordinance (PECO) 2007 has been enforced by Government of Pakistan, under which Federal Investigation Agency (FIA) has been made responsible to deal with all types of electronic offences through out the country. Before this ordinance, Electronic Transaction Ordinance (ETO-2002) was being used by FIA to deal with Cyber Crimes.

Objectives of NR3C

- To enhance the capability of Government of Pakistan and Federal Investigation Agency to effectively prevent growing cyber crimes.
- Establishment of Computer Forensic Laboratory, of National level, equipped with Hi-Tech tools for supporting NR3C operations in cyber crime cases.
- To establish a reporting centre for all types of Cyber Crimes in the country.
- Investigation and prosecution of cyber criminals and to cope with high-tech crimes.
- To enforce existing laws to combat electronic crime and to protect consumers.
- Develop and maintain expertise investigations of crimes involving high technology.
- To provide on demand state-of-the-art electronic forensic services and cyber investigator to Law Enforcement Agencies of Pakistan

- International liaison/coordination with Law Enforcement agencies of other countries.

Investigative Tools and Equipment:

In most cases, items or devices containing digital evidence can be collected using standard seizure tools and materials. First responders must use caution when collecting, packaging or storing digital devices to avoid altering, damaging or destroying the digital evidence. Avoid using any tools or materials that may produce or emit static electricity or a magnetic field as these may damage or destroy the evidence.

Tools and Materials for Collecting Digital Evidence:

First responders should have the following items in their digital evidence collection toolkit:

- Cameras (To photograph the crime scene).
- Cardboard boxes (all Computer necessary cables).
- Notepads.
- Gloves.
- Evidence inventory logs.
- Evidence tape.
- Evidence bags.
- Evidence stickers, labels, or tags.
- Crime scene tape.
- Antistatic bags (To protect the Evidence from magnetic field).
- Permanent markers.
- Nonmagnetic tools.

Note:

First responders should also have radio frequency-shielding material such as Faraday isolation bags or aluminum foil to wrap cell phones, smart phones and other mobile communication devices after they have been seized.

Preliminary Interviews:

First responders should separate and identify all suspect(s) at the crime scene as well as to record their locations and did not access to any suspect(s) to computer(s) or Electronic device(s). In the interview gather or collect the following information from the suspect(s).

- Names of all users of the computer(s) and device(s).

- Computer(s) and Internet user information.
- Login names and user account names including Passwords.
- Detail about different applications in use.
- Type of Internet access.
- Any offsite storage.
- Detail of Internet service provider.
- Installed software documentation.
- Detail of e-mail accounts.

Search, Seizure &Arrest Warrants:

Introduction:

This guide will support the law Enforcement Officers of Pakistan to search seizure and arrest Cyber Criminals/Cyber Terrorism as per Standard Operating Procedures (SOPs).

Grounds for Obtaining Search and Arrest Warrants:

There must reasonable grounds for conducting search and obtaining search warrants prior to raiding the crime scene. The following points describe the procedures which Enquiry officer(s) or Investigation officer(s) must have to follow.

- During the enquiry/ Investigation of any case, if there exists sufficient suspicion that any electronic device located at some place was involved in committing the crime then the Enquiry officer(s) must inform his reporting officer and must obtain search warrant from the magistrate for search, seizure or arrest the suspect(s).

- Sufficient suspicion can only be made with the consultation with forensic expert or principal investigator. If they think that any place may contain some electronic evidence or suspect which leads towards the investigation or enquiry in question then Enquiry officer or Investigation officer may obtain search, seizure or arrest warrants from the concerned magistrate.

Powers to Search, Seizure and Arrest:

Search and Arrest powers are to be exercised as mentioned in Cr.P.C 1898, as narrated below.

Search

The police can exercise their power of search under the section 165 of Cr.P.C. 1898, where the reasonable grounds are available which cause the police to investigate any matter which is falling in the jurisdiction.

Arrest

Under the section 46 of Cr.P.C. 1898, the police making arrest of person are made for purpose preventing that person from committing offence or putting that person in custody of police for the alleged committing of offences. The section 47 of Cr.P.C. says that where the arrest is essential for the purpose of the making arrest of that person, they can make search of the premises where the person supposed have take abode or hiding himself.

Collection of Electronic Evidence:

Multiple computers may indicate a computer network. Likewise computers located at businesses are often networked. In these situations specialized knowledge about the system is required to effectively recover evidence and reduce your potential for civil liability. When a computer network is encountered, consult the computer Forensic Expert for assistance.

A "stand-alone" personal computer is a computer not connected to a network or other computer(s). Stand-alones may be desktop machines or laptops. Laptops incorporate a computer, monitor, keyboard and mouse into a single portable unit. Laptops differ from other computers in that they can be powered by electricity or a battery source. Therefore they require the removal of the battery in addition to stand-alone power-down procedures.

If the computer is on, document existing conditions and call your expert or consultant. If an expert or consultant is not available, continue with the following procedure:

Procedure:

After securing the scene, read all steps below before taking any action.

1. Record in notes all actions you take and any changes that you observe in the monitor, computer, printer or other peripherals that result from your actions.
2. Observe the monitor and determine if it is on, off or in sleep mode. Then decide which of the following situations applies and follow the steps for that situation.

Situation 1:

Monitor is on and desktop is visible.

1. Photograph the monitor screen.
2. Record information displayed on the screen included software & processor.

Situation 2:

Monitor is on and screen is blank (sleep mode) or screen saver (picture) is visible.

1. Move the mouse slightly (without pushing buttons). The screen should change and show work product or request a password.
2. If mouse movement does not cause a change in the screen, may be monitor/system is off.
3. Then turn on the monitor/system to proceed.

Situation 3:

Monitor is off.

1. Make a note of "off" status.
2. Turn the monitor on, then determine if the monitor status is as described in either situation 1 or 2 above and follow those steps.

Regardless of the power state of the computer (on, off or sleep mode), remove the power source cable from the computer (Not from the wall outlet). If dealing with a laptop, in addition to removing the power cord, remove the battery pack. The battery is removed to prevent any power to the system. Some laptops have a second multipurpose battery. Check for this possibility and remove that battery as well. Check for outside connectivity. If a telephone connection is present, attempt to identify the telephone number. To avoid damage to potential evidence, remove any floppy disks that are present, package the disk separately and label the package. If available, insert either a seizure disk or a blank floppy disk. Do not remove CDs or touch the CD drive. Place tape over all the drive slots and over the power connector. Record make, model and serial numbers. Photograph and diagram the connections of the computer(s) and the corresponding cables. Label all connectors and cable ends (including connections to peripheral devices) to allow for exact re-assembly at a later time. Label unused connection ports as "unused." Identify laptop computer docking stations in an effort to identify other storage media. Record or log evidence according to departmental procedures. If transport is required, package the components as fragile cargo.

Note:

If Electronic Evidence is off then don't turn it 'on' & if electronic Evidence is 'on' then consult with Technical Expert for further process & seize the evidence.

Procedure for Search, Seizure and Arrest:

1. The Enquiry Officer(s) or Investigation Officer(s) must follow already defined procedures, which are described in Cr. P.C. 1898 and in conformed to F.I.A rules and regulations.
2. The Enquiry Officer(s) or Investigation Officer(s) must have reasonable grounds for search, seizure and arrest.
3. Enquiry Officer(s) or Investigation Officer(s) must consult the Forensic Expert to identify the evidence at the crime scene.
4. The First Responders must fill the following forms at the Crime Scene.
   - The Investigation summary form is annexed as **F-29**.
   - The Electronic Evidence Collection Form is annexed as **F-30**.
   - The receiving of Electronic Evidence Form is annexed as **F-31**.
   - The check list for Crime Scene Analysis/Investigation is annexed as **F-32**.
   - The check list for analysis of Computer System is annexed as **F-33**.

****

Investigation Summary Form

Date and Time	*Investigation Notes*

F-30

Form for the Collection of Electronic Evidence

Federal Investigation Agency (HQs)
National Response Centre for Cyber Crimes (NR3C)

Date		**Case/Enquiry No**	
NR3C Police Station		**Investigation Officer**	
Nature of the case	*		
Required data for further case processing	**		
Location from where the evidence was obtained	***		

Electronic evidence recovered from crime scene

Item No	Description of the evidence	Model No/Serial No	Brand /Manufacturer Name
1			
2			
3			
4			
5			

Evidence Recovered By		Date & Time
Name, Designation & Signature of technical officer		
Name, Designation & signature of Investigation officer		

F-31

Formfor Receiving Evidence in Forensic Lab.

Laboratory Case File No		**Date & Time of Receiving**	
Name of the Organization form which the equipment is received	**Name**		
	Address		
	Contact No		
Type of evidence to be required by the said organization			

Detail of electronic equipment received:

Item No	Description of the evidence	Model No/Serial No	Brand /Manufacturer Name
1			
2			
3			
4			
5			

Chain of Custody Log:

S.No	Received From / Sig/ Date & Time	Received By/ Sig/ Date & Time	Remarks

F-32

Check List for Crime Scene Analysis/Investigation

National Response Centre For Cyber Crimes (NR3C)
Federal Investigation Agency Headquarters
Sector-G-9/4, Islamabad
Ph. 051-9261686, Fax. 051-9261685

Checklist for Crime Scene Analysis/Investigation

S.No	Task/Operation	Check Box
1	Prepare the Raid Team	
2	Identify the team leader	
3	Team leader should demonstrate about the crime/ case reported to all other team member	
4	Plan the crime scene search	
5	Establish team members safety prior to entry	
6	Identify & arrest the suspect(s)	
7	Thoroughly search the suspect(s)	
8	On spot interview of the suspect(s)	
9	Start documentation of every event	
10	Photograph the crime scene	
11	Use latex gloves to preserve the finger print of the suspect	
12	Search the drawer, dust bin, table, etc	
13	Identify the evidence(s)	
14	Label the evidence(s)	
15	Photograph the evidence(s) from front and back	
16	Sketch the crime scene	
17	Collect the evidence(s)	
18	Preserve the evidence(s)	
19	Search & collect email record	
20	Search & collect notes	
21	Search & collect letter or any other correspondence	
22	Search & collect financial/assets record	
23	Search & collect telephone record	
24	Search & collect CD's/Software/Floppy/USB/ External storage devices, etc	
25	Search & collect Credit Card(s)/Debit Card(s)/MSR Cards, etc	
26	Search & collect Magnetic Strip Reader and Writer machine	
27	Search & collect credit card skimmer	
28	Search & collect diaries	
29	Search & collect digital camera	
30	Search & collect Sim(s)	
31	Search & collect Mobile Phone/PDA/iPOD/Black Berry, etc	
32	Search & collect all other portable devices	
33	Pack the magnetic media and wireless devices in anti-static bags	
34	Properly pack all other evidence(s)/device(s)	
35	Properly fill form F-30 (for the collection of digital evidence) duly signed by the IO and Forensic Expert/Principal Investigator	
36	Keeping in view the perishable & fragile nature of electronic evidence, make swift way for the transportation of the said equipment	

F-33

Check List for Computer system

National Response Centre For Cyber Crimes (NR3C)
Federal Investigation Agency Headquarters
Sector-G-9/4, Islamabad
Ph. 051-9261686, Fax. 051-9261685

Federal Investigation Agency (HQs)

Checklist for the Analysis of Computer System in Forensic Laboratory of NR3C FIA HQs

S.No	Task/Operation	Check Box
1.	Always use latex gloves	
2.	Physically examine the received electronic/digital media devices in order to identify the significant problems/damaged items.	
3.	Verify the integrity of seized items.	
4.	Tagged all received items like CPU, hard disks, CDs, USBs, etc	
5.	Photograph all received items.	
6.	Fill form "F-31" (Electronic Device Receiving Form).	
7.	Entry in the register before the start of forensic analysis procedure.	
8.	Always use write blocker.	
9.	Open/remove the CPU case and Photograph the internal components	
10.	Search for fire flash drives.	
11.	Document all the items along-with serial #/model # and brands name	
12.	Firstly read the requirement(s) of investigation officer/reporting agency.	
13.	Always use physical/bit stream image for forensic analysis/examination.	
14.	Analyze the evidence such that analysis should meet the requirements of investigation officer/reporting agency	
15.	Record/ print the timeline and directory structure of the evidence.	
16.	Perform keyword search	
17.	See recent documents/files	
18.	Search for deleted items	
19.	Visualize the internet history/cookies/email correspondence, etc	
20.	Search in normal files/hidden files/encrypted files, etc.	
21.	Evaluate the file slack and swap files, etc	
22.	Document the computer media analysis report	
23.	Verify your findings in comparison with the requirements provided by the IO/reporting agency	
24.	Stored the item / evidence securely in lock	
25.	Prepare and signed the forensic report for further case processing.	

Packaging, Transportation & Storage of Electronic Evidence:

Introduction:

Computers are fragile electronic instruments that are sensitive to temperature, humidity, physical shock, static electricity and magnetic sources. Therefore, special precautions should be taken when packaging & transporting electronic evidence.

The nature of electronic evidence is such that it poses special challenges for its admissibility in court. To meet these challenges, this document will act as Standard Operating Procedures (SOPs) to be followed for Packaging, Transportation & Storage of electronic evidence.

Policy:

Ensure that proper procedures are followed for packaging, transporting and storing electronic evidence to avoid alteration, loss, physical damage or destruction of data.

Packaging Procedure:

All actions related to the identification, collection, packaging, transportation and storage of digital evidence should be thoroughly documented. When packing digital evidence for transportation, the first responder should:

Ensure that all digital evidence collected is properly documented, labeled, marked, photographed, video recorded or sketched and inventoried before it is packaged. All connections and connected devices should be labeled for easy reconfiguration of the system later.

- Remember that digital evidence may also contain latent, trace or biological evidence and take the appropriate steps to preserve it. Digital evidence imaging should be done before latent, trace or biological evidence processes are conducted on the evidence.
- Pack all digital evidence in antistatic packaging. Only paper bags and envelopes, cardboard boxes and antistatic containers should be used for packaging digital evidence. Plastic materials should not be used when collecting digital evidence because plastic can produce or convey static electricity and allow humidity and condensation to develop, which may damage or destroy the evidence.
- Ensure that all digital evidence is packaged in a manner that will prevent it from being bent, scratched or otherwise deformed.
- Label all containers used to package and store digital evidence clearly and properly.

- Leave cellular, mobile or smart phone(s) in the power state (on or off) in which they were found.
- Package mobile or smart phone(s) in signal-blocking material such as faraday isolation bags, radio frequency-shielding material or aluminum foil to prevent data messages from being sent or received by the devices. (First responders should be aware that if inappropriately packaged or removed from shielded packaging, the device may be able to send and receive data messages if in range of a communication signal.)
- Collect all power supplies and adapters for all electronic devices seized.

Transportation Procedure:

When transporting digital evidence, First responder should:

- Keep digital evidence away from magnetic fields such as those produced by radio transmitters, speaker magnets and magnetic mount emergency lights. Other potential hazards that the first responder should be aware of include seats heaters and any device or material that can produce static electricity.
- Avoid storing electronic evidence in vehicles for prolonged periods of time. Heat, cold or humidity can damage electronic evidence.
- Ensure that computers and electronic devices are packaged and secured during transportation to prevent damage from shock and vibration.
- Document the transportation of the digital evidence and maintain the chain of custody on all evidence transported.

Storage Procedure:

Ensure that evidence is inventoried in accordance with departmental policies. Store evidence in a secure area away from temperature and humidity extremes. Protect it from magnetic sources, moisture, dust and other harmful particles or contaminants.

The following procedures must be followed to ensure proper storage and retrieval of electronic evidence. These procedures describe the safeguards that are needed to ensure that original evidence is protected from contamination while in the possession of Evidence store incharge or evidence custodian.

1. All physical electronic and digital evidence must be stored in a safe custody within "Evidence Store" operated under the supervision of store incharge.
2. The store incharge is responsible for receiving and issuing evidence to the officers (who require it).

3. The store incharge and the concerned officer must fill, verify and sign the Chain of Custody Sheet at the time of handing or taking of electronic evidence. If the electronic evidence is to be transported outside the building then follow the SOP for transportation of electronic evidence. Concerned officers must also fill and sign the "handing and taking Evidence sheet/ Chain of Custody Form" that details the list of equipments, their serial numbers, equipment's physical condition, the case reference number and the authority letter to collect or submit the electronic evidence.
4. The Forensic Experts must store the original evidence to Evidence store after taking images of digital evidence (if possible).
5. After the completion of forensic report, all original evidence, original forensic images and its copies and case documentation in electronic form must be archived and labeled with case reference numbers and to be stored in the separate hard disk or CD-R/DVD-R for each case along with the cryptographic hash values to ensure the integrity of the information. All these CD-R, DVD-R and hard disk must be labeled with Case reference number and are to be submitted to Evidence Store once an investigation ends. .

Examination & Analysis of Electronic Evidence by Computer Forensic Expert:

Introduction/Scope:

Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device. As such, electronic evidence is latent evidence in the same sense that fingerprints or DNA (deoxyribonucleic acid) evidence is latent. In its natural state, we cannot "see" what is contained in the physical object that holds our evidence. Equipment and software are required to make the evidence visible. Testimony may be required to explain the examination process and any process limitations. Electronic evidence is, by its very nature, fragile. It can be altered, damaged, or destroyed by improper handling or improper examination. For this reason, special precautions should be taken to document, collect, preserve, and examine this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion.

The nature of electronic evidence is such that it poses special challenges for its admissibility in court. To meet these challenges, this guide will act as a Standard Operating Procedure (SOP) to be followed by Forensic Experts of NR3C for examination of electronic evidence.

Presumption:

This document assumes that the following pre-requisites would be followed before starting

any examination of digital evidence.

1. The physical electronic evidence would be handed over to Incharge of forensic lab by following SOPs for secure chain of custody.
2. Potential Evidence would be collected and transported from the crime scene by following SOPs for search, seizure and transportation of electronic evidence.

Analysis & Recovery Of Digital Evidence:

The Forensic examination, analysis and recovery of all volatile and non-volatile digital evidence must be conducted in the computer Forensic Laboratory.

Evidence Examination Procedure:

General forensic principles apply when examining digital evidence. Different types of cases and media may require different methods of examination.

Principle 1:

Persons conducting an examination of digital evidence should be trained for this purpose.

Principle 2:

Ensure the integrity of received Electronic Evidence for examination using validity of cryptographic signatures or hash values.

Principal 3:

Whenever possible, the examination should not be conducted on original evidence. Always make a working copy for forensic examination and analysis.

Principal 4:

Document each and every step and action you perform and maintain the sequence of events to use it for writing forensic report.

Use Certified Forensic Work Media and Hard Drives.

It is imperative that all work media and hard drives used in the examination process must be sanitized and certified or verified as clean. This eliminates the possibility of data corruption due to residual information from previous investigations be processed.

Process Forensic Image Working Copy Only.

Analysis, research or any investigative work must never be performed on the actual digital evidence or forensic image. When forensic images of digital evidence are made, insist that a working copy be created and verified at the same time. Since disk drives come in varying sizes, it may be difficult to find a disk drive to match the original evidence drive. It is recommended that an image file be created on certified hard drives. This approach insures

that cryptographic hashes will match the original evidence drive. The image can be mounted under Encase Forensic workstation and be processed as a normal file system.

Note: If you are taking the image of evidence storage media or creating image copy of received, always use software or hardware write blocking mechanism, so that the original evidence must not get any change or alteration

5. ANALYSIS

Temporal Analysis.

This is the process of correlating known events with digital objects date and time stamps. The result of this correlation is a timeline reflecting computer activity. Computer object's date and time stamps are constantly being updated by routine Operating System activity. As the timeframe between the computer incident being investigated and the beginning of the forensic investigation grows, the ability to create a comprehensive activity record diminishes. Depending upon the crime or incident being investigated, the detail of the timeline may be of less importance. Another important aspect of temporal analysis is the proper synchronization of different time sources. Electronic components usually require human intervention during the initial setup and configuration. This manual initiation of the starting time is extremely inaccurate at reflecting the exact time. In order to accurately synchronize all pieces of digital evidence, the investigator must determine the difference in time between the digital evidence and the timeframe of the base timeline. This difference is referred to as skewing or time skew. Another consideration often overlooked is the difference in time associated for time zones. When analyzing digital objects, all times must be normalized to central timeframe for reference, all times should be normalized to coordinated universal time (UTC) and then calculate Pakistan Standard Time (PST) with reference to it.

Relational Analysis.

This is the process of determining how digital objects are connected to the various components of the investigation. The cohesion or strength of the connectivity between objects is determined by the number of connections between the objects. The simple process of associating value to common characteristics should illustrate that objects with high values share more common characteristics. These high value objects represent higher degrees of connectivity between the objects. This should illustrate the relationship between the different objects or evidence. There are several methods for documenting relational analysis; such as a matrix illustrating object class attributes or a more graphical presentation such as a bubble diagram.

Functional Analysis:

This process documents how objects function and how illustrating or diagramming those functions reveals similarities and context connections between each object. For example, a phone modem has a particular function, establish a telephone connection to another telephone modem via an analog signal. A phone modem must use a phone line and telephone switch in order to complete the connection. If a suspect accesses a web site, numerous functions are executed; internet connectivity is established, access to a computer, knowledge of computer, knowledge of a computer program to access the web site, knowledge of the web site. In this particular example, there are five distinct functions. No one function can accomplish the task, but all five are needed. This example could be broken down into additional functions such as, connecting to the internet, logging in or on the computer and performing information searches. All of the activities perform a particular function. These functions are related to each other in some form or manner. All functions will affect change upon the system, some at a very minuscule level while others provide a wealth of information. Functional analysis presents the shared or common dependency of functions and objects. The stronger the bond or greater the dependency between objects, the more objects are connected. For example, a phone modem requires a phone line, telephone switch and another distant modem to function. If a phone line does not exist, then there is no relationship between the modem on the computer and the distant modem.

Evidence Analysis.

Forensic Expert may use all three of these analysis techniques to prove a position. The Forensic expert must be completely objective in this analysis. Exculpatory evidence must be given equal weight as incriminating evidence. All evidence must be validated and crosschecked. The evidence must be tied to the suspect and not possess any ambiguities. For example, just because a pornographic picture was found on the computer does not necessarily mean the owner of the computer was the person responsible for putting the image on the computer. Maybe the owner of the computer was away on a business trip when the image appeared on his computer. As the Forensic investigator, you would have to prove that the owner was able to access the computer and place the image on the computer. Or you would have to present a provable scenario by which the computer image could have gotten on the computer.

FORENSIC REPORT

The Forensic Expert is responsible for completely and accurately reporting his or her findings and the results of the analysis of the digital evidence examination. Documentation is an ongoing process throughout the examination. It is important to accurately record the steps taken during the digital evidence examination

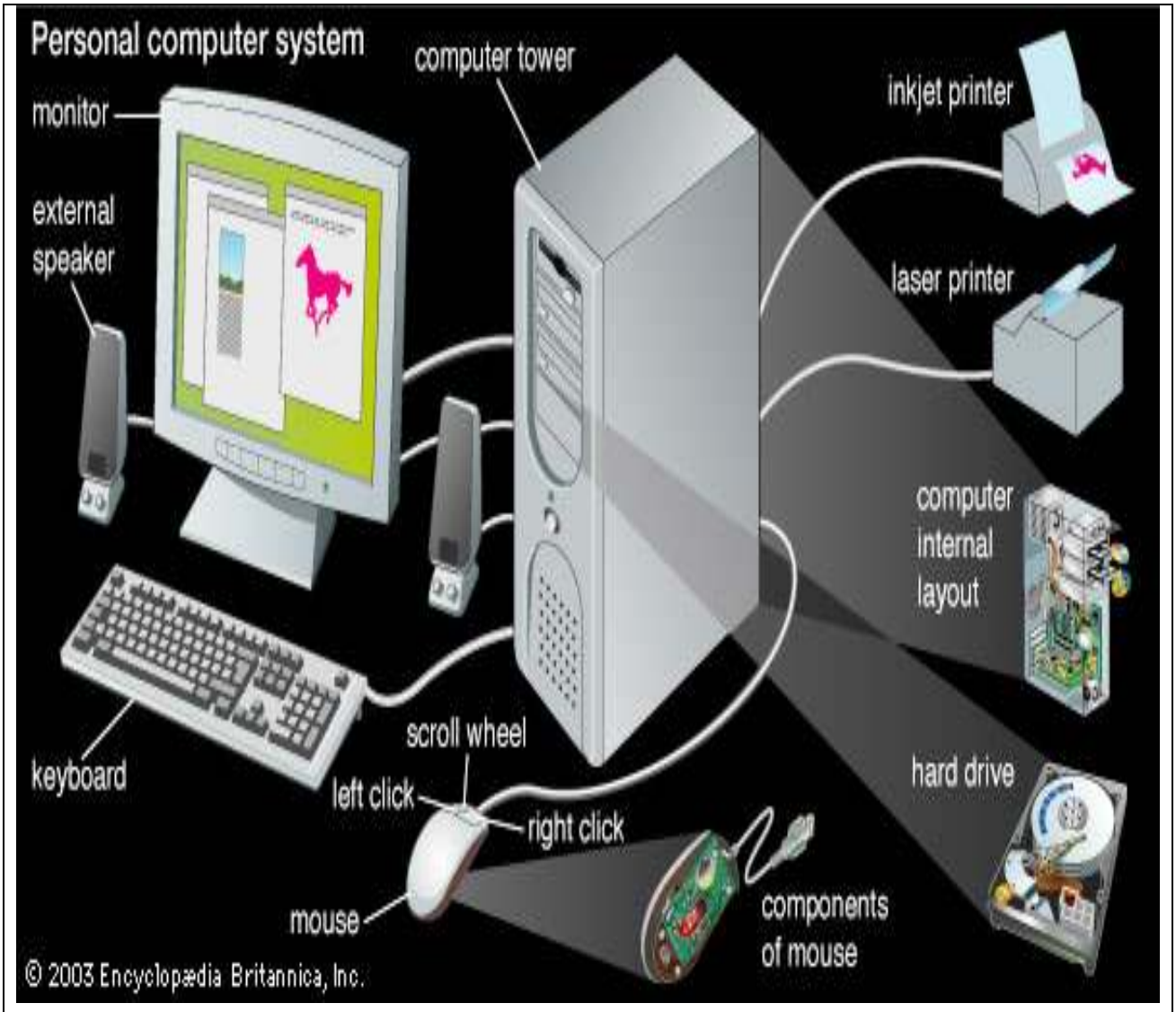
Examiner's Note:

The following is a list of general considerations that the Forensic examiner must consider throughout the documentation process.

- Take notes when consulting with the case investigator and/or prosecutor.
- Maintain a copy of the search authority with the case notes.
- Maintain the initial request for assistance with the case file.
- Maintain a copy of chain of custody documentation.
- Take notes detailed enough to allow complete duplication of actions.
- Include in the notes dates, times, and descriptions and results of actions taken.
- Document irregularities encountered and any actions taken regarding the irregularities during the examination.
- Include additional information, such as network topology, list of authorized users, user agreements, and/or passwords.
- Document changes made to the system or network by or at the direction of law enforcement or the Forensic examiner.
- Document the operating system and relevant software version and current, installed patches.
- Document information obtained at the scene regarding remote storage, remote user access, and offsite backups.
- During the course of an examination, information of evidentiary value may be found that is beyond the scope of the current legal authority. Document this information and bring it to the attention of the Investigation officer because the information may be needed to obtain additional search authorities.

****

Components of Computer System.



PERSONAL COMPUTER SYSTEM