Republic of the Philippines
Department of the Interior and Local Government
National Police Commission
NATIONAL HEADQUARTERS, PHILIPPINE NATIONAL POLICE
DIRECTORATE FOR INVESTIGATION AND DETECTIVE MANAGEMENT
Camp Crame, Quezon City

MEMORANDUM

FOR	:	**See Distribution**
FROM	:	OIC, DIDM/TF USIG Commander
SUBJECT	:	**Mandatory Conduct of Digital Forensic Examination on the Recovered Cellular Phones, Computers, Digital Storage Media, and other Electronic Digital Storage Devices in All Cases Handled by SITG**
DATE	:	JUN 13 2012

1. References:

a. European Union – Philippines Justice Support Program (EPJUST);

b. SOP Number 02/11 re: Procedures in the Creation of Special Investigation Task Group (SITG) to Handle Heinous and Sensational Crimes dated January 26, 2011; and

c. Memo Directive from TDIDM re: Mandatory Examination of All Firearms, Shells and Slugs Recovered During Police Operations dated February 11, 2011.

d. Memo of CIDG re: Format for Request of Digital Forensic Examination.

2. This pertains to the recovered electronic evidence such as Cellular Phones, Computers, Digital Storage Media (Hard Disk Drives, USB Flash Drives, CD, DVD, etc.) and other electronic digital storage devices that may contain digital evidence that must be submitted to the Criminal Investigation and Detection Group (CIDG), Digital Forensic Laboratory for the conduct of Digital Forensic Examination and Analysis. The European Union (EU) experts thru the EPJUST program observed that the capability of CIDG in conducting digital forensic examinations is not being fully utilized in the investigation of cases.

3. The process will ensure the integrity of digital evidence as well as to prevent any accidental tampering of the original evidence. The extracted information may provide evidentiary value as well as indispensable leads in the identification of suspect(s).

4. Please be informed also that the CIDG, as of this date has already six (6) functioning digital forensic laboratories which were strategically situated in the following CIDG Offices with the attached capabilities to wit: (ANNEX-A)

a. CIDG Headquarters - Anti-Transnational and Cyber Crime Division
b. 5 RCIDU - Camp Simeon A Ola, Legazpi City
c. 7 RCIDU – Cebu City, Police Provincial Office
d. 9 RCIDU – Camp Batalla, Zamboanga City
e. 11 RCIDU – Camp Domingo Leonor, Davao City
f. 12 RCIDU – Camp Fermin Lira, General Santos City
g. 10 RCIDU – Camp Alagar, Cagayan De Oro City - Forthcoming

5. Based on the foregoing, concerned PNP units/offices are hereby directed to undertake the following directives:

a. In all cases handled by SITG, concerned PNP units/offices shall ensure that all recovered or seized electronic evidence such as Cellular Phones, Computers, Digital Storage Media (Hard Disk Drives, USB Flash Drives, CD, DVD, etc.) and other electronic digital storage devices are forwarded to the Criminal Investigation and Detection Group (CIDG), Digital Forensic Laboratory for digital forensic examination at the soonest possible time taking into account the weather condition, availability of transportation and travel time from post to CIDG office operating a digital forensic laboratory.

b. Concerned PNP unit/office requesting digital forensic examination shall adhere to the policy, standards, and requirements set by the CIDG digital forensic laboratories. The requesting party should indicate on their request that the evidence to be submitted for digital forensic examination is handled by SITG and indicate priority of the request. Requesting party shall also adopt the standard request memorandum format and completely fill-up all necessary forms given by the CIDG digital forensic laboratories. (ANNEX-B)

c. Upon completion of the digital forensic examination, the CIDG should immediately notify the requesting party within 24 hours using the fastest means of communication available but not limited to such as: Email, SMS text, or by telephone that the official result of the digital forensic examination is already available for release to the requesting party.

d. The requesting party shall pick-up the report of the digital forensic examination within five (5) days upon receipt of said notice or such longer period, taking into account the weather condition, availability of transportation and the travel time from post to CIDG office.

6. This directive shall be applicable only on cases handled by Special Investigation Task Group (SITG) considering the manpower and financial requirements it would entail.

7. In addition, this directive shall not prevent PNP Crime Laboratory from conducting all available and applicable forensic examinations, relevant to the crime committed, on the recovered electronic evidence.

8. Further, it is imperative that the rule on chain of custody be strictly and meticulously observed.

9. For strict compliance and widest dissemination.

CHRISTOPHER A LAXA, CSEE
Police Senior Superintendent

Distribution:
RDs, PROs
Dirs, NOSUs

Copy Furnished:
Command Group
D-Staff

Republic of the Philippines
Department of the Interior and Local Government
National Police Commission
NATIONAL HEADQUARTERS, PHILIPPINE NATIONAL POLICE
DIRECTORATE FOR INVESTIGATION AND DETECTIVE MANAGEMENT
Camp Crame, Quezon City

MEMORANDUM

FOR	:	**Director, CIDG**
FROM	:	OIC, DIDM/TF USIG Commander
SUBJECT	:	**Proposed Mandatory Conduct of Digital Forensic Examination on the Recovered Cellular Phones, Laptops and Other Electronic Digital Storage Devices in All Cases Handled by SITG**
DATE	:	MAY 2 4 2012

1. References:

a. European Union – Philippines Justice Support Program (EPJUST);

b. SOP Number 02/11 re: Procedures in the Creation of Special Investigation Task Group (SITG) to Handle Heinous and Sensational Crimes dated January 26, 2011; and

c. Memo Directive from TDIDM re: Mandatory Examination of All Firearms, Shells and Slugs Recovered During Police Operations dated February 11, 2011.

2. This pertains to the recovered cellular phones (CPs), laptops and other electronic digital storage devices which must be submitted to your Office for the conduct of digital forensic examination. The European Union (EU) experts thru the EPJUST program observed that the capability of CIDG in conducting digital forensic examinations is not being fully utilized in the investigation of cases.

3. Considering that not all investigators are aware of the capability of your Digital Forensic Laboratory to retrieve deleted messages, documents, pictures, etc. which might be used as possible leads in the investigation of cases, this Directorate plans to issue a memo-directive that will make the conduct of digital forensic examinations on the recovered CPs, laptops and other electronic digital storage devices mandatory. Attached is a copy of said draft memo-directive. (Tab A)

4. ITCON, kindly submit comments/inputs regarding this matter NLT May 30, 2012.

CHRISTOPHER A LAXA, CSEE
Police Senior Superintendent

MESSAGE CENTER - HCIDG
RECEIVED
DATE: MAY 24 2012
TIME: 2:00 P.M.
BY:

Republic of the Philippines
Department of the Interior and Local Government
National Police Commission
PHILIPPINE NATIONAL POLICE
CRIMINAL INVESTIGATION AND DETECTION GROUP
Camp Crame, Quezon City

MEMORANDUM

FOR	:	OIC, DIDM/TF USIG Commander
FROM	:	Director, CIDG
SUBJECT	:	**Proposed Mandatory Conduct of Digital Forensic Examination on the Recovered Cellular Phones, Laptops and Other Electronic Digital Storage Devices in All Cases Handled By SITG**
DATE	:	June 7, 2012

1. Reference : Memo from OIC, DIDM/TF USIG Commander dated May 24, 2012, with subject same as above.

2. In connection with the above reference, attached is the proposed draft for mandatory conduct of digital forensic examination on the recovered cellular phones, laptops and other electronic digital storage devices in all cases handled by SITG and necessary form needed by all Digital Forensic Laboratories to be filled-up by requesting parties.

3. Request acknowledge receipt.

FOR THE DIRECTOR, CIDG:

GILBERT CAASI SOSA, PESE, MCSE, EnCE
Police Senior Superintendent (DSC)

0607-016

Republic of the Philippines
Department of the Interior and Local Government
National Police Commission
PHILIPPINE NATIONAL POLICE
CRIMINAL INVESTIGATION AND DETECTION GROUP
ANTI-TRANSNATIONAL AND CYBER CRIME DIVISION
Camp Crame, Quezon City

Digital and Electronic Forensics Laboratory

Capabilities

- **Cyber Crime Incident Response (Handling of Digital Evidence)**
  - Recover volatile data currently running on the computer system and network;
  - Analyze volatile data recovered during incident response procedure; and
  - Conduct search and seizure of electronic evidence found in the computer crime scene.

- **Computer Forensic Examination and Analysis**
  - Using international standard hardware and software for computer forensic examination such as Forensic Computers, Tableau Write Blockers, EnCase, Forensic Tool Kit (FTK), and FTK Imager;
  - Conduct digital media forensic imaging and authentication;
  - Recover and analyze operating system artifacts;
  - Recover deleted files and folders, Internet history files, Internet cache files, and email artifacts from computer system storage media;
  - Access some encrypted and password protected files
  - Analyze files metadata and properties;
  - Conduct file system analysis (FAT, NTFS, HFS+, EXT2);
  - Conduct hash value analysis and file signature analysis;
  - Conduct live acquisition forensic imaging; and
  - Provide Digital Forensic Examination Reports.

- **Cellphone Forensic Examination**
  - Using international standard Cellphone forensic hardware and software such as Cellebrite UFED/PA, XRY/XACT, EnCase Neutrino, SimCon, Data Pilot, Fernico ZRT, and Mobile Edit application;
  - Recover deleted text messages (SMS and MMS);
  - Recover deleted files from Cellphone storage media;
  - Recover Phone Book, Contacts, Dialed Numbers, Received Calls and Miss Calls; and
  - Generate Cellphone Forensic Examination Reports.

- **Computer Network Logs and Stego Analysis**
  - Conduct network logs analysis;
  - Conduct Malware analysis; and
  - Conduct Steganography analysis.

- **Training**

  - Conduct Cyber Crime Incident Response and Digital Evidence Handling Training;
  - Conduct Computer Forensic Training; and
  - Conduct Cyber Crime Awareness Training

- **Serve as an expert witness in court proceedings concerning digital evidence.**

Department of the Interior and Local Government
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE

MEMORANDUM

FOR : **Director, CIDG**
(Attn: C, ATCCD)

FROM :

SUBJECT : **Request for Digital Forensic Examination**

DATE :

1. References:

2. Request that Anti-Transnational and Cyber Crime Division (ATCCD), CIDG conduct digital forensic examination on the accompanying specimen specifically describe on the attached Digital Forensic Examination Request Form.

3. Background of the case with the following information:

a) **NATURE OF CASE** :
b) **VICTIM** :
c) **SUSPECT** :
d) **T D P O** :

4. Facts of the Case:_____
_____
_____.

5. Herewith is/are the required storage media necessary for the digital forensic examination:

Submitted Digital Media for Examination	**Required Storage Media**
Cellular Phone	2 pcs. ***DVD-R*** with Case
Computer System Unit / Hard Drive and other storage media.	***External Storage Media*** or ***Hard Drive***, which capacity must be twice the capacity of evidence submitted storage media.

6. The bearer of this request is _____investigator-on case.

Note:
a. *(For cases from Region 3, 4a, and NCR must be delivered personally by the investigator-on case.),*
b. *(For cases from other Regions preferably delivered by investigator-on case or official Liaison Officer.)*

7. Further request that this Office be furnished a copy of the ATCCD digital forensic examination result for our reference.

_____
(CHIEF OF OFFICE)

REPUBLIC OF THE PHILIPPINES
Department of the Interior and Local Government
National Police Commission
PHILIPPINE NATIONAL POLICE
CRIMINAL INVESTIGATION AND DETECTION GROUP
ANTI-TRANSNATIONAL AND CYBER CRIME DIVISION
Camp Crame, Quezon City

Digital Forensic Laboratory

EVIDENCE CUSTODY FORM

Lab Case #:	Date/Time:
Submitting/Requesting Agency:	Agency Case #:
Agency Address:	Nature of Crime/s:
Contact Official/Investigator:	Contact #:

Item Number	Quantity	Description of Evidence (Manufacturer, Model #, S/N, condition, marks/scratches, distinguishing characteristics, etc)

Received By: (Rank/Name)	Received From: (Rank/Name)
Signature:	Signature:

CHAIN OF CUSTODY

Item #	Date/Time	Received From:	Received By:	Reason:
		Type/Print:	Type/Print:	
		Signature:	Signature:	
		Type/Print:	Type/Print:	
		Signature:	Signature:	

Republic of the Philippines
Department of the Interior and Local Government
National Police Commission
PHILIPPINE NATIONAL POLICE
CRIMINAL INVESTIGATION AND DETECTION GROUP
ANTI-TRANSNATIONAL AND CYBER CRIME DIVISION
Camp Crame, Quezon City

Digital Forensic Laboratory

REQUEST FOR DIGITAL FORENSICS ASSISTANCE

SECTION I: TYPE OF REQUEST

A. Request For:

☐ Lab: ☐ On-site ☐ Technical Assistance ☐ Training

☐ Others: _____

B. Mode of Request:

☐ Initial (Original agency investigation) ☐ Follow-up (Prosecutor follow-up request)

☐ Others:_____

SECTION II: CASE INFORMATION

A. Submitting Agency:	**B.** Date:	**C.** Time:
D. Agency Address:		
E. Agency Case Number:	**F.** Nature of the Crime/s:	
G. Legal Authority: ☐ Search Warrant ☐ Court Order ☐ Consent to Search ☐ Others* _____	Note: Provide a copy of the Search Warrant, Affidavit, Written Consent, Consent Acknowledgement Form, and Synopsis of the case or other Documentation.	
H. Investigators Name: (last, first)	**I.** Cellphone Number:	**J.** Office Number:
K. Investigators Email:	**L.** Is Investigator ISDE Trained? ☐ Yes ☐ No	

SECTION III: COURT/SUSPECT/S INFORMATION

A. Prosecutor Assigned: (last, first)	**B.** Phone Number:	**C.** Email Address:
D. Suspect/s Name: (last, first)	**E.** In custody/Detained: ☐ Yes ☐ No	

SECTION IV: EVIDENCE INFORMATION

A. Search/Seized/ Date:	**B.** Time:	**C.** Location:

D. Items to be Examined:

Item #:	Type of Items/Media	Description (make & model)	Serial Numbers

E. Has anyone viewed/examined/accessed this evidence prior to submission?

☐ Yes * ☐ No

F. List any Digital Forensic Lab members consulted:

G. Special Handling: (check all that apply) *

☐ Bio Hazard ☐ Classified Material ☐ Drug Related ☐ National Interest
☐ Suspected Terrorism ☐ Others:_____

SECTION V: SERVICES REQUESTED

- Describe in detail services requested and provide detailed keywords, nature of the case, and victim/suspect information. Identify any investigative and/ or court deadlines.
- Explain all checked items with " * " from above.

Please identify the types of evidence/information to be searched for/ recovered:

Financial Records	☐	Word Processing /Text Documents	☐	(Other/Keywords – Please be specific)
* Internet History and log files	☐	Credit Card info/Check-writing programs	☐	
*Email/IM/Text Messages	☐	Child Pornography	☐	
Contact Lists	☐	Images	☐	
Call History	☐	Owner Information	☐	

* Clarification and comments

If child pornography images are found during the course of an examination, the examiner will:

1. Use a hard drive duplicator from the Digital Forensic Lab to duplicate the original hard drive.
2. Replace the original drive with a duplicate hard drive of equal or greater size.
3. Remove all child pornography from the duplicate hard drive (which will remain on-site or will be returned to the victim/suspect (when required to do so)).
4. Maintain the original hard drive and image in the Digital Forensic Lab for analysis.

SECTION VI: REQUESTING CASE AGENT /INVESTIGATOR CONFIRMATION

A. Rank / Name /Title:	**B.** Signature:

SECTION VII: DIGITAL FORENSIC LAB USE ONLY

A. Lab Case #:

Process	Rank/Name	Signature	Time/Date
B. Received by			
C. Assigned by			
D. Assigned to			
E. Priority			
F. Lab Case Status	☐Imaging ☐ Examination/Analysis ☐Report Submitted ☐Archived ☐ Pulled out Remarks:_____		