The PNP ACG
Specialized Anti-Cybercrime Trainings

Philippine National Police
Anti-Cybercrime Group

By: PSSUPT GILBERT CAASI SOSA
Director, PNP ACG

Activation of PNP ACG

- NAPOLCOM RESOLUTION NO. 2013-220 dated February 27, 2013; and
- GENERAL ORDER NO. DPL-12-09

Specialized Anti-cybercrime Trainings

- Introduction to Cybercrime Investigation Course (ICIC)
- Identification and Seizure of Digital Evidence (ISDE)
- Proactive Internet Investigation Course (PIIC)
- Introduction to Digital Forensic Investigation (IDFI)

Introduction to Cybercrime Investigation Course (ICIC)

- The purpose of this course is to enhance the capability of the PNP investigators in combating cyber criminals by providing a broad overview about cybercrimes, modus operandi, tools of cyber criminals such as computer hardware and software to include network connectivity, and applicable laws.

- This course provides PNP investigators the complete knowledge in building Cybercrime cases, to take it beyond the apprehension of the Cyber criminals and collection of evidence.

- One of the highlights of this course is the Cybercrime investigative process to include the mock-scenario in investigation Cybercrime incident.

Introduction to Cybercrime Investigation Course (ICIC)

Module Nr	MODULES
1	Course Introduction
2	Facing the Cybercrime Problem
3	Reviewing the History of Cybercrime
4	Understanding the People on the Scene
5	Understanding Computer Basics
6	Understanding Computer Network Basics
7	Understanding Cybercrime Prevention
8	Building Cybercrime Case

Identification and Seizure of Digital Evidence (ISDE)

- This course was developed to provide frontline police officers and investigators an overview of the process on securing a Cybercrime scene that may involve the seizure of electronic or digital evidence.

- Emphasis is placed on proper evidence collection techniques or what we called vital “Bag and Tag” procedures to avoid computer crime miscarriage that often result to technical circumvention of cases in court. This include other basic investigative and documentation activities including:

  - Photographing the scene
  - Shutting down computer systems properly
  - Identifying the many types of media that may contain digital evidence
  - Performing proper interviewing techniques on Cybercrime suspects

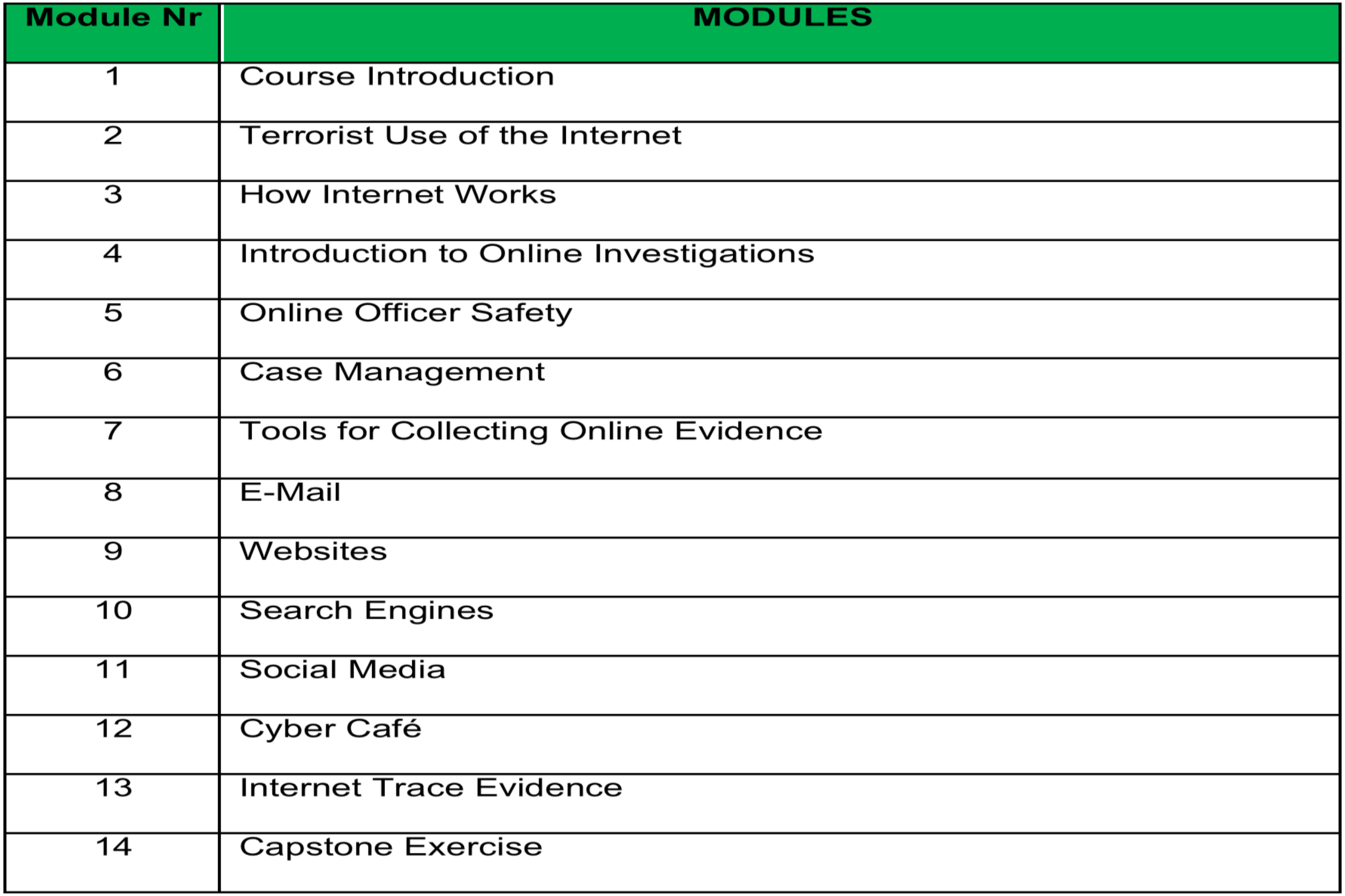
IDENTIFICATION AND SEIZURE OF DIGITAL EVIDENCE (ISDE)

Module Nr	MODULES
1	Course Introduction
2	Laws and Rules of Digital Evidence
3	Basic Computer Literacy
4	Introduction to Computer Network
5	Hard Disk Drive Configuration and Windows Artifacts
6	Computer Assembly and Disassembly
7	Search and Seizure of Computers “Bag and Tag”
8	“Bag and Tag” Demonstration and Practical Exercises
9	Basic Forensic Principles
10	Forensic Imaging and Verification

Proactive Internet Investigation Course (PIIC)

- The goal of Proactive Internet Investigation Course is to provide investigators with technical skills to investigate using online resources and to conduct ongoing terrorist/criminal investigations.
- The course is very hands-on in nature. Participants will consider each of these questions during the course:
  - How is the Internet being used by the terrorist today?
  - How does the Internet work and what can investigators do to exploit available sources of information, including communications, collaboration, search, and social media?
  - What should they do to manage evidence and maintain the chain of custody on-line?
  - How do investigators protect themselves online?
  - What tools are available to collect evidence from different sources such as e-mail, websites, search engines, and social media?
  - What are the implications and challenges of tracing communications that originate from environments such as cyber cafés.

Proactive Internet Investigation Course (PIIC)

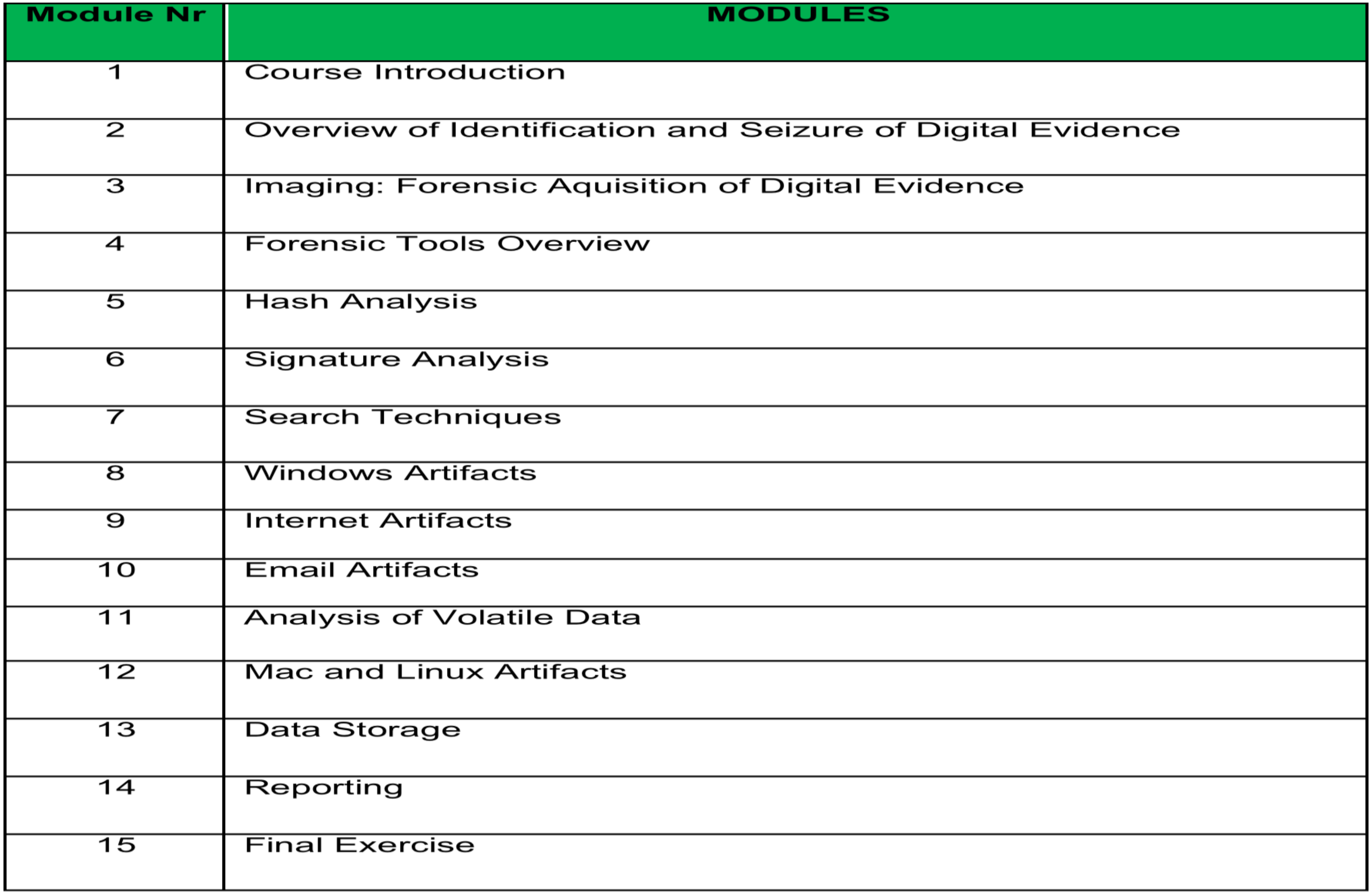


Module Nr	MODULES
1	Course Introduction
2	Terrorist Use of the Internet
3	How Internet Works
4	Introduction to Online Investigations
5	Online Officer Safety
6	Case Management
7	Tools for Collecting Online Evidence
8	E-Mail
9	Websites
10	Search Engines
11	Social Media
12	Cyber Café
13	Internet Trace Evidence
14	Capstone Exercise

Introduction to Digital Forensic Investigation (IDFI)

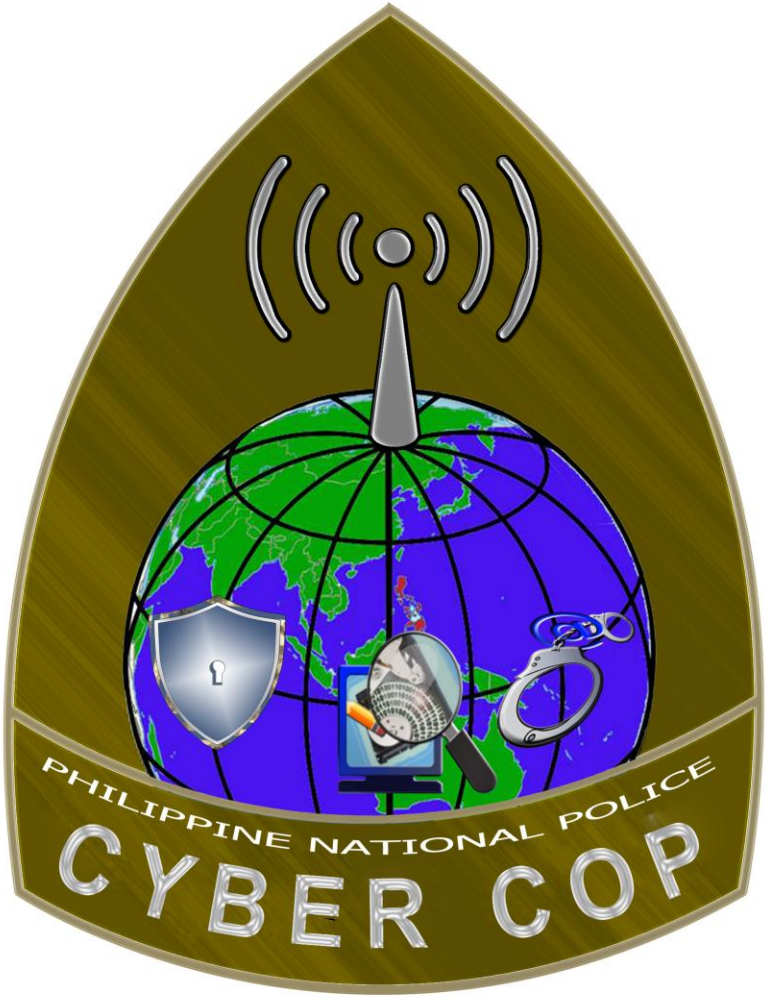
- This course was designed to enhance the capabilities of the PNP in the field of Digital Forensics. It provides digital forensic examiners with thorough understanding on the principles, best practices, and procedures in the conduct of digital forensic examination.
- The course exposes participants to the process of identifying evidence on digital media pertinent to a live case or investigation. Participants will also learn valuable investigative techniques and discover how to effectively articulate relevant findings.

Introduction to Digital Forensic Investigation (IDFI)



Module Nr	MODULES
1	Course Introduction
2	Overview of Identification and Seizure of Digital Evidence
3	Imaging: Forensic Aquisition of Digital Evidence
4	Forensic Tools Overview
5	Hash Analysis
6	Signature Analysis
7	Search Techniques
8	Windows Artifacts
9	Internet Artifacts
10	Email Artifacts
11	Analysis of Volatile Data
12	Mac and Linux Artifacts
13	Data Storage
14	Reporting
15	Final Exercise

THE "CYBER COP" BADGE



The "Cyber Cop" Badge

Welcome
1ST ANTI-CYBERCRIME GROUP ANNIVERSARY
WITH
PDG ALAN LA MADRID PURISIMA
CHIEF, PHILIPPINE NATIONAL POLICE
Guest of Honor and Speaker
THEME: "STRATEHIYA, OPERASYON AT SOLIDONG AKSYON GAMIT ANG MAKABAGONG
TEKNOLOHIYA S PAGSUGPO NG K MINALIDAD TUNGO SA TAPAT AT
SERBISYONG MA ATOTOH AN"
QUEZON CI

The Pinning of "Cyber Cop" Badge

2. ADVANCE CYBER COURSES

- Digital Forensic
  - Mobile Forensic
  - Computer Forensic
  - Network forensic
  - Mac Forensics

- Advance Cybercrime investigation
  - Covert Online Investigation

- Cyber Security
  - Malware Analysis

END

THANK YOU