



Indonesian National Police Headquarters  
Criminal Investigation Board  
Forensic Laboratory Centre



# CYBER CRIME and DIGITAL FORENSIC INVESTIGATION

**Kombes Pol. Muhammad Nuh Al-Azhar, MSc., CHFI., CEI., ECIH.**  
Police Grand Commissioner – Principal Digital Forensic Examiner

*dedicated for digital forensic development in Indonesia, Sept. 2020*

# Jokes in Forensic World

A forensic analyst is seen from behind, sitting at a desk in a computer lab. He is working on a laptop. On the desk, there is a yellow evidence bag that is open, showing various tools and equipment inside. The background shows other desks with computers and monitors.

**CLIENT ASKS ME TO COME ONSITE  
TO IMAGE A COUPLE LAPTOPS**

**ARRIVE TO FIND THERE ARE FORTY  
COMPUTERS AND THREE SERVERS**

A close-up shot of Morpheus from the movie The Matrix. He is wearing his signature black sunglasses. The reflection in the sunglasses shows two women, one of whom is Trinity. The background is a blurred green.

**WHAT IF IT TOLD YOU**

**LIKING AND SHARING A PHOTO ON  
FACEBOOK DOESN'T MEAN GOD LOVES YOU.**

**Formal Education**

- 2006: 35<sup>th</sup> Indonesian Advanced Police College  
Award: *The Best Graduate in Academic*
- 2009: MSc in Forensic Informatics, University of Strathclyde, UK  
*Distinction for Dissertation* on Steganography Forensic
- 2017: 57<sup>th</sup> Indonesian Police Middle Chief & Staff School
- 2020: National Leadership Training (PKN) Level 1 Batch 45: *The Best Graduate #1*

**Professional Qualifications**

- 2004: Professional Commendation on Crime Scene Management from Senior Investigator (Retired) of New York Police, US
- 2007: Computer Hacking Forensic Investigator (CHFI) from EC-Council
- 2008: Certified EC-Council Instructor (CEI) from EC-Council, US
- 2009: Professional Member (MBCS) from British Computer Society, UK
- 2014: EC-Council Certified Incident Handler (ECIH) from EC-Council
- 2017: Certified Assessor for Forensic Laboratory Examiners

**Short CV**

**Professional Awards**

- 2008: British Chevening Scholarships Award from UK FCO
- 2010: Indonesian Super Six UK Alumni from British Council
- 2013: 16 year Dedication Medal from President of the Republic of Indonesia
- 2014: ISO 17025 Accreditation for Digital Forensic Lab.
- 2018: Individual Category of BSSN Award in National Internet Security Day

**Memberships/ Networking**

- 2007: EC-Council
- 2009: British Computer Society
- 2013: Association of Certified Fraud Examiners (ACFE)
- 2015: Indonesian Digital Forensic Association, as *Chairman for 2015-2019*
- 2016: INTERPOL Digital Forensic Experts Group



Experience as  
Instructor/Speaker

## INDONESIAN NATIONAL POLICE (*POLRI*)

General Attorney (*Kejagung RI*)

Ministry of Communication and Information (*Kemenkominfo RI*)

Ministry of Finance (*Kemenkeu RI*)

Finance Auditors Board (*BPK RI*)

National Resilience Institute (*Lemhannas RI*)

University of Strathclyde, Glasgow, UK

University of Islamic Indonesia, Yogyakarta

Krida Wacana University, Jakarta

State Islamic University, Tangerang

State Cryptography Institute, Tangerang

Islamic University of Riau

Indonesian Al-Azhar University, Jakarta

Bina Sarana Informatika Academy, Jakarta

Mercu Buana University, Jakarta

Bina Nusantara University, Jakarta

STIKOM Bali, Denpasar

State Islamic University of North Sumatera

Sriwijaya University, Palembang

Trunojoyo University, Madura

STIKOM Cirebon, etc.

Bank of Indonesia, Mandiri Bank, BRI, BNI, BCA, CIMB Niaga, OCBC NISP, etc.

UNODC, INTERPOL, ACFE, EC-Council, TELKOMSEL, ASTRA, etc.

Supreme Court (*Mahkamah Agung RI*)

Corruption Eradication Commission (*KPK RI*)

Financial Service Authority (*OJK RI*)

State Cryptography and Cyber Agency (*BSSN RI*)

University of Indonesia, Depok

Paramadina University, Jakarta

Airlangga University, Surabaya

Muhammadiyah University, Jember

State Polytechnic, Batam

Swiss Germany University, Serpong

Telkom University, Bandung

Bandung Institute of Technology

Gunadharma University, Depok

Langlangbuana University, Bandung

Siliwangi University, Tasikmalaya

STMIK Bani Saleh, Bekasi

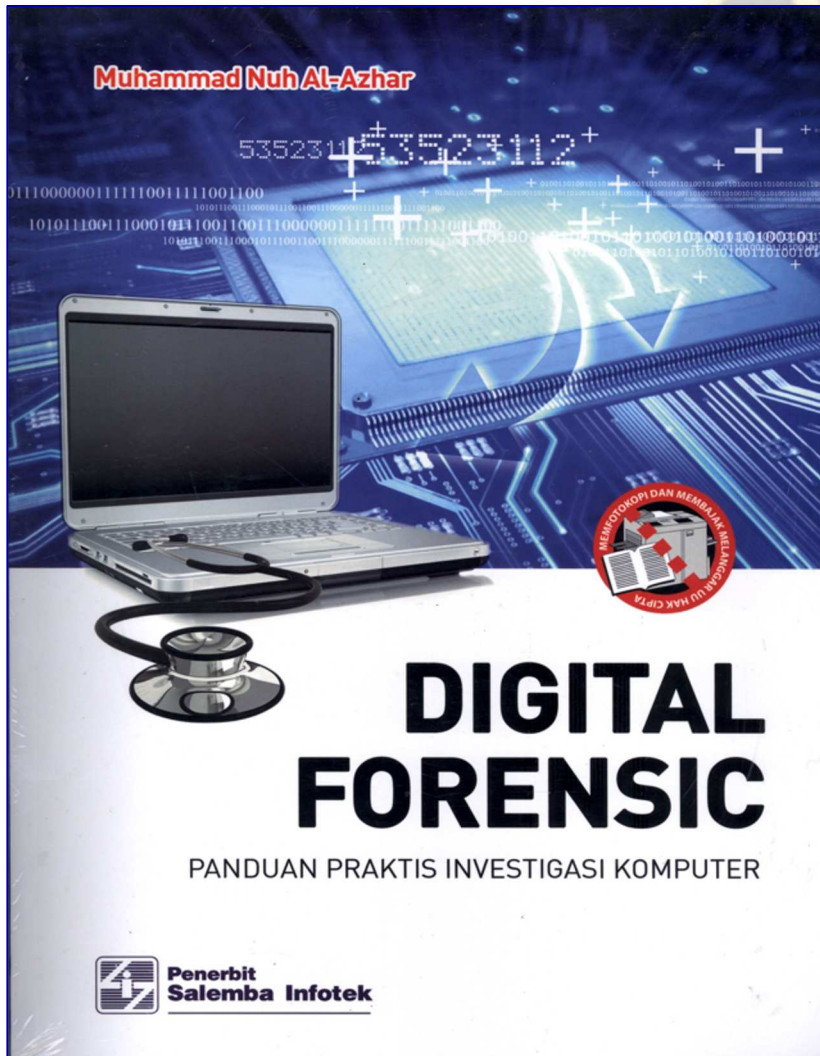
PLN Engineering College, Tangerang

STIESIA, Surabaya

## Short CV



# Author of Books



Steganography is an art to hide secret message inside a carrier file which is commonly image file in the form of JPG or BMP. After created, the carrier file is then sent to other members of a certain group for secure communication. Only the group members identify the carrier file and understand the message embedded. Each steganography tools has their own method to perform the hiding process in which the tools are different one another. For digital forensic analyst, steganography is a challenge to detect it. The carrier file still looks good and nothing is suspicious visually on it. This book explains how to perform Metadata Analysis to detect the existence of a steganography carrier file. Moreover, with Metadata Analysis, digital forensic analyst could identify the type of steganography tools used to embed the secret message into the image file. At this moment, this steganography technique is frequently used by many intelligent agencies as their telecommunication channel which is secured from detection and interception of third parties. Even the third parties do not have an idea about to recognize it.

Steganography Forensic



Muhammad Nuh Al-Azhar

## Steganography Forensic: Metadata Analysis for Steganography Detection



I am Muhammad Nuh Al-Azhar, a Senior Digital Forensic Analyst of the Indonesian Police Forensic Laboratory Centre. Currently I am holding the job as the Chief of Computer Forensic Laboratory and responsible for digital forensic analysis on electronic and digital evidence, as well as the Chairman of the Indonesian Digital Forensic Association.



978-3-330-00459-7

Al-Azhar

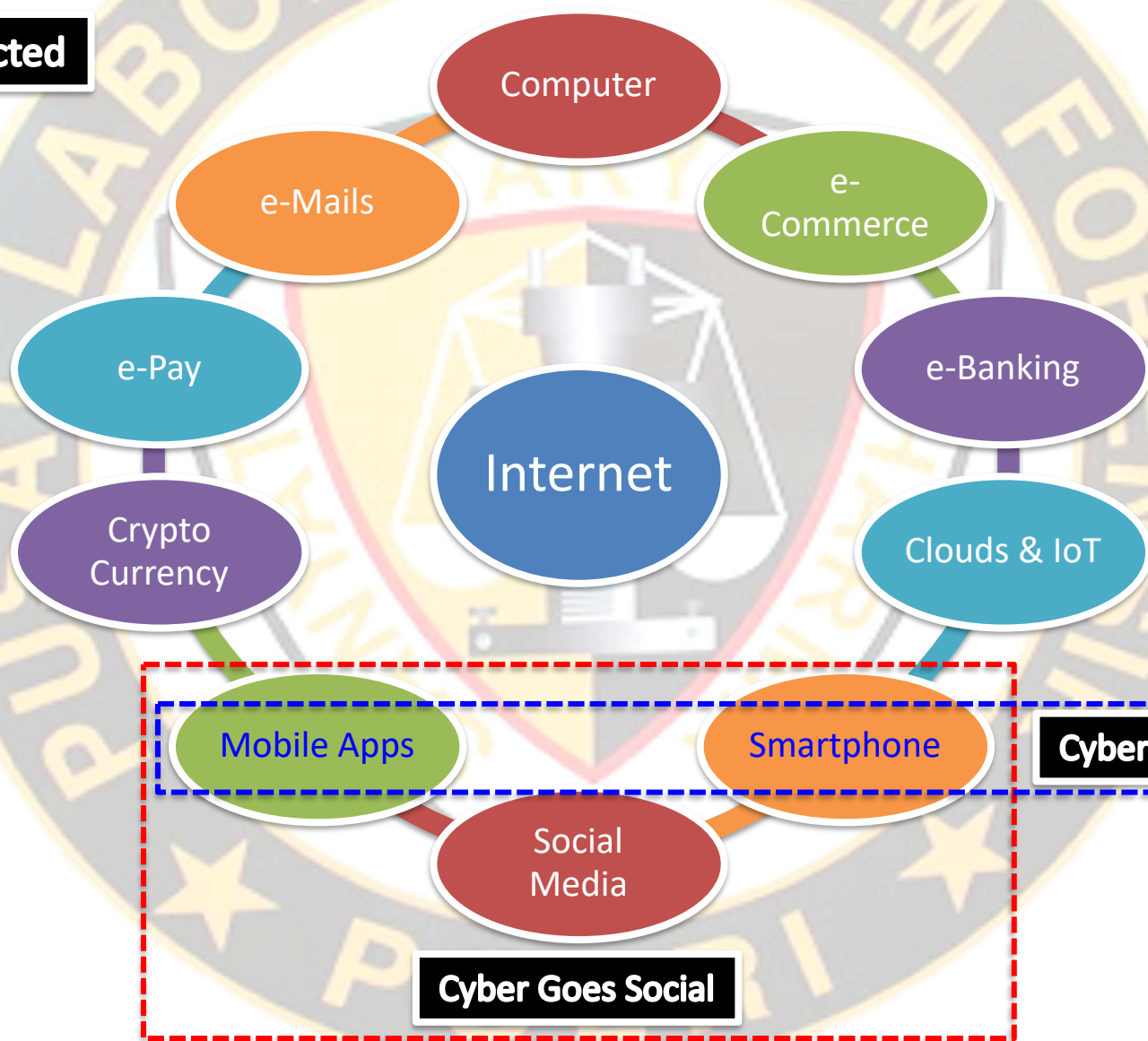
LAP **LAMBERT**  
Academic Publishing

# Sharing & Expertise



# Cyber Goes Mobile & Sosial

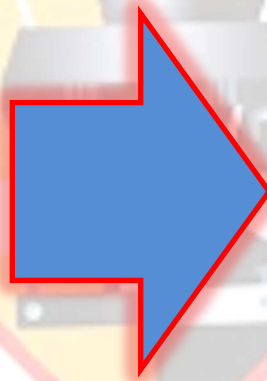
Everything is Connected



Cyber Goes Mobile

Cyber Goes Social

# Crime as Side Effects



**CYBER CRIME (INCIDENTS)**  
Computer/Smartphone  
as Tools and Targets

**COMPUTER-RELATED CRIME**  
Any Type of Crime with  
Computer/Smartphone as Evidence



# The Question

How to Respond it porperly...?



Cyber Crime/Incidents

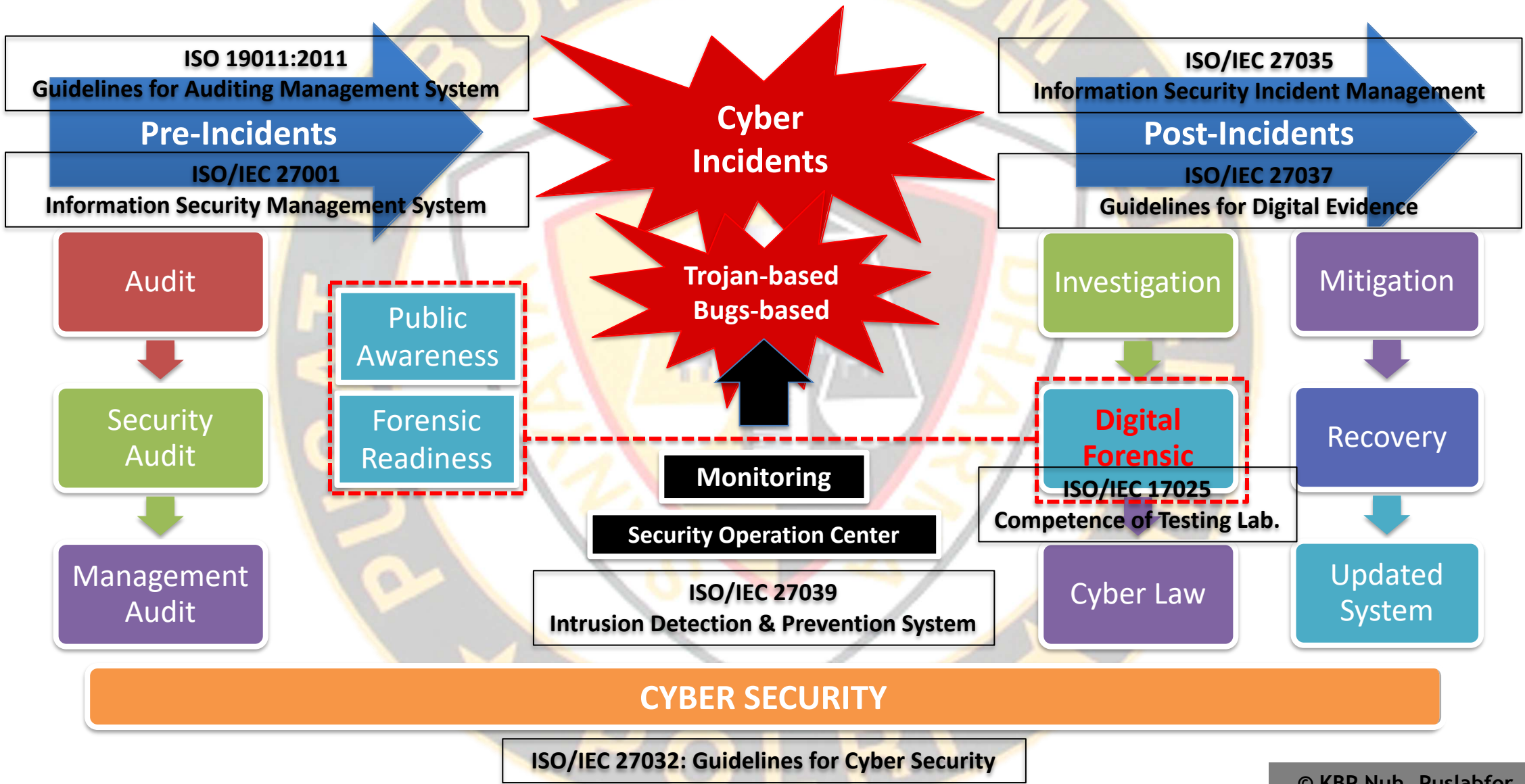
Computer-related Crime



Scientific Investigation

DIGITAL FORENSIC

# Management on Cyber Incidents Handling



# Steps of Digital Forensic

**ISO 27037:** Guidelines for Identification, Collection, Acquisition & Preservation of Digital Evidence

## HANDLING PROCESS:

**Identification** → Types of Evidence  
**Collection** → Evidence Bag & Documenting  
**Acquisition** → Triage & Forensic Imaging  
**Preservation** → Write Protect & Hash

## PRINCIPLES → KEY ASPECTS:

**Relevance** → Justifiability  
**Reliable** → Auditability & Repeatability  
**Sufficiency** → Reproduceability

## Crime Scene:

Identification,  
Collection &  
Acquisition

## Electronic Evidence:

Acquisition &  
Preservation

## Examination:

Investigative  
Data

## Analysis:

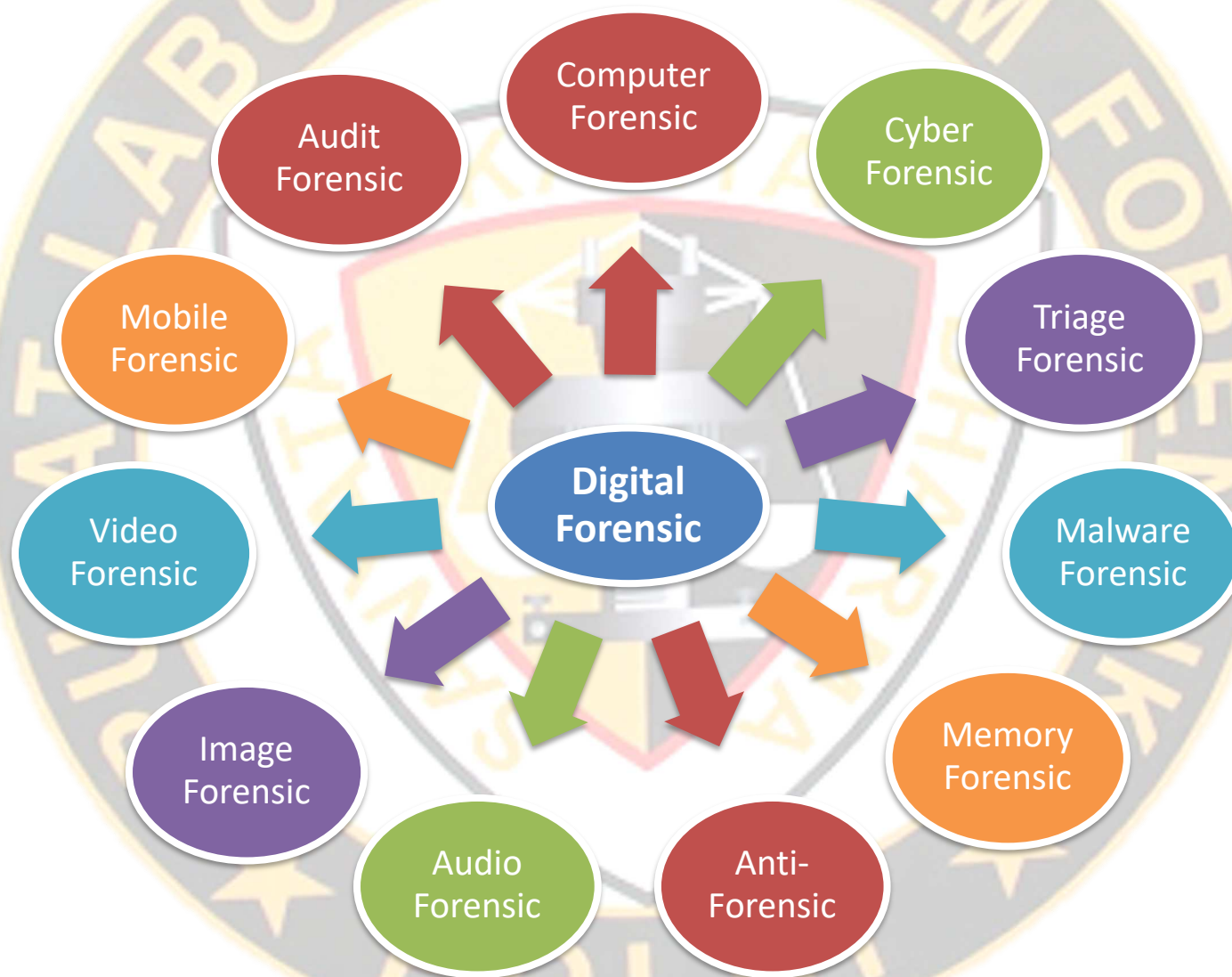
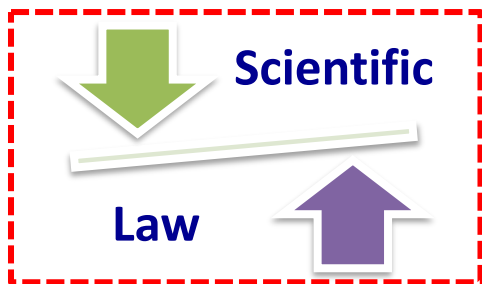
Digital  
Evidence

**Expert  
Testimony**  
at Court

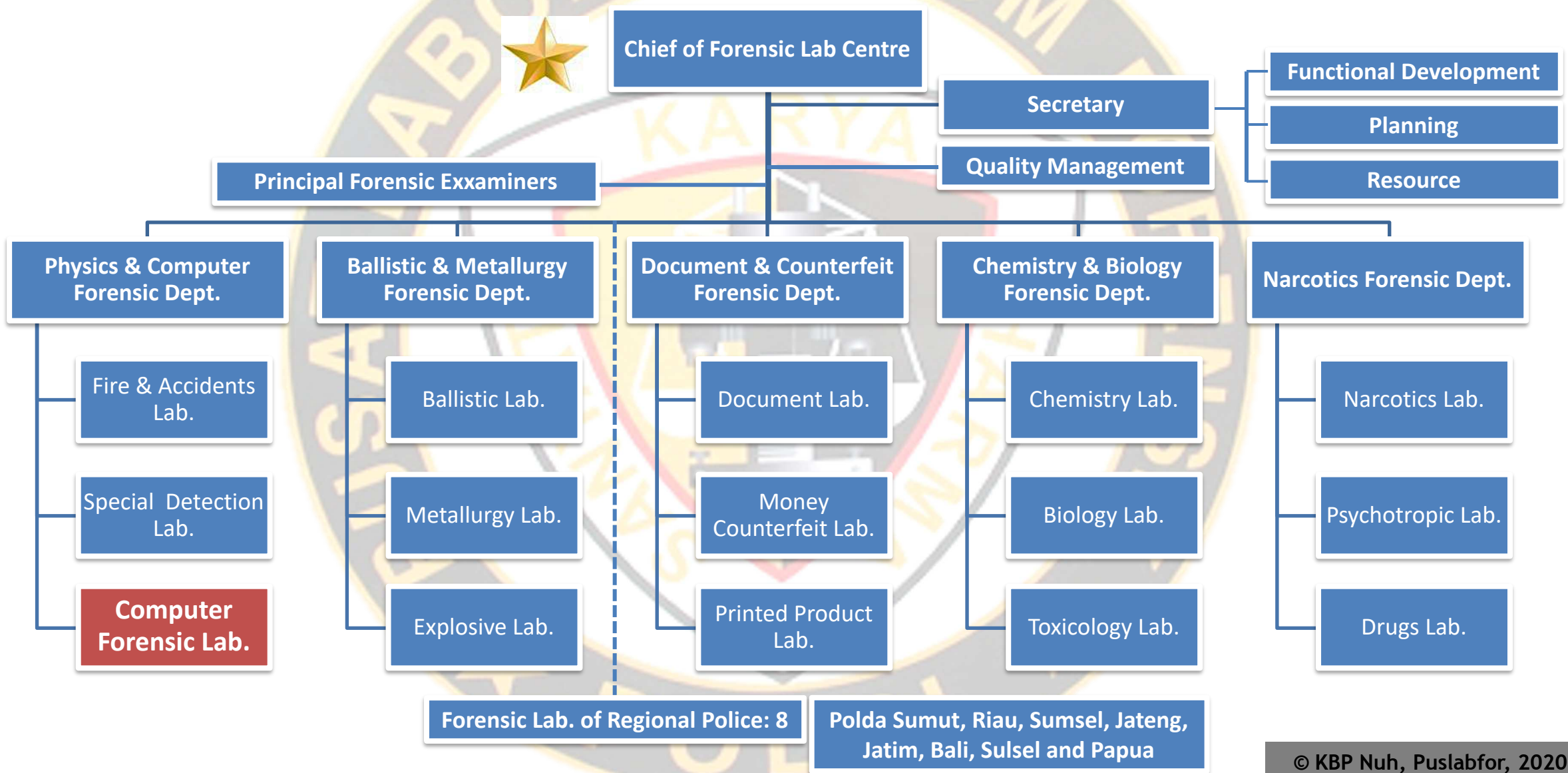
Key Component → **CHAIN OF CUSTODY**



# Digital Forensic is Developing



# Structure of INP Forensic Lab. Center



# Milestone of Digital Forensic Development

**DFAT**

Digital  
Forensic  
Analyst  
Team



• **2000**: Started to learn about the significance of digital forensic to support examination on electronic/digital evidence

• **2007, 2008, 2012, 2014, 2019**: Awards of EC-Council's Certificates of Computer Hacking Forensic Investigator (CHFI) and EC-Council Certified Incident Handler (ECIH) and so on for the Analysts of Centre and Regional

• **2009**: Award of MSc in Forensic Informatics from the University of Strathclyde, UK with distinction mark for dissertation

• **2010**: DFAT (Digital Forensic Analyst Team) was founded

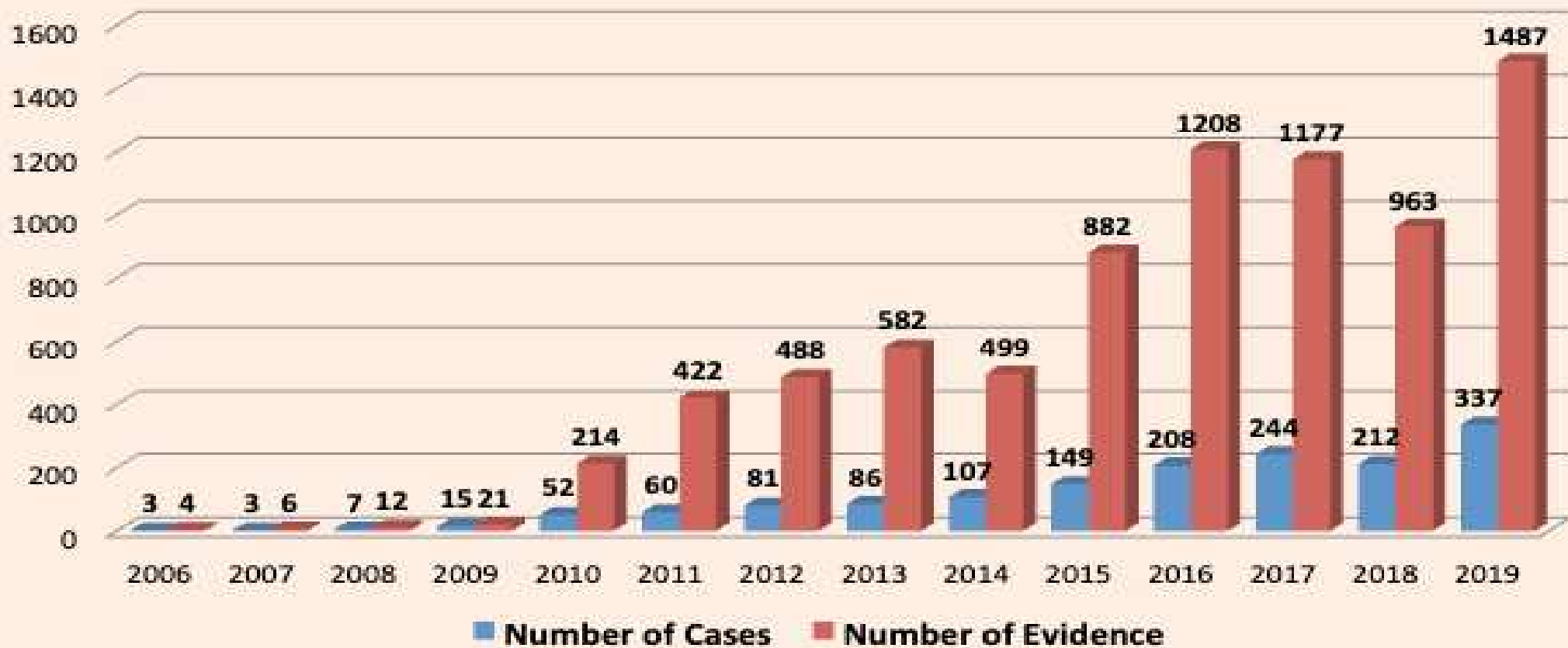
• **2011**: Computer Forensic Sub-Department was founded

• **2014**: Computer Forensic Lab. accredited for the ISO 17025

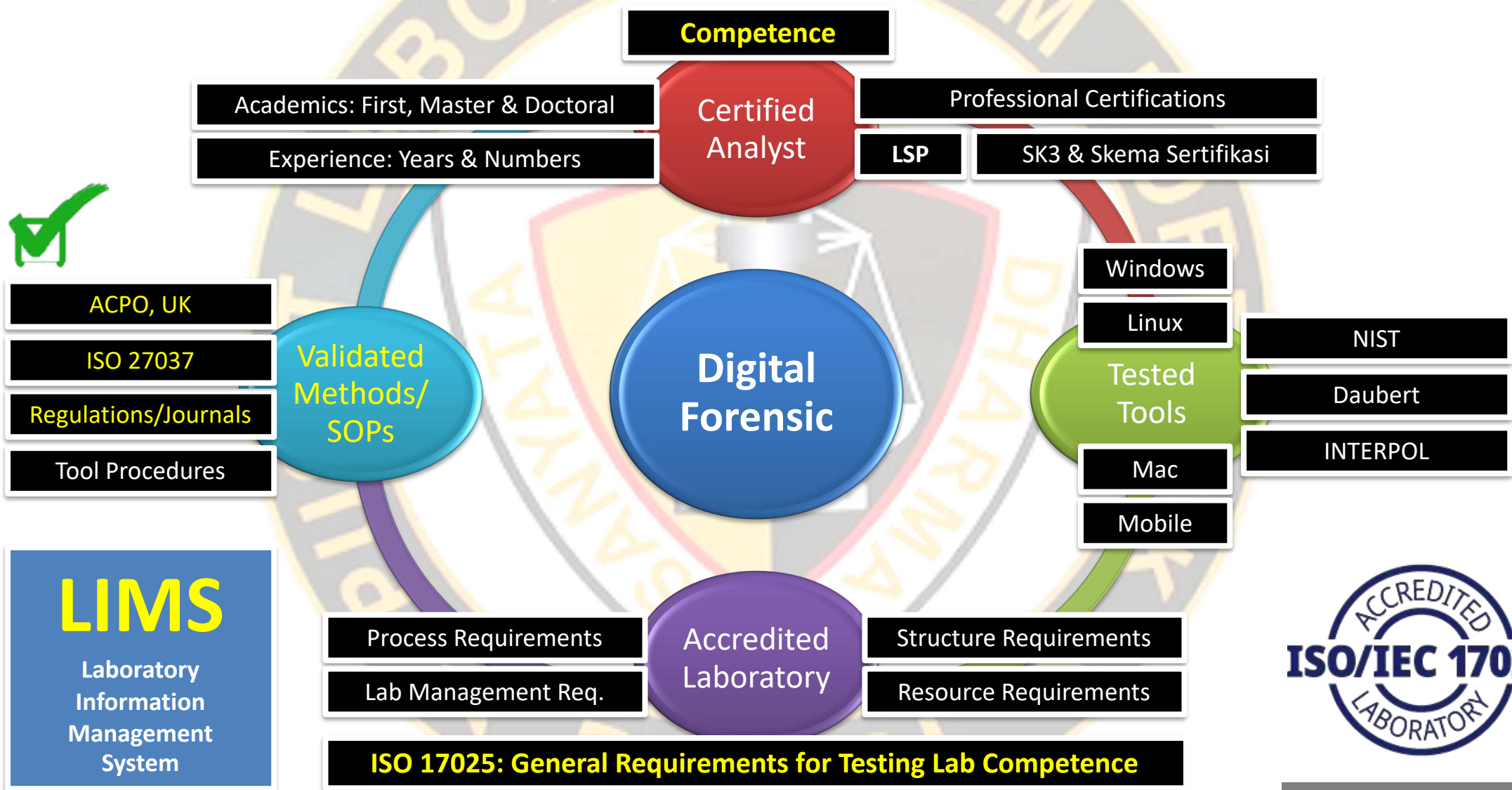
• **2015**: To support establishing the Indonesian Digital Forensic Association

# Digital Forensic Statistics

**Statistics of Digital Forensic Examination  
Indonesian Police Forensic Laboratory Centre (Puslabfor Bareskrim Polri)**

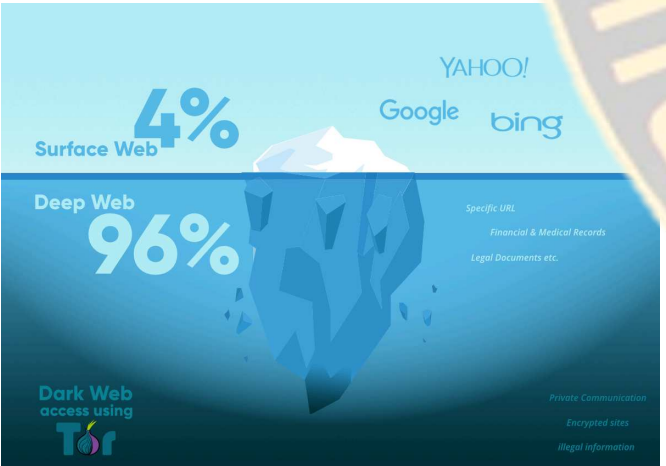
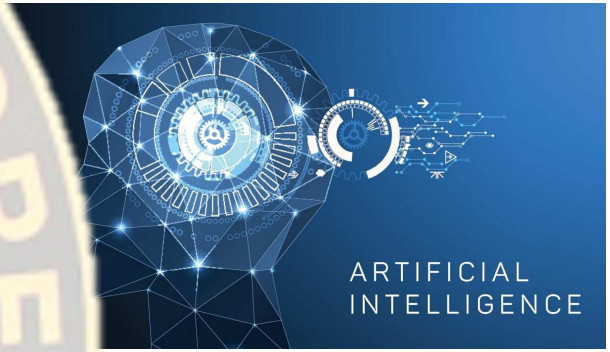
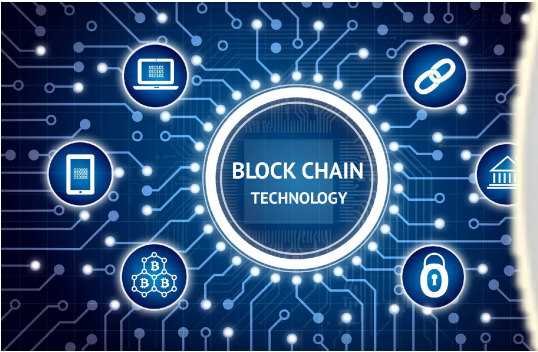
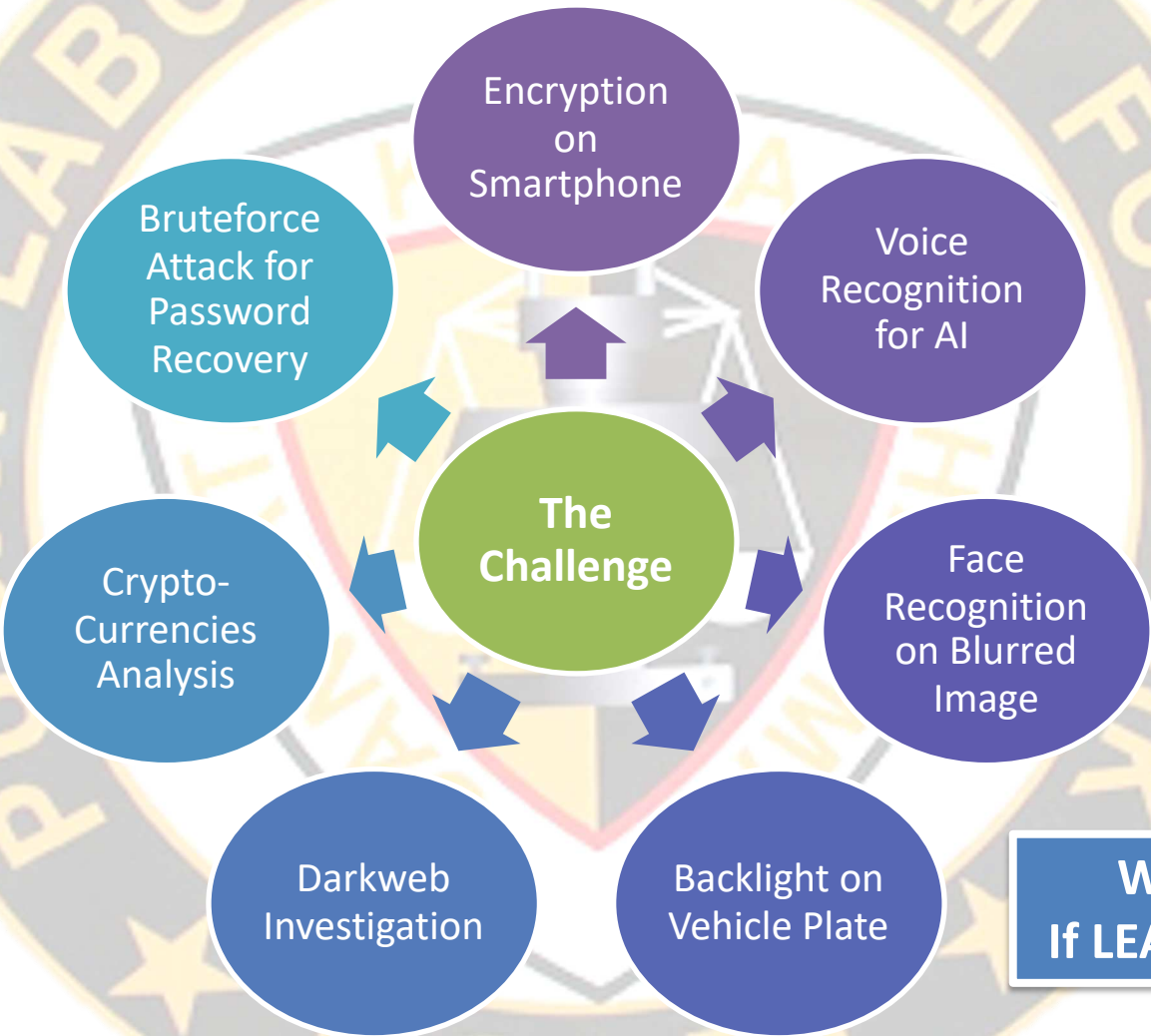


# Protocol of Digital Forensic





# Challenge of Digital Forensic



What next to do..?  
If LEA does not have Lab.



**DIGITAL FORENSIC WITH JOY**

**BE SOMEONE WHO BENEFITS OTHERS**

**THANKS FOR YOUR ATTENTION**

**YOU'LL  
NEVER  
WALK  
ALONE**