“ Forensic Tools and Techniques ”

เทคนิคการสืบค้นหาหลักฐานทางด้านการบัญชีนิติวิทยา

พันธ์ศักดิ์ เสตเสถียร

Risk Consulting Partner : PwC

สมชาย ศุภธาดา

ประธานคณะทำงานพัฒนาหลักสูตรป้องกันการทุจริต การฟอกเงิน และการสนับสนุนการก่อการร้าย : สภาวิชาชีพบัญชีแห่งประเทศไทย

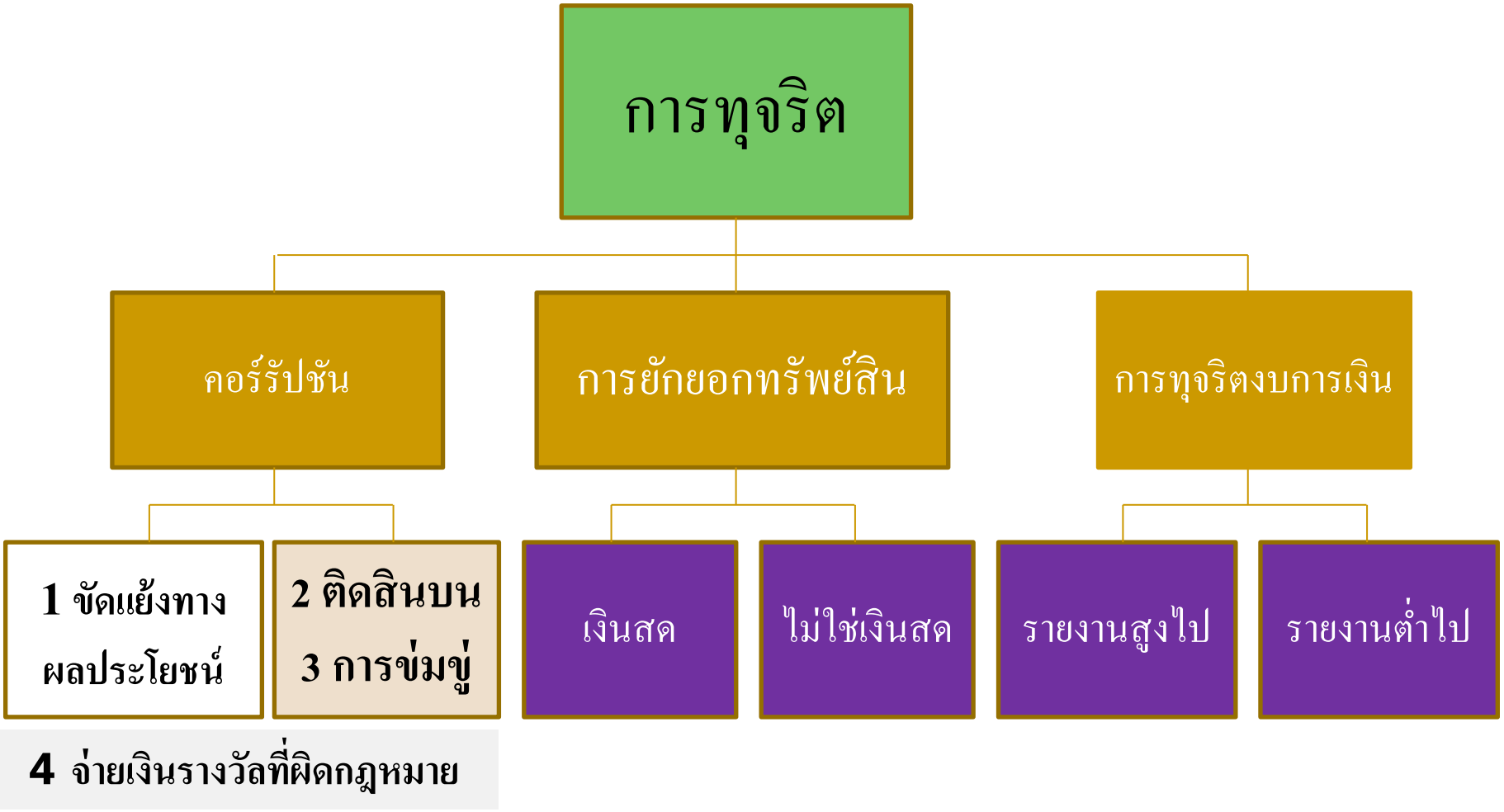
September 23 , 2021

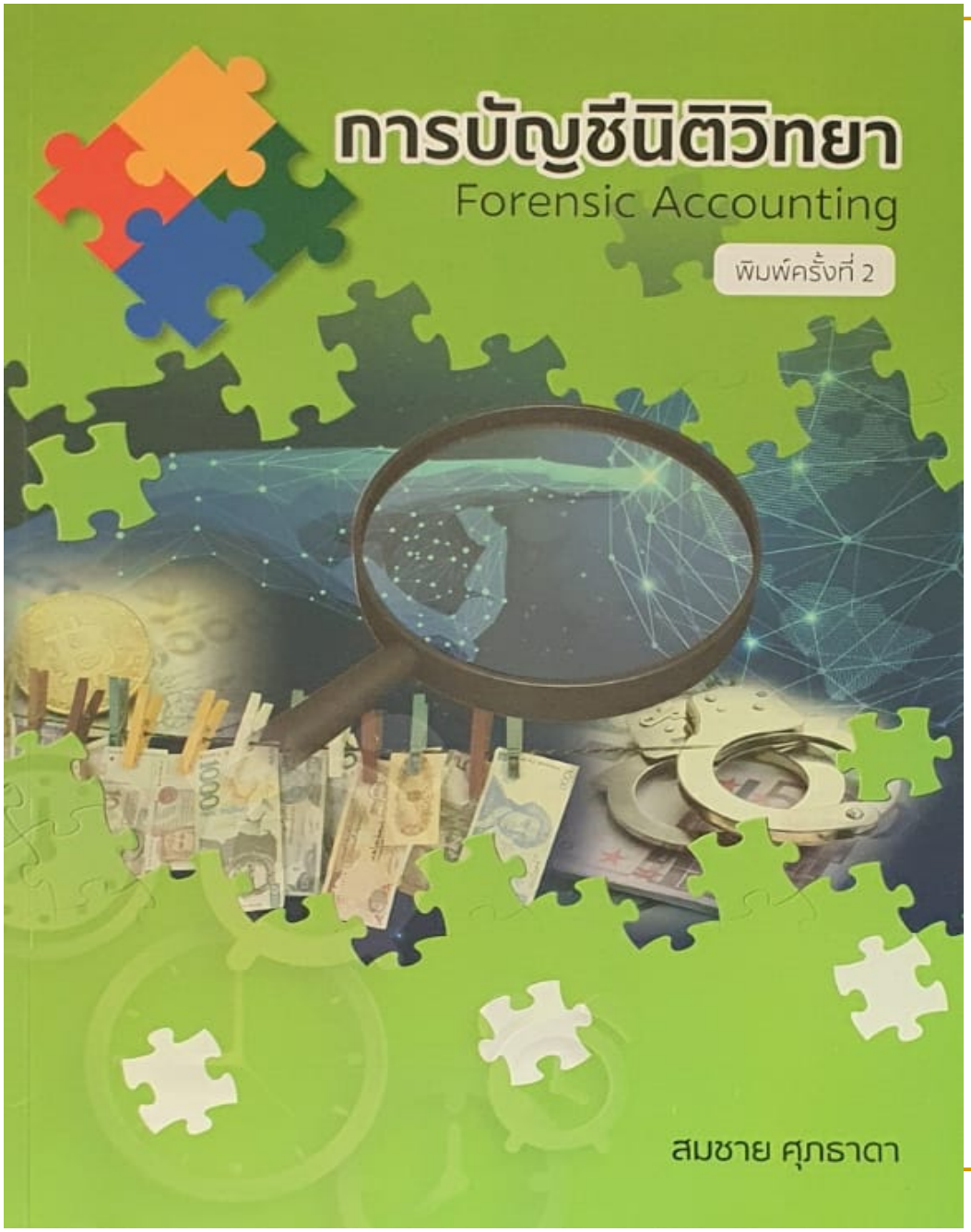
หัวข้อประเด็นการเสวนา (Agenda)

- ๑ รูปแบบของการทุจริตคอรัปชัน และ คดีความที่เกิดขึ้นในองค์กร มีความซับซ้อนเพียงใดในปัจจุบัน
- ๒ สัญญาณเตือนคืออะไร และ ควรดำเนินการสอบสวนเมื่อไร
- ๓ ประเภทและแหล่งที่มาของพยานหลักฐาน
- ๔ เทคนิคของนักบัญชีนิติวิทยา ในการสืบค้นหาหลักฐานเพื่อให้ได้ข้อเท็จจริงที่เป็นประโยชน์ต่อคดีความ
- ๕ ปัญหาและอุปสรรคที่นักบัญชีนิติวิทยาต้องเผชิญ ในการปฏิบัติงาน และ แนวทางการปฏิบัติงานให้บรรลุวัตถุประสงค์
- การอธิบาย และ ตอบประเด็นคำถาม

๑ รูปแบบการทุจริตคอร์รัปชัน ความซับซ้อนในปัจจุบัน

ต้นไม้ การทุจริต (Fraud Decision Tree)





การบูรณาการองค์ความรู้ด้าน **การบัญชีและนิติศาสตร์** ประยุกต์เข้ากับศาสตร์แขนงอื่น ที่มีส่วนสัมพันธ์กันอาทิเช่นสังคมวิทยา สถิติ จิตวิทยา เศรษฐศาสตร์ พฤติกรรมศาสตร์ และเทคนิคการสืบสวนสอบสวน และ สื่อสารสิ่งที่ค้นพบจากการวิเคราะห์ **เพื่อประโยชน์ต่อการให้บริการด้าน (และเสริมสร้างปฏิรูป) กระบวนการยุติธรรม**

บทที่ 1 วิชาชีพการบัญชีนิติวิทยา

บทที่ 2 ทฤษฎี ประเภทของการทุจริต ผลสำรวจ

บทที่ 3 กระบวนการด้านการบัญชีนิติวิทยา

บทที่ 4 วิธีการสืบสวน การจัดการพยานหลักฐาน

บทที่ 5 การสอบสวน การสัมภาษณ์ซักถามข้อมูล

บทที่ 6 แผนการทุจริต และการประยุกต์

บทที่ 7 การทุจริตรายงานทางการเงิน

บทที่ 8 อาชญากรรมทางเศรษฐกิจ

บทที่ 9 การทุจริตคอร์รัปชัน

บทที่ 10 การฟอกเงิน การสนับสนุนการก่อการร้าย

บทที่ 11 วิทยาศาสตร์ข้อมูล กับ การบัญชีนิติวิทยา

บทที่ 12 อาชญากรรมไซเบอร์ และการตรวจพิสูจน์ พยานหลักฐานดิจิทัล

บทที่ 13 การประเมินมูลค่าความเสียหาย

บทที่ 14 การเขียนรายงานการบัญชีนิติวิทยา

บทบาท ของ การบัญชีนิติวิทยา

- **สืบสวนและวิเคราะห์หลักฐานทางการเงิน**
- สื่อสารสิ่งที่ค้นพบจากการสืบสวนในรูปรายงาน ตารางบัญชี และ รายงานสรุป
- **ประสานงาน ให้ความสนับสนุนการสืบสวนในขั้นต่อไป รวมทั้ง การให้การในชั้นศาลในฐานะผู้ชำนาญการ**

หัวข้อประเด็นการเสวนา (Agenda)

- ***สืบสวน สอบสวน ไต่สวน*** **สามคำจำให้แม่น**
- **ประเภทของหลักฐาน**
- **เครื่องมือเทคนิคในการสืบค้นหาหลักฐานทางด้านการบัญชีนิติวิทยา**
- **การสืบสวนในบริบทของ Blockchain & Digital Currency**
- **ประเด็นร่วมสมัยในการทำงานของนักบัญชีนิติวิทยา**

- ปุจฉา วิสัชนา [Q&A]

สามคำ จำให้แม่น

- **<u>สืบสวน</u>** : Investigation หมายถึงการแสวงหาข้อเท็จจริงและหลักฐานเพื่อทราบรายละเอียด *เป็นขั้นตอนหาผู้ต้องสงสัย*
- **<u>สอบสวน</u>** : Inquiry หมายถึงการรวบรวมพยานหลักฐานและการดำเนินการทั้งหลาย เพื่อให้ได้ข้อเท็จจริง พิสูจน์ความผิด หรือ เอาผู้กระทำผิดมาลงโทษ *ขั้นตอนนี้คือทราบผู้ต้องสงสัยแล้ว*
- **<u>ไต่สวนมูลฟ้อง</u>** : Preliminary examination เป็นกระบวนการยุติธรรมทางด้านศาลที่จะทำการวินิจฉัยมูลคดี *ขั้นตอนนี้ผู้ต้องหาจะถูกเรียกว่า “จำเลย”*

Forensic Tools and Techniques

- **Forensic Specialist** >>> นักบัญชีนิติวิทยา
  - an individual having expertise and/or training and experience in one or more disciplines that can be used in a forensic environment
- **Forensic Procedures**

  กระบวนการด้านการบัญชีนิติวิทยา
  - tools and/or techniques employed in the systematic gathering of evidentiary data that can be presented in a court of law

- ตรวจพบการฉ้อฉลฉ้อโกงทุจริต ได้อย่างไร

  - Tips/Whistleblowers (40%)
  - Internal Audits/Internal Controls (31%)
  - Accident (20%)
  - External Audits (8%)
  - Notified by Police (1%)

แหล่งที่มาของเบาะแส

- Employees (57%)
- Customers (18%)
- Vendors (13%)
- Anonymous (12%)

๒ สัญญาณเตือน และ ควรดำเนินการสืบสวนเมื่อไร

- **สัญญาณธงแดง**
  - The so-called "**Indicia of Fraud**"
    - do not necessarily indicate the existence of fraud
    - exercise caution in forming an opinion before investigating

- **Some "Indicia"**
  - **Lack of Corporate Governance** การขาดธรรมาภิบาล
    - no written policies and/or procedures
    - lack of Internal Controls
    - frequent or unusual Related Party transactions
  - **Questionable Accounting Activities**
    ธุรกรรมทางบัญชีที่น่าสงสัย
    - Management override of Internal Controls
    - unreconciled subsidiary & General Ledger accounts
    - continuous adjustments of book to physical inventories
    - topside Journal Entries (ดูสไลด์ถัดไป)
    - Excessive number of manual checks

- In accounting, ***a top-side journal entry***

  is a *manual adjusting entry recorded at the corporate level, often when preparing consolidated financial statements for subsidiaries.*

  Although such entries can be valid, they are often used to perpetuate fraud by closing gaps between actual operating results and the results reported to the investing public

- **Some "Indicia":** (cont'd)
  - Behavioral Issues ประเด็นทางด้านพฤติกรรม
    - failure to take vacations
    - living beyond one's means
    - Insider trading
    - early arrival – late departure

การฉ้อฉลที่แตกต่างกันในสภาพแวดล้อมที่แตกต่างกันไป

ย่อมมีสัญญาณธงแดงแยกต่างกันในบริบทนั้น ๆ

Different frauds in different environments each have their own red flags

- **Predication**
  - "the totality of circumstances that would lead a reasonable, prudent, and professionally trained person to believe that a fraud has occurred, is occurring, or will occur"

Notification and Plan of Action

- Who needs to know? (Boss? Audit Committee?, Board of Directors? General Counsel?)
- What resources do we have to do the work?
- Do we need help?
- Where do we get help if we need it?

Forensic Tools and Techniques

- Audit procedures
- Audit software
- Develop specialized procedures/routines

But what else can be done?

๓ ประเภท และ แหล่งที่มาของพยานหลักฐาน

ประเภทของหลักฐาน โดยทั่วไป

- **Physical** This type of evidence includes tangible objects that can be physically carried into a courtroom and shown to a jury. It is said to speak for itself.
- **Testimonial** This evidence includes testimony made under oath by eyewitnesses, expert witnesses, and character witnesses as well as confessions and hearsay evidence.
- **Documentary** This evidence type normally includes recorded information, such as an audio or video recording or a transcript of a telephone intercept. Unlike physical evidence, documentary evidence does not speak for itself but requires support from an expert witness
- **Demonstrative** Includes charts, graphs, and computer reconstructions that attorneys or expert witnesses can prepare for use in either direct testimony or cross-examination.

Testimonial Evidence หลักฐานคำให้การของประจักษ์พยาน	**Documentary Evidence** พยานเอกสาร
Physical Evidence วัตถุพยานทั่วไป	**Personal Observation** การสังเกตการณ์ส่วนบุคคล

Physical Evidence <u>วัตถุพยานทั่วไป</u>

- การสืบสวนเพื่อคลี่คลายคดีความมักพึ่งพิง physical evidence หลักฐานพยาน และ คำรับสารภาพ
- <u>คดีทางเศรษฐกิจการเงิน</u> ต้องใช้หลักฐานเอกสารจำนวนมากเช่น หลักฐานจากคอมพิวเตอร์ เอกสารทางธนาคาร การรับจ่ายโอนเงิน หลักฐานที่ดีส่วนช่วยอย่างมากในการที่ผู้ต้องสงสัยจะสารภาพได้ง่ายขึ้น และ พยานเองมีแนวโน้มให้ความร่วมมือมากขึ้นเมื่อตระหนักดีว่ามีหลักฐานที่แน่นหนา
- *โดยทั่วไปบันทึกทางการเงินเป็นหลักฐานทางกายภาพ**ที่สำคัญที่สุด** สำหรับนักบัญชีนิติวิทยา อาชญากรรมทางการเงินส่วนใหญ่มักทิ้งร่องรอยทางด้านการเงิน หรือ บันทึกเส้นทางการเคลื่อนย้ายแปรเปลี่ยนรูปของเงินตรา*

Forensic Identification

- **การระบุหลักฐาน**ทางนิติวิทยาศาสตร์เกิดขึ้นเมื่อหลักฐานทางกายภาพสามารถเชื่อมโยงกับวัตถุหรือบุคคลใดวัตถุหนึ่ง**โดยเฉพาะและชัดเจน**

- หลักการเกี่ยวกับการระบุตัวตนทางการบัญชีนิติวิทยามาจาก **Locard exchange principle** ที่กล่าวว่า **“every contact leaves a trace.” ทุกการสัมผัสย่อมทิ้งร่องรอย**

- การระบุหลักฐานทางการบัญชีนิติวิทยามักจะขึ้นอยู่กับจุดเปรียบเทียบ จากการจับคู่ (matching) หรือการรับรู้แบบแผน (pattern recognition) บางอย่างสามารถนำมาระบุถึงการจำแนกกลุ่มเฉพาะ หรือ การระบุตัวตนที่เป็นเอกเทศได้

Legal Evidence หลักฐานทางกฎหมาย

- หลักฐานที่อ้างเป็นพยานหลักฐานได้ (Admissible Evidence)

หลักฐานที่สามารถรับไว้พิจารณาได้โดยศาล มาตรา ๒๒๖ แห่งประมวลกฎหมายวิธีพิจารณาความอาญา บัญญัติว่า “พยานวัตถุ พยานเอกสาร หรือพยานบุคคลซึ่งน่าจะพิสูจน์ได้ว่าจำเลยมีผิดหรือบริสุทธิ์ ให้อ้างเป็นพยานหลักฐานได้ แต่**ต้องเป็นพยานชนิดที่ไม่ได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวงหรือโดยมิชอบประการอื่น และให้สืบตามบทบัญญัติแห่งประมวลกฎหมายนี้หรือกฎหมายอื่นอันว่าด้วยการสืบพยาน**”

เครื่องมือเทคนิคการสืบสวน 7 อย่าง

The 7 Recognized Investigative Tools and Techniques

used by

Forensic Specialists / Fraud Examiners

[Presented by Richard Nossen]

Forensic Tools and Techniques

1. Public Document Reviews and Background Investigations
   สอบทานเอกสารสาธารณะและสืบสวนภูมิหลัง
2. Interviews of Knowledgeable Persons
   สัมภาษณ์ผู้รู้ผู้เชี่ยวชาญ
3. Confidential Sources
   จากแหล่งข่าวไม่เปิดเผย
4. Laboratory Analysis of Physical and Electronic Evidence
   วิเคราะห์หลักฐานในห้องปฏิบัติการ

Forensic Tools and Techniques

(ต่อ)

5. Physical and Electronic Surveillance
   การเฝ้าสอดแนมทุกรูปแบบ

6. Undercover Operations
   ปฏิบัติการลับ

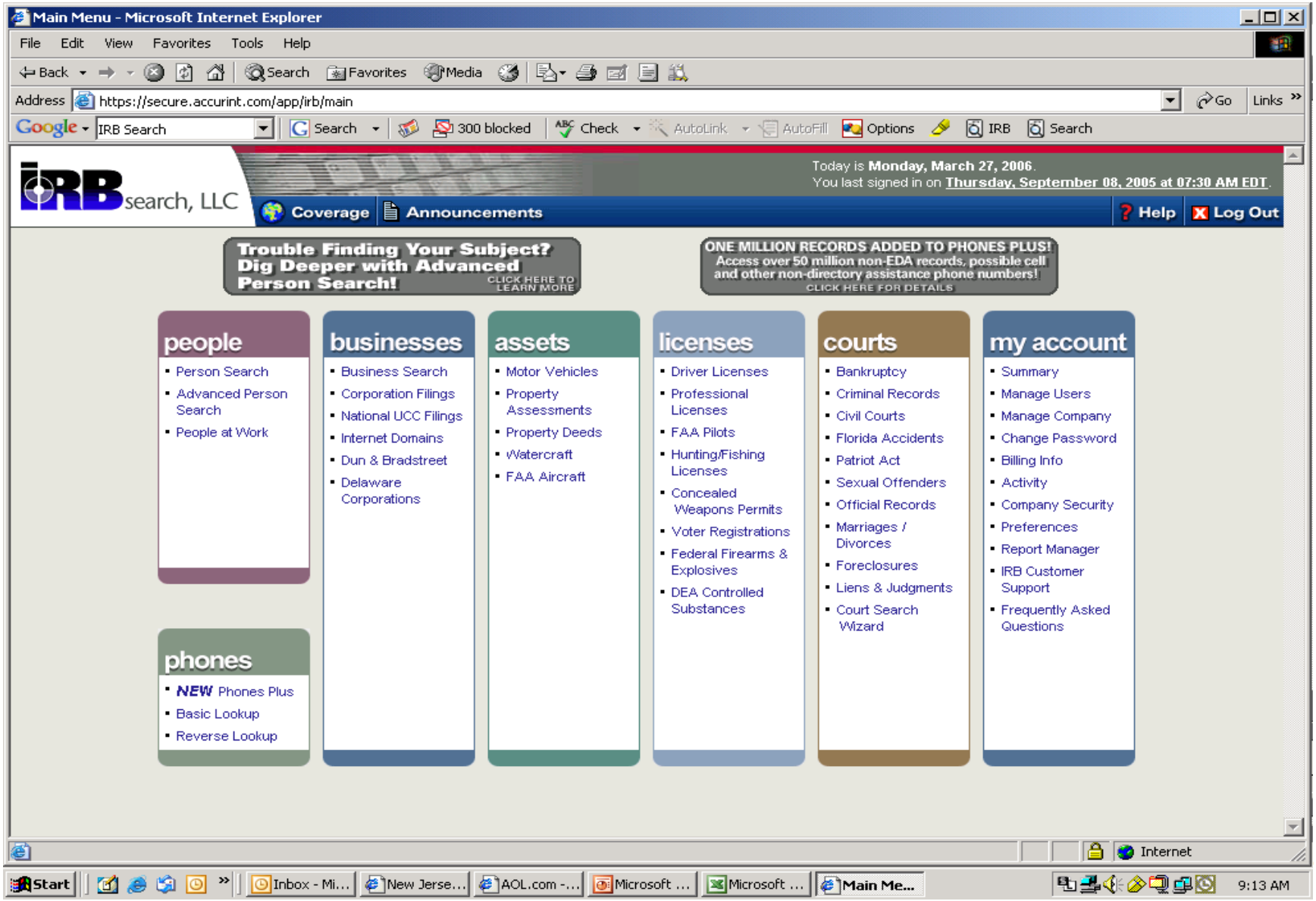
7. Analysis of Financial Transactions
   การวิเคราะห์ธุรกรรมทางการเงิน

1 Public Document Reviews and Background Investigations

- Public Databases
- Websites ของหน่วยงานต่าง ๆ
- ข้อมูลส่วนงานราชการ ส่วนงานปกครองท้องถิ่น
- Corporate Records
- Internet

- **Public Databases**
  - มีแหล่งรวบรวมข้อมูลและให้ข้อมูลโดยการบอกรับเป็นสมาชิก
  - Reliability of data
  - What type of data is available?

Forensic Tools and Techniques



Forensic Tools and Techniques

- **Website ของหน่วยงานต่าง ๆ**
  - แตกต่างกันไปตามแต่ละหน่วย
- **ข้อมูลส่วนงานราชการ ส่วนงานปกครองท้องถิ่น**
  - Real Estate records; business registrations
- **Corporate Records**
  - Stock Transfer records; Accounting data; vendors; competitors; customers

- **Internet**
  - Search Engines
  - News Sources/Newspapers
  - Telephone Numbers and Addresses
  - Maps
  - Legal Resources
  - Government Sites

2 Interviews of Knowledgeable Persons

- Interview vs. Interrogation
- Continuous process throughout an investigation
- Gain additional information with each interview
- Evidence from witnesses provides additional leads
- May identify additional witnesses
- Interview the target only after completing the interviews of the peripheral witnesses

3 Confidential Sources

- Hotlines
- E-mail
- Letters
- Current Employees
- Former Employees
- Vendors & former vendors
- Customers & former customers

- **Confidential Sources** (cont'd)
  - **Cautions**
    - Use professional skepticism in assessing information
    - Information supplied to discredit or embarrass the target
    - Weigh the value of the evidence provided against the possibility that it may be false or cannot be proven
    - Validate all evidentiary matter provided
    - Do not assure absolute confidentiality

4 Laboratory Analysis of Physical and Electronic Evidence

- Protection/Validation of Evidence
  - Federal Rules of Evidence
  - Chain of Custody

“The only thing worse than a bad document is a bad document that has disappeared!!!”

- **Laboratory Analysis of Physical and Electronic Evidence** (cont'd)

  - Altered & Fictitious Documents
    - physical examination
    - fingerprint analysis
    - forgeries
    - ink sampling
    - document dating

- **Laboratory Analysis of Physical and Electronic Evidence** (cont'd)

  - Computer Forensics
    - hard disk imaging
    - E-mail analysis
    - search for erased files
    - analyze use & possible misuse
    - computer software to analyze data

- **5 Physical and Electronic Surveillance**
  - Physical
    - usually done by law enforcement or PI's
    - surveillance cameras
    - can also be used to verify addresses for vendors, employees, etc.
  - Electronic
    - Internet surveillance
    - E-mail

- **6 Undercover Operations**
  - usually a recommendation to use
  - can be done
  - **best left to professionals**

7 Analysis of Financial Transactions

- Horizontal/vertical analysis
- Authorization of new vendors & employees
- Comparison of employee & vendor addresses
- Analysis of sales returns & allowance account
- Management override of controls
- Different reviews based on known industry fraud schemes

สรุป

- Some useful definitions (Forensic, Specialist, Procedures)
- Fraud detection sources
- Red Flags
- Action to be taken
- The tools & techniques of the forensic specialist

๔ เทคนิคในการสืบค้นหาหลักฐานยุค **Digital**

Forensic Science &
Information Technology

Investigatory Tools in Forensic Science

- **Forensic science** can be used not only to collect court-admissible evidence but also as an investigatory tool

- Some investigatory tools
  - Brain printing
  - Biometrics
  - Profiling
  - Data mining

Computer Forensics

- **Computer forensics** involves applying computer science techniques to assist in investigations relating to a wide range of legal matters.
- Three typical tasks of computer forensics:
  - Identify the perpetrator(s) of a crime or other type of malfeasance. **ระบุผู้บุกรุกผู้กระทำผิด**
  - Locate and recover data, files, or e-mail messages relating to a crime or civil matter. **หา กู้คืน ข้อมูลที่เกี่ยวข้อง**
  - Reconstruct damaged databases and files. **จัดสร้างข้อมูลและทำฐานข้อมูลที่ถูกทำลายขึ้นมาใหม่**

Audit Goals of a Forensic Investigation

Rules of Evidence

- Complete ครบถ้วน
- Authentic ของแท้
- Admissible รับเป็นหลักฐานได้
- Reliable ไว้ใจได้
- Believable เป็นที่เชื่อได้

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ (ที่แก้ไขเพิ่มเติม)

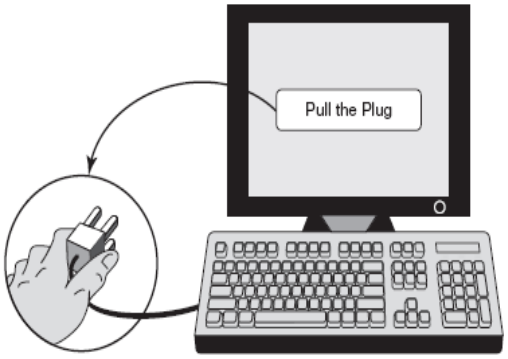
- **มาตรา ๑๘** *ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวน ในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือในกรณีที่มีการร้องขอตามวรรคสองให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด*

- (๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดมาเพื่อให้ถ้อยคำส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้
- (๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง
- (๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน
- (๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

- (๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่
- (๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐาน หรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้
- (๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว
- (๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

ขั้นตอนในการสืบค้นหาหลักฐานทางการบัญชีนิติวิทยาในเครื่องคอมพิวเตอร์

1. Size Up the Situation
2. Log Every Detail
3. Conduct the Initial Survey
4. Assess the Possibility of Ongoing Undesirable Activity
5. Power Down
6. Check for Booby Traps
7. Duplicate the Hard Drive or Other Permanent Storage Unit
8. Analyze the Hard Drive



Computer Analysis and Response Team (CART)

- Content determine the content of computer files
- Comparison compare the content to known reference files
- Transaction determine the exact time and sequence of creation
- Extraction extract data from computer storage
- Deletion recover deleted data files
- Format conversion convert data from one format to another
- Keyword searching find data that contains keywords
- Password recovery find or recover passwords
- Limited source code study computer program to identify processing steps that can be of interest to investigate

Digital Evidence

- หลักการสำคัญที่เจ้าพนักงานซึ่งมีอำนาจสืบสวนสอบสวนรวบรวมพยานหลักฐานดิจิทัล และผู้ปฏิบัติงานด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัลพึงต้องระมัดระวังคือ **การได้มาซึ่งพยานหลักฐานดิจิทัล**ต้องปฏิบัติให้ถูกต้องชอบด้วยประมวลกฎหมายวิธีพิจารณาความอาญา และบทกฎหมายเฉพาะอย่างอื่นซึ่งระบุขั้นตอนปฏิบัติในการได้มาซึ่งพยานหลักฐานดิจิทัล โดยเฉพาะอย่างยิ่ง บรรดาข้อมูลคอมพิวเตอร์ ซึ่ง**มาตรฐานในการจัดเก็บพยานหลักฐานดิจิทัลควรต้องเป็นไปตามมาตรฐานสากล**ในการเข้าค้นและยึดอุปกรณ์อิเล็กทรอนิกส์ซึ่งเป็นมาตรการพื้นฐานที่จะทำให้พยานหลักฐานที่รวบรวมได้มานั้นมีความน่าเชื่อถือและชอบด้วยกฎหมายเพียงพอที่ศาลจะรับฟังและให้น้ำหนักกับพยานหลักฐานดิจิทัลในการลงโทษผู้กระทำความผิด

การระบุตัวบุคคลในเครือข่าย
Identify Individuals in a Network Environment

- Trace individuals by **IP Address**
- Email can be traced by reading IP addresses in the internal mail headers
- IP addresses can be hidden by proxy servers
- **IP addresses can be “spoofed” (i.e., falsified)**

ตัวอย่าง ฐานข้อมูล และ เครือข่าย ของหน่วยงานที่บังคับใช้กฎหมาย (ในต่างประเทศ)

Automated Fingerprint Identification

- System (IAFIS)
- National DNA Index System (NDIS)
- Combined DNA Index System (CODIS)
- National Integrated Ballistics Information Network (NIBIN)
- National Law Enforcement Telecommunications Systems (NLETS)
- National Crime Information Center (NCIC)
- **Financial Crimes Enforcement Network (FinCEN)**

Amount of digital evidence stored in South Korea as of 2020

YEAR	Pcs/laptops	CCTV	Smartphones	Databases	TOTAL
2014	3,079	510	10,626	654	14,899
2015	3,357	712	19,526	700	24,295
2016	3,923	794	26,408	1,156	32,281
2017	4,198	867	30,238	767	36,060
2018	6,239	1,065	36,986	813	45,103

การสืบสวนในบริบทของ Blockchain & Digital Currency

- Q : ทำไมสกุลเงินดิจิทัลจึงเป็นที่นิยมในหมู่อาชญากร
- A : การทำธุรกรรมสามารถเกิดขึ้นได้อย่างรวดเร็ว และ ยากที่จะติดตาม (แต่มีความเป็นไปได้ที่จะตามรอย) สกุลเงินที่อาศัยบล็อกเชนได้รับความนิยมเพิ่มขึ้นในชุมชนอาชญากร เนื่องจากนามแฝง "ธุรกรรมจะถูกจัดเก็บอย่างเปิดเผยและถาวรไว้บนเครือข่าย ซึ่งหมายความว่าทุกคนสามารถดูยอดคงเหลือและ การทำธุรกรรมของ Bitcoin addressใด ๆ ได้ อย่างไรก็ตาม ตัวตนของผู้ใช้ที่อยู่เบื้องหลังที่อยู่นั้น จะยังไม่ทราบจนกว่าจะมีการเปิดเผยข้อมูลในระหว่างการซื้อ หรือ ในสถานการณ์อื่น ๆ “
- นามแฝง ไม่ใช่ นิรนาม >> Pseudonymous Doesn’t Mean Anonymous

พัฒนาการความร่วมมือในสหภาพยุโรป

- ในฐานะพันธมิตรในโครงการ**“TITANIUM”** ที่ได้รับทุนจากสหภาพยุโรป INTERPOL ตำรวจสากลได้ช่วยพัฒนาเครื่องมือวิเคราะห์บล็อกเชนที่เรียกว่า **GraphSense** ซึ่งรองรับการติดตามธุรกรรมสกุลเงินดิจิทัล

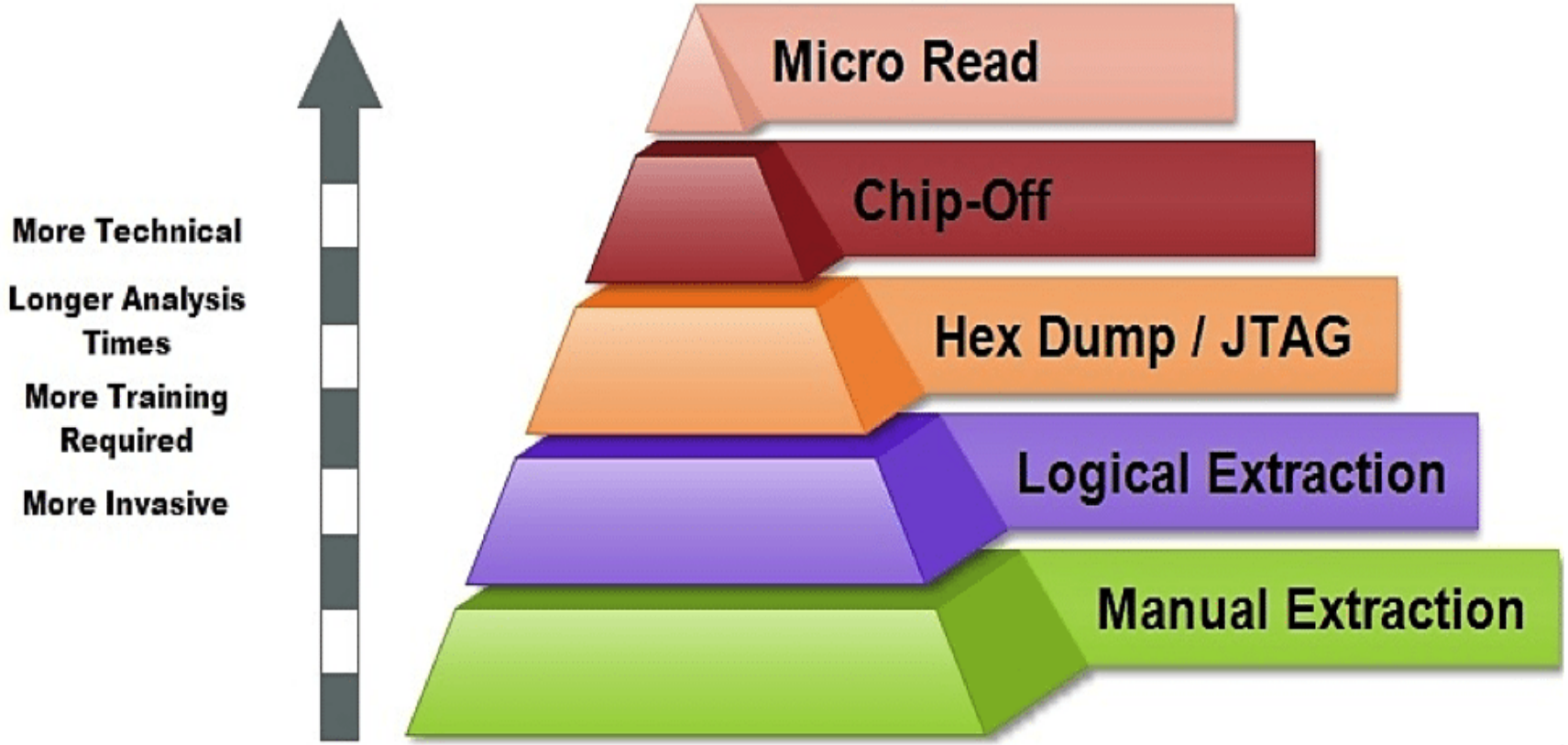
เครื่องมือนี้ช่วยให้ผู้ตรวจสอบสามารถค้นหาที่อยู่ แท็ก และธุรกรรมสกุลเงินดิจิทัลเพื่อระบุคลัสเตอร์ที่เกี่ยวข้องกับที่อยู่ และดำเนินการ 'ติดตามเงิน' เพื่อสนับสนุนการสืบสวน

จากความต้องการที่ระบุโดยประเทศสมาชิก ได้มีการดำเนินการพัฒนาเครื่องมือวิเคราะห์ที่เรียกว่า **Darkweb Monitor** ซึ่งรวบรวมข้อมูลเกี่ยวกับอาชญากรรมบน Darknet และใช้เพื่อให้ข่าวกรองที่สนับสนุนการสืบสวนของตำรวจทั่วโลก

รายละเอียดที่จะมีในฐานข้อมูลประกอบด้วย:

- ที่อยู่สกุลเงินดิจิทัล
- ปุ่ม PGP (Pretty Good Privacy encryption programme โปรแกรมเข้ารหัสความเป็นส่วนตัว)
- ที่อยู่ IP ชื่อผู้ใช้และนามแฝง
- ที่อยู่อีเมล
- โดเมนตลาดมืด
- ฟอรัมดาร์คเน็ต
- ข้อมูลในอดีตที่รวบรวมจาก Darknet ตั้งแต่ปี 2015

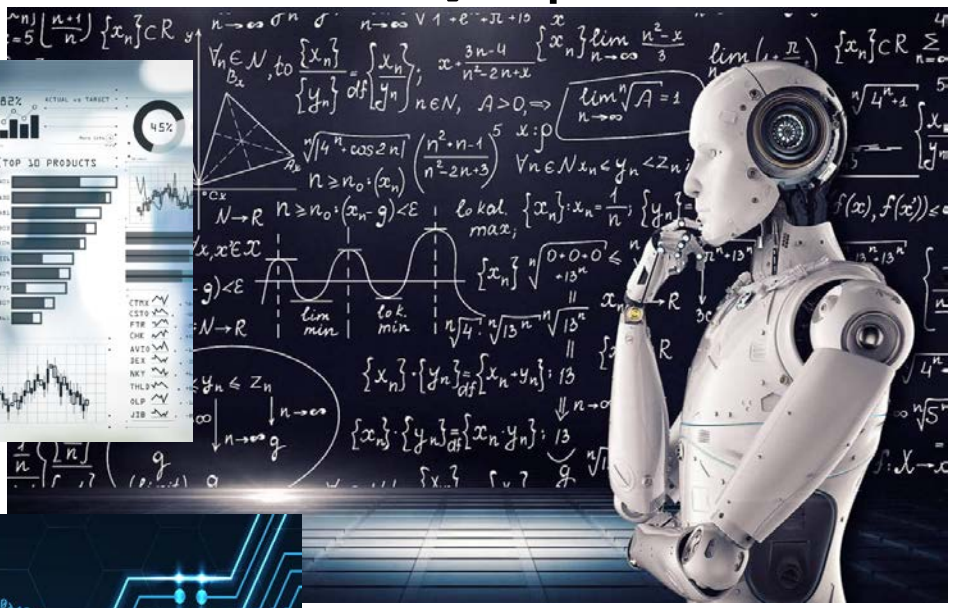
Mobile Forensic Process

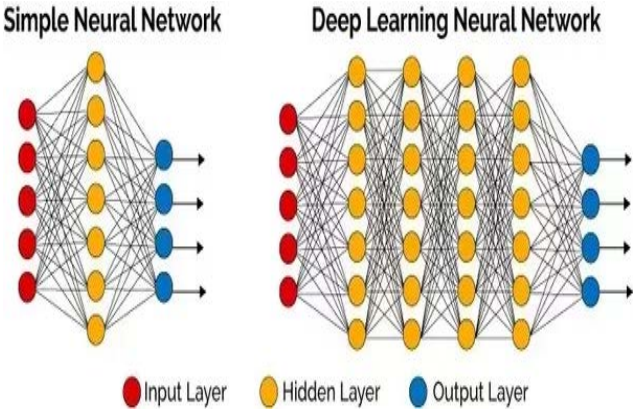


Mobile Forensic Process

วิธีแบบ Non-invasive	วิธีแบบ Invasive
1 Manual Extraction	5 Chip-off
2 Logical Extraction	
3 JTAG	6 Micro Read
4 Hex Dump	

๕ ปัญหาและอุปสรรคร่วมสมัยที่นักบัญชีนิติวิทยาต้องเผชิญ แนวทางการปฏิบัติงานให้บรรลุวัตถุประสงค์ในการเก็บรวบรวมหลักฐานยุคดิจิทัล





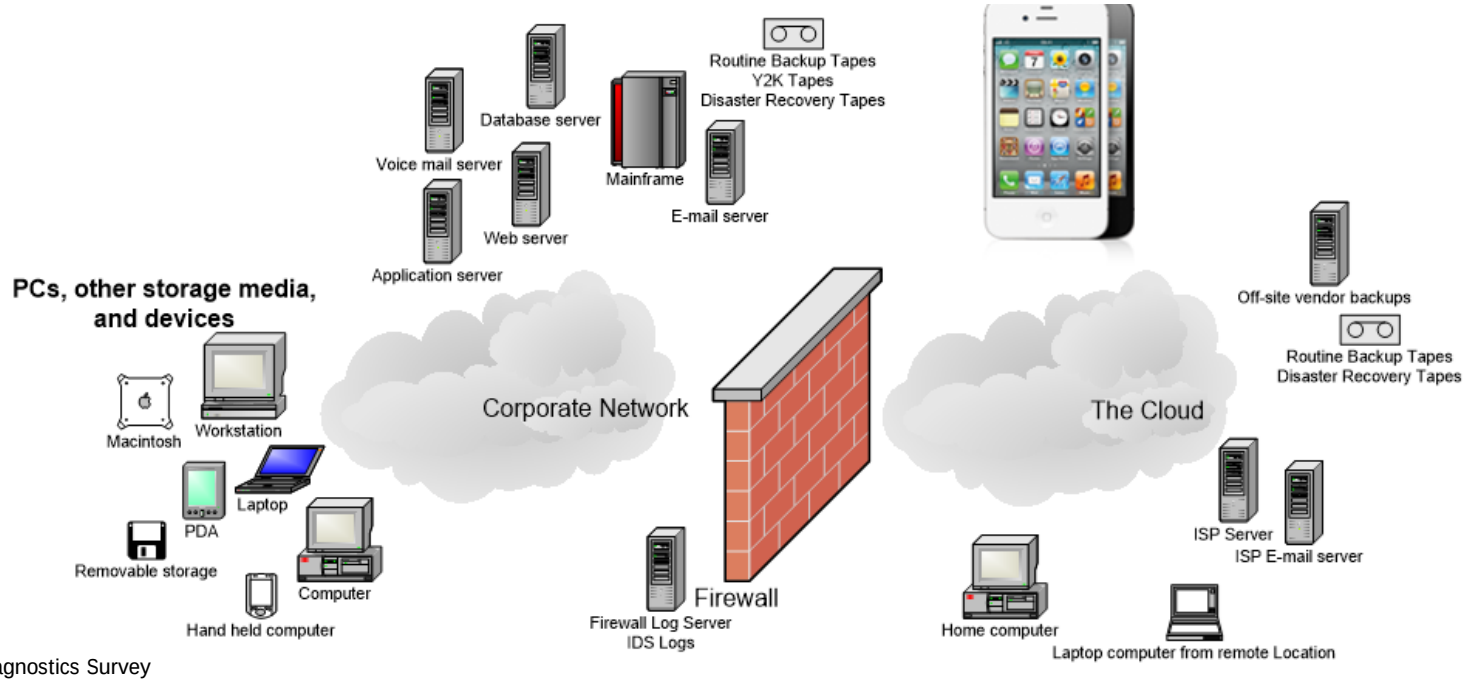
How big of your data

Fact 1: On average, every human created at least 1.7 MB of data per second in 2020

Fact 2: We created 25,000,000,000,000,000,000 data bytes (quintillion) daily in 2020

Fact 3: There were 4.66 billion active internet users around the world in January 2021

Fact 4: The end of 2021 could see 2,000,000,000,000 (two trillion) Google searches



Source: Techjury
Bain Big Data Diagnostics Survey

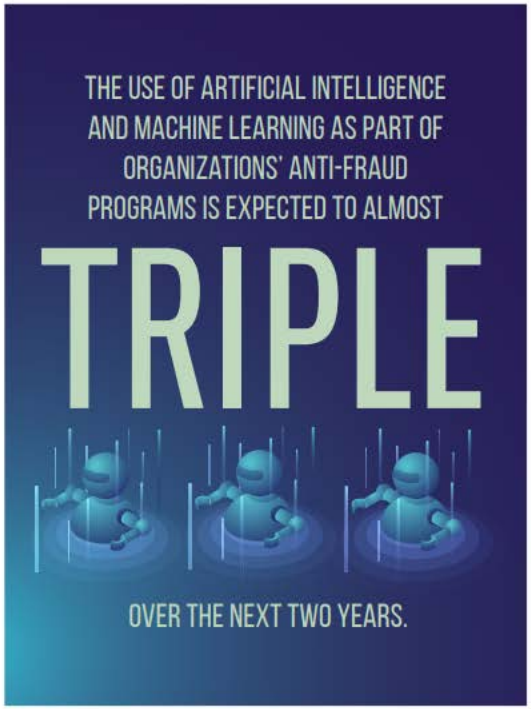
Some facts about technologies to fight against fraud

NEARLY **2/3** of organizations currently use **exception reporting or anomaly detection techniques** in their fraud-related initiatives

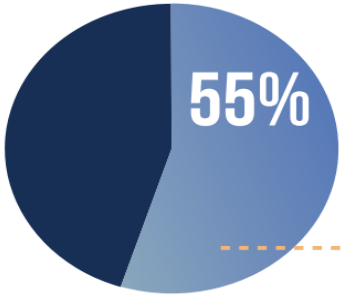
AND

MORE THAN **1/2** use **automated monitoring** of red flags or violations of business rules.

Over the next two years, the use of each of these types of analytics is expected to grow to **72%** of organizations.



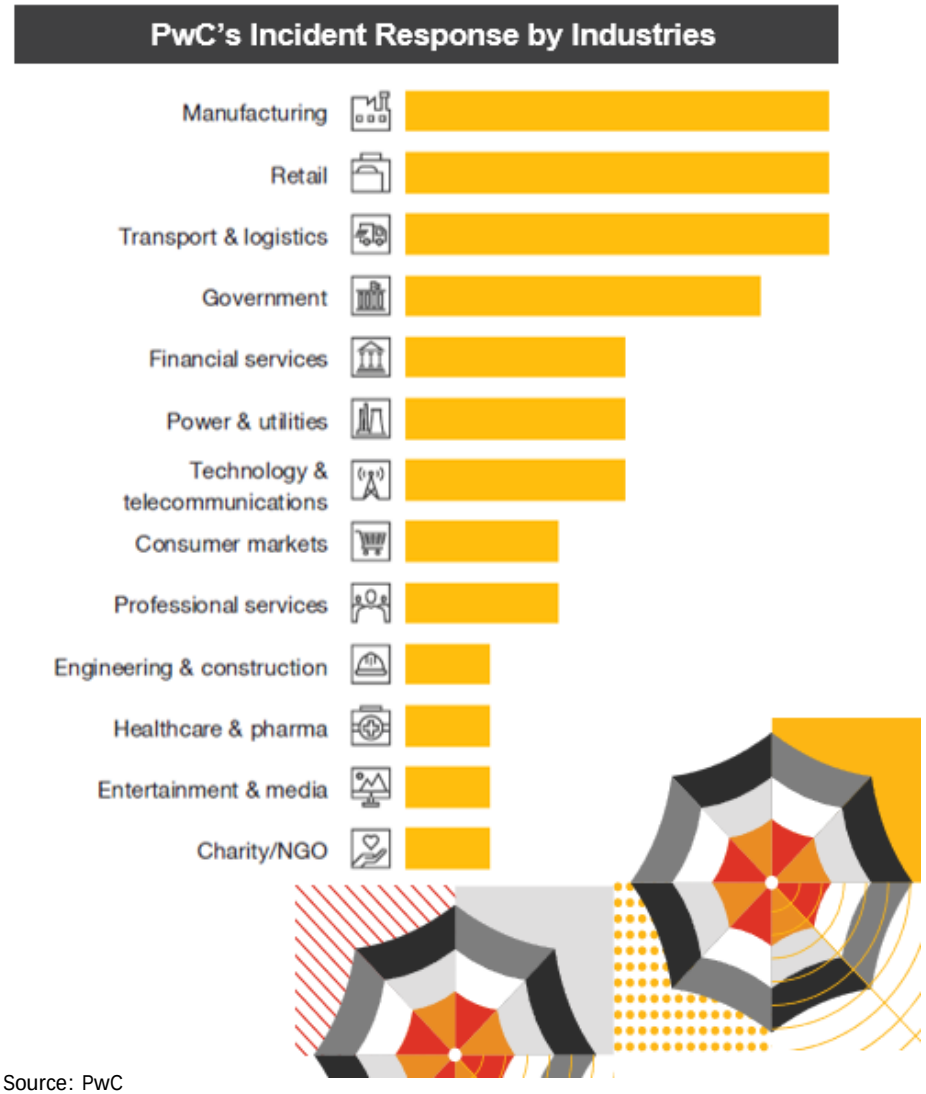
ONLY **9%** OF ORGANIZATIONS CURRENTLY USE **BLOCKCHAIN/DISTRIBUTED LEDGER TECHNOLOGY** OR **ROBOTICS** AS PART OF THEIR ANTI-FRAUD PROGRAMS.



OF ORGANIZATIONS EXPECT TO **INCREASE** THEIR BUDGETS FOR **ANTI-FRAUD TECHNOLOGY** OVER THE NEXT TWO YEARS.

Source: ACFE

Fraud & Economic Crime in a Digitized World

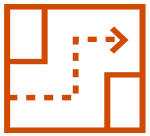


Source: PwC

Recognise the controls that help minimize fraud activities

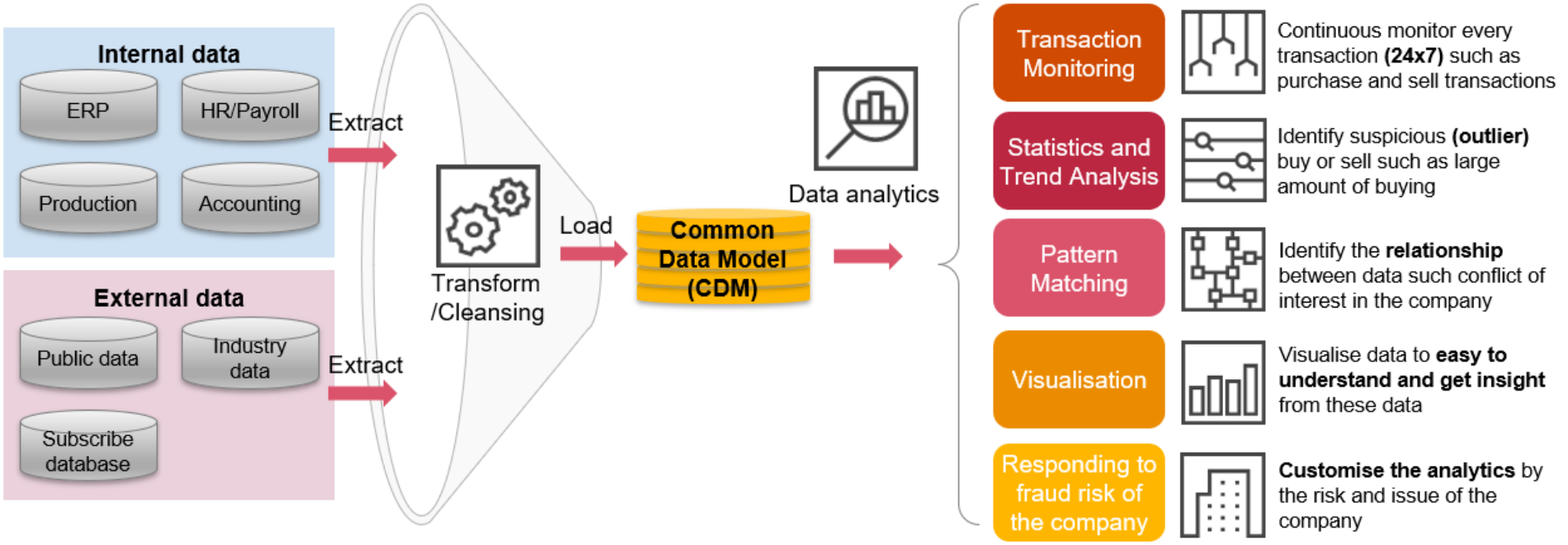
Understand how to protect personal/customer data so it is not used fraudulently

Find the fine balance between monitoring for fraud and employee privacy



Build deep understanding of customer habits through analytics, to aid in anomaly detection

Data will give you what you want to know



Source: PwC

The need for a modern fraud system

Rules are **easy to design, deploy and explain**

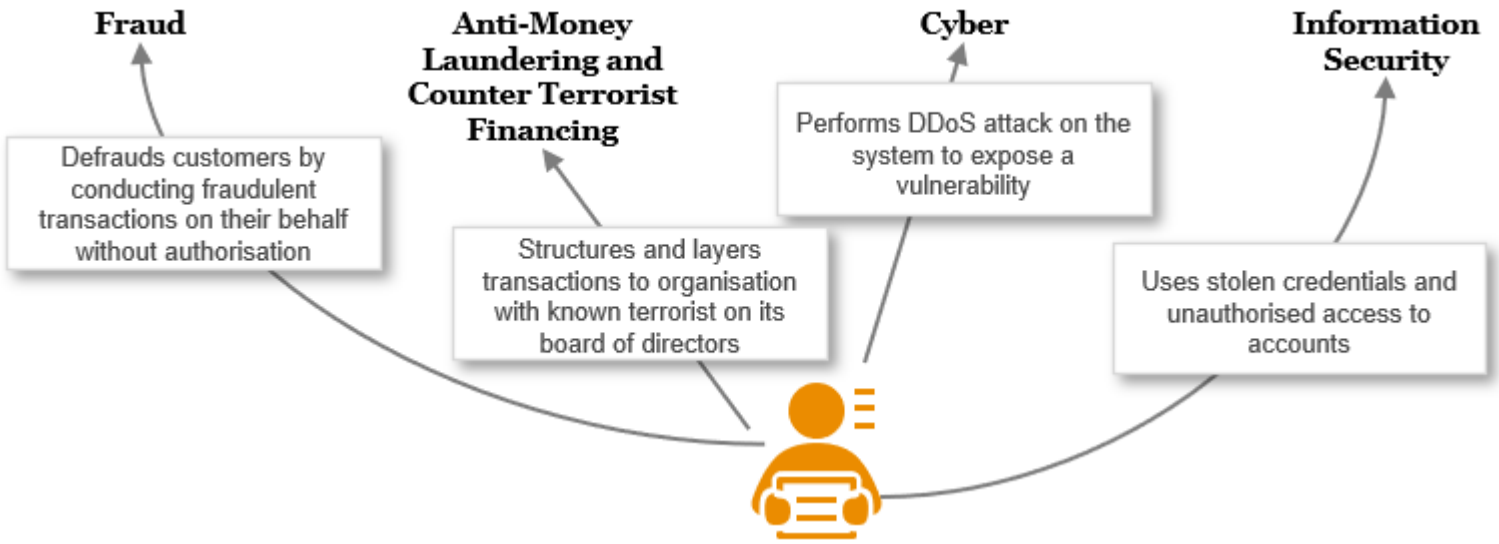
Rules are **static and do not adapt** to change in criminal behaviour

Rules **do not maximize the potential of wide ranging data** available to the organization

Rule based systems have a **high false positive rate**

Rule based systems **are unable to recognize complex patterns** to detect suspicious activity

Characteristics of rule based monitoring and detection systems



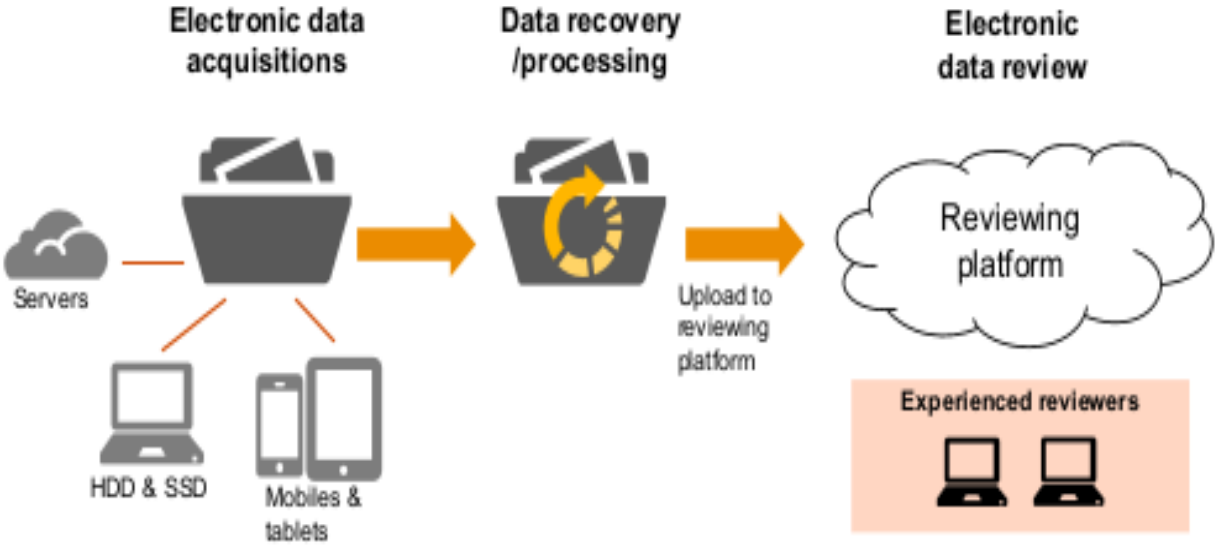
Computer Forensics

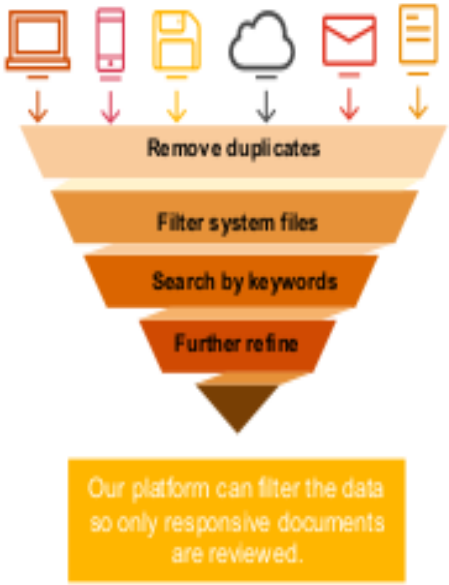
- Scientific examination and analysis of recovered (active, deleted, corrupted, hidden or partially overwritten) data in such a way that the information can be used as evidence in a court of law.
- Main focus: Preservation, Analysis, and Reporting
- Process of preserving and analysing electronic data while maintaining data integrity
- Identifying historical artifacts to trace user and system activity
- Dependent on data source and activity being analysed
- Important to use multiple tools to confirm repeated results
- Critical to maintain sound audit trail and reporting

Computer forensics is one of the techniques for the e-Discovery process.

Source: PwC

Computer Forensics





We use widely recognised acquisition tools, such as:

- Forensics Toolkit (FTK)
- Forensics Falcon
- Cellebrite

We perform:

- backup
- recovery of deleted data
- encryption
- indexing.

In the review we:

- exclude all the obviously irrelevant files
- categorise files by type, date, custodian, etc., and provide data statistics
- use keywords and other criteria to **conduct efficient reviews**

Source: PwC

Is crypto platform still secured?

Source: https://www.reddit.com/r/trinicrypto/comments/p2dvew/top_10_biggest_crypto_hacks_in_history/