Komputer Forensik

CEH4D3

About Class

- Time : Thursday 13.30 – 16.30
- Place : KU3.02.09
- Instructor : Muhammad Faris Ruriawan (FRW)
- Contact : +628123304892 (Telegram/Signal)

  muhammad.faris.ruriawan[at]gmail.com

Rules

- Attendance > 75%

References

Text Book

- Guide to Computer Forensics and Investigation [Nelson]
- Hacking Exposed: Computer Forensics 2nd, Davis, Philipp and Cowen [Davis]
- Digital Watermarking and Steganography [Ingemar]
- A Practical Guide to computer forensics Investigation Darren R. Hayes [Hayes]
- File System Forensic Analysis [Carrier]
- Internet Forensic R. Jones [Jones]
- Forensics With Open Source Tools Cory Altheide, Harlan Carvey [Cory]

Others

- Computer Hacking Forensic Investigator [CHFI]

Class Assessment

- Attendance 5 %
- Assignment 25 %
- Quiz 10 %
- Exam 60 %

Grading Scale (NMK)

- A NSM > 80
- AB 80 ≥ NSM > 70
- B 70 ≥ NSM > 65
- BC 65 ≥ NSM > 60
- C 60 ≥ NSM > 50
- D 50 ≥ NSM > 40
- E 40 ≥ NSM

Note: NSM = Nilai Skor Matakuliah, NMK = Nilai Mata Kuliah

Penilaian menggunakan Penilaian Acuan Kriteria (PAK)

Course Objectives

- Memahami dasar komputer forensik berdasarkan beberapa undang-undang yang berlaku
- Memahami point penting pada forensik
- Dapat melakukan analisa terhadap beberapa jenis partisi pada harddisk
- Mampu melakukan analisa terhadap komunikasi internet
- Mampu melakukan analisa terhadap beberapa jenis data test dan multimedia
- Memahami sistem kerja steganografi, dan dapat membedakan steganografi dan kriptografi
- Mampu melakukan analisa terhadap sistem pada perangkat mobile
- Mampu memahami kasus-kasus forensik yang terjadi di dunia

Syllabus

Week		
1	Syllabus and Introduction to Computer Forensics	[Davis] Ch 1
2	Computer Fundamentals	[Davis] Ch 2
3	Volume Analysis	[Carrier] Ch 4
4	Volume Analysis 2	[Carrier] Ch 5
5	Windows Analysis	[Carrier] Ch 9 [Carrier] Ch 11
6	Linux Analysis	[Carrier] Ch 14
7	Unix Analysis	[Carrier] Ch 16
8	Internet Analysis	[Jones] Ch 2
9	File Analysis	[Cory] Ch 8
10	Steganography	[Ingemar] Ch 12
11	Steganography 2	[Ingemar] Ch 12
12	Steganography 3	[Ingemar] Ch 12
13	Mobile Forensics	[Hayes] Ch 9
14	Expert Witness	[Nelson] Ch 12 [Nelson] Ch 16

Introduction

Topics

- UU No 11/2008 tentang Informasi dan Transaksi Elektronik
- ID-SIRTII/CC → Badan Siber dan Sandi Negara
- US-CERT

Cyber Crime

Definition

- Cyber crime is a term used broadly to describe criminal activity in which computer or network are a tool, a target, or a place of criminal activity. These categories are not exclusive and many activities can be characterized as falling in one or more categories

- Cyber crime is defined any illegal act involving a computer, is systems, or its application
  - Crime directed against a computer
  - Crime where the computer contains evidence
  - Crime where the computer is used as a tool to commit the crime

A cyber crime is intentional and not accidental.

Modes of attacks

Cyber crime can be categorized into two types based on the line of attack:

- Insider attack
  - Breach of trust from employees within the organization.
- External attack
  - Attackers either hired by and insider or by an external entity to destroy the competitor’s reputation

Types of cyber crimes

Hukum di Indonesia

- Pasal 5 ayat (1) UU 11/2008

  (1) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.

- Pasal 5 ayat (2) UU 11/2008

  (2) Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.

Hukum di Indonesia

- Syarat formil bukti
- Pasal 5 ayat (4) UU 11/2008

  Ketentuan mengenai Informasi Elektronik dan/atau Dokumen Elektronik sebagaimana dimaksud pada ayat (1) tidak berlaku untuk:

  a. surat yang menurut Undang-Undang harus dibuat dalam bentuk tertulis; dan

  b. surat beserta dokumennya yang menurut Undang-Undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

Hukum di Indonesia

- Syarat Materiil Bukti
- Pasal 6 UU 11/2008

  Dalam hal terdapat ketentuan lain selain yang diatur dalam Pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi Elektronik dan/atau Dokumen Elektronik dianggap sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Hukum di Indonesia

- Syarat Materiil Bukti
- Pasal 15 UU 11/2008

  Penyelenggara sistem elektronik bertanggung jawab terhadap penyelenggaraan sistem elektronik

Hukum di Indonesia

- Syarat Materiil Bukti
- Pasal 16 ayat (1) UU 11/2008

  Penyelenggara sistem elektronik harus:

  a. dapat menampilkan kembali Informasi Elektronik dan/atau Dokumen Elektronik secara utuh sesuai dengan masa retensi yang ditetapkan dengan Peraturan Perundang-undangan;

  b. dapat melindungi ketersediaan, keutuhan, keotentikan, kerahasiaan, dan keteraksesan Informasi Elektronik dalam Penyelenggaraan Sistem Elektronik tersebut;

Kesimpulan

- Email, file rekaman atas chatting, rekaman video CCTV, rekaman audio, dan berbagai dokumen elektronik lainnya dapat digunakan sebagai alat bukti yang sah.
- Untuk mendapatkan informasi dan/atau dokumen elektronik yang layak digunakan sebagai bukti digunakan teknik forensik digital.

Forensic

- Related to answering question of a legal system.
- Computer forensics answer question of legal system related to computers

Forensic investigations

- Must be concerned with maintaining evidence integrity
- Chain of custody
- Investigating what happens on a computer system, relating to the case

Expert witness

- Forensic investigator may be called to provide testimony in a court trial
- Ethics and integrity are important

History computer forensics

- **1984 :** FBI Magnetic Media Program created. Later it become Computer Analysis and Response Team (CART)
- **1987 :** Acces Data – Cyber Forensic Company formed
- **1988 :** Creation of IACIS, the International Association of Computer Investigative Specialists

  First Seized Computer Evidence Recovery Specialists (SCERS) classes held
- **1993 :** First International Conference on Computer Evidence held
- **1995 :** International Organization on Computer Evidence (IOCE) formed
- **1997 :** The G8 countries in Moscow declared that “Law enforcement personnel must be trained and equipped to address high-tech crimes”.
- **1998 :** In March G8 appointed IICE to create international principles, guidelines and procedures relating to digital evidence
- **1998 :** INTERPOL Forensic Science Symposium
- **1999 :** FBI CART case load exceeds 2000 cases, examining 17 terabytes of data
- **2000 :** First FBI Regional Computer Forensic Laboratory established
- **2003 :** FBI CART case load exceeds 6500 cases, examining 782 terabytes of data

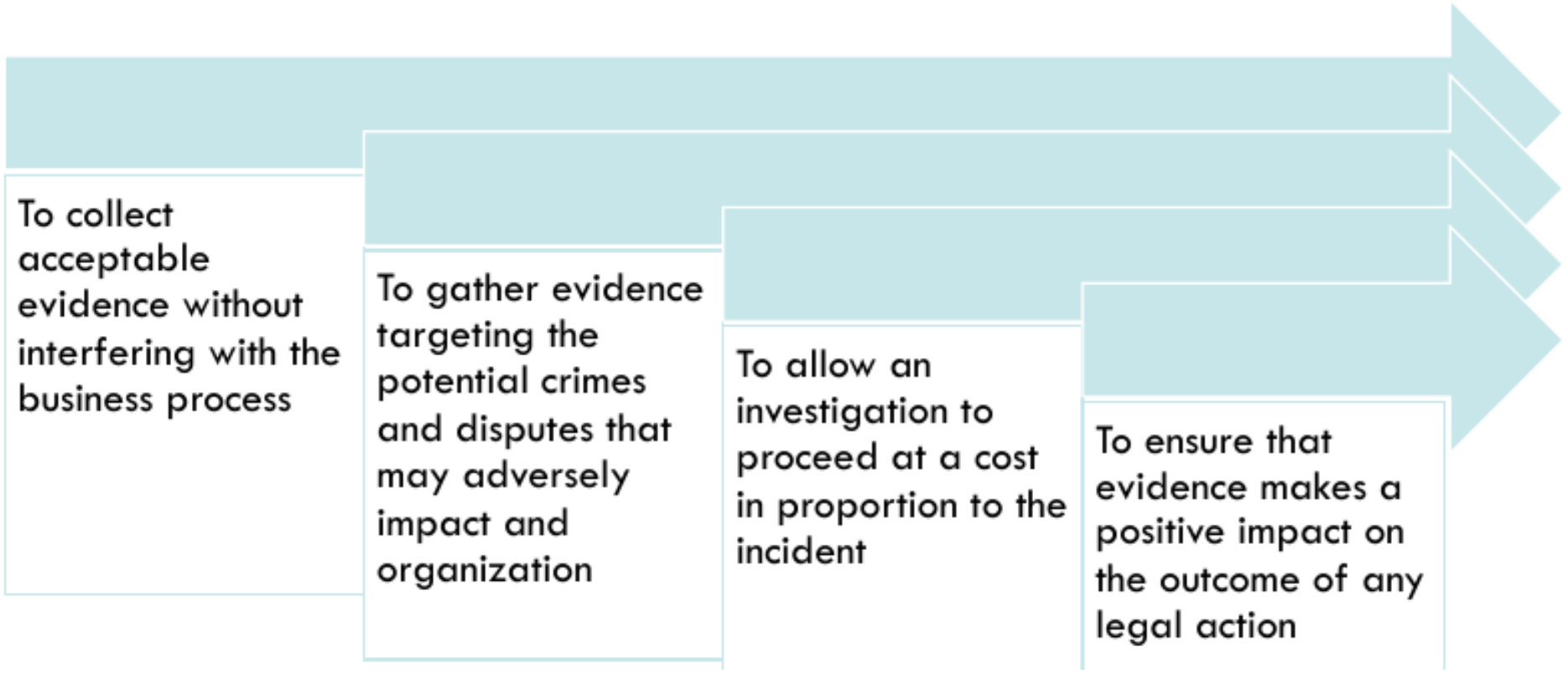
Objective of computer forensics

- To recover, analyze, and preserve computer and related materials in such a way that they can be presented as evidence in a court of law.
- To identify the evidence quickly, estimate the potential impact if malicious activity on the victim and assess the intent and identity of the perpetrator.

Benefits of forensics readiness

- Evidence can be gathered to act in the company's defense if subject to a lawsuit.
- In the event of major incident, a fast and efficient investigation can be conducted and corresponding actions can be followed with minimal disruption to the business.
- Forensic readiness can extend the target of information security to the wider threat from cybercrime, such as intellectual property protection, fraud, of extortion.
- Fixed and structured approach for storage of evidence can considerably reduce the expense and time of an internal investigation.
- It can improve and simplify law enforcement interface
- In case of a major incident, proper and in-depth investigation can be conducted

Goal of forensic readiness



Forensics readiness planning

- Define the business states that need digital evidence.
- Identify the potential evidence available.
- Determined the evidence collection requirement
- Decide the procedure for securely collecting the evidence that meets the requirement in a forensically sound manner.
- Establish a policy for security handling and storing the collected evidence
- Ensure that the observation proses is aimed to detect and prevent the important incidents
- Ensure investigative staff are capable to complete any task related to handling and preserving the evidence
- Document all the activities performed and their impact
- Ensure authorized review to facilitate action in response to the incident

Key steps in forensic investigation

- Identify the computer crime
- Collect preliminary evidence
- Obtain court warrant for seizure (if required)
- Perform first responder procedures
- Seize evidence at the crime scene
- Transport evidence to the forensic laboratory
- Create two bit stream copies of evidence
- Generate MD5 checksum on the images
- Maintain a chain of custody
- Store the original evidence in a secure location
- Analyze the image copy for evidence
- Prepare a forensic report
- Submit the report to the client
- If required, attend the court and testify as ab expert witness

Rules of forensic investigation

- Minimize the option of examining the original evidence
- Follow rules of evidence

  https://www.law.cornell.edu/rules/fre
- Do not tamper with the evidence
- Always prepare for a chain of custody
- Handle evidence with care
- Never exceed the knowledge base
- Document any change in evidence

What you should report cybercrime?

- Companies might be reluctant to share information regarding the impact to their business and the sensitivity if the data involved
- Only by sharing information with law enforcement and appropriate industry groups, cyber criminals will be identified and prosecuted.
- New cyber security threats identified, and successful attacks on critical infrastructures and economy will be prevented
- Law enforcement’s ability to identify coordinated threats is directly tied to the volume of reporting

Investigating computer crime

- Determine if an incident has occurred
- Find and interpret the clues left behind
- Conduct preliminary assessment to search for the evidence
- Search and seize the computer’s equipment
- Collect evidence that can be presented in the court of law or at a corporate inquiry

Before the investigation

- Have work station and data recovery lab
- Build investigating team
- Enter into alliance with a local district attorney
- Review policies and laws
- Notify decision makers and acquire authorization
- Assess risks
- Build a computer investigator toolkit
- Define the methodology

Build a forensic workstation

- Computer forensic approach should clearly defined before building the forensic workstation.

- The computer forensics workstation should have facilities and tools to:
  - Support hardware-based local and remote network drive duplicate
  - Validate the image and the file’s integrity
  - Identify the date and time when the files have been modified, accessed or created
  - Identify the deleted files
  - Support the removable media
  - Isolate and analyze free drive space

Building investigation team

- Keep the investigation team as small as possible to ensure confidentiality and to protect the organization against unwanted information leaks
- Determined the person who should respond to an incident for a successful internal computer investigation
- Ensure that every team member has the necessary clearance and authorization to conduct assigned tasks
- Identify team members and assign a responsibility to each team member
- Engage trusted external investigation team if your organization does not have personnel with the necessary skills
- Assign one team member as the technical lead for investigation

People involved in computer forensics

- Expert witness
- Evidence manager
- Evidence documenter
- Evidence examiner
- Attorney
- Photographer
- Incident responder
- Decision maker
- Incident analyzer

Notify Decision Makers and Acquire Authorization

- Decision maker are the people who implement policies and procedures for handling an incident
- Notify the decision maker to be authorized when there is no written incident response policies and procedures
- After the authorization, assess the situation and defined the course of action

Risk assessment

- Identify the incident and the problems caused by it.
- Characterize the incident according to its severity.
- Determine the data loss or damage caused to the computer due to the incident
- Determine the possibility of other devices and systems being affected by the incident
- Break the communication with other device to prevent the incident from spreading

Build a computer investigation toolkit

- Computer investigation toolkit contains:
  - A laptop computer with appropriate software tools
  - Operating system and patches
  - Application media
  - Write-protected backup devices
  - Blank media
  - Basic networking equipment and cables

Chain of Custody

“chain of custody is a legal document that demonstrates the progression of evidence as it travels from original evidence location to the forensic laboratory”

“original evidence should NEVER be used for analysis”

Duplicating data (imaging)

- Duplicate the data to preserve the original data.
- The data should be duplicated bit by bit to represent the same original data.
- The data can be duplicate either through hardware or software.
- The duplicated data is sent to the forensic lab for further analysis.

Handing over evidence

- All transfers must be documented
- Documentation should be complete and accurate

Inaccessible

- Provable that evidence not be accessible to anyone else.
- Evidence must be proven to be not tampered with.

Guideline

- Plan to protect evidence BEFORE you get in
- Do your work on a copy of the evidence
- Closely guard evidence
- Keep your chain of custody up to date and accurate
- Don’t keep evidence longer than necessary

Recover lost or deleted data

- Collect data
  - Collect the lost or deleted data for evidence in the internal and external device
- Software used to recover data
  - Recover My Files
  - Digital Rescue Premium
  - EASEUS Data Recovery Wizard
  - Advanced Disk Recovery
  - Total Recall

Data analysis tools

- ProDiscover
- F-Response
- FTK
- EnCase
- Sleuthkit/Autopsy
- Oxygen
- viaForensics

CERT

CERT

- Computer Emergency Response Team
- An expert group that handles computer security incidents.
- The history of CERTs is linked to the existence of malware, especially computer worms and viruses.
- The first worm in the IBM VNET was covered up.
- Morris Worm hit the Internet on 3 November 1988.
- This led to the formation of the first computer emergency response team at Carnegie Mellon University under U.S. Government contract → CERT-CC

US-CERT

- National CERT of the US.
- Responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world.
- Part of the Department of Homeland Security’s (DHS) National Protection and Programs Directorate (NPPD).

US-CERT

- Accepts, triages, and collaboratively responds to incidents
- Provides technical assistance to information system operators
- Disseminates timely notifications regarding current and potential security threats, exploits, and vulnerabilities to the public via its National Cyber Awareness System (NCAS)

Id-SIRTII/CC

- Indonesia National CERT
- Saat ini dilebur dengan Badan Siber dan Sandi Negara (BSSN)
- Didirikan 4 Mei 2007, dengan Peraturan Menteri Nomor 26/PER/M.KOMINFO/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet
- Tugas utama melakukan pengawasan keamanan jaringan telekomunikasi berbasis protokol internet.

Id-SIRTII/CC

- Melakukan sosialisasi dengan pihak terkait tentang IT security (keamanan sistem informasi)
- Melakukan pemantauan dini, pendeteksian dini, peringatan dini terhadap ancaman terhadap jaringan telekomunikasi dari dalam maupun luar negeri khususnya dalam tindakan pengamanan pemanfaatan jaringan
- Membuat/menjalankan/mengembangkan dan database log file serta statistik keamanan Internet di Indonesia.

Id-SIRTII/CC

- Memberikan bantuan asistensi/pendampingan untuk meningkatkan sistem pengamanan dan keamanan di instansi/lembaga strategis (critical infrastructure) di Indonesia
- Menjadi sentra koordinasi (Coordination Center/CC) tiap inisiatif di dalam dan di luar negeri sekaligus sebagai single point of contact
- Menyelenggarakan penelitian dan pengembangan di bidang pengamanan teknologi informasi/sistem informasi.

Id-SIRTII/CC

- Memiliki peran pendukung dalam penegakan hukum khususnya terhadap kejahatan yang memanfaatkan teknologi informasi.
- Terutama dalam penyajian alat bukti elektronik, Id-SIRTII/CC memiliki fasilitas, keahlian dan prosedur untuk melakukan analisa sehingga dapat menjadikan material alat bukti tersebut bernilai secara hukum.
- Salah satu metode analisa yang digunakan adalah forensik digital.